

# Practical Cyber Intelligence

How action-based intelligence can be an effective response to incidents



**Packt**>

[www.packt.com](http://www.packt.com)

By Wilson Bautista Jr.



**INVESTIGADOR\_Z**

**INVESTIGADOR\_Z**



# Practical Cyber Intelligence

How action-based intelligence can be an effective response to incidents

**Wilson Bautista Jr.**



**BIRMINGHAM - MUMBAI**

# Practical Cyber Intelligence

Copyright © 2018 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

**Commissioning Editor:** Gebin George

**Acquisition Editor:** Heramb Bhavsar

**Content Development Editor:** Abhishek Jadhav

**Technical Editor:** Mohd Riyan Khan

**Copy Editor:** Safis Editing

**Project Coordinator:** Judie Jose

**Proofreader:** Safis Editing

**Indexer:** Rekha Nair

**Graphics:** Tom Scaria

**Production Coordinator:** Shantanu Zagade

First published: March 2018

Production reference: 1280318

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK.

ISBN 978-1-78862-556-2

[www.packtpub.com](http://www.packtpub.com)

## INVESTIGADOR\_Z



Go to [www.packtpub.com](http://www.packtpub.com)  
and use this code in the  
checkout:

**HBBI80OFF**

**Packt>**

*To my mother, Rebecca Bautista, and my father, Wilson Bautista Sr., for their support,  
guidance, and for putting up with a lifetime of my shenanigans  
To my wife, Veronica, for her sacrifices, love, and encouragement throughout our life-journey  
To my children, Andrew, Devin, and Daniella, thank you for being my daily inspiration  
To Alex and Marta—Gracias por todo  
To my sisters, Katrina and Jasmine—Much love to you both*

*—Wilson Bautista Jr.*





`mapt.io`

Mapt is an online digital library that gives you full access to over 5,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

## Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Mapt is fully searchable
- Copy and paste, print, and bookmark content

## PacktPub.com

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at [www.PacktPub.com](http://www.PacktPub.com) and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at [service@packtpub.com](mailto:service@packtpub.com) for more details.

At [www.PacktPub.com](http://www.PacktPub.com), you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

# Contributors

## About the author

**Wilson Bautista Jr.** is a retired military officer who is the Director of IT and InfoSec at i3 Microsystems. His expertise is in the domains of InfoSec leadership, policy, architecture, compliance, and risk. He holds multiple InfoSec and IT certifications as well as a master's degree in Information Systems from the Boston University. He's an INTP on the Myers-Brigg Type Indicator test with a Driver-Driver personality. As a practitioner of Agile and SecDevOps, he develops innovative, integrated, enterprise-scale cyber security solutions that provide high value to businesses.

I'd like to thank my family's (specifically my wife) support in allowing me to finish this book, my global information security colleagues who have provided me with friendship, mentorship, and perspective on culture and business communications, and all of the military personnel in my career that helped me get where I am today. Lastly, I would like to thank wine, beer, and coffee.

## About the reviewer

**David J. Gallagher** CISSP is a senior security consultant who specializes in security intelligence and data protection solutions. With over 25 years of experience in testing, development, and business analytics across multiple industries, he has led global teams and works across multiple business units to achieve common goals and improve development/quality assurance processes. He specializes in advanced emerging threats and vulnerabilities as a security researcher and has a strong interest in understanding the vulnerabilities and developing solutions for them.

## Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit [authors.packtpub.com](https://authors.packtpub.com) and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

# Table of Contents

<b>Preface</b>	1
<b>Chapter 1: The Need for Cyber Intelligence</b>	6
<b>Need for cyber intelligence</b>	6
<b>The application of intelligence in the military</b>	8
Intel stories in history	8
The American Revolutionary War	9
Napoleon's use of intelligence	9
<b>Some types of intelligence</b>	10
HUMINT or human intelligence	10
IMINT or image intelligence	11
MASINT or measurement and signature intelligence	11
OSINT or open source intelligence	11
SIGINT or signals intelligence	12
COMINT or communications intelligence	12
ELINT or electronic intelligence	12
FISINT or foreign instrumentation signals intelligence	13
TECHINT or technical intelligence	13
MEDINT or medical intelligence	13
All source intelligence	14
<b>Intelligence drives operations</b>	15
Putting theory into practice isn't simple	19
<b>Understanding the maneuver warfare mentality</b>	22
Follow the process, the process will save you	22
What is maneuver warfare?	23
Tempo	23
The OODA Loop	25
Center of gravity and critical vulnerability	26
Surprise – creating and exploiting opportunity	27
Combined arms – collaboration	28
Flexibility	28
Decentralized command	28
<b>Summary</b>	29
<b>Chapter 2: Intelligence Development</b>	30
<b>The information hierarchy</b>	30
<b>Introduction to the intelligence cycle</b>	32
The intelligence cycle steps	33
Step 1 – Planning and direction	33
Requirements development	34
Requirements management	34



Directing the intelligence effort	35
Requirements satisfaction	36
Planning the intelligence support system	37
Step 2 – Collection	38
Step 3 – Processing	39
Step 4 – Analysis and Production	39
Step 5 – Dissemination	40
Methods	40
Channels	41
Modes	42
Dissemination architecture	42
Step 6 – Utilization	43
<b>Summary</b>	44
<b>Chapter 3: Integrating Cyber Intel, Security, and Operations</b>	45
<b>A different look at operations and security</b>	45
<b>Developing a strategic cyber intelligence capability</b>	46
Understanding our priorities	47
The business architecture	48
The data/application architecture	48
Technology architecture	48
Application of the architectures and cyber intelligence	48
A look at strategic cyber intelligence – level 1	50
<b>Introduction to operational security</b>	51
OPSEC step 1 – identify critical information	51
OPSEC step 2 – analysis of threats	52
OPSEC step 3 – analysis of vulnerabilities	52
OPSEC step 4 – assessment of risk	52
OPSEC step 5 – application of appropriate countermeasures	54
<b>OPSEC applicability in a business environment</b>	55
<b>Cyber intel program roles</b>	56
Strategic level – IT leadership	57
Strategic level – cyber intelligence program officer	57
Tactical level – IT leadership	58
Tactical level – cyber intelligence program manager	59
Operational level – IT leadership	60
Operational level – cyber intelligence analysts	60
<b>Summary</b>	61
<b>Chapter 4: Using Cyber Intelligence to Enable Active Defense</b>	62
<b>An introduction to Active Defense</b>	63
<b>Understanding the Cyber Kill Chain</b>	64
<b>General principles of Active Defense</b>	65
Active Defense – principle 1: annoyance	66
Active Defense – principle 2: attribution	66
<b>Enticement and entrapment in Active Defense</b>	67

Scenario A	67
Scenario B	68
<b>Types of Active Defense</b>	68
Types of Active Defense – manual	69
Types of Active Defense – automatic	69
<b>An application of tactical level Active Defense</b>	70
<b>Summary</b>	72
<b>Chapter 5: F3EAD for You and for Me</b>	74
<b>Understanding targeting</b>	75
<b>The F3EAD process</b>	79
<b>F3EAD in practice</b>	81
<b>F3EAD and the Cyber Kill Chain</b>	87
Cyber Kill Chain and OODA loop	87
Cyber Kill Chain and OPSEC	89
Cyber Kill Chain and the intelligence cycle	91
Cyber Kill Chain and F3EAD	92
<b>Application of F3EAD in the commercial space</b>	92
Limitations of F3EAD	93
<b>Summary</b>	94
<b>Chapter 6: Integrating Threat Intelligence and Operations</b>	95
<b>Understanding threat intelligence</b>	95
<b>Capability Maturity Model – threat intelligence overview</b>	98
Level 1 – threat intelligence collection capability	99
Phase initial	100
Example 1 – Open Threat Exchange – AlienVault	100
Example 2 - Twitter	107
Example 3 - Information Sharing and Analysis Centers	111
Example 4 - news alert notifications	112
Example 5 - Rich Site Summary feeds	113
Phase A	114
Example 1 - Cisco – GOSINT platform	116
Example 2 - The Malware Information Sharing Platform project	116
Phase B	116
Phase C	117
Level 2 – Threat Information Integration	118
Phase initial	119
Phase A	120
Categorization of items that are applicable to multiple teams	121
Phase B	121
Phase C	122
<b>Summary</b>	123
<b>Chapter 7: Creating the Collaboration Capability</b>	124
<b>Purpose of collaboration capability</b>	124
Formal communications	125

Informal communications	126
Communication and cyber intelligence process	126
Methods and tools for collaboration	128
Service level agreements and organizational level agreements	128
Responsible accountable supporting consulted informed matrix	129
Using key risk indicators	129
<b>Collaboration at the Strategic Level</b>	131
Executive support	133
Policies and procedures	133
Architecture	134
Understanding dependencies	134
Prioritized information	136
Intelligence aggregation	137
Intelligence reconciliation and presentation	138
<b>Collaboration at the Tactical Level</b>	140
Breaking down priority information requirements	140
Application of the theory	141
Theory versus reality	142
Creating the tactical dashboard	144
<b>Collaboration at the Operational Level</b>	147
<b>Summary</b>	149
<b>Chapter 8: The Security Stack</b>	150
<b>Purpose of integration – it's just my POV</b>	150
<b>Core security service basics</b>	151
<b>Security Operations Center</b>	153
The spider	154
Capabilities among teams	155
<b>Capability deep dive – Security Configuration Management</b>	156
Security Configuration Management – core processes	158
Security Configuration Management – Discovery and Detection	159
Security Configuration Management – Risk Mitigation	159
Security Configuration Management – Security State Analysis	160
Security Configuration Management – Data Exposure and Sharing	161
<b>Prelude – integrating like services</b>	163
<b>Integrating cyber intel from different services</b>	166
Overview – red team methodology	166
Red team – testing methods	167
White box	167
Gray box	167
Black box	167
Red team constraints	168
Red team – graphical representation	169
Data integration challenges	170
The end user perspective	170

The service level perspective – cyber intelligence – Data Exposure and Sharing	171
The SOC perspective	173
<b>Capability Maturity Model – InfoSec and cyber intel</b>	174
Capability Maturity Model - InfoSec and cyber intel – initial phase	175
Capability Maturity Model - InfoSec and cyber intel – Phase A	176
Capability Maturity Model - InfoSec and cyber intel – Phase B	177
Capability Maturity Model - InfoSec and cyber intel – Phase C	178
<b>Collaboration + Capability = Active Defense</b>	179
<b>Summary</b>	179
<b>Chapter 9: Driving Cyber Intel</b>	180
<b>The gap</b>	180
<b>Another set of eyes</b>	181
The logic	182
Event	183
Incident	184
Mapping events and incidents to InfoSec capabilities	184
<b>Capability Maturity Model – security awareness</b>	186
Capability Maturity Model - security awareness Phase - Initial	187
Capability Maturity Model - security awareness – Phase A	187
Capability Maturity Model - security awareness – Phase B	188
Capability Maturity Model - security awareness – Phase C	190
Capability Maturity Model - security awareness – Phase C +	191
Just another day part 1	192
<b>Summary</b>	193
<b>Chapter 10: Baselines and Anomalies</b>	195
<b>Setting up camp</b>	195
Baselines and anomalies	196
<b>Continuous monitoring – the challenge</b>	197
Part 1	197
Part 2	198
Part 3	200
<b>Capability Maturity Model – continuous monitoring overview</b>	201
Level 1 – phase A	202
Level 1 – phase B	203
Level 1 – phase C	204
<b>Capability Maturity Model – continuous monitoring level 2</b>	205
Scenario 1 – asset management/vulnerability scanning asset inventory	206
Phase initial	208
Information gathering	208
Developing possible solutions	209
Phase A	210
Procedure RASCI (example)	210
Phase B	210
Regional data centers	211
Local office environment	212



Phase C	212
Scenario 2 – security awareness/continuous monitoring/IT helpdesk	214
Phase initial	215
Information gathering	216
Developing possible solutions	217
Phase A	217
Procedure RASCI (example)	218
Phase B and C – sample questions	218
Just another day part 2	219
<b>Summary</b>	221
<b>Chapter 11: Putting Out the Fires</b>	222
<b>Quick review</b>	222
<b>Overview – incident response</b>	223
Preparation and prevention	224
Detection and analysis	225
Containment, eradication, and recovery	225
Post-incident activity	225
Incident response process and F3EAD integration	226
Intelligence process tie-in	227
<b>Capability Maturity Model – incident response</b>	228
Initial phase	228
Phase A	228
Phase B	229
Phase C	231
<b>Summary</b>	233
<b>Chapter 12: Vulnerability Management</b>	234
<b>A quick recap</b>	235
<b>The Common Vulnerability Scoring System calculator</b>	236
Base metric group	236
Temporal metric group	238
Environmental metric group	238
CVSS base scoring	239
Metrics madness	240
<b>Vulnerability management overview</b>	240
<b>Capability Maturity Model: vulnerability management – scanning</b>	242
Initial phase	243
Phase A	245
Phase B	246
Phase C	247
<b>Capability Maturity Model: vulnerability management – reporting</b>	248
Initial phase	248
Phase A	250
Phase B	251
Phase C	252

<b>Capability Maturity Model: vulnerability management – fix</b>	252
Initial phase	254
Phase A	255
Phase B	256
Phase C	258
<b>Summary</b>	260
<b>Chapter 13: Risky Business</b>	261
<b>Risk overview</b>	261
Treating risk	261
Risk tolerance and risk appetite	262
<b>Labeling things platinum, gold, silver, and copper</b>	263
Differentiating networks	264
<b>Taking a different look at risk</b>	264
Review of threat intelligence integration	265
Capability Maturity Model: risk phase – initial	266
Improving risk reporting part 1	267
Capability Maturity Model: risk phase – final	268
Improving risk reporting part 2	269
Open source governance risk and compliance tools	270
Binary Risk Assessment	270
STREAM cyber risk platform	270
Practical threat analysis for information security experts	270
SimpleRisk	270
Security Officers Management and Analysis Project	271
<b>Summary</b>	271
<b>Chapter 14: Assigning Metrics</b>	272
<b>Security configuration management</b>	272
Developing the risk score	273
Working in key risk indicators	275
<b>Summary</b>	277
<b>Chapter 15: Wrapping Up</b>	278
<b>Just another day part 3</b>	278
<b>Lessons learned</b>	279
<b>Other Books You May Enjoy</b>	282
<b>Index</b>	285

---

# Preface

When I was first asked to write this book, it was supposed to be about applying military targeting methodology to threat intelligence. However, when I started writing, I began to ask:

- How is threat intelligence beneficial to organizations?
- How can we create value from threat intelligence?

So, the topic began to change to something I believe that is missing in how we operate as IT organizations. Threat intelligence is worthless to organizations if it is not applicable to them. Once it becomes applicable to an organization, it has to be communicated to someone to take action on. It sounds so simple but when we look further, there are so many touch points with different parts of the organization and different processes between teams, that the topic eventually morphed into what I call cyber intelligence.

If you spend some time looking at the cyber security news on your social media, you can read about the latest exploitation, the need for more cyber security professionals, and how insecure we are. It feels like sensationalism and further drives paranoia of being labeled "the next victim" for senior leadership. How many times have we seen senior leadership step down because of a breach? Perhaps some breaches were due to neglect, but I'm keen to think that we (collectively) are riddled with archaic and bureaucratic business processes that do not allow flexibility for decentralized decision making.

Does your IT Operations and IT Security leadership act as one in decision making for the overall IT decisions, using information that impacts each side? If they do, then you should just put this book down because this isn't for you. If they don't, then you understand the pain of when separation of duties impact how quickly things get done.

In the military, intelligence capability allows a commander to understand the environment around them in order to make decisions. This book is about how we can take a variation of military intelligence processes and apply it across the organization. Whether you are an entry-level analyst or a senior manager, there is something for you to learn and put into practice right away in your organization.

## Who this book is for

The main audience of this book is for mid-level to senior management professionals in small to medium businesses that are looking to improve their IT and InfoSec operations utilizing a variation of military processes and concepts. It is also meant for future leaders in the industry to take another look at a holistic approach to improving IT operations in their organizations. No prior management or technical experience is assumed.

## What this book covers

Chapter 1, *The Need for Cyber Intelligence*, introduces a brief history of intelligence use in the military, the different types of intelligence, and the military mindset.

Chapter 2, *Intelligence Development*, introduces the intelligence cycle, shows you how intelligence is developed, and how to develop priority information requests.

Chapter 3, *Integrating Cyber Intel, Security, and Operations*, introduces OPSEC and lays the foundation for understanding how cyber intelligence can be integrated into Information Security and IT operations.

Chapter 4, *Using Cyber Intelligence to Enable Active Defense*, introduces the Cyber Kill Chain and develops another look into how we can utilize cyber intelligence to enable proactive defense measures.

Chapter 5, *F3EAD For You and For Me*, introduces how we can use the Find, Fix, Finish, Exploit, Analyze, and Disseminate process that is deployed for high value targets and it's applicability to the Cyber Kill Chain.

Chapter 6, *Integrating Threat Intelligence and Operations*, takes a deeper look into how we can develop meaningful and actionable information to stakeholders through incorporating threat intelligence information.

Chapter 7, *Creating the Collaboration Capability*, gives an overview of how we can create communication channels to provide cyber intelligence information throughout the organization.

Chapter 8, *The Security Stack*, provides a view on how information captured from different security capabilities can be developed into cyber intelligence that supports sound decision making.



Chapter 9, *Driving Cyber Intel*, goes into detail on how we can enable the users as another means of collecting and reporting information to develop intelligence packages.

Chapter 10, *Baselines and Anomalies*, highlights the complexity of reporting, teaches you how to take a look at entities and their processes horizontally and vertically, and provides a method to integrating an end-to-end continuous monitoring capability.

Chapter 11, *Putting Out the Fires*, introduces ways to improve incident response through developing good intelligence communication channels.

Chapter 12, *Vulnerability Management*, goes into more detail on a specific capability within InfoSec and how to improve what information gets into the hands of the stakeholders for action.

Chapter 13, *Risky Business*, gives a broad overview of risk and how we can use risk management tools and techniques to further improve the information being passed to stakeholders for action.

Chapter 14, *Assigning Metrics*, introduces a concept in assigning risk metrics and key risk indicators for an end-to-end process.

Chapter 15, *Wrapping Up*, provides a broad overview of the preceding chapters and takes you through an ideal situation, where a cyber intelligence capability is fully functional within an organization.

## To get the most out of this book

You will want to read this book from start to finish as I've written each chapter to build off of each other. Each concept you learn in these chapters will relate to one another in some fashion. If you don't, you'll find yourself completely lost as a lot of what has gone into this have customized processes that have worked or is working in the organizations and teams I've helped develop.

So I want you to read this book with an open mind and ask yourself "what if this could work?" I only ask you to do this because I believe that we should all be on a path to improving our own processes (IT and business) within our organizations. The amount of breaches in 2017 alone is an indicator that some organizational processes don't work.

1. We cannot accept "this is how it has always been done" anymore
2. We need to reduce friction between each other
3. We need to increase the speed of decision making
4. We need to reduce the risk of exploitation

This book is another way to enable sound decision making at all levels by developing an intelligence capability between IT teams using the resources that we already have. It is definitely a "bastardization" of military and civilian processes that have been put together to "make it work" for my teams. This book is not a solution, but a way to taking what we already know and trying to make an organization's collaboration and communication more efficient. By doing this, we are one more step closer in reducing the risk of exploitation to our organization.

Let's get started.

## Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: [http://www.packtpub.com/sites/default/files/downloads/PracticalCyberIntelligence\\_ColorImages.pdf](http://www.packtpub.com/sites/default/files/downloads/PracticalCyberIntelligence_ColorImages.pdf).

## Conventions used

There are a number of text conventions used throughout this book.

**Bold:** Indicates a new term, an important word, or words that you see onscreen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: "Select **System info** from the **Administration** panel."



Warnings or important notes appear like this.



Tips and tricks appear like this.

## Get in touch

Feedback from our readers is always welcome.

**General feedback:** Email [feedback@packtpub.com](mailto:feedback@packtpub.com) and mention the book title in the subject of your message. If you have questions about any aspect of this book, please email us at [questions@packtpub.com](mailto:questions@packtpub.com).

**Errata:** Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit [www.packtpub.com/submit-errata](http://www.packtpub.com/submit-errata), selecting your book, clicking on the Errata Submission Form link, and entering the details.

**Piracy:** If you come across any illegal copies of our works in any form on the Internet, we would be grateful if you would provide us with the location address or website name. Please contact us at [copyright@packtpub.com](mailto:copyright@packtpub.com) with a link to the material.

**If you are interested in becoming an author:** If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit [authors.packtpub.com](http://authors.packtpub.com).

## Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions, we at Packt can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about Packt, please visit [packtpub.com](http://packtpub.com).

# 1

# The Need for Cyber Intelligence

*"Business intelligence (BI) leverages software and services to transform data into actionable intelligence that informs an organization's strategic and tactical business decisions."*

– <https://bicorner.com/2017/12/01/what-is-bi-business-intelligence-definition-and-solutions/>

In this chapter, you will learn about the necessity of transforming data into actionable intelligence. You will also learn that there is a difference between cyber intelligence and cyber threat intelligence. In this chapter, we will review:

- The need for cyber intelligence
- The application of intelligence in the military
- Different types of intelligence
- How intelligence drives operations
- Introduction to maneuver warfare

We will take a look at how intelligence has been used in the military and how the military incorporates intelligence to plan for missions. We will review high level concepts of maneuver warfare and use these as a new approach to understanding how to utilize information, so we can remove uncertainty and be proactive against threats to our environment.

## Need for cyber intelligence

Are we using the data from our security software and services to transform the data into actionable intelligence that informs an organization's strategic and tactical business decisions?

In a recent SANS survey, phishing (72%), spyware (50%), ransomware (49%), and Trojans (47%) are the threats most seen by respondents' organizations in 2017. Organizations are being attacked daily by numerous threats. Alert fatigue is developing from the overwhelming amount of data to sort through and understand where to start remediating. There are many tools to discover vulnerabilities and potential threat vectors. In our world, sorting through this information is a challenge as there are always competing interests within the information security organization and the business. Leaders must strike the right balance of security and operations, as well as risk and compliance.

From textbooks, we've been taught that in security we should identify, contain, and eradicate vulnerabilities on the network so that we reduce the risk of being compromised. We've been led to believe that security will save the company from the bad guys and that we will be given the power to do that. However, the reality is much more complex, with **chief information security officer (CISO)** and managers balancing budgets, engineers trying to get change requests approved, lack of human resources due to burn out or availability, dealing with vendors, company culture, world culture, and organization processes hindering our ability to respond to these threats that can cause a considerable risk to the organization and its information. Uncertainty, fog of war, and friction are a part of life as a security professional.

The questions that come to mind are as follows:

- How do we reduce this uncertainty?
- What is the priority?
- How do we focus our efforts?
- How do we provide actionable information so that I can get my stakeholders on board?
- How do I train my team?
- Where do we begin to remediate? Can I even remediate?

The threat landscape is always changing. Every day we hear of a new group of hackers that are targeting systems that are vulnerable to X and Y. There are reports of nation-state cyber espionage attempts on the national media. The scary thing is that there may be an attack happening and no one has caught on. There seems to be general paranoia about who will be next and if that day comes, I hope it isn't me.

This book is meant to help executives and analysts understand their role in raising the bar, from effective communication of the state of their security, to gathering information about their environment. How we address this is by building a **cyber intelligence capability** that provides accurate information about the exploitation potential of vulnerabilities that exist within the environment by known adversaries, resulting in appropriate measures taken to reduce the risk to organizational property.

## The application of intelligence in the military

*"Intelligence is the ability to gain knowledge or a skill."*

**Cyber threat intelligence** is an analysis of an adversary's intent, opportunity, and capability to do harm. This is a discipline within information security that requires a specific skill set and tools used by threat intelligence analysts.

**Cyber intelligence** is the ability to gain knowledge about an enterprise and its existing conditions and capabilities in order to determine the possible actions of an adversary when exploiting inherent critical vulnerabilities. It uses multiple information security disciplines (threat intelligence, vulnerability management, security configuration management, incident response, and so on) and tool sets to gather information about the network through monitoring and reporting to allow decision makers at all levels to prioritize risk mitigation.

Over the past few years, we've seen a list of new certifications focusing on penetration testing and ethical hacking. These skills are perfect for the personnel on the ground looking for vulnerabilities within organizations using tools and methods that a malicious actor would use. There are so many tools that provide the ability to look, find, monitor, and report on their environment. How do we apply those same concepts to the architecture of an enterprise? How do we think like an attacker and build the capability within our architectures with the capability to mitigate and/or reduce the risk? The goal of the following few sections is to create a proactive defense mindset and lay the foundation for building a cyber intelligence capability architecture in your organization.

## Intel stories in history

*"Intelligence drives operations"*

– Gen A.M. Gray 29th Commandant of the United States Marine Corps

Having the capability to gather information on an adversary has been in practice in the art of warfare for centuries. The importance of using intelligence helps guide military commanders' decision-making for future operations. Military organizations have sections dedicated to operating their intelligence capability. In order to understand how to apply intelligence in our security operations, we should have an understanding of what intelligence is and how it has been used in military history.

## The American Revolutionary War

*"Washington did not really outfight the British. He simply out-spied us."*

*– British intelligence officer*

In order to combat an intimidating and larger British force, General George Washington needed to do something to even the playing field. The odds were against the fledgling American army as they were understaffed, under trained, and had little to no budget. The answer to this problem was espionage.

The Americans needed to know about their adversary's actions in order for them to win the Revolutionary War. Washington needed patriots who were close to the British at all levels of society. So he employed ordinary people, such as farmers, tailors, housemaids, and other patriots to build spy rings. Additionally, he turned British spies into double agents. The Americans had established multiple networks of agents passing information between the lines, informing Washington of the whereabouts of the British and what their next plans were. As mail was intercepted, General Washington proposed to, *"...contrive a means of opening them without breaking the seals, take copies of the contents, and then let them go on. By these means we should become masters of the whole plot."* The intelligence that was gathered was used to conduct a massive man-in-the-middle / deception operation, actively changing the narrative, causing confusion, and disrupting communications for the British.

## Napoleon's use of intelligence

Anyone who has opened a history book has heard of Napoleon Bonaparte. As a military leader, he led multiple campaigns during the French Revolutionary Wars and went on to lead France against other nations during the Napoleonic Wars. His military innovations in military tactics at the time are now studied by many military organizations and he is known to many as one of the greatest commanders in history.

What was Napoleon's take on the importance of intelligence? A study of *The Jena Campaign of 1805* by Jay Luvaas stated that Napoleon directed intelligence gathering and actions, as follows:

*"To reconnoiter accurately defiles and fords of every description. To provide guides that may be depended on. To interrogate the cure and postmaster. To establish rapidly a good understanding with the inhabitants. To send out spies. To intercept public and private letters. To translate and analyse their contents. In a word, to be able to answer every question of the general-in-chief when he arrives at the head of the army. A general should neglect no means of gaining information of the enemy's movements, and, for this purpose, should make use of reconnaissance, spies, bodies of light troops commanded by capable officers, signals, and questioning deserters and prisoners."*

Napoleon had an understanding that intelligence is multi-faceted and was not limited to understanding the strengths and weaknesses of the opponent. He wanted to use the information gathered about the land to find the best place to move his army, to have the advantage and know where to avoid. His officers didn't send out spies arbitrarily to any town to gather information, they sent them to strategic areas of interest.

## Some types of intelligence

To better understand the importance of an intelligence capability in the military, we must also recognize the different disciplines.

### HUMINT or human intelligence

HUMINT is the collection by a trained HUMINT collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources as a tool and a variety of collection methods, both passive and active, to gather information to satisfy the commander's intelligence requirements and cross-cue other intelligence disciplines.

HUMINT operations collection can be executed overtly or by clandestine operations.

Overt collection is normally done in the open and through legal means without concealment. Clandestine collection is normally done by personnel who are trained in the foreign languages and cultures of the country they are assigned so that collection efforts are secret and that they mix in with the local populace.



Examples:

- Espionage
- Interrogation of personnel
- Patrolling
- Reconnaissance

## **IMINT or image intelligence**

IMINT means the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials.

Examples:

- Aerial reconnaissance photos
- Satellite imagery

## **MASINT or measurement and signature intelligence**

MASINT is technically derived intelligence that detects, locates, tracks, identifies, and/or describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the additional advanced processing and exploitation of data derived from IMINT and SIGINT collection.



You can find the subdisciplines of MASINT at: <https://www.globalsecurity.org>.

## **OSINT or open source intelligence**

OSINT is public information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience in order to address a specific question.

Examples:

- Anything that can be found on the internet: Facebook, Twitter, LinkedIn

- Information that is acquired from newspapers, magazines, television, radio, and so on
- Whitepapers, conference presentations, and public studies
- Photos

## **SIGINT or signals intelligence**

SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.

Examples:

- Intercepting messages and using cryptanalysis to decipher them
- Listening to who is communicating and how many times they are communicating to a person or group

## **COMINT or communications intelligence**

A sub-discipline within SIGINT where technical and intelligence information is derived from interception of foreign communications by other than the intended recipients; it does not include the monitoring of foreign public media or the interception of communications obtained during the course of counterintelligence investigations within the United States.

For example: listening in, analyzing, and decoding military radio traffic, teletype, and fax signals.

## **ELINT or electronic intelligence**

Technical and geolocation intelligence derived from foreign non-communication, electromagnetic radiation emanating from anything other than nuclear detonations or radioactive sources that do not contain speech or text.

Examples:

- Analysis of beeps on magnetic tape
- Analysis of emanations of a source to identify what it is and where it is coming from

## **FISINT or foreign instrumentation signals intelligence**

A subcategory of SIGINT, COMINT, and MASINT that consists of technical information and intelligence derived from the interception of foreign electromagnetic emissions associated with the testing and operational deployment of non-United States aerospace, surface, and subsurface systems.

Examples:

- Analysis of machine to machine language
- Remote access and control transmissions, such as from remote keyless systems, wireless doorbells, and wireless traffic light control systems

## **TECHINT or technical intelligence**

Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages.

Examples:

- Reconnaissance missions showing that the adversary has a new aircraft that is capable of doing X and Y
- Competing businesses developing a new product that is capable of reducing X percentage of work and decreasing Y percentage of price

## **MEDINT or medical intelligence**

The category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information that is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors.

Example:

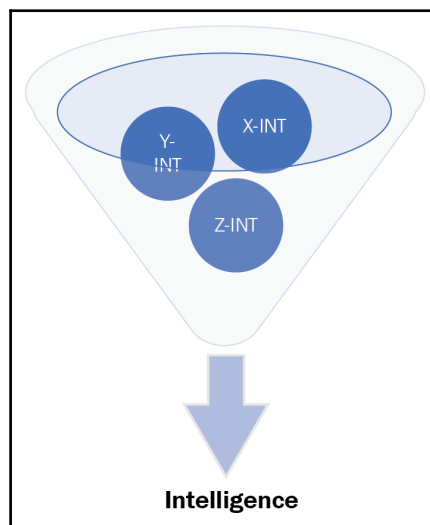
- Understanding where medical facilities are within an area and what their capabilities are

## All source intelligence

The intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open source information, in the production of intelligence. All-source intelligence is a separate intelligence discipline, as well as the name of the function used to produce intelligence from multiple intelligence or information sources.

Examples:

- Drives collection to answer the priority information requirements
- Provides the enemy situation
- Provides intelligence summary reports and other intelligence reports
- Supports situational understanding
- Provides predictive estimates of enemy actions; specifically, enemy courses of action
- Provides all source target packages



## Intelligence drives operations

Operations rely on sound decision-making from leaders who are capable of making them. Like many IT projects, we don't go from idea to reality in seconds. It takes planning, managing stakeholders, getting people on board with the idea, massaging egos, and so on. But how did we get that idea in the first place? It also didn't just pop up from nowhere.

Ideas are born from trying to fix or improve something that we've dealt with using data that we believe may or may not be true. Babies do not learn how to walk and crawl on their own. They see a toy, they get frustrated because they can't get it, and then they learn to crawl. They see people walking on two feet, practice, struggle to stand, and eventually take their first steps. This is because they had a problem, used data from their own experiences, tested their theories, and came to conclusions.

Every organization has a vision and a mission statement that is meant to be the core of its existence. It is the same way business leaders communicate their intent to their employees.

The military has a concept called **commander's intent**, which mirrors the intention of that particular unit, brigade, regiment, division, or corps. It drives all of the supporting units to a single unified purpose of meeting that intent so that they can complete the mission.



Commanders have a lot of responsibility and don't want to make a decision on every piece of data coming at them. They make decisions based on specific pieces of data that pertain to solving a specific question. Gathering of that information for the commander is based on a term called **Priority Information Requirements (PIRs)**. These PIRs are what drives intelligence gathering operations as it provides guidance on what information is the most important to the commander so that they can plan for the next steps.

Good PIRs have three criteria:

- They ask only one question
- They focus on a specific fact, event, or activity
- They provide intelligence required to support a single decision

Military examples:

- What size force is defending objective A?
- Will enemy battalion X arrive before Y time on Z date?
- How many obstacles are on D road that will impede our movement?

Can we not apply the same logic within our IT/InfoSec organizations? The idea is no different to gathering metrics for **Key Performance Indicators (KPIs)**. When we have targets, we need to measure them and analyze them to see whether or not we have met or missed the mark. Either way, the information gathered will decide what we do next.



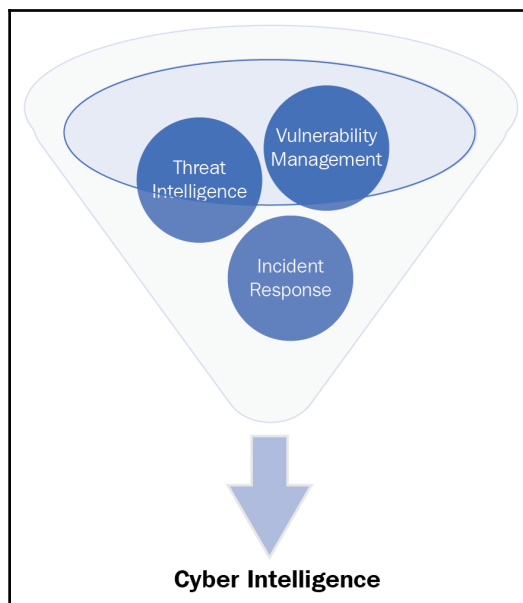
Having a top-down approach when defining specific information to be derived from our security tools, will fuel our intelligence capabilities when evaluating the best way to move forward.

Let's use the Center for Internet Security Controls top five as commercial PIR examples. These are high level PIRs that can be filtered down to the tactical and operational teams to answer:

1. Do we have an inventory of authorized and unauthorized devices?
  - **Tactical:** Do we have a complete list of authorized devices?
    - **Operational:** How are we continuing to gather this list?
  - **Tactical:** Do we have the capability of identifying unauthorized devices?
    - **Operational:** Where are we finding these devices?
2. Do we have an inventory of authorized and unauthorized software?
  - **Tactical:** Do we have a list of authorized software?
  - **Tactical:** What are our most critical applications?
    - **Operational:** Where are these located?
  - **Tactical:** How are we protecting these?
    - **Operational:** What security tools are in place to ensure that the information does not get compromised?
  - **Tactical:** Do we have a list of unauthorized software?
    - **Operational:** Where do the systems with this software exist?

3. Do we have secure configurations for hardware and software?
  - **Tactical:** What systems and software have secure configurations?
    - **Operational:** How are we monitoring any deviation from the standard?
  - **Tactical:** What systems and software do not have secure configurations?
    - **Operational:** How do we develop secure configurations for systems and software?
4. Do we have a continuous vulnerability assessment and remediation capability?
  - **Tactical:** Do we have the capability of scanning for vulnerabilities in all areas of the network?
    - **Operational:** Do we have an accurate list of subnets allocated to the organization?
  - **Tactical:** Do we have the capability to patch vulnerabilities that have been found?
    - **Operational:** How can we influence application/system owners to patch when we do not have the authority to tell them to do it?
5. Do we control the use of administrative privileges?
  - **Tactical:** Do we have a list of privileged users?
    - **Operational:** Who are they?
  - **Tactical:** What are the levels of privileged user access?
    - **Operational:** Who has what level of access?

Once we begin to look at the different functions of an information security organization, we can treat them as separate disciplines of intelligence gathering internally and externally. We begin to see that each security team utilizes the answers from high level PIRs to provide the status to the senior leadership of the organization.



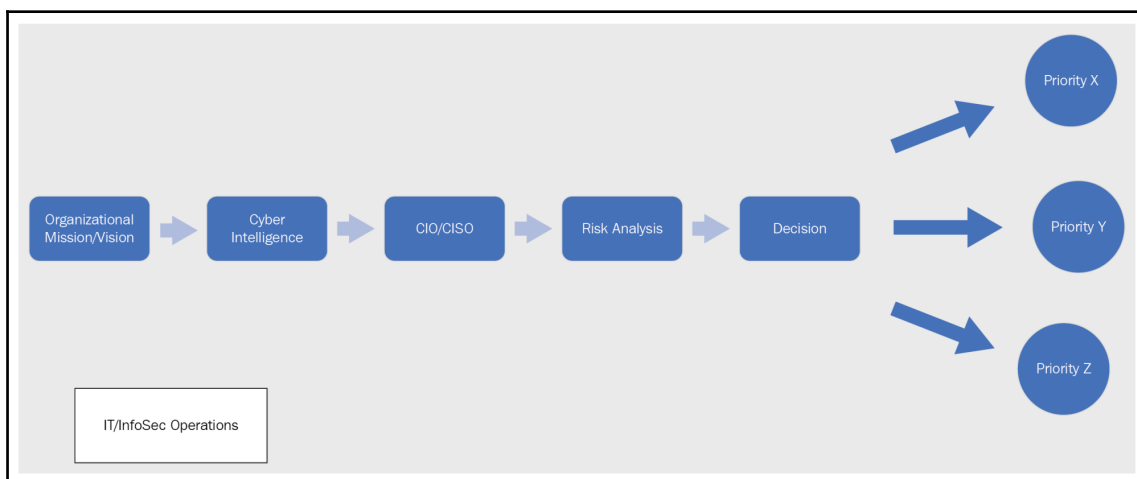
This would provide the capability of an organization's leadership to understand the environment, apply the risk management processes, and make a decision on where to dedicate resources:



The reality is that it is difficult to begin processing the information from multiple sources to make a *big picture* or *battlespace*. We have to accept that there will be ambiguity and not-clearly defined targets. Building this capability will take time, collaboration, and a mindset change at all levels.



Flow of IT/InfoSec operations can be seen in the following image:

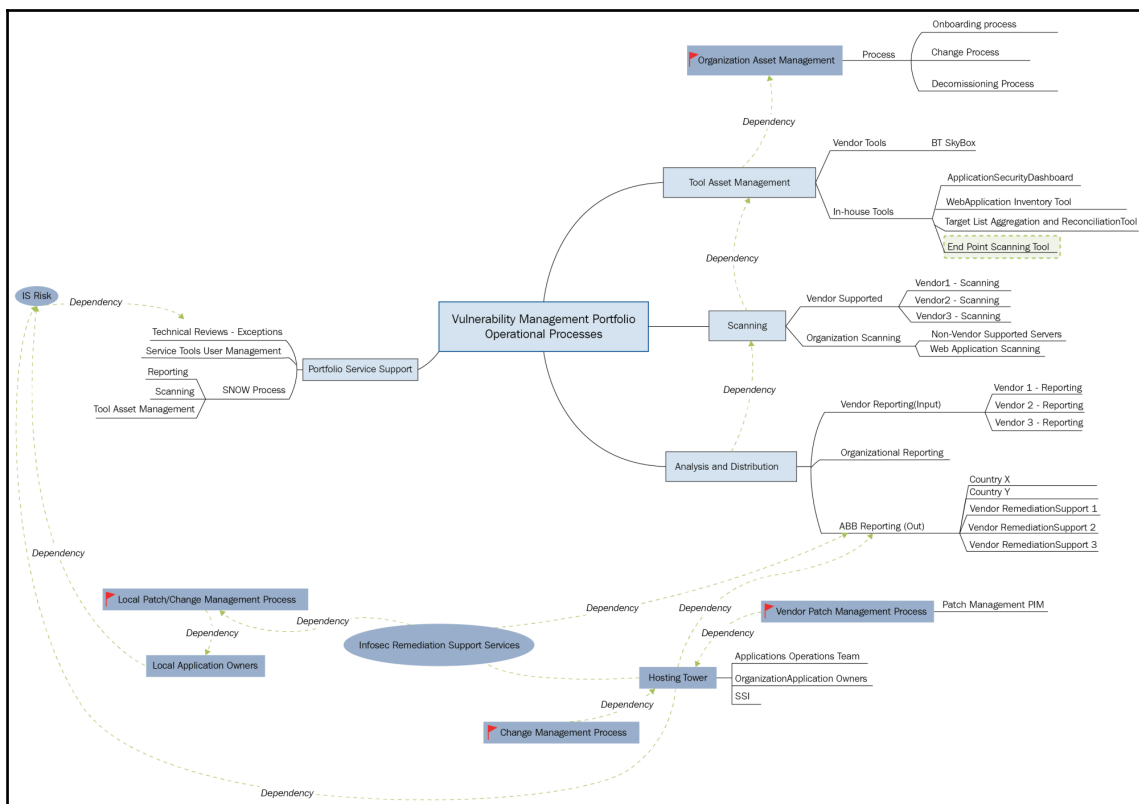


In later chapters, we will go into some suggested capability maturity models for the different disciplines in security so that we can lay the foundation to build an intelligence capability.

## Putting theory into practice isn't simple

Rachel was a friend that was asked by a CISO to solve a problem. At the time, her marching orders were simple. Identify vulnerabilities and report vulnerabilities. But she wondered, what does identifying and reporting vulnerabilities solve? It doesn't solve anything. She had identified a problem but there was no means to solve it. Why? She was in a huge environment stretching across the globe that required change requests to be put in and multiple entities to sign off on a single patch.

Let's not even talk about the sheer amount of patches that needed to be reviewed and approved by non-technical staff, or the fear of impacting operations. There isn't a simple solution for this problem as there were other dependencies and unknowns, such as vendors and shadow IT. Her team did not have the ability to patch, which was a huge problem. It was difficult to get anything done. There was an organizational culture change that needed to be addressed. There were policies and procedures that needed to be updated. There were multiple problems in security that need to be prioritized. There were organizational changes, personnel moves, people leaving, people on-boarded, that is, more dependencies.



Maybe a single set of services look like the preceding mind map. The IT operations and IT security operations in the organization were a complex beast. But this was just a small problem in the bigger picture.

The real question was, how does your piece of the pie keep this organization safe? Well, her piece of the pie didn't keep her organization safe. The reality was that she had a team that highlighted known vulnerabilities and provided inputs to a risk metric that was presented on a global risk dashboard. On this dashboard were other security teams' pieces of the pie. A dashboard that consisted of red, amber, and green. The more red there was meant the more you were going to be harassed. More green meant that you weren't going to be harassed. Sound familiar?

Does more green really mean that you are at less risk? Does being more red really mean that you are a risk?

The data isn't complete. Maybe it told her that there are certain areas that need attention, but what this didn't tell her is where she needed to pay attention the most as a service manager. More on her story later.

I can't imagine how it would be for the CISOs or security professionals who have to manage all of this data. It's like looking at a ship and knowing all of the holes but not knowing where to plug up first, all while asking for an additional supply of corks to use to fix them, because you may have five or six. Wait! One or two corks are rotted. It's a never-ending cycle of which holes to plug up first. What gator is closest to the boat? Which fiery hoop do I jump through now?

If organizations were castles, we'd have to man the walls and keep a constant eye out for trouble. But castles get breached and it doesn't matter how big or well defended the castle is because there will always be a blind spot. Where are your security blind spots?

So how is it that companies with plenty of resources for tools and personnel still get breached? How many conferences have I been to where I've seen the next big thing in security? There are tools for cyber deception. There are tools that use artificial intelligence and machine learning. We have heuristic analysis and two-factor authentication. NextGen AV! Defense in depth! We have best practices, certifications, and bootcamps. We are manning our castles with personnel who have the best equipment and training but we've still seen major institutions get hacked left and right. Target, JP Morgan, Dun & Bradstreet, they may or may not have been compliant, but they were not secure. We know that compliance is not security. Frameworks, compliance, standards, benchmarks, and so on are all foundation references to building a program but it shouldn't be where we stop. We need to level up, change how we think and operate.

Call it DevSecOps. Call it agility. Call it synergy or collaboration. Our teams have to be as flexible and adaptable as our adversary so that we can anticipate their next moves. We can only do that by processing all of the intelligence that we receive and utilizing it to guide how we decide to protect our organizations.

## Understanding the maneuver warfare mentality

We've seen the movies, of soldiers lined up in rows marching towards each other with their officers shouting orders, horns blaring, armor glistening, and flags in the air. This is called attrition warfare, where the point of winning was wearing down the opponent by constantly reducing their resources, such as supplies and personnel. The one who was the victor typically was the one with more resources. This was considered normal until someone did something else that wasn't in the rulebook or wasn't expected. Officers were being targeted at the onset of battle, causing dysfunction in the lower ranks. Enemy soldiers did not have uniforms, causing paranoia for opposing forces. Suddenly, military organizations needed to change their tactics in order to survive in combat. They needed to adapt to opponents that did not follow conventional rules.

## Follow the process, the process will save you

I went through some military training where the instructor had us all stand up in a room, raise our right hands, and do the *wax-on, wax-off* motion, and we repeated the word *follow the process, the process will save you*. It was meant for us to stay within our box and not deviate from the rules. It meant that we should not question the process because this process has been in existence and it is proven to work. There were people that loved the process so much that they breathed it. It was their doctrine. Groups of these people would band together and perfect the idiosyncrasies of the process. Processes are necessary for running operations, as they provide a sequence of what to do when and who will do what when. It is simple. Stay in your lane.

Well, today is different to yesterday. There have been processes that have been in place for years. Like lanes on a road, processes need to be reinforced, reworked, and improved. All organizations are different in the way that they run their IT operations. Maneuver warfare fits the description of what a malicious actor would utilize to get into a network. Defense in depth is another way of saying attrition warfare. Screened subnets, network segmentation, and sandboxing; it is the idea that we should be taking ground from our opponents at different levels to decrease the possibility of exploitation. We need to change the game. Our adversaries are maneuvering for our crown jewel information, finding different vectors, or avenues of approach, to gain access to it.

Defeat is extraction of information or critical loss of business capability.

How do we build processes within our organization that allow for agility, initiative, trust, and collaboration to take action? We need a strategy that allows us to be flexible and continuously monitor our strengths and weaknesses within our organizations' security programs. We must be able to adapt to change quickly and have the capability to anticipate the probability of exploitation of our critical vulnerabilities in strategic areas of interest. We need to have the support and authority to take initiative in exploiting opportunities to improve security.

If we continue to follow our processes, will they save us from compromise?

## What is maneuver warfare?

A Prussian general and military theorist, Carl Von Clausewitz, introduced maneuver warfare to the world in his book *On War*. He was a combat veteran, and was interested in studying the art and science of war, in particular, the campaigns fought by Frederick the Great and Napoleon. Both of these men took their smaller armies and were able to carry out successful campaigns against their opponents through maneuvering.

Maneuver warfare advocates that strategic movement can bring about the defeat of an opposing force more efficiently than by simply contacting and destroying enemy forces until they can no longer fight.

There are six main elements of maneuver warfare. Each of them is explained in the following sections.

## Tempo

Tempo is the rate or speed of motion or activity; pace.

KPIs are measurable values that provide a metric to gauge how well a function is achieving business objectives.

Here are a few examples from ITIL KPI Service Operation that we can use to understand how activity or tempo can be measured:

- **Mean time to resolve:** The average time between the start and resolution of an incident
- **Mean time to detect:** The average time to detect incidents
- **Incident resolution effort:** The average work effort for resolving incidents

We use KPIs to continuously improve processes within our organizations using values that we can be certain are true. Zero-day exploits, advanced persistent threats, new ransomware attacks—uncertainty is a constant for a security professional. It can be crippling to the decision-making process and it makes things much more difficult. Some are afraid to make a call because they haven't received all of the information yet. Some call it *paralysis by analysis*. How do you manage the uncertainty?

Let's take an excerpt about uncertainty from intelligence operations:

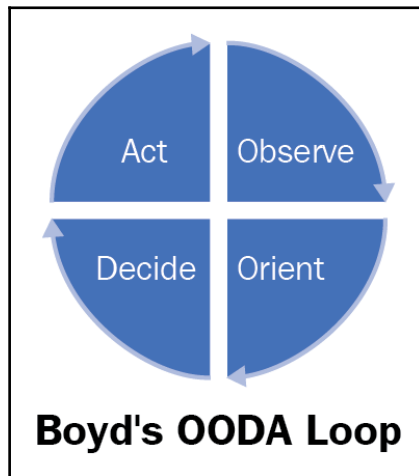
*"Uncertainty pervades the battlespace—it is a fundamental attribute of war. First and foremost, intelligence should support the commander's decision making process by reducing uncertainty about the hostile situation. Intelligence should accomplish the following actions to achieve this objective:*

- *Identify and evaluate existing conditions and capabilities*
- *On the basis of those existing conditions and capabilities, estimate possible enemy courses of action and provide insight into possible future actions*
- *Aid in identifying friendly critical vulnerabilities that the threat may exploit*
- *Assist in developing and evaluating friendly courses of action"*

Military officers undergo training where they have to make decisions on data that is incomplete. It prepares them to make decisions when they are in critical or otherwise crisis situations. It is called recognition decision-making. This method of decision-making can increase the tempo and the ability to maintain the initiative against the enemy. However it requires a large amount of study on the topic prior to the crisis occurring, moral courage, and the leader assuming the risk of quick planning without the aid of other experienced personnel.

## The OODA Loop

Recognitional decision-making is taught using Boyd's cycle, also known as the **OODA Loop**:



- **Observe:**
  - Situational awareness of yourself, your environment and your adversaries; noting any changes surrounding those variables.
  - From a security perspective, consider tool sets used by an adversary who scans a network, actively looks for vulnerabilities, tracks their targets, and is looking at what their target is doing or is about to do. In this regard, the defender can begin to anticipate future moves and get into the mind of the adversary.
- **Orient:**
  - After observation, we begin to develop a mental image of the situation thus gaining awareness
  - With this, we recognize that a decision is necessary in order to influence the situation
  - We will diagnose, recognize, and analyze changes in the environment
- **Decide:**
  - After recognition that a decision is necessary, a course of action is determined
  - In this case, decisiveness is sought, frequently with an acceptable degree of risk

- Effective and succinct communication of this decision is key when we talk about leading subordinates
- **Act:**
  - Timely and tactically sound decisions are useless alone
  - In order to influence the situation effectively, leaders must turn decision into action in a time competitive environment

Every organization has their version of the OODA Loop. Every adversary has their version of the OODA Loop.



The one who has the most advantage is the one who can cycle through the loop the fastest.

This decision-making model can be used in organizations to think about their ability to perform each step in the loop:

- What is the problem?
- Is my organization capable of observing a problem?
- Can my team(s) orient themselves in a position to address the problem?
- Who is responsible for making the call?
- How quickly and efficiently can we address the problem?

Decision-making is not a simple process in communicating. With so many components that are interfacing with each other, it is challenging to get a consensus on a topic without impacting another stakeholder. If business is a battlefield, it is wrought with uncertainty for a security leader of where to put their time and energy into. Using the concepts from maneuver warfare, we can begin to define how these tenets are applicable to our situation.

## Center of gravity and critical vulnerability

The concept of center of gravity is the idea that each organization has a focal point of strength. It may be a specific capability that is possessed and being utilized. It may be a relationship of two or more factors that creates a larger source of strength. We want to use our centers of gravity and take away our adversaries' center of gravity. Maneuver warfare requires that the practitioner identify and understand what the other sides' center of gravity is. We should not try to eliminate that strength directly, however, we should concentrate our strength on some relative weakness that would adversely impact the enemy's center of gravity.



Where is the enemy weakest? Where is the flank? Where can we cause the most disruption to their operations? Our adversaries' center of gravity is their ability to move around the battlespace as they wish, and exploit opportunity at their will until they are discovered. Ethics, laws, and regulations prohibit us from counterattacking our opponents but we still have to defend our network in the following ways:

- By identifying the capabilities that we have established in our IT organizations, we can conduct gap analyses against known capability maturity models to find our critical vulnerabilities for each function as well as identify our center of gravity
- By understanding our current capabilities and identifying gaps in capability, we will begin to develop how the strategy to improve capability will support operations and how best we can employ our teams
- Once this is place, we start to look how our teams are able to understand how their work integrates with current operations, it opens the doors to possibilities to be proactive in our defense

## Surprise – creating and exploiting opportunity

In addition to improving our decision-making and understanding our strength and weaknesses, we should be able to adapt to the unexpected. Imagine a car race, where you see individual vehicles go around the track, jockeying for position, and trying to win the race. With each lap, a car may make a move to pass if they see an opening between vehicles. In another moment, there may have been a crash where either you hit the vehicles involved or you get out of the way. All of these are examples of a set of circumstances that were not expected but created an opportunity to exploit.



For more information refer to *Warfighting* by Marine Corps Doctrinal Publication - 1, present at: <http://www.marines.mil/Portals/59/Publications/MCDP%201%20Warfighting.pdf>.

How do we *surprise* our opponent if our job is to defend? Combining information about adversaries, their capabilities, and their intent as well as having a full understanding of our organization's capabilities and gaps provides us a view to possible threat vectors to our most coveted information. If we are able to estimate the path of least resistance, we may have a tactical advantage to reinforce known weak points in the architecture, process, or procedures.

## **Combined arms – collaboration**

The armed forces do not consist of one mass force. It separates into each warfighting domain. The army emphasizes fighting on land, the navy focuses on the sea, the air force are masters of the air space, and the marines are amphibious. Each of these organizations are important and must combine their capabilities to ensure success of military campaigns. Prior to any engagement, leaders of the organizations are planning together to best use their tools to complete their mission objectives.

Collaboration and synergy are terms we have heard in the business world that express working with another group or organization to achieve business objectives. In large organizations, it is understandable that the complexity of IT and remote management of teams can cause silos to be formed and communication to be challenging. When we break down silos and establish proper communication channels we will be able to address incidents, problems, and solutions faster.

## **Flexibility**

Where as collaboration tries to ensure communications between entities are smooth and seamless, a military organization must remain flexible in order to be able to react to an opponent(s) who changes their tactics. Flexibility is achieved through understanding the strengths and weaknesses of capabilities within the organization and training to address the different scenarios. It is the ability to establish redundant capabilities to reduce single points of failure in processes, people, and skills.

## **Decentralized command**

Decentralized command is the delegation of authority to subordinates to carry out the commander's intent. Within the proper guidance, this allows leaders to take initiative in the planning, training, and execution of their assigned missions. By training the leaders to act independently, it allows for operational and tactical flexibility.

## Summary

In this chapter, we've learned that intelligence is a capability and a discipline with various sub-disciplines. Understanding this concept, we can gain an abstract view of how intelligence can be gathered from different disciplines within an information security organization to provide our leaders with actionable data. This is only the tip of the iceberg. As organizations and technology grow more complex, it is necessary to have a process and capability established to grab data from multiple sources, aggregate it, and provide it to the team leads to take action on. We've reviewed the high-level tenets of maneuver warfare and its application in the information security domain. Maneuvers are dependent on having the right information given to commanders so that they can make a decision on what steps to take next. Understanding maneuver warfare gives us another view of how we can operate in an uncertain world. All of this does not mean anything if we do not have the capability to gather, analyze, and disseminate.

In the next chapter, we'll talk about the intelligence cycle and each of its phases so that we can develop the initial framework for an intelligence capability within your organization.

# 2 Intelligence Development

In this chapter, we will learn about what is required to support an intelligence capability. We will also set the foundation for understanding the intelligence process cycle that an organization maintains. We will go through each phase of the process to provide a framework we can use to aggregate, structure, and apply information to be used as intelligence products.

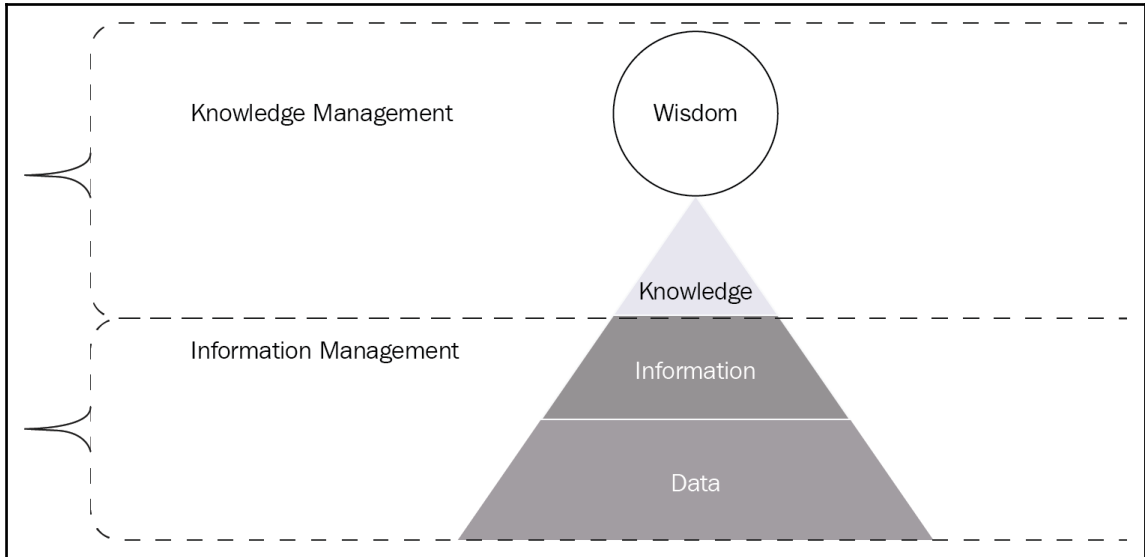


Another way of looking at intelligence capability is how Lord Varys from Game of Thrones has little birds to give him pieces of information that are important to him or those around him (PIRs). He isn't the commander in the series but he is what would be representative of an intelligence lead in the organization. How he gets his information is part of the collection architecture that he sets up, but how he processes the data that he's gained and how he communicates, to whom, and when is another process in itself, which we will learn about in this chapter.

## The information hierarchy

Actionable intelligence is what we get when we start sorting through the data. This data is gathered on the guidance given from the commander for items that they need to make a decision. How does information go from data to actionable intelligence?

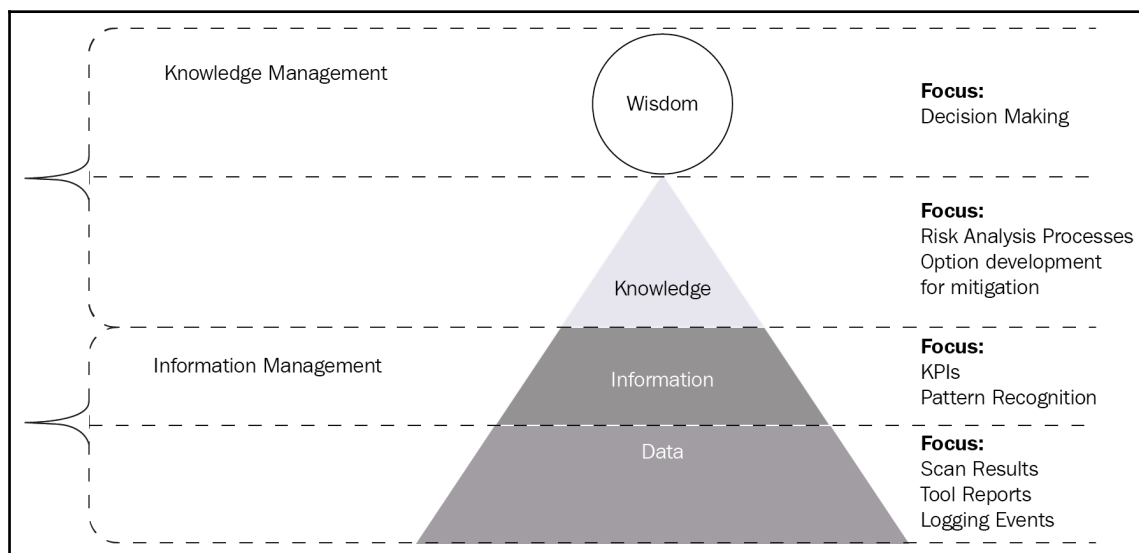
A common answer to this is the use of the **Data, Information, Knowledge, and Wisdom** pyramid also known as the **DIKW** pyramid:



This pyramid is a graphical representation of how data is transformed into wisdom:

- The **Data** and **Information** levels are located within the **Information Management** section because we will need to gather data based on the PIRs
- This data needs to be managed so that we can filter out the unnecessary pieces to obtain information
- After all of the information has been analyzed, it can then be moved and maintained in the **Knowledge Management** section
- From all of the information that has been gathered, the intelligence that has been developed will support the commander in making a decision

How does this look in an information security organization?



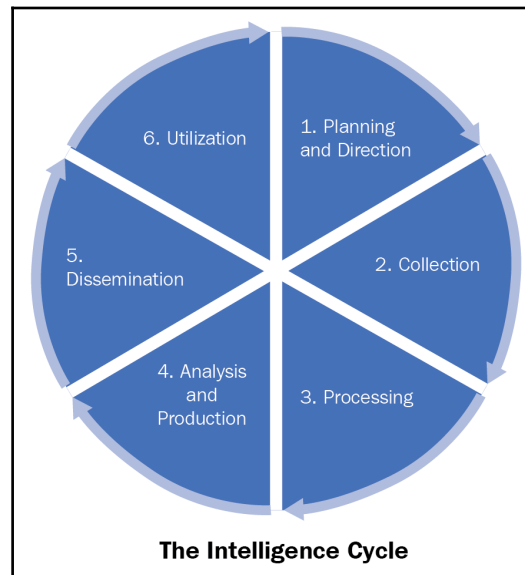
- At the **Data** level, we will begin by gathering information from the security tools that we implement within the environment.
- At the **Information** level, we will filter out information based on our PIRs. Examples can be KPIs or pattern recognition from AI or machine learning tools.
- Once the information is filtered, we can move it through our risk analysis processes and weigh what our options are.
- We will then be able to present to our stakeholders with the information necessary to make a decision.

## Introduction to the intelligence cycle

In the last chapter, we briefly went over the concepts of maneuver warfare and how intelligence drives the operations to accomplish the mission. In order to have an intelligence capability, a process needs to be developed to take raw information and produce a product that can be used for decision-making and action. The intelligence cycle is a six-step process that has been used by many government intelligence agencies as well as the military.

## The intelligence cycle steps

The intelligence cycle consists of six steps:



The steps of the intelligence cycle is explained in detail in the following sections.

### Step 1 – Planning and direction

The **Planning and Direction** phase is composed of all activities that identify information requirements as well as a means to ensure that those requirements are met. This step in the cycle manages the end-to-end intelligence effort. These information requirements are prioritized, collection plans are prepared, and collection capabilities (such as the various security and operation teams) are tasked.

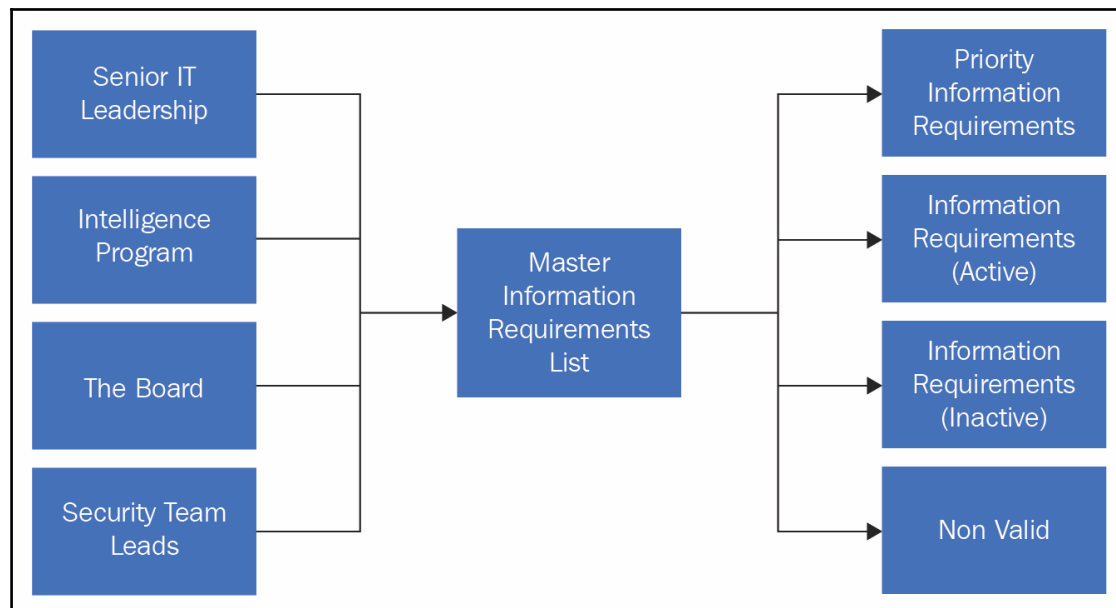
The executive leadership directs the intelligence effort, the intelligence program manager manages the effort based on the intent, priority of PIRs, and any guidance that was noted during the planning process.

## Requirements development

Everyone who is supporting the intelligence effort has a role in the development of the **information requirements (IRs)** for the organization. An intelligence program manager will be the one who is responsible for making the initial requirements based on the original intent of the senior leadership. From this guidance, the other teams will be able to provide their IRs to a *master list* for the intelligence program manager to record and to tie to potential decisions or courses of action. As time goes by, IRs will change as new information is found relevant or irrelevant, the intelligence program manager will continue to refine and reconcile IRs in this consolidated list.

## Requirements management

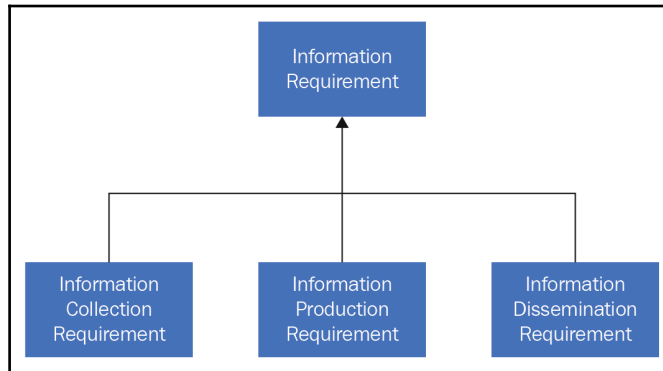
We learned about *Priority Information Requirements* in Chapter 1, *The Need for Cyber Intelligence*. As the situation changes, we must also have a system that can manage IRs as well as prioritize them. The intelligence program manager must have a system to aggregate information from the different sources for IRs into a master list and continuously monitor the senior leadership's IRs so that they can be assigned priority.



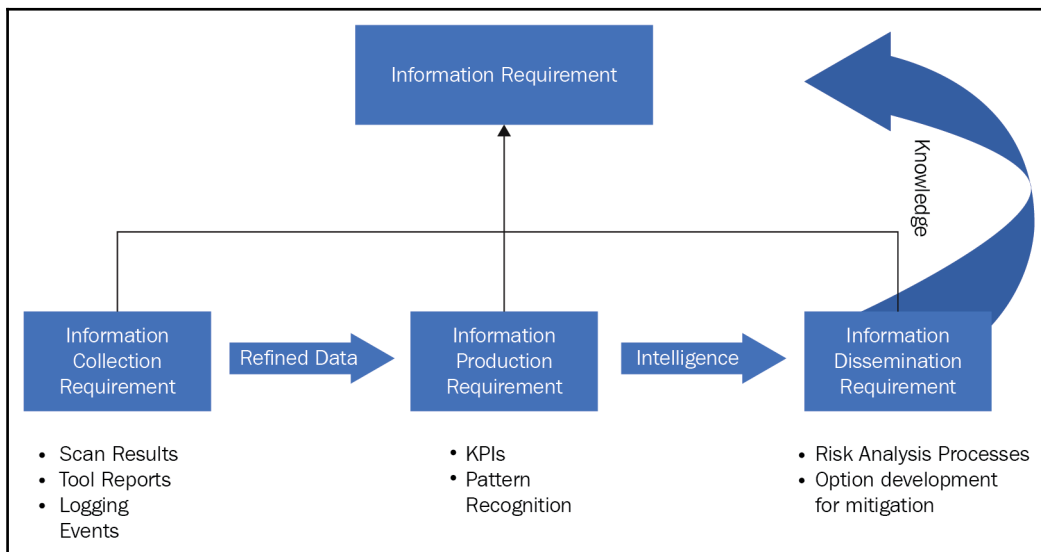


## Directing the intelligence effort

Intelligence direction uses the products of information requirements development and information requirements management and combines them with the functions of collections management, production management, and dissemination management. All of these efforts must be aligned to ensure that the focus remains on the efforts to obtain information to satisfy PIRs.



How does this work with the DIKW pyramid?



So, as raw data is being collected from various tool sets (**data**), we will need to start refining the data into usable information (**information**). Usable knowledge (or intelligence) can be gathered information for KPIs or understanding patterns or behavior against an established baseline. As intelligence is information that can be acted upon, this **knowledge** can provide decision makers with cognizance of the situation and enable the **wisdom** for developing options on the way forward.

## Requirements satisfaction

Requirements are met during the process within collection management, production management, and dissemination management. Following is a high-level overview, as we will get to these processes in later sections in this chapter:

- **Collection management:**
  - Ensures that collection resources are tasked and used effectively
  - Monitors collection efforts
  - Converts IRs to collection requirements and prioritizes them
  - Coordinates support from collection sources or agencies
  - Aggregates data collected and prepares data for analysis
- **Production management:**
  - Manages and organizes the analysis of information that has been received from the collection management process
  - Takes the data and converts it to an information product
  - Information products:
    - Have a defined scope, content, and format
    - Are prioritized and a plan/schedule is developed for each product
  - Prepares information products for dissemination
- **Dissemination management:**
  - Ensures that the right information in the correct format gets to the right people at the right time
  - Establishes the priorities for dissemination
  - How the product will be distributed
  - Monitors the flow of intelligence throughout the organization

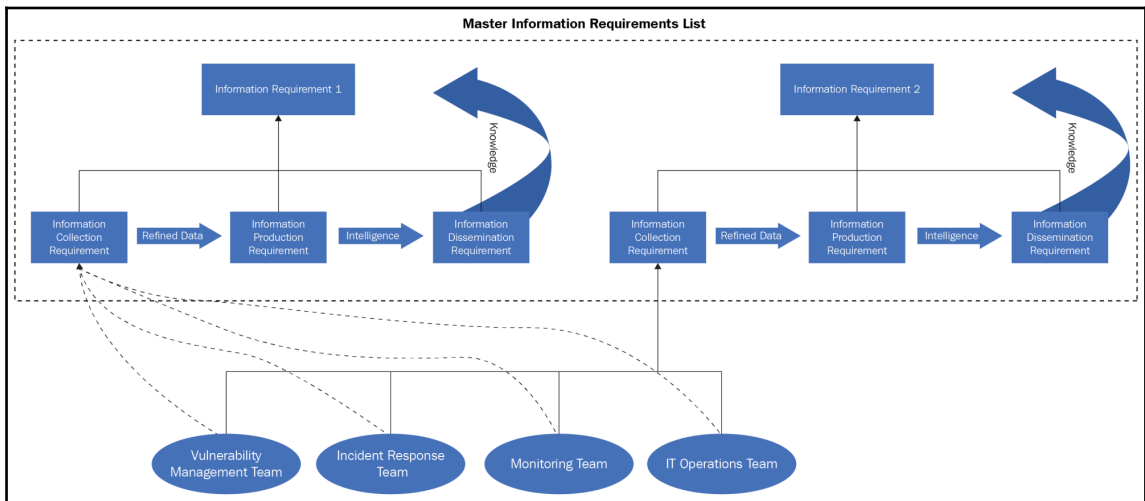
## Planning the intelligence support system

For requirements to be met, an overarching analysis needs to be completed to build the support structure for intelligence operations. A cyber intelligence program manager can consider the following:

- Organizational chart of intelligence sources from various teams for specific IRs
- Relationship management with all levels of leadership in the organization
- Vendor management
- Logistical requirements
- Information system requirements
- Connectivity to various intelligence assets such as:
  - **Sector Information Sharing and Analysis Center (ISAC):**
    - Defense Industry Base ISAC (<http://www.dibisac.net/>)
    - Electricity ISAC (<http://www.eisac.com/>)
    - Maritime ISAC (<http://www.maritimesecurity.org/>)
    - Retail Cyber Intelligence Sharing Center (<http://www.r-cisc.org/>)
  - Membership in public—private cyber security information exchanges:
    - Federal Bureau of Investigation—InfraGuard (<https://www.infragard.org/>)
    - US Department of Homeland Security—Cyber Information Sharing and Collaboration Program (<https://www.dhs.gov/ciscp>)
    - European Financial Institutes—Information Sharing and Analysis Centre (<https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership>)

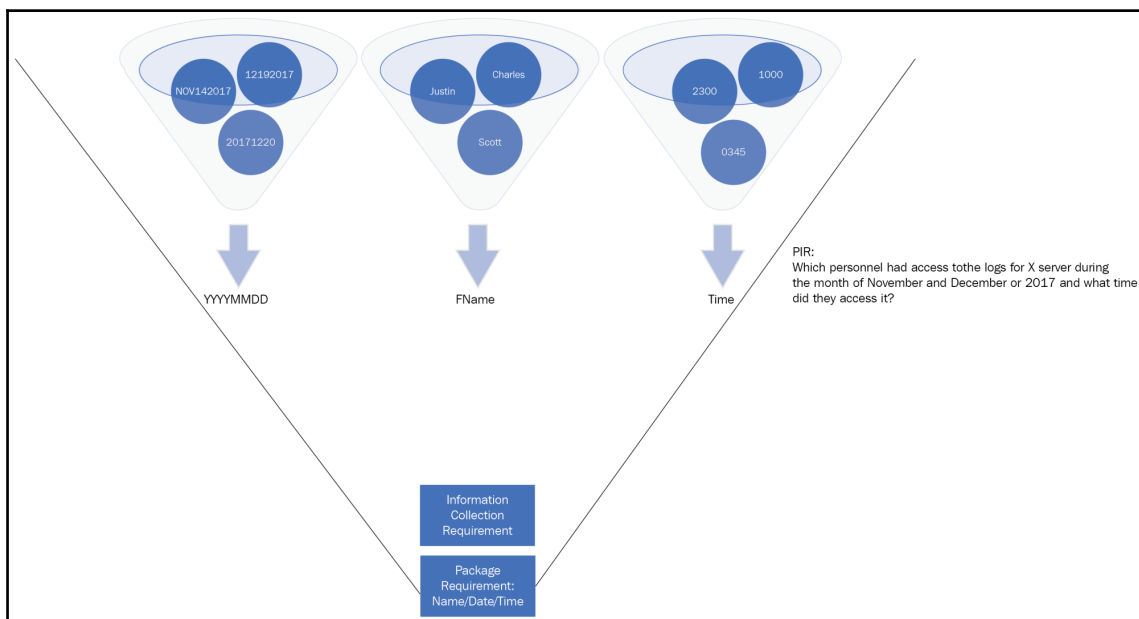
## Step 2 – Collection

The **Collection** step acquires and provisions information to be handed over to the processing and production steps. Collection management manages the information given by the various intelligence sources or agencies. Allowing various teams to collect their portion of the IR contributes to redundancy of information. This raw information can be used to confirm or disprove potential assessments, as well as provide opportunities for cross, communication between each of the teams. Once information is collected, it is reconciled and forwarded to the processing and production steps.



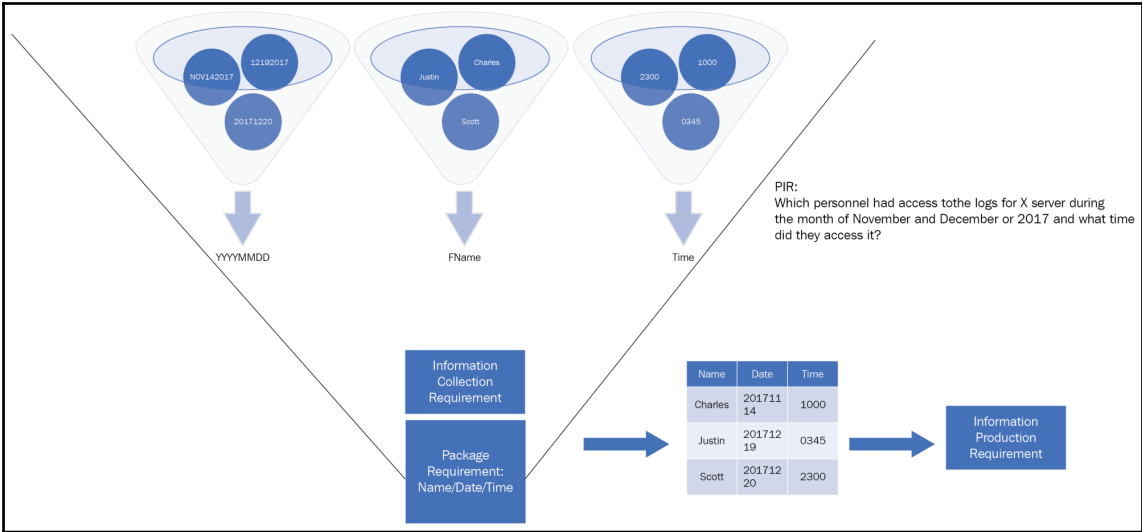
## Step 3 – Processing

All the collected information needs to be in a format that is specific to the organization. During the **Processing** step, this information will be processed, and items will be mapped to correlating points, and prepared for input into *Step 4, Analysis and Production*:



## Step 4 – Analysis and Production

The fourth step, **Analysis and Production**, is the process of analyzing, evaluating, interpreting, and integrating raw data and information into finished intelligence products for known or anticipated purposes and applications. The products are focused on the needs of the stakeholders so it is complete, delivered in a timely manner, and accurate. After analyses have been completed, there may be a determination that additional collection effort is required to fill in some information that wasn't present in the initial collection effort or other sources. The intent is that this product provides the stakeholder an overview of the subject area whereby they will be able to draw conclusions from the available information.



# Step 5 – Dissemination

The final step of the intelligence cycle is **Dissemination**. The goal of intelligence dissemination is to portray an accurate picture of the environment/problem/process/threat to the leadership in a form that facilitates rapid understanding of that picture.

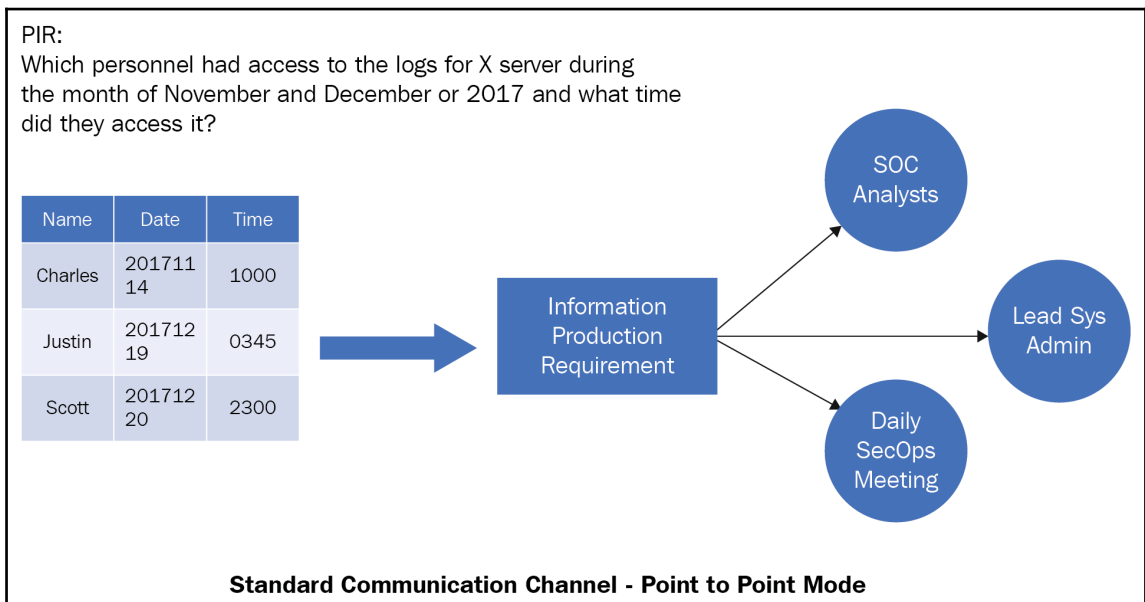
## Methods

There are a wide array of formats including dashboards, verbal reports, written reports, slide presentations, images, and so on. A dissemination system can deliver intelligence by a supply-push and a demand-pull. Both methods have their advantages and disadvantages and the dissemination system should have a balance of both methods. In supply-push, users do not have to request the information as it will already be in place. However, this information should be tailored to what is actually needed and not a data dump. For example, if we wanted to look at the amount of failed login attempts during a time period, the way that it is presented should not require additional filtering. The demand-pull works on an as-needed basis using querying. It reduces the possibility of overflowing personnel with information, as well as decreasing the time it takes to receive the information, as it will only provide intelligence when it is requested.

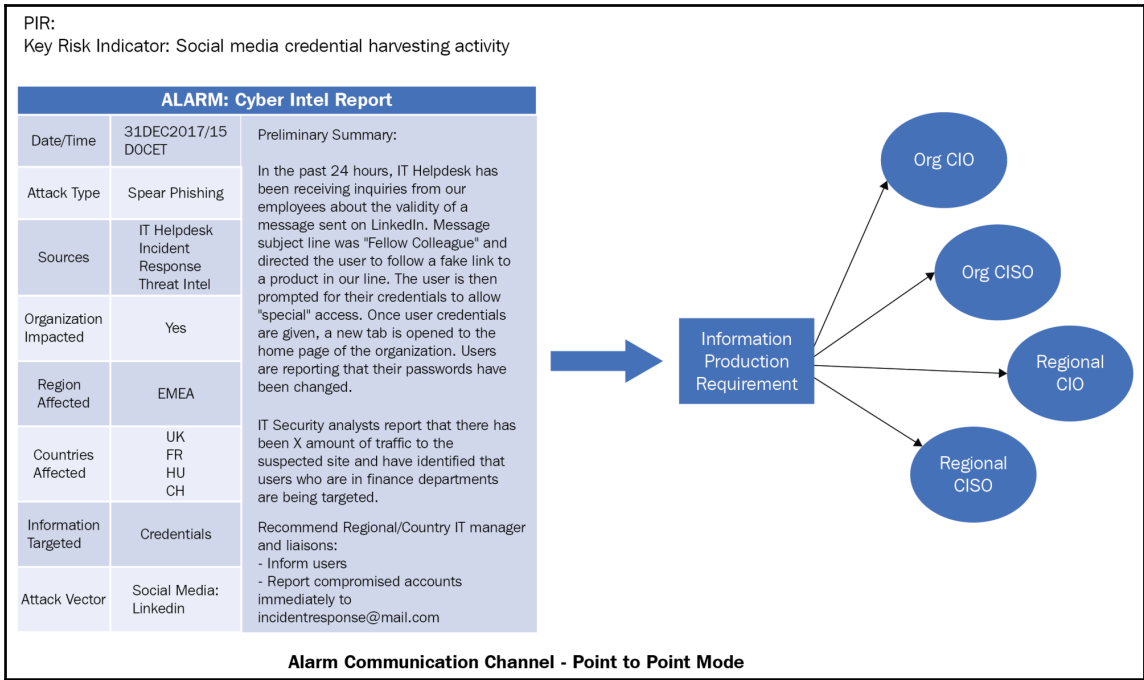
## Channels

Need-to-know is a common phrase we hear in security. We need to establish the *need-to-know* by creating channels in which the dissemination of intelligence will flow. There are two kinds of channels: standard and alarm.

Standard channels are used for routine intelligence from IRs through standardized reports, dashboards, and meetings:



Alarm channels are used for critical intelligence to be passed to teams that are immediately affected by the intelligence:



Modes

In addition to difference in channels, modes are a concept that helps with bringing intelligence to stakeholders as need-to-know. There are two modes of dissemination: broadcast and point-to-point. Broadcast mode disseminates all of the users that have the authority and access to the particular channel. An undisciplined use of dissemination in this mode will lead to information overload. In contrast, point-to-point mode is when intelligence is sent to specific users or teams that is typically in response to a specific request. It is slower than broadcast mode because it may require sequential delivery to specific units or the intelligence being produced is customized for that particular team.

Dissemination architecture

The intelligence program manager can provide an architecture for dissemination but it would be also best utilized if there was a team to communicate cyber intelligence to the organization. This is the point where large organizations can use their security awareness teams as I feel that security awareness is in its infancy.



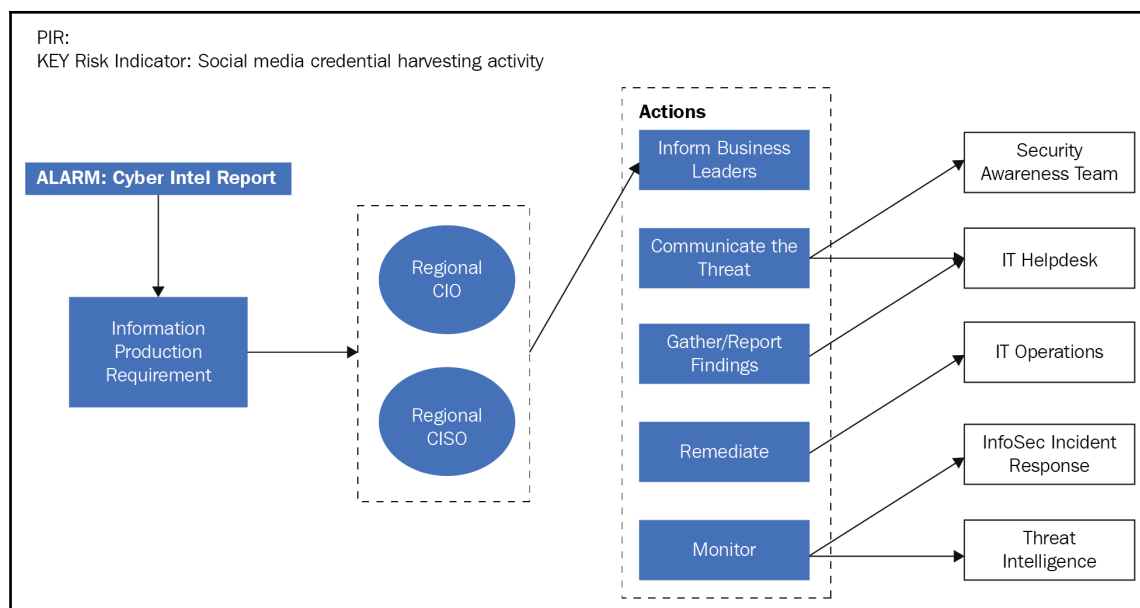
If we can use the relationships built internally within IT groups, as well as externally through the use of security education awareness to our colleagues outside of IT, we have a skeleton dissemination architecture. From a SMB perspective, we may be able to manage this dissemination within IT but would still need to establish the relationships with the stakeholders who can take action on the intelligence they will be given.

## Step 6 – Utilization

*"Intelligence has no inherent value; its value is realized through its support to operations."*

*– Intelligence Operations, MCWP 2-1*

This is where the foundation of top-down sponsorship of the intelligence program and relationship building with stakeholders is the key to success. Once intelligence products have been developed and disseminated through the channels of communication, they are meant to be used for action in at all levels of operations.



## Summary

We learned from the information hierarchy that in order to create actionable intelligence, we need to transform data into information, and finally to knowledge. Once we have knowledge, we gain wisdom to make a decision based on what we know. The intelligence cycle gives us a method for taking Priority Information Requirements to create intelligence products:

1. Planning and Direction
2. Collection
3. Processing
4. Analysis and Production
5. Dissemination
6. Utilization

In the next chapter, we will be discussing the challenges of integrating a cyber intelligence capability into organizations, more on the OODA loop, and the fundamentals of operational security.

# 3

## Integrating Cyber Intel, Security, and Operations

This chapter is about understanding how cyber intelligence, security, and operations are separate disciplines. There are challenges in fusing the three, and we will start breaking down how an IT organization can integrate a cyber intel team into their operations. We will introduce the concept of **operational security (OPSEC)**, and discuss how the concepts of OPSEC can be used as a strategic framework. Following this, we will start to understand the levels of leadership, how they would map to an intel capability team, and the levels of a strategic Capability Maturity Model in order to develop a cyber intelligence program. In this chapter, we will cover:

- Developing a strategic cyber intelligence capability
- Introduction to operational security
- Operational security in the business environment
- Cyber intelligence program roles

### A different look at operations and security

Establishing a cyber intelligence capability is not an easy feat to achieve, as many organizations are different in size, scope, composition, and culture.

Let me use an orchestra as an example. We know that all of the instruments take their cues from the conductor. Although the conductor is the one that is most visible on the stage, they are not the one who is solely in charge of how the orchestra sounds. The conductor interprets the music and conveys how it should sound to the orchestra.

An orchestra is composed of various instruments that can be grouped into families or sections. The conductor guides these sections to create statements or phrases with their lines, bringing out the important parts of a section while other sections soften their voices so that the melody can be heard. Each family of instruments has a leader or two that are responsible for their family of instruments to play in unison with the conductor. Each instrument in the section has to *listen across* to ensure that one is not overpowering the other. It is this understanding of how an orchestra performs that the phrase *everyone on the same sheet of music* derives from.

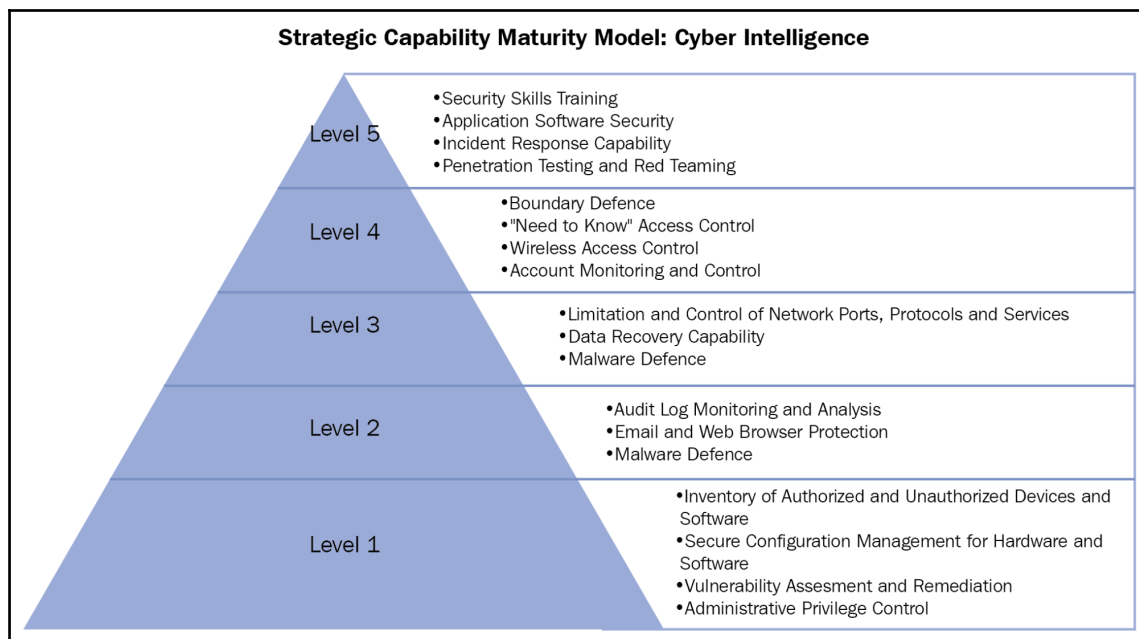
IT operations and IT security operations are no different to an organization trying to perform their functions as an orchestra performing a piece of music. Development to production, projects to operation is the rehearsal. The challenge is whether or not the entirety of an information systems division is in harmony or cacophony, within itself. Integrating cyber intelligence helps us listen across to one another and helps the IT leadership convey their next steps with operations.

## Developing a strategic cyber intelligence capability

Building a cyber intelligence capability is no small feat and every organization is different. As discussed in earlier chapters, there needs to be a means to collect, analyze, and disseminate information to specific stakeholders. The question is where do we begin?

A **Capability Maturity Model (CMM)** is used to show the different levels of how well the organizational practices, behaviors, and processes can produce required outcomes.

Here is an example of how we can begin developing the cyber intelligence capability using the Center for Internet Security top 20 critical security controls as a baseline:



From this point, we can ask these questions to frame the business need:

- Do we have the capability of doing this?
- Why is this important?
- What are our challenges?
- Who are our stakeholders and how will we communicate?
- When do we need this?

## Understanding our priorities

**The Open Group Architecture Framework (TOGAF)** defines an enterprise as any collection of organizations that has a common set of goals and/or a single bottom line. TOGAF organizes the enterprise into three parts:

- The business architecture
- The data/application architecture
- The technology architecture

## **The business architecture**

The business architecture is defined as a blueprint of the enterprise that provides a common understanding of the organization and is used to align strategic objectives and tactical demands.

As an IT and information security organization, we should have an understanding of how we support the business. Therefore, we need to understand the business priorities and strategic objective of the business to plan our innovation projects.

## **The data/application architecture**

All enterprises have a type of application architecture with its underlying data architecture. We will need to understand the relationship between the two and how it supports or supported previous business objectives.

## **Technology architecture**

We will need to understand how the data/application architecture is being supported from a technology point of view.

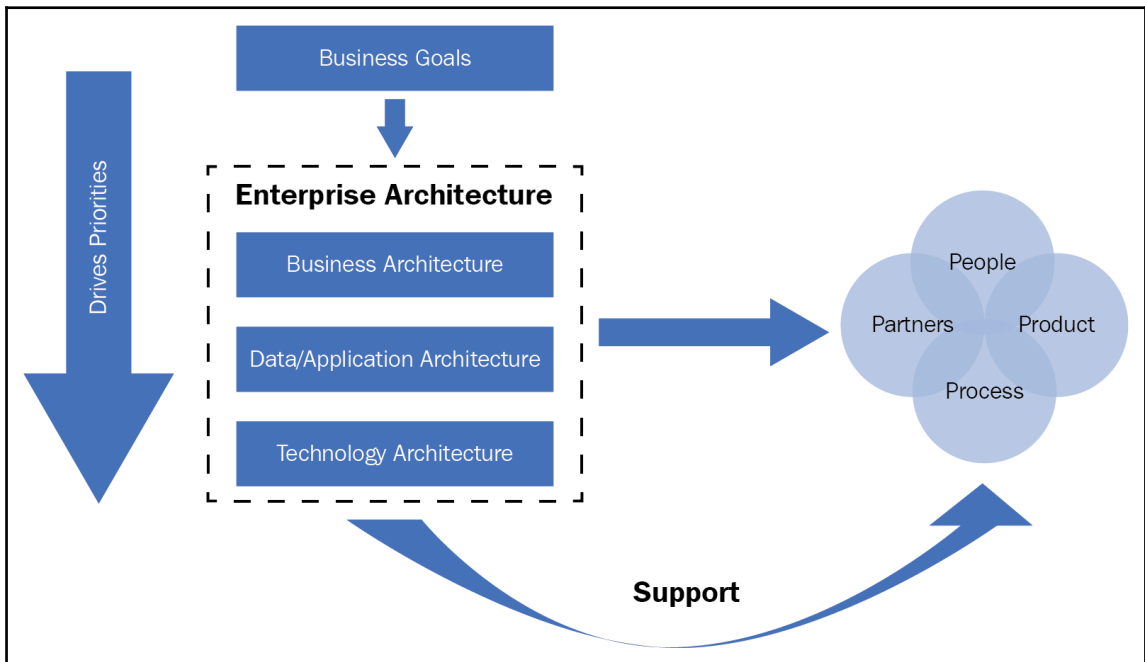
## **Application of the architectures and cyber intelligence**

Now that we have a model, where do we even begin?

Here's an example:

1. Understand your organization's business goals.
2. Identify the people, processes, products, and partners that are **critical** to meeting those goals:
  - Executive stakeholders
  - Single points of failure
  - Reputation
  - Manufacturing equipment and systems
  - Intellectual property
  - Core systems: databases, servers, networking devices

3. Identify the people, processes, products, and partners that **support** in meeting those goals:
  - Human resources
  - IT helpdesk
  - Program/project management office
  - Remote offices
4. Prioritize between **critical** and **support**.
5. Move forward in the prioritized implementation of establishing the means to communicate, collaborate, and execute actions based cyber intelligence to applicable parties:



## A look at strategic cyber intelligence – level 1

Level 1 of the Capability Maturity Model is where an organization must lay the foundation for the success of the cyber intelligence program. The processes and procedures that are developed at this level will set the tone of how the rest of the capability is built to support this initiative. This level largely concentrates on ensuring that basic information can flow between IT operations and IT security.

Use the following as examples for information requests:

- Inventory of authorized and unauthorized devices and software:
  - Do we have an inventory of authorized devices and software?
    - Where is it located?
    - Who administers this list?
  - Do we have an inventory of unauthorized devices and software?
    - Do we have a policy that addresses this?
    - What are the procedures to control this situation?
- Secure configuration management for hardware and software:
  - Do we have hardware and software hardening standards?
  - Are they communicated to our vendors who support us?
  - How do we ensure compliance to our standards?
- Vulnerability assessment and remediation:
  - Do we have the capability to perform vulnerability scans on our network?
  - Who is responsible for remediation?
  - Do we have timelines to remediate specific vulnerabilities?
- Administrative privilege control:
  - Who has administrative privileges?
  - Who doesn't need administrative privileges?
  - What do they have access to?

We will go through some maturity models for different points throughout the book in more detail. To help us understand how to establish and maintain each level of capability, we will introduce the concept of operational security.



Without a solid integration of IT operations and security for collection, analysis, and dissemination at level 1 in the **Strategic Capability Maturity Model**, it will be difficult to have clear intelligence about items on any other level.



## Introduction to operational security

Operational security was developed to promote operational effectiveness and deny adversaries information that can be observed publicly. This includes the following for an organization:

- **Capabilities:** What you can or have the ability to do
- **Limitations:** What you can't or are unable to execute
- **Intent:** What your plans are and when you will do them

For our purpose, we can use the OPSEC process to better understand how to develop a cyber intel capability to improve the defense and roadmap for a more secure network.

The OPSEC process has five steps:

1. Identification of critical information
2. Analysis of threats
3. Analysis of vulnerabilities
4. Assessment of risks
5. Application of appropriate countermeasures

## OPSEC step 1 – identify critical information

What is critical information? This is the factual information that an adversary would need in order to degrade services, disrupt operations, and impact the reputation of an organization. This is also commonly referred to in the commercial space as *Crown Jewels*.

For example:

- Core network infrastructure
- Information security capability
- Business information:
  - Mergers and acquisition
- Business critical applications:
  - Manufacturing applications
  - Enterprise resource management platforms
- Employee information:
  - Identification of system administrators

- Intellectual property:
  - Planning documentation
  - Schematics
  - Blueprints

## OPSEC step 2 – analysis of threats

This deals with identifying the adversaries (internal or external), their intent, and their capability to use the information against an organization. Once we identify the threats, we then can study their **Techniques, Tactics, and Procedures (TTPs)** and start prioritizing how we can monitor for these specific activities.

## OPSEC step 3 – analysis of vulnerabilities

A vulnerability is the state of being unprotected from the likelihood of being attacked, physically or emotionally.

By understanding the adversary, their intent, and their capability, an organization can then focus on identifying the potential vulnerabilities that exist in the enterprise.

## OPSEC step 4 – assessment of risk

Risk is a measurement of how much an organization is exposed to danger. Once vulnerabilities are identified, the vulnerabilities must go through the organizational risk process. This process evaluates each vulnerability and assigns it based on the sum of the probability of exploitation and impact to the organization.

Examples of probability levels:

- **Certain:** 100% chance it will happen
- **Likely:** >80% chance it will happen
- **Possible:** 60-79% chance it will happen
- **Unlikely:** 11-59% chance it will happen
- **Rare:** Less than 10% chance it will happen

Examples of impact levels:

- **Negligible Loss:** If this happens, it won't bother us too much
- **Marginal Loss:** If this happens, it will be an annoyance but we can get by
- **Moderate Loss:** If this happens, there will need to be a few projects to get us back to where we were
- **Critical Loss:** If this happens, there will be some major projects to get us back to where we were
- **Catastrophic Loss:** If this happens, we need to start from the beginning because there will be nothing left

A risk matrix is typically used as a visual representation to better understand the relationship between probability and impact:

Example Risk Matrix						
		Impact				
Probability		Negligible	Marginal	Moderate	Critical	Catastrophic
	Certain	Low	Medium	High	High	High
	Likely	Low	Medium	Medium	High	High
	Possible	Low	Low	Medium	Medium	High
	Unlikely	Low	Low	Medium	Medium	Medium
	Rare	Low	Low	Low	Medium	Medium

From the preceding example, we can begin to measure each vulnerability by understanding the probability of the vulnerability being exploited and if exploited, how much impact it would have on the organization.

Examples of levels of risk:

- **High:** This is probably something we should have a lot of oversight and control over. We'll probably need to have regular and more frequent reporting on this.
- **Medium:** These items are good to know about and we should monitor these to see if they change too much. We'll probably need to look at these every month or quarter.
- **Low:** These items are also good to know about but we don't need to worry as much as the high and medium risk items. We should look at these twice a year or once a year.

## OPSEC step 5 – application of appropriate countermeasures

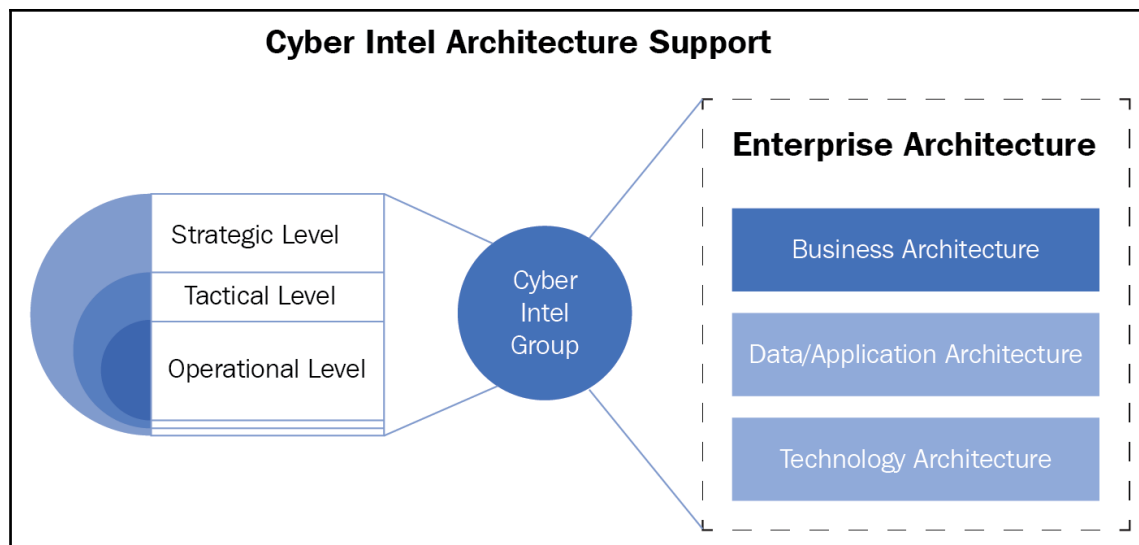
After the risk assessment, organizations should be able to prioritize resources to do the following:

1. Avoid the risk:
  - Change planning to work around the problem
2. Control/mitigate the risk:
  - Isolate the problem and reduce the impact to the organization:
    - Network segmentation
    - Access control lists
    - Credential management
3. Accept the risk:
  - Acknowledgement that the problem exists
4. Transfer the risk:
  - Cyber insurance
  - Service providers

## OPSEC applicability in a business environment

Business environments are not as structured as they are in the military. It is also a lot easier for a commander to dictate what is going to happen and drive it to execution. The OPSEC process should be looked at as a *strategic planning* initiative to a cyber intelligence program in that it covers very broad topics. It can help reign in the information that is critical to senior leadership's handling of all levels of operation in the organization and within each architecture in the enterprise starting at level 1.

The following is an overview of how the Cyber Intelligence Group can integrate the different operational levels of an organization as well as integrating the different enterprise architectures as defined by TOGAF:



Here are some considerations in building a cyber intel capability with OPSEC in mind:

- Buy-in from stakeholders:
  - Cyber intelligence is an ability not only about security, but also about IT operations
  - Authority and responsibility is clear in the military but not as clear in business

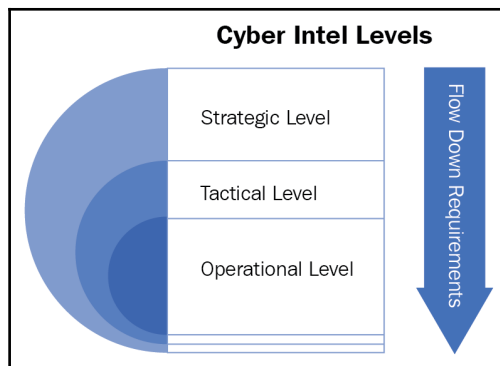
- Dotted line management and matrix managed organizations make buy-in difficult as direct reports may not be being evaluated
- It is much more difficult to establish this capability in a more mature IT organization because of the following:
  - Processes and procedures have been formalized and approved
  - Teams have worked in siloed environments for numerous years
  - Large organizations may have federated IT divisions based on geographical location
- Cyber intelligence can be integrated with an established or developing basic information security program:
  - Intel capability needs to be built on top of a framework of information security processes that support the organization
- Allow for collaboration:
  - Cross-communication and support for team resources to analyze the data and create intelligence products
  - Integrate with communication mechanisms to deliver intel to the right people at the right time
- Delegate authority to allow for subordinate leaders to take the initiative based on a commander's intent:
  - Intelligence developed without the intent of taking action is a waste of resources

## Cyber intel program roles

Who runs the show? All businesses have a chart that maps the role of each member in the organization. Typically, the higher a person is in the hierarchy, the more responsibility they have. However, each business is different in that, with startups, it is not uncommon for a CIO to be configuring servers, whereas in a larger organization, this is done by a technician. To better understand how a cyber intel program will fit into an organization, we will define three levels of leadership:

- Strategic
- Tactical
- Operational

From each of these levels, requirements will flow down to ensure that collection effort priorities are communicated to the teams:



Flow down requirements are communicated by the cyber intelligence program officer to their respective teams and liaisons. Let's take a look at each level, their roles and responsibilities.

## Strategic level – IT leadership

The *strategic level* of a cyber intel program begins with the collaboration of the IT and InfoSec leadership:

- Chief information officers
- Chief information security officers
- Regional chief information officer
- Regional chief information security officers
- Vice Presidents—senior managers

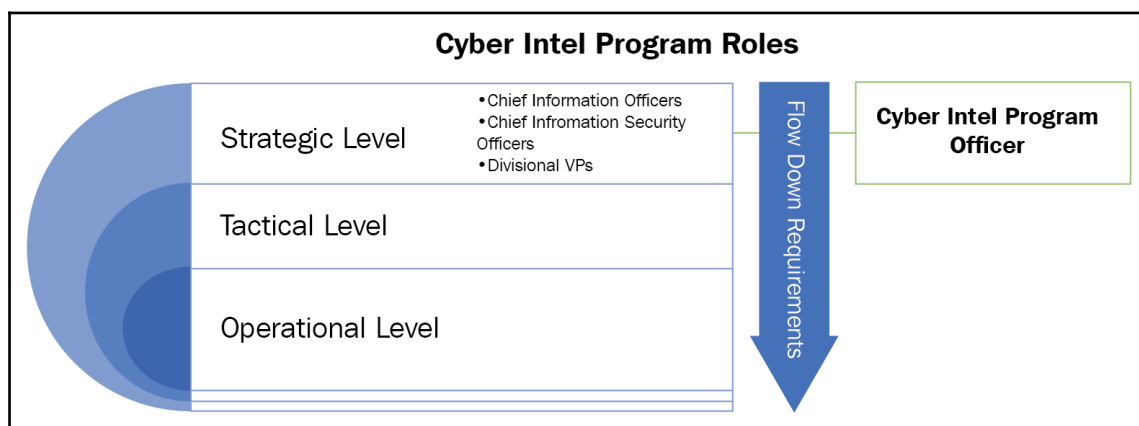
At this level, leaders should:

1. Identify critical information, systems, or technology.
2. Understand the threats and vulnerabilities to the enterprise.
3. Be able to make a risk-based decision on information to reduce threats and vulnerabilities.
4. Establish policy and procedures that are in line with business objectives.

## Strategic level – cyber intelligence program officer

At this level, an organization can designate a cyber intelligence program officer who will be responsible for the following:

1. Leading the cyber intelligence program
2. Gathering and prioritizing requirements from strategic leaders
3. Mobilizing resources and establishing the collection effort
4. Supervising the compilation and analysis of information



## Tactical level – IT leadership

The tactical level of a cyber intel program begins with the collaboration of the IT and InfoSec leadership:

- IT service managers
- Security operations managers
- Security managers



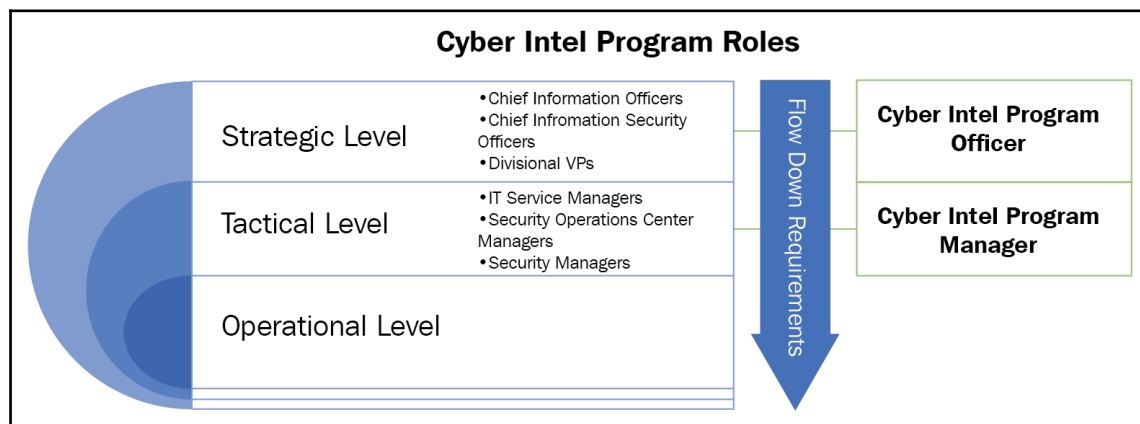
At this level, leaders should do the following:

1. Support the identification of critical information, systems, or technology
2. Report the threats and vulnerabilities to the enterprise
3. Provide support to leadership to make a risk-based decision on information to reduce threats and vulnerabilities
4. Support the development and enforcement of policy and procedures that are in line with business objectives

## Tactical level – cyber intelligence program manager

The cyber intel program manager will be responsible for:

1. Leading analysts within the cyber intelligence program
2. Gathering and prioritizing requirements from the cyber intelligence program officer
3. Mobilizing resources and establishing the collection effort
4. Supervising the compilation and analysis of information
5. Delivering intel products to stakeholders



## Operational level – IT leadership

The operational level of a cyber intel program begins with the collaboration of the following:

- IT service subject matter experts
- Security team leads
- Analysts

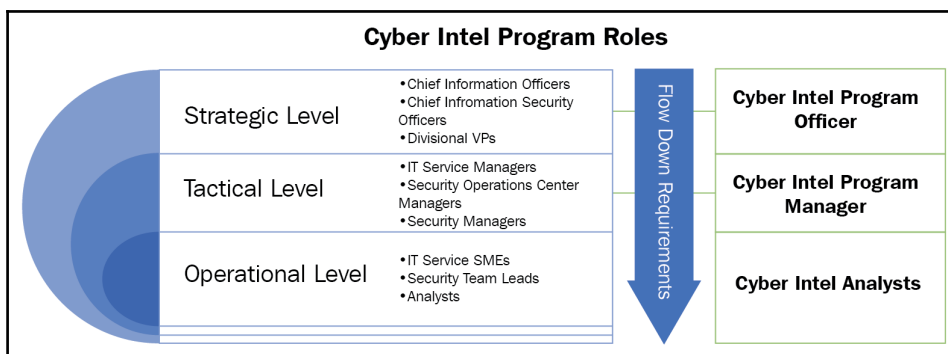
At this level, leaders should do the following:

1. Support the identification of critical information, systems, or technology
2. Gather and report the threats and vulnerabilities to the enterprise
3. Collect the information required to support the leadership's decision making process to reduce threats and vulnerabilities
4. Enforce policy and procedures that are in line with business objectives

## Operational level – cyber intelligence analysts

The cyber intel program manager will be responsible for:

1. Executing the cyber intelligence program.
2. Gathering requirements from the cyber intelligence program manager.
3. Compiling and analyzing information.
4. Developing intel products for stakeholders.



## Summary

Leaders at all levels need to understand the importance and support the integration of operations and security through building a cyber intelligence capability/program. To better understand how a cyber intelligence program can be thought of at the strategic level, we've introduced OPSEC and its importance in how we can take a high-level view of our organization and secure it using its five steps:

1. Identification of critical information
2. Analysis of threats
3. Analysis of vulnerabilities
4. Assessment of risks
5. Application of appropriate countermeasures

In this chapter, we've also provided examples of roles and responsibilities at each level that help support a cyber intelligence program. With the help of IT operations and IT security, the cyber intelligence capability provides support, utilizing top level requirements for collection, analysis, and dissemination. We've reviewed a high level Capability Maturity Model where each item on each level should answer the following:

1. Do we have the capability of doing this?
2. Why is this important?
3. What are our challenges?
4. Who are our stakeholders and how will we communicate?
5. When do we need this?

In the next chapter, we will be discussing how IT managers, SOC managers, and service managers can support the cyber intelligence program/capability in the organization by covering the tenets of active defense and its application from a tactical level.

# 4

## Using Cyber Intelligence to Enable Active Defense

In the last chapter, we learned about how we can integrate a cyber intelligence capability using a **Capability Maturity Model (CMM)**. This chapter is all about the tactical level of utilizing cyber intelligence. Using the principles of OPSEC, where we identify our threats, vulnerabilities, and prioritize decisions using risk assessments, we can use the levels of the strategic capability maturity model as a priority for our resources to focus on from top management. Now that these are in place, the middle management can step in and start providing useful decision-making information to senior leadership, as well as knowing their priorities.

At this level, middle management must also have a means to collect, analyze, and disseminate information to their teams. By identifying the threats, we can now start looking at how those threats exploit vulnerabilities. If we can identify the threat and know how threats will exploit possible vulnerabilities, we can start thinking about establishing a means to be proactive about security. This concept of proactive security, or offensive security, is also known as **Active Defense**.

From a high level, we will discuss the following:

- What is Active Defense?
- The principles of Active Defense
- Legal concerns
- Techniques, tactics, and procedures
- Communication and collaboration

## An introduction to Active Defense

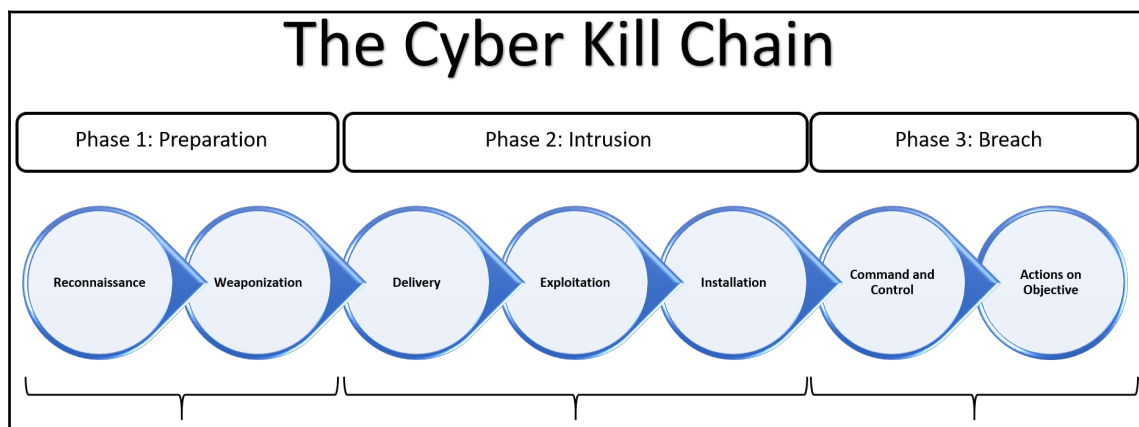
Let's talk about what we have now. We may have all the tools and blueprints necessary to build a house, but it doesn't mean that we can. Having all of the tools and the resources available to defend the network is meaningless unless we know how to be effective in using them. It would also be a pipe dream to think that we can look at our strategic Capability Maturity Model and build things one by one. In many organizations, these capabilities are at different levels of maturity. As discussed in Chapter 3, *Integrating Cyber Intel, Security, and Operations*, level 1 of our maturity model is the most important as it will provide us our scope, and the other *capabilities* are prioritized based on the needs of the organization. If we look at the building capabilities at the other levels in the same way we look at building a home, you can imagine that all organizations have their own version with their own challenges of building their dream home. Some will have their homes built on a solid foundation but lack a roof and vice versa. However, we will leave planning and building (projects and development) the *dream home* to the top leaders, our mid-level leaders need to use their current capabilities to secure the home that they are in.

I've always used the term *ugly baby* to describe a situation that you're put in that is less than desirable. We all have our ugly babies, but when you are talking IT and security, there always seems to be ugly babies all over the place. While top-level management is diligently working on building that house, you are handed the ugly baby to take care of. Maybe your vulnerability management program is weak or you don't have the authority to patch up your house. Guess what? This house and all of its ugly babies are our responsibility to defend. We have to make it work.

We can make it work by delivering the cyber intelligence capability to power the OPSEC process that will make our OODA loop smaller. When we make the OODA loop smaller, we can be proactive and prioritize our defenses using Active Defense.

## Understanding the Cyber Kill Chain

The Cyber Kill Chain framework was developed by Lockheed Martin to identify the actions required for adversaries to successfully exploit their targets:



There are three phases that are comprised of seven steps in this framework:

- **Phase 1: Preparation:** The adversary is looking for the soft spots in your organization and figuring out a way to exploit a vulnerability:
  1. Reconnaissance
  2. Weaponization
- **Phase 2: Intrusion:** The adversary has found a vulnerability to exploit, a means to deliver it, and needs their target to take the bait so that it can begin taking control of targeted systems:
  1. Delivery
  2. Exploitation
  3. Installation
- **Phase 3: Breach:** The adversary has control and is now taking follow-on steps to maintain and improve their position on the network for other malicious actions:
  1. Command and Control
  2. Actions on Objective

The framework helps contextualize the steps that are taken from the viewpoint of an **advanced persistent threat (APT)** and similar variations of these steps are performed by penetration teams globally. The idea is to be able to understand these steps, identify where a particular threat is within the chain, and stop it. As each organization is different in executing their business process, APTs, hackers, and script kiddies have their own. This would be referred to as the **techniques, tactics, and procedures** of the specific threat. By understanding that different threats have TTPs, through cyber intelligence we can begin to attribute specific actions or behaviors to threats.



Techniques, tactics, and procedures have been focused on specific hacker groups and nation-state organizations. However we cannot limit TTPs to just these organizations or actors. There is the threat that a system administrator may venture into a database that is not intended for them to view. We can look at the system administrator as the threat but we can also start to treat the capability in our network that allowed the system administrator to traverse over as a threat.

## General principles of Active Defense

If you search for the term Active Defense and cyber, you'll find a treasure trove of material, as it is a popular topic in the information security field. Why it is so popular is that the underlying idea is to *get back* or *hack back* an attacker. This *fight fire with fire* comes with some major legal and ethical caveats, and rightly so. Since we are learning how to utilize cyber intelligence, we need to narrow our focus. There are plenty of books on understanding the *hacker mindset* or *offensive mentality* and after that, what's next? We can't attack back. Beyond the day-to-day security and IT operations, once we start utilizing the OPSEC process, we can start understanding who our adversaries are, how they operate, and how to defend against them from breaching our network and/or stealing information.

There are three principles to Active Defense:

- **Principle 1:** Annoyance
- **Principle 2:** Attribution
- **Principle 3:** Attack



Due to legal and ethical ramifications, we will only be focusing on principles 1 and 2.

## Active Defense – principle 1: annoyance

If we are to be proactive in taking away a currency that is important to our adversaries, we would have to take something that we do have control over in our network, which is time. From script kiddies to nation-state actors, there is a *time threshold* where it's just not worth trying. Our job is to not make it worth their while to continue trying their specific attack by **blocking** it or deceiving our attackers into believing that their exploitation efforts are working by **deflecting** them to where we want them to go.

Examples of blocking:

- Geographical blocking firewall rules
- Port security
- Security training to report possible malicious actions

Examples of deflection:

- Route to null
- Honey docs
- Honey pots

With an understanding that we cannot be 100% secure all of the time, we want our adversaries to expend mental and computational resources to figure out how to get to their target.



A way that I think of annoyance and Active Defense is by relating it to the Warner Bros. cartoon with the Roadrunner and Wile E. Coyote. The Roadrunner's primary means of defense is speed. It did not matter what techniques, tactics, or procedures that the Coyote executed to catch the target, as the Roadrunner continually frustrated Wile E. with its speed.

## Active Defense – principle 2: attribution

Attribution is about validating a threat or adversary by recording their actions. With an understanding of annoyance and identifying the threats (internally or externally) we can start to:

1. Validate the reality of the threat or threat actor and their potential impact
2. Map specific actions to identified threats
3. Create opportunities for our adversaries to reveal themselves in our network prior to their attempts at exploitation



For example:

- The CIO and CISO of Dadi Inc wanted to ensure that they addressed their **capability to manage and monitor privileged users**. One of the threats they identified is employees with privileged access leave. What are the processes to ensure that they do not have access to the network? How will they flag an incident if a terminated employee with privileged access tries to log in (**validation and threat mapping**)? What actions do they take?
- Duyen, a database administrator at a small agricultural organization, reads a news article online that reports that the hacker group *Date Shake* is using a variant of malware to infect systems in an effort to exfiltrate intellectual property. After attending an IT security awareness training, she knows that groups such as *Date Shake* have an interest in what her company is doing with *hybridization* of different species of fig trees. Knowing that the systems that are being infected around the world are using the same operating system as her organization, and that *Date Shake* is a known threat to the organization, Duyen makes the calls to her IT teammates to report the possible vulnerability and to take action.

## Enticement and entrapment in Active Defense

Before we go on any further, we should discuss the difference between enticement and entrapment in Active Defense:

- **Enticement:** Something used to attract or to tempt someone
- **Entrapment:** The action of deceiving someone to do something illegal so that you can prosecute them

### Scenario A

Dogs like to eat and will take an opportunity to eat *people food*. At least in my house, feeding the dog people food is (in a sense) illegal.

An example of enticement is that you've cooked the food, walked over to the table, and left the food in plain view of the dog. Although the dog knows that eating people food is illegal, it has a choice of either eating it or not eating it. We will know whether or not the dog eats the food because it will either be consumed or left alone.

An example of entrapment is that you've cooked the food, walked over to the table, and left the food in plain view of the dog. Although the dog knows that eating people food is illegal, it has a choice of either eating it or not eating it. However, *you pick up the piece of food, tell the dog that they shouldn't eat it, then you feed the dog the food that it shouldn't have eaten in the first place, and then discipline the dog.*

Which of these scenarios sounds morally and ethically correct?

Now let's replace a few things and say the same story.

## Scenario B

Hackers like **personal identifiable information (PII)** and will take an opportunity to get files when they can. At least in our country, not protecting this kind of information is illegal.

Knowing that this information is important, we've created a file (HoneyDoc) with the name `Organization_PII_Roster.doc` that once opened, will alert my incident response team that someone is looking at something that they are not supposed to be looking at.

An example of enticement is that we've taken the file, placed it in an obscure human resources directory, and left the file in plain view of a potential hacker. Although the hackers know that going into systems and stealing information is illegal, they have a choice of either taking it or not taking it. We will know whether or not there is activity to investigate because that special file will either be opened or left alone.

An example of entrapment is that we've taken the file, placed it in an obscure human resources directory, and left the file in plain view of a potential hacker. Although the hackers know that going into systems and stealing information is illegal, they have a choice of either taking it or not taking it. However, you get on Tor, start posting the location of this file in the organization in multiple forums, wait for the file to be opened so you can attribute the person who exploited the network, and then go to court to prosecute them.

## Types of Active Defense

Active Defense can be thought of as martial art. Each martial art has its school of moves that focus on attacking, defending, or a mix of both. Each discipline has its own style and moves that makes it unique and addresses the basic need for self-defense. Krav Maga is a combination of attacking the opponent's critical vulnerabilities, while defending is something that we can relate military cyber operations to.

We are going to talk about how to use a Jiu Jitsu approach, which is to redirect an opponent's energy and momentum to where they want them to go.

Information gathering can come from two sources, either internally or externally, to be inputs in our cyber intelligence capability. Some information can be automatically gathered through log aggregation and other information can be acquired through word of mouth. How we handle the actions once the information is received will rely on the level of integration of the different components of an IT and security team to address the issues. To better understand how we can achieve this integration, we will discuss the manual and automated aspects of Active Defense.

## **Types of Active Defense – manual**

We can think of developing cyber intelligence, the Capability Maturity Model, and the manual of Active Defense as a belt system that is used in martial arts. At each belt level, there are techniques and skills that are studied, practiced, and maintained by the student. As students continue to progress, they improve their skills and master the fundamentals so that when an actual self-defense situation occurs, the multiple hours of martial arts theory then become applied practice through muscle memory.

Just as students must anticipate putting theory into practice, we have to test our IT Ops and security controls against real-life scenarios. Some examples include:

- Tabletop exercise gauging the interaction between the incident response team and IT operations in a data breach
- A chartered penetration test and the security operations center in its ability to effectively identify anomalous traffic

By practicing and improving these activities between different teams and personnel, we improve our ability to be proactive in the event of an incident.

## **Types of Active Defense – automatic**

Automatic measures to enable Active Defense are the tools or systems configured to measure specified data against established baselines. By leveraging automation we can increase the speed in which we go around our OODA loop. These tools should alert the proper teams and automatically mitigate the issue or stop the event based on programmatic logic.

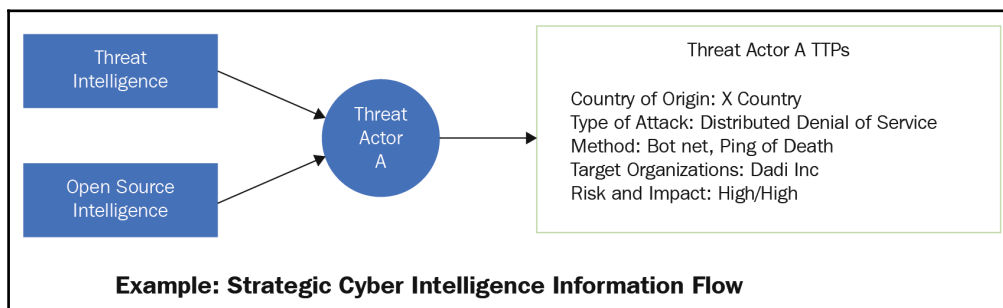
We can think of this as the abilities that a hero's sidekick(s) or partner brings to the fight in movies. These roles are typically the ones that cover the shortfalls of a situation or character. They automatically give a warning when danger is present or will stop a projectile without thinking. But how did they know how to do these things? Sidekicks and partners also have to train with the heroes. In our case, if we can start training and utilizing machine learning and artificial intelligence tools as partners, we will increase our cognizance and be able to anticipate events better.

For example, a **security incident event monitoring (SIEM)** tool is a means to evaluate possible events through log aggregation. Assuming that the organization has defined what incidents it would like to monitor and the SIEM tool is tuned to measure those incidents, an automated Active Defense mechanism would interface between administrative systems to cut off malicious systems. Now you may say, *"well if an incident has happened then we are reacting to an event that occurred and are not being proactive."* Remember that to be proactive in our defenses is to understand the tenets of OPSEC. If we apply OPSEC then we've already identified all of our critical information and systems, our adversaries, and their capabilities so that we can focus our SIEM resources on monitoring.

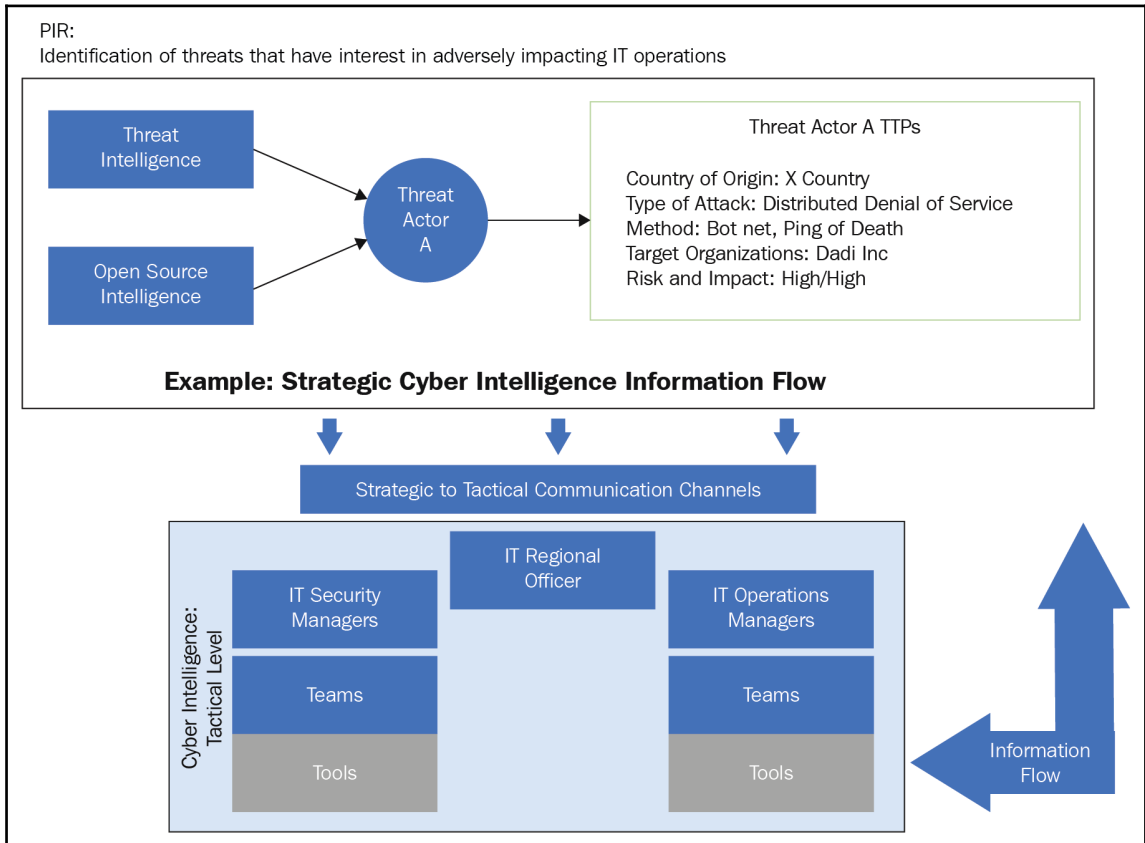
## An application of tactical level Active Defense

Let's try to apply what we've just learned.

The Dadi Inc. CEO just learned about *threat actor A* from a news source and how they have been causing other organizations' websites to go offline. Much to the CEO's surprise, Dadi Inc's CIO has already established that *threat actor A* is a credible threat to the organization with a high impact on the operation of Dadi Inc:



The CIO explains that the communications infrastructure is in place and that he is getting reports from his regional teams. Operations are ready to take action if the threat materializes. The CEO nods his head and the CIO resumes his plan for the day:



Meanwhile, at the regional office the IT regional officer is getting reports from the corporate cyber intel program officer that *threat actor A* is on the move again. The IT regional officer ensures that the IT security managers and IT operations managers are also kept in the loop by providing them information they need to take action:

**Threat Actor A TTPs**

**Country of Origin:** X Country

**Type of Attack:** Distributed Denial of Service

**Method:** Bot net, Ping of Death

**Target Organizations:** Dadi Inc

**Risk and Impact:** High/High

Although there are many things to monitor, after a call with the CIO, the IT regional officer starts the requests to change monitoring from other priorities to start targeting more information on threat actor A. These changes are passed down through the channels to the IT security and IT operations managers to their teams for action at the tactical level.

With threat actor A in mind, the managers begin to reassess their priorities and task out their teams accordingly. With the help of the IT risk department, each team has **Key Risk Indicators** that have been assigned for them to monitor in regards to a DDOS attack and will make any further calibrations to their tools so that they can provide the most accurate reports to their supervisors. Until threat actor A starts an attack, the day grinds on for the team.

Will Dadi Inc. be safe from a DDOS attack from threat actor A? How will the teams use cyber intelligence to enable Active Defense?

*To be continued...*

## Summary

As we've learned in previous chapters, cyber intelligence focuses on the aggregation of information and providing actionable intelligence for personnel to carry out operations. Intelligence collection information is prioritized by the key stakeholders of the organization so that they can have the data necessary in order to make a decision. The raw data comes from the operational level, from teams at the ground level, and flows into the tactical areas of operations for middle management to take decisions on.

Understanding this, we look at strategic priorities for information as a means to enable the right resources to concentrate on the correct items that need to be addressed. The collection efforts and actions can be addressed by automated or manual means, which, if we utilize the tenets of OPSEC and understand OODA, we can create an Active Defense capability for, as a method on the tactical level of operations to proactively address threats. This capability can help reduce the probability of exploitation of vulnerabilities by making it difficult to penetrate the network by deception as well as mapping and providing a means to validate a specific threat to their TTPs.

This chapter was about the tactical level of how cyber intelligence enables an Active Defense capability. We need to also discuss how our operating teams can take the information and incorporate it in their own operations. Before we dig into each team and how to do it, we will need to provide an example of a tailored framework that utilizes information specific for a specialized team. In the next chapter, we will learn about how US special forces teams utilize intelligence to carry out their operations using a process called **Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD)**.

# 5 F3EAD for You and for Me

*"Information and Intelligence' is the 'Fire and Maneuver' of the 21st Century."*

*-Major General Michael Flynn, March 2011*

The intelligence cycle doesn't stop at the Tactical Level. Information needs to go down to the teams, but at the same time, not all of the strategic priorities necessarily need to be known by the teams that are doing the work. The strategic priorities have to be sorted and distributed to the teams so that they can take action. This is where the F3EAD process comes in, as it is another process that is used by specialized teams to achieve their targets.

F3EAD is a version of the targeting methodology employed by the special operations forces (SOF) that are accountable for some of the most highly-publicized missions in support of incidents happening overseas. F3EAD is a system that enables them to foresee and estimate enemy operations, spot, pinpoint, and target enemy forces, and to perform intelligence exploitation and analysis of captured enemy personnel and material.

In this chapter, we are going to learn about:

- Overview of the **Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD)** process
- F3EAD application in the military
- F3EAD and the Cyber Kill Chain
- Application of F3EAD in the commercial space

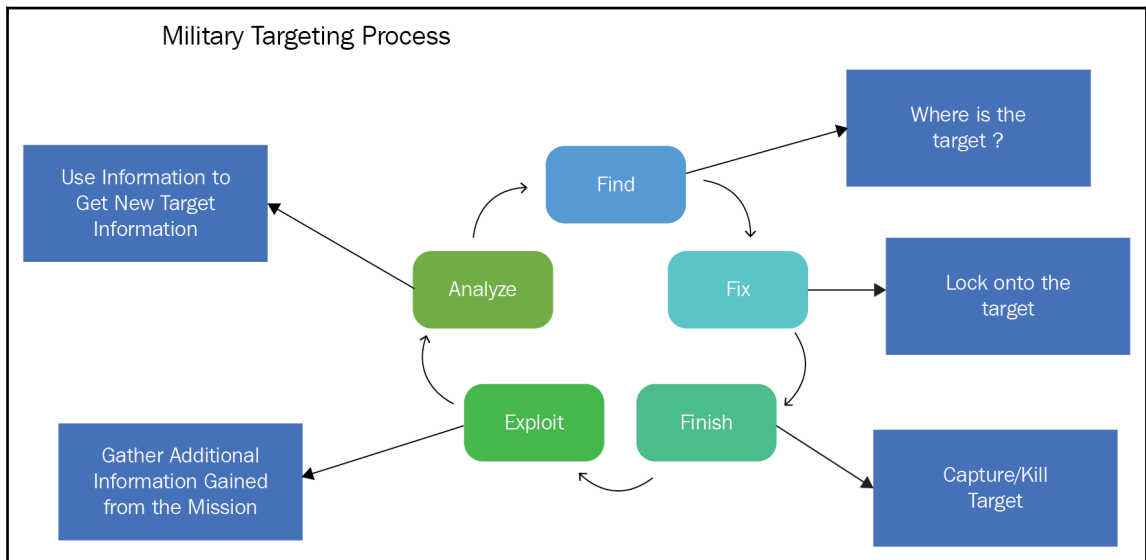


## Understanding targeting

The information that is required to make decisions is prioritized based on what goal or milestone needs to be reached. Think about everything that we've learned so far about the intelligence cycle. Once strategic priorities have been identified, they are passed down to the Tactical Level for prioritization. After the Tactical Level priorities are defined, they are passed down to the operational teams to tackle. The prioritized items at each level can be considered *targets* that need to be reached to gain information for action or establish a capability.

The US military has used a *targeting* process to provide steps for actions against an enemy:

1. **Find** a target by identifying it and locating it
2. **Fix** on the target so that they know its whereabouts
3. **Finish** a target (capture or kill) with assigned resources
4. **Exploit** information gathered during the mission from available sources
5. **Analyze** information to find additional targets to take action on



This process is called F3EA which is a precursor to F3EAD where *D* in the latter means *Disseminate*.

Although there can be similarities, the definition of targets for the military, and the definition for businesses is different. In the military, the objective may be to capture or kill a *high-value target* or *high-value individual*. Of course, this does not entirely translate between the two worlds. However, we can put them into items that we can understand in the business world.

An example of how the business world sets targets is by using an acronym called S.M.A.R.T.:

- **Specific:** Defines what needs to be achieved
- **Measurable:** Establishes a metric for progress
- **Assignable:** Attributes who is responsible for the objective
- **Relevant/realistic:** Ensures that the target is achievable and pertinent to the organization
- **Time limited:** Specifies the date when it will be completed

Here are some business target examples:

- **Budgets:** The amount of funds that an organization has to complete a task (or series of tasks) for development, operations, or maintenance:
  - Project to be completed at or under budget spend
  - Funds allocated to operations must not go over X dollar amount per quarter
- **Project milestone:** An achievement within a project that takes place at a predetermined time:
  - Milestone A is complete when all deliverables are presented to the stakeholder for review at the end of the 3rd quarter
  - Milestone B is complete when all deliverables are accepted by the stakeholder at the end of the 4th quarter
- **Project deliverable:** A product, capability, or result that provides value to a customer at the end of a project
- **Key Performance Indicators:** A quantifiable measurement that is used to gauge the performance of a process, capability, and so on to meet key business objectives:
  - Decrease the total average of HIGH severity vulnerabilities to 5 per system
  - Initial contact for all MEDIUM category helpdesk tickets is within 24 hours

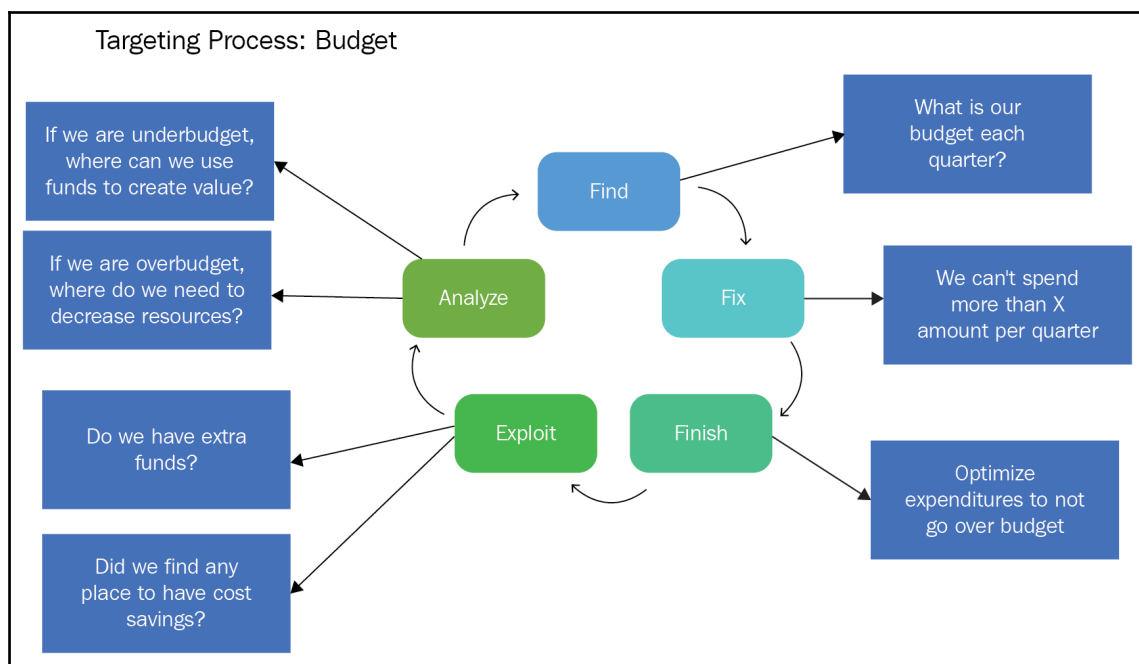
- Software testing metrics:
  - Decrease the number of defects found
  - Decrease the number of defects accepted
  - Decrease the number of defects rejected
  - Decrease the number of defects deferred
  - Total number of test cases
- **Key risk indicators:** A measurement that conveys the early signs that certain activities or areas are increasing or decreasing in risk:
  - The baseline remediation time for incidents must be 5 days over a 3-month period, provide a warning to X personnel if average remediation time for an incident is 7 days over a 1-month period
- **Risk levels:** A measurement based on the product of impact and probability:
  - Due to the legacy equipment and systems used to build our widgets, we must meet a low-risk rating for the Z application through mitigating controls

To better understand how we can apply the targeting process, we will use the target of a quarterly budget as an example:

- **Find:**
  - First, we need to establish an annual budget
  - Without this information, we will not be able to continue planning
- **Fix:**
  - Once we have our annual budget, we can divide it equally for each quarter
  - This information will help us understand our spending limits per quarter
- **Finish:**
  - We will need to monitor and control our expenditures to ensure that we do not go over what we've allocated for each quarter
  - Once the quarter is complete, we can now begin to look at the information that we've gathered
- **Exploit:**
  - We can now look at the information and begin to ask some questions:
    - Did we spend more than we anticipated?
    - Did we spend exactly what we expected?
    - Did we spend less than we anticipated?

- **Analyze:**

- We can now start addressing new targets for the next quarter:
  - If we were under budget, where can we use extra funds to provide value?
  - If we were over budget, where can we decrease resources to ensure that we don't follow the same path in the current quarter?



Understanding the difference between the application of this version of the targeting process between military and commercial is essential in that the term *target* can be applied to several things non-military related. For our purposes, we want to be able to target the capabilities that enable cyber intelligence throughout the organization. By filtering the priorities of information to be collected, Operational Level teams can begin the targeting process to provide the information as required as well as build the capability between teams to communicate cyber intelligence.

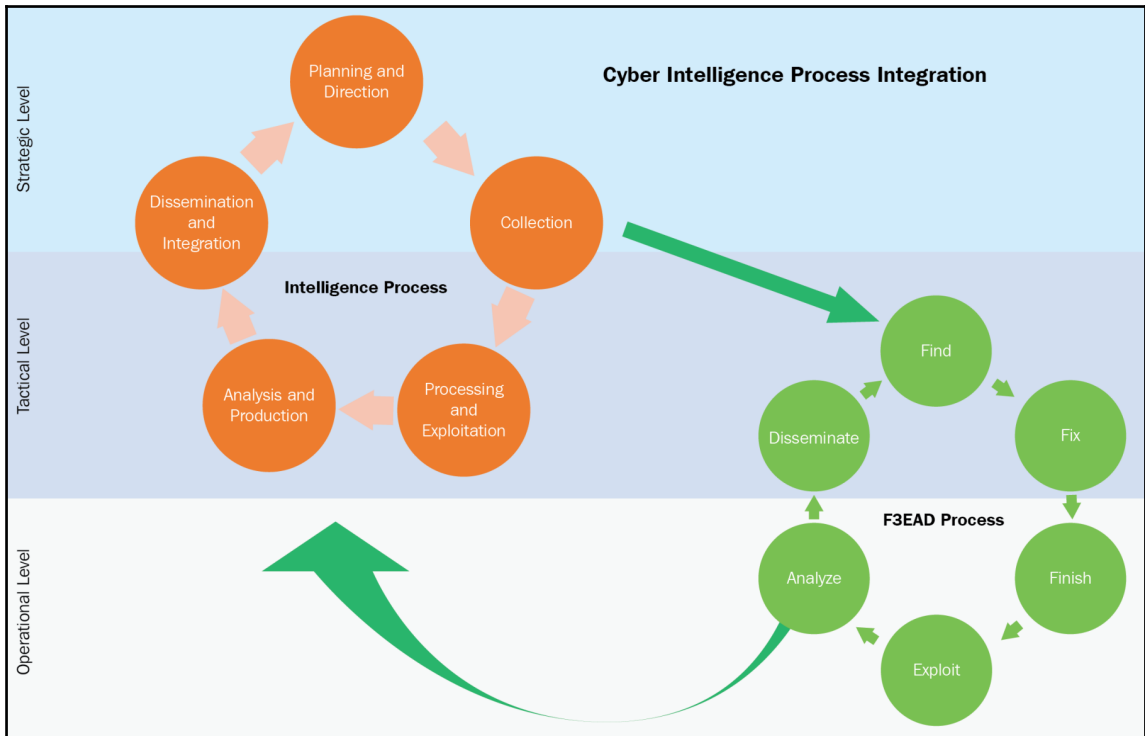
## The F3EAD process

The F3EAD process is a targeting methodology that has been popularized by the United States Military Special Forces in capturing high-value targets. If you can think of the Navy SEALs as the GUI or frontend of an application, then the F3EAD process is the backend system components, data processing, and circuitry. Just like a well-oiled machine, the F3EAD process drives special mission operations by focusing resources on gathering intelligence on specific targets, and using it so that decision makers can take action and follow-on actions.

The six components of this process can be divided equally between operations and intelligence:

- **Operations:**
  - **Find:**
    - What are the priorities for our operations?
    - What is the problem we are trying to solve for our organization?
  - **Fix:**
    - Where can we find the information that is required?
    - Where are the problems that we've identified?
  - **Finish:**
    - What is the answer to the problem?
    - How are we going to fix the problem?
    - What is the definition of *done* to our stakeholders?
- **Intelligence:**
  - **Exploit:**
    - Where is all of the information about the operation?
    - What information is essential for us to analyze?
  - **Analyze:**
    - What did we learn from this operation?
    - What information is required for our stakeholders?
    - How will this information be presented?
  - **Disseminate:**
    - Who needs to know this information and when?

We can see that F3EAD will be able to integrate with the intelligence process between the tactical and operational levels. This process can be thought of as another option of establishing the main processes for an intelligence capability, a sub-process, or a supporting process within the intelligence cycle:



In the preceding diagram, we can see that the **Planning/Direction Process** at the **Strategic Level** and **Tactical Level** of the intelligence cycle will set the tone of what intelligence information needs to be gathered at the **Operational Level**. **Collection** efforts will be tasked down to the operational teams and will begin the **Find** step of the F3EAD process. As we move through the F3EAD process, once the operational teams **Fix** onto the specific target, they will complete (**Finish** step) and then take the lessons learned to **Exploit** any additional information to send to the **Analysis** step. Notice that **Analysis** information will be brought back into the **Tactical Level** intelligence cycle. At the **Tactical Level**, multiple analyses from the different teams will be pooled together for review, disseminated to other teams, and utilized at the **Strategic Level**, **Tactical Level**, or **Operational Level**.

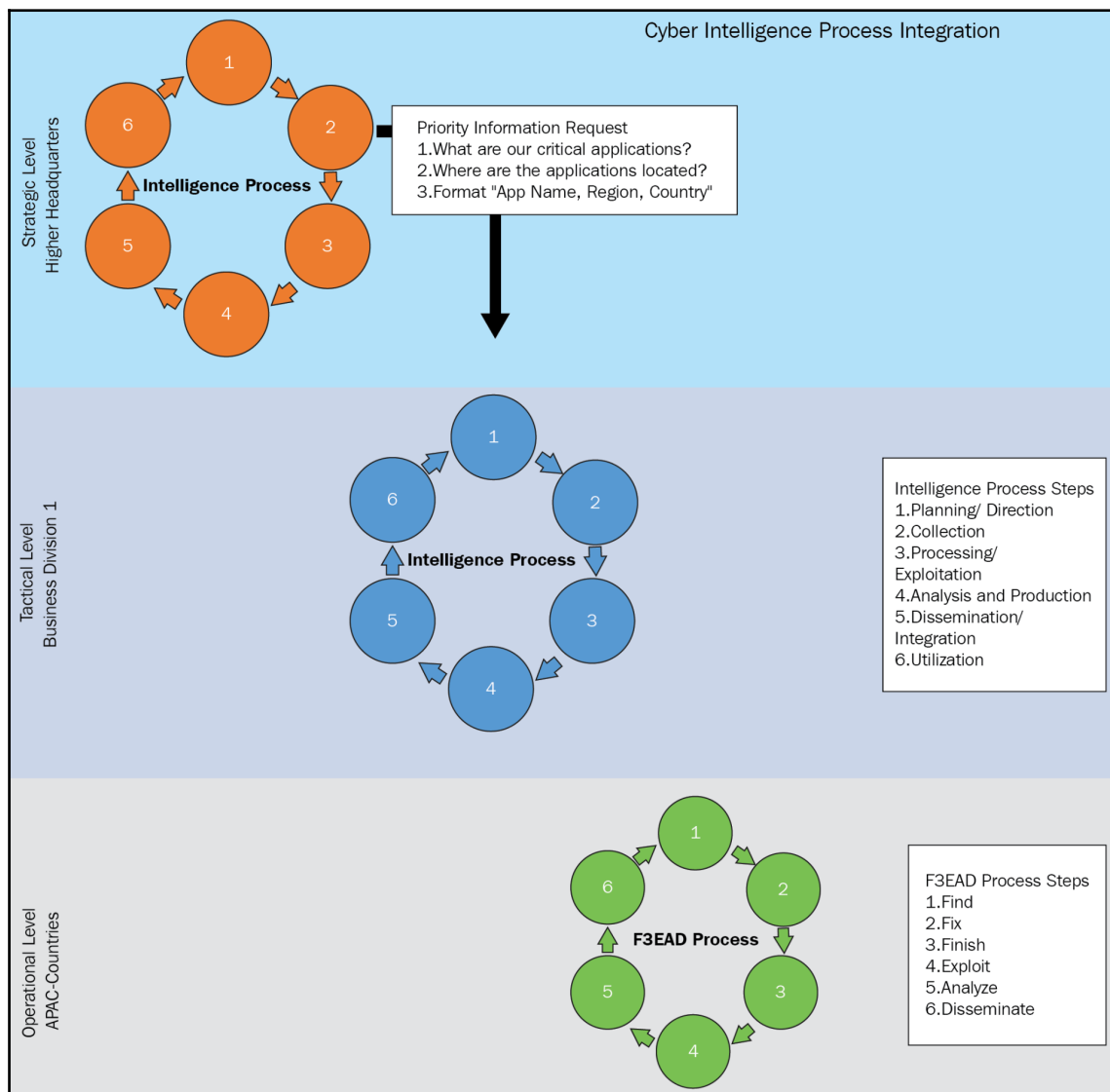
## F3EAD in practice

The following is a basic example of how the intelligence cycle and F3EAD can be integrated.

### Scenario:

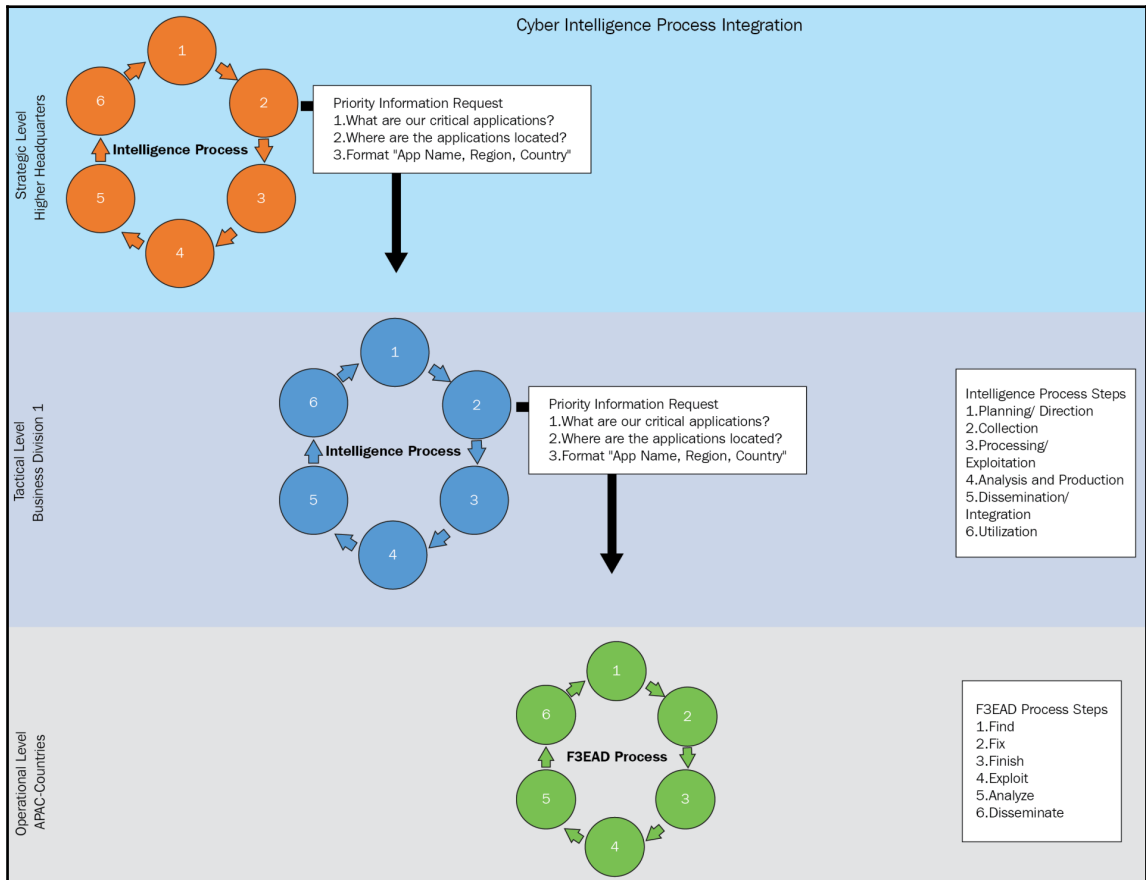
RonV corporation started as a family business in Antarctica in 2018 and has transitioned into an organization with worldwide operations in the widget making industry. Due to increased concerns of cyber attacks, RonV is trying to centralize security services so that headquarters can monitor the security posture of the organization. Over the years, mergers and acquisitions increased the complexity of the IT architecture with each additional business. Following the CIS Critical Security Controls, the CIO of the company has already begun maturing the capability to inventory authorized hardware and software, as well as have a means to block unauthorized hardware and software from the network. Now the CIO is looking to find the most critical applications of the organization so that she has awareness of what the applications are and where they are located.

- CIO delivers a **Strategic Level** priority information requirement to his **Tactical Level** leaders:
  - What and where are our critical applications to the business?
  - Format: **App Name**, **Region** of the world it is located, **Country** where it resides



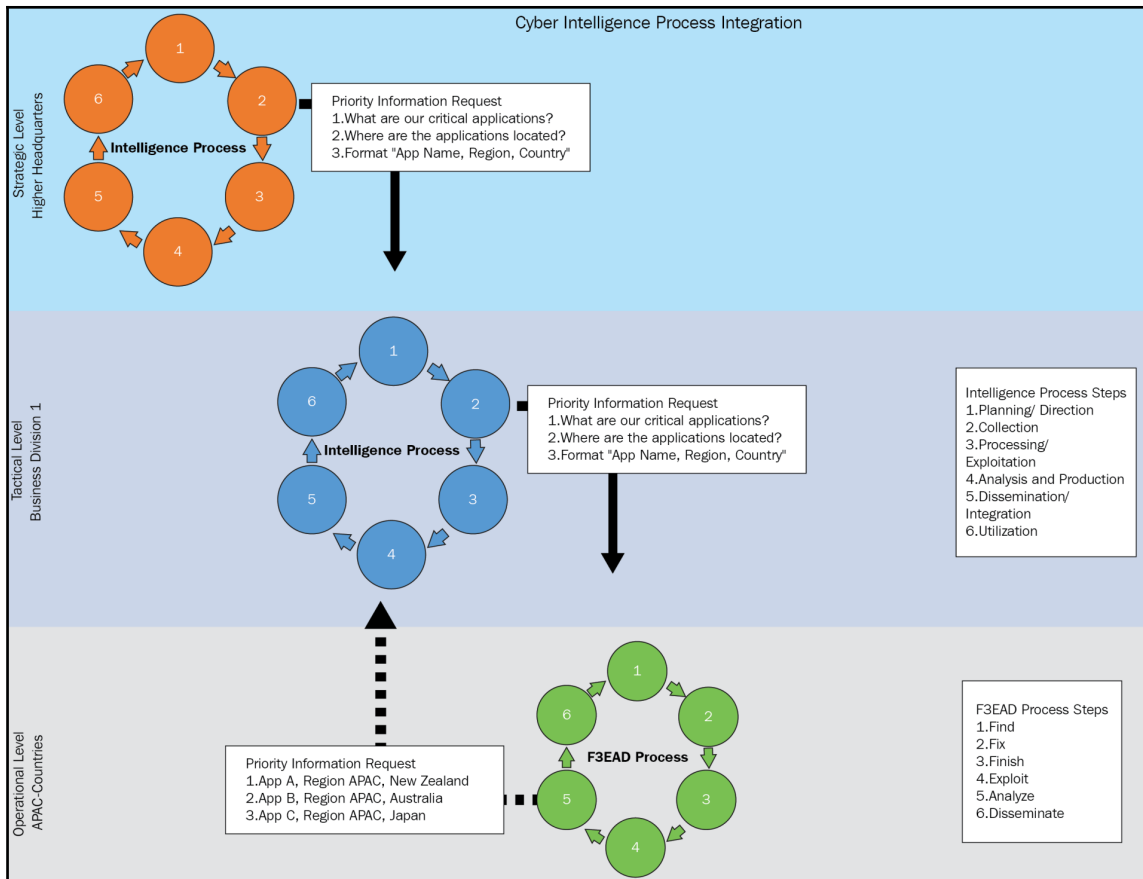


- **Tactical Level** leadership issues a priority information requirement to **Operational Level** leaders and requests information from the business divisions:
  - What and where are the critical applications to your business?
  - Format: **App Name**, **Region** of the world it is located, **Country** where it resides.



- **Operational Level** leadership will then take on the **Tactical Level** information requirements and go through the F3EAD process to:
  - **Find:** What and where are the critical applications to your business?
  - **Fix:** Navigating to the application registry and finding the applications labeled *critical*
  - **Finish:** Collecting the critical application information that is on hand
  - **Exploit:** Filtering out to only provide the information that is required and placing it in a centralized area in preparation for analysis
  - **Analysis:** Enriching the information and putting it in a usable format to deliver to the customer:
    - Format: **App Name**, **Region** of the world it is located, **Country** where it resides

- **Disseminate:** Providing the information to tactical operations



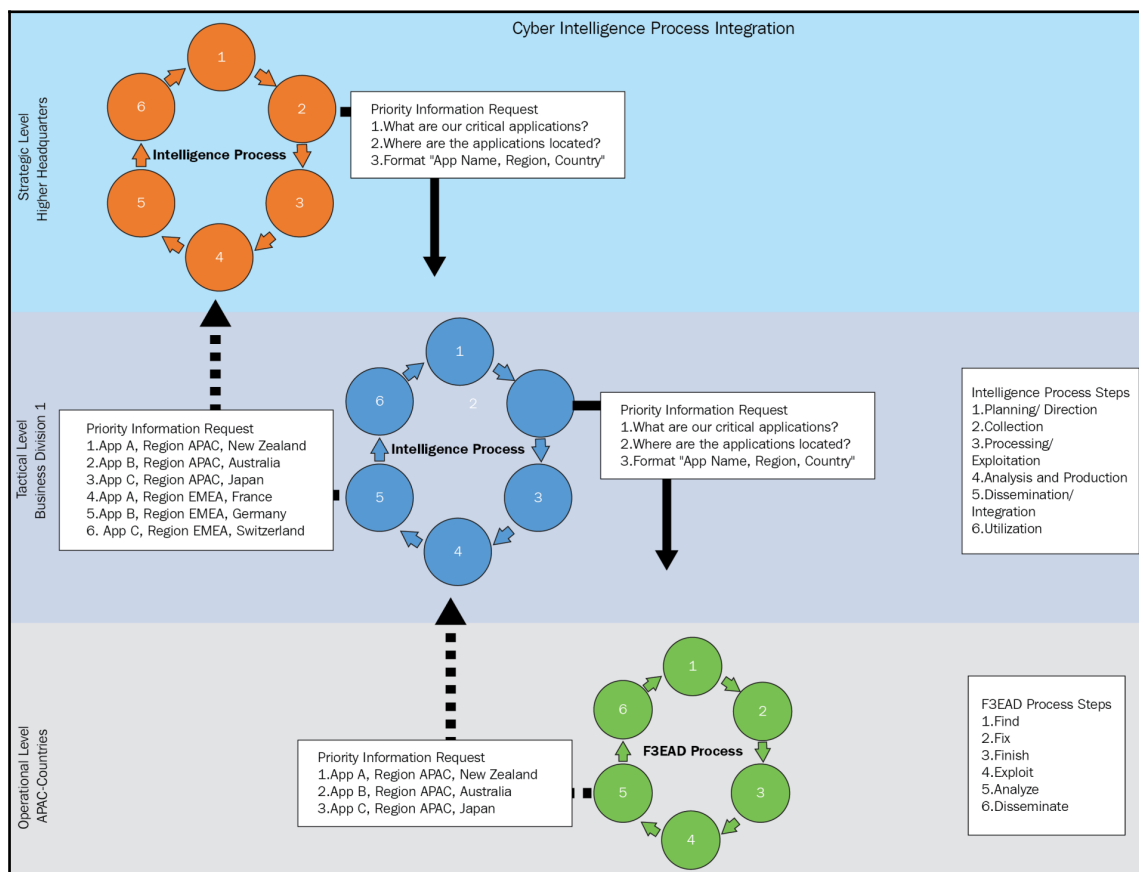
- Once tactical operations receive the information from the **Operational Level**, further analysis is done to reconcile and combine information to be prepared to pass to the **Strategic Level** for action. The following are the results:

- **Business Division I:**

- App A, Region APAC, New Zealand
- App B, Region APAC, Australia
- App C, Region APAC, Japan
- App A, Region EMEA, France
- App B, Region EMEA, Germany
- App C, Region EMEA, Switzerland

• **Business Division II:**

- App A, Region LATAM, Venezuela
- App C, Region LATAM, Chile
- App B, Region NAM, USA
- App C, Region NAM, Canada



Now that the CIO has the information that was provided from the tactical leaders in the requested format, they are now able to move forward with the next steps in their planning to protect these critical applications.

This scenario was very basic, but we need to understand how we can incorporate the F3EAD process within operations to protect the network, as well as build capability, using SMART targets and Capability Maturity Models. To further understand how F3EAD fits into the larger picture, we need to be able to relate it with the other processes and concepts that we've learned in the previous chapters, OODA, OPSEC, and the Cyber Kill Chain.



For the remainder of the book, we will look at the F3EAD process as an interfacing process between the tactical and operational levels.

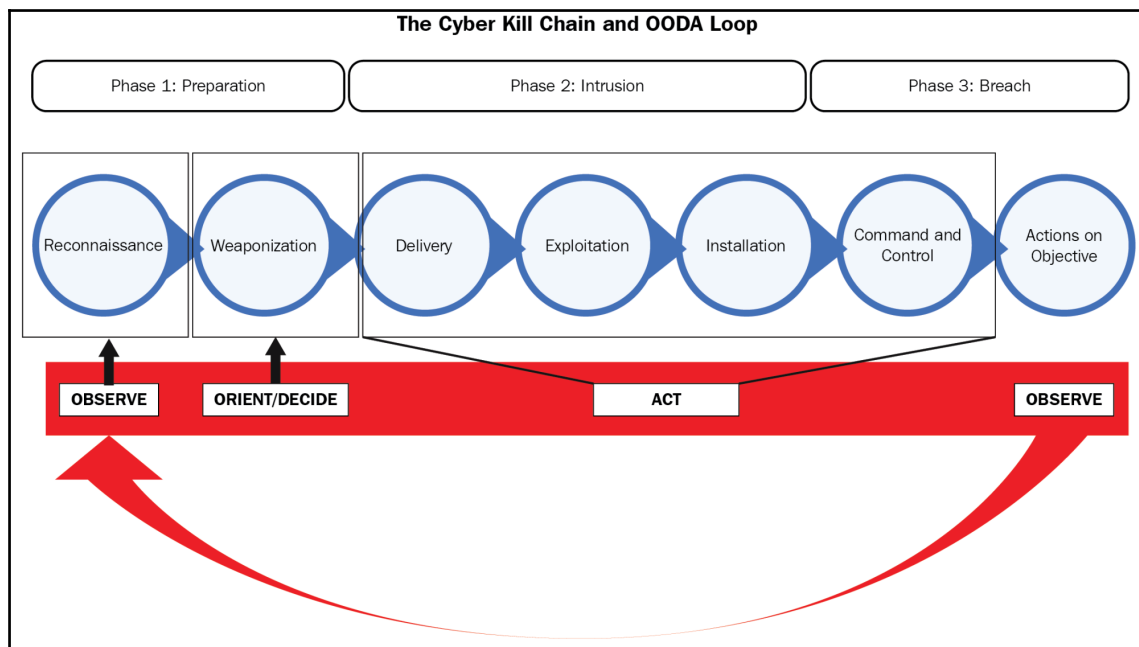
## F3EAD and the Cyber Kill Chain

As each branch of the military has their own special forces (for example, Marine Corps Raiders, Navy SEALs, and Army Green Berets), we can look at F3EAD as an intelligence process that is executed at the operational level, mapped to specific teams in their defense in relation to the different phases of the Cyber Kill Chain.

## Cyber Kill Chain and OODA loop

As we've learned in previous chapters, the Cyber Kill Chain consists of logical steps that are required to exploit a target, whether it be a system or a person. By understanding the steps an adversary must take, we can then look at how these steps map to the steps within the OODA loop.

Let's take a look at how we can correlate a threat's OODA loop with the Cyber Kill Chain:



Phase 1 of the Cyber Kill Chain:

- **Reconnaissance** maps to **Observe** because the threat is looking for any vulnerabilities on the target that they can exploit
- **Weaponization** maps to **Orient** because the threat needs to start target prioritization for exploitation
- **Weaponization** also maps to **Decide** because once the threat has prioritized how it will exploit a target, they will also find the vehicle with which to prepare to deploy

Phases 2 and 3 of the Cyber Kill Chain:

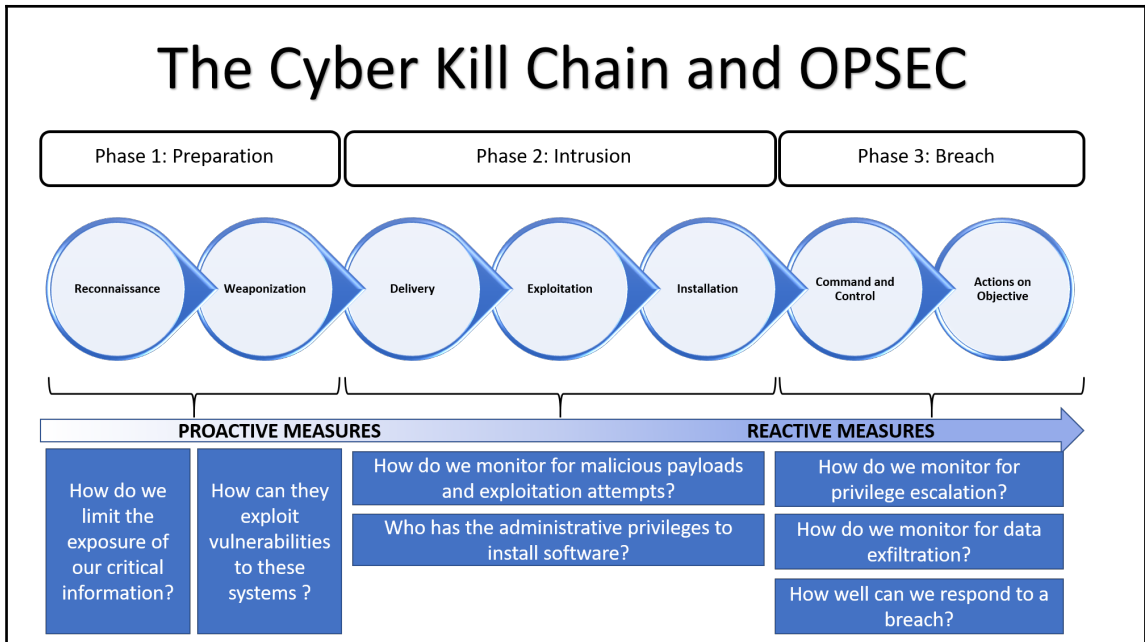
- **Act** maps to **Delivery** | **Exploitation** | **Installation** | **Command and Control** because these are the steps that are taken in order to initiate a successful **intrusion** and **breach** into a system
- Once the threat has access to and control of the targeted system we cycle back to **Observe** on **Actions on Objective** because the threat is now looking for additional opportunities to exploit resources to their advantage

## **Cyber Kill Chain and OPSEC**

Now that we've mapped the Cyber Kill Chain and OODA, we can now start looking at how this applies to the OPSEC process:

1. Identification of critical information and systems:
  - Where are my crown jewels and what systems are supporting them?
2. Analysis of threats:
  - Who wants our information and why?
  - How do they typically operate?
3. Analysis of vulnerabilities:
  - Where are the gaps in our defenses?
  - What are the capabilities that we lack?
4. Assessment of risk:
  - What is the probability of exploitation of vulnerabilities that may impact our organization's critical systems?
5. Application of appropriate countermeasures:
  - How can we be proactive in addressing potential exploitation opportunities?
  - How do we monitor, communicate, and mitigate at each step of the Cyber Kill Chain?

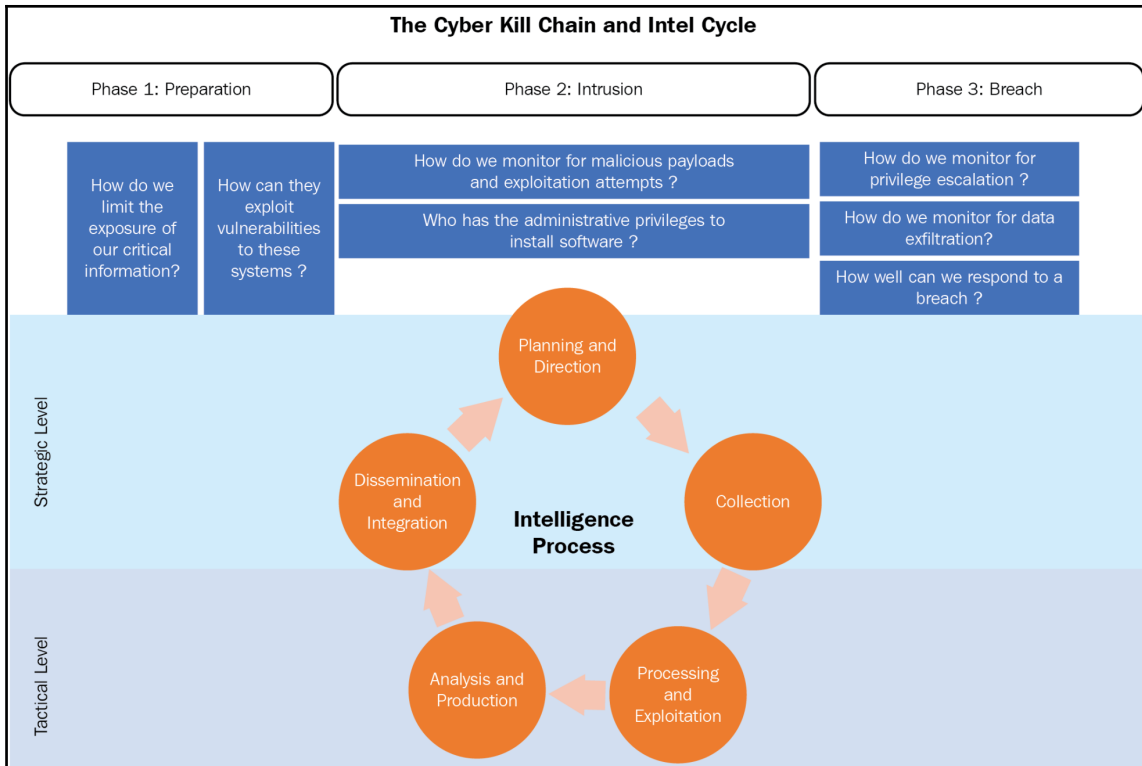
By understanding and evaluating step 1 to step 4, we can now look at the Cyber Kill Chain to answer step 5:





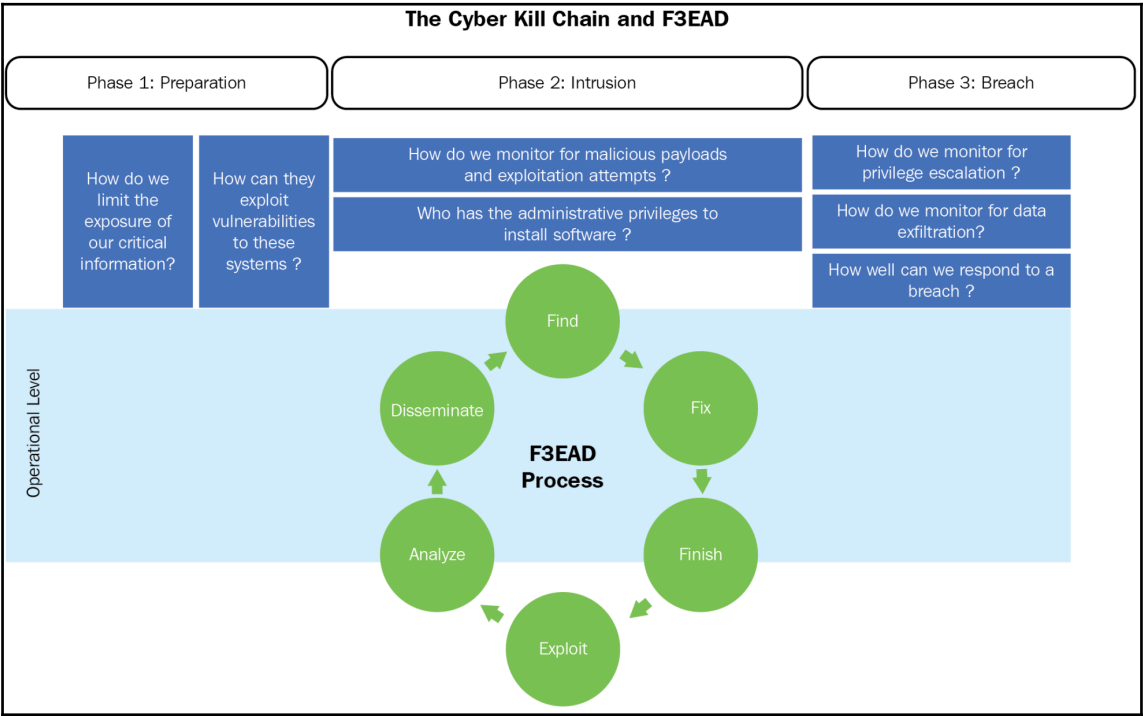
## Cyber Kill Chain and the intelligence cycle

Once we start looking at the different phases of the Cyber Kill Chain and map it to specific queries for OPSEC step 5, we can start looking at how we can collect the data to answer these questions at the **Strategic Level** and then **Tactical Level**.



# Cyber Kill Chain and F3EAD

After planning and direction is completed and prioritized at the strategic and Tactical Levels, the collection effort moves down to the operational level to the teams where they can use the F3EAD process to feed their analyses into the higher level intel process.



## Application of F3EAD in the commercial space

In war, there is a common enemy, with their own way of doing things. F3EAD is a continuous study of that common enemy and commanders continue to gather intelligence to help decide how to outmaneuver them.

It would be quite difficult if we were to use F3EAD as a framework in the commercial space as most organizations do not have dedicated assets for targeting specific threats.

The way that I envision the F3EAD process in the commercial space is that:

1. **Specialized teams:** Provide targeted operational information to the Tactical Level based on prioritized requirements
2. **Targeted capabilities project planning:** Allows us to look at how we can approach developing the cyber intelligence capability within our organizations
3. **IT operations / security integration for incident response:** Allows a holistic approach to incident response

The best way to describe how the F3EAD process works for those in the special forces community is that it is the same as the Agile Manifesto for the DevOps or DevSecOps community:

- It is an organizational culture, in that each member understands their responsibility to ensure the success of the organization through establishing lines of communication between each other on their targets so that they can complete the mission
- It is an understanding that information gathering on priority targets allows an organization's stakeholders to take decisive actions to achieve their missions
- It is knowing once decisive actions have been taken, that the resulting information will help drive actions on the next objective

All of the processes that we've learned up to this point are theoretical ways we can look at cyber intelligence as an enabler between operations and security. If we can see the importance of establishing the priorities of effort, communicating them across all parties, and starting to collect actionable information from the operational level through to the Tactical Level, then we can begin to grow as a team to be collaborative and act as one.

## Limitations of F3EAD

As with all processes, F3EAD has some limitations:

1. Intelligence is only as good as its source. If the top level intelligence is not correct, the resources will be wasted on the targeting efforts of the operational teams.
2. Priority information requests coming from the Tactical Level must be broken down into workable packages for the teams, or else teams will not be focused on a few things but many.

3. Targets have to be clearly defined and a definition of *done* must be established from the beginning, or else teams will be wasting their resources on a moving target.
4. Communication between all elements of the team has to be fluid and transparent, as decision-making within each part of the team demands it.

## Summary

In this chapter, we had a high-level review of the F3EAD process and its application in military special forces. To better understand how the F3EAD process fits into the bigger picture, we worked from the top down using the concepts that have been discussed in previous chapters. The F3EAD can be thought of as a variant and/or subprocess within the intelligence cycle that takes its inputs from Tactical Level *collection* priorities and outputs to the Tactical Level *analysis* step. As the Cyber Kill Chain is an example of the steps that are required to exploit an organization from an adversary's perspective, we've mapped these steps to the OODA loop to visualize the decision-making process. From there, we've related the phases of the Cyber Kill Chain to OPSEC and put into context how the intelligence cycle maps to how we can establish countermeasures. Next, we've learned how F3EAD fuels the tactical and strategic intel process cycle by providing information that is required for analysis from the operational level.

The next few chapters are going to be talking about how we can better implement specific information that we get from tools. The specific information that we are looking for comes from specialized teams, thus different disciplines of intelligence. Because there are different types of intelligence, we will introduce examples of Capability Maturity Models with milestones for each of the teams to meet a strategic target capability.

First up, is understanding how we incorporate **cyber threat intelligence** into the enterprise's operations.

# 6

# Integrating Threat Intelligence and Operations

This chapter is about threat intelligence and how we can incorporate it into our cyber intelligence program.

In this chapter, we will talk about:

- Overview of threat intelligence
- Sources of threat intelligence
- Information Sharing and Analysis Centers
- Capability Maturity Model – threat intelligence integration

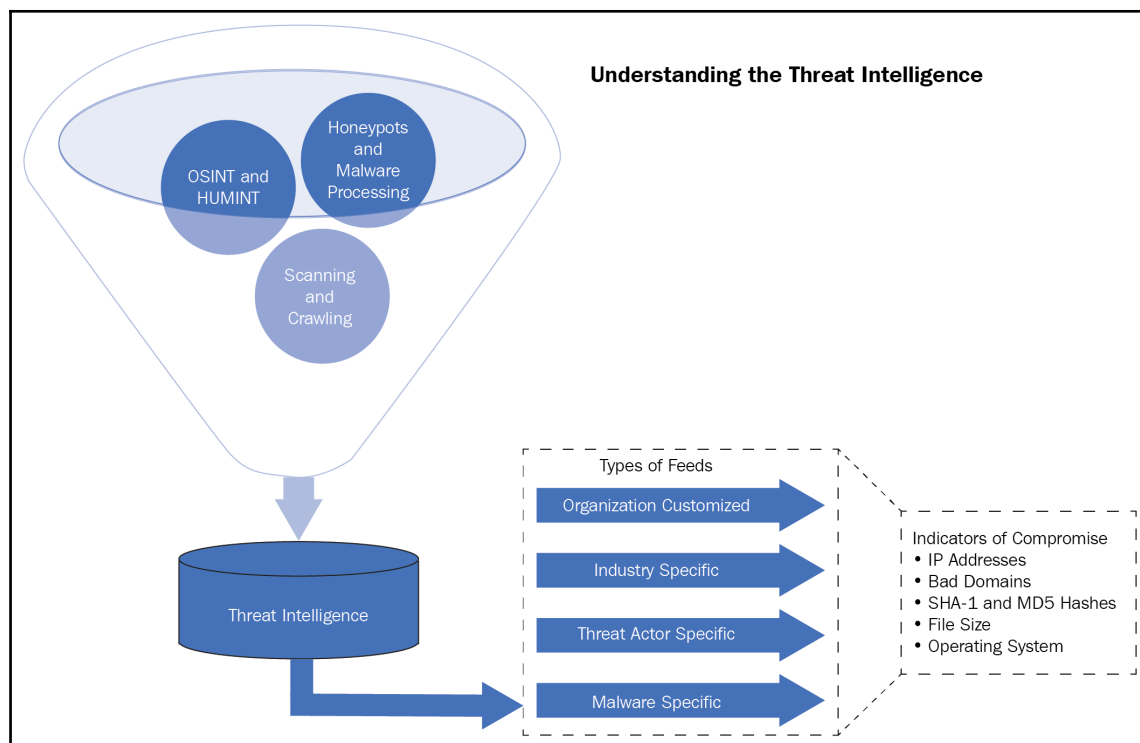
## Understanding threat intelligence

There are plenty of opinions as to what threat intelligence is or isn't. I've gone around and around with executives about its place in a security organization. Is it part of the incident response toolset? Is it a part of the vulnerability management toolset? Does it belong to the security operations center? Maybe it belongs to risk? Maybe it is its own service?

Depending on who you are talking to, they can make a case for each scenario.

My opinion is that the information that is derived from the threat intelligence feeds/tools are useful to all of the preceding questions. The information from these feeds must be tempered and tailored for use by all of these teams. We've discussed the importance of providing actionable information to stakeholders about decisions in the upper echelons of the organization in previous chapters.

We can look at threat intelligence as a means to provide actionable information from the tactical level to the operational level.



How do we do this? Let's first start with what threat intelligence is. Gartner (<https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms>) defines threat intelligence as:

*"evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."*

This *evidence-based* knowledge is gathered from several means, including:

- Honeypots
- Malware processing
- Open source
- Human intelligence

- Scanning
- Crawling

The information gathered from these activities contain items of **Indicators of Compromise (IoCs)** that are related to a specific threat. Some examples of IoCs are:

- IP addresses
- Bad domains/URLs
- SHA-1 and MD-5 hashes
- File sizes
- Operating system information

Ericka Chickowski wrote an article on Dark Reading where she highlights 15 key IoCs:

- Unusual outbound network traffic
- Anomalies in privileged user account activity
- Geographical irregularities
- Other log-in red flags
- Increases in database read volume
- HTML response sizes
- Large numbers of requests for the same file
- Mismatched port-application traffic
- Suspicious registry or system file changes
- Unusual DNS requests
- Unexpected patching of systems
- Mobile device profile changes
- Bundles of data in the wrong place
- Web traffic with unhuman behavior
- Signs of DDoS activity



*Top 15 Indicators Of Compromise* by Ericka Chichowski:

<https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?>

There are organizations and people who are dedicated to passing threat intelligence information to a wider and specific audience. These feeds can be specific to:

- Industry
- Threat actor
- Malware

You can find threat feeds that are provided as open source, or as a service provided from a vendor. However, as you are building the threat intelligence capability within your organization, you will be taking these feeds and making them more relevant to you.

## Capability Maturity Model – threat intelligence overview

Threat intelligence is a great tool to use if used correctly. The more I talk to folks around the world, I've realized that part of the problem is that even if they have the threat intelligence capability, the information that they get is really used only for reporting purposes. If there is one thing that isn't helpful it's a report *for reporting's* sake. If we cannot act on the information that we receive from the tools that we use, it was wasted time and effort to put the report information together in the first place!

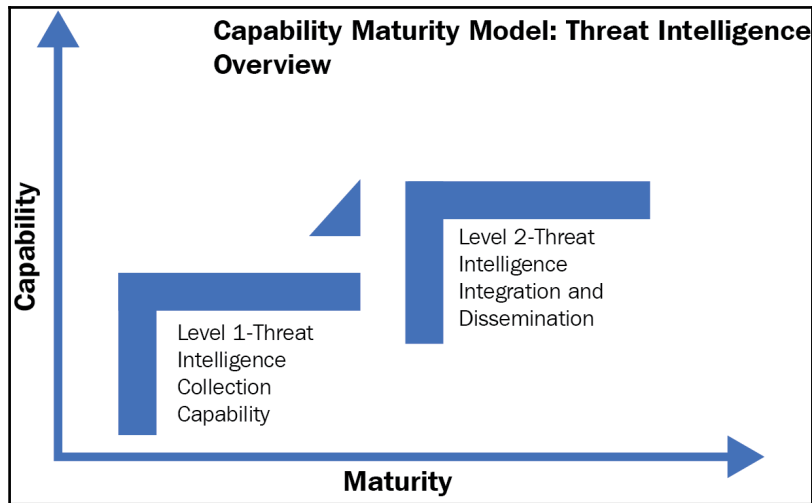
My point is that once we start talking about information, we want to analyze it to provide the most actionable items for our teams to take on. But before we start getting to that point, we need to know where we get the information from and how we can tailor it to our needs. For threat intelligence, I've created a two-level capability maturity model to specifically tackle a few things.

Capability Maturity Model—threat intelligence:

- **Level 1:** Threat intelligence collection capability:
  - At this level, we are going to discuss the phases of maturing the capability to collect the information that we need and make it relevant to our organization
- **Level 2:** Threat intelligence integration and dissemination:
  - At this level, we are going to take the information that we've gathered and go through the phases of maturing the process in which we can integrate it into the operational team



- We will also discuss what we can expect as outputs from the operational teams and how we can aggregate information to a threat intel dashboard for use at all levels of decision-making

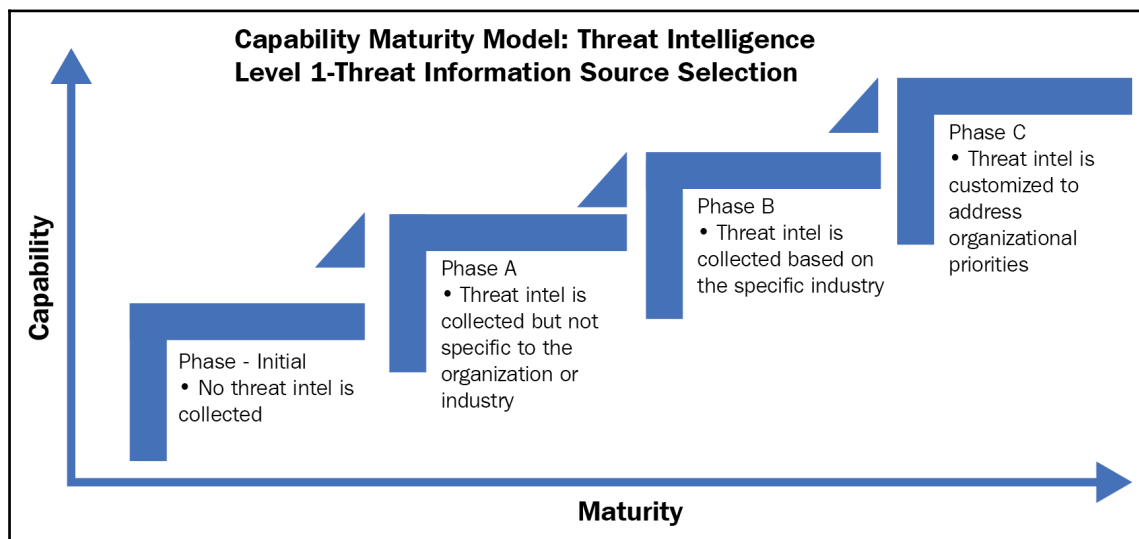


## Level 1 – threat intelligence collection capability

Threat intelligence level 1 is about building the collection capability of your organization. This level has four phases:

1. Initial
2. Phase A
3. Phase B
4. Phase C

The intent is to start from little to no intelligence gathering, to collecting large amounts of information, and to finally filtering out unnecessary information to prepare a more useful intelligence product for the organization.



## Phase initial

In this phase, an organization doesn't have a threat intelligence capability.

The objective for level 1 initial phase is to identify a threat intelligence feed.

So where do we begin? Let's start with finding feeds!

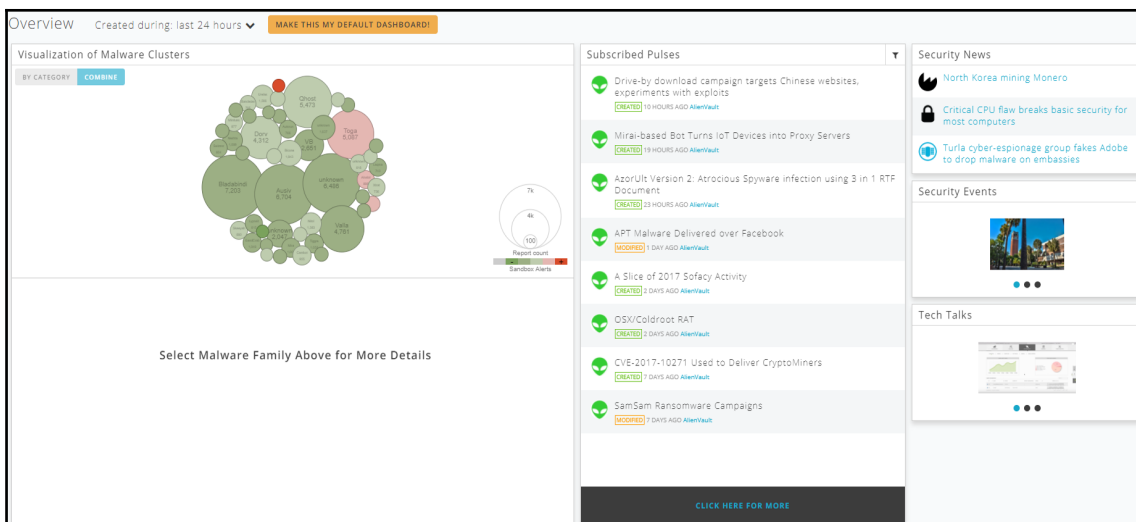
There are many feeds out there and the ones listed in the following section are some examples of where you can get threat intelligence.

### Example 1 – Open Threat Exchange – AlienVault

AlienVault proclaims that its Open Threat Exchange is *The world's first truly open threat intelligence community*. This tool is used globally by over 65,000 people that include security enthusiasts, researchers, and security professionals. It is community driven, meaning that information is provided by the users. This can have its own set of challenges, so beware! (<https://otx.alienvault.com/>)

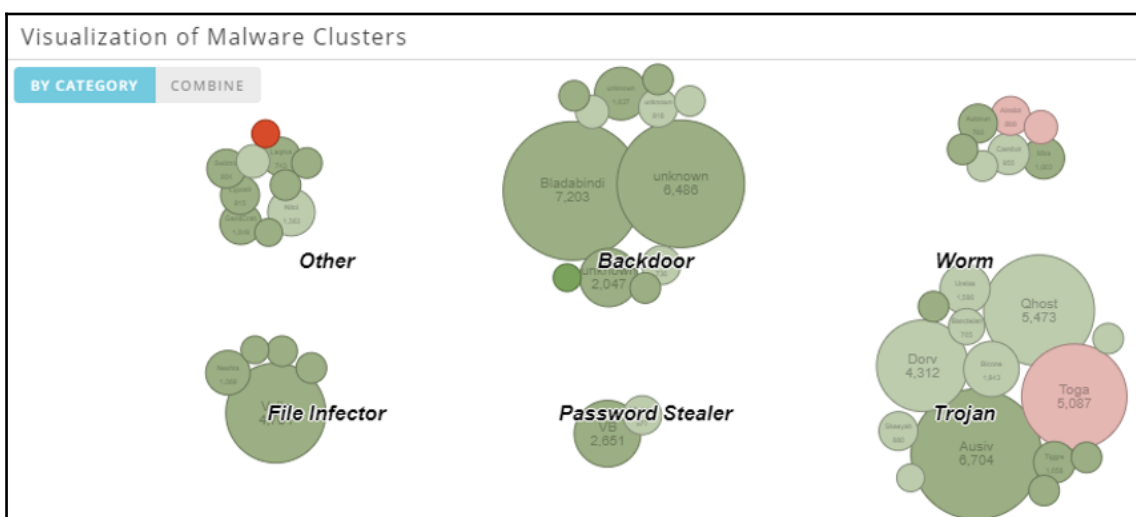
## AlienVault dashboard

The dashboard that is provided is relatively easy to understand:



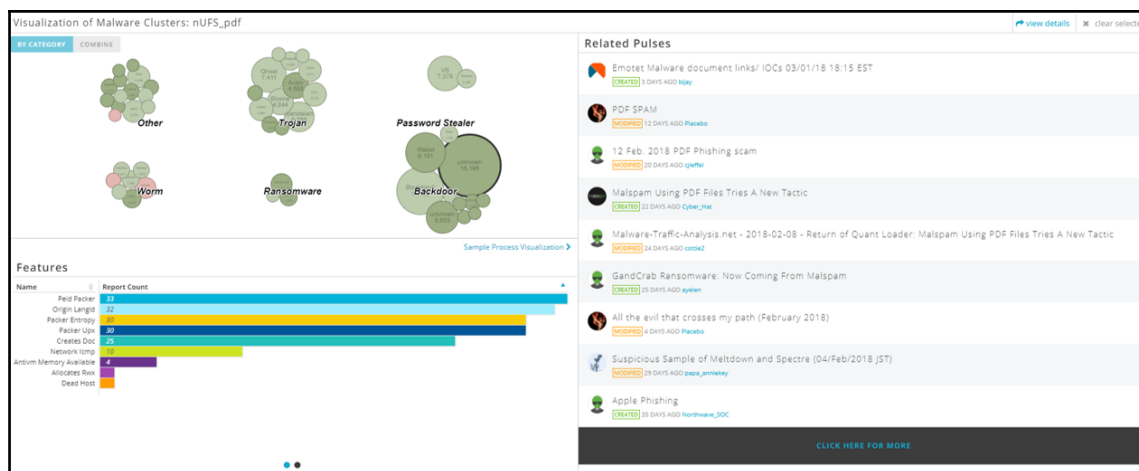
Users can use the **Visualization of Malware Clusters** in two ways:

- **BY CATEGORY:**



The preceding example is based on activity that has been reported within the last 24 hours. If we click on a specific bubble within a cluster, we will get more information about the type of malware that has been reported.

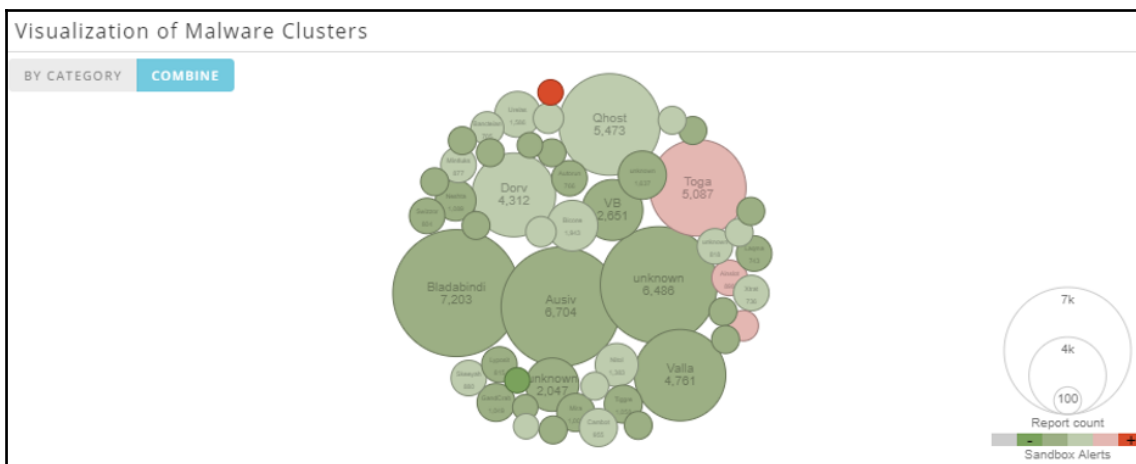
In the following example, the **Password Stealer** and **Backdoor** cluster have been selected. Notice the **Features** and **Related Pulses** sections:



Features show the names that are specific to the nUFS\_pdf malware being reported.

**Related Pulses** shows the pulses that have been reported on this specific malware.

- **COMBINE:** This view is another view that shows that clusters' all malware reported in the last 24 hours. Notice that in the bottom-right corner, there is **Report count**, which is represented by the size of the bubble. The larger the bubble, the more reports there have been. This means that we can visualize what is *hot* and what is *cold*, or not as *hot*, on the malware that is being reported on our feeds:



## AlienVault pulses

AlienVault OTX uses a pulse to provide a high-level view of the threats and their IoCs. These pulses can be later integrated into some network security tools such as pfSense, an open source firewall, and Suricata, another open source threat detection engine:

We've found 18,814 pulses

[SORT: RECENTLY CREATED](#) [SHOW: SHOW ALL PULSES](#)

**FEATURED THREAT INTELLIGENCE RESOURCE:**

**Free Guide to Open Source Network Security Tools**

[DOWNLOAD NOW](#)

**TELNET/SSH honeypot access IP 23/Feb/2018 : Location:Japan**

CREATED 3 MINUTES AGO by [papa\\_arnley](#) | Public | TLP: White

41 [SUBSCRIBE](#)

**TELNET/SSH honeypot access IP 22/Feb/2018 : Location:Japan**

CREATED 4 MINUTES AGO by [papa\\_arnley](#) | Public | TLP: White

41 [SUBSCRIBE](#)

**Go Daddy Phish**

CREATED 1 HOUR AGO by [dymenick](#) | Public | TLP: White

URL: 1 | Domain: 1 | Email: 2

Hi, GoDaddy has upgraded email security. Click here to enjoy maximum protection. You will be prompted to sign in again. No further action is required after a successful sign-in. Thank you. GoDaddy Support Te...

1 [SUBSCRIBE](#)

**Oops! OilRig Uses ThreeDollars to Deliver New Trojan**

CREATED 2 HOURS AGO by [mpetwos](#) | Public | TLP: White

Filehash-SHA256: 1 | Domain: 1 | Hostname: 1 | IPv4: 3

The OilRig group remains highly active in their attack campaigns while they continue to evolve their toolset. On January 8, 2018, Unit 42 observed the OilRig threat group carry out an attack on an insurance agen...

42 [SUBSCRIBE](#)

**test pulse**

CREATED 3 HOURS AGO by [branjali](#) | Public | TLP: Green

IPv4: 1

0 [SUBSCRIBE](#)

Pulses can be broken down further by:

- **User-specific user contributions:** Security researchers post their findings for other users to use in their threat intelligence analysis processes:

We've found 52,825 users			SORT: MOST PULSES ▾		
	JNAZARIO 648 DAYS AGO 2225 PULSES   0 CONTRIBUTIONS	445 FOLLOWERS	486 SUBSCRIBERS	679931 CONTRIBUTED INDICATORS	
	MARCORAMILLI 281 DAYS AGO 2222 PULSES   0 CONTRIBUTIONS	216 FOLLOWERS	240 SUBSCRIBERS	558158 CONTRIBUTED INDICATORS	
	MALWAREPATROL 864 DAYS AGO 1679 PULSES   0 CONTRIBUTIONS	502 FOLLOWERS	692 SUBSCRIBERS	64587 CONTRIBUTED INDICATORS	
	METADEFENDER 280 DAYS AGO 1189 PULSES   0 CONTRIBUTIONS	59 FOLLOWERS	136 SUBSCRIBERS	3198831 CONTRIBUTED INDICATORS	
	ALIENVAULT 1106 DAYS AGO 1181 PULSES   110 CONTRIBUTIONS	1628 FOLLOWERS	49963 SUBSCRIBERS	62489 CONTRIBUTED INDICATORS	
	BURBERRY 725 DAYS AGO 976 PULSES   15 CONTRIBUTIONS	361 FOLLOWERS	450 SUBSCRIBERS	321536 CONTRIBUTED INDICATORS	

- **Groups-based on interest:** Groups of security researchers post their research findings for other users to use in their threat intelligence analysis processes:

A screenshot of a web interface showing a list of threat intelligence groups. Each group entry includes a profile picture, a name, a 'CREATED' timestamp, a description, and member/pulse counts.

Group Name	Created	Description	Members	Pulses
Spyware	4 HOURS AGO		1	0
APT	2 YEARS AGO	For those focused on intel related to Advanced Persistent Threats.		86
Blue Team Intelligence - Open Forum	2 YEARS AGO	A place for Infosec teams and researchers to collaborate and share threat data observed in the wild or their corporate environments. In your request for access please include your twitter handle, your role(s) in infosec, and your intent to share/consume threat intelligence. Always, always, verify your threat data before posting IOC's and APT activity. The more accurate your intel is the better it serves the...	383	258
MISP FEED	4 YEAR AGO	Intel added to this group feed downstream MISP platforms through the API key	349	1,277
Nuisances which waste server time and bandwidth	9 MONTHS AGO	As the name already says it loud and clear: Spam/harvester/proxy morons which waste server time and bandwidth :)	4	16

- **Indicators:** The use of indicators to narrow down threat intelligence research on malware or attacks:

A screenshot of a web interface showing a list of threat intelligence indicators. The interface includes a header with the total count of indicators and a sort button. The list contains five entries, each with an indicator name and its type.

We've found 2,759,678 indicators SORT: NAME ASCENDING

Indicator	Type
`-javascript:alert(1)-`	FilePath
__wretw_w4523_345	Mutex
_DECRYPT_FILE.html	FilePath
_DECRYPT_FILE.txt	FilePath
_sipfederationtls._tcp.40gmail.com	

- **Malware families:** Results based on the different families of malware:


We've found 9,220 malware

SORT: ▾


Backdoor:MSIL/Bladabindi	83
Category: Backdoor	PULSES
Virus:Win32/Nabucur	29
Category: File Infector	PULSES
Trojan:Win32/Skeeyah	18
Category: Trojan	PULSES
Worm:Win32/Mira	1
Category: Worm	PULSE
Worm:Win32/Allaple	55
Category: Worm	PULSES

- **Industries:** Threat intel feed results based on a particular industry:


We've found 17 industries




Aerospace




Agriculture




Chemical




Construction



Defense



Education



Energy

SORT: DESCENDING

- **Adversaries:** Threat intel feed results based on a particular adversary:





## Example 2 - Twitter

Social media is a powerful communications tool and Twitter is an example of how information can quickly be spread with less than 140 characters. We can follow information security researchers, companies, keywords, and so on to get the latest tweets on what is going on in the world. Be forewarned that there is a lot of noise to filter through because anyone can hashtag a keyword in their tweets.

However, every once in a while, you can get some good information to take action on. Here are some examples of things that you can search:

- #0day
- #zeroday
- #exploit
- #vulnerability
- #threatintel
- #infosec



Did you know that squirrels are more of a threat to the critical infrastructure of the US than a cyber attack is? Forget Stuxnet. Squirrels are the real problem and apparently, they are winning the **industrial control system (ICS)** cyber war.

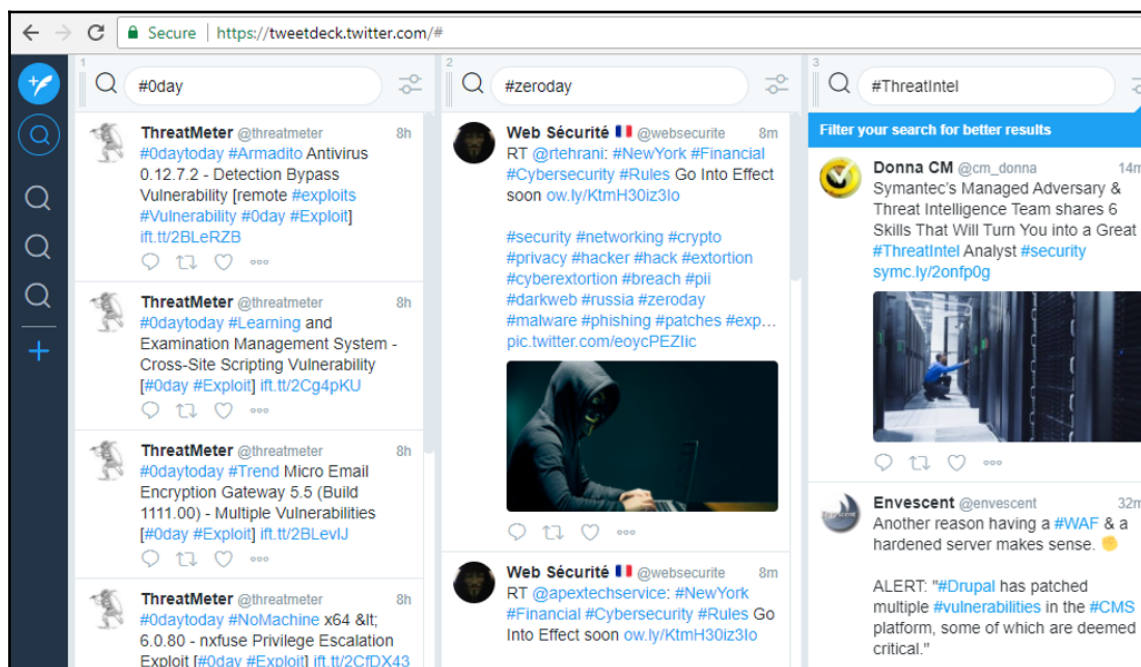
@CyberSquirrel1  
#Cyberwar4ever

## TweetDeck

I like using TweetDeck (<https://tweetdeck.twitter.com/>) for OSINT because it is free and it takes the hassle out of going through my entire Twitter feed and searching each hashtag. TweetDeck allows us to add columns on the items that we want to search.

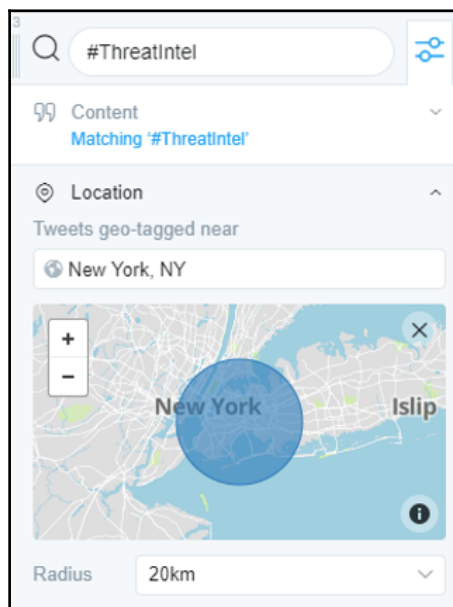
Here are columns that I've created for the following hashtags:

- #0day
- #zeroday
- #ThreatIntel

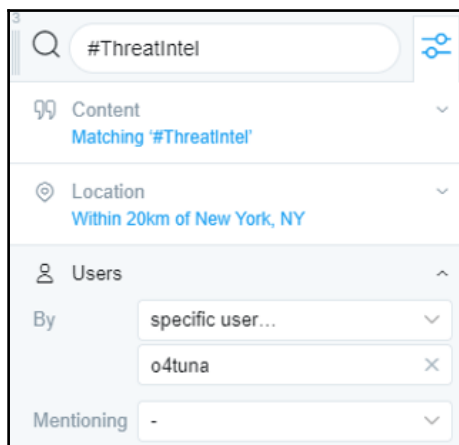


If we want to dig deeper into the Twitter-verse, we can filter tweets based on specific attributes:

- **Location:** Specify if a specific threat is coming from a certain area:

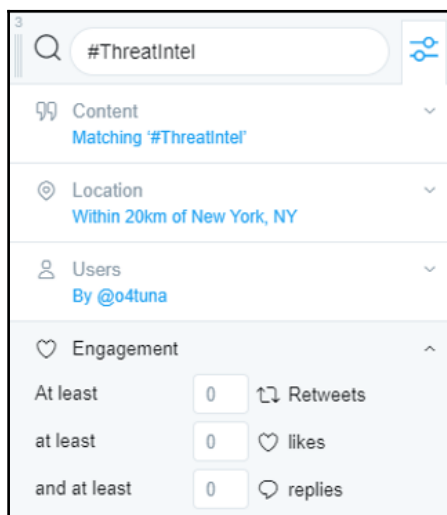


- **User:** Using the handles of groups or users that you are interested in:



A screenshot of a search filter interface. At the top is a search bar containing the text "#ThreatIntel". Below the search bar are three filter categories: "Content" with the value "Matching '#ThreatIntel'", "Location" with the value "Within 20km of New York, NY", and "Users". The "Users" filter is expanded, showing a "By" dropdown menu with the value "specific user...", a text input field containing "o4tuna", and a "Mentioning" dropdown menu with the value "-".

- **Engagement:** Using the number of times a tweet is retweeted as a metric to filter out more tweets:



A screenshot of a search filter interface, similar to the one above. It shows the same search bar and "Content" and "Location" filters. The "Users" filter is now collapsed, and the "Engagement" filter is expanded. The "Engagement" filter section contains three rows of options: "At least" with a value of "0" and a "Retweets" icon, "at least" with a value of "0" and a "likes" icon, and "and at least" with a value of "0" and a "replies" icon.

### Example 3 - Information Sharing and Analysis Centers

Information Sharing and Analysis Centers are another source of threat intelligence as they provide feeds for their specific member organizations. These organizations are sorted by sector such as finance, manufacturing, or defense, and the most recent threat feeds are provided to members.

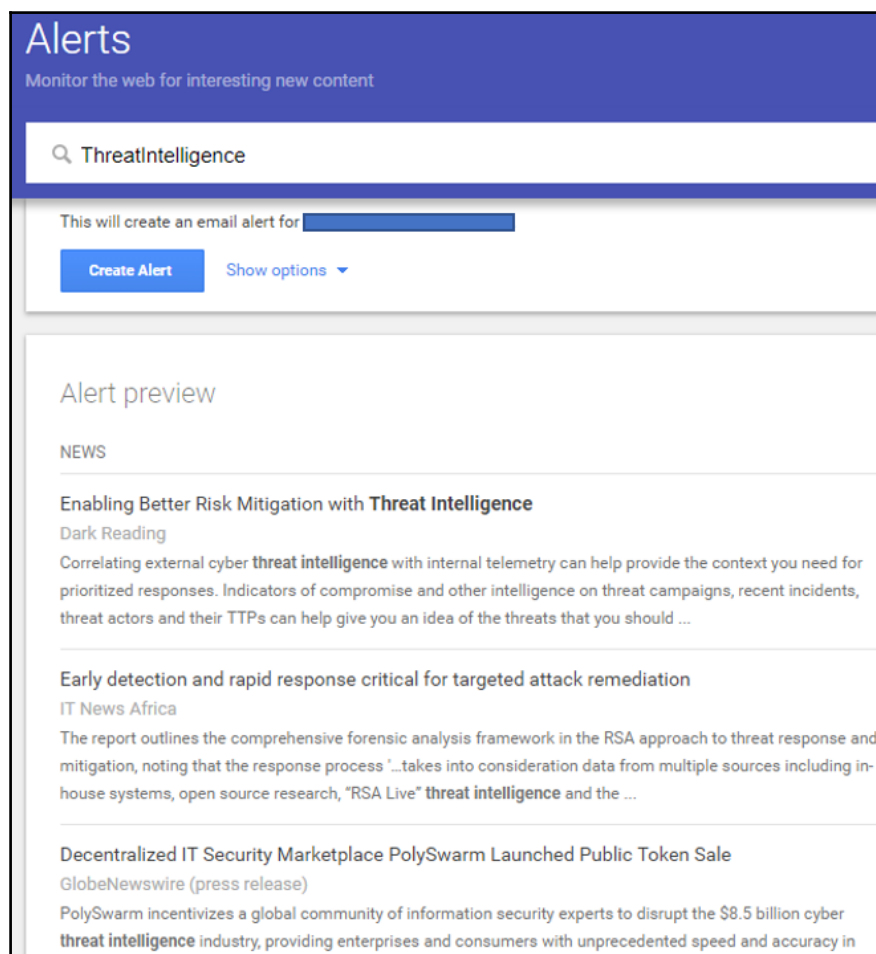
Here is a list of ISACs from the *National Council of ISACs*:

- **AUTOMOTIVE ISAC:** [www.automotiveisac.com](http://www.automotiveisac.com)
- **AVIATION ISAC:** [www.a-isac.com](http://www.a-isac.com)
- **COMMUNICATIONS ISAC:** [www.dhs.gov/national-coordinating-center-communications](http://www.dhs.gov/national-coordinating-center-communications)
- **DEFENSE INDUSTRIAL BASE ISAC:** [www.dibisac.net](http://www.dibisac.net)
- **DOWNSTREAM NATURAL GAS ISAC:** [www.dngisac.com](http://www.dngisac.com)
- **ELECTRICITY ISAC:** [www.eisac.com](http://www.eisac.com)
- **EMERGENCY MANAGEMENT AND RESPONSE ISAC:** [www.usfa.dhs.gov/emr-isac](http://www.usfa.dhs.gov/emr-isac)
- **FINANCIAL SERVICES ISAC:** [www.fsisac.com](http://www.fsisac.com)
- **HEALTHCARE READY:** [www.healthcareready.org](http://www.healthcareready.org)
- **INFORMATION TECHNOLOGY ISAC:** [www.it-isac.org](http://www.it-isac.org)
- **MARITIME ISAC:** [www.maritimesecurity.org](http://www.maritimesecurity.org)
- **MULTI-STATE ISAC:** [www.ms-isac.org](http://www.ms-isac.org)
- **NATIONAL DEFENSE ISAC:** [www.ndisac.org](http://www.ndisac.org)
- **NATIONAL HEALTH ISAC:** [www.nhisac.org](http://www.nhisac.org)
- **OIL & NATURAL GAS ISAC:** [www.ongisac.org](http://www.ongisac.org)
- **REAL ESTATE ISAC:** [www.reisac.org](http://www.reisac.org)
- **RESEARCH AND EDUCATION NETWORK ISAC:** [www.ren-isac.net](http://www.ren-isac.net)
- **RETAIL CYBER INTELLIGENCE SHARING CENTER:** [www.r-cisc.org](http://www.r-cisc.org)
- **SURFACE TRANSPORTATION, PUBLIC TRANSPORTATION AND OVER-THE-ROAD BUS ISACS:** [www.surfacetransportationisac.org](http://www.surfacetransportationisac.org)
- **WATER ISAC:** [www.waterisac.org](http://www.waterisac.org)

## Example 4 - news alert notifications

Another information source is having an email sent to you based on search criteria.

An example of this is using Google Alerts:



The screenshot shows the Google Alerts web interface. At the top, the word "Alerts" is displayed in a large font, with the subtitle "Monitor the web for interesting new content" below it. A search bar contains the text "ThreatIntelligence". Below the search bar, a message states "This will create an email alert for" followed by a blue rectangular box. To the right of this box are two buttons: "Create Alert" and "Show options" with a downward arrow. Below this section is an "Alert preview" area. It starts with the word "NEWS" in all caps. The first preview item is titled "Enabling Better Risk Mitigation with Threat Intelligence" by "Dark Reading". The text below the title reads: "Correlating external cyber threat intelligence with internal telemetry can help provide the context you need for prioritized responses. Indicators of compromise and other intelligence on threat campaigns, recent incidents, threat actors and their TTPs can help give you an idea of the threats that you should ...". The second preview item is titled "Early detection and rapid response critical for targeted attack remediation" by "IT News Africa". The text below the title reads: "The report outlines the comprehensive forensic analysis framework in the RSA approach to threat response and mitigation, noting that the response process '...takes into consideration data from multiple sources including in-house systems, open source research, 'RSA Live' threat intelligence and the ...". The third preview item is titled "Decentralized IT Security Marketplace PolySwarm Launched Public Token Sale" by "GlobeNewswire (press release)". The text below the title reads: "PolySwarm incentivizes a global community of information security experts to disrupt the \$8.5 billion cyber threat intelligence industry, providing enterprises and consumers with unprecedented speed and accuracy in".



These are helpful, but can really overwhelm your inbox if you are not very specific on what you want delivered to you. For example: *threat intelligence* is a very broad query to receive news from. *Threat intelligence, Africa* will limit the search to articles with *threat intelligence* and *Africa*.

## Example 5 - Rich Site Summary feeds

**Rich Site Summary (RSS)** feeds are widely used to access updates to information from various sources in a format that is computer readable. Many cyber security, industrial security, and news organizations, as well as other groups, have their own RSS feeds that you can tap into to get the most up-to-date content.

Here are a few that we can start from:

- **Government defense:**
  - **National Vulnerability Database:** <https://nvd.nist.gov/download/nvd-rss.xml>
  - **US CERT National Cyber Awareness System Alerts:** <https://www.us-cert.gov/ncas/alerts.xml>
  - **US CERT National Cyber Awareness System: Current Activity:** <https://www.us-cert.gov/ncas/current-activity.xml>
- **Product security:**
  - **Threatpost:** [https://www.kaspersky.com/blog/feed/?\\_=9489](https://www.kaspersky.com/blog/feed/?_=9489)
  - **Adobe Product Security Incident Response Team:** <http://blogs.adobe.com/psirt/?feed=rss2>
  - **Cisco Security Advisory:** <http://tools.cisco.com/security/center/psirt/rss2/CiscoSecurityAdvisory.xml>
  - **CheckPoint Security Update Advisories:** [http://www.checkpoint.com/defense/advisories/public/smartdefense\\_atomz.xml](http://www.checkpoint.com/defense/advisories/public/smartdefense_atomz.xml)
- **Information security groups:**
  - **Latest hacking news:** <https://newsblur.com/site/6044769/latest-hacking-news>
  - **The Hacker News:** <http://feeds.feedburner.com/TheHackersNews>

We will need a place to aggregate these feeds to, so we must choose an RSS reader:

- **Feedly:** [www.feedly.com](http://www.feedly.com)
- **NewBlur:** [www.newsblur.com](http://www.newsblur.com)
- **Digg:** [www.digg.com](http://www.digg.com)
- **Inoreader:** [www.inoreader.com](http://www.inoreader.com)
- **The Old Reader:** [www.theoldreader.com/](http://www.theoldreader.com/)
- **G2Reader:** [www.g2reader.com](http://www.g2reader.com)
- **Feeder:** [www.feeder.co](http://www.feeder.co)

Whichever RSS reader that we pick, we will be able to continue to filter out keywords or topics from multiple RSS feeds one at a time.

## Phase A

Now that we have researched where we want to get our threat intelligence from, we should recognize the sheer amount of information that will be coming to us. Before we get into the relevance of the information in respect to the organization, we must now have a place to collect all of it. Phase A will be complete once we have identified the **platform** that we will use to aggregate all of the data in preparation for analysis.

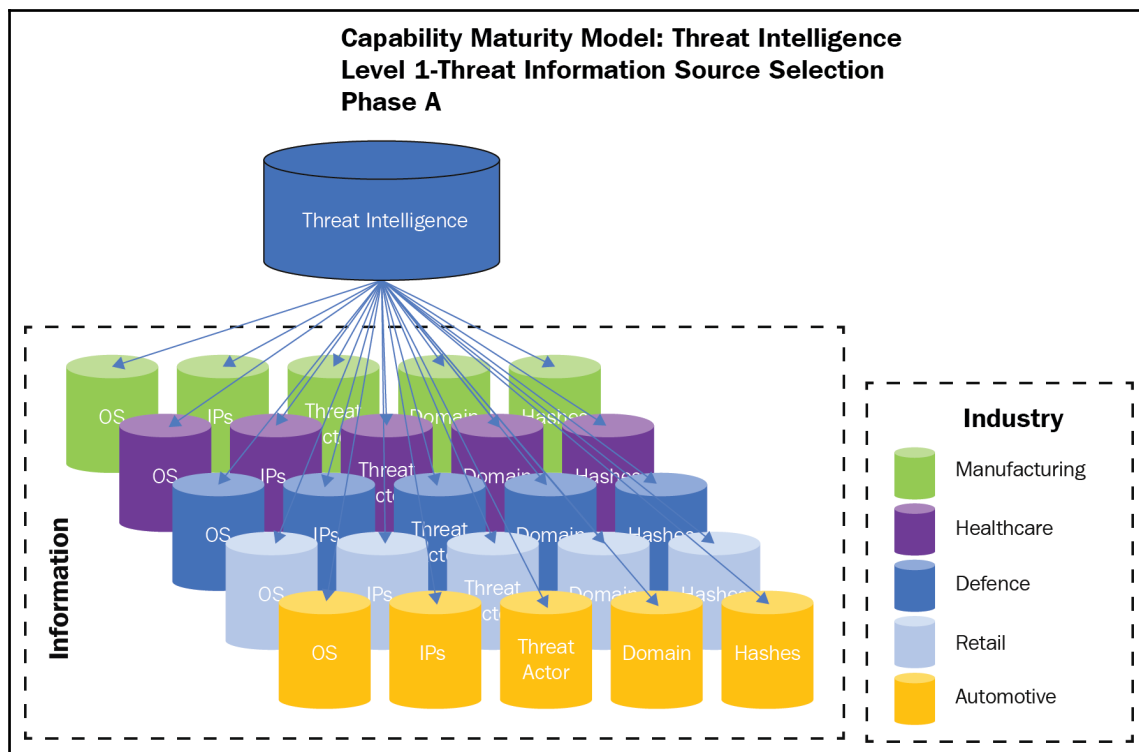
### Objectives for level 1 phase A:

- Identify a threat intelligence platform
- Begin to consume raw threat intelligence



A threat intelligence platform is a tool that allows for the aggregation of multiple information/source feeds so that they can be processed, analyzed, and prepared for distribution definition.





Although there are plenty of premium options for threat intelligence platforms, here are a few community-driven, open source threat intelligence platforms.

To better understand the information that is coming in, we will need a framework to process the threat feed information. This is where these platforms fit in. These tools will take structured and unstructured threat intelligence and put it in a format that can be reviewed by a security analyst or team member. To help enrich the data, the framework will reconcile with third parties for similar IOCs that have been submitted, which will also allow stakeholders to prioritize or address potential threats.

## Example 1 - Cisco – GOSINT platform

The GOSINT framework is a project from Cisco that can be used for collecting, processing, and exporting high-quality IoCs:

- **GitHub website:** <https://github.com/ciscocsirt/gosint>
- **Documentation:** <http://gosint.readthedocs.io/en/latest/>

## Example 2 - The Malware Information Sharing Platform project

Another piece of open source software dedicated on sharing threat intelligence is the **Malware Information Sharing Platform (MISP)** project. Its platform's primary goal is to make threat intelligence information useful for organizations by keeping it utilitarian. IOCs are provided in a way to allow for correlation and automation of data for use in IDS or SIEMs. The MISP project is also another tool that is powered by input and the collaboration of the community.

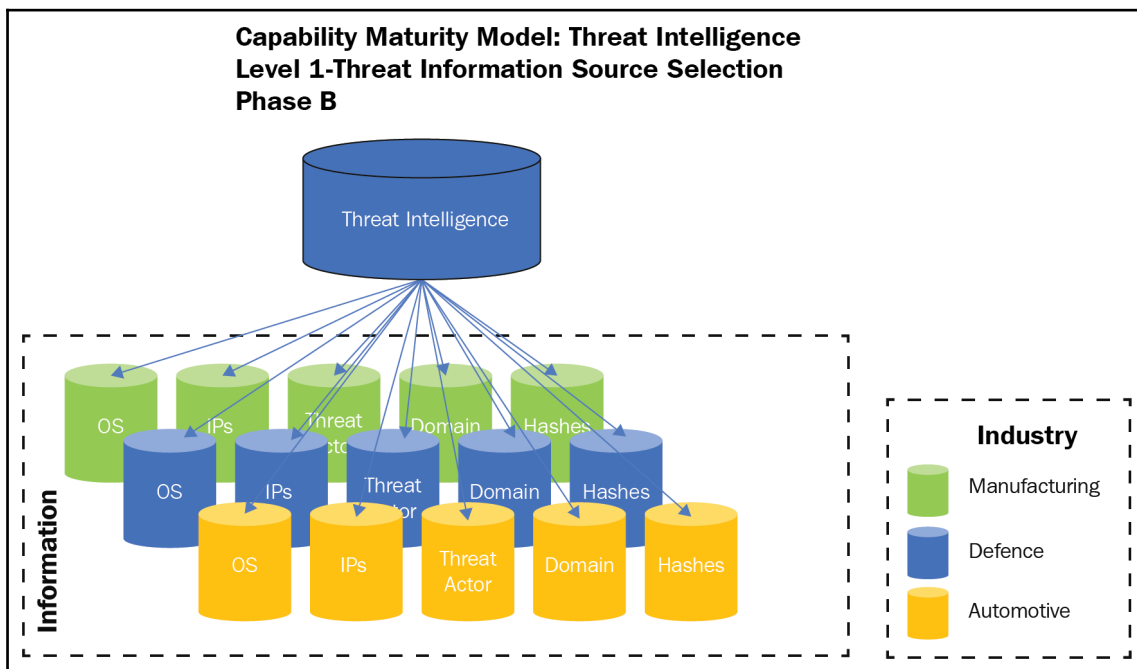
For more information on this, please go to the following site: <http://www.misp-project.org/>.

## Phase B

At this point, we will need to begin to filter out the information that we are receiving to be more applicable to our organization. In the following example, the threat intelligence that is collected is now being sorted by the example organization. In this case, the OS, IP, threat actor, domain, and hash information is collected by the manufacturing, defense, and automotive threat intelligence sources.

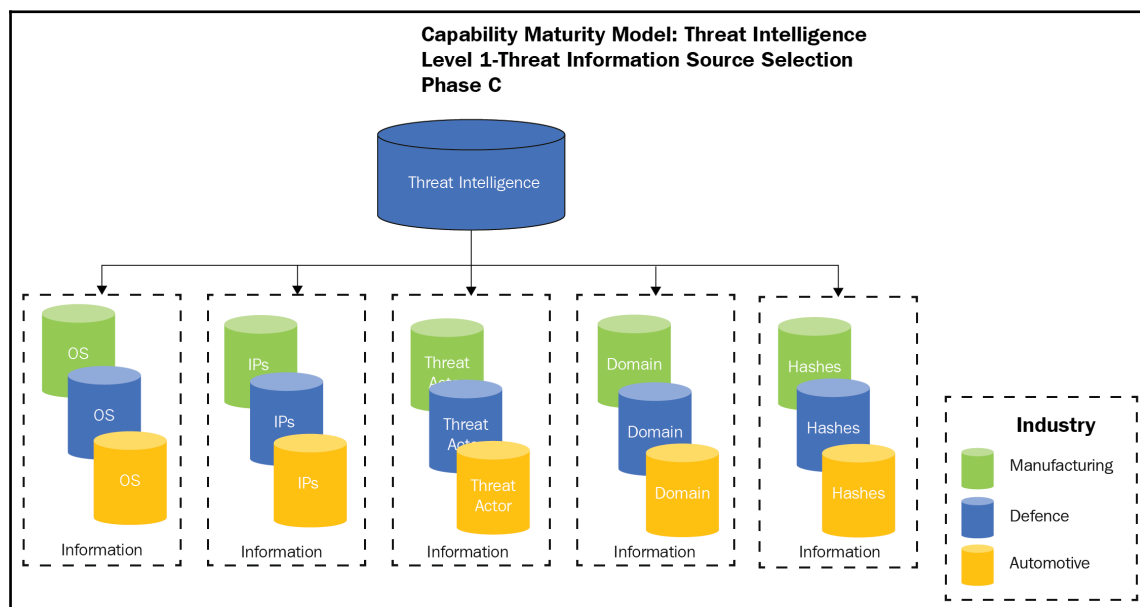
**Objectives for level 1 phase B:**

- Filter out threat feeds to only include the most relevant to your organization
- Begin to identify attributes of threat information that will provide value to your organization

**Phase C**

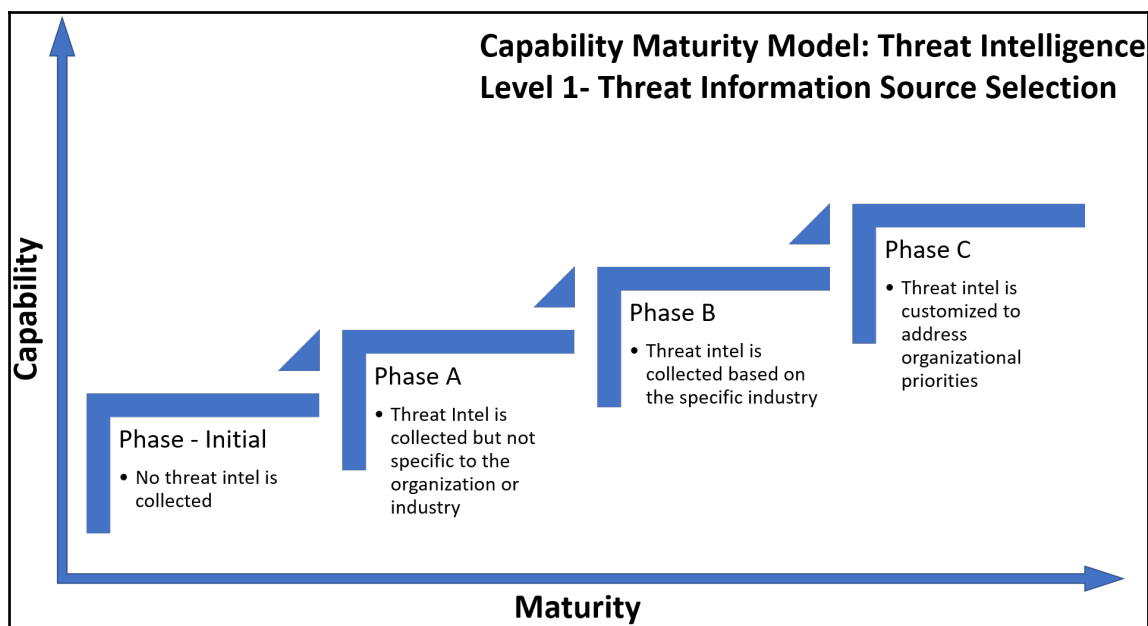
During this phase, we will build the capability to sort out the information based on its attributes. This is in preparation for creating intelligence packages to be distributed to the different teams for action or review.

**Objective for level 1 phase C:** Separate information by attributes:



## Level 2 – Threat Information Integration

Now that we've separated the threat intelligence based on attributes and industry, we need to recognize that all of this information will not be applicable to every party, for example, your help desk technicians not understanding how to use hash values from your threat intelligence like a cyber security incident responder. However, if you know that a particular threat actor is engaging targets in a specific region, you may use that information to pass on to your help desk techs so that they can report any unusual outages or requests.



## Phase initial

In this phase, we are gathering the intelligence, but it has yet to begin to be integrated with teams. What will be important to achieve during this phase is to build the foundation to pass the most pertinent information on to the teams. Therefore, it is important that all of the critical applications and all business-critical information is understood and identified.

### Objective for level 1 phase initial:

- 80/20% assurance of the identification of critical applications and information
- Establishing a *responsible, accountable, supporting, consulted, and informed* matrix for each application



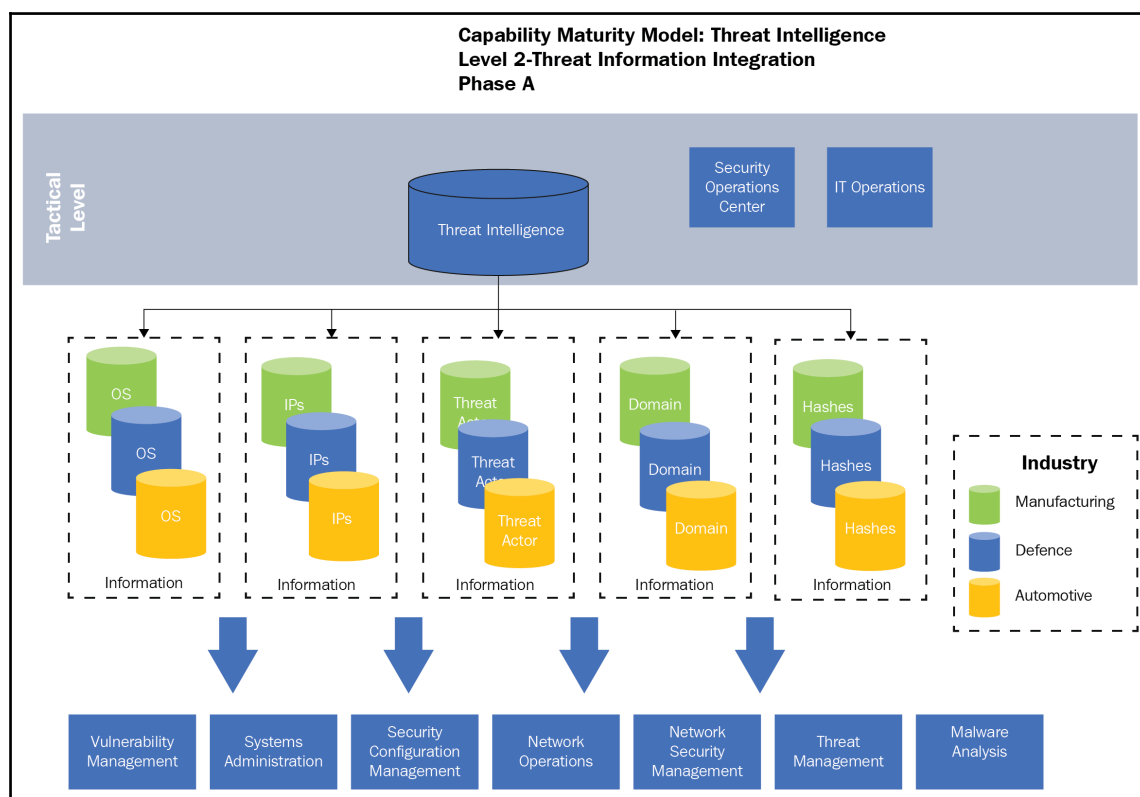
A *responsible, accountable, supporting, consulted, and informed* matrix is used for understanding the roles and responsibilities of cross-functional teams. It is commonly used in project management methodologies, contracts between service providers and clients, as well as understanding the responsibility of processes that interface between teams.

## Phase A

Once we understand our critical applications and information, as well as who to pass on information to, we need this pseudo-mature information to be passed to the teams.

Level 2 phase A has the following objectives:

- Begin the integration of the threat intelligence capability with both the security operations center and IT operations center
- Begin to pass threat intelligence information down to the teams
- Basic internal reporting from teams on their status



## **Categorization of items that are applicable to multiple teams**

To enable an intelligence package to be useful, at this point we need to ask ourselves:

- What information is applicable to the teams?
  - Vulnerability management, security configuration management, and systems administration may need to know OS information and IP information
  - Network security and continuous security monitoring may need to know IP information and domain information
  - Threat intel management and malware analysis may need to know TTP information and hash information
- Who are the key stakeholders that need to know this information?
- How does it need to be delivered?

## **Phase B**

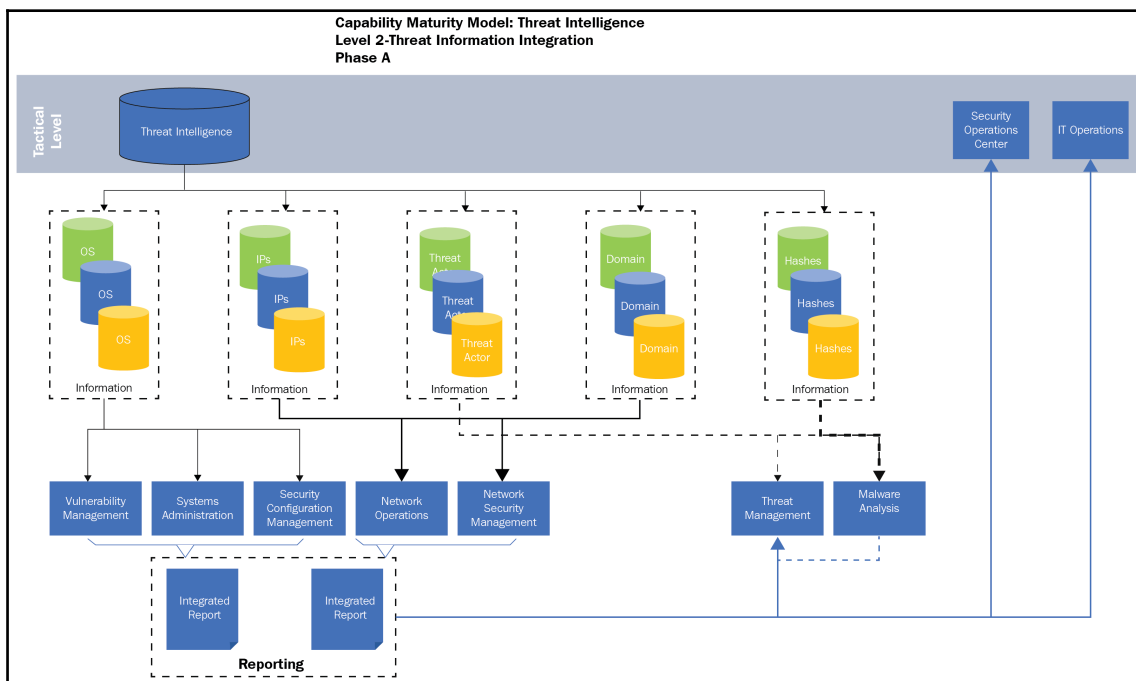
Now that we have information flowing to teams individually, there will need to be more customization for information being passed to be useable. During this phase, we will begin to combine the threat intelligence information and measure our progress to address findings through trend analyses.

Examples:

- Combining the total amount of vulnerabilities and OS configuration compliance for a specific application and providing a trend analysis on remediation efforts
- Network operations and network security teams working together to close ports and block IPs based on threat intel received, and also reporting the trend in remediation efforts

Level 2 phase B has the following objectives:

- Teams begin to combine reports to show security and IT ops a clearer picture of vulnerabilities that exist based on threat intelligence information



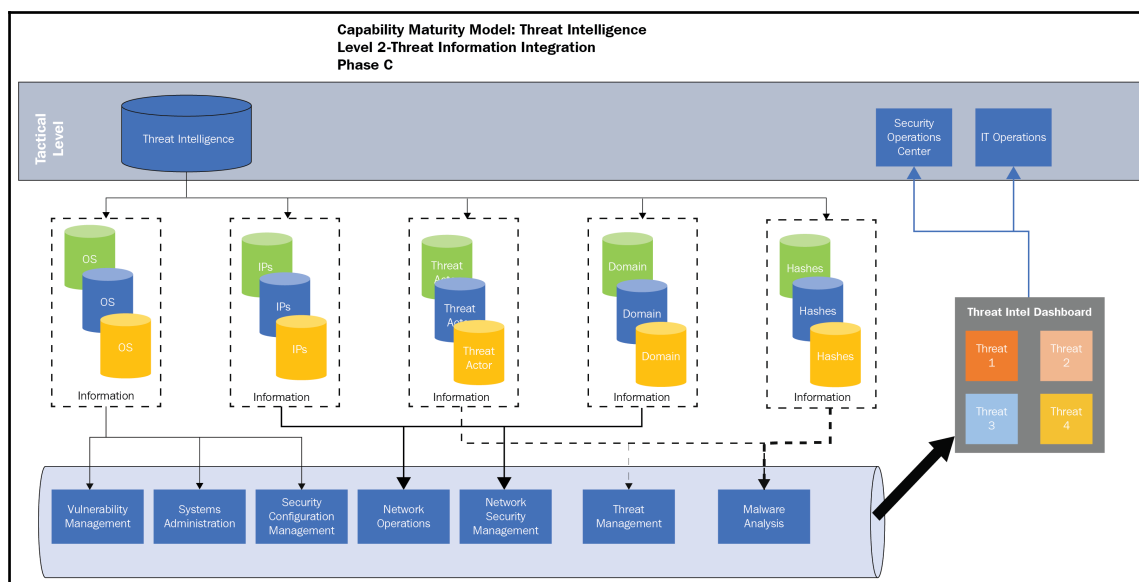
## Phase C

The final phase of threat intelligence level 2 is concerned with being able to take all of the information and effectively use it to proactively address threats based on their probability and impact.

Level 2 phase C has the following objectives:

- Teams are communicating with each other and understanding specific threats through a threat dashboard
- Threats are addressed based on the measurement of risk (more on this later)





Conceptually, the threat intelligence Capability Maturity Model is easily understood. However, although we can understand the theory behind the model itself, it is in the implementation where we will find it more difficult.

## Summary

In this chapter, we had a high-level overview of threat intelligence and where we can find it. These sources can be from ISACs or from OSINT sources such as Twitter. Being able to consolidate all of this information is important because we will need to process it so that we can create intelligence for the teams who will be responsible for reducing the risk and mitigating the vulnerabilities. By providing a Capability Maturity Model to follow, we can build the communication capability to push information down to the teams, as well as be able to follow the results. Ultimately, we want to have a tight integration between teams to provide the most correct and most complete information, so that we can possibly produce a dashboard that highlights the known threats, their probability, and their impact to the organization.

In the next chapter, we will dig a little deeper into communication and how we can build channels to enable teams.

# 7

## Creating the Collaboration Capability

This chapter is about how we can establish the collaboration capability to support our cyber intelligence program.

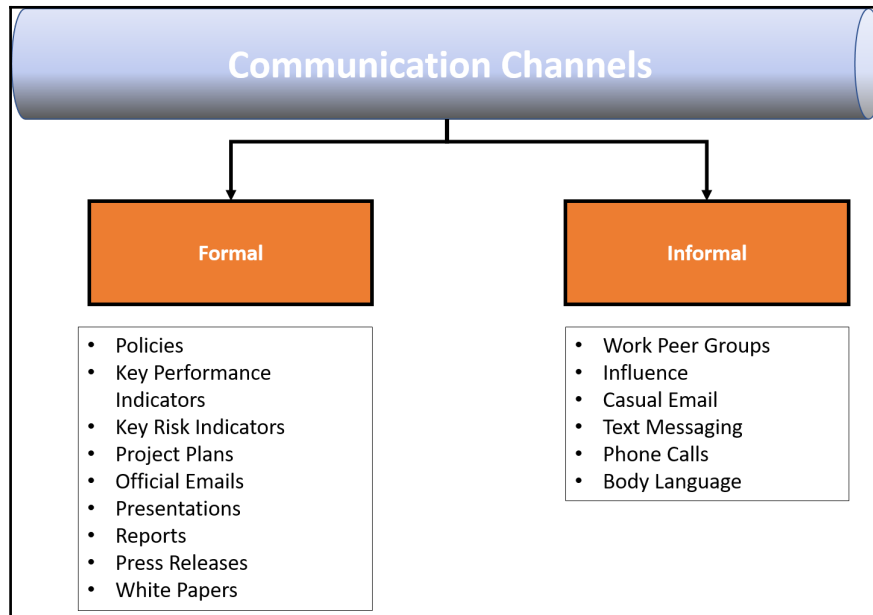
In this chapter, we will discuss:

- Purpose of the collaboration capability
- Communication channels
- Methods and tools for collaboration
- Strategic, tactical, and operational collaboration

### **Purpose of collaboration capability**

We all understand that communication is one of the key components of improving any process. We would be running our operations inefficiently without it.

There are two types of communication that form a communication channel. We will discuss each of them in the following sections:



## Formal communications

Formal communications are any information that is passed down through formal and official channels. These come in the form of:

- Policies
- Key Performance Indicators
- Key risk indicators
- Project plans
- Official emails
- Presentations

- Reports
- Press releases
- White papers

Typically, they are the top-down information of *the official stance* of the organization on a particular topic or idea.

## Informal communications

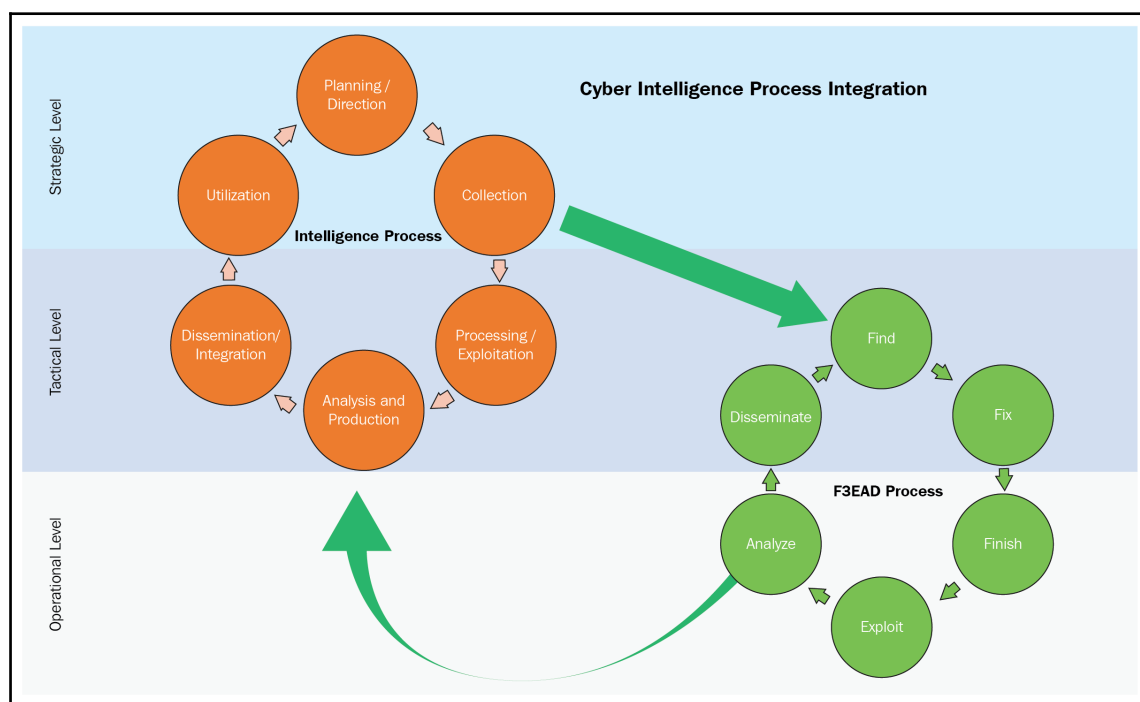
Information communications are more casual. These *off-the-record* means of communicating are used to pass information through:

- Work peer groups
- Influence
- Casual email
- Text messaging
- Phone calls
- Body language

## Communication and cyber intelligence process

As we've already learned, building the necessary channels of communication is required to establish a cyber intelligence capability. We first need to understand how communication fits into the cyber intelligence process throughout the different levels. Although in the beginning, we will be getting information about the status of other processes through **informal** communication, we will have to build the **formal** communication channels through projects.

Let's revisit the *Cyber Intelligence Process Integration*:



Collection efforts in the form of priority information requirements are sent from the **Strategic Level** to the **Tactical Level** at the **Collection** to **Find** phases of the intelligence and F3EAD processes, respectively. In previous chapters, we've used *corporate to region* as a means to convey this point. We should now look at what that means from the overall IT perspective. When the CIO says that they need information, it would be very easy to say that the **Tactical Level** passes the request over to the **Operational Level** and then back up again, but we need to build the communication lines between all three levels.

In the last chapter, we touched on how we can build the capability using threat intelligence. Throughout the rest of the book, we will be using the same concept of building through a Capability Maturity Model; however, we need examples on how we can get information to the right people, at the right time, and in the right way.

Each organization is different in the way it communicates and the following collaboration techniques are ideas and guidelines. These are not set on *this is the right way* because *the right way* is a subjective statement. The only correct way of doing things is if what you requested meets what you intended. If there was any deviation in the message, that means that there was a break in the communication that needs to be rectified or what was requested was not clear enough.

## Methods and tools for collaboration

We have different means to establish a collaboration capability between levels of an organization, as well as between teams. Let's review some methods and tools that we can use for collaboration.

### Service level agreements and organizational level agreements

Between entities, an agreement must be made between groups that they will provide a certain level of support or information to one another. These are known as:

- **Service level agreement:** An agreement between a service provider and client
- **Organization level agreement:** An agreement between organizational units

Building these agreements within an organization as well as with service providers will require that multiple stakeholders agree with the terms and conditions. This is especially true when dealing with outside vendors as they will push to stay *within contractual* limits and will charge additional fees for additional services (that is, reports, monitoring, and consulting hours). So it is important that we think about the end-to-end process of how you will want a specific set of services to collaborate with each other and what metrics you will decide that you want reported to you.

# Responsible accountable supporting consulted informed matrix

A **responsible accountable supporting consulted informed (RASCI)** matrix is used to describe the different attributes to key tasks within a process:

- **Responsible:** The organization responsible for doing the task
- **Accountable:** The organization/person who is accountable for the task being complete
- **Supporting:** The organization/person who will be supporting the completion of the task
- **Consulted:** The organization/person who will be contacted for consultation
- **Informed:** The organization/person who will be receiving information about the task

Responsible Accountable Supporting Consulted Informed Matrix				
	A Service	B Service	C Service	D Service
Task 1	Responsible	Informed	Consulted	Accountable
Task 2	Accountable	Responsible	Informed	Consulted
Task 3	Consulted	Accountable	Responsible	Supporting
Task 4	Supporting	Consulted	Accountable	Responsible

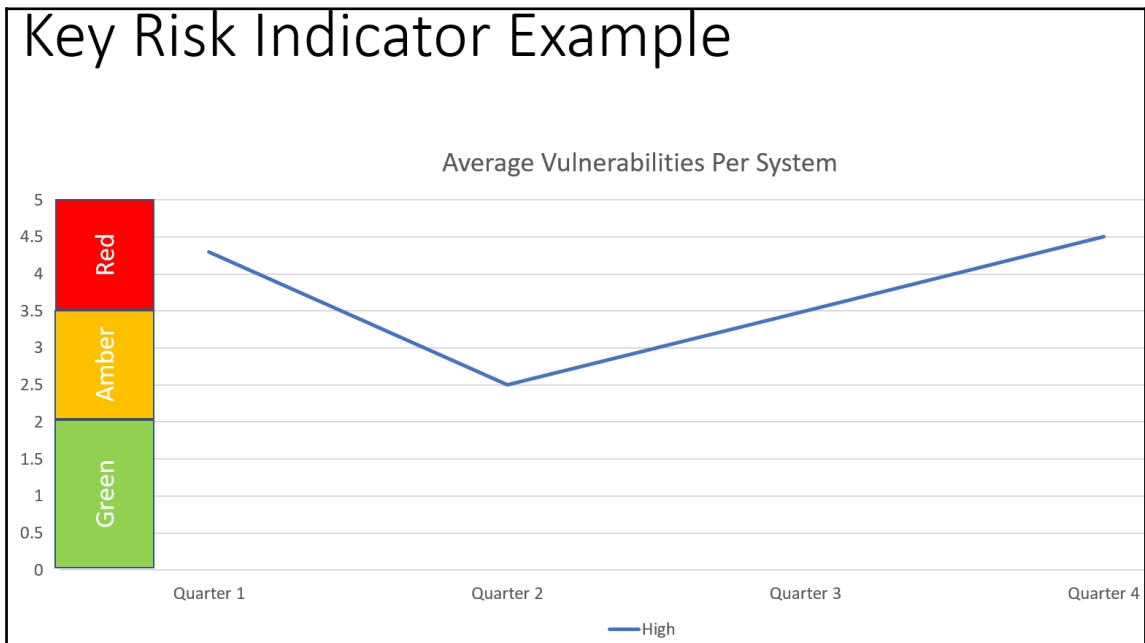
## Using key risk indicators

A key risk indicator is a measurement used in risk management that tracks the probability and impact a specific risk has against an organization's risk appetite.

Let's consider the following scenario—an organization wants to measure the average vulnerabilities per system it has on the enterprise.

It establishes that:

- Green = 0-2 high-level vulnerabilities per system
- Amber = 2-3.5 high-level vulnerabilities per system
- Red = anything over 3.6 high-level vulnerabilities per system

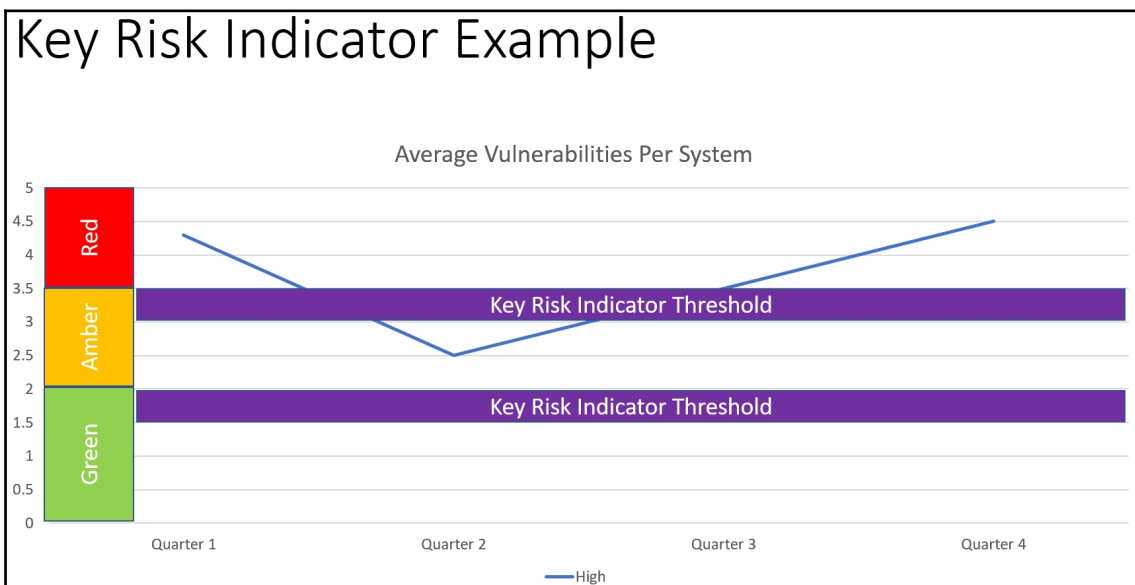


Understanding this, we can look at key risk indicators as the analysis of the trending information that warns that if current thresholds are met, stakeholders need to be notified to start remediation.



In our case, the organization has established that actions start taking place:

- **From Green to Amber:** When the average vulnerability count is between 1.5 and 2 per system
- **From Amber to Red:** When the average vulnerability count is between 3 -3.5 per system



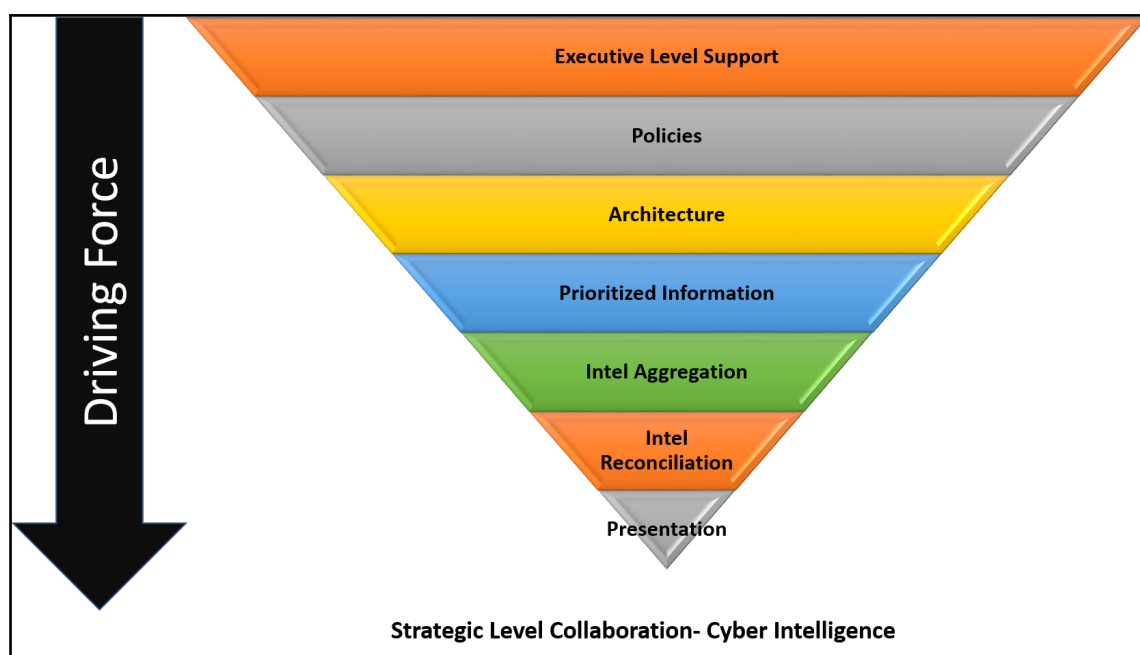
These are just a few methods and tools that we can use for collaboration. Let's see how these can actually be applied.

## Collaboration at the Strategic Level

All communication must be driven from the top down in building a cyber intelligence capability. This begins with executives buying into the idea that multiple sources of information that are consolidated and presented in a manner that impacts their decisions are important. If executives do not understand the foundation of building this capability, then collaboration for a cyber intelligence program will risk only using information from informal communications.

The following are the steps to strategic cyber intelligence collaboration:

1. High-level support for a cyber intelligence capability among executives and communicated to the organization
2. Policy makers and enterprise architects ensuring that collaboration methods are developed and documented
3. Prioritization of information collection requirements
4. Means to aggregate multiple information feeds from the intelligence processes
5. Ability to process information and produce dashboards that help define decision making



Let's take a look at each of the layers and get a better understanding.

## Executive support

The concept of business intelligence is not so different than collecting information about the enterprise and using it to make IT business decisions. If you are in a small to medium business, you may be in a position to walk up to the CIO or CEO and say "*hey, this is a good idea and I think we should do it.*" If you are part of a large organization, this may seem a bit of a stretch. As much as there has been talk on *agility* and *innovation* in business, in a large organization this means it takes time to get there because there have been processes that have been in place for years. Also, a lot of people don't like change and go with the phrase *if it ain't broke, then don't fix it*. Just as business requirements change and organizations are trying to be competitive, as information technology leaders, we must adapt to those requirements and influence those to follow us down the unfamiliar road.

Here are a few questions for you to answer that can help with your business case proposal:

- Why do you think that a cyber intelligence capability is important to your organization?
- From an IT perspective, how do you think that a cyber intelligence capability would improve the business?
- How is consolidating and reconciling information from other IT teams beneficial to your decision-making process?
- How can we improve how we communicate to other IT teams across the enterprise?

This is by far the most important requirement because, without buy-in from the executive stakeholders, there will be no reason for a project/program to get the resources it needs to become a reality.

## Policies and procedures

**Policies** are the rules of the enterprise. Much like the ten commandments, they say what you can and cannot do in the enterprise. From the Strategic Level, there needs to be a policy in place that the other teams can reference for your cyber intelligence program and it should at least cover the following:

- The intent of your cyber intelligence program
- Description
- Targeted audience
- The reason that the policy exists

**Procedures** tell you how to do a particular process. This is where we explain (at the Strategic Level) how the cyber intelligence program works. It should include:

- Written procedures and explanations
- Process diagrams



These documents are typically an output or deliverable from a project that is up and operational. As you are building your capability based on the Capability Maturity Model, you can modify the document as appropriate.

## Architecture

From a *green field* or *starting from scratch* to a *well-established* infrastructure, with strategic direction from stakeholders, enterprise architects must build services and processes to include communication channels to help achieve the end state cyber intelligence program.

Dependencies need to be addressed at the enterprise level so that the proper channels can be developed in parallel with establishing architecture components.

## Understanding dependencies

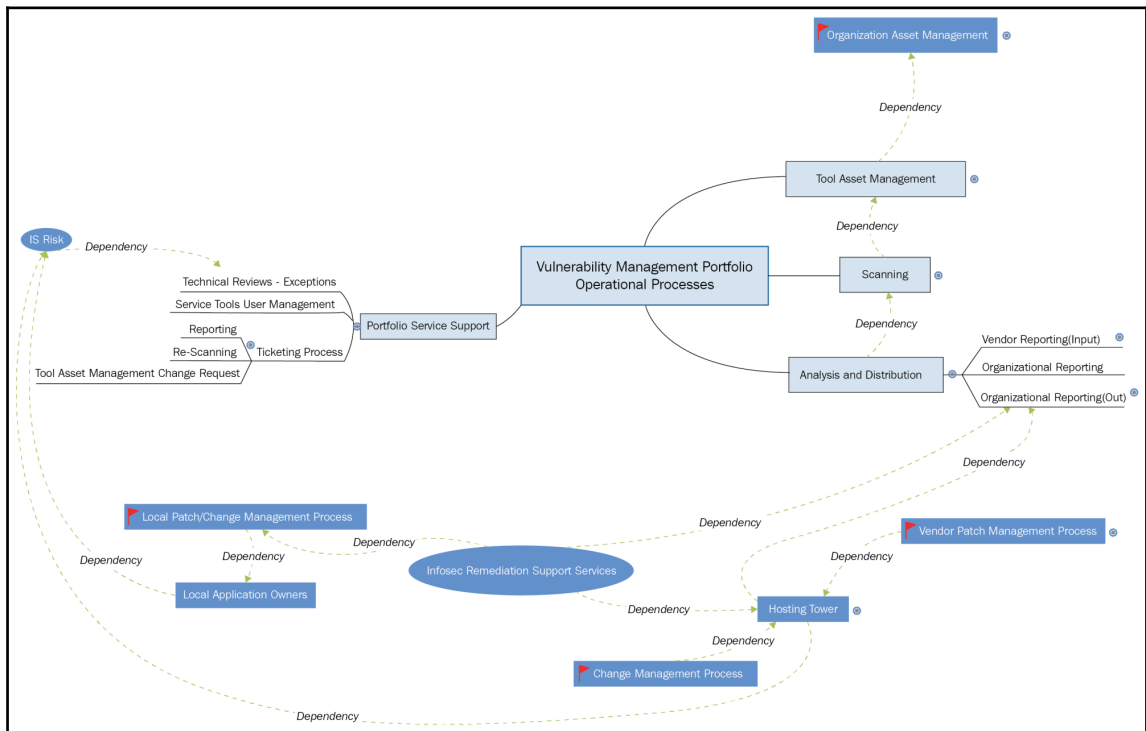
Being able to provide the architecture for a cyber intelligence capability for an enterprise means that you have to understand the dependencies of each major process from end to end.

For example, let's look at some of the major processes for vulnerability management:

- **Enterprise asset management:** This is the process that manages all of the assets that exist in the enterprise
- **Vulnerability management tool asset management:** This is the process that ensures that all of the enterprise systems are correctly loaded into the scanning tool
- **Scanning process:** This is the process that finds vulnerabilities within systems that are in the tool asset management database
- **Analysis and distribution:** This is the process that processes scanning results, sorts out what needs to go to who, and delivers the information

- **Remediation:** This is the process that fixes identified vulnerabilities:
  - **Local change management process:** This is the change management process that is developed and maintained by the resident business units or local office
  - **Regional change management process:** Local change management processes route to the regional process that ensures that these procedures are monitored and in line with organizational standards
  - **Vendor supported change management process:** Integrated support from vendors into the organizational change management processes
- **Risk:** The process that evaluates the probability and impact of vulnerabilities that exist within an enterprise

A graphical representation can be seen here:



There are dependencies for each step and we need to understand these to answer a few questions:

- How can we create good interaction between all dependent process owners?
- Who are the main stakeholders within each of these processes?
- How do we evaluate the interaction between the teams?
- How do we evaluate the risk of each part of the process?

By answering these questions, we can at least gain an understanding of who the key players are in the process, begin creating the means of communicating, and start a RASCI matrix to begin assigning and attributing specific tasks to teams.

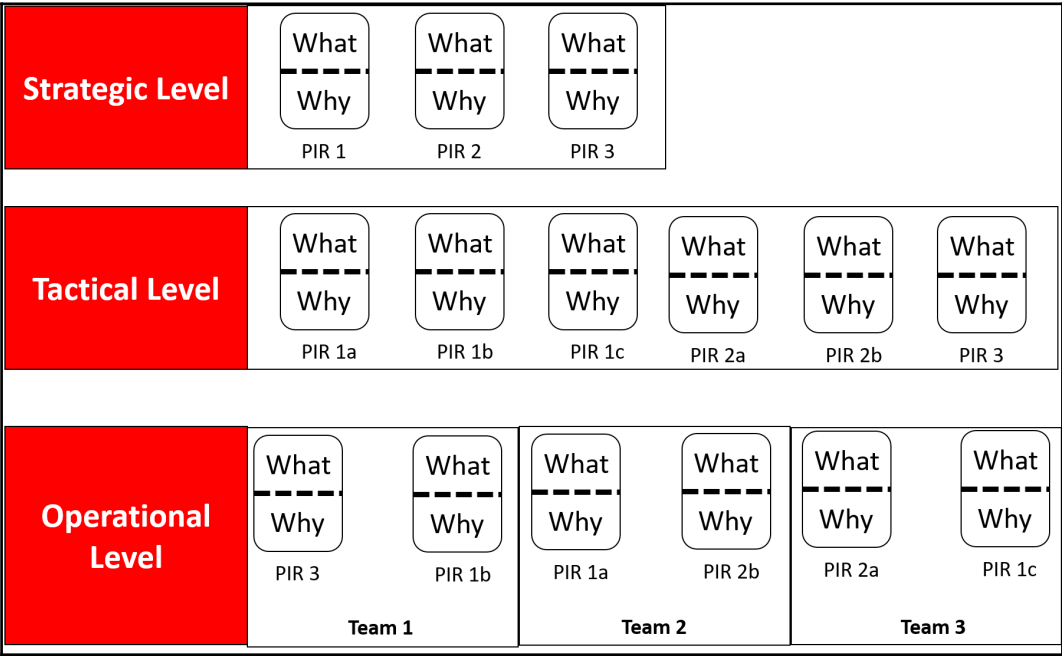
## Prioritized information

Information requests need to be prioritized by key stakeholders at the Strategic Levels as they are the decision makers on the strategy of the IT organization.

At this level, the most important queries have to include:

- The *what*:
  - It is the information that is critical to making a decision on a strategic objective
  - It provides the tactical leadership with an idea of what teams to pass the request for information to, so that the specific targets are sent to the correct people to engage them
- The *why*:
  - It is the information that needs to be understood at the Tactical Level so that they can look for any other opportunities to exploit more information in the collection process

- It shows the tactical leadership the importance of the information to the mission



The preceding diagram shows how the PIRs are driven from the Strategic Level to the Tactical Level. Notice that once the PIR information is received at the Tactical Level, the PIRs are split into smaller PIRs and are distributed to the operational teams for action.

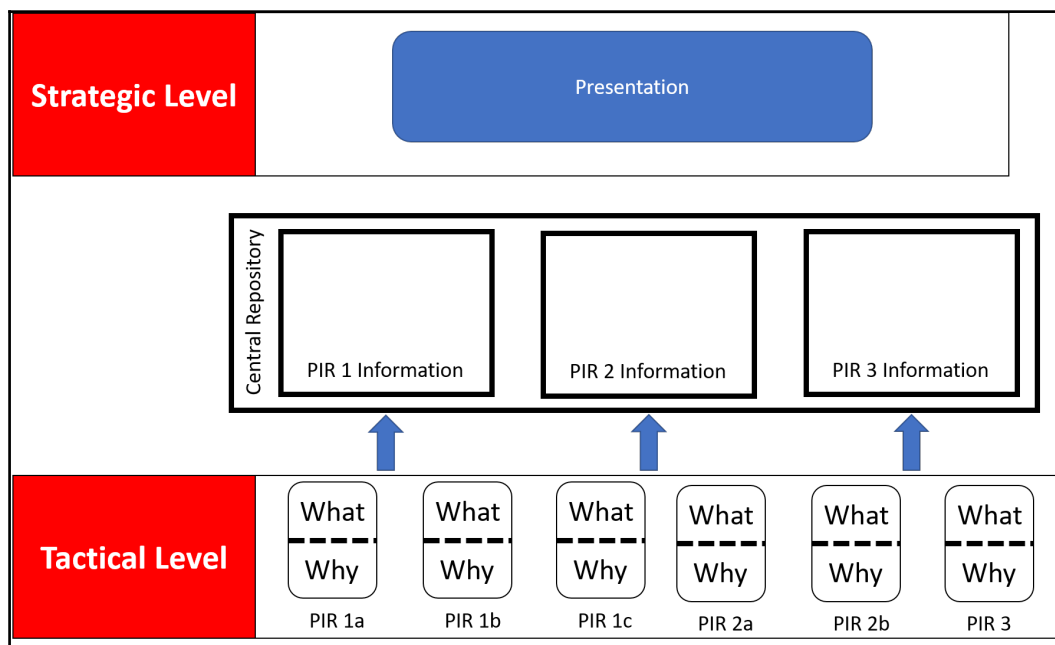
## Intelligence aggregation

The capability to aggregate the information gathered from the Tactical Level is important as it prepares the intelligence for a strategic analysis.

The following are some key components of an aggregation capability:

- Strategic Level central repository for information to be imported through manually or through automation
- Information provided in intelligence products are in a standard format:
  - Saves time
  - Increases efficiency with data mining tools

The following diagram shows that once the information is received from the operational teams, it is processed and moved into the strategic central repository. Once there, the information will continue the intelligence processes of analysis and production in preparation for *dissemination/integration*, which is depicted as **Presentation**:



## Intelligence reconciliation and presentation

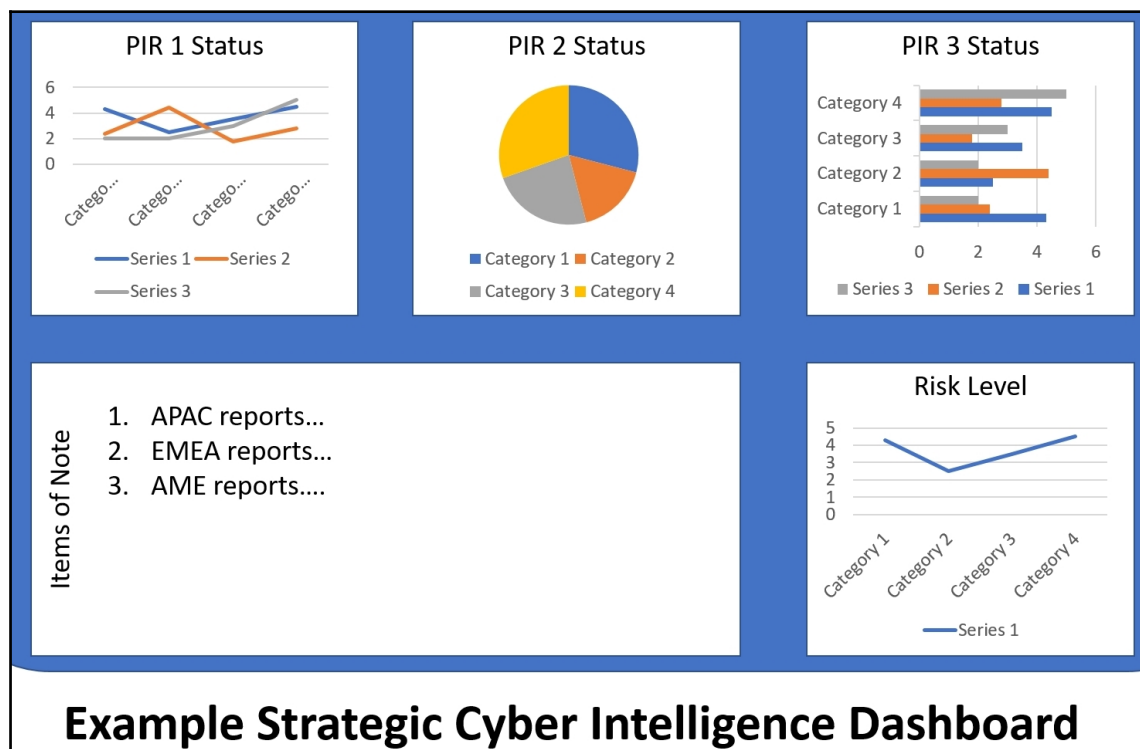
An enterprise solution to take all of the information and reconcile it is necessary to be able to present it. Ultimately, we want to be able to make all of the information that we've requested to be acted upon and/or monitored visually and graphically represented for us to use.

This can be established by using:

- **Red, Amber, Green (RAG)** charts
- Trend analyses
- Pie charts
- Bar charts
- Risk analyses



These are depicted in the following figure:



Although this dashboard is simple to understand, we can imagine how many PIRs the leaders would like to know. A recommendation would be to:

- Have a main dashboard with items displayed that are agreed upon with the main stakeholders
- Have the ability to have a stakeholder customize their dashboard to show what data they would like to see

At the end of the day, strategic leaders want to be able to easily identify where the issues are based on the information that is requested to be collected. A properly configured and customized dashboard provides the information to the stakeholders in a meaningful way so that they can monitor, track, and decide on the different items/issues that they focus on.

## **Collaboration at the Tactical Level**

Tactical communications are different than strategic communications in that they are relevant to the day-to-day operations. Strategic communications will drive the PIRs for higher level, big picture issue/solution information gathering. These will influence how future projects will be decided on and resourced.

The following are the steps for tactical cyber intelligence collaboration:

1. High-level support for a cyber intelligence capability and collaboration defined and communicated to the organization
2. Collaboration methods must exist and procedures must be documented
3. Prioritization of information collection requirements from strategic and tactical leadership
4. Means to aggregate multiple information feeds from the intelligence processes
5. Ability to process information and produce dashboards that help define decision making

Although the steps are similar to strategic cyber intelligence collaboration, the goal for creating tactical communication channels is to improve how IT service operations and IT security operations enable intelligence products to flow to and from each entity. The better integration of communication channels between tactical teams, the faster we can make decisions.

## **Breaking down priority information requirements**

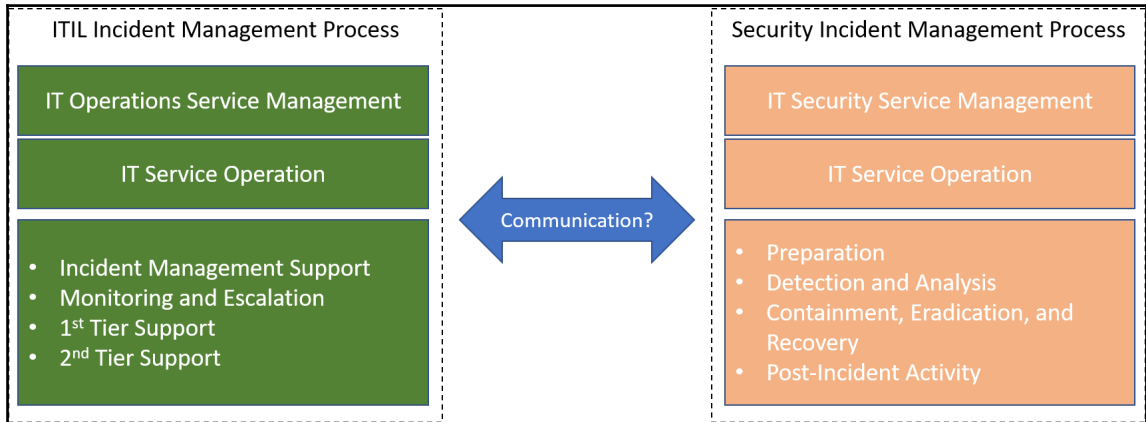
When PIRs flow down from the Strategic Level to the Tactical Level, they may be relevant to one or more tactical teams. For example, PIR is the status of account attempted logins using former employee administrative accounts:

- This implies that user account management must have a procedure in place that checks that former employees lose their administrative credentials (IT operations)
- InfoSec should probably have that list available and is monitoring for this activity (IT security)

This means that it will take two collaborative efforts to create an answer to the Strategic Level PIR.

## Application of the theory

To better understand this concept of a marriage between IT operations and IT security operations, let's review the following diagram:



There are two services/processes depicted in the diagram, the **ITIL Incident Management Process** and the **Security Incident Management Process**. Individually, they are very simple to understand, but what we want to understand is if one of these processes impacts the other.

Using this as an example of trying to build the communication channels between the two service organizations, we can start by asking some questions:

- Are there any service level agreements in place between these two entities?
- Are there any organizational level agreements in place between these two entities?

If the answer is yes or no, we would next have to understand the following:

- At what point does an IT incident become a security incident?
- At what point does an IT security incident become an IT incident?

- Are there specific items from an IT incident that the IT security incident response should be concerned with?
  - What are they?
  - How is this communicated to them?
  - How is this followed up?
  - Where is it documented?
- Who is **responsible** for what during this process?
- Who is **accountable** for what during this process?
- Who is **supporting** during this process?
- Who is **consulted** during this process?
- Who is **informed** during this process?

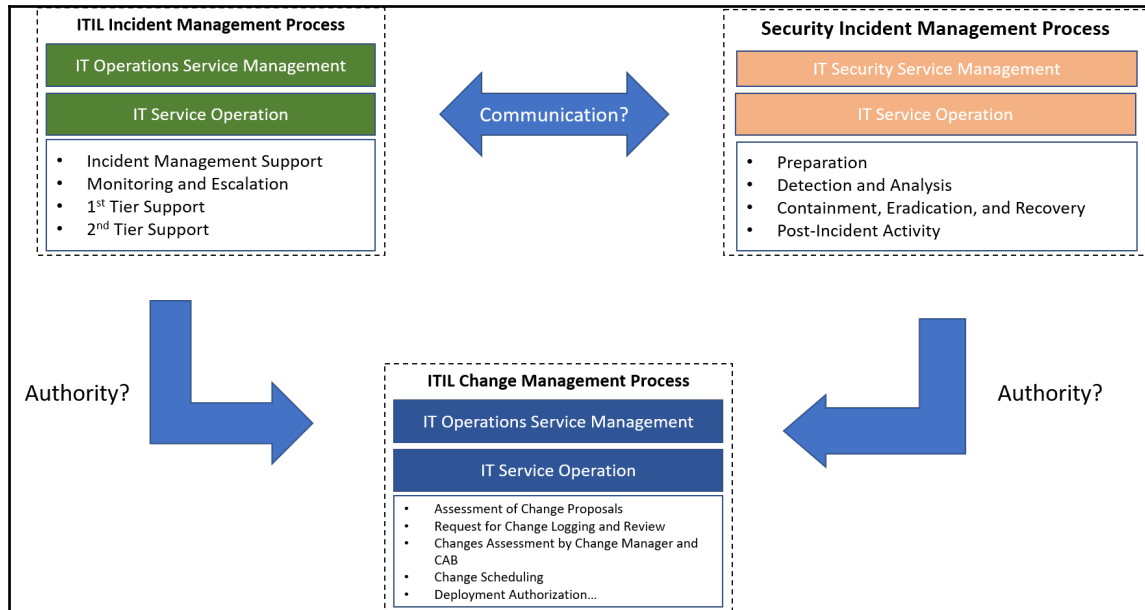
Between the managers of the IT incident response and IT security incident response organizations, the goal would be to:

- Understand the information requirement requests from higher management
- Understand the strategic relevance of communicating
- Develop and establish a collaborative and integrated process
- Develop and establish SLAs/OLAs
- Develop and establish metrics and accountability for handling the incidents

## Theory versus reality

Understanding the theory and applying it is one thing, but understanding the theory and applying it to reality is another.

Two entities is a very simple concept to understand, but let's add another service: the **ITIL Change Management Process**.



Using this as an example of trying to build the communication channels between the three service organizations, we can start by asking some questions:

- Are there any service level agreements in place between these three entities?
- Are there any organizational level agreements in place between these three entities?

If the answer is yes or no, we would next have to understand the following:

- At what point does an IT incident go through the **change management process**?
- At what point does an IT security incident go through the **change management process**?
- Who is **responsible** for what during this process?
- Who is **accountable** for what during this process?

- Who is **supporting** during this process?
- Who is **consulted** during this process?
- Who is **informed** during this process?

Now between the managers of the IT incident response, IT security incident response, and change management organizations, the goal would be to:

- Understand the information requirement requests from higher management
- Understand the strategic relevance of communicating
- Develop and establish a collaborative and integrated process
- Develop and establish SLAs/OLAs
- Develop and establish metrics and accountability for handling the incidents
- Establish who has the **authority** to initiate a change request

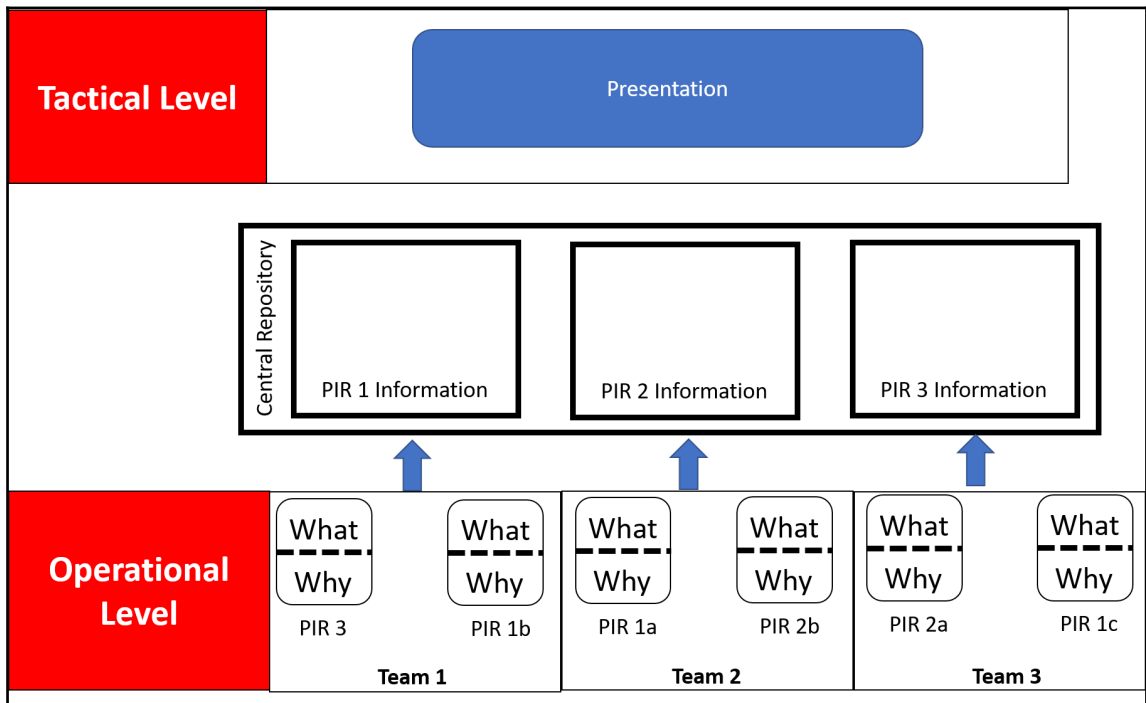
All of these items are things to consider when trying to create a consolidated metric and communication channel for an end-to-end process.

## Creating the tactical dashboard

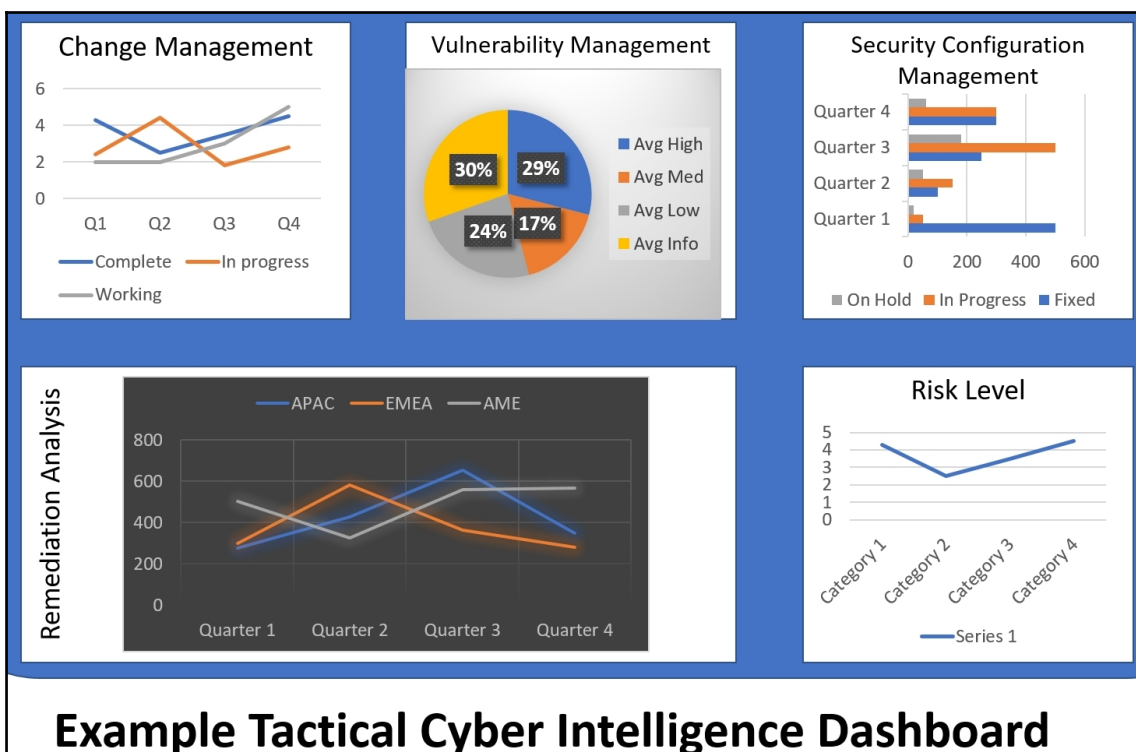
Much like the Strategic Level dashboard, we can look at the Tactical Level dashboard as the more detailed version of understanding each step and sub-step of the major processes.

Think about it like this, there is a hose, there is a faucet, and there is a plant. Your goal is to turn on the faucet, so that water goes through the hose, so that you can water your plant. If you can't water your plant, you will have to troubleshoot whether it was a pinch on the hose or a plumbing issue at the faucet. By monitoring the *what is expected* against *what is reality*, we can start to figure out where the process needs work if the outcome is not what is expected.

By working together, splitting the PIRs into smaller packages, and delivering them to their respective teams, tactical leaders can understand how their processes can contribute or hinder the process to produce the expected product.



We can look at the dashboard as understanding the possible *pinches* in the process by displaying information that is relevant to the main groups of the process.



By understanding who are the key stakeholders for these processes, we can begin to create a dashboard that benefits all of those who are required to monitor the process status. So in addition to strategic PIRs, the tactical leadership should be looking at developing their own PIRs:

- What information is pertinent to be depicted on the dashboard?
- What are the thresholds that we can establish for KRIs?

We will talk about some ideas in later chapters.



## Collaboration at the Operational Level

Once PIRs are delivered from the strategic and tactical layers, they should be divided and delivered to the teams.

Examples:

- Business division IT—business unit IT
- Regional IT—country IT
- Security Operations Center—incident response/blue team

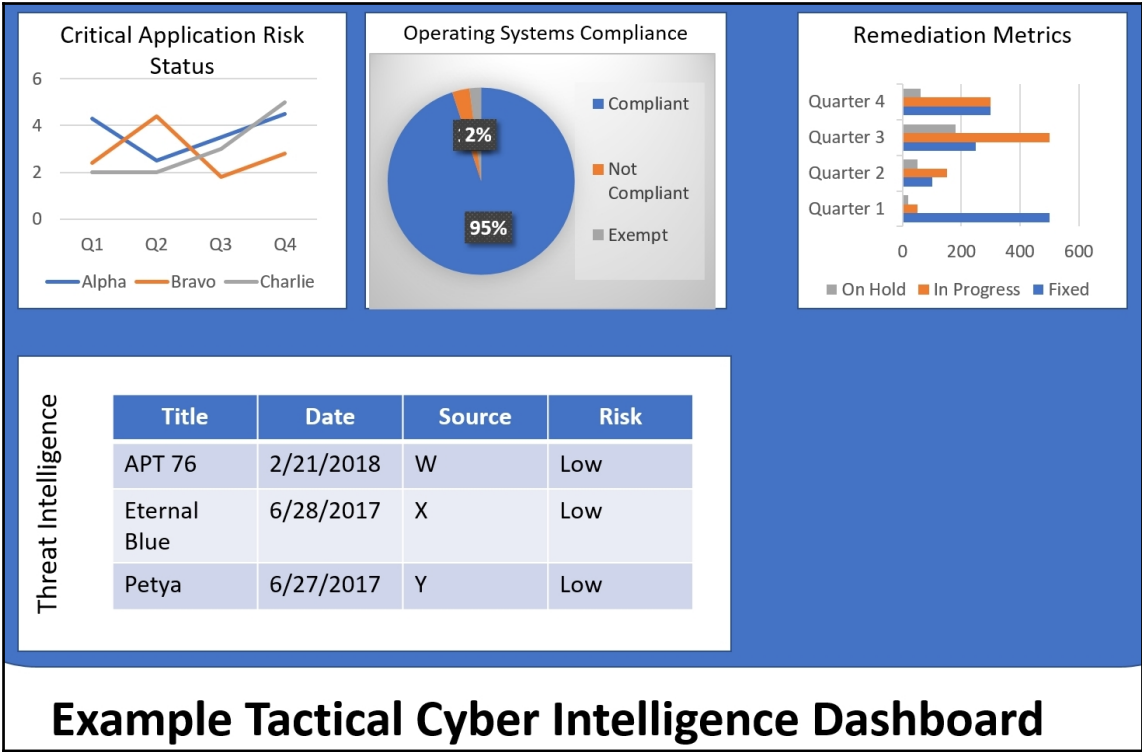
Depending on the type of information that is collected, these teams may or may not know the overall intent of the information that is being gathered, but it is important that the teams understand (to the extent that they are allowed) the *what* and the *why* of gathering it.

Here are the steps for operational cyber intelligence collaboration:

1. High level support for a cyber intelligence capability and collaboration defined and communicated to the organization
2. Collaboration methods must exist and procedures must be documented
3. Prioritization of information collection requirements from tactical leadership
4. Means to **deliver** information feeds to the intelligence processes
5. Ability to **process information** and **produce internal dashboards** that enable decision making

Here is an example of a tactical cyber intelligence dashboard that would be useful to the following operational teams:

- Information systems management
- Application management team
- Change management
- Vulnerability management
- Incident response



The information that is provided in the preceding section is an example of a dashboard that can be developed to help the teams understand how their daily operations impact what is displayed:

- By displaying the *critical application risk status*, teams in this business unit will see how their efforts are impacting the risk of the organization
- By displaying the *operating systems compliance* status, teams will see how well their systems are configured against organizational standards
- By displaying *remediation metrics*, teams will see how many change requests there have been
- By displaying *threat intelligence*, teams will understand that the information that is provided in this section is applicable to them

Whatever is displayed on the dashboard, the preceding is just an example of what could be delivered to our teams to provide cognizance on processes so that they can be proactive in addressing their portion of the process.

## Summary

In this chapter, we've discussed how we can build communication channels at each level using different methods and techniques. These are meant to establish a means to understand the hangups, progress, and/or status of major processes among multiple teams so that they all can be on the same page.

In the next chapter, we will discuss how we can incorporate cyber intelligence into the security architecture.

# 8

## The Security Stack

Up to this point, we've introduced how we can integrate a threat intelligence capability into improving our organization's security. Threat intelligence is externally focused. However, I wanted to take a moment in this chapter to lay a foundation to improve the internal communication capability.

In this chapter, we will undertake the following:

- Discuss some core security service basics
- Talk about security operation center capabilities
- See how we can integrate services and improve their communication
- Discuss a Capability Maturity Model for information security that enables cyber intelligence
- *Collaboration + Capability = Active Defense*

### **Purpose of integration – it's just my POV**

When I think of how I would begin to build a security program and integrating a cyber intelligence capability, I like to keep things very simple:

1. What is the mission of the information security program?
2. What is the core set of services that are required in a security program that will enable me to understand and improve my security posture?
3. What has been defined as the most important to the least important system, application, and data?
4. I want to know what good, bad, and ugly look like. How is risk defined in the organization?
5. Who needs to talk to who in order to get things done?
6. How do I need to share this information with those who need to know?

## Core security service basics

ITIL defines a service as *"a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks"*.

Services have metrics such as:

- **First response time averages:** The average amount of time it takes for a tech to respond to a ticket
- **Ticket close time averages:** The average amount of time it takes a service to close an assigned ticket
- **Vulnerability findings close average:** The number of findings closed during a specific amount of time

So beyond identifying the names of core security services, we need to understand:

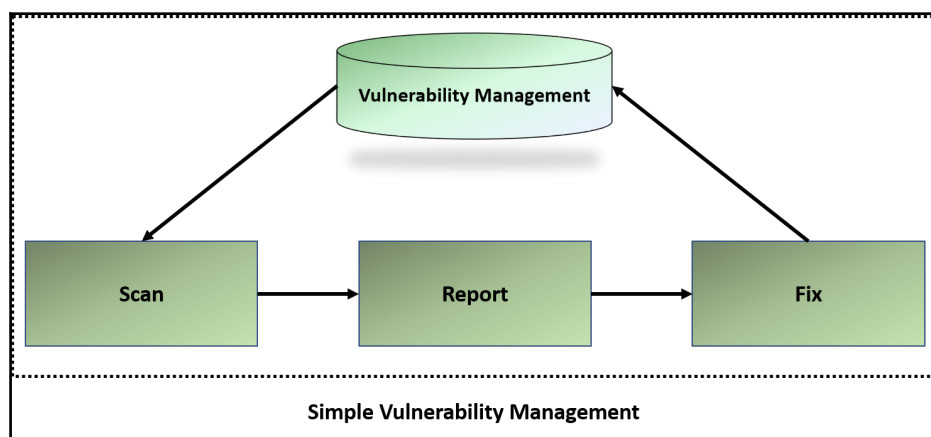
1. Who is the customer?
2. What is the service that is being provided to that customer?
3. What is the value that is being brought to the customer as a result of our service?
4. What is the definition of good and bad service?

Knowing this, we can start to see some of the dilemmas that we have in some security services, in that:

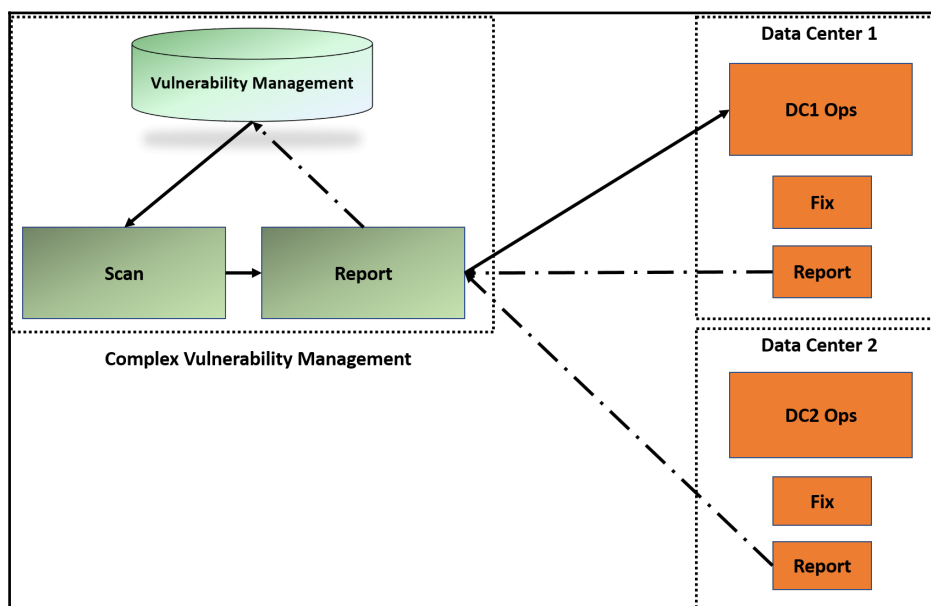
- If the intent of the vulnerability management service is to manage vulnerabilities, then the service should have the ability and the authority to manage vulnerabilities:
  - If it doesn't have that capability, then it is only a reporting service where the value of the service is measured by how well and accurately the service reports
- If the intent of the incident response team is to respond to incidents, then the team should have the ability and authority to investigate incidents:
  - If it doesn't have that capability, then it is only a reporting service where the value of the service is measured on how well and accurately the service reports

In smaller organizations, issues like these are fewer, as teams can provide guidance and assistance more quickly than in larger organizations.

The following is a simple process that explains vulnerability management:



The more complex the organization is, the more complex the solution is:



However, the solution for the security service remains the same, just as  $1 + 1 = 2$  is the same as  $\sqrt[3]{\sqrt{x108} + 10} - \sqrt[3]{\sqrt{x108} - 10} = 2$ .

The way in which the service provides value may (or may not) be how well the service can evaluate and report on the *end-to-end* process to create the desired result.

## Security Operations Center

The way I'm going to portray the **Security Operations Center (SOC)** may be counter to what you currently have in place. This is only because, at an SMB, everything regarding cyber/information security is under the SOC.

So let's just set the baseline of some basic parameters so we can all be on the same page:

- The SOC will be viewed from the Tactical level
- Capabilities that the SOC will be viewed at the Operational level
- Some basic security teams are:
  - InfoSec governance enforcement
  - Vulnerability discovery and detection
  - Threat management
  - Threat intelligence
  - Security configuration baseline management
  - Incident response/blue team
  - Red team
  - Security State Analysis/continuous monitoring
  - Application security

These basic teams are what I would consider the *security stack*.

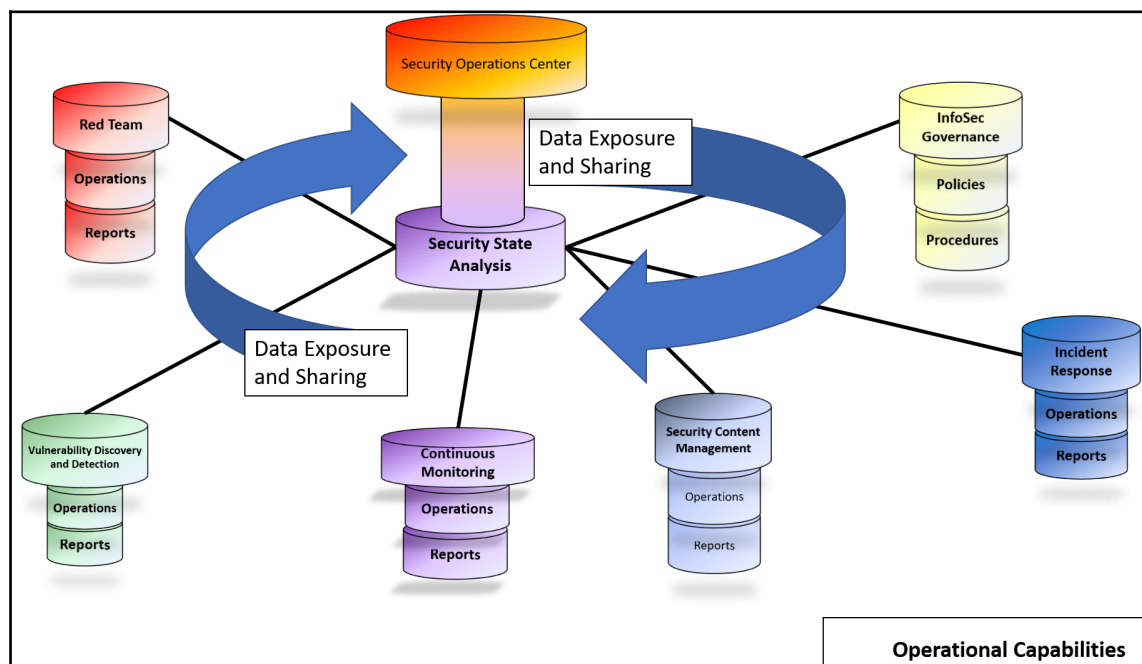
## The spider

When I think about the capabilities that an SOC should have, I have to relate to a spider. Each part of the spider has a unique purpose. The legs of the spider have small hairs that allow it to know when danger is present or when prey arrives.

In relation to information security:

- Do all of the capabilities work together to **know** when danger is present?
- Do all the capabilities work together to **defend** the organization?

The **operations** and **reporting** from each leg must report their status to the body (**Security State Analysis**), but at the same time, the capabilities must be in tune with each other through open communication (**Data Exposure and Sharing**).

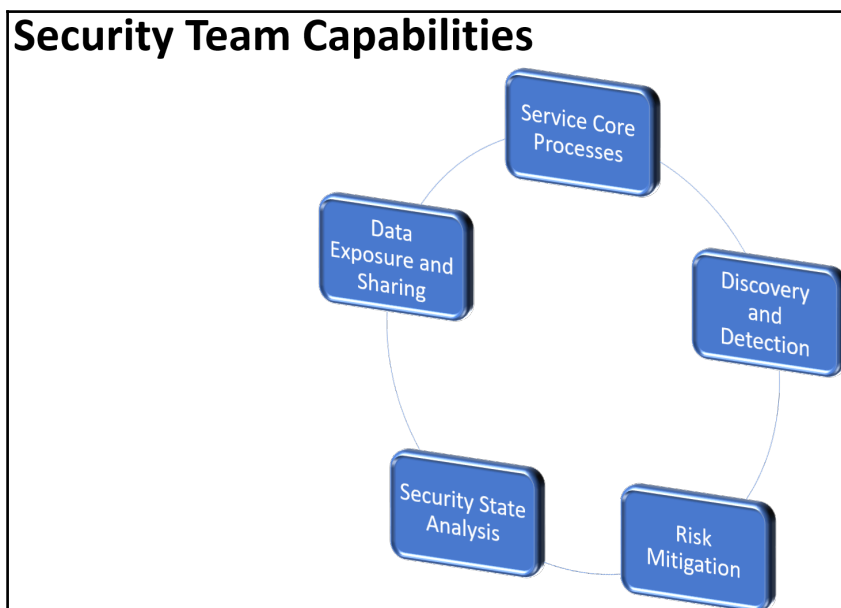




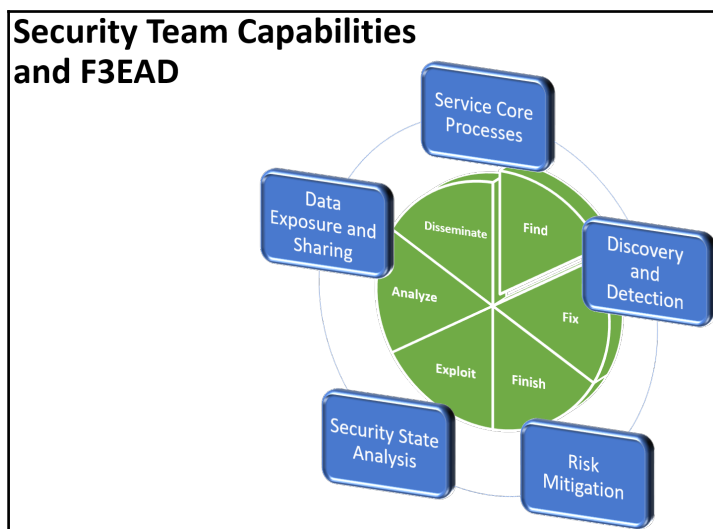
## Capabilities among teams

Let's start to talk about breaking down the different capabilities of teams:

1. Each team has their core set of processes that measure against **Key Performance Indicators (KPIs)** set by management.
2. The process of finding deviations against baselines is part of **Discovery and Detection**.
3. The process of evaluating the level of risk and taking action on the findings against the baselines is part of **Risk Mitigation**.
4. The data that is to be shared to the rest of the teams and at each phase is part of **Data Exposure and Sharing**.
5. The monitoring of KPIs is completed by the team's input into **Security State Analysis** the SOC (through the F3EAD process).



We know that we need to be able to share the results of the processes that we are measuring or the information that is required to be delivered to management. We can take these core capabilities and now apply them to the F3EAD process, as depicted in the following diagram:



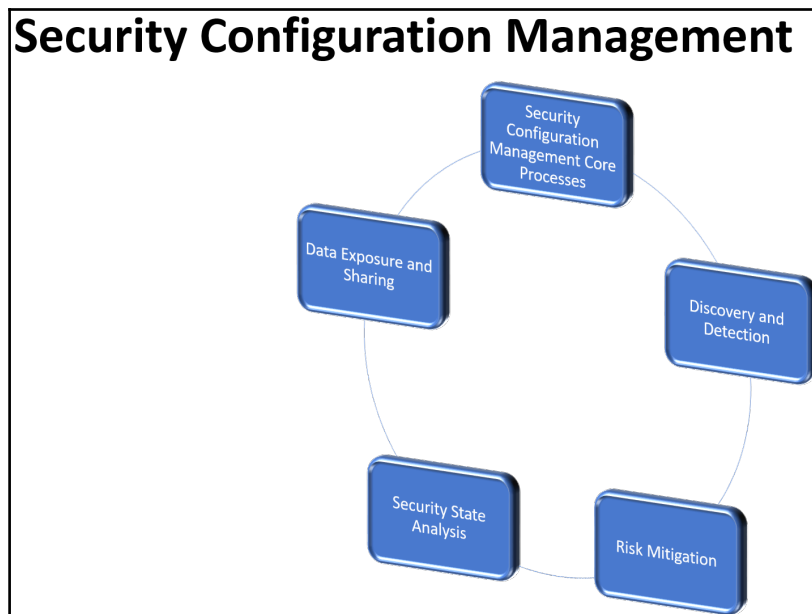
We now have to understand how all of these security team's capabilities and the targeting process can work together in an SOC through cyber intelligence by building the communication channels.

## Capability deep dive – Security Configuration Management

To better understand the concept of the capabilities of securities in their relation to providing intelligence to the SOC, we will look at how we can incorporate each step using the service that is responsible for setting the security baselines for the organization, Security Configuration Management.



A more in-depth chapter on building the cyber intelligence capability within Security Configuration Management will be discussed later.



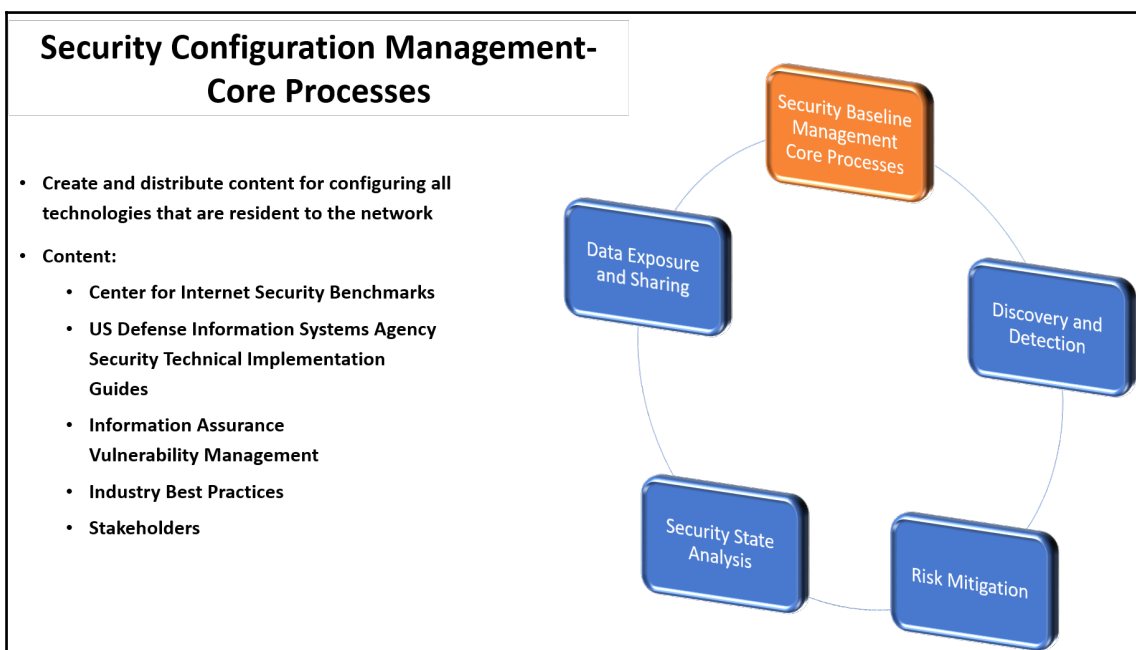
Using the preceding figure as a guide, we will review in more depth the capabilities that an SCM should provide:

1. What their core processes are
2. How the service is able to enable their processes (**Discovery and Detection**)
3. How the service is able to inform the appropriate stakeholders or reduce risk (**Risk Mitigation**)
4. How the service assesses the state of security for their area of responsibility (**Security State Analysis**)
5. How the service shares information *across and up* (**Data Exposure and Sharing**)

## Security Configuration Management – core processes

The Security Configuration Management service is responsible for:

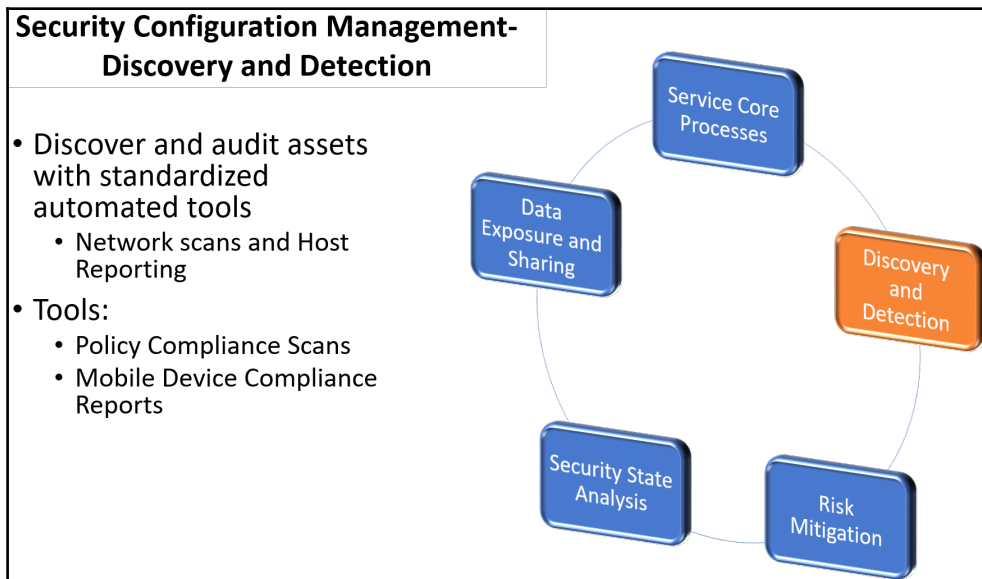
- Developing the security baselines for all of the technologies that exist on the network
- Distributing the baselines to the applicable stakeholders
- Scanning and reporting for controls that are non-compliant to organizational standards
- Assisting in a risk in any exception request reviews



## Security Configuration Management – Discovery and Detection

**Discovery and Detection** are executed by scanning and reporting for controls that are non-compliant to organizational standards using various security tools:

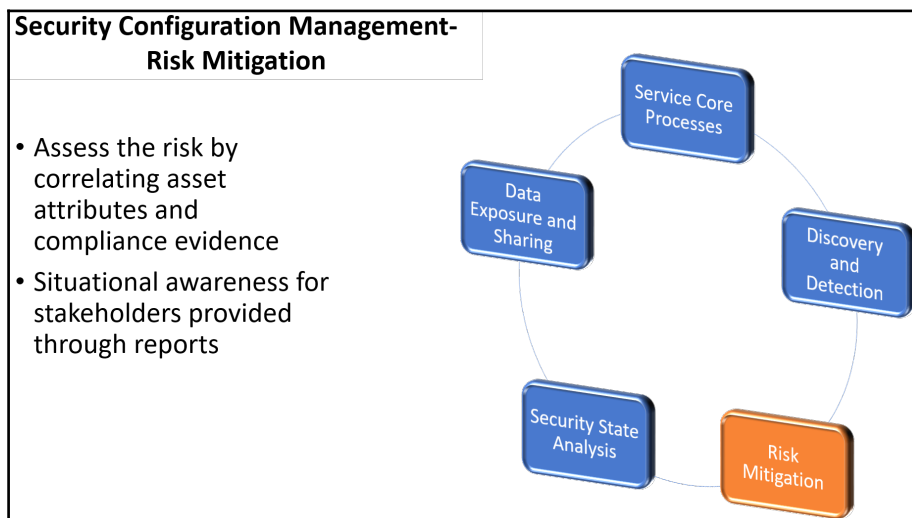
- OS configurations
- Network configuration
- Application security configuration



## Security Configuration Management – Risk Mitigation

The level of risk for each control is determined by the organization that the control was derived from. If the baseline was developed from several sources, the control's risk will be discussed and changed in accordance policy change management procedures.

Reports of non-compliant controls are given to stakeholders for action and given a grace period to fix or request an exemption for non-compliance. After this grace period is completed, the control will be counted against the stakeholder's risk score.



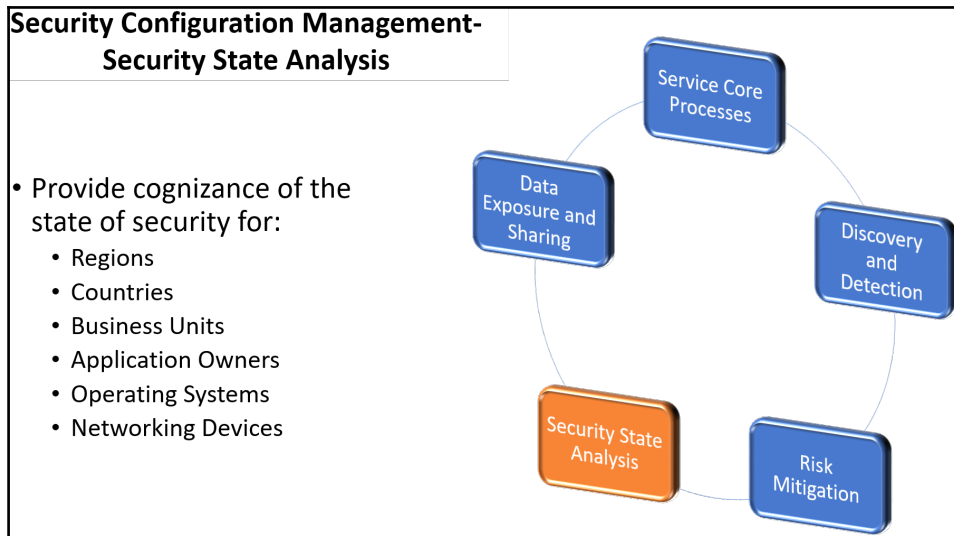
The results are provided as regular reports for the teams to begin analysis and Risk Mitigation activities.

## Security Configuration Management – Security State Analysis

During this phase, the overall identification of non-compliance with policies is provided as a calculated risk metric for review by the stakeholders. The **Security State Analysis** provides the state of compliance against this metric for several categories, such as:

- Operating system
- Region
- Country

- Application



## Security Configuration Management – Data Exposure and Sharing

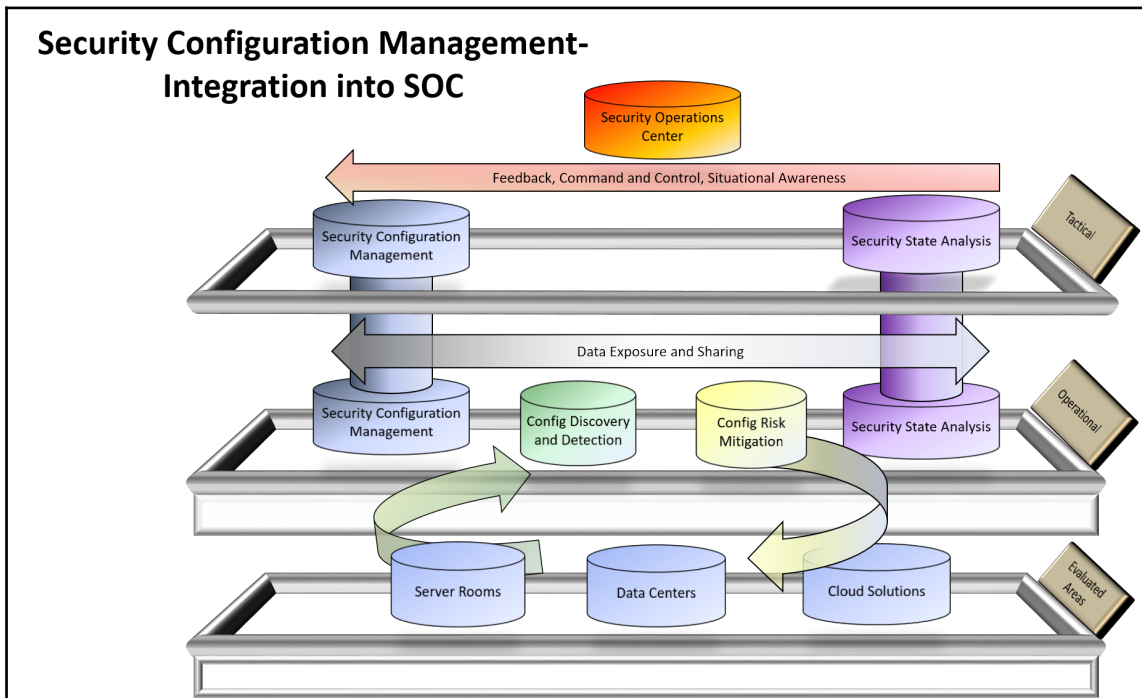
Cyber intelligence is driven by the service's capability of communicating *across and up*:

- Across = Operational level teams
- Up = Tactical level SOC through F3EAD process and Security State Analysis

The main questions to answer here are:

- Who needs to know this information for:
  - Remediation efforts?
  - Reference to their processes and analyses?
- What do they need to know?
  - How does this need to be delivered?
  - Is there customization of the information that needs to be done so that it is actionable?

By the end of this phase, the information should be distributed to the right people in the proper format for action. The following is a graphical representation of the service capabilities and how they integrate with the SOC:



In the preceding diagram, we have three layers:

- Tactical
- Operational
- Evaluated Areas



As we can see in the Tactical layer, the Security Content Management service interfaces with the SOC. The SOC would be providing the **Feedback, Command and Control**, and **Situational Awareness** for this particular service, as well as all of the other services that it is responsible for.

Going counterclockwise, the service drives down **Tactical** initiatives to the **Operational** level through their core processes. In the **Operational** level is where the interface between the operational team and the stakeholders is. The SCM service discovers and detects, and may or may not reduce risk through communicating with stakeholders in the evaluated areas.

Through the constant communication and interaction between the team and the stakeholders, the data being collected is reconciled at the **Operational** level in preparation to move to the **Tactical** level. If it is normal reporting, then the information would go through the normal reporting channels and cyber intelligence information on specific, targeted data would go through F3EAD processes up to the **Tactical** level.

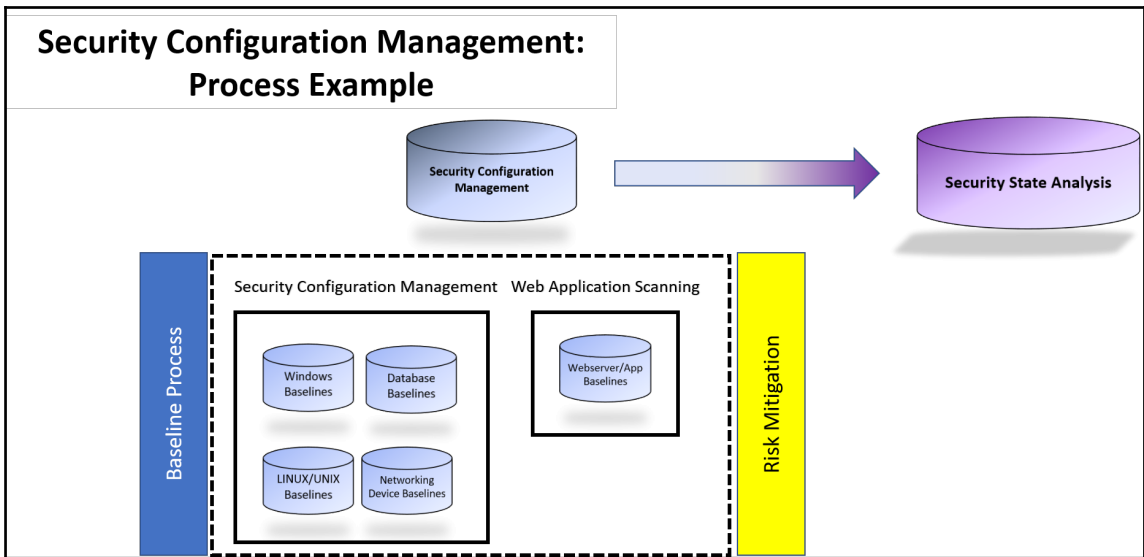
## Prelude – integrating like services

Now that we have an understanding of how we can integrate a service's processes into the SOC's cognizance, let's explore how we can integrate a *like* service and achieve the same result.

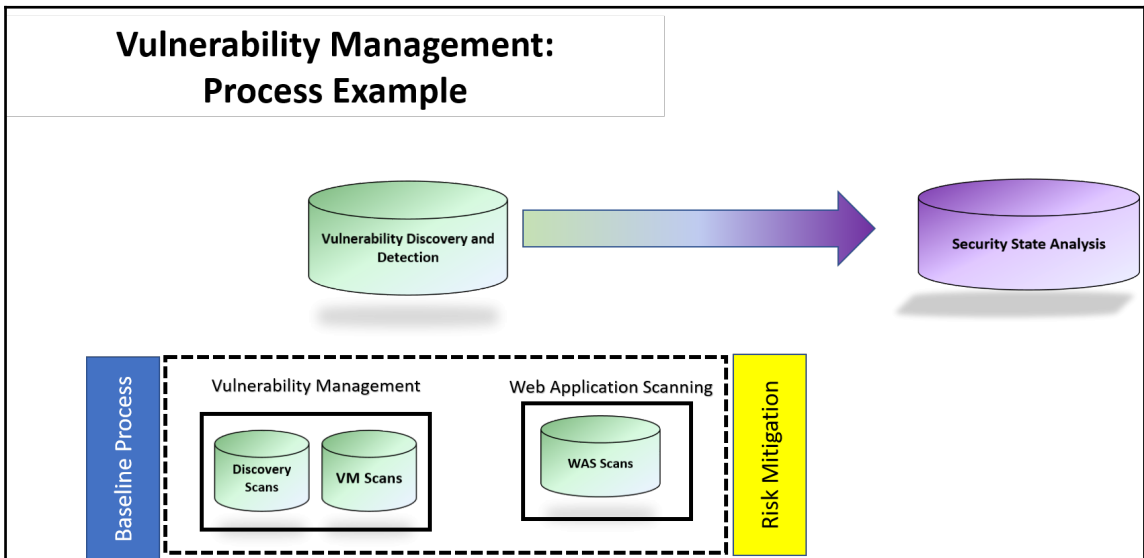
The most compatible service with SCM is **vulnerability management (VM)**. Just as SCM scans and looks for non-compliance with a standard set of configurations, VM looks at the applications that exist on a system and sees if they are up to date with their security patches, as well as revealing any vulnerabilities. The main difference here is if a Windows 7 baseline has 50 standard controls, SCM will check only those 50 controls multiplied by the number of systems it scans, producing a finite result. However, VM looks at the OS and every application on a system. Unless each system has the same image and library of applications (from a VM or virtual application), the results will be more dynamic. We will get more into how we can standardize this in a later chapter.

Let's take a different view of these services using terms that we've learned in this chapter.

If we compact core process, discovery detection, Risk Mitigation, and security analysis for Security Configuration Management services, it would look as follows:

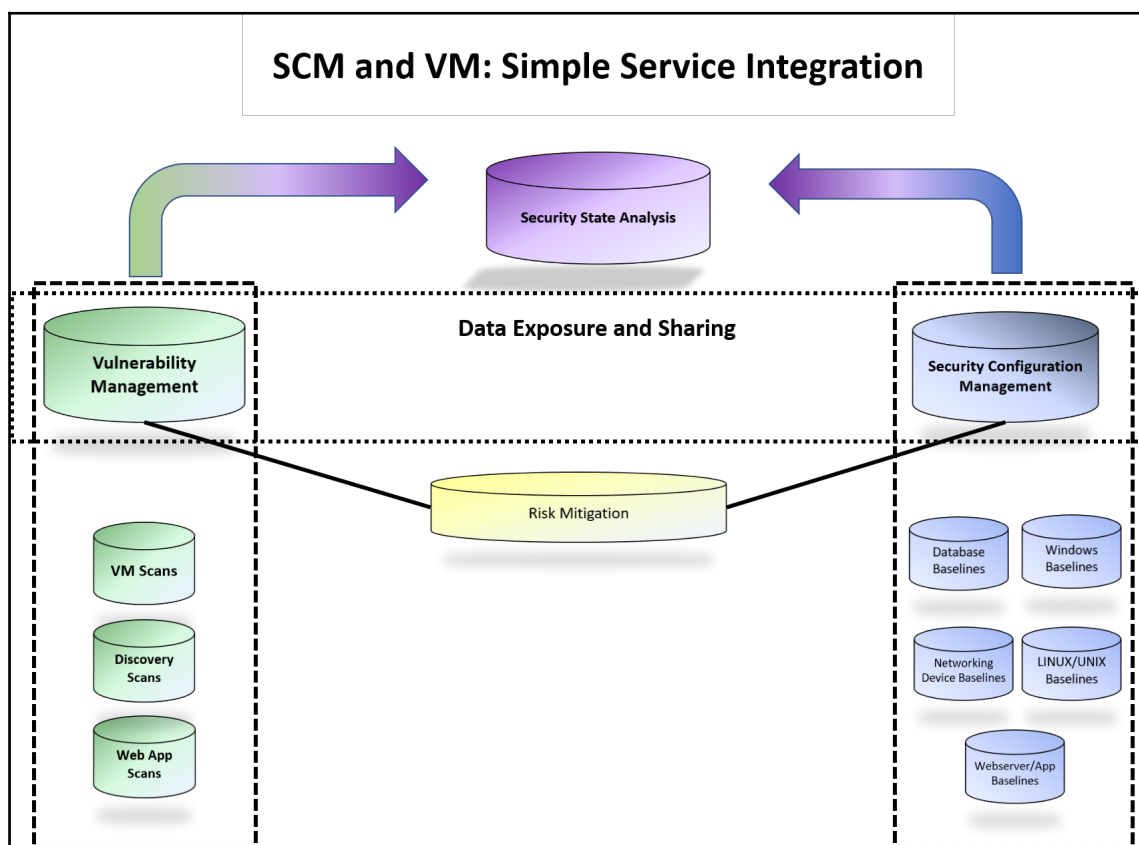


If we compact core process, discovery detection, Risk Mitigation, and security analysis for vulnerability management services, it would look as follows:



The critical part we are missing to enable communication to be passed between the two is Data Exposure and Sharing. As these are like services, we've discussed the concept of integrated reports because these services are scanning the same systems. I'm suggesting integrated reports because *would you rather have two reports or one report that tells you what to fix on your systems?* Honestly, I've run into so many stakeholders that have told me that they simply can't prioritize what to fix because the cyber security teams keep on sending them random reports.... more on ideas for this later.

Ultimately, what we are trying to achieve are two legs of the spider that can interact with each other to report to the body/head through *Security State Analysis*. This is depicted in the following diagram:



# Integrating cyber intel from different services

When I think of a service or team that incorporates different methods to exploit their targets which are applicable to the same processes of a tradition information security organization, I relate it to the red team function.

## Overview – red team methodology

The red team uses multiple means to test an organization's controls and behaviors of personnel in the organization, using their own methodology that is similar to what we've learned about the Cyber Kill Chain:

- **Reconnaissance:**
  - What can we find out about the target?
  - Where are the weaknesses?
  - How can we exploit them?
- **Weaponization:**
  - What do we need to develop to exploit the vulnerability that we found?
- **Delivery:**
  - How are we going to package this?
- **Exploitation:**
  - How are we going to get the vulnerability to do what we want?
- **Post-Exploitation:**
  - We are in! What are we going to do now?
- **Reporting:**
  - Did we get what we wanted?
  - Why or why not?
  - Who needs to know this?

## Red team – testing methods

The types of testing that this team does depends on the amount of information that they are given to complete their mission.

### White box

The team is given a target, mission, and all the information necessary to complete the mission:

- **Pros:**
  - Reduces the time spent on earlier phases
  - Focused testing on specific areas
- **Cons:**
  - Not realistic as all the information is known to the team

### Gray box

The team is given a target, missions, and some information to complete the mission:

- **Pros:**
  - Semi-realistic in that by giving incomplete information, it allows the teams to attempt to exploit unknown vulnerabilities that were found during the reconnaissance phase
- **Cons:**
  - Increases the amount of time spent on earlier phases

### Black box

The team is given a target, a mission, and no information to complete the mission:

- **Pros:**
  - The testing is done without bias
  - Most realistic as it allows for the organization to:
    - Validate known vulnerabilities
    - Test controls and processes of multiple teams:
      - Continuous monitoring
      - SIEM

- Privileged Access Management

- **Cons:**

- Most time and resource intensive
- Areas of infrastructure may not be tested

## Red team constraints

There are many constraints with this team, but I wanted to list just three main ones:

- **Time:**

- As with any project, the resources can't last forever. There is a definitive start and stop date.
- Red teams have to bear this in mind, whereas adversaries don't have to worry about time as they can take as long as they like.

- **Skillset:**

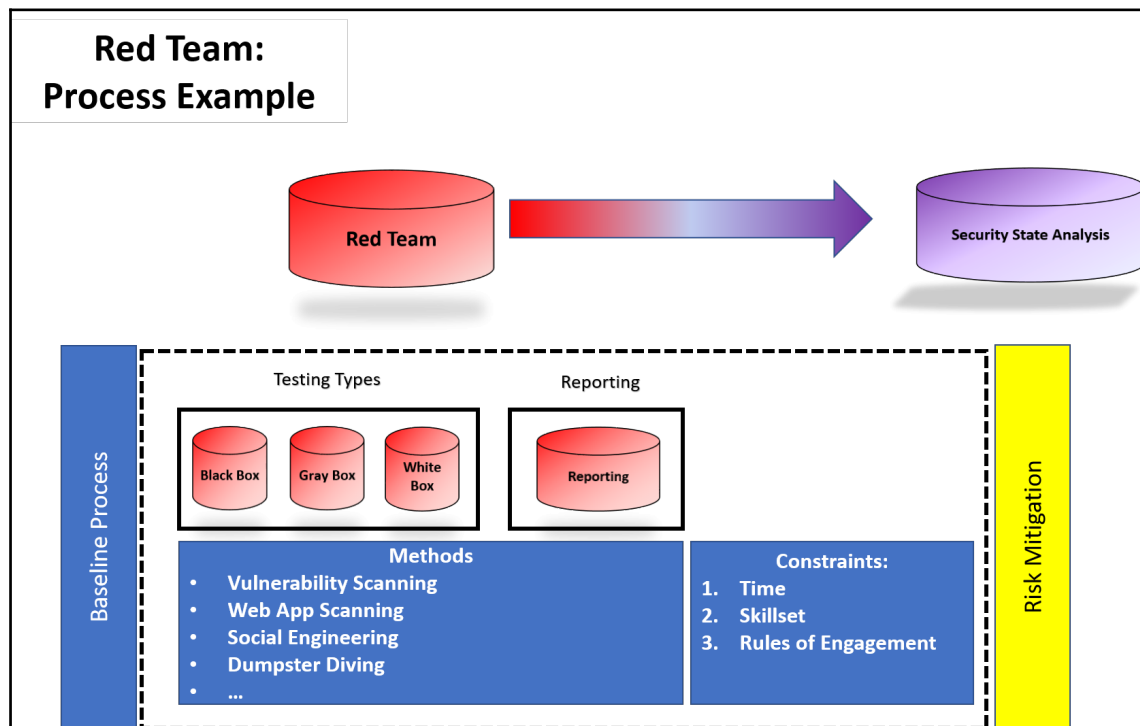
- If the team is in-house, you will have a skillset deficit unless your team is constantly training on the newest TTPs.
- If the team is outsourced, you will be paying a premium for those skill sets.

- **Rules of engagement:**

- Red teams have rules that they have to follow, which does not allow them to exploit:
  - Production networks and systems
  - Out of band vulnerabilities, such as:
    - Family members
    - Neighbors
    - Personal home networks

## Red team – graphical representation

We've gone over the basic principles of what a red team is, as well as some of the constraints that are inherent with this team's capabilities. Once the team provides its assessment at the end of the engagement through **reporting**, these results would then go into the overall **Security State Analysis** reconciliation point to be forwarded on to the SOC at the Tactical level. This is represented in the following figure:



## Data integration challenges

At first, we can look at the preceding section and say "*hey, that's pretty easy. All we have to do is provide the non-compliance, vulnerabilities, and red team reporting to the users. They'll be able to take care of it!*" Sadly, if you have ever been on the receiving end of an audit, you would know that no one likes getting bad news. Security as a service (although important) is also looked at as a burden to operations as it's just more things for the stakeholder to do. Fix this, fix that...it's kind of annoying. So when we think about integrating security service information, we should think (in parallel) about how we package up the data as cyber intelligence to each other as well as the end user.

We want our reporting to not just be another CSV we have to sort through, we want the information that we provide to be actionable. So let's look at what challenges with data integration we will face from different perspectives.

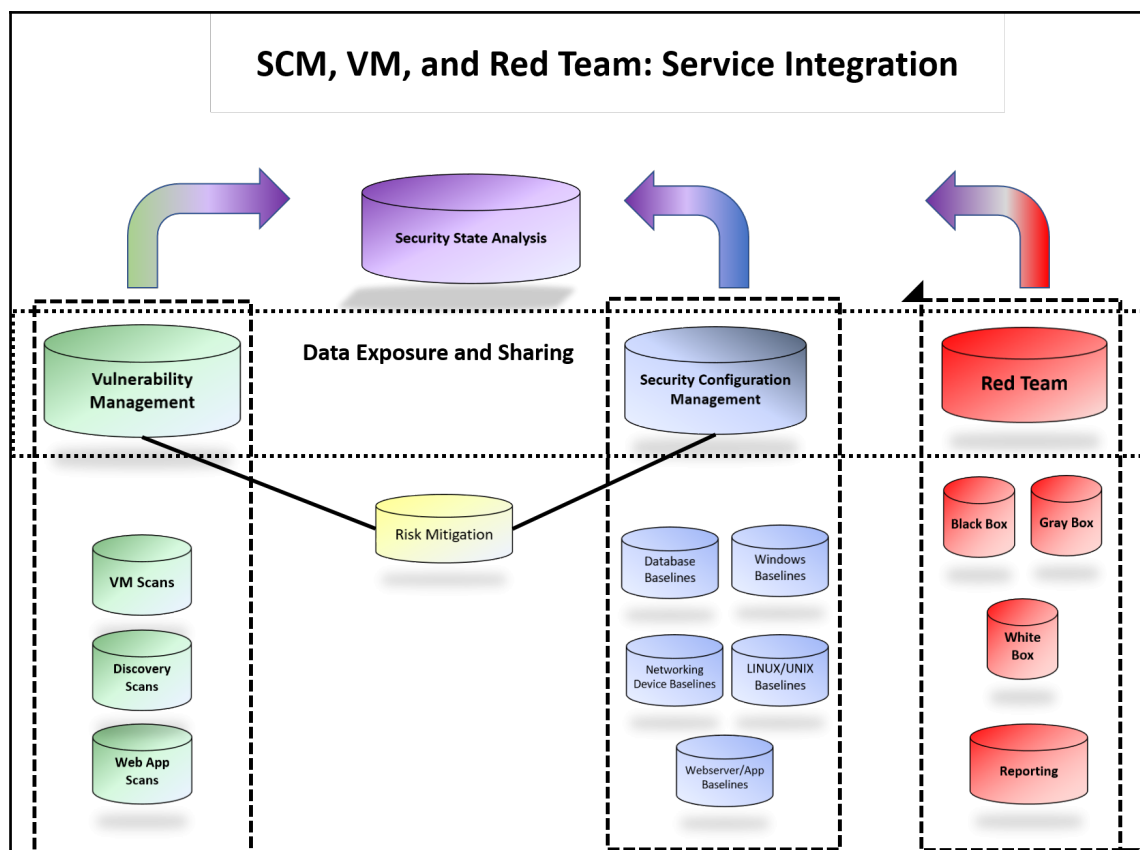
## The end user perspective

- What do I do with three different reports from each of these services?
  - Imagine getting one report that says *Hey, you are not right here*. Then think about getting another two reports that say the same thing. As an end user, I would rather have a single report explaining to me what things I need to fix, why, and how **we** can do it.
- Where do I even begin? What do I fix first?
  - Another thing that gets under my nerves is that when given a report, there is absolutely no guidance on what I need to fix first
  - Integrating information should include at least a starting point:
    - For example—fix your *crown jewel* systems first perhaps? Platinum, gold, silver, then copper, and so on

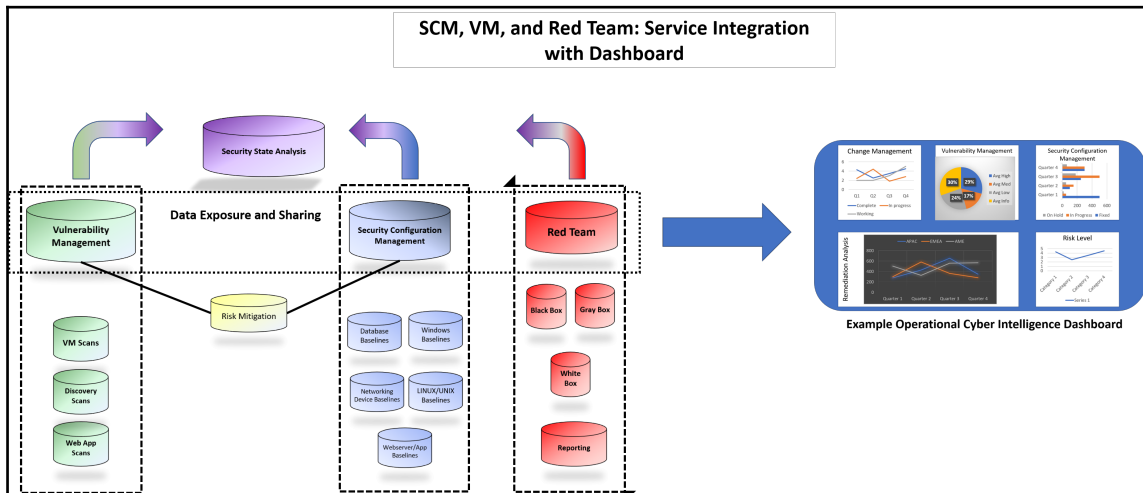


## The service level perspective – cyber intelligence – Data Exposure and Sharing

- Who needs to know my info?
  - The three services are just a few examples, but some other services may want to know some information that has been developed by the teams. Identify which services they are and figure out:



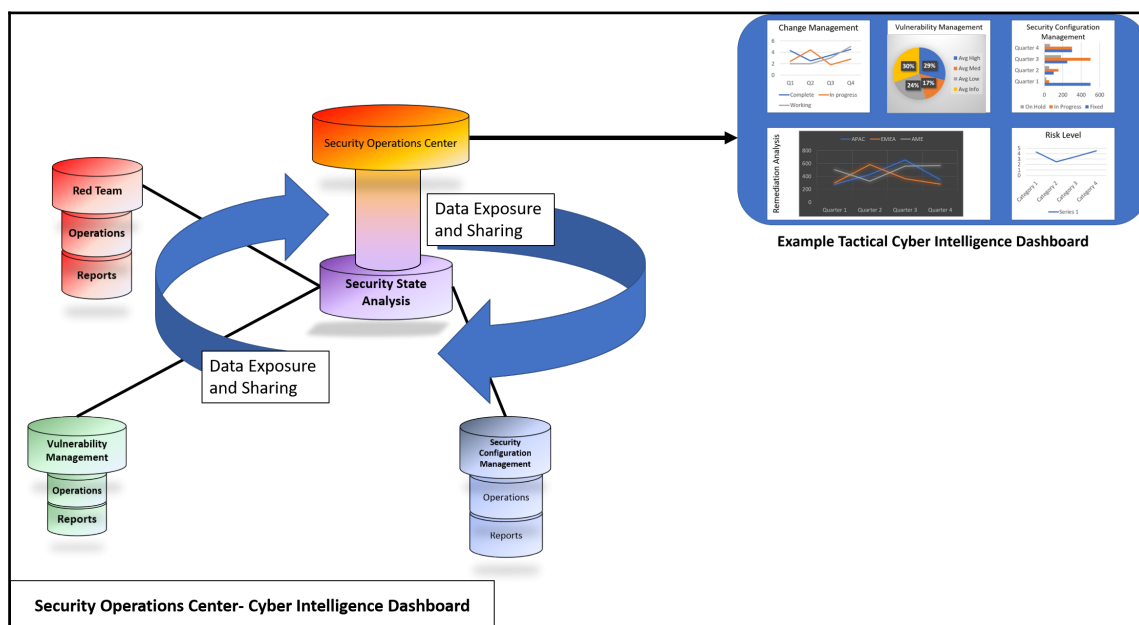
- What do the other services need to know?
  - We need to be able to figure out what the other teams need to know and at what frequency
  - Develop Key Risk Indicators among services
  - Automate to create the operational cyber intelligence dashboard



- How will we track results? How do we ensure that the results that are found are mitigated?
  - The left-hand needs to know what the right hand is doing. It will be the same with the teams that are sharing this information with each other.
  - If the red team and vulnerability management team found the same vulnerability in the base processes, it would be good to know (at the same time) when the vulnerability was fixed by the Risk Mitigation process.

## The SOC perspective

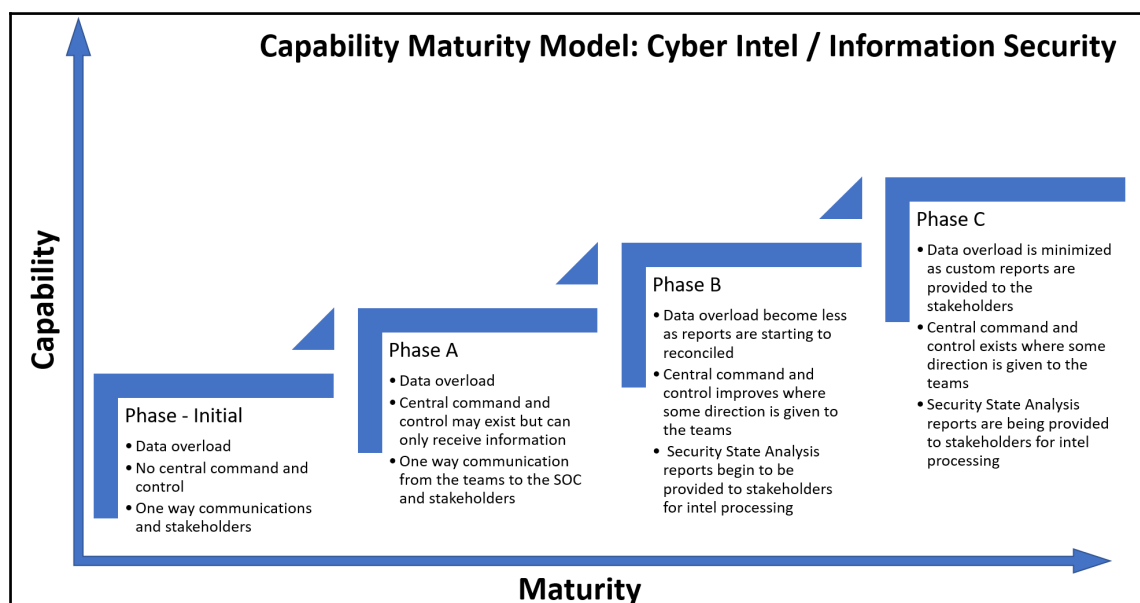
- How do we make the information that we've gathered from SCM, VM, and the red team useful to us?
  - Which area has more weight than the others?
- How do the results from the information gather impact the overall security of the organization?
  - In addition to SCM, VM, and red team results, we need to be able to fit them into understanding the security posture of the organization.
  - How will we be able to present this?
  - Automate to create the Tactical cyber intelligence dashboard.



# Capability Maturity Model – InfoSec and cyber intel

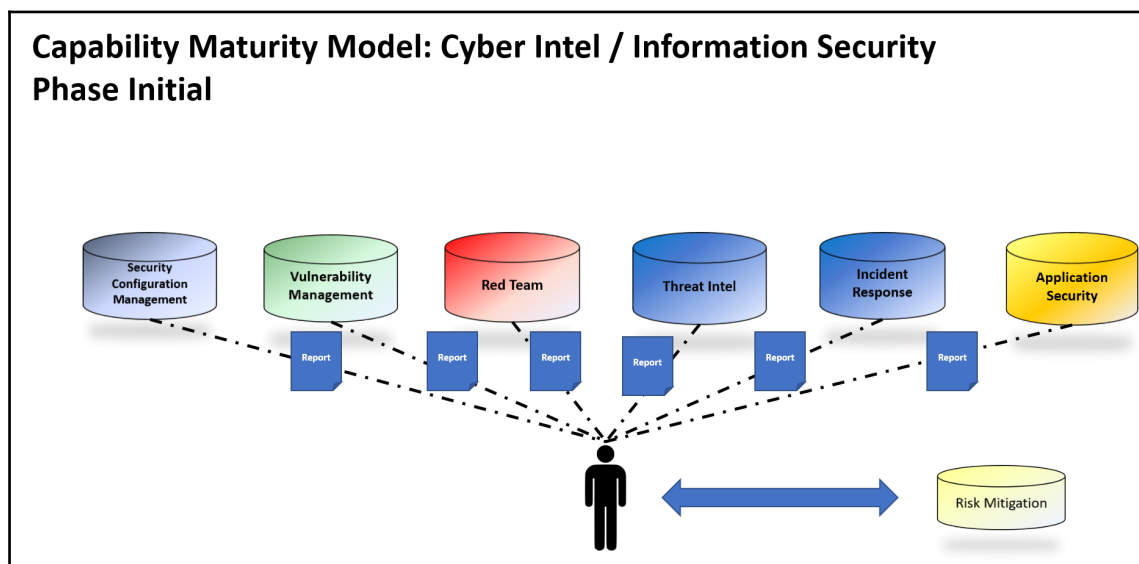
All of the subsequent sections have led up to the Capability Maturity Model: InfoSec and cyber intel. If three services are complicated to interface with one another, we only complicate it more by adding more services to interface with each other. Again, not a simple task, but we can at least build a foundation and start managing some of our own internal expectations of how we can establish the capability to communicate between the teams and provide the intelligence to and from the Tactical level.

Here is a review of what we are about to go over:



## Capability Maturity Model - InfoSec and cyber intel – initial phase

In the following diagram, we see that the information security teams are providing multiple reports to the customer. The customer is responsible for mitigating the risk through their own processes:

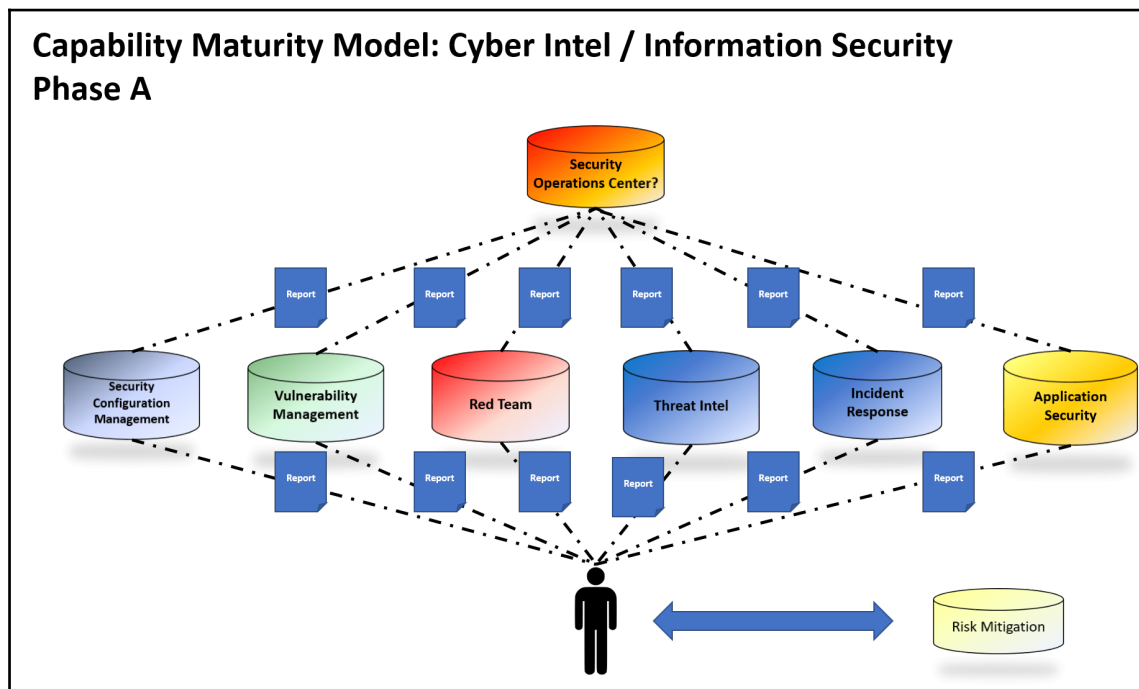


These are the main highlights from this phase:

- This would be what I consider *data overload*, where the customer has so many things on their plate that they simply give up
- This is a one-way street or a radio that broadcasts to anyone who is listening
- There is a lack of interaction between information security teams
- There is no accountability for fixes

## Capability Maturity Model - InfoSec and cyber intel – Phase A

In this diagram, we begin to see somewhat of a resemblance of the centralization of reports to an SOC. The SOC may not be very mature at this point, but it is also just gathering the information that it receives from the teams.

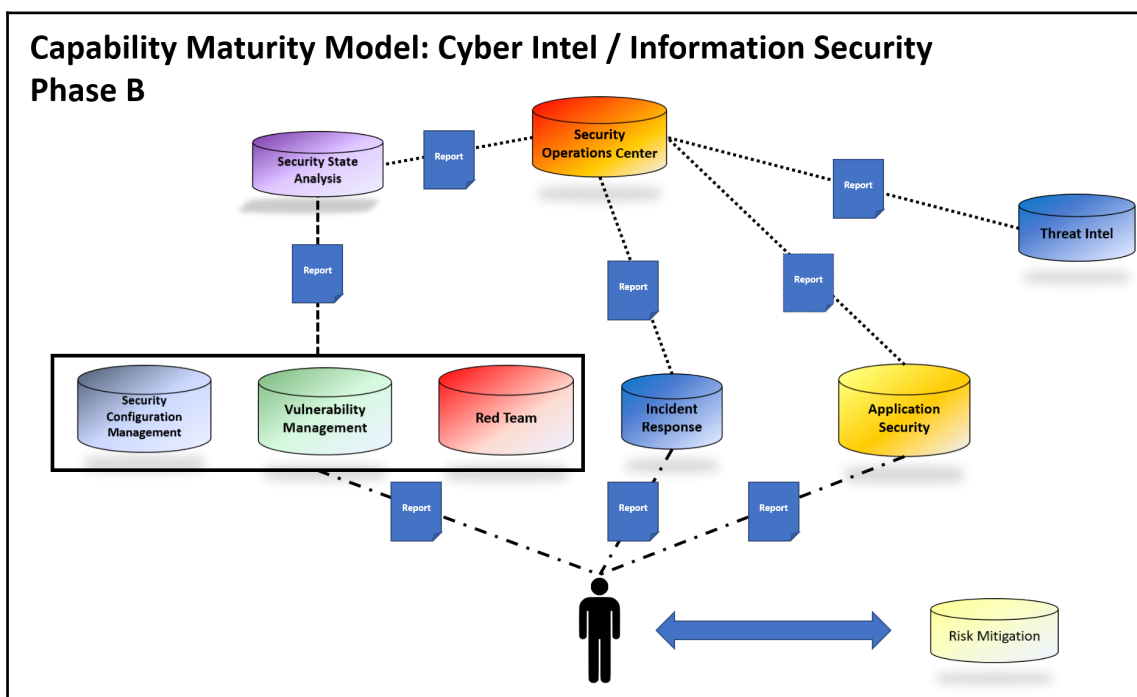


These are the main highlights from the phase:

- This is another variation of *data overload* where the customer and the SOC have multiple reports delivered
- It is still a (longer) one-way street or a radio that broadcasts to anyone who is listening
- There is still a lack of interaction between information security teams
- There is no accountability for fixes

## Capability Maturity Model - InfoSec and cyber intel – Phase B

In this phase, we start to see the consolidation of reporting for teams, as well as changes in reporting to the customer and the SOC. At this point, information is starting to be processed in *Security State Analysis*, where information is being analyzed in both directions to provide the most value to the stakeholders. However, we can still see that there are still multiple reports going to the customer that may or may not cause confusion as to what risk to mitigate first.



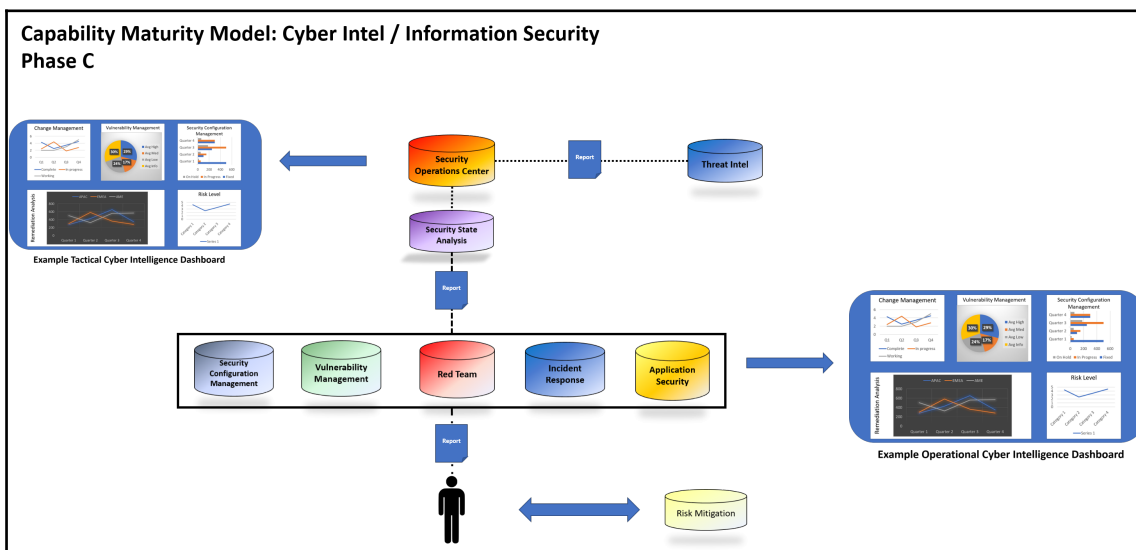
These are the main highlights from the phase:

- *Data overload* may or may not exist for the customer as reporting is becoming more customized.
- The SOC begins to analyze reports from the services and provides guidance and direction to the teams.

- The one-lane road is starting to become two lanes that are going to and from the customer: from Operational Level to Tactical Level.
- There is an improvement in the interaction between information security teams, but they do not fully interface with each other.
- With the improvement in communication, the customers have more of an idea of what needs to be fixed and when. Building relationships and improving governance will contribute to the accountability for findings being addressed.

## Capability Maturity Model - InfoSec and cyber intel – Phase C

Phase C of this Capability Maturity Model is a desired end state where information security teams are fully interacting with each other and providing useful information, up to the SOC and down to their customers.





These are the main highlights from the phase:

- *Data overload* is minimal or does not exist for the customer as reporting is customized to their needs
- The SOC is able to continuously analyze reports from the services and provides guidance and direction to the teams as PIRs flow down, across, and back up through the communication channels
- The two lanes that are going to and from the customer: from Operational Level to Tactical Level is now a highway
- There is full interaction between information security teams

## Collaboration + Capability = Active Defense

The examples that I've given in this chapter lead to this section in that *Collaboration + Capability = Active Defense*. Like I've stated in previous chapters, Active Defense does not have to be considered as *defend and hack back* or *defend and strike*. An organization's security service provides value to the stakeholder when the information allows them to make a decision based on information that is customized to them. By developing customized intelligence for the stakeholders, we can continue to build rapport and relationships that give us the flexibility to increase the speed of our OODA loop. In doing so, **we've created the communication channels necessary to take action on external and internal PIRs, thus enabling Active Defense.**

## Summary

This chapter was a long one and it was a lot of information to digest. So, to review what we covered:

- Discussed some core security service basics
- Talked about Security Operation Center capabilities
- Had a discussion about how we can integrate services and improve their communication
- Discussed a Capability Maturity Model for information security that enables cyber intelligence
- *Collaboration + Capability = Active Defense*

# 9

## Driving Cyber Intel

Cyber intelligence doesn't only come from IT operations and IT security. The dimension that we have not discussed is how we can leverage the user as a source of information. Through training, we can empower users to help us report the things that our scanning, monitoring, and processes miss.

In this chapter, we will cover:

- Integrating the user into cyber intelligence
- Security awareness now and where it can go
- Capability Maturity Model - security awareness

### The gap

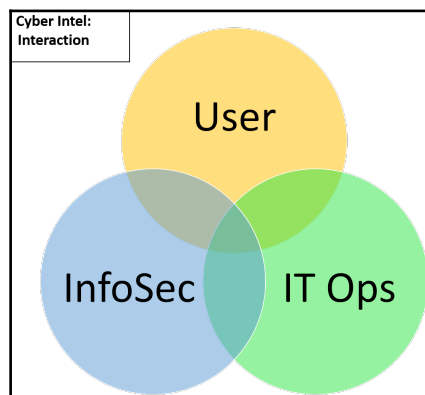
So far, we've looked at *the gap* as a linear *where we are* and *where we want to be* on a Capability Maturity Model. This has been (up to this point) addressing the gap between IT operations and IT security.

We've talked about some ways that we can interface between these teams through the use of:

- Service level agreements
- Organizational level agreements
- Processes
- Policies and procedures

However, we need to take another gap into account. The user, stakeholder, or customer is at the receiving end of every service that we provide.

Creating useful information is important to communicate through formal and informal channels between IT and InfoSec; however, the user can also use cyber intelligence to drive their decision making.



What makes the userspace interesting is that the level of interaction between either InfoSec/IT ops is limited through the methods we've discussed:

- The users must use the process and procedures that are put into place
- The users must agree to the organizational policies

Since collaboration is the theme we are trying to convey in this book, we need to look at the user as an entity that we should be working with. We shouldn't be only pushing down edicts.

## Another set of eyes

When I think of security awareness, I see a lot of opportunities to engage with the users, not only with training that is important, but with information (cyber intelligence) that will be useful for them to make a decision. Sometimes, when I see a security awareness team, I only see them as developing content that emphasizes good cyber security hygiene and a reiteration of the protocols of the organization.

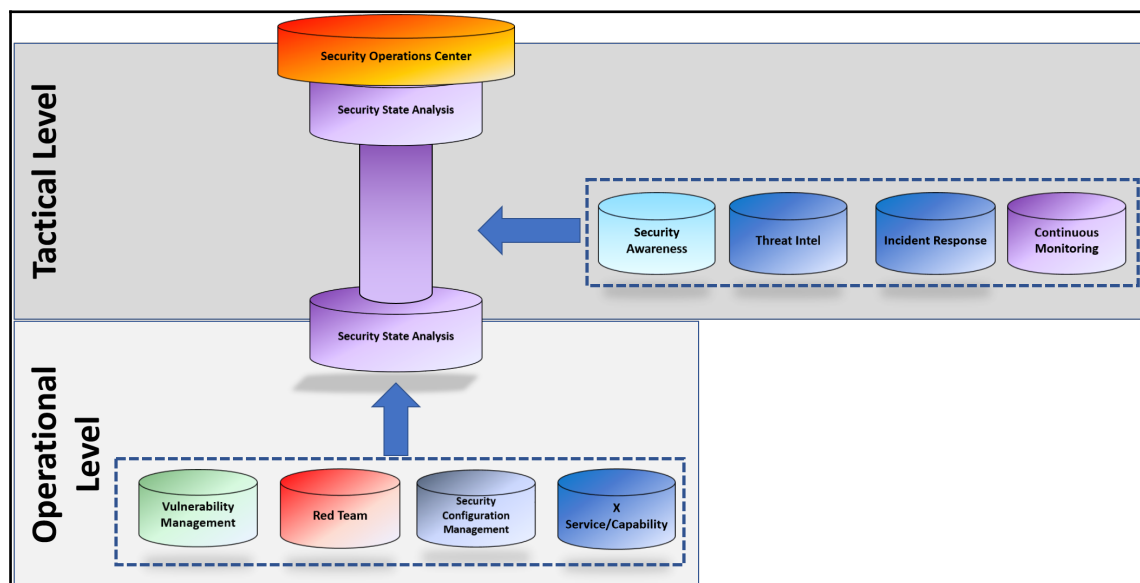
Have you ever asked the question, *what else can they do?*

My opinion is that security awareness is the interface between IT ops, InfoSec, and the user. If knowledge is power, then we should take the opportunity to develop the capability of this team to go beyond protocols and cyber security hygiene. We should develop this capability to enable the users to be another set of eyes for the organization.

## The logic

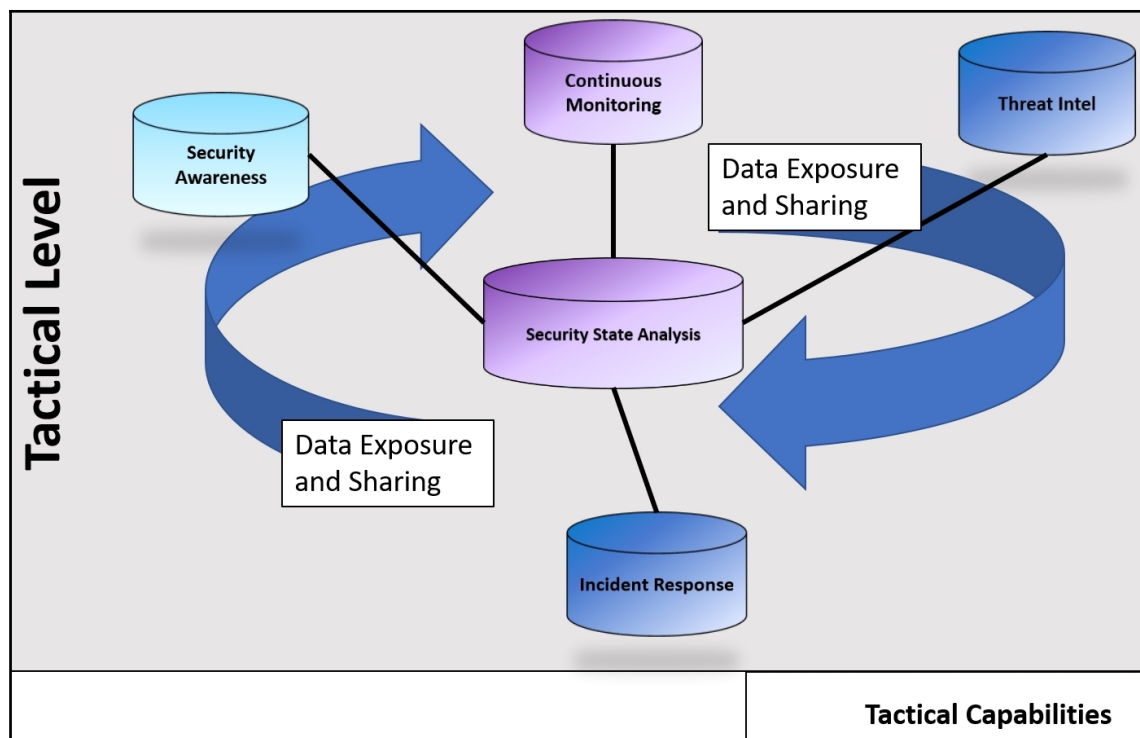
I tend to believe that security awareness sits in the Tactical level as it receives the requirements from the strategic level and then devises its own planning to provide training and education down to the Operational level.

As the SOC sits at the Tactical level as well, we can also imagine that the continuous monitoring, threat intelligence, and incident response capabilities also are at this level.



As depicted in the following diagram, each of these capabilities helps shape the *Security State Analysis* of the InfoSec spider.

It is also at this level where *Data Exposure and Sharing* is done between the services so that they are all in tune with one another:



But how are these services connected to each other? They are all connected by how they view **events** and **incidents**.

## Event

An **event** in information security is an occurrence or something that has happened out of the normal operations of a system or process.

Here are some examples:

- User reports that they cannot access a website on Fridays
- Firewall rules were unknowingly updated
- System administrator reports that users were added to the domain controller without proper authorization

## Incident

An **incident** in information security is something that has or is threatening to happen to an information system's confidentiality, integrity, and/or availability.

Here are some examples:

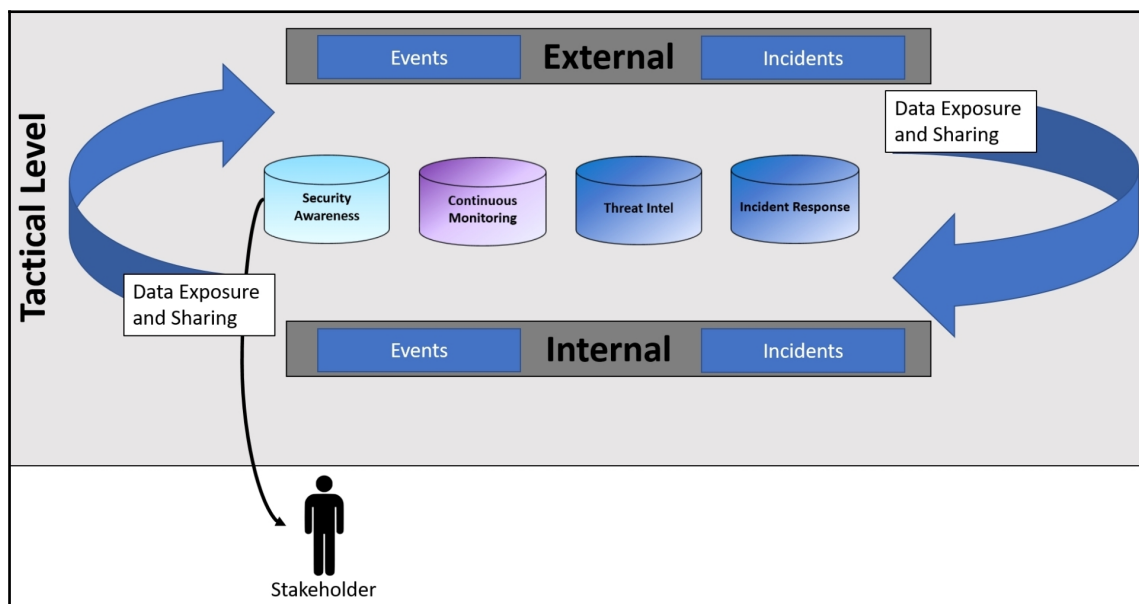
- Denial of service attack being reported in specific regions
- Personal identifiable information of government officials has been posted on DarkNet forums
- User reports that they clicked on a link, downloaded an application, ran it, and the system is locked up by ransomware

## Mapping events and incidents to InfoSec capabilities

Three services deal directly with incidents and events:

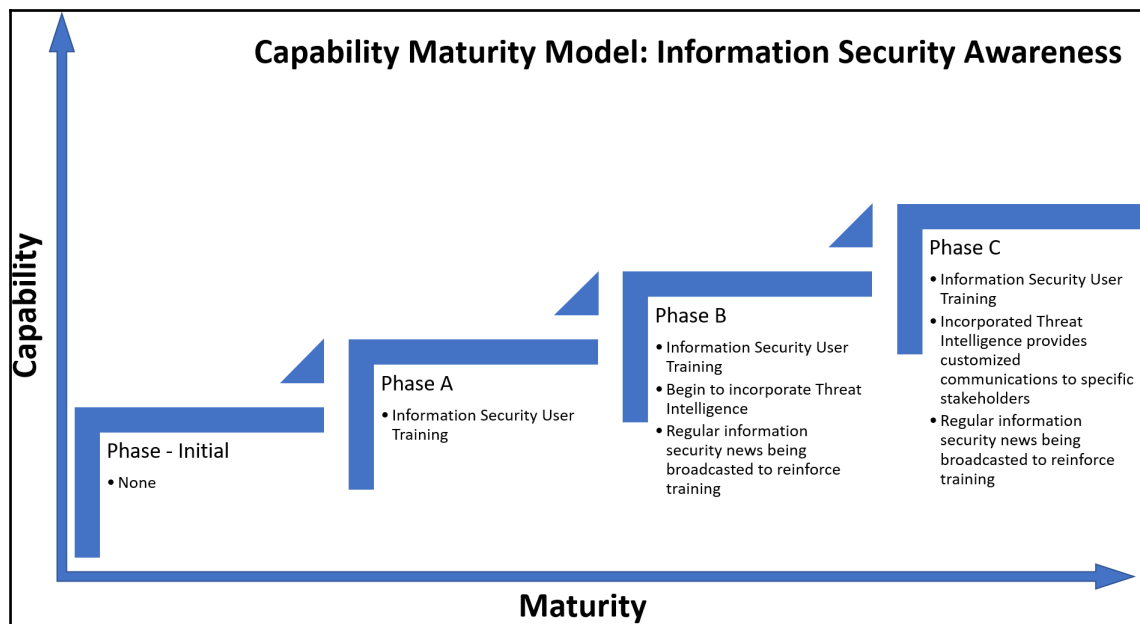
- **Threat intel:**
  - Externally focused on incidents and events that are reported in threat intel feeds
  - May map external threat intel to applicable **internal** systems to provide enriched cyber intelligence
- **Incident response:**
  - Internally focused on incidents and events that are reported
- **Continuous monitoring:**
  - Both internally and externally focused on evaluating anomalies against established baselines

Through *Data Exposure and Sharing*, security awareness allows pertinent **external** threat sources to be communicated to the users, as well as providing the training and support (through formal policies and procedures) to report **internal events and incidents** through IT ops or InfoSec channels.



# Capability Maturity Model – security awareness

So to begin on this journey of interfacing capabilities to lead to another set of eyes, we have another example of a Capability Maturity Model for security awareness.





## **Capability Maturity Model - security awareness Phase - Initial**

In this phase, we do not have the capability of informing our users about anything. This may be because the security awareness capability is lower on the priority list of things to do than all of the other capabilities that are being developed. However, it is important to the organization and there needs to be a push to establish some basic items for users, such as:

- Acceptable use of organizational systems
- Email safety

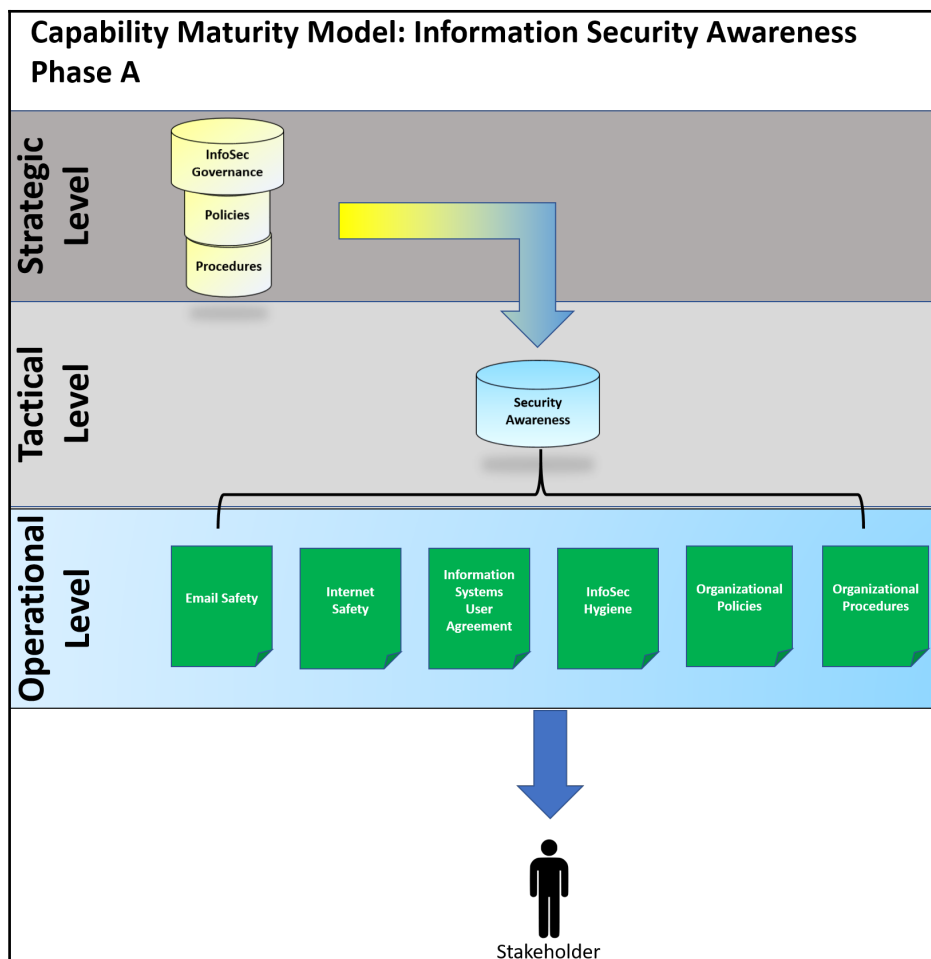
But as the IT and InfoSec organization becomes more mature, so must the security awareness program.

## **Capability Maturity Model - security awareness – Phase A**

During this phase, the security awareness program becomes more developed and accepted in the organization. The strategic level begins to issue the policy and the procedures of the security awareness program. Basic training is provided to the organization's users on:

- Internet safety
- Cyber hygiene
- Organization policies
- Organizational procedures

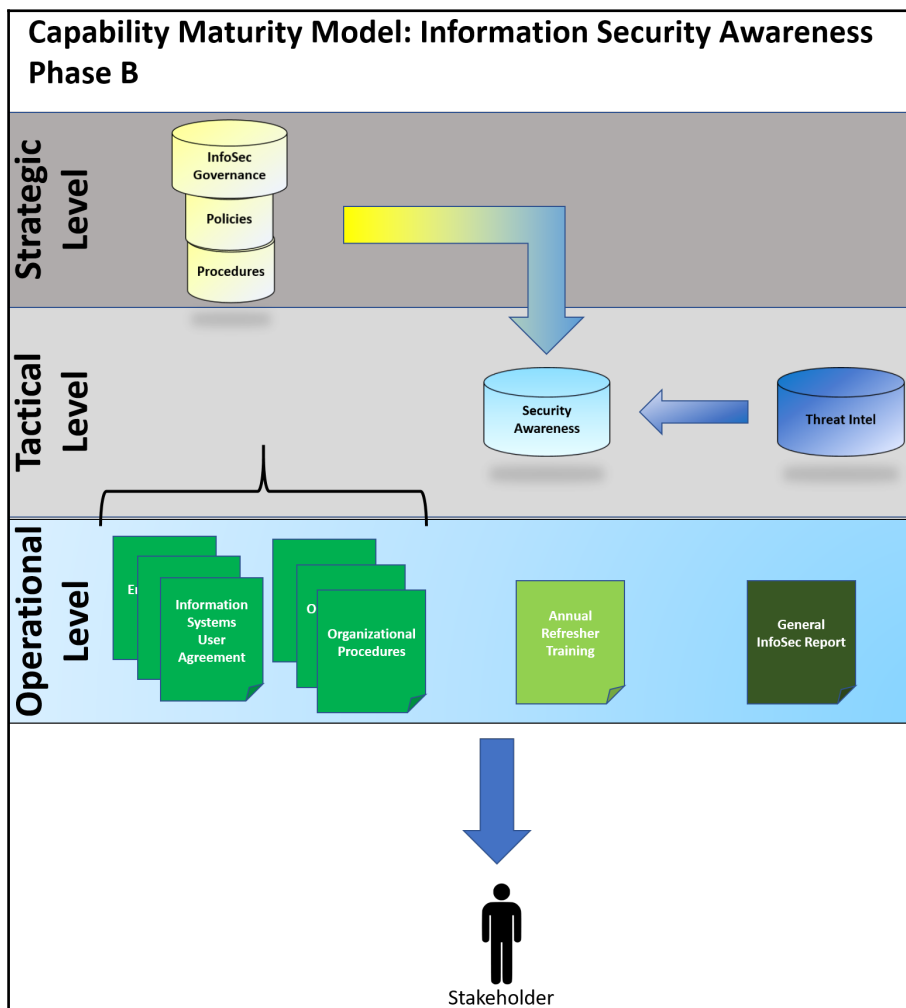
At this point, users know what to do as well as what not to do. The security awareness maintains its capabilities by updating their material as required.



## Capability Maturity Model - security awareness – Phase B

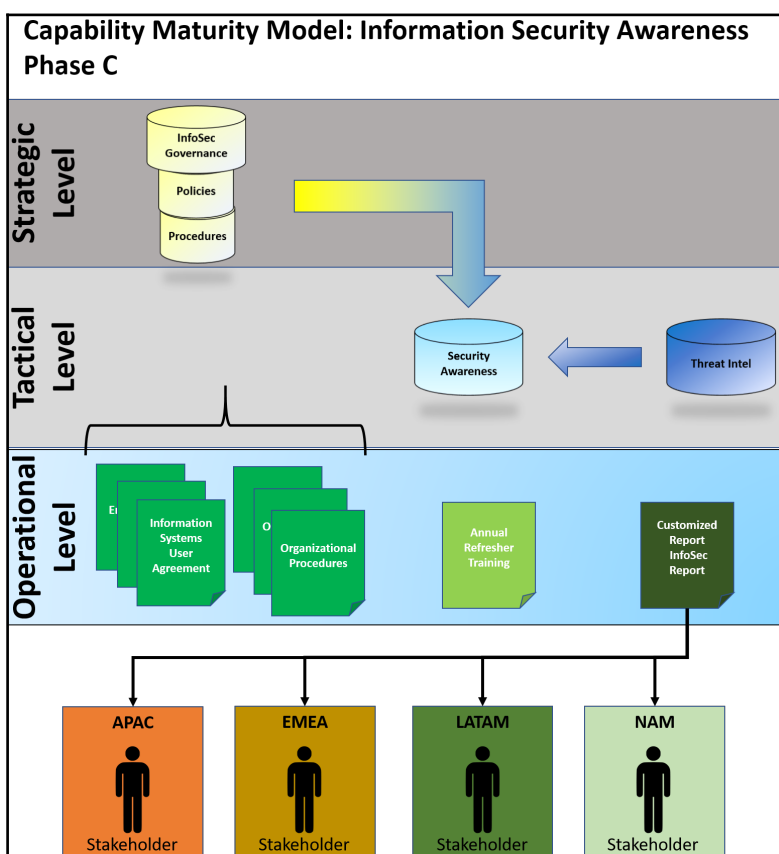
Phase B in the security awareness Capability Maturity Model is a more mature service that provides basic training as in Phase A, but also enhanced training annually to keep material fresh for their customers.

There is a need to improve the education of an organization on the current threats that exist in cyberspace. So, we now begin to see the inclusion of threat intelligence information driven down to the user as *general reports* that are not specific to the organization, but just a *good to know* kind of information. The threat intelligence information provided isn't catered to anything specifically. These reports may come out regularly as an email newsletter or during a regularly scheduled meeting:



## Capability Maturity Model - security awareness – Phase C

This is the final phase where the security awareness capability is fully developed. Threat intelligence is now being provided in reports that are applicable to the users that receive them. For example, the users in the regions depicted in the following figure are informed about threats that exist in those countries that are currently being reported by threat intelligence sources. This allows them to take this cyber intelligence and use it when they make decisions on the actions that they take:



If you are thoroughly confused at this point, I don't blame you. The question I would be asking is:

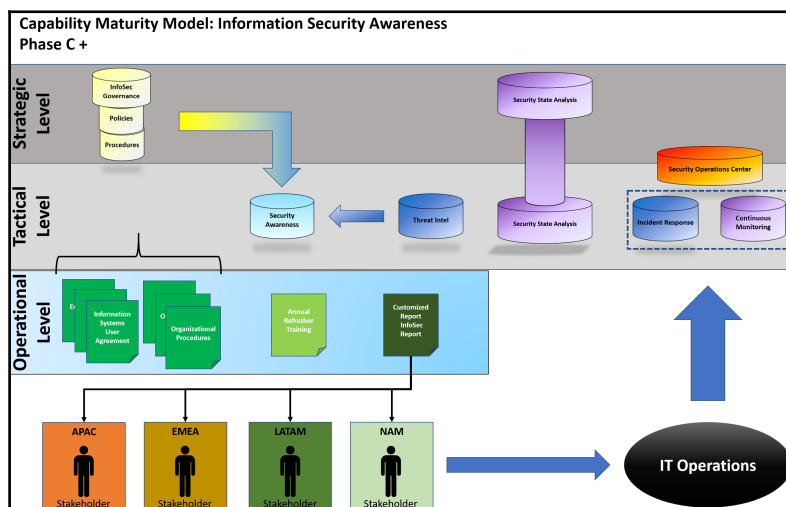
- How is developing a security awareness capability in accordance with the Capability Maturity Model going to give us another set of eyes?

The answer is how we will incorporate the user into IT Ops processes to help us know what we don't know.

## Capability Maturity Model - security awareness – Phase C +

Phase C+ is the endpoint for all the services discussed in this chapter so far. By training and providing actionable information to our customers (the user), we enable them to provide information that our scanning and monitoring may or may not miss.

We want these services to map events and possible incidents so that *Data Exposure and Sharing* information is enriched with user reporting so that the organization can take action faster.



## Just another day part 1

It's a blistering hot day in Bengaluru, India, and Sandeep is thankful for being in an air-conditioned building. In 2013, CorQue Boards Inc hired him as an engineer right out of university, and now he's one of the lead engineers of his group, building circuit boards that are distributed globally. The company provided him with the usual desk with dual monitors that hook into his laptop's dock so that he can design and improve the product with his team. Other than the IT guy giving him the laptop and phone, there was little to no interaction with the IT department.

Every year he was reminded by HR in an email that he needed to complete his annual *cyber risk* training. *This is so annoying* thought Sandeep as he started to look at the portal where he was to log in.

Meanwhile, in Warsaw, Poland, Malgorzata (aka Gosia) was working on the next CorQue Boards information security newsletter for her assigned region, APAC. She was on a team where each team member worked on building the training and information security news for their regions as well. Their job was to provide the region's IT divisions up to date information on threats that may impact their region, country, or specific business unit. Because she wanted to do her job well, Gosia went to other sources of open source intelligence just in case the threat feeds missed anything.

*Hmm...APT 1.8 is at it again with another ransomware campaign* she thinks to herself after reading a tweet. APT 1.8 was well known for their use of social engineering to get users to download antivirus software by posing as the organizational IT helpdesk. "Eh, I already posted a newsletter about these guys" Gosia said to herself "I'll have to write about something more exciting..."

Sandeep was plugging away at his training...

*"Don't click on links"*

*"If you see something, say something"*

*"You are reminded that..."*

*"This has to be the worst...every year, 45 minutes of 'interactive' training and a quiz. To top it off, if you fail the quiz, you have to do it again....from the beginning!"* Sandeep sighed...\*ding

Oh, what now? Sandeep took a deep breath and looked into his inbox.

**FROM: IT.HELP@CO.RQUE.NET**

**TO: <Undisclosed Recipients>**

**SUBJ: IT HELPDESK- "ANTIVIRUS UPDATE"**

**IMPORTANCE: HIGH**

Noticing that the **FROM** field was not @corque.com Sandeep was a little puzzled. He had remembered from his training to look at where an email was coming from and make sure that if it was an organizational email, that the domain was correct. Curiously, Sandeep opened up the email and read:

*Dear User,*

*As you know, ransomware is on the rise globally and our IT team is working hard to ensure that our data is protected at all times. In addition to our outstanding monitoring capabilities to detect these types of malware, we have purchased additional protection through "SeaQuenchAle" a well known cyber security company. To help facilitate this additional protection, please follow this link, download, and install the application as soon as time permits. If not done within 24 hours, this application will be pushed to your system, a forced restart will commence, and you will lose any data that is not saved.*

*We appreciate your cooperation in this matter.*

*-IT Helpdesk*

Learning about hovering his mouse cursor over the link from his training to preview the URL, Sandeep found that the link did not go to a sequenceable domain at all. *Really weird*, he thought. Knowing that this may or may not be real, Sandeep decided to call the IT helpdesk for support.

*"Hey, I got this email from you guys about installing some additional protection app or something...it doesn't look right"*

*"Oh yeah?" Jidnesh said, "You and everyone else got it. Send it over to the incident response email and they'll analyze it. I'll open up a ticket so we can follow up. Seems like something is going on..."*

*Will Sandeep and his IT helpdesk team figure out what is going on?*

*Will CorQue get compromised?*

*How will CorQue Boards handle the situation?*

*To be continued...*

## Summary

In this chapter, we covered:

- Integrating the user into cyber intelligence
- Security awareness now and where it can go
- Capability Maturity Model - security awareness

In the next chapter, we will learn more about the fate of Sandeep and friends as we discuss cyber intelligence and continuous monitoring!



# 10

## Baselines and Anomalies

Just as your hands have fingers, we don't judge the capability of grasping an object by looking at creating metrics for each finger. Each finger has a purpose, one to tighten, one to stabilize, and so on. Of course, we can improve our grasp, but we first must learn what it is to grasp (baseline) and what it is to improve the grasp (understanding the anomaly of improvement).

This chapter is about understanding the baselines and anomalies that exist on our network which extend across teams. As there is an ebb and flow with operations, we are able to establish normalcy among the daily tasks that are performed. We will discuss:

- The challenge of continuous monitoring
- Continuous monitoring Capability Maturity Model
- Examples of integration of capabilities for continuous monitoring to improve defense

## Setting up camp

I spent a lot of time in the field training for combat and after hours of running around in the woods, we would need to stop and rest. Wherever the location that we decided to camp in the evenings to rest up, our leadership made sure that we had a good foundation to set up a defense.

Here are a few examples:

1. Never set up in an open field because then the adversary can see your strengths and weaknesses:
  - **Cyber intelligence application:**
    - Good training in security awareness will decrease one of the likelihoods of exploiting users

- Reducing visibility (through collaboration between IT ops and IT security) for an adversary reduces the attack vectors
2. If you are going to get attacked, don't make it easy. Guide them to where your strengths are:
    - **Cyber intelligence application:** Active defense techniques—guide the adversaries to the locations where they will most likely be found out
  3. Set up your camp in a location where you can observe the surrounding area to spot any movement:
    - **Cyber intelligence application:** Enabling good IT operations and InfoSec processes allows for identification of anomalies to the baseline

## Baselines and anomalies

If you've been in IT and watched the level of traffic through your network on some tool, then you know that baselines are the starting point for comparisons. We can consider that baselines are what *normal* is. Conversely, anomalies are anything that trends against a baseline. These anomalies can be a positive impact or negative impact to the baseline that is being evaluated.

Establishing baselines can be difficult because we have to define what *normal* is and then start measuring against that normalcy. We define normalcy by monitoring the regular activities of the items that we are interested in against a specific amount of time.

The following are examples of anomalies against a baseline:

- Regular users trying to access directories that they are not permitted access to more than five times in a week
- Network usage spikes in off hours

So, before we go down a baselining/anomaly rabbit hole of *what if* statements (because we can establish baselines for numerous amount of things), let's narrow down our focus on the cyber intelligence to provide a *continuous monitoring* capability of identifying deviations to baselines on a few items between IT operations and IT security.

## Continuous monitoring – the challenge

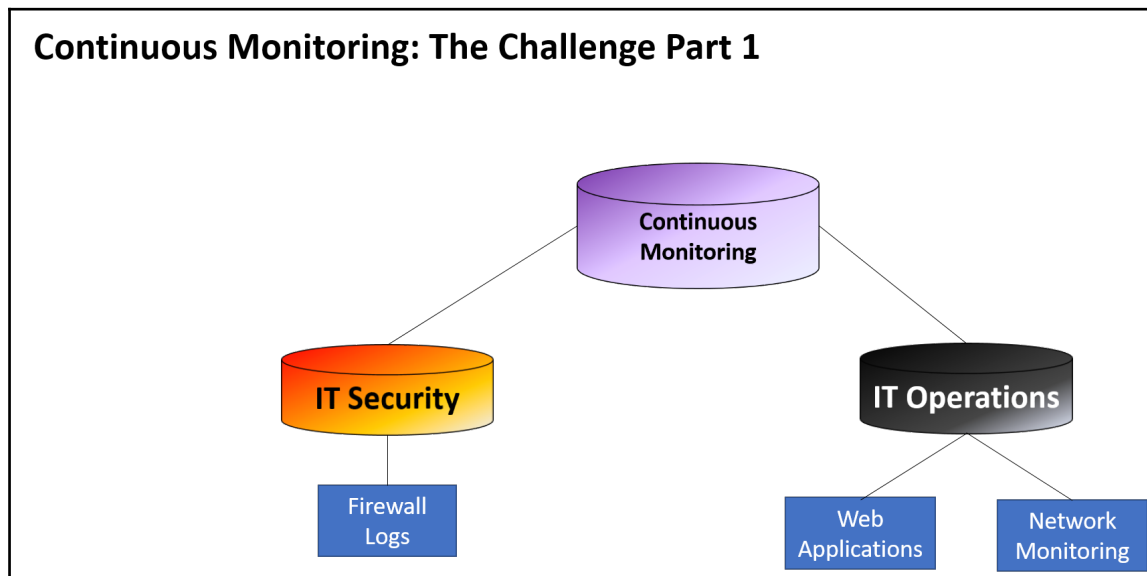
In the field, we would dig our fighting holes close enough to where we could communicate with each other on either side and spaced far enough to where a single attack by a mortar would not cause multiple casualties. The leader's fighting hole would be further back, but would have full view of where the teams set in so that the leader can go and communicate with the team as necessary in the heat of battle.

Just as preparing for combat in the field, in IT we need the right hand and the left hand to know what each is doing. If we can consider a local business unit as a platoon in my preceding example, comparatively we can add to the complexity of an enterprise to a battalion, regiment, or brigade.

### Part 1

What makes it more challenging is the subjectivity of what needs to be monitored, as well as establishing normalcy.

For example, let's review the following diagram:



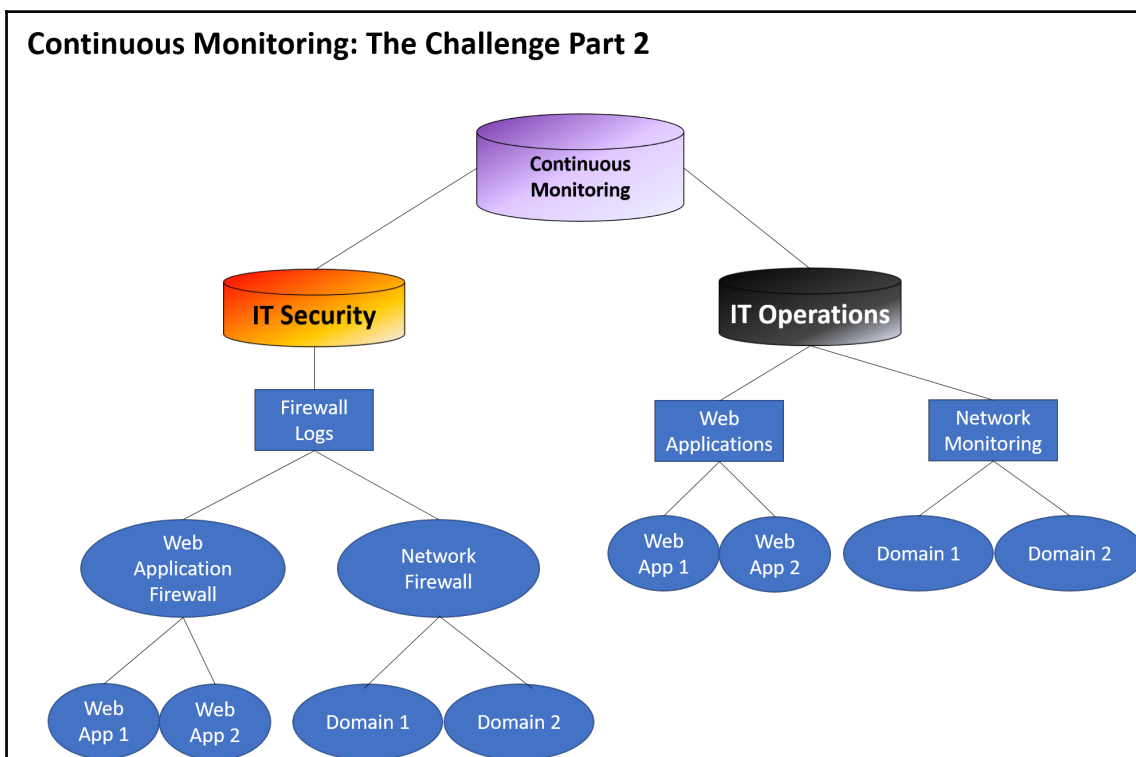
The concept here is relatively simple:

- IT security takes care of reviewing the firewall logs
- IT operations take care of the web applications and monitoring the network

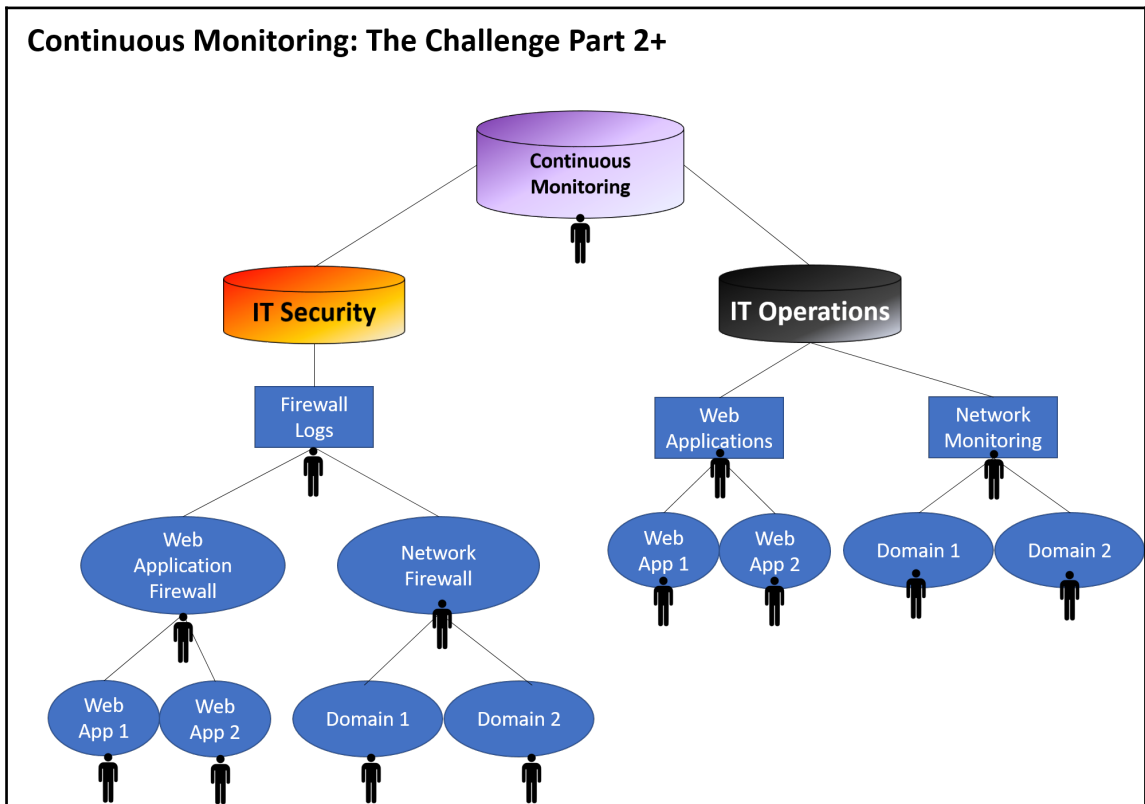
## Part 2

However, we know that the reality is much different and that we need to take some things into account:

- There are different types of firewalls that have their own logs. These logs need to be reviewed for each firewall:
  - Network firewalls between network segments
  - Each web application firewall log
- There are multiple applications that IT operations need to maintain and manage.
- There are multiple domains that may need to be monitored and managed.



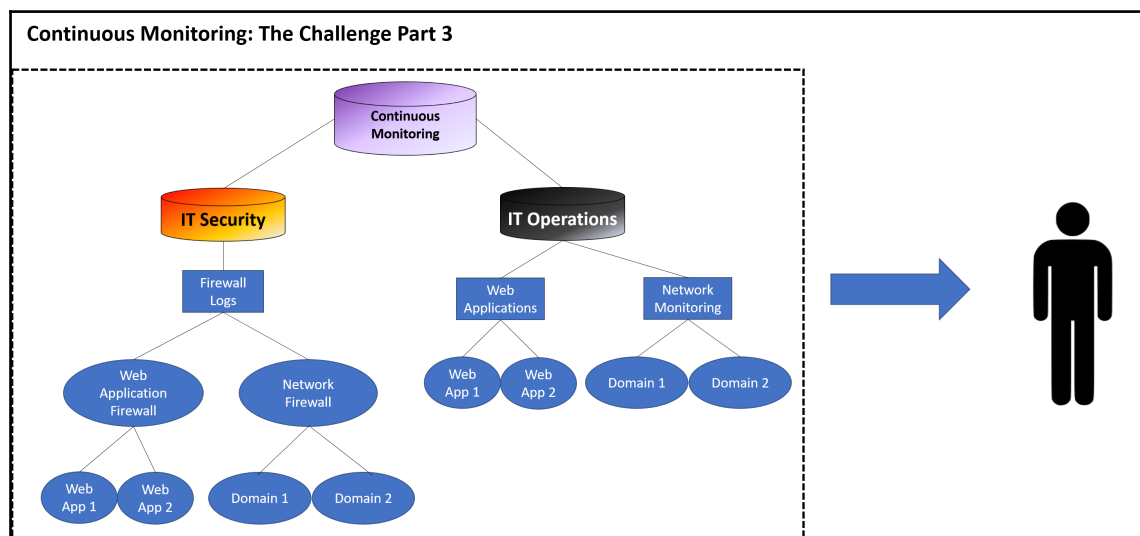
As depicted here, we've only started with two web applications and two domains. We can assume to an untrained eye that the solution may be as simple as ensuring that we have an RASCI set up to manage these items, as depicted in the following figure:



However, this is not the case as one or two people may be responsible for the entire IT continuous monitoring capability.

## Part 3

With all of this information that needs to be analyzed, the final result for an under-resourced IT team is burnout and information overload.



If you are in an SMB or a large organization, you deal with this on a daily basis. Let's try to break this down to something more palatable.

Even in parts 1 and 2, we should try to understand a few things about our dilemma:

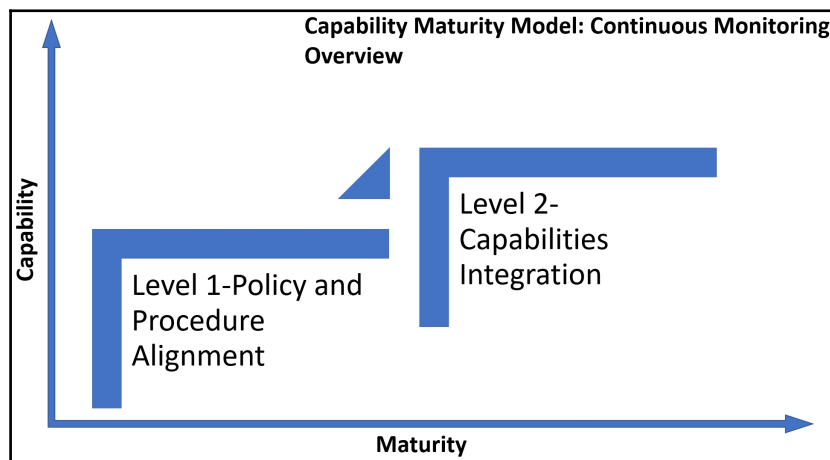
- How do we establish a tactical communications channel?
  - How will IT security communicate with IT operations on any issues?
  - How will IT operations communicate with IT security on any issues?
- What can we do to reduce information overload and burnout?
  - What is the information that we need to review?
  - Where can we automate?

# Capability Maturity Model – continuous monitoring overview

At a very high level, we need to set the foundation of a continuous monitoring capability that can be understood from both the IT operations and IT security organizations. We will focus this discussion on two levels.

**Level 1** will discuss a generalized Capability Maturity Model that we would need to apply to enable continuous monitoring for a single process, team, or capability.

**Level 2** will discuss how we will build from level 1 with the integration of continuous monitoring into the targeted process, team, or capability.

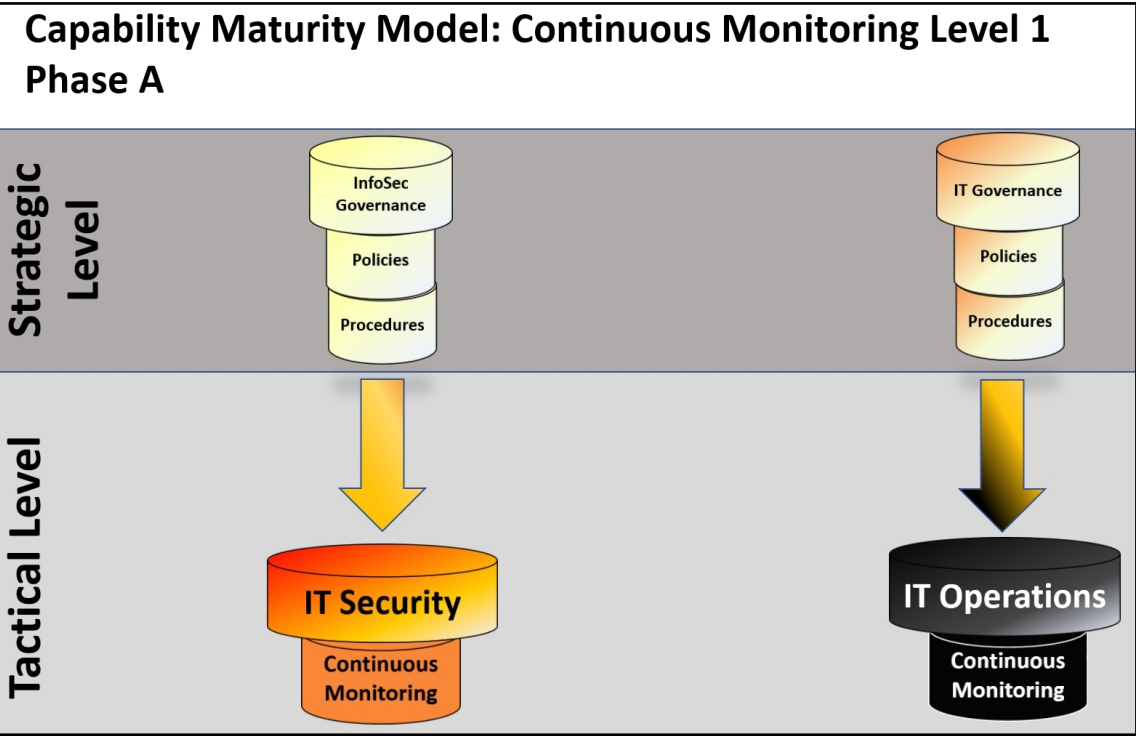


Bear in mind that we cannot go and review every item that should and could be continuously monitored as that is not the point of this text. That may be a topic for another book.

So, let's begin with how we can start understanding how to get IT operations and IT security to work together to monitor the enterprise.

# Level 1 – phase A

In level 1 phase A, we have two separate entities with their own *policies* and *procedures* that they follow. Both teams are able to review their baselines against their policies and procedures, and report them from the tactical to strategic levels on their compliance.

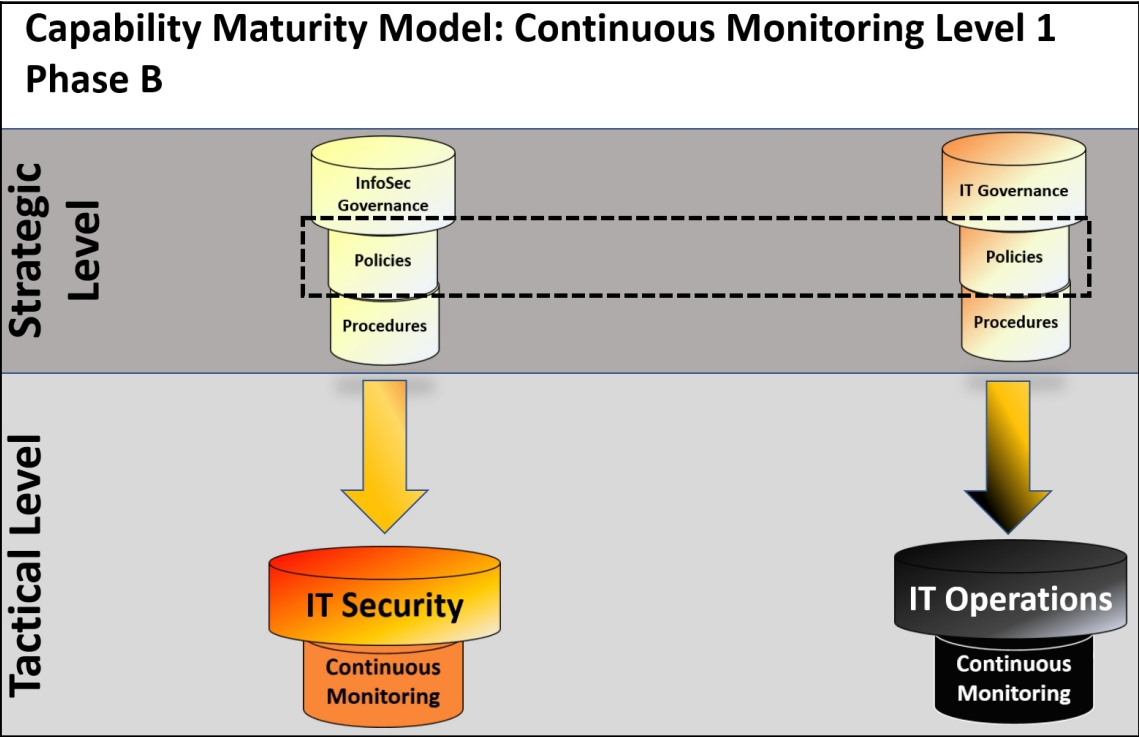


The preceding figure is an example of a siloed organizations or capabilities that have little interaction with one another. There are no checks and balances and neither hand knows what the other is really doing.



# Level 1 – phase B

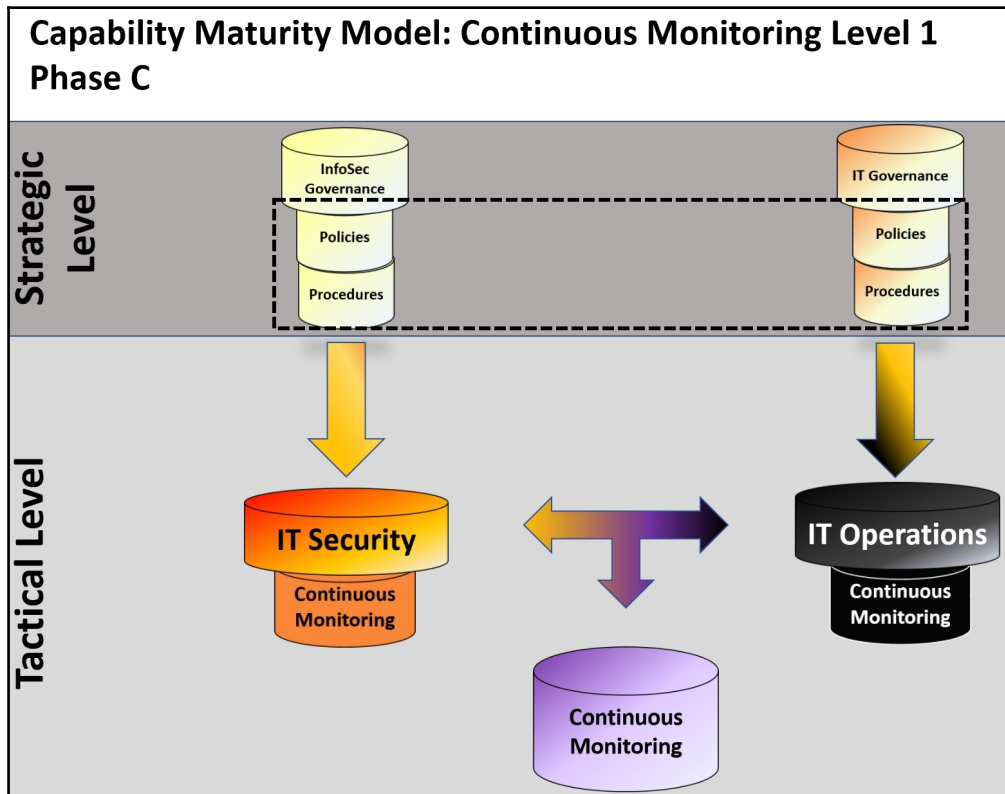
In phase B, we as an organization starting to look at how they can align the policies of the specific item that needs to be monitored. We can use the F3EAD process to target the gaps of information or issues in communication to stakeholders. Once we understand the issues, we can begin developing the policies to put into place that will drive the establishment of OLAs between teams and SLAs between the organization and the service provider.



By establishing the policies for the item to be monitored, it formalizes the collaboration between IT operations and IT security on a specific topic. Now that the *what/why needs to be monitored* has been established, the *how it needs to be monitored*.

## Level 1 – phase C

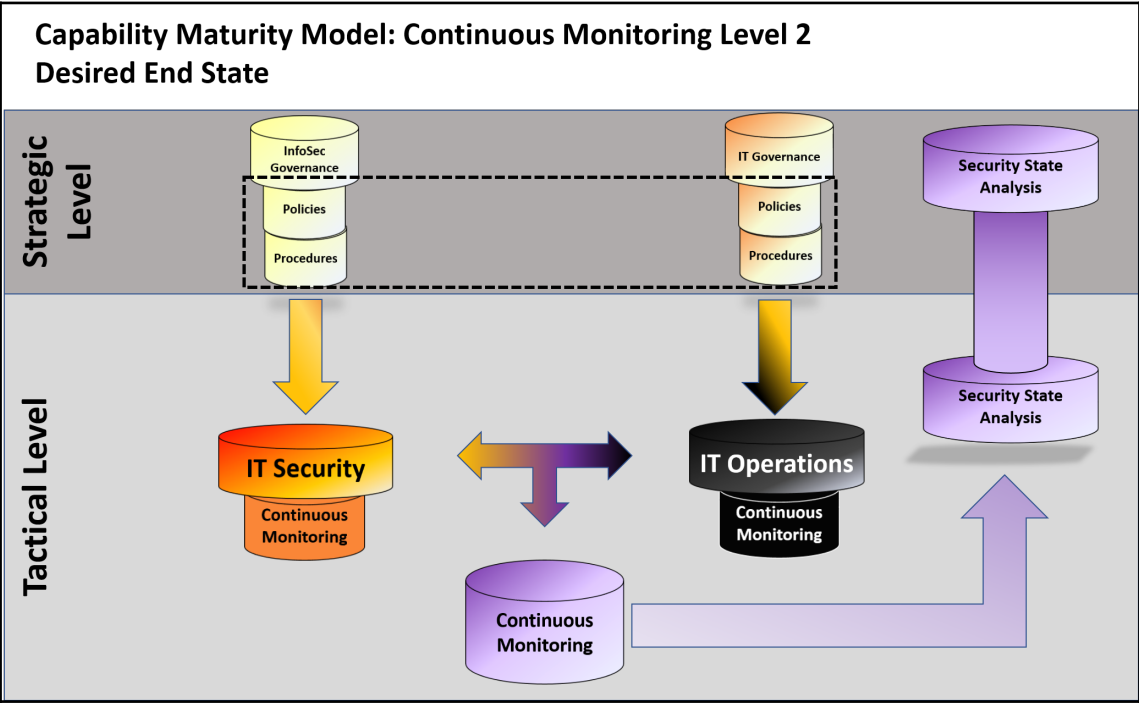
Phase C establishes how we will be communicating and monitoring between entities. With the formalization of policies, the hope is that with the policy development, those procedures were also produced. Either way, if they weren't, that is what phase C is about: finding the issues in the current processes for continuous monitoring on the item and improving them to an 80% solution.



Now that we have a broad overview of what continuous monitoring is, let's start integrating with some capabilities.

# Capability Maturity Model – continuous monitoring level 2

The continuous monitoring capability feeds into the security state analysis through inputs from the continuous monitoring items from both IT security and IT operations. The desired end state of this capability is the solid interaction between the two organizations to monitor items that may impact each other and provide inputs for an overall security analysis. The items that are monitored should be prioritized by PIRs that have been agreed by both organizations and these may turn into policies followed by the procedures to monitor.



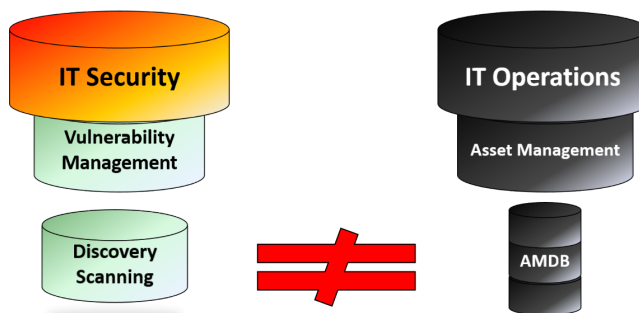
The preceding illustration describes the encompassing concept, but the continuous monitoring capability consists of the multiple interactions between teams within each organization and then the interaction between themselves.

To better explain this concept, I'll use several scenarios and apply a Capability Maturity Model to the item to be monitored. The only assumption for consideration here is that **strategic** policies and procedures have been defined and tactical procedures must be developed.

## Scenario 1 – asset management/vulnerability scanning asset inventory

- **The problem:** A worry for a lot of IT departments is rogue devices also known as *stuff that appears on your network hasn't gone through the onboarding process*. There may be reasons for this, such as poor onboarding procedures, users have excessive privileges, or less than optimal access management policies in place. Whatever the reason is, it is a risk and we need to understand if this is an issue and how we can monitor this over a period of time to get a trend analysis.
- **Baseline:** Asset Management Database serves as master data for systems in the organization.
- **Anomaly:** Systems that are found on the production network that are not in the asset management database.
- **Priority Information Request:** We need to know when more than 10% of the systems discovered from discovery scans on our network are not in our inventory.

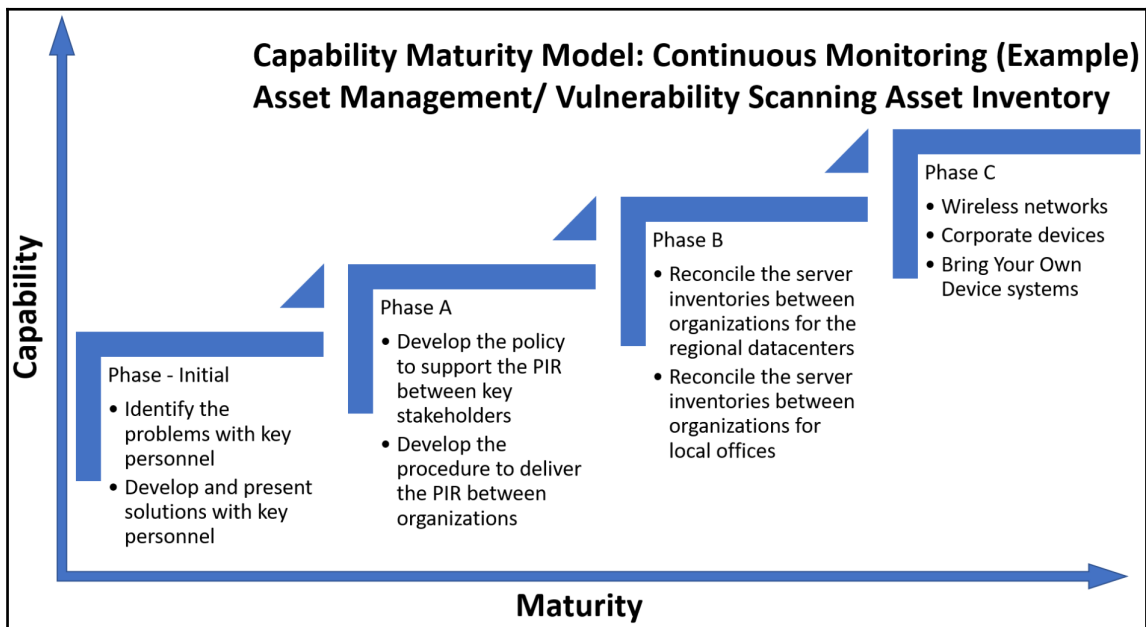
### Capability Maturity Model: Continuous Monitoring Level 2 The Problem



We will have an issue if there is a more than a 10% difference between IT Operations Asset Management Database and systems found during Vulnerability Management Discovery Scanning

- Key stakeholders:
  - Vulnerability Management:

- This capability is responsible for performing discovery scanning to find devices on the subnet they are preparing a vulnerability scan for
- Responsible for ensuring that a vulnerability scanning database is aligned with the information systems inventory
- **Information Systems Administration:** Responsible for keeping track of the information systems inventory
- **Continuous Monitoring:** End to end process of syncing information system asset inventory with vulnerability management systems database:
  - **Key risks:** Uncontrolled systems that exist on the network pose a security risk
- **The targets—overview:**
  - **Phase Initial:** Planning with key personnel
  - **Phase A:**
    - Develop and establish the policy
    - Develop and prepare to implement the procedure
  - **Phase B:** Reconcile the server inventories
  - **Phase C:** Improve system inventories and coverage



## Phase initial

The initial phase is about planning with key personnel.

The goal is to:

- Identify the problems with key personnel
- Develop and present solutions with key personnel

Example steps:

1. Identify the key personnel.
2. With the key personnel:
  - Draw the end to end process from when the system is commissioned and decommissioned in the asset inventory
  - Draw the end to end process from when the system is onboarded and offboarded in the vulnerability management database
  - Define (if any) points and document where these processes intersect:
    - This means, when the system is onboarded in IT ops, when does IT security find out?
    - When IT security finds a system that is not in its database, when do they tell IT ops?
  - Identify and provide solutions to any challenging areas or areas for improvement:
    - How can we ensure that our databases are synced?
    - What KRI do we put in place to know when we have an issue?
    - How can we report to one another if the threshold is met?
    - How do we report to our supervisors when the thresholds is met?

## Information gathering

The main teams to tackle the PIR were the vulnerability management team and the asset management team. Each of the teams had a separate process to track the inventories.

The asset management team's process required that system owners log their systems that they put on the network in a central database and track them through the test, development, and production environments:

- **Item #1:** Process control is not centralized
- **Item #2:** Systems can be put on the network without any accountability of ownership at the local offices

As most commercial scanning tools are subscription-based, the vulnerability management team was responsible for keeping their toolset inventories up to date. This was done with a reconciliation between the toolset database and the asset management team's central database:

- **Item #3:** Discovery scanning is only being done on *production* networks
- **Item #4:** If the central database is not being maintained for *production* networks, the vulnerability scanning team is not providing the most accurate reports

## Developing possible solutions

After reviewing the end-to-end process of both teams, it was determined that a solution would include an example of the following:

1. The central asset database would be considered *master data*
2. Asset management process control will need to be developed and established as an action from the initial findings to satisfy a more accurate PIR
3. Development and testing environments are at a lower risk for exploitation as they are completely segregated from the production network
4. Discovery scanning will continue to only be executed on the production network
5. Systems that are found in production that are not correctly labeled as **production** in the central asset database would be quarantined
6. Systems that are found in production that are not in the central asset database would be kicked off the network

## Phase A

Phase A is about developing the policy and procedures to support the PIR for continuous monitoring:

- 1. The policy should provide the teams the course of action that is required to achieve the PIR
- 2. Procedures should detail how the policy will be met between the teams

### Procedure RASCI (example)

Actions	Information system owner	IT ops—asset management	InfoSec—vulnerability management	Security state analysis
1. Manage asset management database		R/A		
2. Label information system	R	A		
3. Discovery scan network	S	C	R/A	
4. Report discovery scan deviations from asset management database		A	R	I
5. Quarantine/kick from a network	I	R/A		I

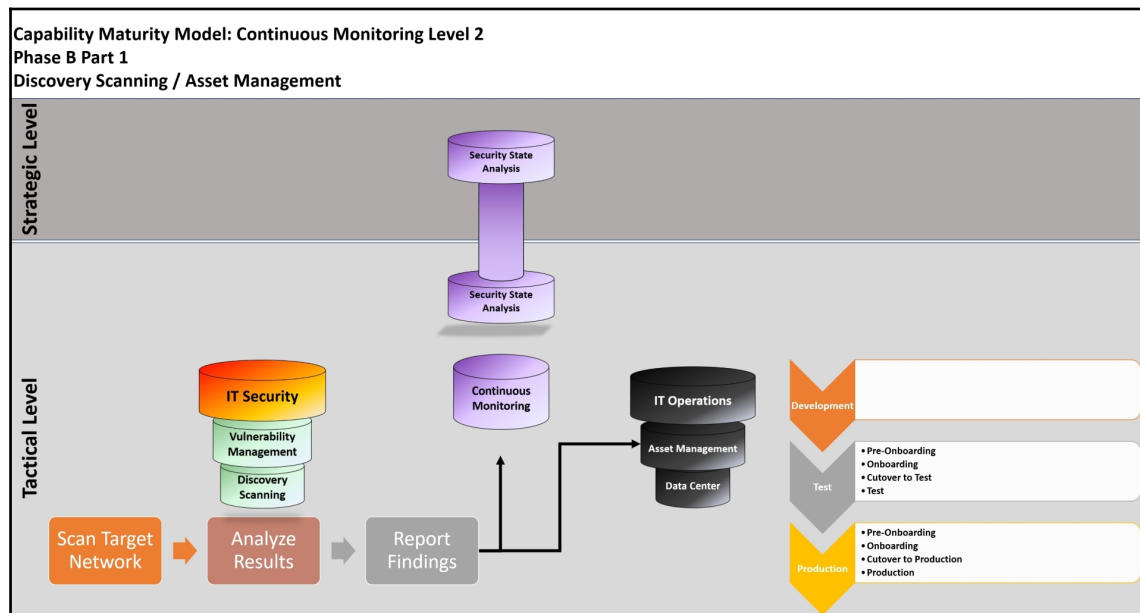
## Phase B

Because the team can't tackle everything at once, phase B was broken into two parts, which are explained in the following sections.



## Regional data centers

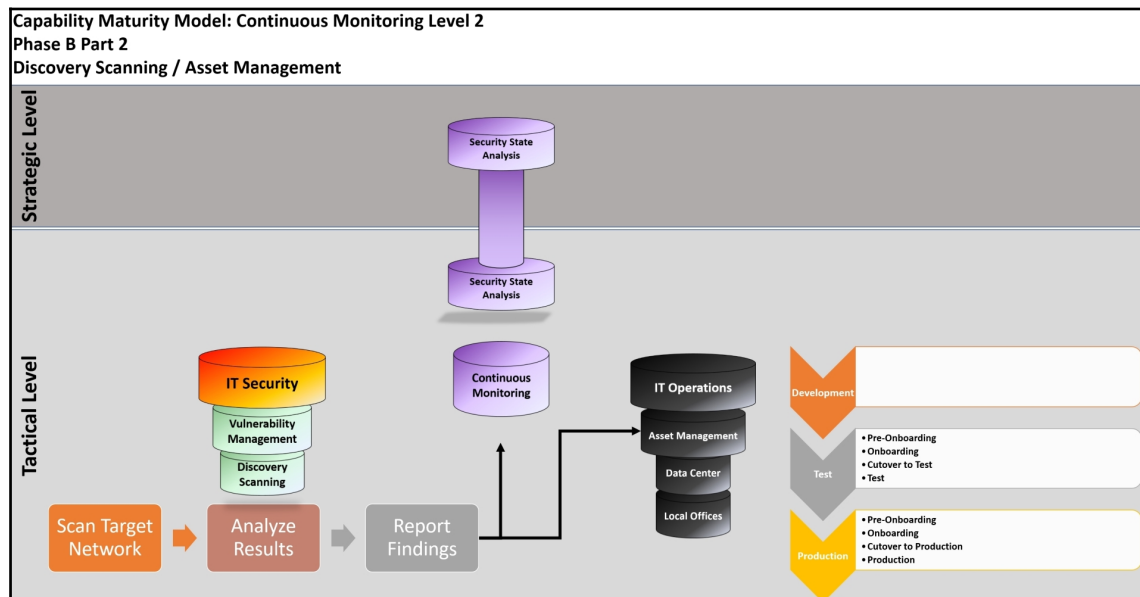
Let's look at how we can plan to incorporate the regional data centers:



- We are focusing on the regional data centers because:
  - These would have the most logical controls in place to put a system on the data center network:
    - Separate development, test, and production environments
    - Pre-onboarding
    - Onboarding
    - Cutover to test or production
  - There is a measure of certainty, we can test and refine the process that we have developed to ensure consistency throughout rollout to the local offices
- Notice that reporting is now feeding into both continuous monitoring for cyber intel purposes as well as IT ops so that they can take on and follow-on actions

## Local office environment

Now that we've looked at the regional data centers, let's go down to the local offices:

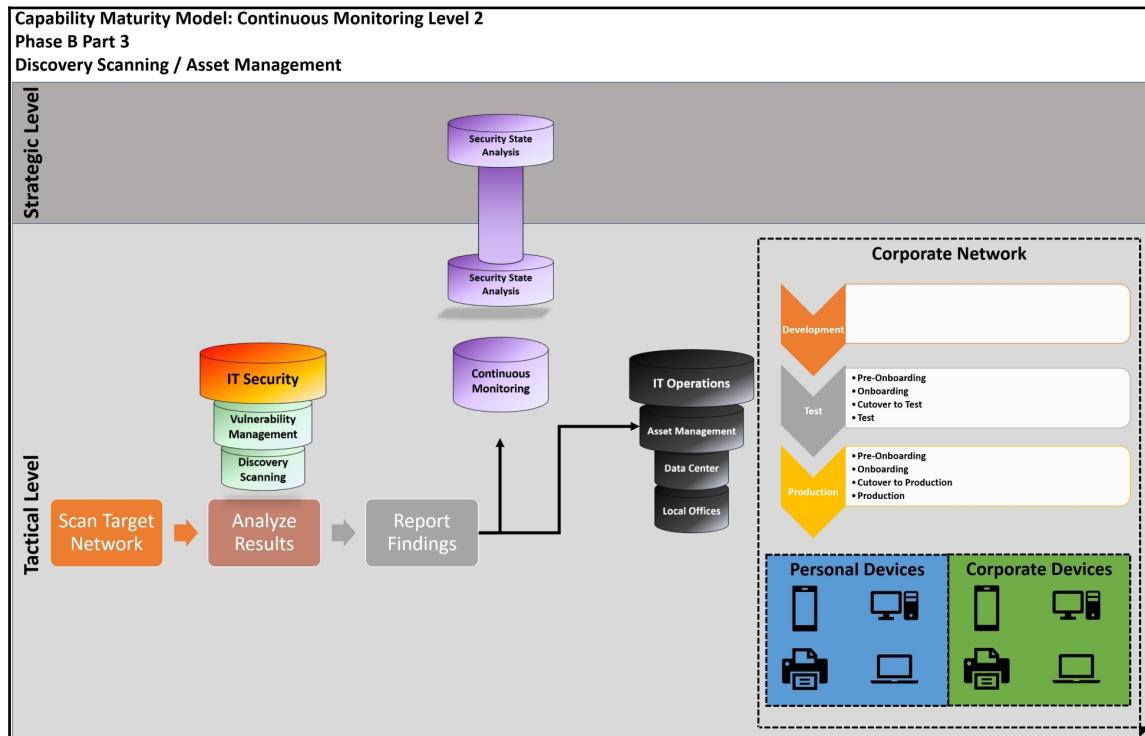


- We are focusing on the local offices, as it was discussed previously, because system owners are able to put systems on the network without much control:
  - There is more risk in doing this action second
  - This would also open up an opportunity to train system owners and establish better processes
- Again, please notice that reporting is now feeding into both continuous monitoring for cyber intel purposes as well as IT ops so that they can take on follow-on actions

## Phase C

Now that we've described the requirements for the servers in the data centers and local offices, we need to ensure that we can cover everything else.

Phase C focuses on BYOD, corporate workstations/laptops, and so on, as it is important to have an inventory of what is owned by the organization, what is not owned by the organization, what is online, and what is offline.

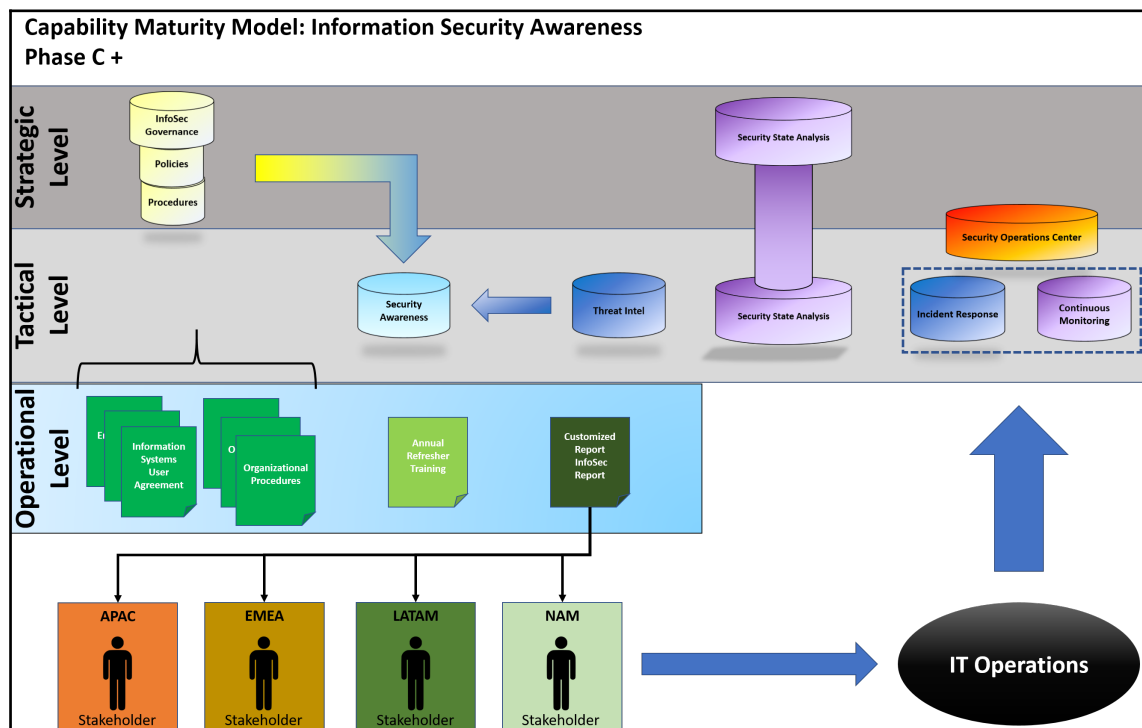


A recommendation would be to look at the lessons learned from phase B for these devices:

1. What is required for a corporate device to access information?
  - Patches up to date
  - Antivirus up to date
  - Properly configured
2. What is required for a personal device to get on the network?
  - Do we have to create a separate network for BYOD?
  - Do we require personal devices to have specific configurations?
    - Password/PIN/Biometrics for phone access
    - Hard drive encryption
3. What constitutes a device being quarantined or kicked off the network?

## Scenario 2 – security awareness/continuous monitoring/IT helpdesk

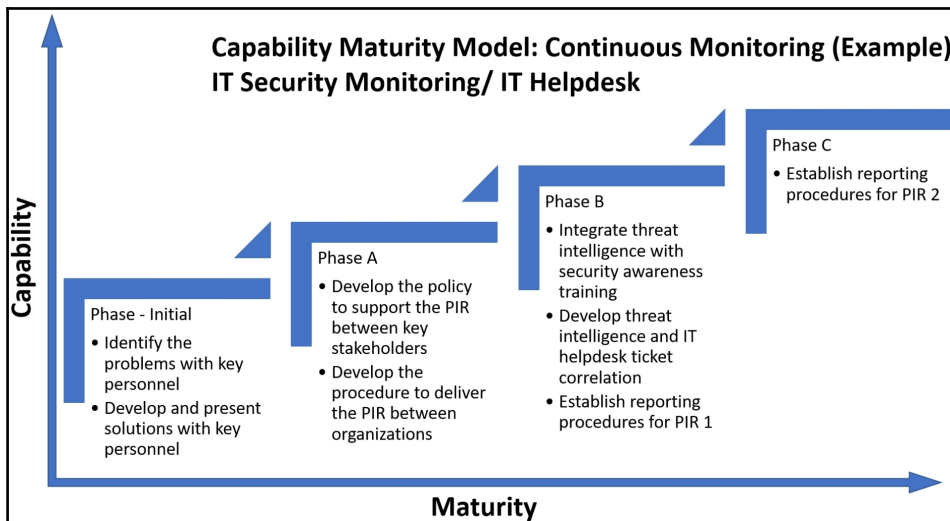
Let's review the Capability Maturity Model diagram for security awareness phase C+:



Understanding that security awareness allows us to use the users to push cyber intelligence to IT operations and IT security, we now need to establish some target PIRs and support the collaboration between teams with policies and procedures:

- **The problem:** There is no way to evaluate if users IT incidents can be related to any specific IT security/threat intelligence incident
- **Baseline:** Between IT help desk and IT security continuous monitoring, there are negligible (less than 25 globally) IT incidents being reported as information security incidents per shift
- **Anomaly:** Between IT help desk and IT security continuous monitoring, there is an increase (more than 25 globally) IT incidents being reported as information security incidents per shift

- **Priority information request 1:** We need to know when threat intelligence correlates to incident tickets reported to IT help desks
- **Priority Information Request 2:** We need to know when any systems are impacted by ransomware—location, time, date, and attack vector
- **The targets—overview:**
  - **Phase initial:** Planning with key personnel
  - **Phase A:**
    - Develop and establish the policy
    - Develop and prepare to implement the procedure
  - **Phase B:**
    - Integrate threat intelligence into security awareness to enable users to identify and report anomalies (PIR 1)
    - Develop threat intelligence and IT help desk correlation monitoring capability for SOC and IT help desk (PIR 1)
    - Establish automated email reporting to key stakeholders for PIR 1
  - **Phase C:** Establish automated reporting to key stakeholders for PIR 2



## Phase initial

Again, the initial phase is about planning with key personnel.

The goal is to:

- Identify the problems with key personnel
- Develop and present solutions with key personnel

Example steps:

1. Identify the key personnel.
2. With the key personnel:
  - Draw the end-to-end process from how threat intelligence is developed
  - Draw the end-to-end process from how an IT help desk incident ticket is created and closed
  - Define (if any) points and document where these processes intersect
  - Identify and provide solutions to any challenging areas or areas for improvement:
    - How can we use and correlate information between our teams?
    - What KRI do we put in place to know when we have an issue?
    - How can we report to one another if the threshold is met?
    - How do we report to our supervisors when the thresholds is met?

## Information gathering

The initial teams identified to tackle these PIRs were the threat intelligence team, the security awareness team, the information security monitoring team, and the IT helpdesk team. We will need to add the IT security incident response team to complete the end-to-end process.

The threat intelligence team was responsible for providing the appropriate information to applicable teams:

- **Item #1:** Threat intelligence is not being provided to IT help desks, resulting in a lack of awareness of a possible incident

The security awareness team is responsible for the training and education of the users:

- **Item #2:** At this point, threat intelligence is developed in relation to the regions for educating the users

The information security monitoring team is responsible for monitoring various baselines for anomalies:

- **Item #3:** There is no cognizance of what users are putting in as incident tickets

The IT help desk team is responsible for creating, working, and closing IT incident tickets:

- **Item #4:** There is no correlation of threat intelligence and IT incident tickets
- **Item #5:** There is no threat intelligence or IOC information being given to the team

## Developing possible solutions

After reviewing the end to end process of all teams, it was determined that a solution would include an example of the following:

- Threat intelligence reports will be customized to complement security awareness initiative and training for users
- Global IT help desks will have fields to fill out their tickets that may *indicate a security issue*:
  - Required fields—location, time, date, potential attack vector
- Tickets that indicate a potential security issue will be monitored by the continuous monitoring team:
  - Continuous monitoring will validate the information against X criteria and move it to the incident response team for action, or mark it as a false positive

## Phase A

Phase A is about developing the policy and procedures to support the PIR for continuous monitoring:

- The policy should provide the teams the course of action that is required to achieve the PIR
- Procedures should detail how the policy will be met between the teams

## Procedure RASCI (example)

Actions	Users	IT security monitoring	IT help desk	Security awareness	Security state analysis	IT security incident response
Provide customized threat intelligence reports	I	I	I	R/A	S/C	
Inform on potential IT Security events/incidents to IT help desk	R	C	A			
Review initial reports of potential IT security incidents		R/A	C	I		
Inform IT security—incident response	I	R/A	S	S	I	
Inform PIR stakeholders		R/A	S	S	I	I
Inform users of major incidents		S	S	R/A		
Perform incident response process	C	C	C	S	I	R/A

## Phase B and C – sample questions

Phase B is now breaking down the overall procedure into implementation. Using the RASCI matrix, we understand who is doing what, but now we need to know how we are going to do that. We need to set the base for this cyber intelligence capability between the services. I've added a few preliminary questions to answer that can later be used as targets to clear the first iteration of phase B.

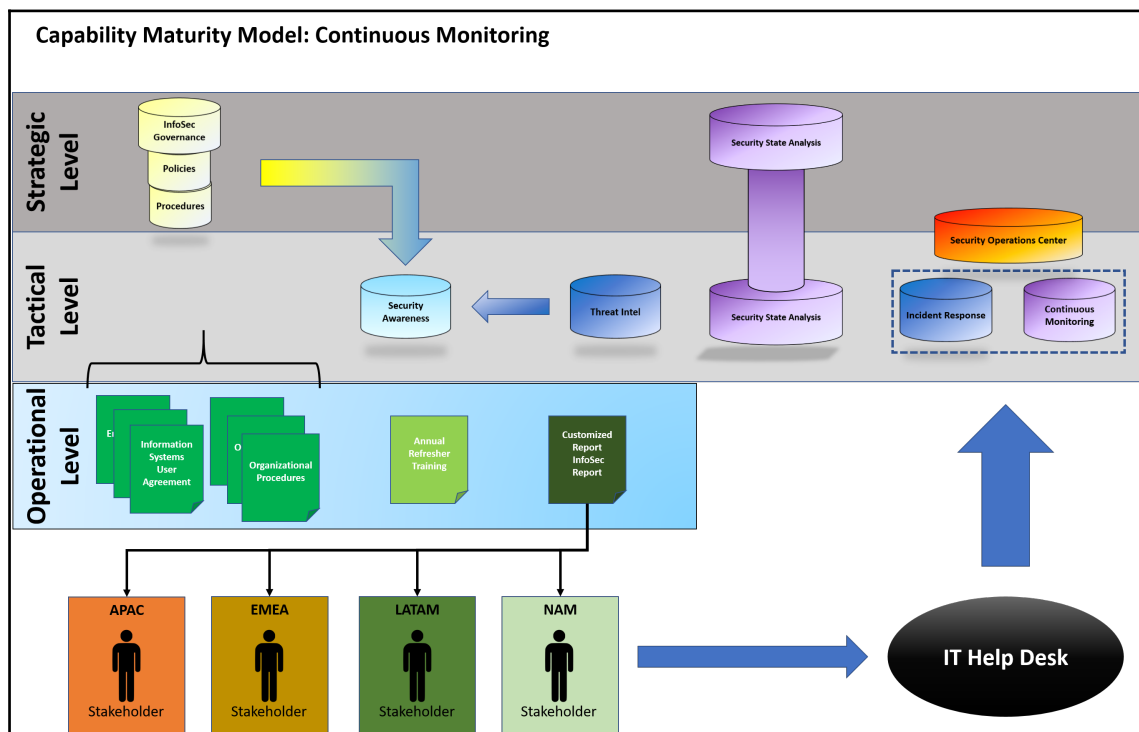
Where do we roll this out first?

- **Security awareness:**
  - Who are the stakeholders?
  - What information do you put in the security awareness communications that will call users to action?
  - How and when do we communicate an incident or event?
- **IT help desk:**
  - How do we add customized fields to indicate a potential security incident?
  - How do we communicate this to IT security-continuous monitoring?



- **Continuous monitoring:**

- How do we incorporate IT help desk tickets that are assigned to us for action?
- What are we defining as an incident or event?



The ultimate goal here is to be able to gather information and have it distributed across the applicable teams and stakeholders.

Once these lines of communication have been established, we can move on to phase C. This phase is about passing the specific information that is required to make a decision.

## Just another day part 2

1230—Eastern Standard Time. Location: Chesty Lewis Puller Security Operations Center-Centralia, Virginia.

"Hey Charles" Justin said, "...look at this"

Charles, the SOC manager, walked over and started looking at the monitors. *"Looks like there are a lot of tickets being put in around APAC for an email."*

*"Yeah, but now look at this"* Justin pointed to the security dashboard. *"These emails are corresponding with an event that had been reported in our threat intelligence feed."*



#### **Priority information request**

We need to know when threat intelligence correlates to incident tickets reported to IT help desks.

*"Damn. How many tickets have been turned in already?"*

*"About 50 from various places. India, Malaysia, Australia, and Japan"* Justin stated, *"...but we have another issue."*

*"Ok. How many systems were impacted?"* asked Charles



#### **Priority information request**

We need to know when any systems are impacted by ransomware—location, time, date, and attack vector.

*"Right now, it's two. Japan and India. The systems were immediately quarantined and the country IT help desk personnel already pulled them off the network."*

*"What's the name of the security folks down there so we can get a call together as soon as possible?"*

*"Tatsuya from Japan and Sandeep from India. They've already been informed to call in at 1300"* Justin stated, *"I've got the APAC incident response team getting together now and have been briefing them while I contact them."*

*"Also..."* a voice came from across the room *"...the CIO and CISO know from the automated email that was sent out."* Wendy was on the security awareness team who ensured that people got the information they needed. *"I've already talked to Gosia in Poland. She's all over it for APAC. She's just standing by for the go-ahead to send an email out to the users. The draft is right here."* she hands off a copy to Charles and to Justin.

*Got it. Charles takes a few seconds to go of the paper, "Please go ahead and tell her to send it off. I'll brief the bosses so they know what's been done already. If there isn't anything else, I'll see everyone in the call at 1300."*

*To be continued...*

## Summary

In this chapter, we had a taste of how we can improve continuous monitoring for the organization by establishing cyber intelligence communication channels. There are multiple services that can interact with each other to pass relevant information and we've gone through only a few.

So to review, we've discussed the following:

- The challenge of continuous monitoring
- Continuous monitoring Capability Maturity Model
- Examples of the integration of capabilities for continuous monitoring to improve defense

Where else can we improve continuous monitoring?

# 11

## Putting Out the Fires

In the past few chapters, we've discussed how continuous monitoring, security awareness, and threat intel can create cyber intelligence communication channels between each other. By understanding the external incidents and events around us, we can train our users to inform IT operations (help desk) of any anomalies in the normal day-to-day operations. This chapter is all about handling anomalies with respect to baselines by empowering the incident response capability in our organizations.

We will review:

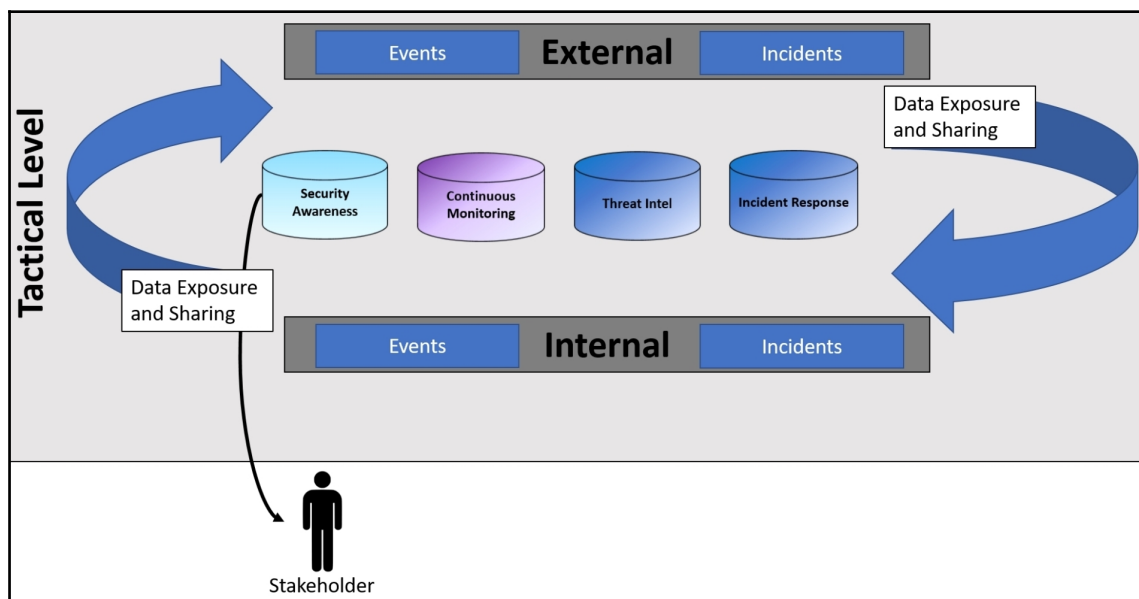
- Incident response processes:
  - Preparation
  - Detection and analysis
  - Containment, eradication, and recovery
  - Post-incident activity
- Integration of F3EAD and incident response processes
- Integration of F3EAD, incident response, and intelligence cycle processes
- Example incident response Capability Maturity Model

### Quick review

The following diagram is a recap of what has been discussed so far:

- If we train our users to look for deviations from normal information system behaviors or suspicious activity, then hopefully, we will have improved defenses where everyone is doing their part to protect the organization

- There is a need for threat intelligence to be customized for teams so that capabilities such as continuous monitoring and the help desk can be cognizant of the threats that may impact the organization



Now, we need to understand how incident response fits into all of this.

## Overview – incident response

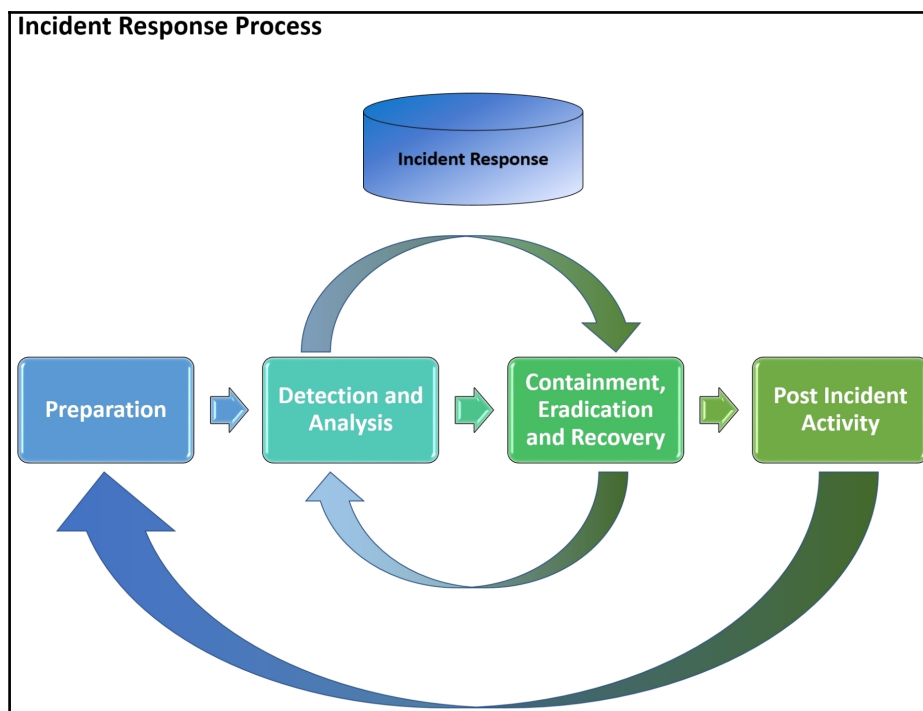
The members of an incident response team are like the superheroes in comics. Whenever there is an issue, they are there to *save the day* for the organization. By creating and establishing cyber intelligence communication channels, we can help the incident response team members to *save the day better*.

To understand how we can do that, let's look at the incident response process.

The incident response process has four main steps, as depicted here:

1. Preparation
2. Detection and analysis
3. Containment, eradication, and recovery

## 4. Post-incident activity



Notice how steps 3 and 4 are cyclical.

Let's go through a brief overview of each step.



A good reference guide for incident response is NIST 800-61 *Computer Security Incident Handling Guide*:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

## Preparation and prevention

The first phase of incident response is preparation and prevention.

Some of the main activities in this phase include:

- Key personnel identification
- Development of policies and procedures:
  - Scenario playbooks
  - RASCI matrices
- Security awareness

## Detection and analysis

The second phase of the incident response process includes two steps: detection and analysis. There are multiple ways that we can detect an incident or event, such as through log analysis, network traffic monitoring, or other security tools. Continuous monitoring on the different attack vectors with various tools provides information for the incident response team members to analyze data for the appropriate actions on incidents and events.

## Containment, eradication, and recovery

The proper steps need to be taken to handle the situation once an incident or event has been validated:

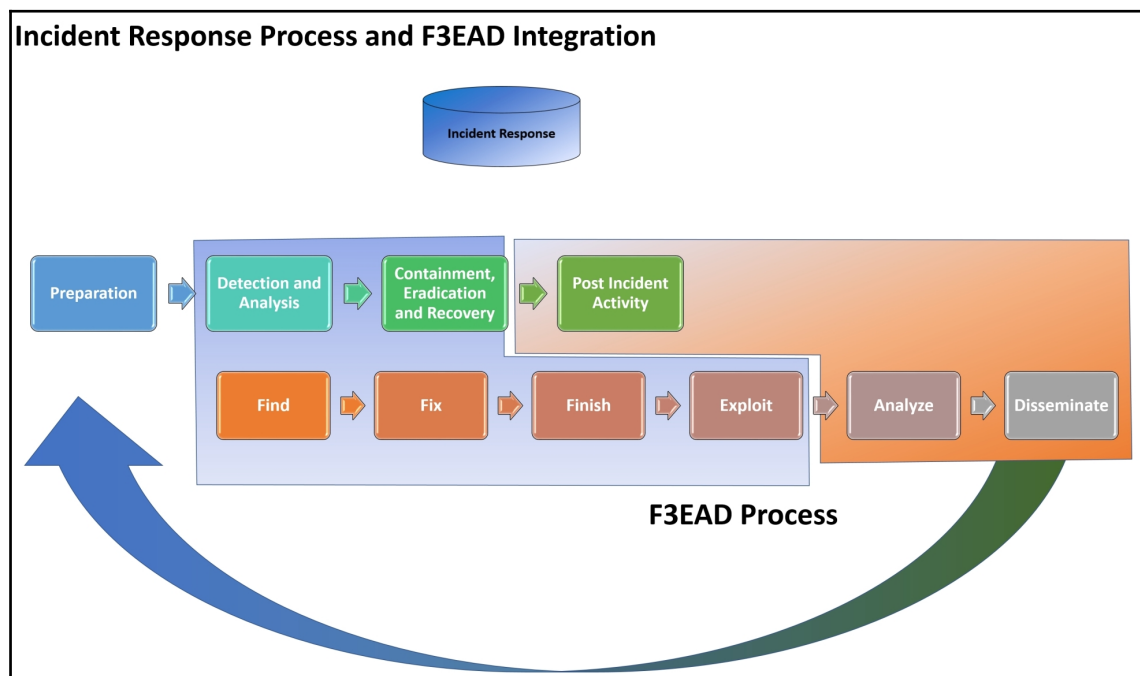
- **Containment:** The actions required to prevent the incident or event from spreading across the network
- **Eradication:** The actions that are required to completely wipe the threat from the network or system
- **Recovery:** The actions required to bring back the network or system to its former functionality and use

## Post-incident activity

Similar to lessons learned, it is the most important part of all of the phases. If done correctly, it will provide the information required for the organization to learn from the gap in controls or the failed process. This is important in that actions can be taken at all levels to reduce the impact to the organization.

## Incident response process and F3EAD integration

Now that we understand the basic concept of the phases in incident response, let's see how we can integrate these phases to enable cyber intelligence in the organization through reviewing the following diagram:

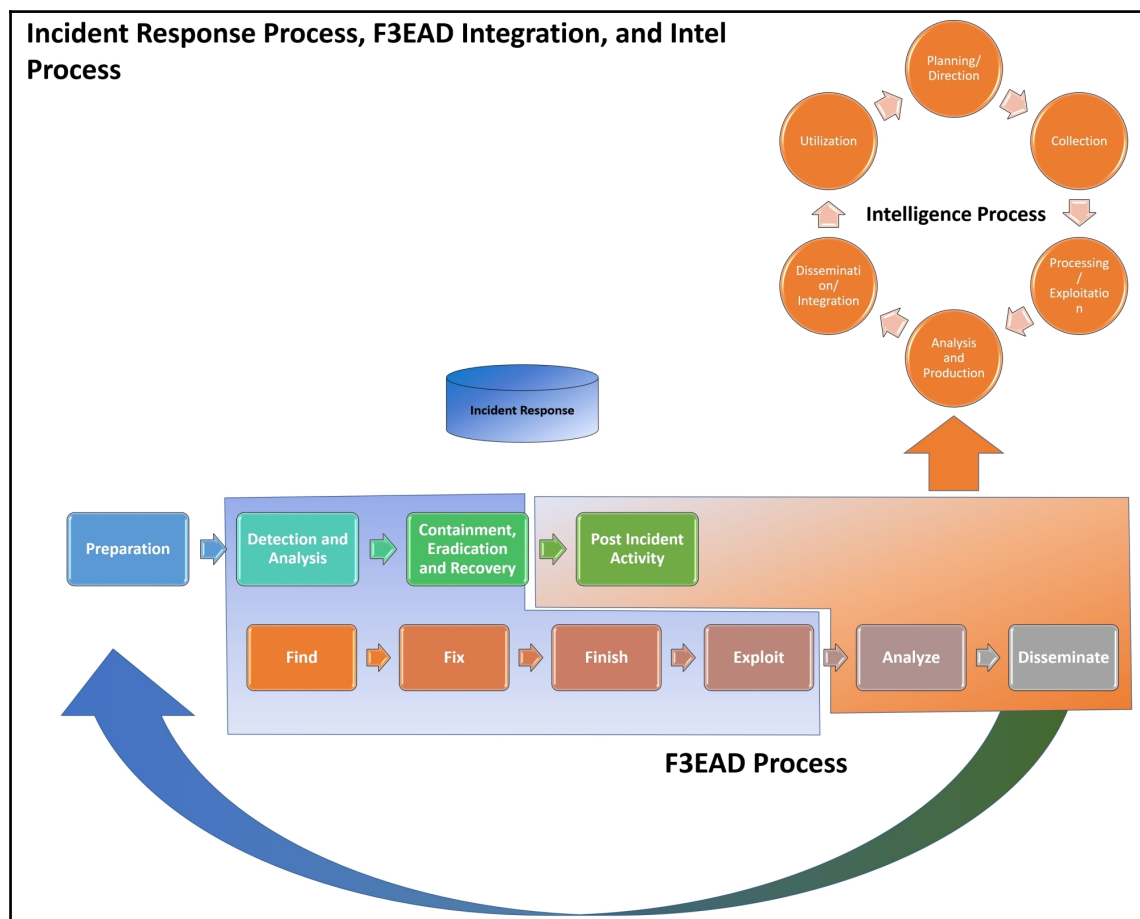


The **Preparation** phase of **Incident Response** is a culmination of policies, procedures, training, and so on that can be mapped to different capabilities within the organization through the use of RASCI matrices. We would see the execution of the processes that are identified in these matrices in the **Detection and Analysis** and **Containment, Eradication, and Recovery** phases of the **Incident Response** process. These two phases are mapped to the **Find, Fix, Finish, and Exploit** steps of the F3EAD process and would be applicable to detecting anomalies to baselines, boxing in threats, removing them, and putting the systems back online. All of the **Post Incident Activity** maps to **Analyze** and **Disseminate**, as this information will be used to improve the organization's ability to prepare for a similar incident in the future.



## Intelligence process tie-in

Just as the incident response process integrates into F3EAD, the following is an example of how it can fit in with the formal intelligence process:

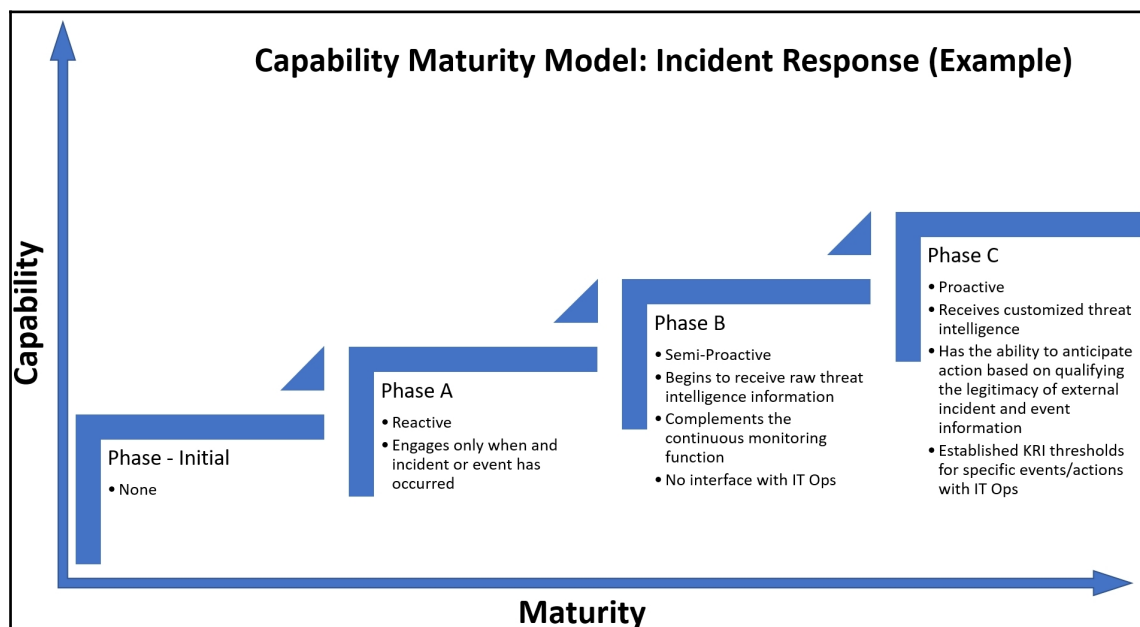


As information would have to be collected and analyzed at different levels, strategic PIRs for Incident Response should be developed to include measurements or thresholds that would have to be met to be considered an event or incident. These will allow the right people to be *activated* or informed at the correct time.

The point here is that by utilizing the F3EAD process within the known incident response process, we can enable the collection, analysis, utilization, and dissemination functions of the intelligence process for better decision making.

# Capability Maturity Model – incident response

The following is an example of a Capability Maturity Model for incident response:



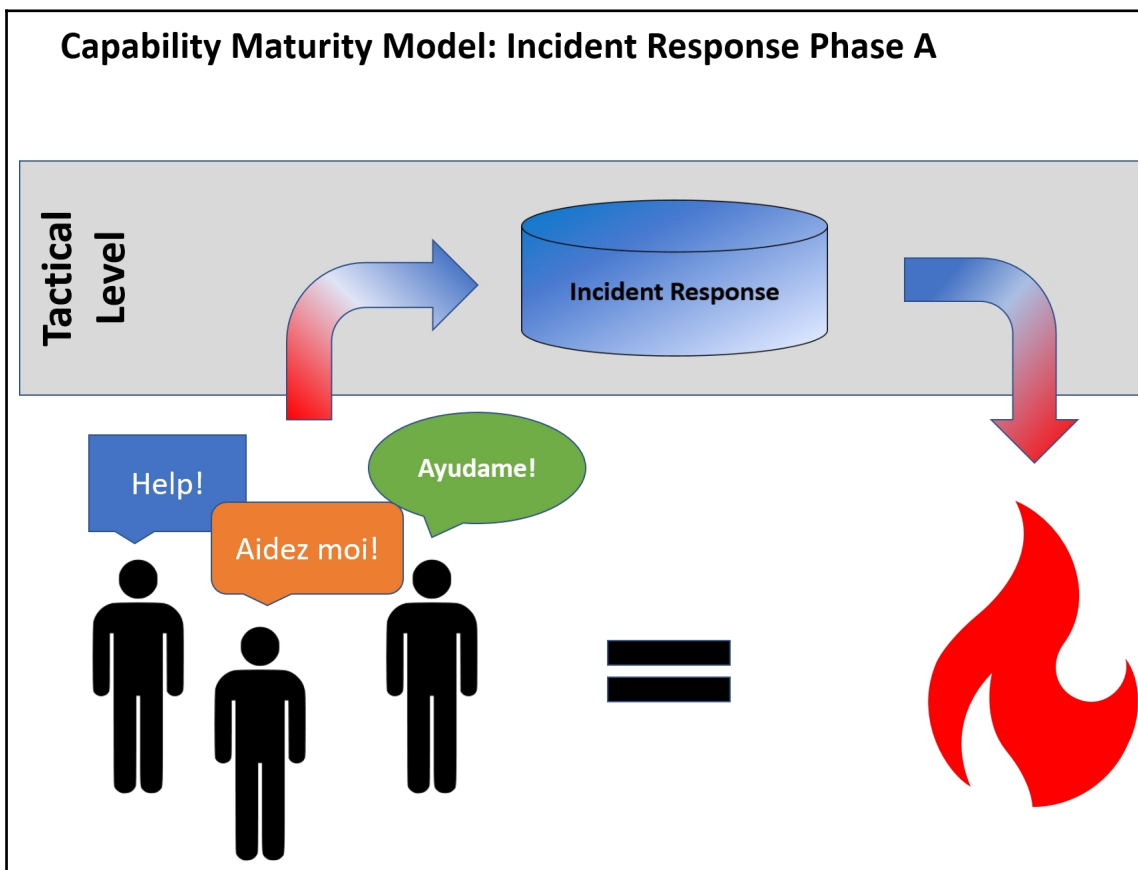
We will go through each step and understand how we can start the process of establishing the communication channels between entities.

## Initial phase

In the initial phase, we have absolutely no capability of handling incidents. This means, there is no help desk or assigned personnel to manage or investigate potential incidents or events. In other words, if there was a fire, no one would know where to report it, and the personnel that would be able to handle this wouldn't know about it.

## Phase A

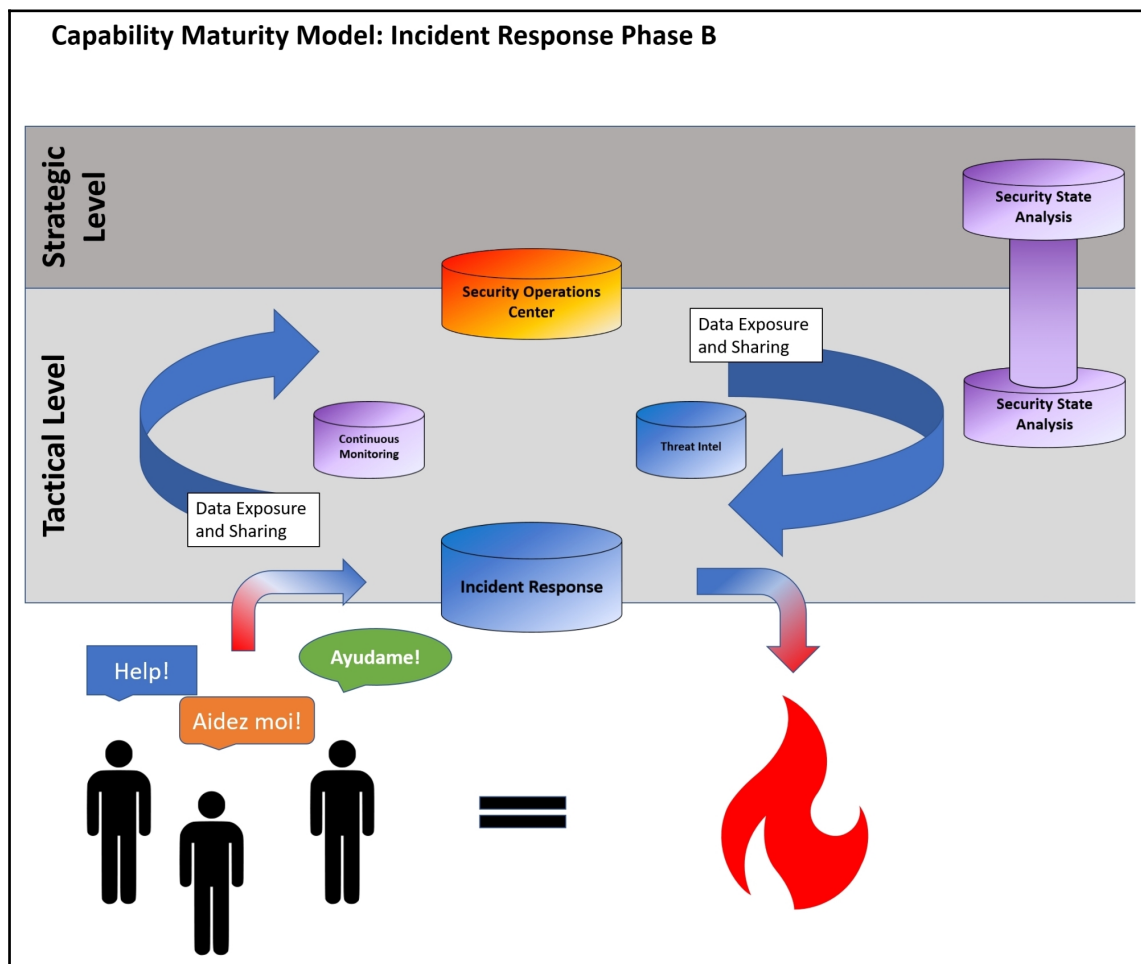
In phase A of this model, we start to see that our users have the capability of requesting for support. During this phase, the incident response team is reactive and responds as they go. It is basic firefighting that this team does on a daily basis, hoping that systems and applications don't break during patching, troubleshooting, or reconfiguration.



We start seeing major improvements as we move into phase B, where we begin to incorporate threat intelligence.

## Phase B

The inclusion of threat intelligence and continuous monitoring capabilities in phase B allows the incident response capability to become more flexible in addressing issues. With SOC oversight, incident response personnel can start to tackle the *bigger* fires and address the *smaller* ones at a later time.



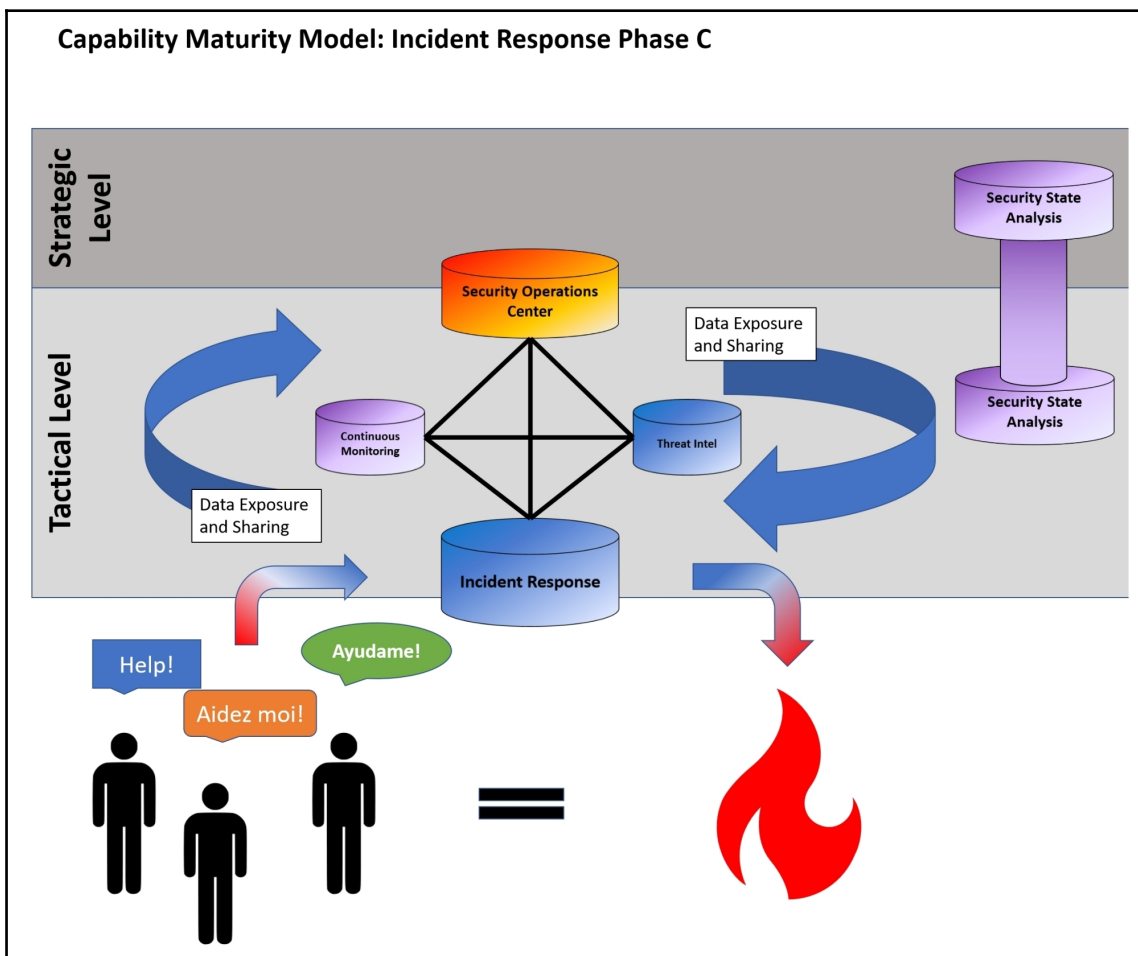
There is a minor integration of *data exposure and sharing* between incident response, threat intel, continuous monitoring, and the SOC. However small, this small integration of capabilities allows the information to flow between the tactical and strategic levels of the organization through the security state analysis channels.

## Phase C

Phase C is the desired state that I think can be another way we fight the fires within the organization, as well as prepare our home with *fire extinguishers* and other countermeasures prior to fires starting in the first place. In the final phase of this Capability Maturity Model, we see a full integration of information between capabilities:

- **Proactive:** Users are aware of threats that may impact the organization and report them through IT ops
- **Receives customized threat intelligence:** The incident response capability receives customized threat intelligence
- **Has the ability to anticipate action based on verifying the legitimacy of external incident and event information:** Threat intelligence information is analyzed in conjunction with continuous monitoring for evaluation against normal baselines
- **Established KRI thresholds for specific events/actions with IT ops:** KRIs are developed, defining incidents and events

RASCI matrices are developed for threat scenarios in the IR playbook:



## Summary

Incident response varies from team to team and organization to organization. Some organizations have a dedicated team for responding to security incidents, but many have these activities built into their daily activities. For better or for worse, we can acknowledge that we can improve our ability to be proactive to incidents, as well as preventing incidents if we have the capability to collaborate and communicate effectively.

In this chapter, we reviewed:

- Incident response processes:
  - Preparation
  - Detection and analysis
  - Containment, eradication, and recovery
  - Post-incident activity
- Integration of F3EAD and incident response processes
- Integration of F3EAD, incident response, and intelligence cycle processes
- Example incident response Capability Maturity Model

# 12

## Vulnerability Management

Vulnerability management is the capability of an organization to effectively identify, report, and reduce weaknesses in the organization. In this chapter, we will be discussing how vulnerability management information provides meaningful information to stakeholders.

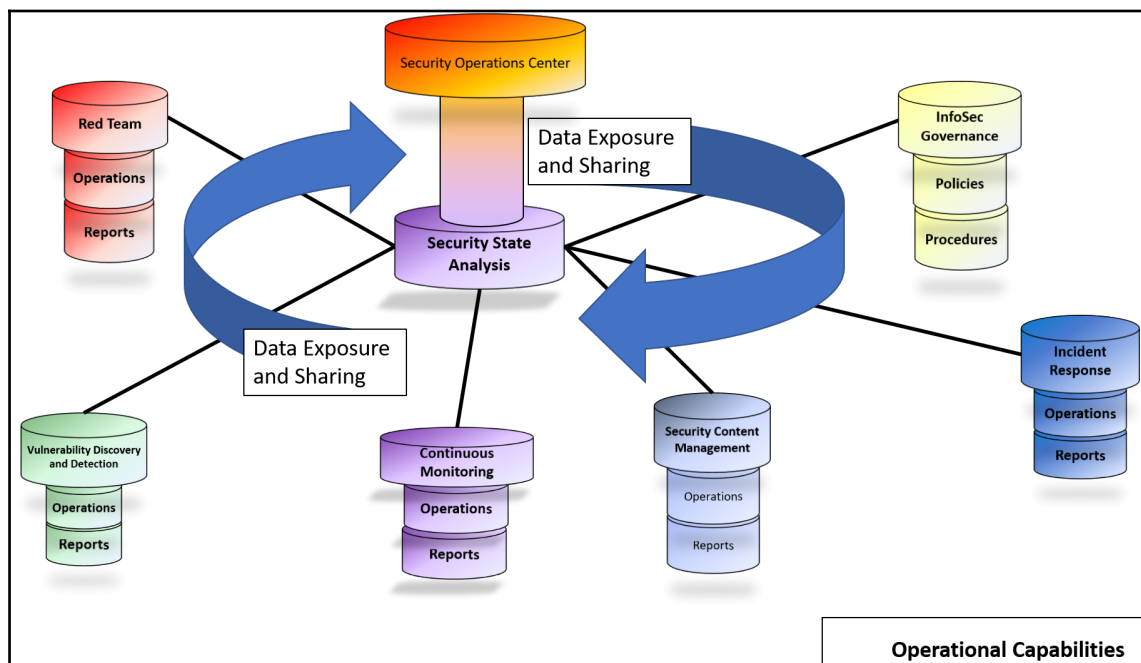
In this chapter, we will cover the following topics:

- Overview of vulnerability management capabilities
- Common vulnerability scoring system
- Capability Maturity Model: vulnerability management – scanning
- Capability Maturity Model: vulnerability management – reporting
- Capability Maturity Model: vulnerability management – fix

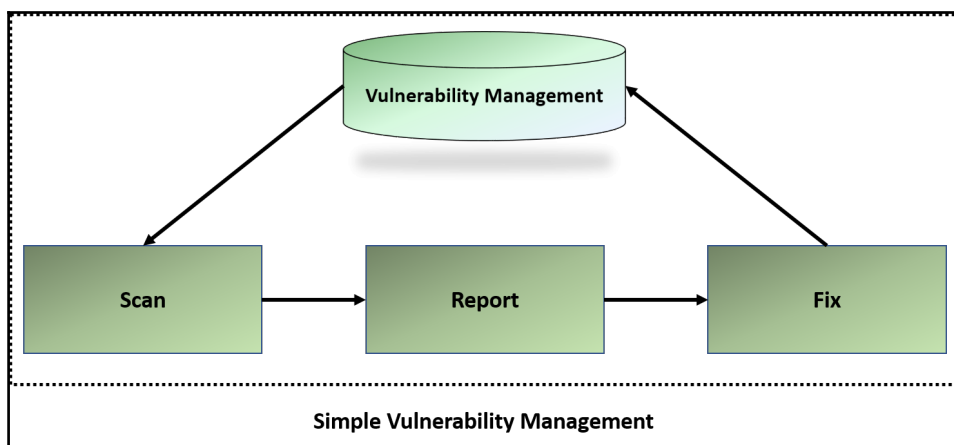


## A quick recap

Vulnerability management is an arm of our security spider that has its own set of processes and procedures:



Vulnerability management provides the capability to find the issues that already exist on our network by scanning against systems and reconciling findings from a vulnerability database. A basic process of understanding this is depicted in the following simple vulnerability management process:



Vulnerability databases are repositories of information about vulnerabilities that have been identified in systems and in software. They are classified by a **Common Vulnerabilities and Exposure (CVE)** identification that has a number, a brief description, and a public source, which is where it came from. The ratings for each vulnerability are dependent on what tool or database is doing the adjudication. However, the majority of tools start with a **Common Vulnerability Scoring System (CVSS)**, since it is an open source application of understanding and communicates the impacts of vulnerabilities that exist in an environment.

## The Common Vulnerability Scoring System calculator

Not all vulnerabilities are equal to each other, and so each vulnerability is placed in a category of risk adjudicated by the CVSS calculator.

There are three metric groups that make up the CVSS, which we will be studying in detail in the following topics.

### Base metric group

These are the main characteristics of the vulnerability, which are consistent over time, and the environment that the systems reside on. These are typically assigned by vulnerability bulletin analysts, security product vendors, or application vendors.

The base metric group consists of six sections, which are as follows:

- **Access Vector (AV):** Determines how the vulnerability is exploited:
  - Local
  - Adjacent network
  - Network
- **Access Complexity (AC):** Measures the types/difficulty of actions required to exploit the vulnerability:
  - High
  - Medium
  - Low
- **Authentication (Au):** Measures the number of times that an adversary must authenticate a system/network so that they can exploit a vulnerability:
  - Multiple
  - Single
  - None
- **Confidentiality Impact (C):** Determines the level of impact to the confidentiality of the system once the vulnerability has been exploited:
  - None
  - Partial
  - Complete
- **Integrity Impact (I):** Determines the level of impact to the integrity of the system once the vulnerability has been exploited:
  - None
  - Partial
  - Complete
- **Availability Impact (A):** Determines the level of impact to the availability of the system once the vulnerability has been exploited:
  - None
  - Partial
  - Complete

## Temporal metric group

These are the characteristics of the vulnerability that can change over a period of time, but do not change in the environment the systems reside in. These are typically assigned by vulnerability bulletin analysts, security product vendors, or application vendors.

The temporal metric group consists of three sections, which are as follows:

- **Exploitability:** Determines and measures the level of difficulty to exploit the vulnerability
- **Remediation level:** Determines the level that the vulnerability may be remediated:
  - Official fix
  - Temporary fix
  - Workaround
  - Unavailable
  - Not defined
- **Report confidence:** Measures the credibility of the source where the vulnerability was reported:
  - Unconfirmed
  - Uncorroborated
  - Confirmed
  - Not defined

## Environmental metric group

These are the characteristics that are specific to the environment. These are typically assigned by the **organization**.

The environmental metric group consists of three sections, which are as follows:

- **Collateral damage potential (CDP):**
  - None
  - Low
  - Low-medium
  - Medium-high
  - High
  - Not defined

- **Target distribution (TD):**
  - None
  - Low
  - Medium
  - High
  - Not defined
- **Security requirements (CR, IR, AR):**
  - Low
  - Medium
  - High
  - Not defined

## CVSS base scoring

A qualitative ranking of severity for vulnerabilities was developed and established by the NIST—National Vulnerability Database— in two versions:

### CVSS v2.0 ratings:

Severity	Base score range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

### CVSS v3.0 ratings:

Severity	Base score range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

NVD does not account for temporal or environmental vectors as they change from organization to organization. However, you can use their calculators to help you find these numbers out:

- **Common Vulnerability Scoring System Calculator Version 2:** <https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator>
- **Common Vulnerability Scoring System Calculator Version 3:** <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

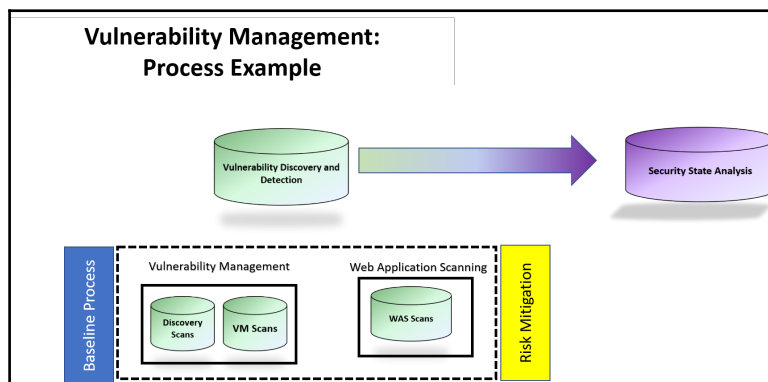
## Metrics madness

The previous section really just shows us how complex it is to gauge a singular vulnerability's impact on your environment. Trying to apply the environmental equation to an organization would be a huge, dynamic undertaking. It would literally be madness to try and do that, although the unfortunate person that is tasked with that job probably has that position for the rest of their lives. It will never end.

Now that you know how each vulnerability is scored, you can understand how they are labeled high, medium, and low.

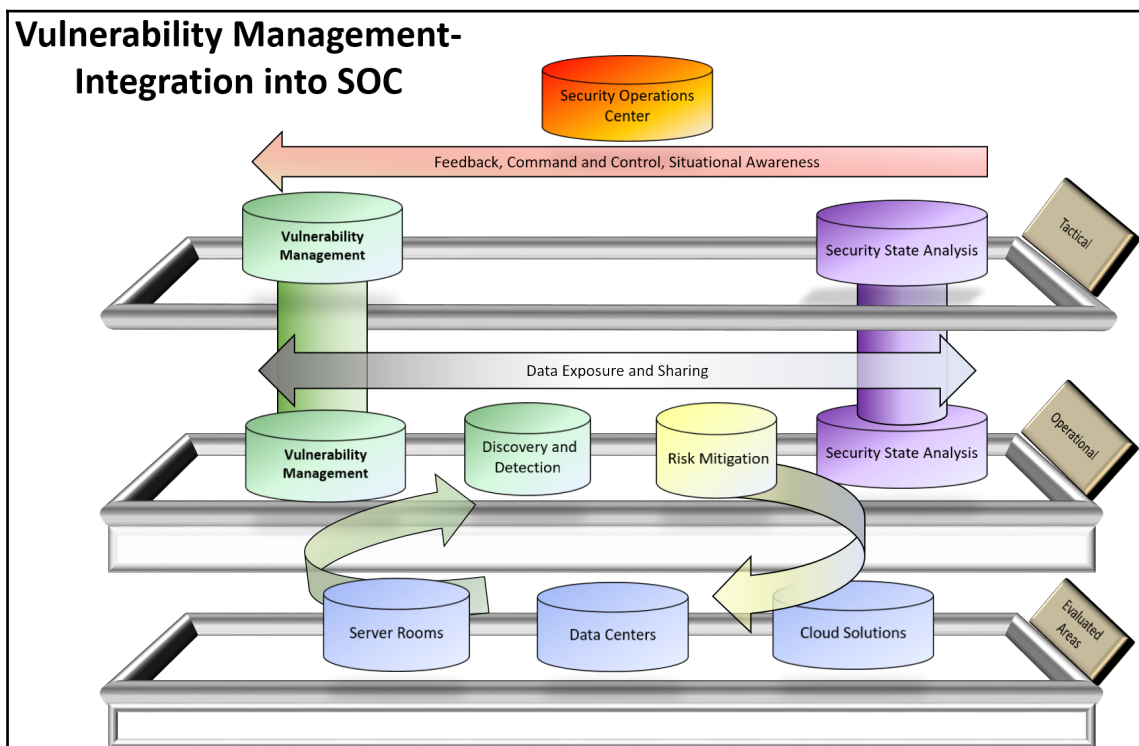
## Vulnerability management overview

As previously discussed, the VM is just a part of the overall security capability, and so we should start looking at the capability as a process from end to end. Let's review the following diagram:



We want the VM processes and results from all scanning activities to flow into security state analysis so that all stakeholders have relevant information from this capability.

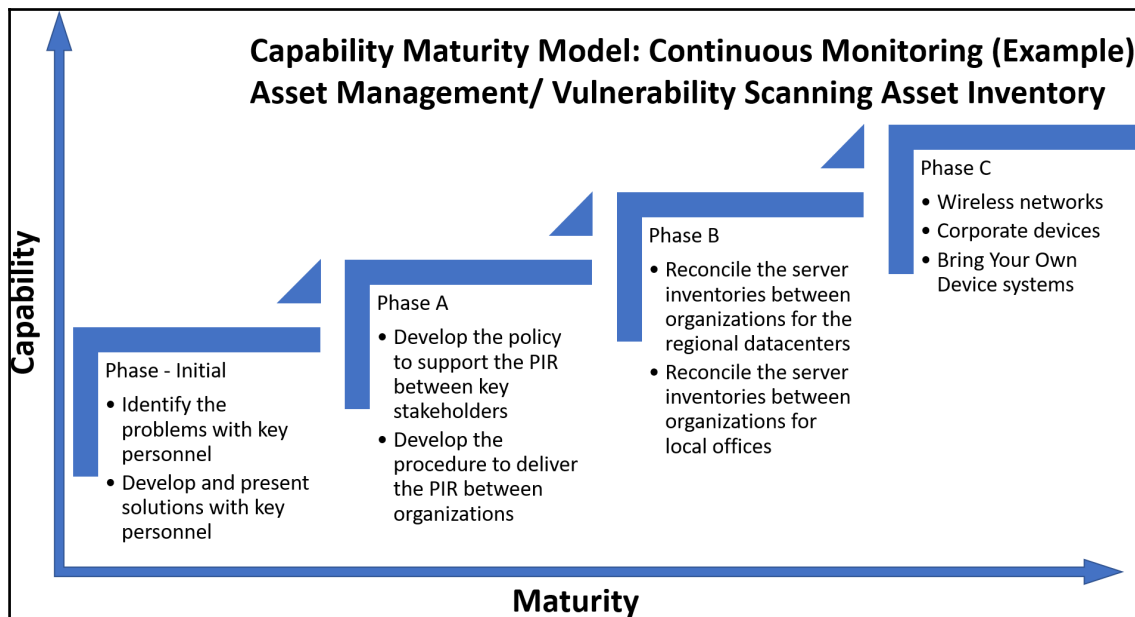
The following is how VM integrates with the SOC at the Tactical Level. This is important as the SOC can provide additional feedback, command and control, and situational awareness to the VM team:



Again, this seems simple, but we need have the mindset of, *if we are scanning and trying to fix everything, in the long run, we are not fixing anything*. We need to apply the same logic of placing our resources where they will make the most impact and improve as we go.

For VM, we have a dependency that we discussed in an earlier chapter. That dependency is to have a complete list of systems and applications to be scanned.

For review, the following is the Capability Maturity Model—continuous monitoring—VM and asset management:



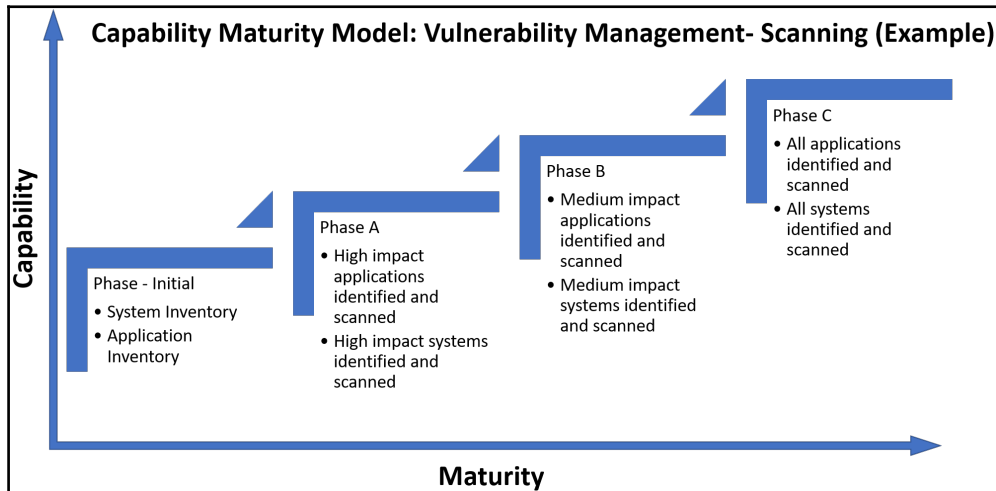
As a minimum, we will need to have completed the initial phase and phase A to begin on our next adventure of building the VM capability of **scanning** and **remediation**.

## Capability Maturity Model: vulnerability management – scanning

We need to start asking the question of what high, medium, and low value applications and systems are. For a small business, this may be quite simple, but as we start looking at multiple businesses and their needs, we can start to see that one business may say that *all* of their applications and systems are critical while another may not even try to participate in the discovery event.



The IT leadership needs to determine what constitutes a high, medium, or low impact system so that this definition is standard across the board. The hope is while an organization is reconciling their asset databases with vulnerability management, that there is some cross work in determining the value of the system. The following is an example of an overarching Capability Maturity Model for the scanning function of vulnerability management:

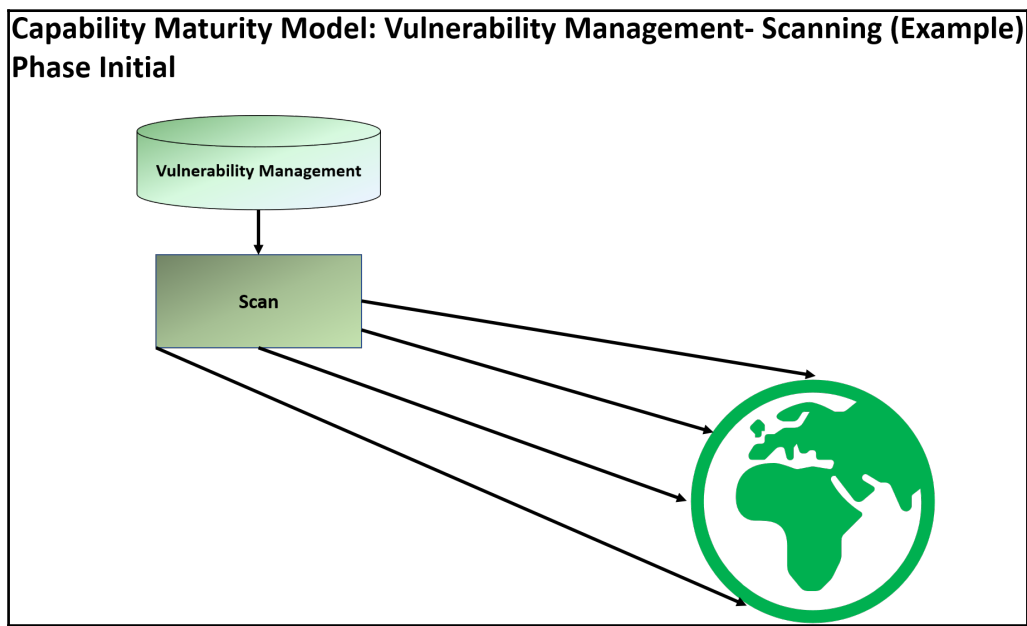


Let's talk about each phase in a little more depth.

## Initial phase

We have all have been there. You have your tool, you have your scanning credentials, you have your inventory, and you have your subnet. That is the extent of vulnerability scanning. You are scanning everything—pretty much the world.

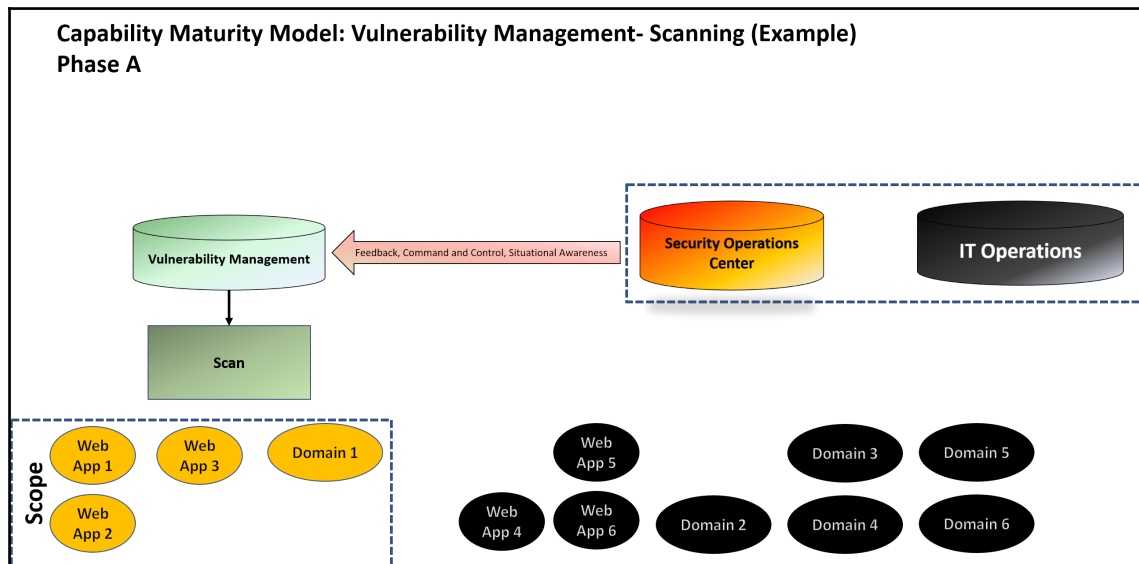
There is hardly any guidance on how to scan or when to scan. It's just scanning to scan:



All joking aside, this is the most immature level we can be at, but I've seen a lot of organizations where this is their reality. With scanning and cyber intelligence, we need to provide the information that is most valuable to our customer. Once we have a solid inventory for both systems and the application, we can then start understanding how we can prioritize our scans to provide the information in our reporting that will make the biggest impact for our stakeholders.

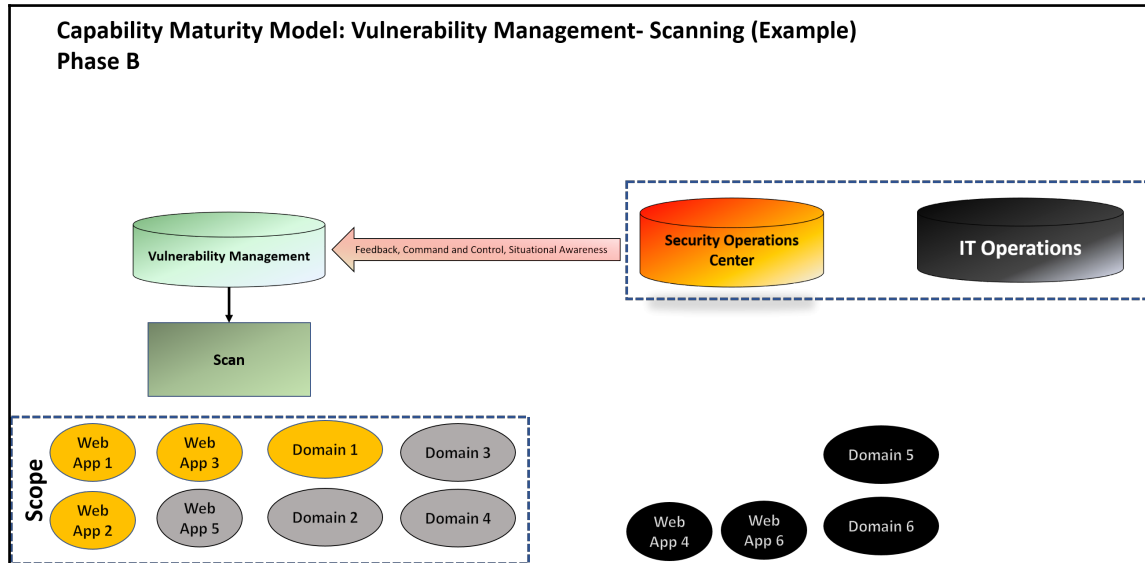
## Phase A

In phase A, we start to see the interaction between the SOC and IT operations. They have to determine with the other business owners what is considered *high impact applications and systems*. This allows the scanning function to narrow down what their scope is so that the information they provide to the **reporting** function of VM provides value first before all other applications or systems:



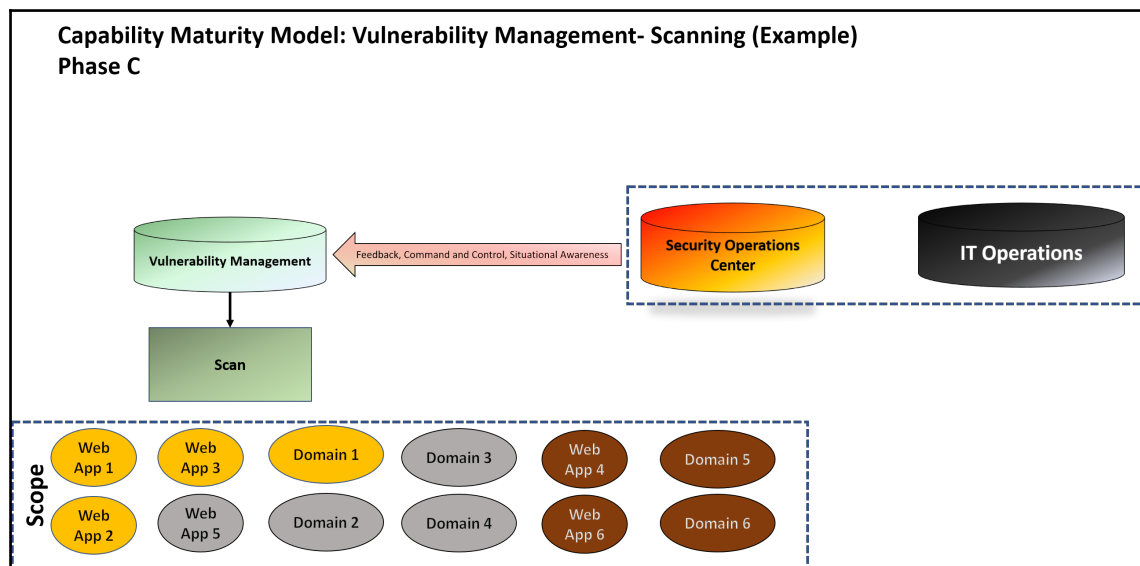
## Phase B

In phase B, we continue to see the interaction between the SOC and IT operations. They have to determine with the other business owners what is considered *medium impact applications and systems*. This allows the scanning function to expand what their scope is so that the information they provide to the **reporting** function of VM provides value on the identified items:



## Phase C

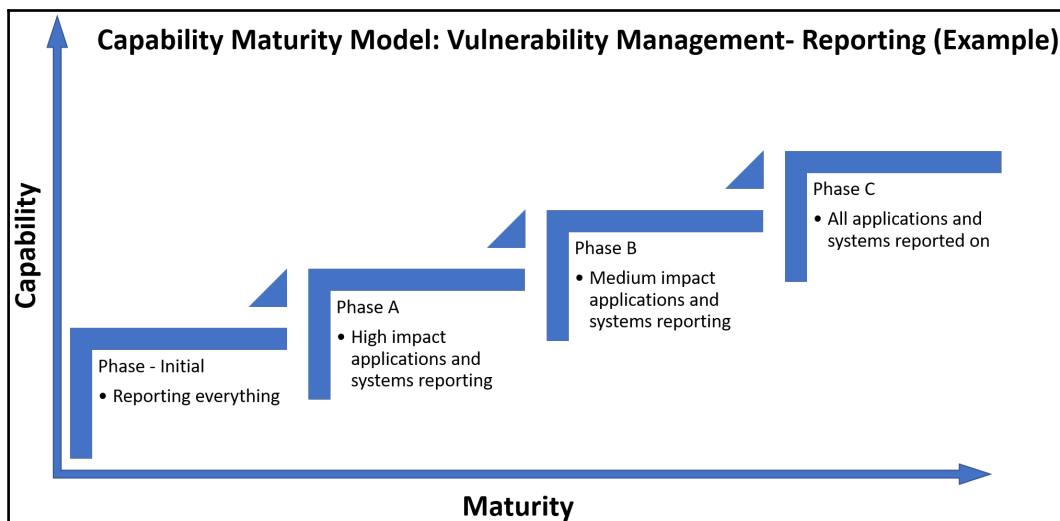
In phase C, we continue to see the interaction between the SOC and IT operations. They have to determine with the other business owners what is considered *lower impact applications and systems*. This allows the scanning function to expand what their scope is so that the information they provide to the **reporting** function of VM provides value on the identified items:



Another important item to note is that while we have built around increasing the scope of the identified applications and domains in the preceding diagrams, we should have also refined the definition of high, medium, and low impact applications and systems.

## Capability Maturity Model: vulnerability management – reporting

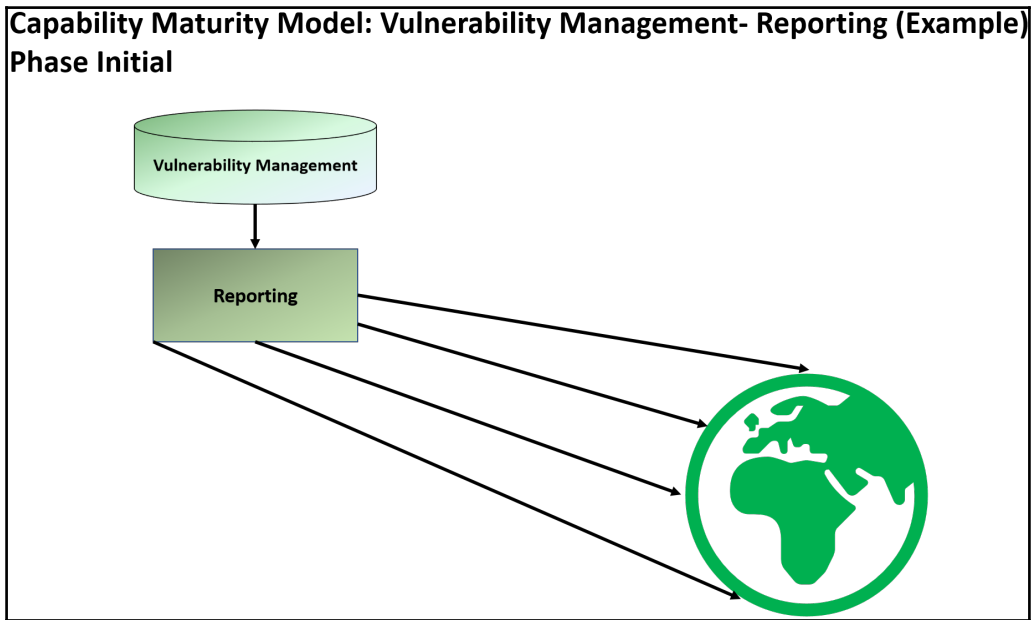
I'd like to keep this simple and say that reporting follows under the same protocol as refining the scope of the scanning function. The following is an overview:



### Initial phase

Imagine that you have just been assigned as a systems owner and application owner for a business unit in your organization. You want to do the right thing and ensure that the systems and applications you're in charge of are properly secured. The security team has just provided you with a report for 15 servers that you are responsible for and they have over 500 items to be addressed. As a week goes by, you've fixed about 100 vulnerabilities; another report comes in for the same 15 servers with another 50 items to be addressed. OK, that is two steps closer to being done, and now it's 1 step back with the additional vulnerabilities. As time goes by, additional servers and applications are commissioned and a few are decommissioned. There are lots of vulnerabilities coming at you now in the form of reports. Automated patching and scheduling help, but it's a never-ending cycle of fixing things as they come.

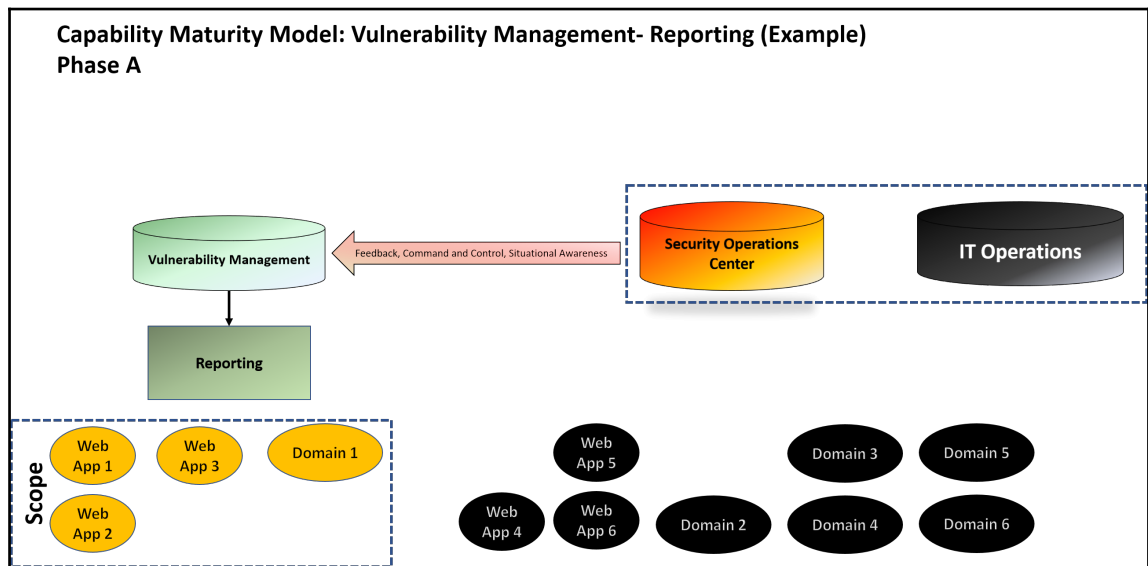
This is the initial phase of **reporting**, and it is information overload with no prioritization for remediation. The vulnerabilities that are being reported are items to be addressed with no meaning other than it needs to be fixed. Again, by reporting on everything, you are really reporting on nothing:



As a systems owner, I want information to come down to me in a way so that I understand why I'm patching in the first place. That comes with the identification and classification of the applications and systems that have the highest impact to the lowest impact to the business.

## Phase A

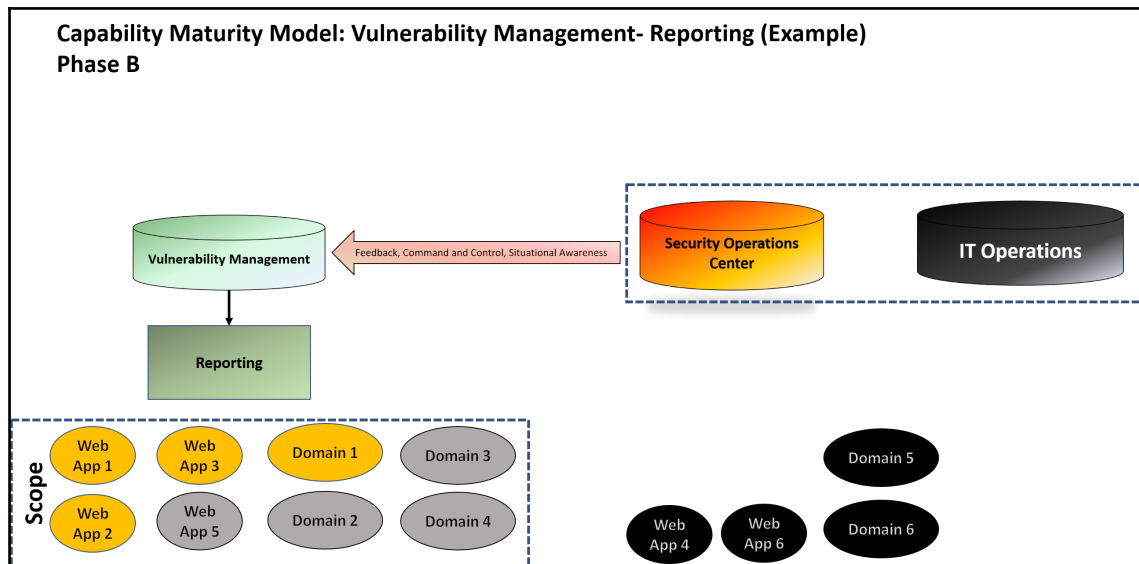
When IT leadership identifies the impact that a system or application has on the organization and the reporting reflects that, the person on the ground starts to begin to prioritize which of the things they should work on. By doing this, and reporting the progress on these specific applications, it provides the tactical leadership a means to analyze the security posture (in this case) of the systems with the highest impact to the organization:





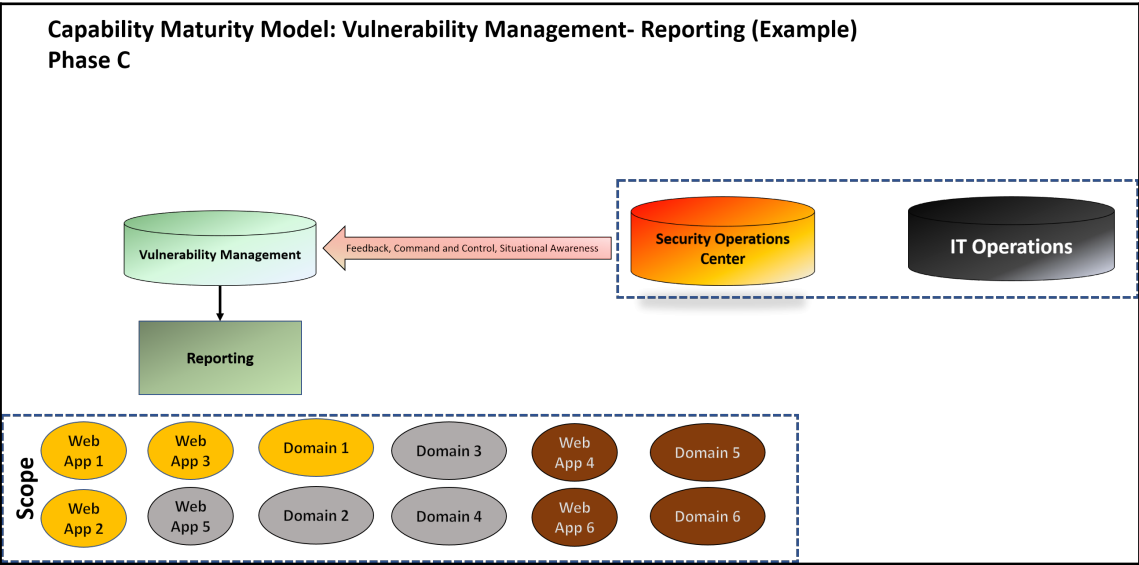
## Phase B

Once the high impact systems and applications have been defined, scanned, and reported on, we can then begin to increase the reporting scope with the scanning scope by adding the medium impact items. By communicating what is high and medium impact, the stakeholder on the ground that is responsible for mitigating the risk (again) has a basis of prioritizing their workload:



# Phase C

Finally, in phase C, stakeholders can now view each system/application, since the reports will reflect the increase of the scope and how they impact the environment. It is in this phase that we introduce another tier for impact determination, which will help drive remediation efforts:



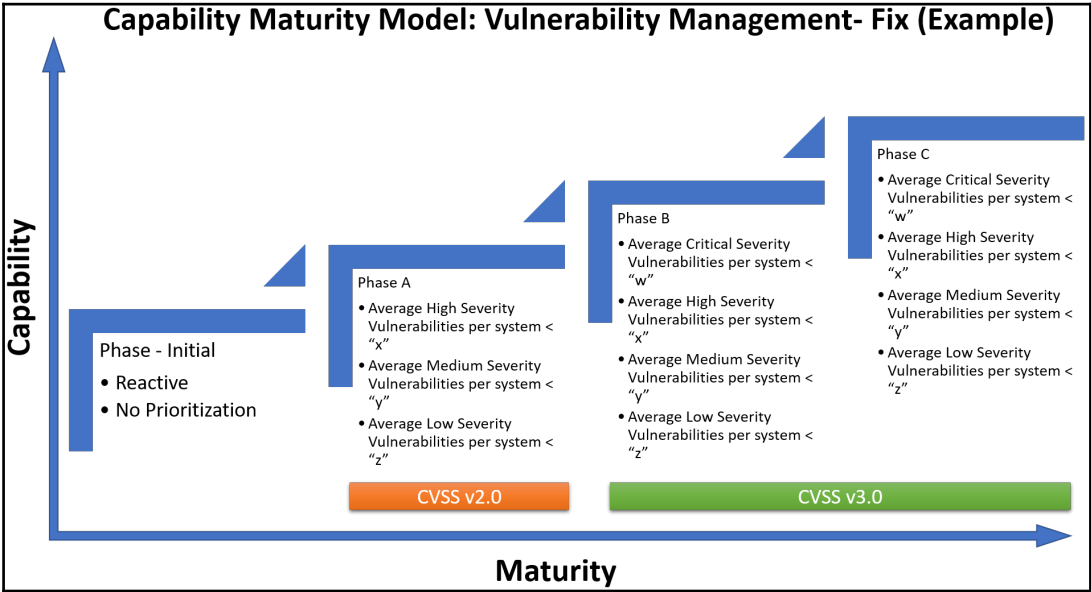
Now that we understand the levels of impact for scanning and reporting, we will go on to how we look at remediation of vulnerabilities.

## Capability Maturity Model: vulnerability management – fix

The *fix* function of the VM process also varies from organization to organization. It could be that the same person who is scanning is also the one who is fixing. Likewise, it is also possible for the person fixing to be the one receiving the vulnerability report. Either way, there needs to be prioritization of what to fix. In reporting, we prioritized how we are going to report based on the impact that a particular system(s) or application(s) has on the organization.

The Capability Maturity Model for fix, at least in my mind, should be running in parallel to what we are building for reporting. What we are trying to achieve is that once high impact systems and applications have been identified and reported on, we will need to prioritize how those items will be addressed.

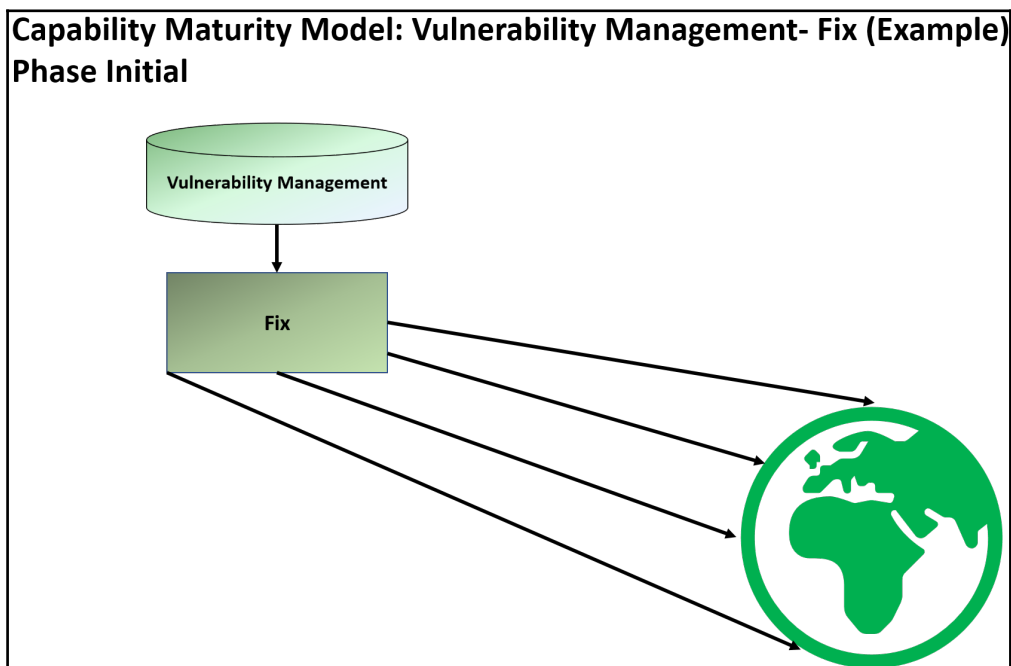
Let's take a look at an example of this:



This Capability Maturity Model includes what we have learned in the previous sections, which is the Common Vulnerability Scoring System that will help our stakeholders identify what they should fix first with an added twist. We need to reduce the exposure to exploitation of these vulnerabilities on systems. Like the example with the systems administrator who is being buried in reports, there may be hundreds of vulnerabilities in them. Without regarding risk exceptions, we should know the average number of vulnerabilities by their severity that exist on each system, and this maturity model takes that into account with one exception: the averages are defined by you and the organization.

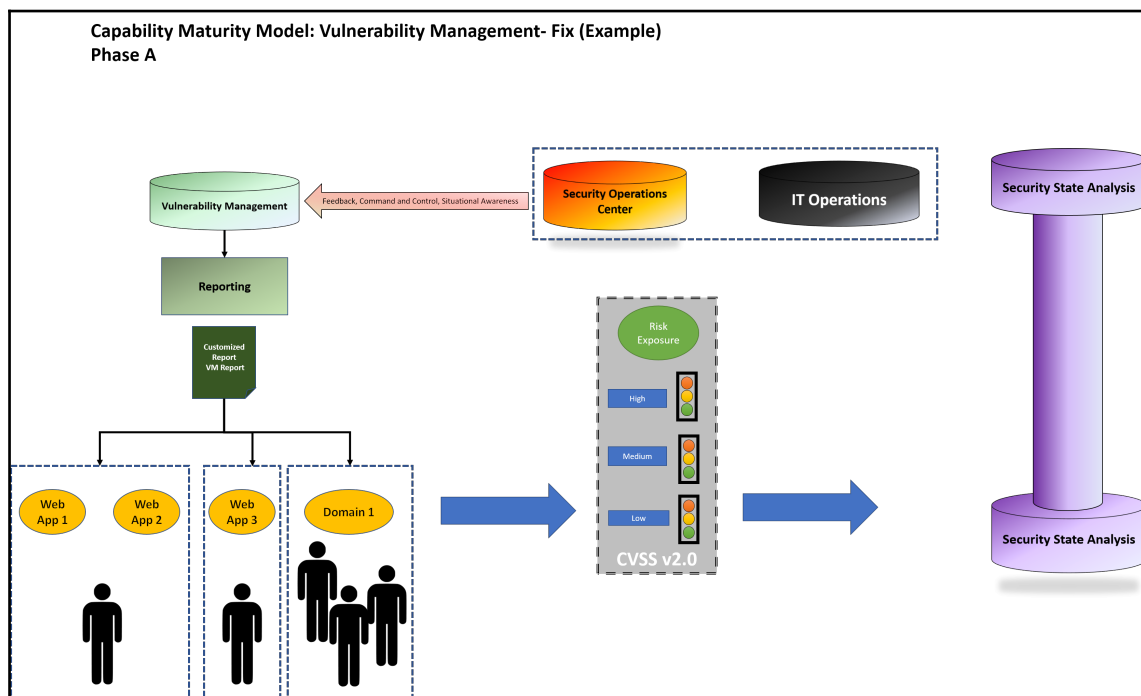
## Initial phase

The initial phase of this maturity model consists of everyone trying to fix as much as they can. There isn't really an RASCI; it's a free for all and a highly reactive environment. Hence, even with a complete asset and application inventory, it's trying to fix the world again, as depicted here:



## Phase A

As we've already (or working towards) identified what the high impact applications and systems are, we should also be identifying the stakeholders who are responsible for fixing these vulnerabilities. Once we start looking at the vulnerabilities, we can then use the CVSS v2.0 as a guide in ranking the vulnerabilities. Notice in the following diagram that we've now placed a high, medium, and low-risk exposure RAG dashboard-esque way to see if we are good, need a little work, or got a lot of work to do:



Of course, the definition of this is up to the organization, but we want to at least begin with understanding what it could be.

For example:

- **High severity:**
  - **Red:** Average of 10 vulnerabilities per system
  - **Amber:** Average of 7-9 vulnerabilities per system
  - **Green:** Average of 0-6 vulnerabilities per system
- **Medium severity**
  - **Red:** Average of 20 vulnerabilities per system
  - **Amber:** Average of 10-19 vulnerabilities per system
  - **Green:** Average of 0-9 vulnerabilities per system
- **Low severity**
  - **Red:** Average of 25 vulnerabilities per system
  - **Amber:** Average of 15-24 vulnerabilities per system
  - **Green:** Average of 0-14 vulnerabilities per system

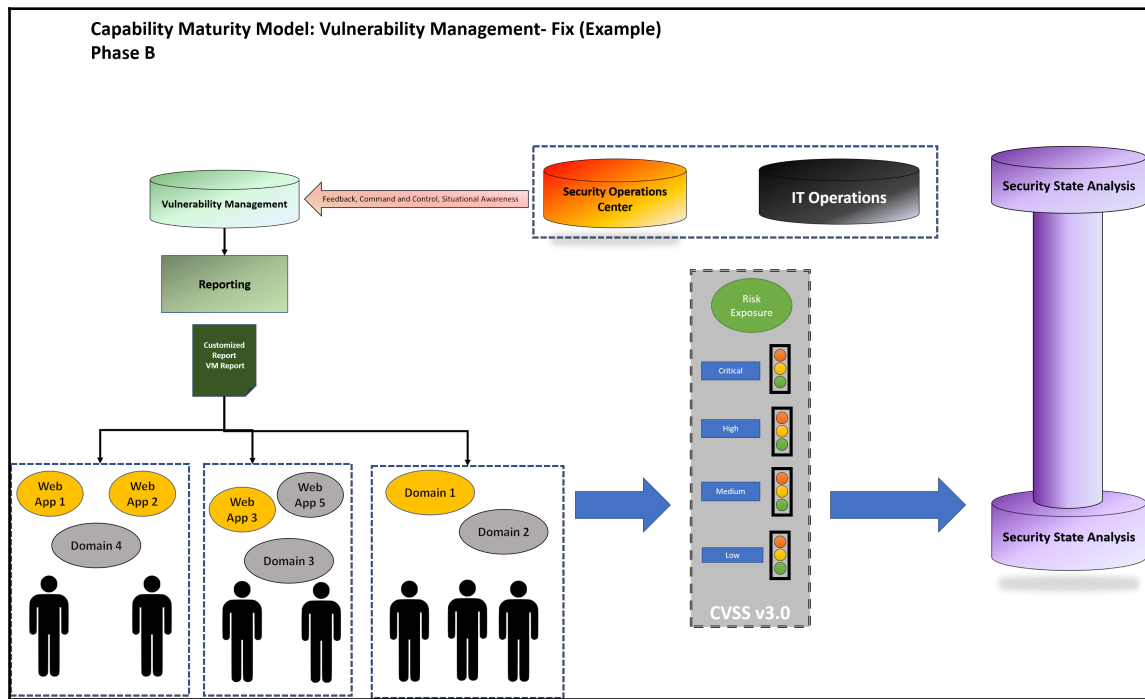
By applying an average per system, it allows a stakeholder to identify what they should work on first. If they are red in the low severity and red in the high severity categories, they would know that they would need to work on the high severity vulnerabilities first. If the high and low severity ratings are green and the medium severity rating is amber, they would know that they should focus on decreasing the average medium severity vulnerabilities per system.

The preceding example can be used across an enterprise, and even further matured within this phase by decreasing the average number of vulnerabilities per system, per category. The main thing for us to understand is that we need to be able to control our network to have an acceptable amount of risk exposure for our high impact systems and applications before we think about increasing the scope of reporting. By doing this, we will lay out the foundation to enable cyber intelligence communication channels to continue on to subsequent phases.

## Phase B

Similar to phase B in the reporting Capability Maturity Model of vulnerability management, we begin to see the scope increase to the medium impact systems and applications. Another important change here is the introduction of the CVSS v3.0 critical category.

It is another prioritization indicator to the stakeholder that *critical* means *fix now*:



Here is an example of how we can utilize this on top of the work that we've done in phase A.

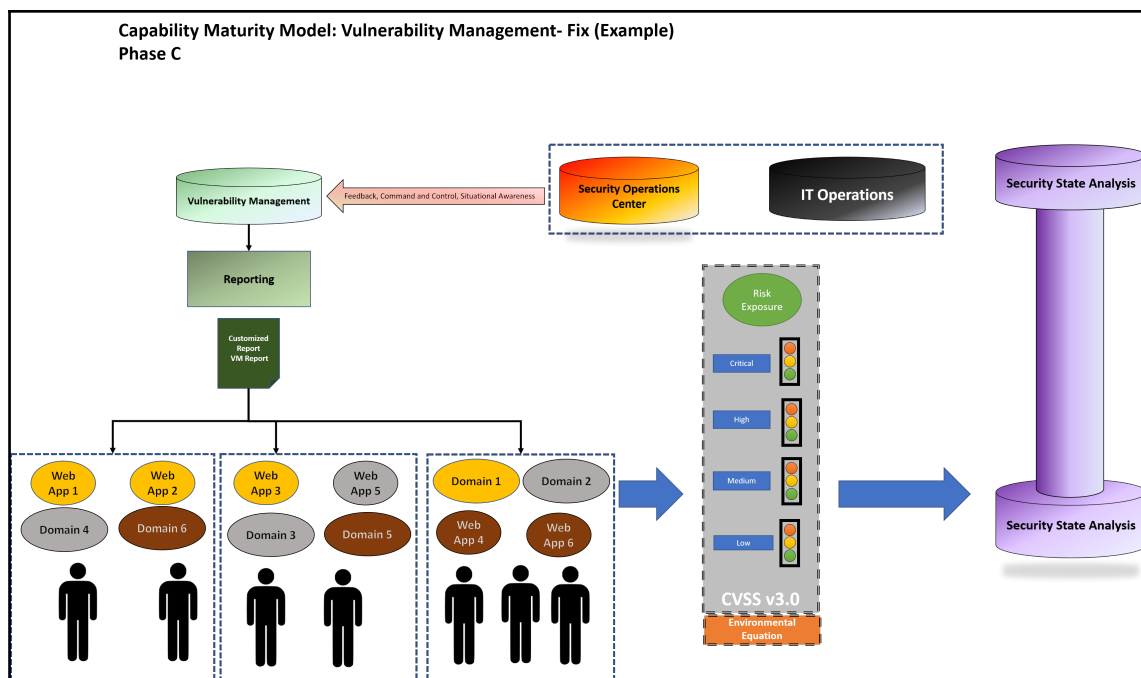
For example:

- **Critical severity:**
  - **Red:** Average of 3 vulnerabilities per system
  - **Amber:** Average of 1-2 vulnerabilities per system
  - **Green:** Average of 0 vulnerabilities per system
- **High severity:**
  - **Red:** Average of 5 vulnerabilities per system
  - **Amber:** Average of 3-4 vulnerabilities per system
  - **Green:** Average of 0-2 vulnerabilities per system
- **Medium severity:**
  - **Red:** Average of 10 vulnerabilities per system
  - **Amber:** Average of 8-9 vulnerabilities per system

- **Green:** Average of 0-7 vulnerabilities per system
- **Low severity:**
  - **Red:** Average of 15 vulnerabilities per system
  - **Amber:** Average of 10-14 vulnerabilities per system
  - **Green:** Average of 0-9 vulnerabilities per system

## Phase C

Finally, we've reached phase C. The scope is now including the low impact applications/systems into the reporting. In addition to the increased scope, we should now be looking at making the CVSS more applicable to our environment by including the environment equation. These metrics measure the impact to the confidentiality, integrity, and availability of a vulnerability to an organization if exploited. The flow is depicted in the following diagram:



By including the environmental equation and the level of impact of the systems and application to the organization, we can then further distinguish what our stakeholders need to fix.



For example:

- **High impact systems:**
  - **Critical severity:**
    - **Red:** Average of 3 vulnerabilities per system
    - **Amber:** Average of 1-2 vulnerabilities per system
    - **Green:** Average of 0 vulnerabilities per system
  - **High severity:**
    - **Red:** Average of 5 vulnerabilities per system
    - **Amber:** Average of 3-4 vulnerabilities per system
    - **Green:** Average of 0-2 vulnerabilities per system
  - **Medium severity:**
    - **Red:** Average of 10 vulnerabilities per system
    - **Amber:** Average of 8-9 vulnerabilities per system
    - **Green:** Average of 0-7 vulnerabilities per system
  - **Low severity:**
    - **Red:** Average of 15 vulnerabilities per system
    - **Amber:** Average of 10-14 vulnerabilities per system
    - **Green:** Average of 0-9 vulnerabilities per system
- **Medium impact systems:**
  - **Critical severity:**
    - **Red:** Average of 3 vulnerabilities per system
    - **Amber:** Average of 1-2 vulnerabilities per system
    - **Green:** Average of 0 vulnerabilities per system
  - **High severity:**
    - **Red:** Average of 9-10 vulnerabilities per system
    - **Amber:** Average of 6-8 vulnerabilities per system
    - **Green:** Average of 1-5 vulnerabilities per system
  - **Medium severity:**
    - **Red:** Average of 15 vulnerabilities per system
    - **Amber:** Average of 10-14 vulnerabilities per system
    - **Green:** Average of 0-9 vulnerabilities per system
  - **Low severity:**
    - **Red:** Average of 15 vulnerabilities per system
    - **Amber:** Average of 10-14 vulnerabilities per system

- **Green:** Average of 0-9 vulnerabilities per system
- **Low impact systems:**
  - **Critical severity:**
    - **Red:** Average of 3 vulnerabilities per system
    - **Amber:** Average of 1-2 vulnerabilities per system
    - **Green:** Average of 0 vulnerabilities per system
  - **High severity:**
    - **Red:** Average of 5 vulnerabilities per system
    - **Amber:** Average of 3-4 vulnerabilities per system
    - **Green:** Average of 0-2 vulnerabilities per system
  - **Medium severity:**
    - **Red:** Average of 20 vulnerabilities per system
    - **Amber:** Average of 15-19 vulnerabilities per system
    - **Green:** Average of 0-14 vulnerabilities per system
  - **Low severity:**
    - **Red:** Average of 25 vulnerabilities per system
    - **Amber:** Average of 20-44 vulnerabilities per system
    - **Green:** Average of 0-19 vulnerabilities per system

This is difficult and it is something to work towards. It is an idea of how we can communicate the prioritization of remediation efforts to the stakeholders.

## Summary

This was a very long chapter that has just briefly covered how we can improve our communication of vulnerabilities and remediation efforts in order to enable cyber intelligence through multiple stakeholders. We should be aware that VM has a huge dependency on the inventory of applications and systems being correct, or we risk missing things that should be accounted for in our scanning. By improving our scanning coverage and through the identification of high to low impact applications/systems that exist on our network, we can then begin prioritizing how we can fix vulnerabilities by customizing the reporting that we provide for the remediation personnel. Finally, by understanding the prioritization of remediation efforts, the work being completed allows us to have an input into our security state analysis capability in order to inform the tactical and strategic levels of leadership about our posture.

# 13

## Risky Business

Risk is a topic that we can't get away from in any aspect of our lives. It is always present, especially in IT. In this chapter, we will talk about the importance of risk and how it is typically handled in an organization.

In this chapter, we will cover the following topics:

- Risk overview
- Data classification
- Capability Maturity Model: risk
- Some GRC tools that you can use

### Risk overview

We've spent a lot of time in the last few chapters talking about threats and vulnerabilities, and their potential to impact our systems and information. How we address these threats is through the application of handling risk.

*Risk = Probability x Impact:*

- *Probability = How likely is it that this vulnerability will be exploited?*
- *Impact = How much is it going to hurt?*

### Treating risk

So once we find a vulnerability and a threat, calculate their probability and impact, what comes next? The risk needs to be addressed.

Risk is handled in different ways:

- **Risk acceptance:** The organization accepts the vulnerability and the possible threat as is
- **Risk avoidance:** The organization removes any exposure to the threat
- **Risk remediation:** The organization fixes the vulnerability so that it cannot be exploited
- **Risk mitigation:** The organization lessens the likelihood of exploitation by putting compensating controls in place
- **Risk transference:** The organization transfers the risk to another party so that if the vulnerability is exploited, the other organization incurs the cost

## Risk tolerance and risk appetite

According to ISO 31000, **risk appetite** is a higher level understanding of *the amount and type of risk that an organization is prepared to pursue, retain, or take on an objective*. **Risk tolerance** is understanding the levels of risk tolerance for that specific objective.

For example:

1. Mother, father, and child are at the park.
2. Father wants to throw the child in the air. The risk identified is that the child will get hurt.
3. Knowing that the father has a bond with his child, the mother allows this risk event to happen. This is the **risk appetite**.
4. The height at which the mother will stop the child from being thrown in the air is the **risk tolerance**.

So, besides knowing that vulnerabilities needed to be addressed through proper risk mitigation, we need to apply the same logic to how we look at the end-to-end processes that require multiple services and capabilities.

We need to be able to assign the appropriate **risk appetite** through communicating PIRs, and establish thresholds of enforcement through defining levels of **risk tolerance**.

If we know that we are going to pursue a change management process, then we will have to understand the risks of doing it in-house or vendor-supported (**risk appetite**), as well as identify and define the levels of performance that are expected (**risk tolerance**) with each entity involved in the process.

# Labeling things platinum, gold, silver, and copper

When I hear the term *crown jewels*, it is usually a binary comparison of what data is important and what data is not important. We can't really think of an organization's data as either/or, because all data is important for an organization. Not only is all data important for an organization, understanding the value of the systems that process, store, and transmit this data is just as important. Just as the *crown jewel* information must be protected, so must the systems that interface with the data.

By understanding this concept, we can look at not just information, but the collective systems, as being classified as *crown jewels*.

Here are a few examples of information classifications:

- **Military information classifications** ([https://fas.org/sgp/library/quist2/chap\\_7.html](https://fas.org/sgp/library/quist2/chap_7.html)):
  - **Top secret:** Disclosure of information that *can cause exceptionally grave damage* to national security
  - **Secret:** Disclosure of information that can cause serious damage to national security
  - **Confidential:** Disclosure of information that can be expected *to cause damage* to national security
- **ISO 27001:**
  - **Confidential** (top confidentiality level)
  - **Restricted** (medium confidentiality level)
  - **Internal use** (lowest level of confidentiality)
  - **Public** (everyone can see the information)

By labeling the value of the networks of systems, applications, and so on, we can prioritize the amount of time and effort that we need to ensure that they stay within an organization's risk tolerance thresholds.

We spend a lot of time trying to figure out how not to get breached. The question we need to ask ourselves is *do we want the thieves to run out with a bag of platinum and golds bars or with a bag of copper coins?*

## Differentiating networks

In the military, you have separate networks based on the classification of the information that is being passed through. Some examples include:

- **Non-Classified Internet Protocol Network (NIPRNet):** Used for unclassified information systems
- **Secret Internet Protocol Network (SIPRNet):** Used for classified information systems
- **Joint World-Wide Intelligence Communications System (JWICS):** Used by multiple agencies for high level classified information communication
- **Combined Enterprise Regional Information Exchange System (CENTRIX):** Used by NATO coalition entities to pass classified information between each other

With these networks, it is rather straightforward to see what the classification of the information is, but this isn't a realistic scenario with most businesses. As previously discussed, in business it is important to us to know the classification of the information in directories, folders, and files so that we can apply some logical controls, such as access control lists and network segmentation.

One challenge for business is when you have multiple applications with various levels of information classification on a physical device. Even more challenging, you can have multiple virtual machines on the same physical device that house various classifications of information. So, how do we handle such complex issues? The answer is in how we address risk.

## Taking a different look at risk

Now that we can look at information and the systems that they interact with, they can be treated in accordance to how much value they mean to the organization. The senior leadership of both IT and security need to:

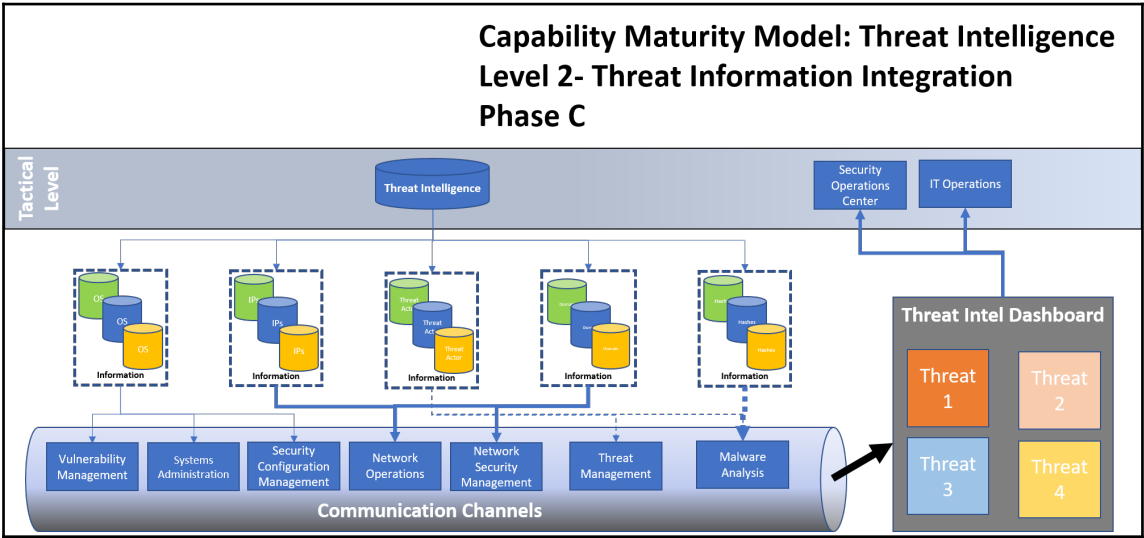
- Define differences in the security level requirements from *copper* networks to *platinum* networks
- Establish metrics of what is good, bad, and ugly for the services and/or end-to-end process
- Monitor and present results visually at all levels

These three things are pretty common when you talk about risk.

Something that is not measured here (that at least I think can be improved) is taking the risk reduction process to a level where we can anticipate relevant threats based on real-time threat intelligence. We want to reduce risk exposure based on **relevant** threat intelligence by establishing a capability (cyber intelligence) to communicate across the organization. This is an attempt to integrate information being generated from security services (threat intelligence, red team, threat hunting, and so on) into the risk management process.

## Review of threat intelligence integration

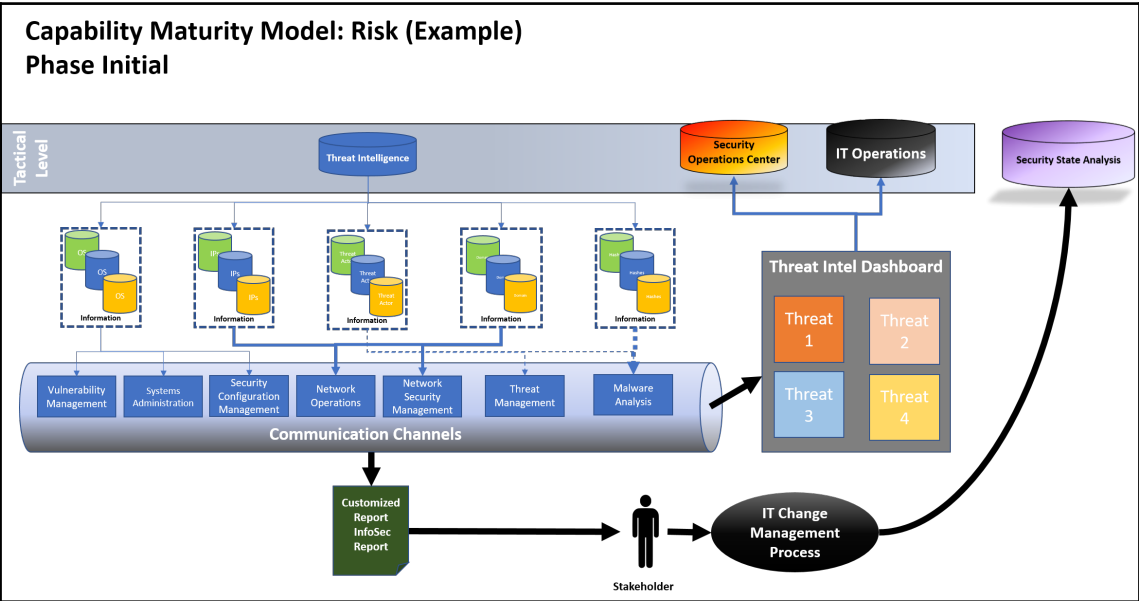
At the beginning of the book, we talked about how we can improve threat intelligence integration into all of the information security teams by providing customized information for them to analyze. A cumulative analysis would be able to provide us with an internal view of how each threat can be relevant to the organization through a threat intel dashboard. This is depicted here:



# Capability Maturity Model: risk phase – initial

We also discussed that the stakeholders have an integral part in improving the security of the organization. We can influence stakeholders through customized information security reporting to fix issues. To enable them to do that, they would have to follow a change management process that is typically run by IT operations. With the continuous reassessment of threats that may impact the environment, the information that is updated in the change management process would allow us to have a view of how the stakeholders are addressing reported issues. This is reflected on the threat intel dashboard and also fed into security state analysis. This enables further analysis inputs for the overarching intelligence cycle of the organization at the strategic and tactical levels.

What makes this phase unique is that the data being produced from each information security team (even integrated reports) is being presented to the stakeholder for action. Multiple reports, for multiple findings, from multiple services *equals* confusion on where to start, which *equals* burnout and frustration:

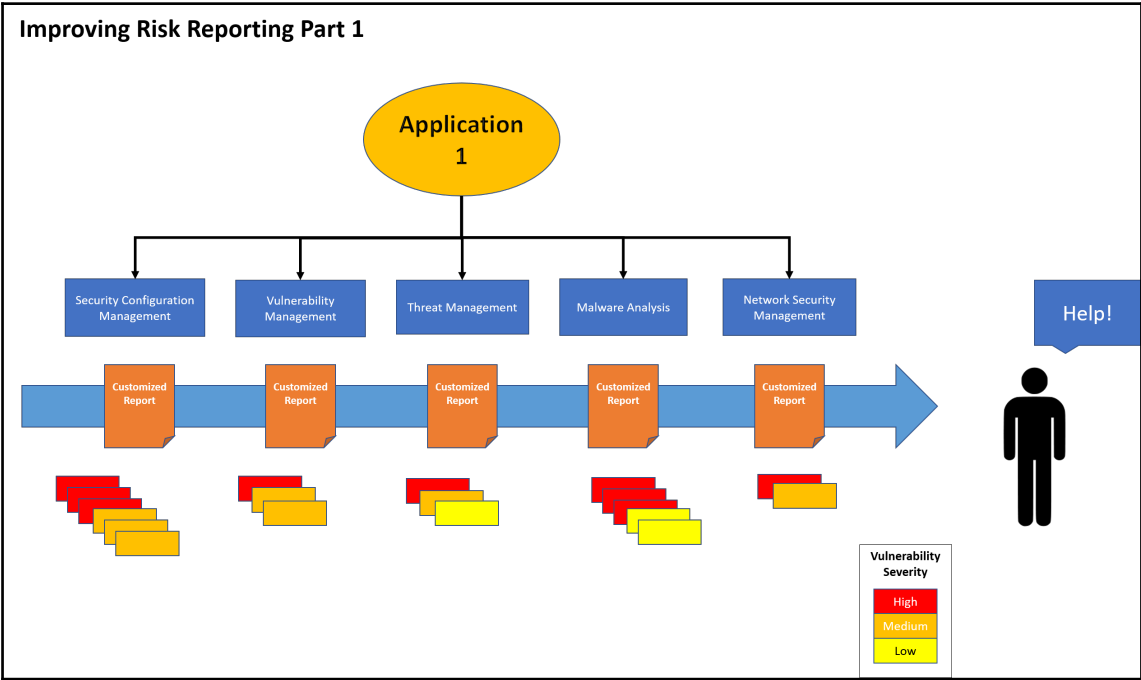




# Improving risk reporting part 1

Let's try to look through the eyes of the folks on the ground. Even if we have a complete inventory of systems and applications, as well as an understanding of labeling the classification of data, the sheer amount of reporting that comes from several services can be overwhelming.

The following is an example of how one application can have multiple findings from multiple assessments:

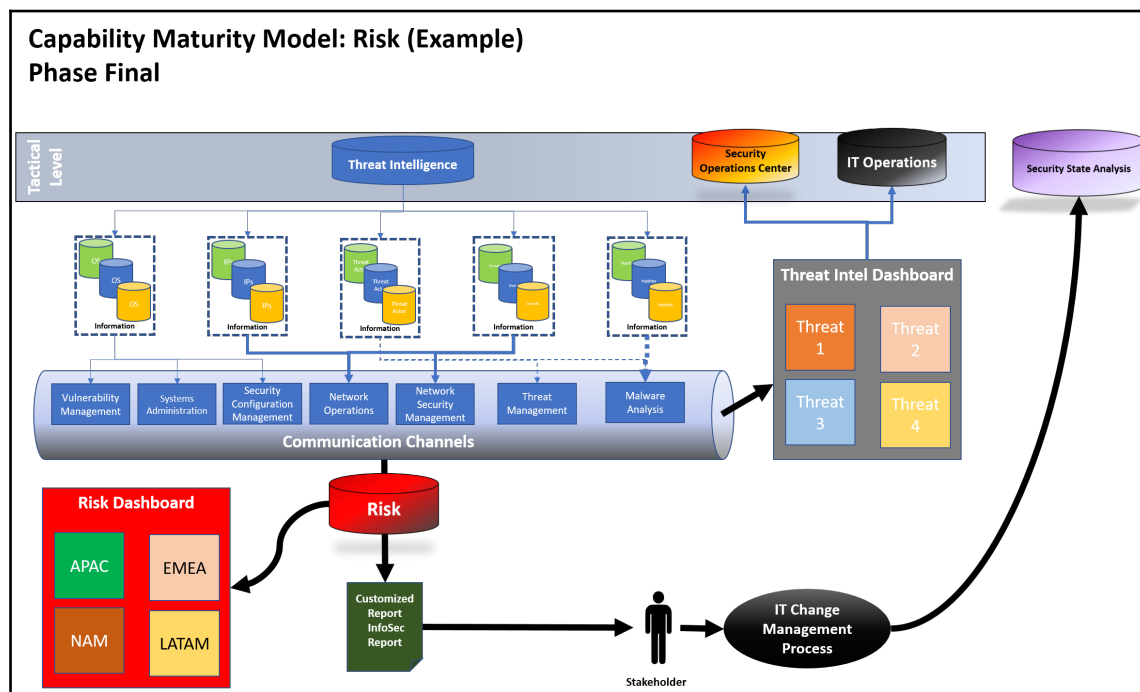


This dilemma only gets more complicated as we add more applications and systems into the mix.

A further analysis needs to be done for the stakeholder, to help them understand which high severity vulnerability needs to be fixed first. Also, a further analysis needs to be done for the stakeholders to understand which application should be fixed first.

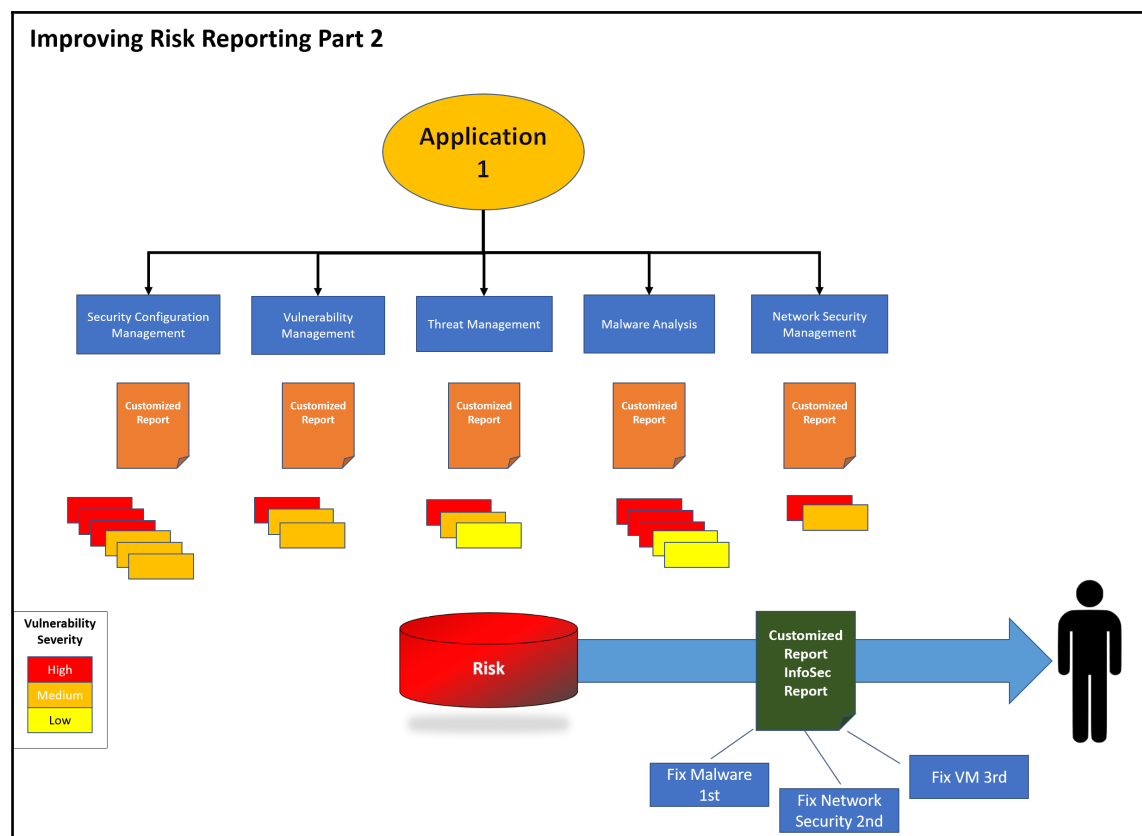
## Capability Maturity Model: risk phase – final

So, on top of improving an organization's risk management practices of gathering and analyzing the results from multiple service processes on a risk dashboard, risk also plays an important role in furthering the customization of reporting what goes to the stakeholders by incorporating threat intelligence:



## Improving risk reporting part 2

Now that we understand how we can utilize the data classification of systems and information to prioritize the remediation of vulnerabilities, we can take this a step further in using threat intelligence as a means of prioritizing the remediation of vulnerabilities based on their relevance:



Here is an example. Threat intelligence reports that the software's HIGH severity vulnerability, A, is being exploited. There is a high impact system that resides on the network that has this vulnerability, but also has another high-level vulnerability, B, and a HIGH impact non-conformance to a configuration, C. As this information is being filtered through risk to amplify threat intelligence information, the report that is delivered to the stakeholder should focus on addressing vulnerability A. It is not that B or C are not as important as A, but it is because a possible exploitation attempt is more likely.

## Open source governance risk and compliance tools

Maybe you already have a means and methodology to calculate risk in your organization. It can be mind-numbing, but there are ways to evaluate your current controls against frameworks such as ISO 27001, PCI-DSS, and the NIST cyber security framework. If you are just beginning your journey in this, what follows is a list of **governance, risk, and compliance (GRC)** tools that you can try out.

### Binary Risk Assessment

Offering printable use and an HTML5 application of their product, the Binary Risk Analysis team has a very quick way of analyzing a vulnerability using queries such as:

- The attack can be completed with common skills
- The attack can be completed without significant resources
- The asset is undefended

This assessment gives the user a very quick and easy view of risk, likelihood, and impact of a singular vulnerability. You can find more information on this here: <http://binary.protect.io/>.

### STREAM cyber risk platform

This platform is brought to us by Acuity Risk Management (<https://acuityrm.com/>). There is a free version of this platform that can give you an idea of how you can maintain compliance with legislation and regulations that are applicable to your industry.

### Practical threat analysis for information security experts

Another tool for information security professionals to calculate risk and threats is the practical threat analysis methodology and suite of software tools. More information can be found here: <http://www.ptatechnologies.com/>.

## SimpleRisk

The name is pretty straightforward: SimpleRisk is **Enterprise Risk Management Simplified** according to their site (<https://www.simplerisk.com/>). You can install your own server with core functionalities such as:

- Risk submissions
- Mitigation planning
- Risk reviews
- Reporting

There are extra features that come at a cost, but again, it's a tool you can evaluate so that you can see if it works for your organization.

## Security Officers Management and Analysis Project

The Security Officers Management and Analysis Project's site (<https://www.somap.org>) contains a portfolio of sub-projects that make up the **Open Source IT Risk Management** project:

1. The Open Risk and Compliance Tool
2. The Open Risk and Compliance Framework
3. The Open Risk Model Repository
4. The Open Governance, Risk, and Compliance Maturity Management Methodology

## Summary

Classifying networks/systems/applications based on impact is only the beginning of how we can address vulnerabilities. The preceding examples are just ideas of how we can incorporate threat intelligence into the business processes of risk management. By integrating threat intelligence into reporting and customizing reporting based on risk analyses, we can improve our OODA loop, reduce potential attack vectors for our adversaries, and decrease the probability of exploitation.

# 14

## Assigning Metrics

An important part of understanding how we can apply cyber intelligence in our organization is by developing metrics that highlight the progress of an end-to-end process. In this chapter, we will be looking at how we can apply a risk metric across capabilities between IT security and IT operations. We will cover:

- Overview of security configuration management
- Developing a risk score

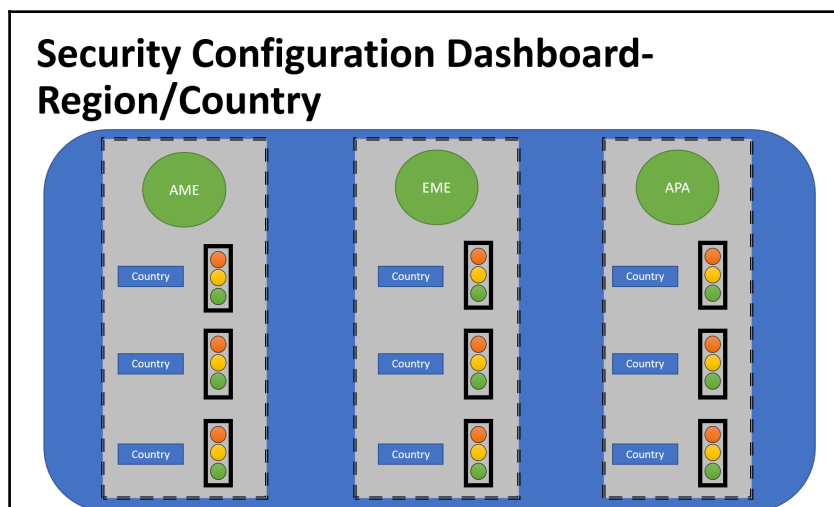
### Security configuration management

An organization should have a standard configuration for all of their technologies, and they need to be evaluated from time to time. In order for *the most correct* scanning to occur, there must be a few requirements that have to be understood across IT and InfoSec teams.

In order to have different views on the compliance with these baselines, stakeholders in the process should be able to visually see the risk metric broken down by the following:

- Region
- Country
- Operating system
- Application

An example dashboard is presented here:



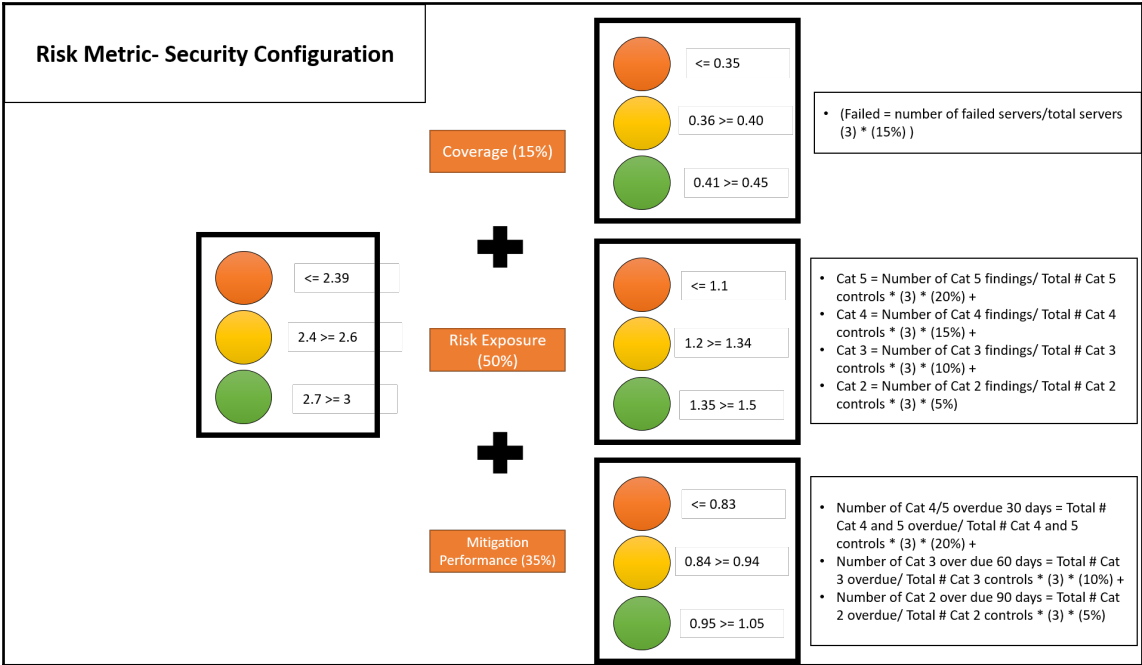
## Developing the risk score

The risk score for this process is based on three factors, and uses three as its base:

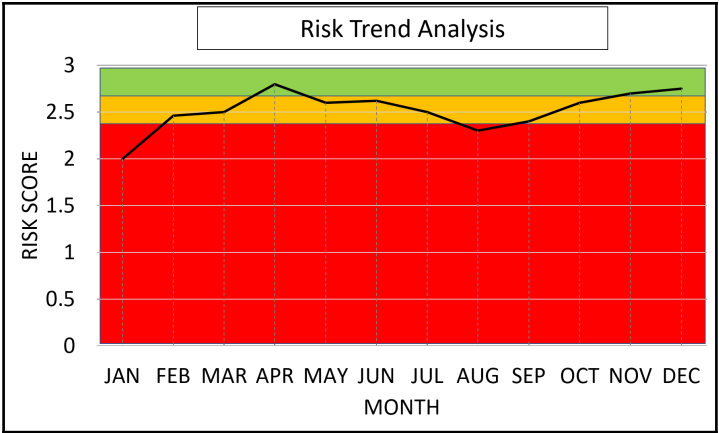
- **Coverage metric** (=15% of the total score):
  - Assets management process (**IT operations**):
    - InfoSec tools require that the assets scanned are the ones that are official
    - Need proper credentials for scanning
  - Discovery scan process (**InfoSec**):
    - Finds potential rogue devices and *shadow IT* in assigned subnets
- **Risk exposure metric** (=50% of the total score):
  - **IT risk** communicates how it will weigh each risk level per control
  - **InfoSec teams** will be evaluated on the frequency of the scans and the distribution of the reports

- As the baseline is finite, each security configuration item is given a level of:
  - **Category 5 (critical impact):**
    - *Number of cat 5 findings / total # cat 5 controls = 20% of the score*
  - **Category 4 (high impact):**
    - *Number of cat 4 findings / total # cat 4 controls = 15% of the score*
  - **Category 3 (medium impact):**
    - *Number of cat 3 findings/ total # cat 3 controls= 10% of the score*
  - **Category 2 (low impact):**
    - *Number of cat 3 findings / total # cat 3 controls = 5% of the score*
- **Remediation performance (=35% of the total score)**
  - This measures the stakeholders (**IT operations**) in the speed in which they can reduce the risk by:
    - Requesting an exception and establishing a compensating control
    - Fixing the finding
  - Stakeholders were given a grace period from when the finding was first established:
    - *Number of cat 4/5 overdue 30 days = 20% of the score:*
      - *Total # cat 4 and 5 overdue / total # cat 4 and 5 controls*
    - *Number of cat 3 overdue 60 days = 10% of the score:*
      - *Total # cat 3 overdue/ total # cat 3 controls*
    - *Number of cat 2 overdue 90 days = 5% of the score:*
      - *Total # cat 2 overdue / total # cat 2 controls*





By using an RAG metric from the preceding figure, the organization can begin looking at creating an analysis like the following:



## Working in key risk indicators

We have to know whether or not a process is having issues. So, each of the risk metrics that develop the score needs to have their KRIs so that it will inform the stakeholders that there may be an issue.

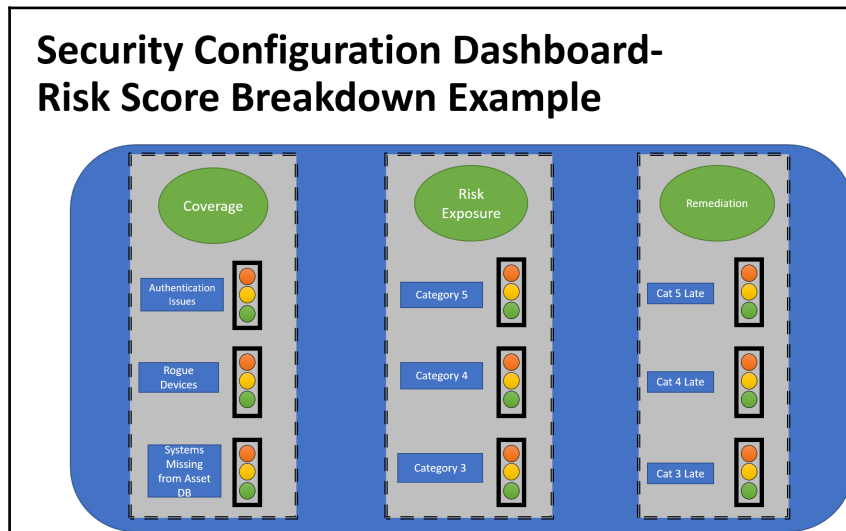
Each of the areas has been weighted according to their importance to the overall score:

- **Coverage** equals to 15% of base 3, which can equal to no more than 0.45:
  - *GREEN = 0.41-0.45 or 90-100% of systems do not have issues being scanned*
  - *AMBER = 0.36-0.40 or 80-89% of systems do not have issues being scanned*
  - *RED = <0.35 or less than 79% of systems do not have issues being scanned*
- **Risk exposure** equals to 50% of base 3, which can equal to no more than 1.5:
  - *GREEN = 1.35-1.5 or 90-100% of the total controls being assessed passed*
  - *AMBER = 1.2-1.34 or 80-89% of the total controls being assessed passed*
  - *RED = <1.1 or less than 79% of the total controls being assessed passed*
- **Mitigation performance** equals to 35% of base 3, which can equal to no more than 1.05:
  - *GREEN = 0.95-1.05 or 90-100% of the total controls assessed are being addressed on time*
  - *AMBER = 0.84-0.94 or 80-89% of the total controls being assessed are being addressed on time*
  - *RED = <0.83 or less than 79% of the total controls being assessed are being addressed on time*

As we know that each area requires that teams work together, we can assign the scores or measurements that will *warn* us that a process is about to go into AMBER:

- *Key risk indicator for coverage = 0.41-0.42*
- *Key risk indicator for risk exposure = 1.34-1.35*
- *Key risk indicator for remediation = 0.95-0.96*

To help us understand how each area is performing and where we can address issues in more detail, we can create another dashboard to monitor the process and highlight areas that need attention. See the following example:



## Summary

In this chapter, we reviewed how we can build some metrics by looking at an example of the end-to-end process of security configuration management. Creating dashboards are a great way for teams across the aisle to know and understand their level of performance throughout the process. By developing KRI thresholds, where warnings can be delivered to teams, we build awareness of possible issues that need to be addressed.

# 15

## Wrapping Up

In this chapter, we are going to conclude what we've learned from the previous chapters. We will discuss final thoughts on cyber intelligence as well as reviewing key points from the book.

### Just another day part 3

**1300- Eastern Standard Time. Location: Chesty Lewis Puller Security Operations Center, Centralia, Virginia.**

*"Alright, let's roll call,"* Charles announced.

After each person presented themselves, Charles went on. *"So we had a situation in APAC that popped up on our dashboard. Seems that we had an email with some malware coming in. I've got Tatsuya from Japan and Sandeep from India on the line to clarify, but it seems that the situation is under control, is that correct gentlemen?"*

*"Yes, hi,"* said Tatsuya, *"I only had one user impacted. We followed our incident response procedures and have the evidence that you need. The user is back online."*

*"It is the same situation here,"* Sandeep said, *"the users received an email from security awareness a few minutes ago informing them of this. If anything else shows up, everyone knows to let the help desk know."*

*"Great. Tatsuya, I'll get you to send that to our guy in the Czech Republic. He loves that stuff,"* Charles said. *"Mauricio, how about the firewalls?"*

*"I've already been working with the IT operations guys and we've gone ahead and blocked the sender domain based on the TTP information we've received from our threat intel folks."*

*"Perfect."* Charles walks over to the risk dashboard monitors. *"Let's move on. Any major KRIs to report, Jacek?"*

*"We were seeing a downward trend on the remediation of high severity tickets on our Tier 1 applications. To stay green, they need to be fixing these to keep the average between 0-3 vulnerabilities per server, per week, and right now there are about 3 for the last four weeks. They know and they are working on it. They lost a guy a month ago so they are working on his replacement," Jacek said. "We've also moved up from amber to green on all severity levels for our Tier 2 applications," he added.*

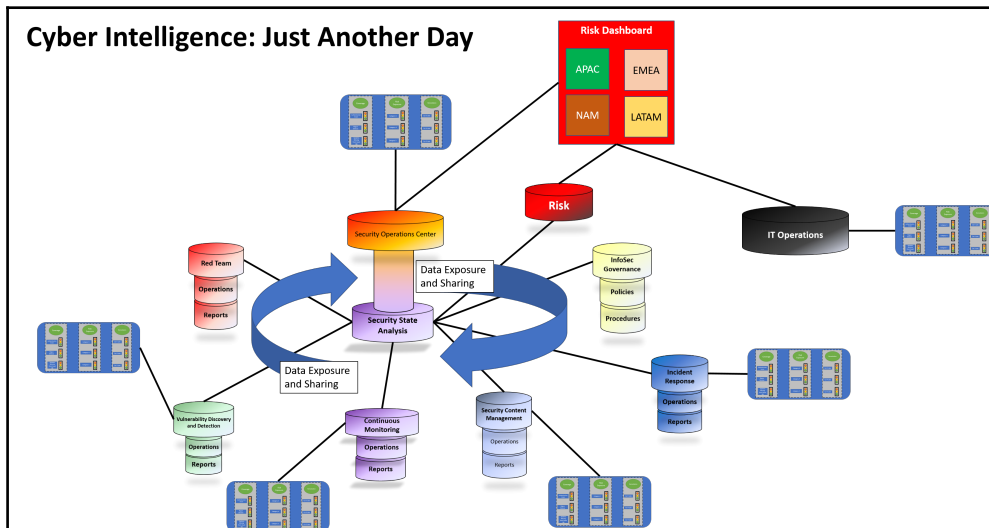
As the SOC meeting went on, each person present provided their updates as required, passing information to each other as appropriate.

*"Alright, folks," Charles said. "It's Friday, and I've got to send up a brief summary to the bosses on APAC as well as other PIRs. If no one has anything else, have a great day."*

## Lessons learned

Honestly, the moral of the story is that you can have increased efficiency if you build the means to collaborate effectively. The information that is passed is applicable to your stakeholders and can be worked on. We can do this through customizing dashboards and reports to visualize end-to-end processes that impact one another. When establishing KRIs, we can identify trends in process performance decline prior to the process failing.

All of the previous chapters lead up to this crazy diagram:



An IT organization is an interconnected web of complex systems that are dependent on one another to function and to be secure. As much as each entity in the team is trying to *make it happen*, we can improve by developing a better means of communicating the priorities that are required at different levels.

How long will it take us to get to this point?

Once we get there, what's next?

I would consider that getting to this point would require the management of PIRs at each level, which would be based on strategic decision-making being passed down to tactical leaders, as we've discussed. We can improve this by creating an actual cyber intelligence capability within the organization to manage all of the PIRs. Is this far reaching? Yes, but I believe a few well-resourced organizations are already implementing this in some capacity.

I think it's next-level stuff, and I've seen it work in the military. I've been a part of some amazing combat operations where they utilized the information around them to develop real-time intelligence to engage our enemies effectively and efficiently. Most people think the military mindset is just to take orders. Sure, that is partly true. However, that military mindset has a purpose. That purpose is to win; that winning is a result of a uniformed force of men and women achieving an objective. When you see the collaboration and interaction within a team of military professionals, it makes me want to use that same type of mentality in my workplace, all of the time.

Cyber intelligence is a move to enable that kind of thinking, and we are already getting there with the adoption of DevOps, agile, and SecDevOps.

Cyber intelligence is something different than what we are already doing, and it will be a challenge to pull off in any organization. However, I recognize that it is an idea that may or may not work for you and your team. This book was just the beginning of a journey to try and explain the concepts.

So, in the end, I offer you this:

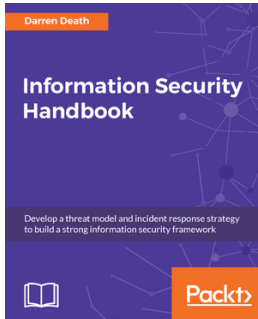
- You and your adversary each have a decision-making cycle (OODA loop). Make your OODA loop smaller and faster by establishing PIRs:
  - Crush your adversaries by being one step ahead
- Utilize what you know (threat intelligence) to disrupt their decision-making cycle by understanding their Cyber Kill Chain:
  - Create chaos (Active Defense) and make it not worth their time

- Develop the intelligence process throughout your organization, PIRs, and enable communication channels back to key stakeholders using F3EAD:
  - Communicate better to decrease exploitation
- Find the weaknesses in your end-to-end processes and decrease potential attack vectors by prioritizing organization projects and using F3EAD:
  - OODA loop and OPSEC
- Create a visualization (through custom dashboards) of processes and identified risks for key stakeholders:
  - After all of the complicated metrics, people want to know if they are good, need improvement, or bad. Keep it simple.
- Establish custom reports that take in data from your different teams to provide actionable items to fix, based on the analysis of risk to the organization:
  - Blasting stakeholders with multiple remediation reports lead to not taking action on the important items. By filtering information from these multiple reports through risk, we can then prioritize items to be work-based.

I hope that this book was as fun for you to read as it was for me to write. I always look forward to constructive criticism of my ideas, as I can only improve on them. Thanks for reading.

# Other Books You May Enjoy

If you enjoyed this book, you may be interested in these other books by Packt:



## **Information Security Handbook**

Darren Death

ISBN: 978-1-78847-883-0

- Develop your own information security framework
- Build your incident response mechanism
- Discover cloud security considerations
- Get to know the system development life cycle
- Get your security operation center up and running
- Know the various security testing types
- Balance security as per your business needs
- Implement information security best practices





## **Cybersecurity – Attack and Defense Strategies**

Yuri Diogenes, Erdal Ozkaya

ISBN: 978-1-78847-529-7

- Learn the importance of having a solid foundation for your security posture
- Understand the attack strategy using cyber security kill chain
- Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence
- Learn how to perform an incident investigation
- Get an in-depth understanding of the recovery process
- Understand continuous security monitoring and how to implement a vulnerability management strategy
- Learn how to perform log analysis to identify suspicious activities

## **Leave a review - let other readers know what you think**

Please share your thoughts on this book with others by leaving a review on the site that you bought it from. If you purchased the book from Amazon, please leave us an honest review on this book's Amazon page. This is vital so that other potential readers can see and use your unbiased opinion to make purchasing decisions, we can understand what our customers think about our products, and our authors can see your feedback on the title that they have worked with Packt to create. It will only take a few minutes of your time, but is valuable to other potential customers, our authors, and Packt. Thank you!

# Index

## A

### Active Defense

- about 63
- automatic 69
- enticement 67
- entrapment 67
- manual 69
- principles 65
- scenarios 68
- tactical level application 70, 72
- types 68

### advanced persistent threat (APT) 65

### AlienVault

- dashboard 101
- pulses 103
- reference 101

### anomalies 196

### asset management/vulnerability scanning asset

- inventory scenario
- about 206
- information gathering 208
- initial phase 208
- local office environment 212
- phase A 210
- phase B 210
- phase C 212
- possible solutions, developing 209
- procedure RASCI (example) 210
- regional data centers 211

## B

### baselines 196

## C

### camp

### setting up, best practices 195

### Capability Maturity Model, continuous monitoring

- about 205
- asset management/vulnerability scanning asset
- inventory scenario 206
- overview 201
- phase A 202
- phase B 203
- phase C 204
- security awareness/continuous monitoring/IT
- helpdesk scenario 214

### Capability Maturity Model, incident response

- about 228
- initial phase 228
- phase A 229
- phase B 230
- phase C 231

### Capability Maturity Model, InfoSec and cyber

- intelligence
- initial phase 175
- phase A 176
- phase B 177
- phase C 178

### Capability Maturity Model, security awareness

- about 186
- initial phase 187
- phase A 187
- phase B 188
- phase C 190
- phase C + 191, 192

### Capability Maturity Model, threat intelligence

- about 98
- levels 98

### Capability Maturity Model, vulnerability

- management
- fix 252
- fix, initial phase 254

- fix, phase A 255
- fix, phase B 256
- fix, phase C 258
- phase B 251
- phase C 252
- reporting 248
- reporting, initial phase 248
- reporting, phase A 250
- scanning 242
- scanning, initial phase 243
- scanning, phase A 245
- scanning, phase B 246
- scanning, phase C 247
- Capability Maturity Model
  - final risk phase 268
  - gap 180
  - initial risk phase 266
  - open source governance risk and compliance tools 270
  - risk reporting, improving 267, 269
- chief information security officer (CISO) 7
- collaboration capability
  - communication and cyber intelligence process 126
  - formal communications 125
  - informal communications 126
  - methods and tools 128
  - purpose 124
- collaboration, at operational level 147, 148
- collaboration, at strategic level
  - about 131
  - architecture 134
  - dependencies 134
  - executive support 133
  - intelligence aggregation 137
  - intelligence reconciliation and presentation 138
  - policies and procedures 133
  - prioritized information 136
- collaboration, at tactical level
  - about 140
  - priority information requirements 140
  - tactical dashboard, creating 144
  - theory application 141
  - theory, versus reality 143
- Combined Enterprise Regional Information
  - Exchange System (CENTRIX) 264
  - Common Vulnerabilities and Exposure (CVE) 236
  - Common Vulnerability Scoring System calculator
    - about 236
    - base metric group 236
    - base scoring 239
    - environmental metric group 238
    - metrics madness 240
    - reference 240
    - temporal metric group 238
  - communications intelligence (COMINT) 12
  - continuous monitoring 197, 198, 199, 200
  - core security service
    - metrics 151
  - cyber intel integration
    - about 166
    - data integration challenges 170
    - graphical representation 169
    - red team constraints 168
    - red team methodology 166
    - testing methods 167
  - cyber intel program roles, at operational level
    - cyber intelligence analysts 60
    - IT leadership 60
  - cyber intel program roles, at strategic level
    - cyber intelligence program officer 58
    - IT leadership 57
  - cyber intel program roles, at tactical level
    - cyber intelligence program manager 59
    - IT leadership 58
  - cyber intel program roles
    - about 56
    - at operational level 60
    - at strategic level 57
    - at tactical level 58
  - cyber intelligence capability
    - integration, purpose 150
  - cyber intelligence
    - about 8, 182
    - drives operations 15
    - events, mapping to InfoSec capabilities 184
    - incidents, mapping to InfoSec capabilities 184
    - intel history 9, 10
    - logic 182
    - need for 6

- types 10
- using, in military 8
- Cyber Kill Chain
  - about 64
  - and F3EAD process 87
  - and OODA loop 87
  - and OPSEC 89
  - breach phase 64
  - F3EAD process 92
  - intelligence cycle 91
  - intrusion phase 64
  - preparation phase 64
- cyber threat intelligence 8

## D

- data integration challenges
  - about 170
  - end user perspective 170
  - service level perspective 171
  - SOC perspective 173

### Digg

- reference 114

- dissemination, intelligence cycle
  - about 40
  - architecture 42
  - channels 41
  - methods 40
  - modes 42

## E

- electronic intelligence (ELINT) 12
- event 183

## F

- F3EAD process
  - about 79, 81
  - and Cyber Kill Chain 87
  - application, in commercial space 92
  - limitations 93
  - using 81, 86
- Feeder
  - reference 114
- Feedly
  - reference 114

- Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD) process 74
- foreign instrumentation signals intelligence (FISINT) 13

## G

- G2Reader
  - reference 114
- GOSINT platform
  - reference 116
- governance, risk, and compliance (GRC) tools 270

## H

- human intelligence (HUMINT) 10

## I

- image intelligence (IMINT) 11
- incident 184
- incident response process
  - and F3EAD integration 226
  - containment phase 225
  - detection and analysis phase 225
  - eradication phase 225
  - integrating, with intelligence process 227
  - overview 223
  - post-incident activity 225
  - preparation and prevention phase 224
  - recovery phase 225
  - reference 224
- Indicators of Compromise (IoCs) 97
- industrial control system (ICS) 107
- information hierarchy 30, 31
- information requirements (IRs) 34
- Information Sharing and Analysis Center (ISAC) 37
- Inoreader
  - reference 114
- intelligence cycle
  - about 32
  - analysis and production step 39
  - collection step 38
  - dissemination 40
  - Planning and Direction phase 33
  - processing step 39
  - utilization 43

## **J**

Joint World-Wide Intelligence Communications System (JWICS) 264

## **K**

Key Performance Indicators (KPIs) 16, 155

Key Risk Indicators 72

## **L**

levels, Capability Maturity Model

collection capability 99

threat information integration 118

like services

integrating 163

## **M**

Malware Information Sharing Platform (MISP)

reference 116

maneuver warfare

about 22, 23

center of gravity 26

collaboration 28

critical vulnerability 26

decentralized command 28

flexibility 28

OODA Loop 25

opportunity, exploring 27

process 22

tempo 23

measurement and signature intelligence (MASINT)

about 11

reference 11

medical intelligence (MEDINT) 13

methods and tools for collaboration

key risk indicators, using 129

organizational level agreements 128

responsible accountable supporting consulted

informed (RASCI) matrix 129

service level agreements 128

## **N**

networks

differentiating 264

NewBlur

reference 114

Non-Classified Internet Protocol Network  
(NIPRNet) 264

## **O**

OPDEC

applying, in business environment 55

open source governance risk and compliance tools

binary risk assessment 270

practical threat analysis, for information security  
experts 270

Security Officers Management and Analysis

Project, reference 271

SimpleRisk 271

STREAM cyber risk platform 270

open source intelligence (OSINT) 11

operational security

about 51

appropriate countermeasures, applying 54

assessment of risk 52

critical information , identifying 51

threat analysis 52

vulnerabilities analysis 52

operations 45

## **P**

personal identifiable information (PII) 68

Planning and Direction phase, intelligence cycle

intelligence effort, directing 35

intelligence support system, planning 37

requirements development 34

requirements management 34

requirements satisfaction 36

principles, Active Defense

annoyance 66

attribution 66

Priority Information Requirements (PIRs) 15

procedures 65

## **R**

risk appetite 262

risk levels

high 54

- low 54
- medium 54
- risk tolerance 262
- risk
  - about 264
  - acceptance 262
  - appetite 262
  - avoidance 262
  - mitigation 262
  - overview 261
  - remediation 262
  - tolerance 262
  - transference 262
  - treating 261

## S

- Secret Internet Protocol Network (SIPRNet) 264
- security 45
- security awareness/continuous monitoring/IT
  - helpdesk scenario 218
  - about 215
  - information, gathering 216
  - initial phase 216
  - phase A 217
  - possible solutions, developing 217
- Security Configuration Management
  - about 156, 272
  - core processes 158
  - data exposure and sharing 161
  - discovery and detection 159
  - key risk indicators, working 276
  - risk management, developing 274
  - risk mitigation 159
  - Security State Analysis 160
- security incident event monitoring (SIEM) 70
- Security Operations Center (SOC)
  - about 153
  - spider 154
  - team capabilities 155
- signals intelligence (SIGINT) 12
- source intelligence 14
- strategic cyber intelligence capability
  - developing 46
  - level 1 50
  - priorities 47

## T

- tactical level Active Defense
  - application 70, 72
- tactics 65
- targeting process
  - about 75
  - business target examples 76
  - S.M.A.R.T., using 76
- technical intelligence (TECHINT) 13
- techniques 65
- testing methods
  - black box 167
  - gray box 167
  - white box 167
- The Old Reader
  - reference 114
- The Open Group Architecture Framework (TOGAF)
  - about 47
  - architectures 48
  - business architecture 48
  - cyber intelligence 48
  - data/application architecture 48
  - technology architecture 48
- theory
  - practising 19, 20
- things
  - labeling 263
- threat information integration
  - initial phase 119
  - intelligence package, categorization 121
  - phase A 120
  - phase B 121
  - phase C 122
- threat intelligence collection capability
  - AlienVault example 100, 103, 105, 106
  - GOSINT platform example 116
  - Information Sharing and Analysis Centers
    - example 111
  - initial phase 100
  - Malware Information Sharing Platform (MISP)
    - project 116
  - news alert notifications 112
  - phase A 114
  - phase B 116

phase C 117

Rich Site Summary (RSS) feeds 113

Twitter example 107

threat intelligence integration

review 265

threat intelligence

about 95

customizing 223

reference 96

TweetDeck

reference 108

## V

vulnerability management (VM)

about 163, 235, 236

overview 240, 242