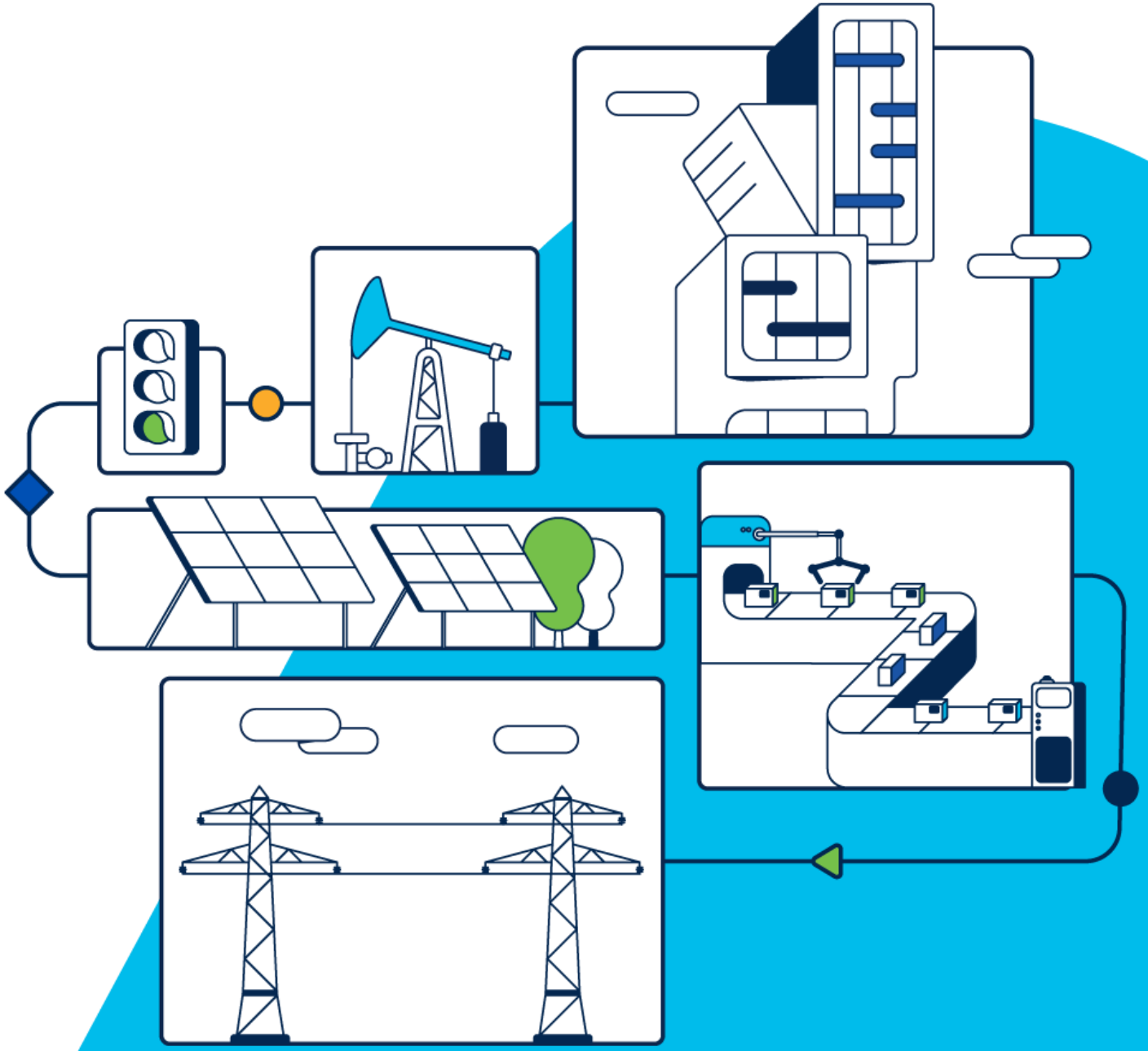
Cyber Risks Facing Modern Manufacturing



David Gutshall
Manufacturing Sales

It’s no secret that most industrial networks have poor network hygiene and inadequate security controls

Security guidelines can make cybersecurity complex

IEC 62443

- 14 documents
- Product Compliance
- System Compliance
- Zones & Conduits or Zero Trust?

NIST SP 800-82

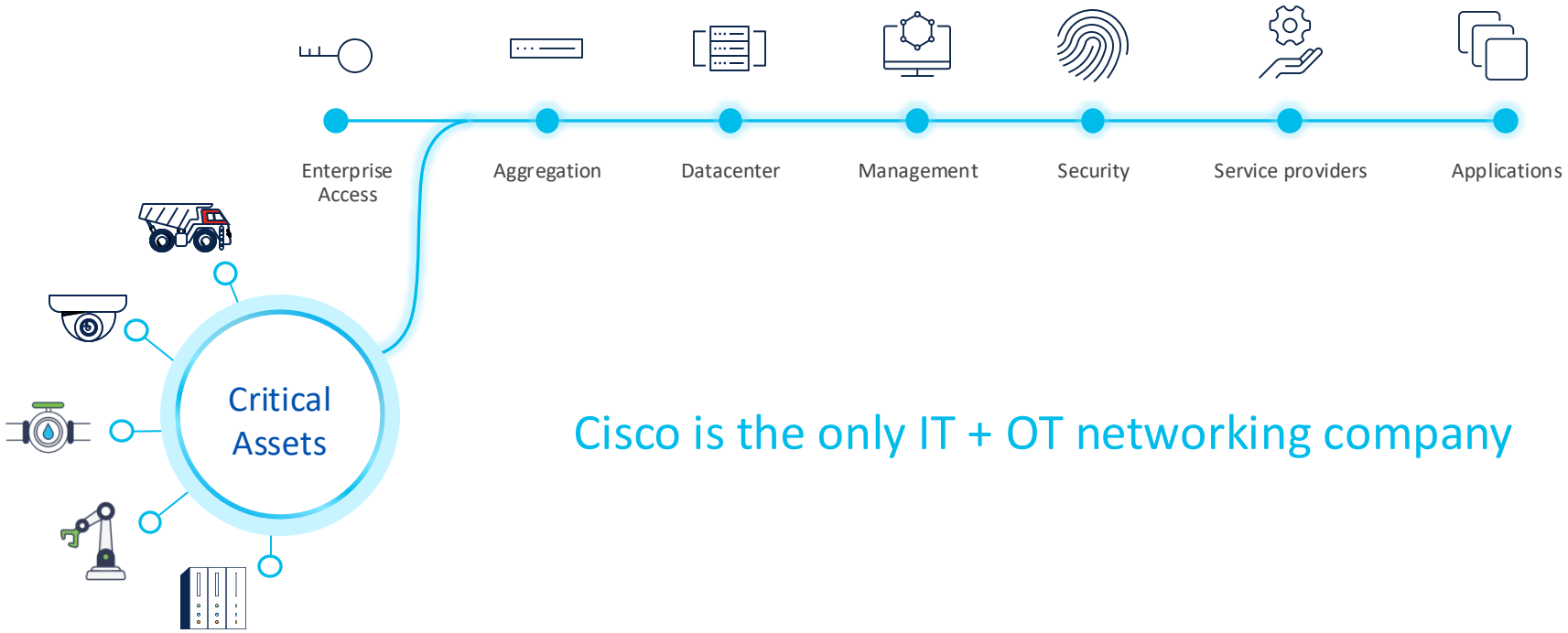
- 300+ Pages
- 1 of 200+ special publications

NIS2

- 46 Articles
- 144 Recitals
- 3 Annexes
- 40000+ words

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

One Cisco Network: Only Cisco provides solutions to connect & protect everything



Cisco is the only IT + OT networking company

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Innovation

Worldwide Leader
Networking, Security & Collaboration

23,000 Patents

$7.0B in R&D

Incidents are only increasing

Clorox says sales and profit took a big hit from cyberattack

Johnson Controls Ransomware Attack: Data Theft Confirmed, C

World's Critical Infrastructure Suffered 13 Cyber Attacks Every Second in 2023

Jan 29, 2024

Cyberattacks on CNI surge by 30% in 2024, study reveals

The report by KnowBe4 details the significant rise in attacks on essential sectors - with the US power grid providing especially vulnerable.

Suzuki Motorcycle India breach forces plant shutdown

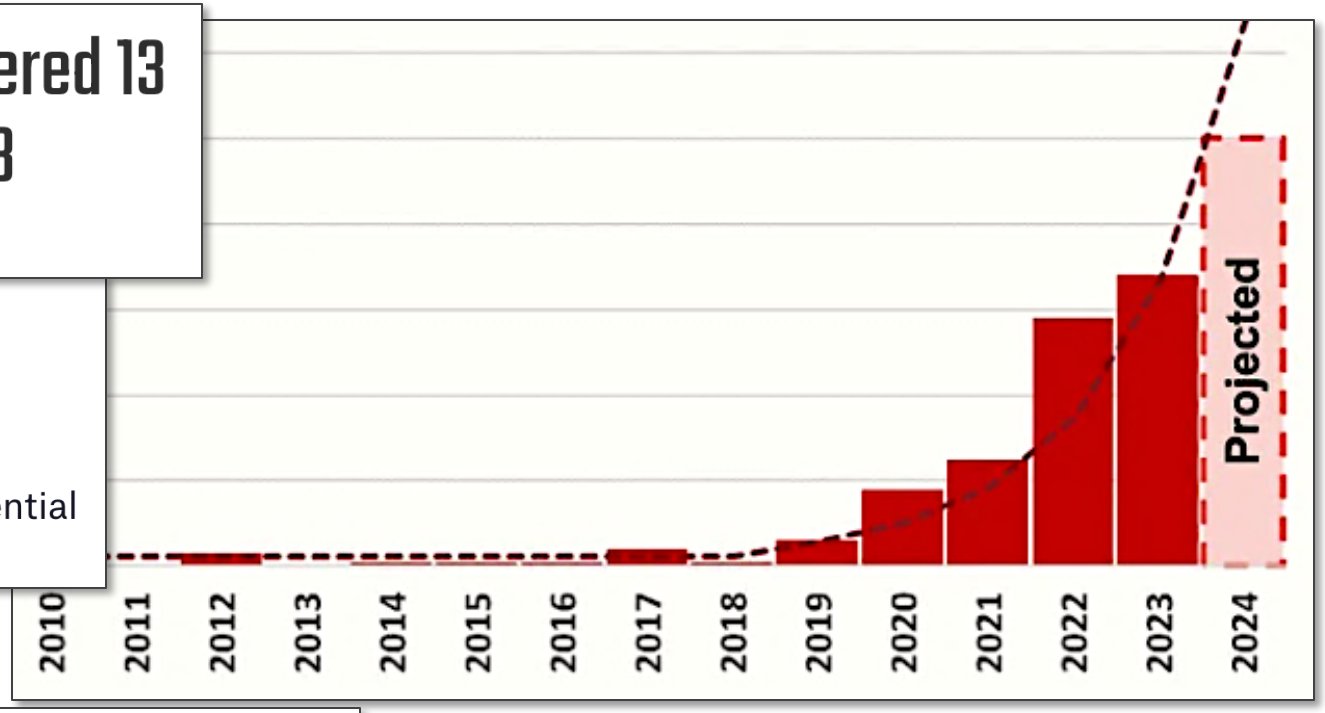
Simpson Manufacturing Takes Systems Offline Following Cyberattack

Simpson Manufacturing is experiencing disruptions after taking IT systems offline following a cyberattack.

Over 50% of incidents occurred in process and discrete manufacturing in 2023

Waterfall 2024 Threat Report

OT Reported Incidents since 2010



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Global IIoT Sales

Cisco Confidential

Cisco Talos Statistics

550B security events/**day**

~9M emails blocked/**hour**

~2,000 new samples/**minute**

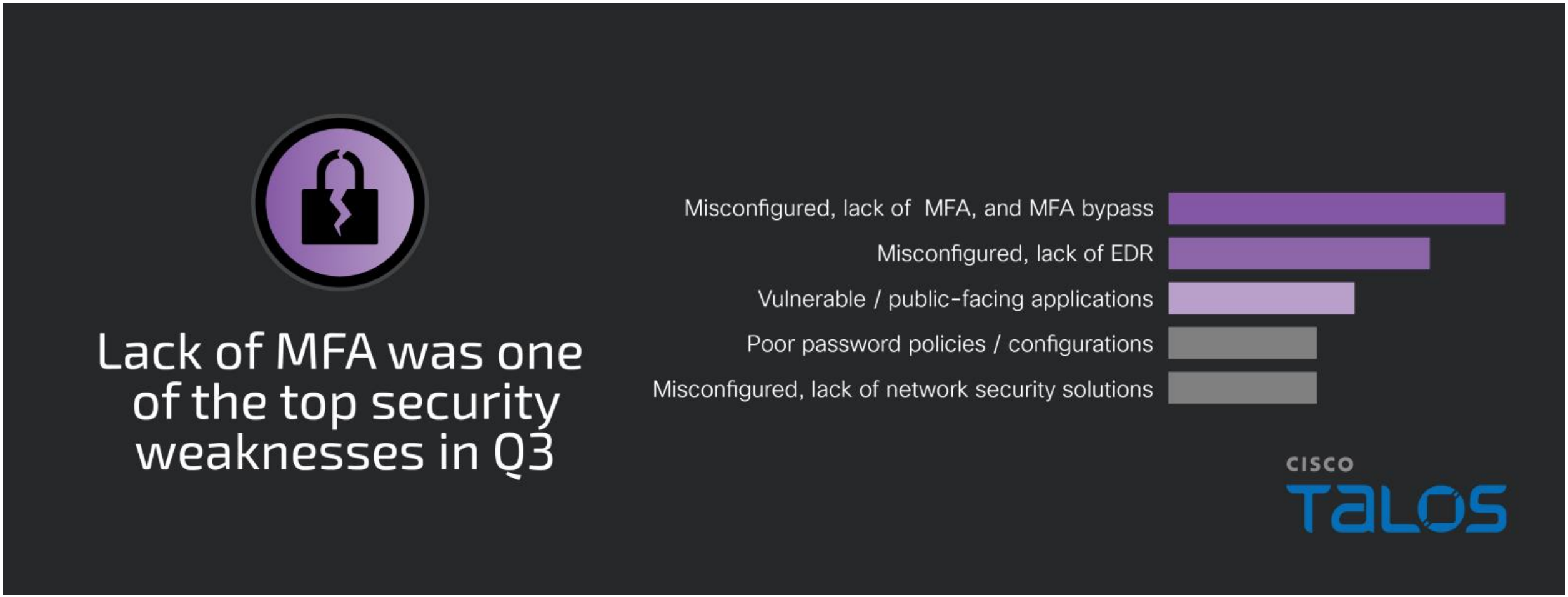
~2,000 domains blocked/**second**

Cisco Confidential

Valid Accounts – Still the usual way in

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Top Security Weaknesses



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What are 90-95% of all Cyber Security Incidents Caused By?

Human Error

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Confidential

ChatGPT + Human Phish

Subject: Quick Favor – Mind Taking a Look?

Hey [Recipient's Name],

Hope you're doin' well! I used to work with your old boss over at McAfee, and they had nothin' but good things to say about you. Figured I'd reach out and see if you might could help me out.

I was sorry to see the Commanders' season end with that tough loss to the Eagles in the NFC Championship. COMMANDERS.COM Are you still livin' in D.C.?

I'm fixin' to make a move and got my resume put together, but I'd sure be grateful if you could give it a once-over. If you've got a little time to take a look and share any thoughts, I'd really appreciate it. No rush—just whenever you can swing it!

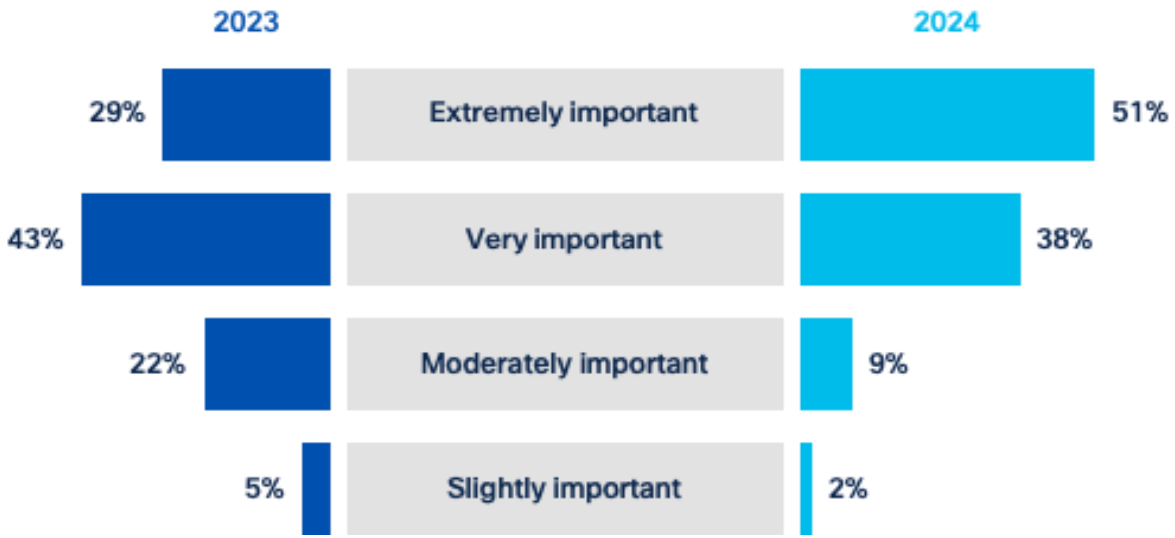
Let me know what you think, and I sure would be thankful!

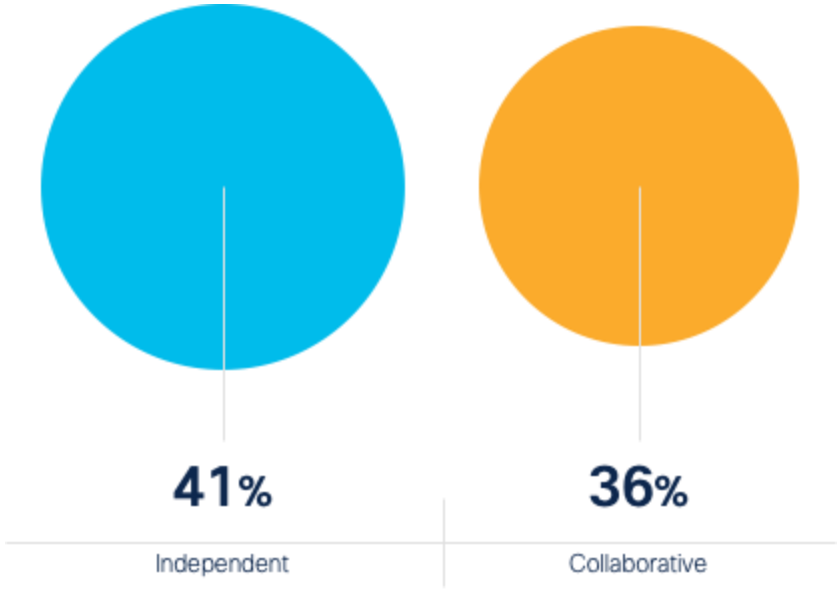
Take care, [Your Name]

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Voice of the customer

How would you describe the importance of **cybersecurity compliance** in your operational network?





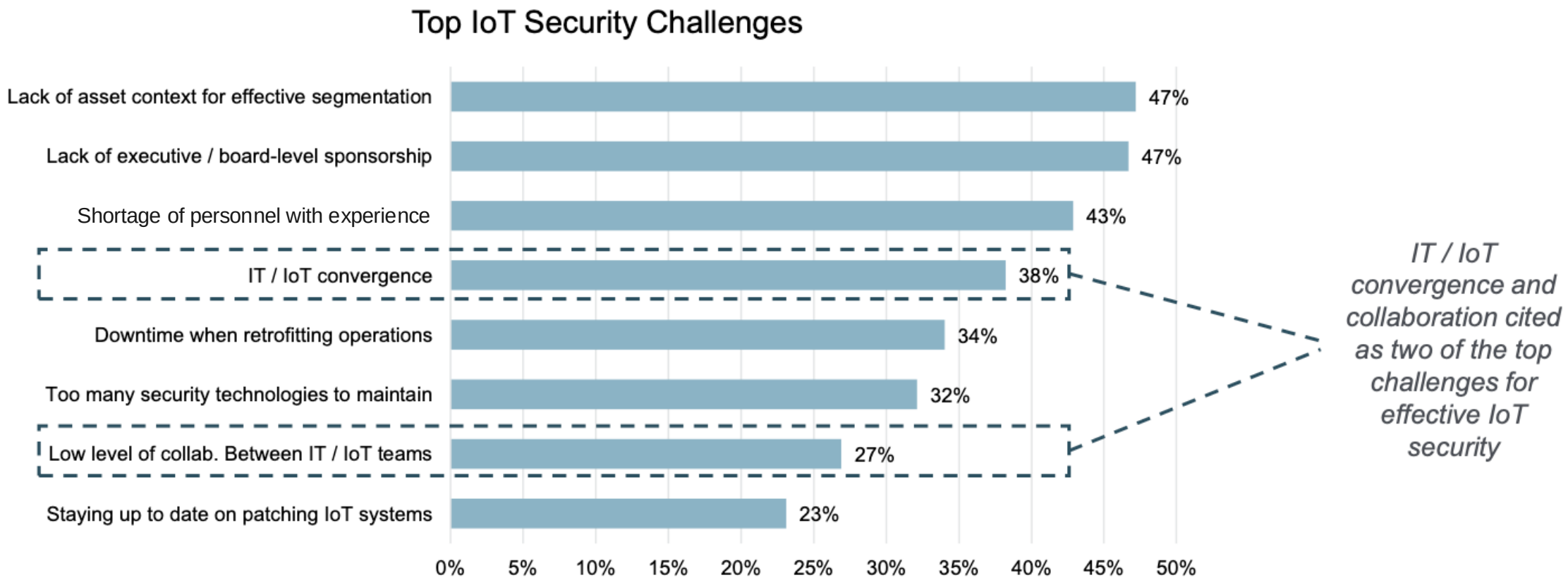
89%

of organizations feel cybersecurity compliance is very or extremely important in OT

41%

of firms' IT and OT teams are working **independently** on cybersecurity

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



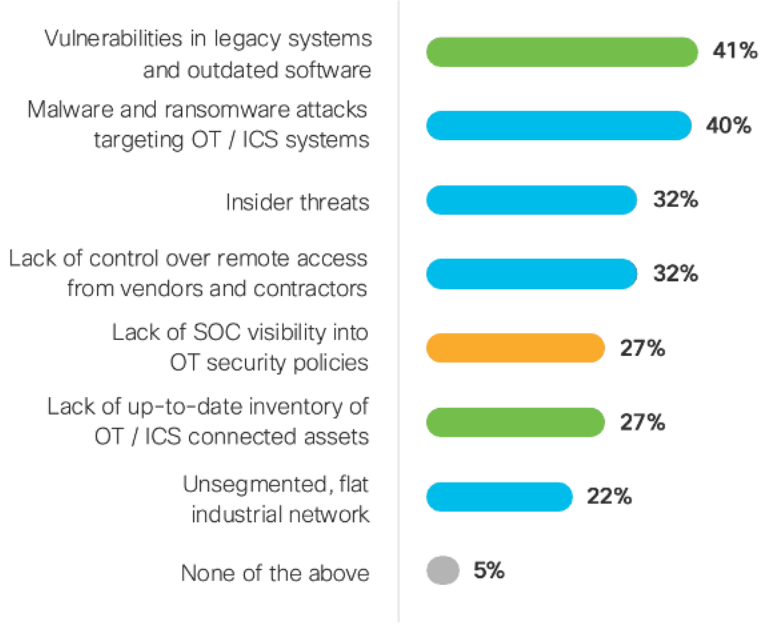
PIPER | SANDLER

Cisco Survey Results

Cybersecurity challenges

2024 State of Industrial Networking Report

The main problems are **vulnerabilities in legacy systems and outdated software (41%) and malware or ransomware attacks specifically targeting operational technology (40%).**



Q. What specific cybersecurity challenges have you encountered in your industrial networks? Select all that apply

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Increased connectivity challenges

Weak Security Posture

Lack of visibility to thousands of OT assets and cyber security vulnerabilities

Lack of Control

Legacy networks that are not equipped to prevent the spread of malware

Too many screens

Too many screens to monitor without cross-domain integration

Cisco Confidential

Specific Asks / Feedback

Scalable Visibility

"High cost of SPAN networks, as there are an order of more assets in OT than in IT"

Adaptive Segmentation

"Avoiding downtime when enforcing segmentation policy for IEC-62443 zones & conduits"

Cross-Domain SOC

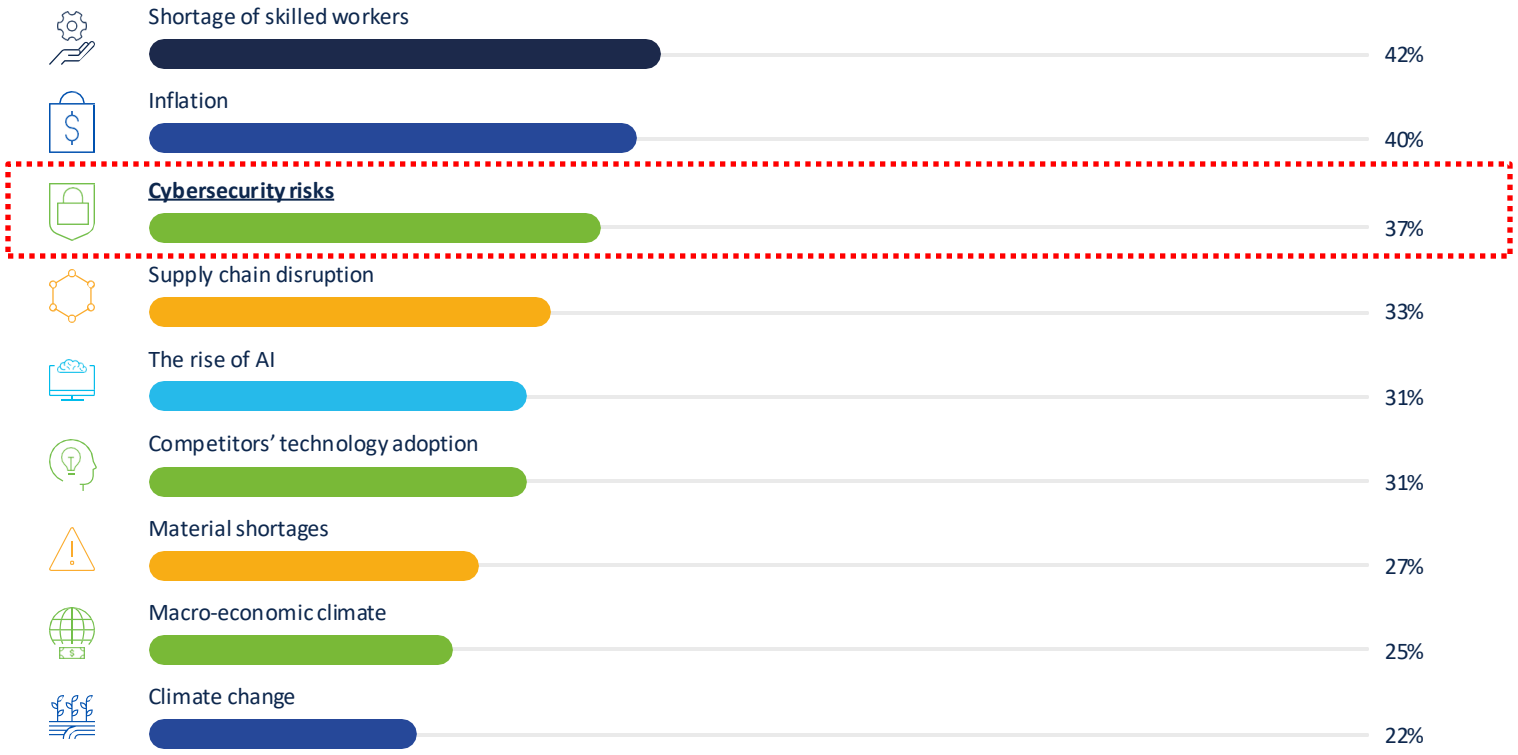
"Difficulty in tracking lateral movement of threats propagating between IT and OT"

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

External Industry Obstacles

Over the past few years, businesses worldwide have faced macro-level challenges ranging from supply chain issues to a global pandemic. But what are the top issues hampering growth in industrial sectors today?

The number one concern—cited by 42% of respondents—is a shortage of skilled workers, closely followed by inflation (40%) and cybersecurity risks (37%). These are global issues: our analysis uncovered minimal regional variations.



> Even with some recent cooling, the labor market remains tight, and the resulting applicant gap may continue. This could impact the ability of manufacturers to fully capitalize on [the] recent growth in public and private investment.
>
> The net need for new employees in manufacturing could be around 3.8 million between 2024 and 2033. And, around half of these open jobs (1.9 million) could remain unfilled if manufacturers are not able to address the skills gap and the applicant gap.[7]

'Taking charge: Manufacturers support growth with active workforce strategies,' Deloitte[1]

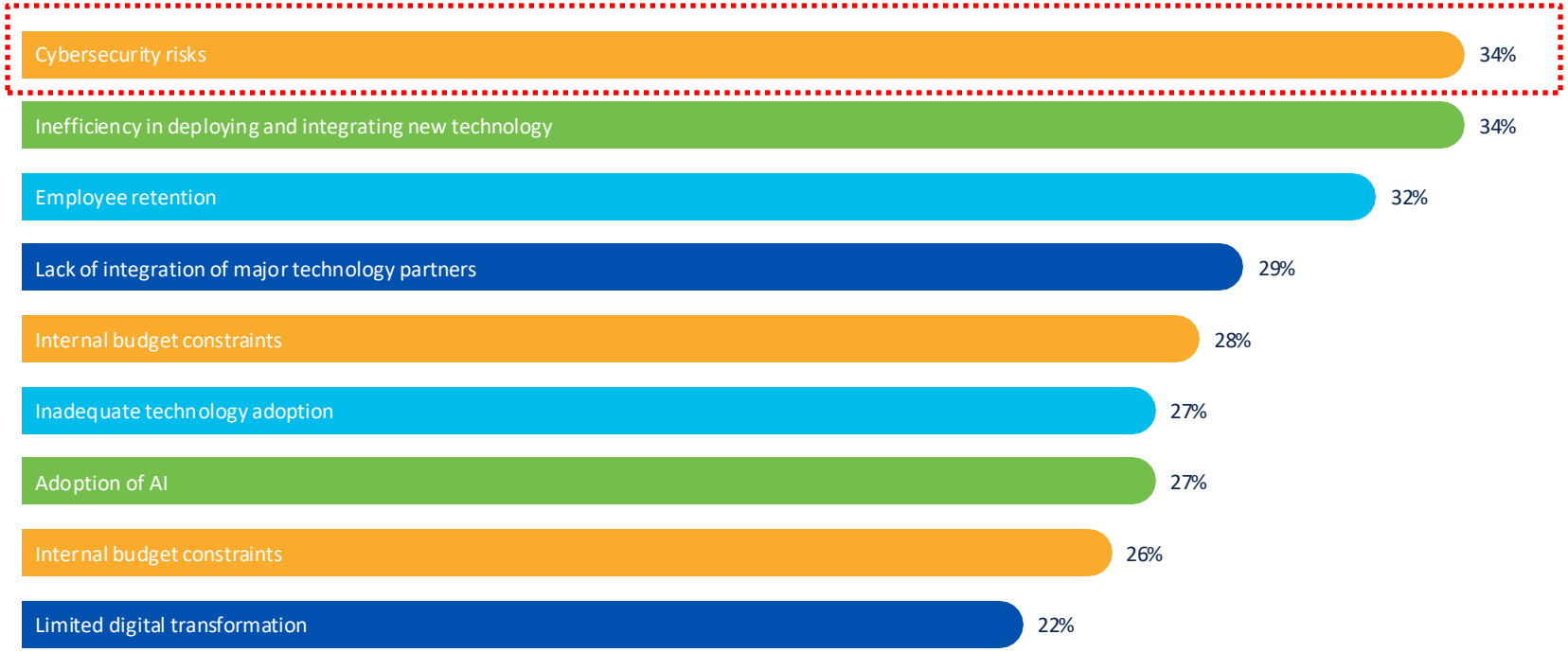
1 https://www2.deloitte.com/us/en/insights/industry/manufacturing/supporting-us-manufacturing- growth-amid-workforce-challenges.html

Internal Industry Obstacles

Compounding the external factors are issues within organizations which hamper progress. Again, we see businesses struggling with cybersecurity risks (#1) and workforce challenges—namely employee retention (#3); alongside a lack of efficiency when deploying new technology (#2).

These barriers are primarily operational, rather than technical: representing human factors such as resistance to change which can lead to difficulties upskilling and retaining a fit-for-purpose workforce.

Market maturity and distribution of skills impact regional results. Retaining employees is proving particularly hard for North American firms, who rated it their top internal obstacle; while inefficiency in deploying technology is the biggest problem for organizations in APAC.

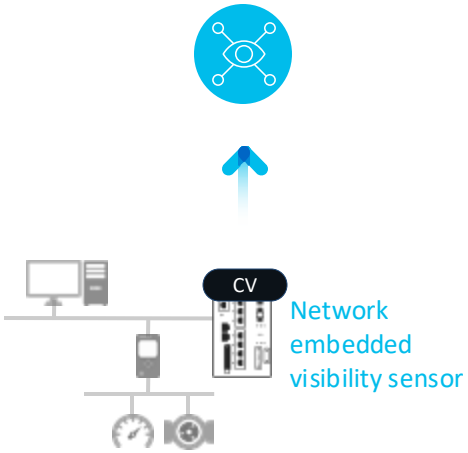


Cisco Industrial Threat Defense

Visibility

OT Asset Visibility
and Security Posture

Cisco
Cyber Vision

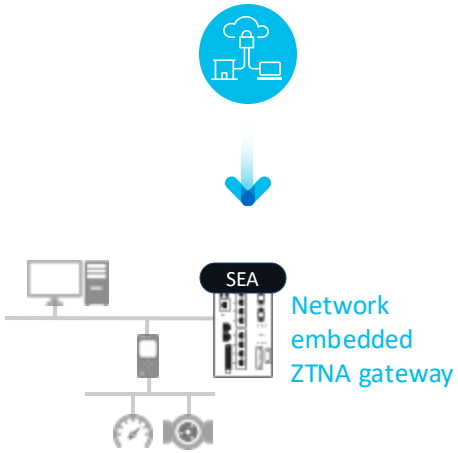


Protection

Zero Trust Security for OT

Secure remote access (ZTNA)

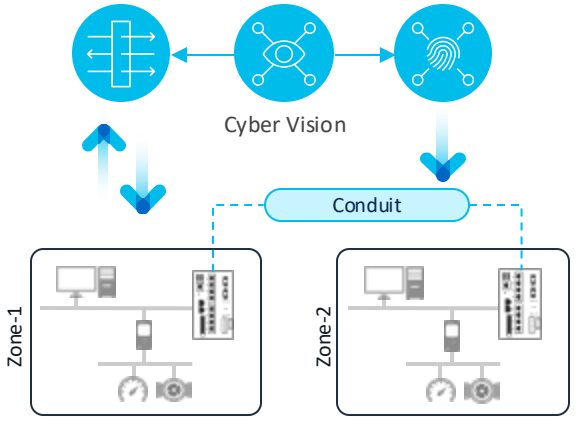
Cisco
Secure Equipment Access



IEC 62443 zone segmentation

Cisco
Secure Firewall

Cisco
ISE

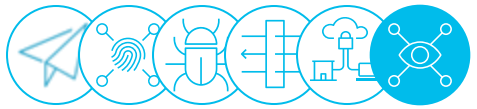


Network enforced segmentation

Response

Cross-Domain Detection,
Investigation & Response

splunk>
a CISCO company



Visibility across the entire attack chain

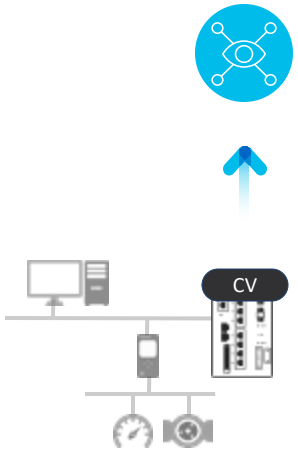
Network as a fabric to secure OT at scale

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 1: Visibility to factory assets

Asset Visibility & Security Posture

Cisco Cyber Vision

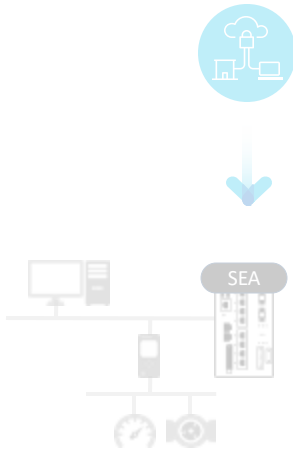


Network embedded CV Sensor

Zero Trust for OT

Zero Trust Network Access

Cisco Secure Equipment Access

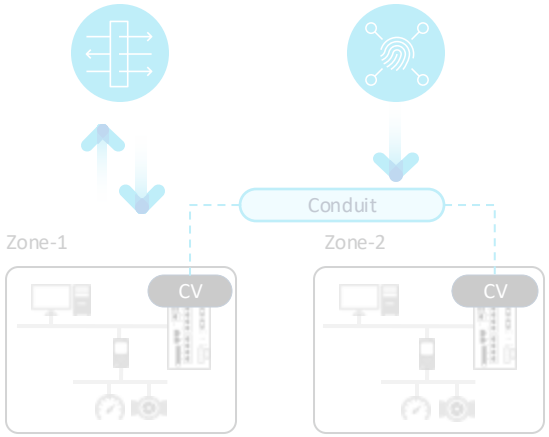


Network embedded ZTNA Gateway

IEC 62443 Zones & Conduits

Cisco Secure Firewall

Cisco ISE



Network enforced segmentation

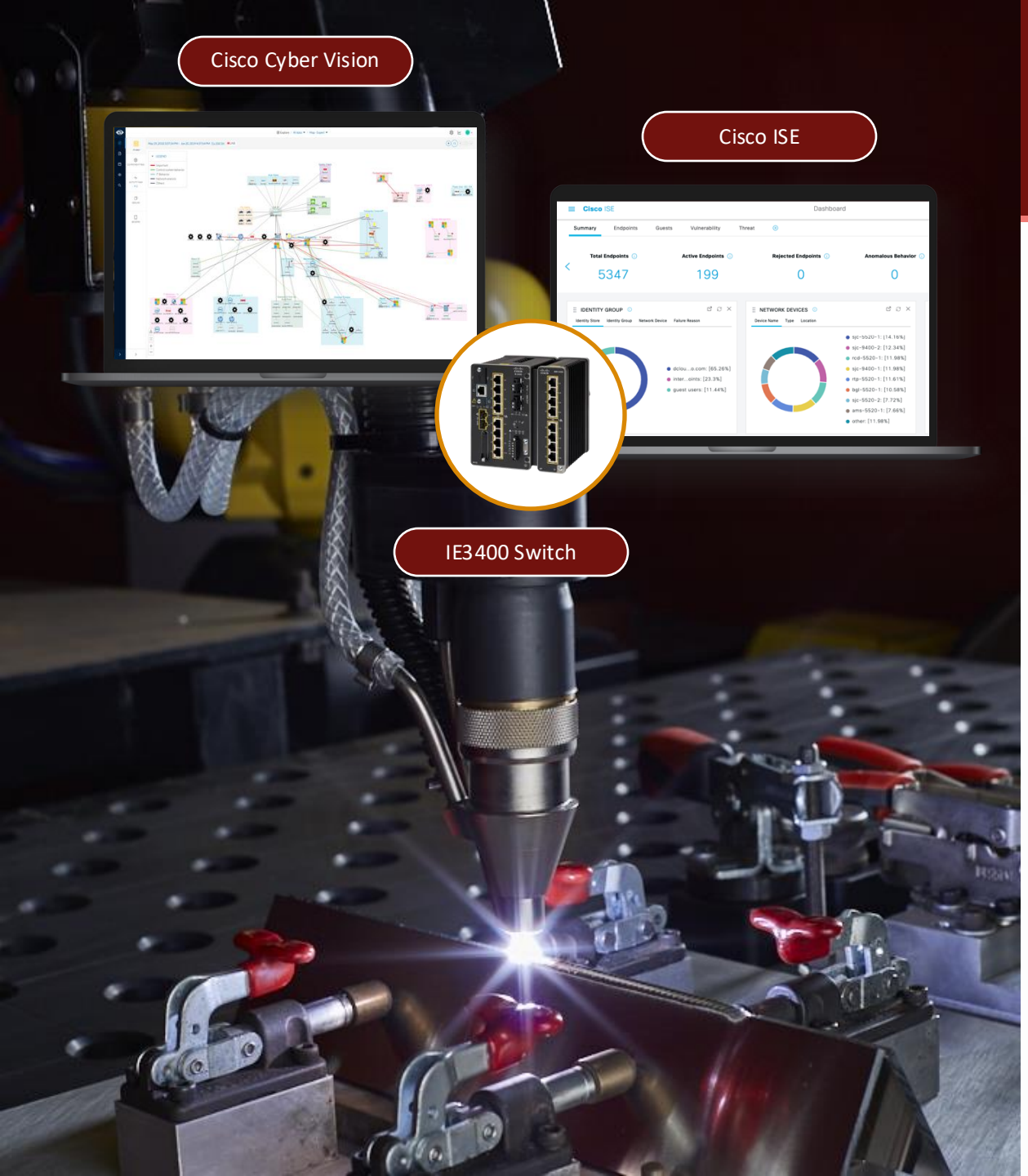
Cross-Domain Detection, Investigation & Response

splunk> a CISCO company

Visibility across the entire attack chain

Network as a fabric to secure OT at scale

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



Visibility drives segmentation

Customer Profile

- World leader in arc welding, robotic welding systems, plasma and oxyfuel cutting equipment.
- 56 manufacturing locations in 19 countries

Business Challenge

- Cybersecurity concerns on ransomware halting productions due to unsegmented industrial networks below the industrial DMZ
- Board directed IT & OT to rollout a segmentation architecture globally across plants in North America, Europe and Asia

Cisco Solution

- Network designed based on C9300 distribution layer and **IE3400 switches** on the plant floor
- **Cyber Vision** deployed on C9300 & IE3400 switches for visibility to the security posture of OT assets
- Cyber Vision visibility used to drive zone level segmentation on IE3400 switches in the OT network using **Cisco ISE and TrustSec**

Step 2: Implement control points in the network

Asset Visibility & Security Posture

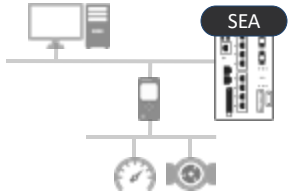
Cisco
Cyber Vision

Network embedded CV Sensor

Zero Trust for OT

Zero Trust Network Access

Cisco
Secure Equipment Access

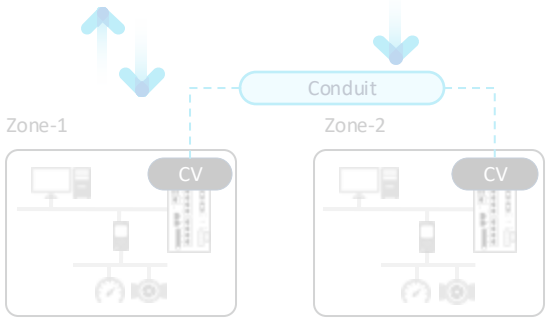


Network embedded ZTNA Gateway

IEC 62443 Zones & Conduits

Cisco
Secure Firewall

Cisco
ISE



Network enforced segmentation

Cross-Domain Detection, Investigation & Response

splunk>
a CISCO company

Visibility across the entire attack chain

Network as a fabric to secure OT at scale

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secure remote access to PLCs in manufacturing plants

Customer Profile

- One of the world's leading manufacturers of high value coatings on plastic for the automotive industry.
- 11 manufacturing facilities across North America, Europe, and Asia Pacific

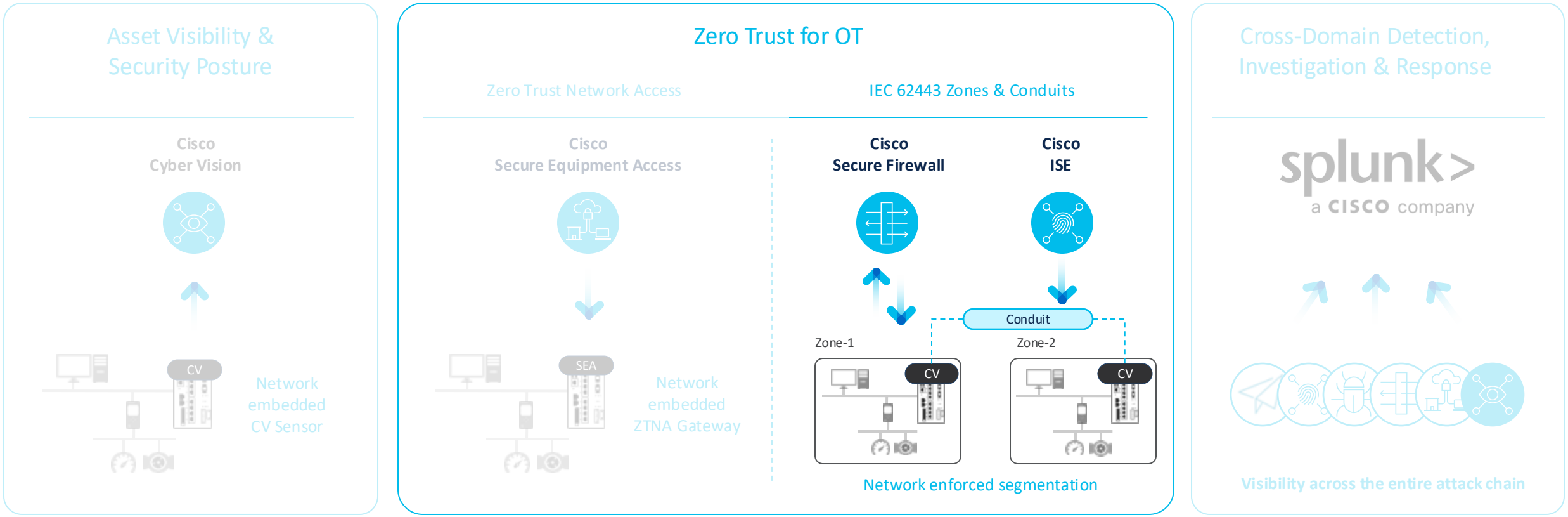
Business Challenge

- Secure access to PLCs distributed across plants without the burden of maintaining cumbersome VPN and jump-servers
- PLCs embedded in manufacturing cells have private IP addresses and not reachable from higher layers of the network

Cisco Solution

- Top of the line switches replaced by **Cisco IE3300** switches that provide connectivity to PLCs
- IE3300 switches with **embedded SEA agents** provides remote access to the PLC without need to NAT private IP address to Levl-3 of the network
- Zero Trust Network Access (ZTNA) resource isolation and access policy controlled through **cloud-based SEA trust broker**

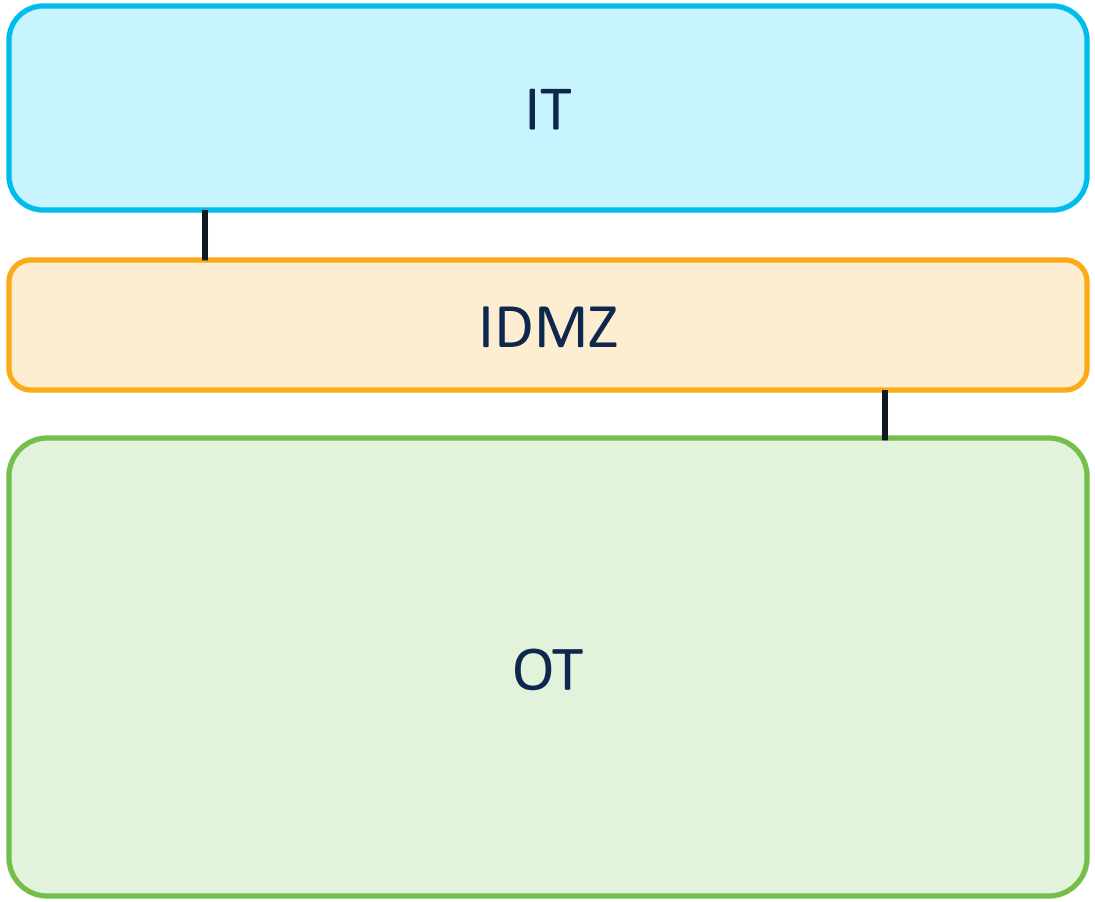
Step 2: Implement control points in the network



Network as a fabric to secure OT at scale

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

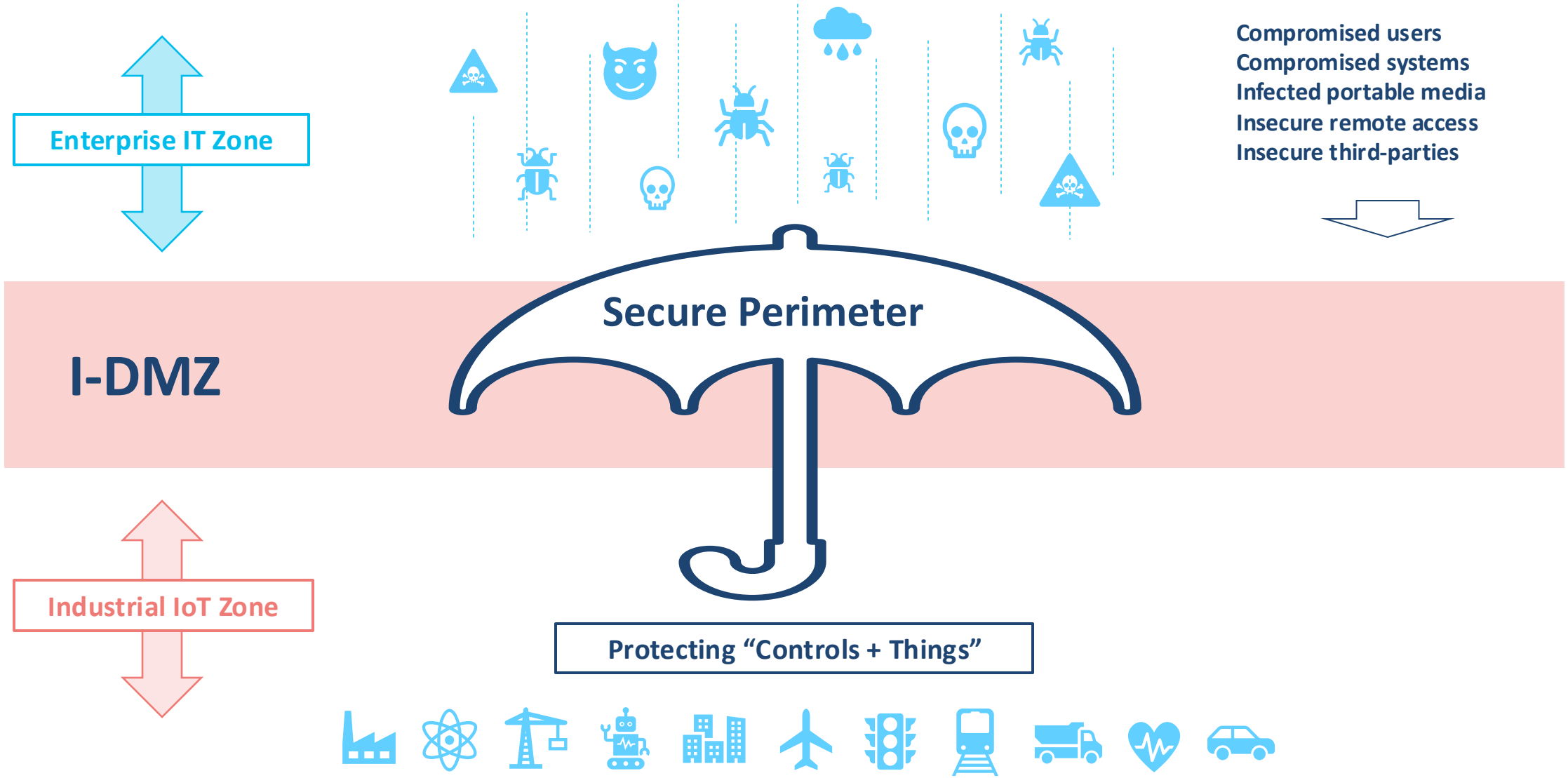
The Purdue Model



- No direct communication between IT (level 4 & 5) & OT (level 0 – 3)
- IDMZ services (level 3.5) are recommended to be segmented from each other
  - i.e. each service in its own VLAN and terminates at the firewall
- OT consists of site operations zone (level 3) and Cell/Area zone (level 0-2)

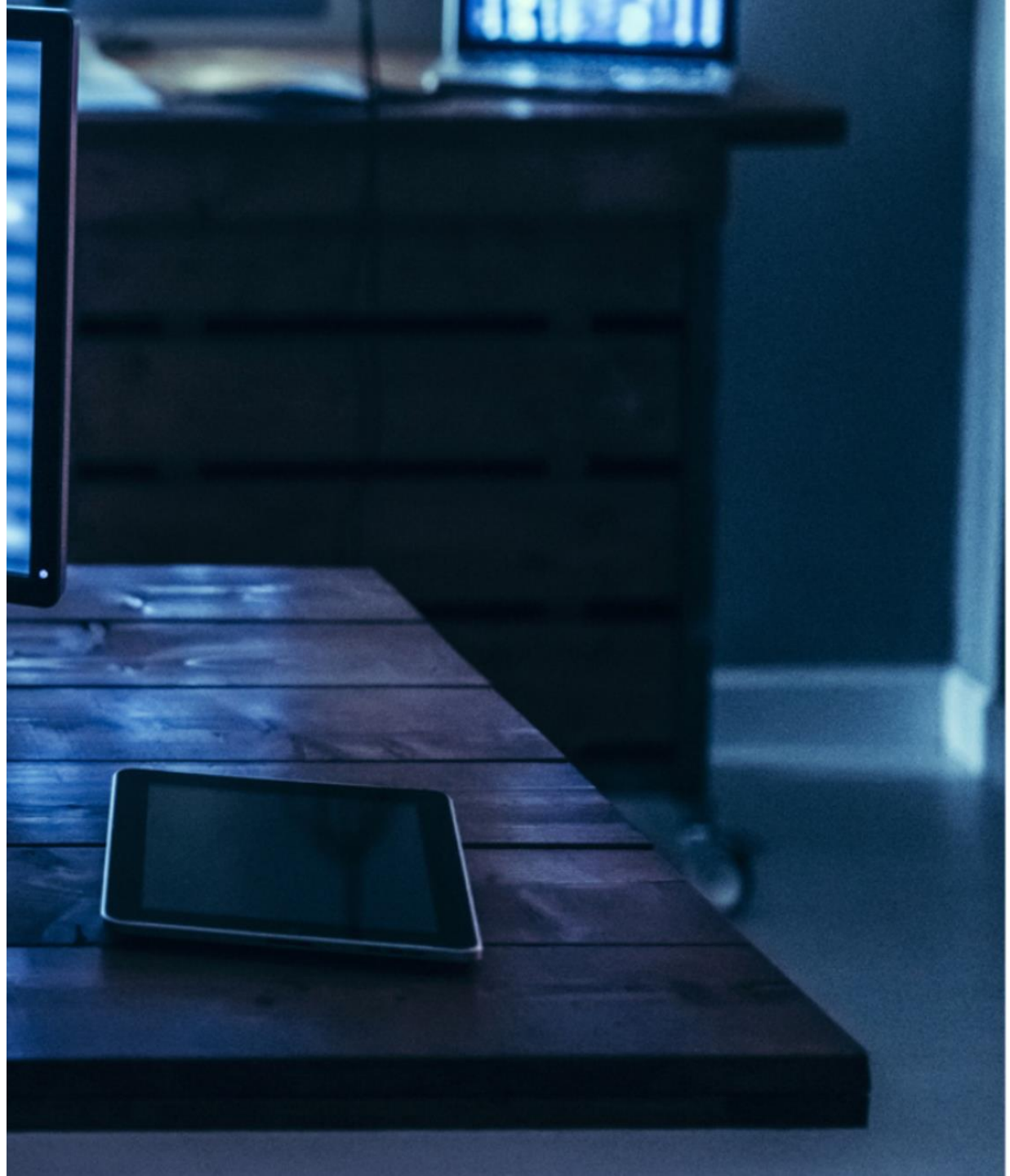
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Securing the Industrial IoT perimeter



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

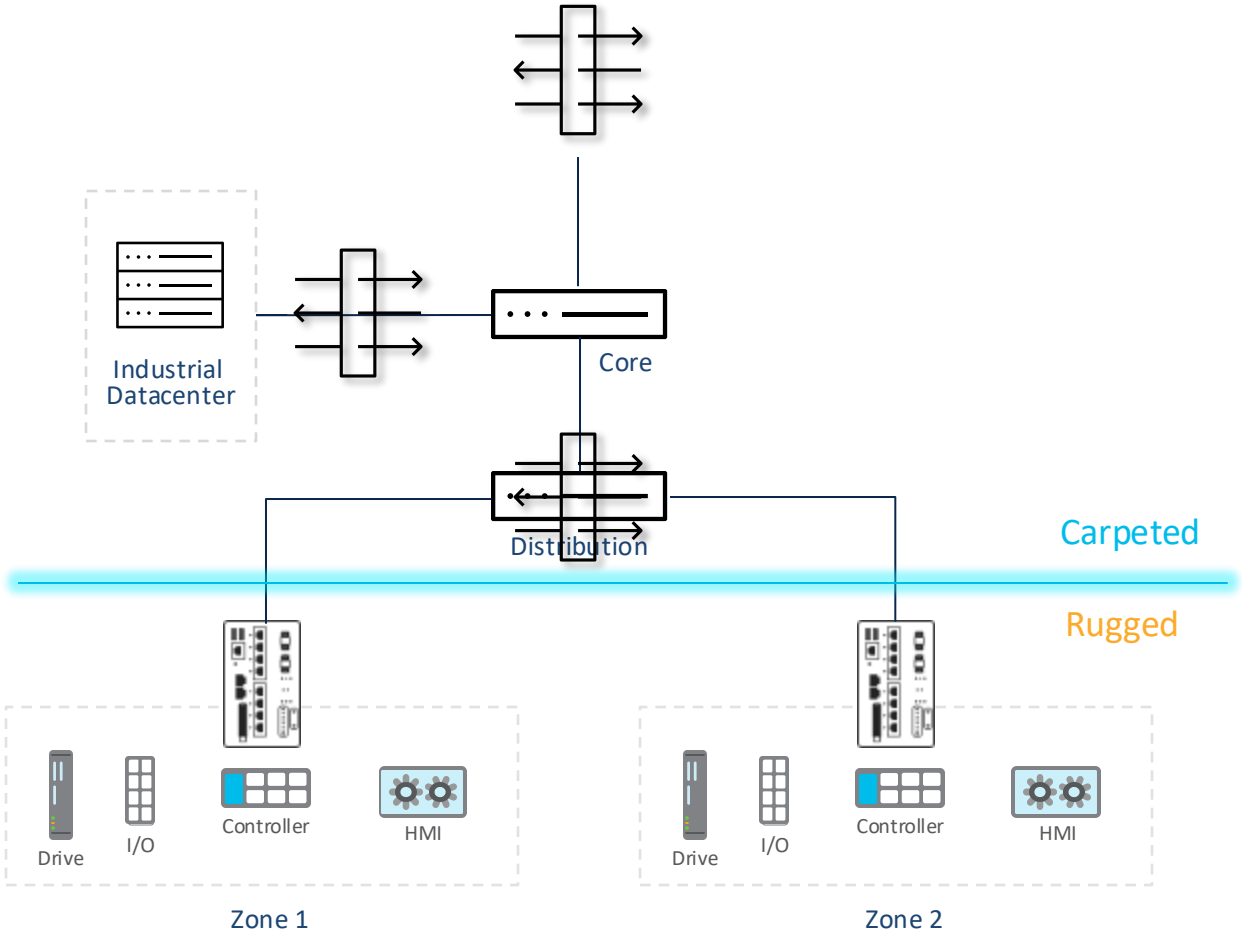
Cisco IoT



"Firewalls alone can't provide the protection that digital-first, smart factories and connected manufacturers need"

RAJ KRISHNA
VP OF STRATEGY & PLANNING, CISCO MERAKI

IT/OT Security Boundary



IT / OT Boundary

Ideally a full IDMZ has been deployed, but at minimum, a firewall between IT and OT is to be expected

Industrial Data Center

Data Center modernization should consider firewalls as an enforcement point for any data that enters or exits the virtual infrastructure on the plant floor

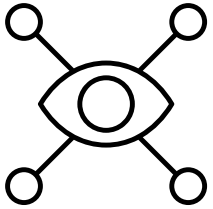
Industrial Distribution Frame (IDF)

A common deployment model in OT is to terminate VLANs at a firewall. This reduces the need for firewalls per cell

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

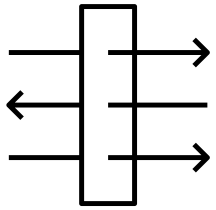
Cisco Confidential

Segmentation Phases



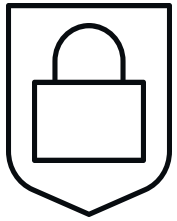
Virtual Segmentation

- Visualizing the zones and conduits model and reacting to data observed between zones



Macro Segmentation

- Pushing policy across ”large” zones (production lines or cell/area zones)
- IDF is typically point of VLAN termination and is a conditioned space



Micro Segmentation

- Pushing policy across “small” zones
- Segmentation within Cell/Area Zone

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Segmentation Design Principles

It is all about the use case

Classification

Group assets based on privileges

Classification may be based on endpoint location (i.e. zone), role (i.e. interlocking), dynamic authentication (i.e. user or profiling rule)

Enforcement

Segmentation needs should define enforcement points

Propagation

Remember: enforcement points needs to know source and destination tag, propagate if required

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 3: Send all data to the SOC

Asset Visibility & Security Posture

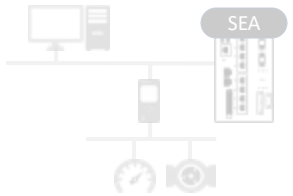
Cisco
Cyber Vision

Network embedded CV Sensor

Zero Trust for OT

Zero Trust Network Access

Cisco
Secure Equipment Access

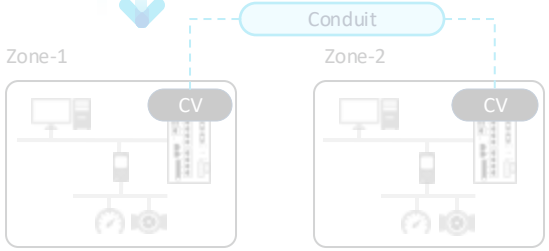


Network embedded ZTNA Gateway

IEC 62443 Zones & Conduits

Cisco
Secure Firewall

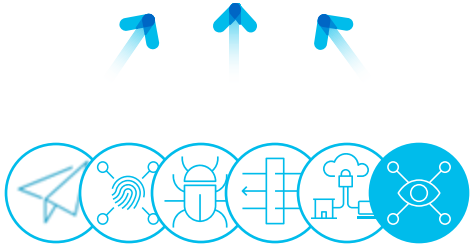
Cisco
ISE



Network enforced segmentation

Cross-Domain Detection, Investigation & Response

splunk>
a CISCO company



Visibility across the entire attack chain

Network as a fabric to secure OT at scale

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What should we be doing?

- Protect Systems against Malware with end-point protection
- Block suspicious emails
- Enforce security at the DNS layer
- Implement Multi-factor Auth (MFA)
- Isolate IT and OT networks

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Else?

- Implement Robust Network Segmentation
- Inventory and Monitor your Industrial Network
- Security Event Management in IT & OT
- Incident Response & Team Readiness Testing

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO
The bridge to possible

Securing the future of manufacturing

Cybersecurity Summit 2025

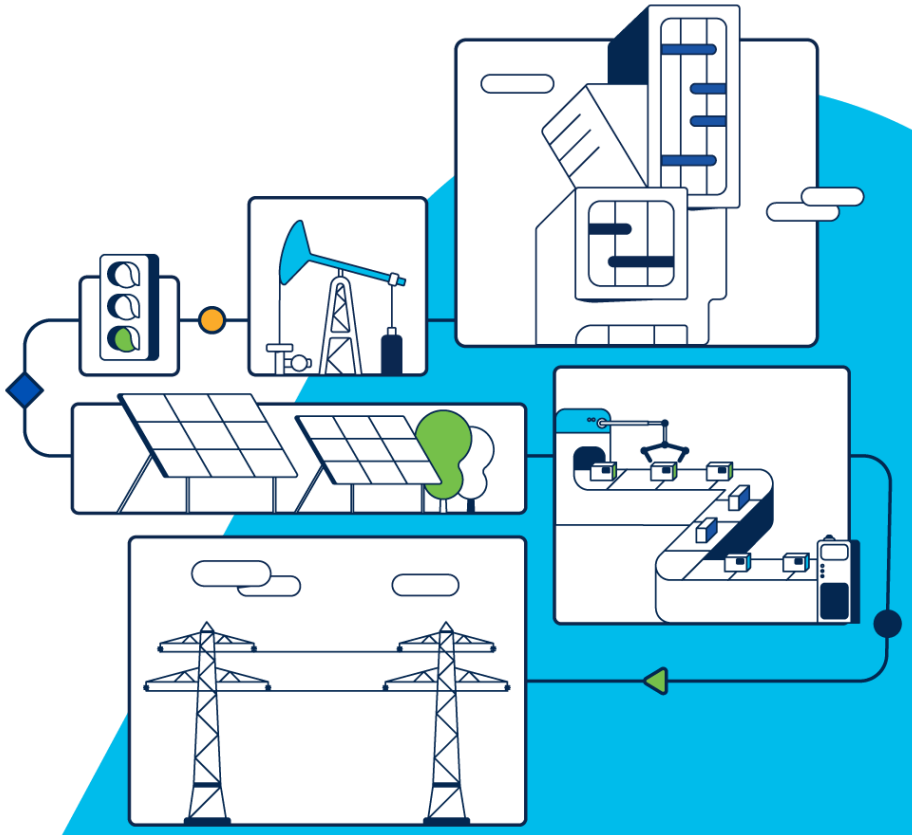
February 27, 2025

Steve Mincica

Account Executive, IIoT

Mike Wooten

Solutions Engineer, IIoT



Agenda

01

Cisco Industrial Security

Customer challenges and how Cisco can help

02

Visibility for OT Networks

Leveraging Cyber Vision for OT visibility, operational insights, and threat detection

03

Zero-Trust Security for OT

Next-generation solutions for secure remote access and IEC 62443 zone segmentation

04

Detection, Investigation, and Response

Feeding the Security Operations Center (SOC) with OT security information

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Agenda

01

Cisco Industrial Security

Customer challenges and how Cisco can help

02

Visibility for OT Networks

Leveraging Cyber Vision for OT visibility, operational insights, and threat detection

03

Zero-Trust Security for OT

Next-generation solutions for secure remote access and IEC 62443 zone segmentation

04

Detection, Investigation, and Response

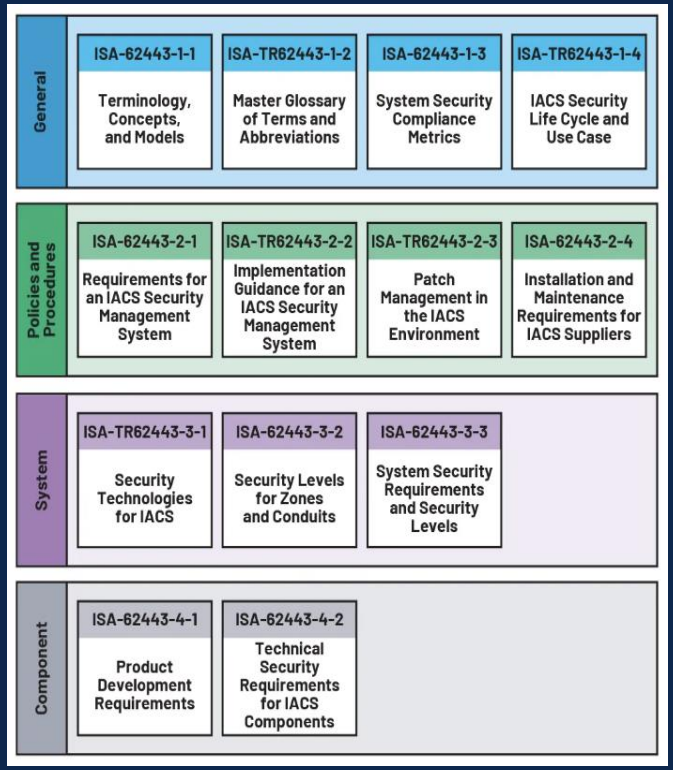
Feeding the Security Operations Center (SOC) with OT security information

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Securing critical infrastructure is a key priority

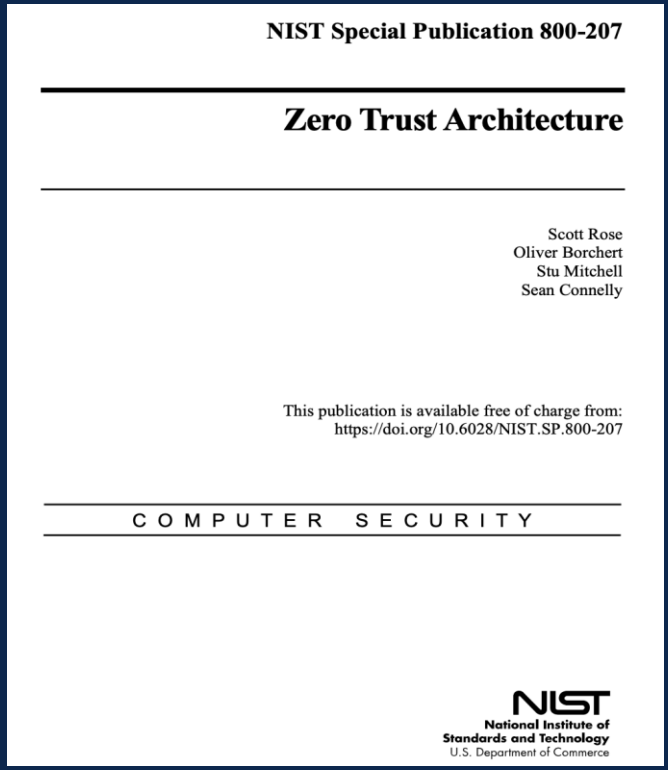
ISA/IEC 62443

Securing Industrial Automation Control Systems



NIST

Zero Trust Architecture



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIS2

Energy, Transport, Water, Manufacturing, …..

BRIEFING
EU Legislation in Progress

European Parliament

The NIS2 Directive

A high common level of cybersecurity in the EU

OVERVIEW

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market.

To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, while the Council agreed its position on 3 December 2021. The co-legislators reached a provisional agreement on the text on 13 May 2022. The political agreement was formally adopted by the Parliament and then the Council in November 2022. It entered into force on 16 January 2023, and Member States now have 21 months, until 17 October 2024, to transpose its measures into national law.

Proposal for a directive on measures for a high common level of cybersecurity across the Union		
Committee responsible:	Industry, Research and Energy (ITRE)	COM(2020) 823 16.12.2021
Rapporteur:	Bart Groothuis (Renew, the Netherlands)	2020/0359(COD)
Shadow rapporteurs:	Eva Maydell (EPP, Bulgaria) Eva Kaili (S&D, Greece) Rasmus Andresen (Greens/EFA, Germany) Thierry Mariani (ID, France)	Ordinary legislative procedure (COD)

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Securing critical infrastructure requires new procedures

More connectivity means airgap is not sufficient anymore

Low visibility over disconnected endpoints

Some OT assets cannot be patched

Legitimate instructions can disrupt processes

Multiple remote operations involved in day-to-day ops

Standard IT cybersecurity solutions and methodologies are not sufficient to fulfil OT cybersecurity requirements

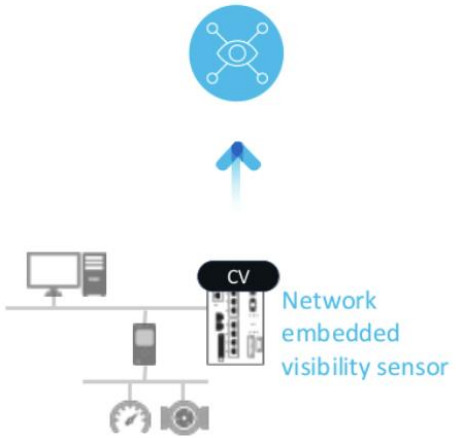
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enabling a comprehensive OT security journey

Visibility

OT Asset Visibility and Security Posture

Cisco Cyber Vision

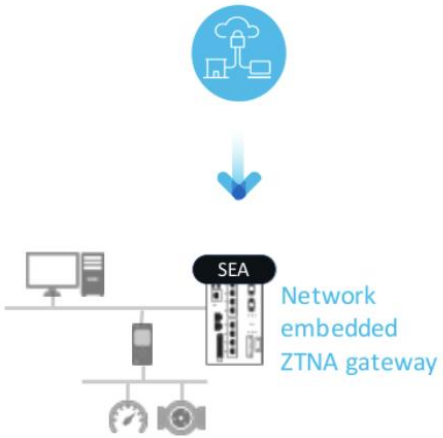


Protection

Zero Trust Security for OT

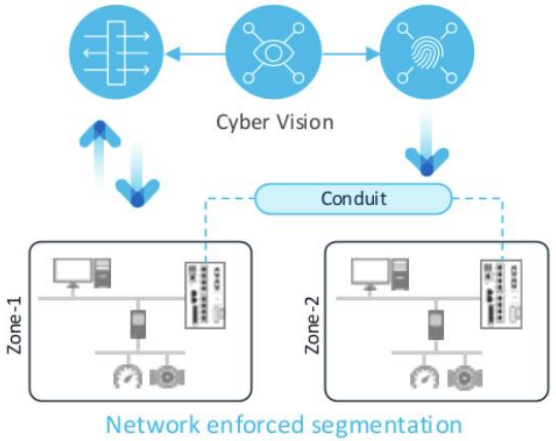
Secure remote access (ZTNA)

Cisco Secure Equipment Access



IEC 62443 zone segmentation

Cisco Secure Firewall **Cisco ISE**



Response

Cross-Domain Detection, Investigation & Response

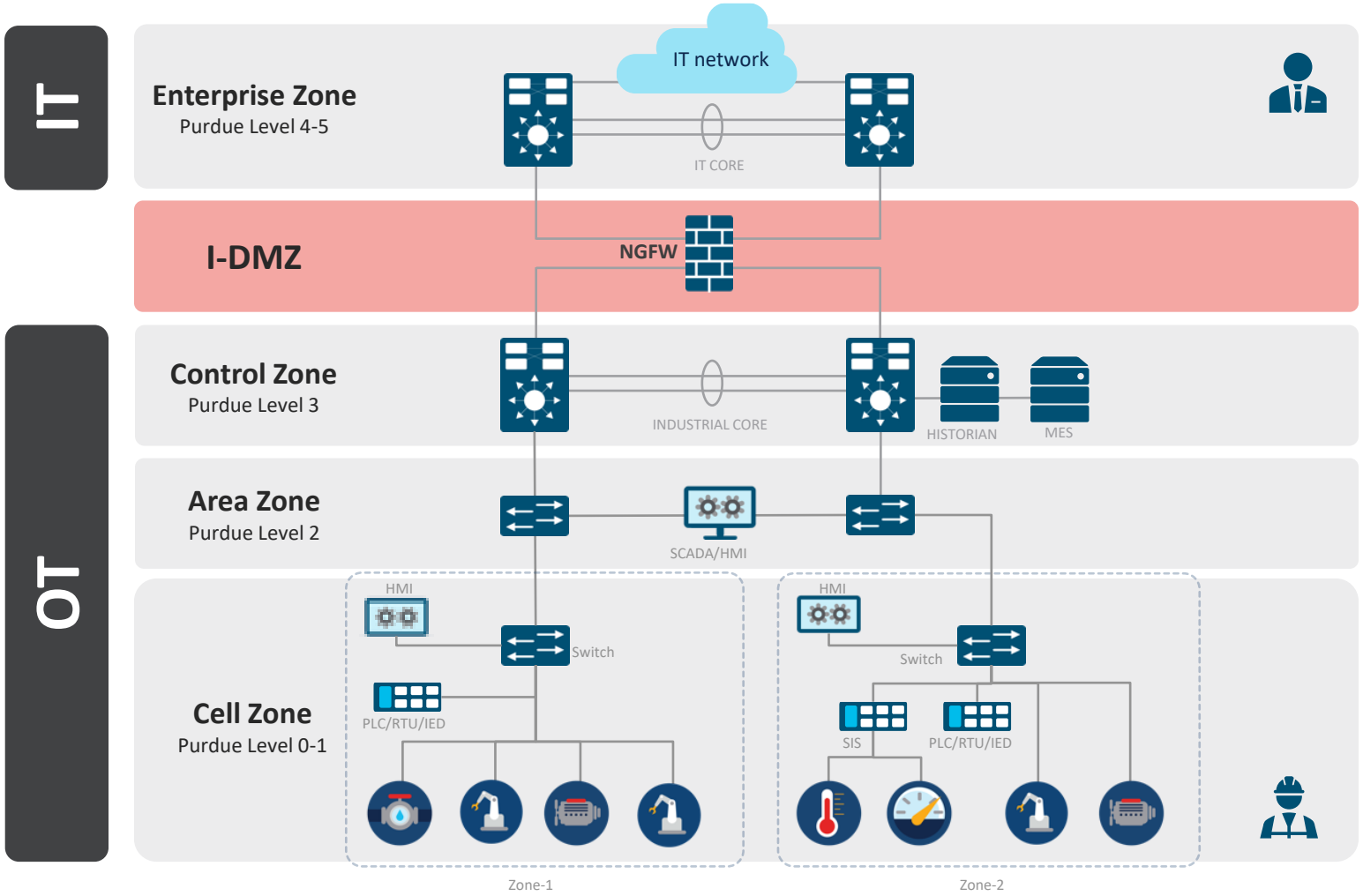
splunk> a cisco company

Visibility across the entire attack chain

Talos Threat Intelligence + Talos Incident Response

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secure the operational boundary



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Agenda

01

Cisco Industrial Security

Customer challenges and how Cisco can help

02

Visibility for OT Networks

Leveraging Cyber Vision for OT visibility, operational insights, and threat detection

03

Zero-Trust Security for OT

Next-generation solutions for secure remote access and IEC 62443 zone segmentation

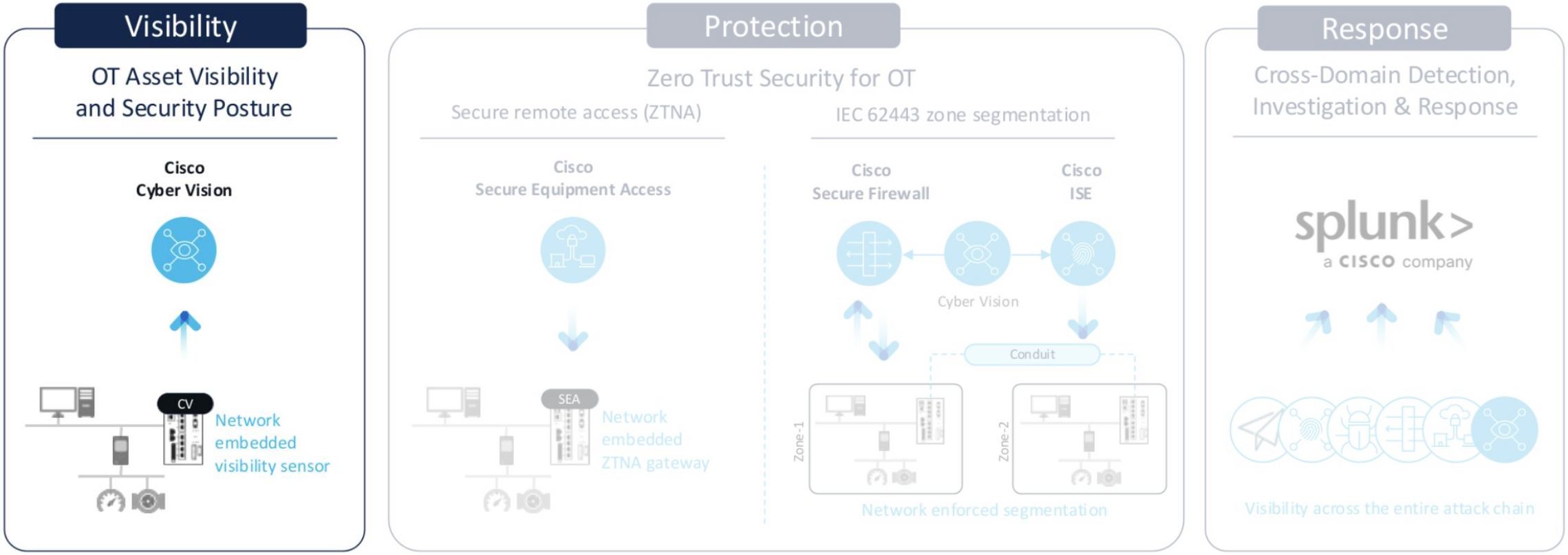
04

Detection, Investigation, and Response

Feeding the Security Operations Center (SOC) with OT security information

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enabling a comprehensive OT security journey



Talos Threat Intelligence + Talos Incident Response

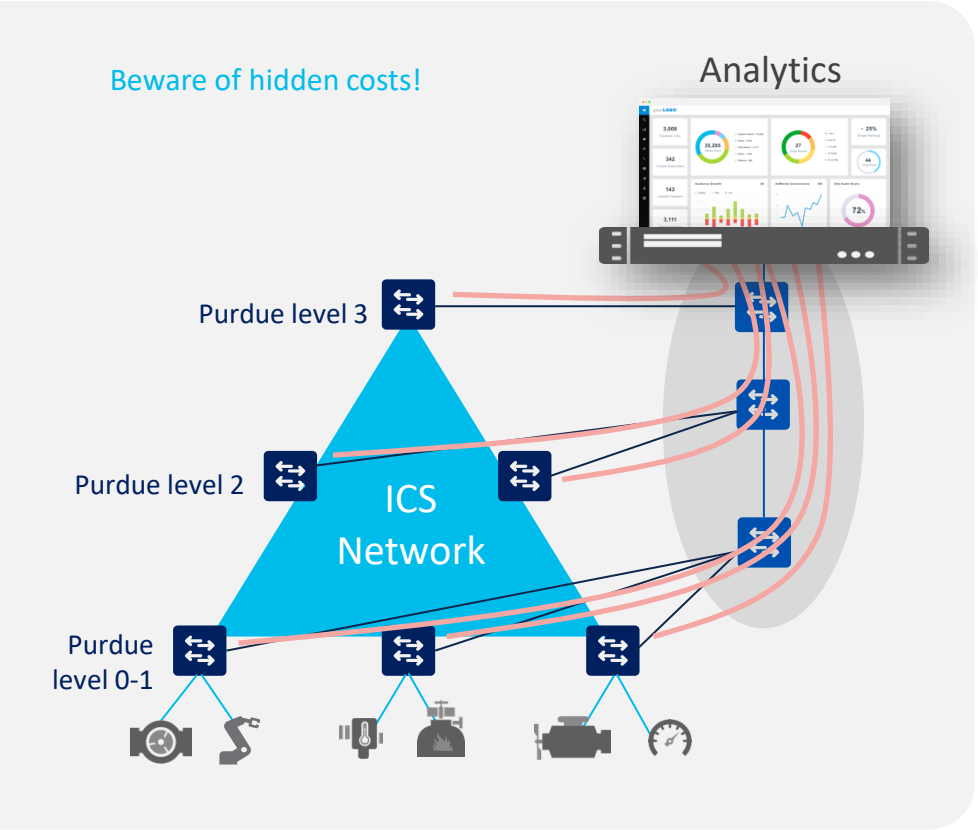
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Why understanding security posture is necessary

- Do I have unknown vendors in my network?
- Are there vulnerabilities in my devices that have active exploits across the network?
- Do my Internet connected assets also have communication paths into my critical network?

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Typical industrial visibility solutions require mirroring industrial network traffic via SPAN



74%

say cost and complexity of SPAN is main blocker to visibility[1]

41%

of organizations are embracing digital transformation to future proof their OT[2]

$ 6500

average per SPAN cable run in an OT network

600+ distribution substations and Cisco was the **ONLY** vendor who could meet their scale

TCO of SPAN based solutions is not sustainable over long-term growth

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

[1] https://www.cisco.com/c/en/us/products/collateral/security/sec-surv-rpt-ind-org-still-lack-vis-wp.html
[2] https://www.cisco.com/c/m/en_us/solutions/industrial-networking-report.html

Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT

Visibility
OT asset inventory
Communication patterns

Security Posture
Device vulnerabilities
Risk scoring

Operational Insights
Track process/device modifications
Record control system events

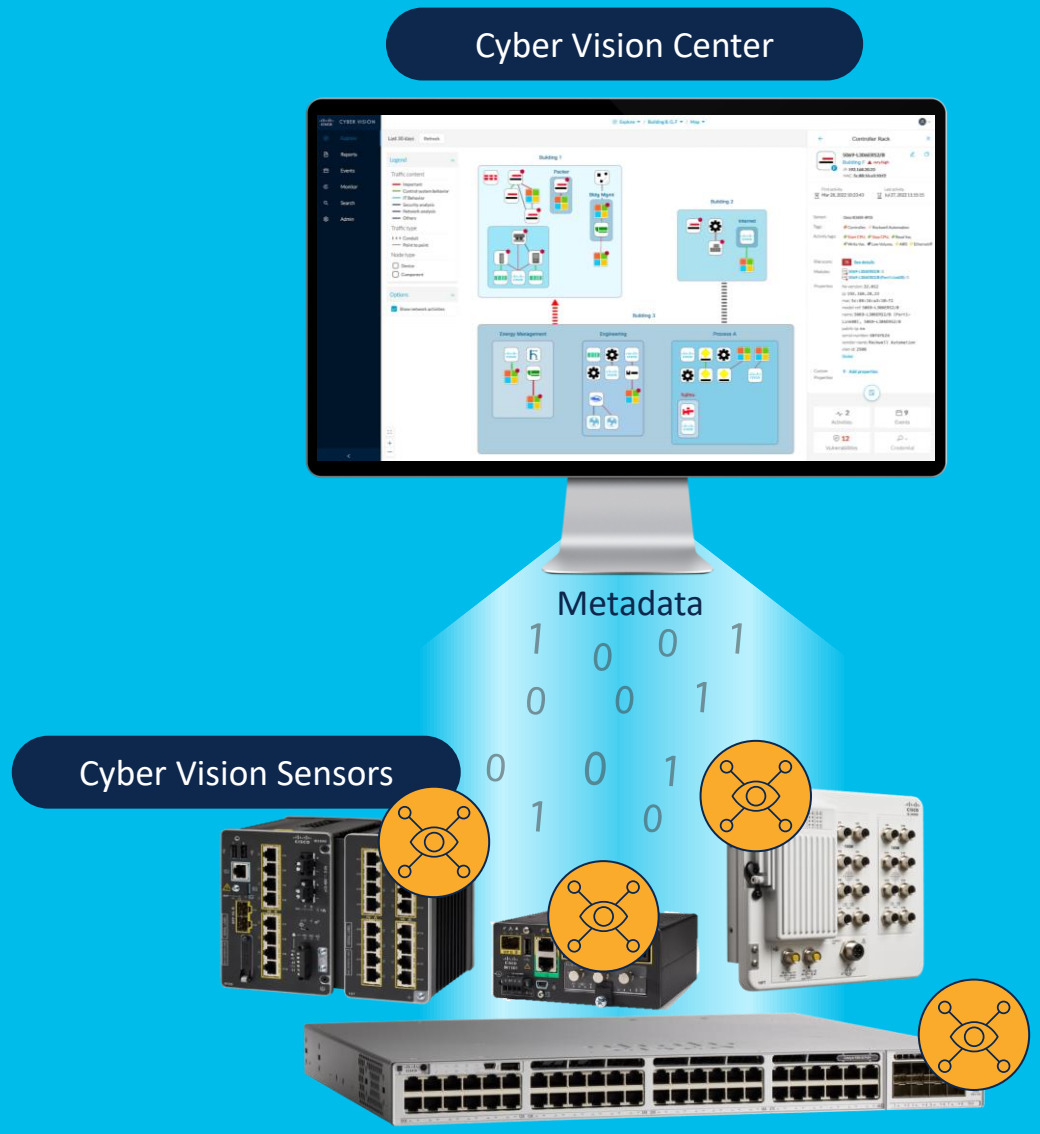
Context and insights that are foundational to building reliable and secure OT networks

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Cyber Vision

Manage risks from OT assets with full visibility on your industrial security posture

- Asset Inventory & Profiling
- Asset Communications
- Asset Vulnerabilities
- Asset Risk Scores
- Behavior Baselining
- Snort Threat Detection
- Talos Threat Intelligence



Deep Packet Inspection & Active Discovery
built into your network infrastructure

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Agenda

01

Cisco Industrial Security

Customer challenges and how Cisco can help

02

Visibility for OT Networks

Leveraging Cyber Vision for OT visibility, operational insights, and threat detection

03

Zero-Trust Security for OT

Next-generation solutions for secure remote access and IEC 62443 zone segmentation

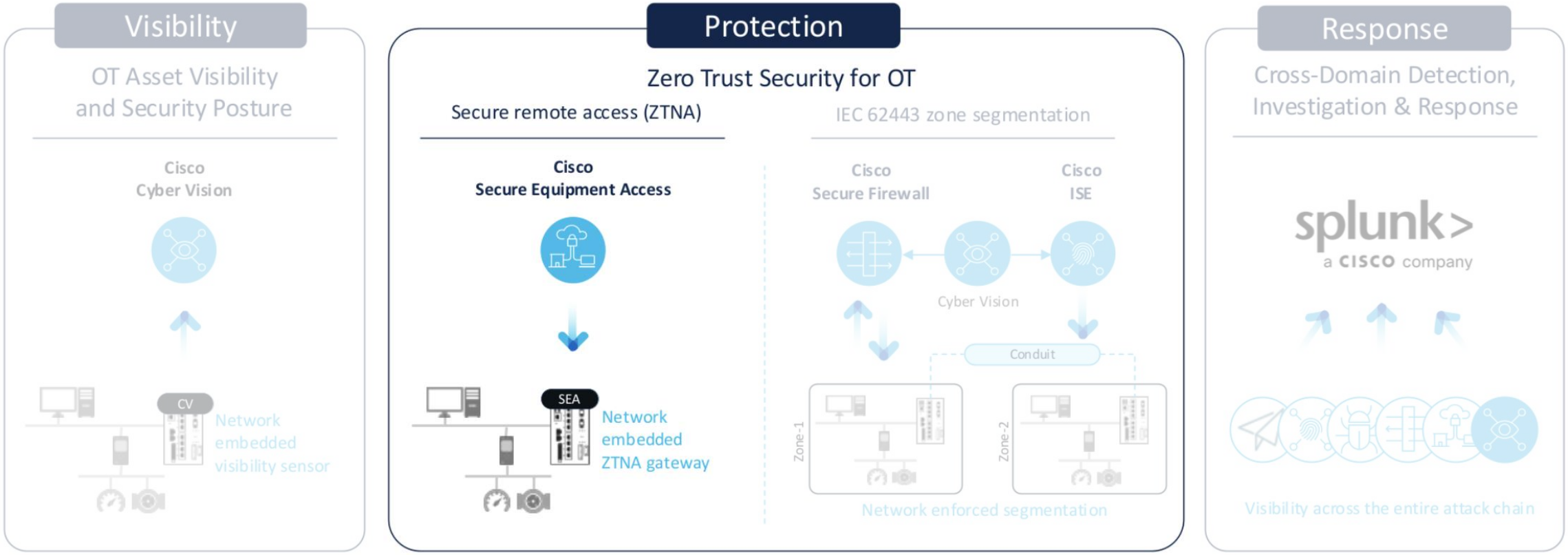
04

Detection, Investigation, and Response

Feeding the Security Operations Center (SOC) with OT security information

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enabling a comprehensive OT security journey



Talos Threat Intelligence + Talos Incident Response

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Existing options are either security backdoors or come with many trade-offs

Ad-Hoc Software

Often installed on operator workstations

Backdoor to IT security policies

Cellular Gateways

Dedicated hardware installed by machine builders

Backdoor to IT security policies

VPN

Always-On, All-or-Nothing access

Need additional controls to deny full network access

ZTNA deployed in iDMZ

Provides controlled identity and context-aware access

Challenging to deploy in industrial settings

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Zero Trust Network Access (ZTNA) for OT Assets

The next generation remote access architecture

"

ZTNA provides controlled **identity and context-aware** access to resources. It starts with a **default deny** posture and **adaptively offers the appropriate trust** required at the time. A **trust broker** mediates connections between applications and users. The result **reduces risk** and offers **more flexible and responsive** ways to connect and collaborate.

Gartner®

Market Guide for Zero Trust Network Access,
August 2023

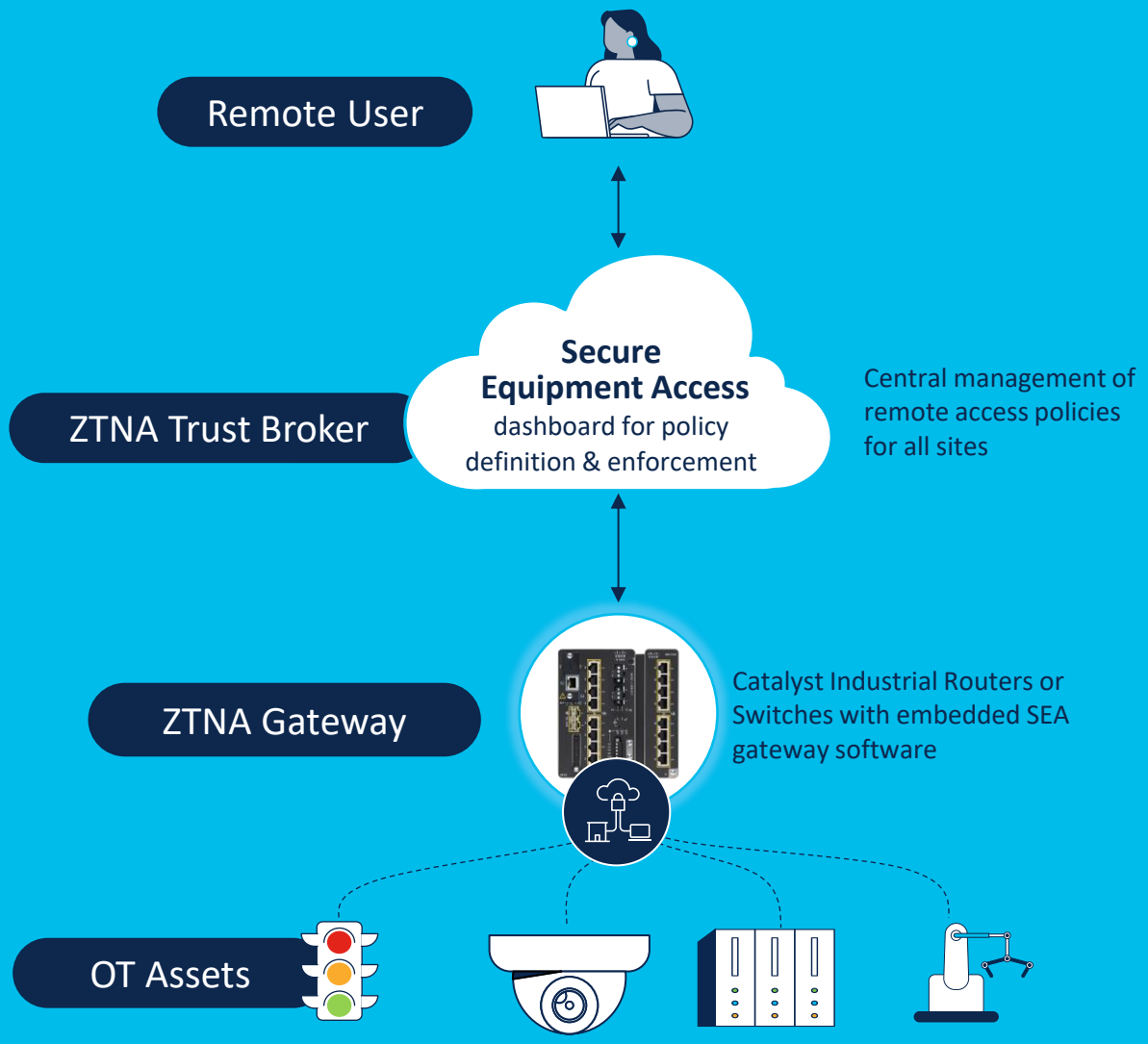
- Least privilege access
- Assets hidden from discovery
- No lateral movement possible
- Device posture compliance
- Time/date restricted access
- Reduced attack surface
- More flexible and responsive

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secure Equipment Access (SEA)

Manage risks from suppliers with ZTNA remote access to OT assets

- Zero Trust MFA & SSO
- OT Asset Resource Isolation
- Clientless & Agent-based Access
- Remote User Host Posture Check
- Session Scheduling
- Session Recording, Monitoring & Kill
- Session Approval on Request



One-click **zero trust remote access to any OT asset** connected to Cisco industrial network

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Secure Equipment Access

Only assets you select can be accessed…

All Access Methods (6)

Refresh As of: Sep 7, 2023 3:15 PM

IR1101-WebApp (WEB_APP)
Via Web App
IR1101-SEA
Availability: Always Active
Last Accessed: Never

NUC - RDP (RDP)
Via RDP
IR1101-SEA
Availability: Always Active
Last Accessed: 8 minutes ago

PLC (SEA Plus) (SEA_PLUS)
Via SEA Plus
IR1101-SEA
Availability: Always Active
Last Accessed: a month ago

RPi-Linux-VNC (VNC)
Via VNC
IR1101-SEA
Availability: Always Active
Last Accessed: 9 minutes ago

SSH-IR1101 (SSH)
Via SSH
IR1101-SEA

…using the protocols you choose

System Management / Network Device Details / 176

1769-L16ER/B

Connected Client Details

Client Name	1769-L16ER/B
Device Type	PLC
Description	Conveyor belt controller

Access Methods (2)

Search Table

Access Method

Method Name

6ER/B (SEA_PLUS)

Add Access Method

Connected Client Details

Client Name	IP Address/Host Name
1769-L16ER/B	192.168.100.101

Access Method Details

Access Method*

- SSH
- RDP
- VNC
- Web App
- Telnet

…at the time/day you define

Remote Sessions

Fanuc Robots (3)
View details

LinuxServer (SSH)
Via SSH
IR1101-SEA
Last Accessed: an hour ago

Group Details

Name	Fanuc Robots
Description	-
Creation Date	Aug 31, 2023 11:22 AM
Enforce Full-Screen Monitoring & Recording	Off
Enforce Inline (SSH/RDP/VNC) Recording	On
Schedule Start	Aug 31, 2023 11:27 AM
Schedule End	Aug 31, 2023 12:27 PM
Duration	1 hour

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Secure Equipment Access

Access remote assets with just a browser

Remote Sessions

Fanuc Robots (2)
View details

LinuxServer (SSH)
Via SSH
IR1101-SEA

Last Accessed: 21 hours ago

```
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $ ls
Bookshelf  Documents  FTP    Pictures  Templates
Desktop    Downloads  Music  Public    Videos
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $ cal
     August 2023
Su Mo Tu We Th Fr Sa
       1  2  3  4  5
 6  7  8  9 10 11 12
13 14
20 21
27 28
```

Session history with recordings and audit info

Access Manag

Access Control Groups | Users | Active Sessions | Session History

Session History (248)

Start Date: May 2, 2023
End Date: Aug 31, 2023
Only Show Recorded Sessions

Search Table

Refresh As of: Aug 31, 2023 12:09 PM

Session Start	Session End	Connected Client	Access Method	User	Terminated	Recorded	Actions
Aug 31, 2023 12:03 PM	Aug 31, 2023 12:07 PM	External-switch	External-switch (SSH)	alzaytse@cisco.com	No	Yes	···
Aug 31, 2023 10:39 AM	Aug 31, 2023 10:59 AM	LinuxServer	SEA+ Filestransfer Linux 192.168.2.2 (NATIVE)	alzaytse@cisco.com	No	No	···
Aug 31, 2023 10:26 AM	Aug 31, 2023 10:36 AM	LinuxServer	LinuxServer (SSH)	alzaytse@cisco.com	No	Yes	···
Aug 31, 2023 10:26 AM	Aug 31, 2023 10:26 AM	External-switch-Linux-Server	External-switch-Linux-Server (VNC)	alzaytse@cisco.com	No		

View Full Auditing Info
View Inline Recording
Download Inline Recording

Session monitoring and termination

Access Management

Access Control Groups | Users | Active Sessions | Session History

Active Sessions (4)

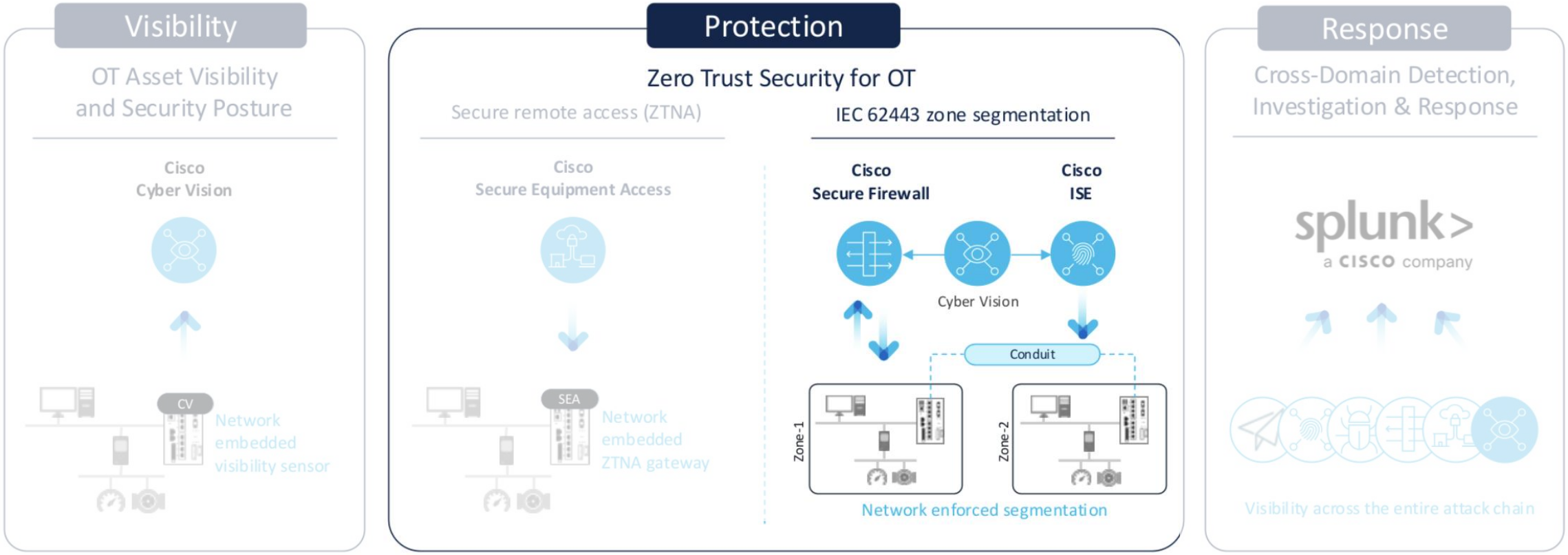
Search Table

Refresh As of: Aug 31, 2023 12:05 PM

Connected Client	Access Method	User	Session Start	Duration	Monitor	Security
External-switch	External-switch (SSH)	alzaytse@cisco.com	2 minutes ago	Unscheduled	Join Session	Terminate
External-switch-Linux-Server	External-switch-Linux-Server (VNC)	alzaytse@cisco.com	a minute ago	Unscheduled	Join Session	Terminate
IR1101	IR1101 (WEB)	alzaytse@cisco.com	a few seconds ago	Unscheduled	Not Monitored	Terminate
Windows10 Server	Windows10 Server (RDP)	alzaytse@cisco.com	a few seconds ago	Unscheduled	Join Session	Terminate

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enabling a comprehensive OT security journey

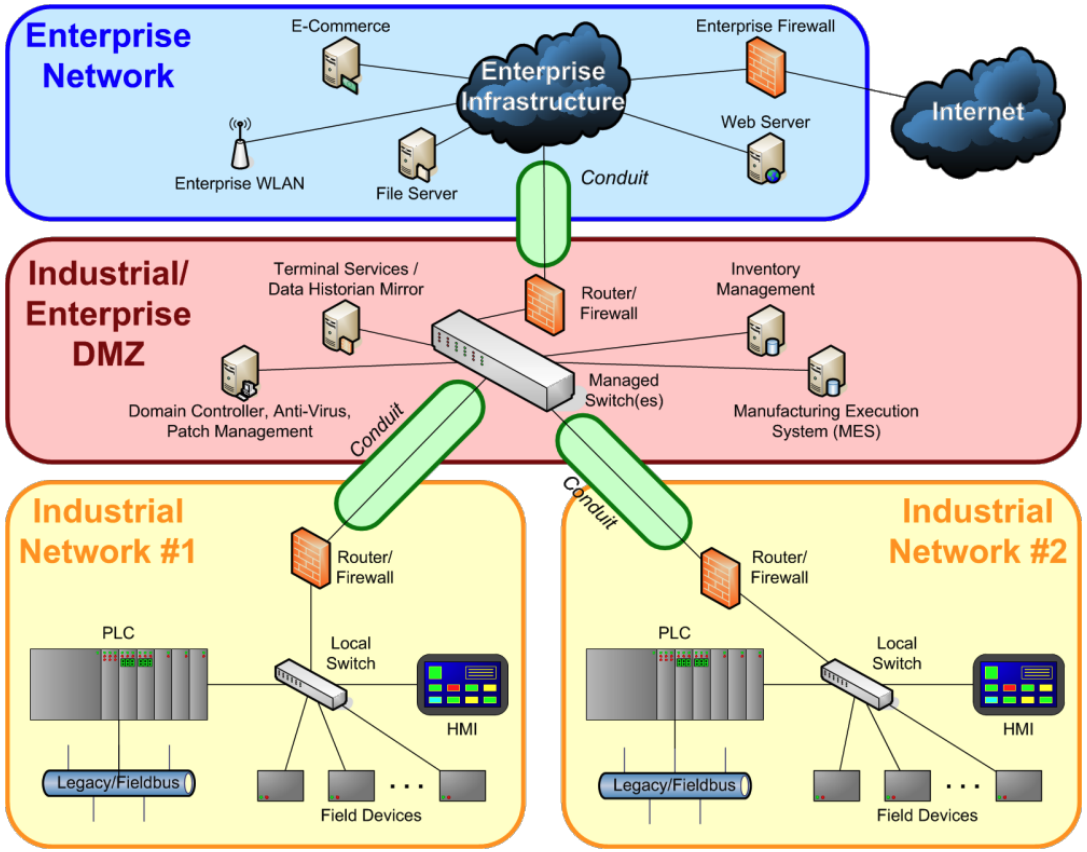


Talos Threat Intelligence + Talos Incident Response

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Guidance per Industry Standards

ISA/IEC 62443



NIST Zero Trust Architecture guidance

3.1.2 ZTA Using Micro-Segmentation

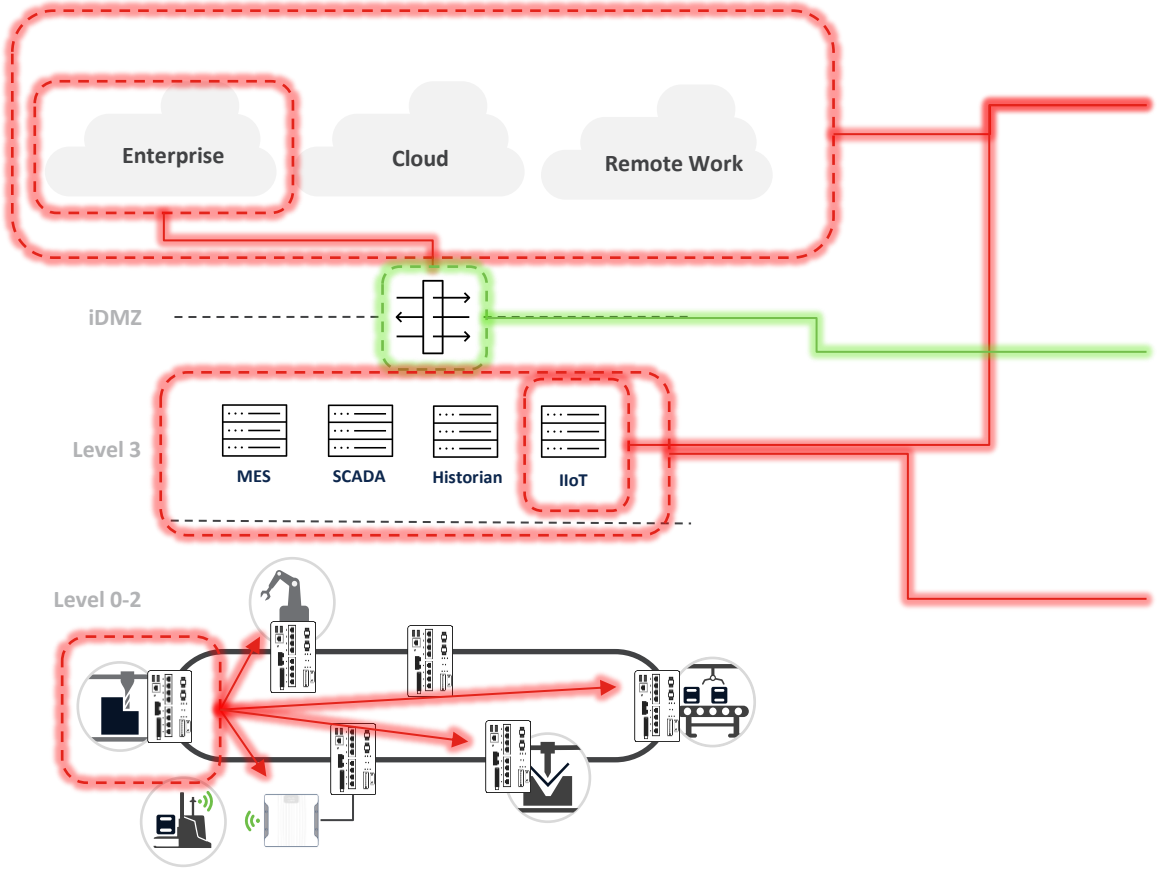
An enterprise may choose to implement a ZTA based on placing individual or groups of resources on a unique network segment protected by a gateway security component. In this approach, the enterprise places infrastructure devices such as intelligent switches (or routers) or next generation firewalls (NGFWs) or special purpose gateway devices to act as PEPs protecting each resource or small group of related resources. Alternatively (or additionally), the enterprise may choose to implement host-based micro-segmentation using software agents (see Section 3.2.1) or firewalls on the endpoint asset(s), These gateway devices dynamically grant access to individual requests from a client, asset or service. Depending on the model, the gateway may be the sole PEP component or part of a multipart PEP consisting of the gateway and client-side agent (see Section 3.2.1).

This approach applies to a variety of use cases and deployment models as the protecting device acts as the PEP, with management of said devices acting as the PE/PA component. This approach requires an identity governance program (IGP) to fully function but relies on the gateway components to act as the PEP that shields resources from unauthorized access and/or discovery.

The key necessity to this approach is that the PEP components are managed and should be able to react and reconfigure as needed to respond to threats or change in the workflow. It is possible to implement some features of a micro-segmented enterprise by using less advanced gateway devices and even stateless firewalls, but the administration cost and difficulty to quickly adapt to changes make this a very poor choice.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

How much control do I need?



Initial Access
Stop attackers gaining an initial foothold on the network. Anything connected to the Internet is a target

IT / OT Boundary
If IT network is exploited, there should be no direct path to the critical network

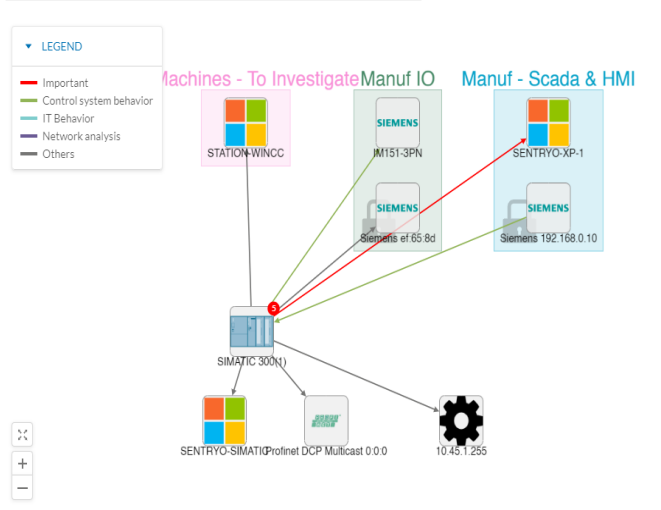
Industrial Data Center
If application in the data center is exploited, there should be protections in place for the shop floor

Lateral Movement in the Control Network
If one process zone is compromised, others should continue to run without interruption

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

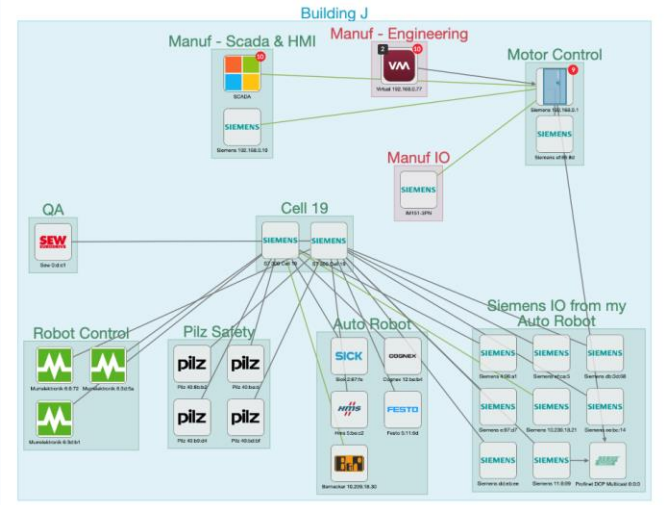
Visibility lets you build Zones and Conduits

Identify Application Relationships



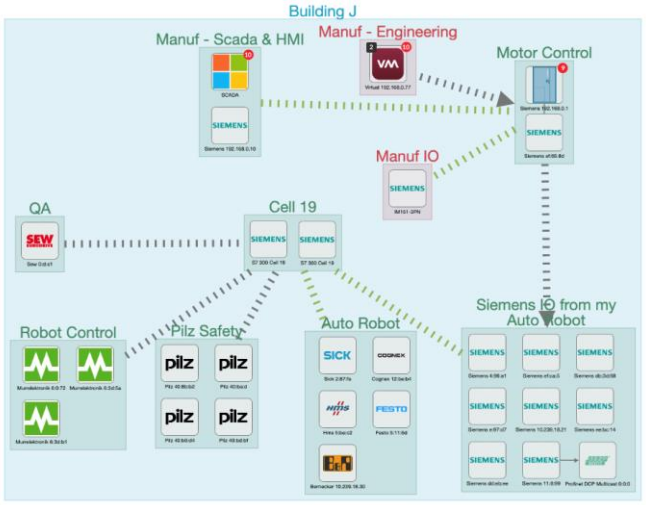
Cyber Vision maps traffic flows between endpoints and provides application-level details within the flows

Group endpoints into Zones



Users can leverage these application relations to group endpoints to match the industrial processes they represent

Visualize Conduits between Zones



The traffic flows can be aggregated into conduits which can be used to inform segmentation policies

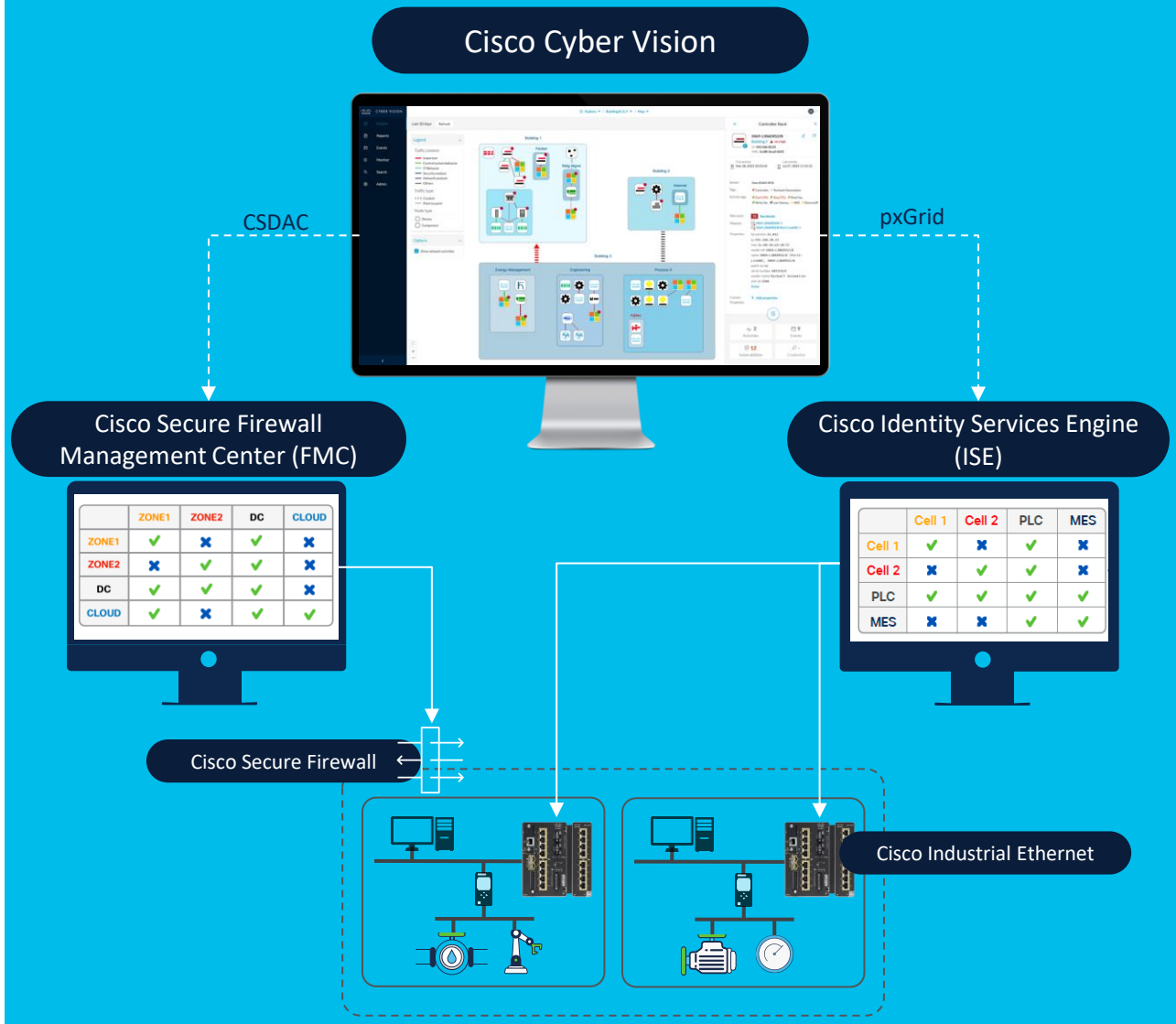
Map your industrial process to build and enforce security policies

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cyber Vision Integrations

Leveraging visibility to drive segmentation

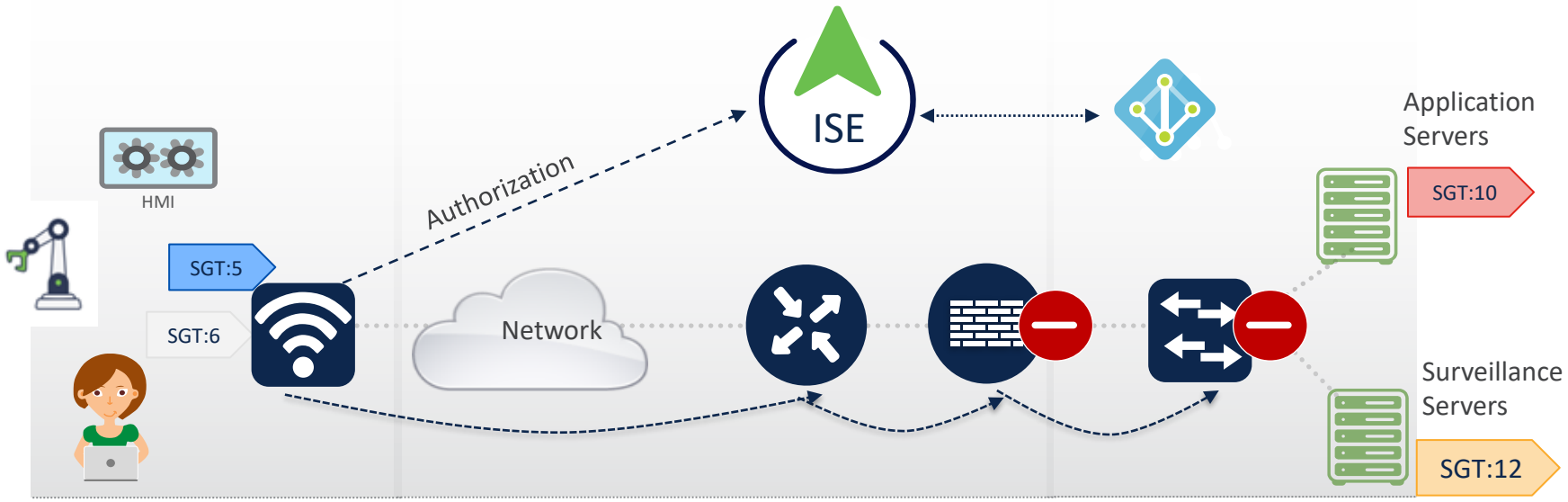
- Enable OT teams to group assets into zones by using Cyber Vision
- Visualize conduits
- Identify traffic violations
- Share context with other platforms to enforce segmentation
- Automatically update security policy as assets move across the network



Automated **ISA/IEC-62443** zone segmentation using firewalls or switches

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Identity Services Engine (ISE) / TrustSec concepts



SGT assignment Propagation Enforcement

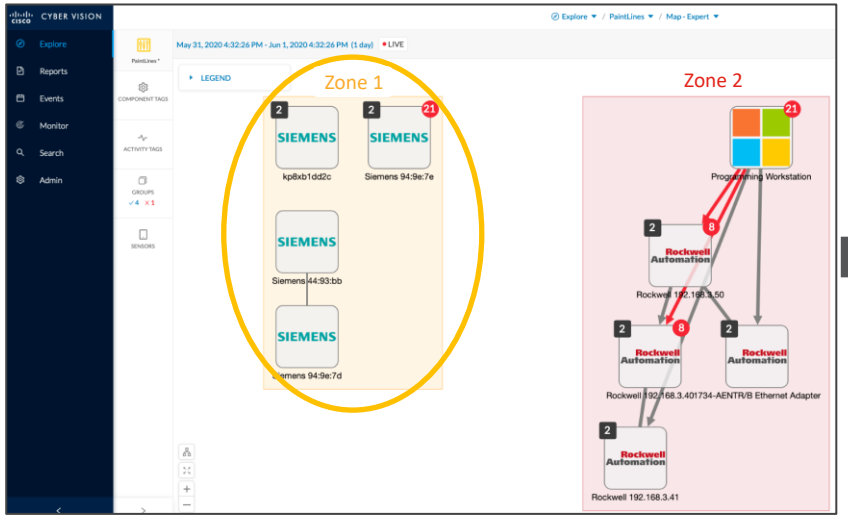
- Assignment of Security Group Tag (SGT) based on context (identity, device group, etc.).
- SGT are carried propagated through the network
- Firewalls, routers and switches use SGT to make filtering decisions via SGACL.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Profiling OT assets enables dynamic segmentation

This user interface understands industrial processes.
I can group assets into zones

I now have OT context to build the right security policies



Cyber Vision Map View

	Zone 1	Zone 2	PLC	MES
Zone 1	✓	✗	✓	✗
Zone 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

pxGrid update with asset endpoint identities and group as custom attribute

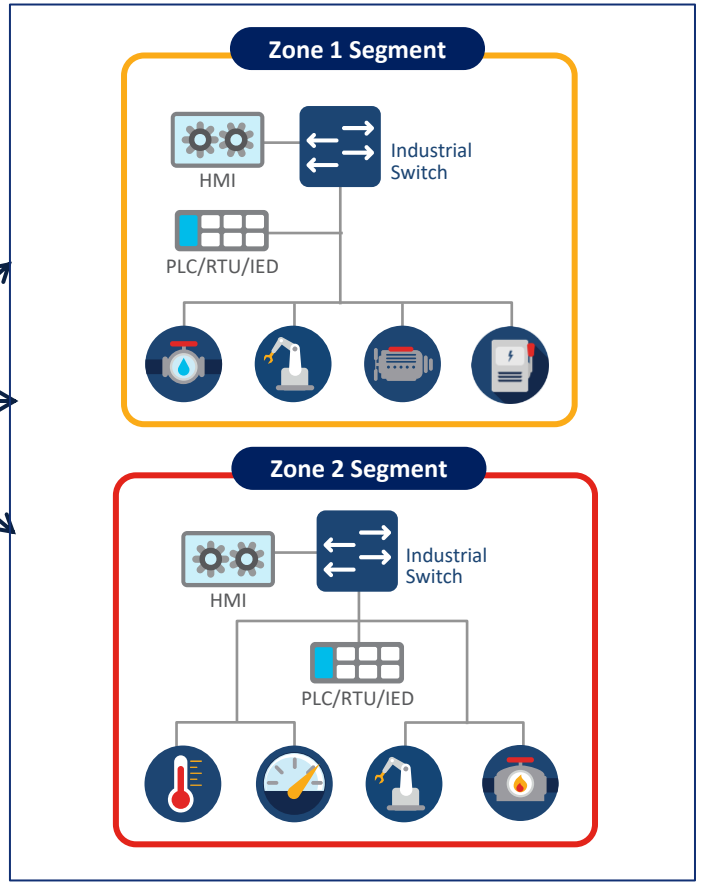
Cisco ISE Policy Matrix

dACL

SGT

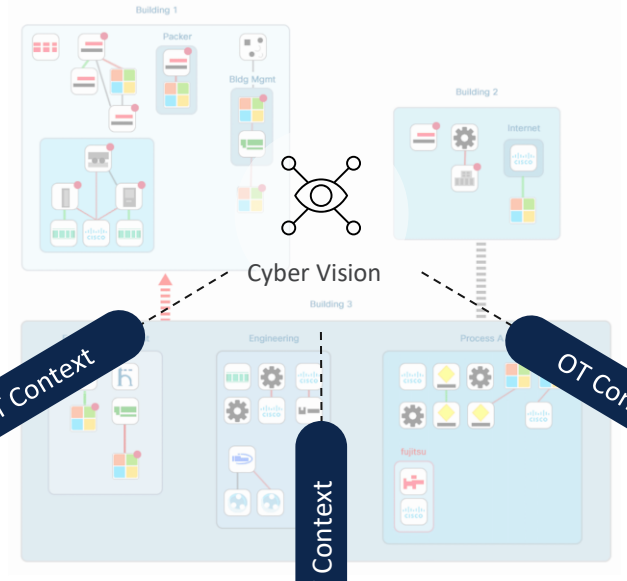
VLAN

Segmentation of industrial network



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Visibility is the catalyst for Industrial Security



Perimeter Security
Automatically apply NGFW policy based on Cyber Vision groups

Secure Firewall

Identity Services Engine

Network Access Control
Automatically update access control policies for the network to enforce zero-trust segmentation based on Cyber Vision data

splunk> a cisco company

Cross Domain Detection, Incident & Response
Automatically enrich the SOC with OT specific context and insights not attainable by traditional security tools

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Agenda

01

Cisco Industrial Security

Customer challenges and how Cisco can help

02

Visibility for OT Networks

Leveraging Cyber Vision for OT visibility, operational insights, and threat detection

03

Zero-Trust Security for OT

Next-generation solutions for secure remote access and IEC 62443 zone segmentation

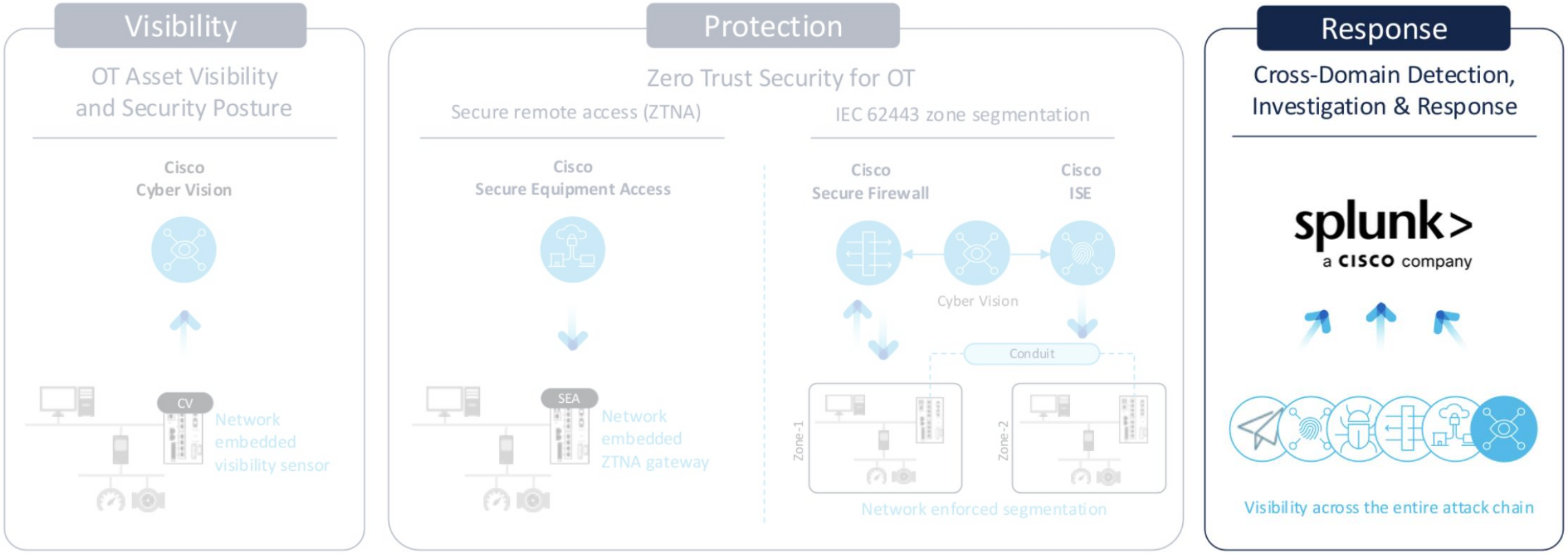
04

Detection, Investigation, and Response

Feeding the Security Operations Center (SOC) with OT security information

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enabling a comprehensive OT security journey

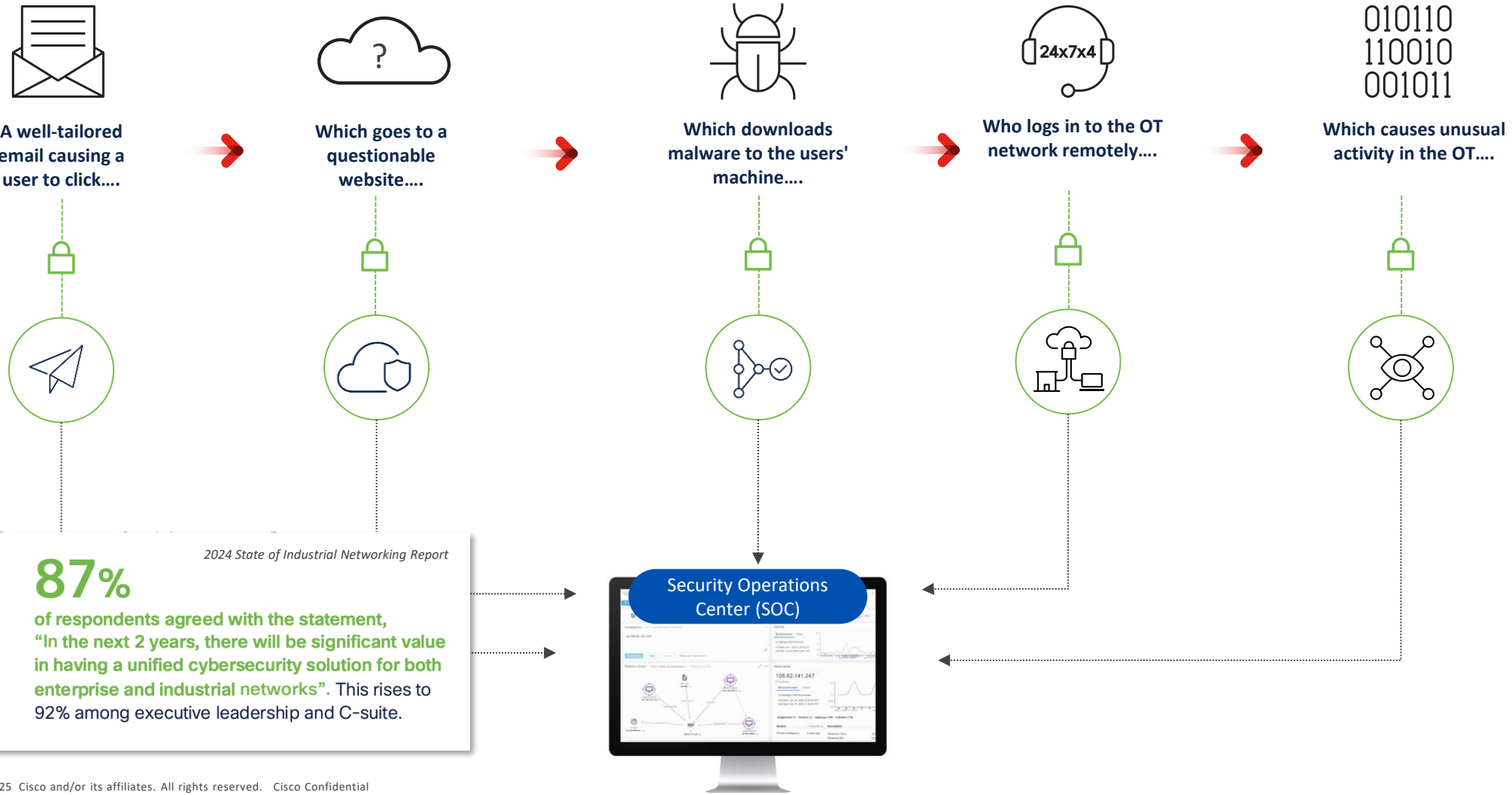


Talos Threat Intelligence + Talos Incident Response

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

How do we unify visibility across the entire attack chain?

ICS Attack Chain



2024 State of Industrial Networking Report

87%

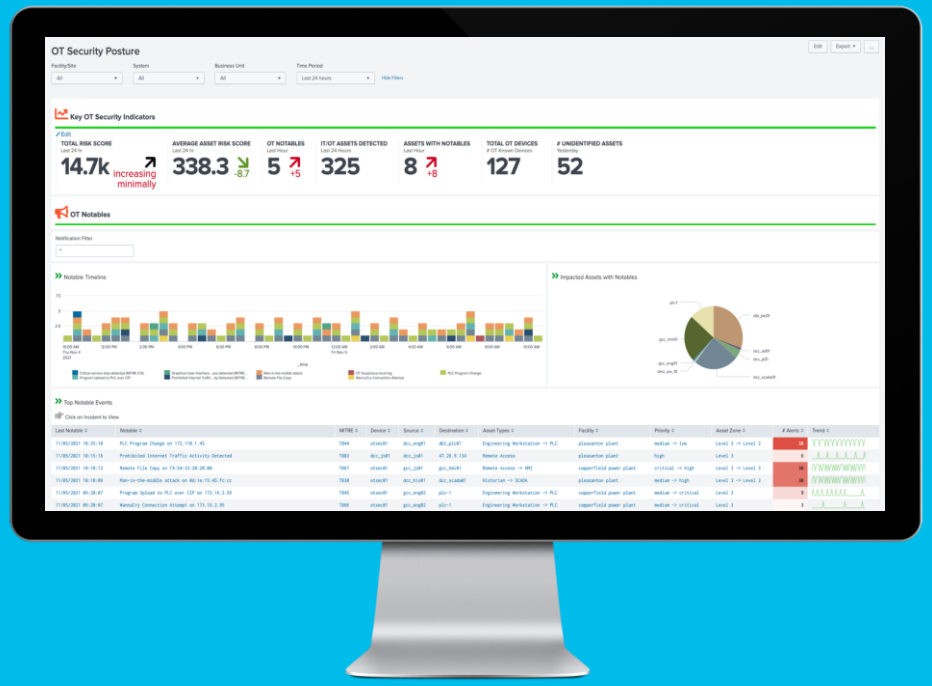
of respondents agreed with the statement, "In the next 2 years, there will be significant value in having a unified cybersecurity solution for both enterprise and industrial networks". This rises to 92% among executive leadership and C-suite.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Splunk OT Security

Break silos between OT & IT domains with cross-domain detection and remediation

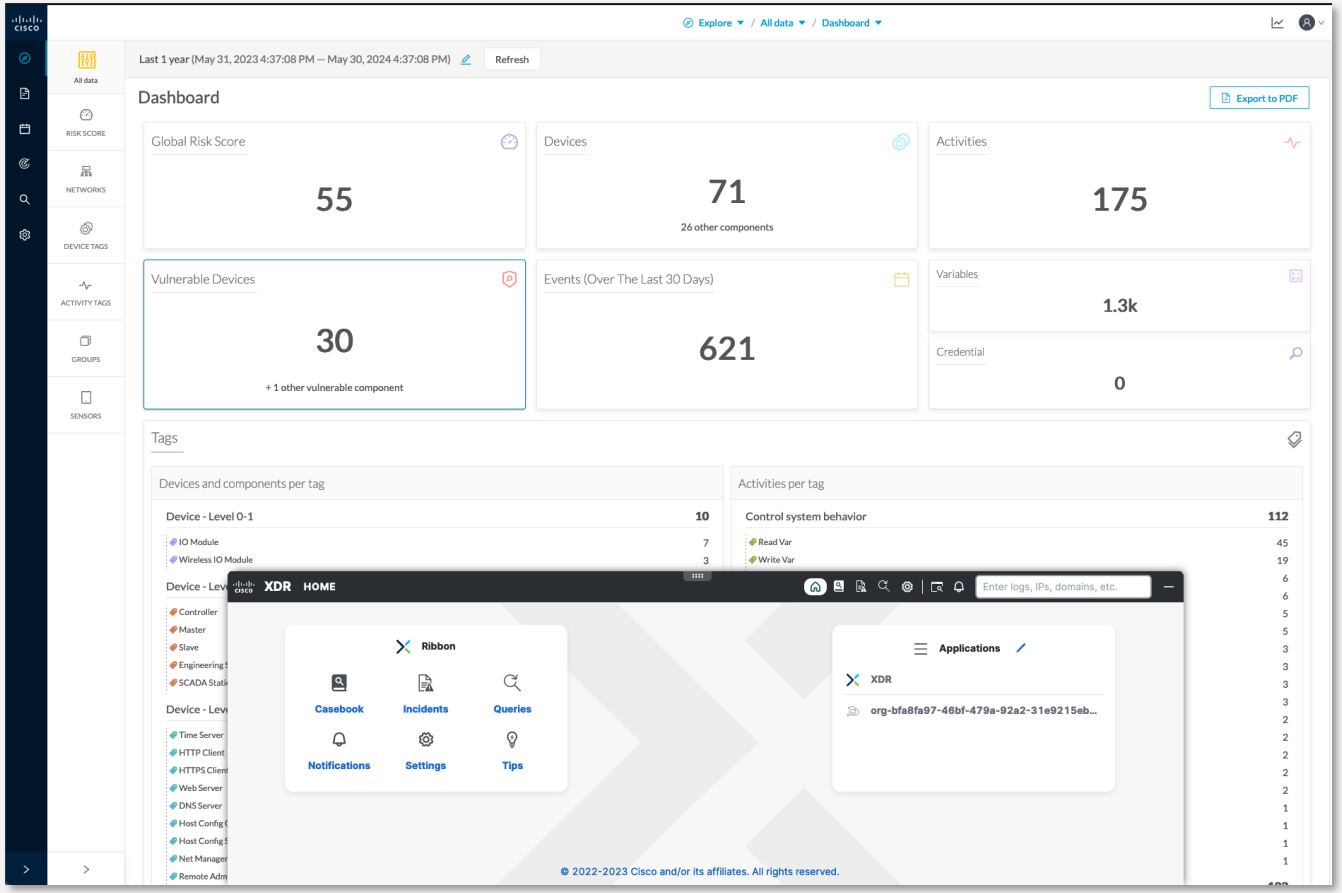
- OT Asset Investigator
- NERC-CIP compliance reports and MITRE ATT&CK ICS correlation rules
- OT Perimeter Monitoring
- Risk Based Alerting
- OT Baselining
- OT Use Case Library
- Unified IT/OT security events management in Splunk SIEM



Improve threat detection, incident investigation, and response **across OT & IT domains** with telemetry from Cisco and 3rd party security products

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Investigate & Respond to Threats with Cisco XDR



Leverage Cyber Vision Observables to:

Create and **manage incidents** in Cisco XDR

Create and **orchestrate playbooks**

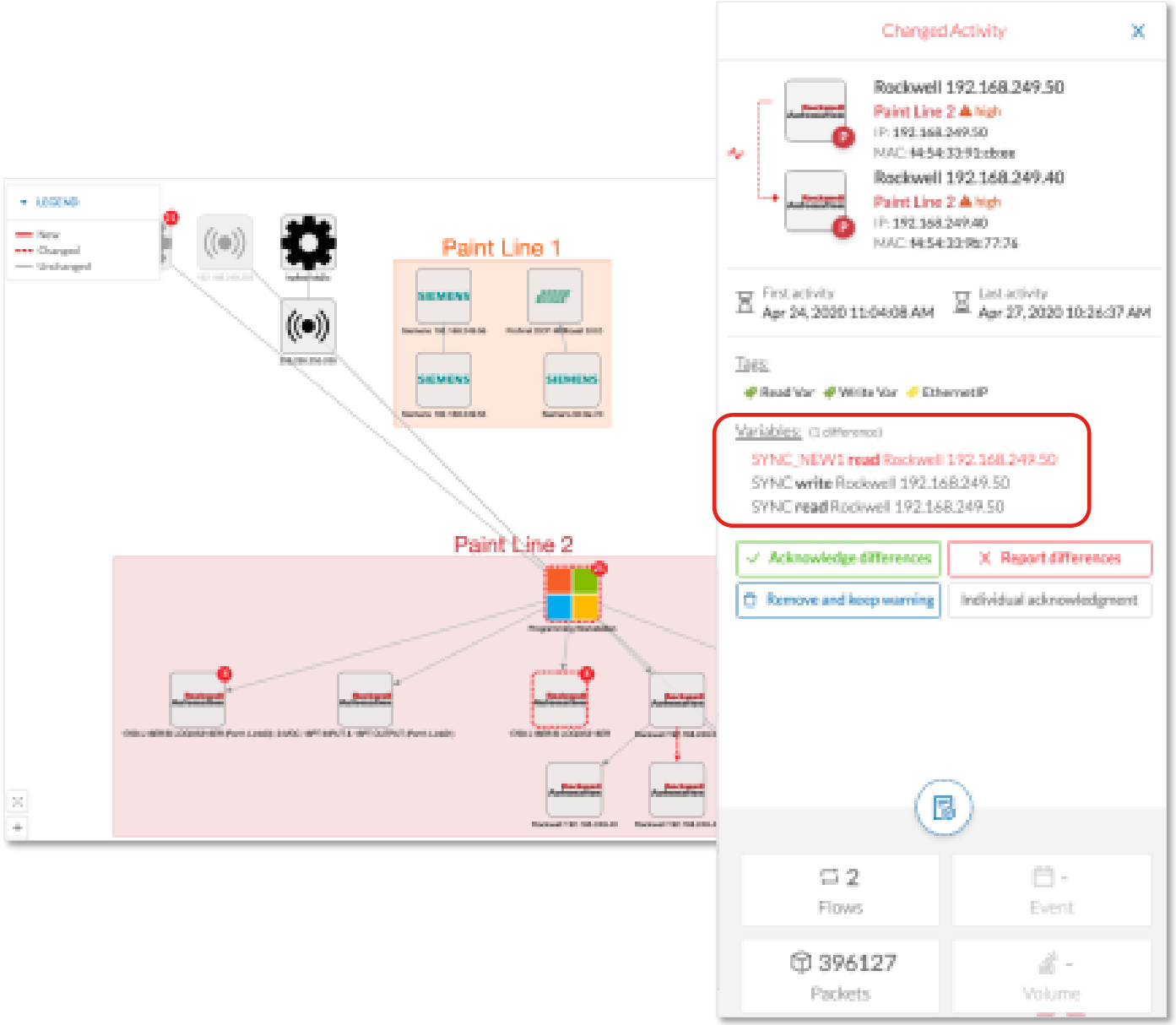
Launch investigations in Talos, Umbrella, Secure Endpoint, Threat Grid, etc.

XDR Ribbon in Cyber Vision for investigations and remediation orchestration

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cyber Vision anomaly detection: Baselines

- Detect deviations from baselines
  - New and modified assets
  - New activities between assets
  - Variable changes
  - Program modifications
- Multiple baselines for multiple states
  - Reduces false positives
- Response options
  - Acknowledge to modify the baseline
  - Report to provide context in investigations
- Send events to firewall, SIEM, etc., to respond



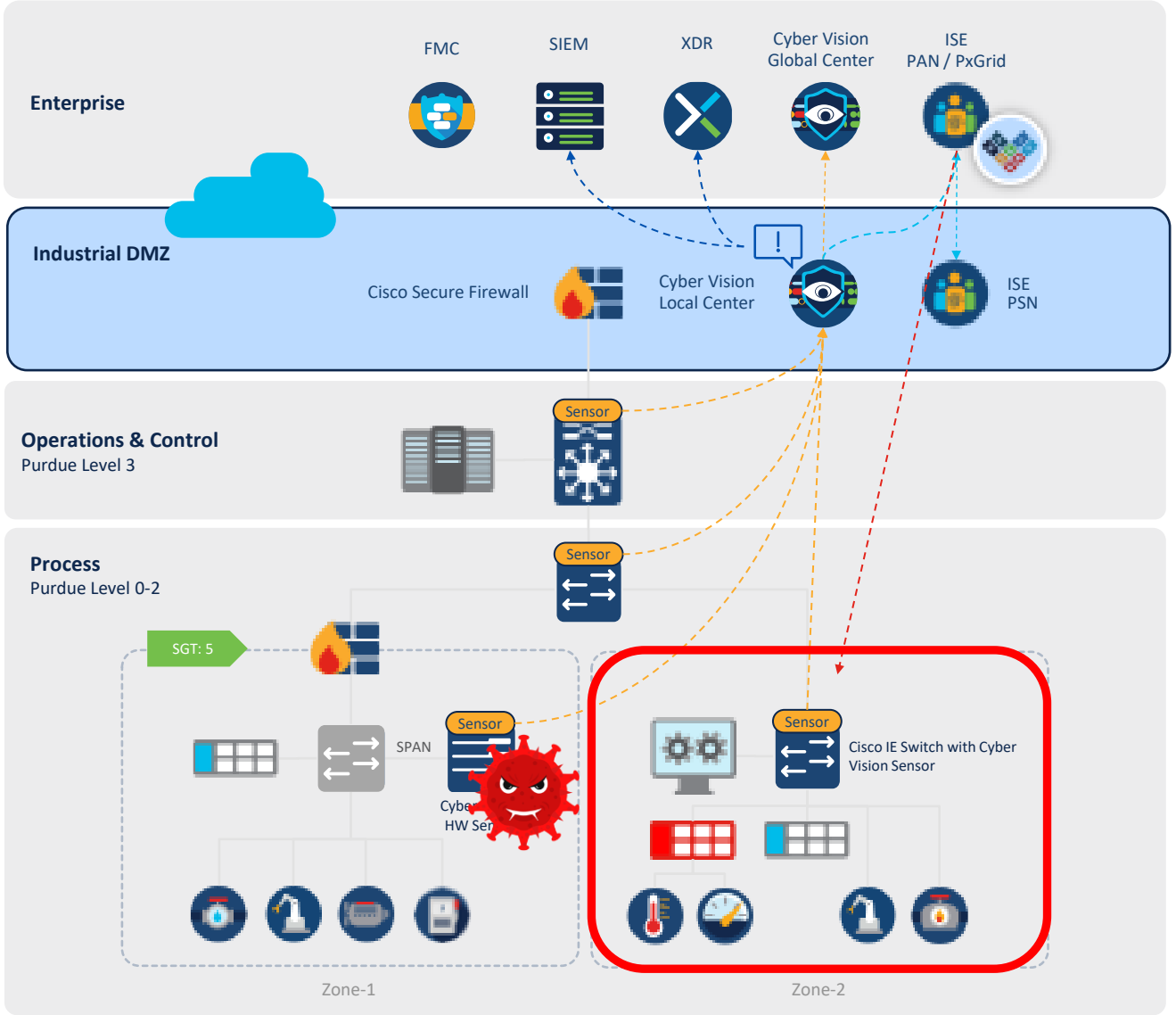
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cyber Vision integrates with your existing security platforms

Access Control	Firewalls	CMDB	SOC
CISCO ISE	CISCO Firepower NGFW	servicenow	CISCO Threat Response
	FORTINET	bmc REMEDY	IBM QRadar
	paloalto NETWORKS		splunk>
			RSA SECURITY
			ALIEN VAULT
			McAfee Together is power.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Let’s put everything together



1. CyberVision discovers industrial assets and communications and groups it into Zones.
2. CyberVision context is shared with ISE.
3. Components are dynamically classified in SGTs via group assignment directly from CyberVision
4. Deploy segmentation with confidence once you are comfortable with the observed network behavior
5. CyberVision or other analytics tools raise alarms on endpoint behavior anomalies and threat detection.
6. Investigate in Splunk, XDR, or other SOC tools.
7. ISE can trigger quarantine of offending asset.

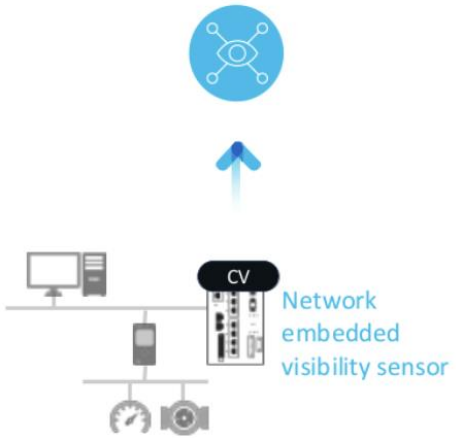
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enabling a comprehensive OT security journey

Visibility

OT Asset Visibility and Security Posture

Cisco Cyber Vision

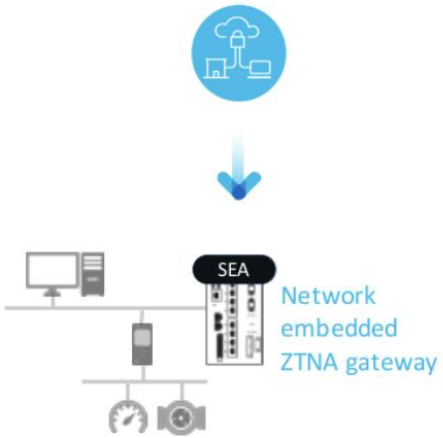


Protection

Zero Trust Security for OT

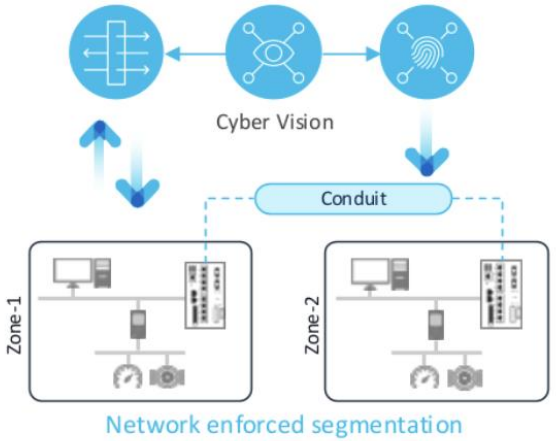
Secure remote access (ZTNA)

Cisco Secure Equipment Access



IEC 62443 zone segmentation

Cisco Secure Firewall **Cisco ISE**



Response

Cross-Domain Detection, Investigation & Response

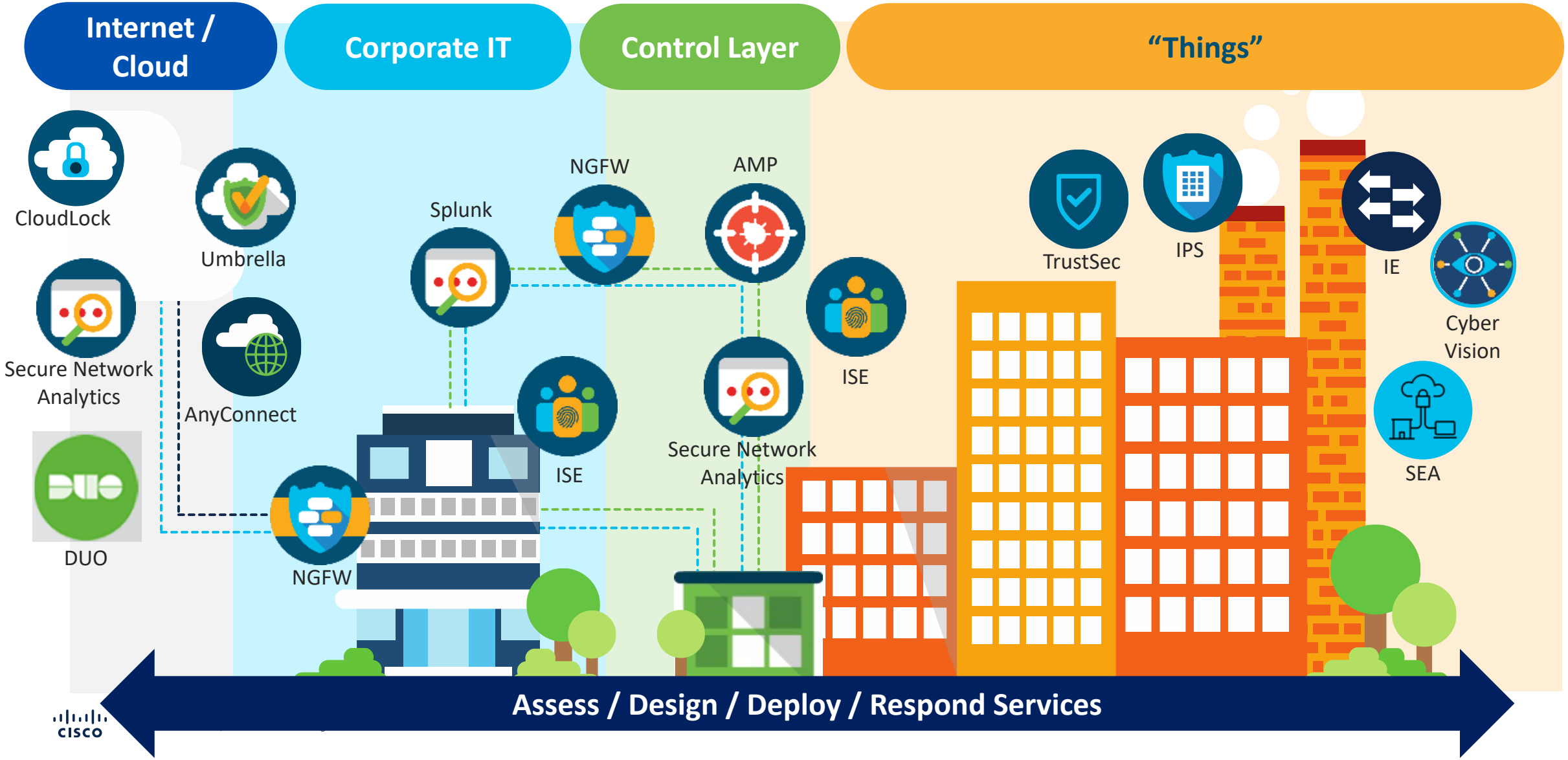
splunk> a cisco company

Visibility across the entire attack chain

Talos Threat Intelligence + Talos Incident Response

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Industrial Security: Cisco's End to End Story



Industrial IoT networking portfolio

Our solutions meet the needs of IT and operations

Industrial Ethernet switches

DIN-Rail, IP67, and Stackable Rackmount

IE3400

IE3300

IE3200

IE3100

IE3400H

IE9300

Industrial Cybersecurity

Cyber Vision, Secure Equipment Access

Industrial Wi-Fi and Ultra-reliable Wireless Backhaul

For outdoor conditions

IW9165E

IW9165D

IW9167i

IW9167E

IW9167E-HZ

Industrial Routers

Modular 4G/5G – for connecting remote and mobile assets

IR1100

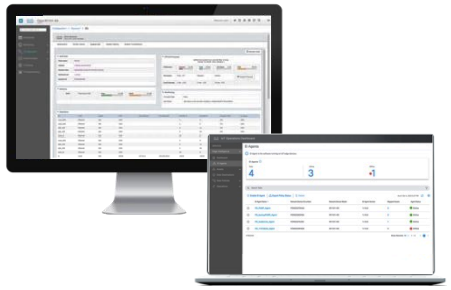
IR1800

IR8300

IR8100

Data Control and Exchange

Edge Intelligence, IOx App Hosting



Embedded Networking

Embedded routers and switches for industrial Makers

ESR6300

ESS3300

ESS9300

Management and Automation

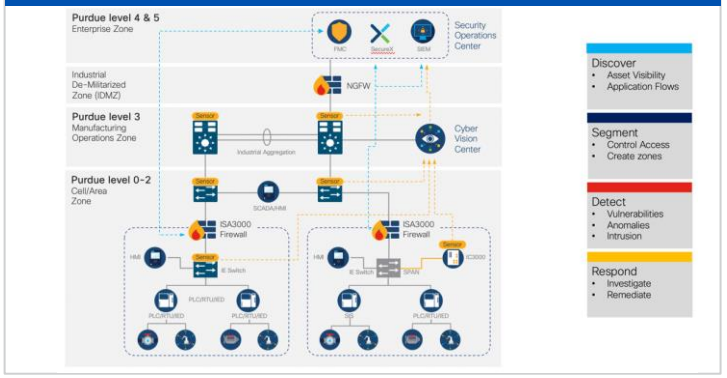
Cisco Catalyst Center, Cisco Catalyst WAN Manager, Field Network Director

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

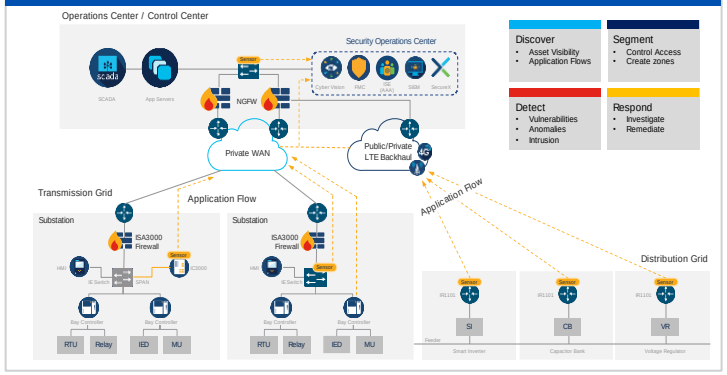
Deploy with confidence using Cisco Validated Designs

Tested to help ensure a faster and more reliable deployment

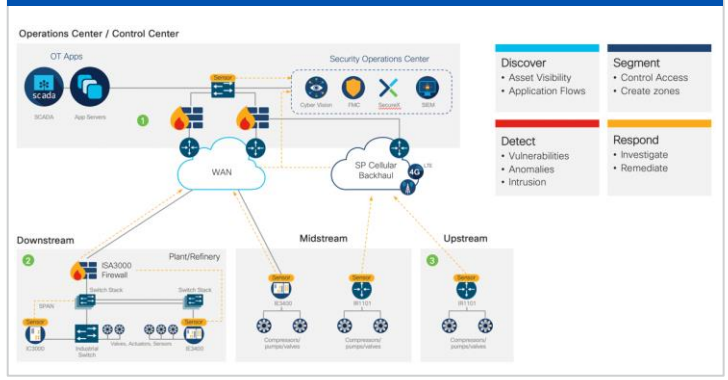
Industrial Automation



Industrial Security



Catalyst Center for Manufacturing



Use Cases

- PLC / DCS / control system connectivity
- Connected Machines
- Remote Access & troubleshooting

Key Features

- Visibility and control into lowest layers of cell area zone
- Segmentation, identity, and policy
- Plantwide PTP (foundation for data)
- SDN Ready for ease of use

Outcomes

- Improve OEE and asset utilization
- Reduce product defects
- Reduce risk from cybersecurity threats
- Drive innovation through end-to-end connectivity

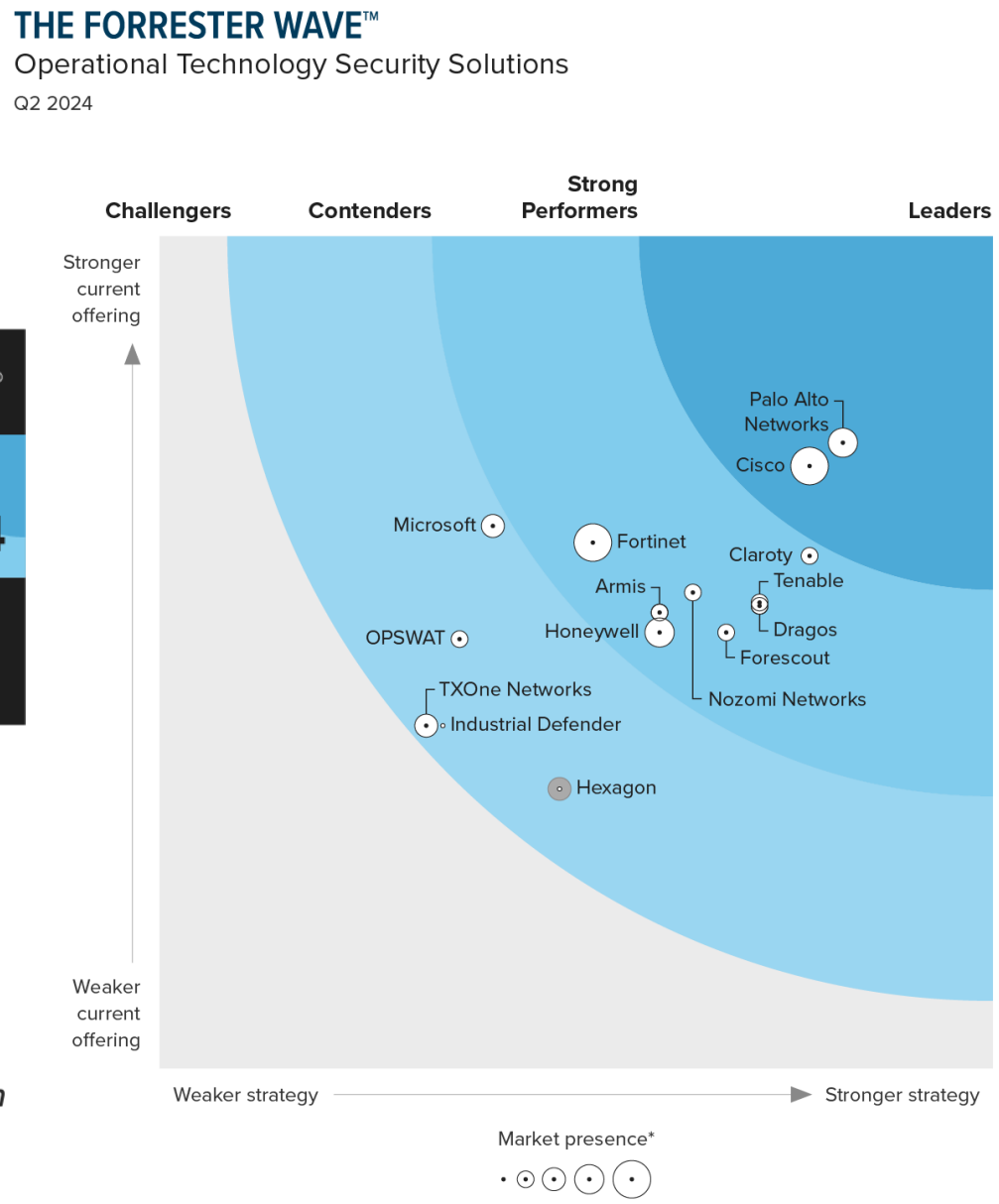
Proven to work with: Rockwell Automation, SIEMENS, Schneider Electric, MITSUBISHI ELECTRIC, PROFINET, Modbus, EtherNet/IP, CC-Link IE

Cisco Named "Industrial IoT Company of the Year" in 9th Annual IoT Breakthrough Awards Program

Cisco Industrial Threat Defense is a comprehensive solution to protect, detect,
and remediate across IT and OT environments.

Cisco envisions **the network as the fabric** to secure OT at scale and is building a comprehensive platform to **unify IT and OT domains**.

- Forrester Research

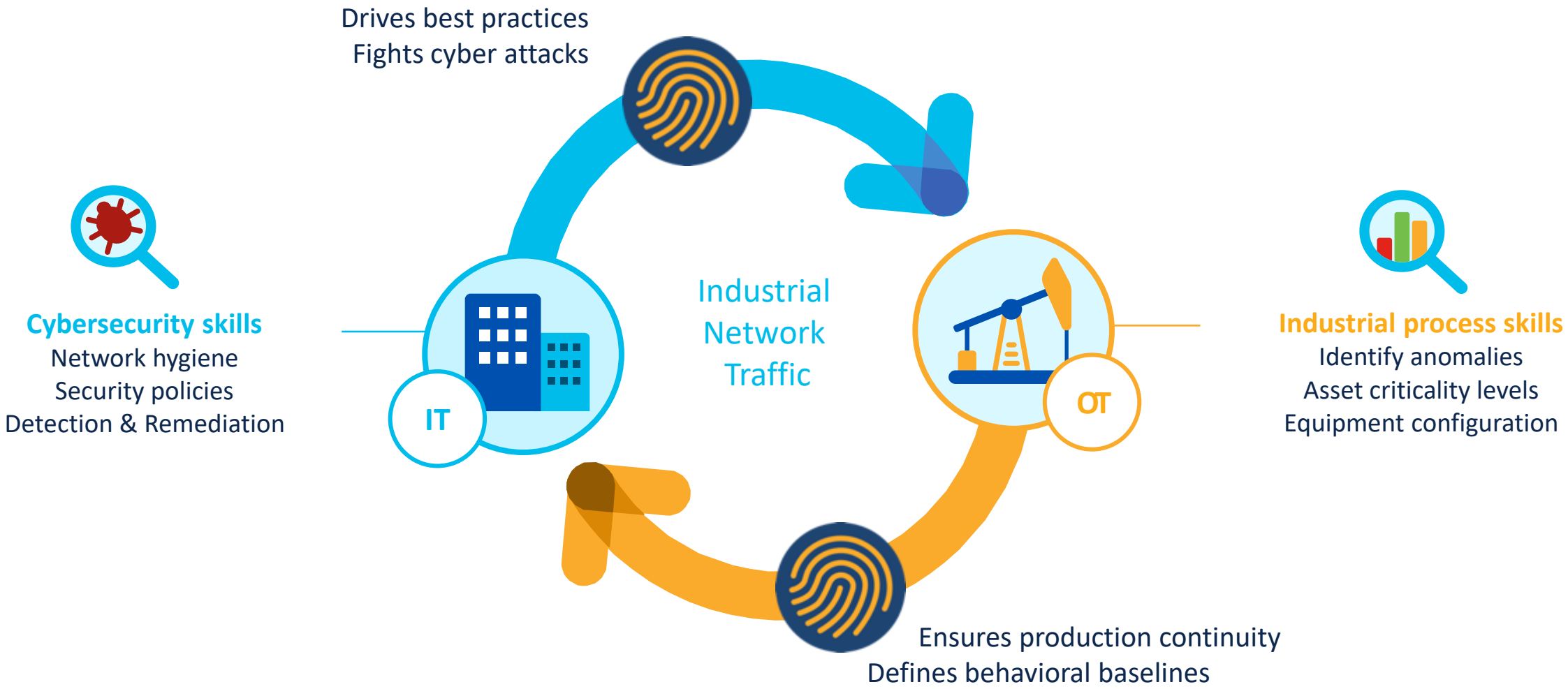


*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IT-OT collaboration is vital for securing ICS



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CISCO

Closing the Cybersecurity Gap

McClone INSURANCE

Legal, Contractual, and Insurance Safeguards

Presented by: Dillon Holewinski & Paul Kaster, JD

Today's Agenda

2025

Cyber risks are increasing, impacting businesses of all sizes.

Today, we'll explore:

- Cyber claims
- Manufacturing trends
- Legal risks
- Insurance as a last line of defense

2024 Travelers Risk Index

62% of business leaders

cite cyber as their top concern, surpassing other risks

24% of businesses

experienced a cyber event, with **36%** reporting a security breach and **27%** dealing with ransomware

30% of companies

do not have cyber insurance, though **80%** believe it's critical

© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

WHAT WE'RE SEEING

Cyber Claim Trends

While ransomware and business email compromise (BEC) lead the way, we're also seeing:

53%

of claims are due to ransomware, with payouts reaching $50 million

56%

of BEC claims occurred in the last three years

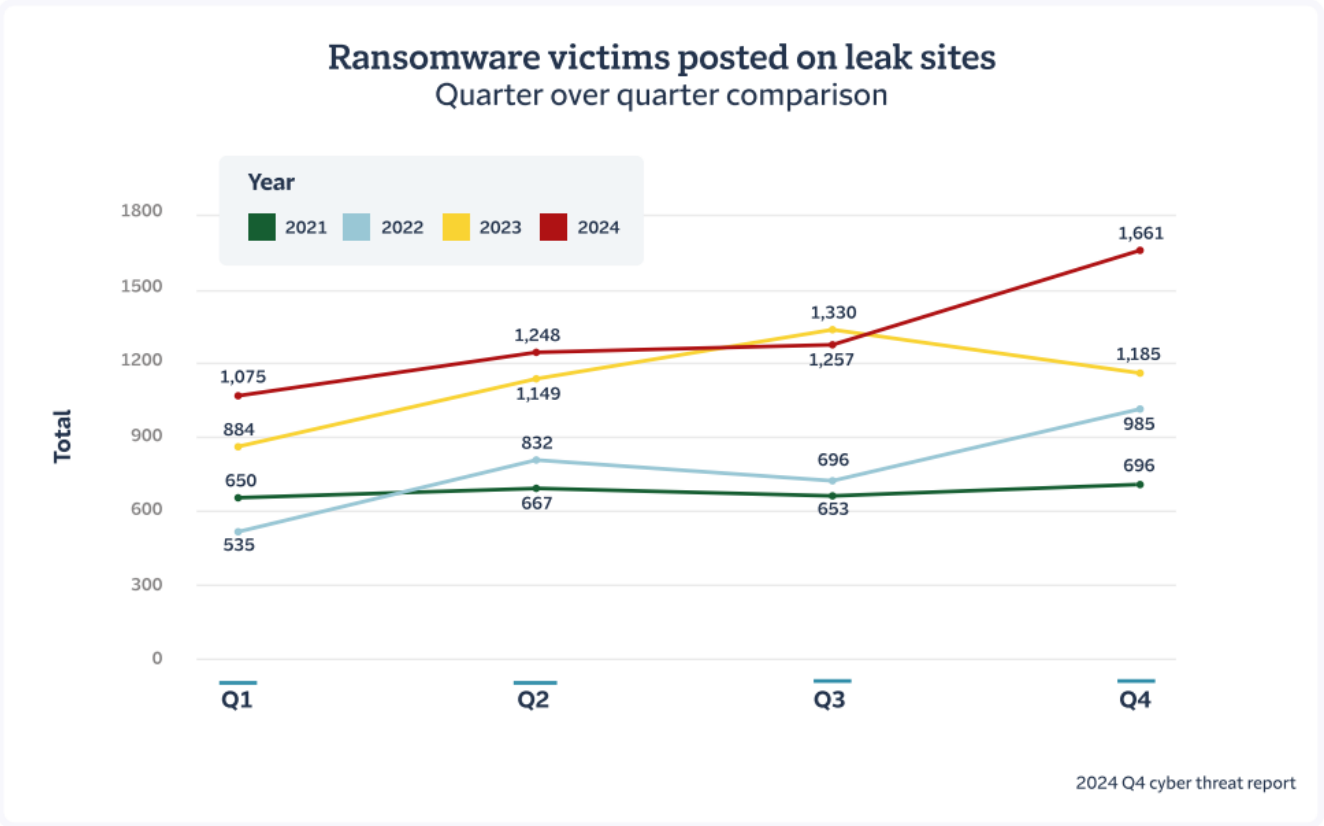
© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

out permission.

Record-Breaking Ransomware Activity in Q4 2024

*For 2024 overall, ransomware attack victims reached 5,243, a **15% increase from 2023***

*Globally, these attacks are believed to have exposed over **195 million records**, and ransomware payments totaled approximately **$813 million***



© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

Trends in Manufacturing

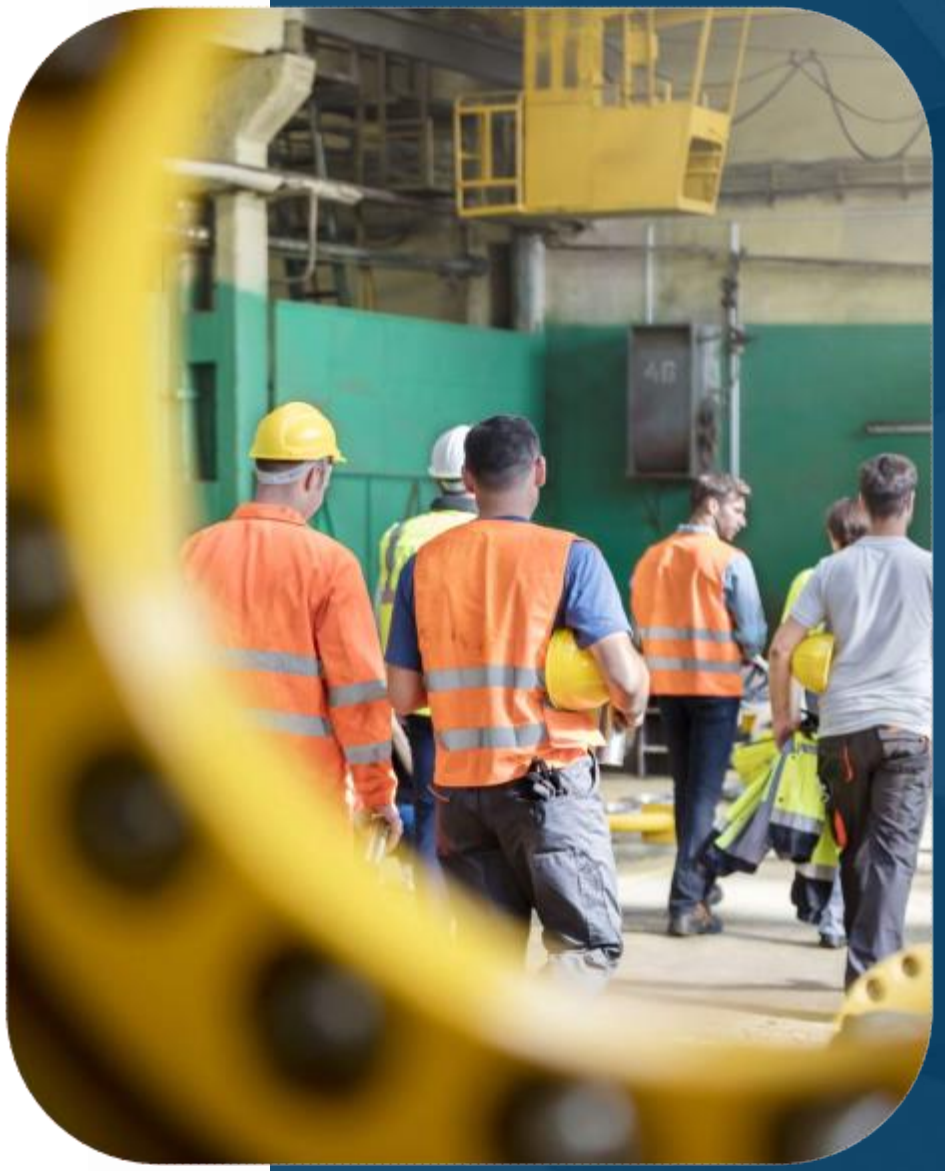
Manufacturing is now the top-targeted industry for ransomware attacks, surpassing financial services

- *Ransomware attacks in manufacturing increased by 1,177% between Q1 2021 and Q1 2023*

Increase in IoT vulnerabilities: More connected devices lead to expanded attack surfaces

Rise in third-party risk: Manufacturing companies heavily depend on suppliers and partners, increasing exposure to supply chain attacks

Regulatory pressures are increasing: Compliance with data protection laws and cybersecurity standards is becoming more complex



© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

FINANCIAL IMPACT

Understanding the Fallout

- Costs vary from $1,000 to over $100M
- Average ransomware recovery costs for small and medium enterprises: $432K
- Business email compromise costs average $101K

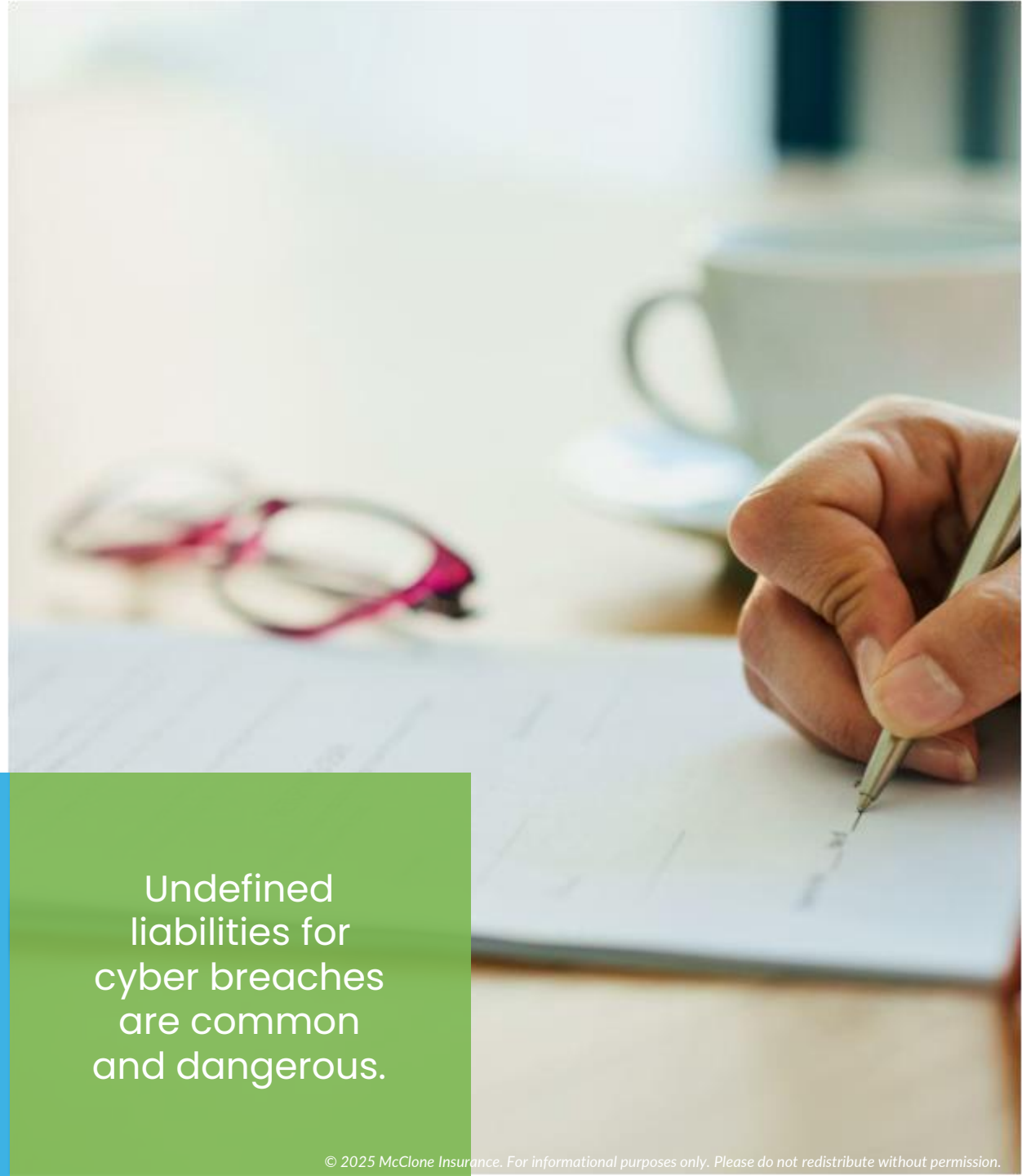
Strategic. T

© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

CYBERSECURITY

Hidden Legal Risks

Non-compliance with regulations, slow incident response, intellectual property theft, breaches of contractual obligations, and failure to protect employee data can lead to penalties, litigation, or loss of sensitive information.



Many contracts fail to address cybersecurity risks.

Third-party vendors and client contracts can introduce additional risk.

Undefined liabilities for cyber breaches are common and dangerous.

© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

MANAGE CYBER RISK

How Contracts Can Help

Include specific cybersecurity clauses in vendor and partner contracts.

Define responsibilities for data breaches, financial losses, and response.

Ensure vendors follow security best practices to minimize exposure.

© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

Let’s guess the average downtime for a cyber incident…

22 days

© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

The Last Line of Defense

- The reality is that cyber insurance is there to help businesses recover from incidents when they do happen.
- Insurance covers costs that go beyond preventive measures: legal defense, business interruption, crisis response, and recovery expenses.
- Insurance ensures a financial safety net after an attack.

© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

Industry Benchmarks

Limit Benchmarks

While recommended limits will vary by the specifics of each risk, these benchmarks approximate the Smart Cyber Insurance coverage purchased by organizations grouped by gross annual revenue. (Corvus offers limits of up to $5m for primary and excess Cyber policies)

Annual Revenue	Typical Limit Purchased
Up to $50m	$2m
$50m - $200m	$2m
$200m - $300m	$3m
$300m+*	$5m

**Data reflects Corvus primary policies only. Policyholders may be achieving aggregate limits greater than $5 million through excess policies.*

© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

FINAL THOUGHTS

Build a Holistic Strategy

Regularly review and update cybersecurity practices & policies.

Include cybersecurity provisions in contracts with vendors & partners.

Secure insurance coverage to manage disruption & financial losses.

© 2025 McClone Insurance. For informational purposes only. Please do not redistribute without permission.

Any Questions?

McClone INSURANCE

Sources:

NetDiligence Cyber Claims Study 2024 Report

Insurance Journal Article: Cyber Hits All-Time High Concern for Business Leaders, Says Travelers Risk Index

Q4 Travelers' Cyber Threat Report: Ransomware Goes Full Scale

CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

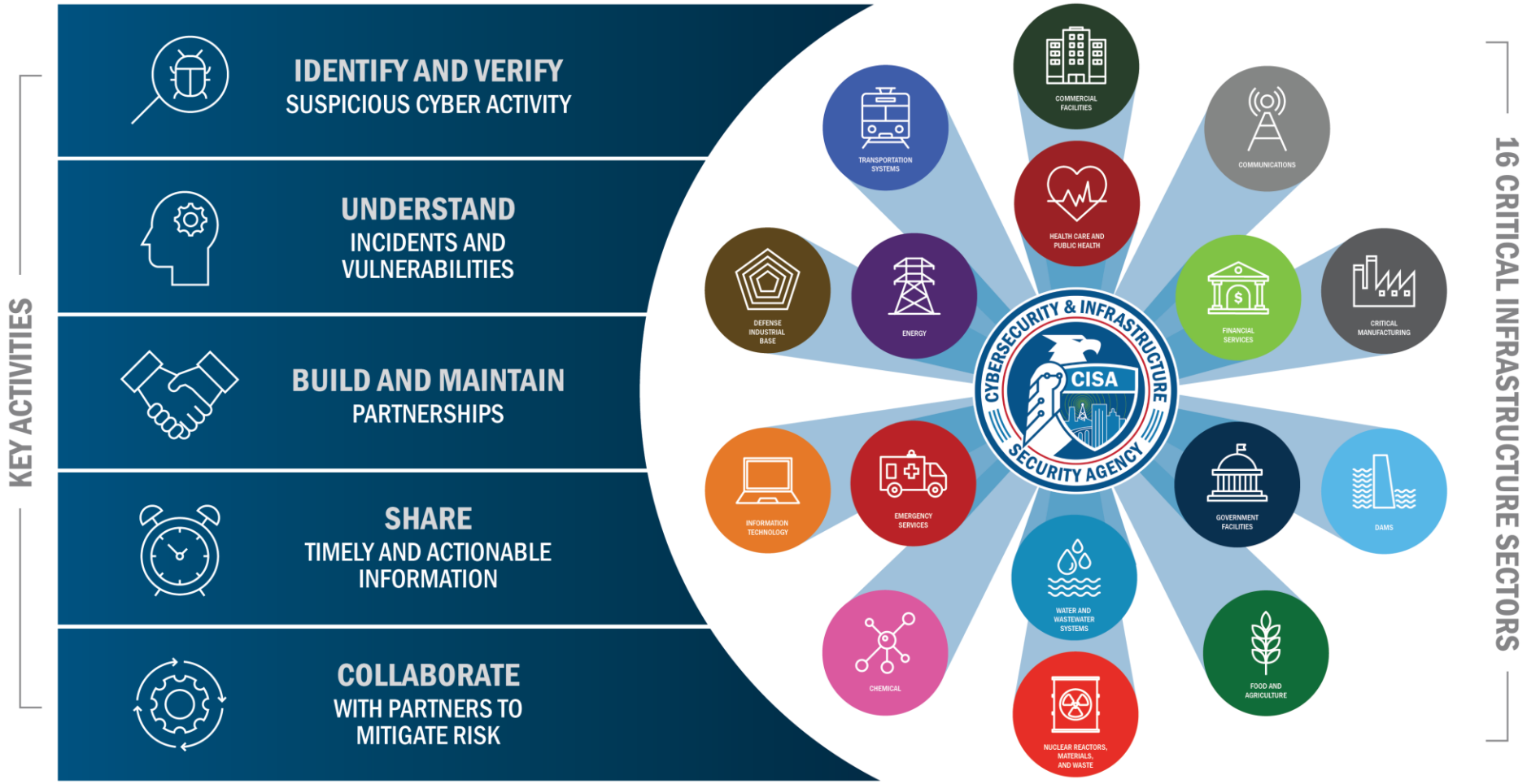
VISION

Secure and resilient infrastructure for the American people.

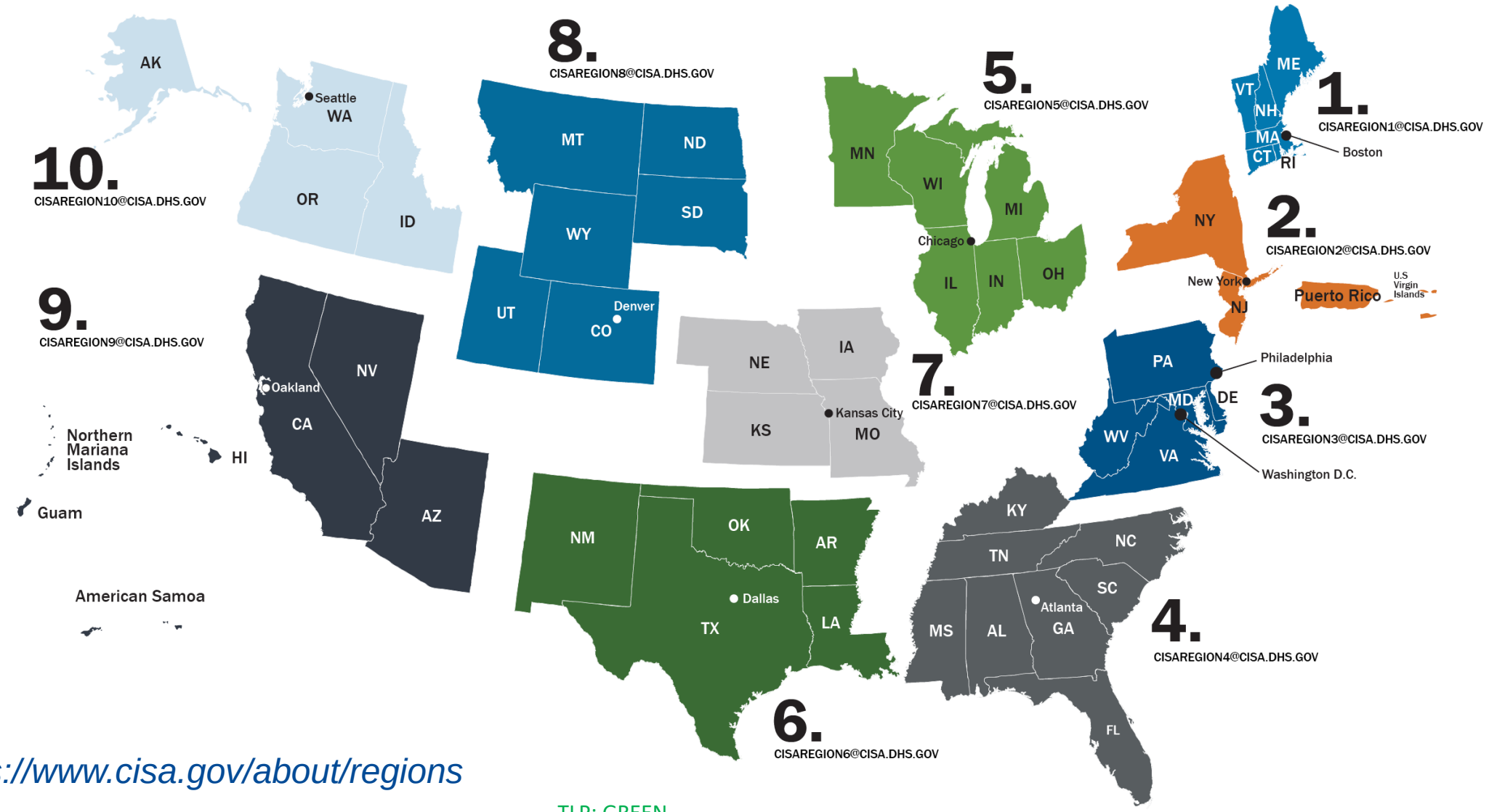
MISSION

Lead the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure.

Serving Critical Infrastructure



CISA Regions



1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA

https://www.cisa.gov/about/regions

TLP: GREEN

CISA Field Resources

Cybersecurity Advisors

- Assessments
- Working group collaboration
- Best Practices private-public
- Incident assistance coordination

Protective Security Advisors

- Coordinate vulnerability assessments, training, and other DHS CISA products and services
- Security Assessment at First Entry assess the current security posture
- Infrastructure Survey Tool (IST) is a web-based vulnerability survey tool

Emergency Communications Coordinator

- Supports and promotes the nationwide improvement of emergency communications capabilities
- Provides coordination and support in times of threat, disruption, or attack.

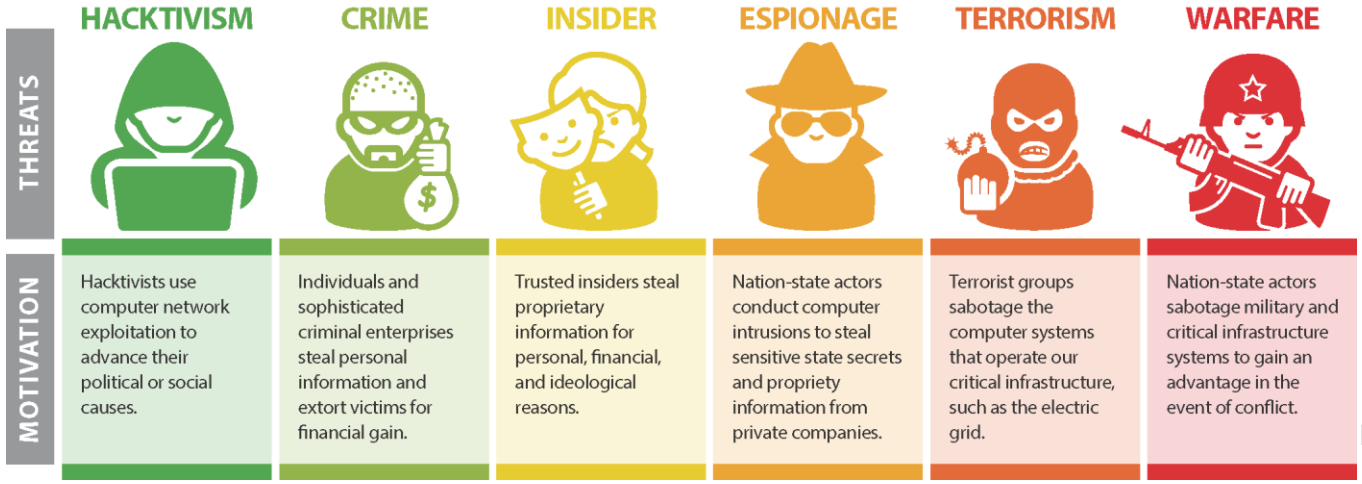
Chemical Security Inspector

- Manage the voluntary ChemLock program
- Assist chemical facilities with enhancing their chemical security posture

CYBER THREATS

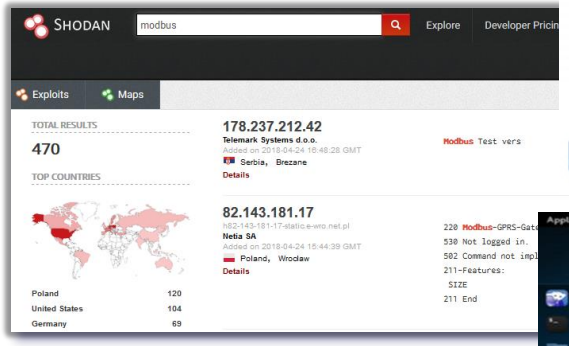
Cyber Threats

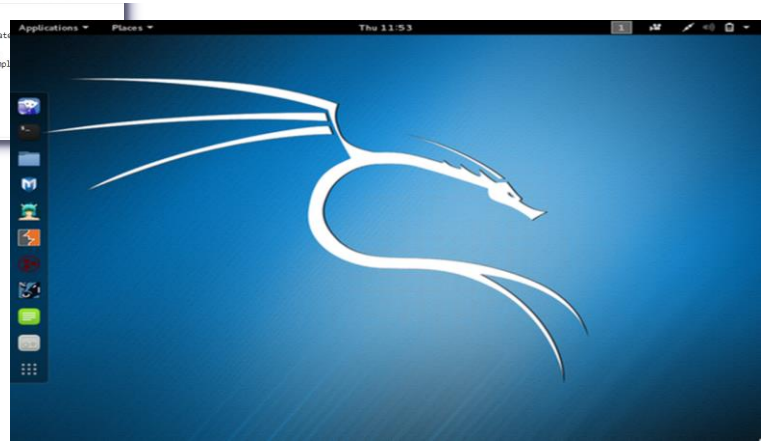
- "Outsiders"
  - Hackers (looking for financial gain)
  - Hacktivists (on ideological mission)
  - Organized crime groups
  - Terrorists
  - Competitors
  - Nation states
- "Insiders"
  - Current/former employees
  - Current/former service providers, consultants, contractors
  - Suppliers/customers
  - Business partners



Targeting you

- Interconnected systems are enabling threat actors.
  - Targets of opportunity
  - Paths of least resistance
- Hacking as a service (HaaS)
- Malicious tools readily available for purchase or download





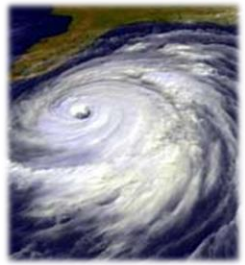
SECURING OUR WORLD

Bring “the Business” into Cybersecurity

Actions of People

Systems and Technology Failures

Failed Internal Processes



External Events

In highly complex, Internet-dependent, technically enabled organizations, cybersecurity is a **business** problem.

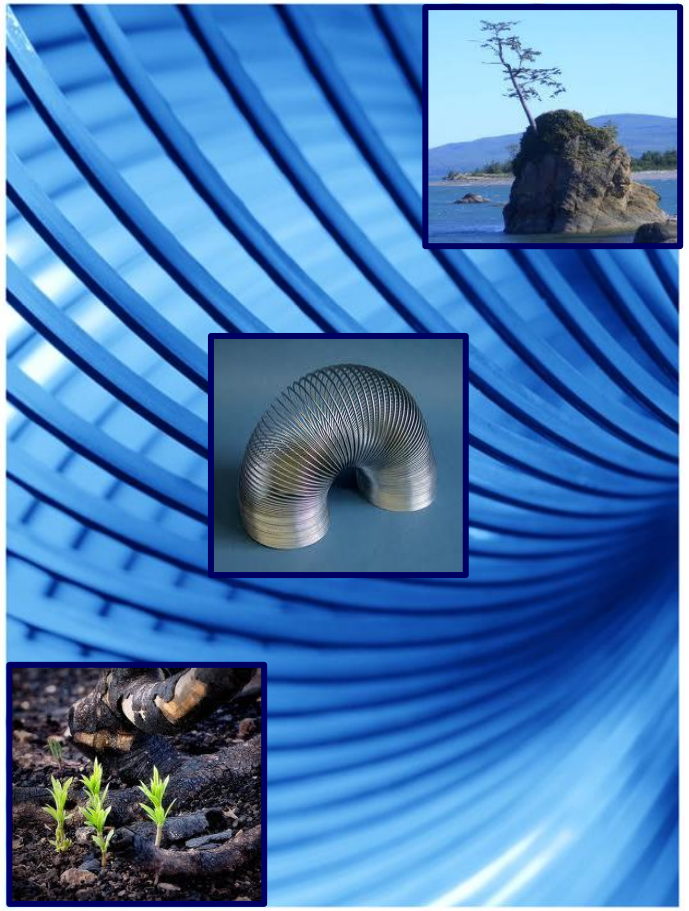
Cyber impacts/risks are not just disruptions of technology, but of the **business missions** that rely on the supporting technology.

Approaching cybersecurity as an **operational business risk brings** cybersecurity into the organization’s risk management process.

Operational Resilience

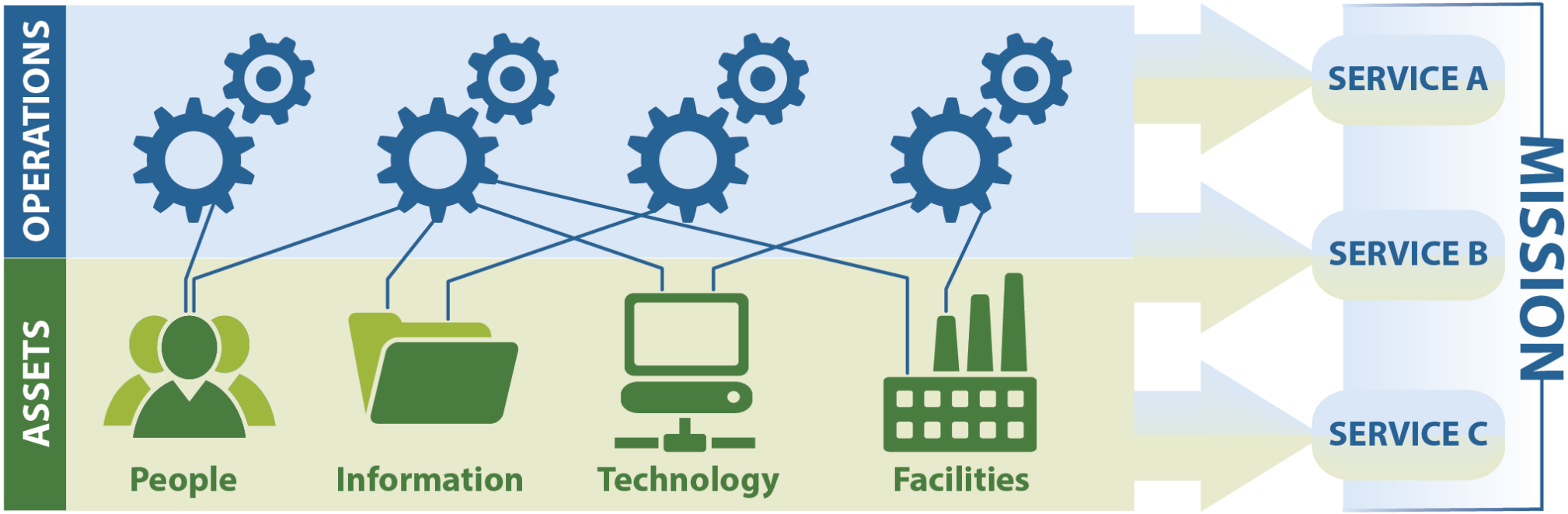
The emergent property of an organization that allows it to:

- prevent disruptions from occurring and,
- quickly respond and recover from a disruption in its most critical business processes.

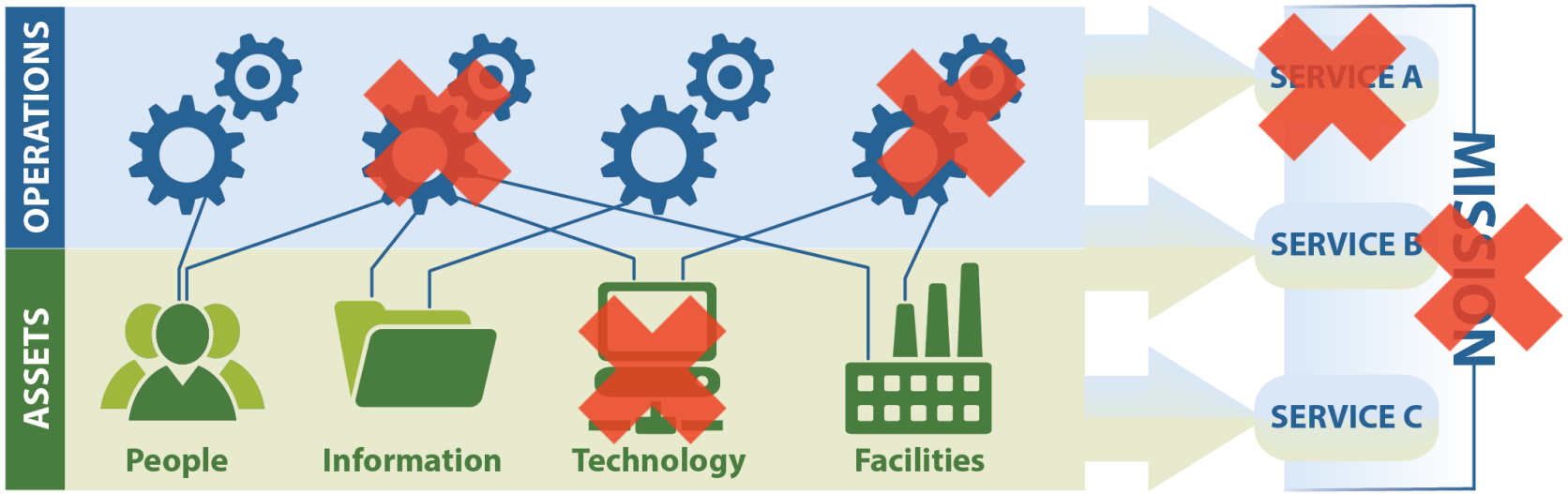


Conduct a Business Impact Analysis

An organization uses its **assets (people, information, technology, and facilities)** to perform **productive activities** to provide operational **services** and accomplish the organization's **mission.**



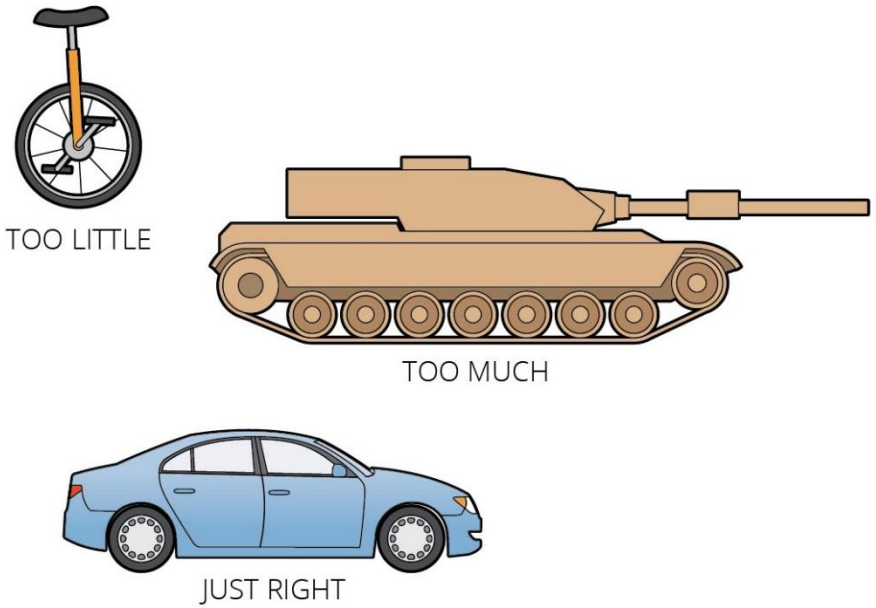
Disruptions Leading to Mission Failure



Disruption of assets can lead to a disruption of operations which can lead to a disruption of business processes. This in turn can lead to mission failure.

A Balanced Approach

Risk tolerance is balancing risk and cost.



Resilience is finding the ***just-right*** level of risk investment.

Cyber Program Preventative Practices

Defense-in-Depth

Adopt a layered approach to cyber protection. Utilize multiple resources that perform similar functions.

Educate

Provide cyber security awareness training to all employees.

Password Policy

Maintain a strong password policy. The policy should illustrate the importance of password security. Passphrase is better than password. Length beats complexity. 16 or more characters with one special character allows for a passphrase.

Enable Multi-Factor Authentication Everywhere Possible

Enable the 2FA/MFA capability on everything. This includes email, network access, remote access, and web-based applications.

Patch

Keep all systems patched with the latest security updates. Computers, servers, and network equipment

Vulnerability scans

Regularly scan internal and external systems for vulnerabilities.

Segmentation

Segment the network to isolate systems that do not need to talk to other systems.

Cyber Program Response Practices

Incident Response Plan (IRP)

Develop and regularly test an IRP as part of your overall Continuity of Operations Plan/Business Continuity Plan.

Logging

Enable logging on every system including network equipment. Logs should be immutable and stored for a minimum of 30-days.

Backups

Backup key systems regularly and keep at least one backup of your data offsite in a secure location. Ensure that backups are immutable.

CISA SERVICES

Sampling of CISA Services

- Assessments & Evaluations
  - Cybersecurity Performance Goals
  - Vulnerability Scanning & Web Application Scanning
  - Cyber Resilience Reviews
  - External Dependencies Management Assessment
  - Cyber Security Evaluation Tool (CSET™)
  - Other technical services (e.g. pen testing, Validated Architecture Design Reviews)
- Preparedness Activities
  - Cyber Protective Visits and Introductory Visits
  - Cybersecurity Alerts & Advisories
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber, Physical, Convergence Tabletop Exercises and "Playbooks"
  - Information Products and Recommended Practices
  - Workshops (Cyber Resilience, Cyber Incident Management, External Dependency Management, etc.)
- Partnership Development
  - Informational Exchanges
  - Working Group Support
  - Joint Cyber Defense Collaborative (JCDC)
- Strategic Messaging
  - Resource Briefings
  - Keynotes and Panels
  - Threat Briefings
  - Topic Specifics (e.g., CAM, SCRM, ICS, etc.)
- Incident Response Assistance
  - Incident Coordination
  - Remote / *On-Site Assistance
  - Malware Analysis
  - Entity Notifications
    - Vulnerability Notifications
    - Cyber threat activity notifications

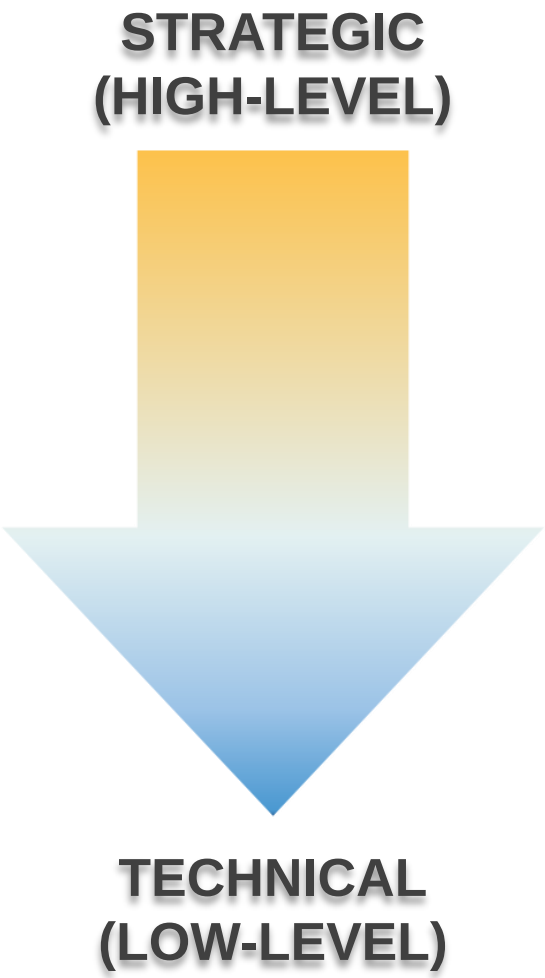
Range of Cybersecurity Assessments

Regional Resources:

- Cybersecurity Evaluations Tool (Strategic)
- Cross-sector Cybersecurity Performance Goals (Strategic)
- Ransomware Readiness Assessment (Strategic)
- Cyber Resilience Review (Strategic)
- Tabletop Exercises (Strategic/Technical)

National Resources:

- Vulnerability Scanning / Hygiene (Technical)
- Web Applications Scanning (Technical)
- Validated Architecture Design Review (Technical)
- Remote Penetration Test (Technical)
- Risk and Vulnerability Assessment (Technical)



Vulnerablity Scanning

Known exploitable vulnerabilities are easy access for attackers, with **incidents averaging $100,000 in damages** for small and medium businesses.

CISA's free vulnerability scanning service helps **identify exposed assets and exploitable vulnerabilities** and is proven to reduce risk for participating organizations.

Avoid costly disruptions with early detection and action. Through weekly reports and timely alerts, we will help you **act before others take advantage**.

BY THE NUMBERS

- **7,200+** current customers nationwide
- **Over 3 Million** vulnerabilities found and fixed
- On average a **40% reduction in risk and exposure** by newly enrolled customers in their first 12 months
- Most enrollees see improvements within the first **90 days**

GETTING STARTED

Email vulnerability@cisa.dhs.gov
Subject: "Requesting Vulnerability Scanning Services"

Known Exploited Vulnerabilities (KEV)

KNOWN EXPLOITED VULNERABILITIES CATALOG

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

Subscribe to the KEV Catalog Updates

Stay up to date on the latest known exploited vulnerabilities.

SUBSCRIBE NOW

Show 10 entries

Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date
CVE-2022-40684	Fortinet	Multiple Products	Fortinet Multiple Products Authentication Bypass Vulnerability	2022-10-11	Fortinet FortiOS, FortiProxy, and FortiSwitchManager contain an authentication bypass vulnerability that could allow an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS	Apply updates per vendor instructions.	2022-11-01

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Cybersecurity Alerts & Advisories

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About | REPORT A CYBER ISSUE

Home / News & Events

SHARE:

Filters

What are you looking for?

Sort by (optional)

Release Date

APPLY

Advisory Type

- [ ] Alert
- [ ] Analysis Report
- [x] Cybersecurity Advisory
- [ ] ICS Advisory
- [ ] ICS Medical Advisory
- [ ] ICS Alert

Release Year

Reset

Cybersecurity Alerts & Advisories

View Cybersecurity Advisories Only

Filters: Cybersecurity Advisory ×

Clear all filters

JUN 14, 2023 ■ CYBERSECURITY ADVISORY | AA23-165A
Understanding Ransomware Threat Actors: LockBit

JUN 07, 2023 ■ CYBERSECURITY ADVISORY | AA23-158A
#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

MAY 24, 2023 ■ CYBERSECURITY ADVISORY | AA23-144A
People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

MAY 16, 2023 ■ CYBERSECURITY ADVISORY | AA23-136A
#StopRansomware: BianLian Ransomware Group

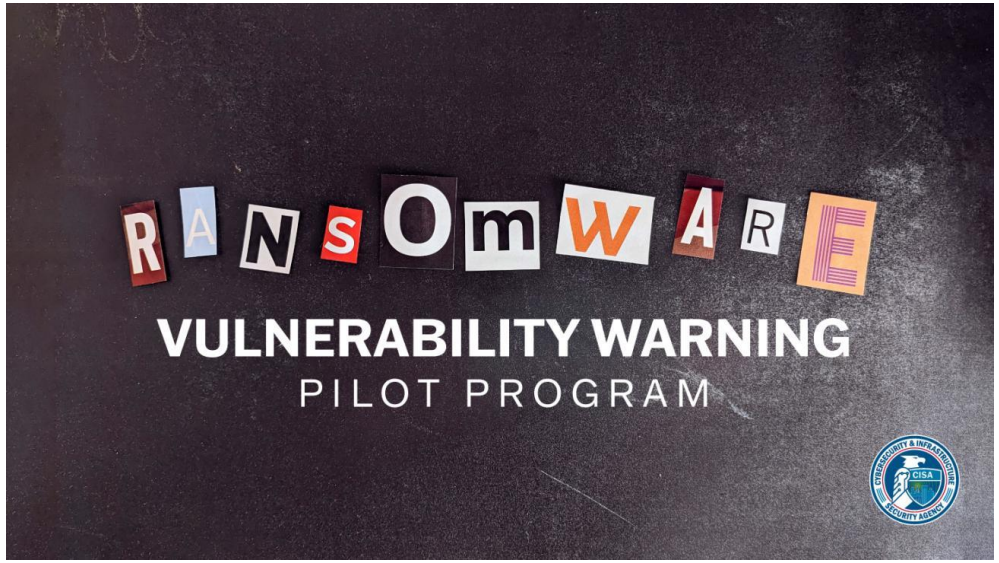
SUBSCRIBE TO ALERTS

Sign up to receive automatic e-mail updates from CISA.gov to keep up with breaking news and information about our various topic areas.

SUBSCRIBE

https://www.cisa.gov/news-events

Pre-Ransomware & Vulnerability Notification



Information from CISA about Pre-Ransomware Notices
Information from CISA re: Ransomware and Vulnerability Warning Pilot

*** All organizations/businesses are included in this. At CISA, it is our duty to warn, and we may call you. To verify our information, call 1-844-Say-CISA or email SayCISA@cisa.dhs.gov

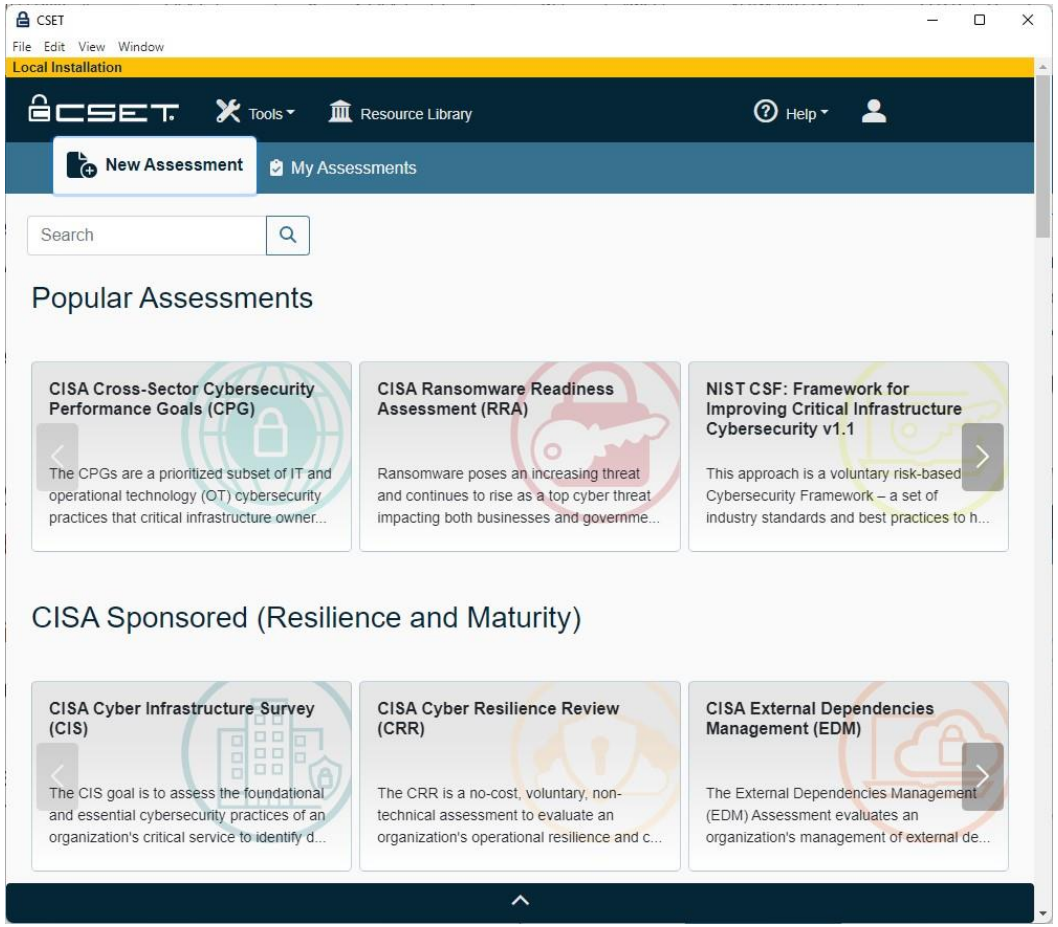
We will never ask you for information or payment other than an out of band email address (we wouldn't want to tip off a threat actor who may be in your system – create a separate email address such as companyname@gmail.com), to send the information we have about the potential vulnerability or exploited vulnerability.

REGIONAL ASSESSMENTS

Cyber Security Evaluation Tool (CSET)

- Stand-alone Software Application
- Self-Assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy
- Understanding of operational technology and information technology network security practices
- Ability to drill down on specific areas and issues

https://www.cisa.gov/downloading-and-installing-cset



Cross-Sector Cybersecurity Performance Goals (CPG)

The CPGs are a prioritized subset of IT and operational technology (OT) cybersecurity practices.

- 38 practices (questions), selected through industry, government, and expert consultation.
- Organized and aligned to the NIST Cybersecurity Framework (CSF).
- Report with results summary and recommended actions for each practice.

https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Ransomware Readiness Assessment (RRA)

The RRA consists of:

- 10 Goals with 48 tiered practices; 18 Basic, 16 Intermediate, 14 Advanced
- Based off CISA Cyber Essentials, Ransomware Guide and leverages the MITRE ATT&CK Framework
- Structured to give organizations a clear path for improvement
- Complete with supplemental resources for each practice

Several types of reports and charts depicting results

- Ransomware Assessment Goal Report
- Deficiency (aka. Opportunities) report highlighting weakest goals

Cyber Resilience Review (CRR)

The goal of the CRR is to assess your organization's operational resilience and cybersecurity practices.

- Derived from the CERT Resilience Management Model (CERT-RMM).

CISA Cyber Resilience Review (CRR)

The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and ...

- The CRR provides a better understanding of your organization's cybersecurity posture.
- The CRR consists of 299 interview-based questions and seeks to understand your organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity practices and behaviors across ten foundational cybersecurity domains.

https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr

NATIONAL ASSESSMENTS

Remote Penetration Test (RPT)

CISA's Remote Penetration Test (RPT) utilizes a dedicated remote team that works with the stakeholder to test internet exposure and eliminate exploitable pathways. RPTs focus only on externally accessible systems.

RPT includes:

- **External Penetration Test** assesses open ports, protocols, and services to verify whether the stakeholder network is accessible from the public domain by an unauthorized user.
- **External Web Application Test** evaluates web applications for potential exploitable vulnerabilities.
- **Phishing Assessment** tests the stakeholder's email infrastructure through carefully crafted phishing emails containing a variety of malicious payloads.
- **Open-Source Information Gathering** identifies publicly available information about the stakeholder environment that may be useful to a malicious cyber actor.

Risk and Vulnerability Assessment (RVA)

CISA's Risk and Vulnerability Assessment (RVA) combines open-source national threat and vulnerability information with data that the CISA RVA team collects through remote and onsite stakeholder assessment activities.

RVA includes:

- **Penetration Testing** to determine susceptibility to an actual attack by infiltrating the target environment, using current, real-world tactics, techniques, and procedures. Specific types of testing and assessments include network, web application, wireless, war dial, and social engineering in the form of an email phishing campaign.
- **Configuration Review** of operating system and database settings and configurations—which the team compares to industry standards, guidelines, and best practices—to identify security issues.

Validated Architecture Design Review (VADR)

CISA's Validated Architecture Design Review (VADR) is an assessment based on federal and industry standards, guidelines, and best practices. The VADR service provides an in-depth analysis of infrastructure.

VADR includes:

- **Architecture Design Review** of network architecture design and interconnectivity to internal and external systems focused on defensive strategies
- **System Configuration and Log Review** of system settings and activity to determine the susceptibility to potential attacks and baseline normal behavior to find anomalies
- **Network Traffic Analysis** utilizes a combination of open-source and commercial tools to identify anomalous communications in packet capture provided by the stakeholder to CISA, which could indicate suspicious activity or misconfiguration

OTHER RESOURCES

ICS Cybersecurity Training

ICS Training Available Through CISA:
https://www.cisa.gov/ics-training-available-through-cisa

CISA Virtual Learning Platform (VLP) Industrial Control System training (register for an account):
https://ics-training.inl.gov/learn

Cybersecurity Training Resources

CISA Learning

- https://learning.cisa.gov/login/index.php

TEEX Cyber Readiness Center

- https://teex.org/program/cybersecurity/

Cyber Career Pathways Tool

- https://niccs.us-cert.gov/workforce-development/cyber-career-pathways

The National Initiative for Cybersecurity Careers & Studies

- https://niccs.cisa.gov

Wisconsin and National Resources

WI-Cyber Response Team (WI-CRT)

- Volunteer emergency response group
- Administered by Wisconsin Emergency Management
- No-cost membership

24x7 contact number: (800) 943-0003 option 2
CRT@widma.gov
https://wem.wi.gov/response-teams/

InfraGard

- Partnership between the Federal Bureau of Investigation (FBI) and members of the public/ private sector for the protection of U.S. Critical Infrastructure.
- No-cost membership

https://www.infragard.org/
https://www.infragardnational.org/

Incident Reporting

CISA provides secure means for reporting incidents, phishing attempts, malware, and vulnerabilities.

- 24x7 contact number: (888) 282-0870
- Email: Report@cisa.gov
- Web: https://www.cisa.gov/report

FBI

- National: 1-800-CALL-FBI (National Threat Operations Center)
- Local: (414) 489-3300 (FBI Milwaukee Field Office)
- Web: fbi.gov/tips | https://www.ic3.gov/ | cywatch@fbi.gov

Region 5 – Wisconsin Team

MILWAUKEE

John Busch
Protective Security Advisor
414-369-8540
john.busch@hq.dhs.gov

Dan Honore
Cybersecurity Advisor
414-573-0899
daniel.honore@cisa.dhs.gov

MADISON

David Melby
Protective Security Advisor
608-405-2931
david.melby@cisa.dhs.gov

Bill Nash
Cybersecurity Advisor
608-590-7105
william.nash@cisa.dhs.gov

Region 5
Jim Stromberg
Emergency Communications Coordinator
james.stromberg@cisa.dhs.gov

For more information, visit **CISA.gov** or contact **central@cisa.dhs.gov**