

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

Fabrizio Guarneri
Solution Engineer IOT

Chris Duffey
Leader - Industry Specialists



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)

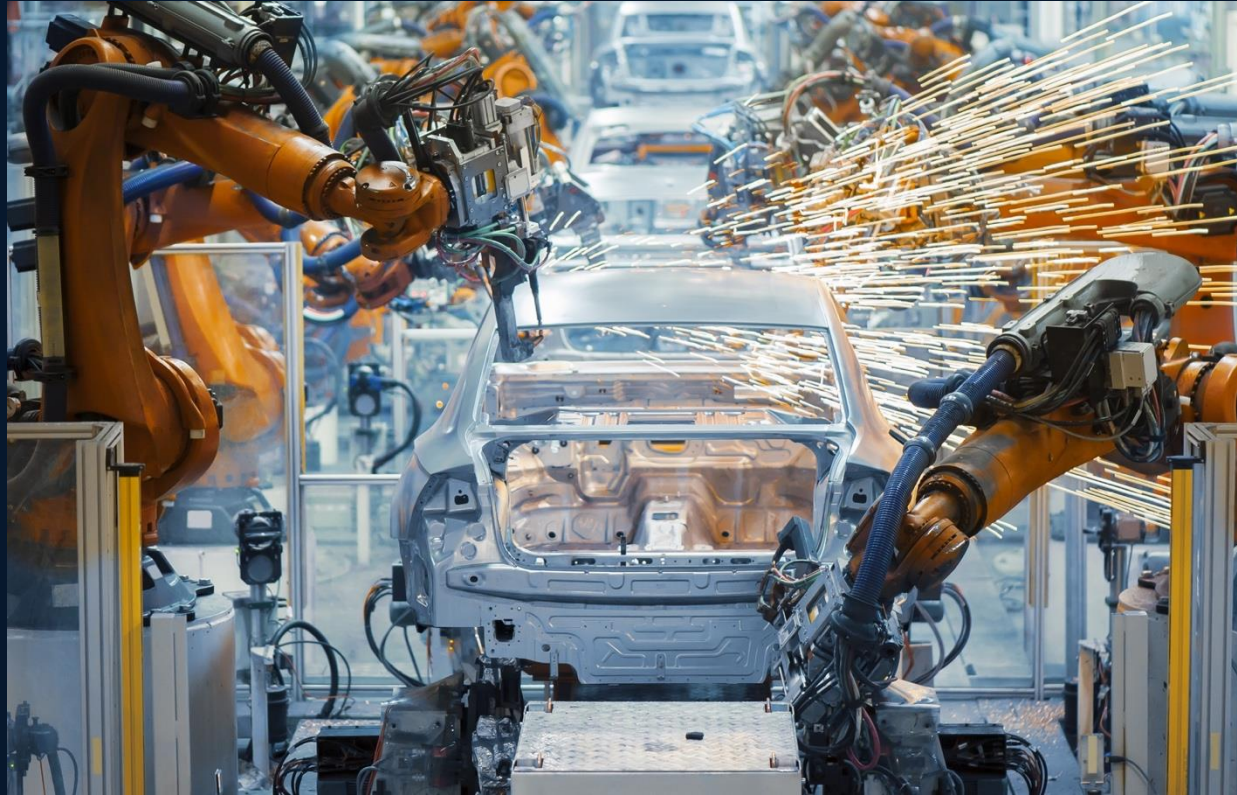
7+ Years at Splunk as part of OT Security Teams

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



Autonomous Vehicles

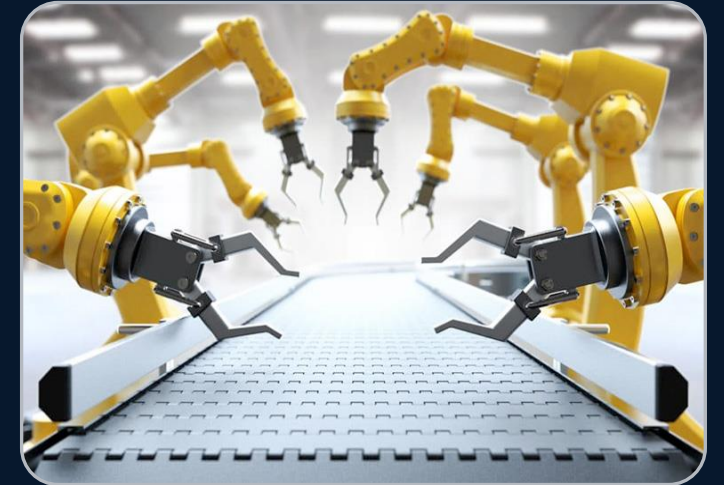


Automated guided vehicles (AGVs), Autonomous mobile robots (AMRs), Tele-remote operations, etc.

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



Software Controls



Software-defined Industrial Automation, Virtual PLCs, etc.

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



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

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

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

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

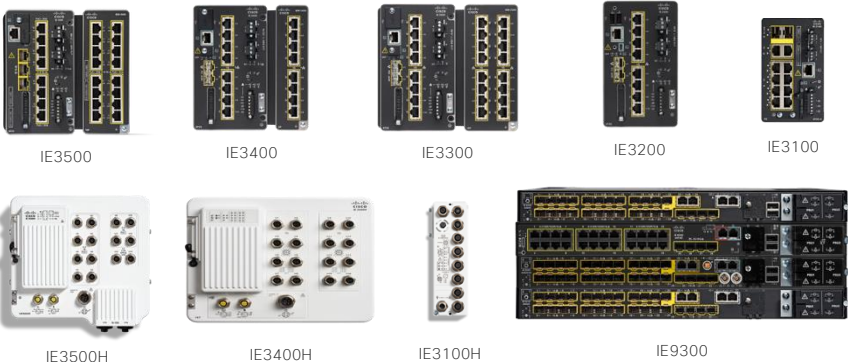
Industry	2022	2021	2020	2019	2018
Manufacturing	24.8%	23.2	17.7	8	10
Finance and insurance	18.9%	22.4	23	17	19
Professional, business and consumer services	14.6%	12.7	8.7	10	12
Energy	10.7%	8.2	11.1	6	6
Retail and wholesale	8.7%	7.3	10.2	16	11
Education	7.3%	2.8	4	8	6
Healthcare	5.8%	5.1	6.6	3	6
Government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



Industrial Cybersecurity

Cyber Vision, Secure Equipment Access



Industrial Wi-Fi and Ultra-reliable Wireless Backhaul

For outdoor conditions



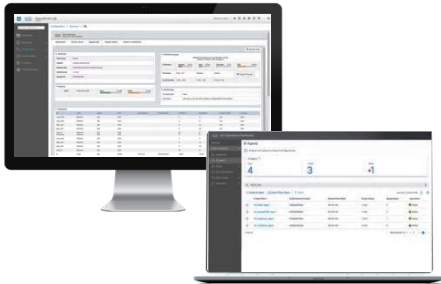
Industrial Routers

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



Data Control and Exchange

Edge Intelligence, IOx



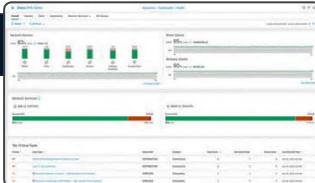
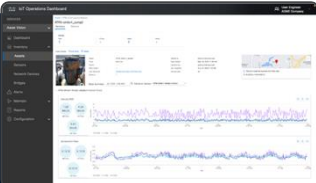
Embedded Networking

Embedded routers and switches for industrial Makers



Management and Automation

Cisco Catalyst Center, Cisco Catalyst WAN Manager, *Meraki



OT Security Framework

Cisco Industrial Threat Defense

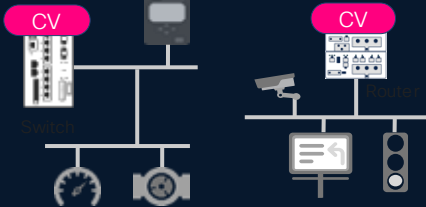
Visibility

OT Asset Visibility and Security Posture

Cisco
Cyber Vision



Network embedded visibility sensor



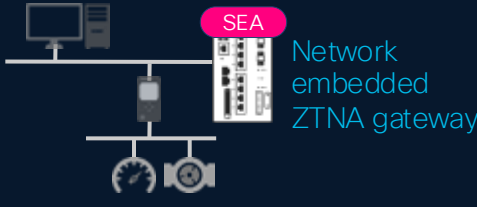
Protection

Zero Trust Security for OT

Secure remote access (ZTNA)

IEC 62443 zone segmentation

Cisco
Secure Equipment Access



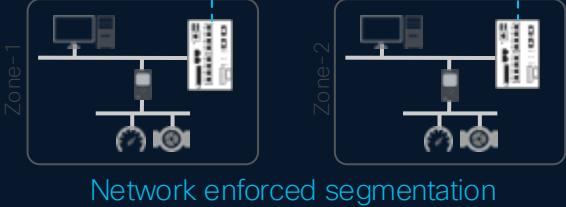
Cisco
Secure Firewall

Cisco
ISE



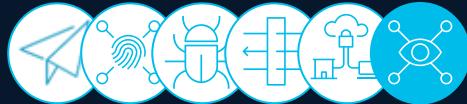
Cyber Vision

Conduit



Detection & Response

Cross-Domain SOC

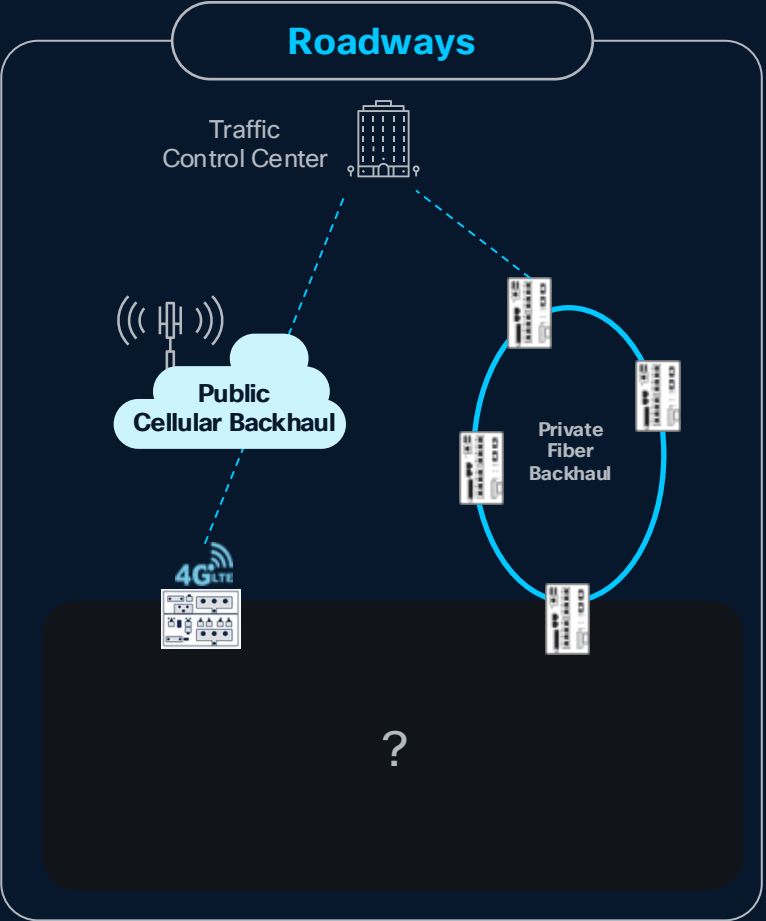
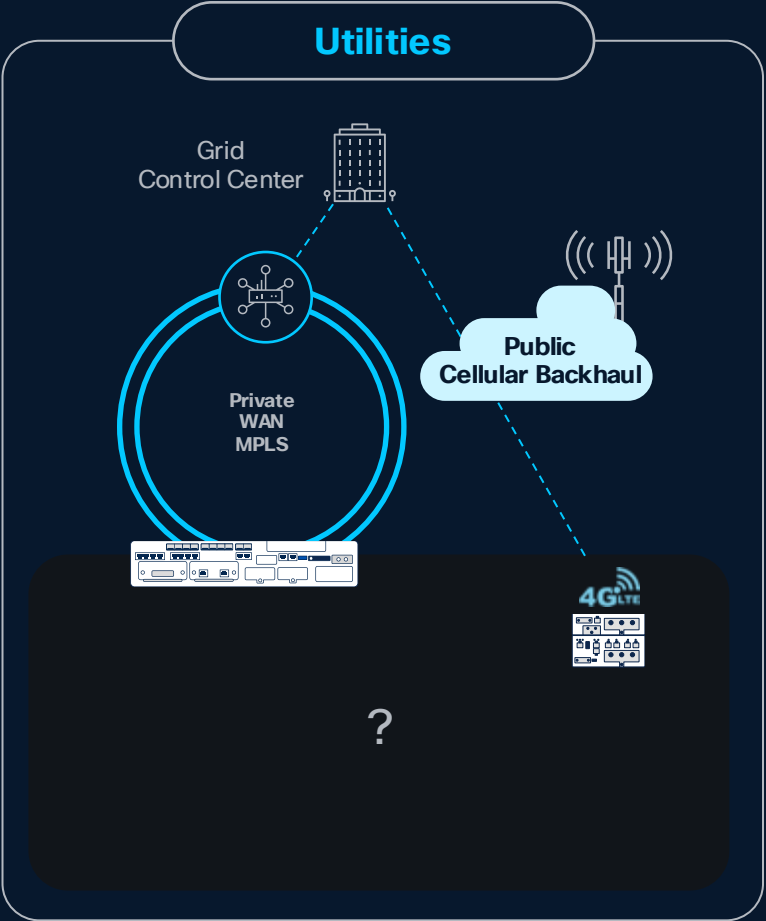
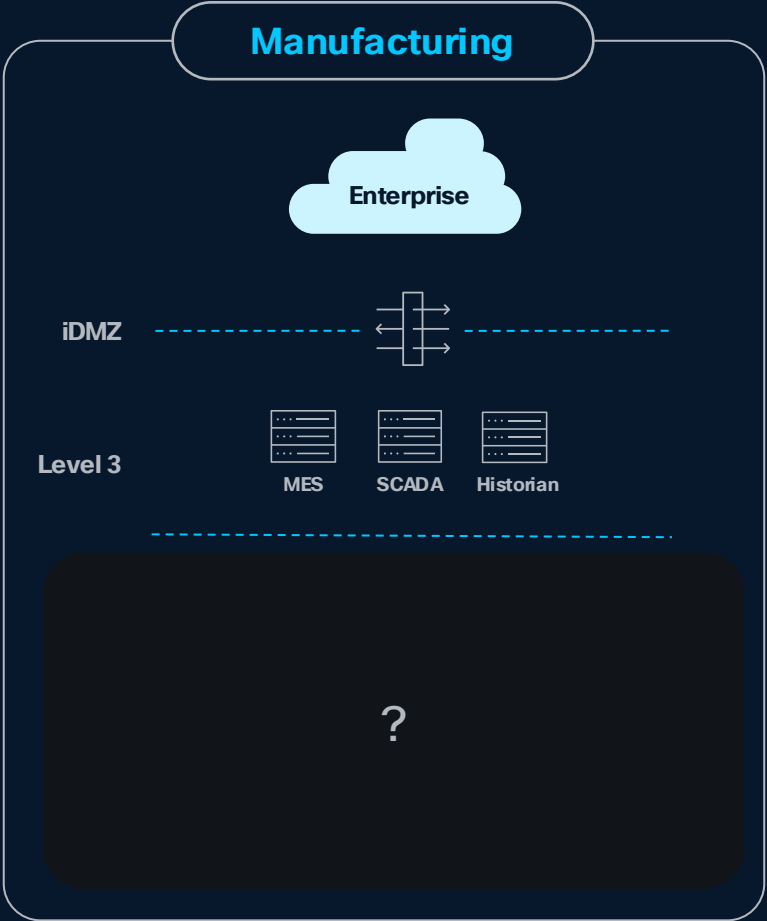


Visibility across the entire attack chain

Network as a fabric to secure OT at scale

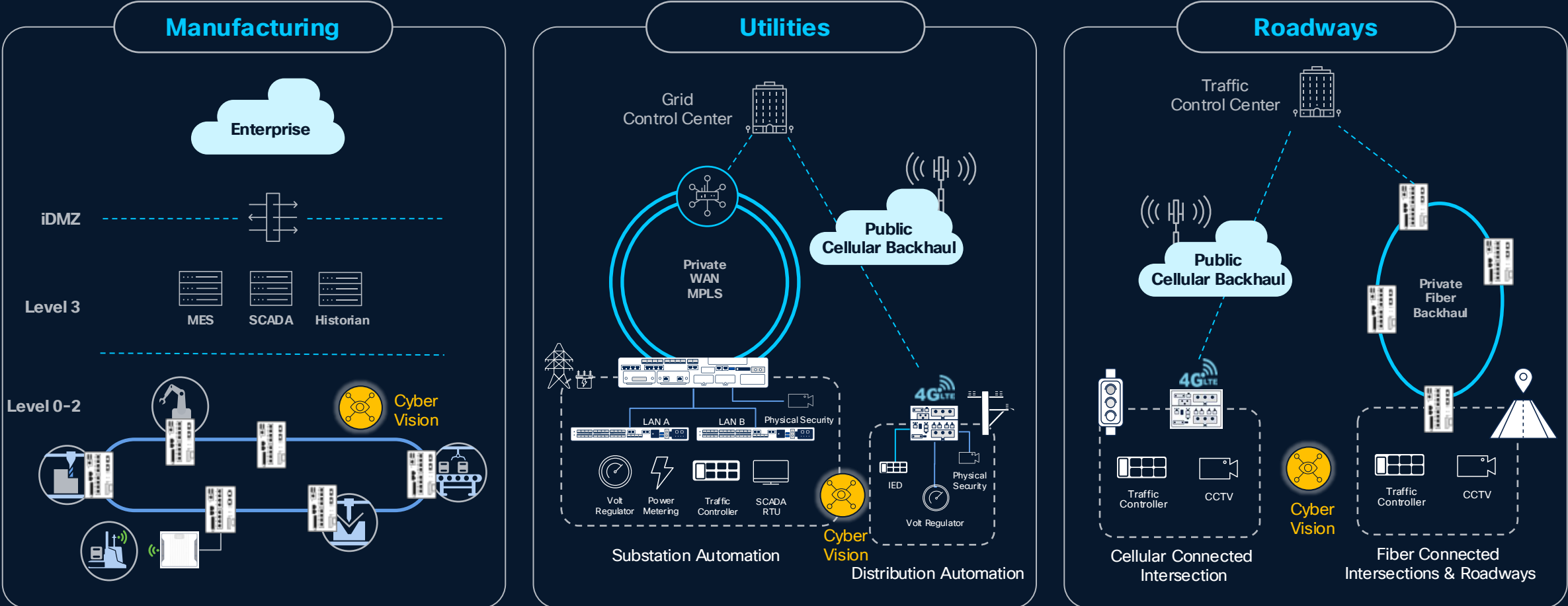
Cisco Industrial Threat Defense: 1 - Visibility

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

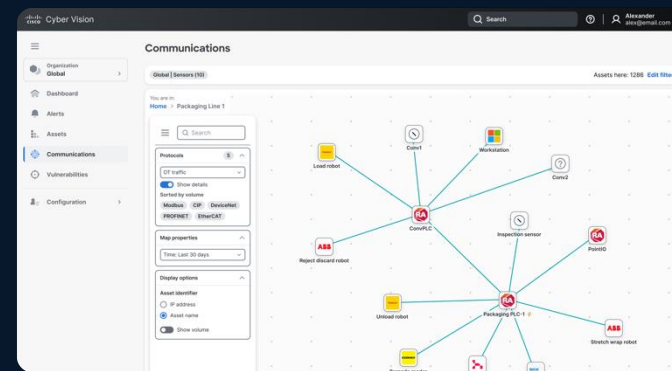


Automated discovery of assets, vulnerabilities, and communication across the industrial network

Visibility built-in, not bolted on

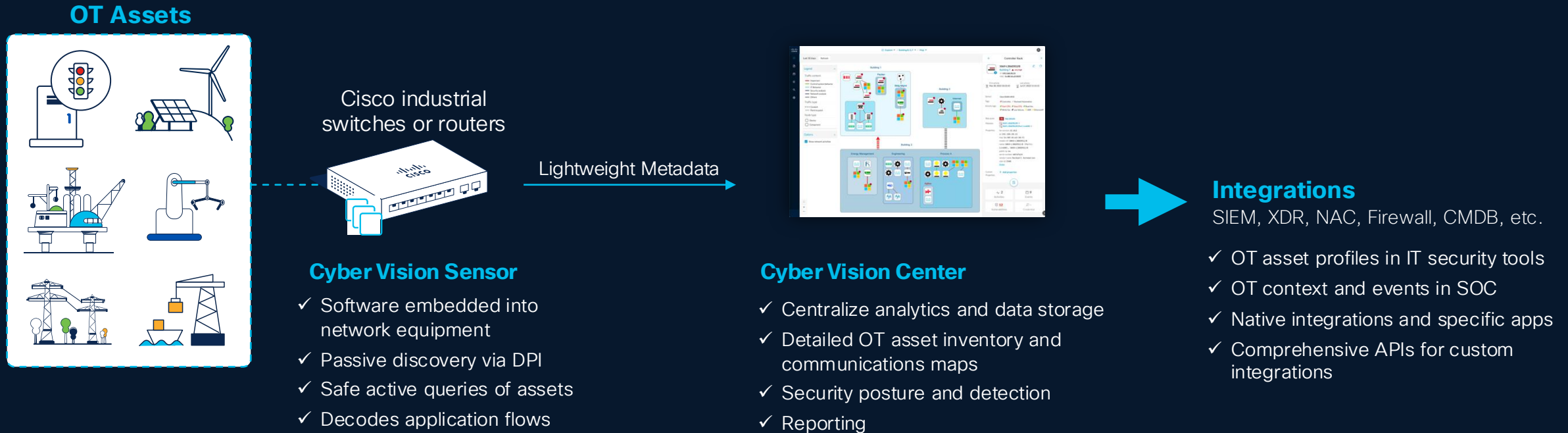
- ✓ Network embedded sensor
No need for addition hardware
- ✓ No need for SPAN collection
networks
- ✓ Active discovery passes NAT
boundaries
- ✓ Comprehensive visibility, even at
lowest Purdue levels

Cyber Vision Center



Cisco Industrial Threat Defense: 1 - Visibility

A two-tier architecture



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



Amazon Web
Services



Microsoft Azure

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

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

Sensors



Sensor

IE3300, IE3400, and
IE3500 Switches



Sensor

IE3400HD and IE3500HD
IP67 Switch



Sensor

Catalyst IR1101
Cellular Router



Sensor

Catalyst IR1800
Cellular Router



Sensor

IDS

Catalyst IR8300
Multiservice Router



Sensor

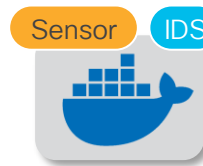
Catalyst IE9300
Rugged Switches



Sensor

IDS

Catalyst 9300/9400
Aggregation Switches



Sensor

IDS

x86 or ARM64 Compute



Sensor

IDS

IC3000 Industrial Compute

Network-Sensors

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

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.

The screenshot displays the Cisco Cyber Vision interface for an asset named **MS206_150LiquidSmoke**. The interface is organized into several sections:

- Summary:** Provides a high-level overview of the asset's status and associated vulnerabilities.
- Attributes:** Lists key details such as Type (PLC), Vendor (Rockwell Automation), Functional Group (Global distributed OT process), Firmware Version (36.12), Model (1756-L72/B LOGIX5572), Reference (1756-L72/B LOGIX5572), Serial Number (00c95608), and Primary Interface (IP Address: 10.112.204.150, VLAN: 204, Network: MS - Line 1).
- Top 5 Vulnerabilities:** A table listing the most critical vulnerabilities for this asset.
- Rack Slots:** A table providing detailed information for each of the 9 rack slots, including slot number, model name, type, firmware version, and serial number.

Alerts	Name	Cisco Security Risk Score	CVSS Score
-	Multiple Rockwell Automation Products CVE-2018-17924 Remote D...	51 Medium	8.6 High
-	Inclusion of Functionality from Untrusted Control Sphere Vulnerability ...	34 Medium	10 Critical
-	Insufficiently protected credentials in Logix controllers	34 Medium	9.8 Critical

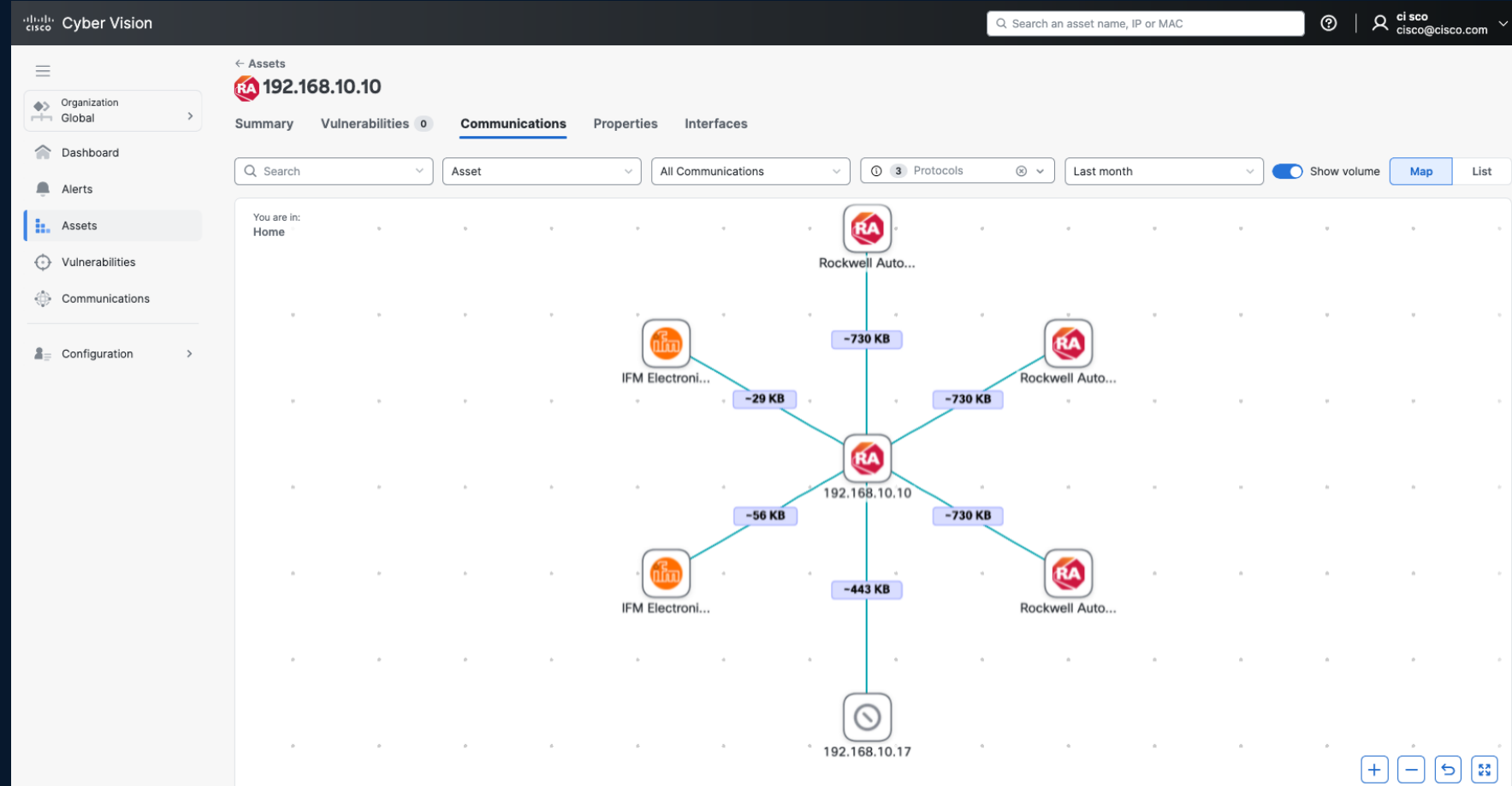
Slot #	Model Name	Type	Firmware Version	Serial Number
Port1-Link00	1756-L72/B LOGIX5572	CPU	36.12	00c95608
Port1-Link01	1756-IB16/A DCIN	IO Module	2.5	001fe071
Port1-Link02	1756-IB16/A DCIN	IO Module	3.3	008fe8e5
Port1-Link03	1756-OB16E/A DCOU ...	IO Module	3.4	00bbb84c
Port1-Link05	1756-IF8/A	IO Module	1.5	002cbabb
Port1-Link06	1756-ENBT/A	Communication Module	6.6	0077c07c
Port1-Link07	1756-HSC/A Ver. 1.5	IO Module	1.5	80203fe0
Port1-Link08	1756-HSC/A Ver. 1.4.35	IO Module	1.4	802026cd
Port1-Link09	1756-EN3TR/B	Communication Module	12.1	0116cdb8

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

CVE-2025-7353

Remote Code Execution Vulnerability in Rockwell ControlLogix Ethernet

Cisco Security Risk Score 56
Medium ⚠️

CVSS Score 9.8
Critical 🔴

Details

Description
A security issue exists due to the web-based debugger agent enabled on released devices. If a specific IP address is used to connect to the WDB agent, it can allow remote attackers to perform memory d...
[View more](#)

Mitigation
Update to version 12.001

Published on
August 14, 2025

Attack Vector
Network

Attack Complexity
Low

Exploit code maturity
Unproven that exploit exists

Links
<https://nvd.nist.gov/vuln/detail/CVE-2025-7353>
<https://www.rockwellautomation.com/literature/0-100-01732-101/industrial-security-advisory.SD1732.html>

MITRE ATT&CK®

⚠️ 3 Tactics matched

Description
Tactics represent an attacker's goals, such as gaining initial access, escalating privileges, or evading detection.

TA0009 - Collection ⚠️ 1 Technique matched

ID	Name
T1005	Data from Local System

TA0002 - Execution ⚠️ 2 Techniques matched

ID	Name
T1106	Native API
T1203	Exploitation for Client Execution

TA0004 - Privilege Escalation ⚠️ 2 Techniques matched

ID	Name
----	------

© 2026 Cisco and/or its affiliates. All rights reserved.

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

The screenshot displays the Cisco Cyber Vision Alerts interface. The top navigation bar includes the Cisco logo, the text 'Cyber Vision', a search bar, and a user profile icon for 'alex@email.com'. The left sidebar contains navigation options: Organization (Global), Dashboard, Alerts (selected), Assets, Communications, Vulnerabilities, and Configuration. The main content area is titled 'Alerts' and shows 4 alerts. A summary bar indicates 2 Critical, 1 High, 0 Medium, and 1 Low alerts. Below this is a table of alerts with columns for Alert Type, Trigger, Instances, Severity, Triggered By, and Last Detected. The first alert is 'Malicious Domains' triggered by 'darkweb.com (4.0.1.20)' with 2 instances and a Critical severity. The second alert is 'Severe Vulnerabil...' triggered by 'CVE-2022-1161 - Inclusion of Functionality f...' with 2 instances and a Critical severity. A detailed view for this alert is expanded, showing the title 'CVE-2022-1161 - Inclusion of Functionality from Untrusted Control Sphere Vulnerability in Rockwell Automation Logix Controllers' and a description: '2 monitored assets are affected by this vulnerability which CVSS score is ≥ than the threshold defined in the alert rules.' Below the description is a table with columns: Cisco Security Risk Score (86 High), CVSS Score (9.2 Critical), Exploitability (Functional exploit exists), and Attack vector (Network). The third alert is 'Severe Vulnerabil...' triggered by 'CVE-2025-9102 - Out-of-bounds Write Vuln...' with 3 instances and a High severity. The fourth alert is 'End of Support Fir...' triggered by 'Allen Bradley / SLC505 / 18.01' with 1 instance and a Low severity. The bottom right of the interface shows 'Rows per page' set to 30 and '1-12 of 12' results.

Alert Type	Trigger	Instances	Severity	Triggered By	Last Detected	
<input type="checkbox"/>	Malicious Domains	darkweb.com (4.0.1.20)	2	Critical	Communication	Dec 10, 2024 10:30 AM
<input checked="" type="checkbox"/>	Severe Vulnerabil...	CVE-2022-1161 - Inclusion of Functionality f...	2	Critical	Vulnerability	Dec 10, 2024 10:30 AM
<input type="checkbox"/>	Severe Vulnerabil...	CVE-2025-9102 - Out-of-bounds Write Vuln...	3	High	Vulnerability	Dec 10, 2024 10:30 AM
<input type="checkbox"/>	End of Support Fir...	Allen Bradley / SLC505 / 18.01	1	Low	Vulnerability	Dec 10, 2024 10:30 AM

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

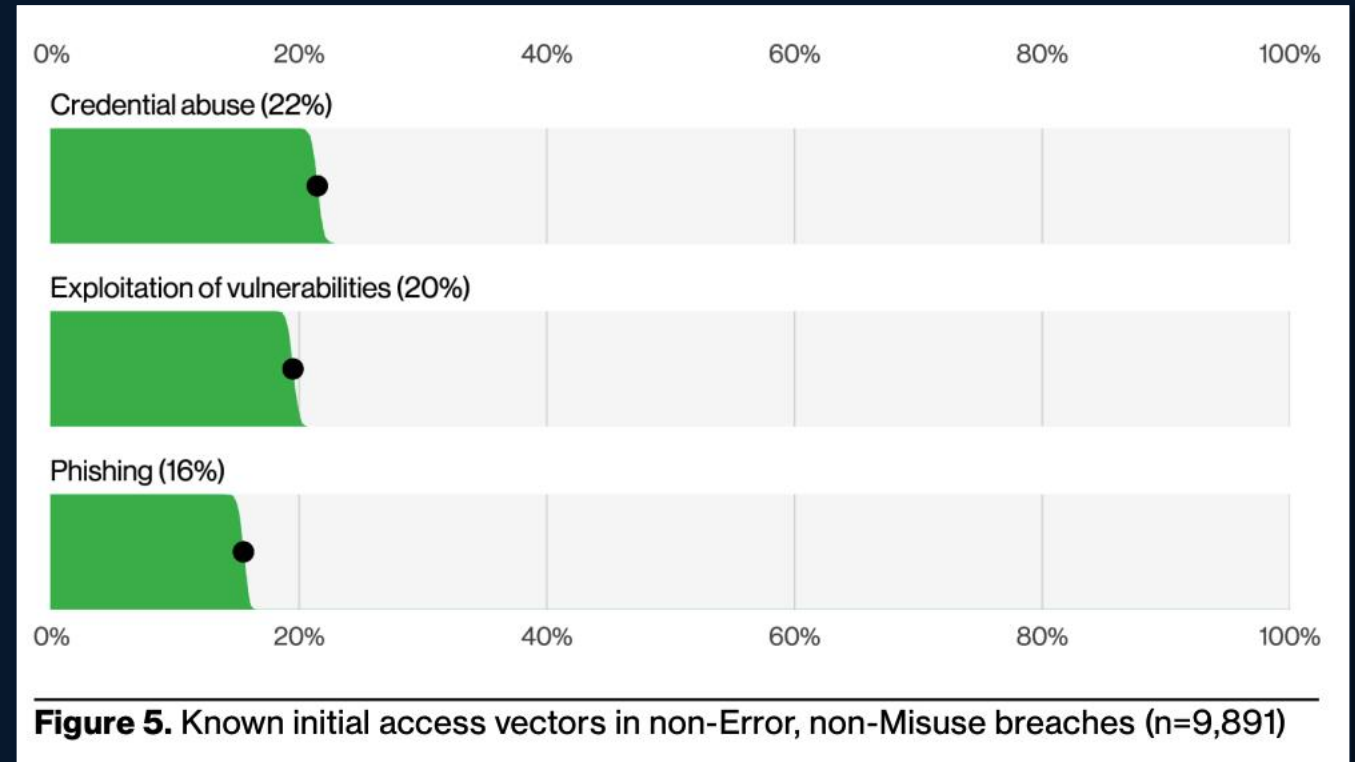
Trends in the market

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



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



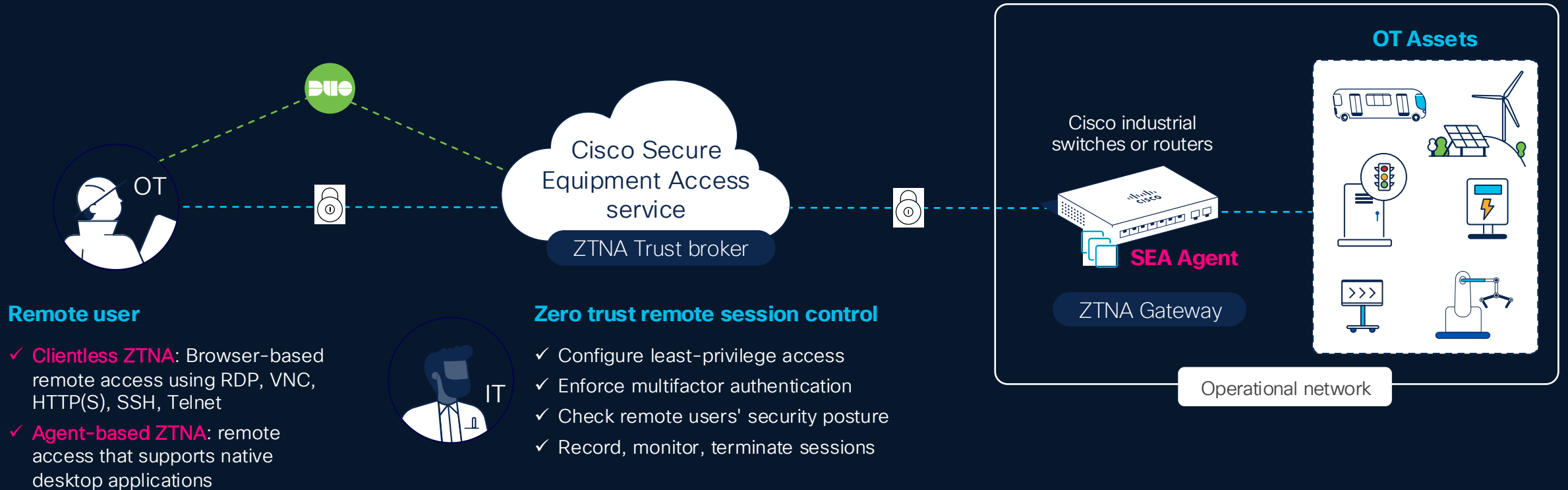
VPN

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



Cloud simple

Accelerate time to value



Cisco secure

Built to keep operations safe



Designed for OT

Drive business outcomes

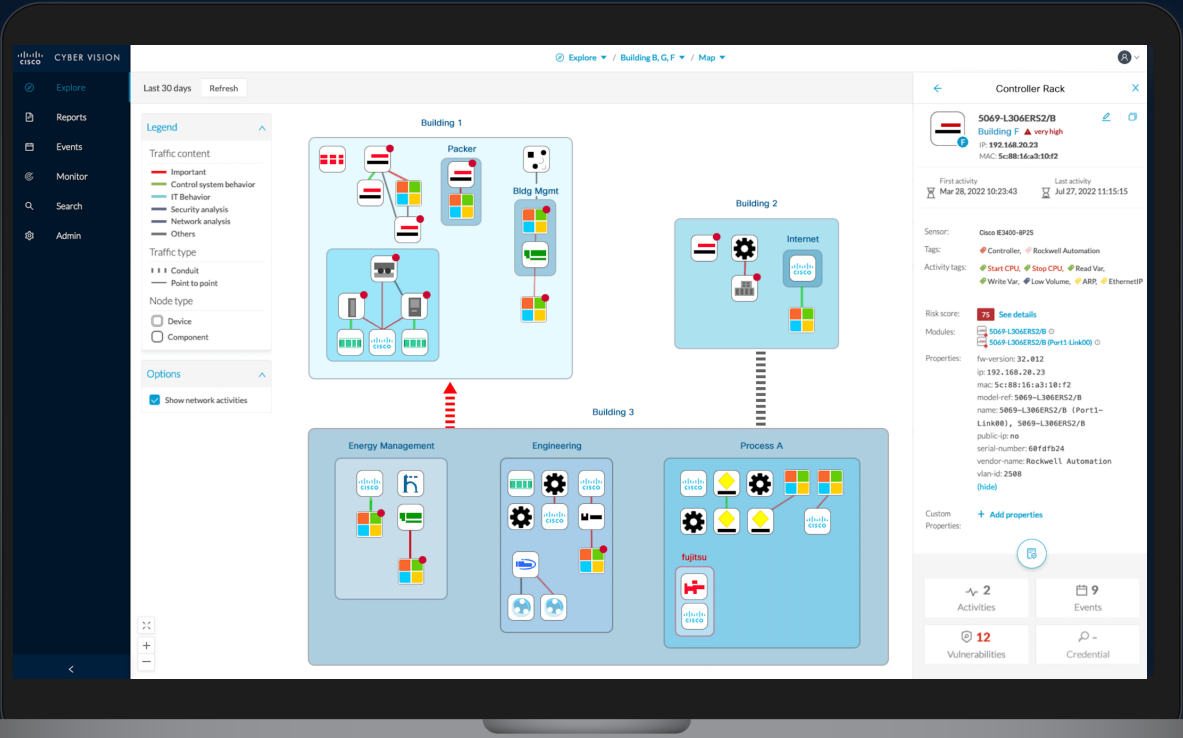


Highly scalable

Cloud + network working together

Cisco Industrial Threat Defense: 2 - Protection (Within)

Leveraging visibility to drive segmentation

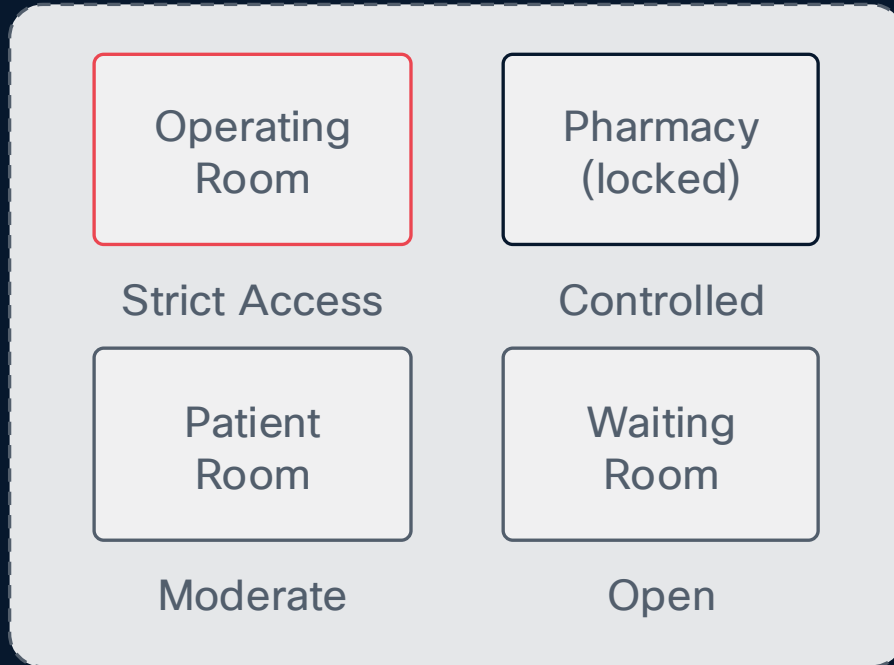


IEC-62443 virtual segmentation

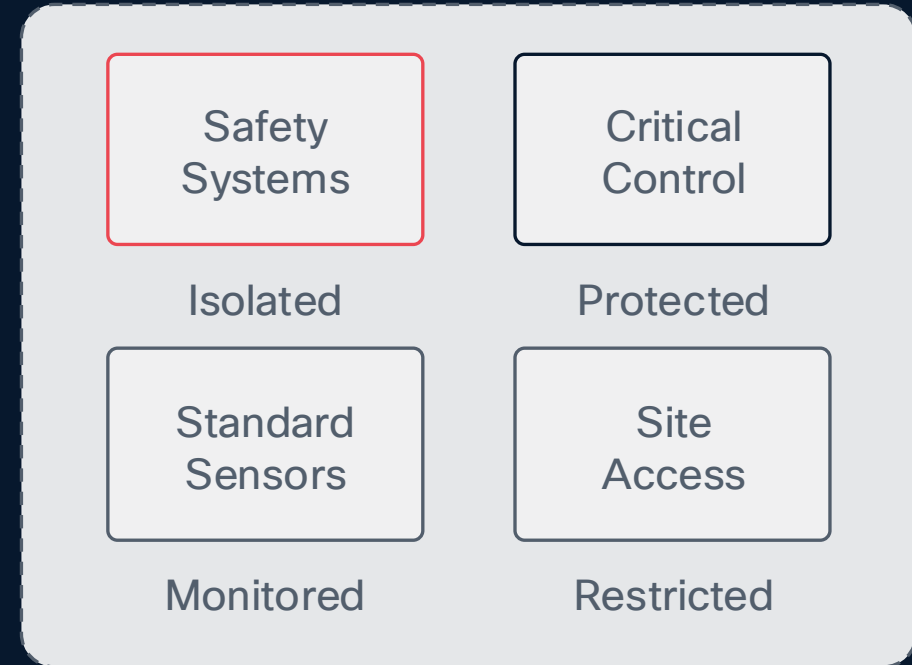
- ✓ Group OT assets into zones
- ✓ Visualize conduits
- ✓ Identify traffic violations
- ✓ Share context with other platforms to enforce segmentation

Cisco Industrial Threat Defense: 2 - Protection (Within)

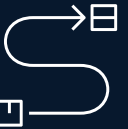
Zone Group Assets with Similar Security Requirements



Hospital Floor Plan



Industrial Plant

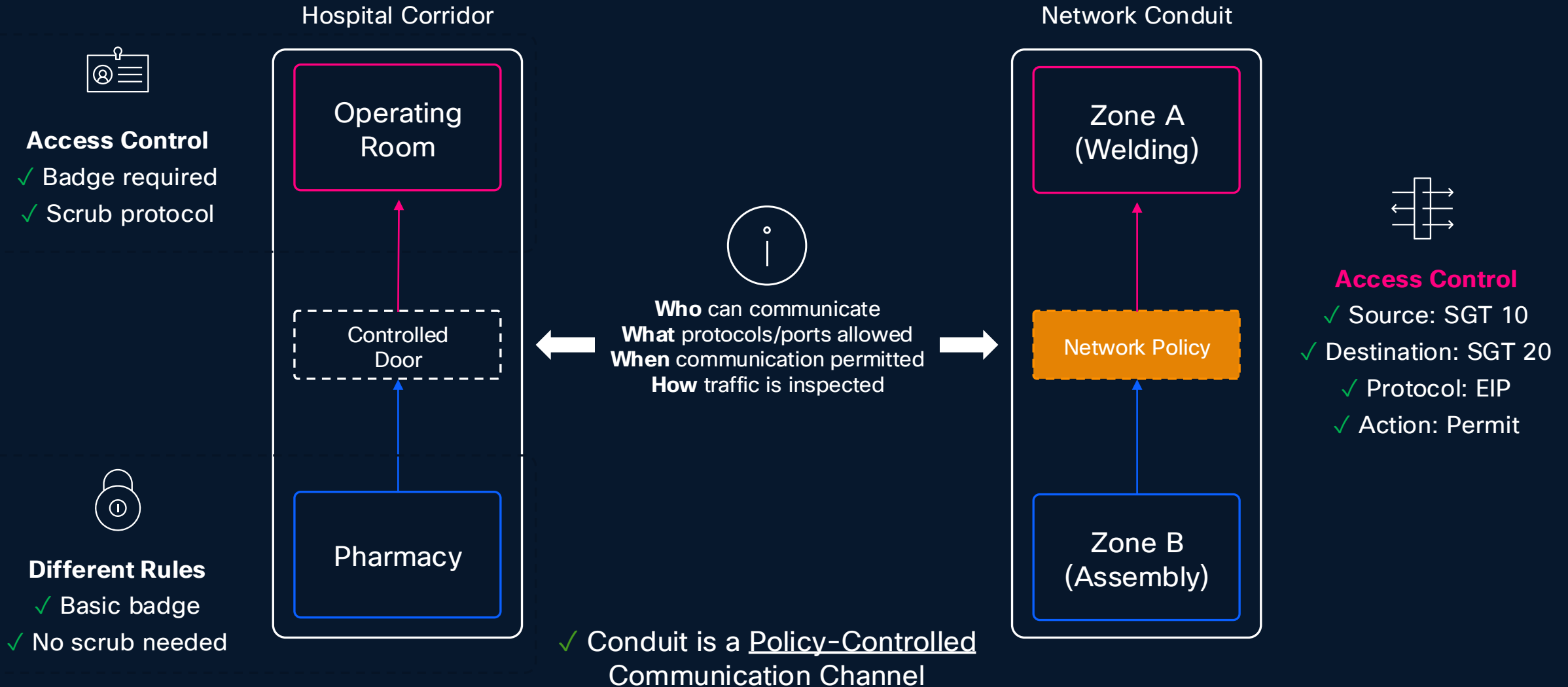


Same Principle in OT Networks

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

Cisco Industrial Threat Defense: 2 - Protection (Within)

Conduits Control Communication Between Zones




Cisco Industrial Threat Defense: 2 - Protection (Within)

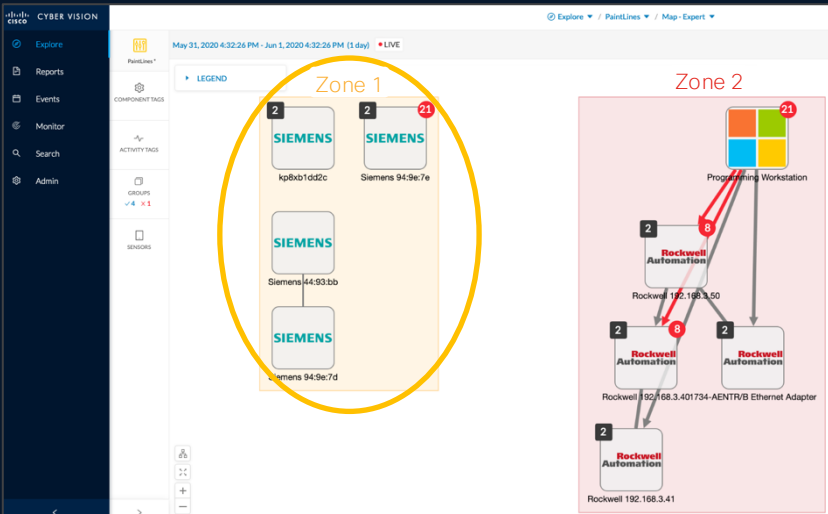
Conduits Control Communication Between Zones



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



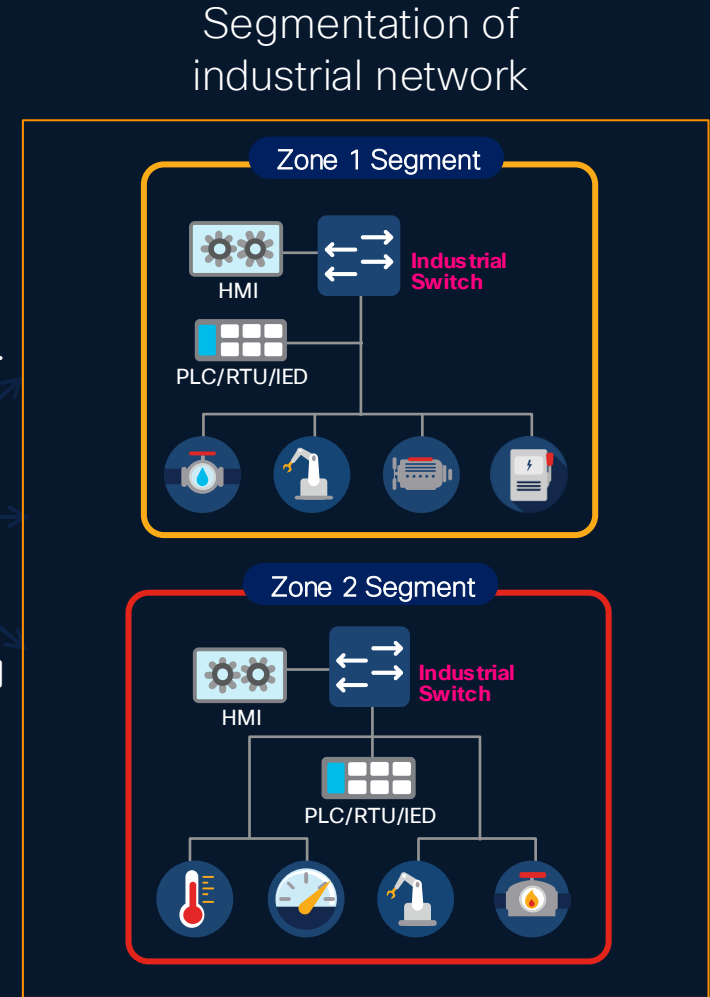
I now have OT context to build the right network access policies



Cisco Cyber Vision Map View

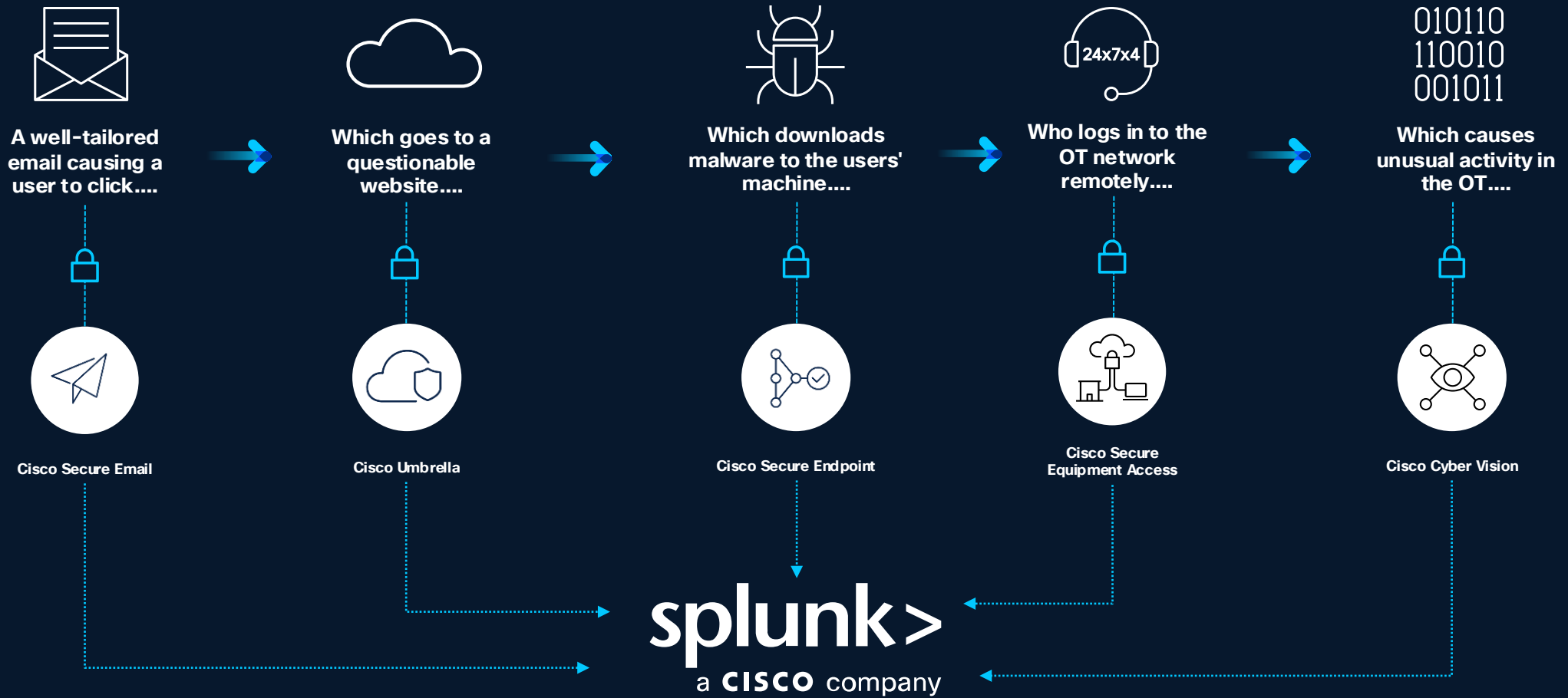
	Zone 1	Zone 2	PLC	MES
Zone 1	✓	X	✓	X
Zone 2	X	✓	✓	X
PLC	✓	✓	✓	✓
MES	X	X	✓	✓

Cisco Firewall Policy Matrix
or
Cisco ISE Policy Matrix



Cisco Industrial Threat Defense: 3 – Detection and Response

Detecting threats requires cross-domain visibility

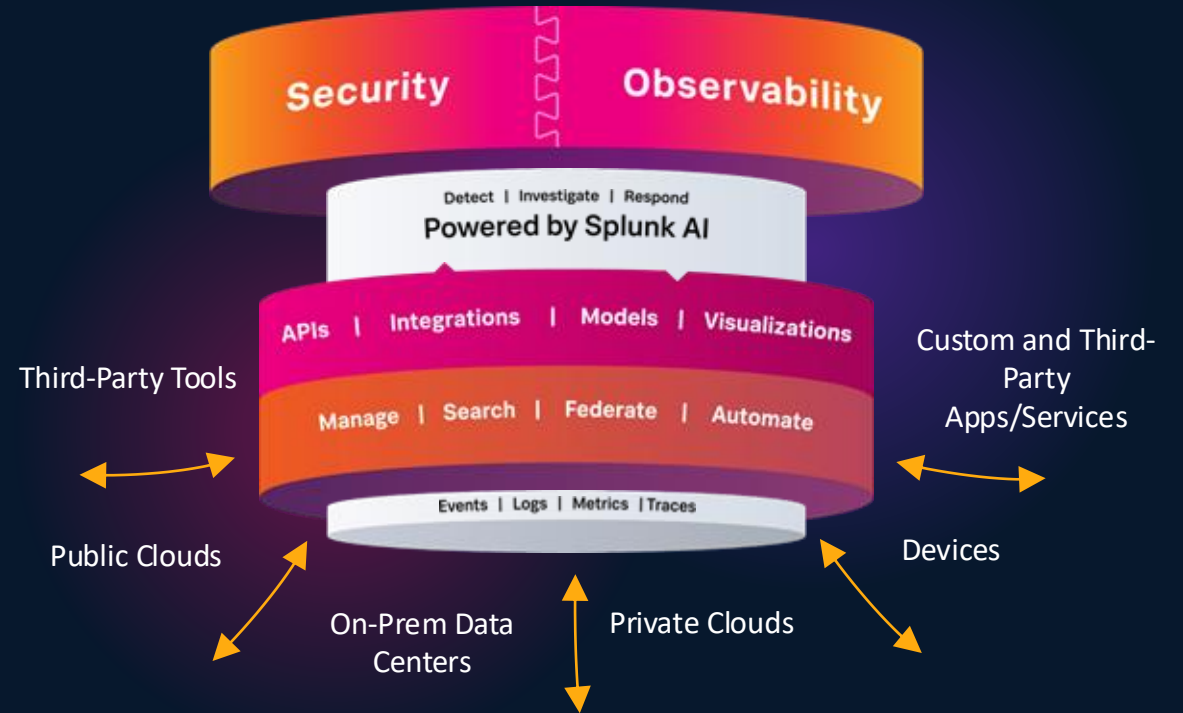


Cisco Industrial Threat Defense: 3 – Detection and Response

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



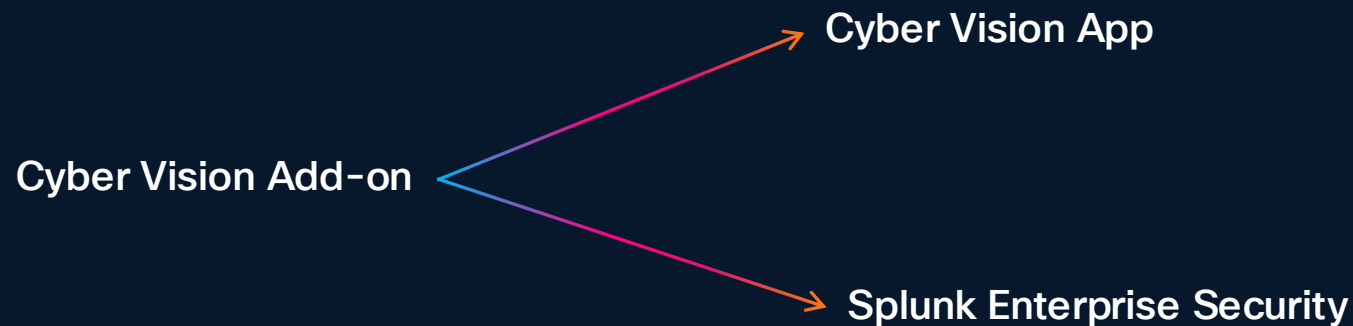
- Logs (OS, App, etc.)
- Vulnerabilities
- Network/Firewall Traffic
- Asset Inventory
- Security Events
- Endpoint activity
- Ticketing

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

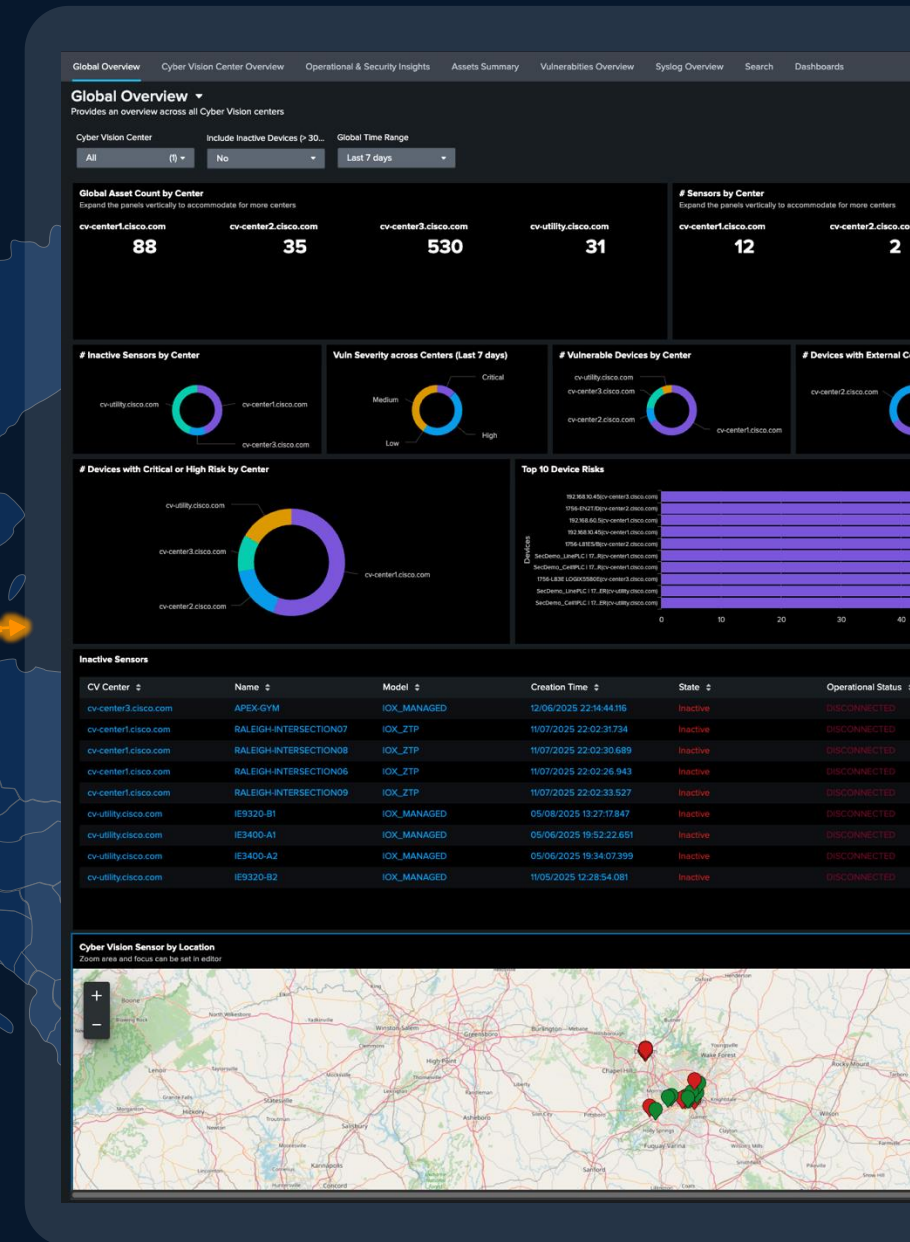


Cisco Industrial Threat Defense: 3 – Detection and Response

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

Global Overview ▾
Provides an overview across all Cyber Vision centers

Cyber Vision Center: All (1) | Include Inactive Devices (>30...): No | Global Time Range: Last 7 days

Global Asset Count by Center

Expand the panels vertically to accommodate for more centers

cv-center1.cisco.com	cv-center2.cisco.com	cv-center3.cisco.com	cv-utility.cisco.com
88	35	530	31

Sensors by Center

Expand the panels vertically to accommodate for more centers

cv-center1.cisco.com	cv-center2.cisco.com	cv-center3.cisco.com
12	2	2

Inactive Sensors by Center

Vuln Severity across Centers (Last 7 days)

Vulnerable Devices by Center

Devices with External Communications

Devices with

Devices with Critical or High Risk by Center

Top 10 Device Risks

192.168.10.45(cv-center3.cisco.com)	65
1756-EN27-D(cv-center2.cisco.com)	60
192.168.60.59(cv-center1.cisco.com)	55
192.168.10.49(cv-center1.cisco.com)	50
1756-L8E5-B(cv-center2.cisco.com)	45
SecDemo_LinePLC1_17_R(cv-center1.cisco.com)	40
SecDemo_CatPLC1_17_R(cv-center1.cisco.com)	35
1756-L8E1-L00X0500E(cv-center3.cisco.com)	30
SecDemo_LinePLC1_17_EB(cv-utility.cisco.com)	25
SecDemo_CatPLC1_17_EB(cv-utility.cisco.com)	20

Inactive Sensors

CV Center	Name	Model	Creation Time	State	Operational Status	Enrollment Status
cv-center3.cisco.com	APEX-GYM	IOX_MANAGED	12/06/2025 22:14:44.116	Inactive	DISCONNECTED	ENROLLED
cv-center1.cisco.com	RALEIGH-INTERSECTION07	IOX_ZTP	11/07/2025 22:02:31.734	Inactive	DISCONNECTED	ENROLLED
cv-center1.cisco.com	RALEIGH-INTERSECTION08	IOX_ZTP	11/07/2025 22:02:30.689	Inactive	DISCONNECTED	ENROLLED
cv-center1.cisco.com	RALEIGH-INTERSECTION06	IOX_ZTP	11/07/2025 22:02:26.943	Inactive	DISCONNECTED	ENROLLED
cv-center1.cisco.com	RALEIGH-INTERSECTION09	IOX_ZTP	11/07/2025 22:02:33.527	Inactive	DISCONNECTED	ENROLLED
cv-utility.cisco.com	IE9320-B1	IOX_MANAGED	05/08/2025 13:27:17.847	Inactive	DISCONNECTED	ENROLLED
cv-utility.cisco.com	IE3400-A1	IOX_MANAGED	05/06/2025 19:52:22.651	Inactive	DISCONNECTED	ENROLLED
cv-utility.cisco.com	IE3400-A2	IOX_MANAGED	05/06/2025 19:34:07.399	Inactive	DISCONNECTED	ENROLLED
cv-utility.cisco.com	IE9320-B2	IOX_MANAGED	11/05/2025 12:28:54.081	Inactive	DISCONNECTED	ENROLLED

Cyber Vision Sensor by Location

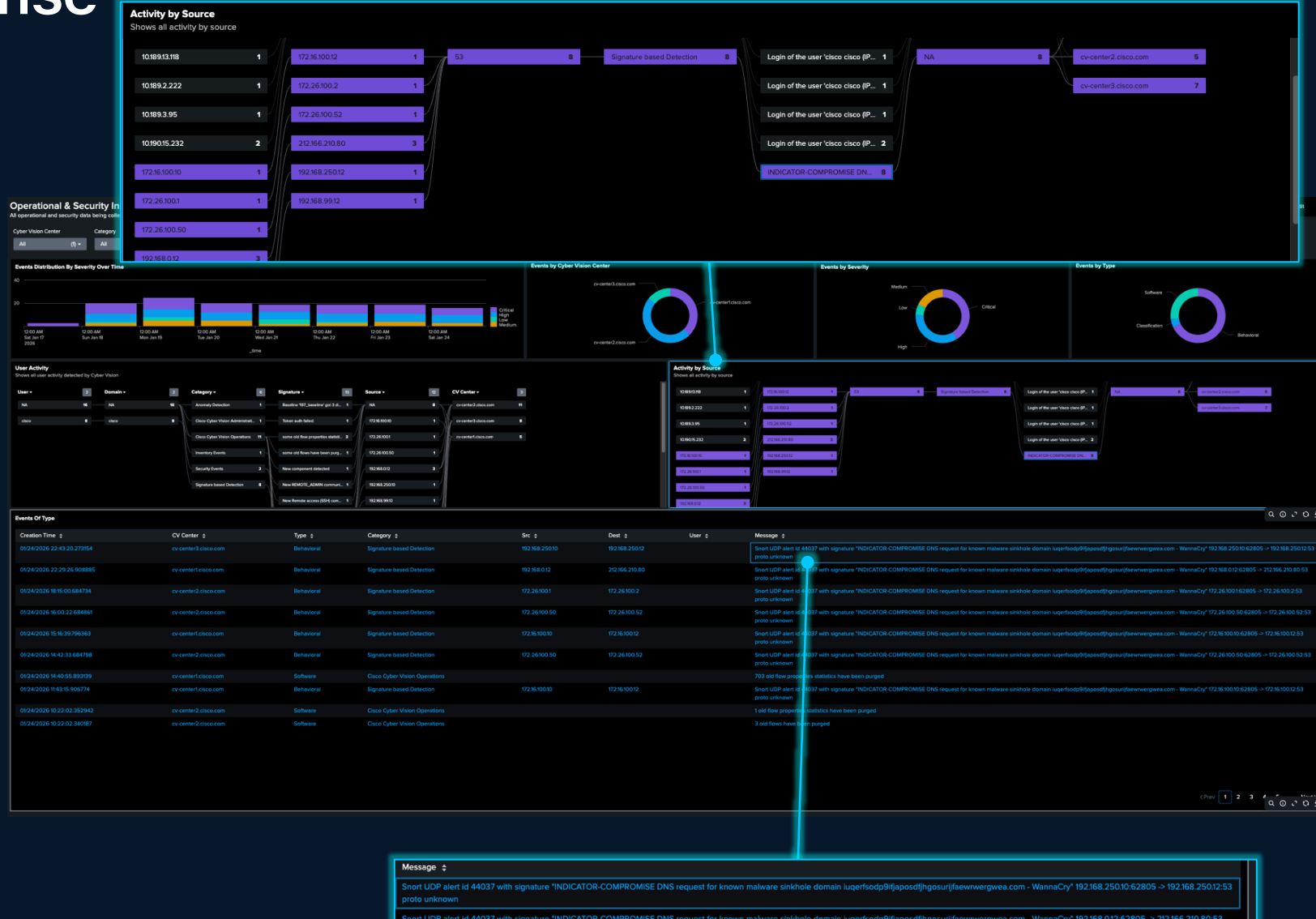
Zoom area and focus can be set in editor

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

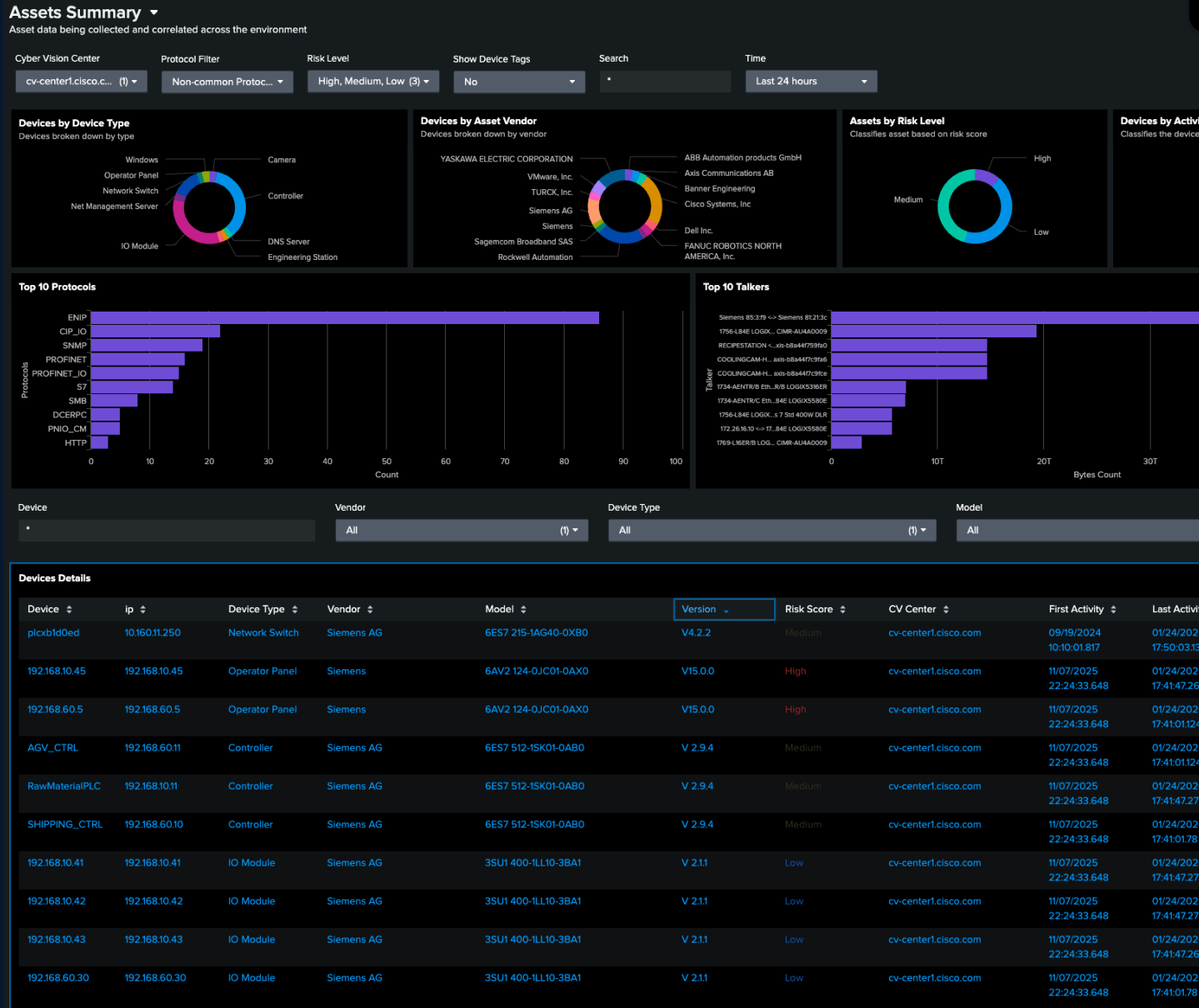


Cisco Industrial Threat Defense: 3 – Detection and Response

Cyber Vision Splunk App

Asset summary

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

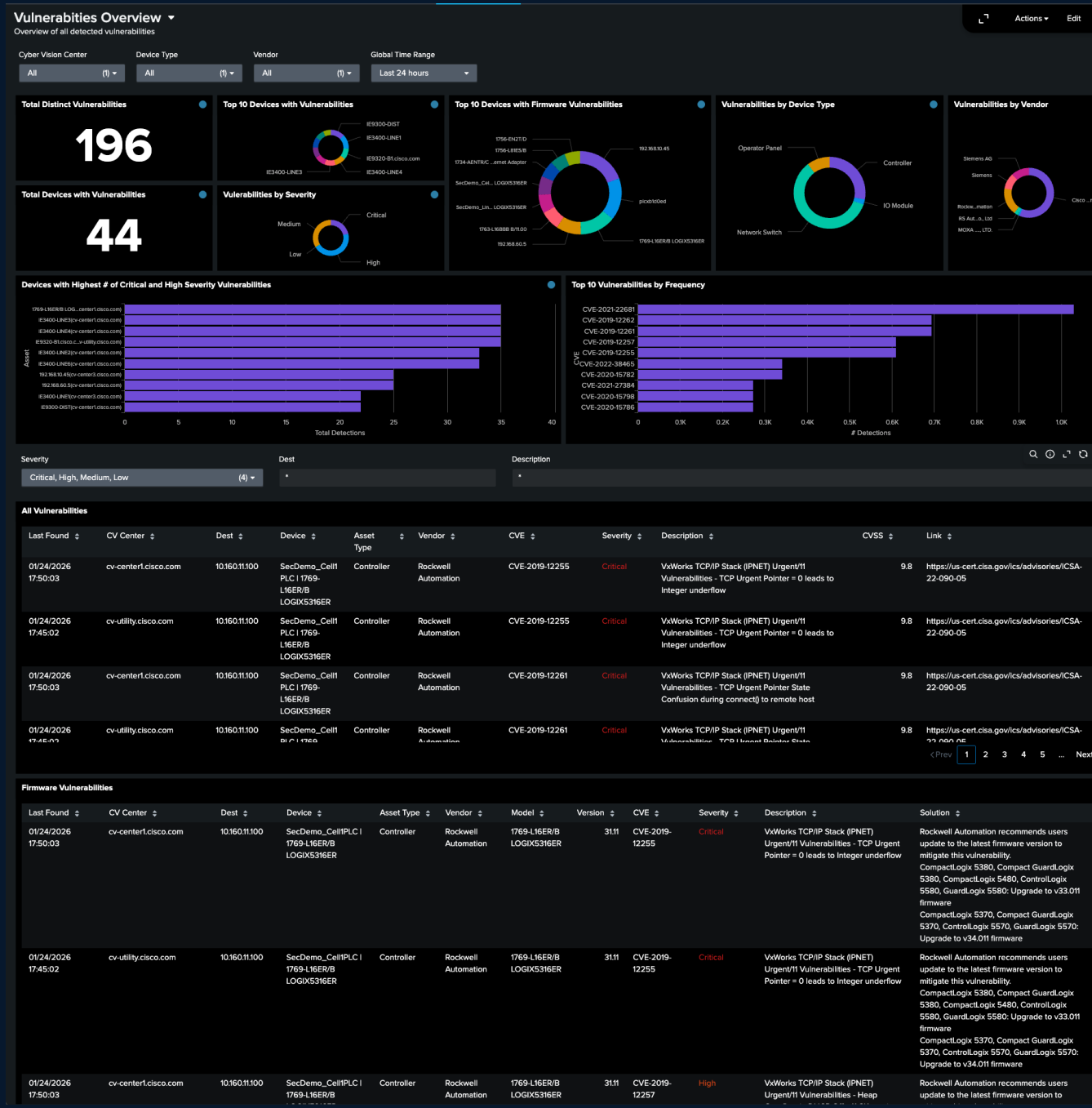


Cisco Industrial Threat Defense: 3 – Detection and Response

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

OT Security Posture

☆ Edit Export ...

Facility/Site: All System: All Business Unit: All Time Period: Last 24 hours [Hide Filters](#)

Key OT Security Indicators

Filter views on specific sites, systems, or business units

Pre-built KPI's

[Edit](#)

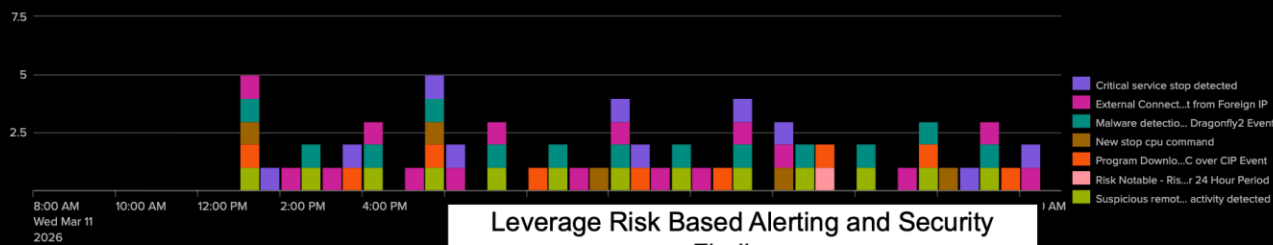
TOTAL RISK SCORE <small>Last 24 hr</small> 7.4k ↑ +7.4k	IT/OT ASSETS DETECTED <small>Last 24 Hours</small> 325	OT NOTABLES <small>Last 24 Hours</small> 2 ↓ -2	SECURITY EVENTS BY ASSET <small># Assets with Security Events</small> 6 0	TOTAL OT DEVICES <small># OT Known Devices</small> 137	# UNIDENTIFIED ASSETS <small>Last Hour</small> 6 ↑ +4	AVERAGE ASSET RISK SCORE <small>Last 24 hr</small> 255.7 ↑ +255.7
--	--	--	---	--	--	--

OT Security Events

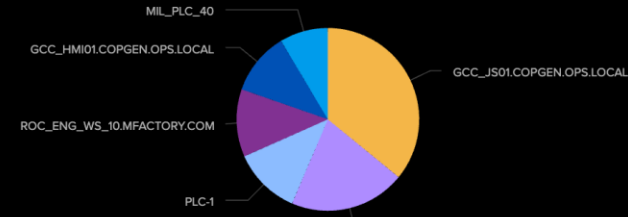
View all Security Events for OT Environment

Event Filter

Security Events Over Time



Security Events by Type



View key details such as asset types, zones, MITRE mappings

Risk Notables

Last Event	Event	Risk Score	Risk Events	Asset	Facility	Priority	Asset Zones	search_name	risk_count
03/12/2026 03:00:29	Risk Threshold Exceeded For OT Asset Over 24 Hour Period	100.0	10	GCC_JS01.COPGEN.OPS.LOCAL	copperfield power plant	Critical	Level 3 -> Level 3	Threat - Risk Notable - Risk Threshold Exceeded For OT Asset Over 24 Hour Period - Rule	10

Findings

Last Event	Event	Asset Zone	MITRE	# Alerts	Source	Destination	Asset Types	Facility	Priority
03/12/2026 08:05:10	External Connection to Environment from Foreign IP	Level 3	T1133;T1078	16	125.77.41.86	GCC_JS01.COPGEN.OPS.LOCAL	Remote Access	copperfield power plant	critical



Cisco Industrial Threat Defense: 3 – Detection and Response

Incident Review

Analyst queue Search findings & investigations Last 24 hours Saved Views Select... Charts Hide Timeline

Time Range: Last 24 hours Clear All Save Apply

Specific OT Alert Views Saved Views OT Incidents

Zoom To Selection Zoom Out Deselect

Findings and investigations 73 Last refresh at 08:37 AM Auto-refresh off

View OT Security Findings

Title	ID	Type	Count	Time
Remote Connection to the OT Environment by Foreign IP Detected		FINDING	75	Today, 8:05 AM
Critical service stop detected		FINDING	3221	Today, 8:00 AM
Program Download to PLC over CIP Event on ROC_ENG_WS_10.MFACTORY.COM from PLC-1		FINDING	3221	Today, 7:56 AM
Suspicious Remote File Copy Activity Detected		FINDING	160	Today, 7:12 AM
Malware detection - Dragonfly2 Event on GCC_JS01.COPGEN.OPS.LOCAL from ...		FINDING	231	Today, 7:05 AM
Remote Connection to the OT Environment by Foreign IP Detected		FINDING	75	Today, 6:30 AM
Critical service stop detected		FINDING	231	Today, 6:28 AM
New stop cpu command on GCC_ENG01.COPGEN.OPS.LOCAL from MIL_PL_C_40		FINDING	231	Today, 5:45 AM
Suspicious Remote File Copy Activity Detected		FINDING	160	Today, 5:42 AM
Malware detection - Dragonfly2 Event on GCC_JS01.COPGEN.OPS.LOCAL from ...		FINDING	231	Today, 5:36 AM
Program Download to PLC over CIP Event on ROC_ENG_WS_10.MFACTORY.COM from PLC-1		FINDING	3221	Today, 5:05 AM
Remote Connection to the OT Environment by Foreign IP Detected		FINDING	75	Today, 4:15 AM
Suspicious Remote File Copy Activity Detected		FINDING	160	Today, 4:12 AM
Malware detection - Dragonfly2 Event on GCC_JS01.COPGEN.OPS.LOCAL from ...		FINDING	231	Today, 4:12 AM

Detailed asset information

Start investigation

Unassigned Undetermined

Time: Mar 12th, 2026 8:05 AM

Last updated: N/A

Reference ID: a8e6fba7-c17e-4198-8444-6c1bc2b1a502@@notable@@a8e6fba7c17e419884446c1bc2b1a502

Detection: Access - External Connection to OT Environment from Foreign IP - Rule

Action: success (success)

Annotation framework: mitre_attack

kill_chain_phases: cis20

Annotations: T1078, PR.AC-3, T1133

winremote (remote)

Authentication method: Negotiate

Destination: GCC_JS01 160

Destination DNS: gcc_js01.copgen.ops.local

Destination IP address: 172.104.104.98

Destination MAC address: 0d:1e:15:21:21:aa

Destination NT hostname: gcc_js01

Destination PCI domain: untrust

Destination business unit: ga plant ops

Destination category: nerc

Destination city:

Destination country: us

Destination expected: true

Leverage security frameworks such as MITRE, Kill Chain, etc

- Access Search (as destination)
- Access Search (as source)
- Asset Center
- Asset Investigator
- Map GCC_JS01
- Intrusion Search (as destination)
- Intrusion Search (as source)
- Search for a finding
- Malware Search
- Nbtstat GCC_JS01
- Nslookup GCC_JS01
- OT Asset Investigator
- OT Host Access Monitoring
- Ping GCC_JS01
- Session Center
- Stream Capture
- OT Analyze Perimeter Traffic
- Traffic Search (as destination)

OT Drill down actions asset or host access information

Cisco Industrial Threat Defense: 3 – Detection and Response

OT Perimeter Security

OT Perimeter Traffic Investigator

Source is required to show data

Include

Perimeter Only

Perimeter and Network

Direction

Inbound

Traffic

Allowed

App

ftp-data

Port

All

Destination

GCC_js01*

Perimeter Device

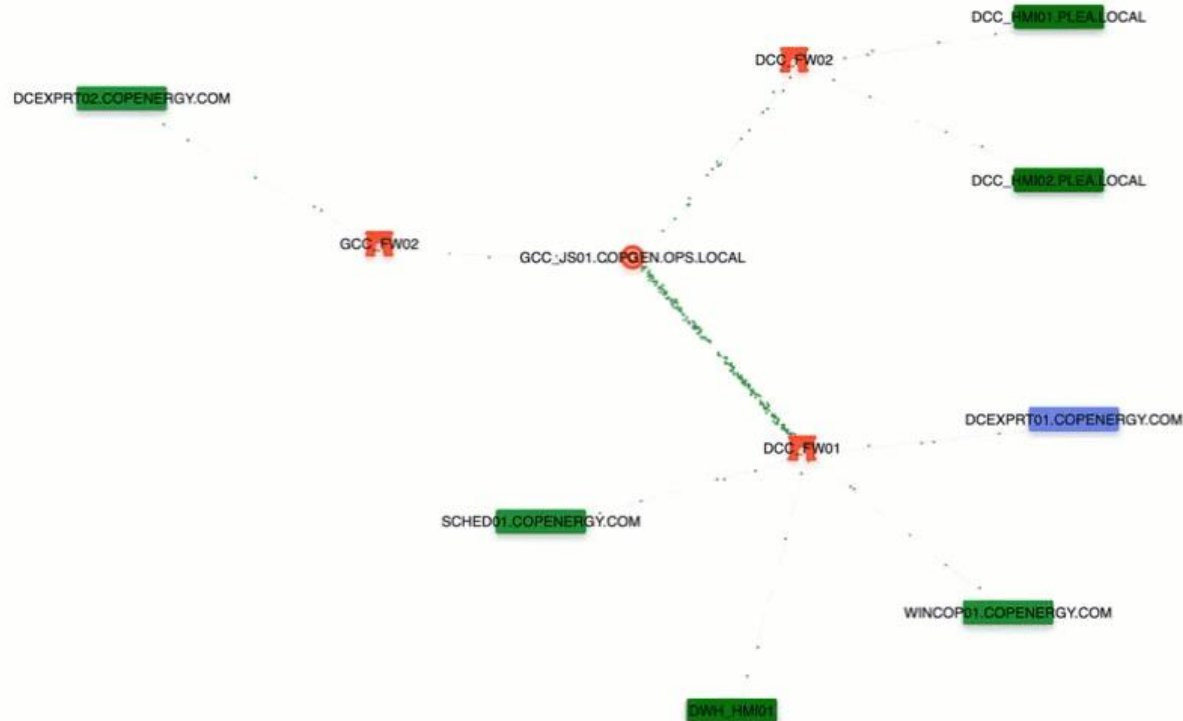
Time Period

Last 24 hours

Hide Filters

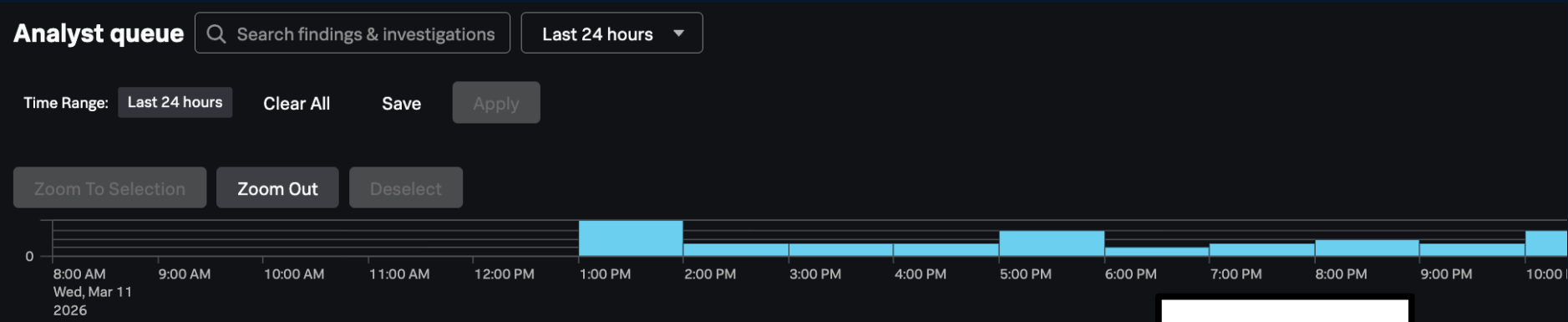
Traffic to Endpoint Map

Communication GCC_js01* as dest (via perimeter devices)



Cisco Industrial Threat Defense: 3 – Detection and Response

Apply Risk Based Alerting



Findings and investigations 77

<input type="checkbox"/>	>	Title	ID	Type	Asset	Risk Score	Event Count	Inte... ↓
<input type="checkbox"/>	>	24 hour risk threshold exceeded for OT Asset GCC_JS01		FINDING	GCC_JS01	140	14	
<input type="checkbox"/>	>	24 hour risk threshold exceeded for OT Asset GCC_JS01.COPGEN.OPS.LOCAL	ES-00002	INVESTIGATION	-	100	1	10

Risk Based Alerting to reduce alert fatigue

Link together related activity

Intermediate findings

GCC_JS01 Risk score: 140.0 Event count: 14

Timeline Threat topology

Asset gcc_js01.copgen.ops.local +3 | Priority Critical | DNS gcc_js01.copgen.ops.local | Owner occ | Business Unit ga plant ops | Category nerc +6 | City Atlanta, ga

Time range Custom time Help

Threat objects	Entity
GCC_JS01.COPGEN.OPS.LOCAL 42	copperfield power plant 14 280
	GCC_JS01.COPGEN.OPS.LOCAL 14
	GCC_ENG01.COPGEN.OPS.LOCAL 14 140

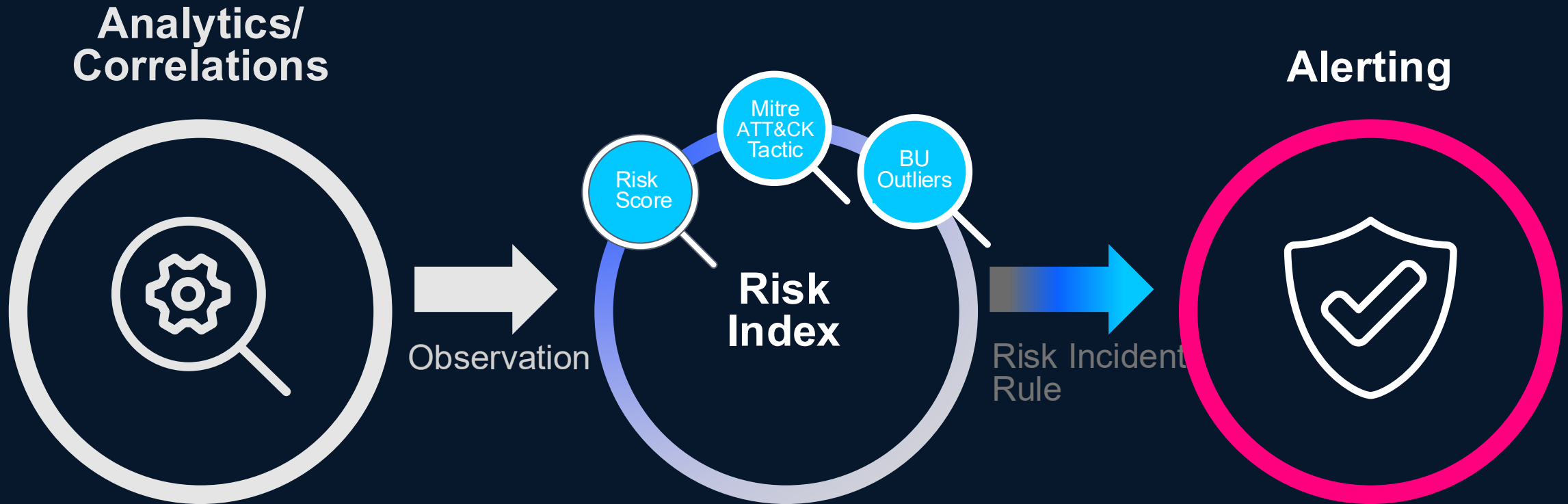
Type host
GCC_JS01.COPGEN.OPS.LOCAL

[View in threat activity](#)
[View threat artifacts](#)
[Search](#)

Automatically correlate different threat objects

Cisco Industrial Threat Defense: 3 – Detection and Response

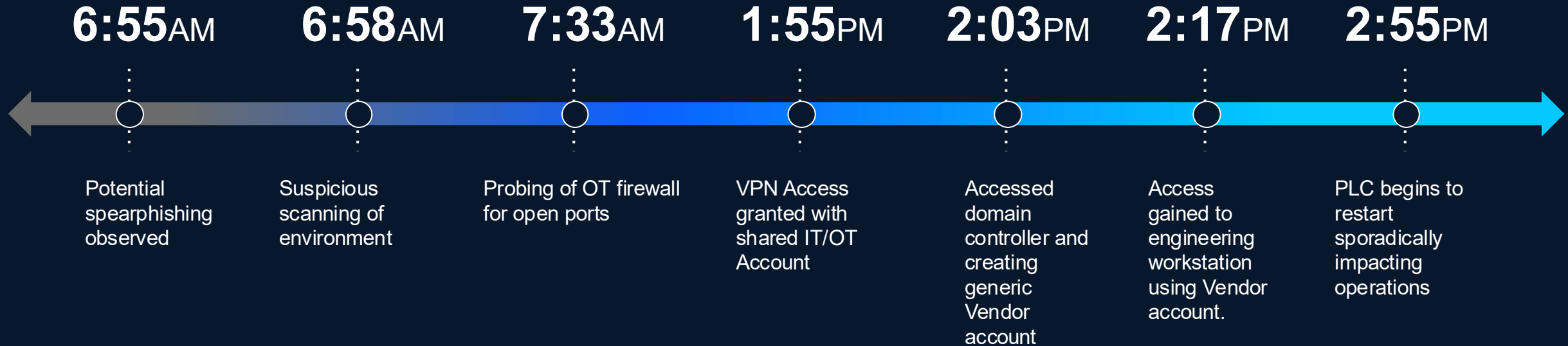
Dramatically reduce alert volumes while improving your security posture



Cisco Industrial Threat Defense: 3 – Detection and Response

Traditional Approach

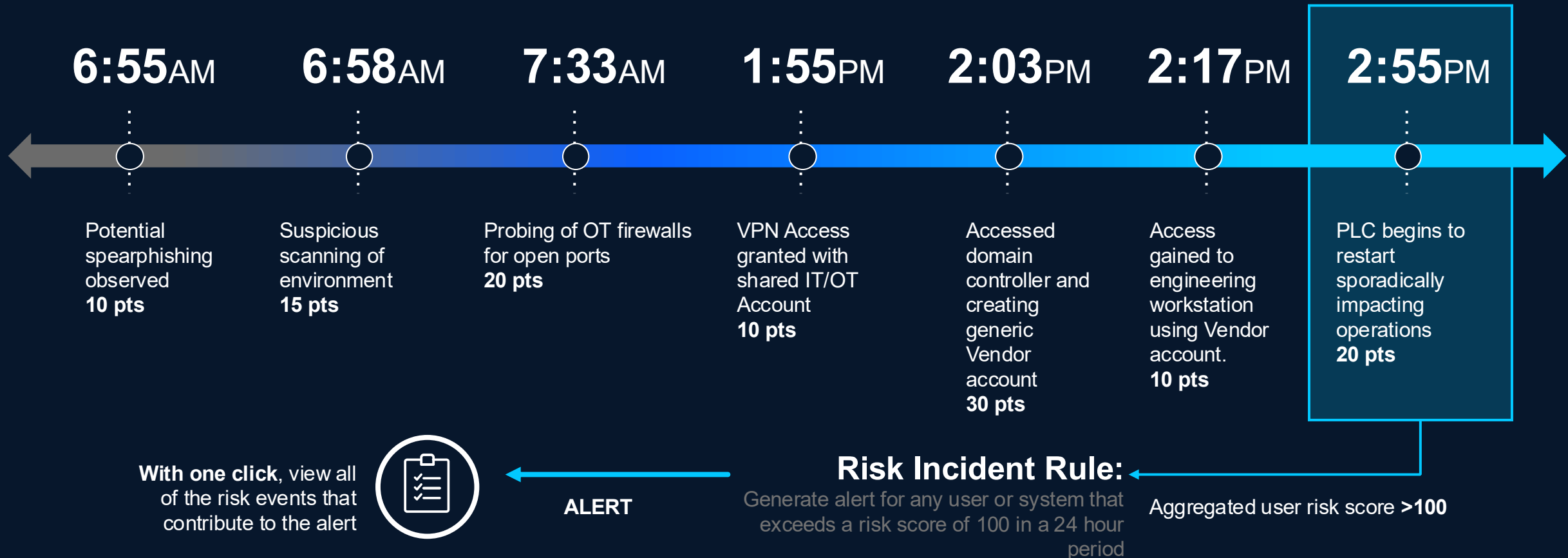
The events below would be considered too noisy and would be abandoned



Cisco Industrial Threat Defense: 3 – Detection and Response

Risk Based Alerting

These events become context that informs high-fidelity alerts



Thank you



