You make **possible**

Critical Infrastructure Security

Exploring End to End Security

Simon Finn

BRKCOC-1659

Agenda

- Introduction
- Critical Infrastructure: Risk and Opportunity
- Anatomy of attacks
- Holistic Security
- The network platform
- Conclusion

About me

Source: Sans.org

Security and Trust Organization

Defend Enterprise Business Operations

- Drive pervasive security
- Defend our global network
- Data protection and privacy
- Security awareness and education
- Report on risk and controls

Secure Our Offers

- Trustworthy technologies
- Cisco Secure Development Lifecycle
- Certifications
- Supply chain security
- Privacy by design

Industry Engagement

- Engage with key customers
- Contribute to Industry bodies and standards
- Share intelligence and leading practices
- Drive trustworthy practices & services

Critical Infrastructure: Risk and Opportunity

You make networking **possible**

68% of security professionals say security is the biggest challenge in IoT

Today we are going to cover how Cisco is going to help our customers address this challenge

Source: *2018 ZK Research Network Purchase Intention Survey*

Cyber Attacks in OT

According to Cisco's 2018 Security Capabilities Benchmark study, 31 percent of organizations have experienced attacks on OT infrastructure.

Those attacks are expected to become more common, while these systems often have few protections.

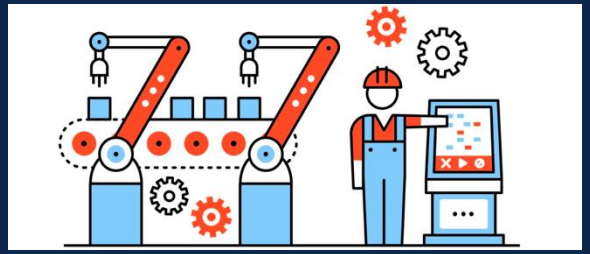
Source: Cisco 2018 Security Capabilities Benchmark Study

Industry **Digitization** Increases The **Attack Surface**

TODAY

Traditional automation systems

Energy, Manufacturing, Transportation, Process Industries



TOMORROW

The Industrial Internet of Things

Cybersecurity is key to control risks in modern industrial processes

Securing Industrial Networks is Challenging

Skills Shortage

How to streamline OT cybersecurity tasks with existing OT and IT staff?

Growing Threats

53% of industrial companies have already suffered cyber-attacks. Are you ready?

Source: IBM report 2017

Compliance

Must comply with new regulatory constraints (NERC CIP, EU-NIS…) and show shareholders that risks are under control

Agility

Converging OT & IT securely to capture the benefits of industry digitization

Impact

Human Harm, Critical Infrastructure, Environment

Scale

Larger Attack Surface, Data Volume, Complexity

Business

New Players, Device Lifecycle, Organizational Conflict

Constraints

Hardware Limitations, Access Issues, Physical Exposure

Brief History of Cyberattacks in ICS Environments

Security Through Obscurity

Security through obscurity

From Wikipedia, the free encyclopedia

Security through obscurity (or **security by obscurity**) is the reliance in security engineering on design or implementation secrecy as the main method of providing security to a system or component. Security experts have rejected this view as far back as 1851, and advise that obscurity should never be the only security mechanism.

* When used as an independent layer, obscurity is considered a valid security tool.

"On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network."

Source: The Subcommittee on National Security, Homeland Defence, and Foreign Operations May 25, 2011 hearing

Lack of Cybersecurity Hinders the Innovation Potential of Digitization

"Cybersecurity risks and threats hinder innovation in my organization."

71%

"My organization halted a mission-critical initiative due to cybersecurity concerns."

39%

Survey: 1014 respondents

"Innovations are moving forward, **but probably at 70%-80% of what they otherwise could** if there were better tools to deal with the dark cloud of cybersecurity threats."

Airline Industry CFO

Please Mind the Gap

Every Challenge is an Opportunity

The **Chinese word for "crisis"** (simplified Chinese: 危机; traditional Chinese: 危機; pinyin: *wēijī, wéi jī*[1]) is frequently invoked in Western motivational speaking as being composed of two Chinese characters signifying "danger" and "opportunity" respectively. While the original meaning of *wēijī* is "danger at a point of juncture," and many linguists and native Chinese speakers highlight the errors in its Western reinterpretation, the term's "danger-plus-opportunity" meaning has been so widely used by politicians, businesspeople, and in popular culture that its alternative etymology has been picked up all over the world, including by some native Chinese speakers.

Security its uniquely positioned to help navigate the divide

Holistic Security

You make security **possible**

End-to-End Security Capabilities

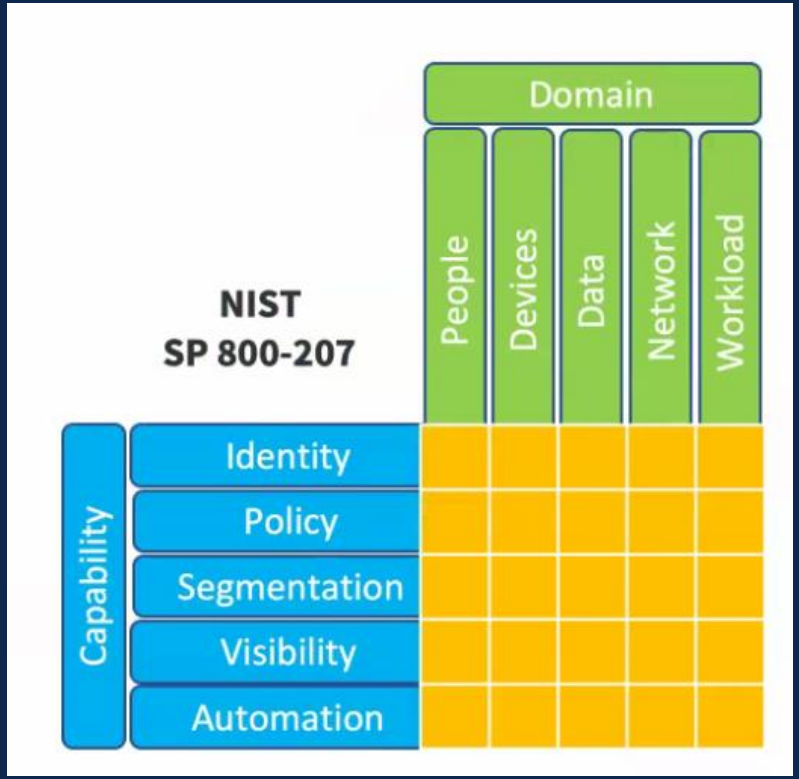
PROCESS	Onboarding Inventory	Policy Access Control	Misbehavior Detection	Alert Ecosystem	Resume Operations
NIST CSF					
	Identify	Protect	Detect	Respond	Recover
TECHNOLOGY	Profiling BRSKI Visibility	Segmentation MUD Secure DNS	NBAD ML / AI	Containment Quarantine	Updates Restore

End-to-End Security Capabilities

When looking at an architecture to determine acceptable levels of security maturity, we can bolster other areas to compensate for weakness in another

NIST CSF

Zero Trust



Anatomy of Attacks

You make the power of data **possible**

Ukraine Power Grid Attack (2015)

Device Attacks

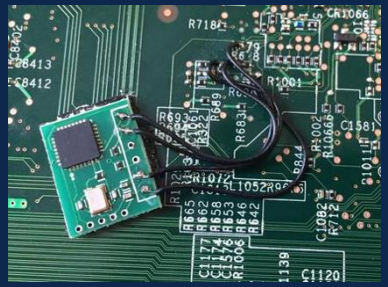
Hardware Attacks – Identity Attack Example

Keystroke Loggers

Doobiekey/Rsa Tokin

Mod Chip

Counterfeit/Bypass



Skimmer

Run Time Attacks

Examples:

- Side channel
- Cache attack
- Overflow/Stack Smash
- Privilege escalation

Goal:

- Increase access
- Allow further compromise
- Lateral movement

Persistence

Examples:

- Replace firmware
- Replace BIOS
- Replace boot loader
- Rootkits

Goal:

- Increase access
- Allow further compromise
- Lateral movement

Attacking a Device (And Cisco Protections)

Multilayered security protections to create defense-in-depth

Network Device Integrity - Attack Detection

Hardware

BIOS

ROMMON

Software

Booted

Hardware Tampering	BIOS Attack	ROMMON Attack	Binary Attack	Run-Time Attack

Harder — Attack Detection — Easier

Network Device Integrity – Threat Mitigations

Hardware

BIOS

ROMMON

Software

Booted

Hardware Tampering	BIOS Attack	ROMMON Attack	Binary Attack	Run-Time Attack
Supply Chain Security	Trust Anchor Module Secure Boot Digitally Signed Software			Run-Time Defenses

The Network Platform

You make security **possible**

The Network is the Foundation for IoT Security

Visibility + Threat Detection

See Everything

Segmentation

Reduce Attack Surface

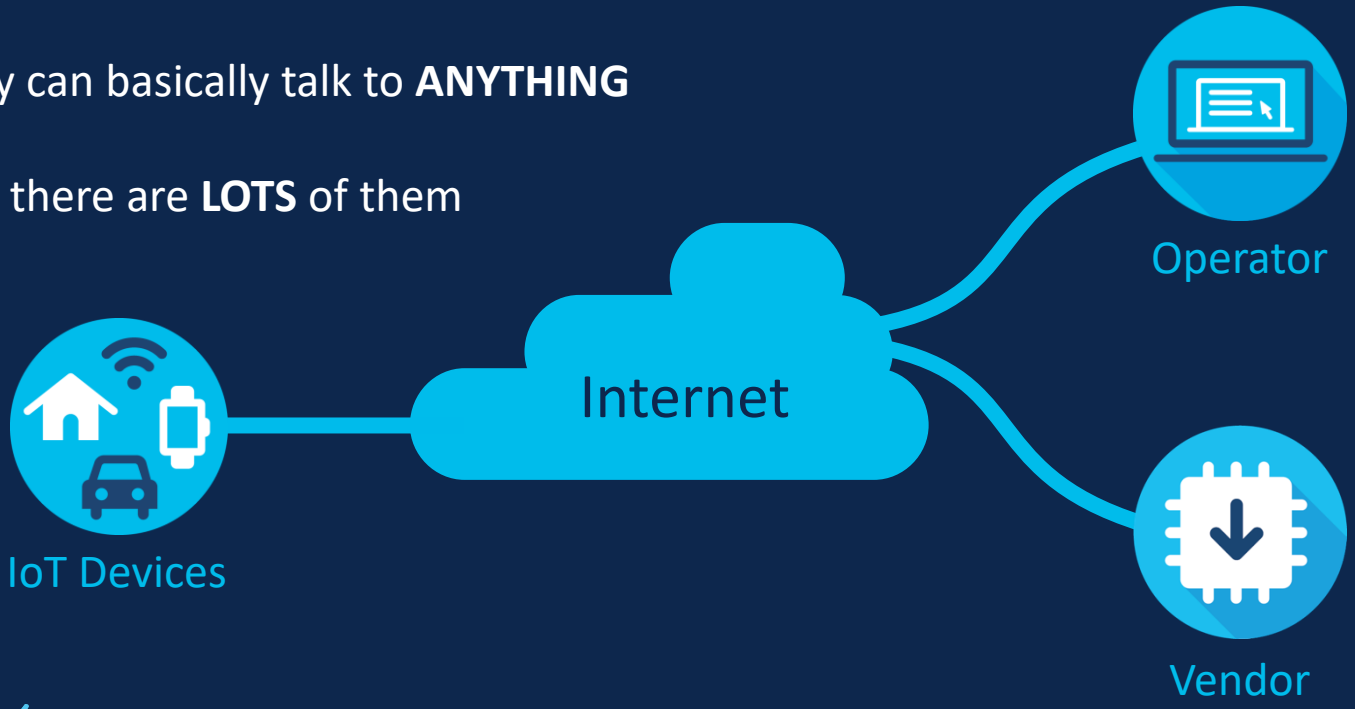
Response + Recovery

Stop the Breach

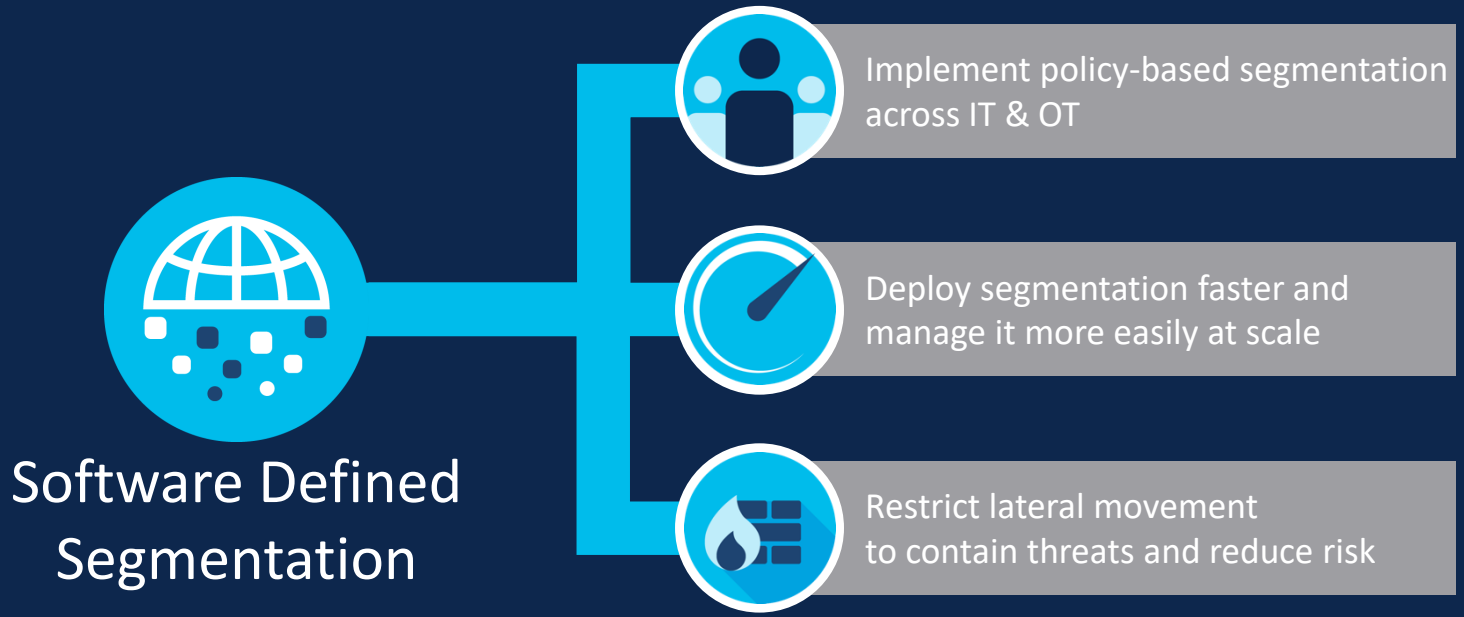
Trusted Infrastructure

Key Security Challenges

1. Device aren't as **SECURE** as they need to be
2. They can basically talk to **ANYTHING**
3. And there are **LOTS** of them



Segment – As Close as Possible to the Device



Impact

Human Harm, Critical Infrastructure, Environment

Scale

Larger Attack Surface, Data Volume, Complexity

Business

New Players, Device Lifecycle, Organizational Conflict

Constraints

Hardware Limitations, Access Issues, Physical Exposure

1:200

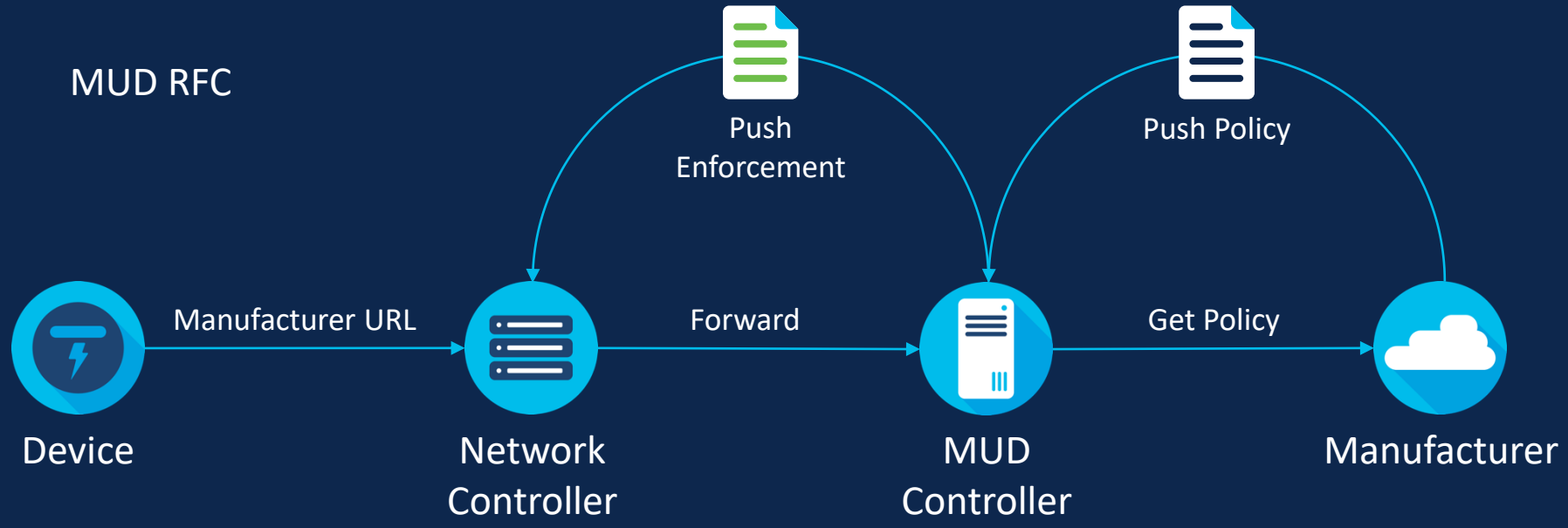
1:1,000,000

Challenge

Understand expected device behavior and turn it into policy

Solution

IETF Standard Manufacturer Usage Descriptions (MUD)



Onboarding Time to Service

Without MUD

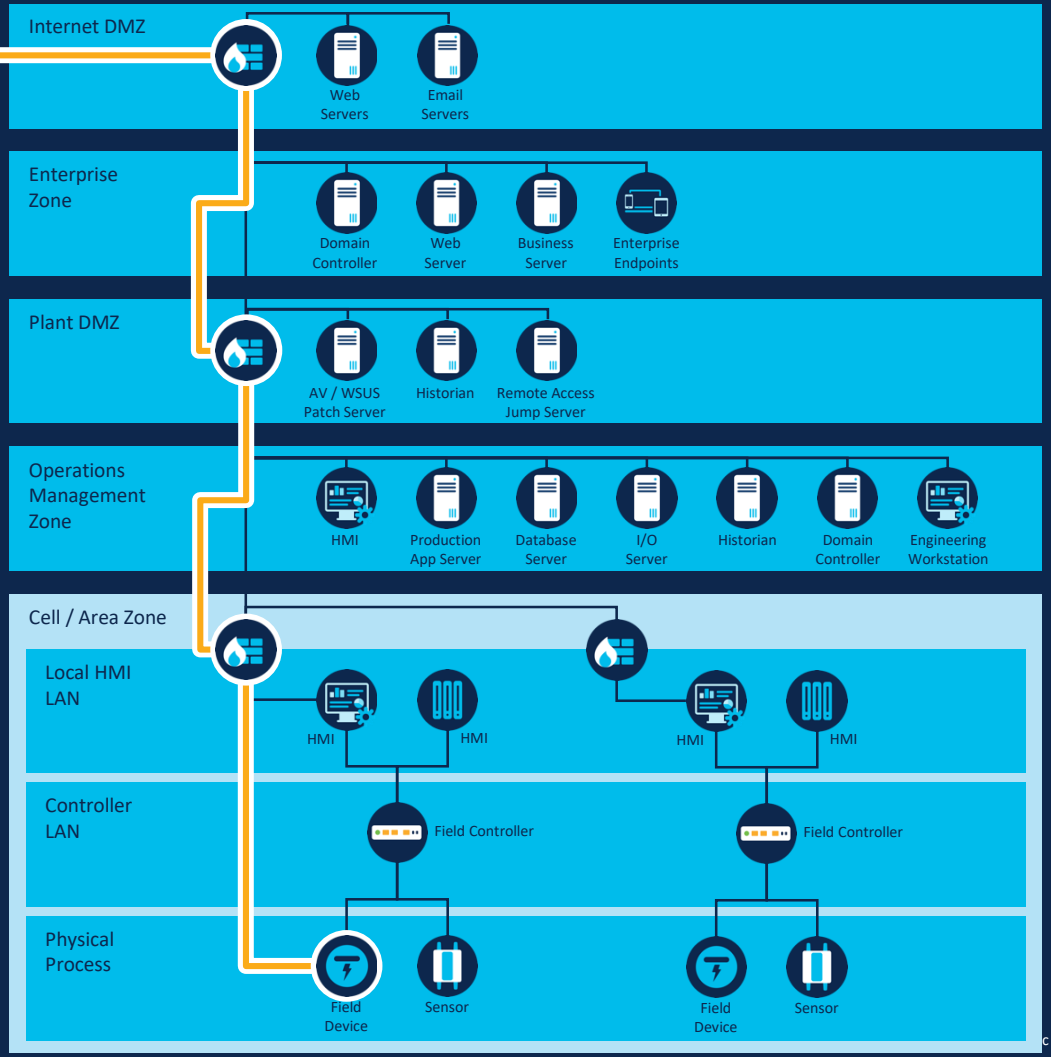
With MUD

[Lower Operational Cost]

~~Remote~~ Access

Encrypt remote access
Enforce multi-factor access control
Ensure vendor security posture
Enforce network path and QoS
Context based access to select devices
Log vendor activity

Connectivity happens everywhere



Connected Roadways - Example

Connecting myriad of things (video, sensors, signage, DSRC, edge compute)

Improve safety and efficiency,

Provide better user experience

Connected Roadways – Security Requirements

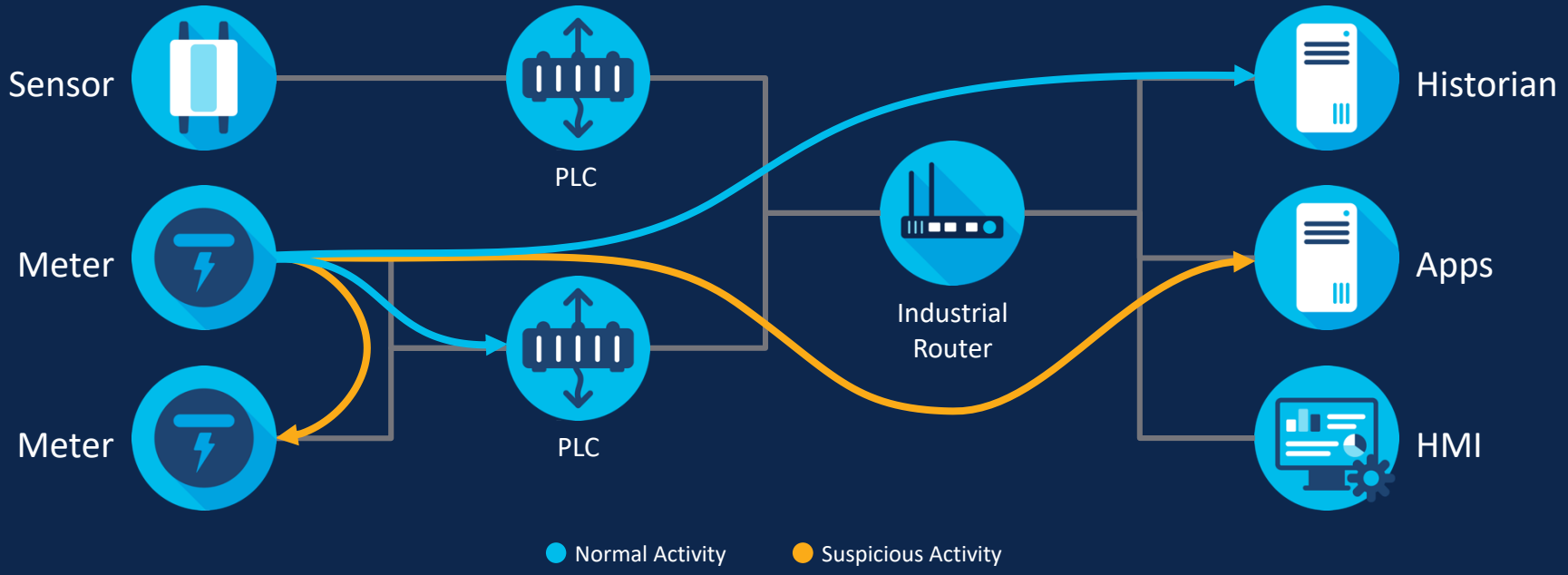
Micro-segmentation of the different services

Reliability, speed, management and assurance

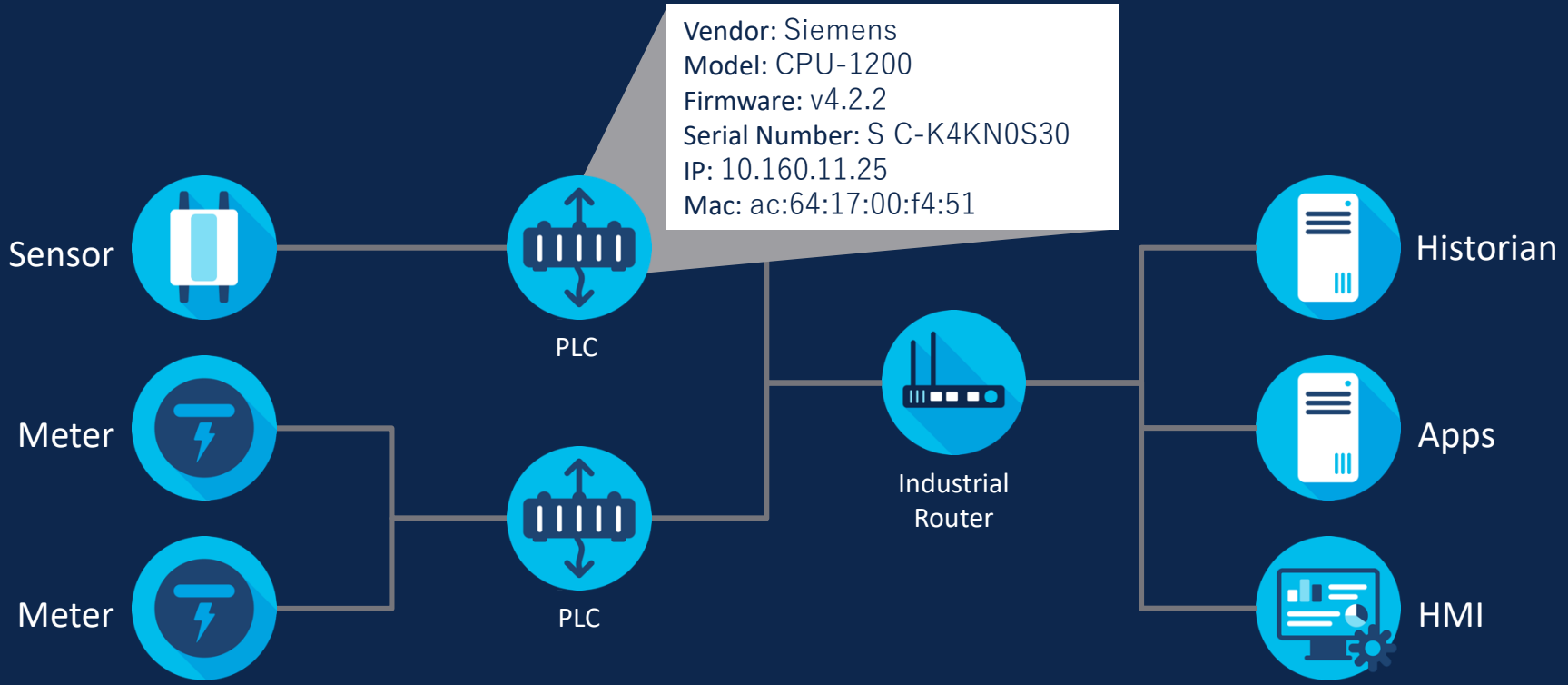
Data security

Key Security Problem #2

Understanding when devices are misbehaving



Visibility Step 1: Know your Assets



Lack of Visibility is a Problem in ICS Environments

You can’t secure “things” in IoT if you don’t know what they are and what they are talking to

Most customers don’t have accurate Asset Inventory

55% have no or low confidence that they know all devices in their network

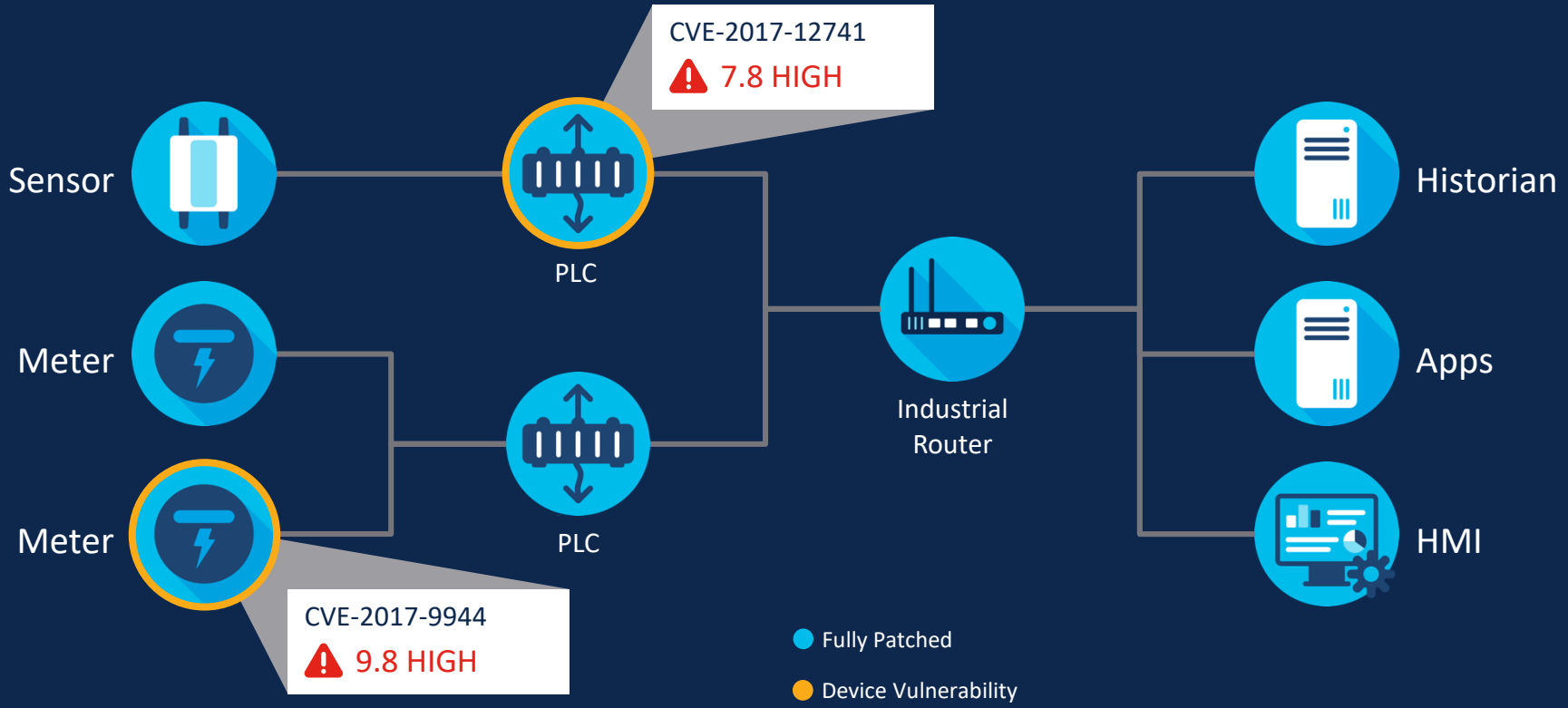
Blind to what their assets are communicating with

Myriad industrial protocols supported by a diverse set of suppliers

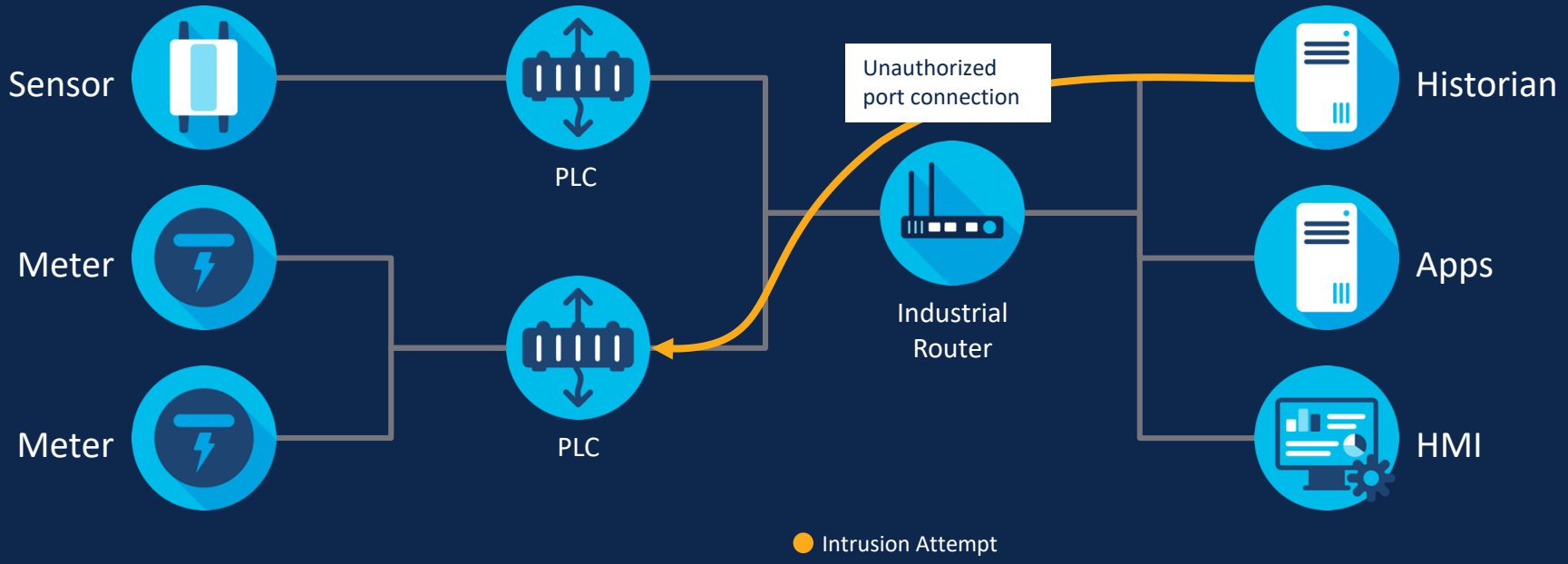
Why did your organization's cyber resilience improve?

Source: Ponemon - The Third Annual Study on the Cyber Resilient Organization

Visibility Step 2: Map Vulnerabilities



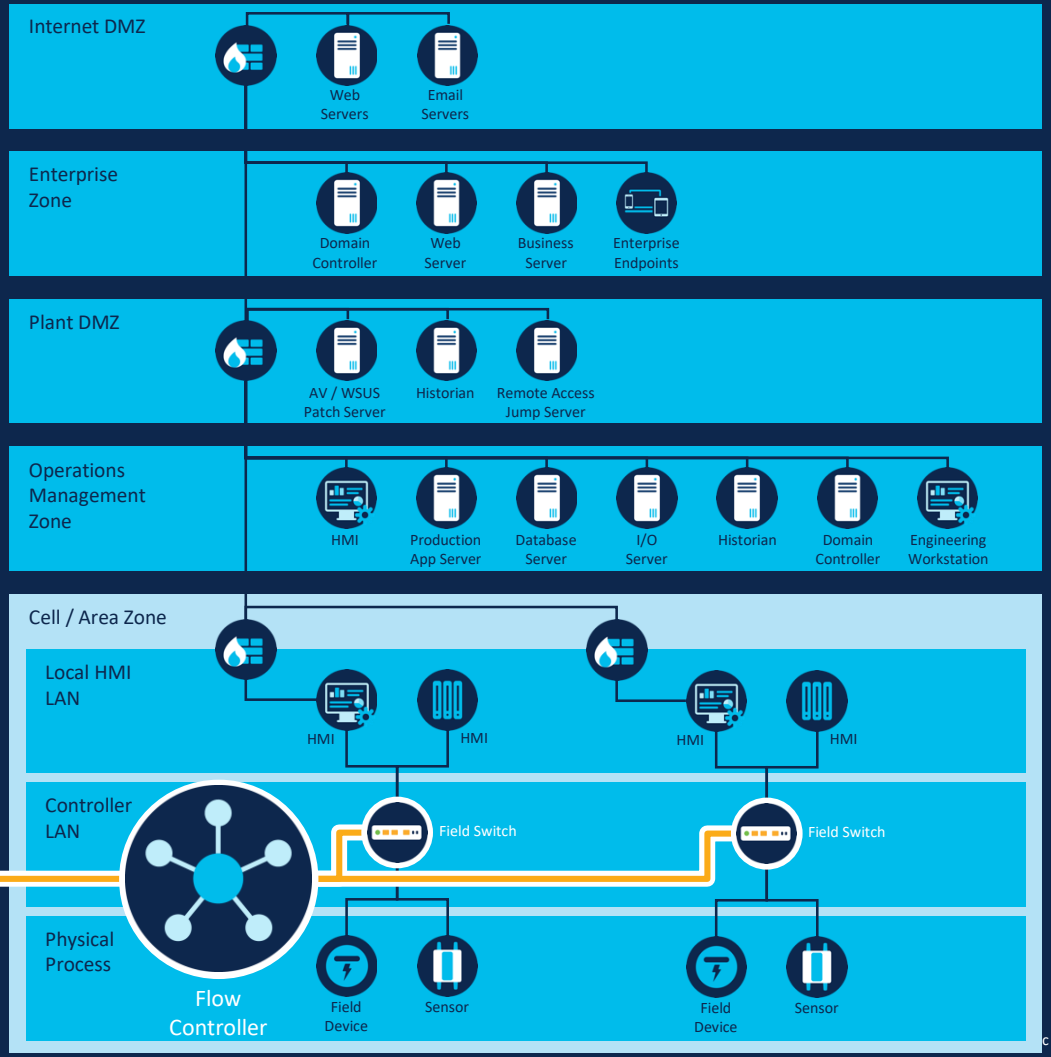
Visibility Step 3 : Detect Intrusions



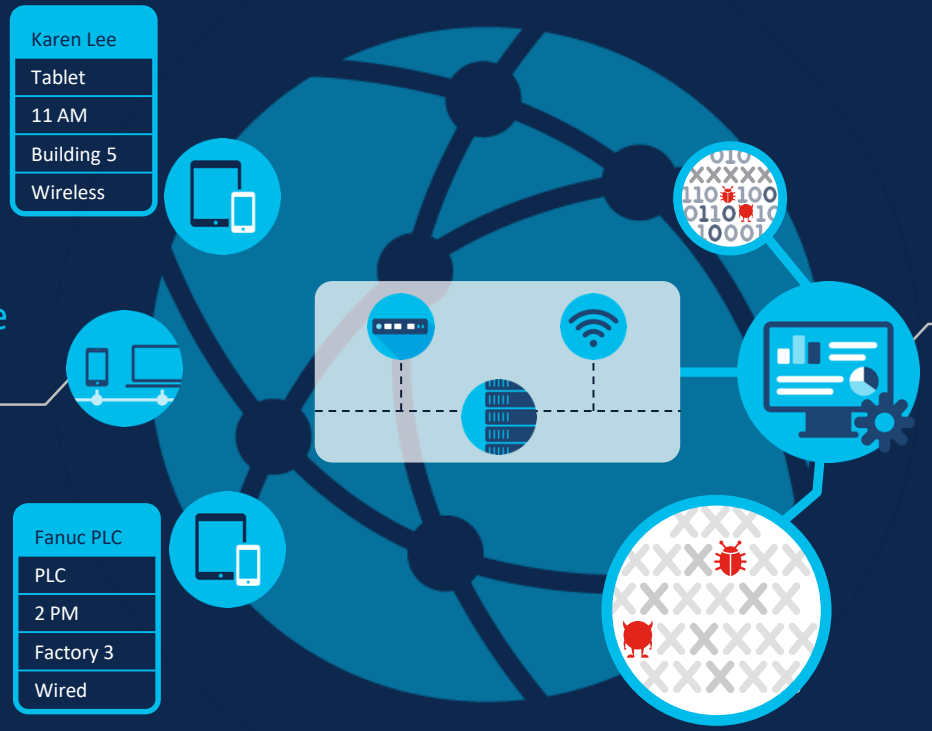
NetFlow Visibility

Flow-based Threat Detection
- Lateral Movement
- Breaches
- Malware Infection
- Data Exfiltration
- Command & Control

Advanced : Encrypted traffic



Leveraging Context Gained from the Network



See user and device details for actionable intelligence

Share context across security and networking products

Device info

Save investigative resources time and get better visibility

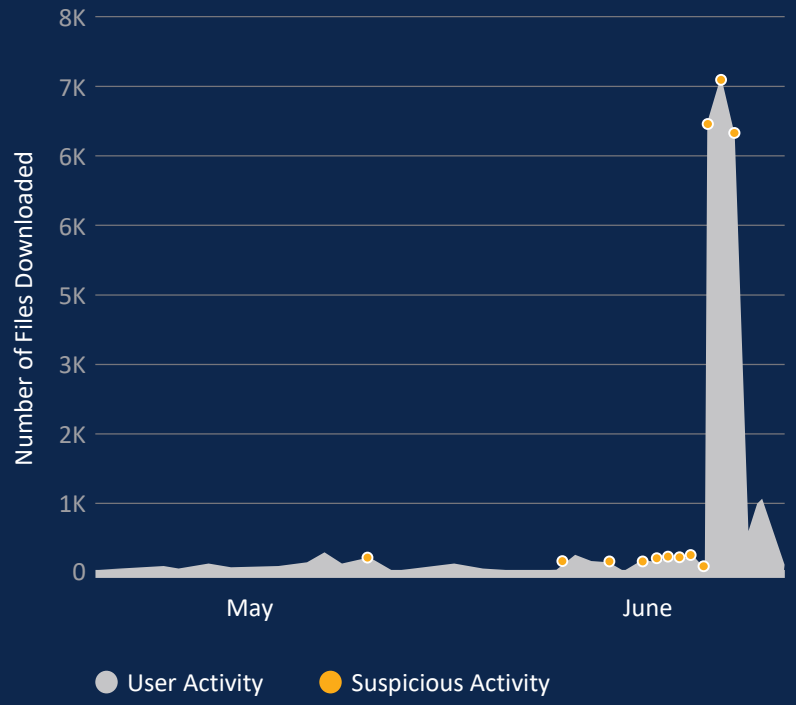
Rich information at their fingertips for faster action

Normalizing Device Behavior with Network Telemetry

User behavior is more complex than the behavior of ‘things’

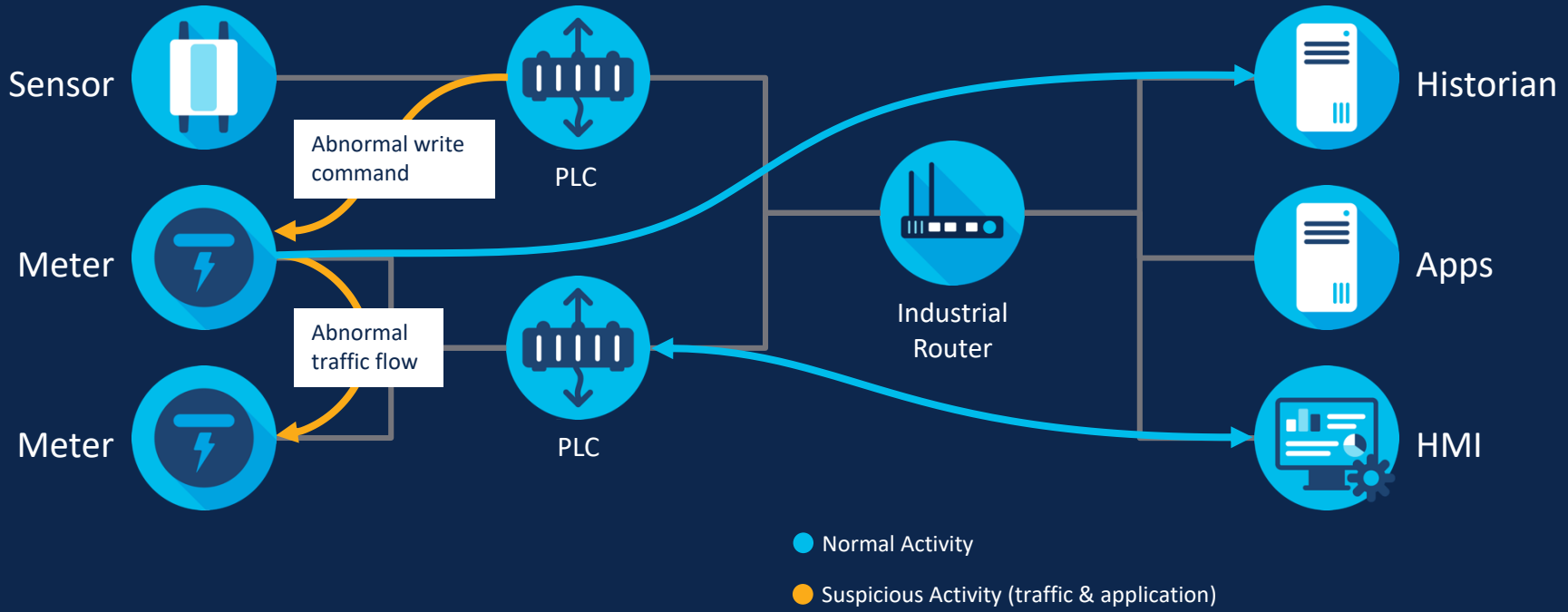
Machine learning is invaluable for detecting anomalies at scale

Machine-learning algorithms capture user download behavior



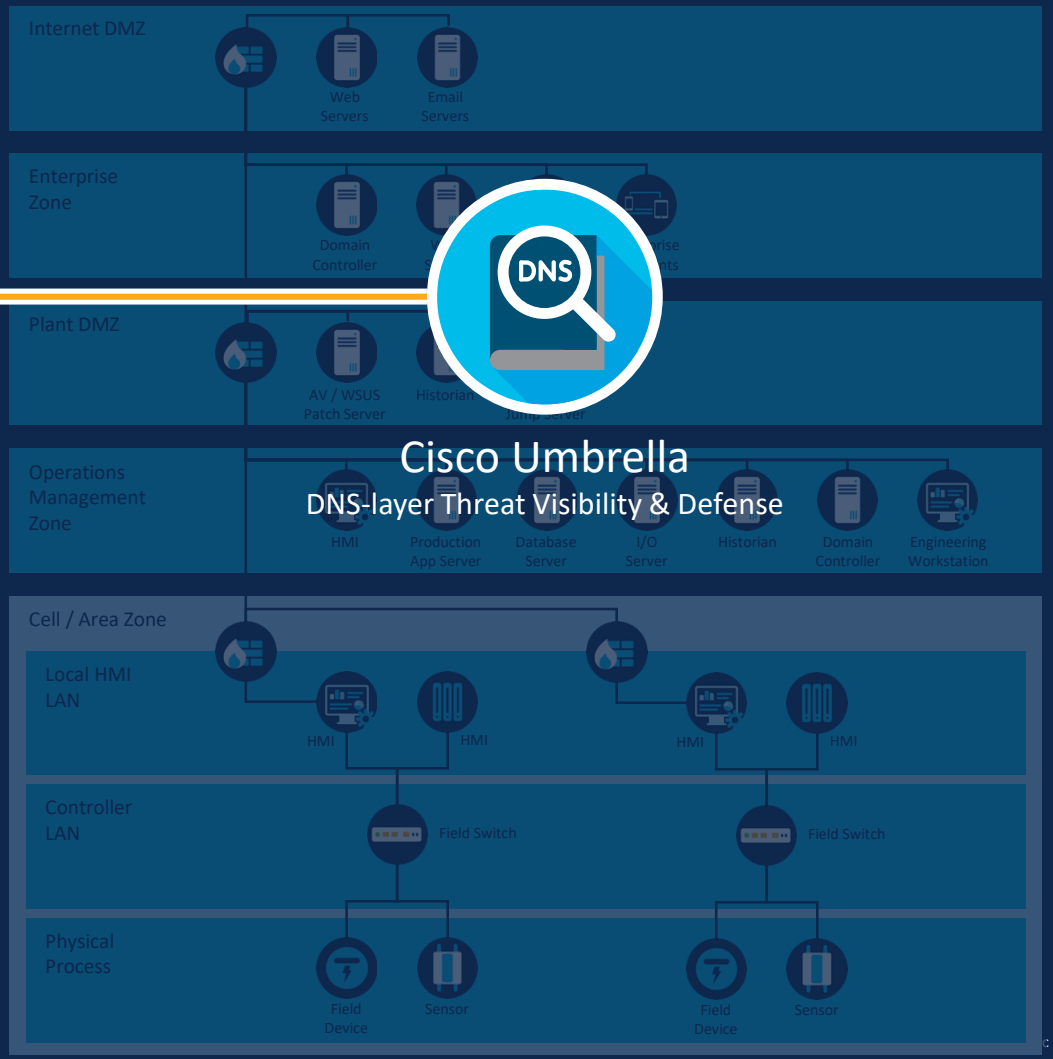
Source: Cisco Annual Cybersecurity Report 2018

Understanding Device Behavior



DNS Visibility

DNS-based Threat Detection
- Command & Control
- Malicious Sites
- Cryptomining



DNS-Layer Security: A Potential Quick Victory

Active attack blocking, forensics, and secure DNS communications

91.3%

of malware uses DNS

68%

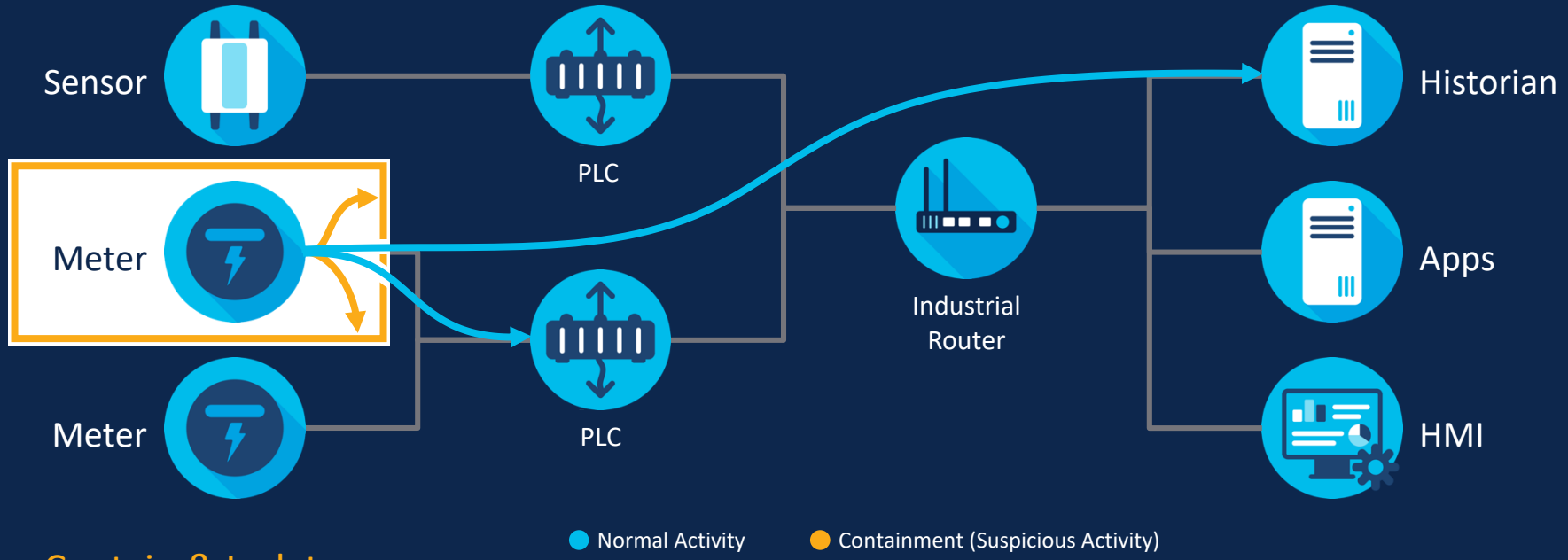
of organisations don't monitor it

Highly Orchestrated Environments

Was the change intended?

Key Security Problem #3

How do we respond and recover, quickly



Contain & Isolate

Software Defined Segmentation for Containment

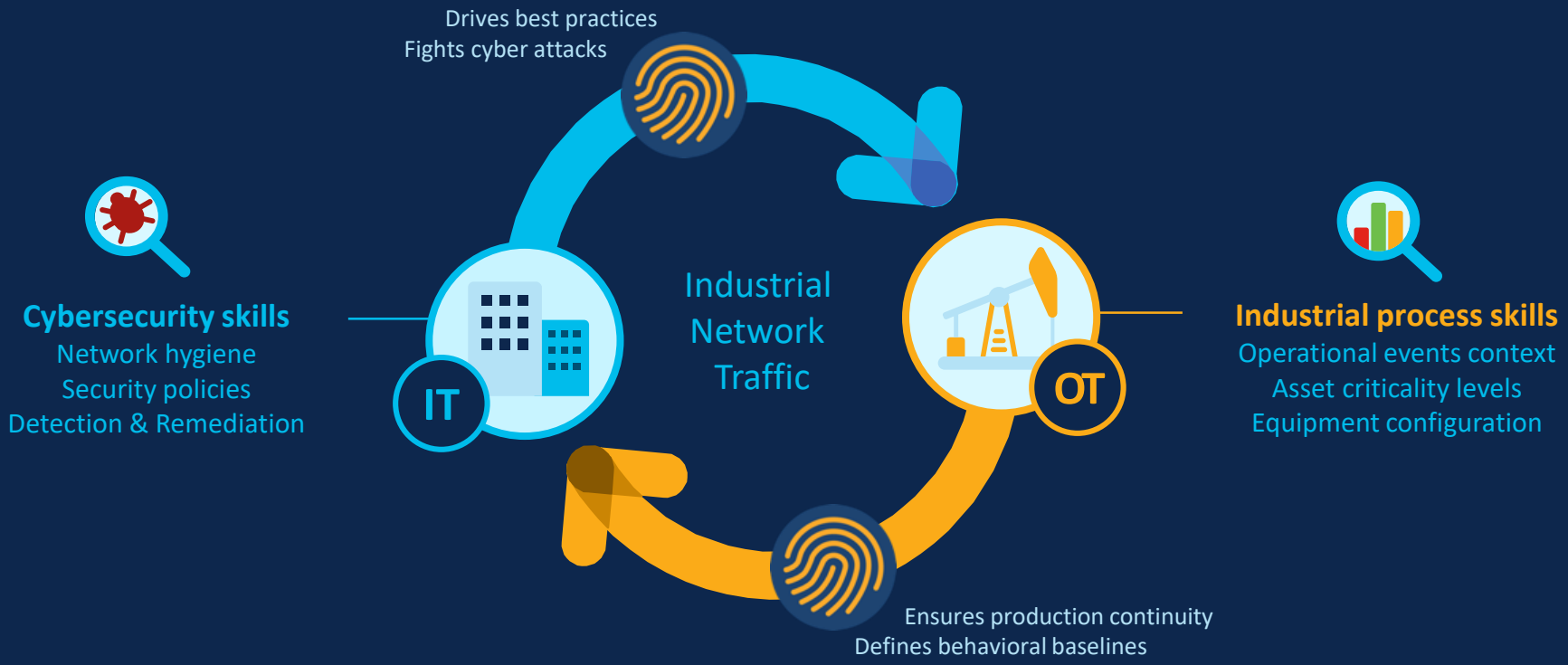
Rapid Containment

Leverage telemetry to pinpoint security threat

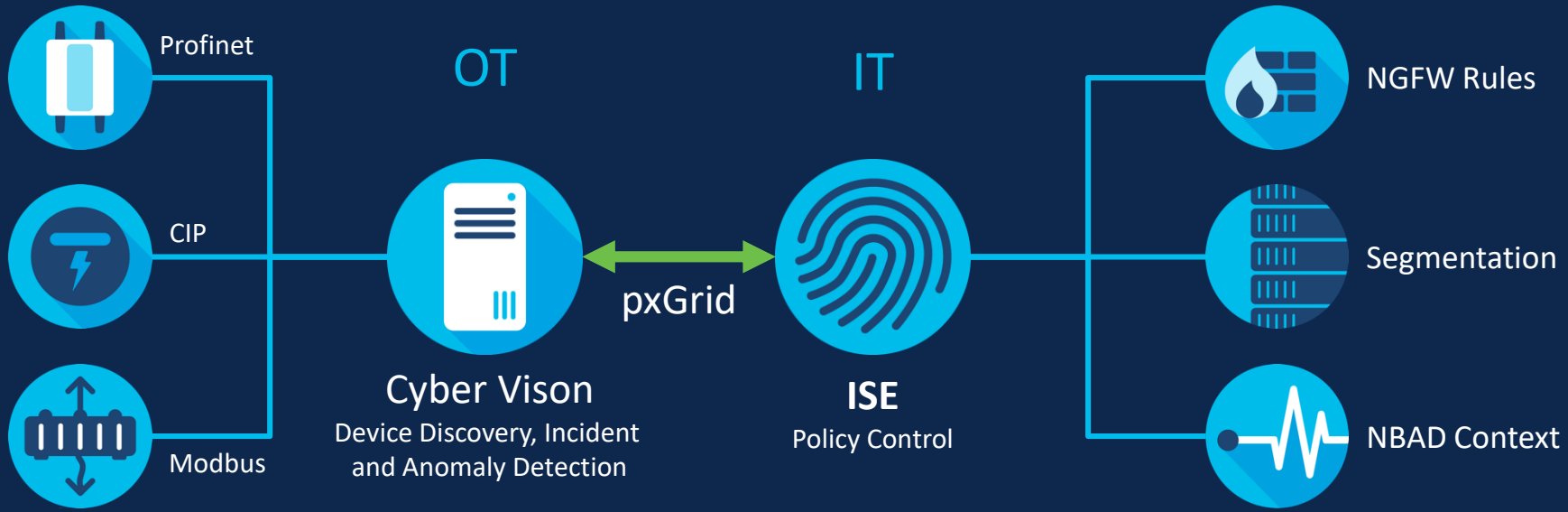
Leverage automated policy to dynamically quarantine threat

Employ integrated security solutions to safeguard environment

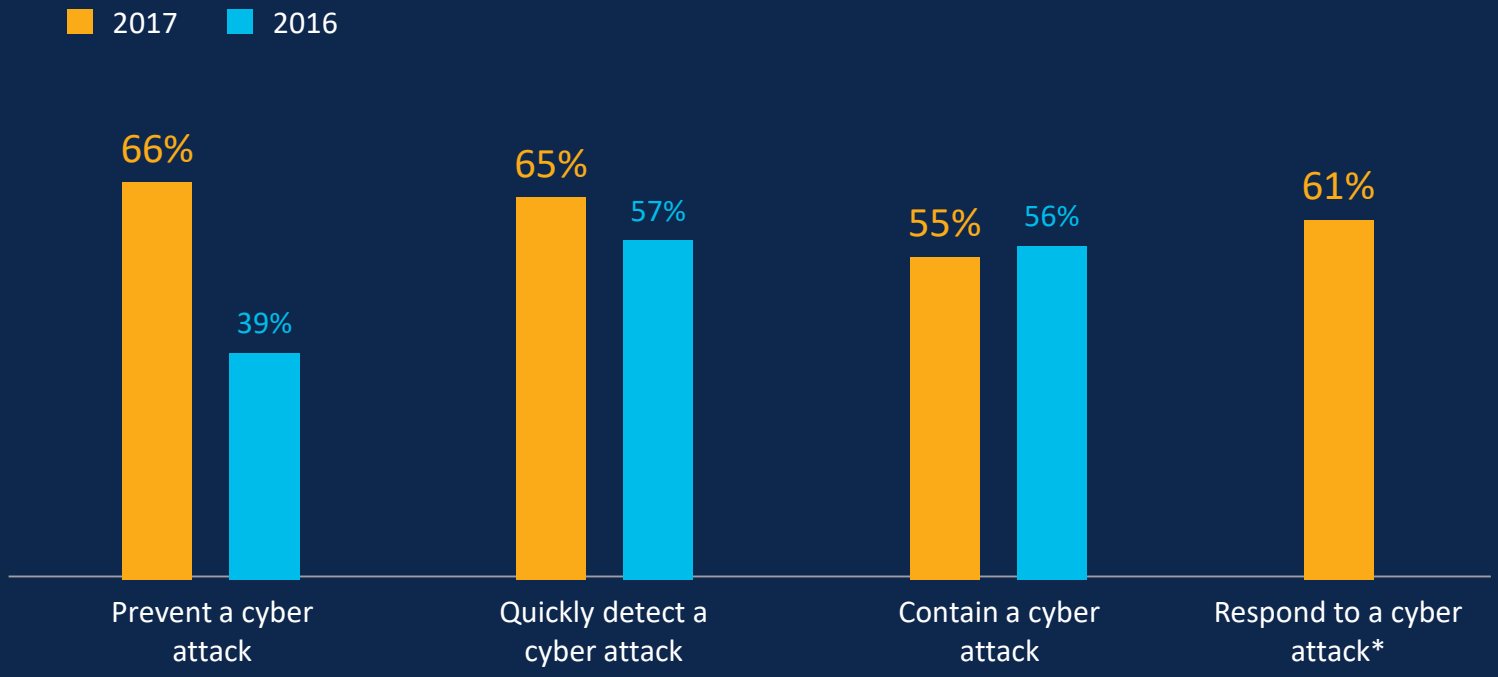
IT-OT Collaboration is Vital for Securing ICS



Enabling IT / OT Security Partnership



Ability to Prevent, Detect & Contain Cyber Attack



Source: Ponemon - The Third Annual Study on the Cyber Resilient Organization

* Response not available in 2016

Collaboration to Speed Response

Recovering Embedded Systems

Trust

Goal: Return to normal operations as soon as possible

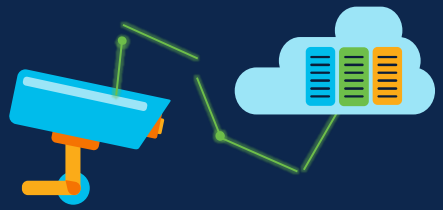
Mechanisms: Firmware updates, rebuild, spares

- Leverage hardware trust anchor
- Leverage secure boot
- Download from a trusted source
- Cryptographic validation of download

The Network is the Foundation for IoT Security

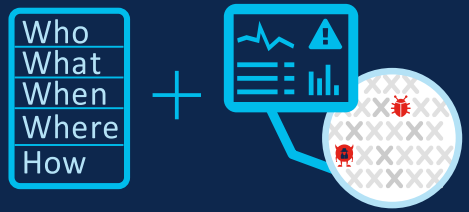
Segmentation

Zero Trust



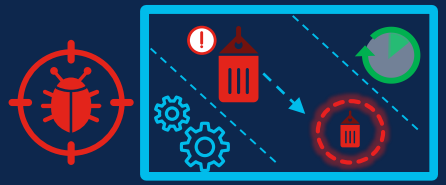
Visibility + Analytics

See Everything



Response + Recovery

Stop the Breach



Conclusion

Conclusion

You make security **possible**

The Network is the Foundation for IoT Security

Visibility + Threat Detection

See Everything

Segmentation

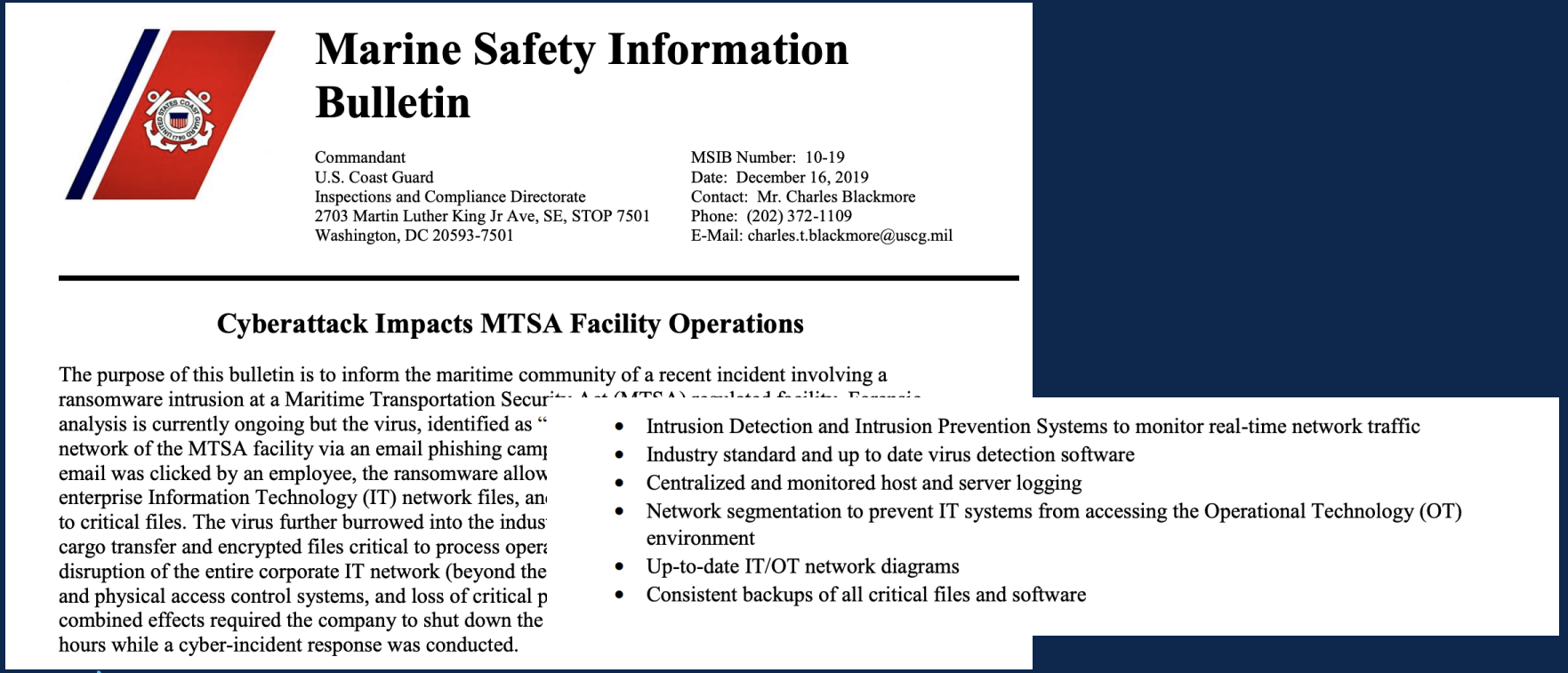
Reduce Attack Surface

Response + Recovery

Stop the Breach

Trusted Infrastructure

In Line with Incident Findings



Marine Safety Information Bulletin

Commandant
U.S. Coast Guard
Inspections and Compliance Directorate
2703 Martin Luther King Jr Ave, SE, STOP 7501
Washington, DC 20593-7501

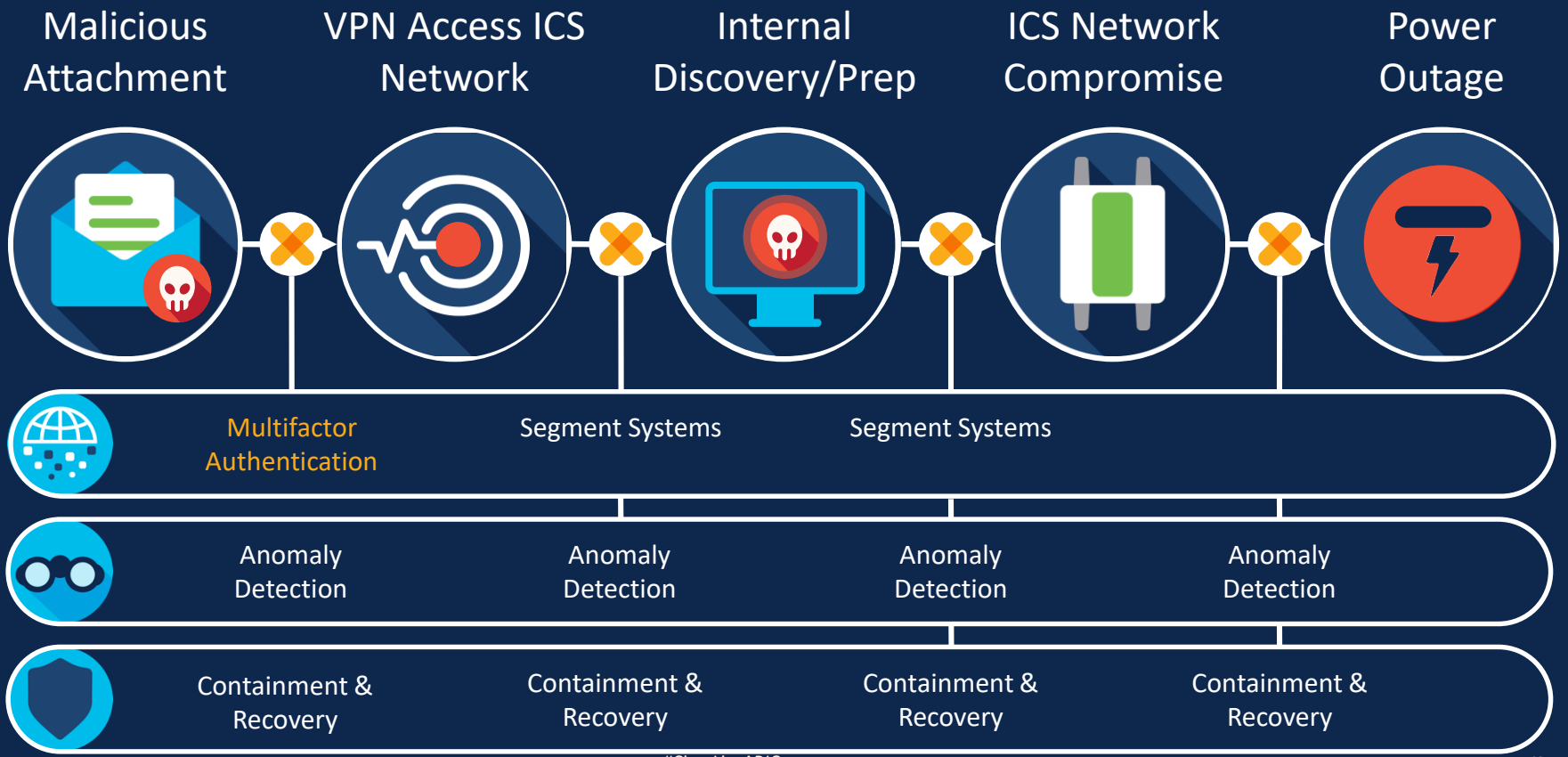
MSIB Number: 10-19
Date: December 16, 2019
Contact: Mr. Charles Blackmore
Phone: (202) 372-1109
E-Mail: charles.t.blackmore@uscg.mil

Cyberattack Impacts MTSA Facility Operations

The purpose of this bulletin is to inform the maritime community of a recent incident involving a ransomware intrusion at a Maritime Transportation Secur[illegible] Act (MTSA) regulated facility. Forensic analysis is currently ongoing but the virus, identified as "[illegible] network of the MTSA facility via an email phishing camp[illegible] email was clicked by an employee, the ransomware allow[illegible] enterprise Information Technology (IT) network files, an[illegible] to critical files. The virus further burrowed into the indus[illegible] cargo transfer and encrypted files critical to process opera[illegible] disruption of the entire corporate IT network (beyond the [illegible] and physical access control systems, and loss of critical p[illegible] combined effects required the company to shut down the [illegible] hours while a cyber-incident response was conducted.

- Intrusion Detection and Intrusion Prevention Systems to monitor real-time network traffic
- Industry standard and up to date virus detection software
- Centralized and monitored host and server logging
- Network segmentation to prevent IT systems from accessing the Operational Technology (OT) environment
- Up-to-date IT/OT network diagrams
- Consistent backups of all critical files and software

Ukraine Power Grid Attack (Revisited)



Thank you

You make **possible**