MACC 2018: SCALING DISRUPTIVE TECHNOLOGIES – MOVING FROM INNOVATION TO ENTERPRISE TRANSFORMATION

Failing Forward to Bake Security Into Your Product Design

Thurs 11/08/18: 10:50 a.m.

Jeremy Swenson, MBA, MSST

Abstract Forward CONSULTING

Securing and improving business technology.

Agenda

1. Brief Bio
2. DevSecOps
3. Think Like An Attacker
4. Use Case 1 – Phone Messaging
5. Use case 2 – CISCO Switches.
6. Security Frameworks
7. Summary

Brief Bio

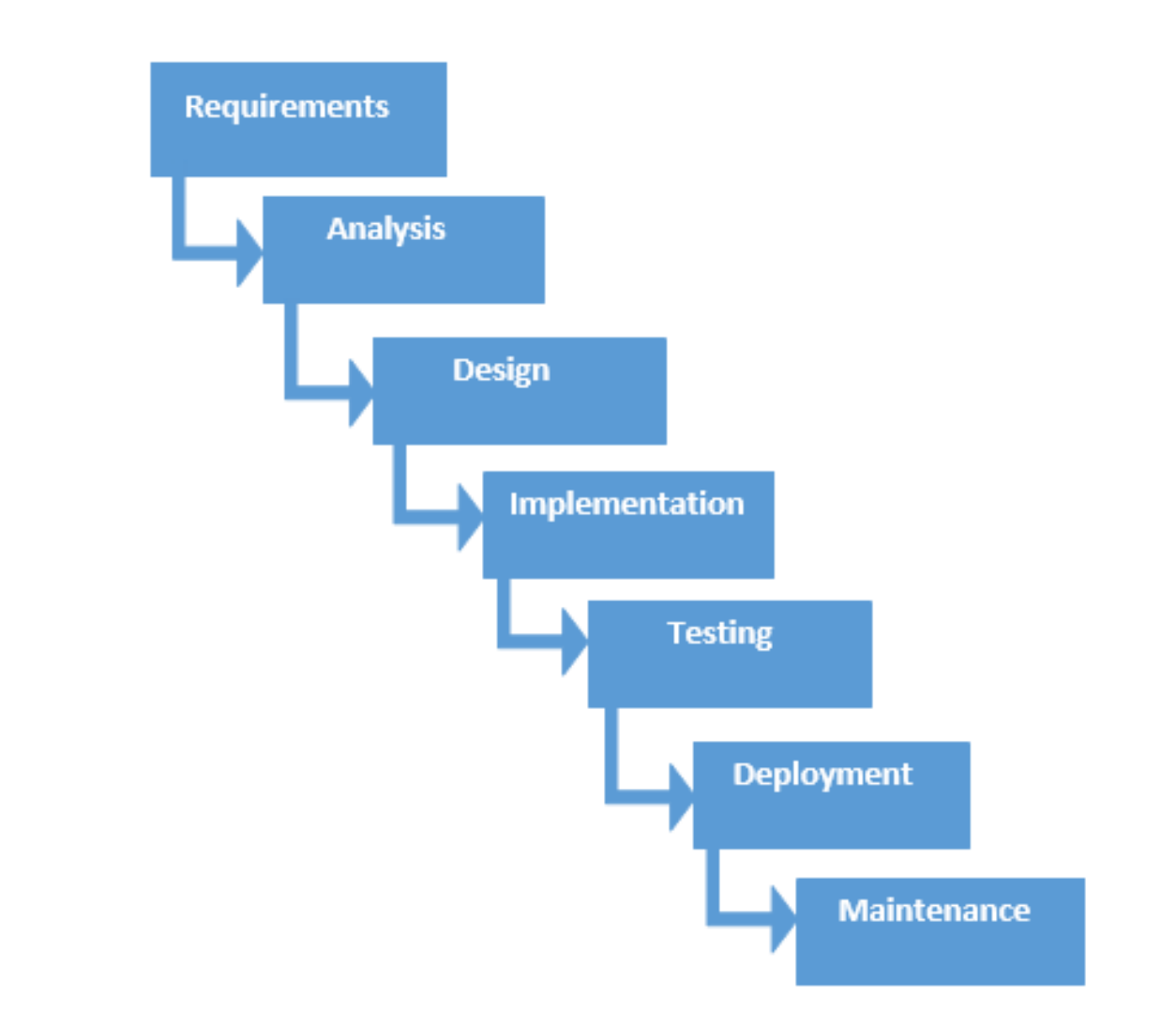
1. MBA, MSST
2. Founder and Prin. Consultant at
   a) www.abstractforward.com
3. Optum Enterprise Decommission 3 years – BA/Sr. Consultant.
4. Cyber / tech blogger 5 years:
   a) https://jeremy-swenson.com/
5. Ramsey County CISO Office – BYOD advisement.
6. Wells Fargo – data governance and business analysis.
7. U.S. Bank – internet banking and data distribution.
8. ING. – audit.

What is DevSecOps

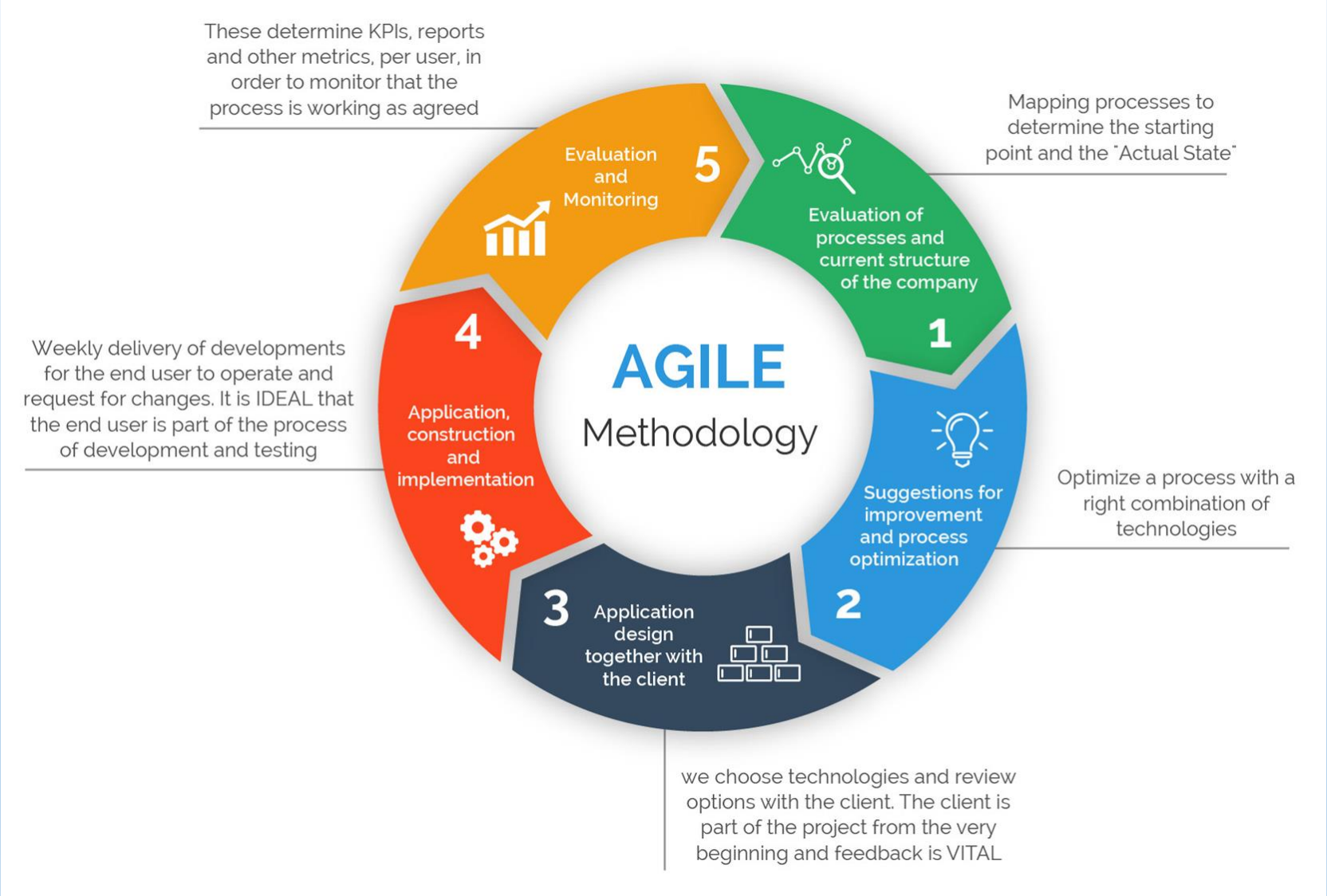
1. DevSecOps is a cultural movement that furthers the movements of Agile and DevOps by including Security features and practices.
2. The DevSecOps manifesto involves principles such as building a platform of least-privilege access.
3. Thinking about application and infrastructure security from the start.
4. Automating some security gates to keep the DevOps workflow from slowing down.

DevSecOps

1. Waterfall only approach – not best suited for strong security.

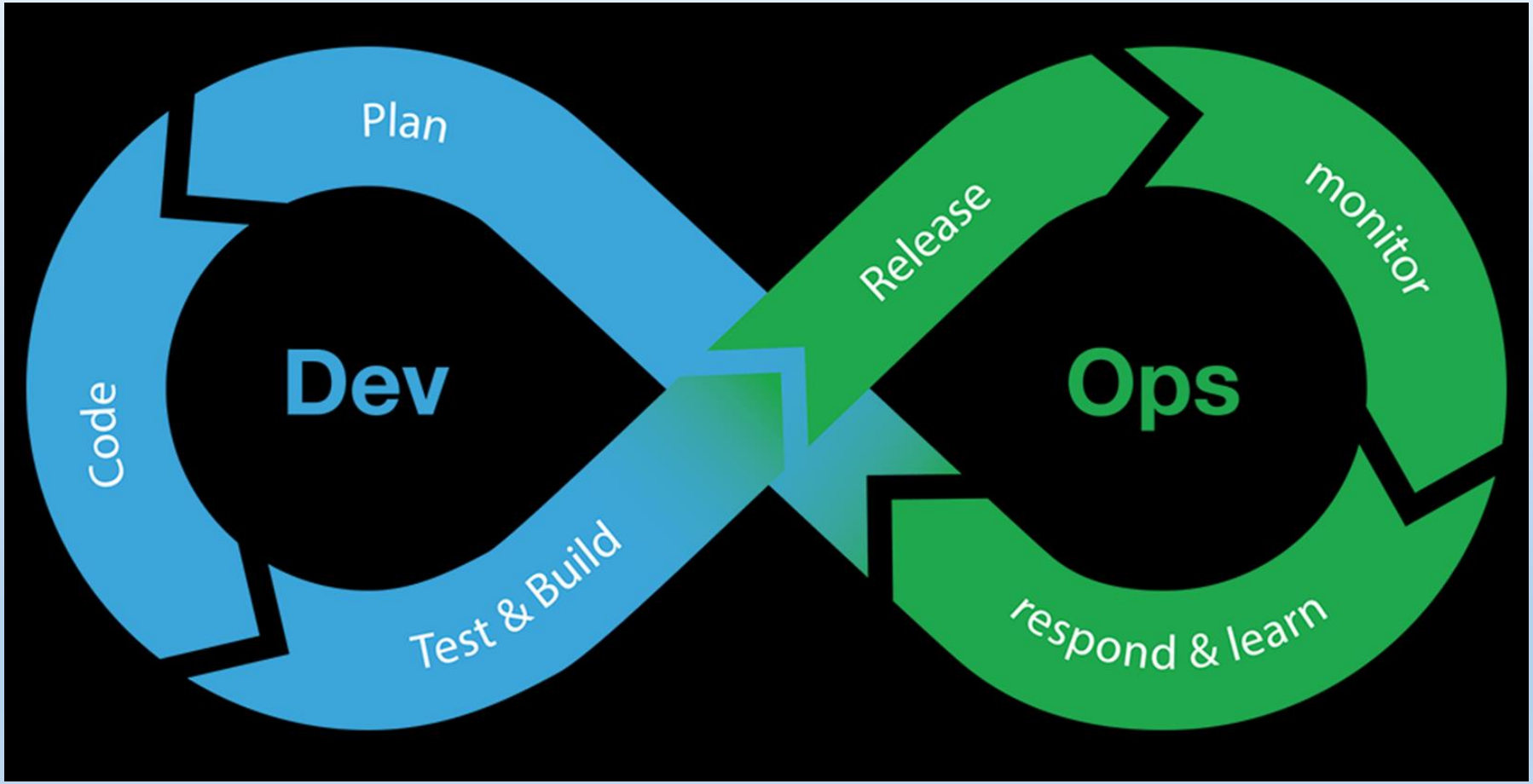


Agile – more aligned with DevSecOps



DevSecOps

- Comes in part from DevOps

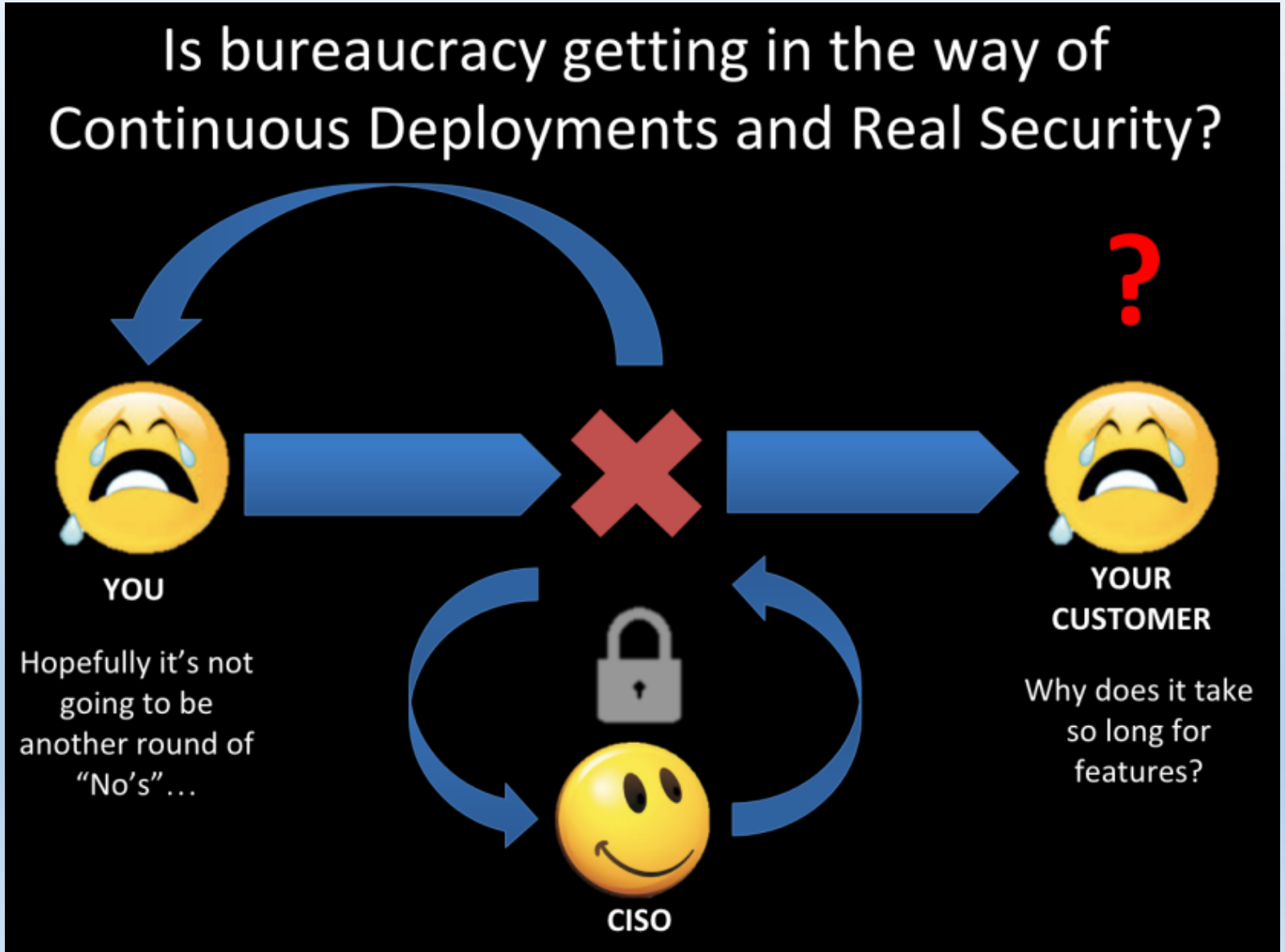


DevSecOps

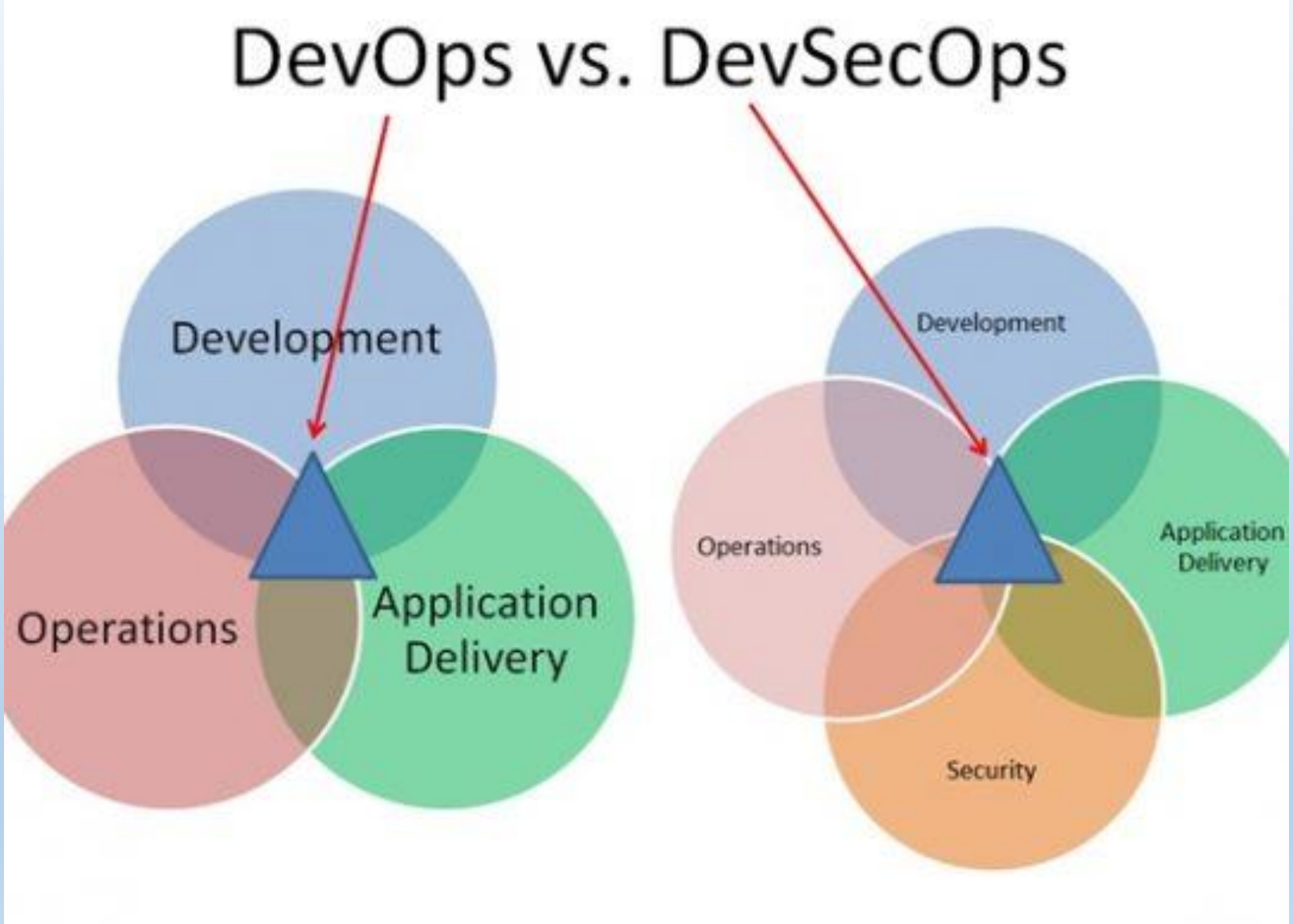
1. Move Left - Culture
   A. What is the company security culture?

DevSecOps

- Move Left - Culture



DevSecOps



DevSecOps

Manifesto

1. Leaning in over Always Saying “No”
2. Data & Security Science over Fear, Uncertainty and Doubt
3. Open Contribution & Collaboration over Security-Only Requirements
4. Consumable Security Services with APIs over Mandated Security Controls & Paperwork
5. Business Driven Security Scores over Rubber Stamp Security

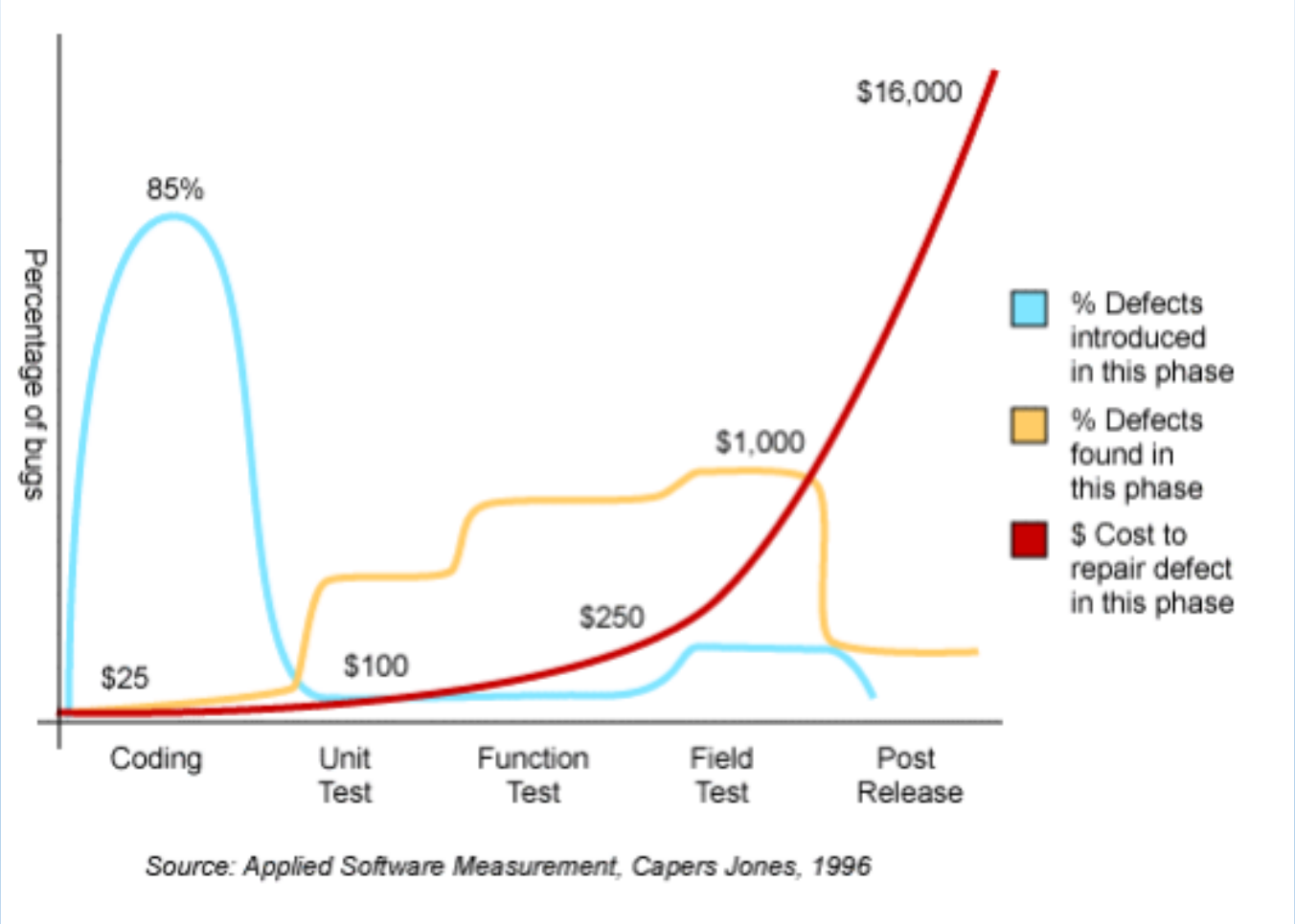
DevSecOps

Manifesto

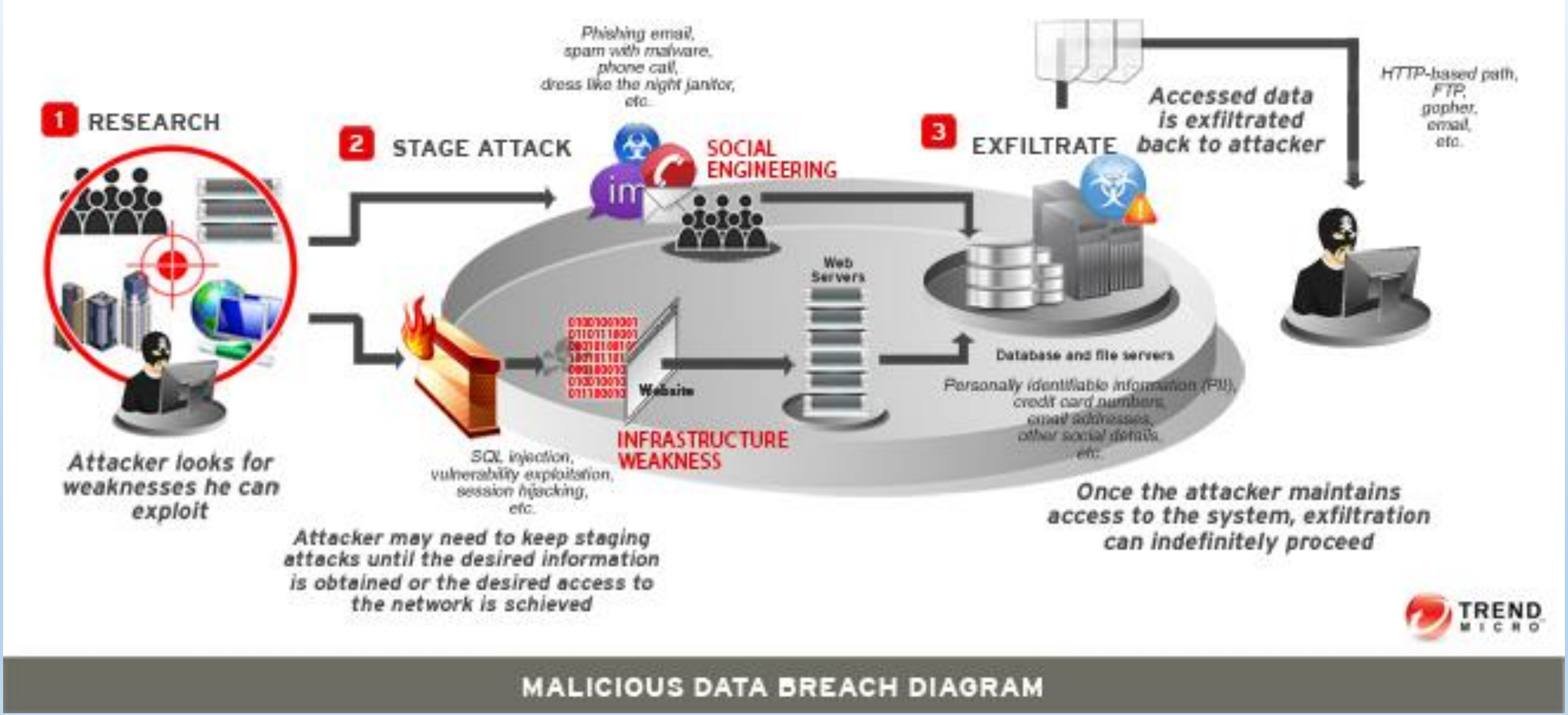
6. Red & Blue Team Exploit Testing over Relying on Scans & Theoretical Vulnerabilities
7. 24x7 Proactive Security Monitoring over Reacting after being Informed of an Incident
8. Shared Threat Intelligence over Keeping Info to Ourselves
   A. Think FBI and CIA pre 9/11
9. Compliance Operations over Clipboards & Checklists
   A. CPA firms often fall short

DevSecOps

- Does it cost more? Yes but…..

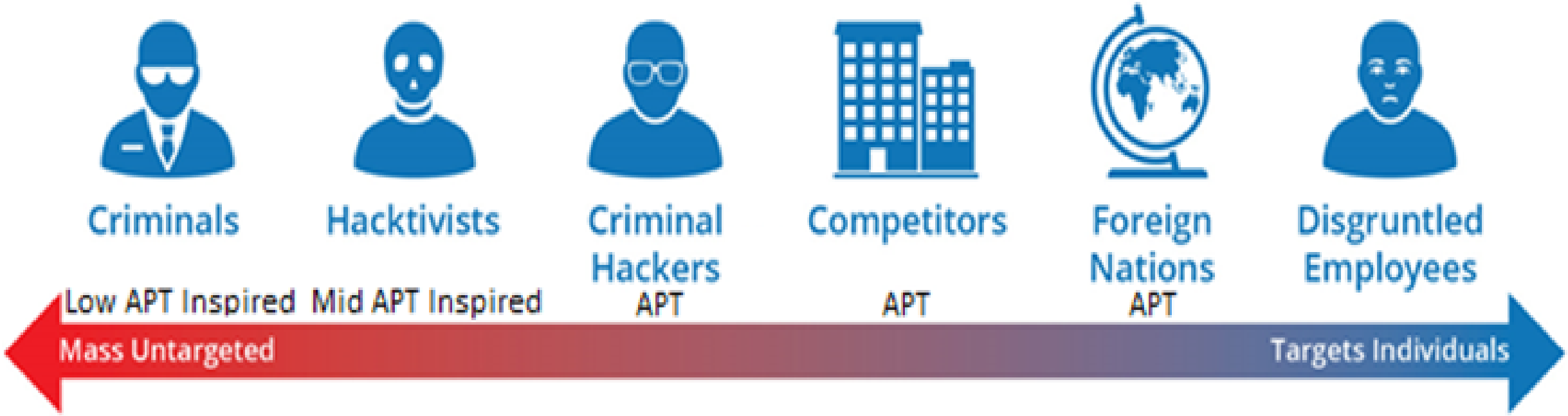


Think Like The Attacker



Think Like The Attacker

APT = advanced persistent threat.

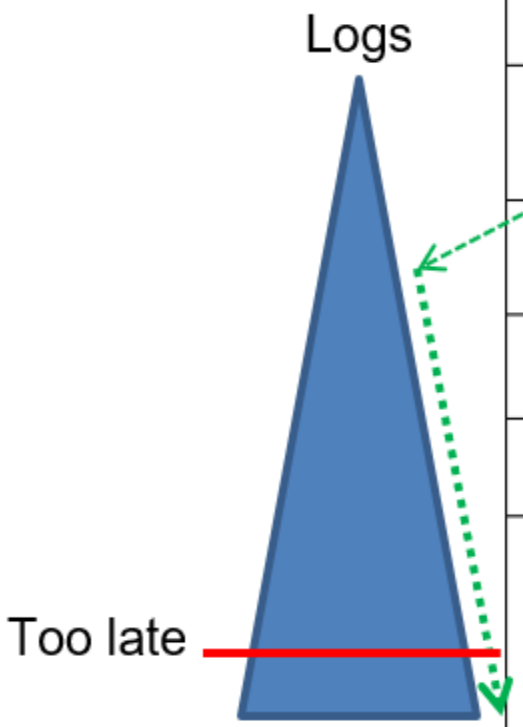


Note: We added the APT indicated for our clarification as we define APT broader.

Figure 20. Data Exfiltration Threat Actors: Mass vs. Targeted [87].

Table 4. Data Exfiltration Precursors Applied to the Cyber Kill Chain with Machine Learning

Phase of the Kill Cyber Chain	Probability of Exfiltration Precurosr	Ability To Control Precursor	Impact of Exfiltration Precurosr	Machine Learning Applicable	Mitigation Focus Rank
Reconnaissance	Very low - Its an absolute dependent precursor.	Very low – based in part off what you put out there.	None	None	7-very low
Weaponization	Low - Its an absolute dependent precursor.	None.	None	None	6-low
Delivery	High	Low – there are lots of uneducated users.	Med	Somewhat	5-High
Exploitation	Very High	High	High	High	4-very high
Installation	Very High	Very High	High	High	3-very high
Command & Control	Very High	Very High	Very High	Very High	2-very high
Actions on Objective	Absolute - but reduction is possible.	Low to high depending on the complexity of the exploit – some controls likely disabled.	Absolute - (the highest) but reduction is possible.	Very High	1-very high but it maybe too late.



There is no real precursor impact until early in the exploitation phase.

Think Like An Attacker

Table 2. Taxonomy of Exfiltration Methods [2].

Taxonomy of Exfiltration Methods				Likely Ports
Network	Usually benign	Conventional	HTTP	TCP 443
			FTP	TCP 21
			SMTP	TCP 25
			SSH	TCP 21
			Instant messenger	TCP and UDP 18
		Custom	Oracle (Java)	TCP 1521, 2424, 2483, and 3872
			MySQL	TCP 1433 and UDP 1434
			Specialty software	Many
	Known malicious	Rootkits		TCP 21
		Botnets		UDP 80
		Spyware		UDP 20 and 21
		Covert Channels		UDP 80
		Phishing		UDP 80
		Pharming		UDP 80
		MITM		8080 TCP and UDP
		Attack	Exploits	Many
			DNS poisoning	TCP and UDP 53
			Directory traversal	UDP 80 and FTP 21
			Privilege escalation	16992, 16993, 16994, 16995, 623, and 664
Physical	Usually benign	Printing devices		170 UDP, 515 TCP, 631 UDP and TCP
		CD, DVD		NA
		Disk		NA
		USB		19540 TCP and UDP
		Digital Media Players		NA
	Known malicious	Laptop theft		NA
Cognitive		Social engineering		Many
		Shoulder surfing		NA

Note: This table has been marked up for this research and the Likely Port column was added.

Think Like An Attacker

Table 2. Taxonomy of Exfiltration Methods [2].

Taxonomy of Exfiltration Methods				Likely Ports
Network	Usually benign	Conventional	HTTP	TCP 443
			FTP	TCP 21
			SMTP	TCP 25
			SSH	TCP 21
			Instant messenger	TCP and UDP 18
		Custom	Oracle (Java)	TCP 1521, 2424, 2483, and 3872
			MySQL	TCP 1433 and UDP 1434
			Specialty software	Many
	Known malicious	Rootkits		TCP 21
		Botnets		UDP 80
		Spyware		UDP 20 and 21
		Covert Channels		UDP 80
		Phishing		UDP 80
		Pharming		UDP 80
		MITM		8080 TCP and UDP
		Attack	Exploits	Many
			DNS poisoning	TCP and UDP 53
			Directory traversal	UDP 80 and FTP 21
			Privilege escalation	16992, 16993, 16994, 16995, 623, and 664
Physical	Usually benign	Printing devices		170 UDP, 515 TCP, 631 UDP and TCP
		CD, DVD		NA
		Disk		NA
		USB		19540 TCP and UDP
		Digital Media Players		NA
	Known malicious	Laptop theft		NA
Cognitive		Social engineering		Many
		Shoulder surfing		NA

Note: This table has been marked up for this research and the Likely Port column was added.

1. **TCP** and **UDP port 21** is frequently used (File Transfer Protocol (FTP).
2. A USB vulnerability is only associated with port: 19540 TCP and UDP.
3. Lesser known printer ports: **170 UDP, 515 TCP, 631 UDP and TCP.**
4. A Domain Name Server (DNS) attack / DNS spoofing is associated with port 53 – forces the incorrect web address.
5. Know if ports allow many formats, and/or applications or not? Use the IANA (Internet Assigned Numbers Authority Directory. https://www.iana.org/form/ports-services

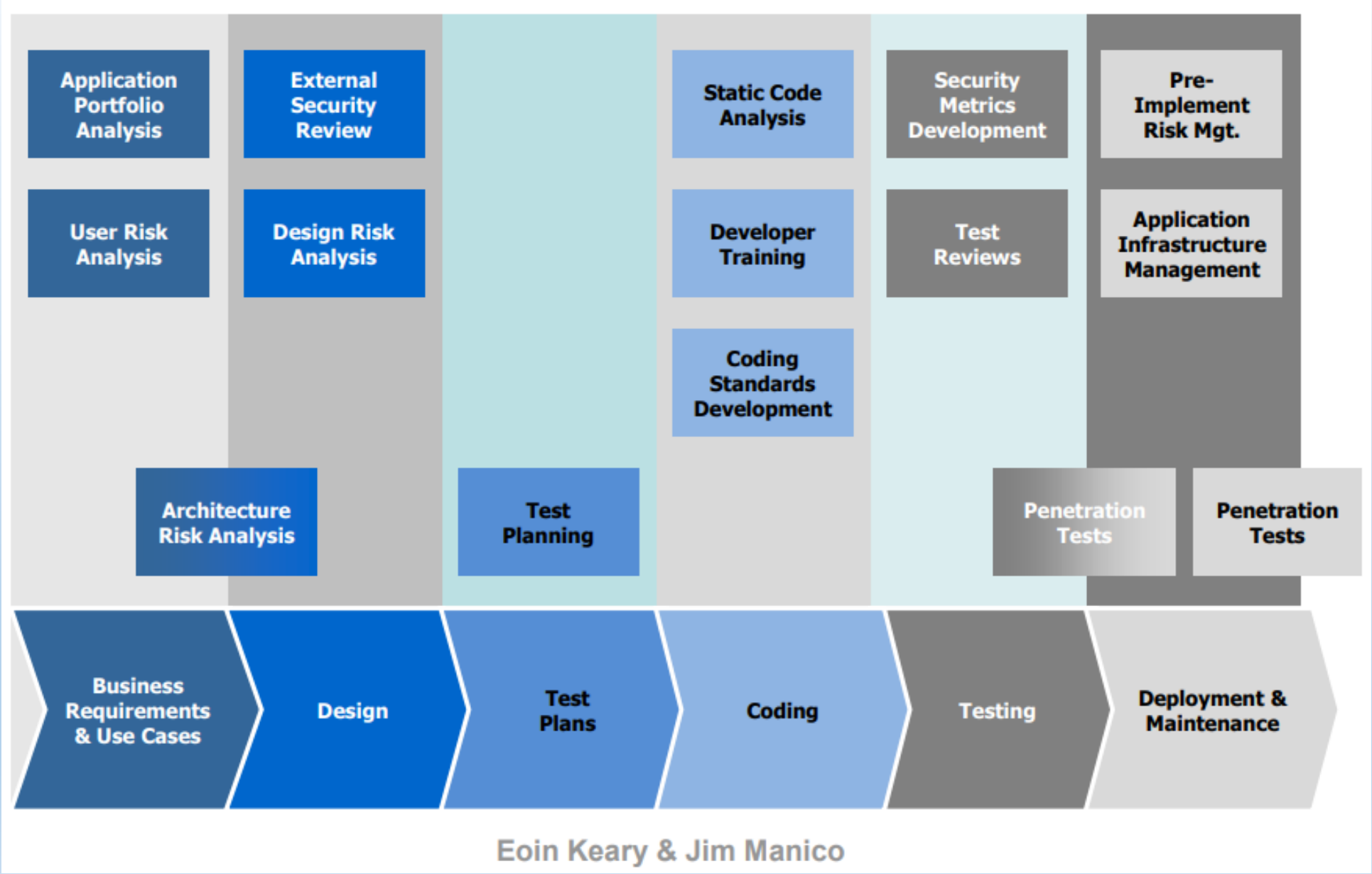
This info helps:

1. Assign dummy ports.
2. Audit your ports.
3. Close unneeded ports.
4. Know what ports and protocols current threats are using.
5. Keep your private port info on a need to know basis.

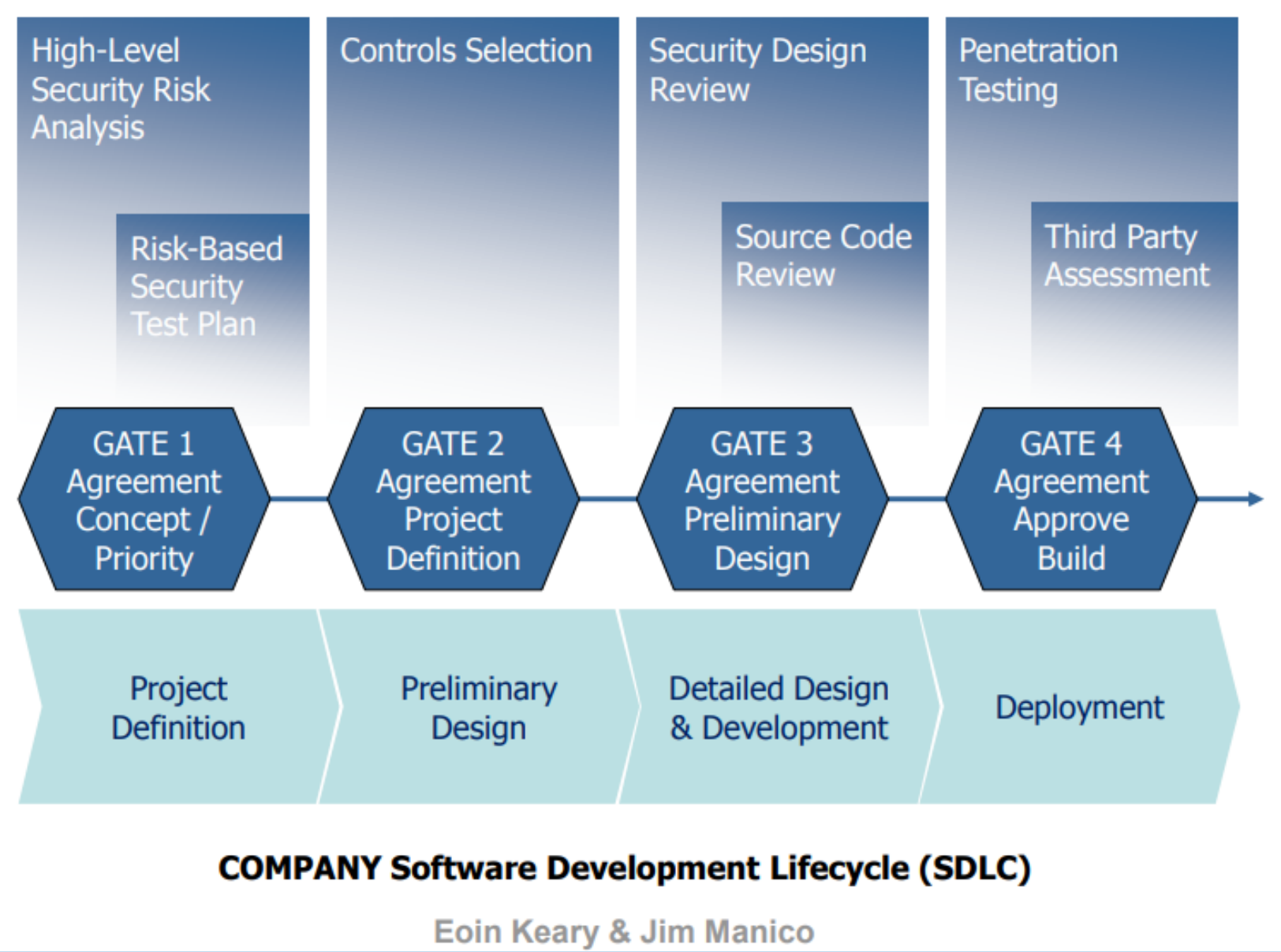
DevSecOps Security in the SDLC

1. What is a misuse case?
2. Where does a misuse case fit in the SDLC?

DevSecOps Security in the SDLC



DevSecOps Security Quality Gates



Use Case 1 – Mobile Device Messaging.

1. Whats App – most secure.
   A. Full end-to-end encryption.
   B. Setting notifies you if a WhatsApp friend changes their device.
2. Facebook Messenger.
   A. Full end-to-end encryption.
   B. Bugs related to video sharing / links / prize scams.
3. Gmail
   A. Can enable multifactor.
   B. Uses geolocation.
4. SMS Text – least secure.
   A. No encryption.
   B. Risk that SMS messages or voice calls may be intercepted or redirected
   C. Easy to spoof phone number.
   D. No multifactor.
   E. Does not use geolocation.

Use Case 1 – Mobile Device Messaging.

Use Case 2 – CISCO Switches.

1. In Oct 2016 Cisco Systems released several critical software patches for its Nexus 7000-series switches and its NX-OS software.
2. Cisco's Security Advisory declared that both the Nexus 7000 and 7700 series switches were vulnerable to this glitch.
3. The vulnerabilities declared allowed **remote access** to systems that could enable a hacker to execute code on targeted devices.
   A. TCP port 3389 and UDP port 3389

Use Case 2 – CISCO Switches.

4. Cisco further declared that this bug (CVE-2016-1453) is a result of “incomplete input validation performed on the size of overlay transport virtualization packet header parameters”.
   A. Buffer Overflow.

Use Case 2 – CISCO Switches.

Cisco Nexus 7000 and 7700 Series Switches Overlay Transport Virtualization Buffer Overflow Vulnerability

Critical

Advisory ID:	cisco-sa-20161005-otv	CVE-2016-1453	Download CVRF
First Published:	2016 October 5 16:00 GMT		Download PDF
Version 1.0:	Final		Email
Workarounds:	Yes		
Cisco Bug IDs:	CSCuy95701		
CVSS Score:	Base 10.0, Temporal 8.3		

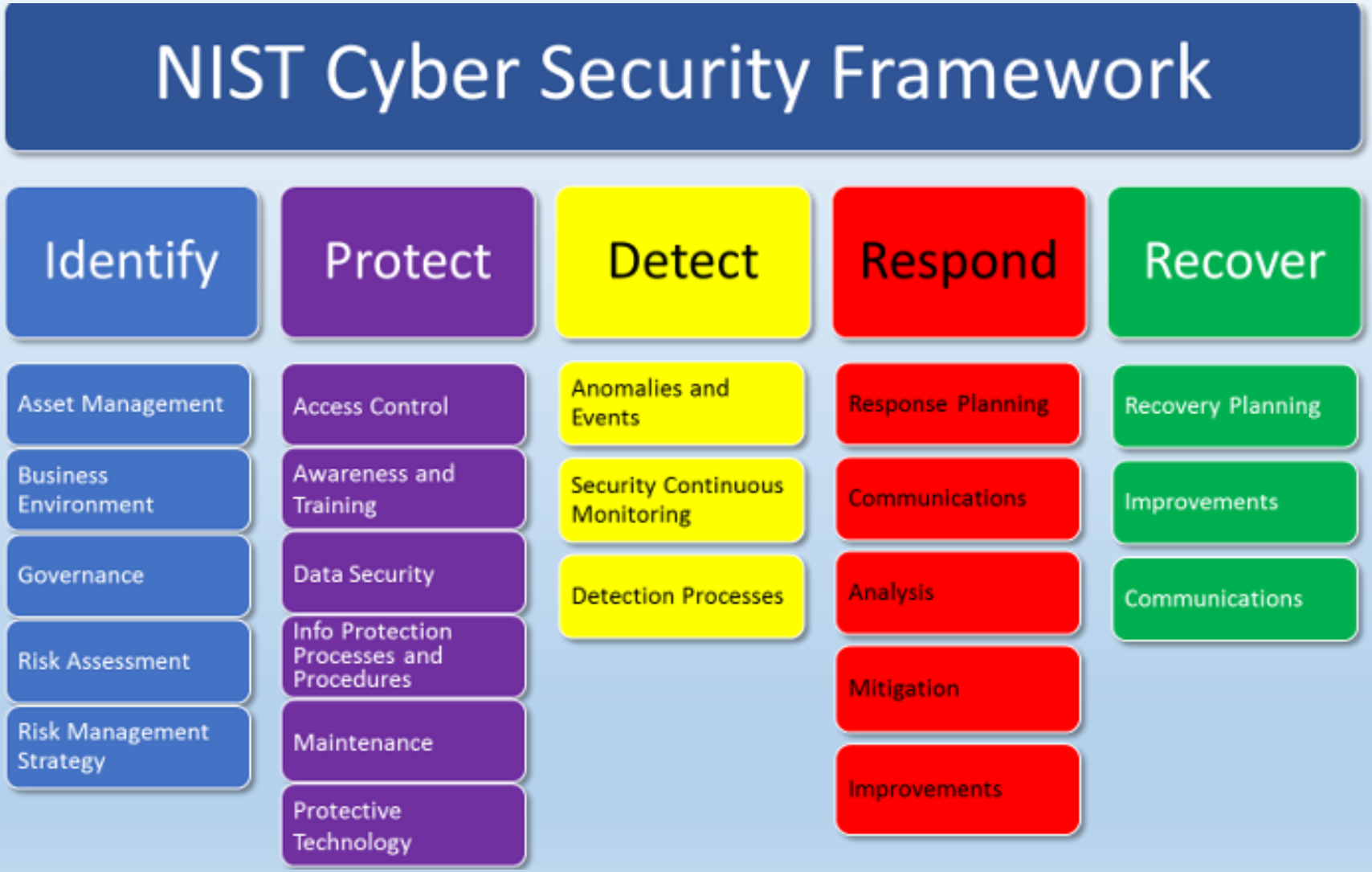
Summary

A vulnerability in the Overlay Transport Virtualization (OTV) generic routing encapsulation (GRE) implementation of the Cisco Nexus 7000 and 7700 Series Switches could allow an unauthenticated, adjacent attacker to cause a reload of the affected system or to remotely execute code.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Frameworks



Frameworks

OWASP Security Knowledge Framework

1. Security Requirements OWASP ASVS for development and for third party vendor applications
2. Security knowledge reference (Code examples/ Knowledge Base items)
3. Security is part of design with the pre-development functionality in SKF
4. Use SKF to gather the right security requirements for your projects
5. SKF then gives extensive knowledgebase items that correlates to the security requirements
6. Developers can close "tickets" and leave an audit trail to determine possible technical depts or improvements
7. Security specialist can follow the "tickets" and audit trail and verify or Fail closed items and provide feedback.

Summary - Security's New Ways

1. Fast and Agile
2. Security is a part of quality
3. Don't slow or block delivery
4. Enable and Be Empathetic
5. Automated Security testing in every phase
6. Join the continuous testing efforts
   A. What else interacts with it?
7. Do Penetration Testing alongside Pipeline delivery

Summary - Build

1. Outside-In Security Testing
2. Infra as Code (Testing)
3. Dynamic Application Security Testing (DAST)
4. Compliance on every build!
5. Cloud provider config as code
6. Using containers

Summary - Factor in Mobile and IOT

1. Android and IOS are different than Windows
   A. Ensure the latest security software and run anti-virus/malware scans are not blocked by your app.
2. Release all software updates as soon as they are available, including all web browsers.
   A. Post to and read the CVA databases.
3. Show respect for privacy for IOT home connected devices.
   A. Factor in the IOT devices terms of service.

Summary - Operations

1. Chaos Engineering and creating stability through instability
2. Circuit Break Pattern in use
3. Instrumentation and Visualization
4. Application security and service abuse and **misuse cases**
   A. Upstream and downstream
5. Bug Bounties
   A. Admit your errors modestly
6. Red Teaming as a Service

Questions

- Jeremy Swenson, MBA, MSST
- Founder and Principal Consultant at: www.abstractforward.com
- Cell: 651-492-4058
- E-mail: Jeremy.Swenson@abstractforward.com
- @abstractforward

Abstract Forward CONSULTING

Securing and improving business technology.

References

1. DevSecOps manifesto: http://www.devsecops.org/
2. Casper, Jones. “Applied software measurement (2nd ed.): assuring productivity and quality.” 1996:
3. NIST Cyber Security Framework 1.1. 2008.
4. Trend Micro, Malicious Breach Data Diagram, 2017.
5. Mike Larson, Principal Security Engineer at Ecolab.
6. Mitre Corporation, CVE-2016-1453P: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1453
7. OWASP. https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework