Cyber Monitoring in Modern Transit

Presented By: Justin K. Smith, CISSP

Rockwell Collins
Building trust every day

© 2018 Rockwell Collins. All rights reserved.

Overview

- Bottom Line Up Front: monitoring operational networks is critical
- What are the cyber-threats facing rail?
- What do monitoring technologies *really do*?
- How to use cyber-monitoring technologies to your advantage
- Scenario based discussion
- Wrap Up

© 2018 Rockwell Collins. All rights reserved.

Bottom Line Up Front

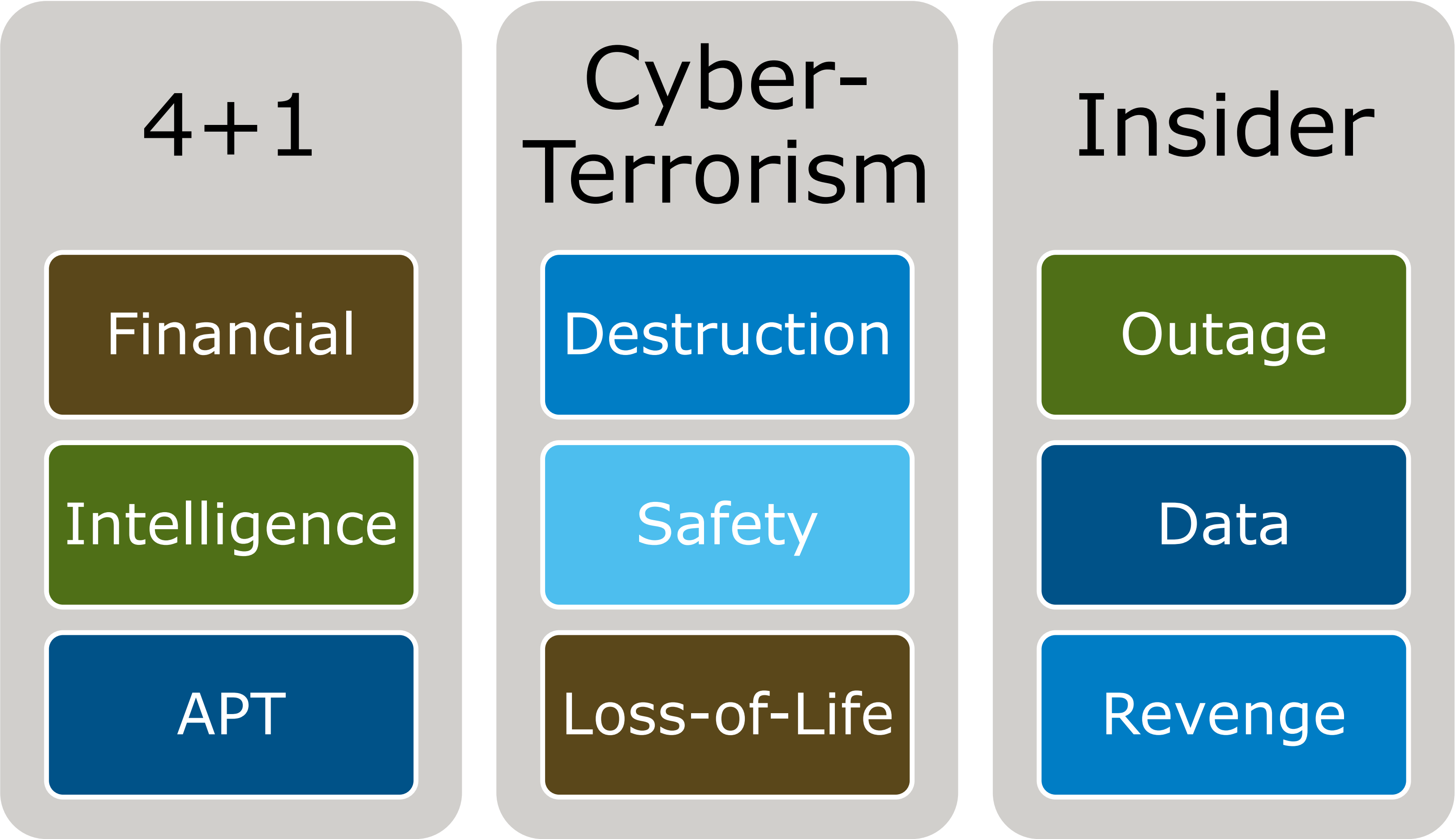
- Yes, rail is vulnerable to cyber-attacks
  - IT – we’ve seen it happen many times in the form of ransomware
  - OT – if we can find viruses on information displays; imagine what else could be found if we looked hard enough
  - Cyber-terrorism, Nation States, & Insider Threats

- Cybersecurity is not a plug-n-play technology; it is an organizational philosophy

- One word can sum up the end goal: ***RESILIENCY***

© 2018 Rockwell Collins. All rights reserved.

Cybersecurity Threats to Rail



4+1

Financial

Intelligence

APT

Cyber-Terrorism

Destruction

Safety

Loss-of-Life

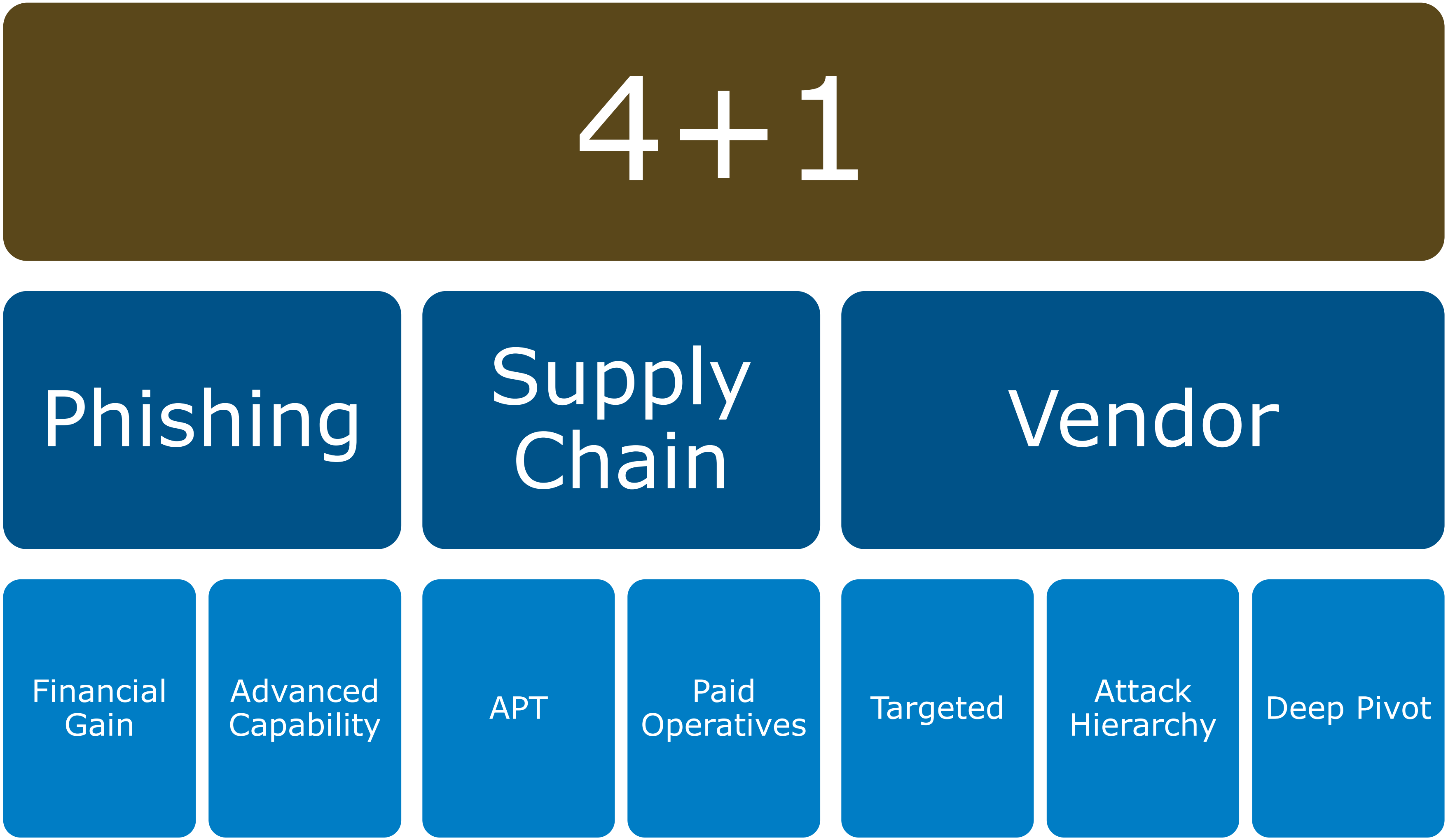
Insider

Outage

Data

Revenge

Cybersecurity Threats to Rail



4+1

Phishing

Supply Chain

Vendor

Financial Gain

Advanced Capability

APT

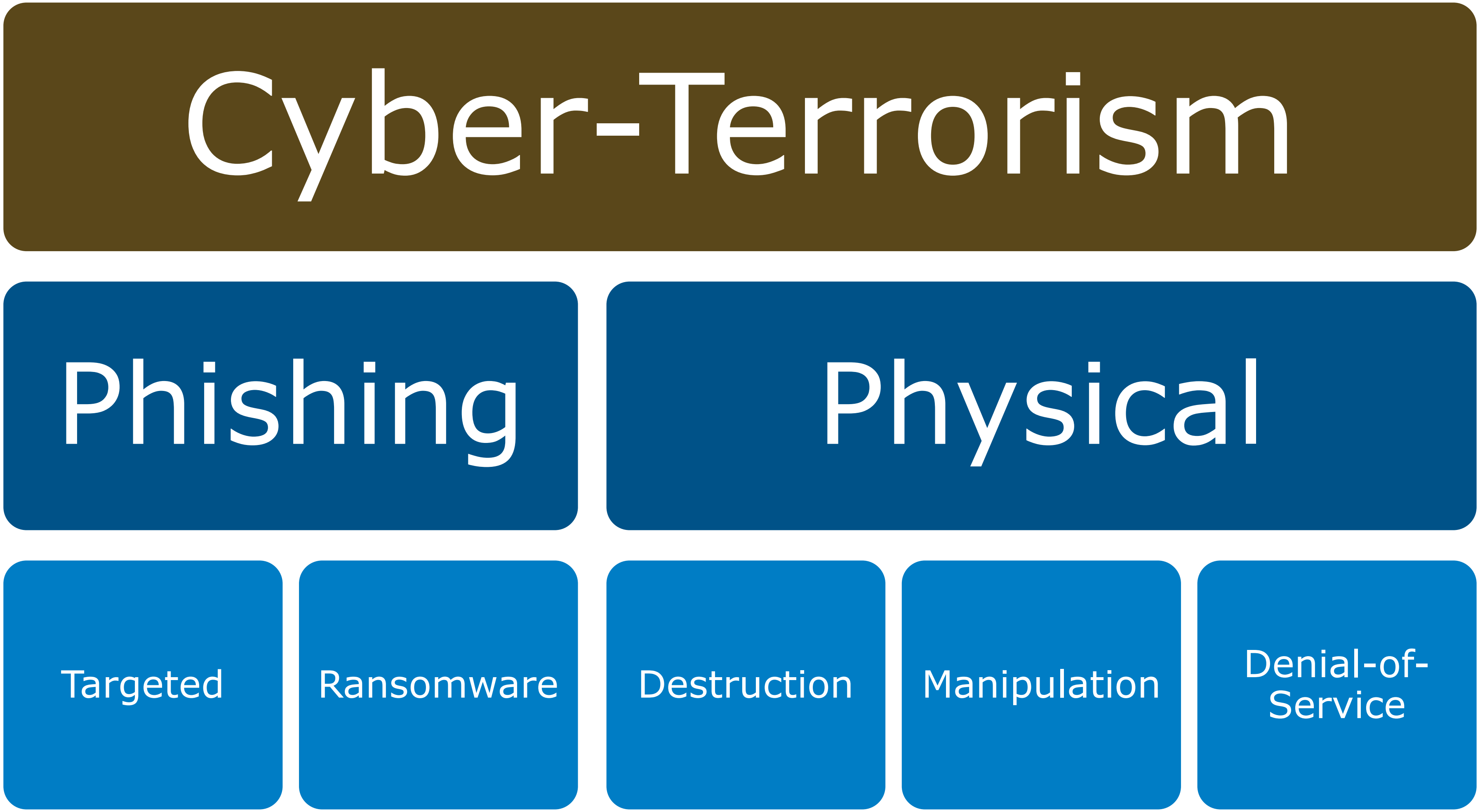
Paid Operatives

Targeted

Attack Hierarchy

Deep Pivot

Cybersecurity Threats to Rail



Cyber-Terrorism

Phishing

Physical

Targeted

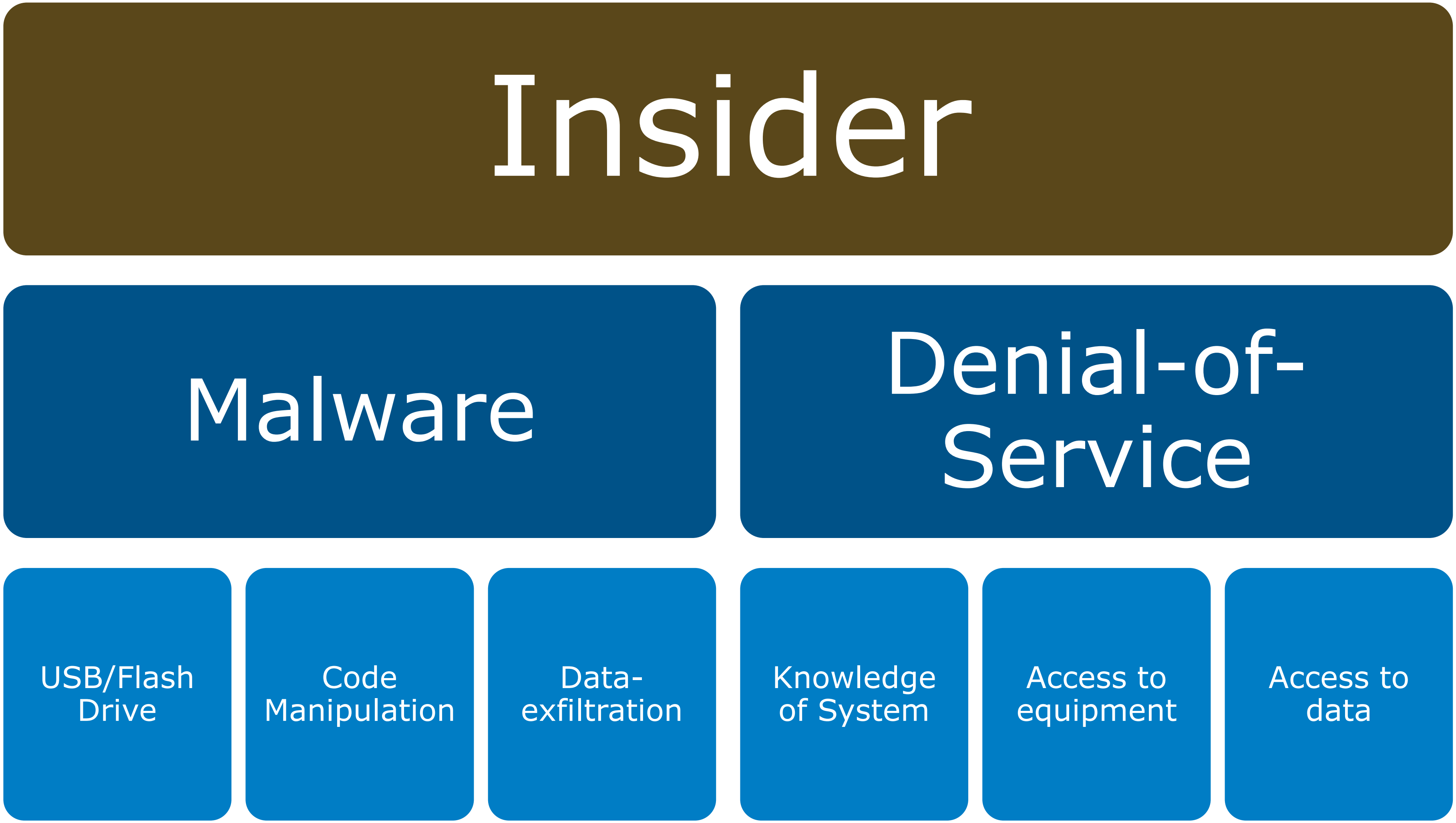
Ransomware

Destruction

Manipulation

Denial-of-Service

Cybersecurity Threats to Rail



Insider

Malware

Denial-of-Service

USB/Flash Drive

Code Manipulation

Data-exfiltration

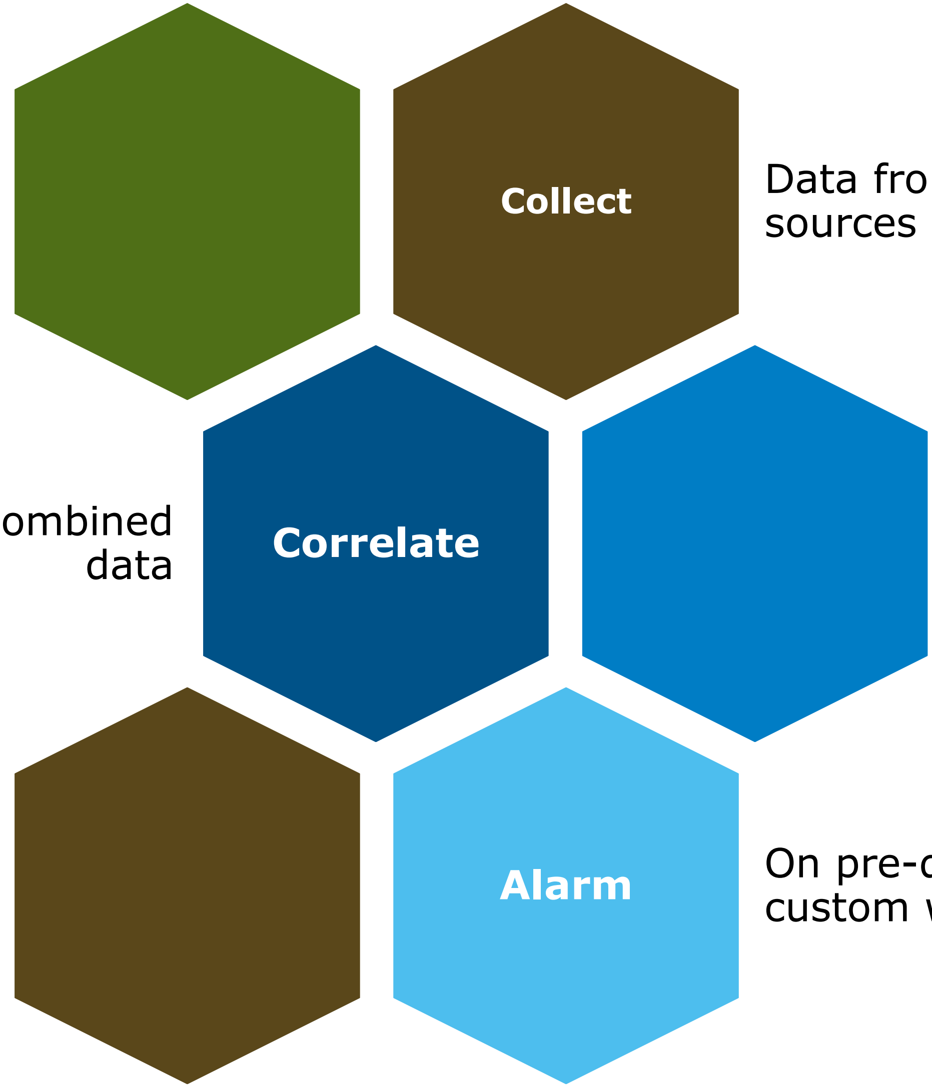
Knowledge of System

Access to equipment

Access to data

© 2018 Rockwell Collins. All rights reserved.

What Do Monitoring Technologies *Really* Do?



Collect

Data from many sources

Correlate

All of the combined data

Alarm

On pre-defined & custom written rules

Using Cyber-monitoring To Your Advantage

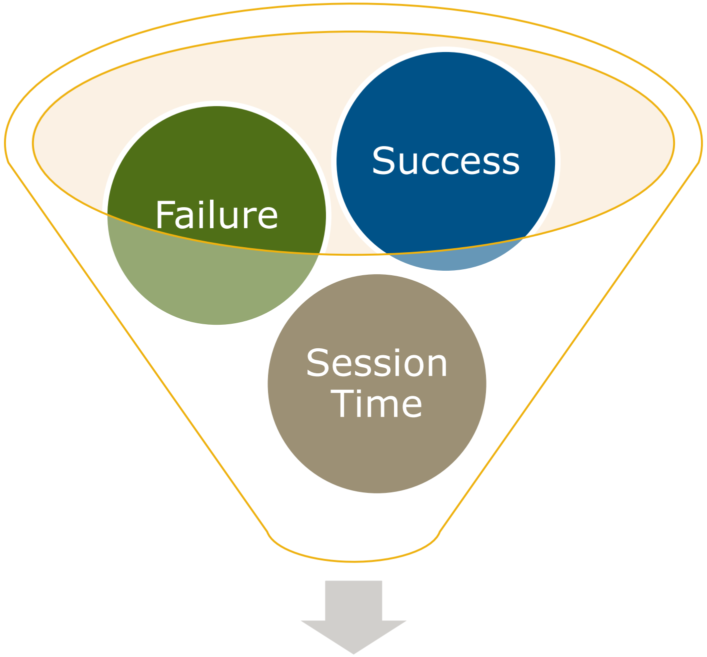
- This is a multi-dimensional challenge

- Yes, collecting, aggregating, and correlating log data will enhance visibility… But…
  - What are your current logging requirements?
  - How can your requirements better enhance monitoring?
  - What happens when an alarm is sounding?

- Buying a product and implementing only solves part of the challenge:
  - How do existing policies and procedures enhance the technology?
  - What needs to be changed to support operation of the technology?
  - Are you staffed and equipped to handle pre and post monitoring activities?

Using Cyber-monitoring To Your Advantage

- Think of logging in levels:
  - **Level 1:** Logging of **FAILED** login attempts
  - **Level 2:** Logging of **SUCCESSFUL** login attempts
  - **Level 3:** Logging of **SESSION** timestamps / windows
- By logging in "levels" you equip your network to more accurately track events from origin to end
- Think of how an attacker would attack your system… log accordingly
- TUNE YOUR EQUIPMENT



Monitoring

© 2018 Rockwell Collins. All rights reserved.

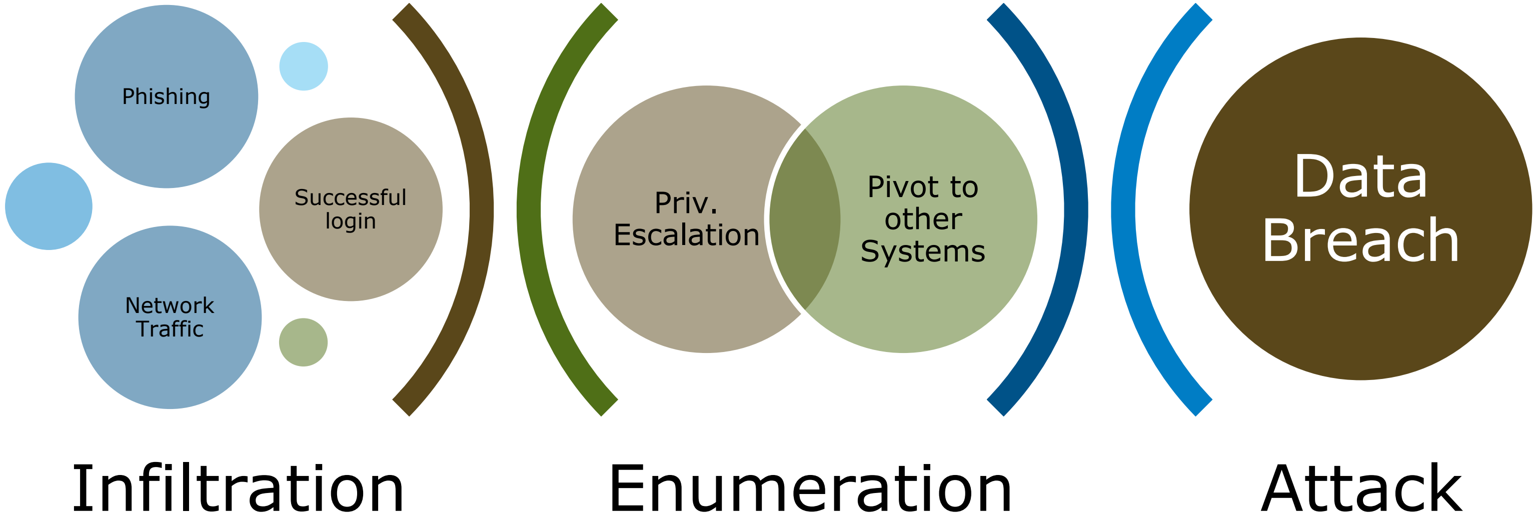
Using Cyber-Monitoring To Your Advantage

Level 1	Level 2	Level 3
Failed Login	Successful Login	File Integrity Checks
FW Block	Successful Connection	Session Timestamps
AV Detection	NIDS Network Traffic	Anomalous User Activity
Unauthorized Devices	Application Failures	Admin Priv. Useage

© 2018 Rockwell Collins. All rights reserved.

Using Cyber-Monitoring To Your Advantage

- When an attack occurs, follow the kill-chain
- A kill-chain is all of the events in sequential order which led to a successful attack
- By logging in "levels" kill-chains have more depth and detail and can enumerate *more* systems which may have been compromised
- Following the kill-chain requires trained and skilled staff who conduct Incident Response (IR)



© 2018 Rockwell Collins. All rights reserved.

Scenario Based Discussion

Cybersecurity Monitoring in Modern Transit

Scenario #1: Nation State Attacker

- You are a local-government subsidized (heavy) passenger rail organization who transports ~2 million monthly
- You have recently implemented a new control system software which has deeper visibility, connectivity, and capability in regards to "controlling" your locomotives
- After being notified of a breach in your vendor's network, you have implemented a Systems Information and Event Monitoring (SIEM) capability

- *How would you enhance your network in hopes of identifying probing and/or breach by a Nation State?*

Nation State attacks may not be malicious in nature… They may seek intelligence or financial gain/intellectual property.

© 2018 Rockwell Collins. All rights reserved.

Scenario #2: Cyber-Terrorism Attacker

- You have recently thwarted a Nation State level attacker because of your due diligence in implementing a SIEM
- Now a terrorist group has decided they are going to target and attack your infrastructure
- While your network is now logging detailed information, your physical and critical field devices have been un-modified
- Your enterprise networks have been getting hit daily by Denial-of-Service (DoS) attacks by other entities and you now fear they may go after your field devices

- *What can be done in terms of monitoring to better enhance your security posture and threat detection?*

Cyber-terrorism or Hacktivism may pose the largest cyber-threat to safety in transportation

© 2018 Rockwell Collins. All rights reserved.

Scenario #3: Inside Attacker

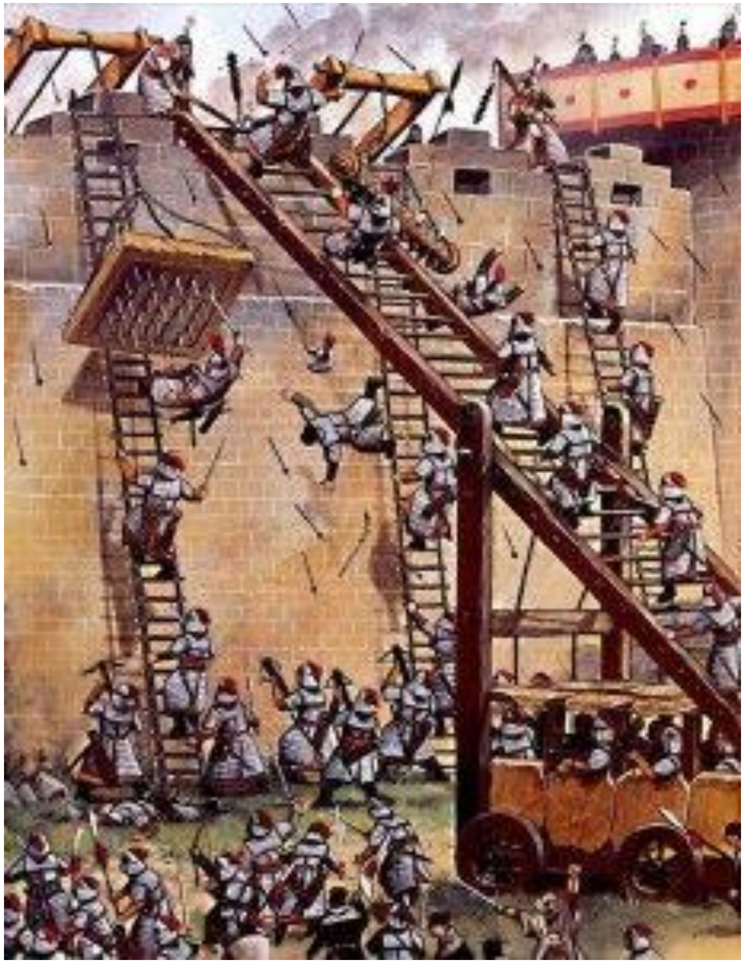
- Your organization has recently undergone a workforce reduction within your control facility
- A number of your long-time, adept systems admins and programmers have been notified they will be let-go at the end of the quarter
- Currently, your organization does not readily track log implementation (you only log at Level 1)
- It was decided years ago that admins and other key personnel would have USB/Flash Storage access on all systems

- *What can be done in terms of monitoring to better enhance your security posture and threat detection?*

Insider threats are a grim reality that every organization must face regardless of industry or purpose.

Wrapping It Up: Cybersecurity Monitoring = Resiliency

- Why won’t cybersecurity monitoring stop an attack?
- How can cybersecurity monitoring assist and enhance the detection of an attack?
- There is no plug-n-play solution
- Follow the kill-chain
- Cybersecurity isn’t a tool. It’s a philosophy
- What’s the end-goal? Resiliency



Contact Information

Justin K. Smith, CISSP, CEH

justin.k.smith@rockwellcollins.com

(410) 266-2353