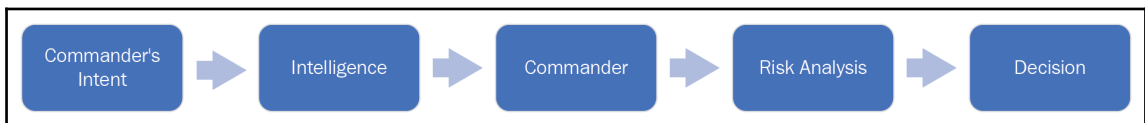
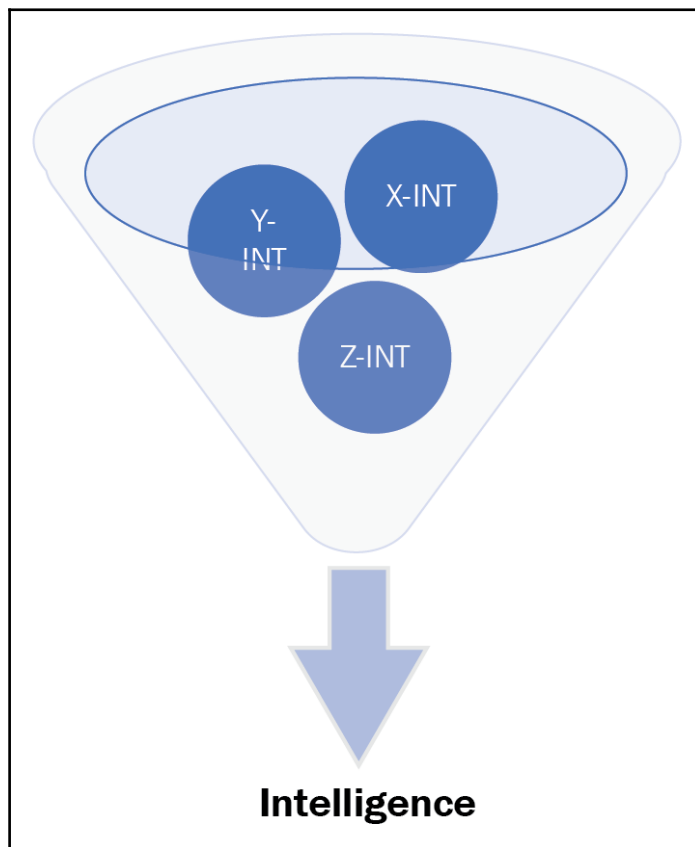
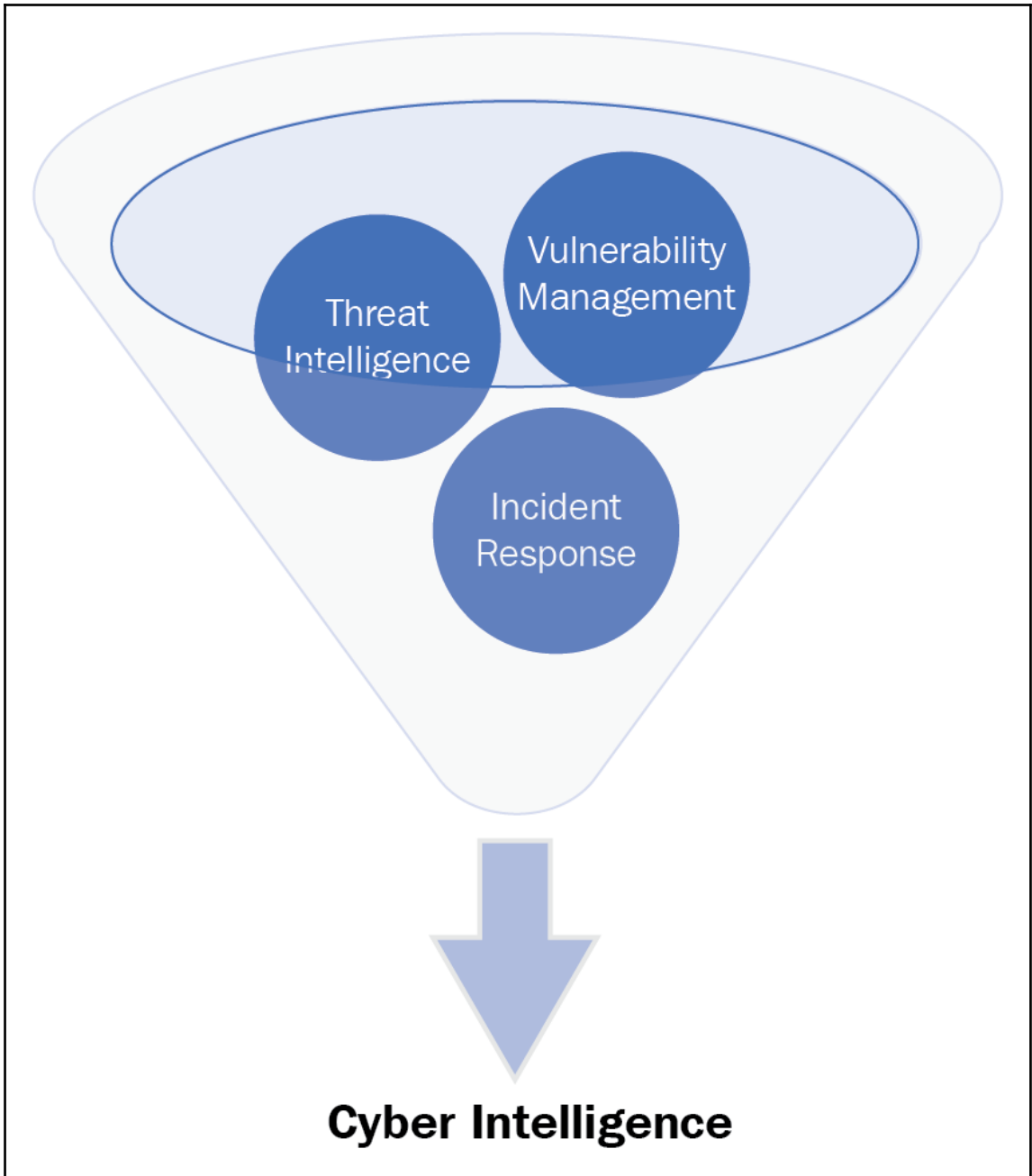
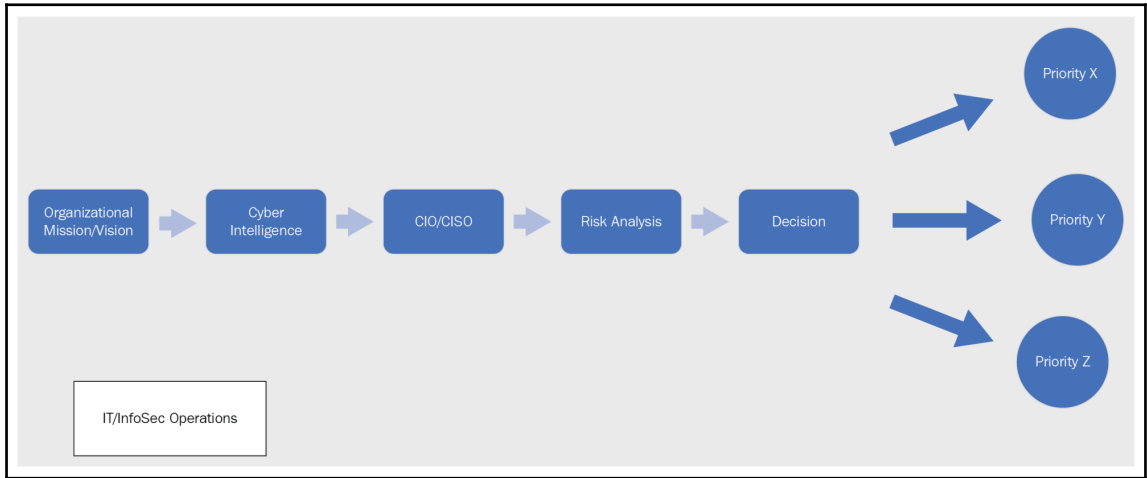
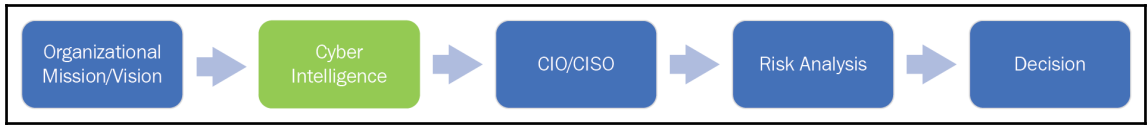


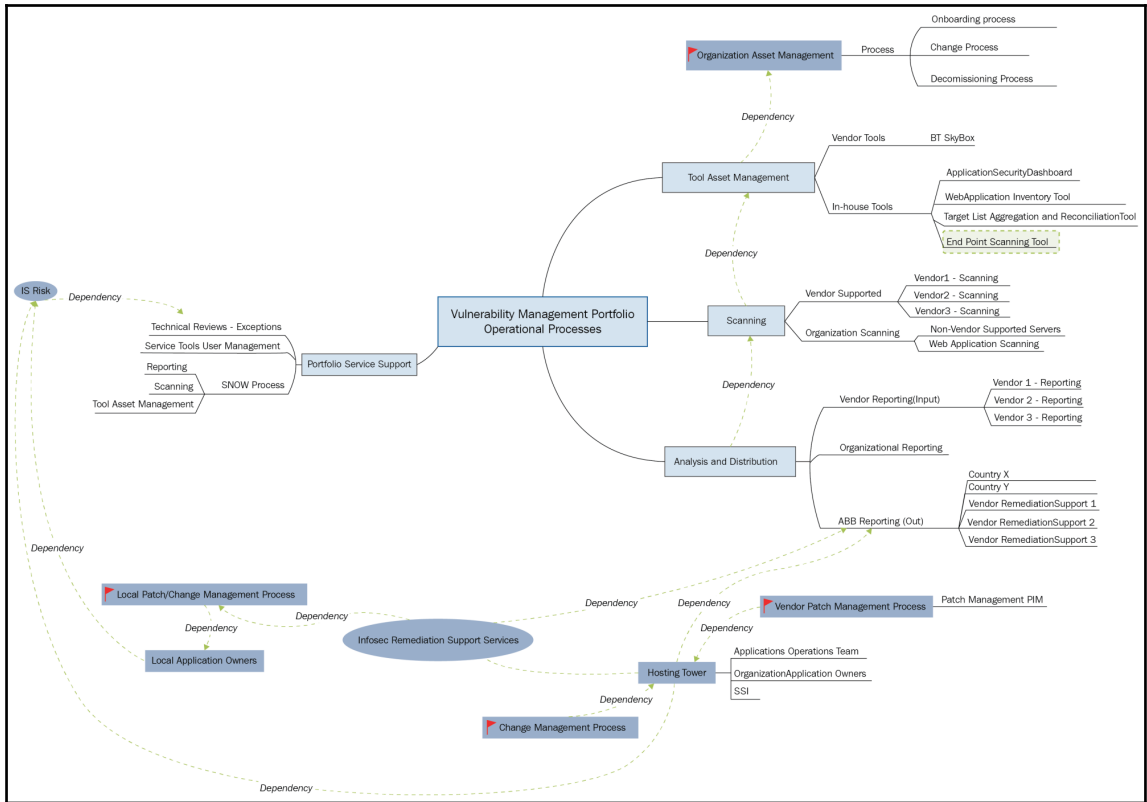
# Chapter 1: The Need for Cyber Intelligence

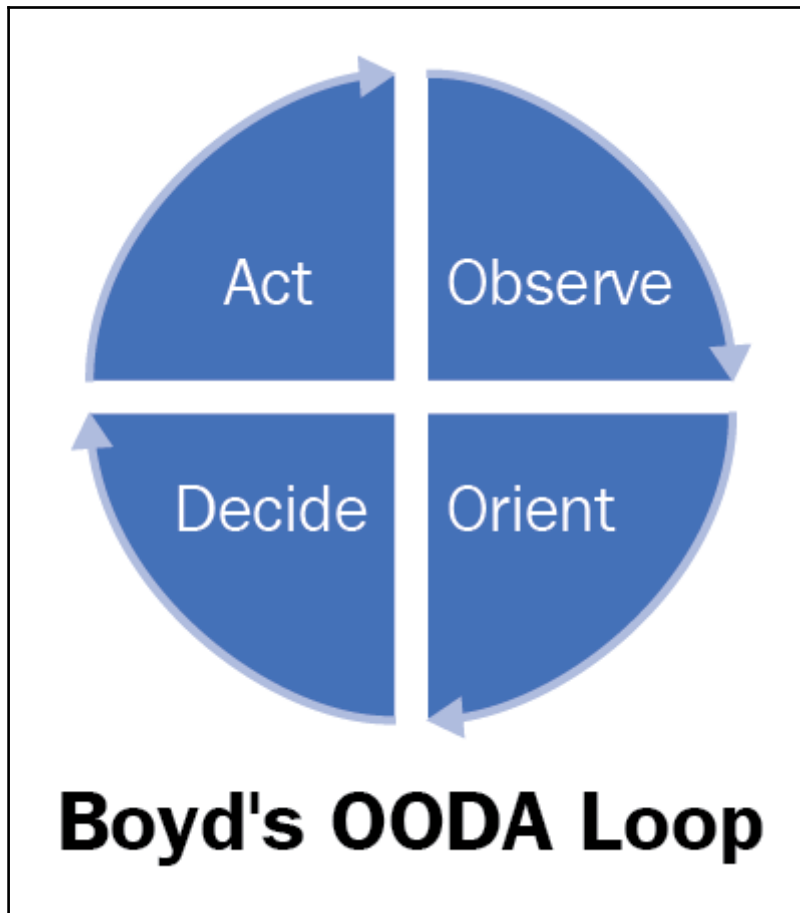




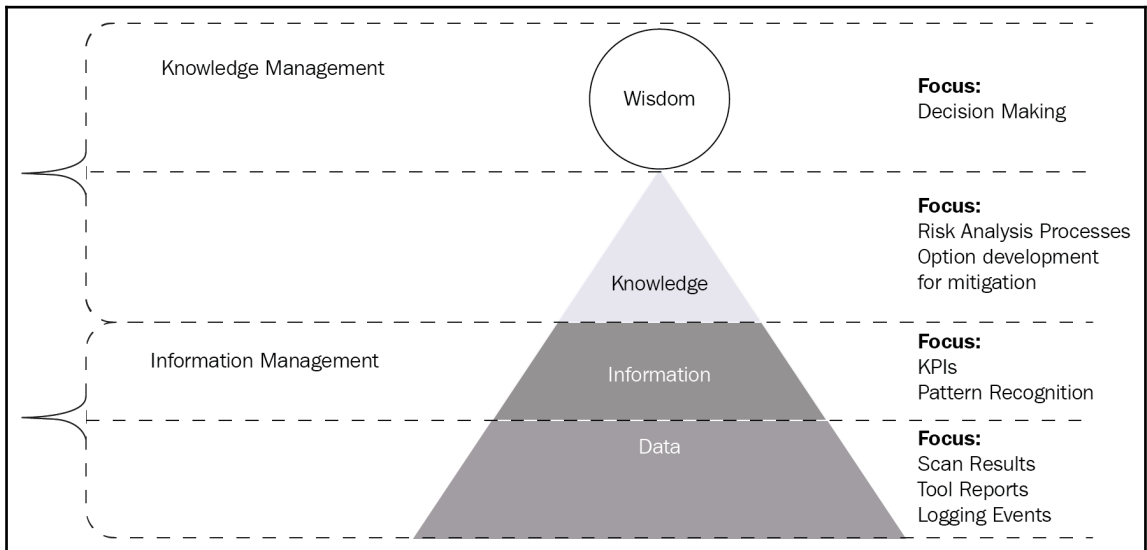
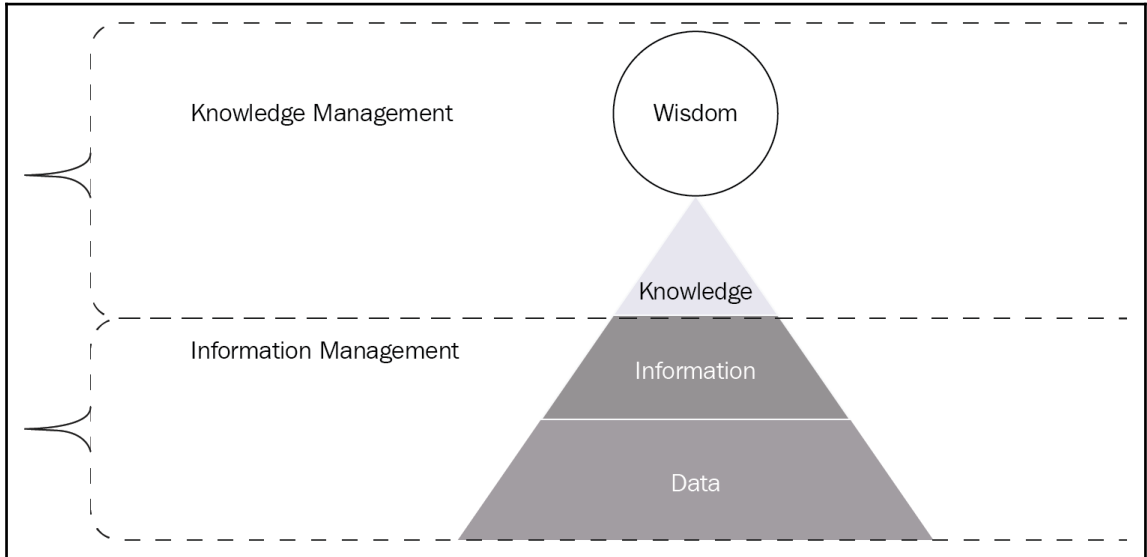


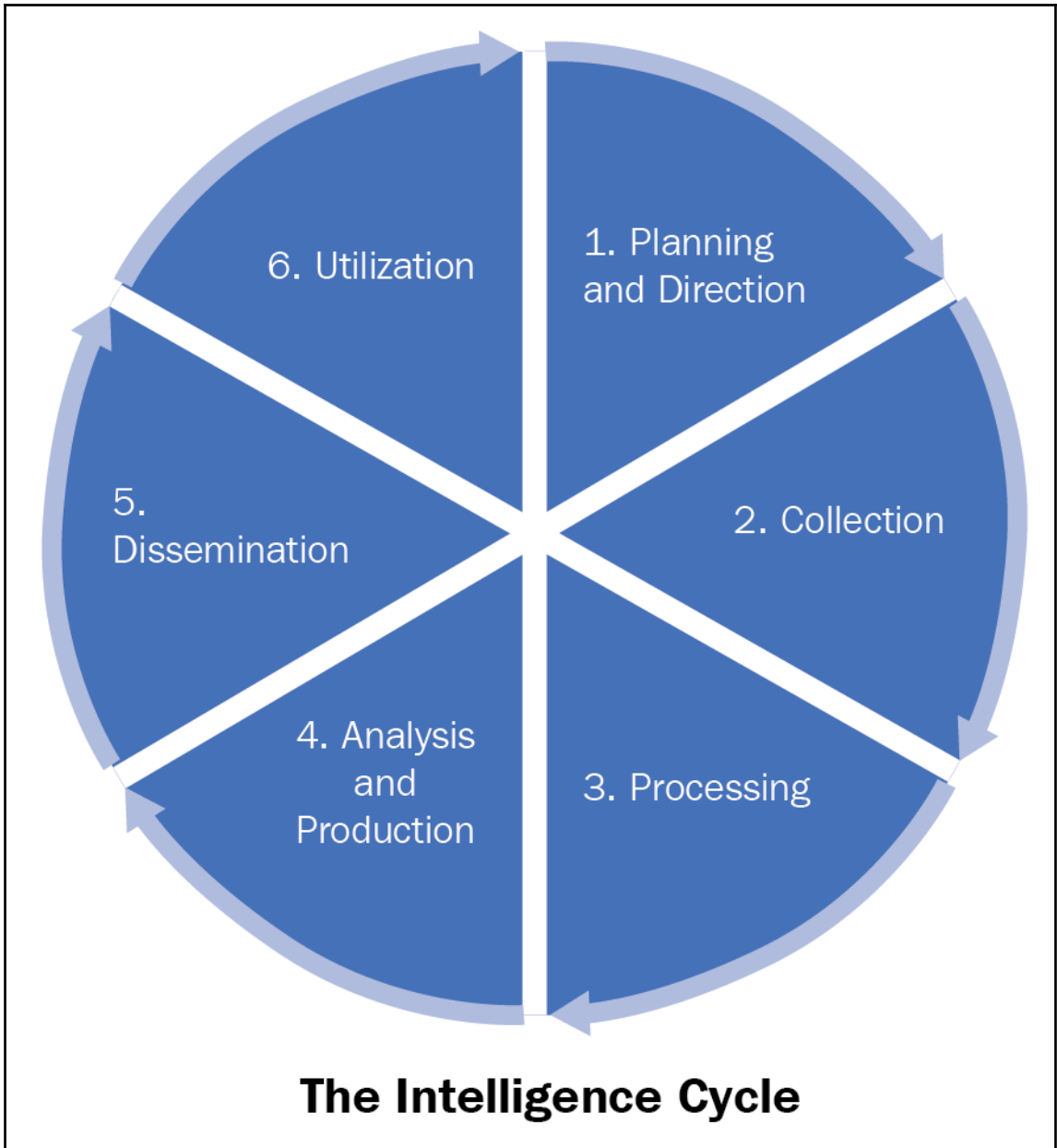




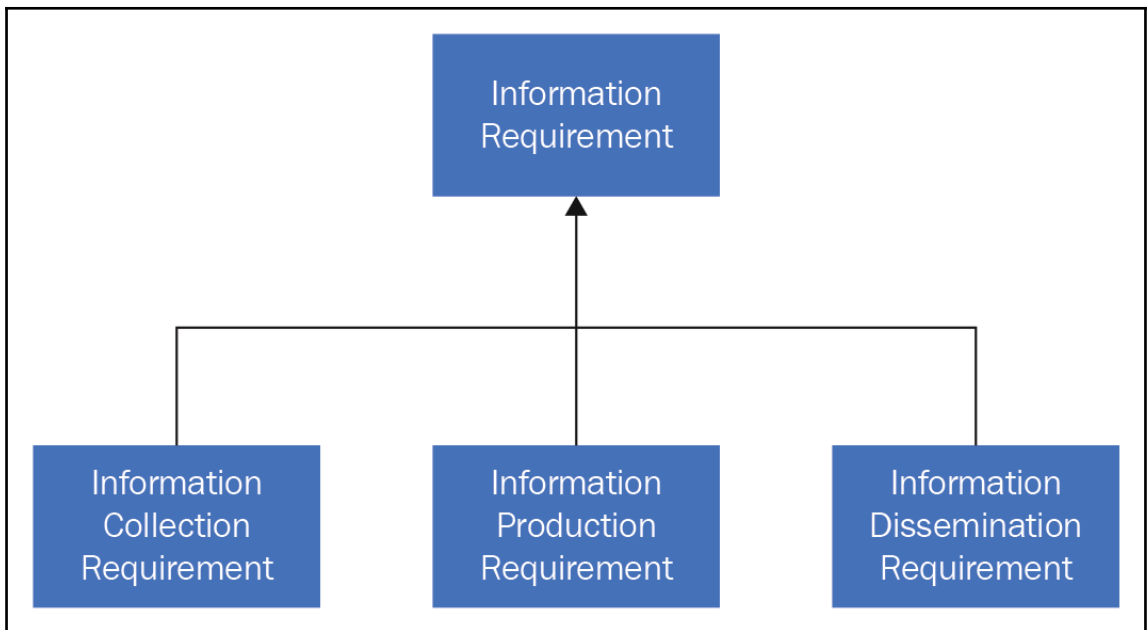
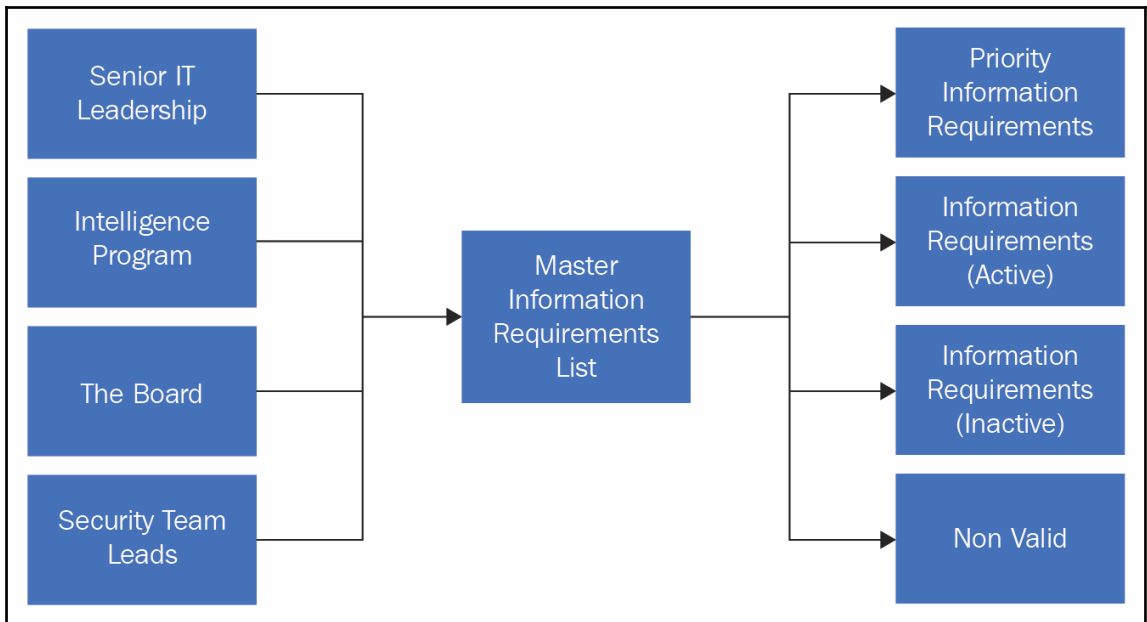


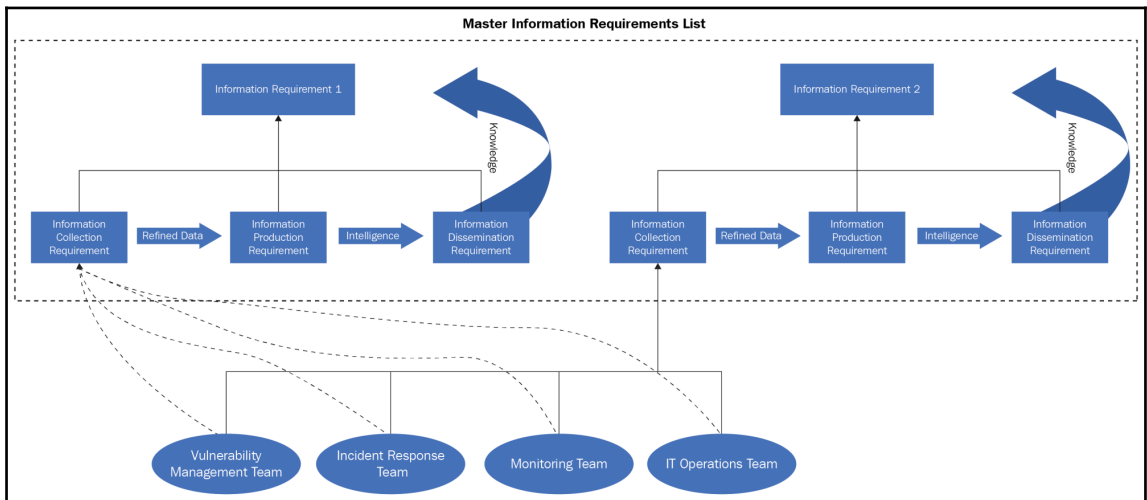
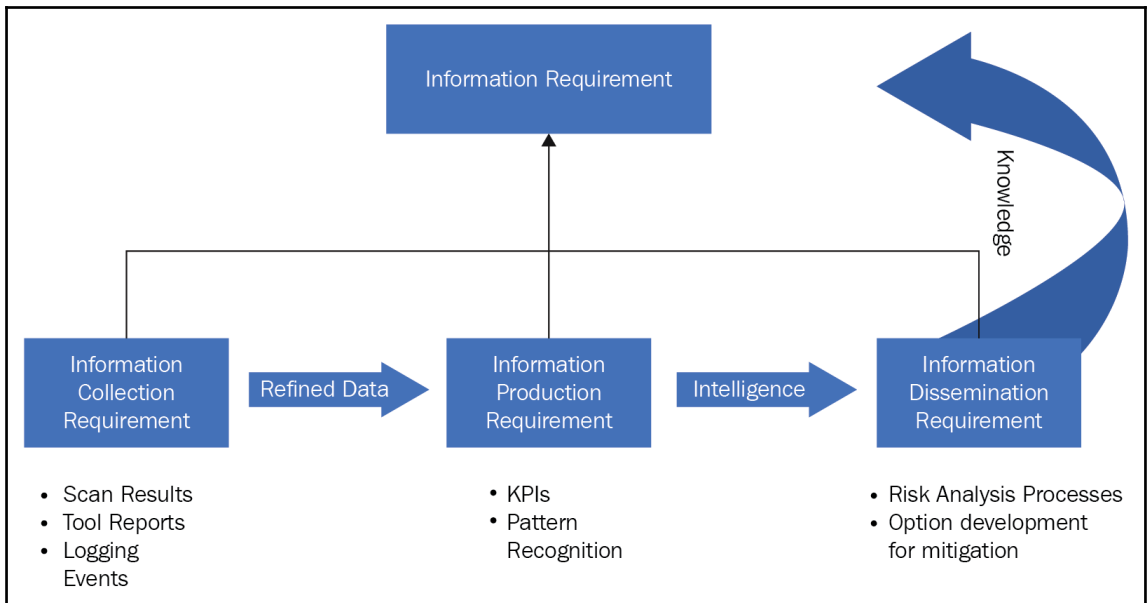
## Chapter 2: Intelligence Development

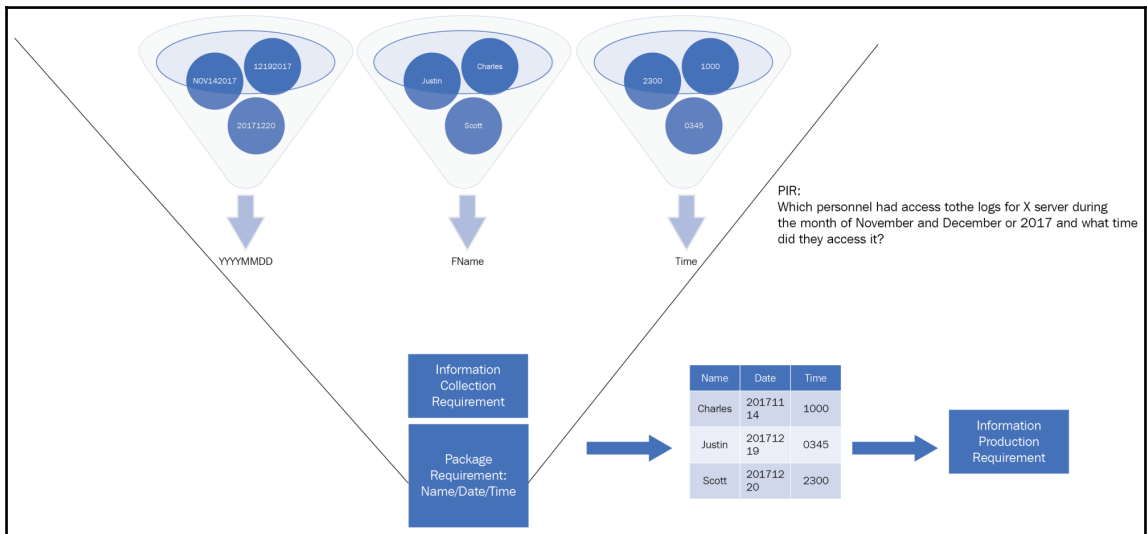
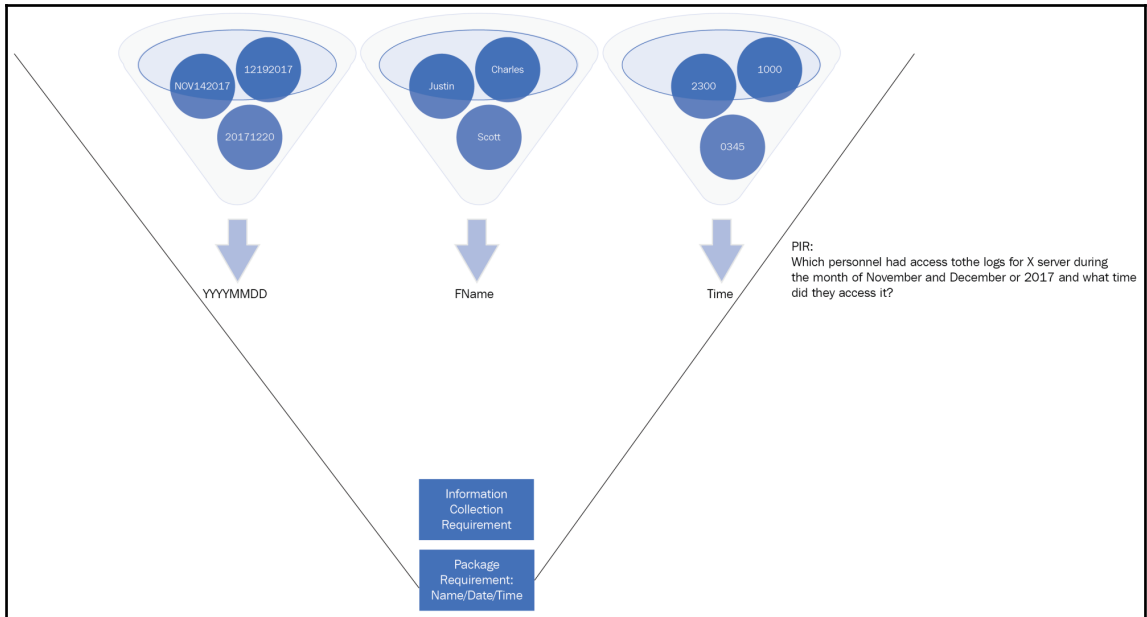


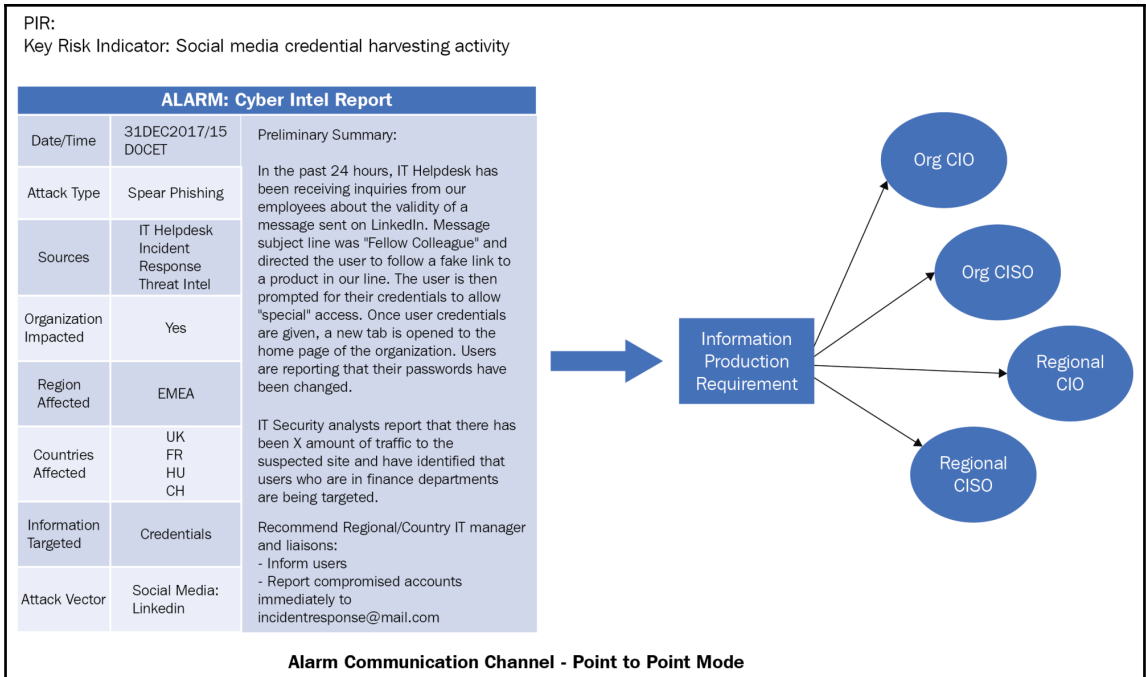
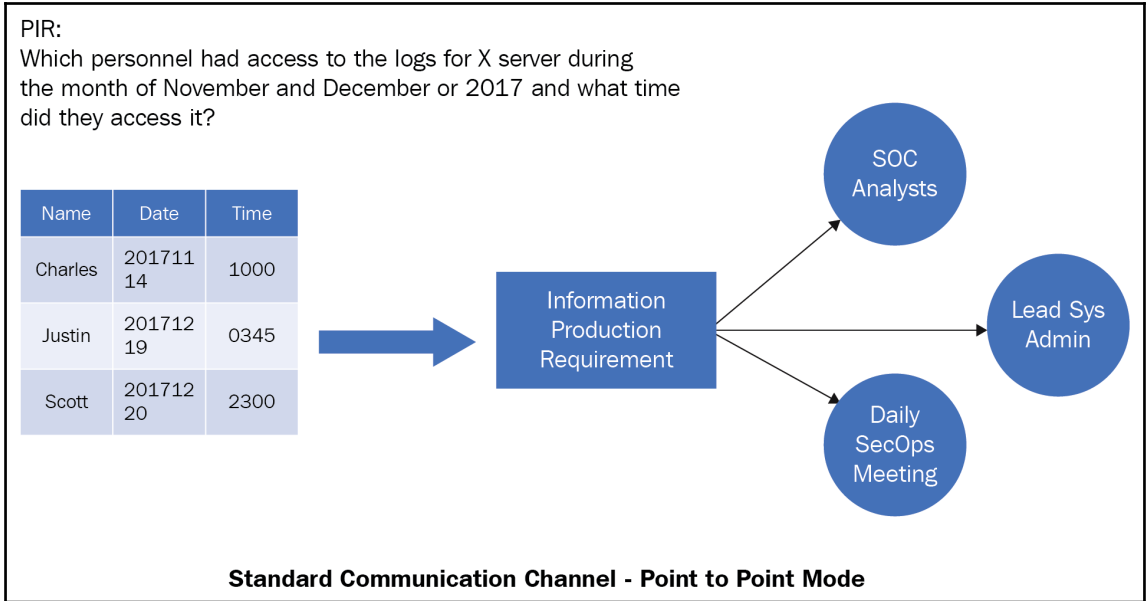


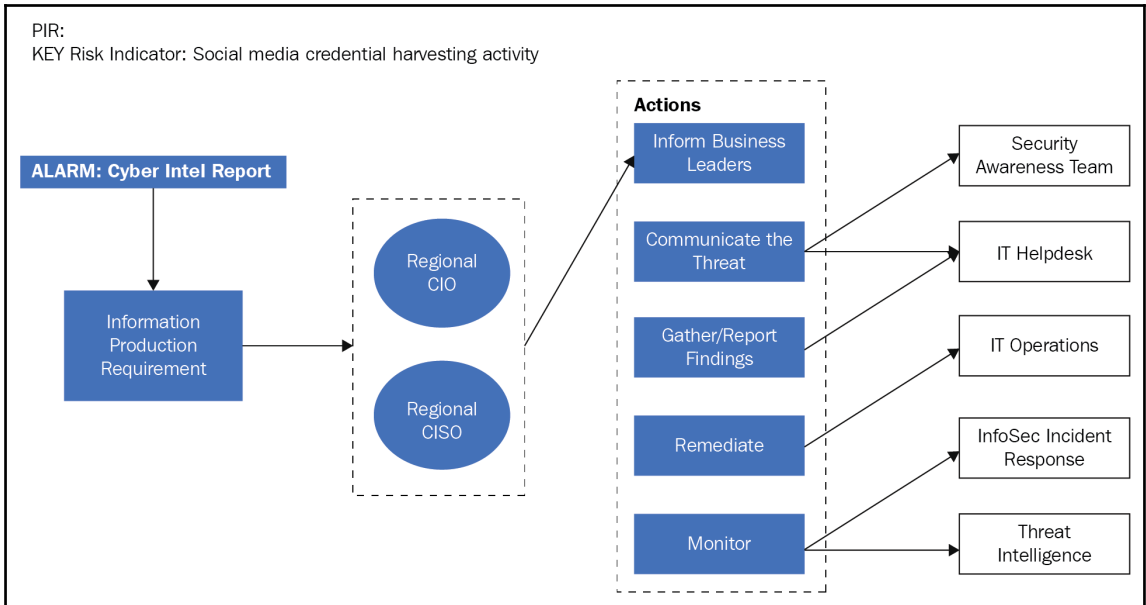




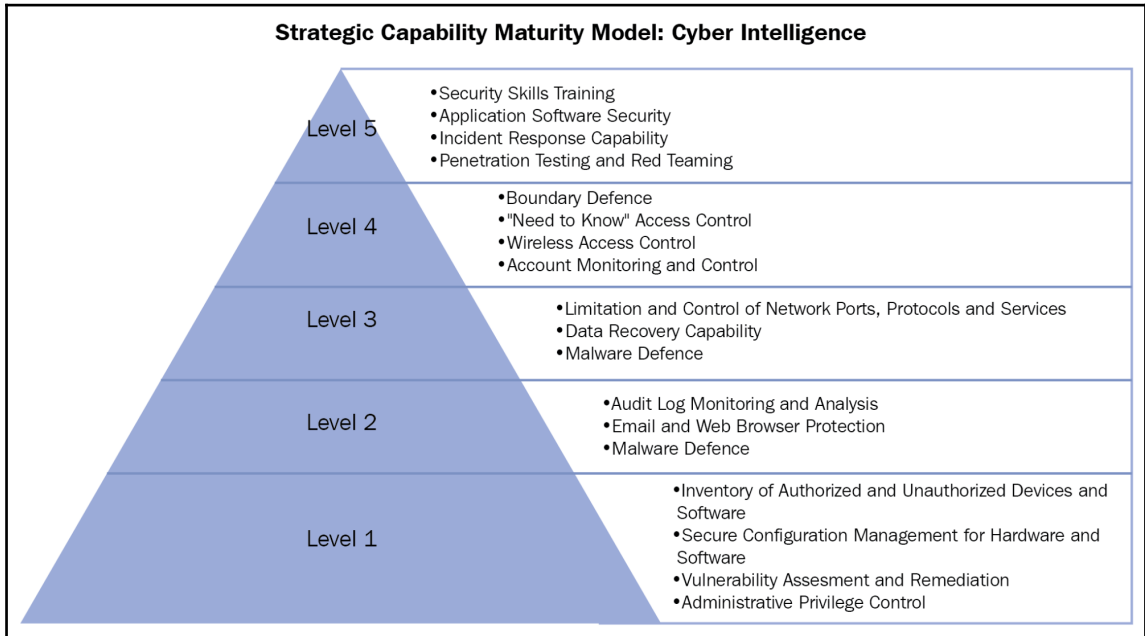


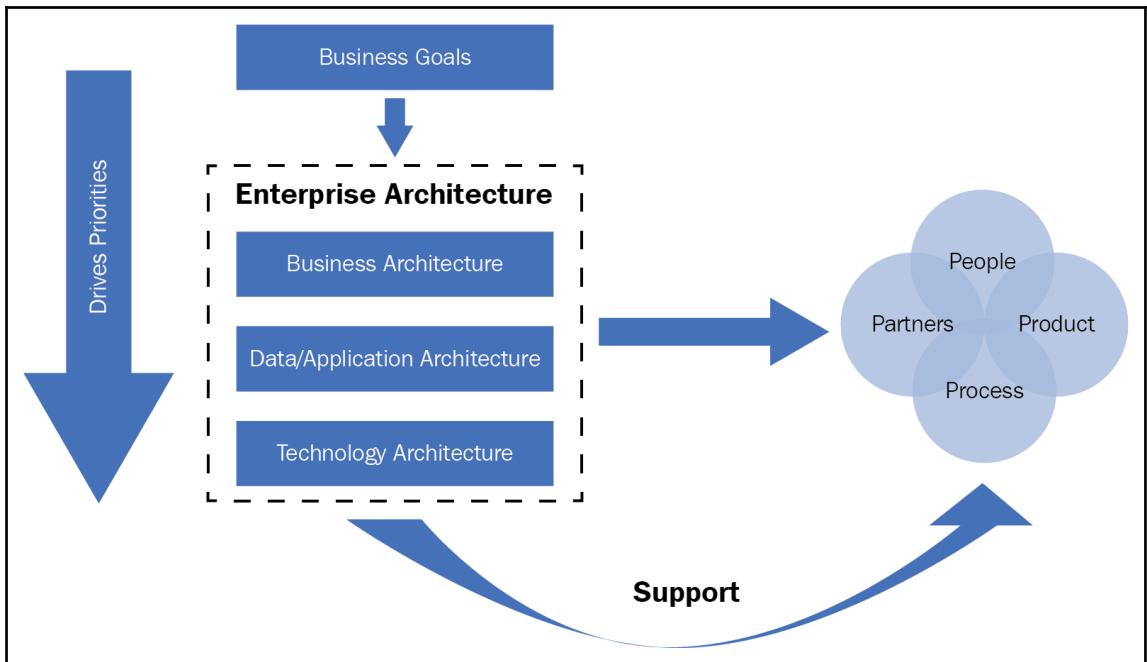






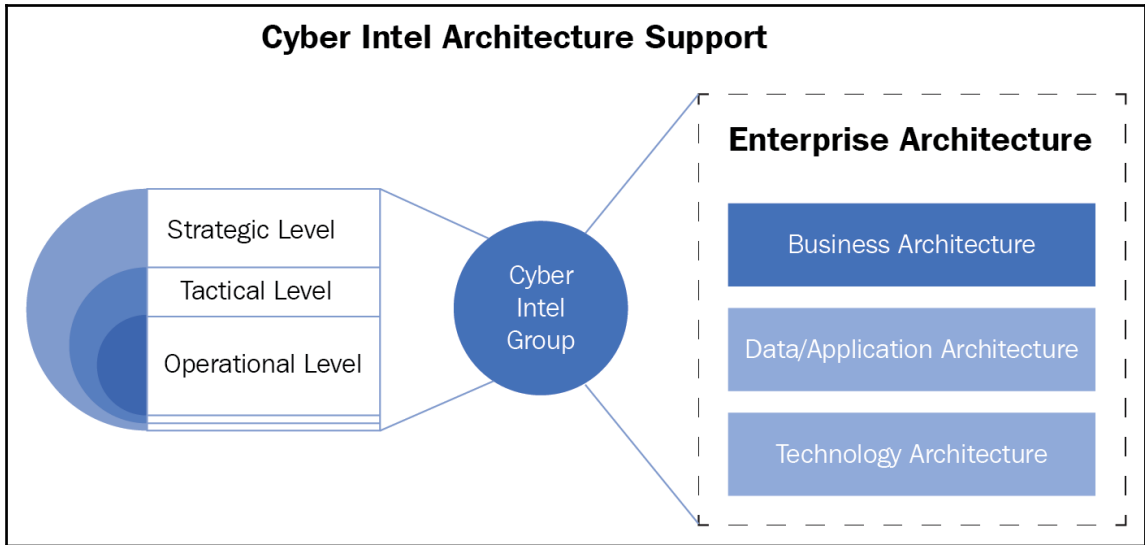
# Chapter 3: Integrating Cyber Intel, Security, and Operations



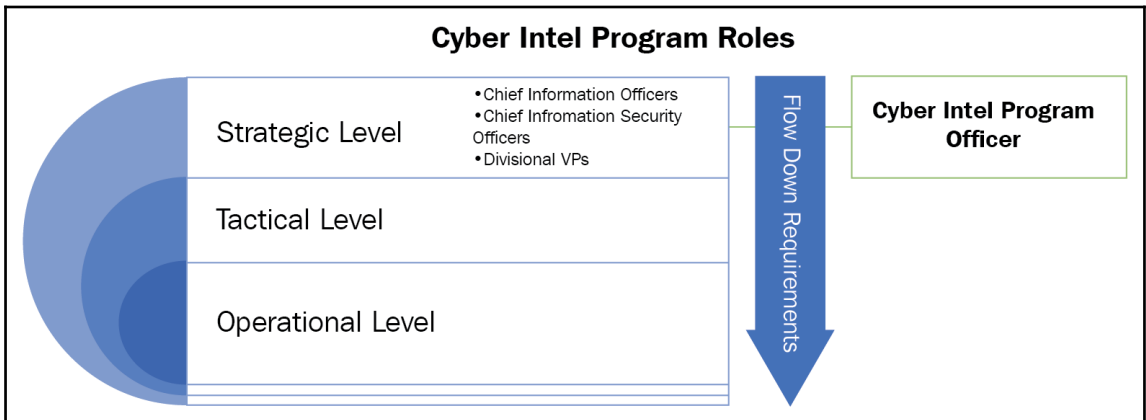
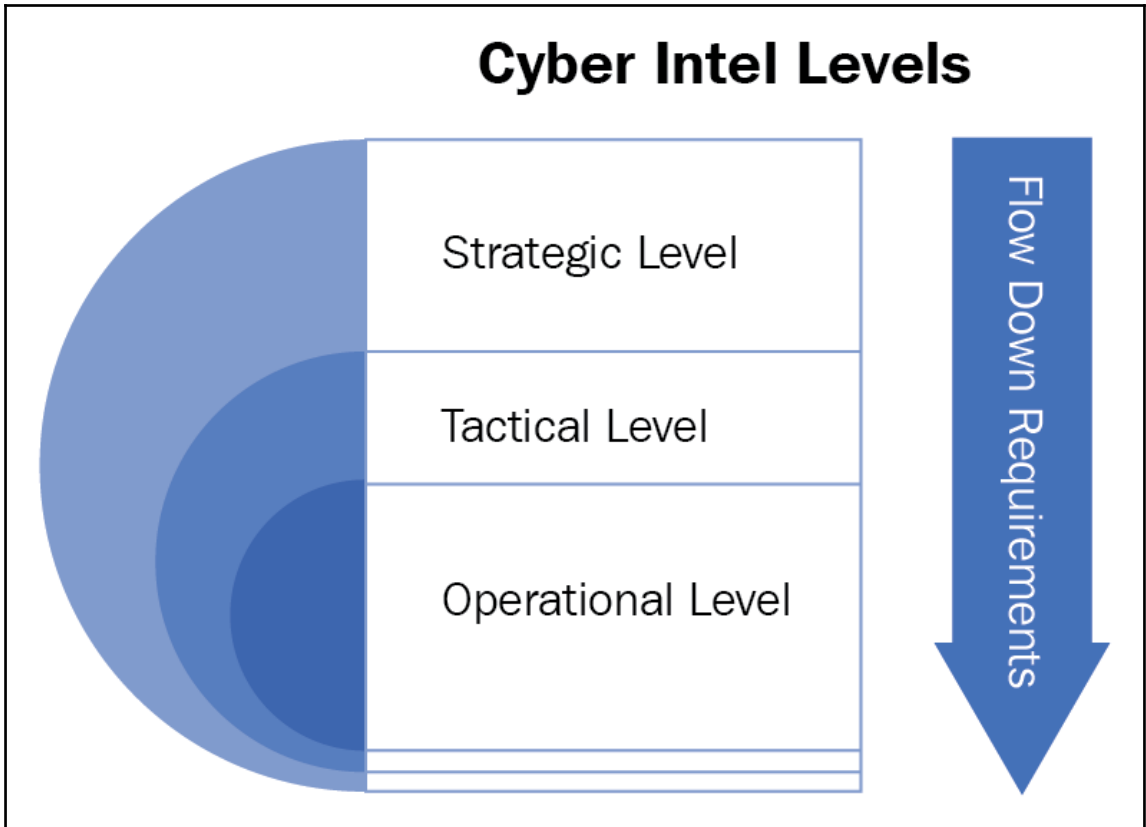


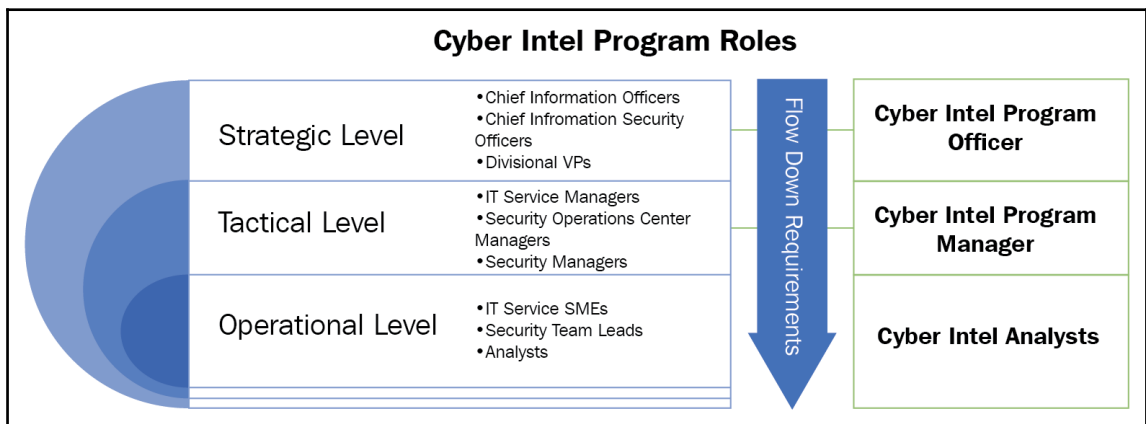
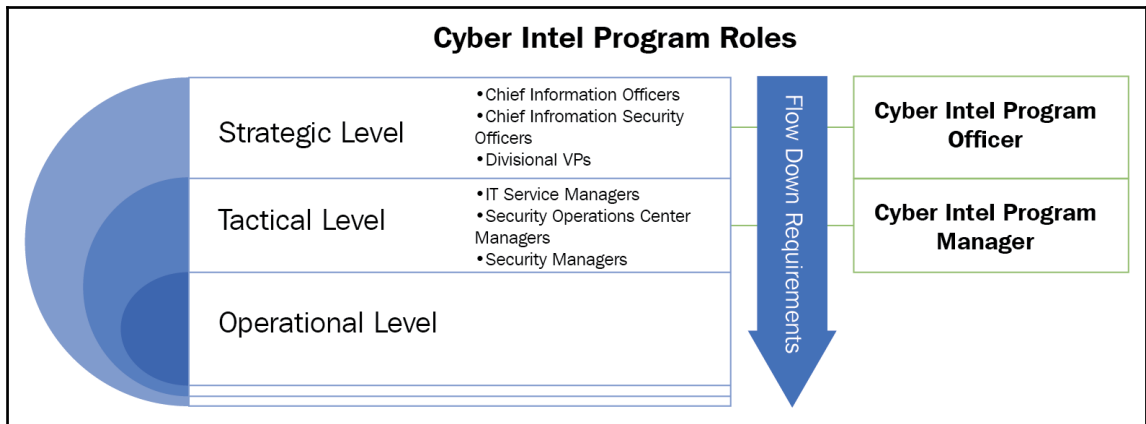
**Example Risk Matrix**

		Impact →				
		Negligible	Marginal	Moderate	Critical	Catastrophic
Probability ↑	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

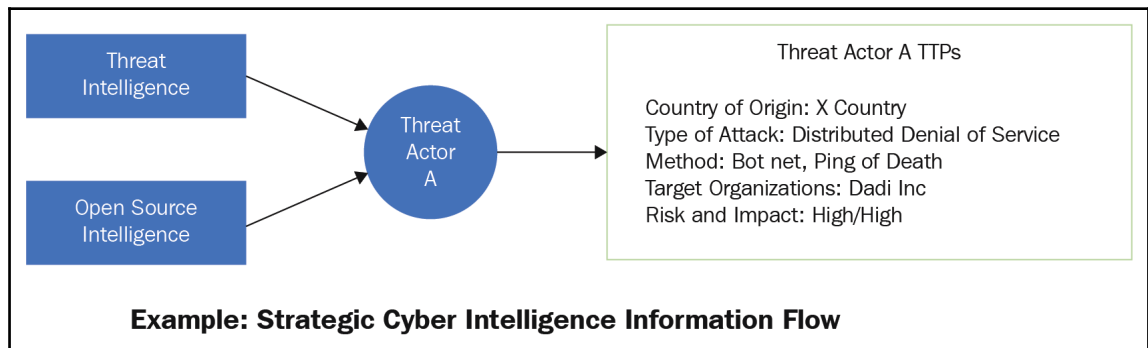
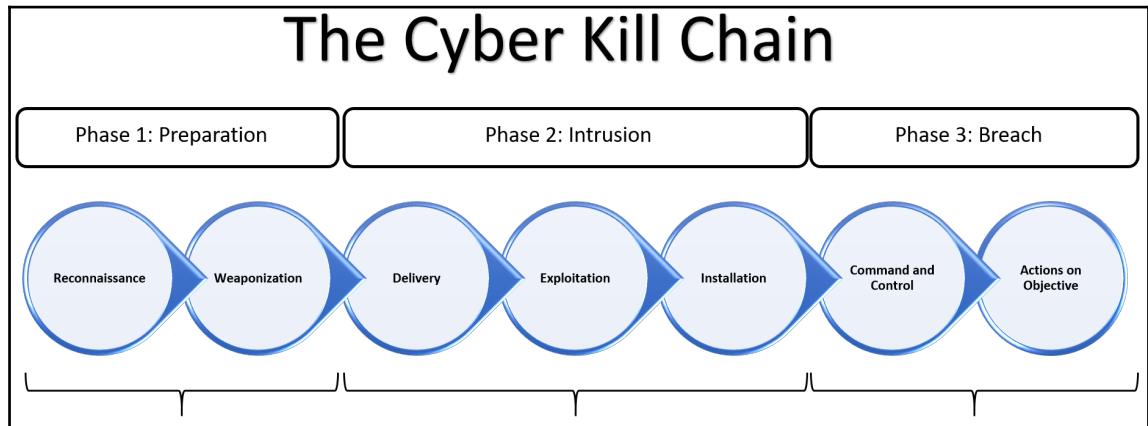


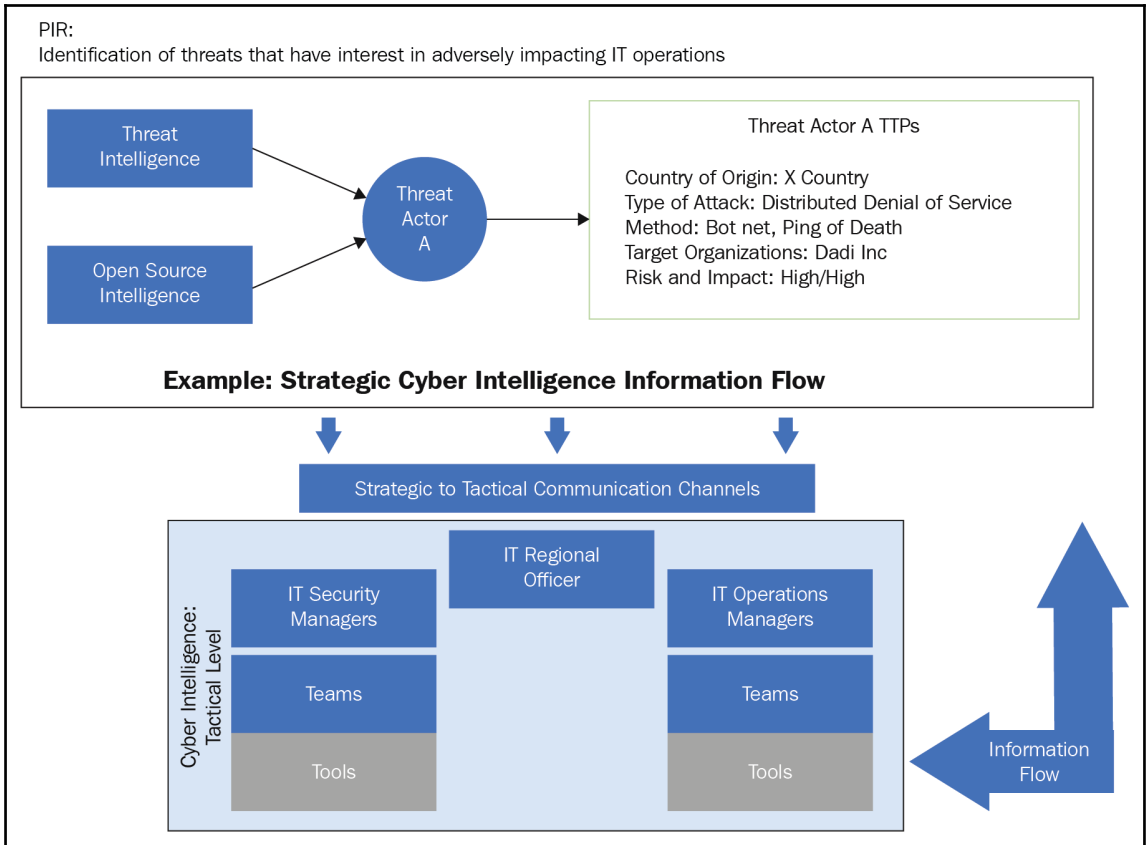




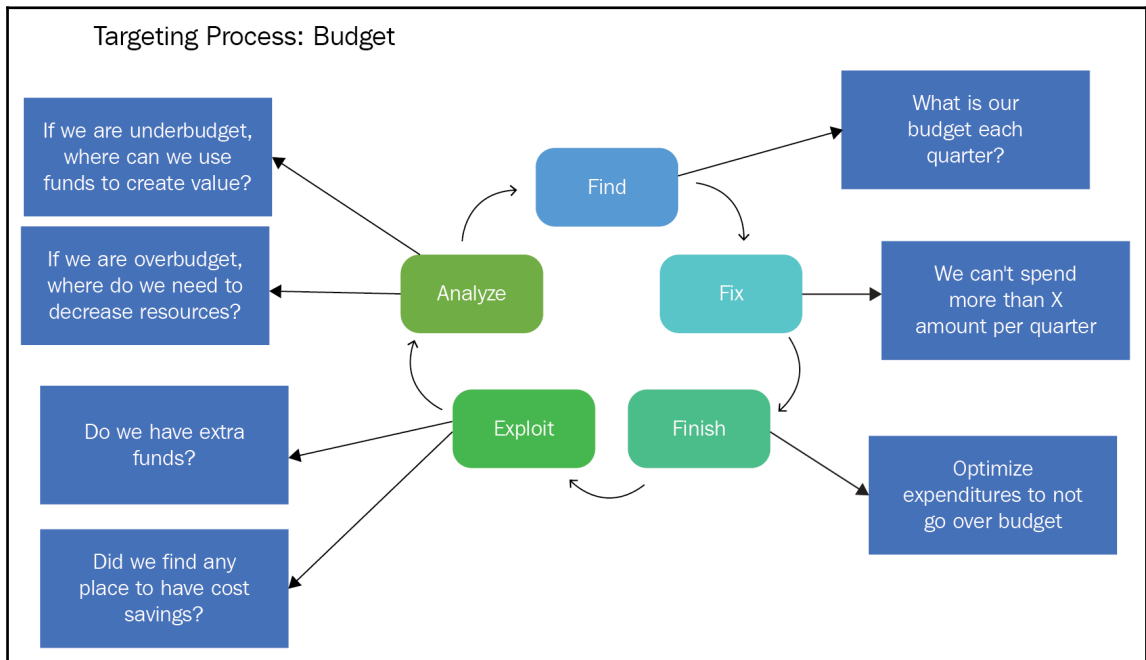
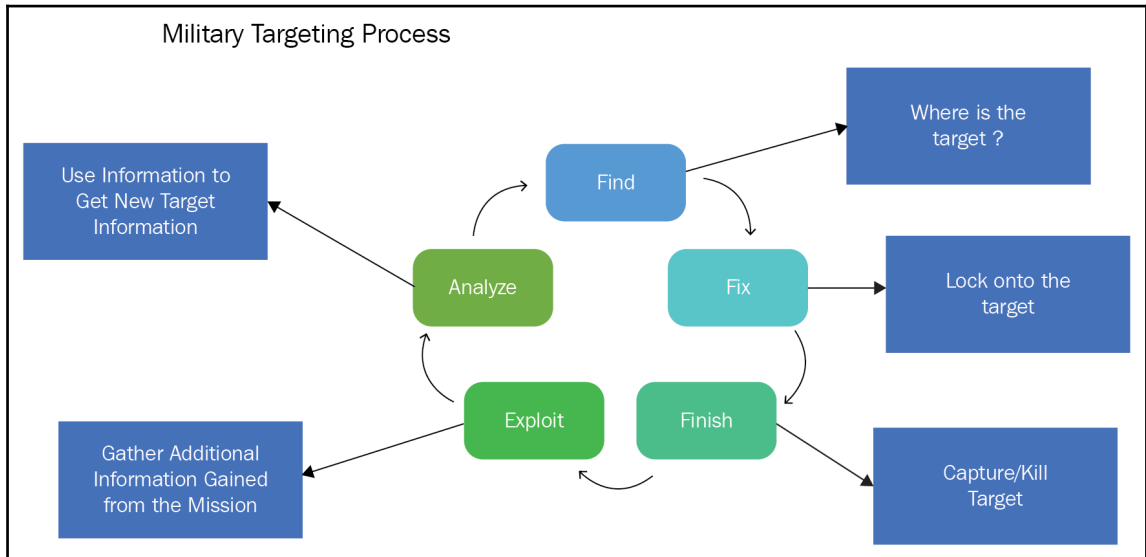


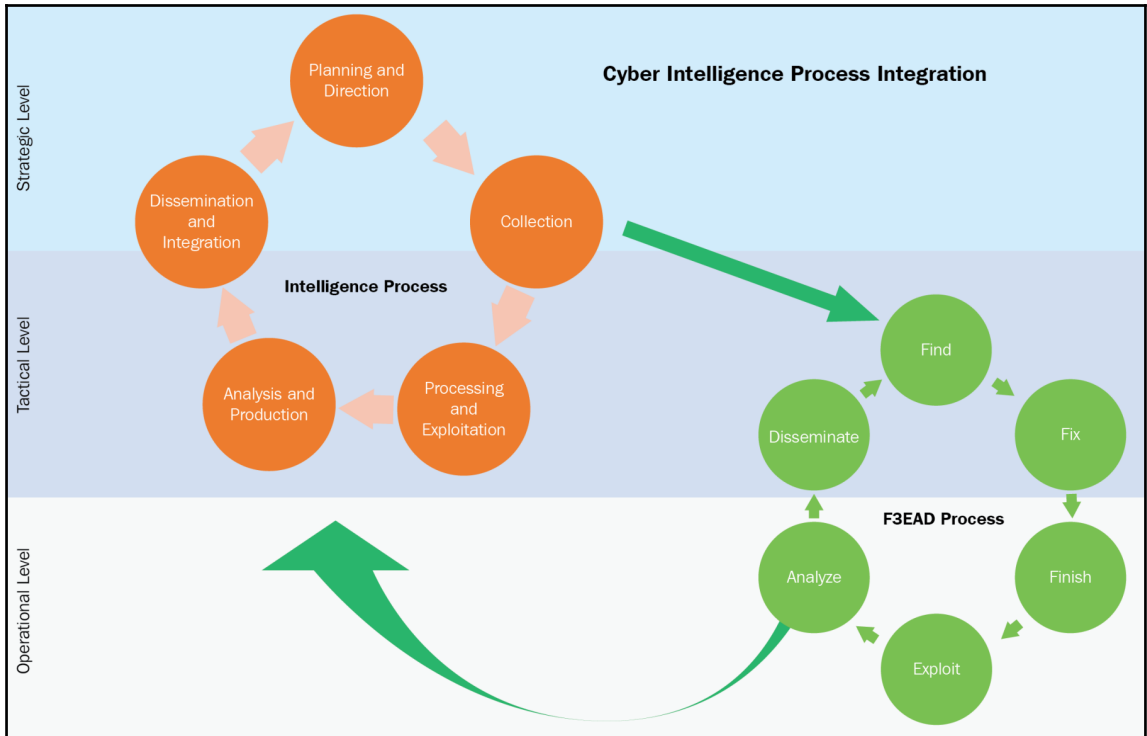
# Chapter 4: Using Cyber Intelligence to Enable Active Defense

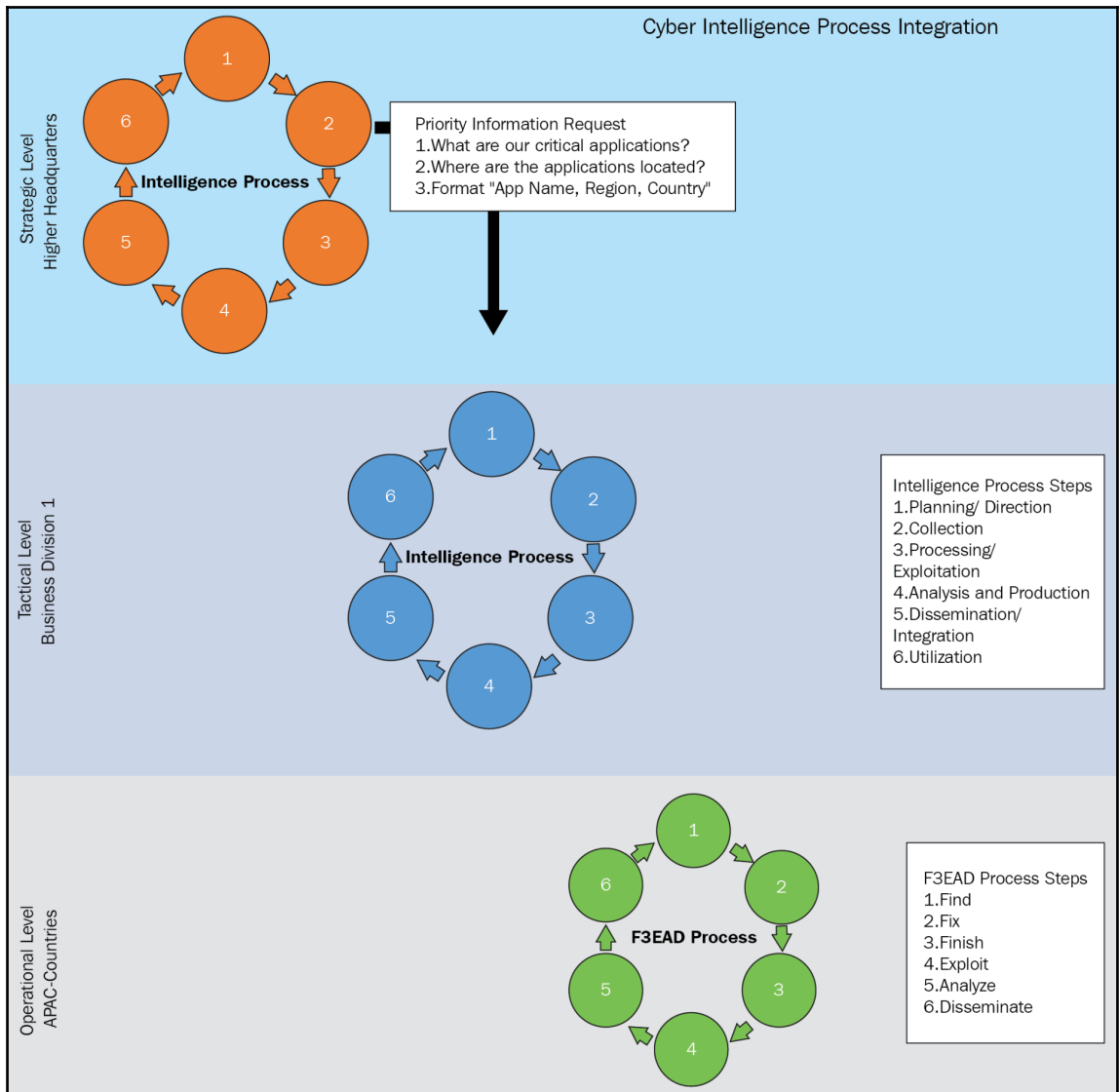


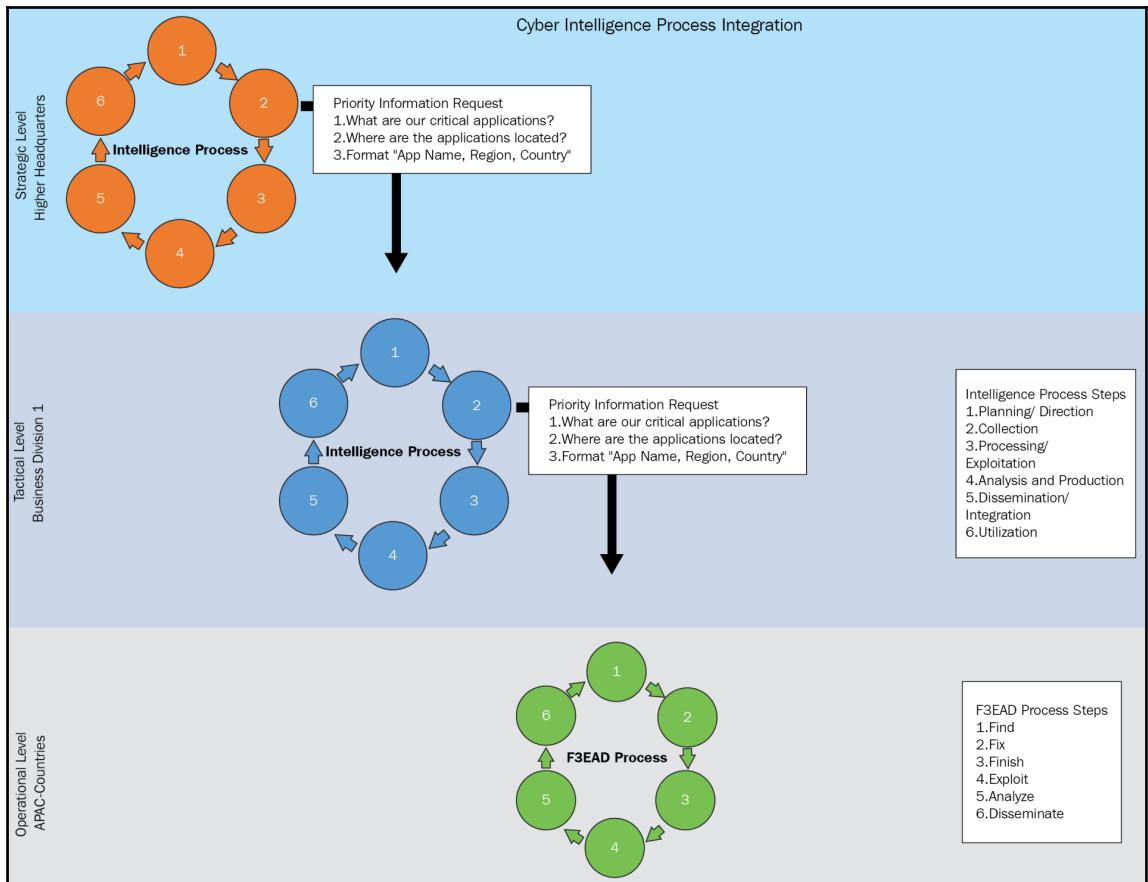


## Chapter 5: F3EAD for You and for Me

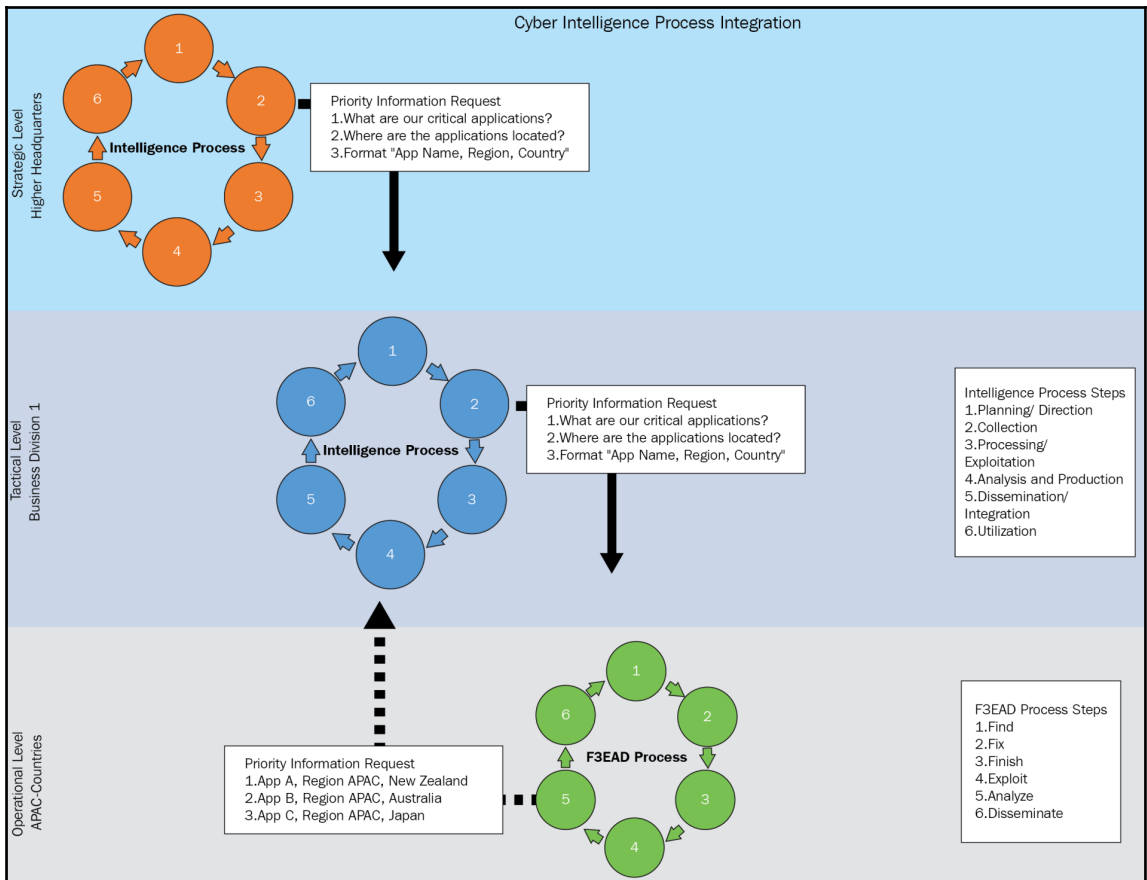


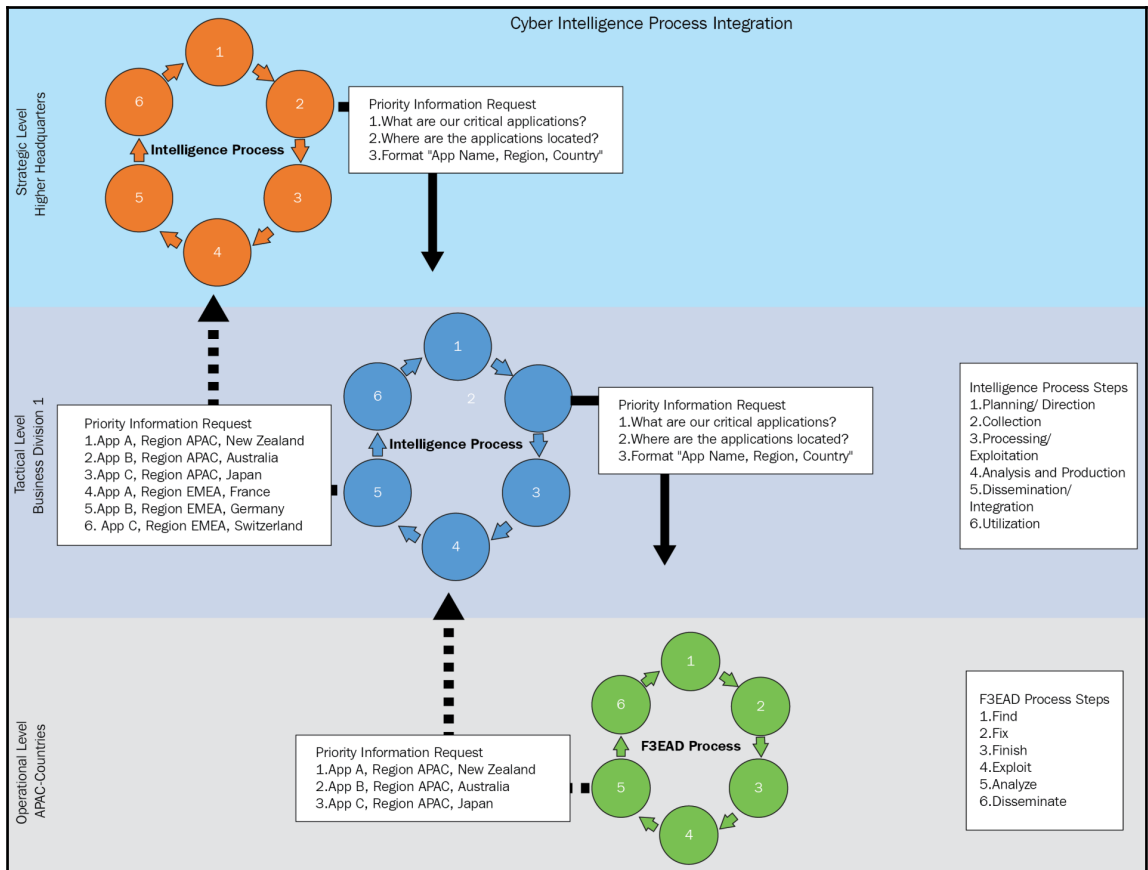


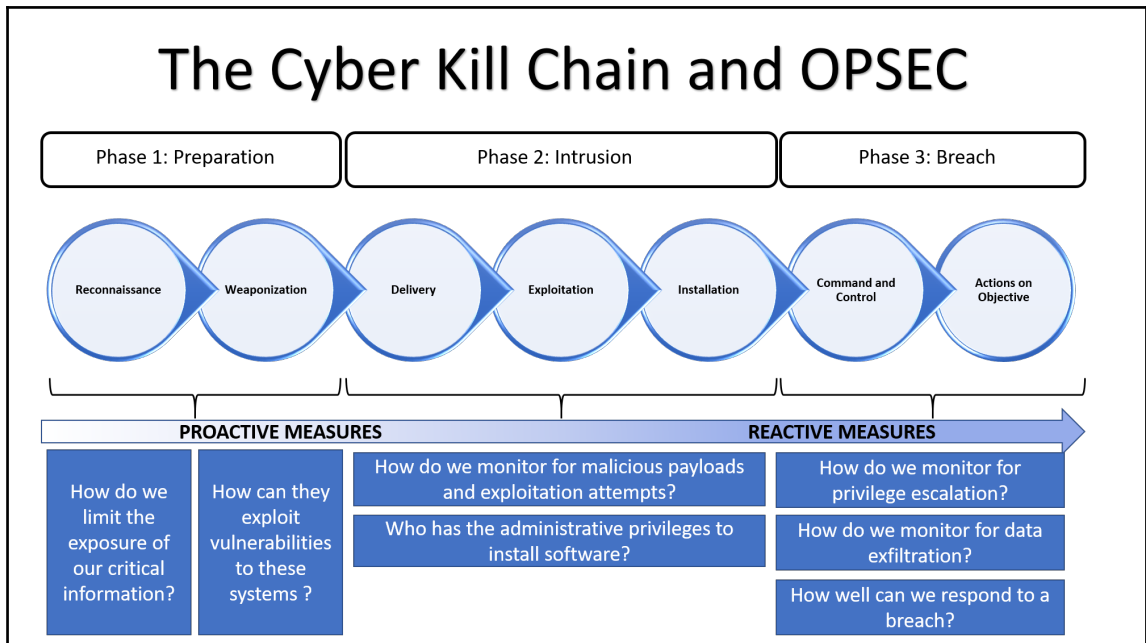
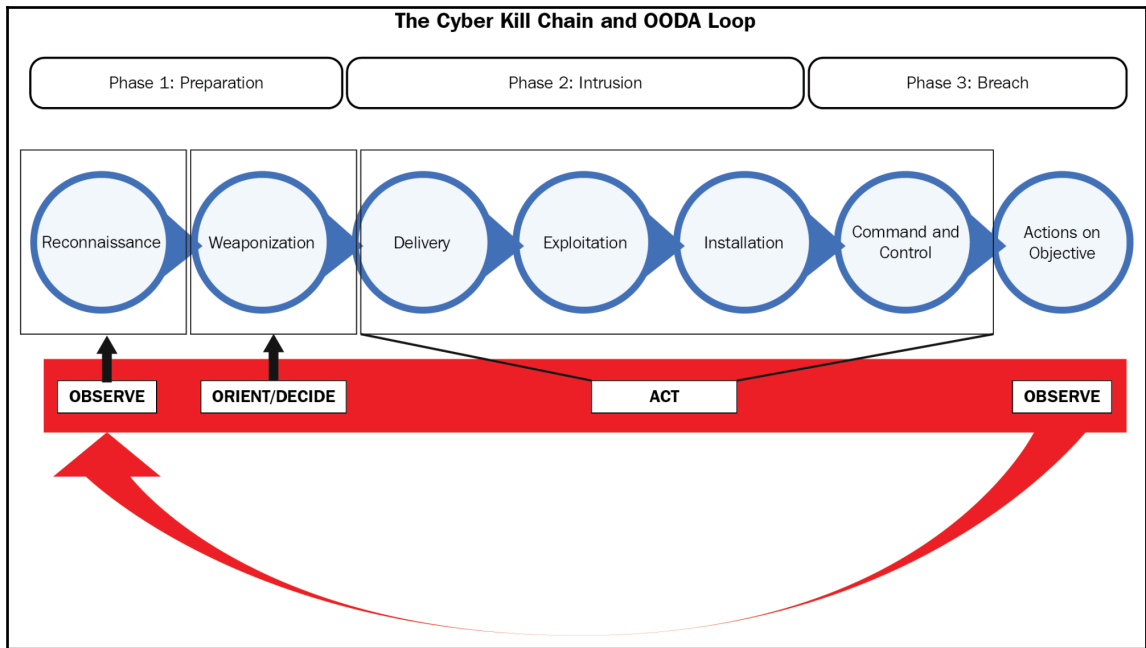


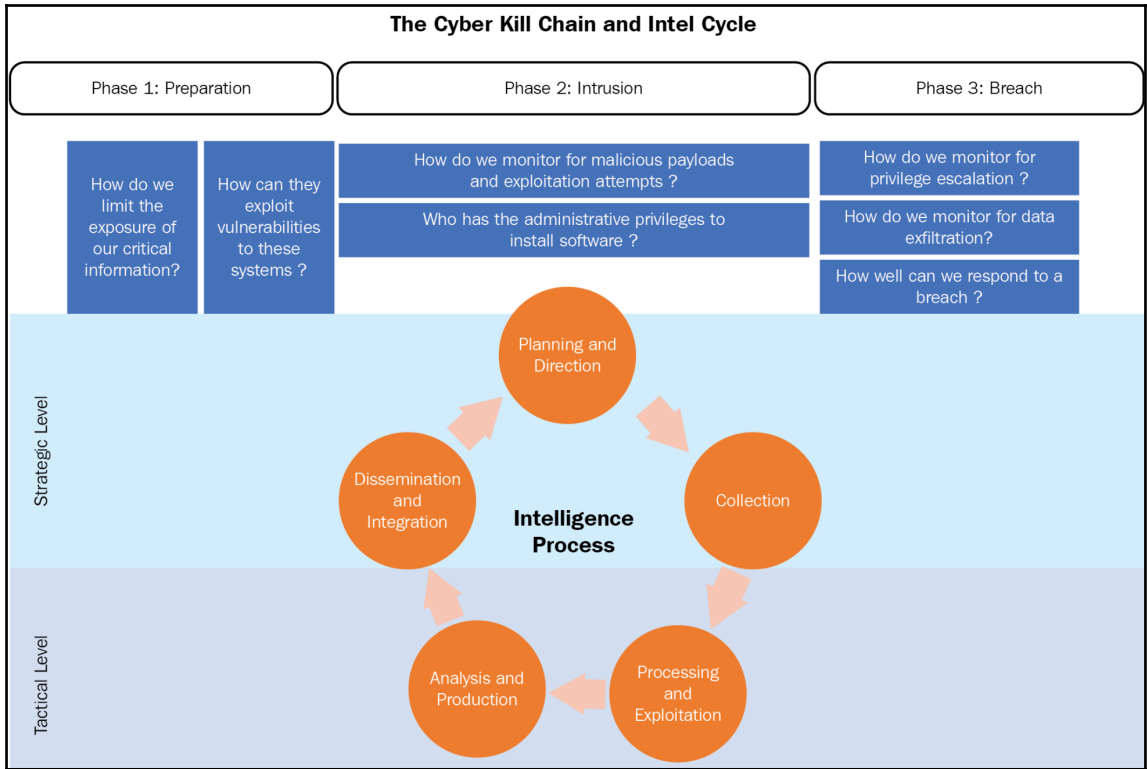


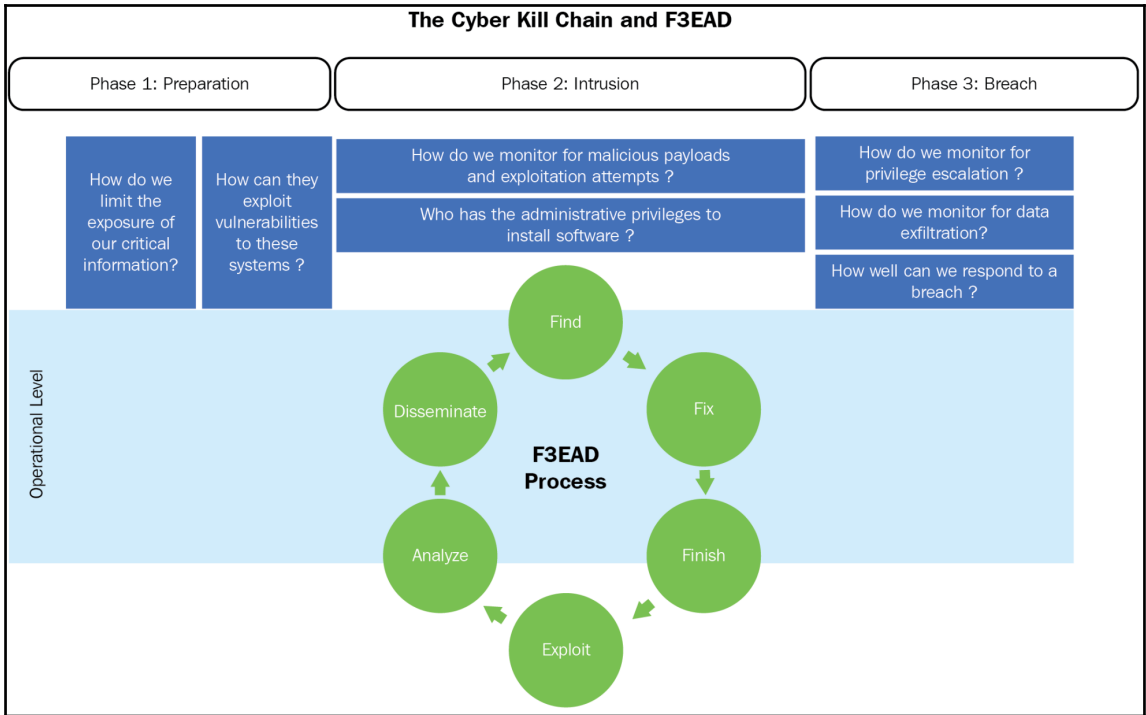




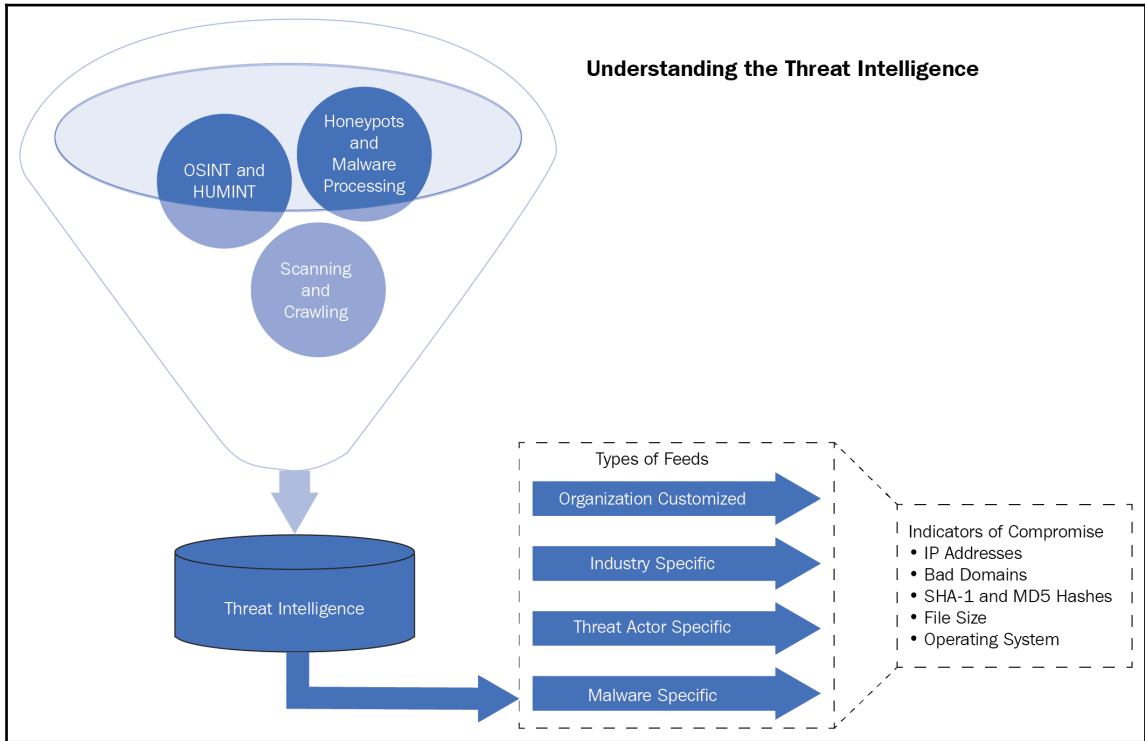


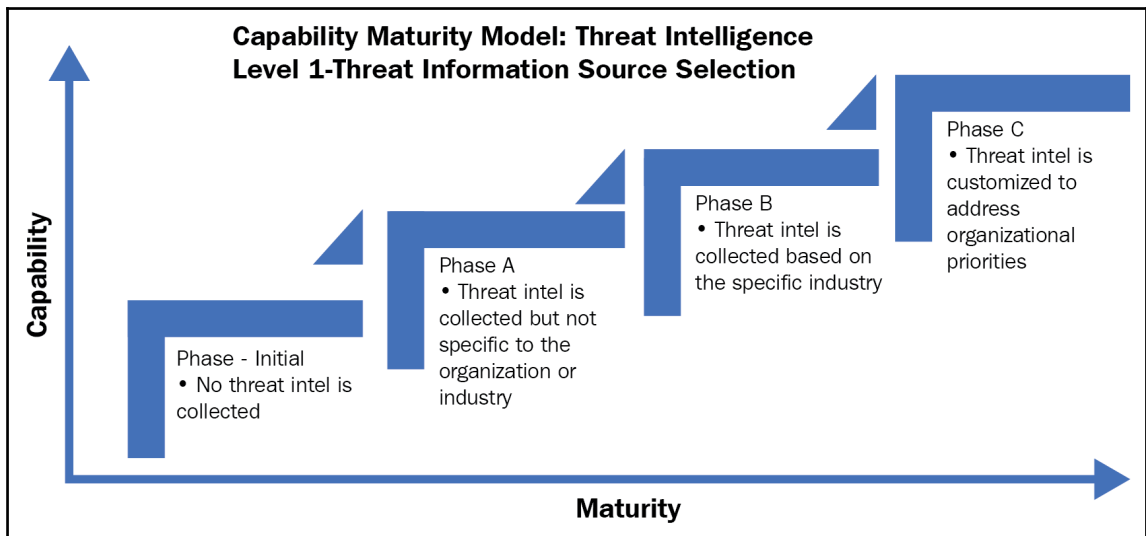
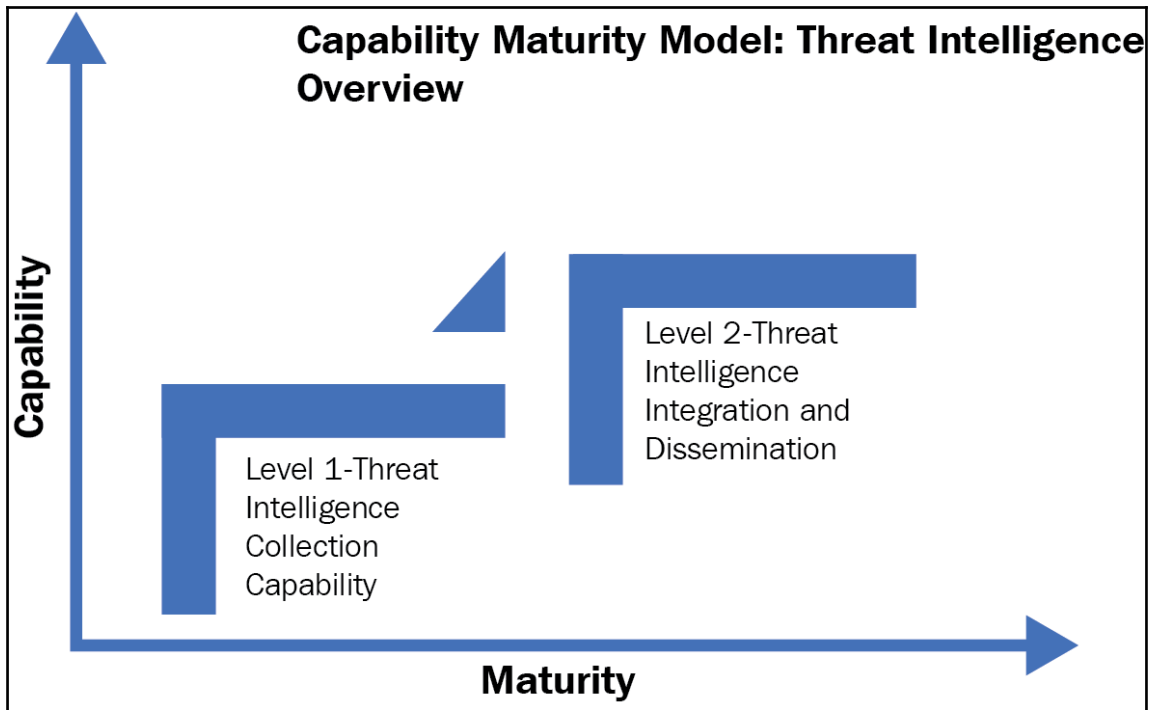






## Chapter 6: Integrating Threat Intelligence and Operations





Overview Created during: last 24 hours [MAKE THIS MY DEFAULT DASHBOARD!](#)

### Visualization of Malware Clusters

BY CATEGORY [COMBINE](#)

Select Malware Family Above for More Details

### Subscribed Pulses

- Drive-by download campaign targets Chinese websites, experiments with exploits  
CREATED 10 HOURS AGO [AlertVault](#)
- Mirai-based Bot Turns IoT Devices into Proxy Servers  
CREATED 19 HOURS AGO [AlertVault](#)
- Absorult Version 2: Atrocious Spyware infection using 3 in 1 RTF Document  
CREATED 23 HOURS AGO [AlertVault](#)
- APT Malware Delivered over Facebook  
MONITORED 1 DAY AGO [AlertVault](#)
- A Slice of 2017 Sofacy Activity  
CREATED 2 DAYS AGO [AlertVault](#)
- OSX/Coldroot RAT  
CREATED 2 DAYS AGO [AlertVault](#)
- CVE-2017-10271 Used to Deliver CryptoMiners  
CREATED 7 DAYS AGO [AlertVault](#)
- SamSam Ransomware Campaigns  
MONITORED 7 DAYS AGO [AlertVault](#)

[CLICK HERE FOR MORE](#)

### Security News

- North Korea mining Monero
- Critical CPU flaw breaks basic security for most computers
- Turfa cyber-espionage group fakes Adobe to drop malware on embassies

### Security Events

### Tech Talks

### Visualization of Malware Clusters

BY CATEGORY [COMBINE](#)

**Other** 5,473

**Backdoor** 7,203

**Unknown** 6,498

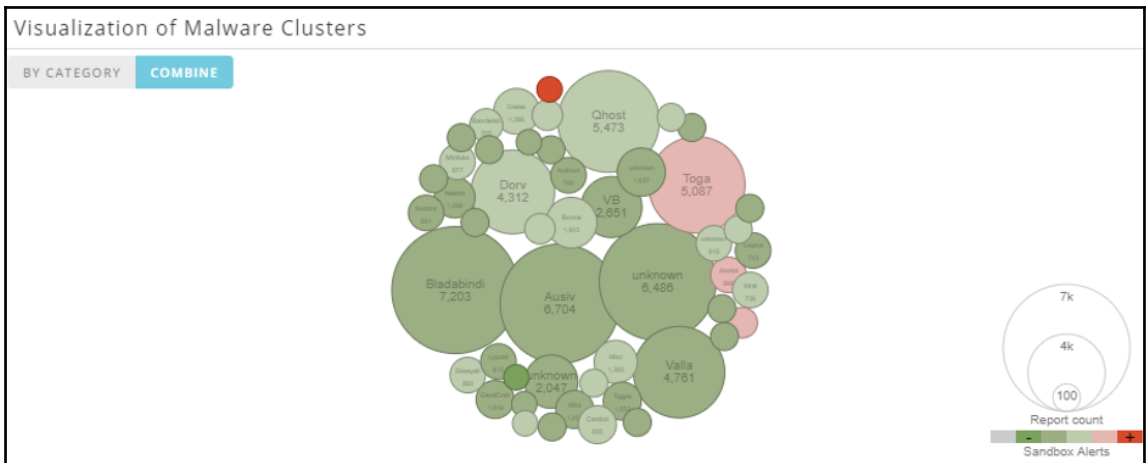
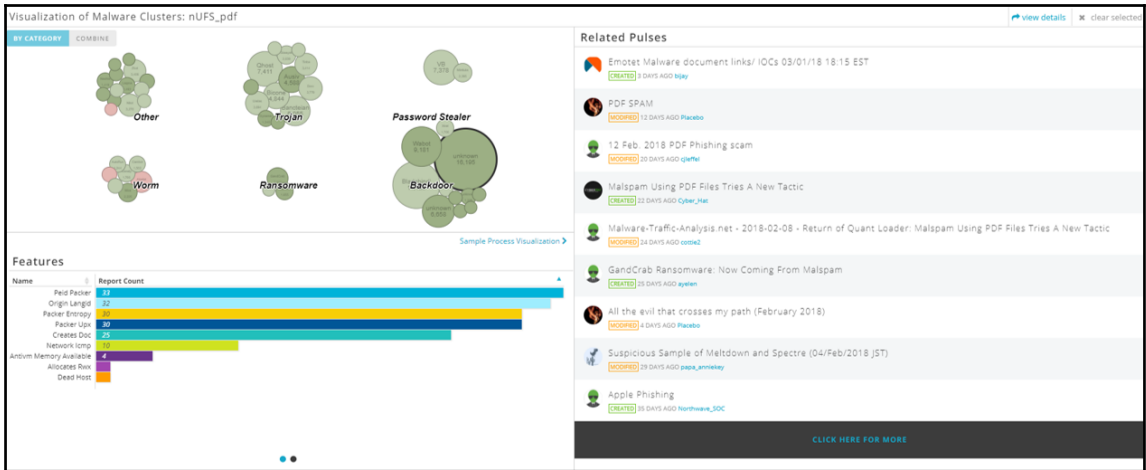
**Password Stealer** 2,651

**File Infector** 1,589

**Trojan** 5,087


**Worm** 5,473






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\\_anna1ay](#) | Public | TLP: White

IPV4: 130

41

SUBSCRIBE




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

CREATED 6 MINUTES AGO by [papa\\_anna1ay](#) | Public | TLP: White

IPV4: 111

41

SUBSCRIBE



**Go Daddy Phish**


CREATED 1 HOUR AGO by [cibernetix](#) | 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 [mpaper05](#) | Public | TLP: White

FileHash: SHA256: 4 | Domain: 3 | 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 [pranjal1](#) | Public | TLP: Green







IPV4: 1

0






SUBSCRIBE

We've found 52,825 users

SORT: MOST PULSES ▾

	<p><b>JNAZARIO</b></p> <p><small>645 DAYS AGO</small></p> <p><small>2225 PULSES   0 CONTRIBUTIONS</small></p>	445	486	679931
		<small>FOLLOWERS</small>	<small>SUBSCRIBERS</small>	<small>CONTRIBUTED INDICATORS</small>
	<p><b>MARCORAMILLI</b></p> <p><small>281 DAYS AGO</small></p> <p><small>2222 PULSES   0 CONTRIBUTIONS</small></p>	216	240	558158
		<small>FOLLOWERS</small>	<small>SUBSCRIBERS</small>	<small>CONTRIBUTED INDICATORS</small>
	<p><b>MALWAREPATROL</b></p> <p><small>854 DAYS AGO</small></p> <p><small>1679 PULSES   0 CONTRIBUTIONS</small></p>	502	692	64587
		<small>FOLLOWERS</small>	<small>SUBSCRIBERS</small>	<small>CONTRIBUTED INDICATORS</small>
	<p><b>METADEFENDER</b></p> <p><small>289 DAYS AGO</small></p> <p><small>1189 PULSES   0 CONTRIBUTIONS</small></p>	59	136	3198831
		<small>FOLLOWERS</small>	<small>SUBSCRIBERS</small>	<small>CONTRIBUTED INDICATORS</small>
	<p><b>ALIENVAULT</b></p> <p><small>1106 DAYS AGO</small></p> <p><small>1181 PULSES   110 CONTRIBUTIONS</small></p>	1628	49963	62489
		<small>FOLLOWERS</small>	<small>SUBSCRIBERS</small>	<small>CONTRIBUTED INDICATORS</small>
	<p><b>BURBERRY</b></p> <p><small>725 DAYS AGO</small></p> <p><small>976 PULSES   15 CONTRIBUTIONS</small></p>	361	450	321536
		<small>FOLLOWERS</small>	<small>SUBSCRIBERS</small>	<small>CONTRIBUTED INDICATORS</small>

[ 34 ]

 <b>Spyware</b> <small>CREATED 4 HOURS AGO</small>	1 MEMBERS 0 PULSES
 <b>APT</b> <small>CREATED 2 YEARS AGO</small> For those focused on intel related to Advanced Persistent Threats.	86 PULSES
 <b>Blue Team Intelligence - Open Forum</b> <small>CREATED 2 YEARS AGO</small> 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 IOCs and APT activity. The more accurate your intel is the better it serves the...	383 MEMBERS 258 PULSES
 <b>MISP FEED</b> <small>CREATED 1 YEAR AGO</small> Intel added to this group feed downstream MISP platforms through the API key	349 MEMBERS 1,277 PULSES
 <b>Nuisances which waste server time and bandwidth</b> <small>CREATED 9 MONTHS AGO</small> As the name already says it loud and clear: Spam/harvester/proxy morons which waste server time and bandwidth :)	4 MEMBERS 16 PULSES








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

<code>`-javascript:alert(1)-`</code> Type: FilePath
<code>__wretw_w4523_345</code> Type: Mutex
<code>_DECRYPT_FILE.html</code> Type: FilePath
<code>_DECRYPT_FILE.txt</code> Type: FilePath
<code>_sipfederationtls_tcp.40gmail.com</code>




We've found 9,220 malware SORT: ▾

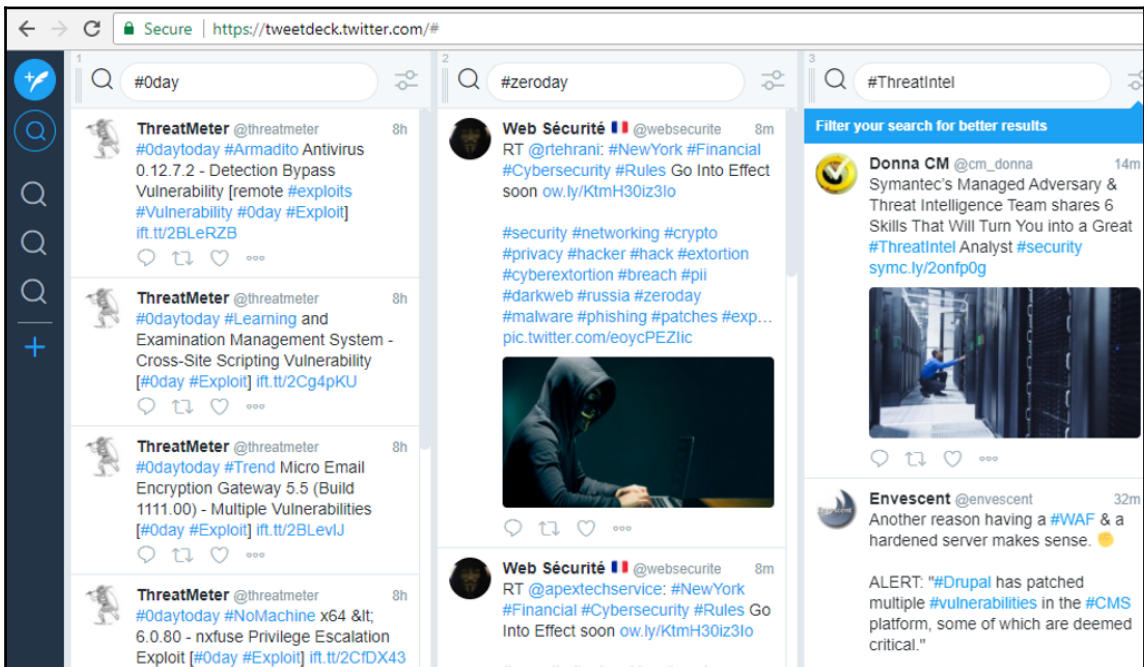
<b>Backdoor:MSIL/Bladabindi</b> Category: Backdoor	<b>83</b> PULSES
<b>Virus:Win32/Nabucur</b> Category: File Infector	<b>29</b> PULSES
<b>Trojan:Win32/Skeeyah</b> Category: Trojan	<b>18</b> PULSES
<b>Worm:Win32/Mira</b> Category: Worm	<b>1</b> PULSE
<b>Worm:Win32/Allaple</b> Category: Worm	<b>55</b>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

We've found 17 industries SORT: DESCENDING ▾

 Aerospace
 Agriculture
 Chemical
 Construction
 Defense
 Education
 Energy

We've found 100 adversaries SORT: DESCENDING ▾

-  **APT 16**
-  **APT 29**  
Also known as: Dukes, Group 100, Cozy Duke, CozyDuke, EuroAPT, CozyBear, CozyCar, Cozer, Office Monkeys, OfficeMonkeys, APT29, Cozy Bear, The Dukes, Minidionis, SeaDuke,
-  **APT 30**  
Also known as: APT30,



Secure | <https://tweetdeck.twitter.com/#>

1 #0day

- ThreatMeter** @threatmeter 8h  
#0daytoday #Armadito Antivirus 0.12.7.2 - Detection Bypass Vulnerability [remote #exploits #Vulnerability #0day #Exploit] <ift.tt/2BLERZB>
- ThreatMeter** @threatmeter 8h  
#0daytoday #Learning and Examination Management System - Cross-Site Scripting Vulnerability [#0day #Exploit] <ift.tt/2Cg4pKU>
- ThreatMeter** @threatmeter 8h  
#0daytoday #Trend Micro Email Encryption Gateway 5.5 (Build 1111.00) - Multiple Vulnerabilities [#0day #Exploit] <ift.tt/2BLvJ>
- ThreatMeter** @threatmeter 8h  
#0daytoday #NoMachine x64 &lt; 6.0.80 - nxfuse Privilege Escalation Exploit [#0day #Exploit] <ift.tt/2CfDX43>

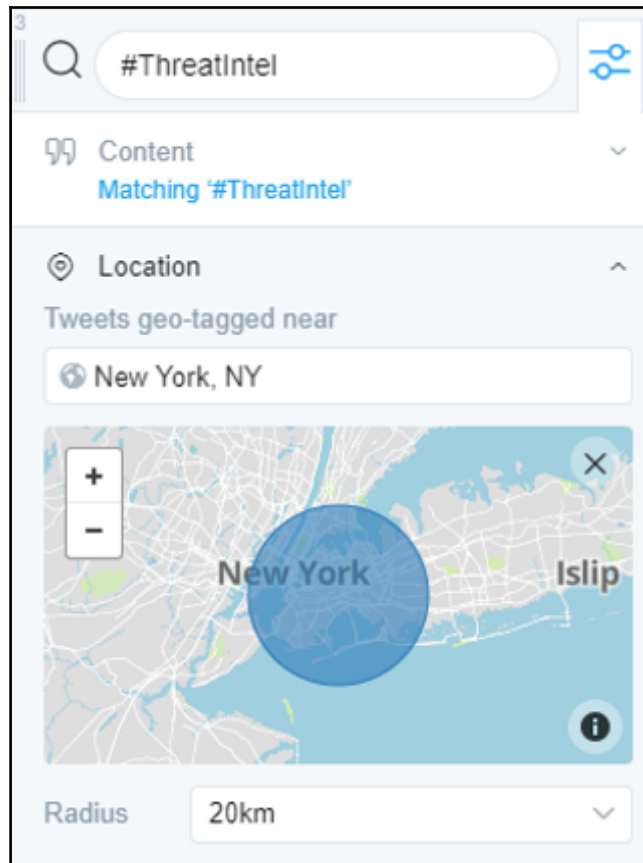
2 #zeroday

- Web Sécurité** @websecurite 8m  
RT @rtehrani: #NewYork #Financial #Cybersecurity #Rules Go Into Effect soon <ow.ly/K1mH30iz3lo>  
#security #networking #crypto #privacy #hacker #hack #extortion #cyberextortion #breach #pii #darkweb #russia #zeroday #malware #phishing #patches #exp... <pic.twitter.com/eoycPEZlic>
- Web Sécurité** @websecurite 8m  
RT @apextechservice: #NewYork #Financial #Cybersecurity #Rules Go Into Effect soon <ow.ly/K1mH30iz3lo>

3 #ThreatIntel

Filter your search for better results

- Donna CM** @cm\_donna 14m  
Symantec's Managed Adversary & Threat Intelligence Team shares 6 Skills That Will Turn You into a Great #ThreatIntel Analyst #security <symc.ly/2onfp0g>
- Envescent** @envescent 32m  
Another reason having a #WAF & a hardened server makes sense. 🟡  
ALERT: "#Drupal has patched multiple #vulnerabilities in the #CMS platform, some of which are deemed critical."



3

🔍 #ThreatIntel 🔗

🔗 Content  
Matching '#ThreatIntel' ▼

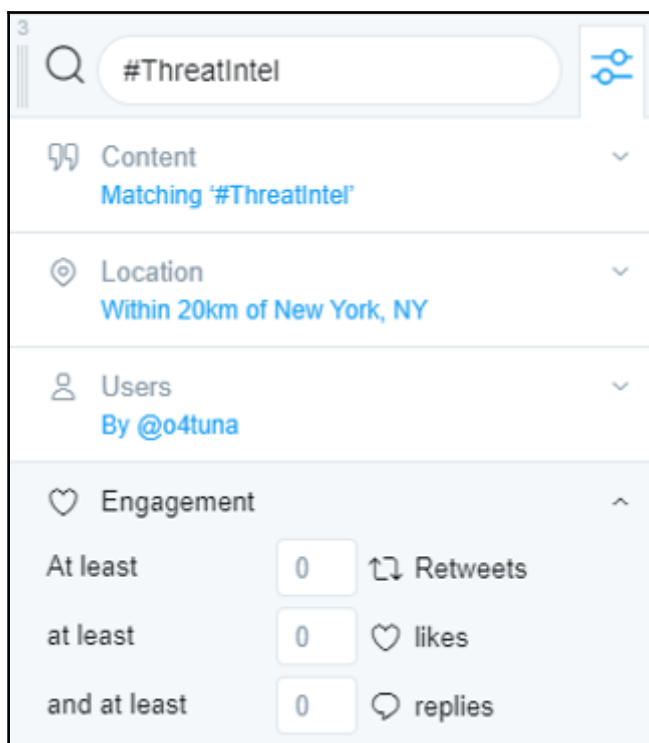
📍 Location  
Within 20km of New York, NY ▼

👤 Users ▲

By  ▼

✕

Mentioning  ▼





# Alerts

Monitor the web for interesting new content

🔍 ThreatIntelligence

This will create an email alert for

[Create Alert](#) [Show options](#) ▼

## Alert preview

NEWS

### Enabling Better Risk Mitigation with **Threat Intelligence**

Dark Reading

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 ...

### Early detection and rapid response critical for targeted attack remediation

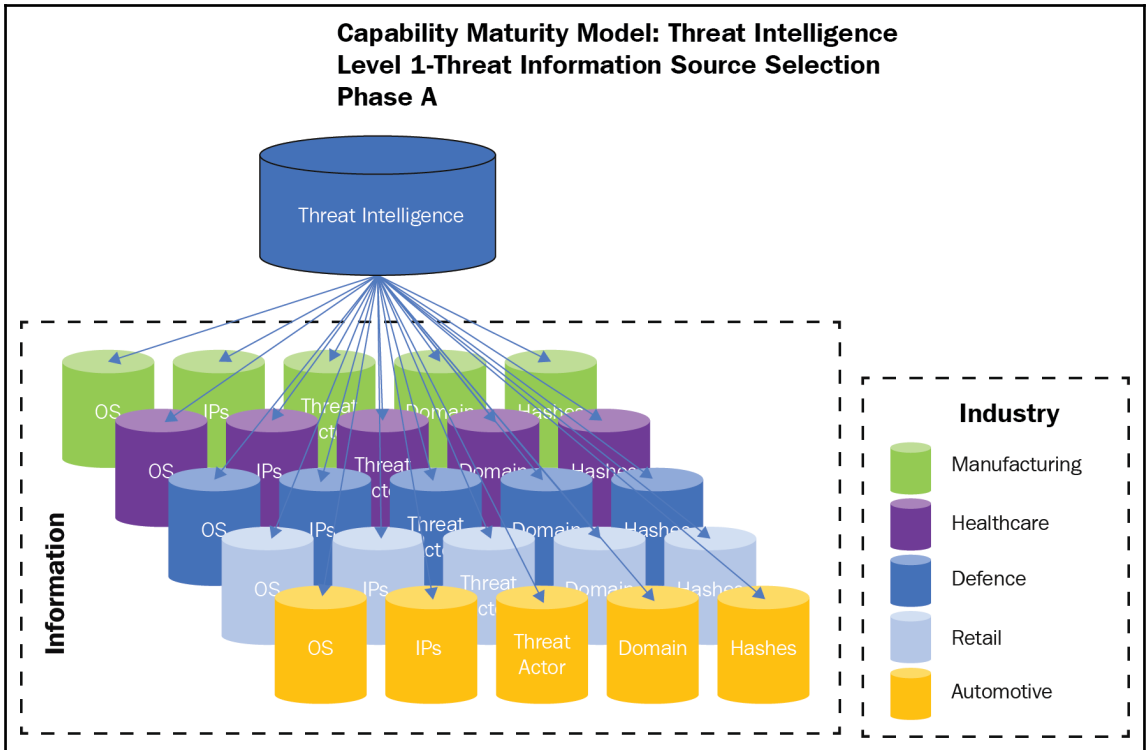
IT News Africa

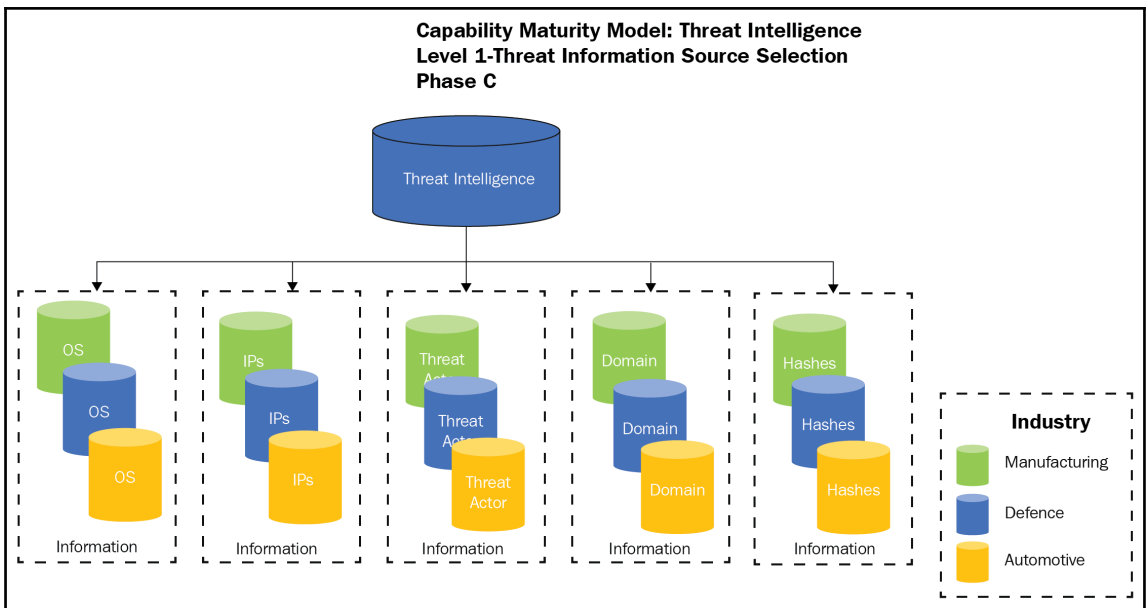
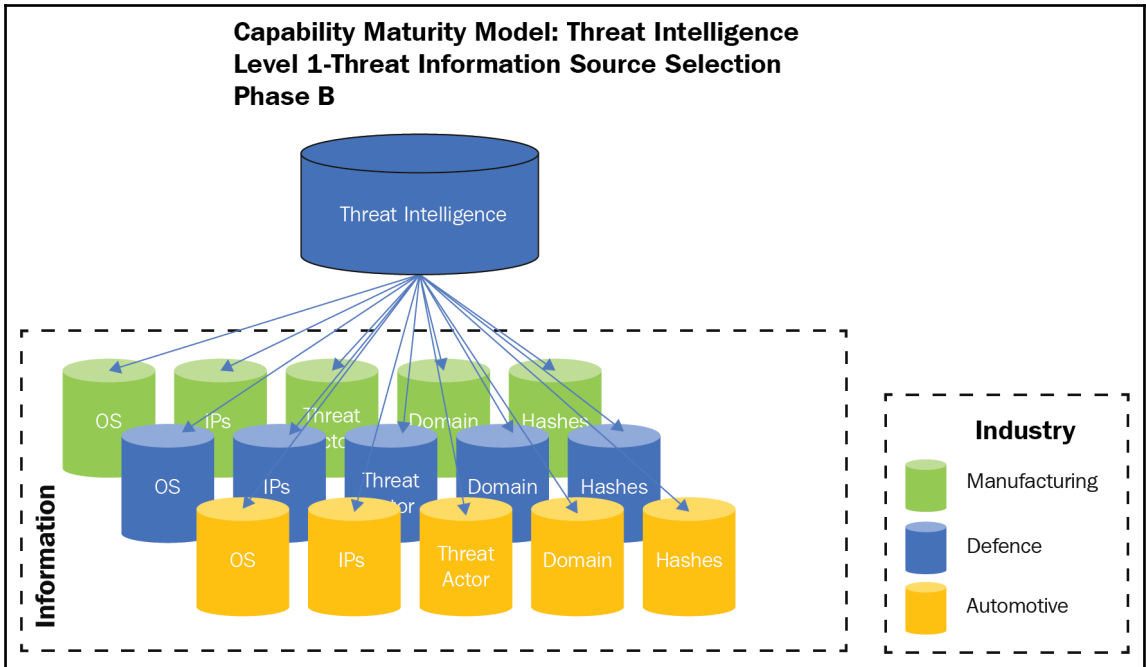
The report outlines the comprehensive forensic analysis framework in the RSA approach to threat response and mitigation, noting that the response process "...takes into consideration data from multiple sources including in-house systems, open source research, "RSA Live" **threat intelligence** and the ...

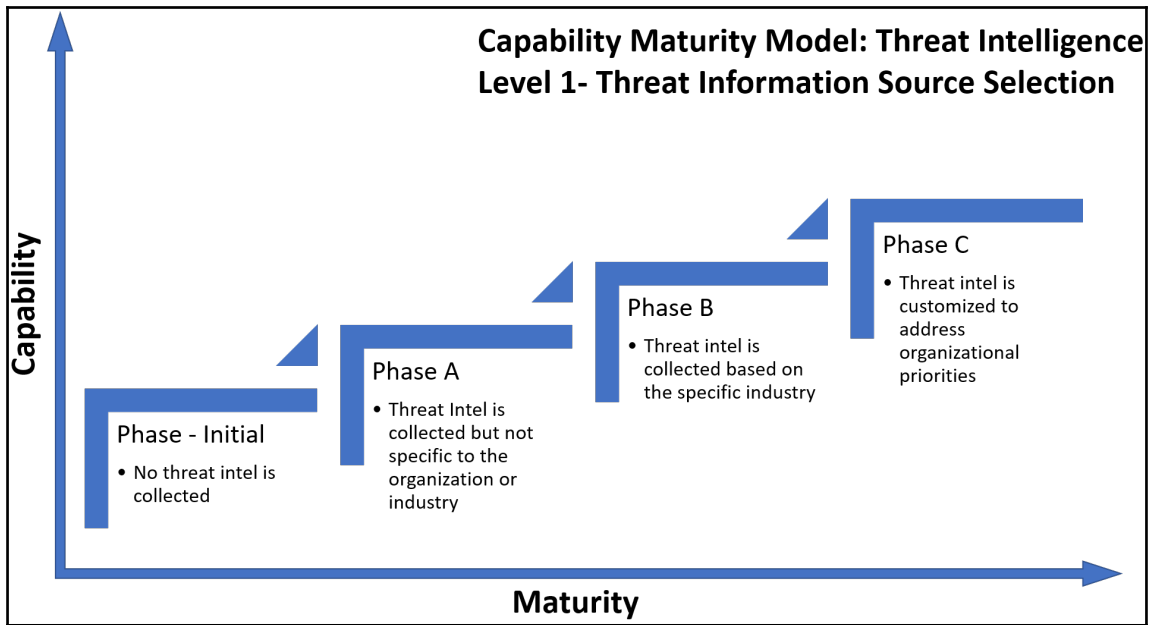
### Decentralized IT Security Marketplace PolySwarm Launched Public Token Sale

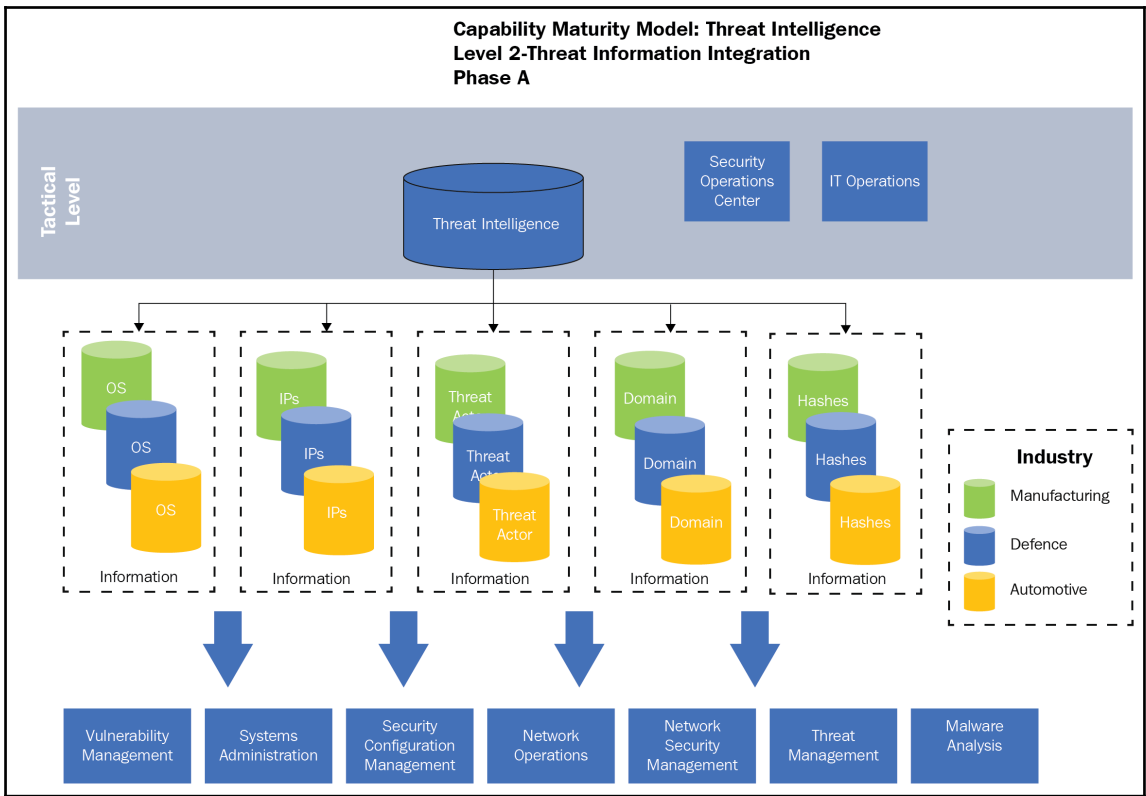
GlobeNewswire (press release)

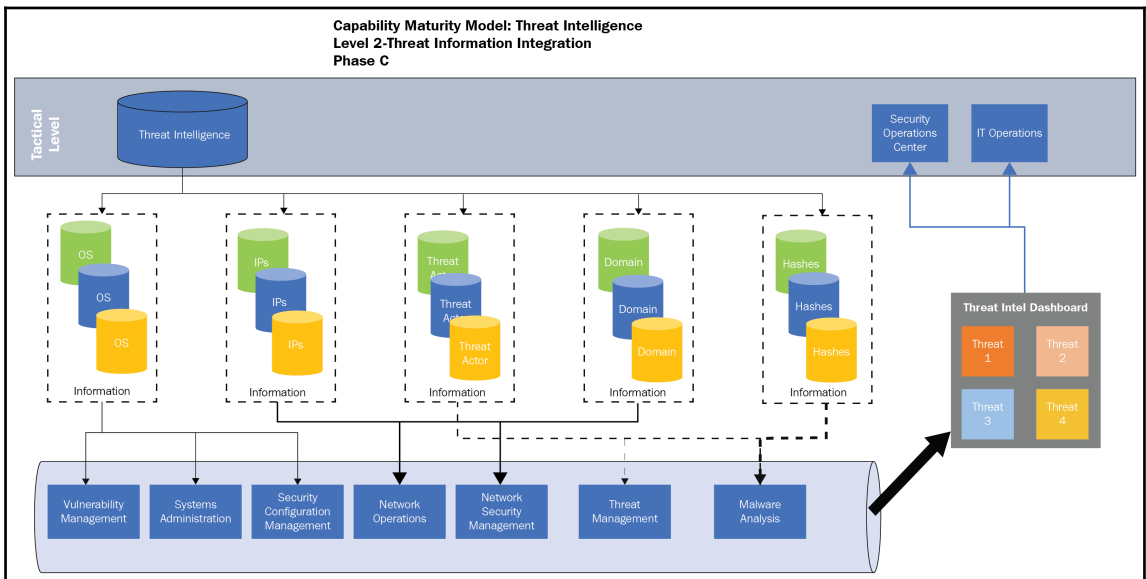
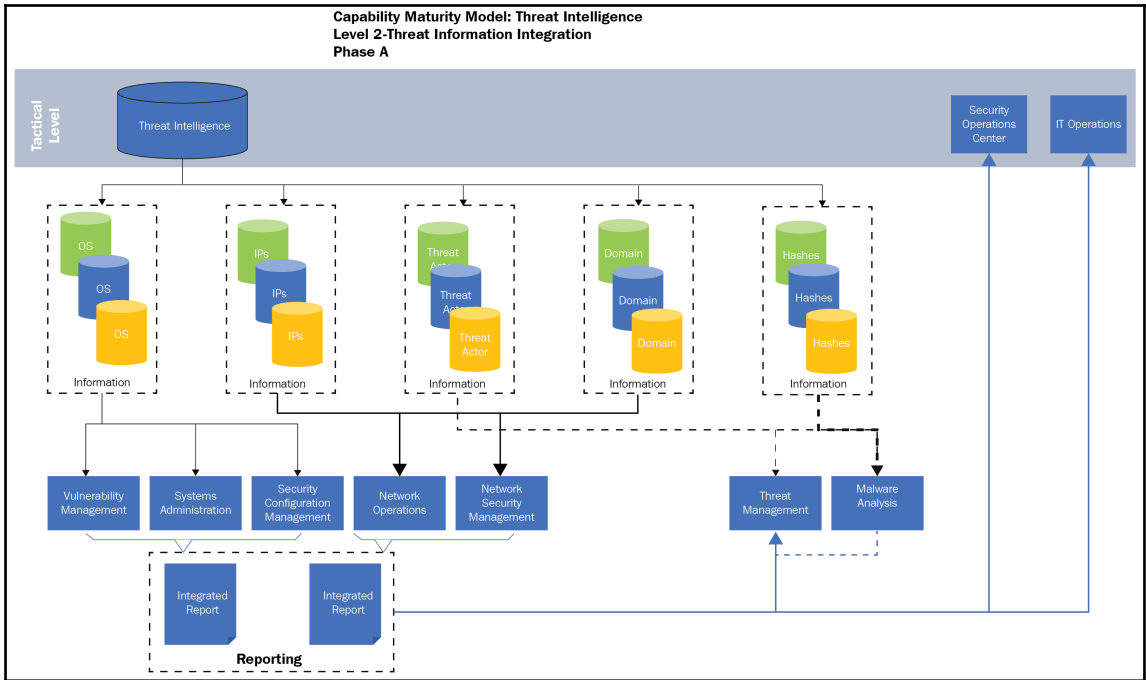
PolySwarm incentivizes a global community of information security experts to disrupt the \$8.5 billion cyber **threat intelligence** industry, providing enterprises and consumers with unprecedented speed and accuracy in



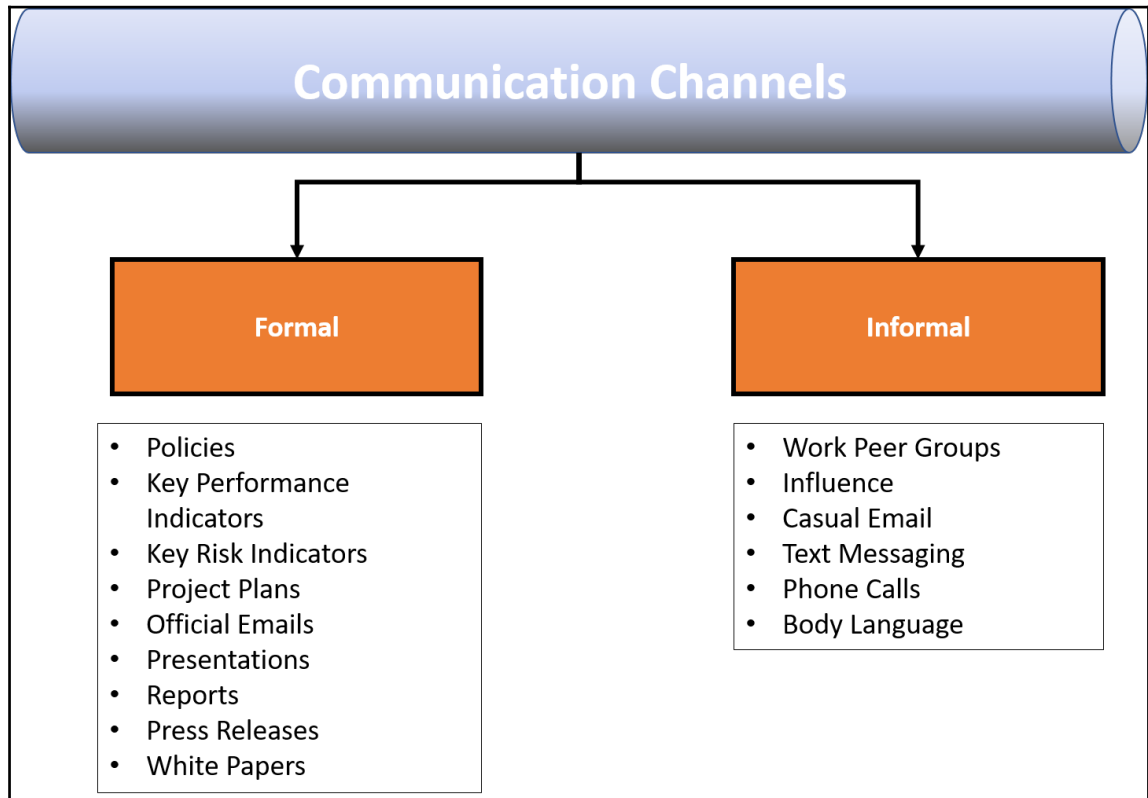


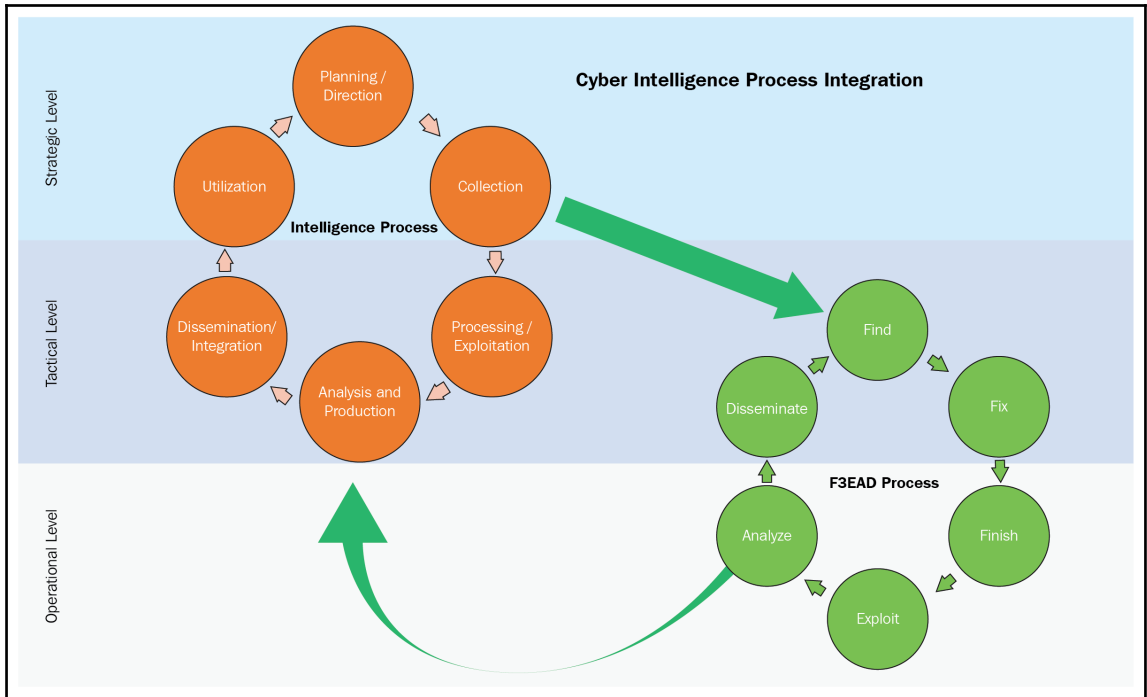






## Chapter 7: Creating the Collaboration Capability

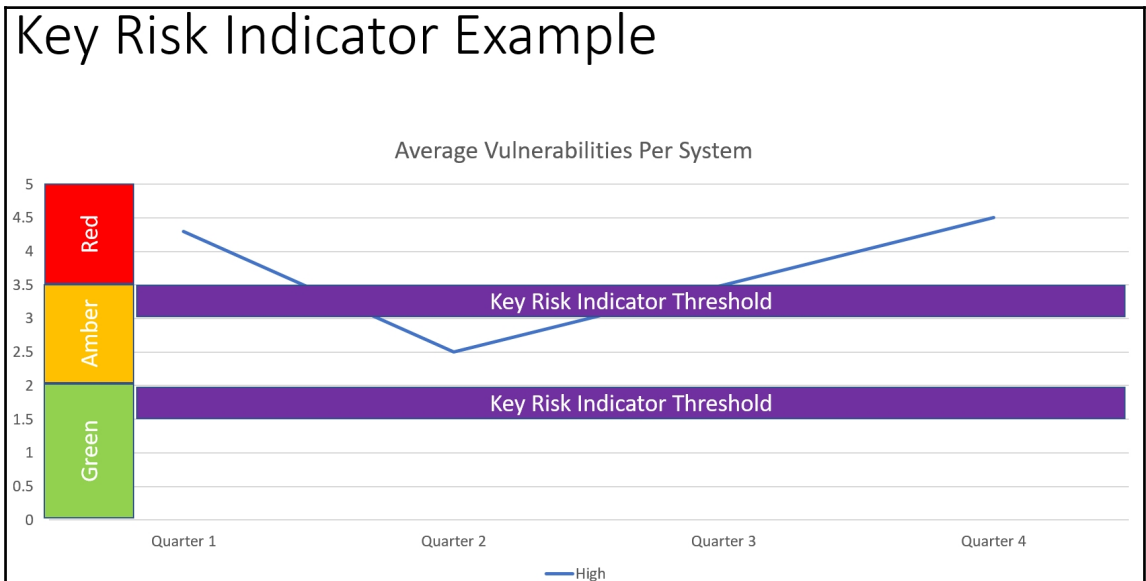
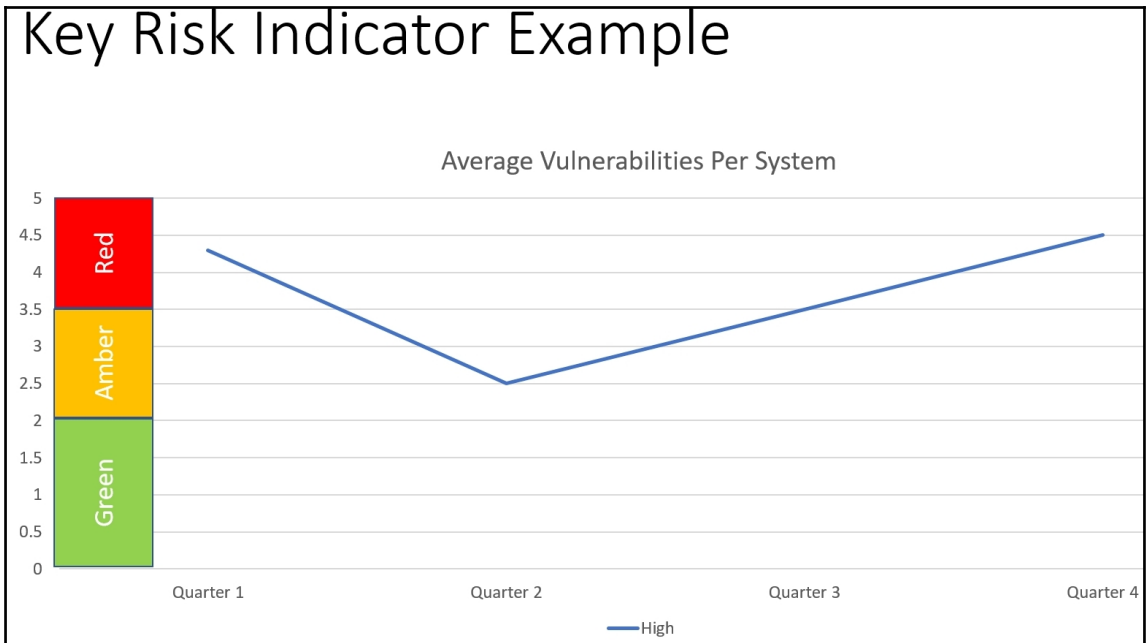


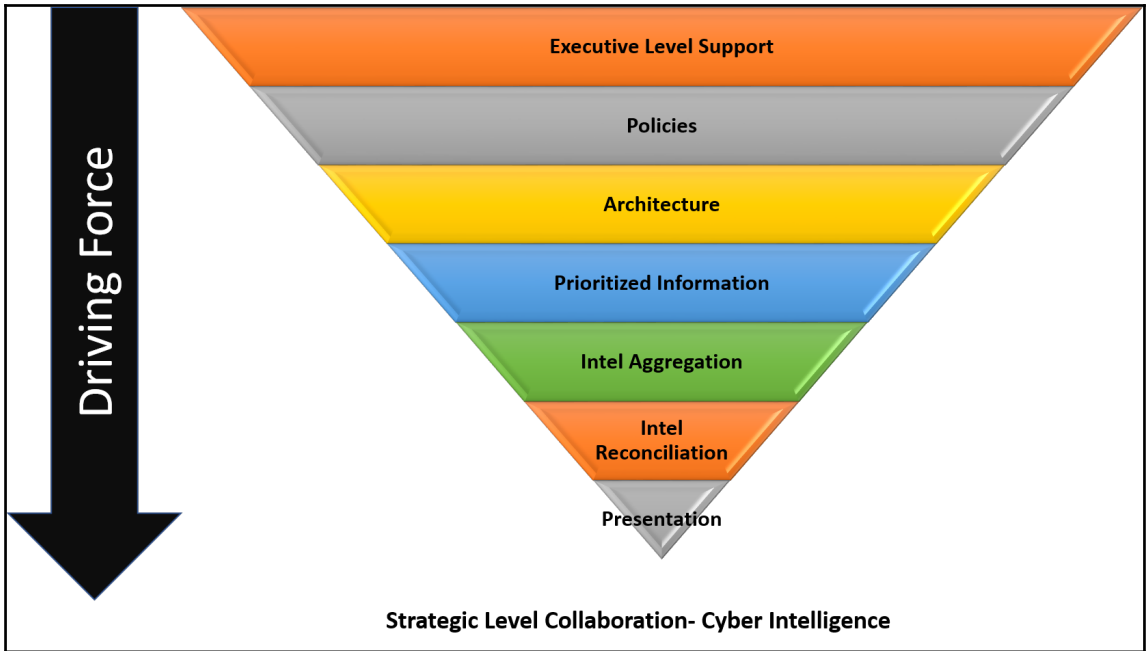


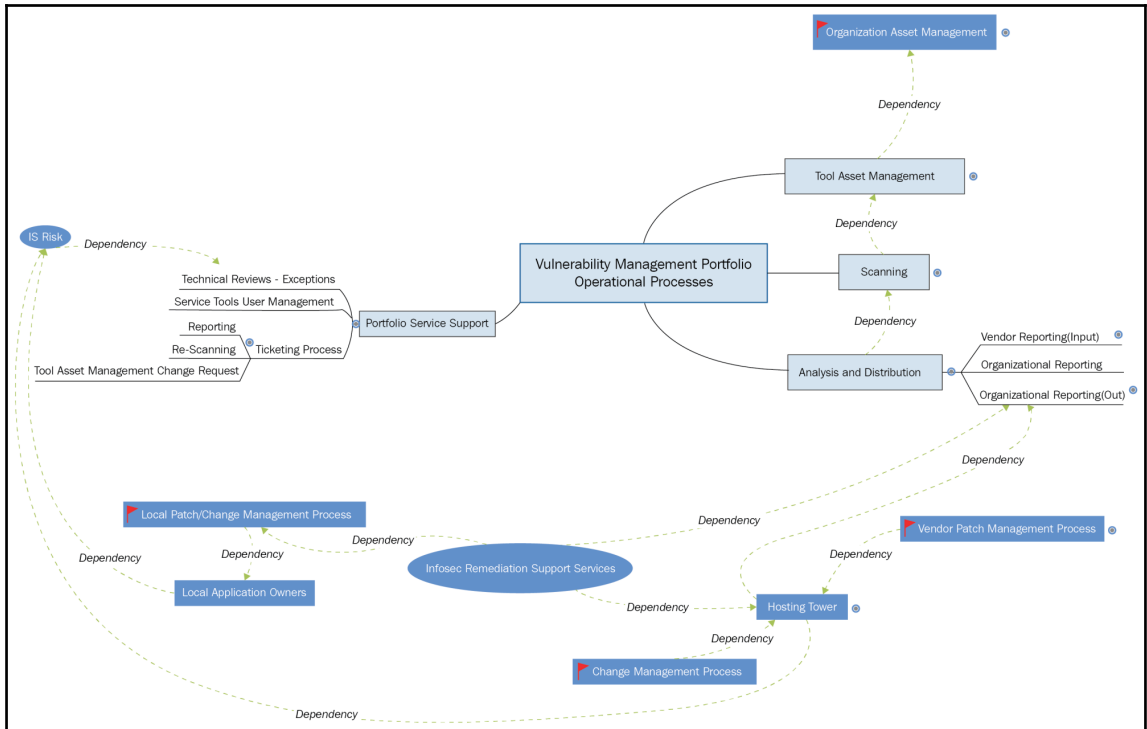
### Responsible Accountable Supporting Consulted Informed Matrix

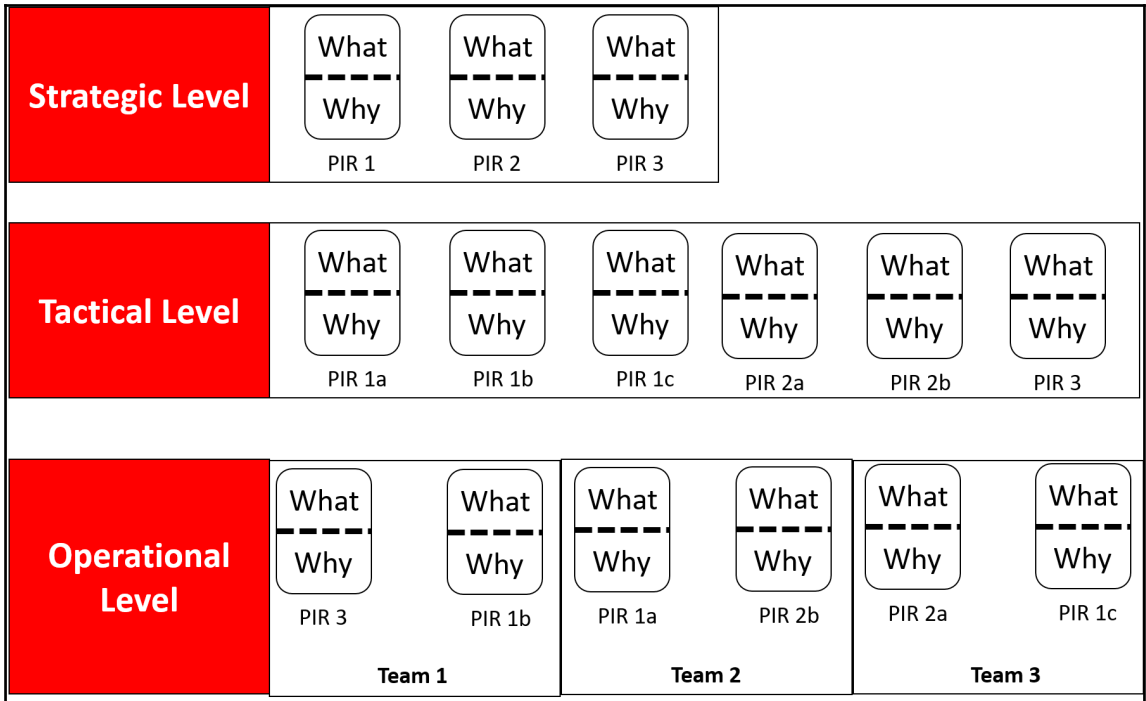
	A Service	B Service	C Service	D Service
<b>Task 1</b>	Responsible	Informed	Consulted	Accountable
<b>Task 2</b>	Accountable	Responsible	Informed	Consulted
<b>Task 3</b>	Consulted	Accountable	Responsible	Supporting
<b>Task 4</b>	Supporting	Consulted	Accountable	Responsible

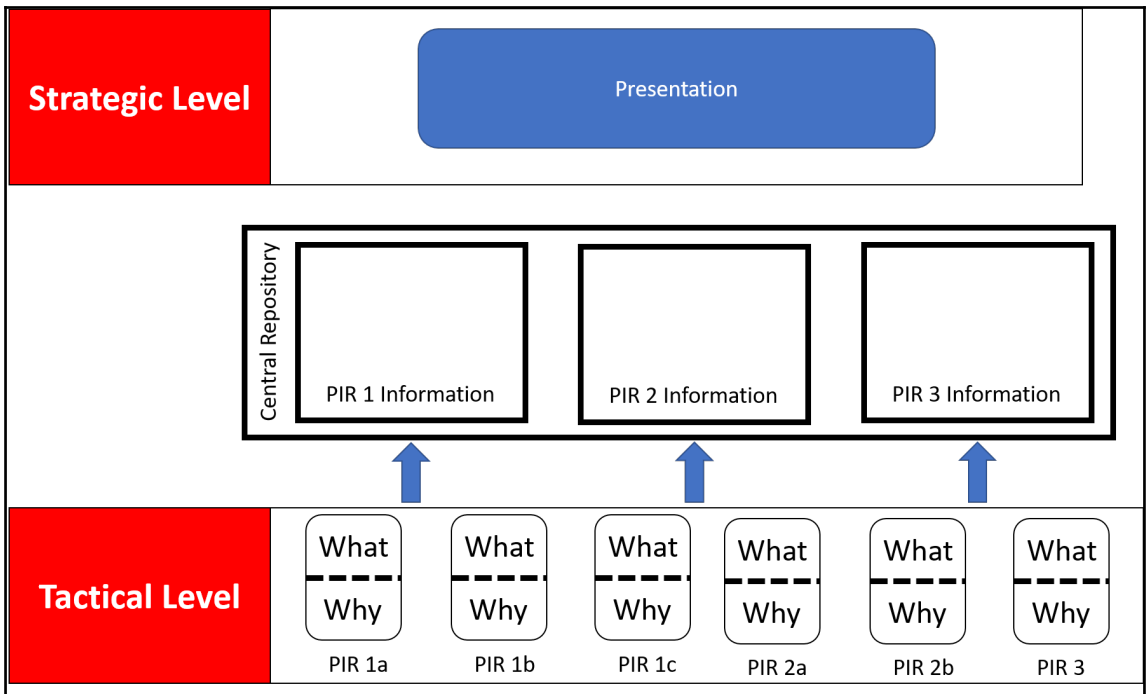


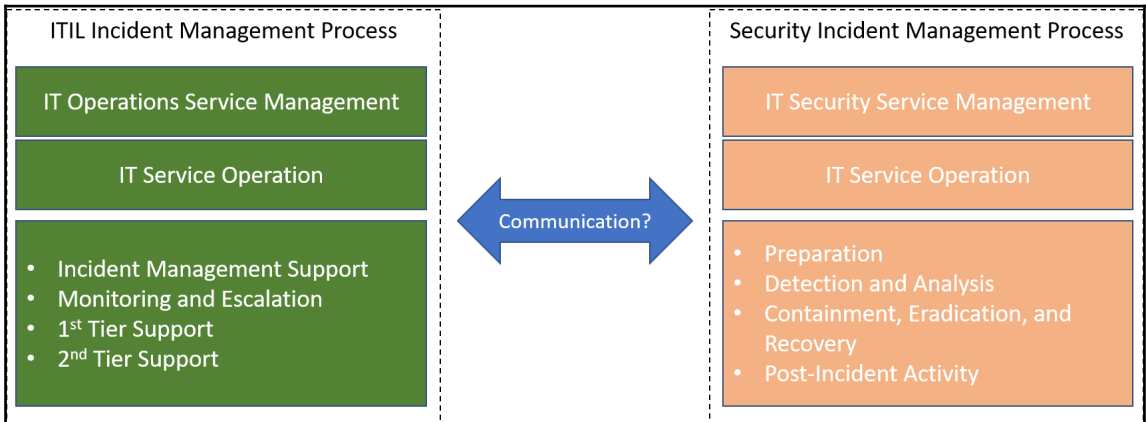
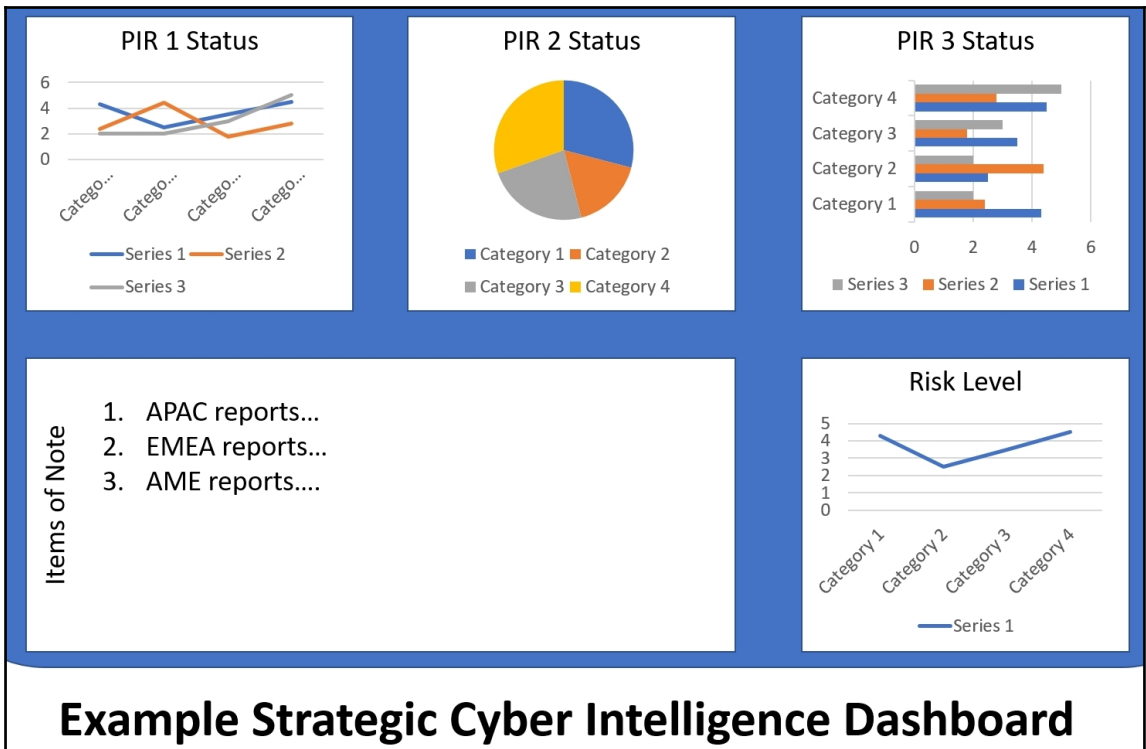


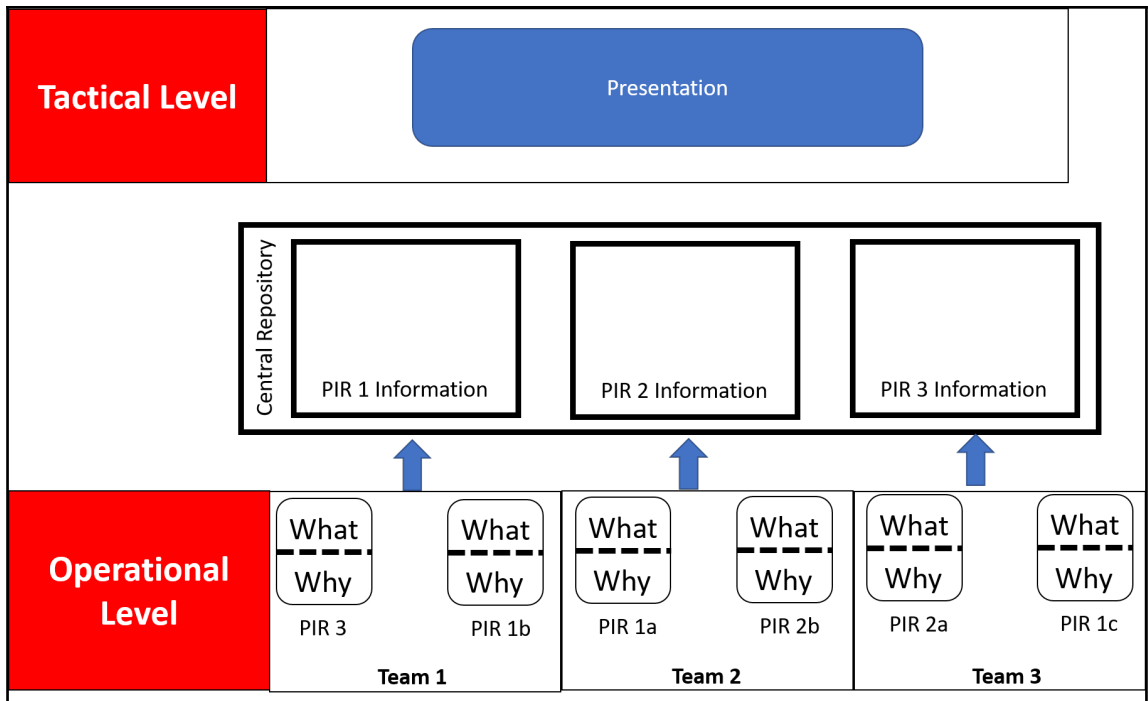
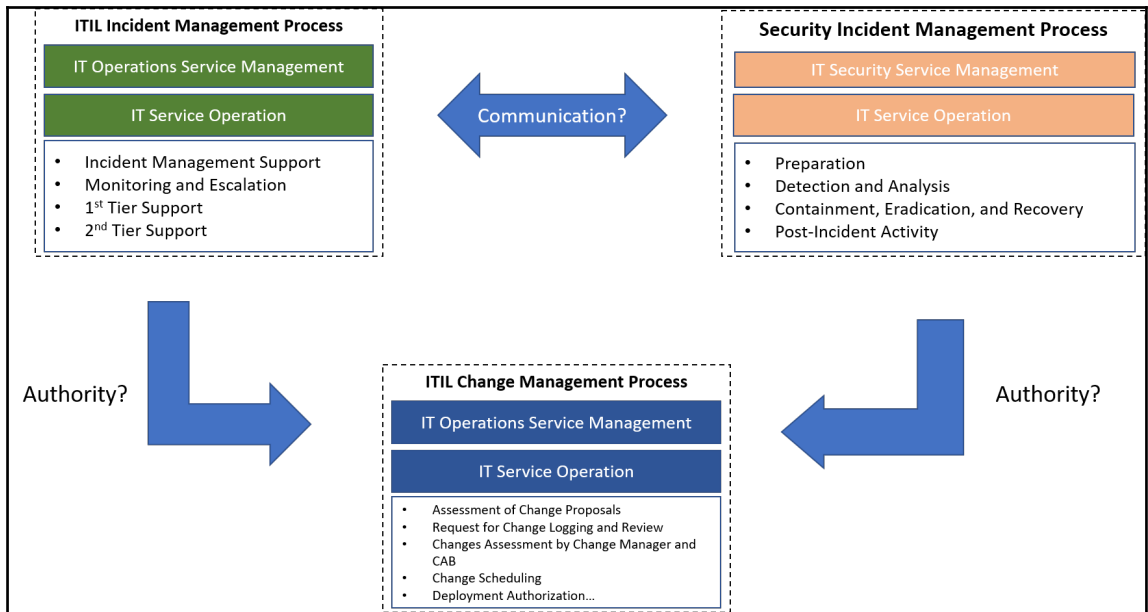


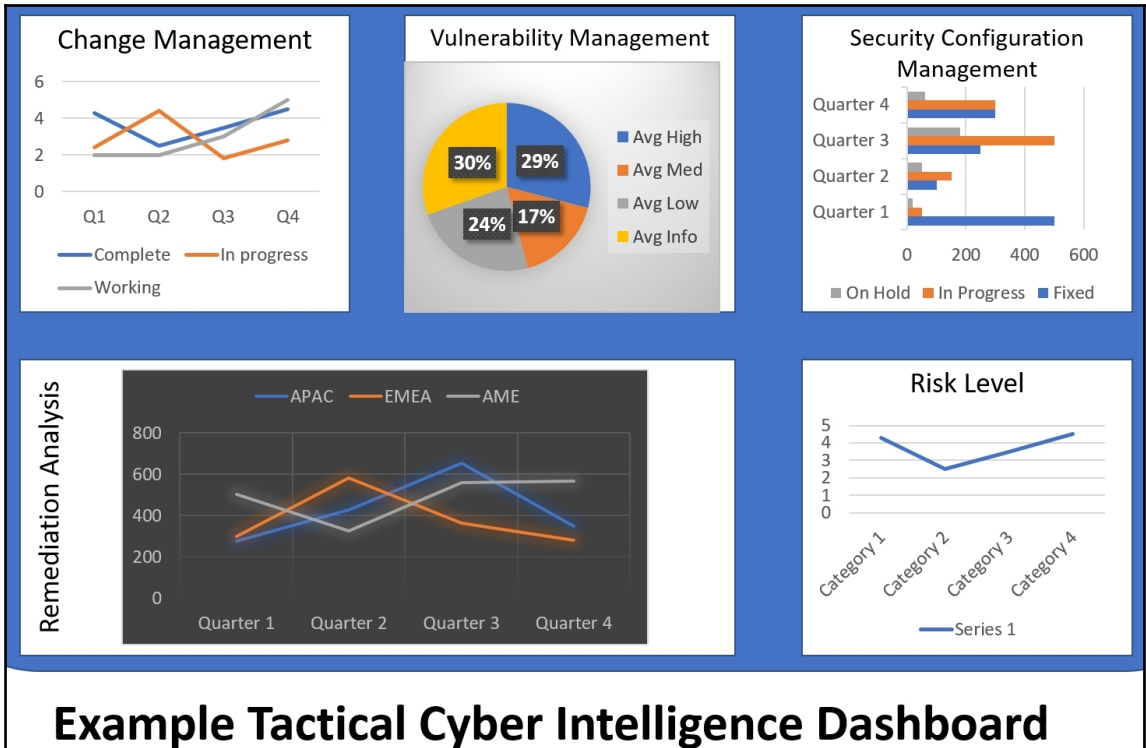




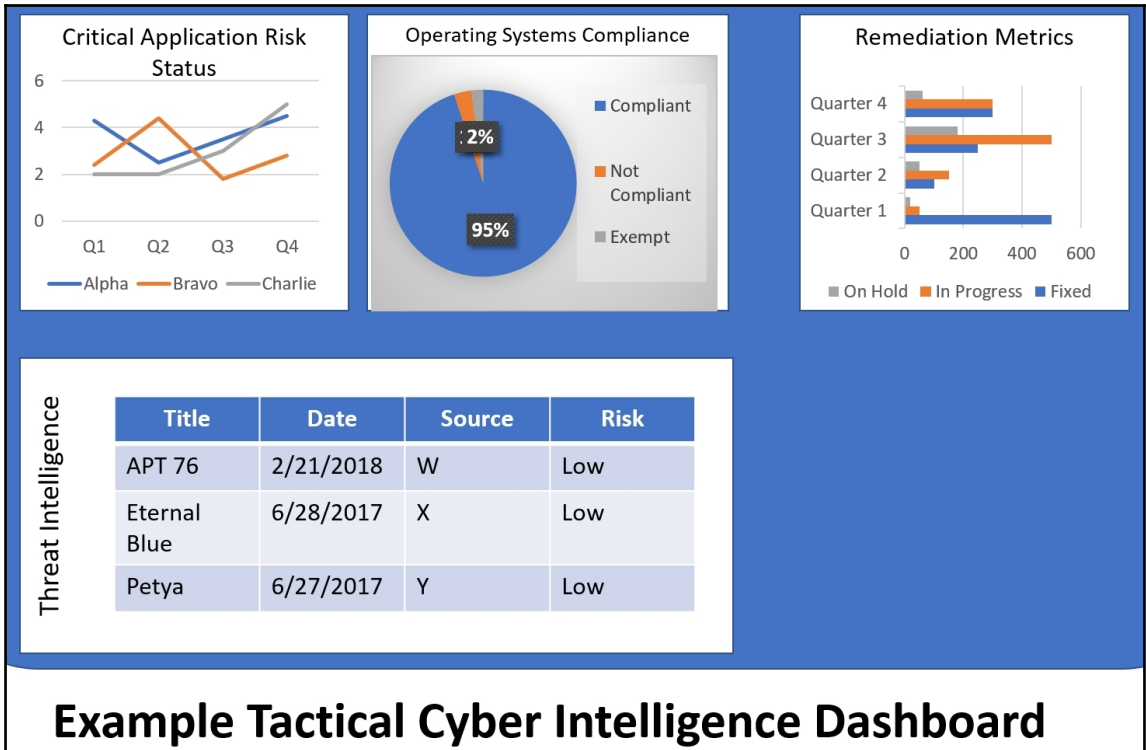




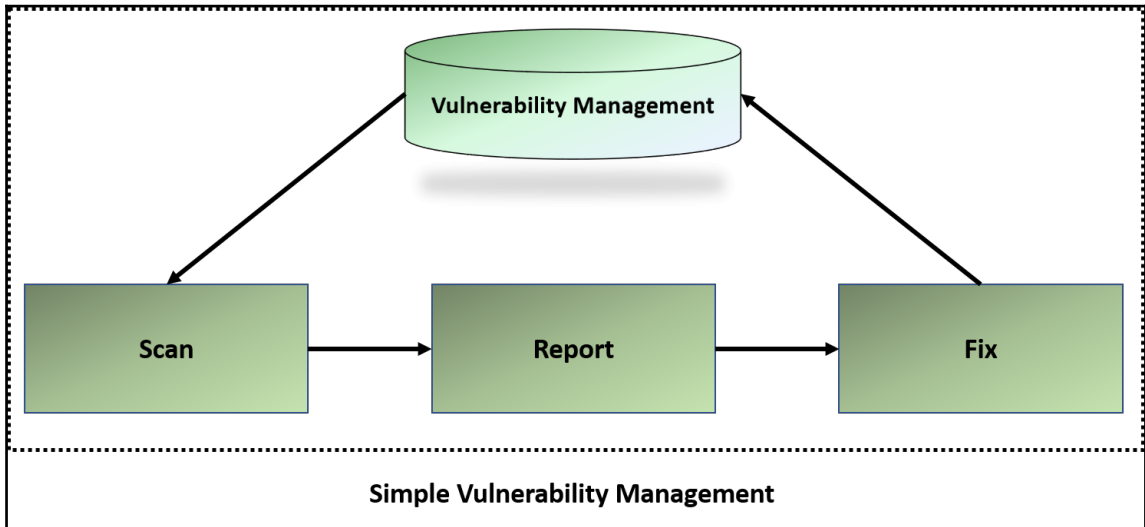


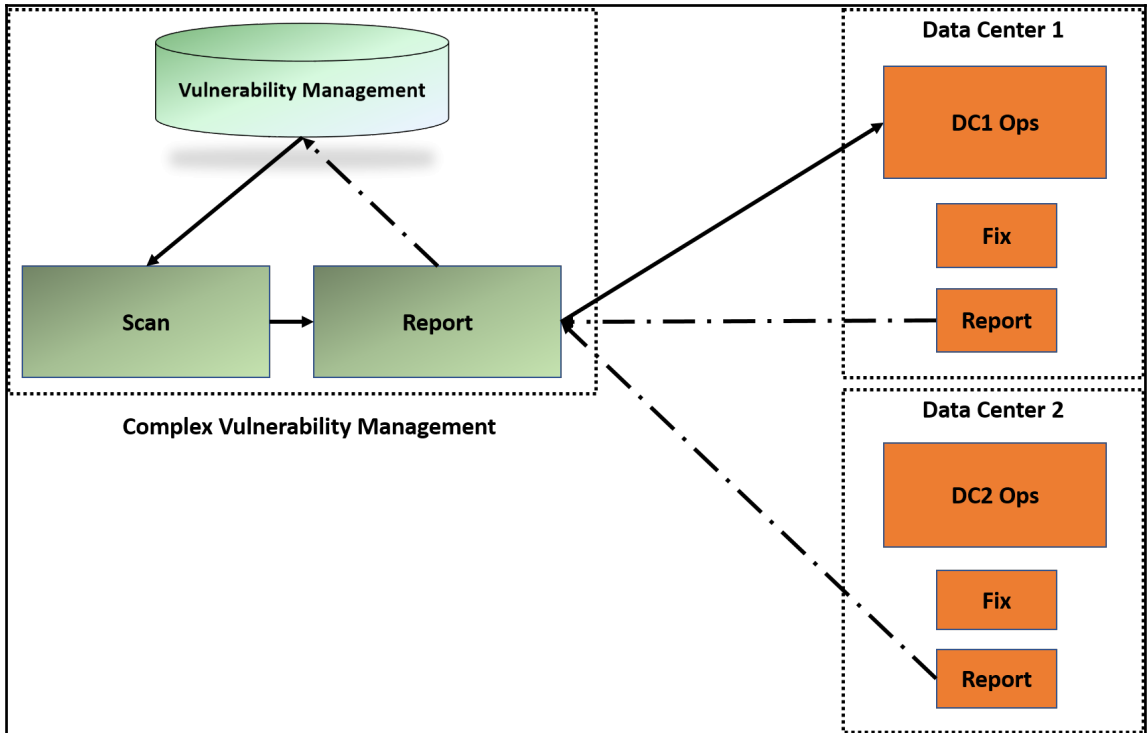


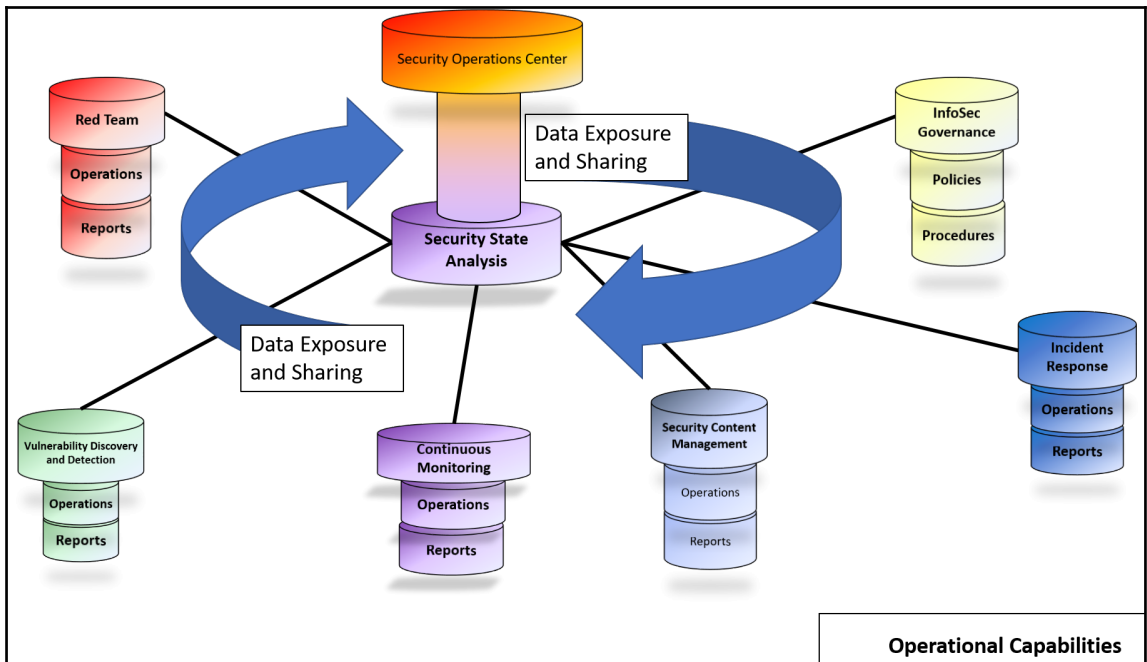




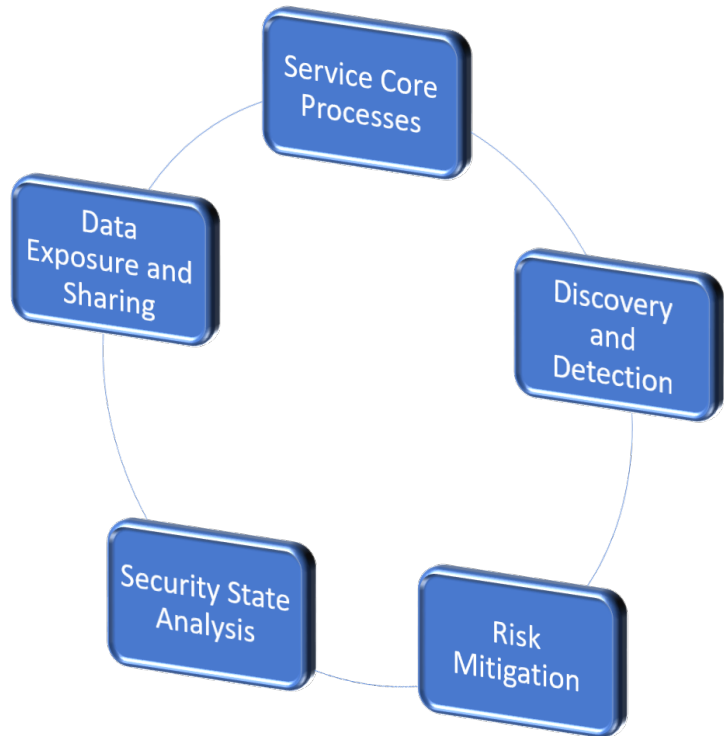
## Chapter 8: The Security Stack



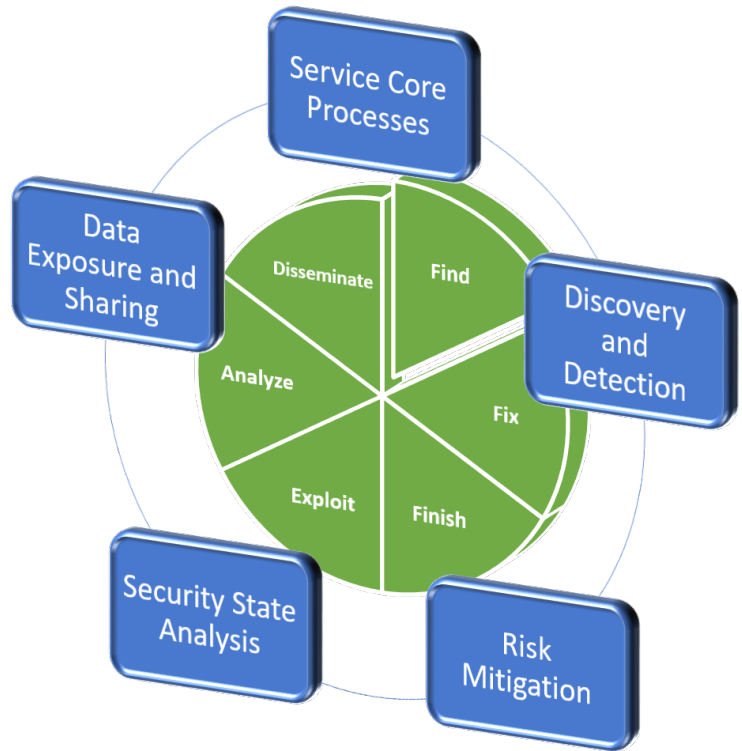




## Security Team Capabilities



## Security Team Capabilities and F3EAD

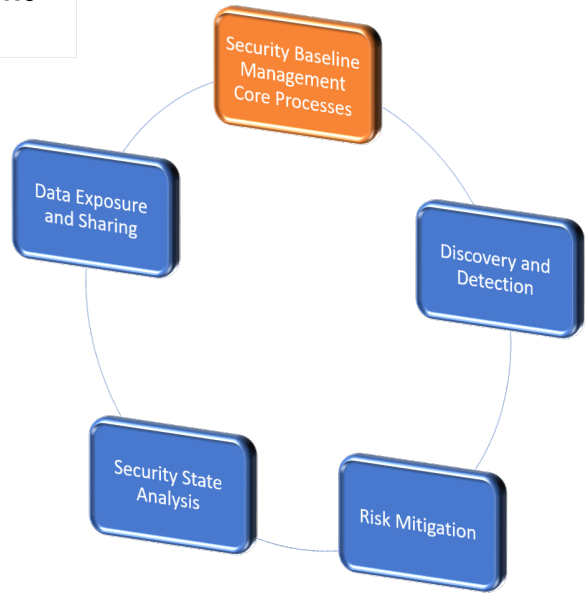


# Security Configuration Management



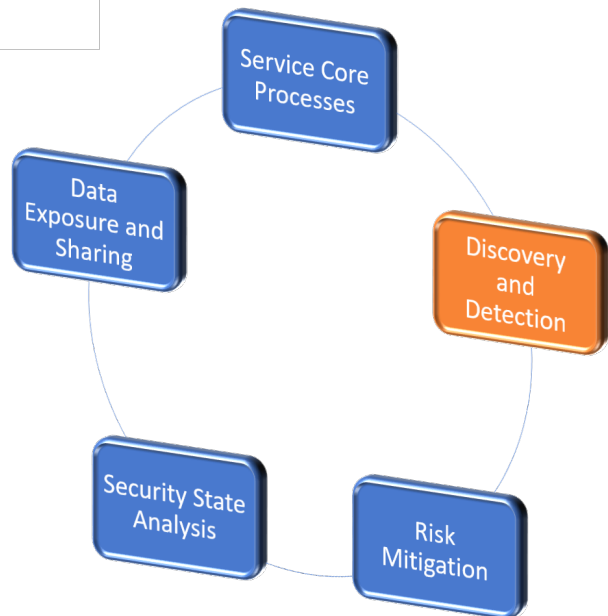
## Security Configuration Management- Core Processes

- Create and distribute content for configuring all technologies that are resident to the network
- Content:
  - Center for Internet Security Benchmarks
  - US Defense Information Systems Agency Security Technical Implementation Guides
  - Information Assurance Vulnerability Management
  - Industry Best Practices
  - Stakeholders



## Security Configuration Management- Discovery and Detection

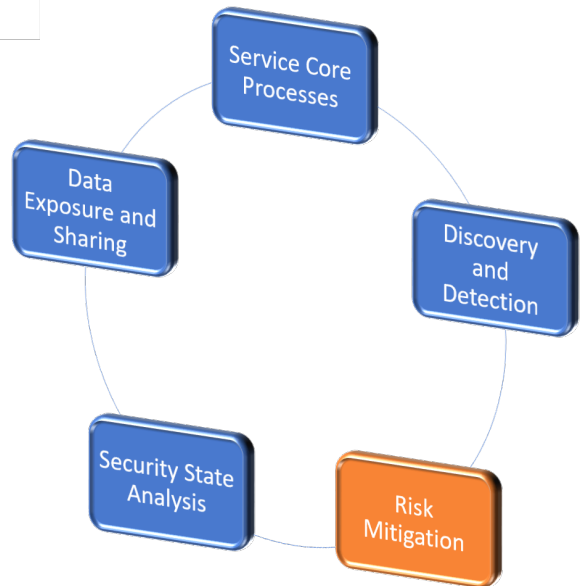
- Discover and audit assets with standardized automated tools
  - Network scans and Host Reporting
- Tools:
  - Policy Compliance Scans
  - Mobile Device Compliance Reports





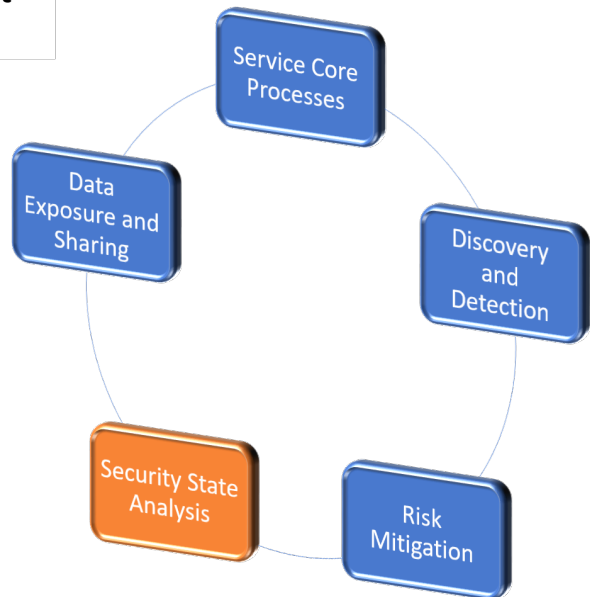
### Security Configuration Management- Risk Mitigation

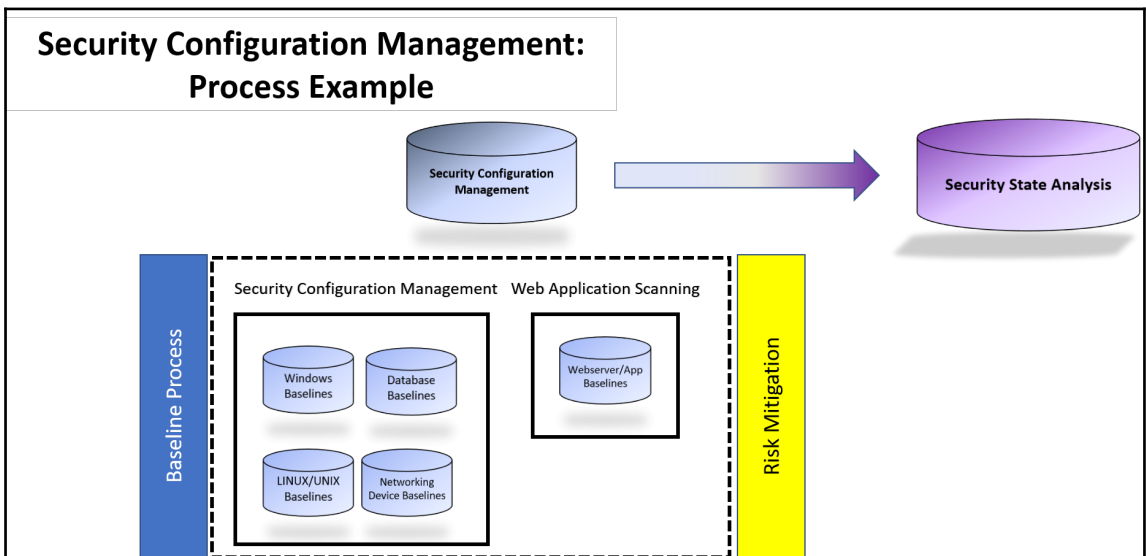
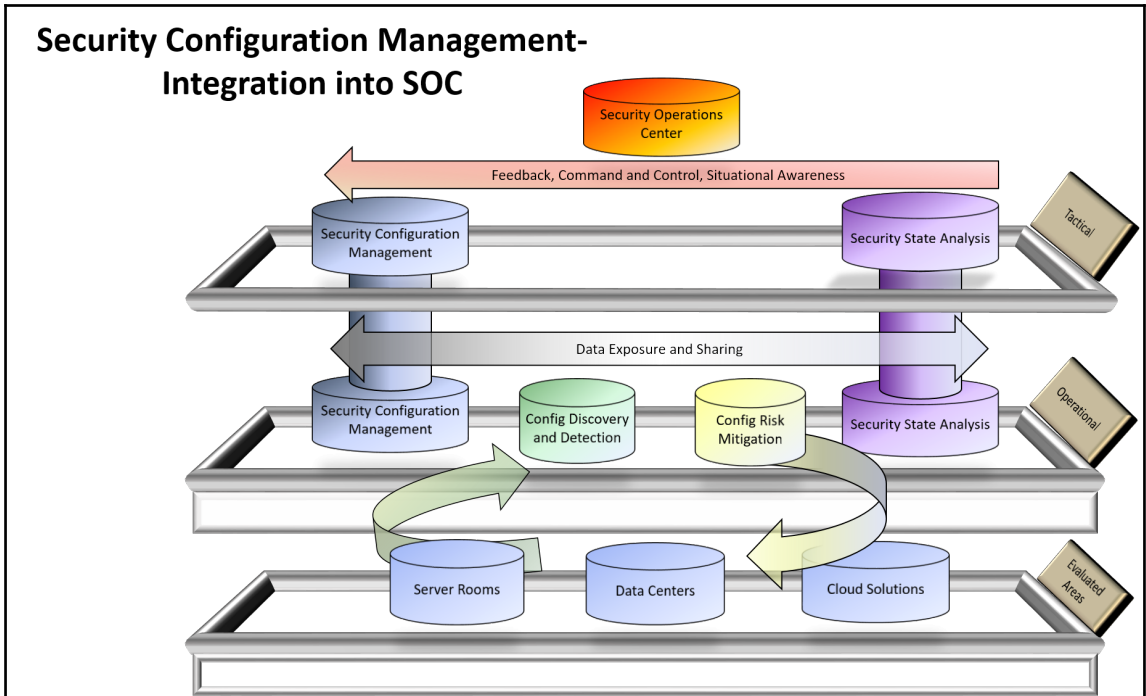
- Assess the risk by correlating asset attributes and compliance evidence
- Situational awareness for stakeholders provided through reports

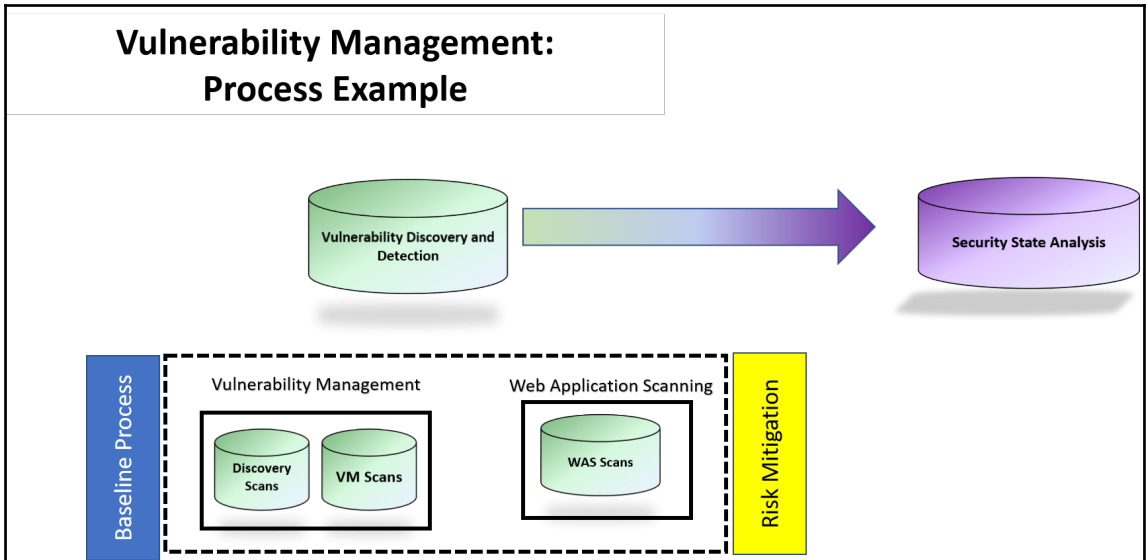


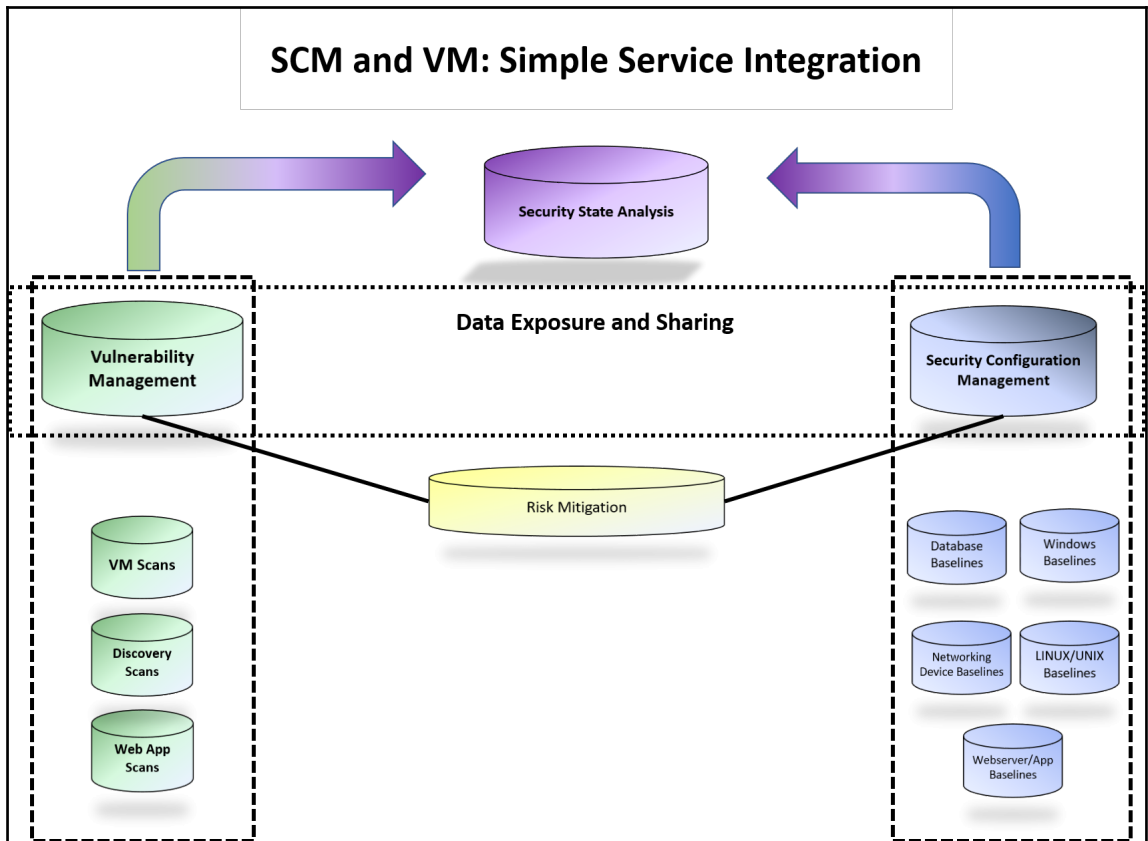
### Security Configuration Management- Security State Analysis

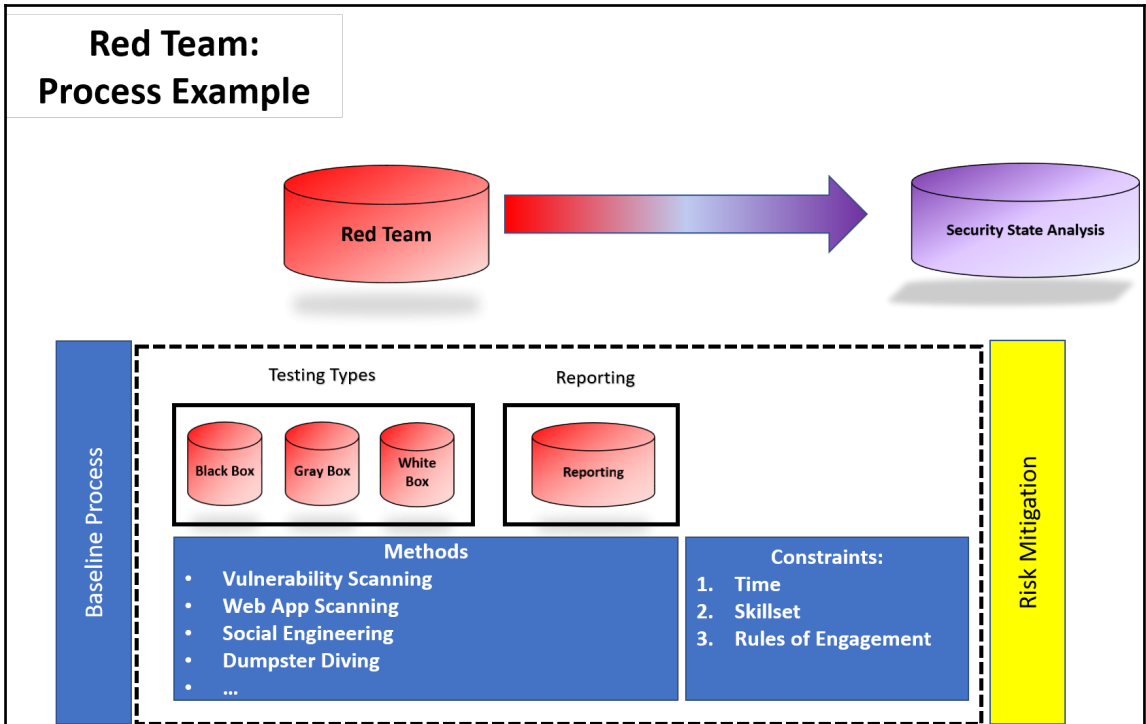
- Provide cognizance of the state of security for:
  - Regions
  - Countries
  - Business Units
  - Application Owners
  - Operating Systems
  - Networking Devices

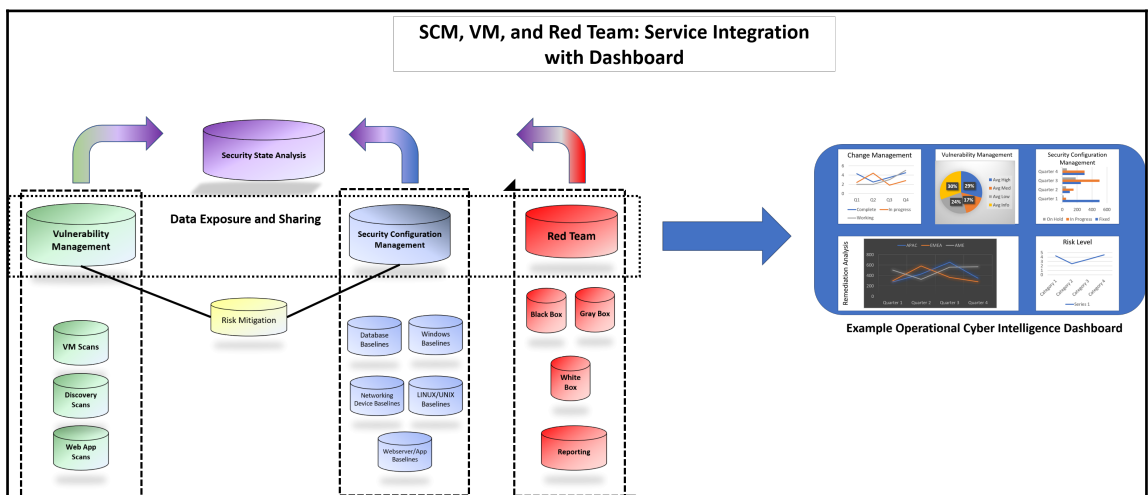
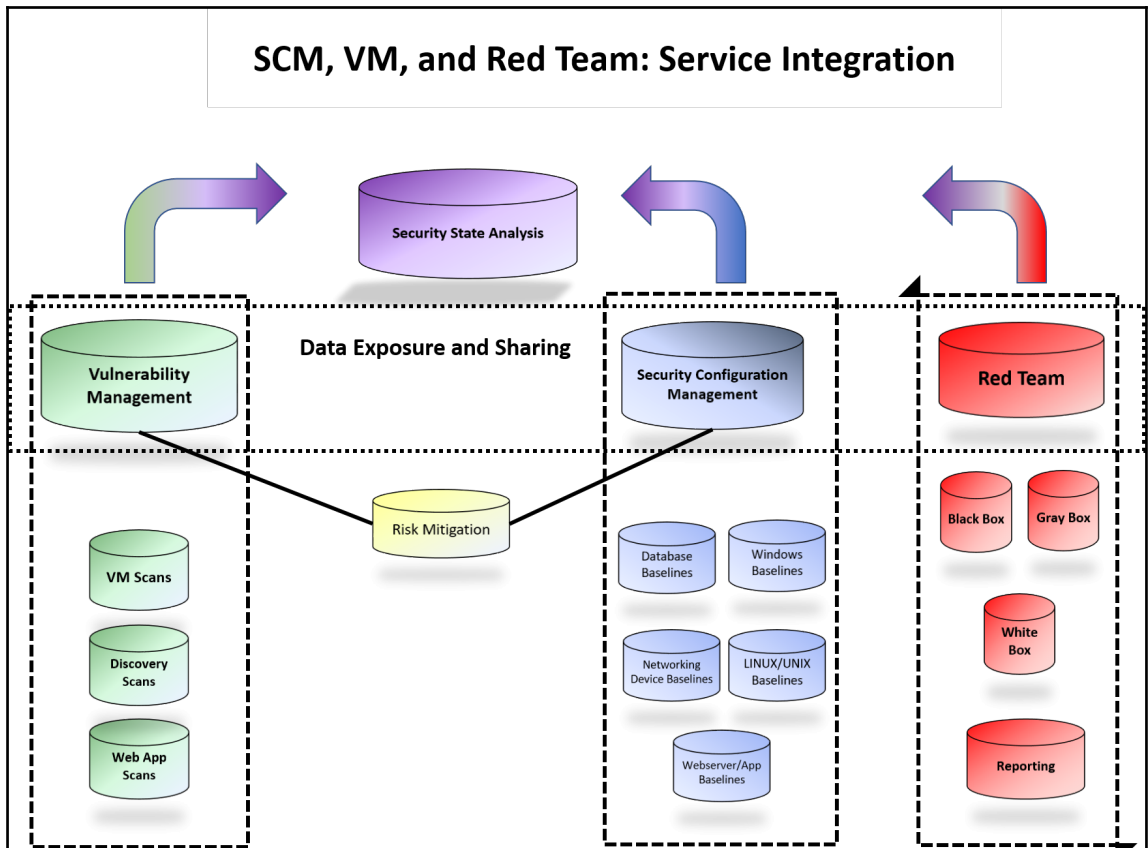


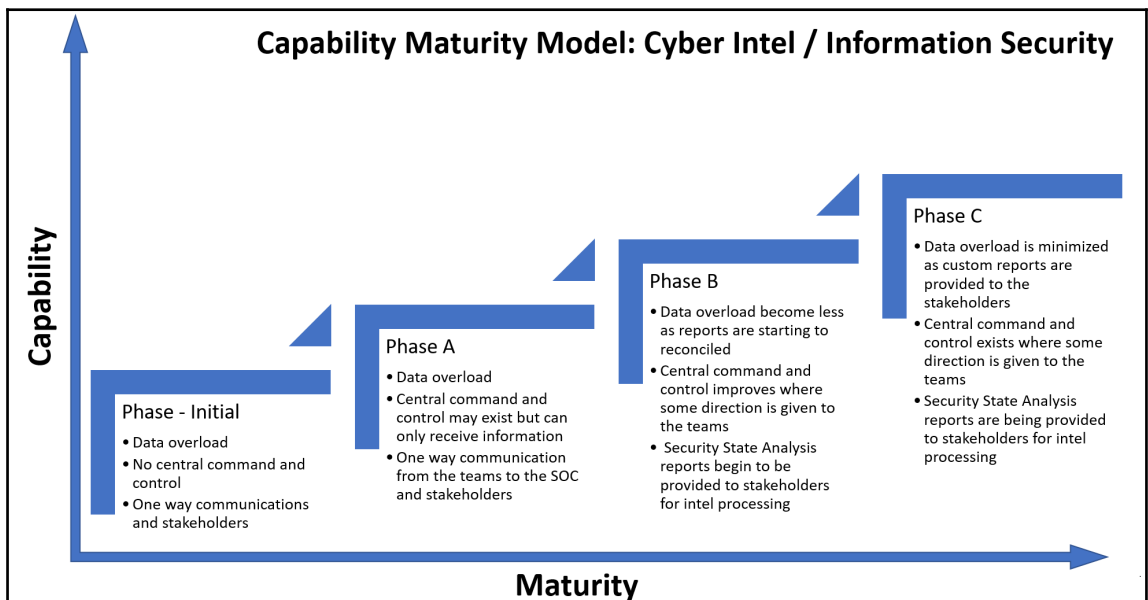
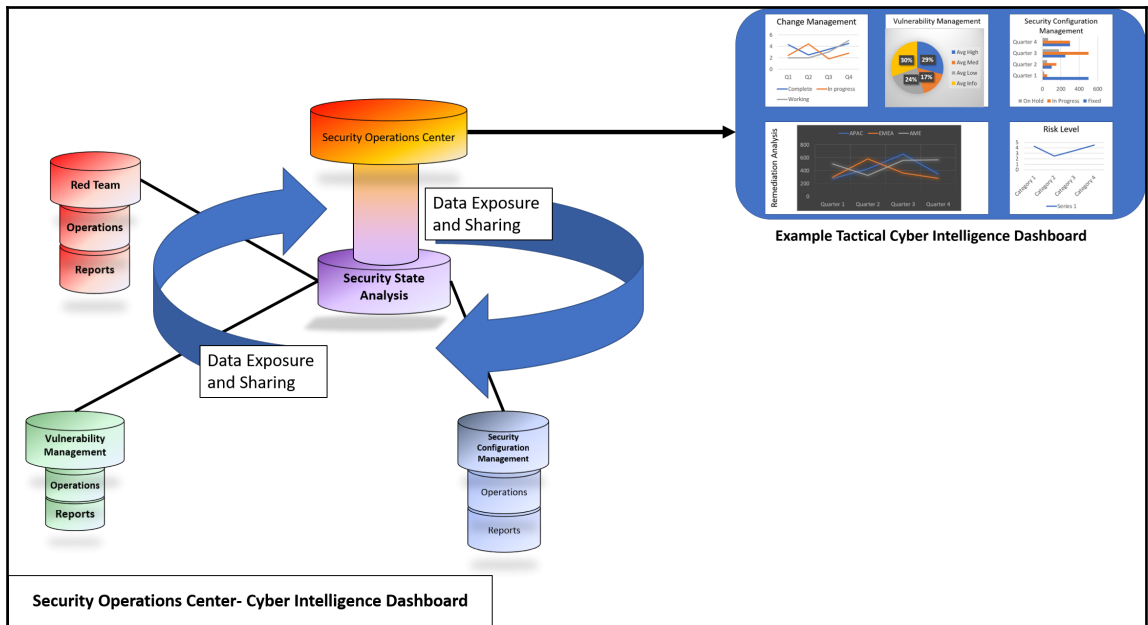




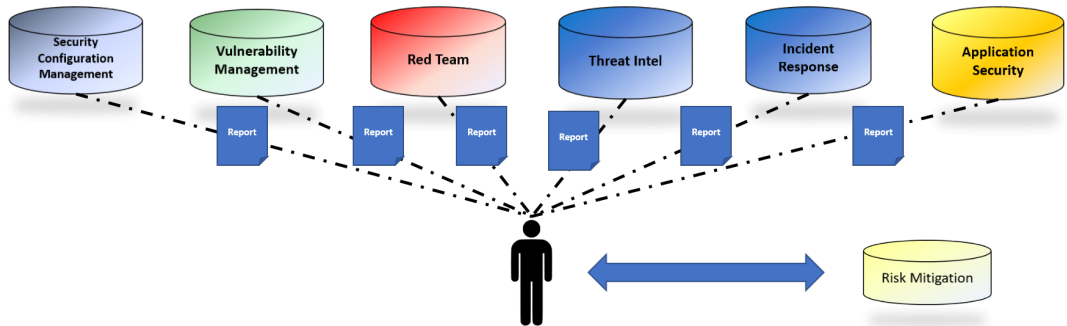




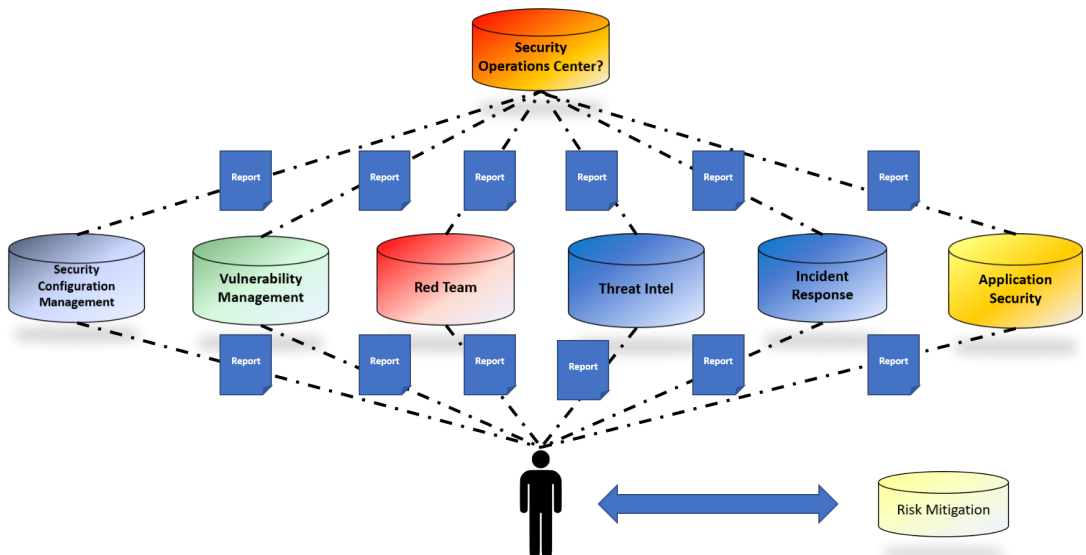




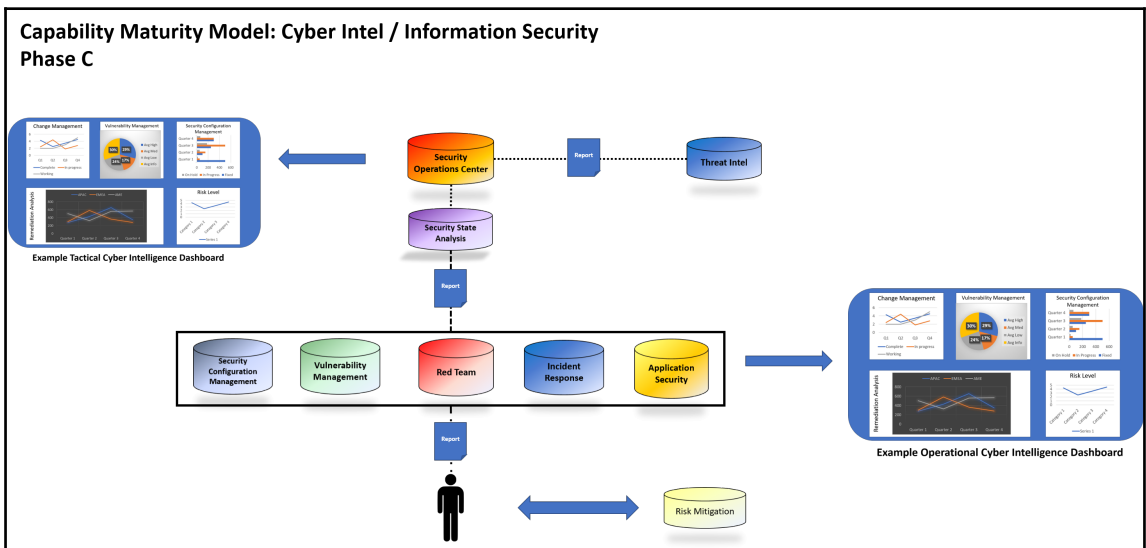
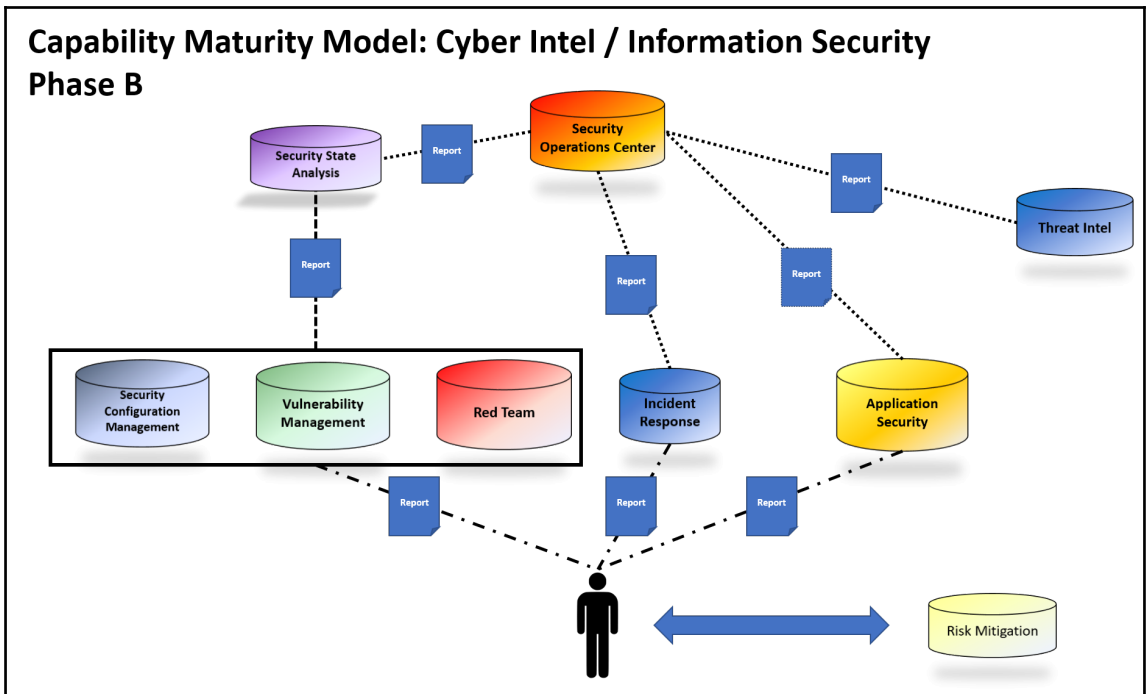
### Capability Maturity Model: Cyber Intel / Information Security Phase Initial



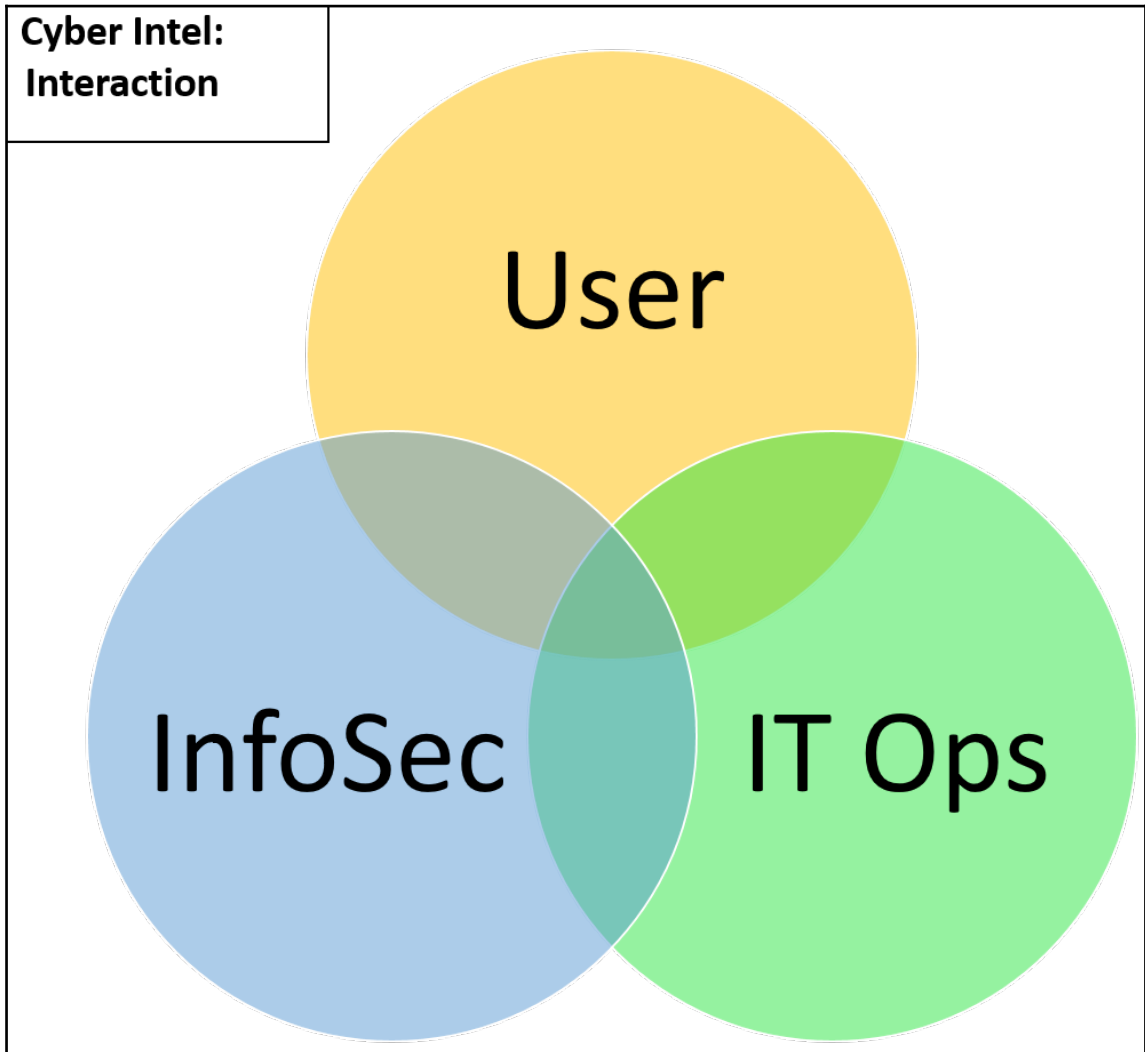
### Capability Maturity Model: Cyber Intel / Information Security Phase A

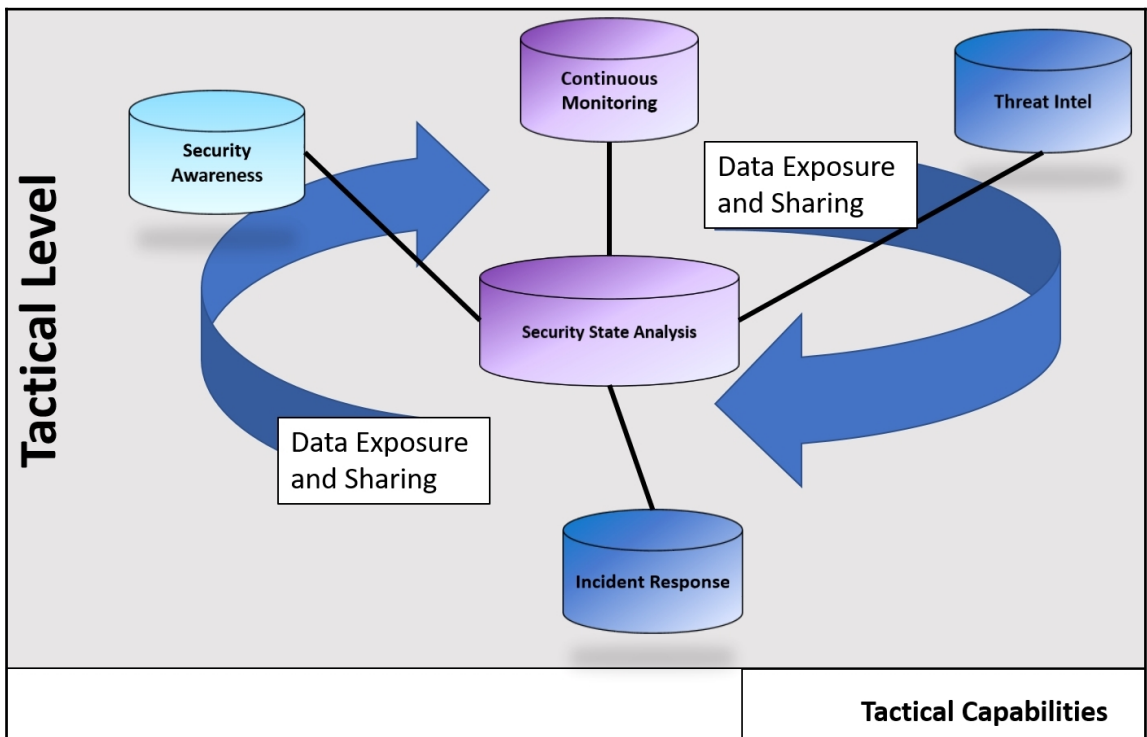
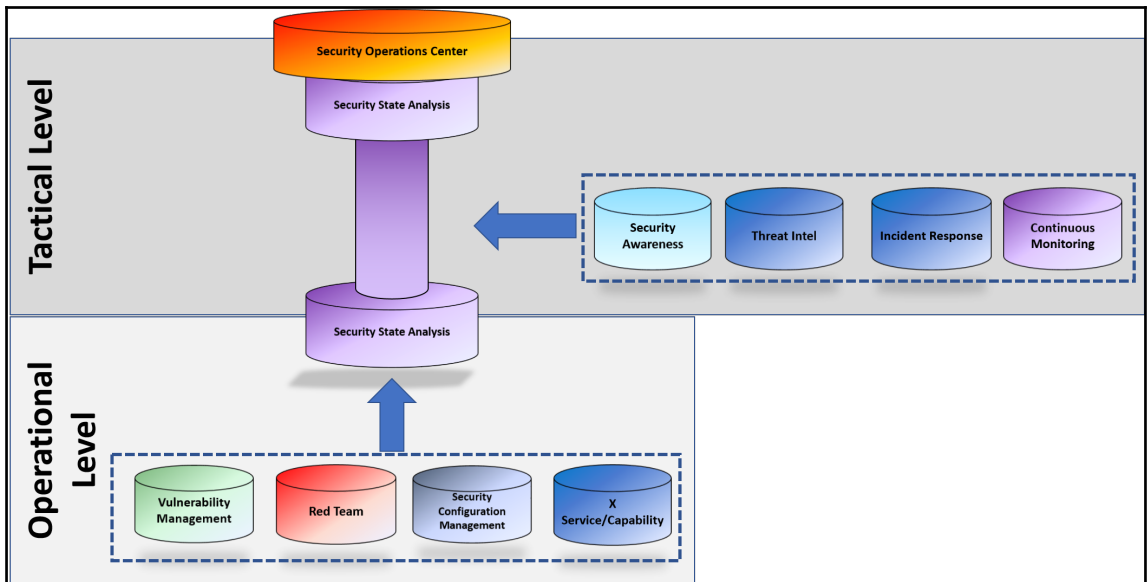


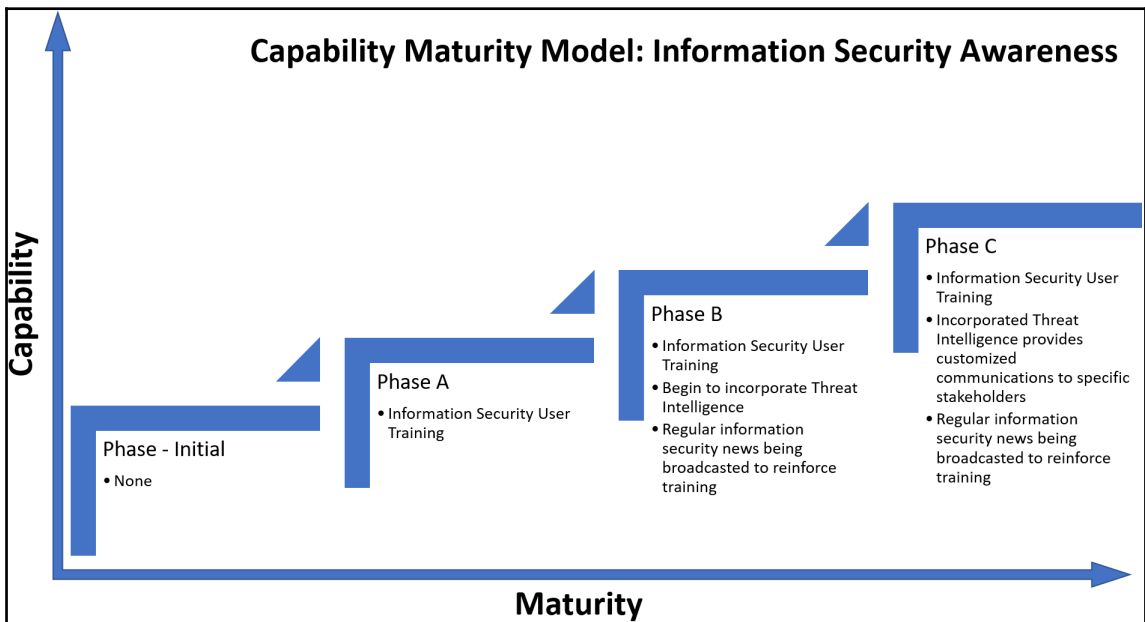
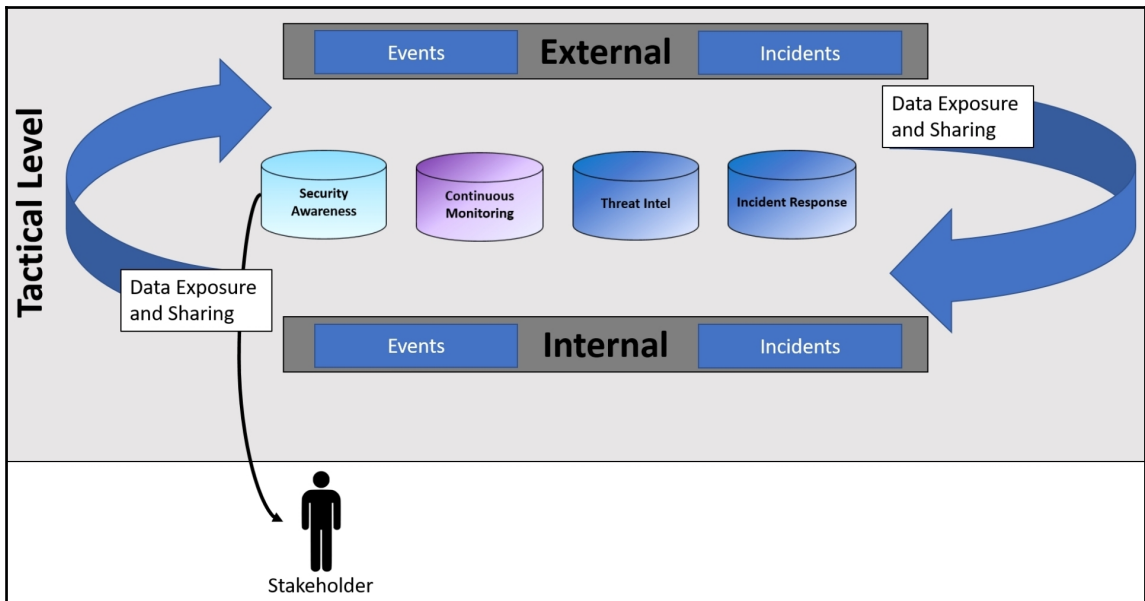


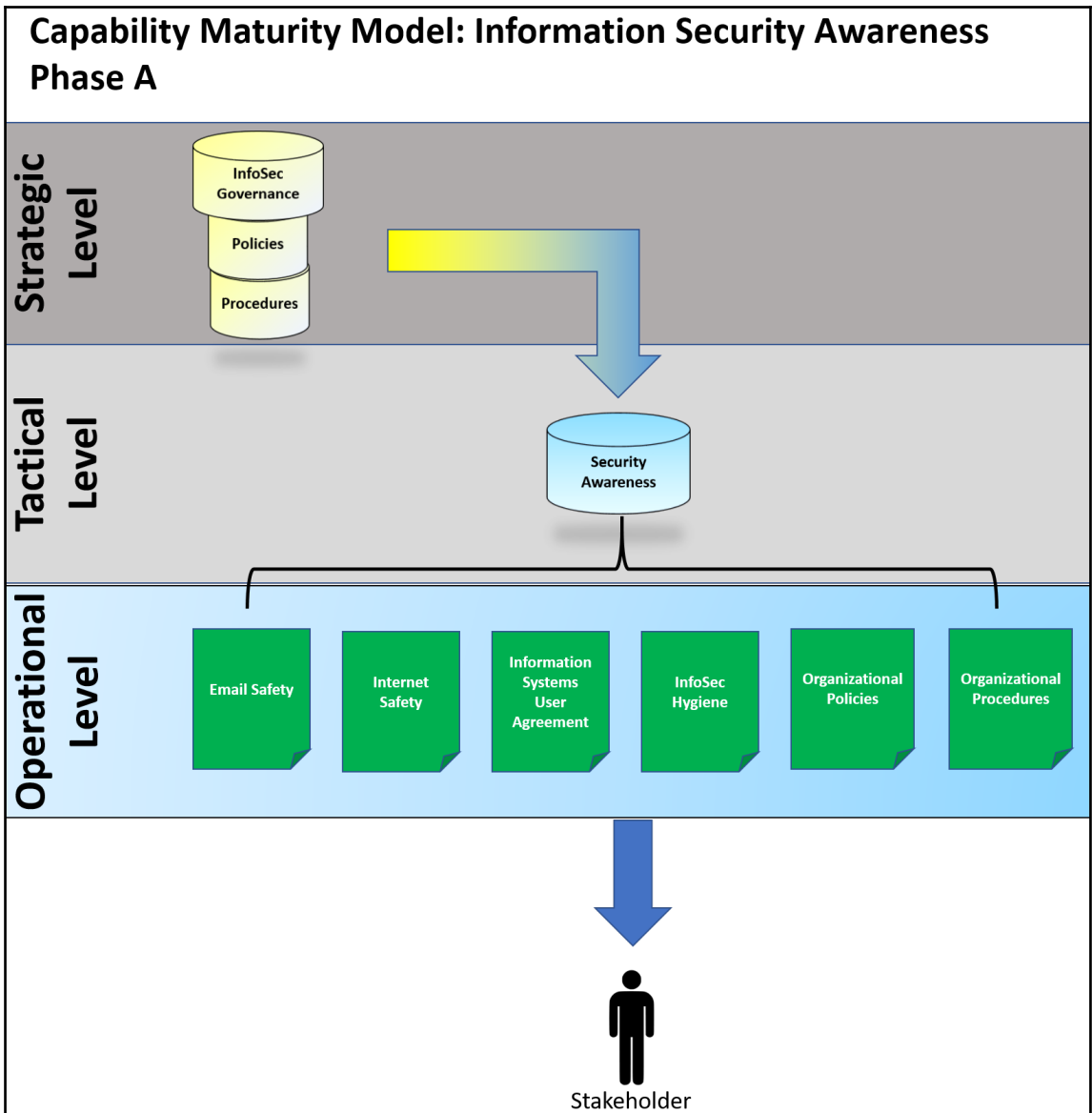


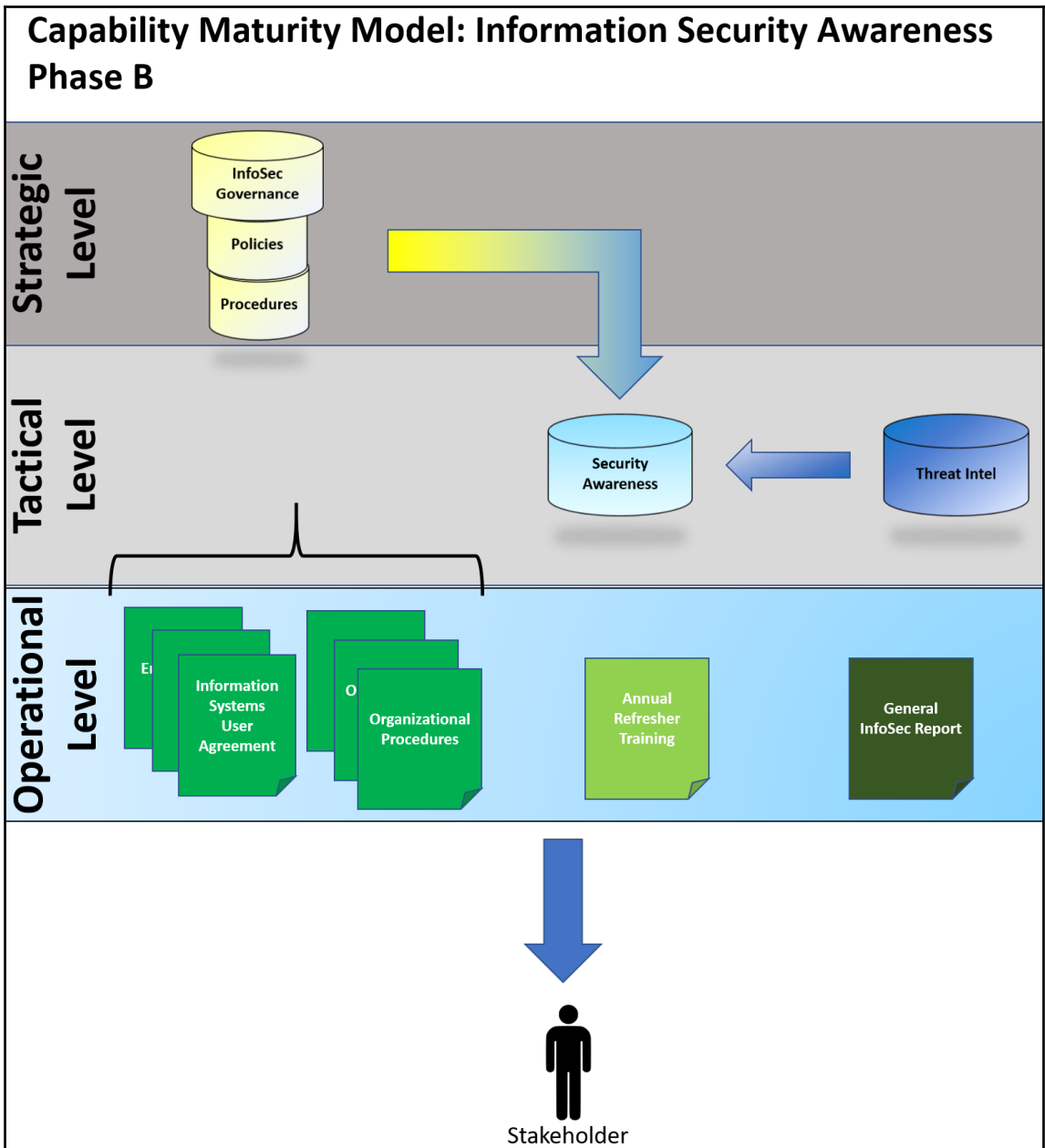
## Chapter 9: Driving Cyber Intel

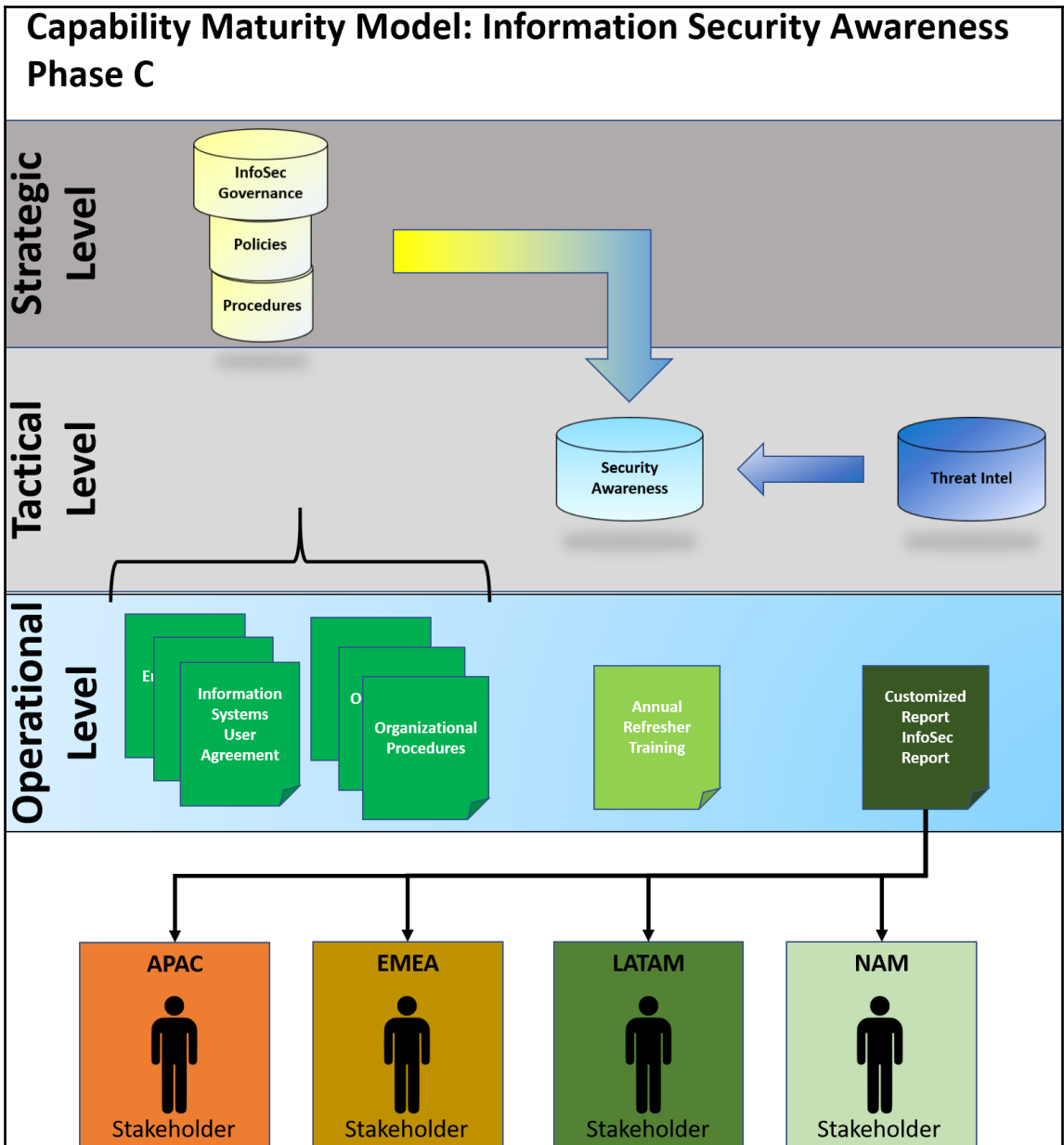


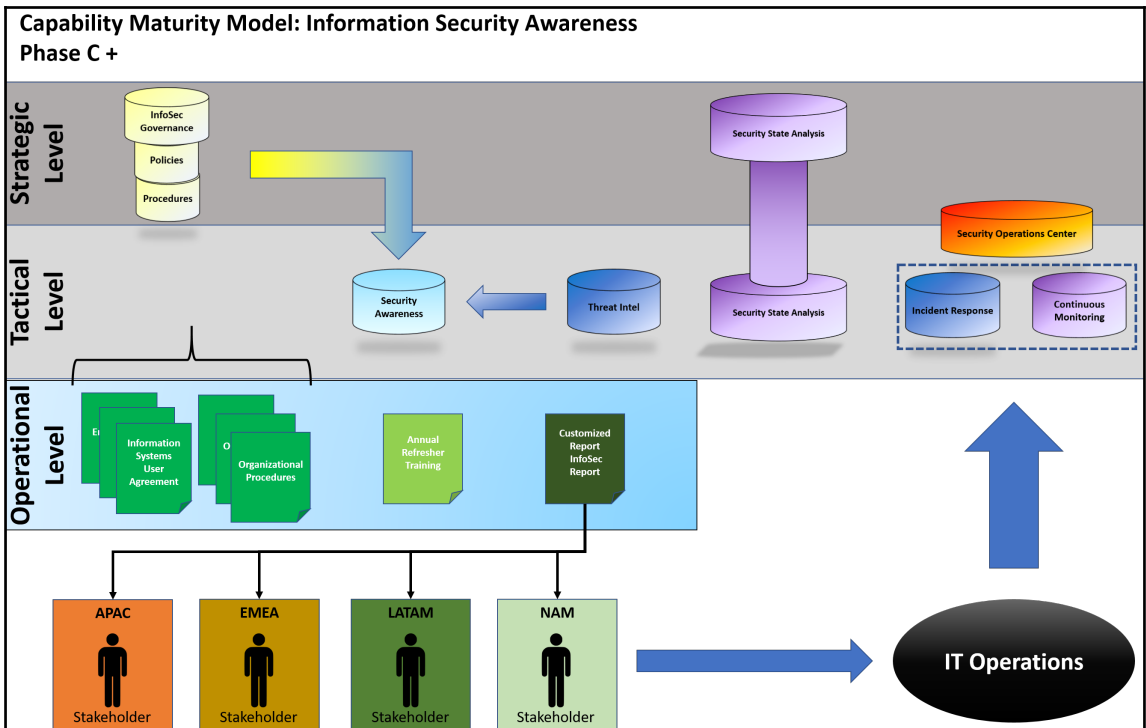






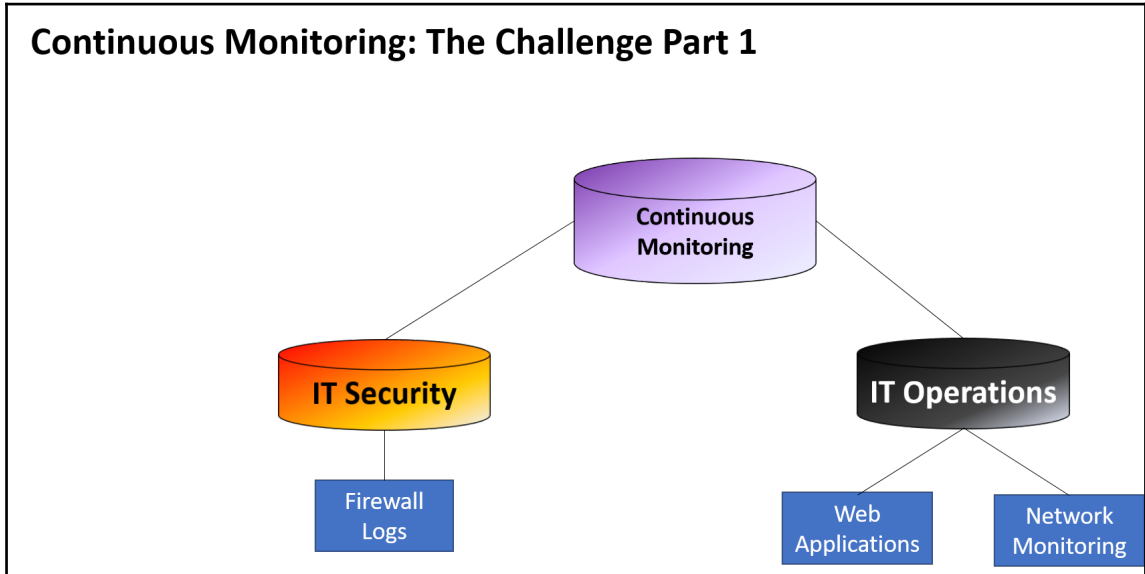


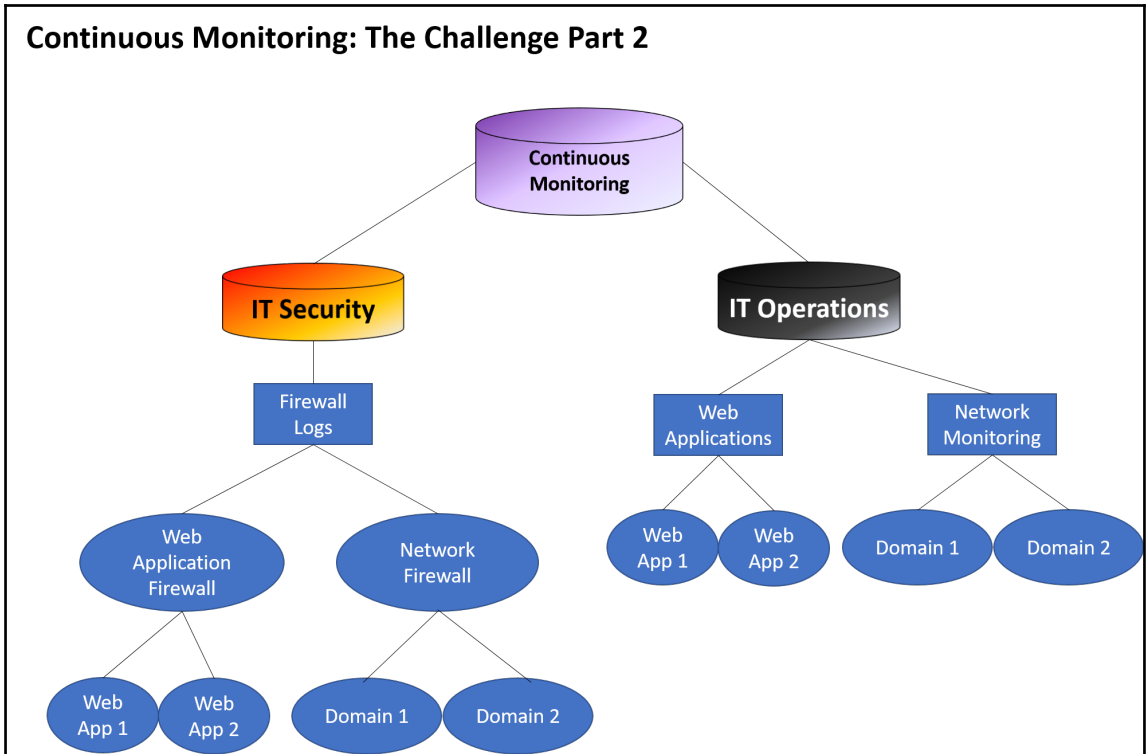




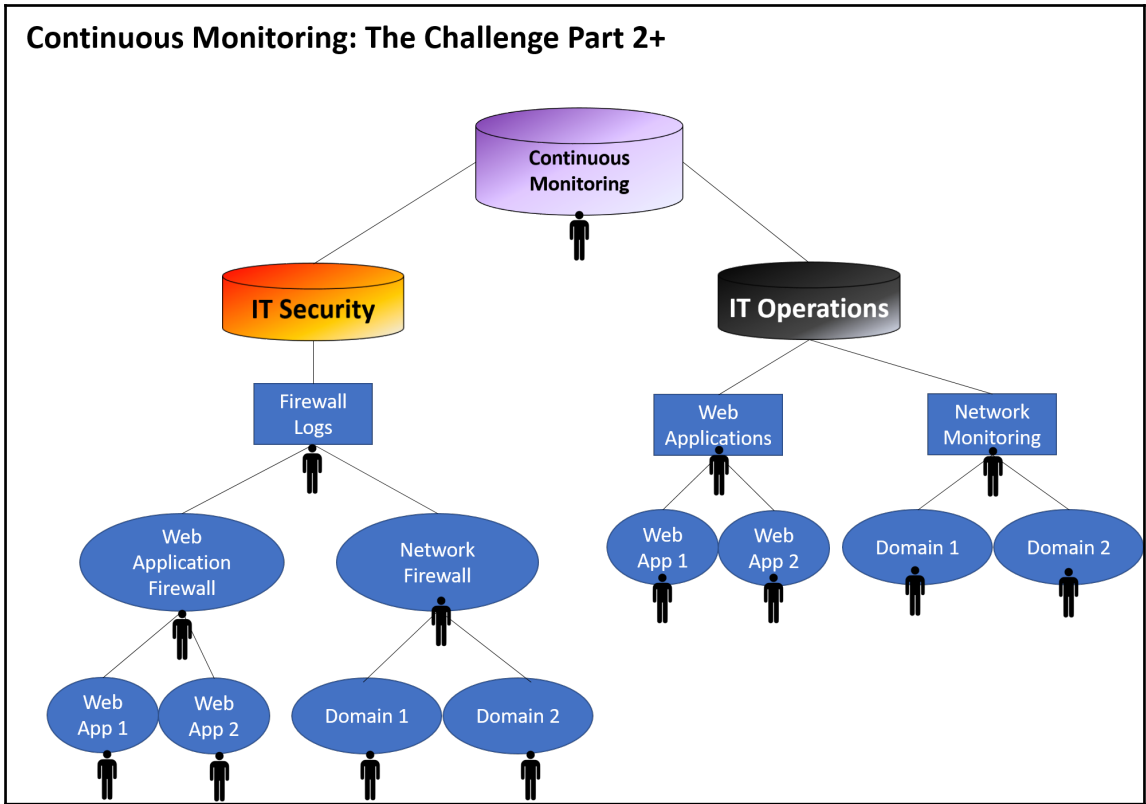


## Chapter 10: Baselines and Anomalies

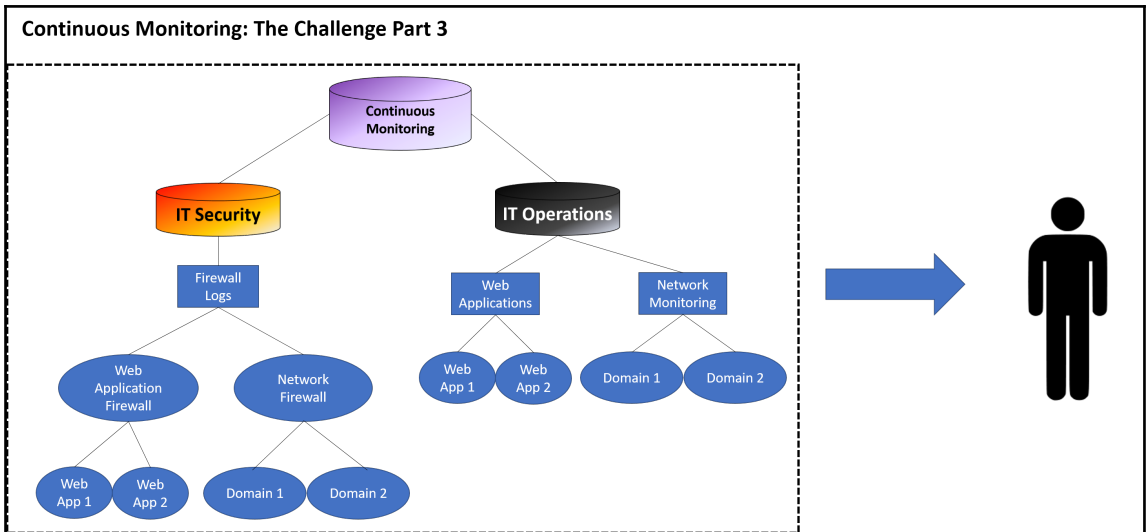


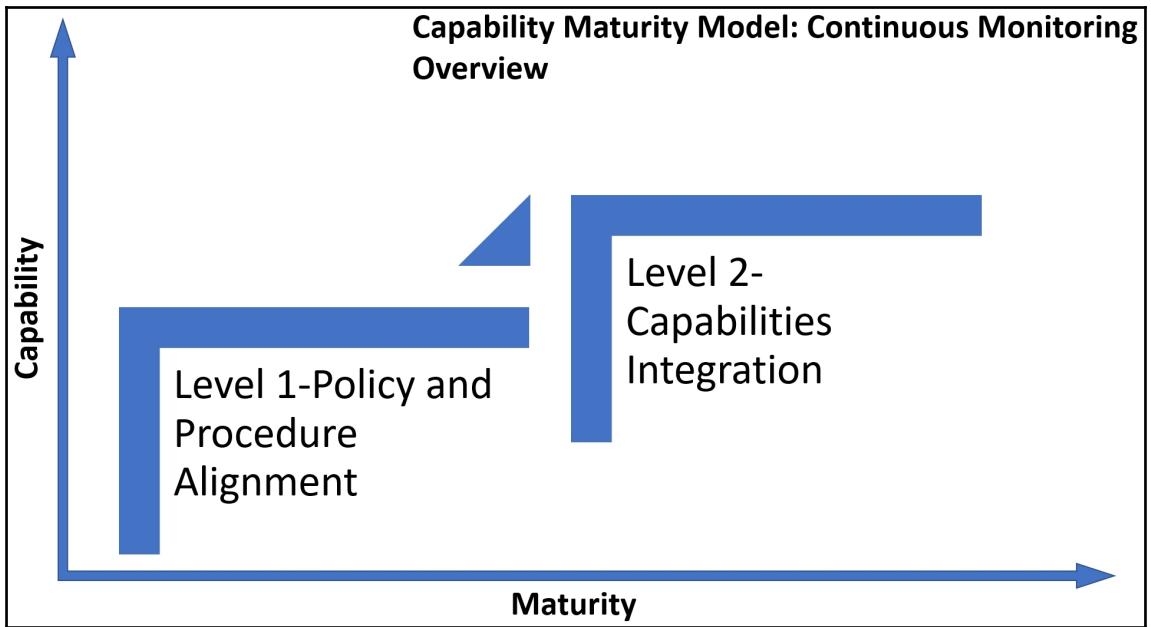


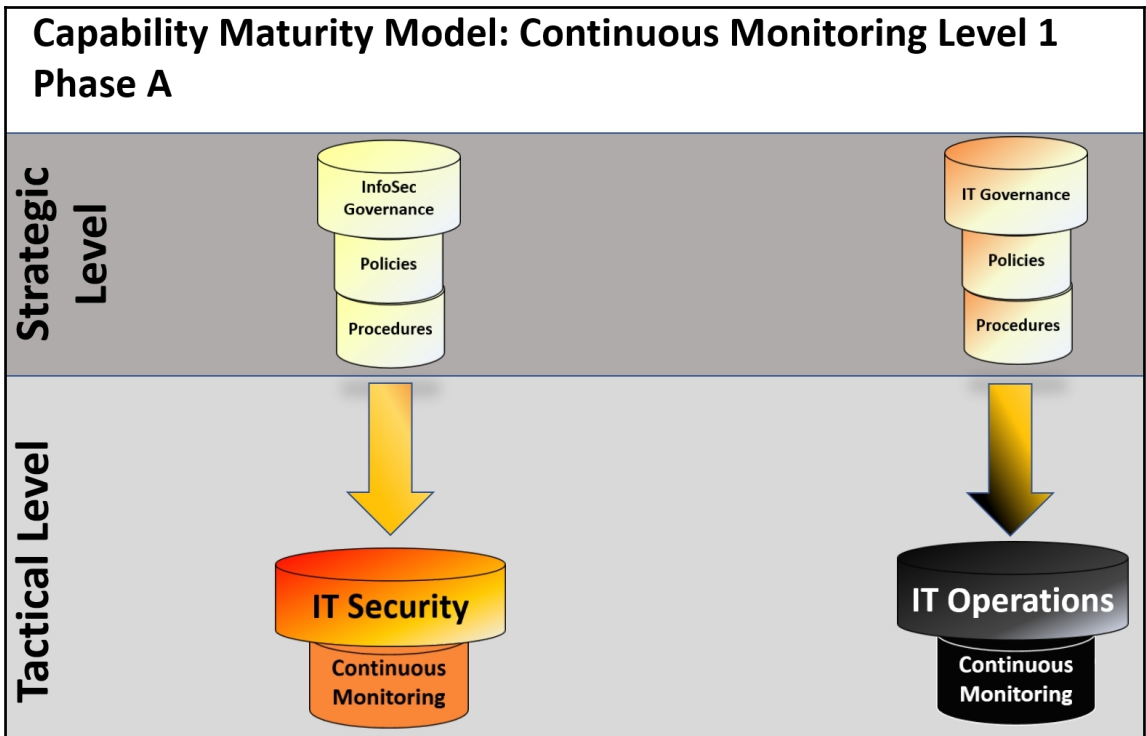
### Continuous Monitoring: The Challenge Part 2+

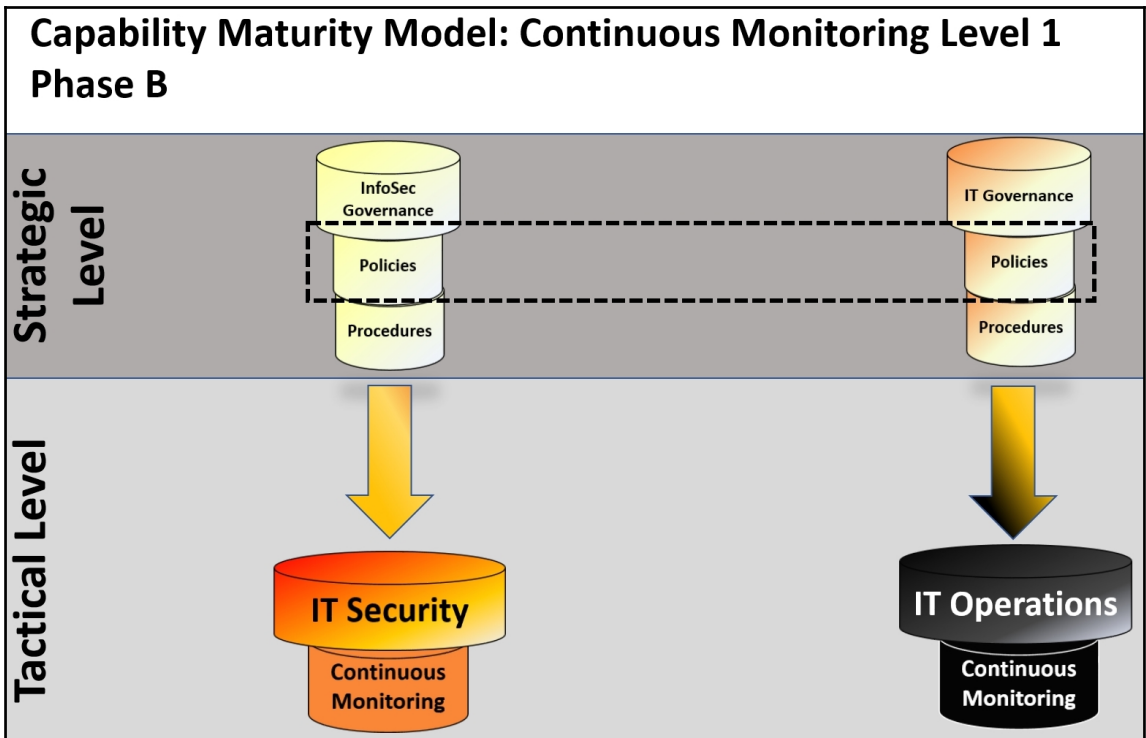


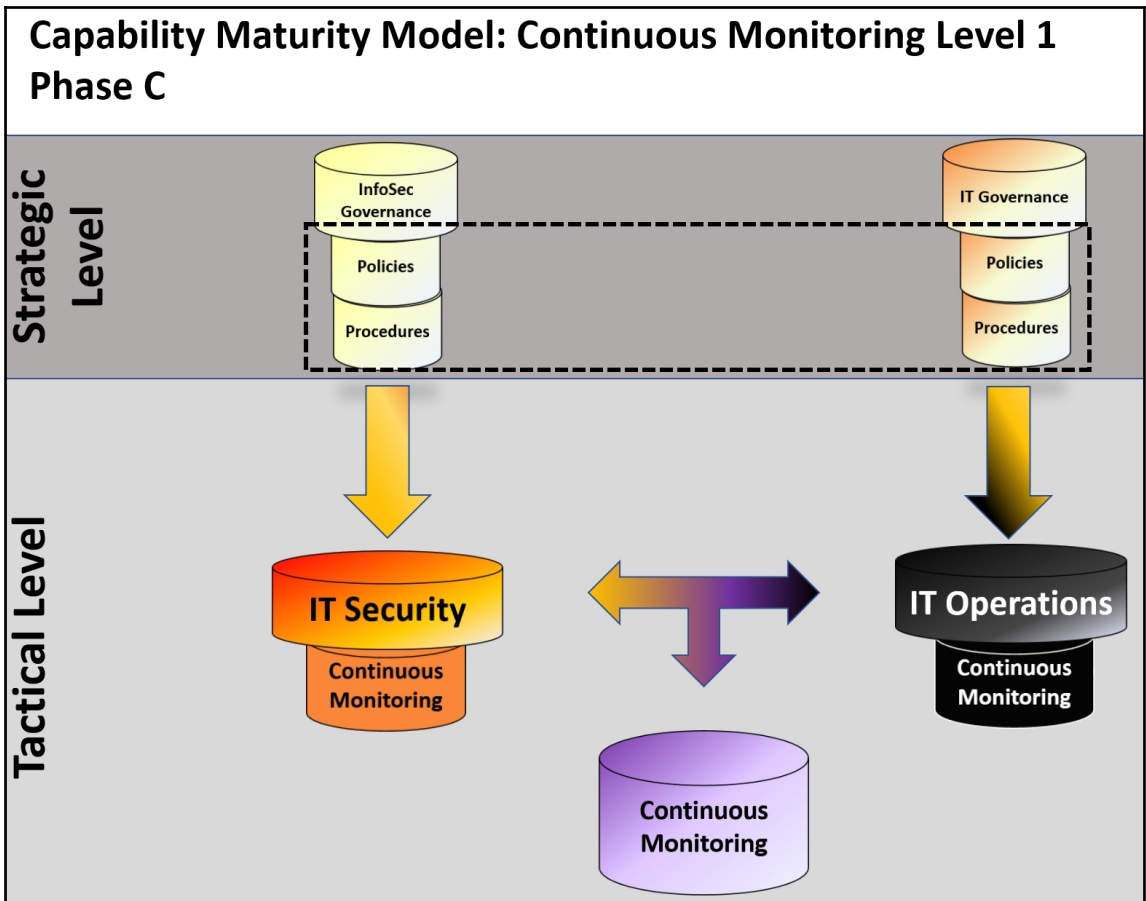
### Continuous Monitoring: The Challenge Part 3

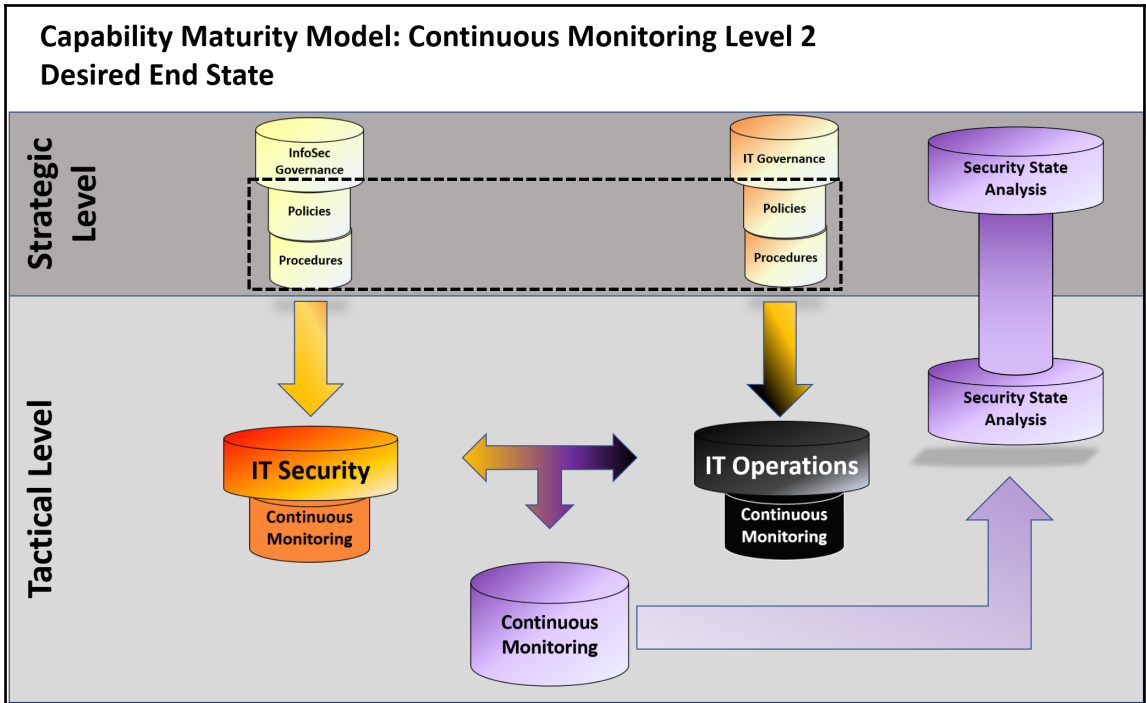






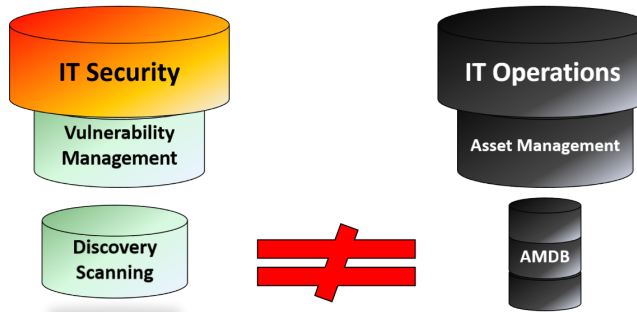






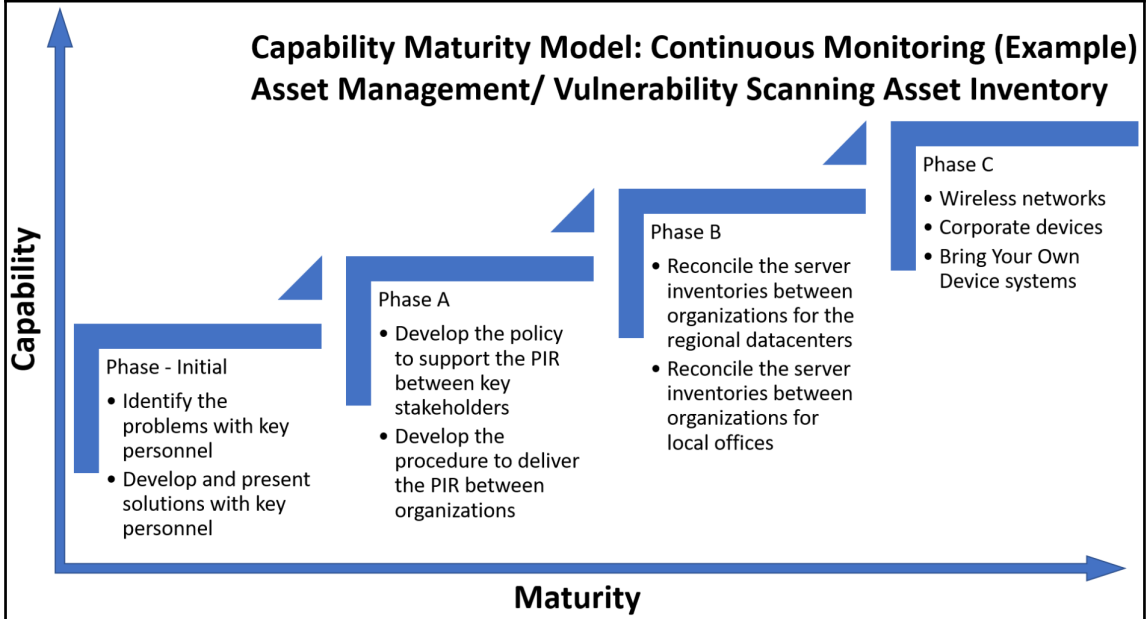


### Capability Maturity Model: Continuous Monitoring Level 2 The Problem



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

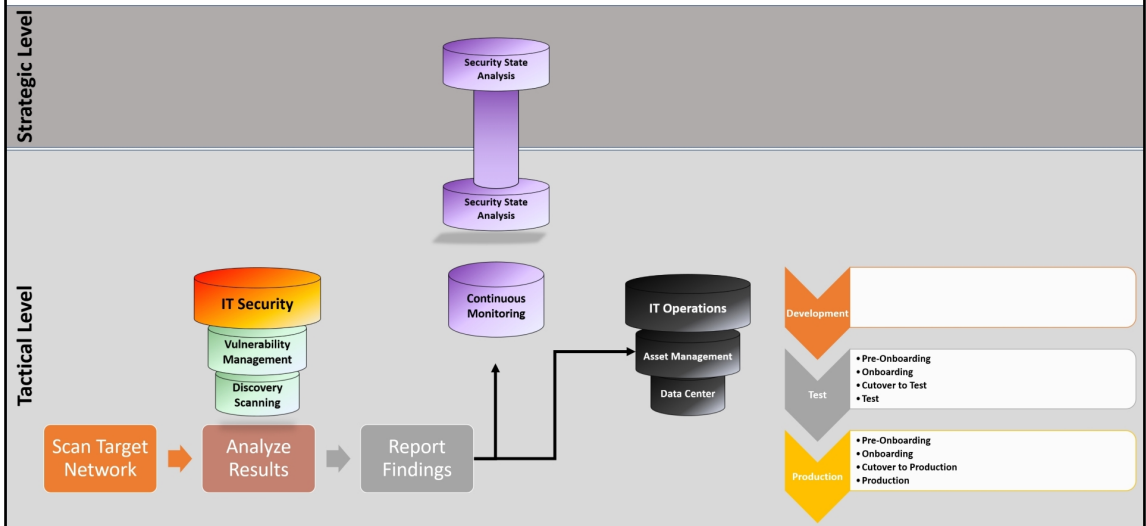
### Capability Maturity Model: Continuous Monitoring (Example) Asset Management/ Vulnerability Scanning Asset Inventory



Capability Maturity Model: Continuous Monitoring Level 2

Phase B Part 1

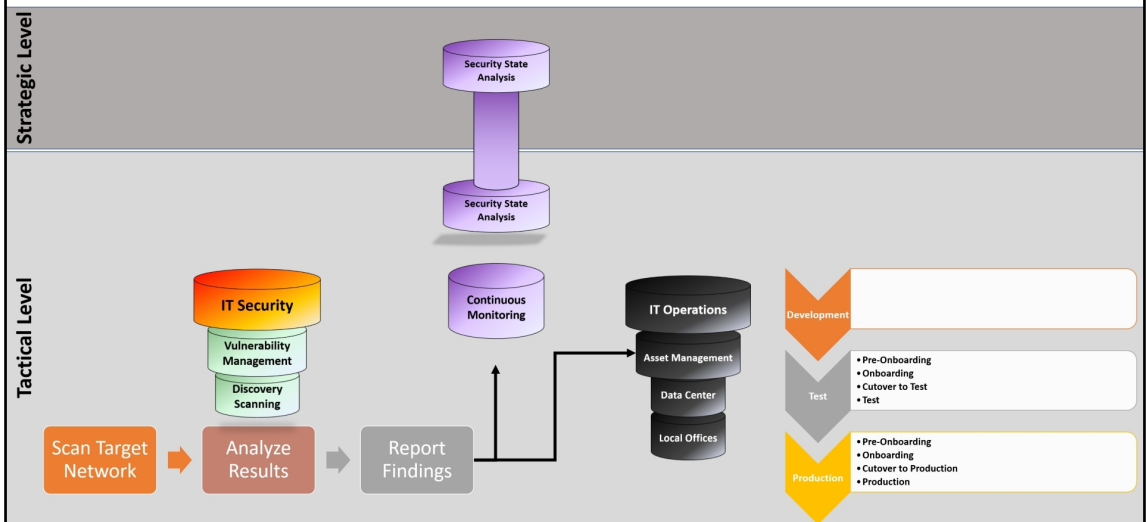
Discovery Scanning / Asset Management



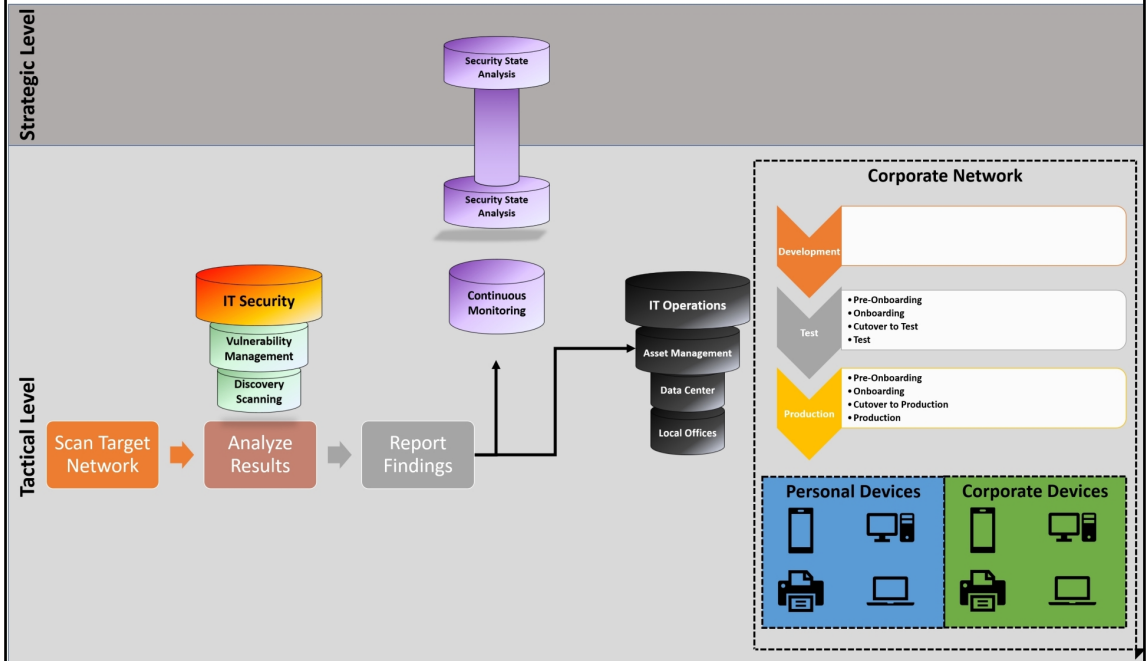
Capability Maturity Model: Continuous Monitoring Level 2

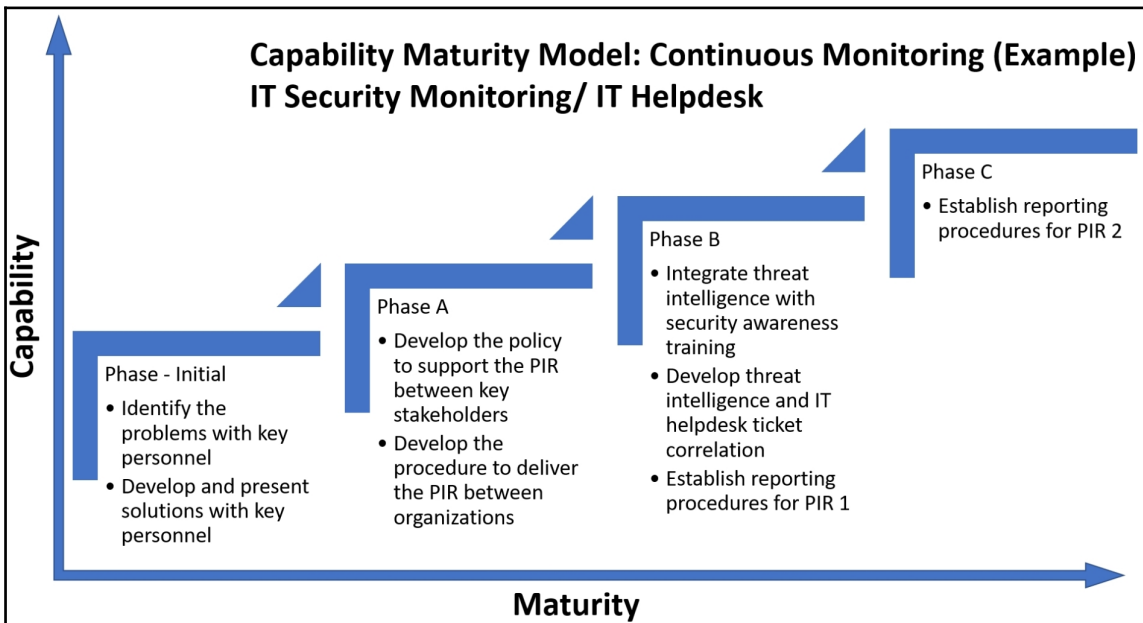
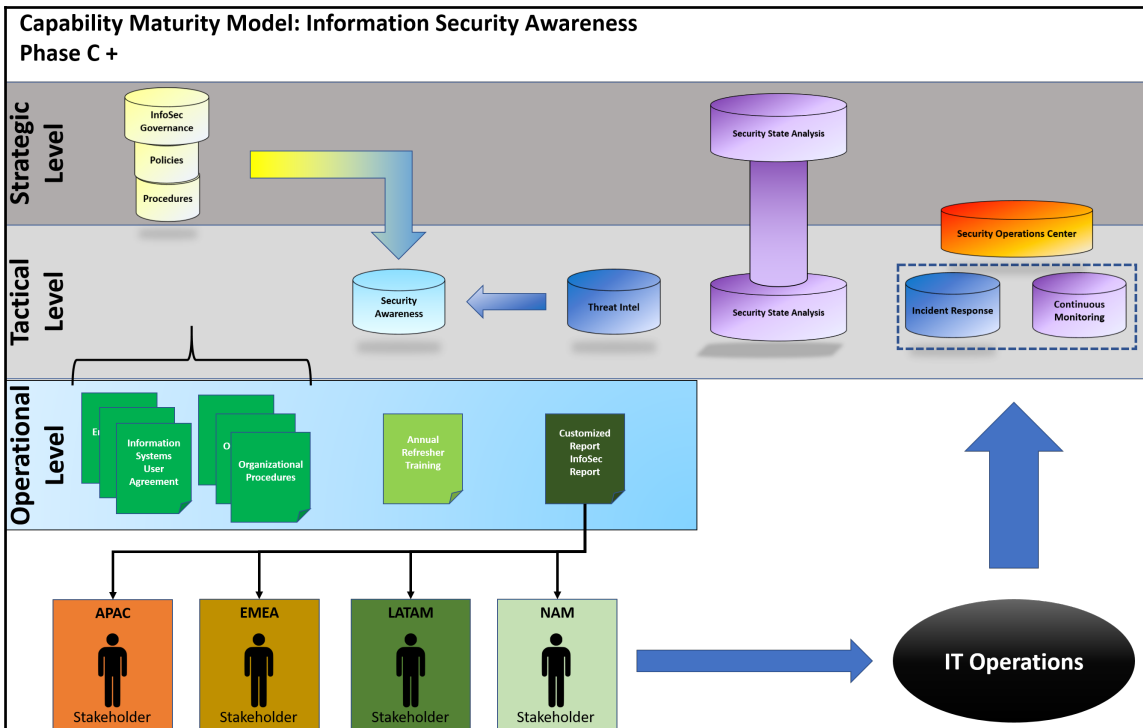
Phase B Part 2

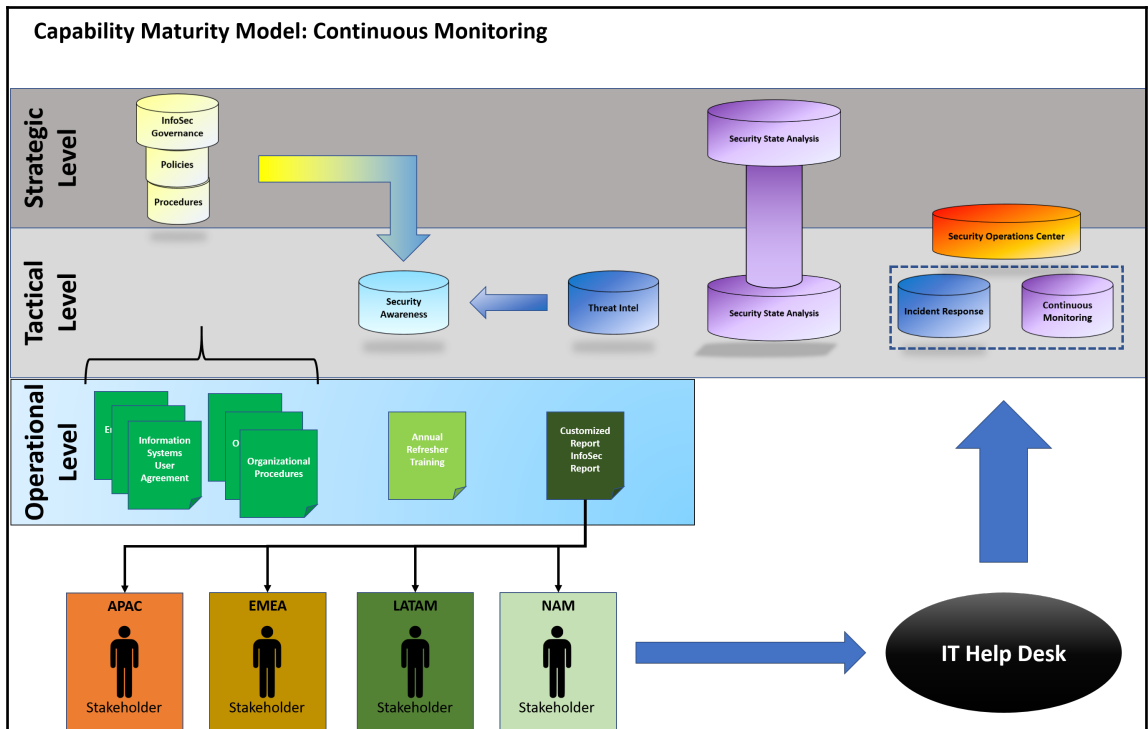
Discovery Scanning / Asset Management



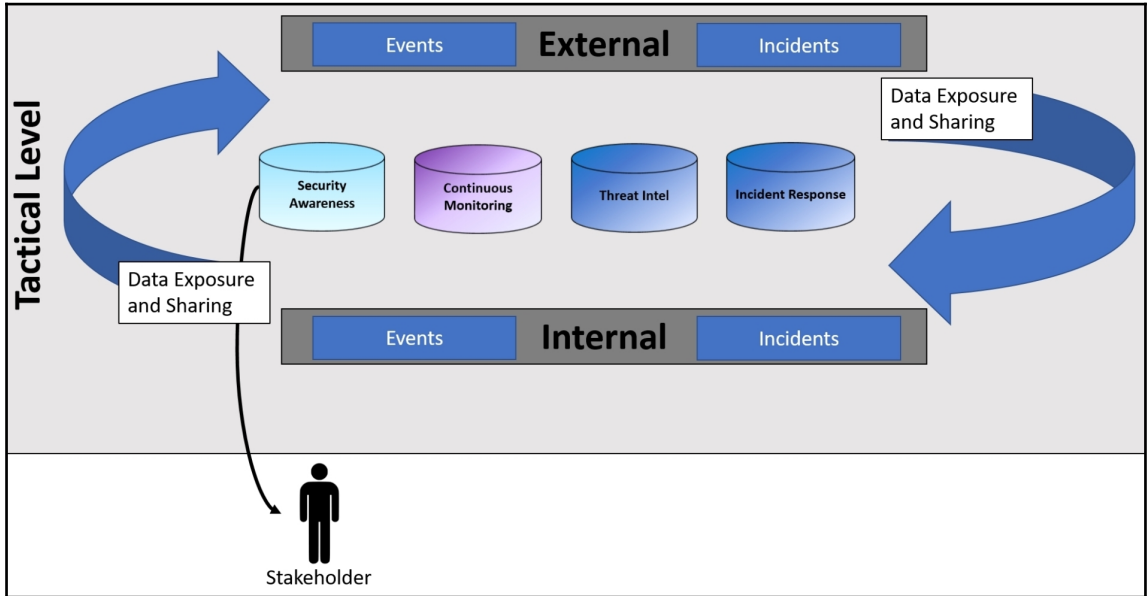
Capability Maturity Model: Continuous Monitoring Level 2  
Phase B Part 3  
Discovery Scanning / Asset Management

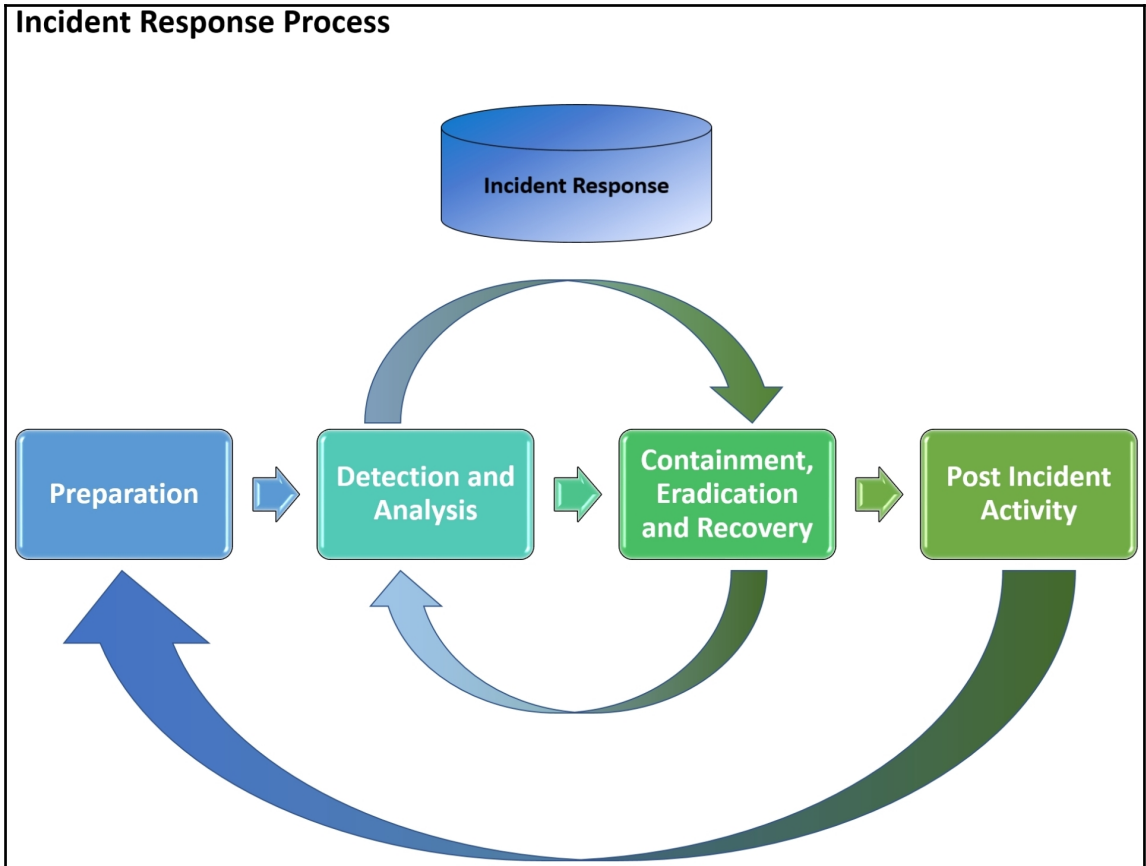


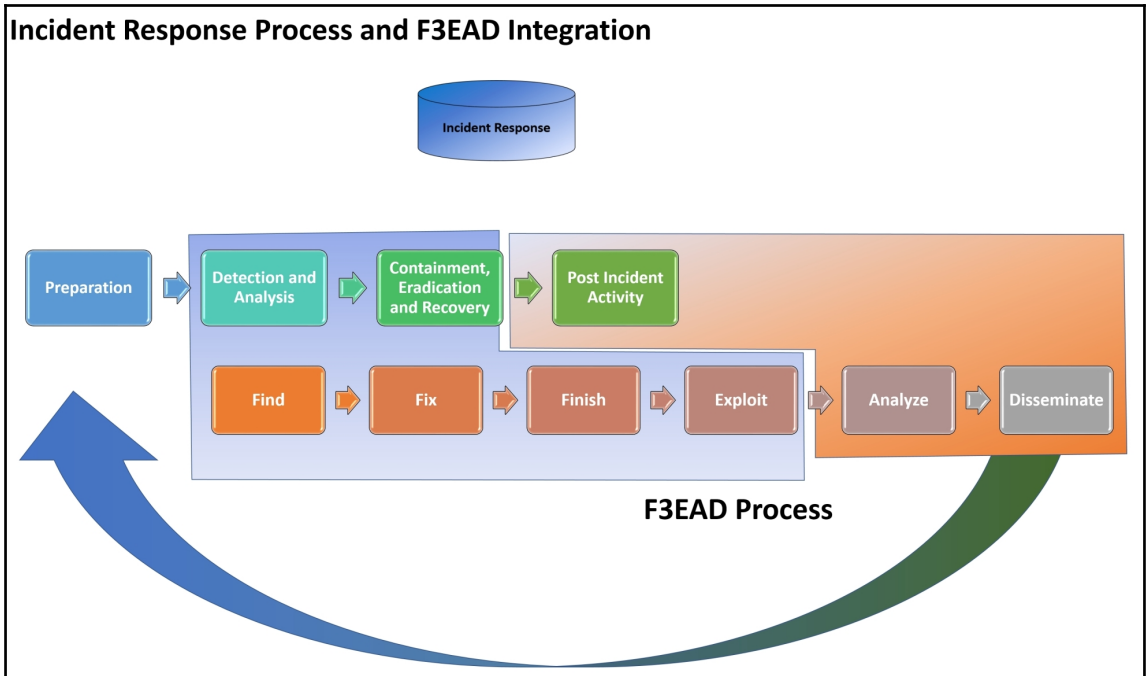




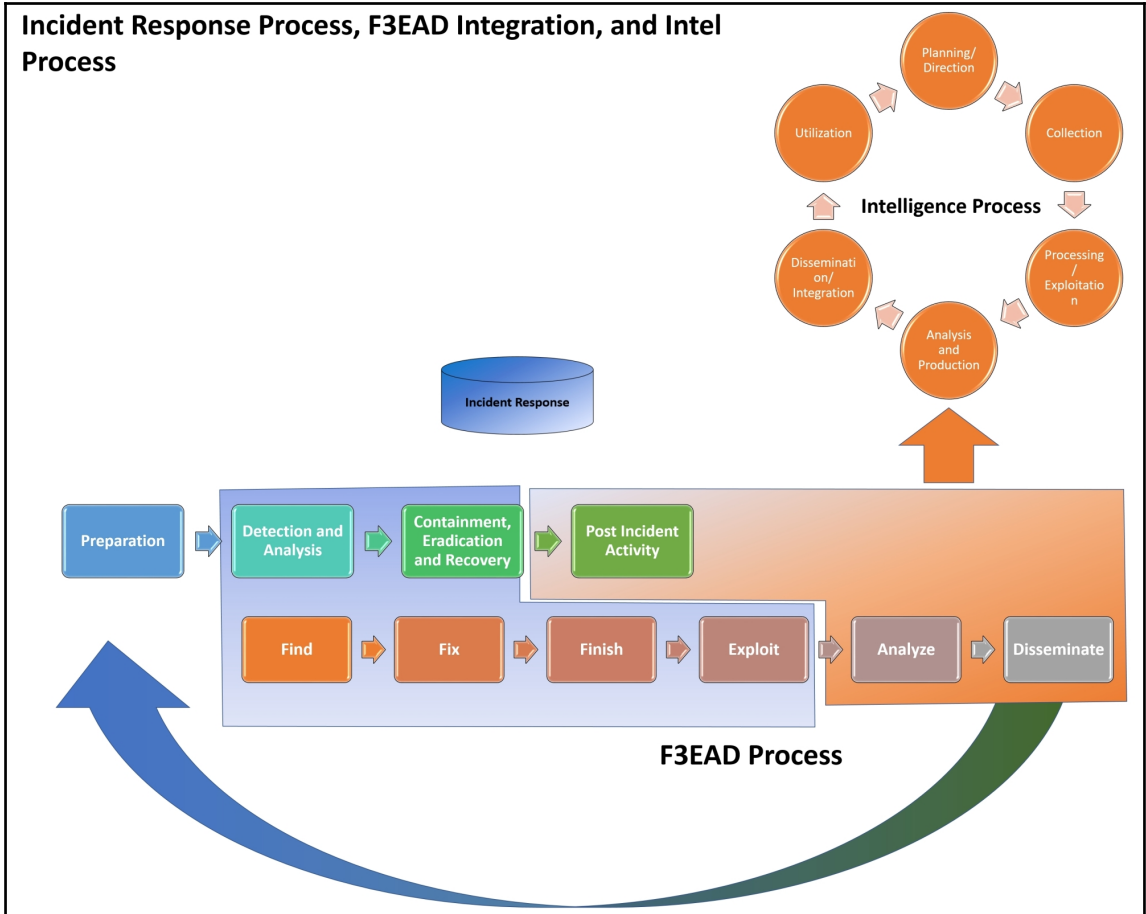
# Chapter 11: Putting Out the Fires

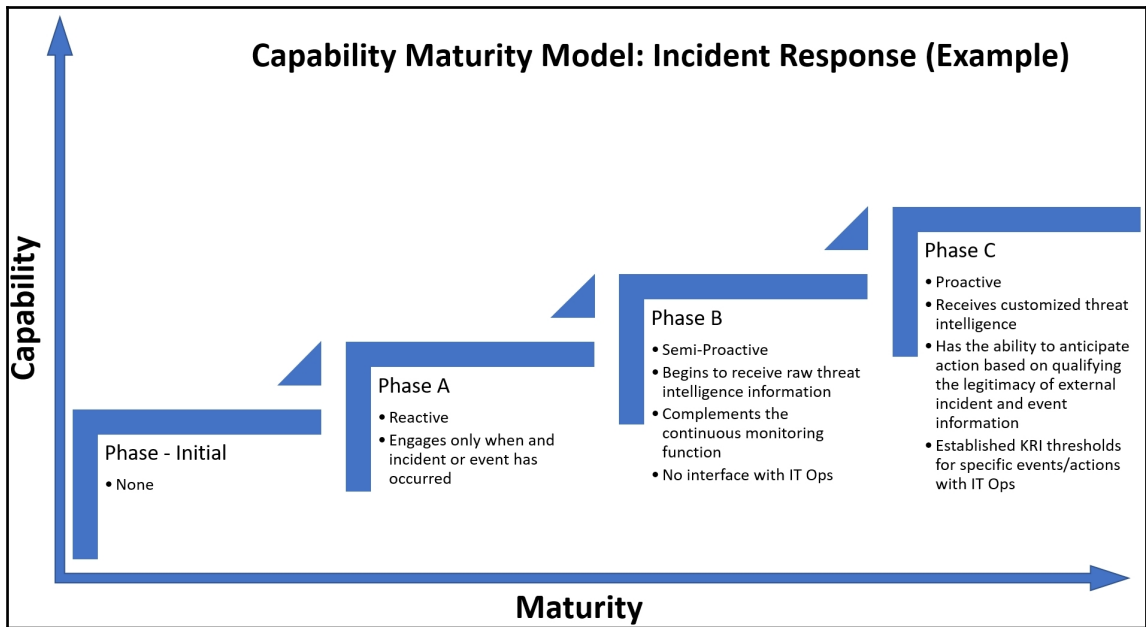


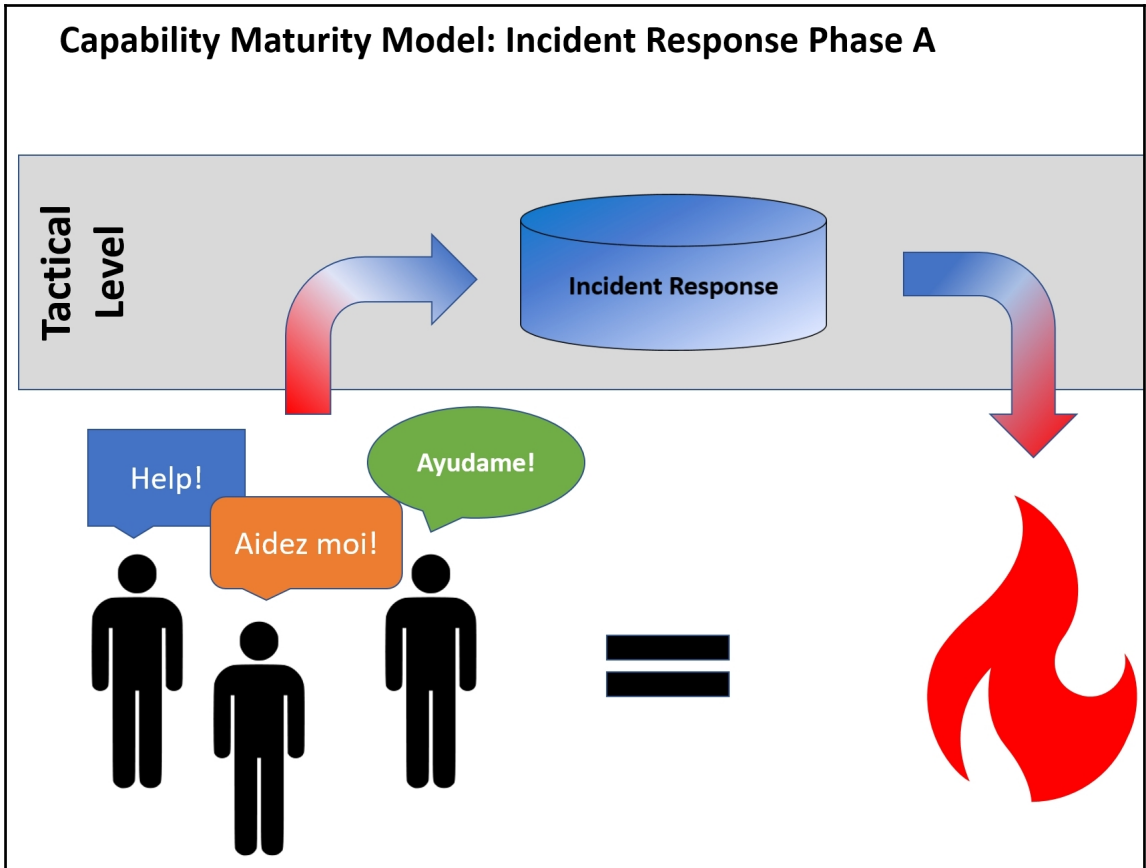


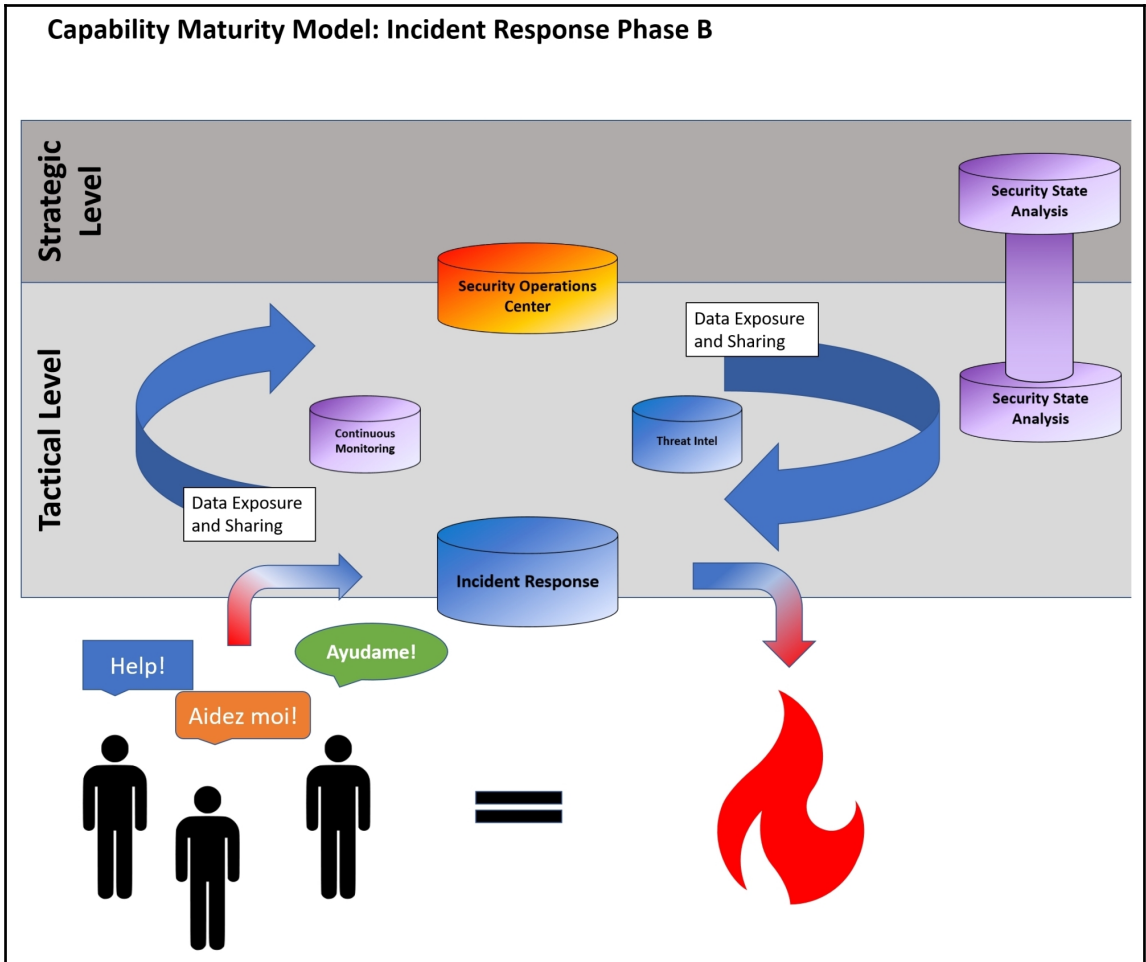


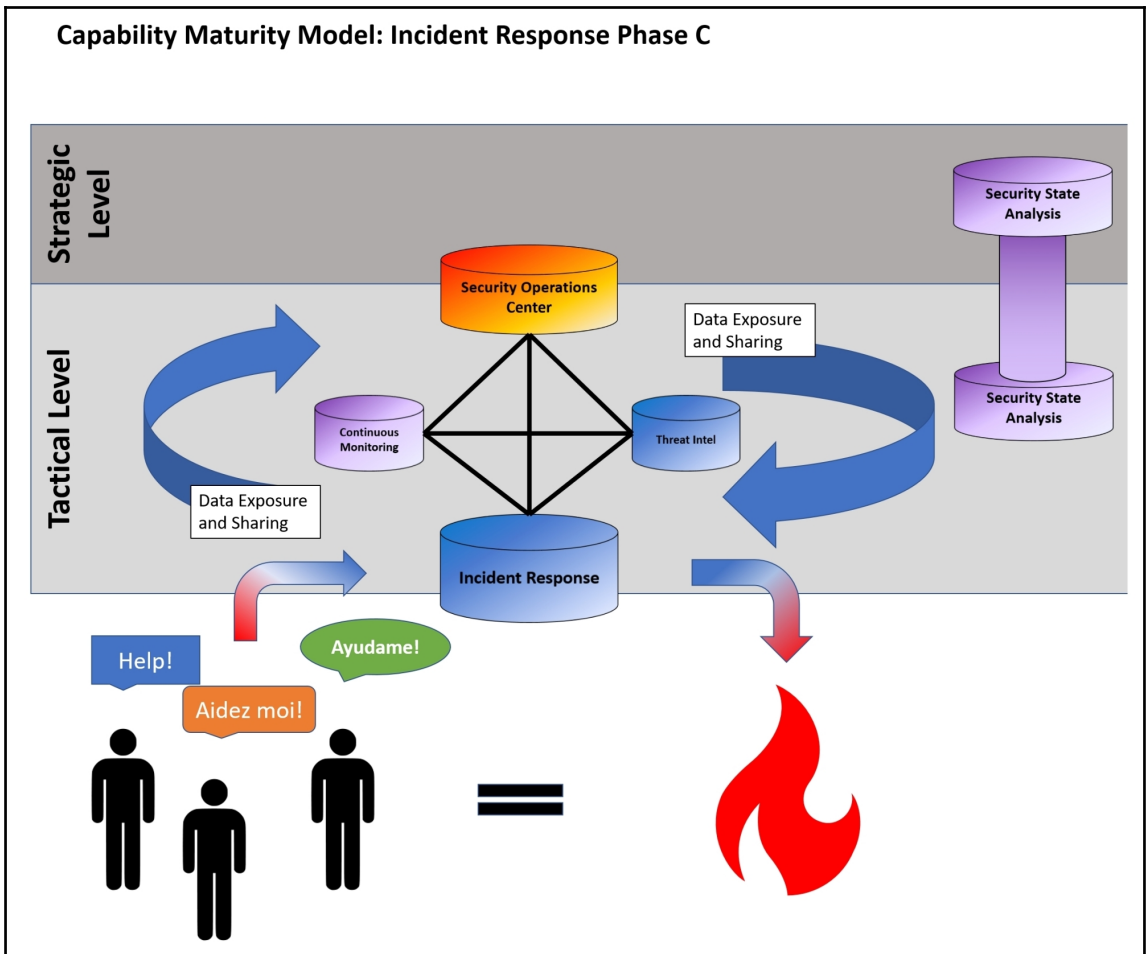




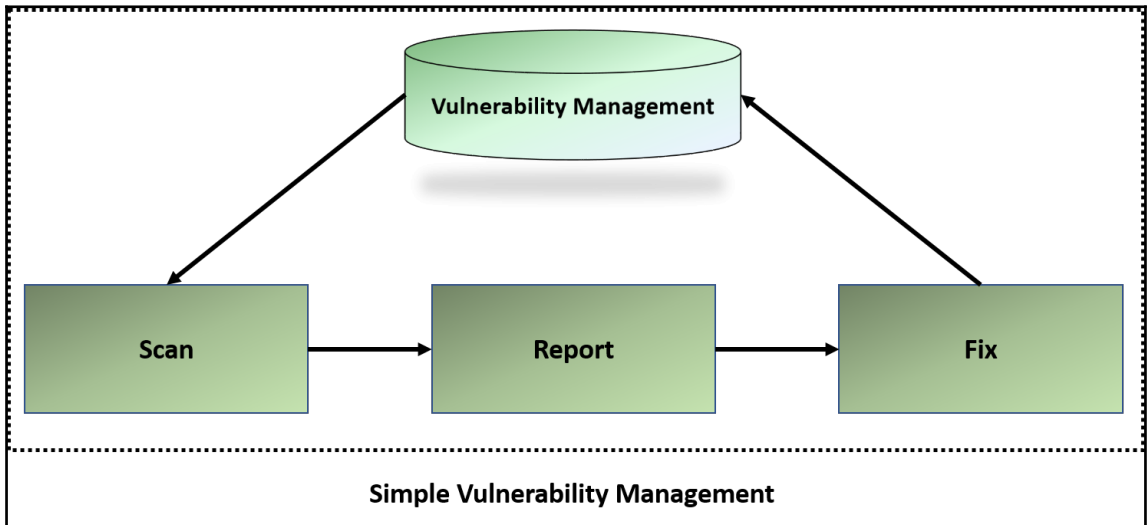
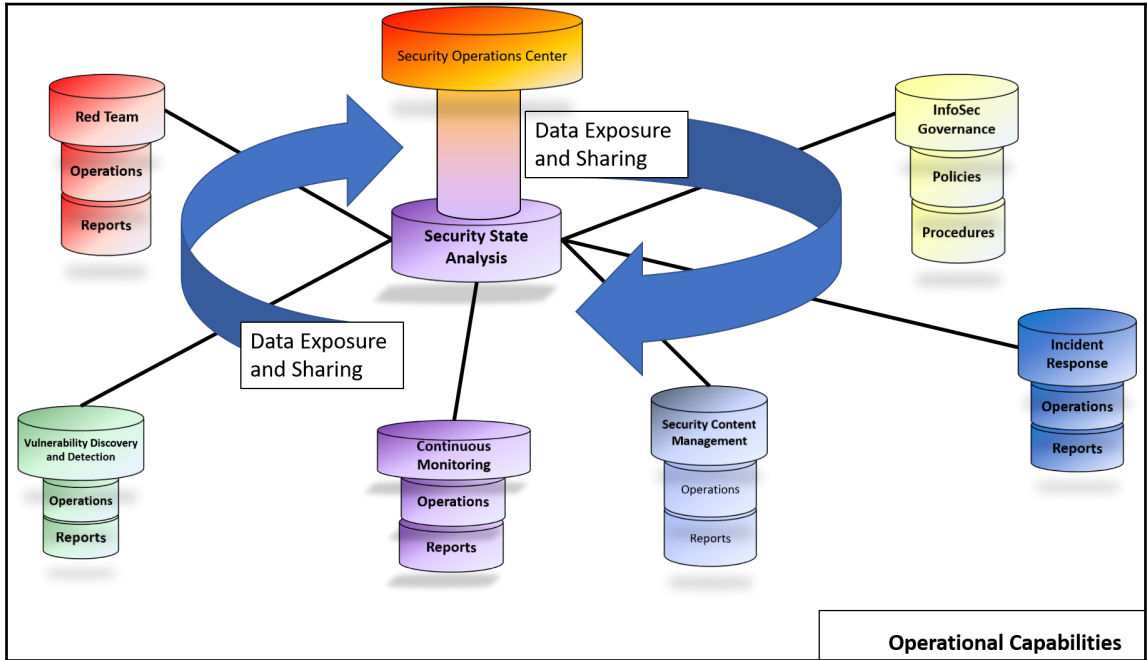


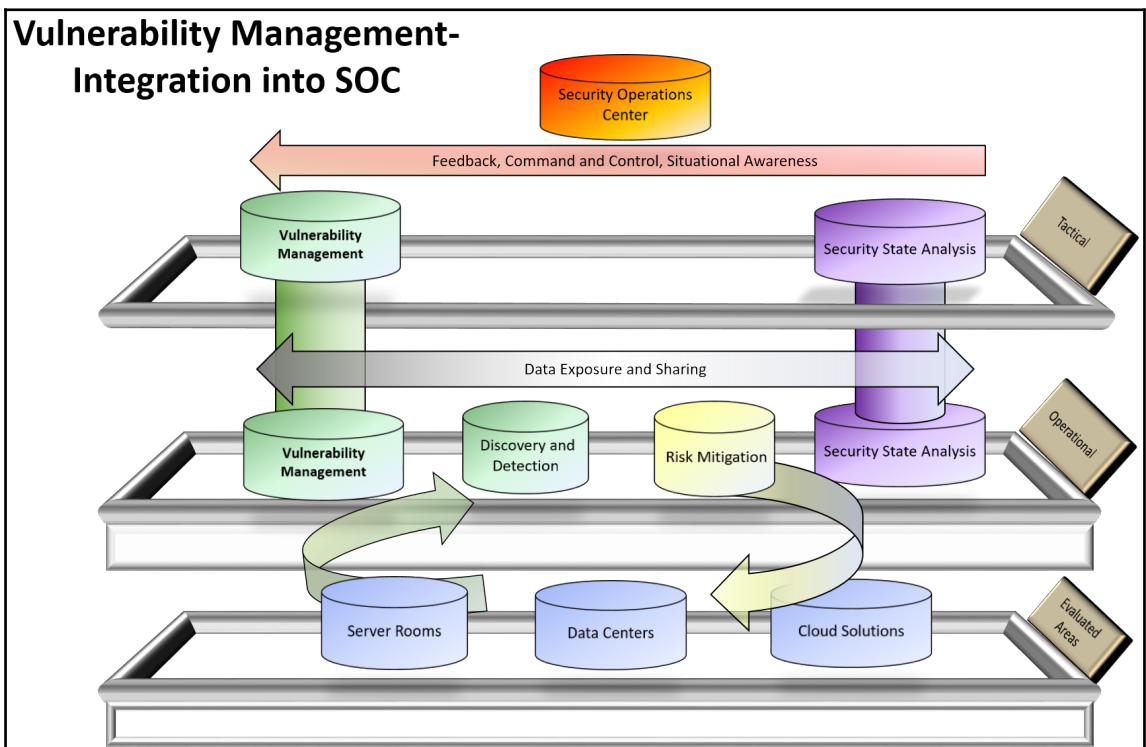
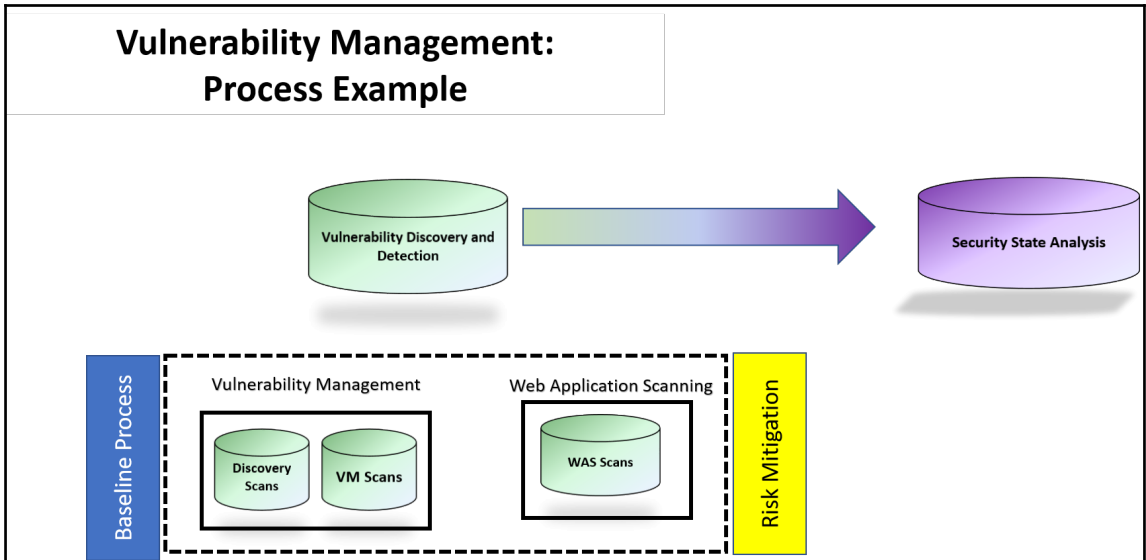


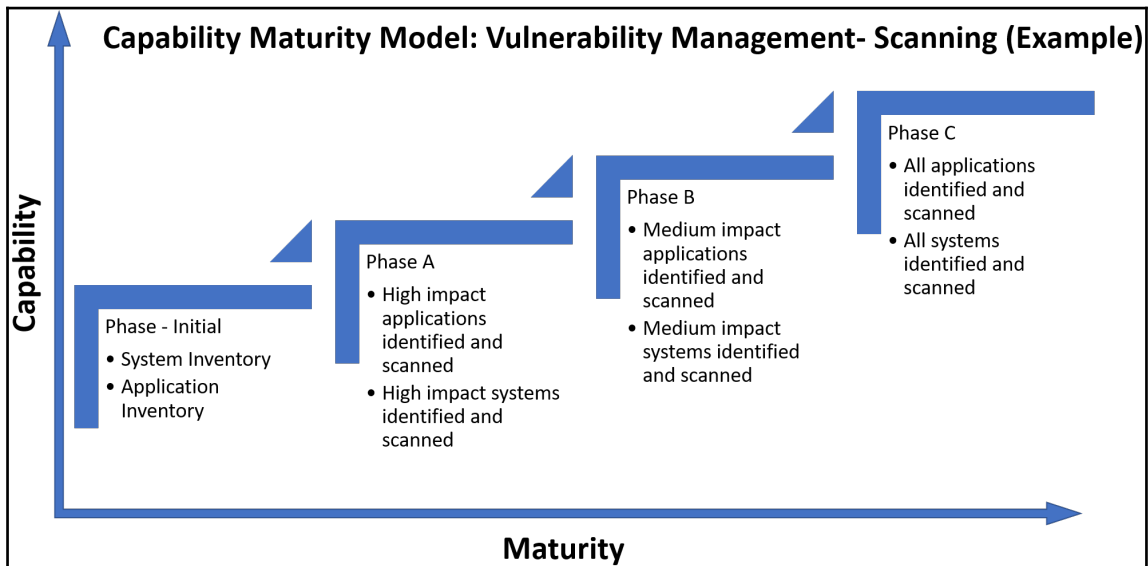
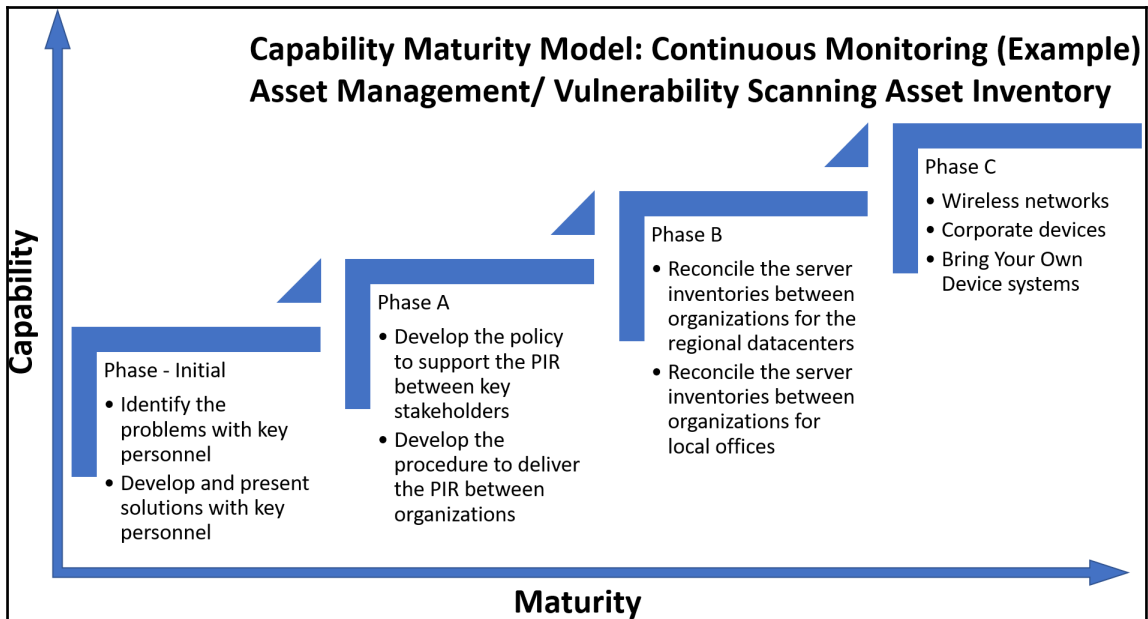




# Chapter 12: Vulnerability Management

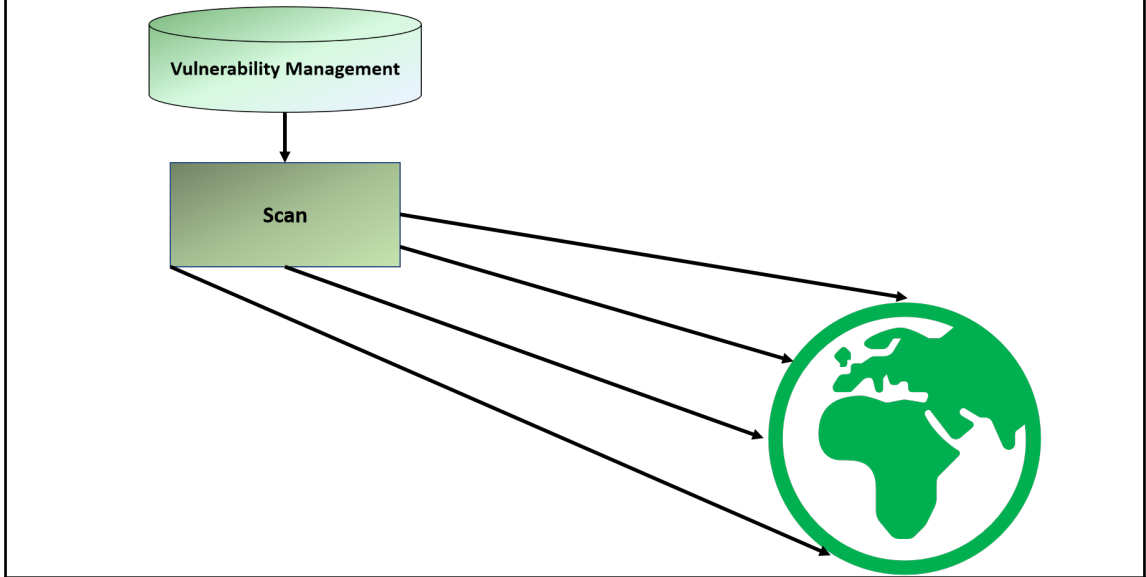




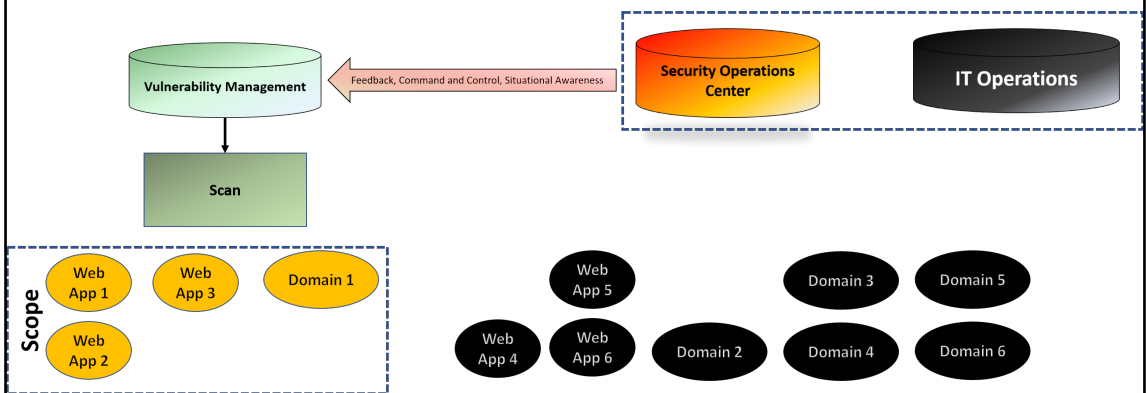


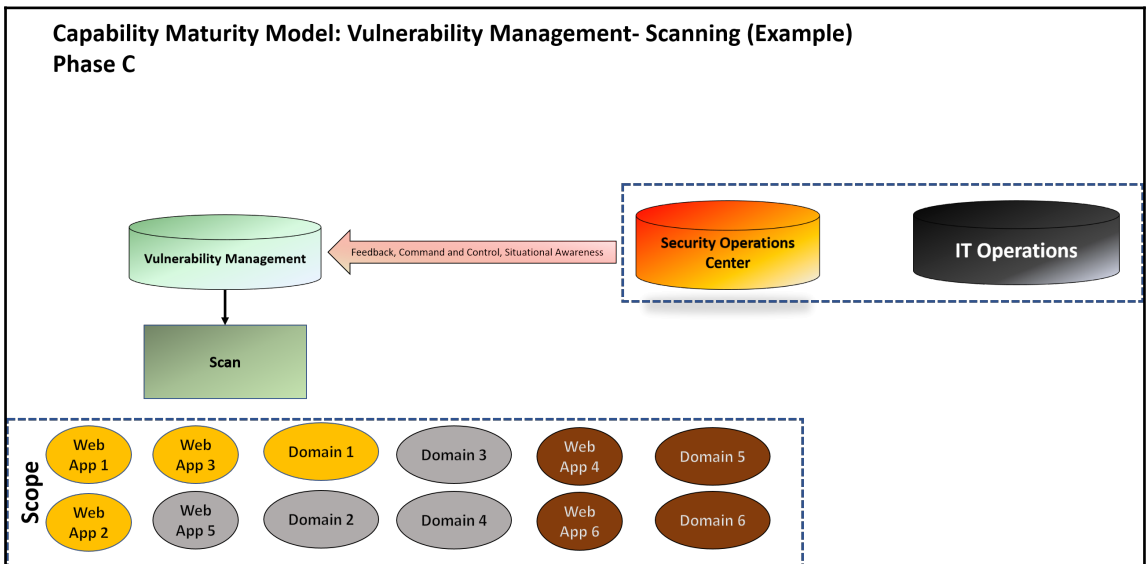
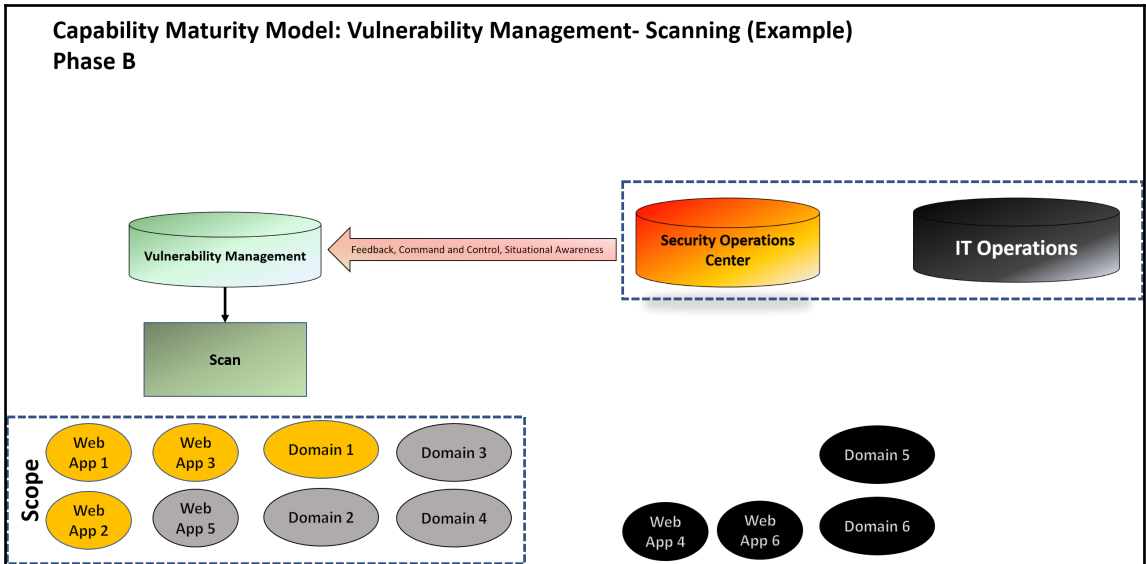


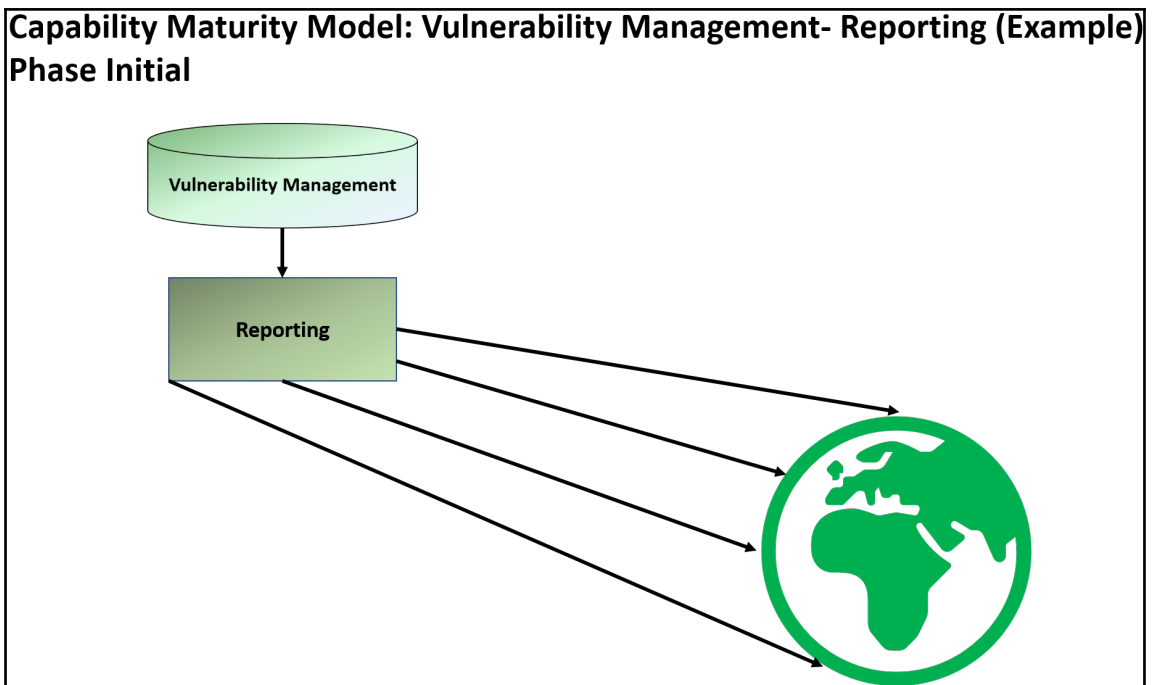
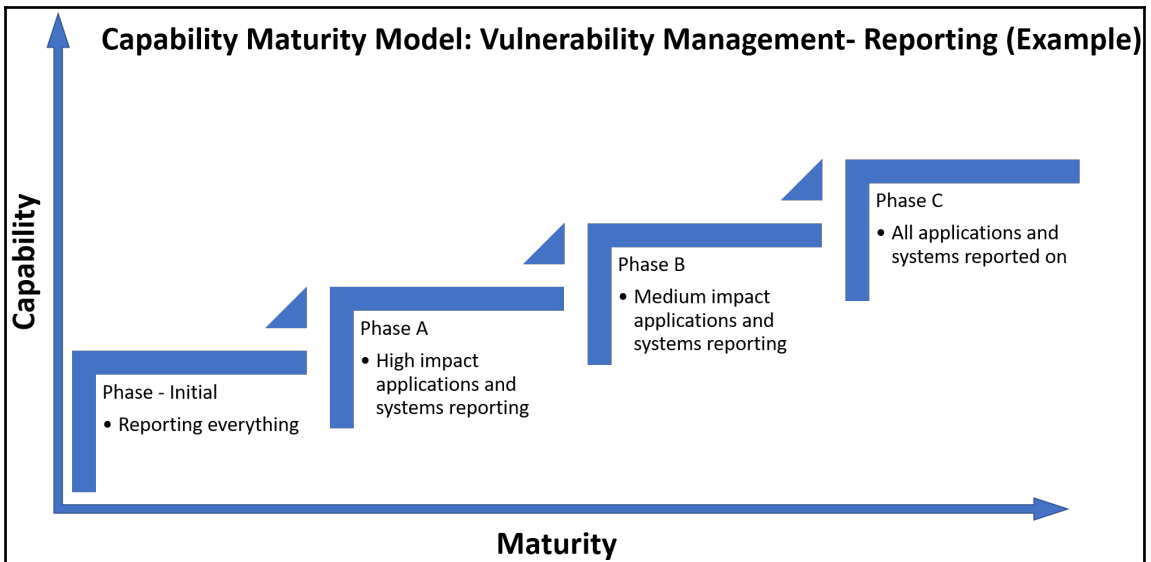
### Capability Maturity Model: Vulnerability Management- Scanning (Example) Phase Initial

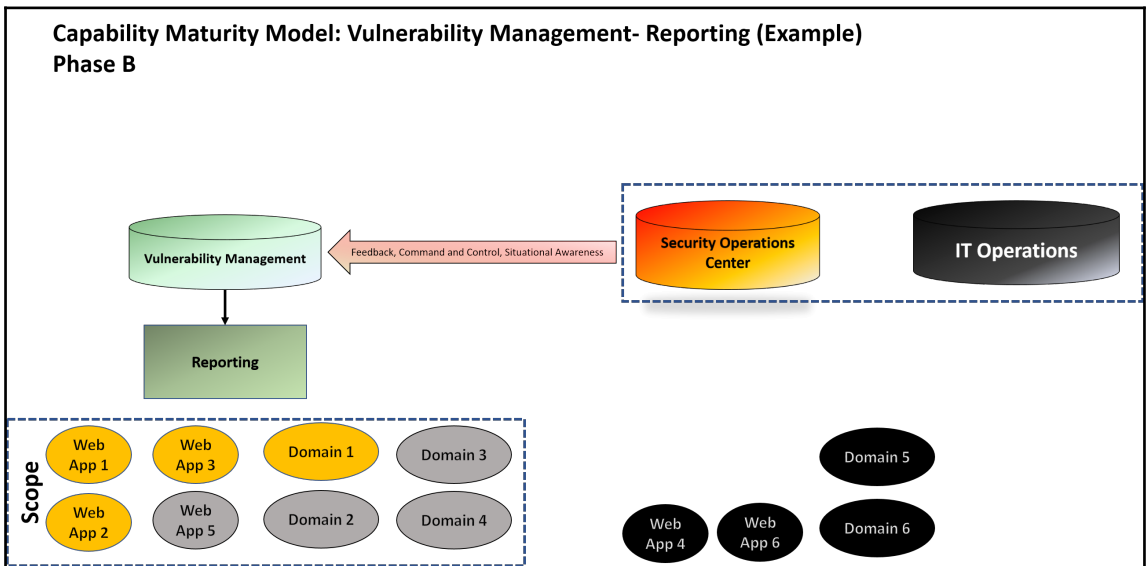
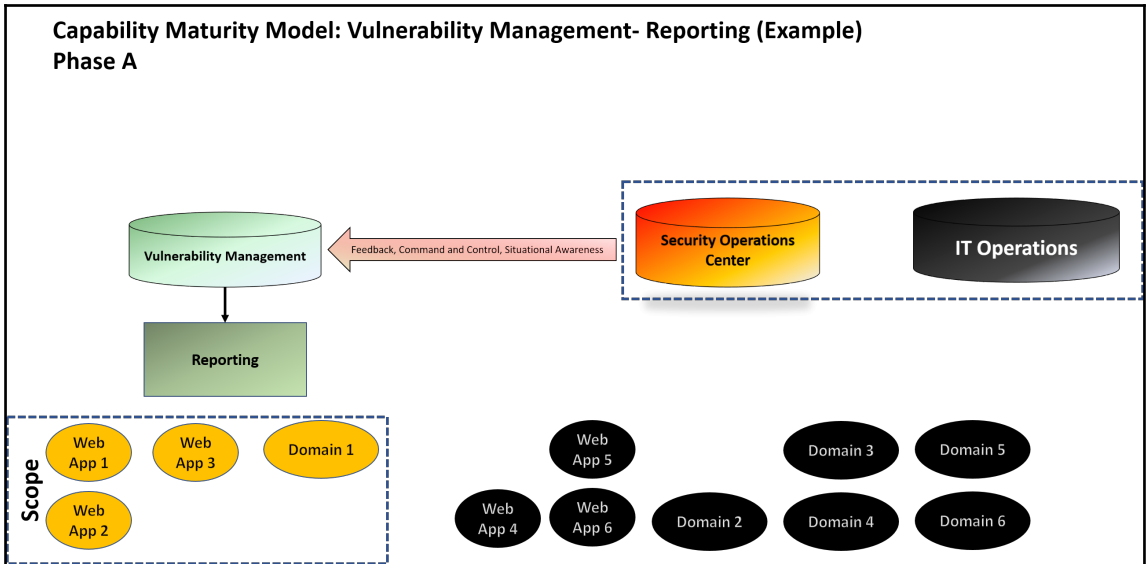


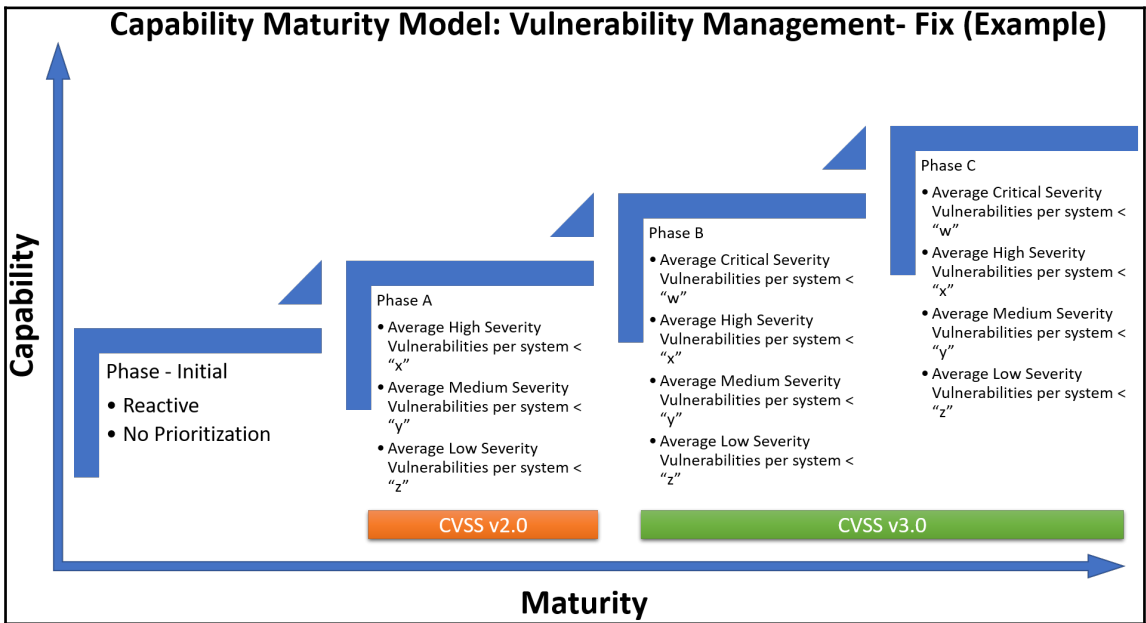
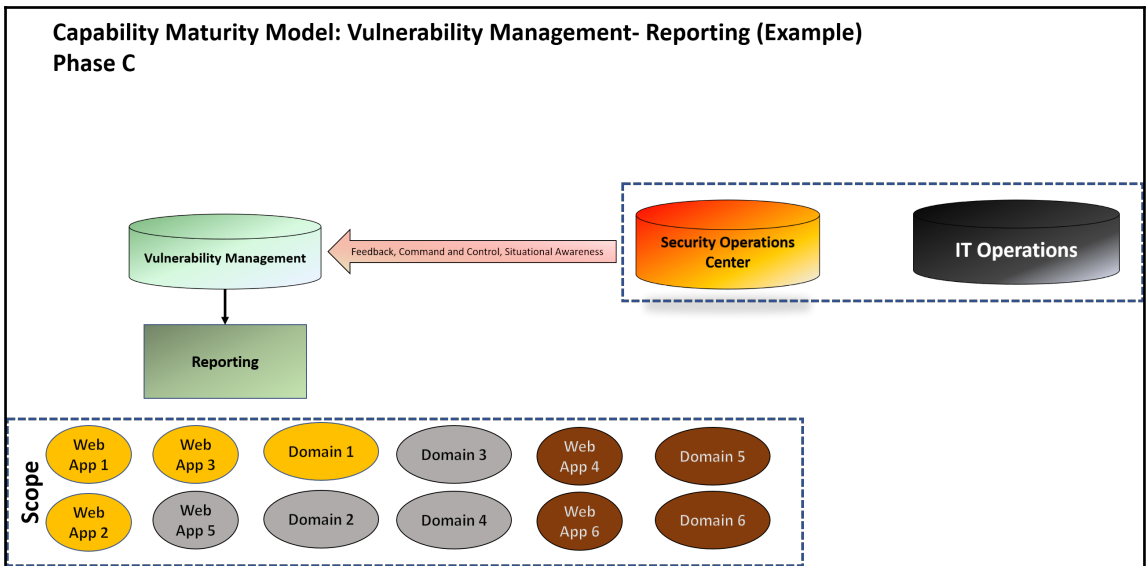
### Capability Maturity Model: Vulnerability Management- Scanning (Example) Phase A



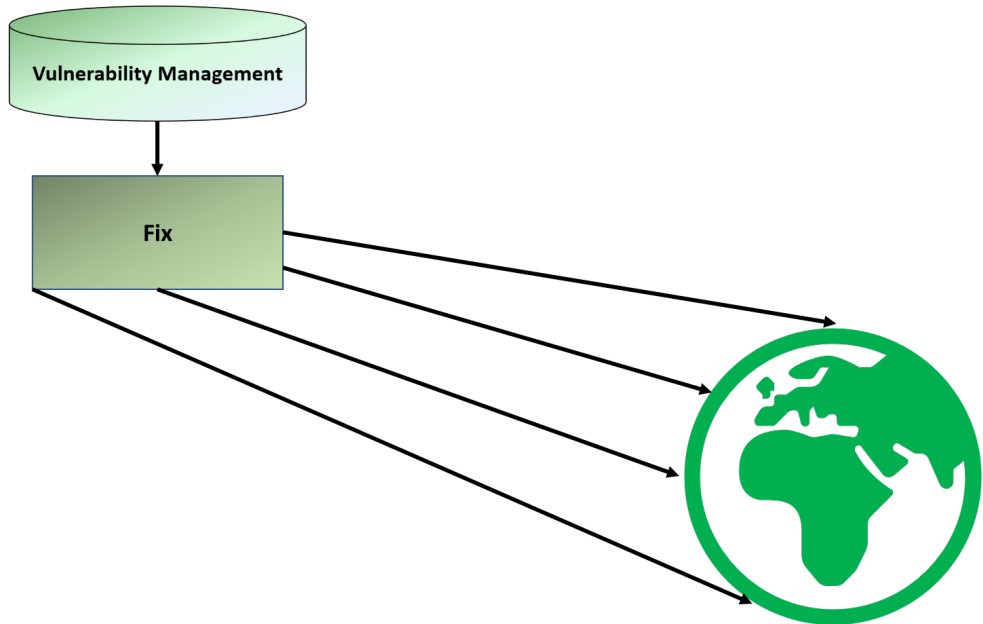


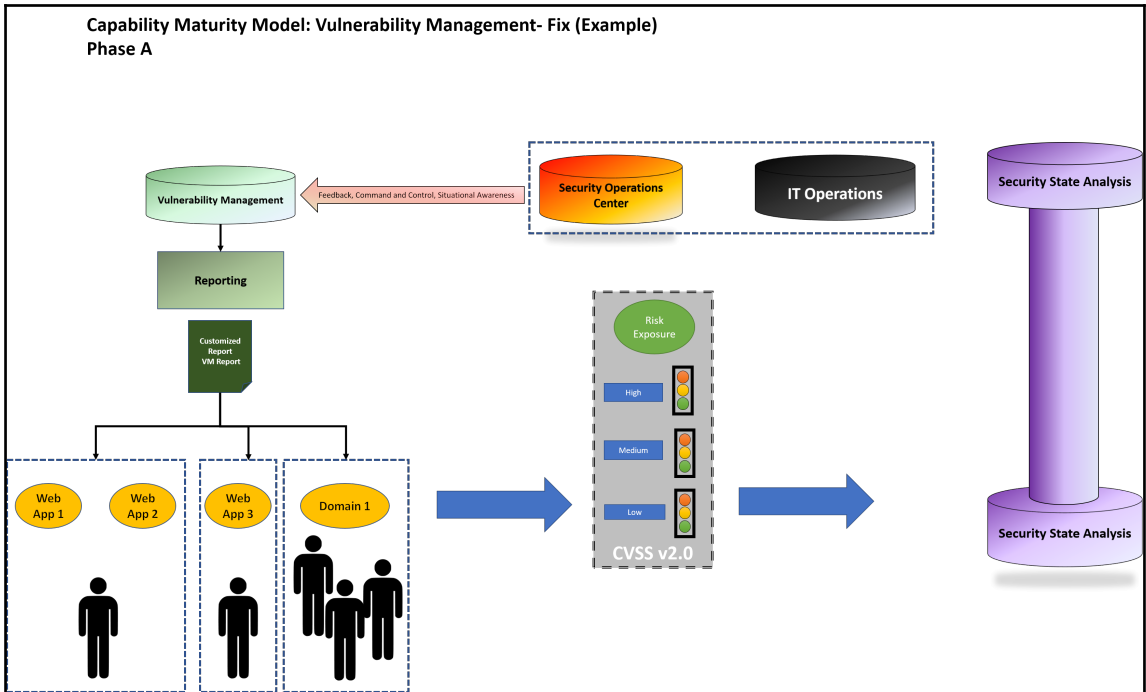


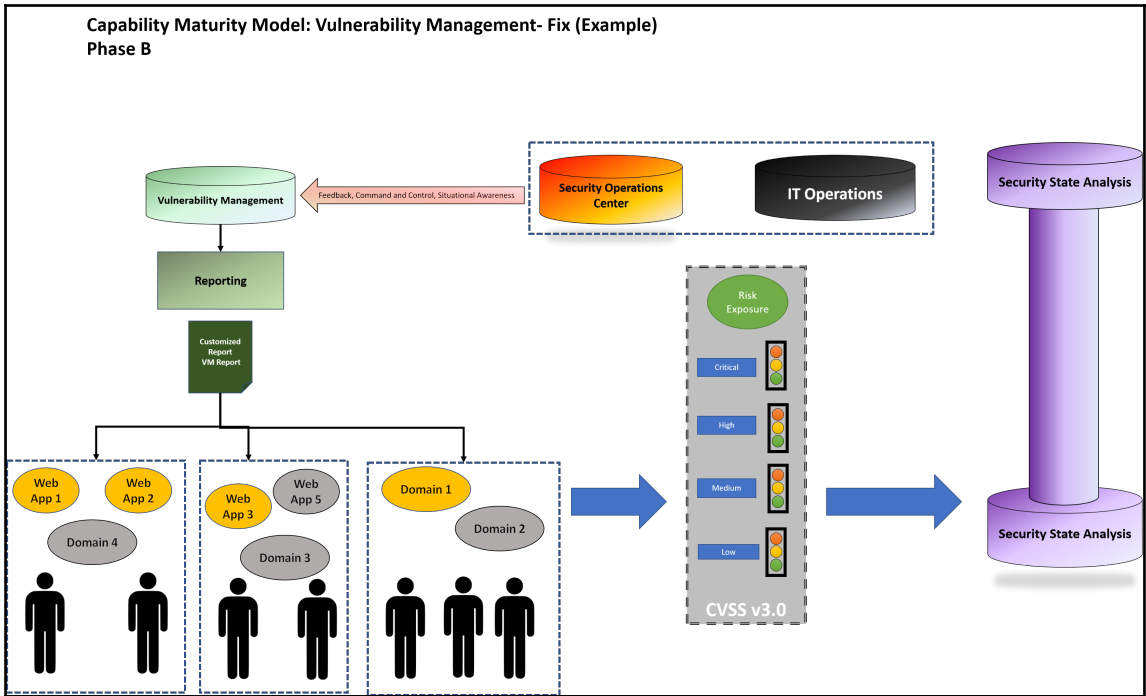




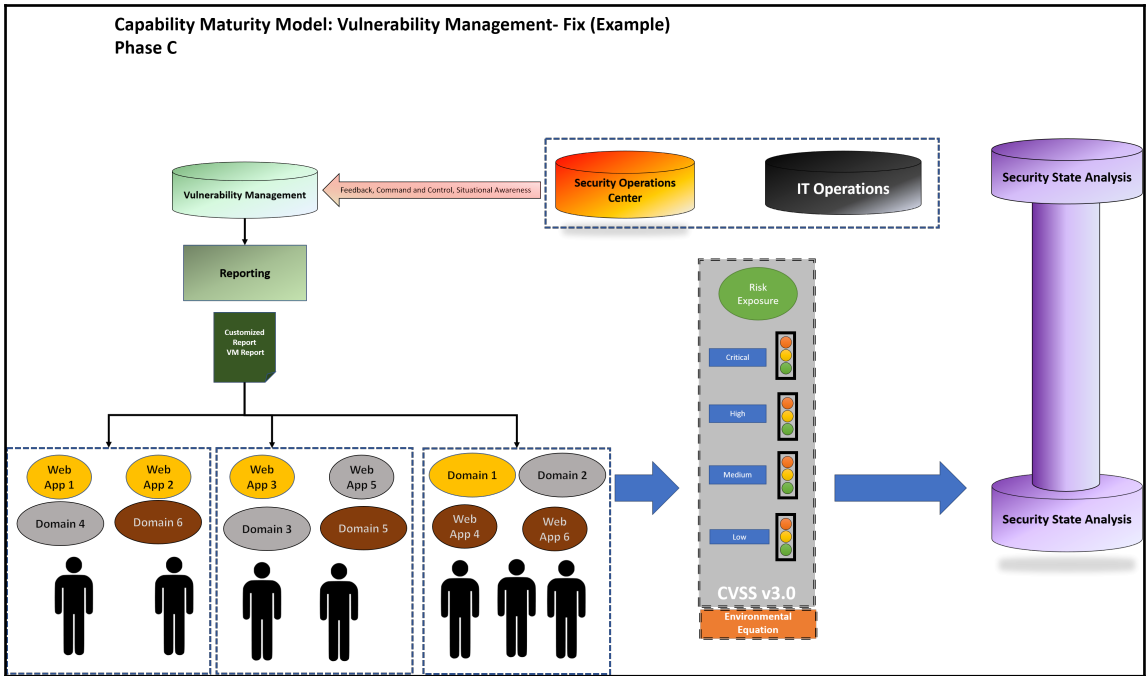
## Capability Maturity Model: Vulnerability Management- Fix (Example) Phase Initial



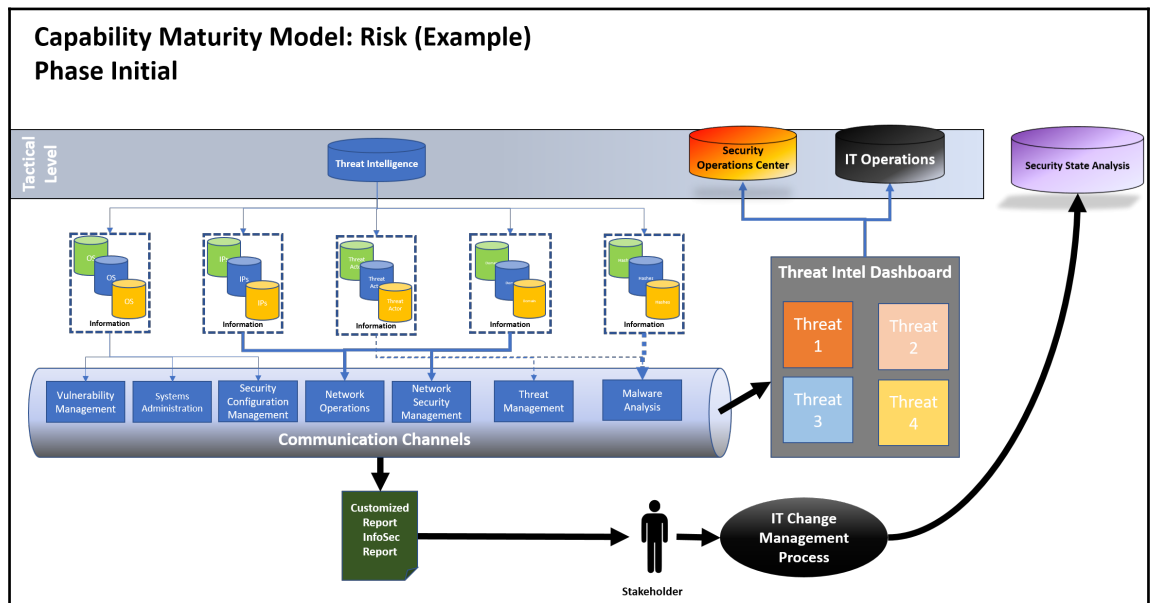
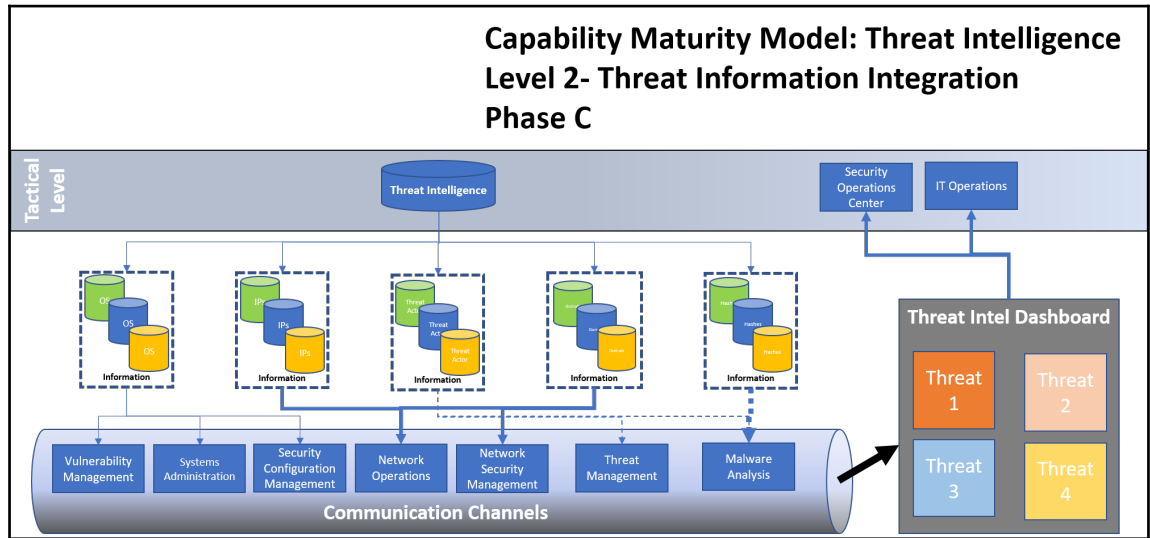


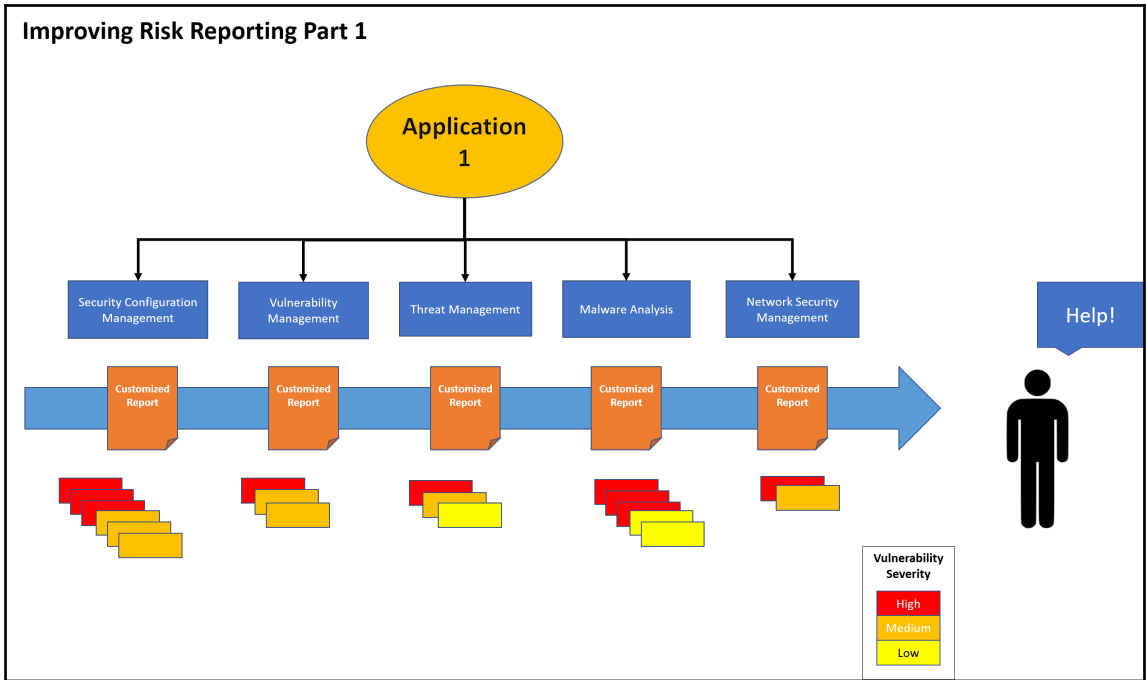


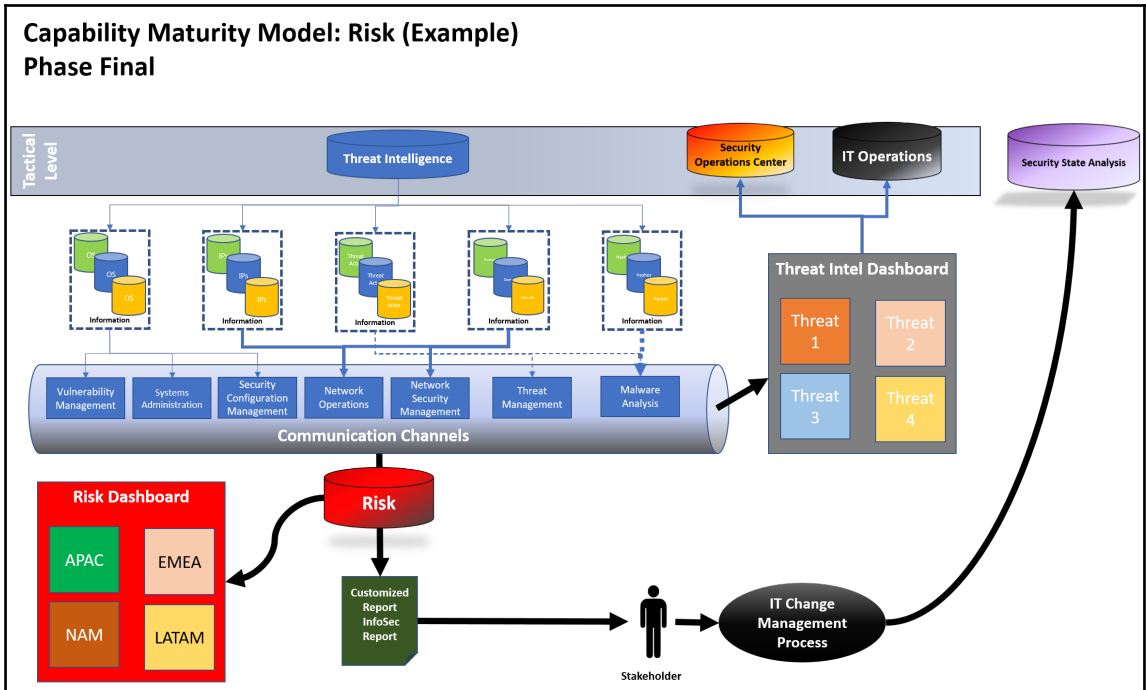


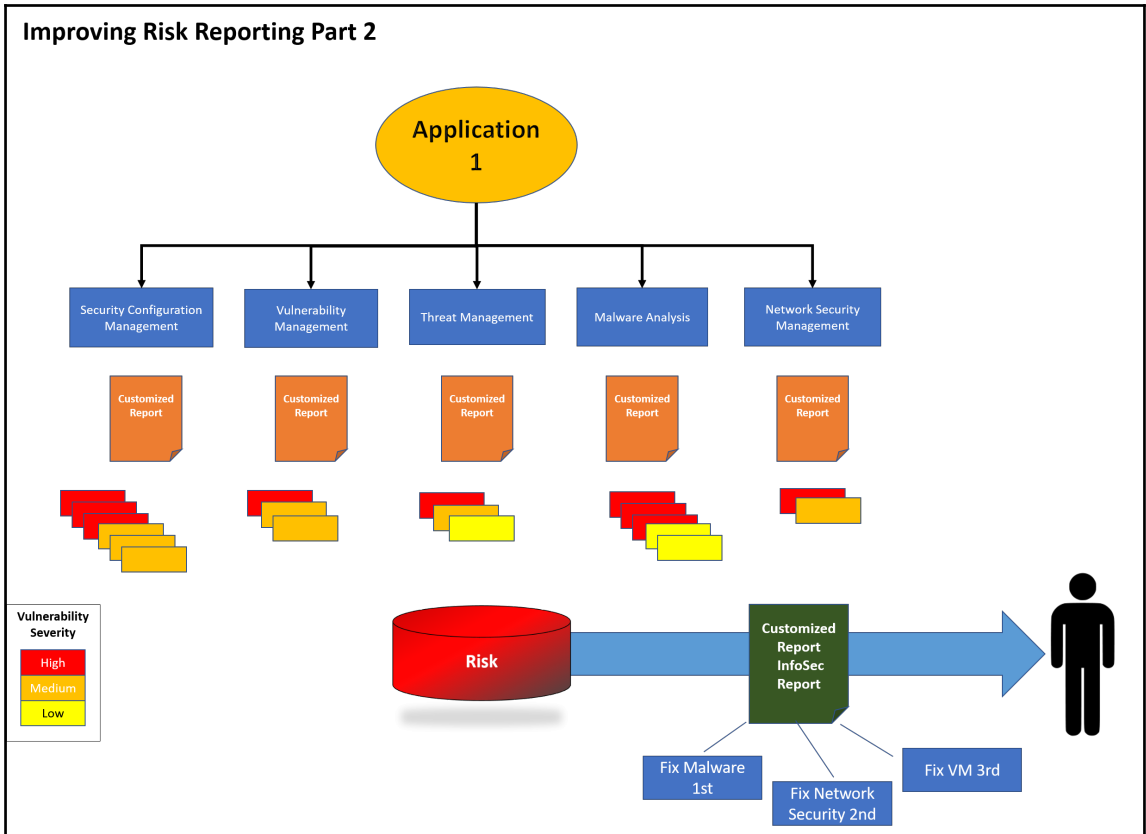


# Chapter 13: Risky Business



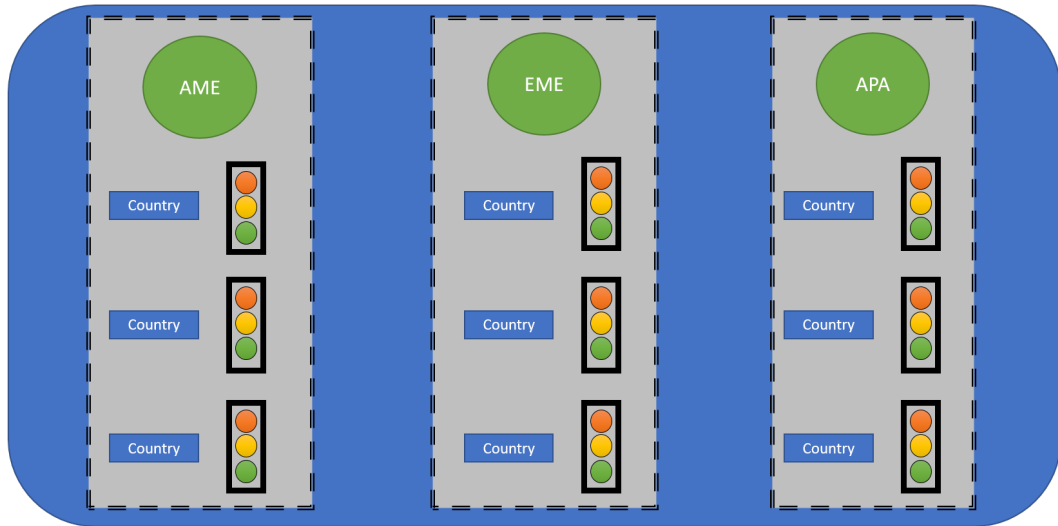


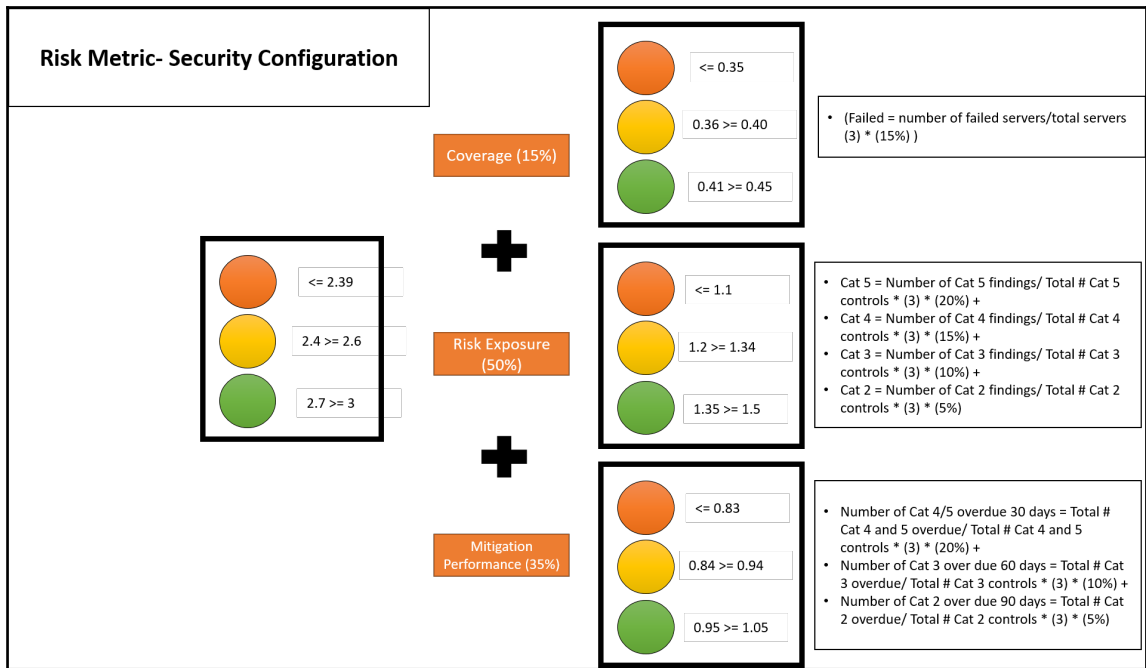


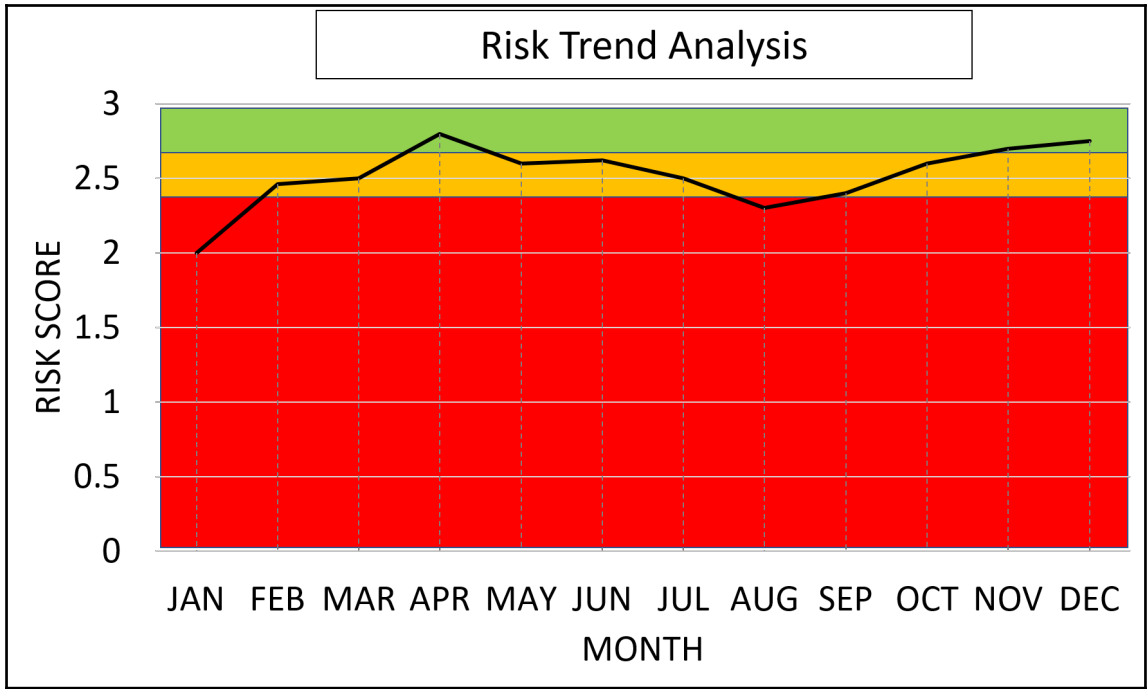


## Chapter 14: Assigning Metrics

### Security Configuration Dashboard- Region/Country

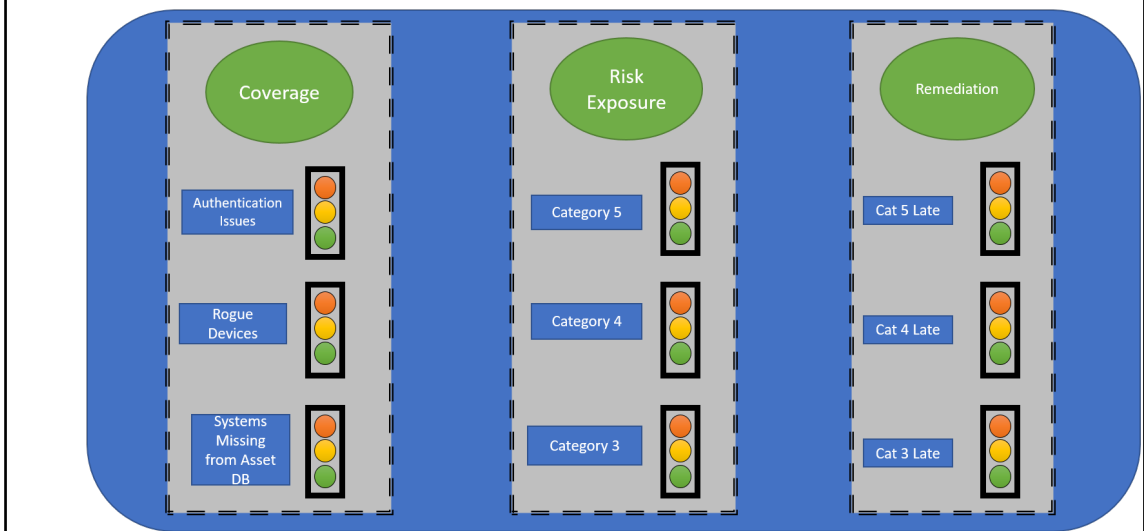








## Security Configuration Dashboard- Risk Score Breakdown Example



# Chapter 15: Wrapping Up

