RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **ZT-M05**

Bringing Zero Trust to Industrial Control Systems

William Malik

VP Infrastructure Strategies
Trend Micro
@WilliamMalikTM

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Agenda

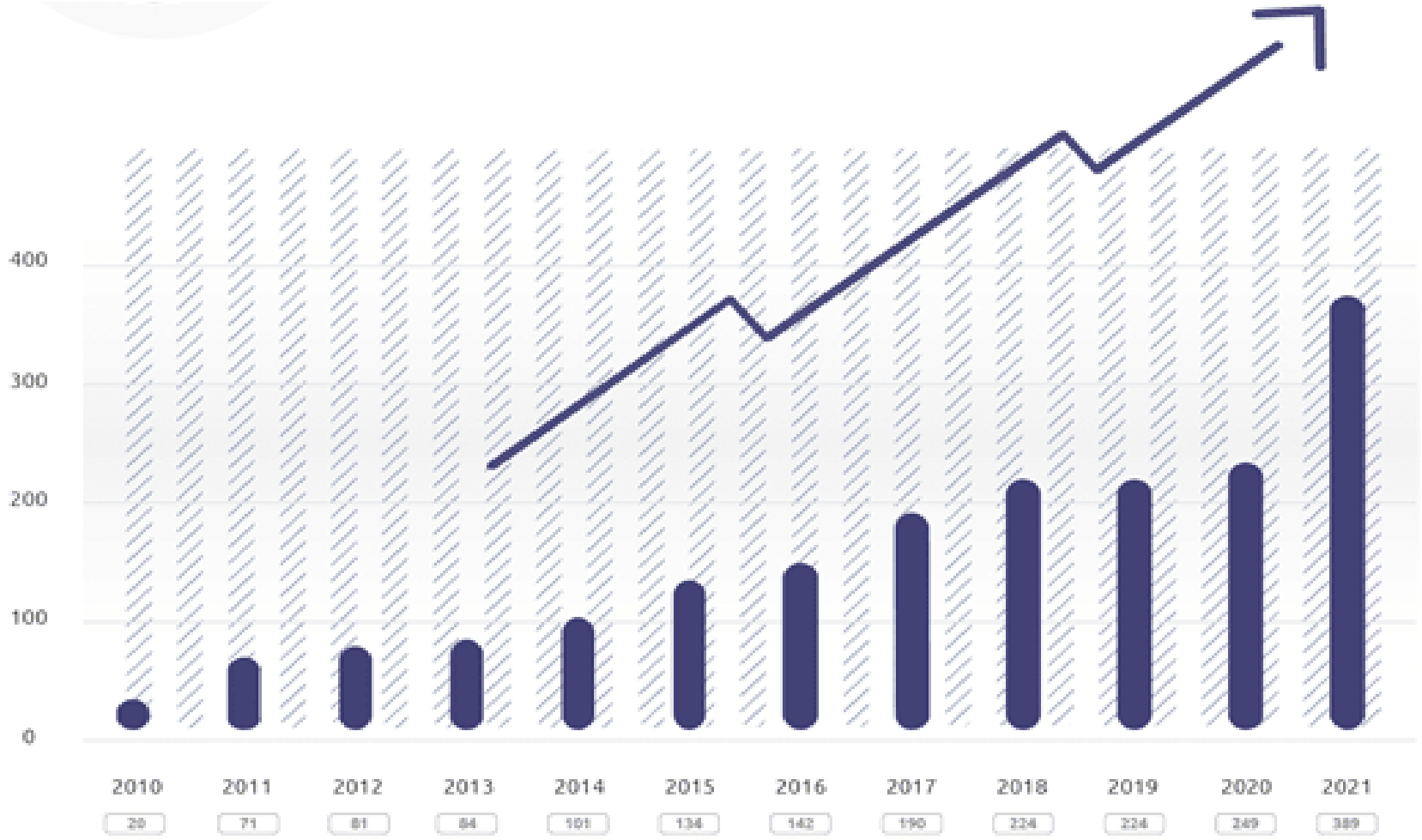
- Industrial Control Systems Vulnerabilities - Recent Attacks on IIoT
- What is Zero Trust?
- Integrating Zero Trust with IIoT
- Augmenting Cyber Process Hazard Analysis
- What ZT Cannot Do
- Future Requirements
  - Vendor requirements
  - OT/IT Alignment
  - Integrating MSPs
- What We've Learned
- References

RSAConference2022

ICS Vulnerabilities

As Factories Become Smarter, the Attack Surface Will Increase

ICS/CERT Advisories 2010 - 2021



Industrial Control Systems Vulnerabilities - History

Saudi oil refinery cyber-attack intended to trigger explosion, claims report

computing

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

WIRED

Timeline: How Stuxnet attacked a nuclear plant

BBC

Boeing production plant hit with WannaCry ransomware attack

THE VERGE

European Car Plants Halted by WannaCry Ransomware Attack

NEWS

TREND MICRO

Industrial Control Systems Vulnerabilities 2022

CISA **Releases** Security Advisories for Rockwell Automation Products

March 31, 2022

Siemens Addresses Over 90 Vulnerabilities Affecting Third-Party Components

March 2022

Schneider Relay Flaws Can Allow Hackers to Disable Electrical Network Protections

March 2022

Toyota's Japan Production Halted Over Suspected Cyberattack

February 2022

GE SCADA Product Vulnerabilities Show Importance of Secure Configurations

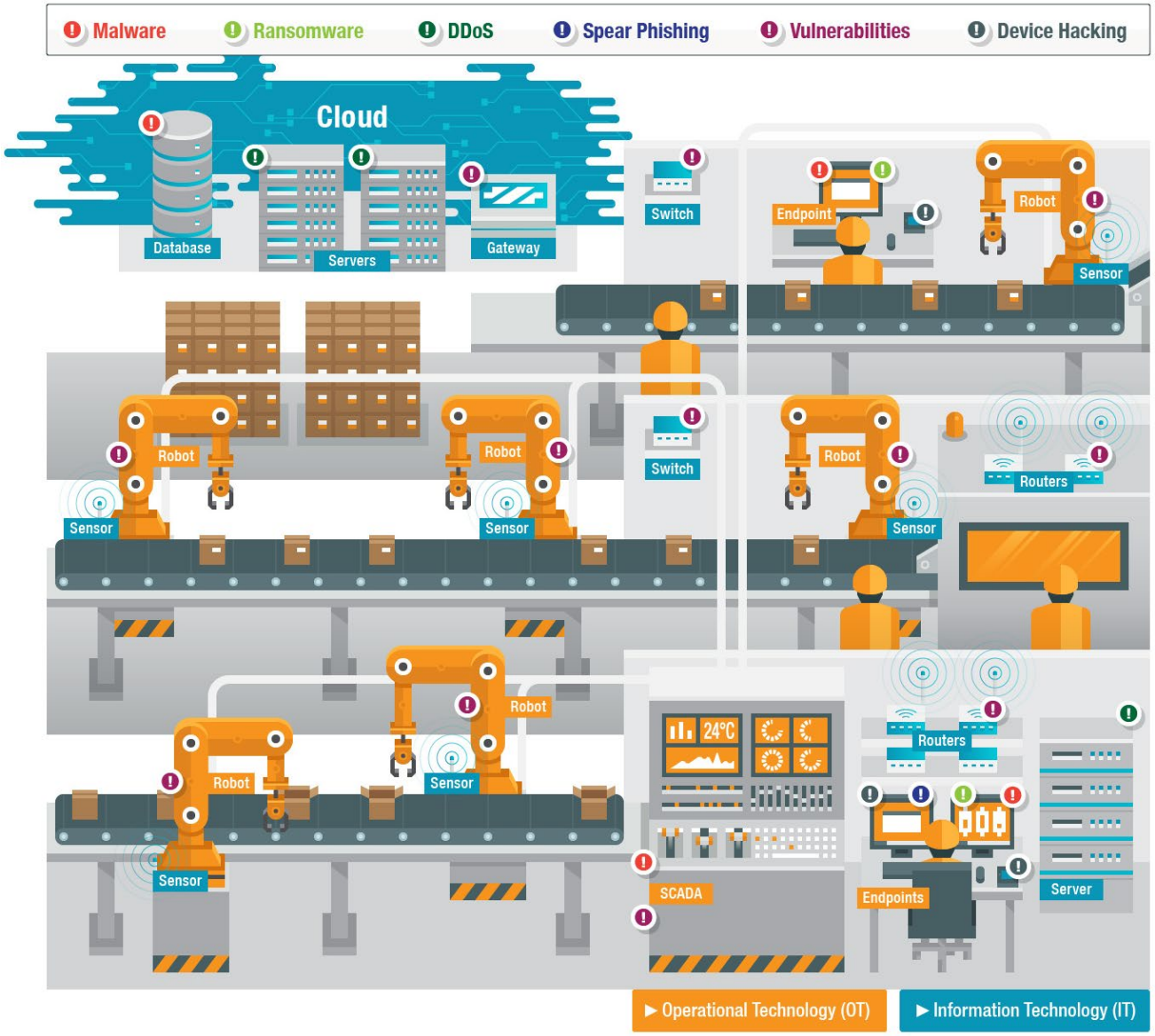
February 2022

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Worms, Old and New

- Conficker (Downadup) 2008
  - Martel bodycams infected at manufacture 2015
- Palevo 2009
  - Mariposa botnet taken down 2010, still active
- Gamarue (Andromeda, Wauchos) 2017 worm via USB
  - CC net disrupted 2017, still active
- EternalBlue 2017 fueled WannaCry and NotPetya
  - NSA developed, exposed by ShadowBrokers, patched 2017, MS17-010

Weak Points in the Industrial Environment



Attacks against Automation Software

Platform		File and configuration handling		Loading and executing code, including dynamically defined code, at runtime		Receiving data from or sending data to external systems
Language	Vendor	File system	Directory listing	Load module from file	Call by name	Communication
AS	Kawasaki					✓
Karel	Fanuc	✓	✓	✓	✓	✓
KRL	Kuka	✓				✓
Melfa	Mitsubishi	✓				✓
PacScript	Denso			✓	✓	✓
PDL2	Comau	✓	Indirect	✓	✓	✓
Rapid	ABB	✓	✓	✓	✓	✓
URScript	Universal Robots					✓

Recent Attacks on IIoT

- https://hub.tisafe.com/

RSAConference2022

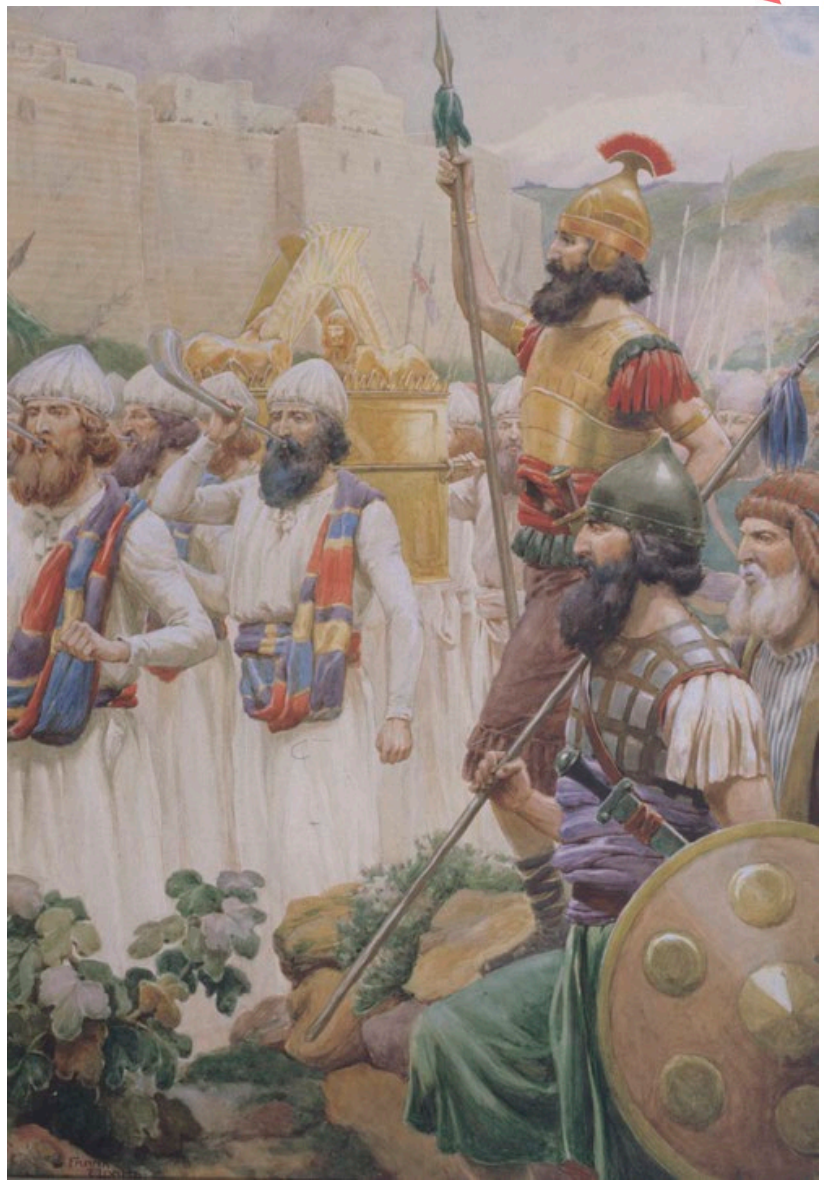
Zero Trust

Introduction

Integration with ICS

What is Zero Trust?

- The cloud has no perimeter
- There is a source of trust
- Assume minimal need to know
- MFA for critical tasks
- Log, verify, audit, review
- Establish separation of duties



Many Paths to Zero Trust

Verify identities:
Multi-factor Authentication

Restrict network access:
Micro-segmentation, DMZ's…

Default-deny app execution:
Application Safe-listing

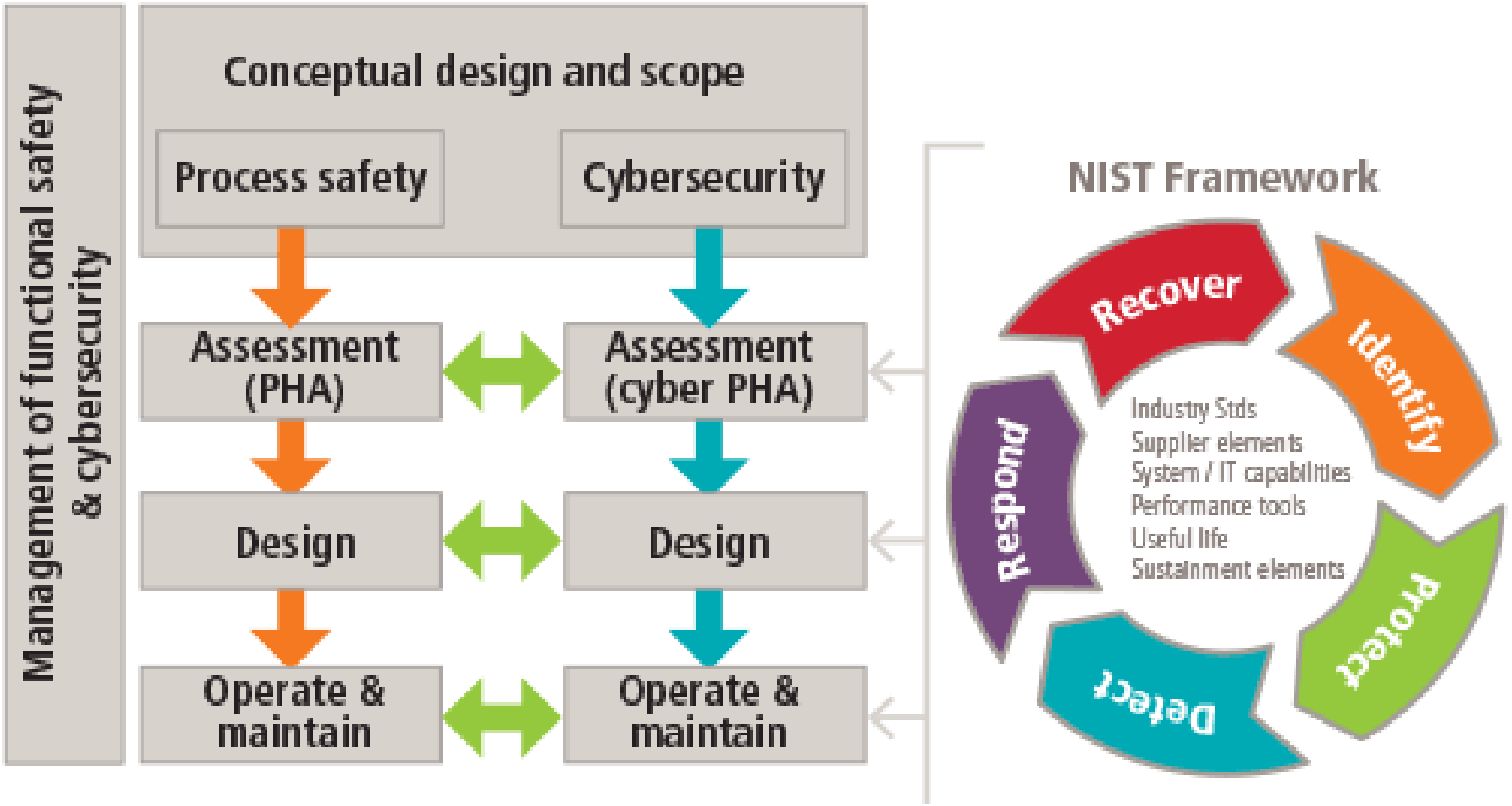
Continuously assess identity & device health:
Zero Trust Risk Insights

SASE / ZTE

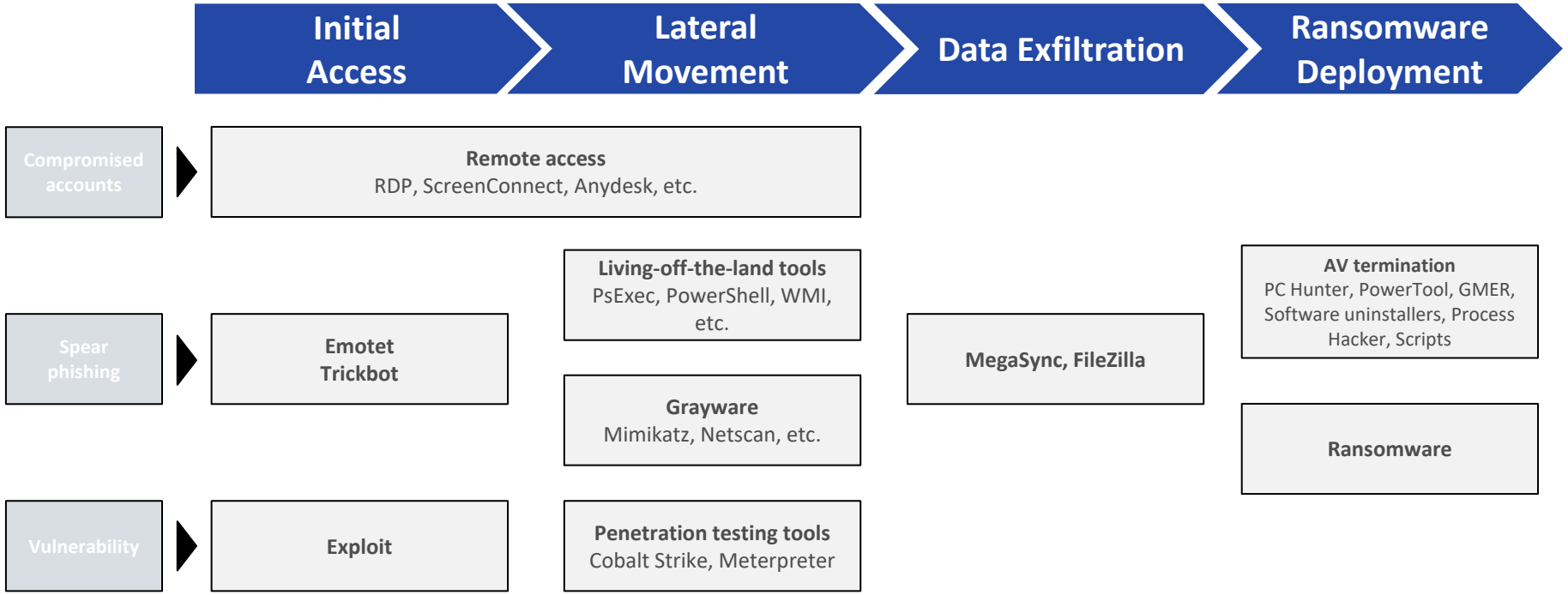
Get visibility to SaaS apps, control access:
CASB + secure web gateway (SWG)

Beyond VPN – provide a secure app-specific connection:
Zero Trust Network Access (ZTNA)

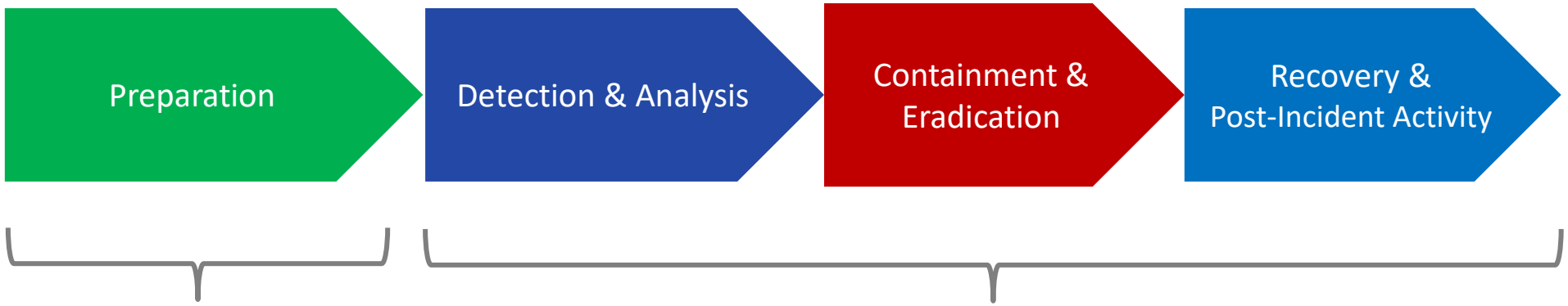
Cyber Process Hazard Analysis



Typical Attack Process and Tools



How to Defend: CISA Recommendations



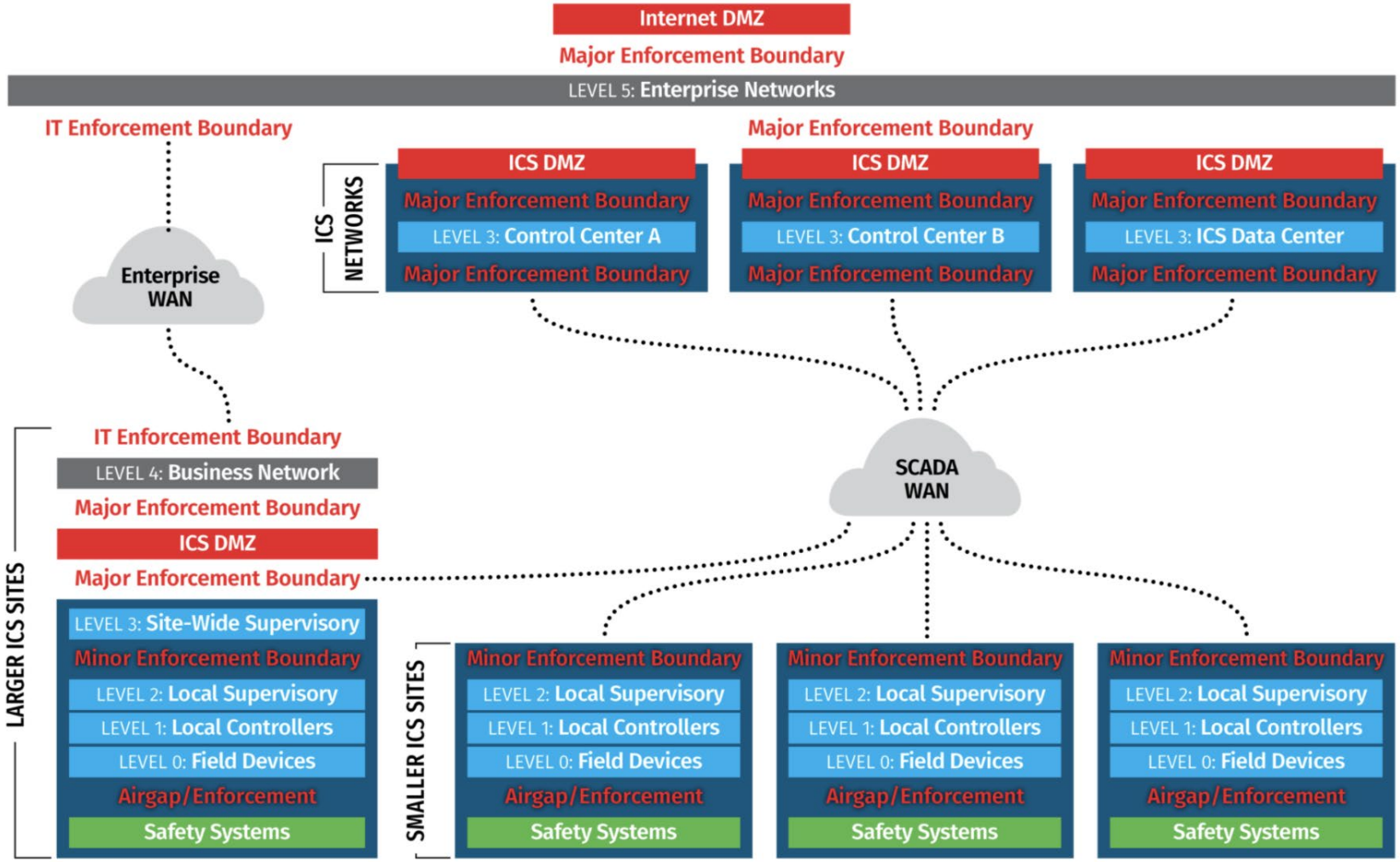
Reduce infection risks

- Asset and account management
- Resolve vulnerabilities
- Configure settings properly
- Determine dependencies and priorities
- Deploy security controls
- Risk management for 3rd parties
- Backup
- IR plan and exercise

Minimize impact

- Determine impacted systems
- Isolation
- Triage
- Rebuild and restore

ICS 410: SANS ICS/SCADA Security Essentials



Deploying Zero Trust - and Beyond - for ICS

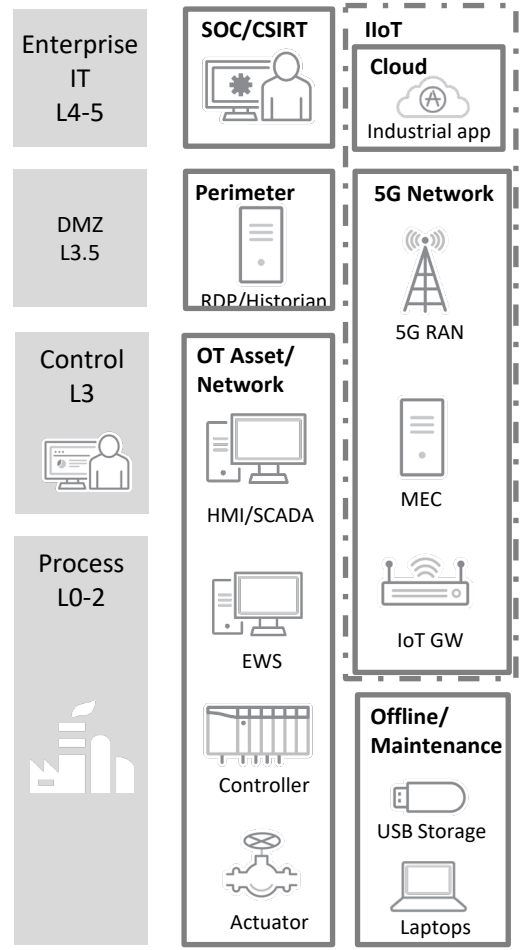
OT and IT perimeter: Establish boundaries between the corporate networks, factory systems, and the field. Segment the networks.

OT assets: Shield and monitor industrial endpoints that cannot run security software or be patched.

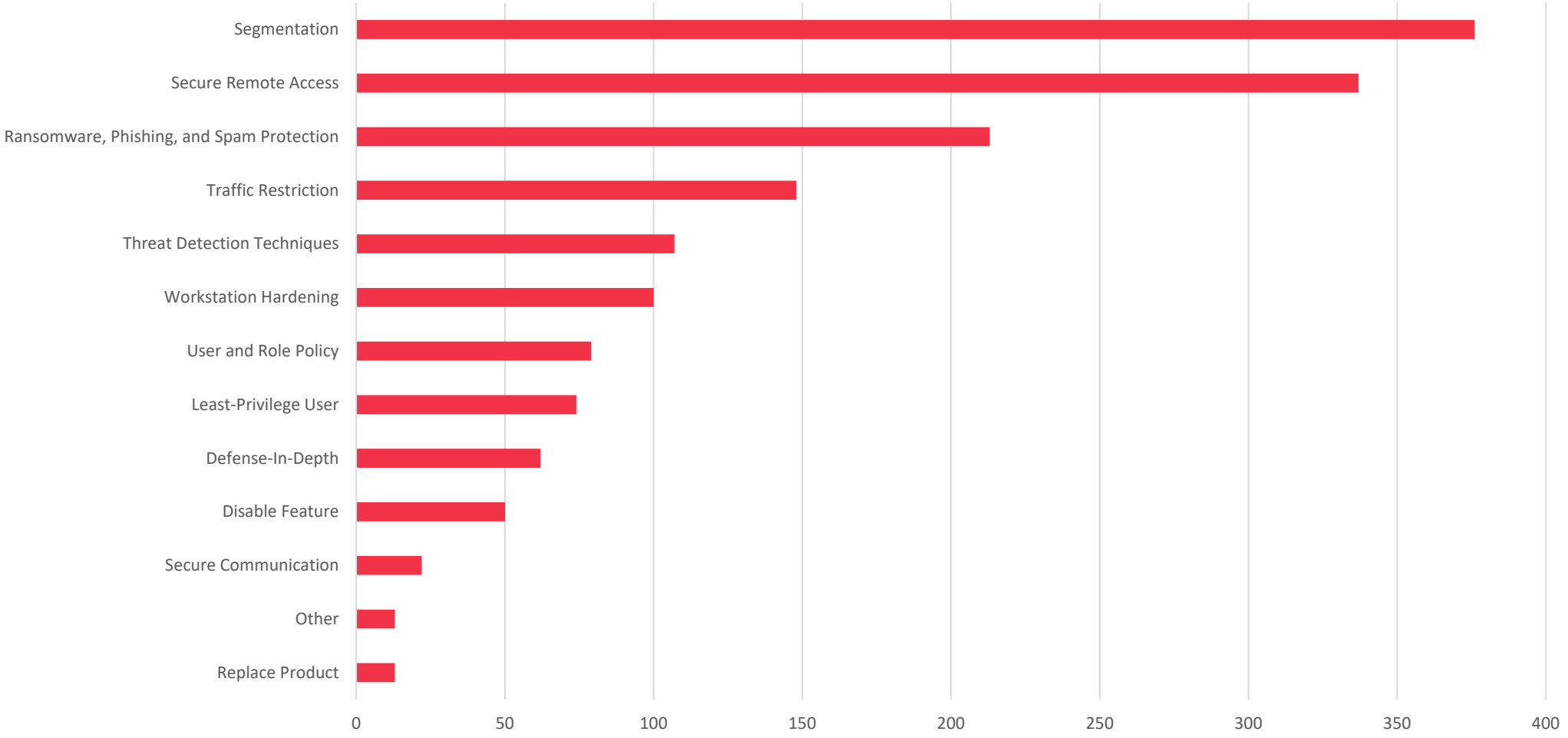
OT network: Use network security adapted to the industrial protocols and technology used in field networks.

Offline operations: Secure removable media and external devices brought in for maintenance.

SOC/CSIRT: Monitor the entire environment to streamline threat detection and incident responses.



Top Mitigation Steps – Claroty 1H21 Analysis



RSAConference2022

ICS Future Requirements

Why is ICS Security So Hard?

Not patched -
Not patchable

No Anti-virus

Easy to access facilities
once threats get in

Harsh, unique
environment

Conflicting
Architectural
Mandates

Worldwide
deployment

TREND MICRO

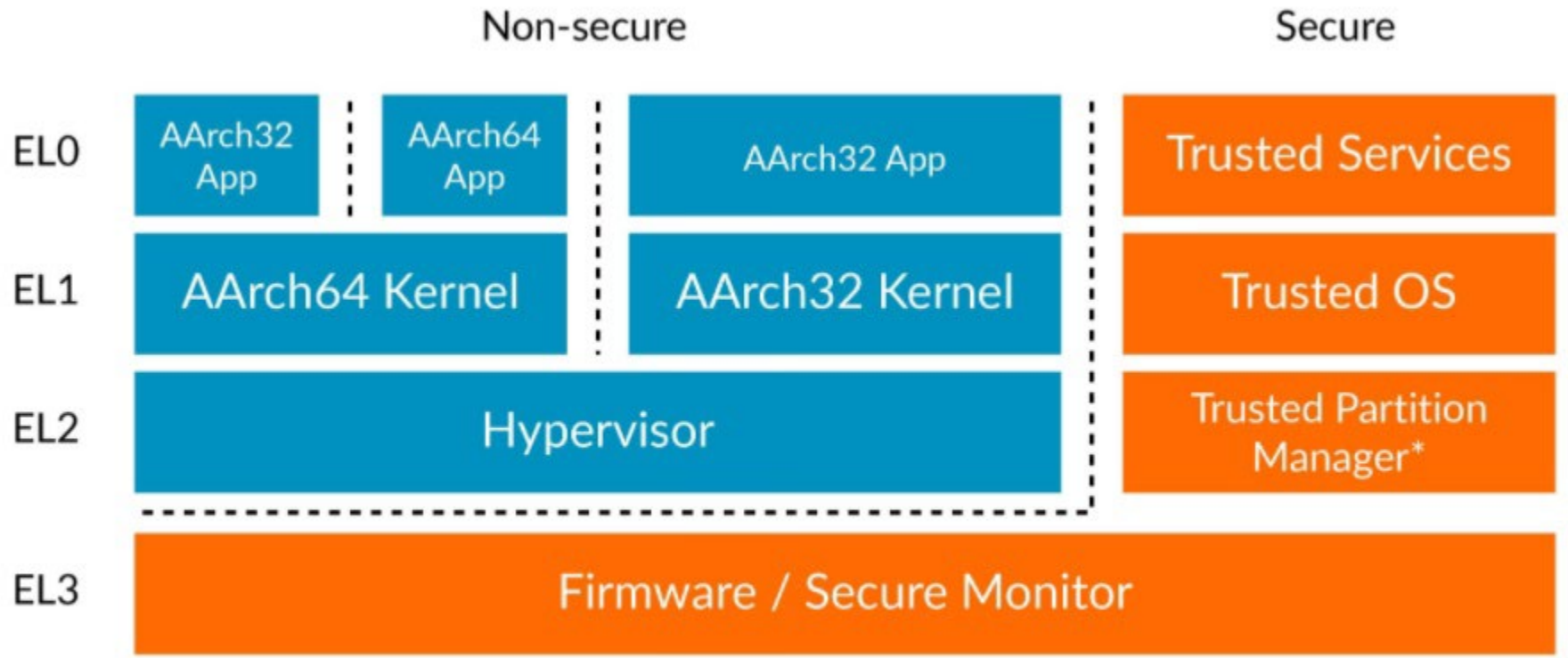
ICS Vendor Requirements

Exploit new processor capabilities

Provide telemetry and alerts

Enable basic authentication

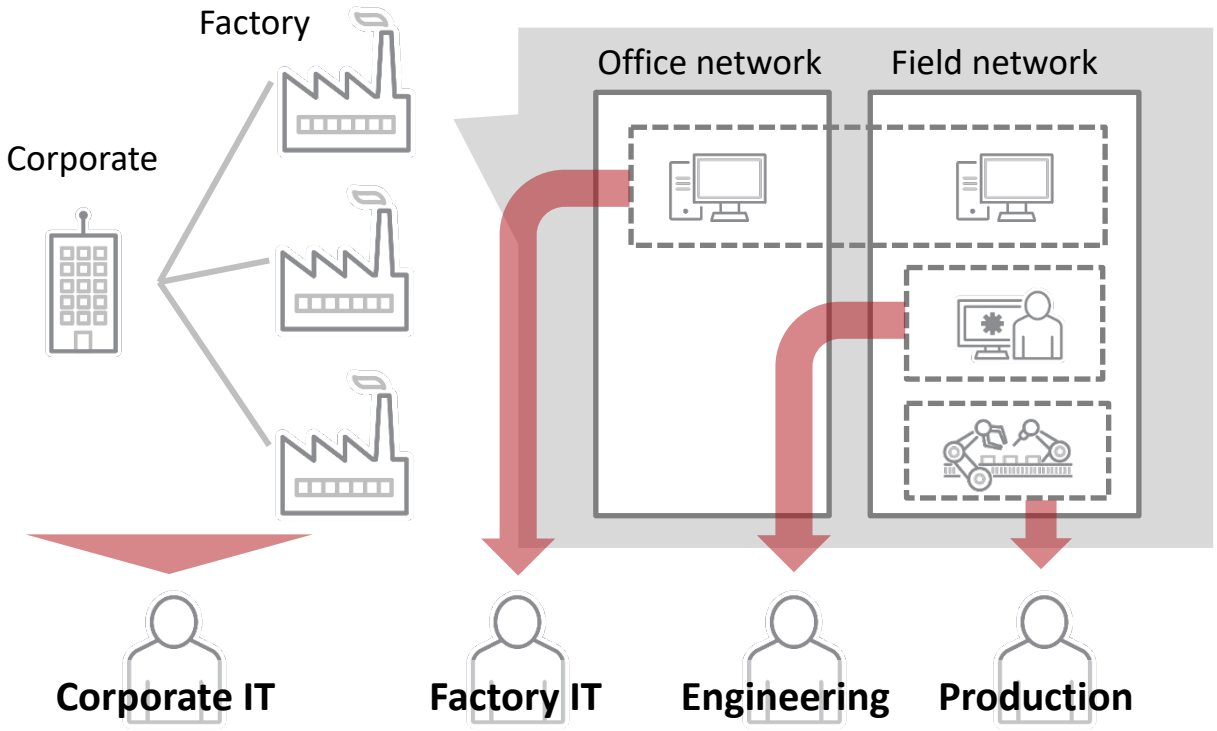
Securely update firmware, s/w



Source: ARM Developer, https://developer.arm.com/documentation/102412/0102/Execution-and-Security-states

* Secure EL2 from Armv8.4-A

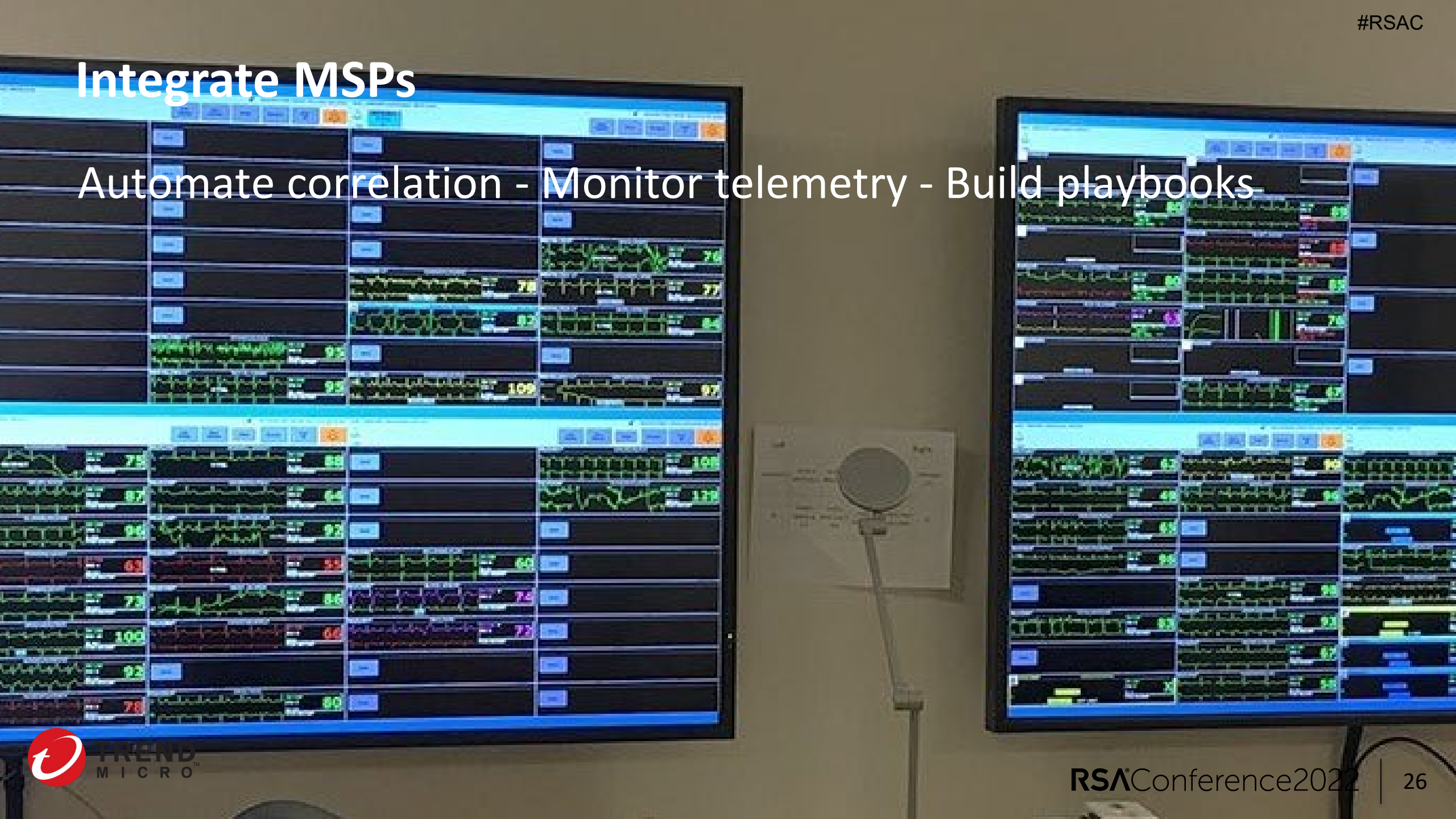
Organizational Silos Create Attack Surfaces



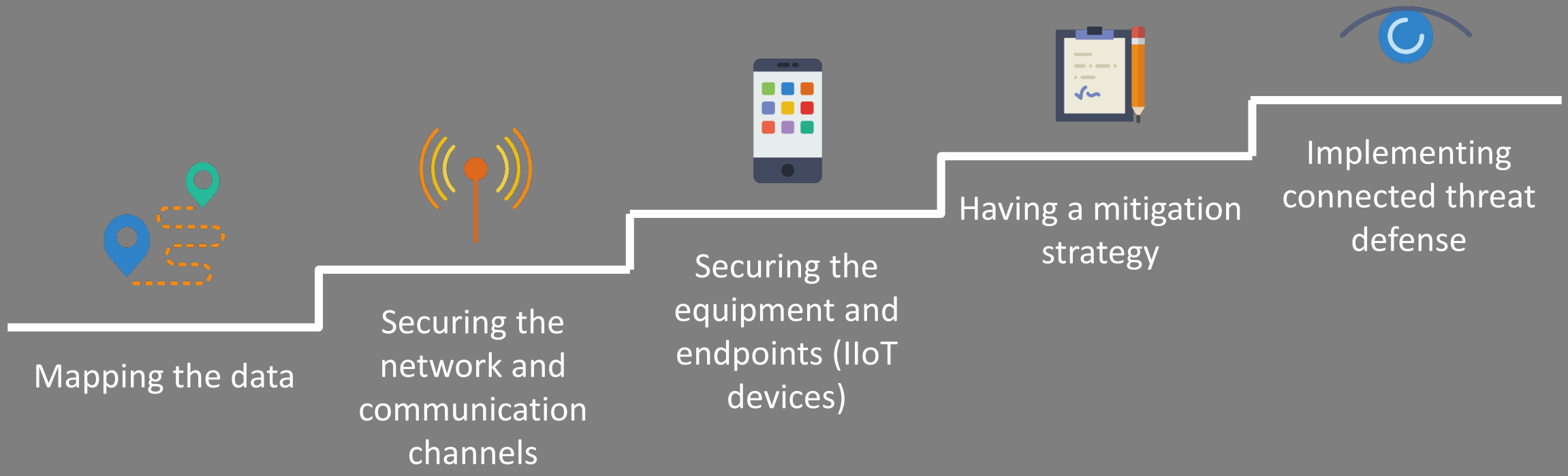
- Corporate IT monitors traffic between enterprise and factory
- Factory IT administers local networks and applications
- Production engineering teams design and integrate field networks
- Production team operates devices on shop floor

Integrate MSPs

Automate correlation - Monitor telemetry - Build playbooks



A Step-by-Step Guide to Securing the Industrial Environment



Apply What You Have Learned Today

- Next week you should:
  - Review Network Segmentation
  - Identify Flawed Air-Gap Assumptions
  - Isolate Critical Level 0/1 Systems
  - Include IT Security in ICT Design Discussions
- In the first three months following this presentation you should:
  - Segment IT and OT Networks
  - Review Supply Chain (hardware and software) for IIoT Environments
  - Institute rotational assignments between IT Security and ICS
- Within six months you should:
  - Deploy Secure Coding Practices for Industrial Systems
  - Incorporate Safety Systems and ICS Network Monitoring into SOC
  - Develop OT Upgrade Plan
  - Deploy 5G NPN Program for Wireless Environments

References

An In-depth Look at ICS Vulnerabilities, Trend Micro, https://www.trendmicro.com/pl_pl/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html

Incident Hub, Industrial Cybersecurity Incidents Database. https://hub.tisafe.com/ accessed March 13, 2022

PLC Vuln https://claroty.com/2021/05/28/blog-research-race-to-native-code-execution-in-plcs/

Army advisory https://gcn.com/articles/2021/05/27/army-iot-free-telework.aspx

Rogue Automation: Vulnerable and Malicious Code in Industrial Programming, Trend Micro, 2000. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/unveiling-the-hidden-risks-of-industrial-automation-programming

"A Blind Spot in ICS Security," Trend Micro, 2020. https://www.trendmicro.com/us/iot-security/news/6149 et seq.)

"TSMC Restarts Operations After Virus Takes Down Factories," 2019 https://www.sourcetoday.com/supply-chain/article/21867120/tsmc-restarts-operations-after-virus-takes-down-factories

"A security expert reportedly warned SolarWinds …" Business Insider, 2020 https://www.businessinsider.com/solarwinds-warned-weak-123-password-could-expose-firm-report-2020-12#:~:text=A%20security%20researcher%20said%20he,to%20a%20Tuesday%20Reuters%20report

"Security of Smart Manufacturing Systems," N. Tuptuk and S/ Hailes, Journal of Manufacturing Systems, v47 April 2018. https://www.sciencedirect.com/science/article/pii/S0278612518300463

"Reference Architecture for Smart Manufacturing: A Critical Review," Moghaddan, M et al. Journal of Manufacturing Systems, v49, Oct 2018. https://www.sciencedirect.com/science/article/abs/pii/S0278612518301043

NIST, "Smart Manufacturing Operations Planning and Control Program," National Institute of Standards and Technology, Gaithersburg, 2017.

Interoperability in Smart Manufacturing: Research Challenges, Machines, Zeid, A. et al. 2019. https://www.researchgate.net/publication/332175465_Interoperability_in_Smart_Manufacturing_Research_Challenges

"The Hallmark of Zero Trust is Simplicity," Wall Street Journal, CIO Journal, https://deloitte.wsj.com/cio/2021/04/07/john-kindervag-the-hallmark-of-zero-trust-is-simplicity/

Software-Defined Perimeter Specifications v2.0 Cloud Security Alliance, March 11, 2022, https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter-and-zero-trust/

Claroty Biannual ICS Risk Vulnerability Report 1H 2021, https://security.claroty.com/1H-vulnerability-report-2021

Learn the architecture: AArch64 Exception Model, ARM Developer, https://developer.arm.com/documentation/102412/0102/Execution-and-Security-states

RSAConference2022

Questions

@WilliamMalikTM

RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **ZT-M05**

Bringing Zero Trust to Industrial Control Systems

William Malik

VP Infrastructure Strategies
Trend Micro
@WilliamMalikTM