CISCO Engage | Tech Day Milwaukee

OT Data Ingestion and Security: Splunk, Cyber Vision, and IoT

Fabrizio Guarnieri
Solution Engineer IOT

Chris Duffey
Leader – Industry Specialists

31st March 2026

Agenda

1. Trends in the market
2. OT Security Framework
3. Cyber Vision overview
4. Splunk Integration

About Fabrizio

Fabrizio Guarnieri (Fab)

Solutions Engineer in the IOT Team, based in Chicago

12 Years in Cisco in different functions (Customer delivery, Technical Presales)

Always been fascinated about technology

Global experience (Italy, Belgium, France, Poland, Australia, USA)

Cisco Live presenter

About Chris

Chris Duffey

Leader, Industry Specialists – Houston, TX

10+ Years Experience in SCADA/ICS (Dev and Cyber Security)

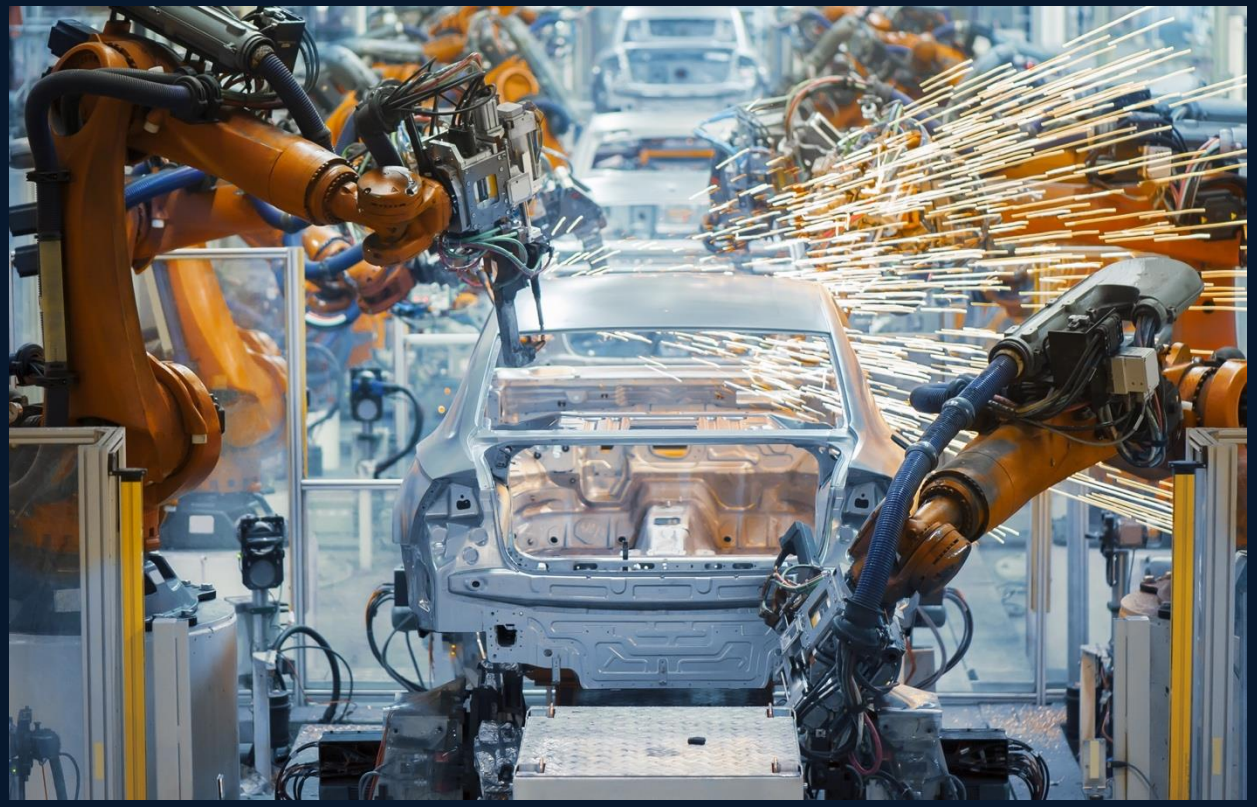
7+ Years at Splunk as part of OT Security Teams

Part of global team specializing in industry use cases

Experience working on OT Security in Utilities, Oil & Gas, Manufacturing, Natural Resources and Government

Trends in the market and our portfolio

Digitization brings new requirements & challenges



- More automation devices
- IoT devices connecting to cloud
- Remote access/Hybrid work
- Malware intrusions
- New regulatory requirements

The role of InfoSec is critical to help OT secure industrial operations

AI is driving game-changing industrial use cases

Machine Vision

Quality inspection, Robot guidance, Packaging, Yield optimization, etc.

Make decisions at high speeds and high accuracy, improving product quality and reducing waste

BASLER ZEBRA COGNEX

Autonomous Vehicles

Automated guided vehicles (AGVs), Autonomous mobile robots (AMRs), Tele-remote operations, etc.

Reduce costs, improve safety, save space, and easily adapt to changing needs

Planet Farms

Software Controls

Software-defined Industrial Automation, Virtual PLCs, etc.

Massively reduce CAPEX and OPEX, improve operational agility, accelerate time to market

AUDI

cisco

AI-Driven Vulnerability Exploitation Fuels Up to 45% of Initial Access

How I Used AI to Create a Working Exploit for CVE-2025-32433 Before Public PoCs Existed

By Matthew Keeley | April 17, 2025

Red Teaming Research Threat Intelligence

Cyber Security News Vulnerability News

AI Systems Can Generate Working Exploits for Published CVEs in 10-15 Minutes

By Florence Nightingale - August 22, 2025

But AI also makes hacking the network easier than ever...

ChaosGPT | The AI That Went Rogue? Exploring Autonomous AI, Its Risks, and the Future of AI Safety

AI-Assisted Malware Evolves into a Daily Threat

cisco

Under attack

Manufacturing was the most extorted industry in 2023. They are an attractive target given their extremely low tolerance for down time.

58%

"The industry was victimized in **58%** of incidents X-Force assisted in remediating."

28%

"Backdoors were implemented by hackers in **28%** of incidents."

23%

"Ransomware incidents accounted for **23%** of cases."

Share of attacks by industry 2018 – 2022

Industry	2022	2021	2020	2019	2018
Manufacturing	24.8%	23.2	17.7	8	10
Finance and insurance	18.9%	22.4	23	17	19
Professional, business and consumer services	14.6%	12.7	8.7	10	12
Energy	10.7%	8.2	11.1	6	6
Retail and wholesale	8.7%	7.3	10.2	16	11
Education	7.3%	2.8	4	8	6
Healthcare	5.8%	5.1	6.6	3	6
Government	4.8%	2.8	7.9	8	8
Transportation	3.9%	4	5.1	13	13
Media and telecom	0.5%	2.5	5.7	10	8

Industrial IoT networking portfolio

Our solutions meet the needs of IT and OT

Industrial Ethernet switches

DIN-Rail, IP67, and Stackable Rackmount


IE3500


IE3400


IE3300


IE3200


IE3100


IE3500H


IE3400H


IE3100H


IE9300

Industrial Cybersecurity

Cyber Vision, Secure Equipment Access

Industrial Wi-Fi and Ultra-reliable Wireless Backhaul

For outdoor conditions


IW9167E


IW9167E-HZ


IW9167I

IW9167E-STA


IW9165D


IW9165E


IEC6400

Industrial Routers

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


IR1100

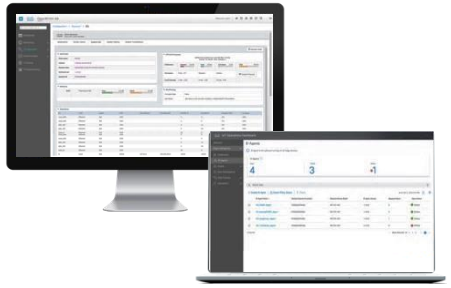

IR1800


IR8300


IR8100

Data Control and Exchange

Edge Intelligence, IOx



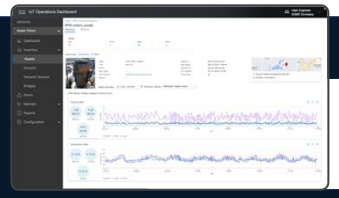
Embedded Networking

Embedded routers and switches for industrial Makers


ESR6300

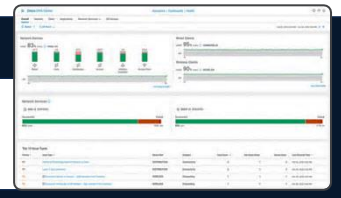

ESS3300


ESS9300



Management and Automation

Cisco Catalyst Center, Cisco Catalyst WAN Manager, *Meraki



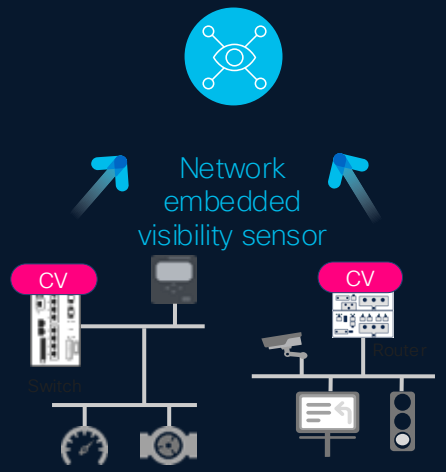
OT Security Framework

Cisco Industrial Threat Defense

Visibility

OT Asset Visibility and Security Posture

Cisco Cyber Vision

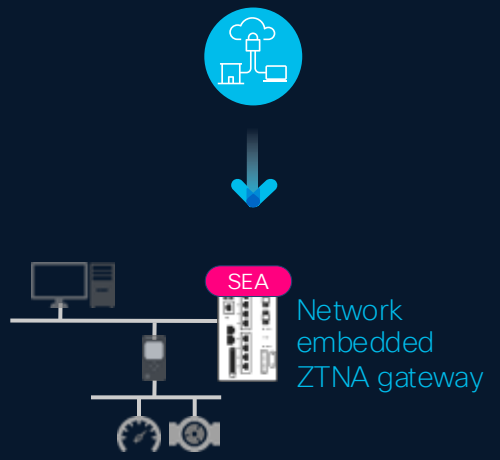


Protection

Zero Trust Security for OT

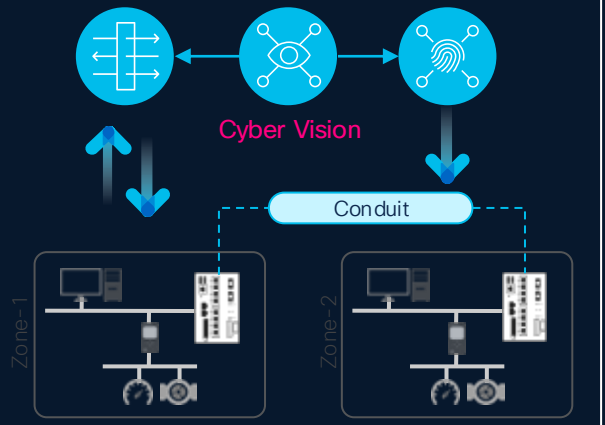
Secure remote access (ZTNA)

Cisco Secure Equipment Access



IEC 62443 zone segmentation

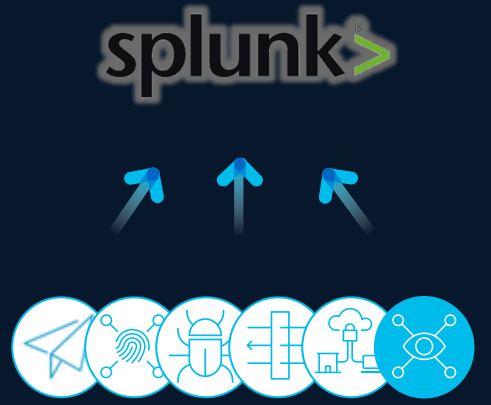
Cisco Secure Firewall **Cisco ISE**



Network enforced segmentation

Detection & Response

Cross-Domain SOC

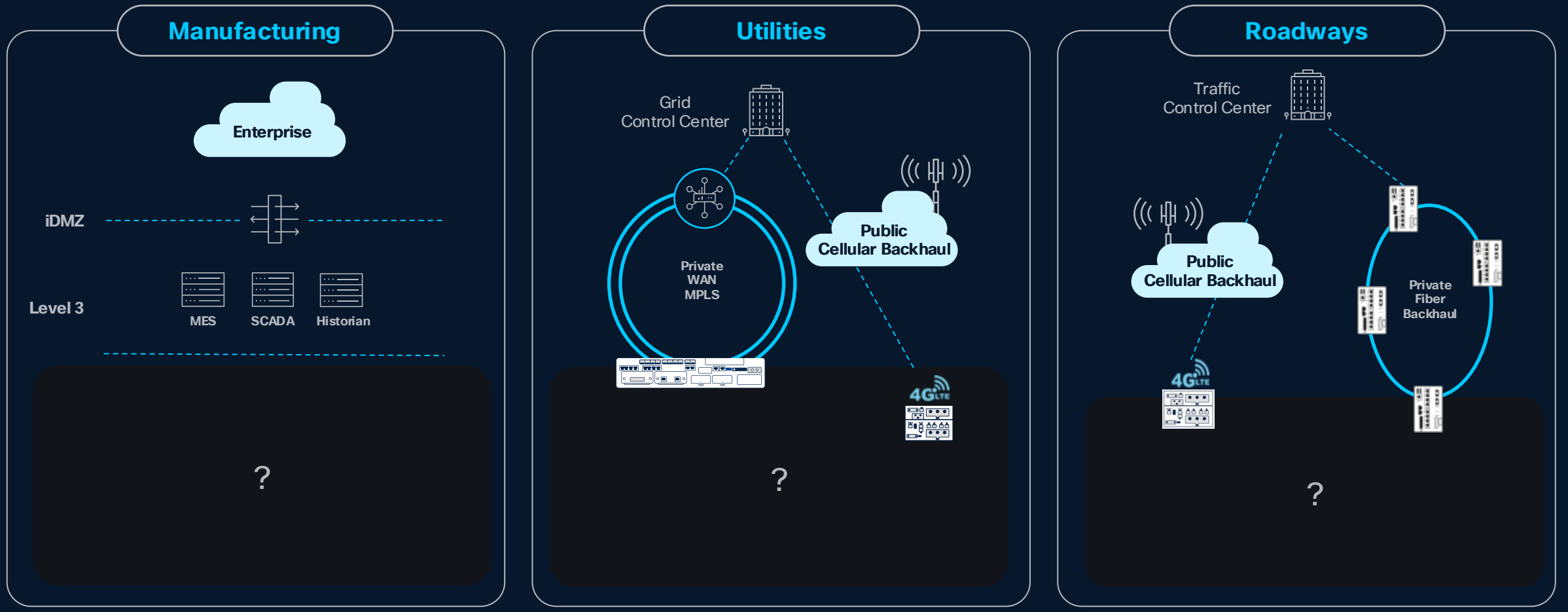


Visibility across the entire attack chain

Network as a fabric to secure OT at scale

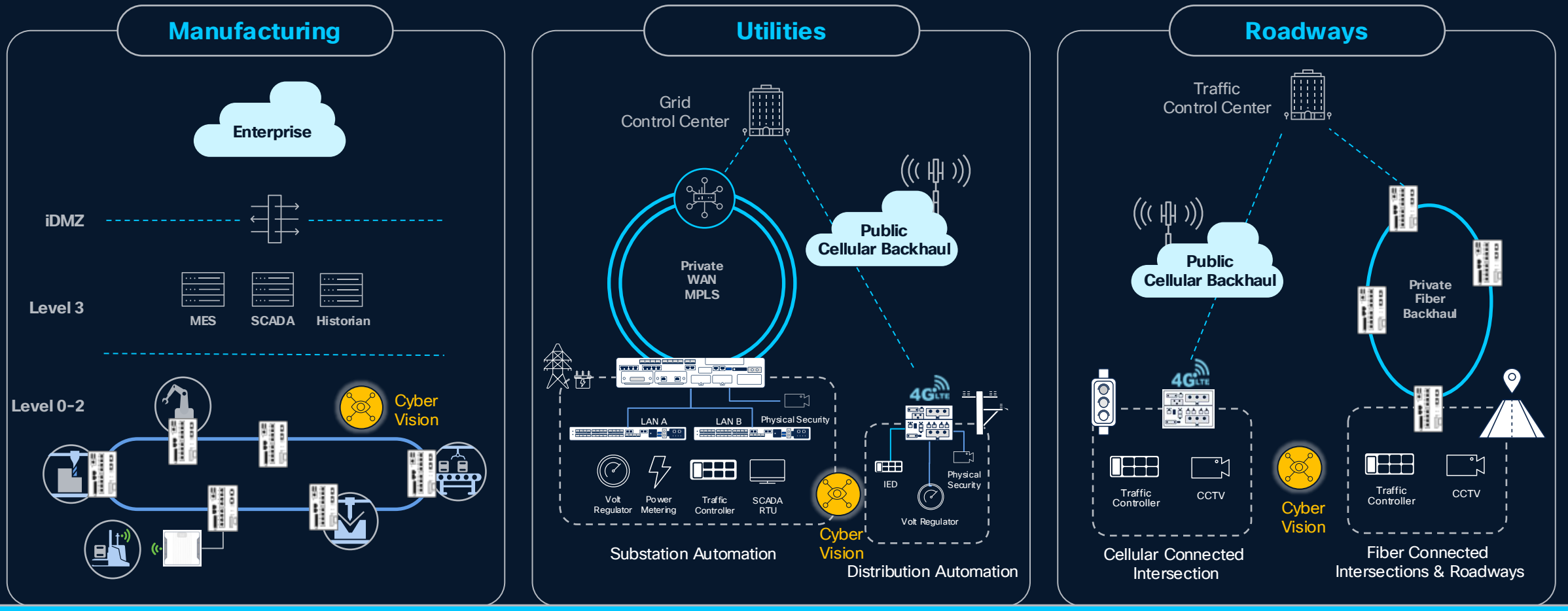
Cisco Industrial Threat Defense: 1 – Visibility

We do not have enough visibility into our most critical assets



Cisco Industrial Threat Defense: 1 – Visibility

Cisco Cyber Vision “turns on the lights” for industries

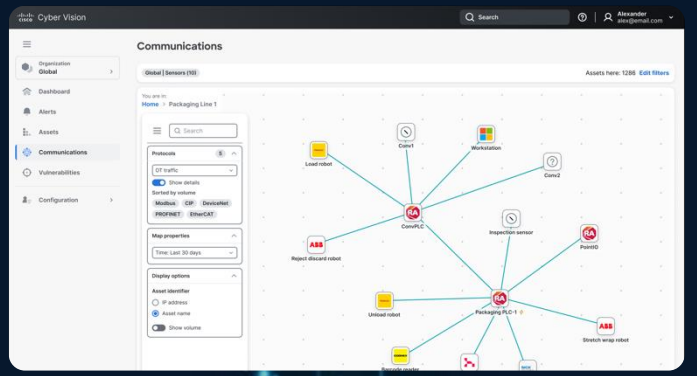


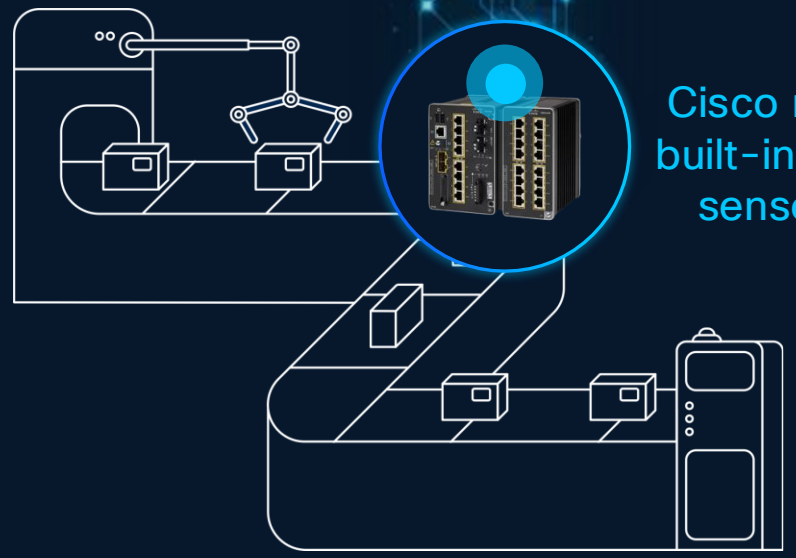
Automated discovery of assets, vulnerabilities, and communication across the industrial network

Visibility built-in, not bolted on

- ✓ Network embedded sensor
  No need for addition hardware
- ✓ No need for SPAN collection networks
- ✓ Active discovery passes NAT boundaries
- ✓ Comprehensive visibility, even at lowest Purdue levels

Cyber Vision Center



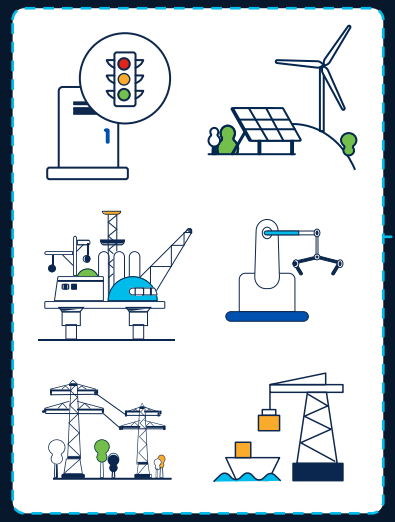


Cisco network with built-in Cyber Vision sensor software

Cisco Industrial Threat Defense: 1 - Visibility

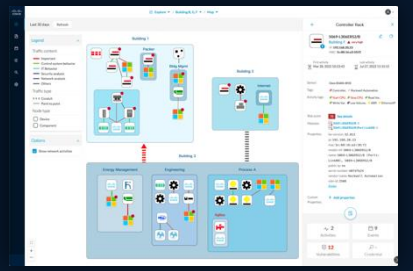
A two-tier architecture

OT Assets



Cisco industrial switches or routers

Lightweight Metadata



Cyber Vision Sensor

- ✓ Software embedded into network equipment
- ✓ Passive discovery via DPI
- ✓ Safe active queries of assets
- ✓ Decodes application flows

Cyber Vision Center

- ✓ Centralize analytics and data storage
- ✓ Detailed OT asset inventory and communications maps
- ✓ Security posture and detection
- ✓ Reporting

Integrations

SIEM, XDR, NAC, Firewall, CMDB, etc.

- ✓ OT asset profiles in IT security tools
- ✓ OT context and events in SOC
- ✓ Native integrations and specific apps
- ✓ Comprehensive APIs for custom integrations

OT visibility sensors embedded into network equipment sees more and is easier to scale

Cisco Industrial Threat Defense: 1 - Visibility

The devices that make everything possible

Center

Hardware Appliance

UCS based servers with Hardware RAID

CV-CNTR-M6N
- 24 core CPU
- 128 GB RAM
- 3.2TB drives

Software Appliance

Virtual Machines

VMWare ESXi OVA

HyperV VHD

Nutanix HAV

Minimum requirements
x386 server CPU, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Amazon Web Services

Microsoft Azure

Minimum requirements
x386 server CPU, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Sensors

IE3300, IE3400, and IE3500 Switches

IE3400HD and IE3500HD IP67 Switch

Catalyst IR1101 Cellular Router

Catalyst IR1800 Cellular Router

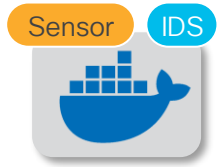
Catalyst IR8300 Multiservice Router

Catalyst IE9300 Rugged Switches

Catalyst 9300/9400 Aggregation Switches

Network-Sensors

DPI and active discovery built into network-elements eliminating the need for SPAN



x86 or ARM64 Compute

IC3000 Industrial Compute

Docker Sensor

Hardware-Sensor

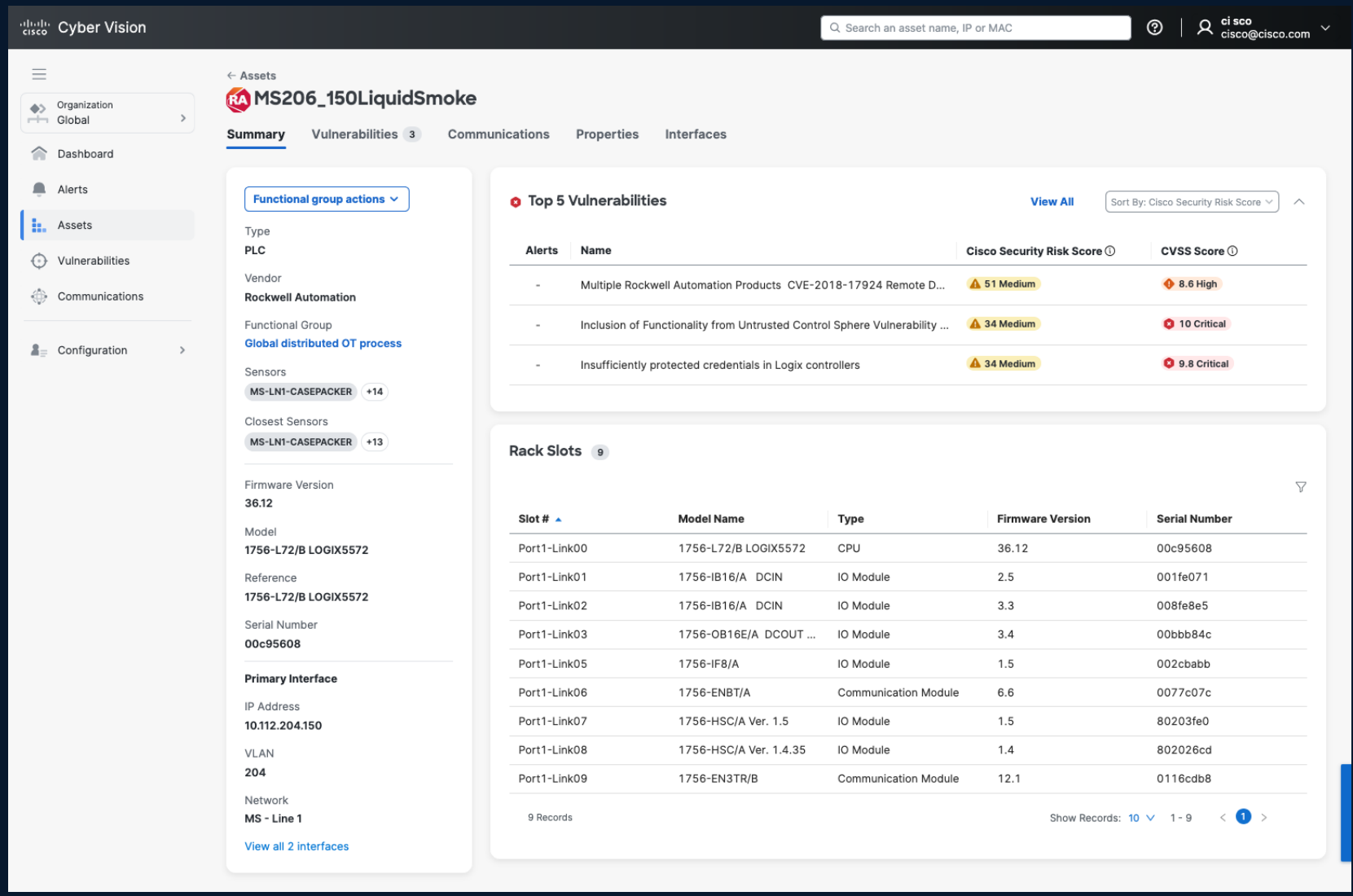
DPI and active discovery via SPAN to support brownfield

Cisco Industrial Threat Defense: 1 – Visibility

Cyber Vision

Visibility into connected industrial assets

Understand the identity of all assets in the environment. View rack slot details for modular assets.

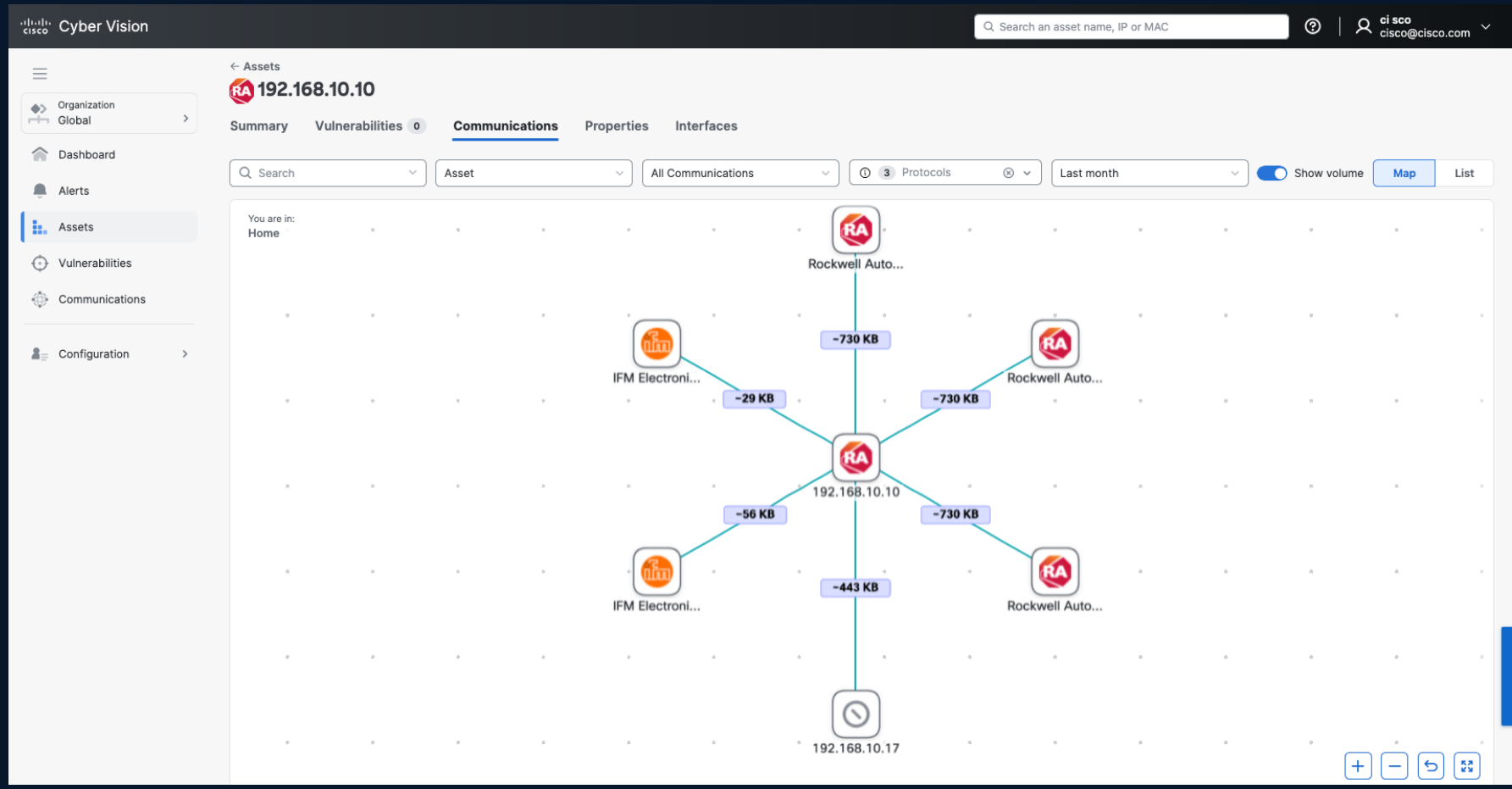


Cisco Industrial Threat Defense: 1 – Visibility

Cyber Vision

Communication Map

- Highly performant rendering for thousands of nodes
- Rich overlay capability to turn on visuals as needed to reduce distractions



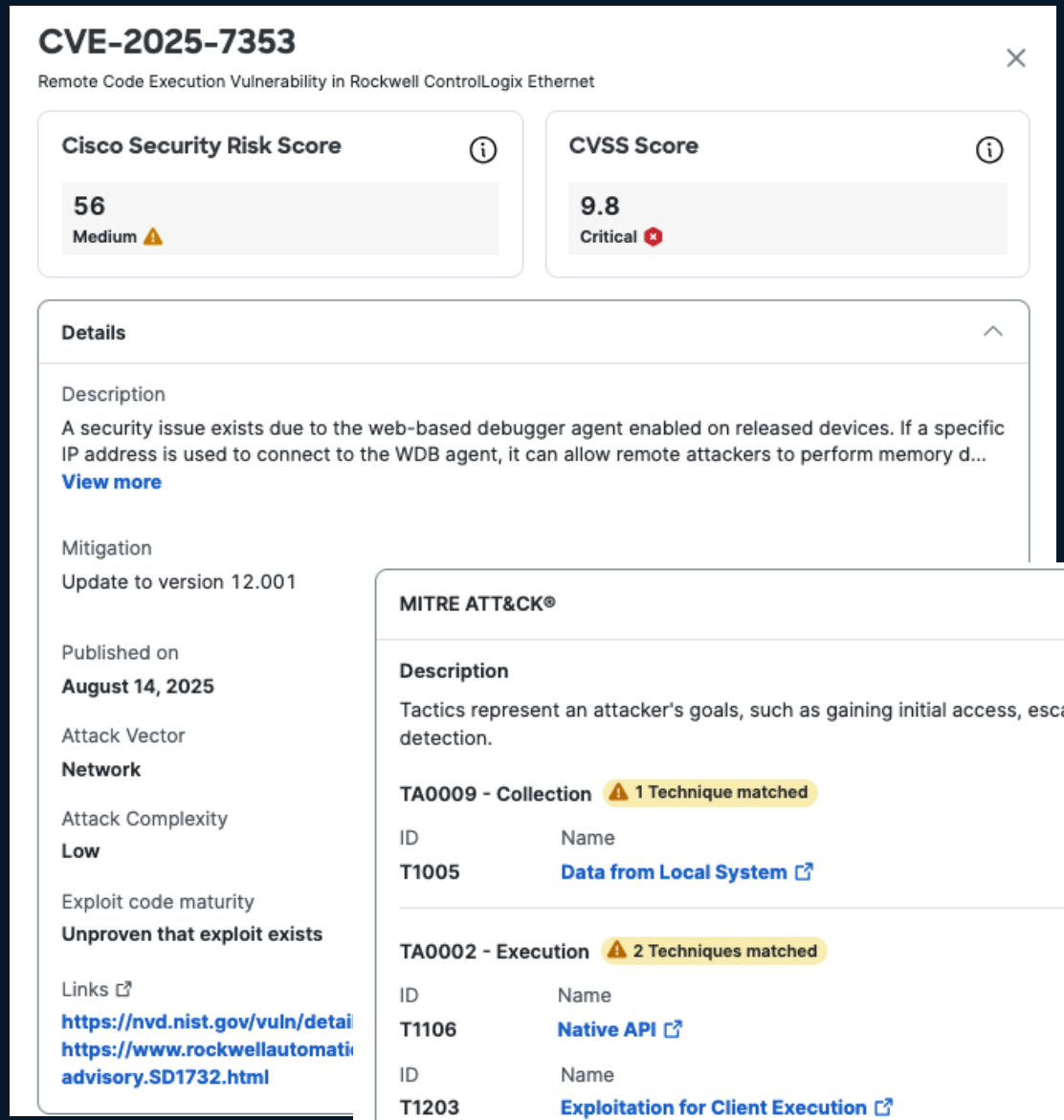
Cisco Industrial Threat Defense: 1 – Visibility

Cyber Vision

Identify & Track Vulnerabilities

Identify known asset vulnerabilities so you can patch or protect them before they are exploited

Cisco Security Risk Score provides dynamic vulnerability scoring using indicators such as being actively exploited in the wild

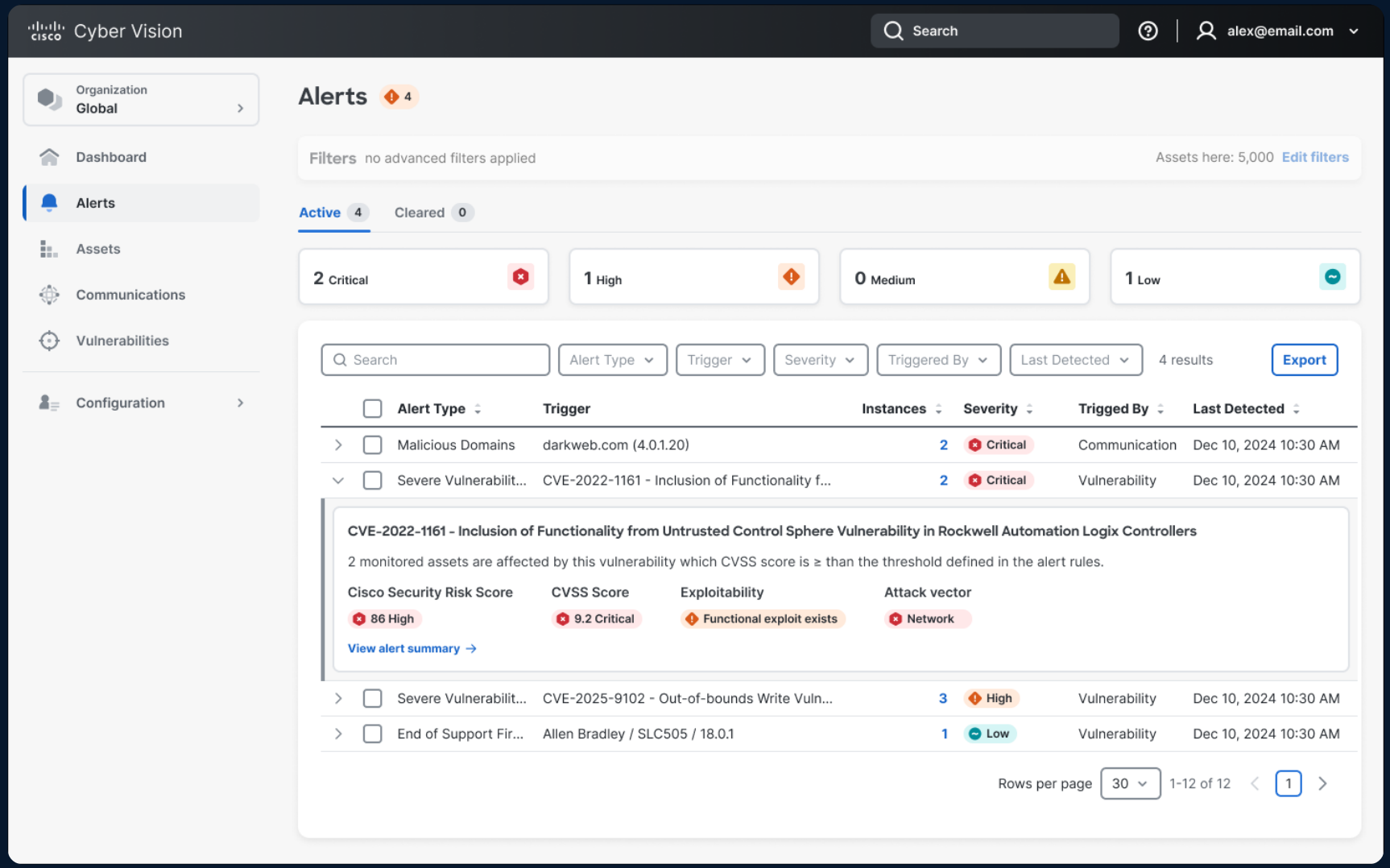


Cisco Industrial Threat Defense: 1 – Visibility

Cyber Vision

Alerts

- New rule engine to configure Alert thresholds
- Alerts grouped based on trigger to reduce number of alerts generated



Cisco Industrial Threat Defense: 2 – Protection (Remote Access)

Trends in the market

User identity is still the top target for attackers:

- Credential abuse is the most common way to breach a network
- Phishing is the most common delivery method

Exploiting the remote access hardware is a new trend:

- 34% rise in successful exploits due to vulnerabilities
- 22% of all vulnerability exploitation breaches targeted edge infrastructure such as firewalls, VPN & remote access gateways which was only 3% in 2023

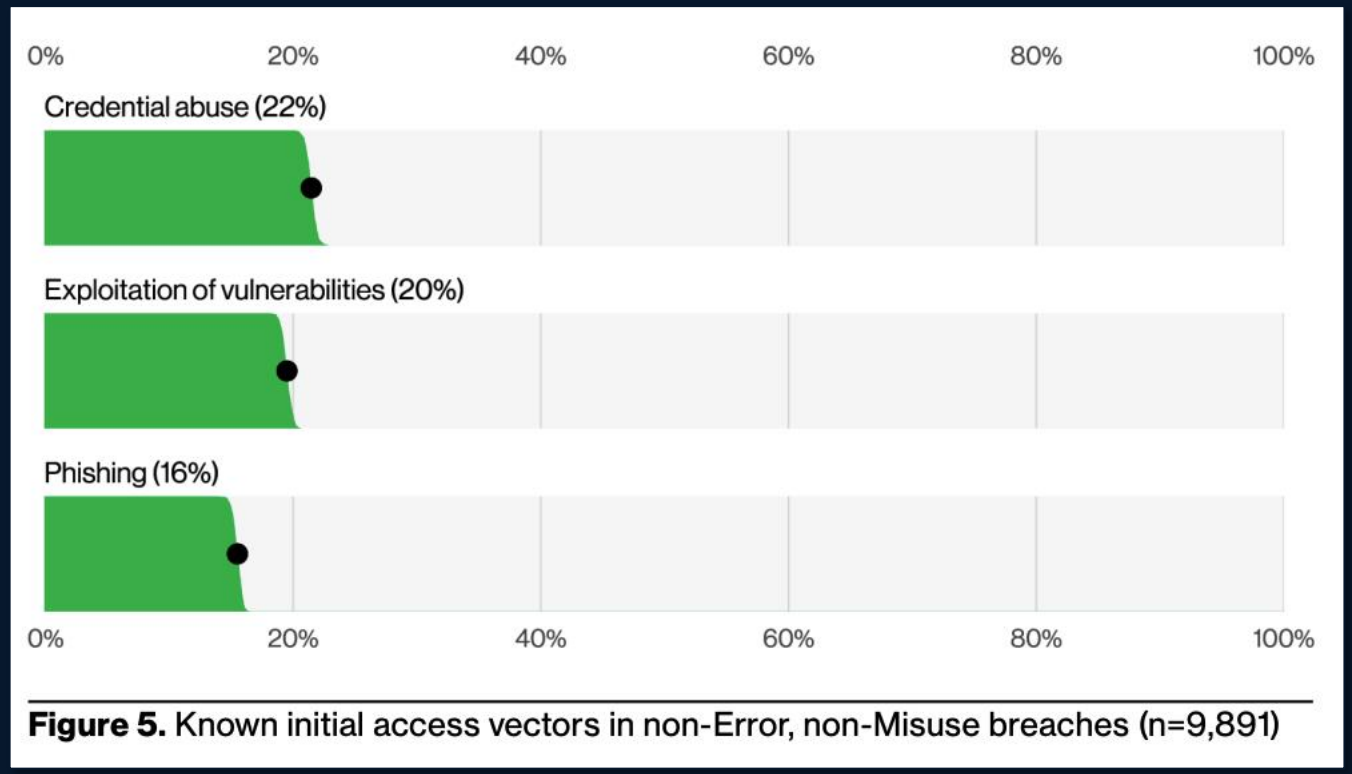


Figure 5. Known initial access vectors in non-Error, non-Misuse breaches (n=9,891)

Verizon 2025 Data Breach Investigations Report

Cisco Industrial Threat Defense: 2 - Protection (Remote Access)

Today's world

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

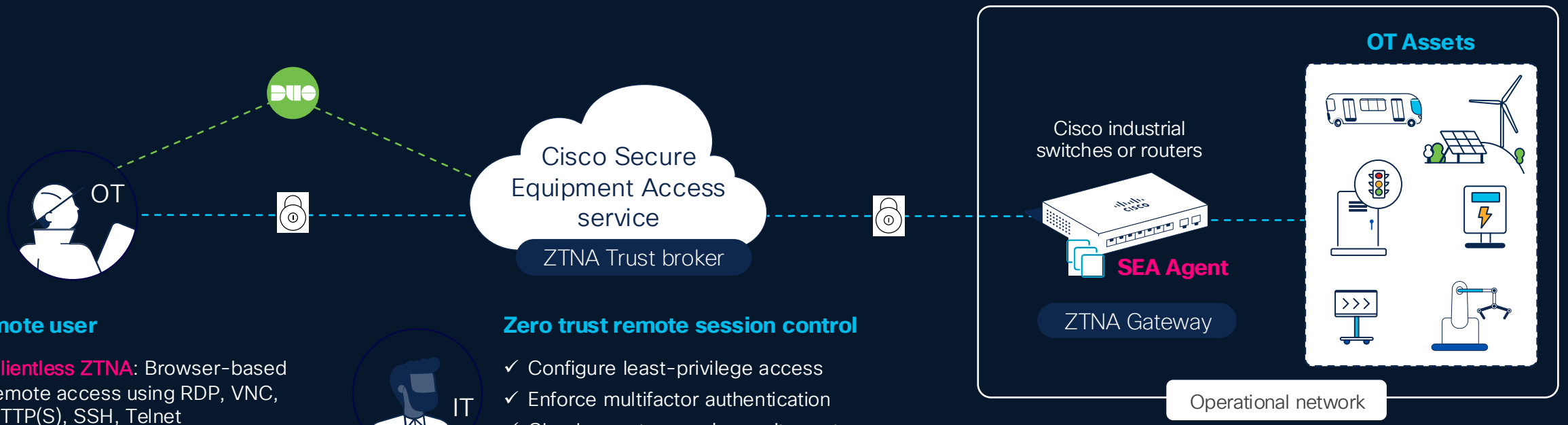
VPN

Always-On, All-or-Nothing access

Need additional controls to deny full network access

Cisco Industrial Threat Defense: 2 – Protection (Remote Access)

Zero Trust Network Access for OT



Remote user

- ✓ Clientless ZTNA: Browser-based remote access using RDP, VNC, HTTP(S), SSH, Telnet
- ✓ Agent-based ZTNA: remote access that supports native desktop applications

Zero trust remote session control

- ✓ Configure least-privilege access
- ✓ Enforce multifactor authentication
- ✓ Check remote users' security posture
- ✓ Record, monitor, terminate sessions

Cloud simple
Accelerate time to value

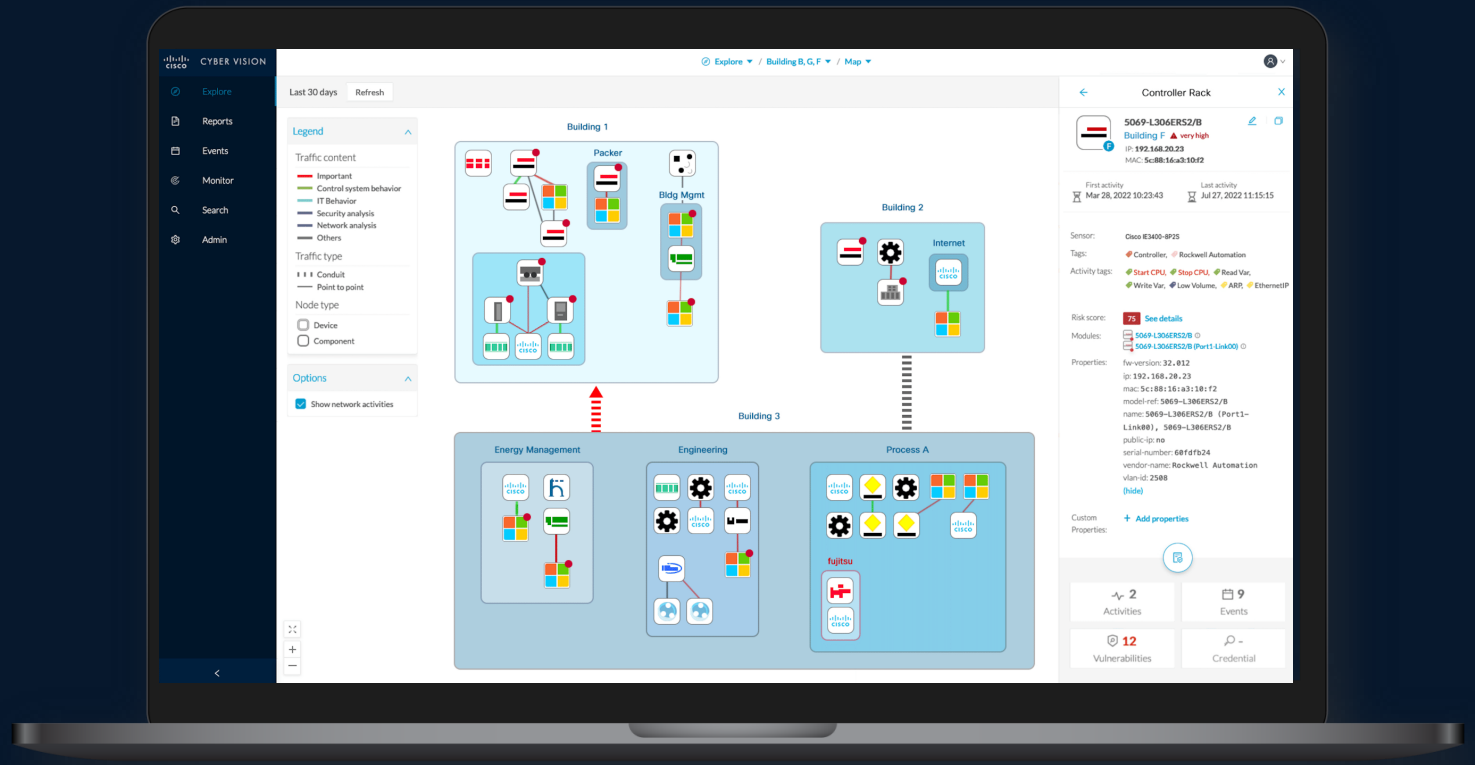
Cisco secure
Built to keep operations safe

Designed for OT
Drive business outcomes

Highly scalable
Cloud + network working together

Cisco Industrial Threat Defense: 2 - Protection (Within)

Leveraging visibility to drive segmentation



IEC-62443 virtual segmentation

- Group OT assets into zones
- Visualize conduits
- Identify traffic violations
- Share context with other platforms to enforce segmentation

Cisco Industrial Threat Defense: 2 – Protection (Within)

Zone Group Assets with Similar Security Requirements

Operating Room	Pharmacy (locked)
Strict Access	Controlled
Patient Room	Waiting Room
Moderate	Open

Hospital Floor Plan

Safety Systems	Critical Control
Isolated	Protected
Standard Sensors	Site Access
Monitored	Restricted

Industrial Plant

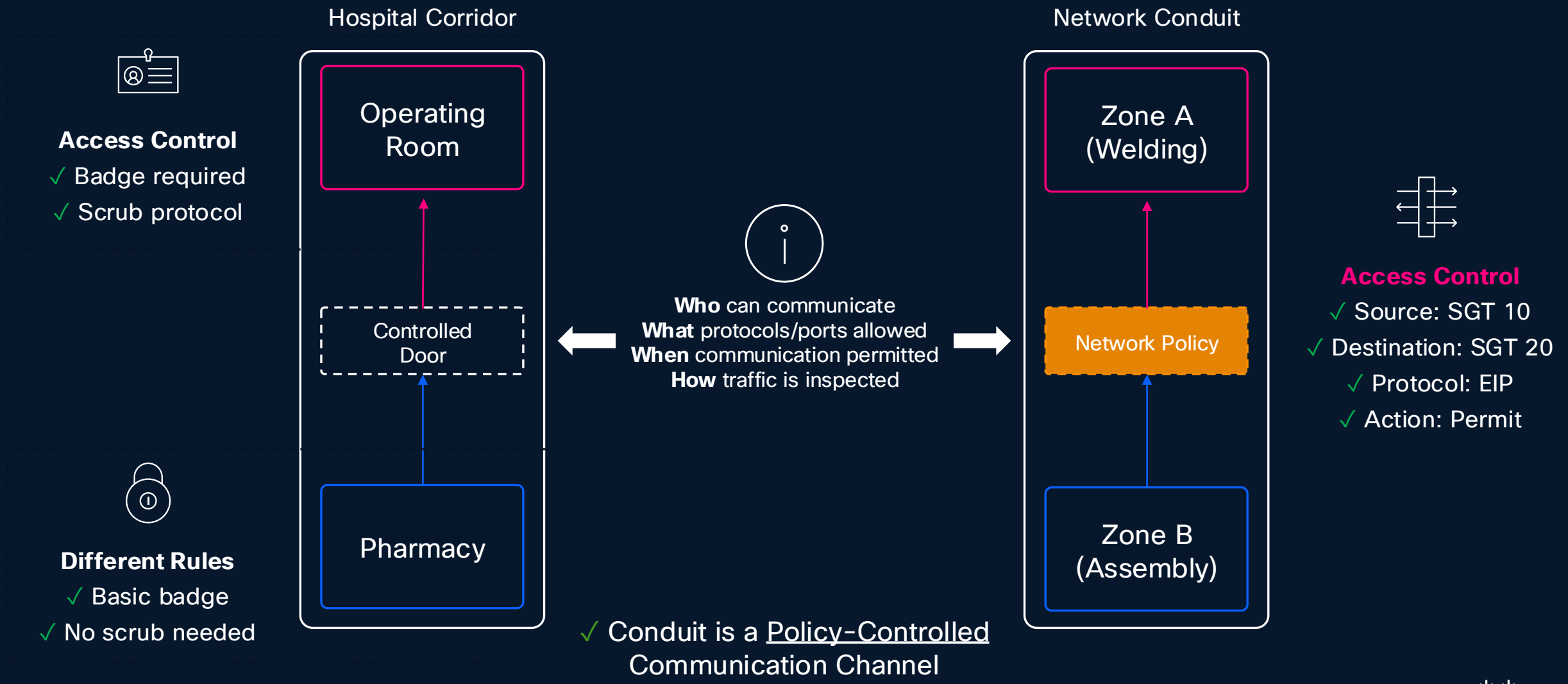
Same Principle in OT Networks

✓ Similar security requirements
✓ Shared risk profile
✓ Common function or location
✓ Defined boundaries

cisco

Cisco Industrial Threat Defense: 2 - Protection (Within)

Conduits Control Communication Between Zones

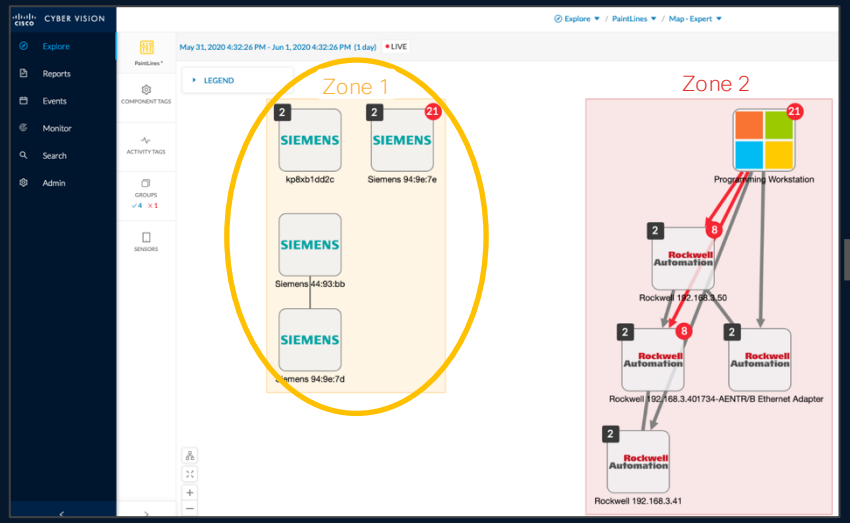


Cisco Industrial Threat Defense: 2 - Protection (Within)

Conduits Control Communication Between Zones

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

I now have OT context to build the right network access policies



Cisco Cyber Vision Map View

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

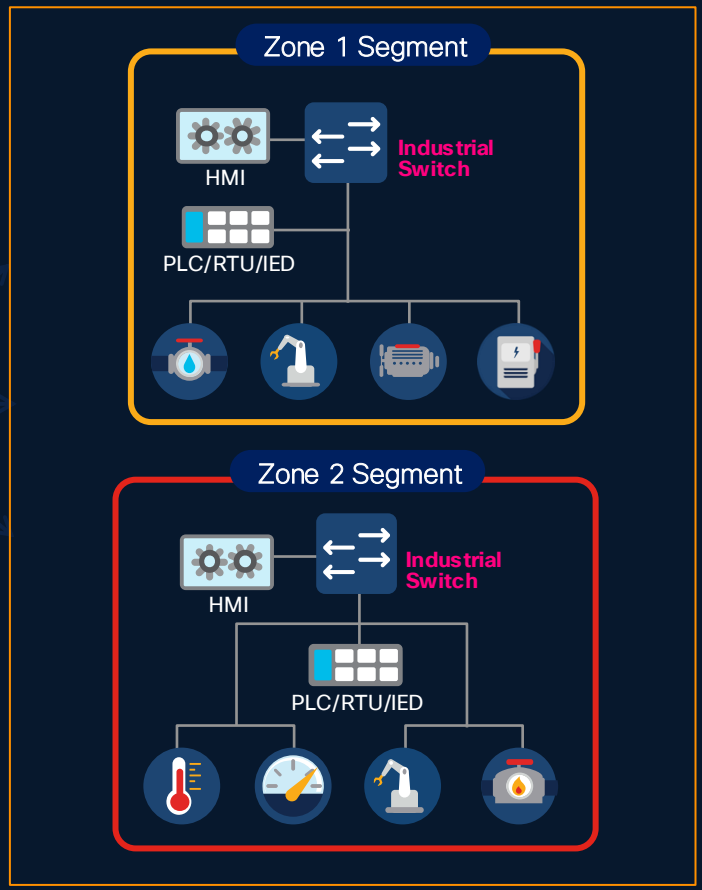
dACL

SGT

VLAN

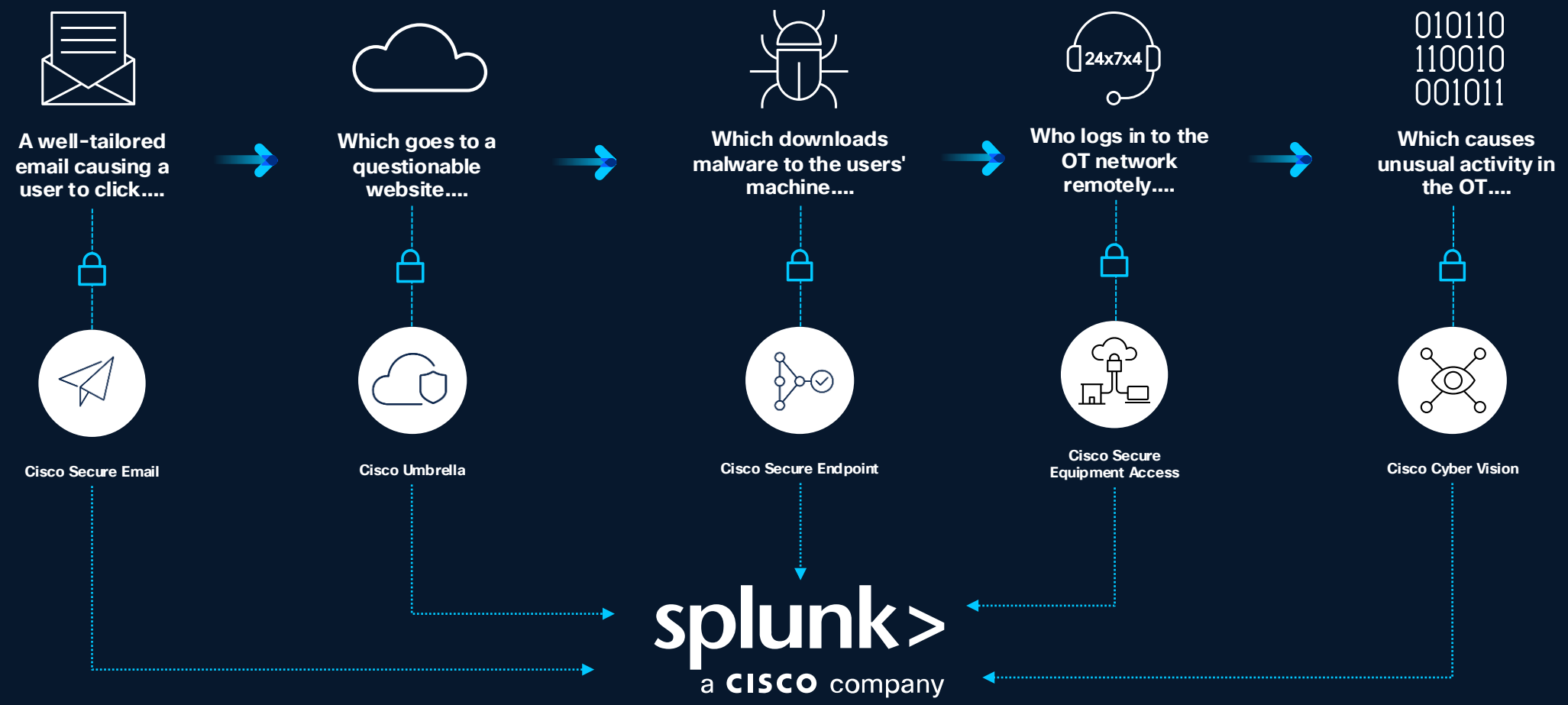
Cisco Firewall Policy Matrix
or
Cisco ISE Policy Matrix

Segmentation of industrial network



Cisco Industrial Threat Defense: 3 – Detection and Response

Detecting threats requires cross-domain visibility

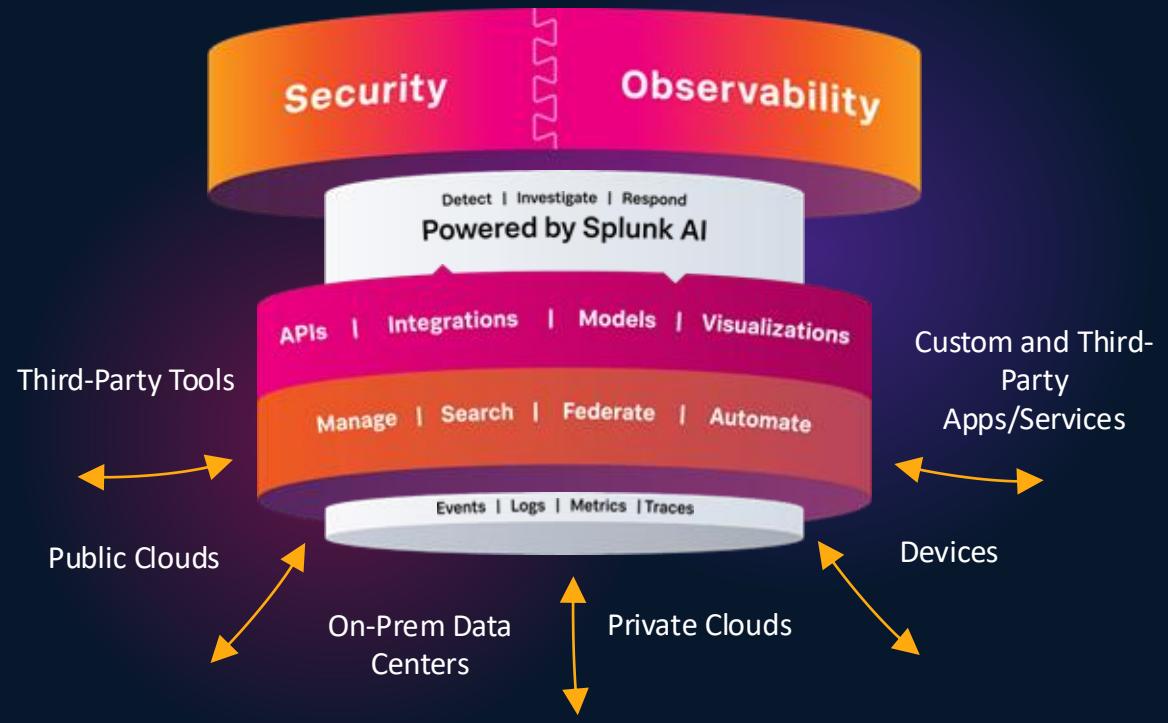


Cisco Industrial Threat Defense: 3 – Detection and Response

What is Splunk?

Splunk Security focuses on finding, investigating and responding to threats

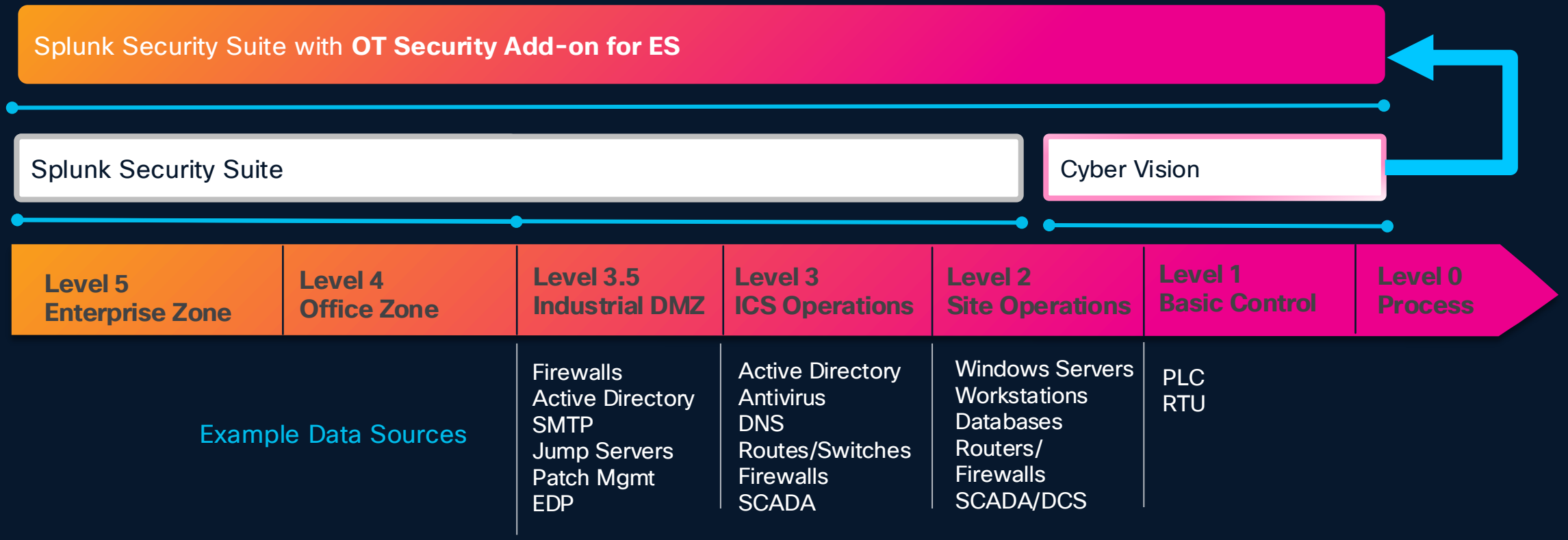
Splunk Observability helps understand the health and performance of systems and applications, to eliminate downtime and find the root cause of failures



Digital resilience is important in a modern industrial environment. **Security** and **Observability** are two sides of the same coin – you can't have a "safe" factory if it's unavailable, and you can't have a "high-performing" factory if it's compromised.

Cisco Industrial Threat Defense: 3 – Detection and Response

Visibility across the entire organization



Leveraging Splunk for OT On Premise, Hybrid, and Cloud Environments

Cisco Industrial Threat Defense: 3 – Detection and Response

Common OT Data Source Integrations

A wide variety of sources integrate to Splunk's Common Information Model

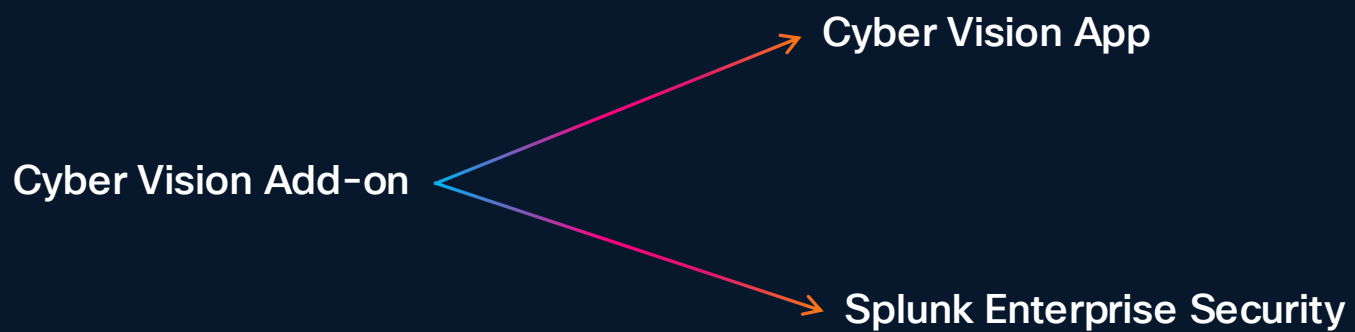
- Logs (OS, App, etc.)
- Vulnerabilities
- Network/Firewall Traffic
- Asset Inventory
- Security Events
- Endpoint activity
- Ticketing

Cisco Industrial Threat Defense: 3 – Detection and Response

Integration between Cyber Vision and Splunk

Cyber Vision Add-on is a background process that contains data parsing rules, field extractions, and configurations to ingest data from Cyber Vision correctly

Cyber Vision App contains dashboards, reports, saved searches and custom navigation menus so humans can make use of the data ingested by the add-on

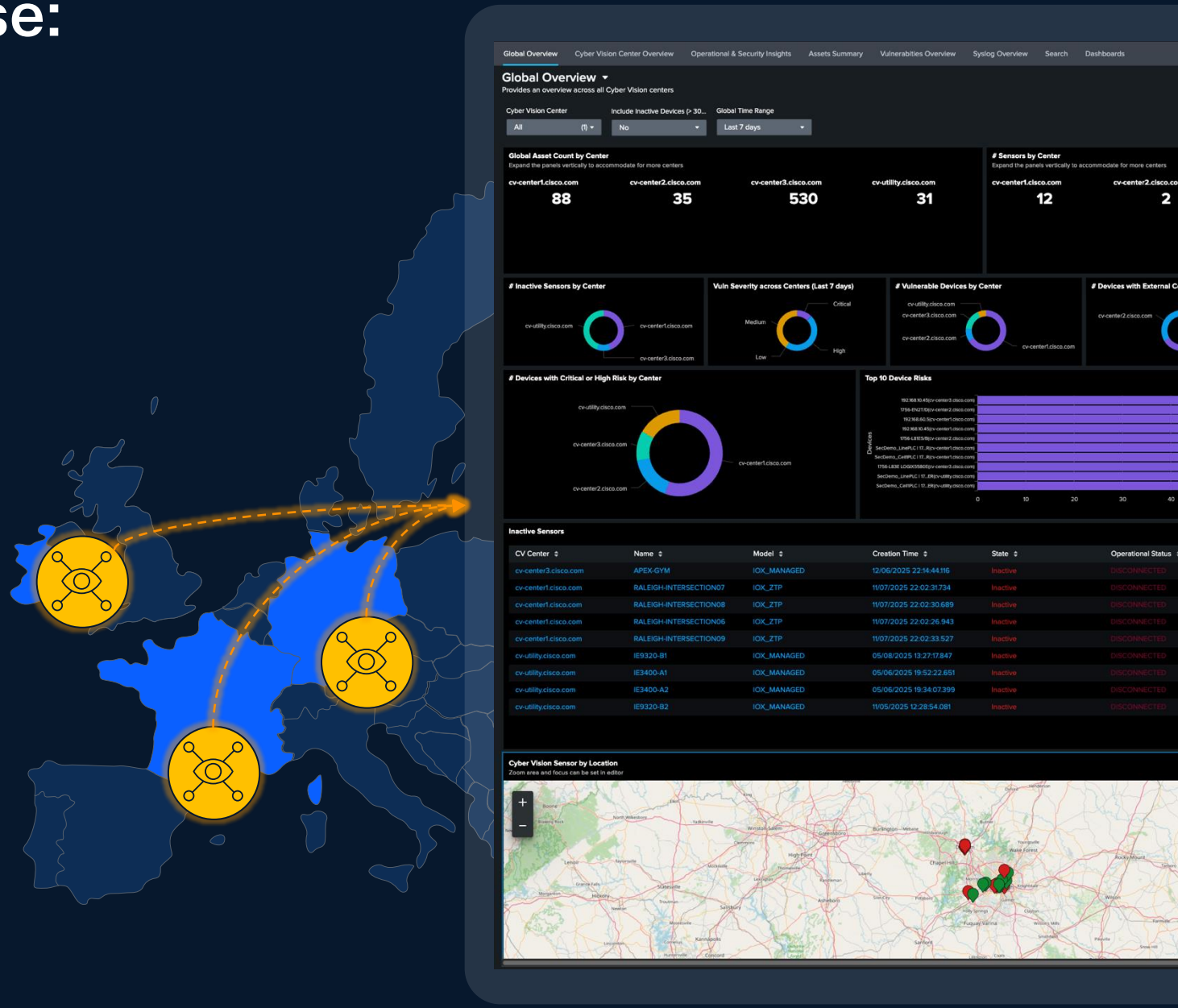


Cisco Industrial Threat Defense: 3 – Detection and Response

Cyber Vision Splunk App

- Aggregate data from all Cyber Vision deployments
- Focused view per local center
- Operational & Security Overview
- Vulnerabilities Overview
- Schedule reports over email

Monitor security posture and drive OT security governance at scale

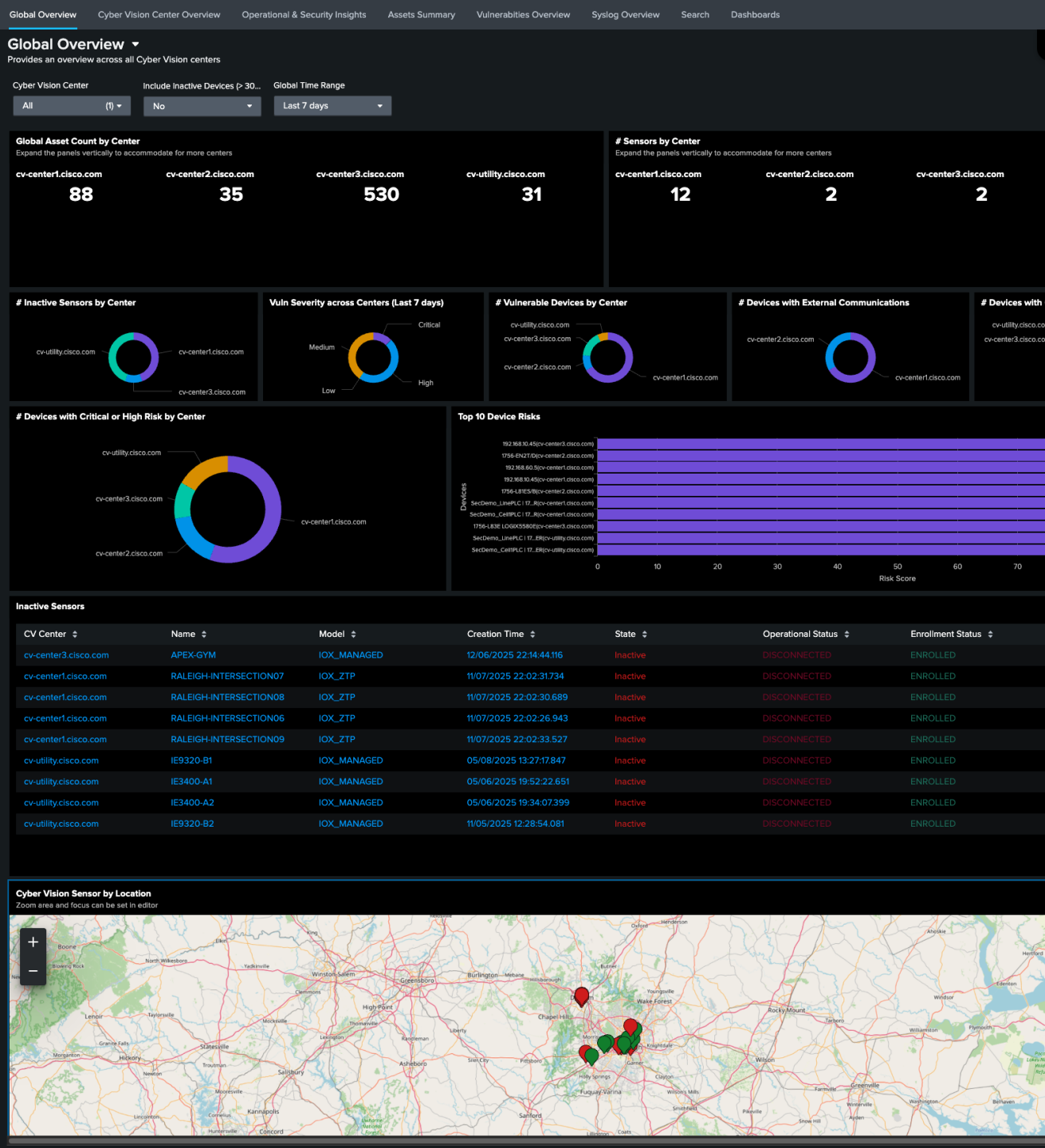


Cisco Industrial Threat Defense: 3 – Detection and Response

Cyber Vision Splunk App

Global and Cyber Vision Overviews

Global overview across your entire installation or for each Cyber Vision Center

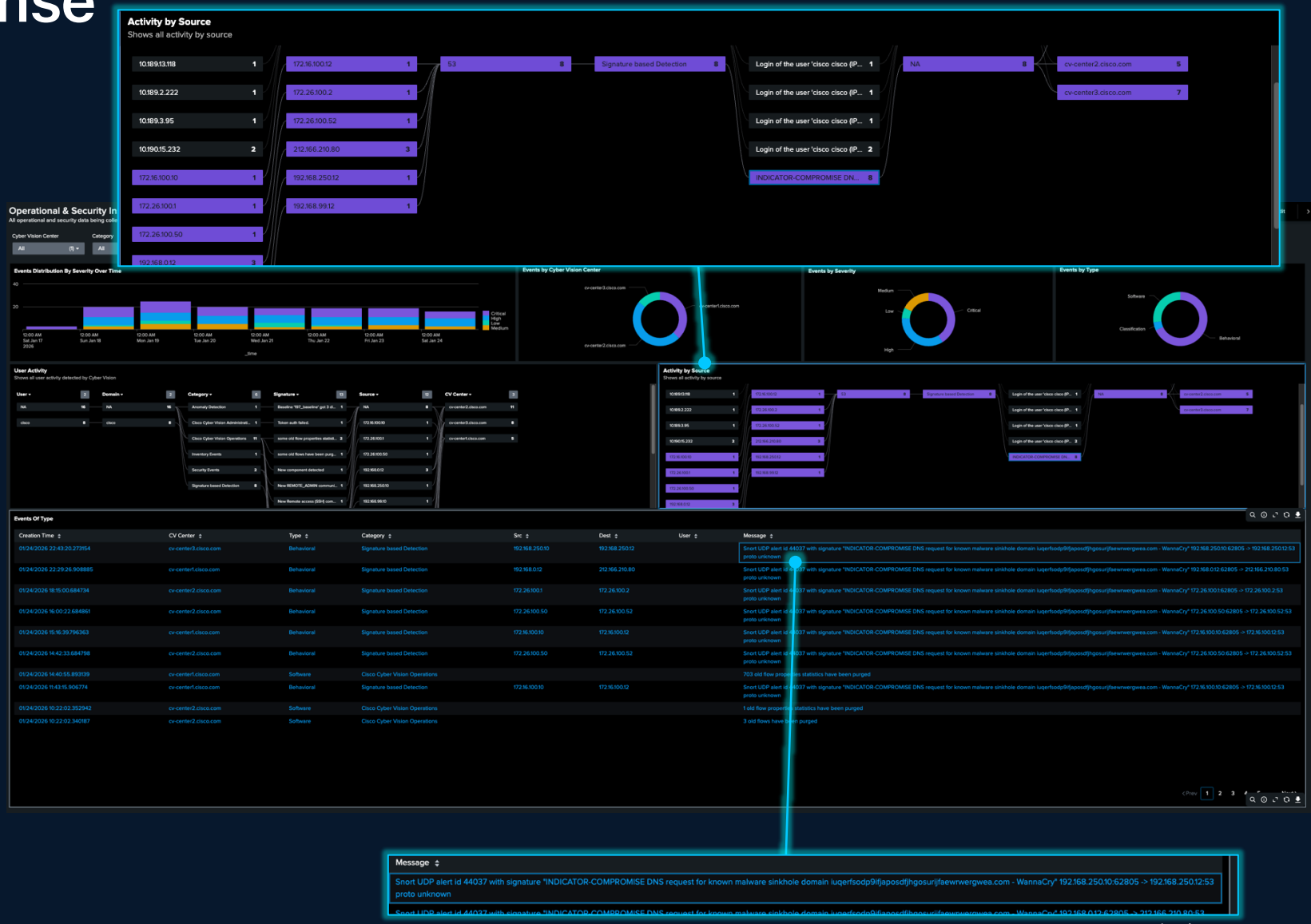


Cisco Industrial Threat Defense: 3 – Detection and Response

Cyber Vision Splunk App

Operational and security overview

Aggregated view of security events with a timeline view to understand origin and impact

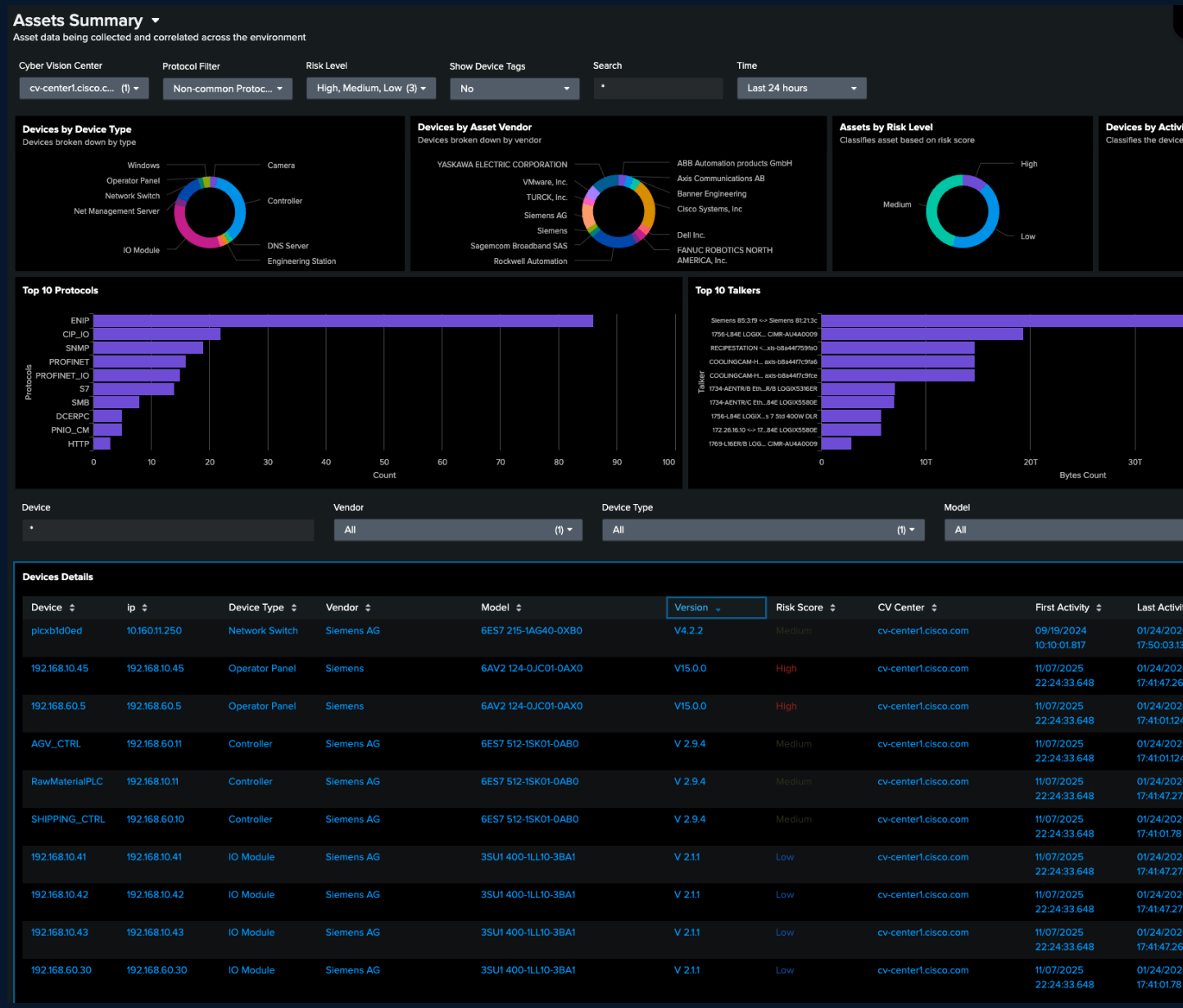


Cisco Industrial Threat Defense: 3 – Detection and Response

Cyber Vision Splunk App

Asset summary

Help understand which assets need refreshed & identify risky vendors in your deployment

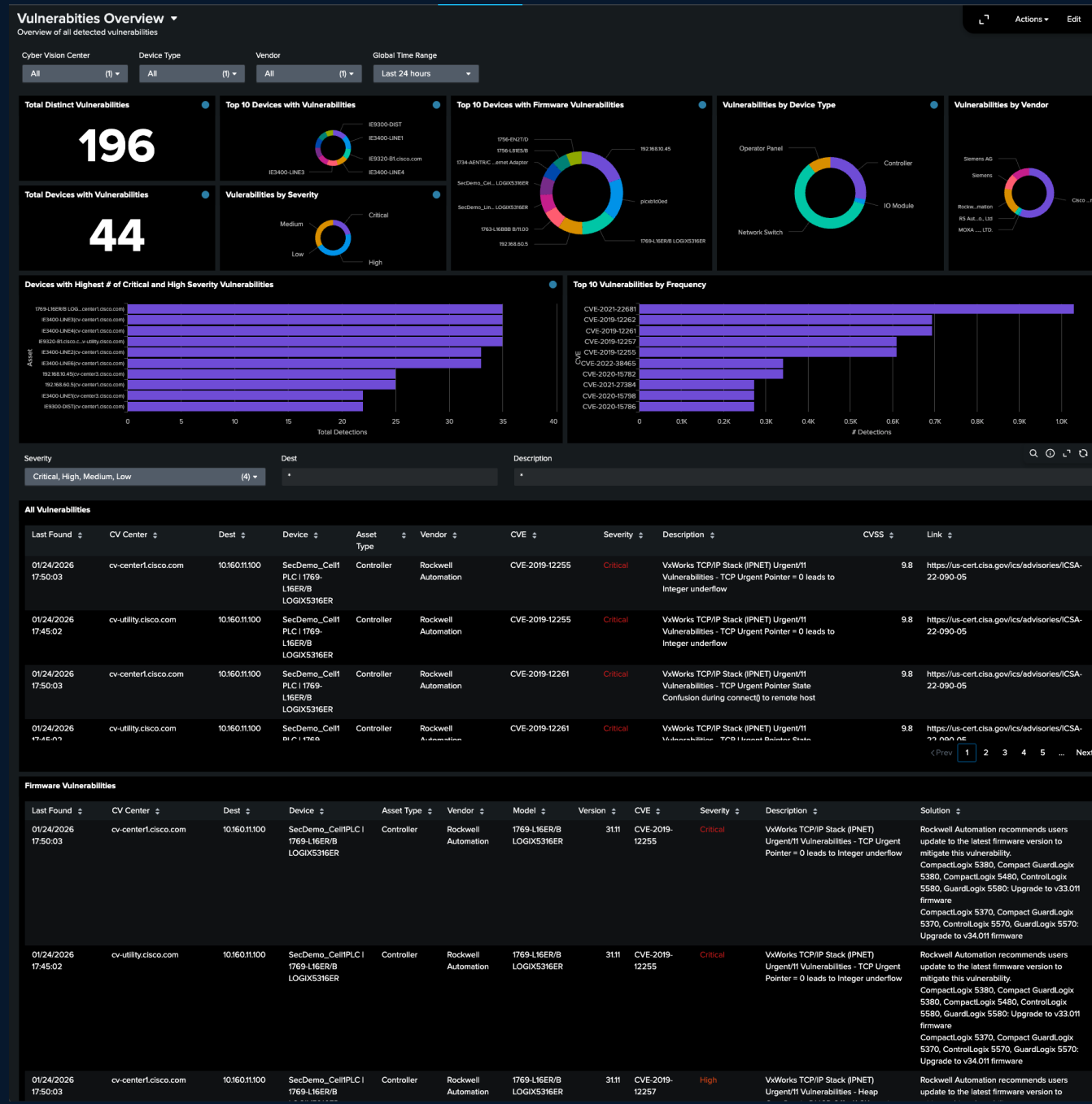


Cisco Industrial Threat Defense: 3 – Detection and Response

Cyber Vision Splunk App

Vulnerabilities overview

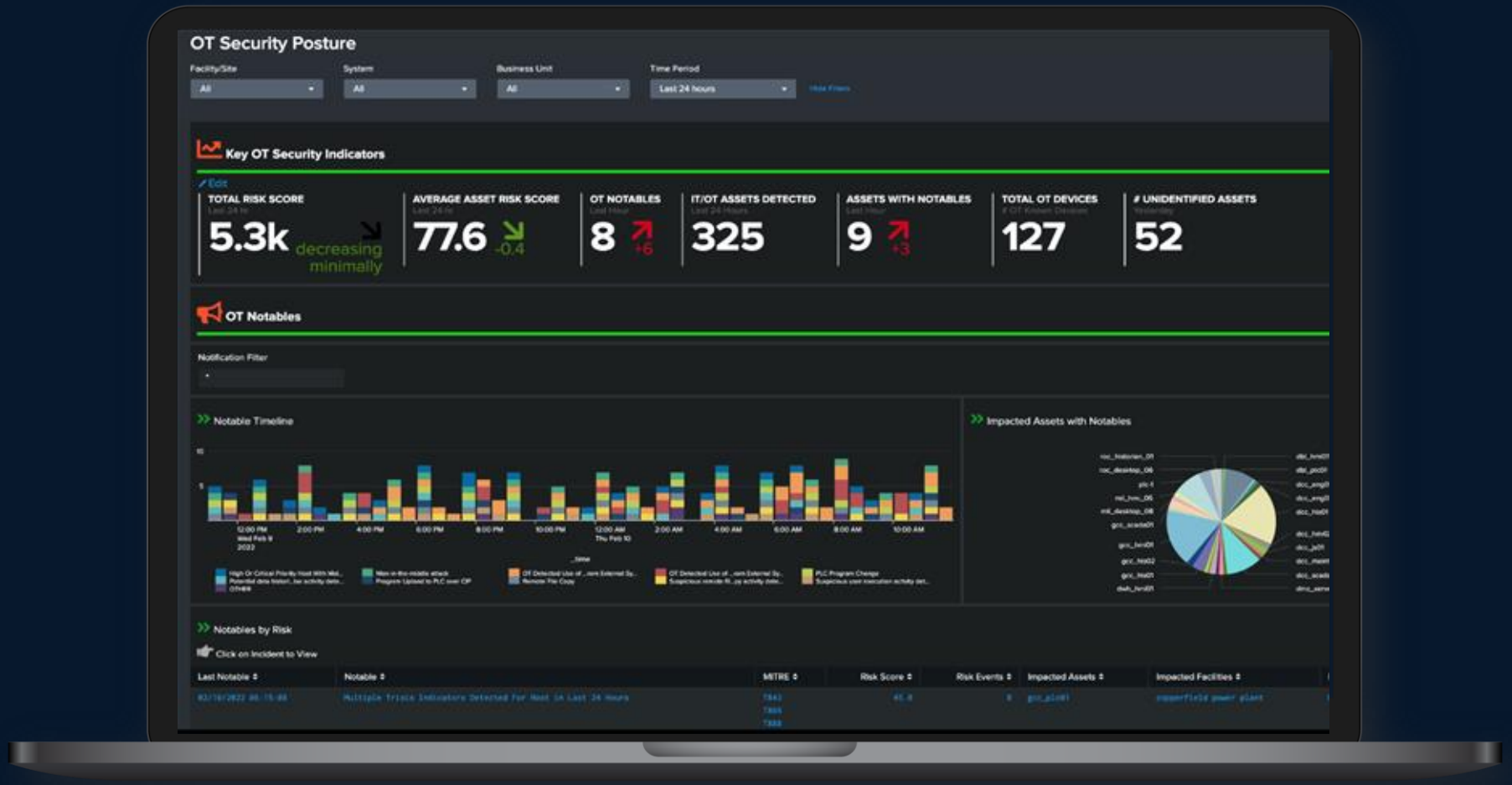
Identify the riskiest vulnerabilities in my environment and which ones can be eliminated in the next maintenance window



Cisco Industrial Threat Defense: 3 – Detection and Response

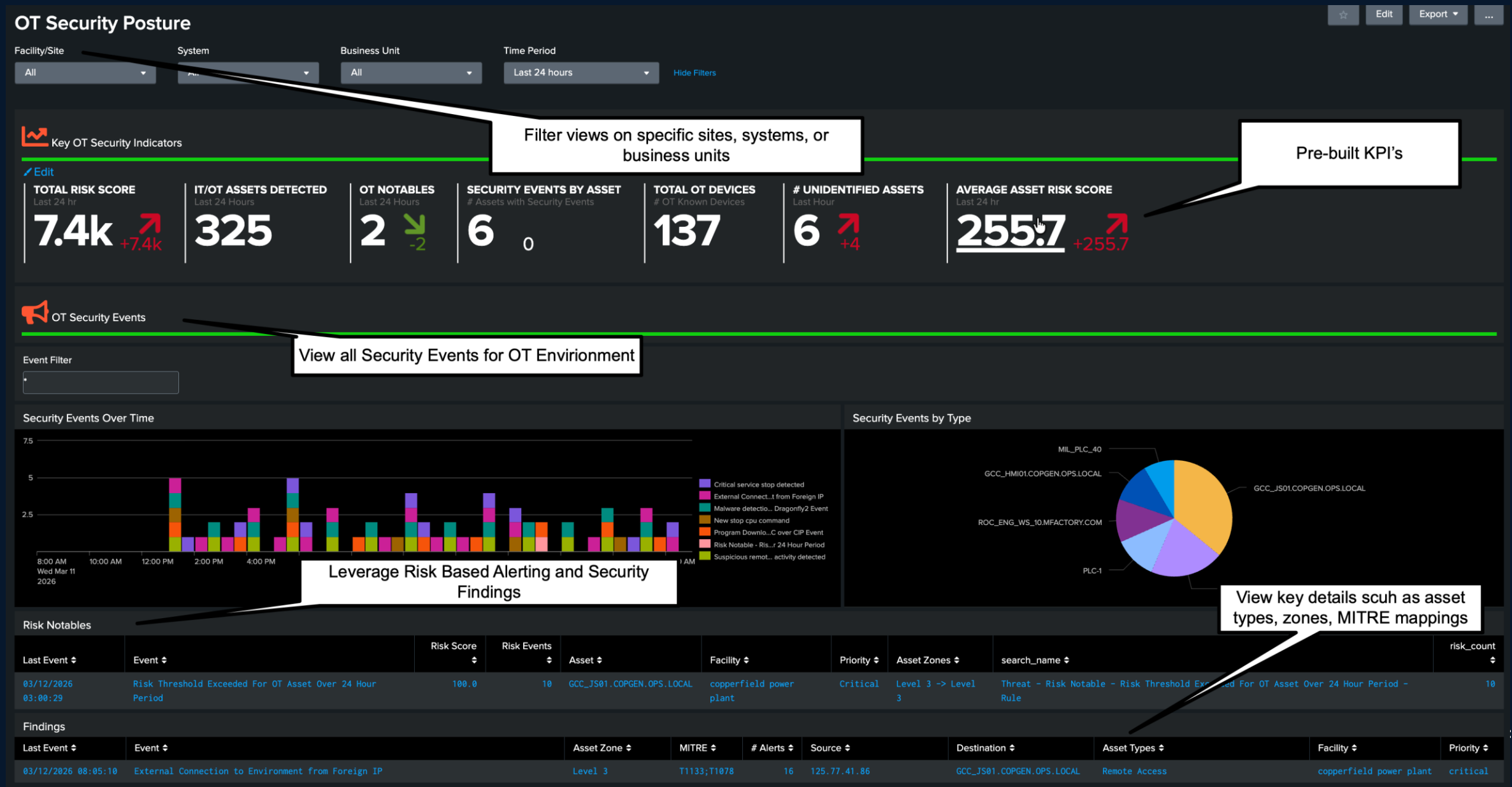
OT Security Add-on for Splunk ES

- **Unified Data Model** – Adjust your incident response based on critical asset content
- **Get Started Faster** – Perimeter Monitoring, Endpoint Protection, External Media, Infrastructure Monitoring
- **Security Frameworks** – leverage common security frameworks along with MITRE ATT&CK for ICS
- **Mitigate Risk** – Leverage features like asset baselining to secure your endpoints
- **Detections & Use Cases** – Prebuilt detections and use case explorer for OT
- **Compliance** – Prebuilt reports and dashboards for NERC CIP audits



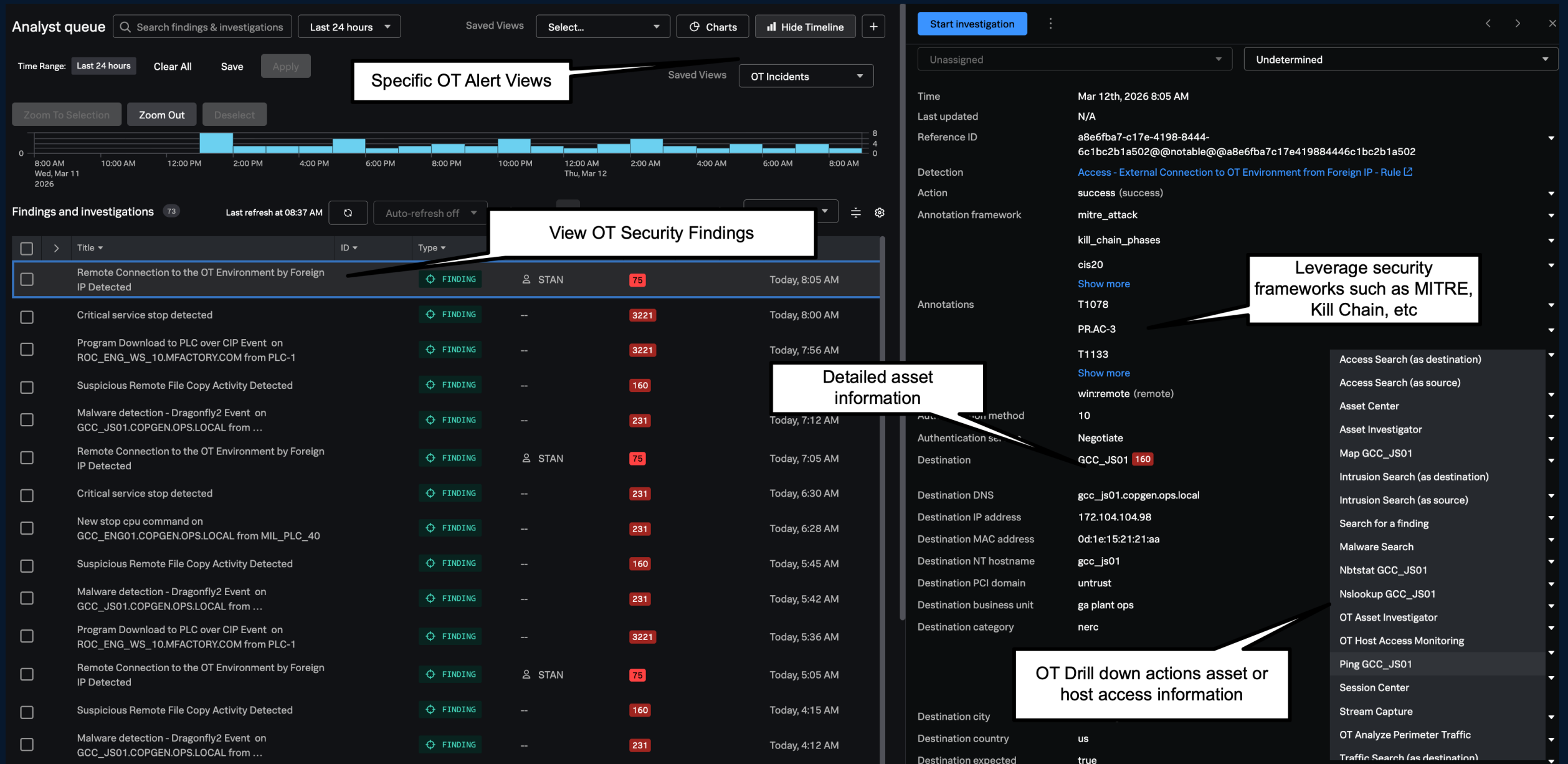
Cisco Industrial Threat Defense: 3 – Detection and Response

OT Security Posture



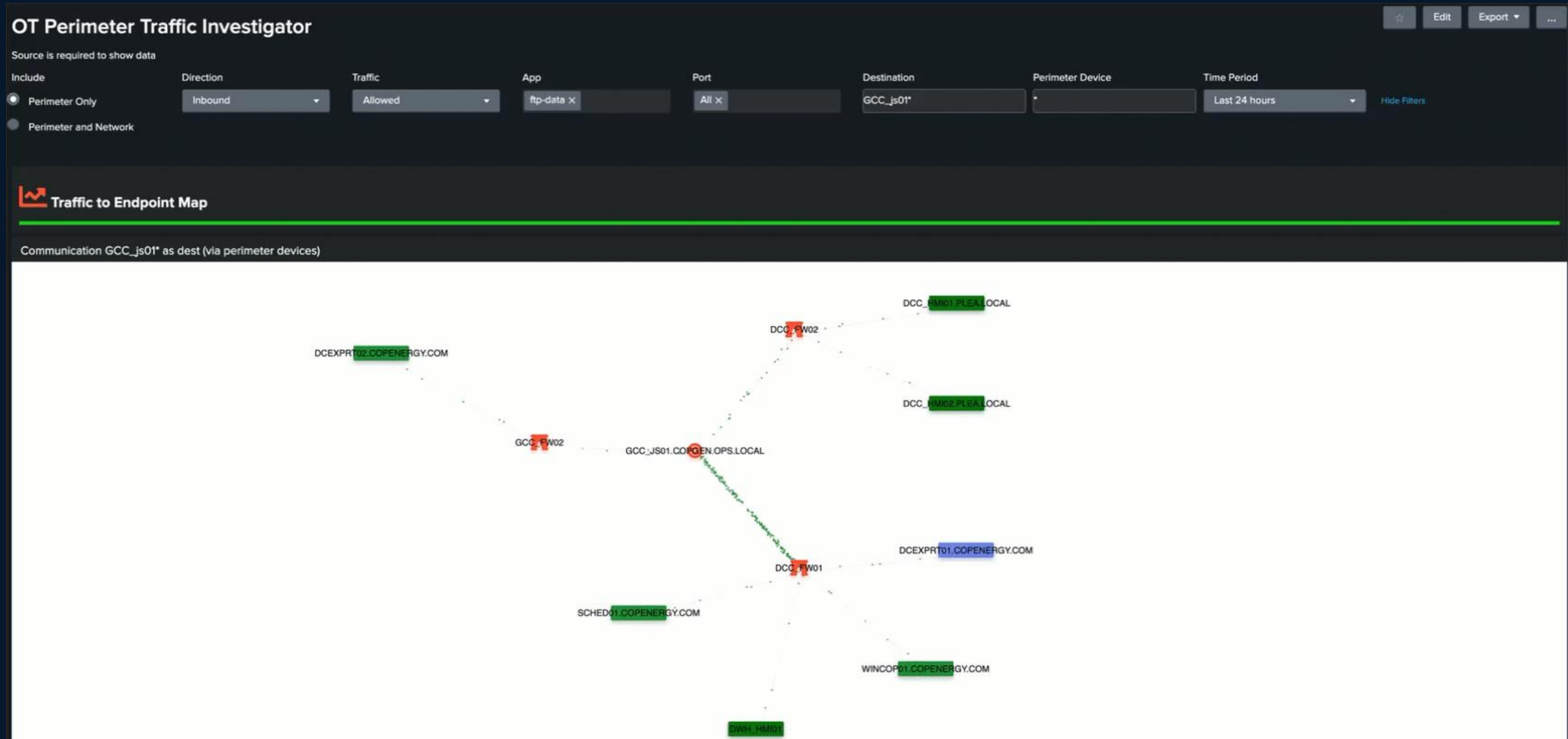
Cisco Industrial Threat Defense: 3 – Detection and Response

Incident Review



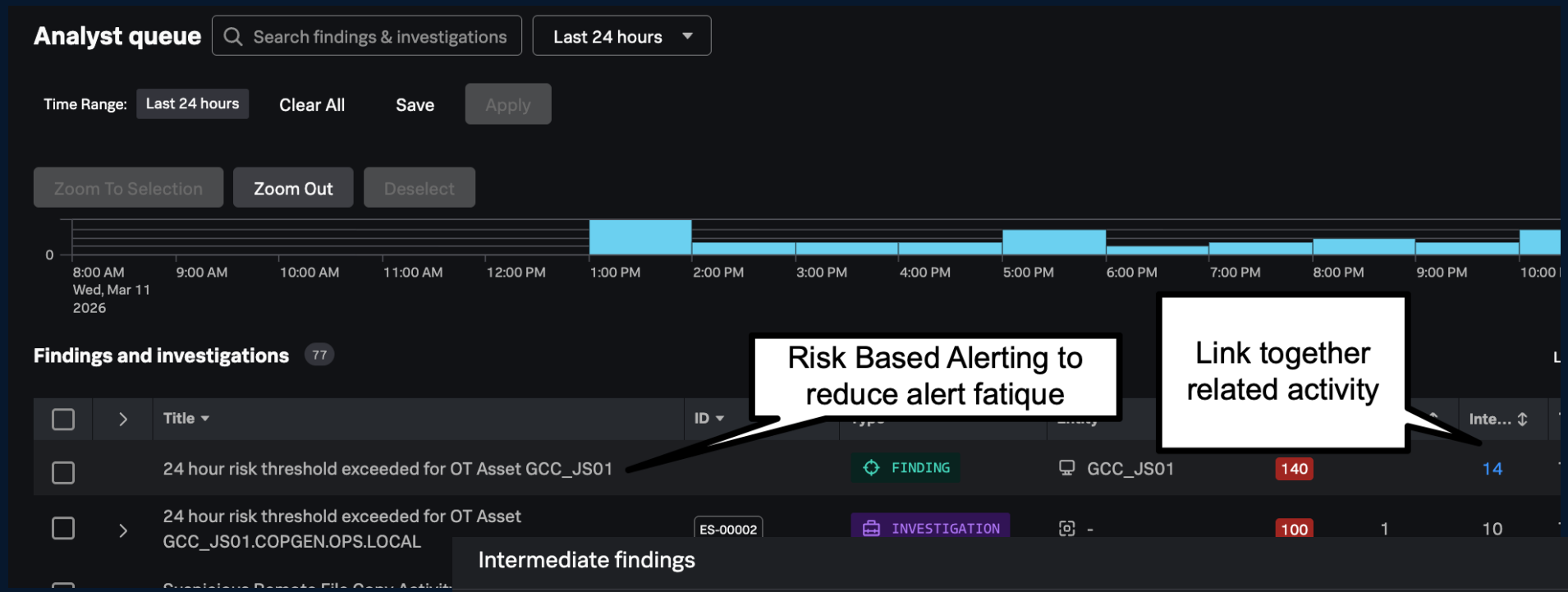
Cisco Industrial Threat Defense: 3 – Detection and Response

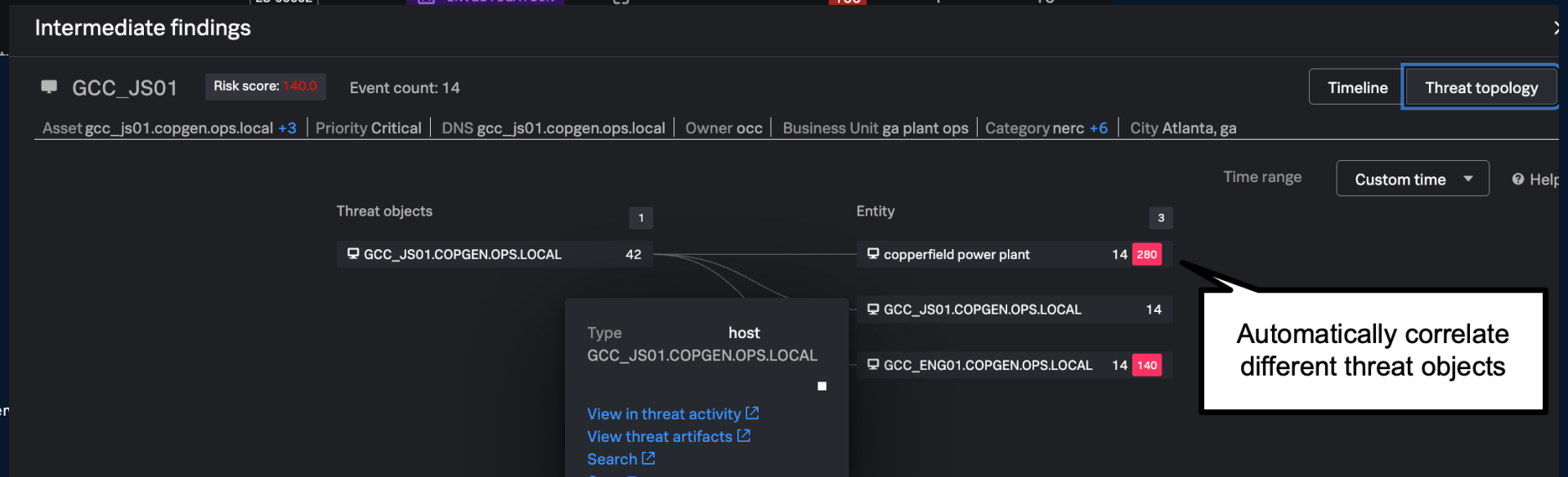
OT Perimeter Security



Cisco Industrial Threat Defense: 3 – Detection and Response

Apply Risk Based Alerting





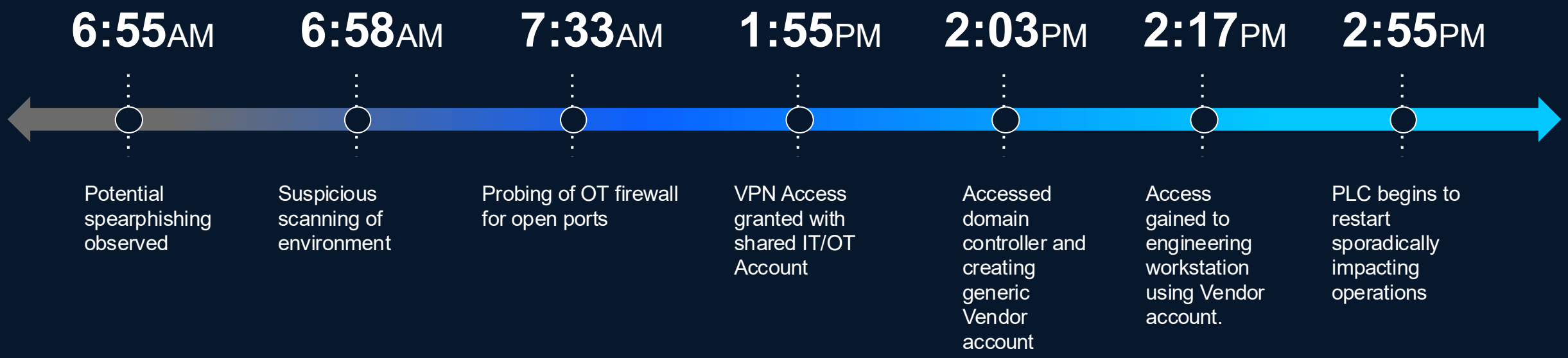
Cisco Industrial Threat Defense: 3 – Detection and Response

Dramatically reduce alert volumes while improving your security posture

Cisco Industrial Threat Defense: 3 – Detection and Response

Traditional Approach

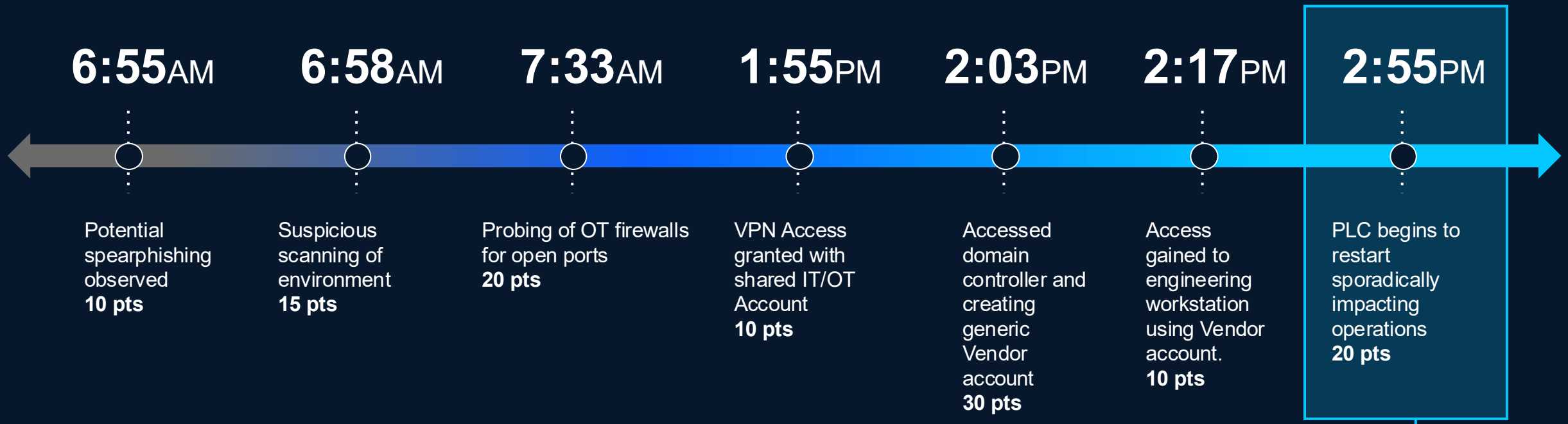
The events below would be considered too noisy and would be abandoned



Cisco Industrial Threat Defense: 3 – Detection and Response

Risk Based Alerting

These events become context that informs high-fidelity alerts



With one click, view all of the risk events that contribute to the alert

ALERT

Risk Incident Rule:

Generate alert for any user or system that exceeds a risk score of 100 in a 24 hour period

Aggregated user risk score **>100**

Thank you


CISCO