Securing Industrial Networks Where to start?

Using Cyber Vision for OT Asset Visibility & Segmentation

Abubakar Maaroof – IIoT Solutions Engineer, EMEA
Nicolas Deville – IIoT Security Product Manager

BRKIOT-2910

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Your presenters

Abubakar Maaroof
IIoT Solutions Engineer

Nicolas Deville
IIoT Security Product Manager

Agenda

- Industrial Network Security
- NIS2: What is happening?
- The Journey to OT security
- Cyber Vision
  - Fundamentals
  - Architecture
  - Spotlight: New Features
  - Network Segmentation: ISE & Firewall
  - Integration: Splunk & XDR
- Conclusion

slido

Please download and install the Slido app on all computers you use

Join at slido.com
#2886115

ⓘ Start presenting to display the joining instructions on this slide.

slido

Please download and install the Slido app on all computers you use

What is top of your mind in OT security?

ⓘ Start presenting to display the poll results on this slide.

slido

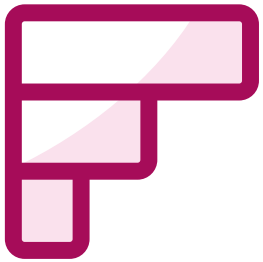
Please download and install the Slido app on all computers you use

What is your role in OT security for your organisation? Multi-Choice

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

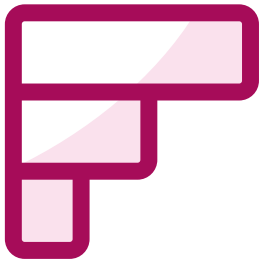


How would you describe your current Industrial network security?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use



How familiar are you with Cyber vision?

ⓘ Start presenting to display the poll results on this slide.

What to expect in this session?

- Session is focused on Cyber vision
  - Some context around OT cyber risk and NIS2 update
  - Fundamentals, Architecture and Spotlight on Key new features
  - Integration of Cyber vision:
    - Segmentation: ISE and Firewall (CSDAC)
    - Incident Response: XDR & Splunk
- What not to expect in this session:
  - Troubleshooting guidelines
  - Deep dive into Integrated products: ISE, Firewall, XDR or Splunk
  - Customer case study

Industrial Network Security

cisco Live!

The need to secure industrial is critical to industrial resilience

Clorox says sales and profit took a big hit from cyberattack

Johnson Controls Ransomware Attack: Data Theft Confirmed,

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

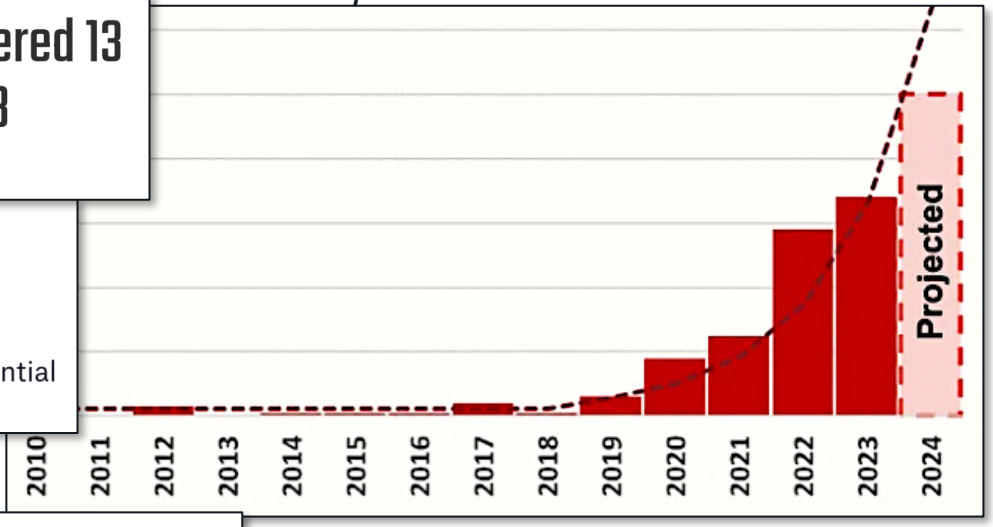
Simpson Manufacturing Takes Systems Offline Following Cyberattack

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



Industry Digitization Increases the Threat Landscape

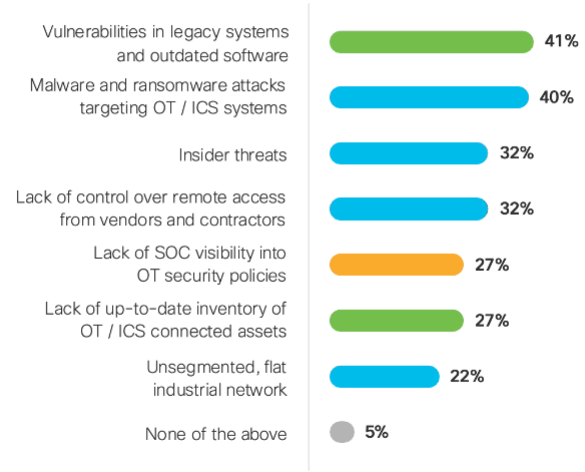
- More connected automation devices
- IoT devices accessing the cloud
- Shadow IT in industrial networks
- Remote access from third parties
- Malware intrusions
- New regulatory requirements

The role of IT is expanding to help secure industrial operations

Security challenges with increased connectivity

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

Weak Security Posture

Lack of visibility to thousands of OT assets with poor cybersecurity hygiene

Lack of Control

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

Scattered Event Logs

Too many screens for security analysts to monitor without cross-domain context

What OT security assessments reveal?

Unauthorized remote access by third parties

OT network fully connected to IT

Default credentials to log into systems

Security Patches not installed

Unknown devices

Bad Firewall or Switch configuration

Firmware uploaded over FTP without Signature

Multiple Time Servers

DNS queries to Amazon

Windows XP SMBv1

Unnecessary network communications

Decommissioned assets still connected

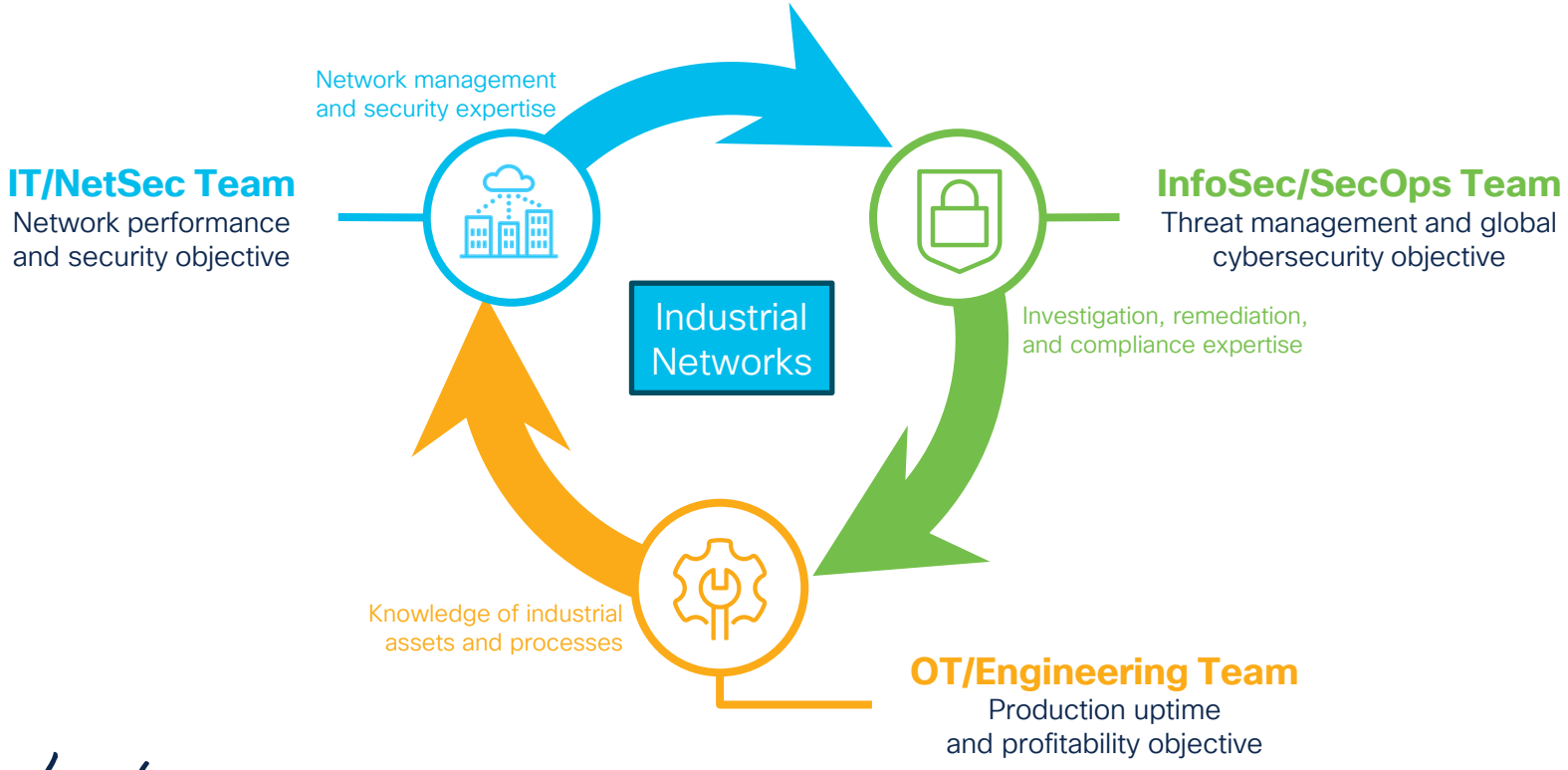
IPv6 traffic in IPv4 networks

Devices in the wrong VLAN

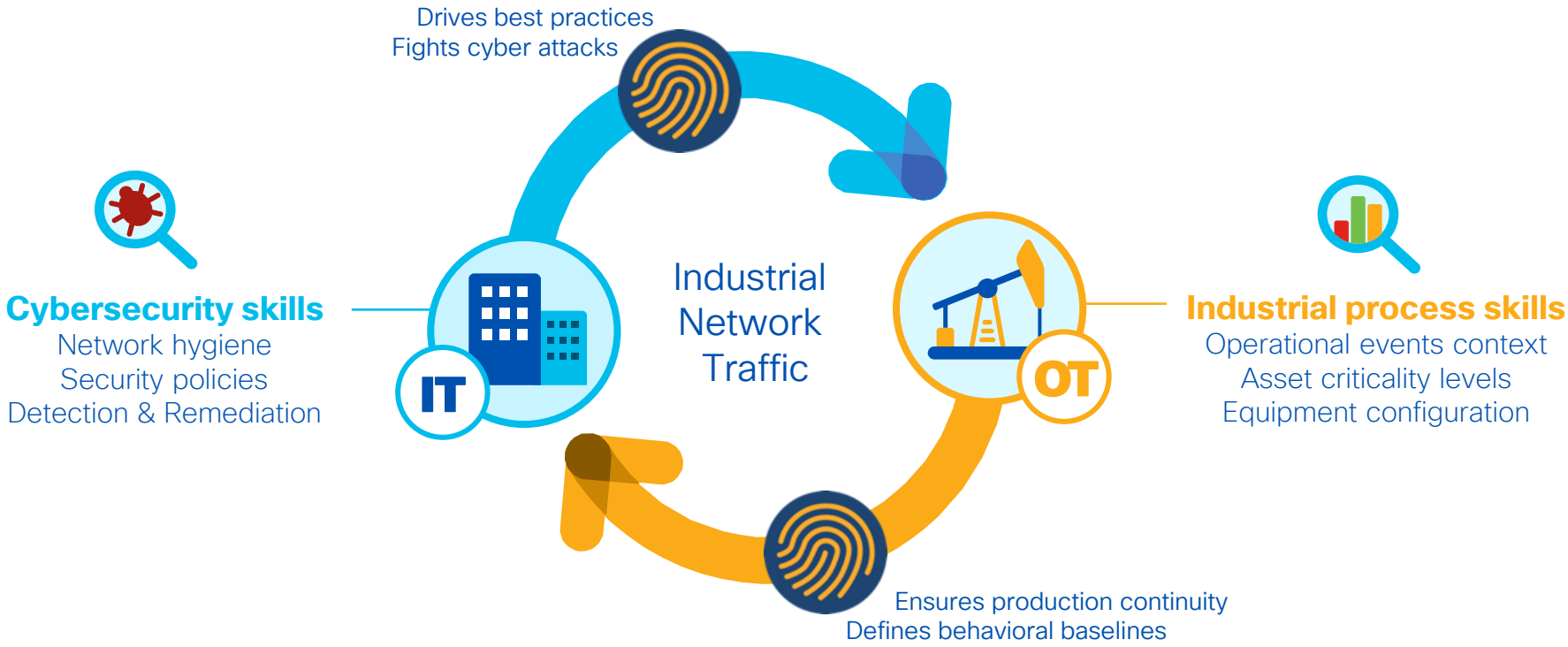
Malware or Virus activities

Program Upload over VPN during the night

Who Manages Security in Operational Networks?



IT-OT collaboration is vital for securing ICS



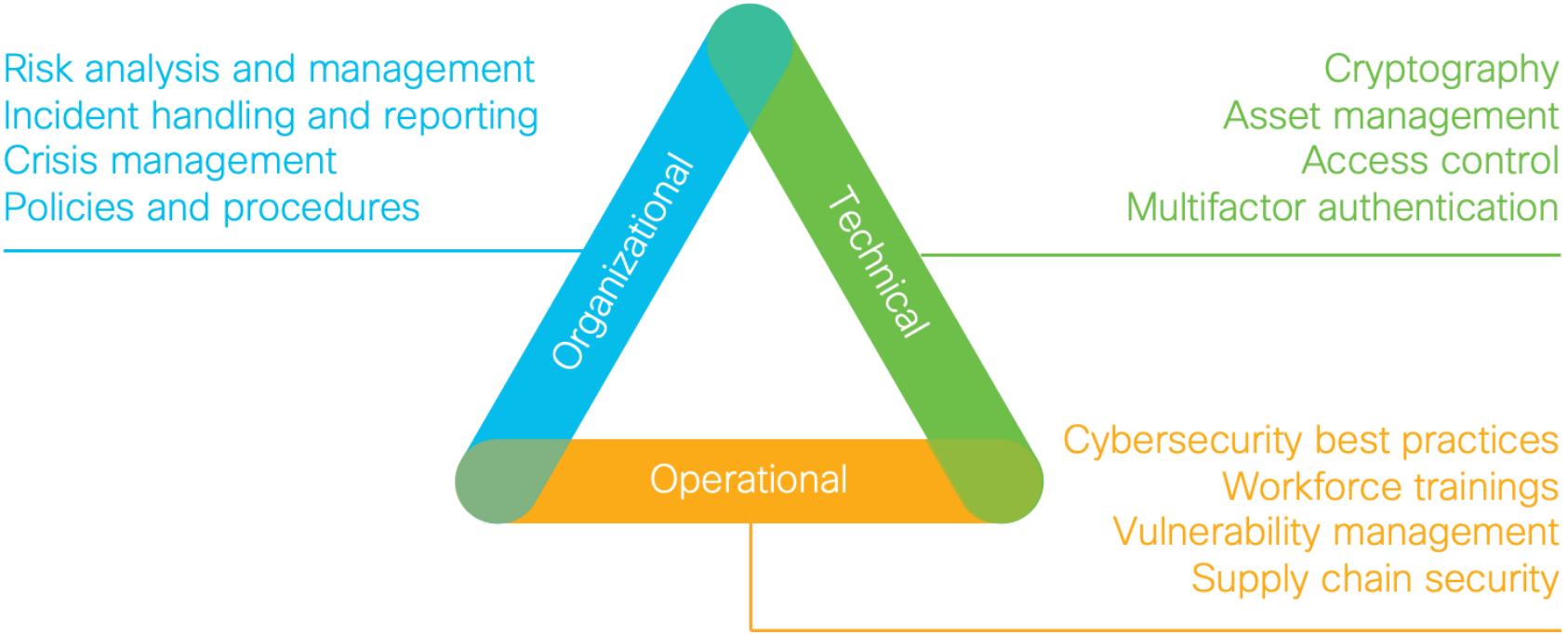
NIS2: Where are we today?

Network and Information Security Directive 2.0 (NIS2)

cisco Live!

NIS2 is an EU wide legally mandated framework for Cyber Security Readiness

(Compliance in Law 18th October 2024)



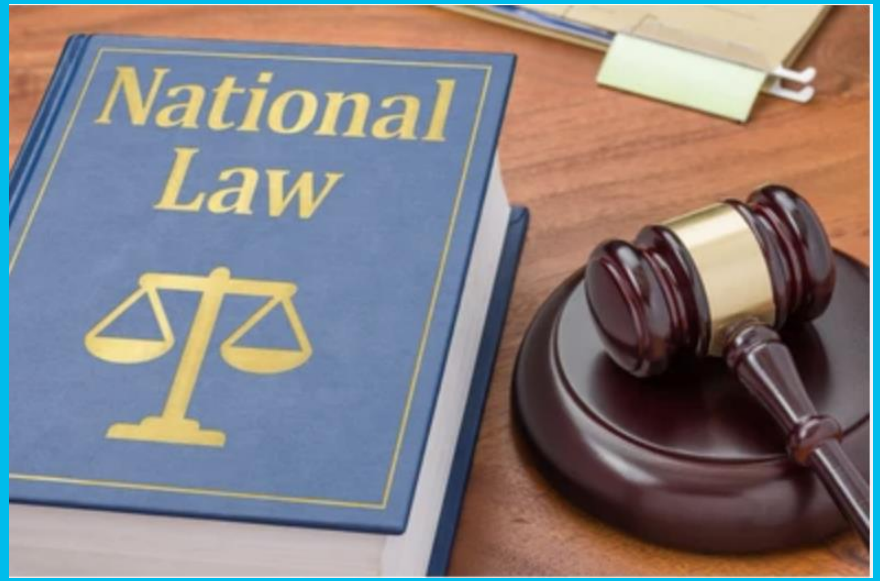
NIS 2 impacts many more sectors than its predecessor NIS

- Energy
- Transport
- Drinking water & Wastewater (NEW)
- Waste (NEW)
- Chemicals (NEW)
- Healthcare & Pharmaceutical (NEW)
- Food & Beverage (NEW)
- Manufacturing (NEW)
- Postal & Courier (NEW)
- Digital infrastructures
- ICT services & Digital platforms (NEW)
- Administrations (NEW)
- Space (NEW)
- Banking & Finance

350,000+ organizations in scope

- NIS2 was enforced Oct 18, 2024
- Requires national bodies to create legislation
- Non-EU organizations taking part of the EU supply chain must comply

NIS2 is enforceable



Mandate to report cyber incidents

- 24hr incident notification
- 72hr follow-up report
- Final report within 1 month

Organizational penalties

- Management liability
- Suspension of certification
- Monitoring officer assigned

Financial penalties

- Essential Entities:
  €10M or 2% annual earnings, whichever is higher
- Important Entities:
  €7M or 1.4% annual earnings, whichever is higher

What is happening on the ground with NIS2 ?

- *Countries needed to be responsible for their own law implementations since Oct 18th 2024*

Countries had been slow to move to Local Law during 2024

The European Commission decided to open infringement procedures by sending a letter of formal notice to 23 Member States on Nov 28th 2024
Most countries have now transposed and are drafting legislation

Accurate information can only be found on the Country Cyber Security Authority Pages – no common repository

NIS2 status: For information only – Feb 2025

Accuracy cannot be confirmed check with your authority!

Country	Transposition Status	Key Legislation/Authority
Austria	Likely Transposed	Federal Chancellery Cybersecurity Act
Belgium	Transposed (Sector Rules Pending)	Centre for Cybersecurity Belgium (CCB)
Bulgaria	Transposed (Enforcement Lagging)	State e-Government Agency Cybersecurity Act
Croatia	Transposed (Delays in Critical Sectors)	Croatian Cybersecurity Agency (CERT.hr)
Cyprus	Transposed (Limited Public Updates)	Digital Security Authority
Czech Republic	Full[illegible]	Nati[illegible]fo Security Agency (NÚKIB)
Denmark	Transposed[illegible]	[illegible] for Cyber Security (CFCS)
Estonia	Fully Transposed	Information System Authority (RIA)
Finland	Transposed (Sector Guidelines Ongoing)	Transport and Communications Agency (Traficom)
France	Transposed Early	ANSSI (Military Programming Law Updates)
Germany	Fully Transposed	Federal Office for Info Security (BSI)
Greece	Transposed (Enforcement Lagging)	National Cybersecurity Authority
Hungary	Transposed (Delays in Healthcare/Energy)	National Cybersecurity Coordination Centre (N3C)
Ireland	Transposed (Focus on Tech/Cloud)	National Cyber Security Centre (NCSC)

NIS2 status: For information only- Feb 2025

Accuracy cannot be confirmed check with your authority

Country	Transposition Status	Key Legislation/Authority
Italy	Fully Transposed	National Cybersecurity Agency (ACN)
Latvia	Transposed (Limited Documentation)	Cert.lv (CERT.LV)
Lithuania	Fully Transposed	National Cybersecurity Centre (NKSC)
Luxembourg	Transposed (Expanded Sectors)	National Cybersecurity Agency (ANSSI-LU)
Malta	Transposed (Enforcement Capacity Issues)	Malta Information Technology Agency (MITA)
Netherlands	Transposed [illegible]	National Cyber Security Centre (NCSC.nl)
Poland	[illegible]	[illegible] NASK
Portugal	Transposed (SME Focus)	National Cybersecurity Centre (CNCS)
Romania	Transposed (Uneven Enforcement)	National Cyber Security Directorate (DNSC)
Slovakia	Transposed (Limited Updates)	National Security Authority (NBÚ)
Slovenia	Transposed (Healthcare Delays)	SI-CERT (CERT.SI)
Spain	Transposed	National Cybersecurity Institute (INCIBE) & CCN-CERT
Sweden	Transposed Early	Swedish Civil Contingencies Agency (MSB)

NIS2 White Paper

- Who's in scope?
- What's the sanction regime?
- What are the requirements?
- How can industries comply?

Free Download at http://cs.co/NIS2

cisco Live!

NIS2 for OT

- Secure supply chain with Cisco networking
- Monitor risk with Cisco Cyber Vision
- Zero-trust segmentation with Cisco ISE
- Zero-trust remote access with Cisco SEA
- Cisco CX Services for NIS2 compliance

Free Download at http://cs.co/NIS2forOT

slido

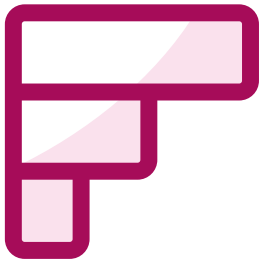
Please download and install the Slido app on all computers you use

Is your business subject to NIS2 Regulations?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use



Do you feel confident that you have a clear strategy to comply with NIS2?

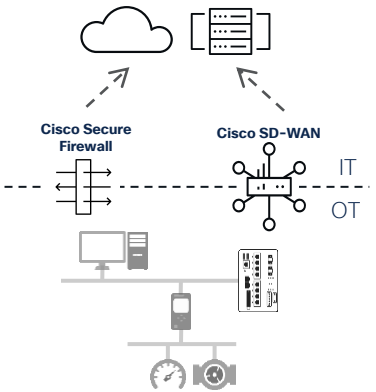
ⓘ Start presenting to display the poll results on this slide.

The Journey to OT Security

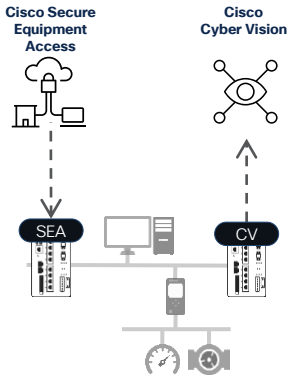
cisco Live!

Enabling a comprehensive OT security journey

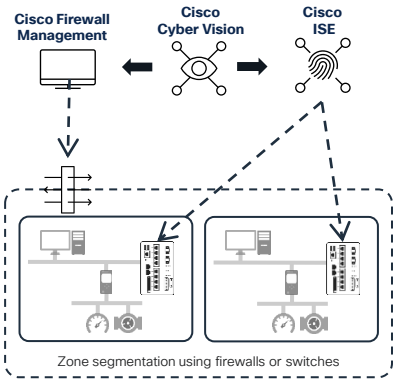
1 Secure the Operational Boundary



2 Security Posture & ZTNA of OT Assets

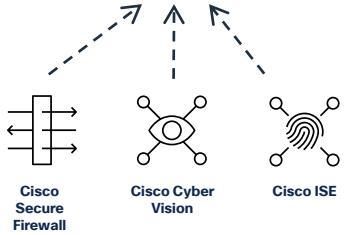


3 Segment Network into Smaller Trust Zones



4 Develop Incident Investigation & Response

splunk> + Cisco XDR



Talos Threat Intelligence + Talos Incident Response

slido

Please download and install the Slido app on all computers you use

Which stage of the OT security Journey are you at?

ⓘ Start presenting to display the poll results on this slide.

Cyber Vision Fundamentals

cisco Live!

Securing industrial operations starts with OT visibility

Identify OT assets and their communications

Spot vulnerabilities to patch or protect

Segment networks with access policies

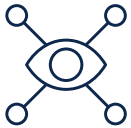
Detect bypass or leaks in the IDMZ

Drive compliance and governance

Visibility helps drive IT/OT collaboration to secure industrial operations

Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT



Visibility
OT asset inventory
Communication patterns

Security Posture
Device vulnerabilities
Risk scoring

Zone Segmentation
Automate segmentation below
the IDMZ to protect operations

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

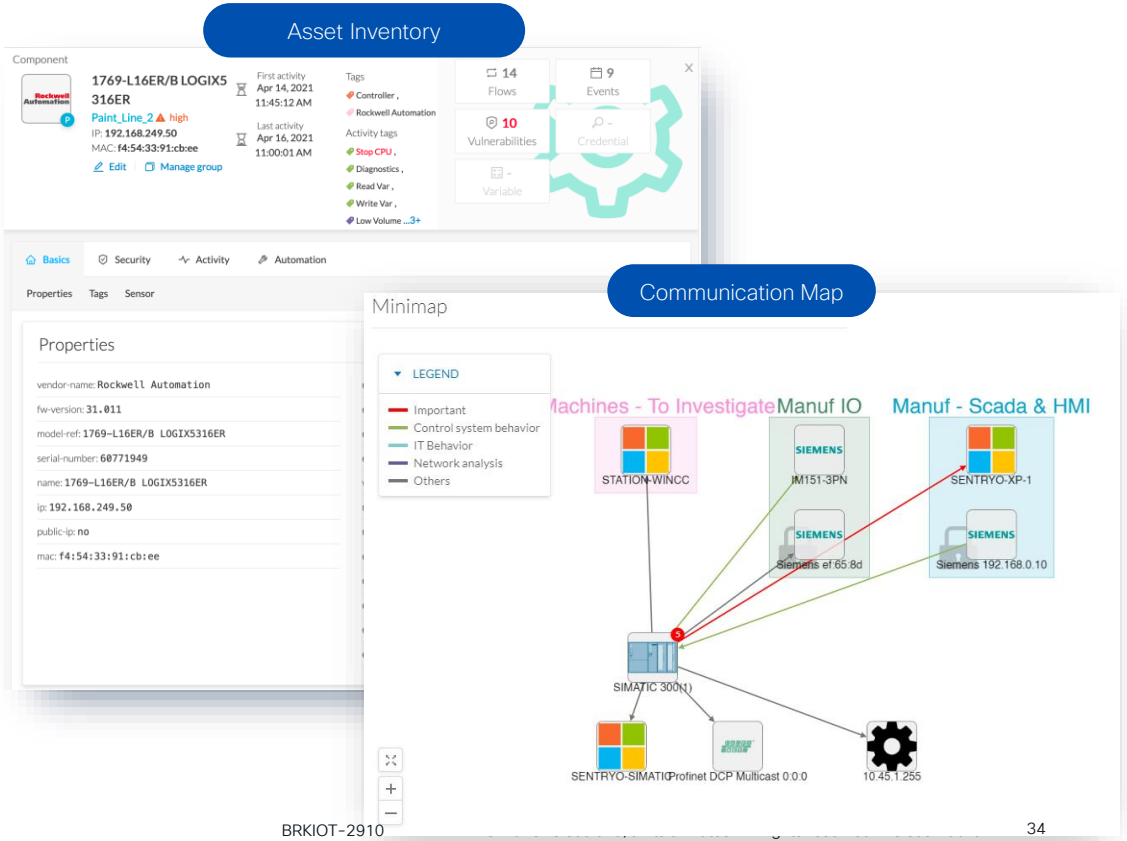
Visibility into connected industrial assets

Asset Inventory

Automated inventory of all assets in your environment with detailed and up to date profile information

Communication Patterns

Dynamic map of all communication activities with detailed application flow level information



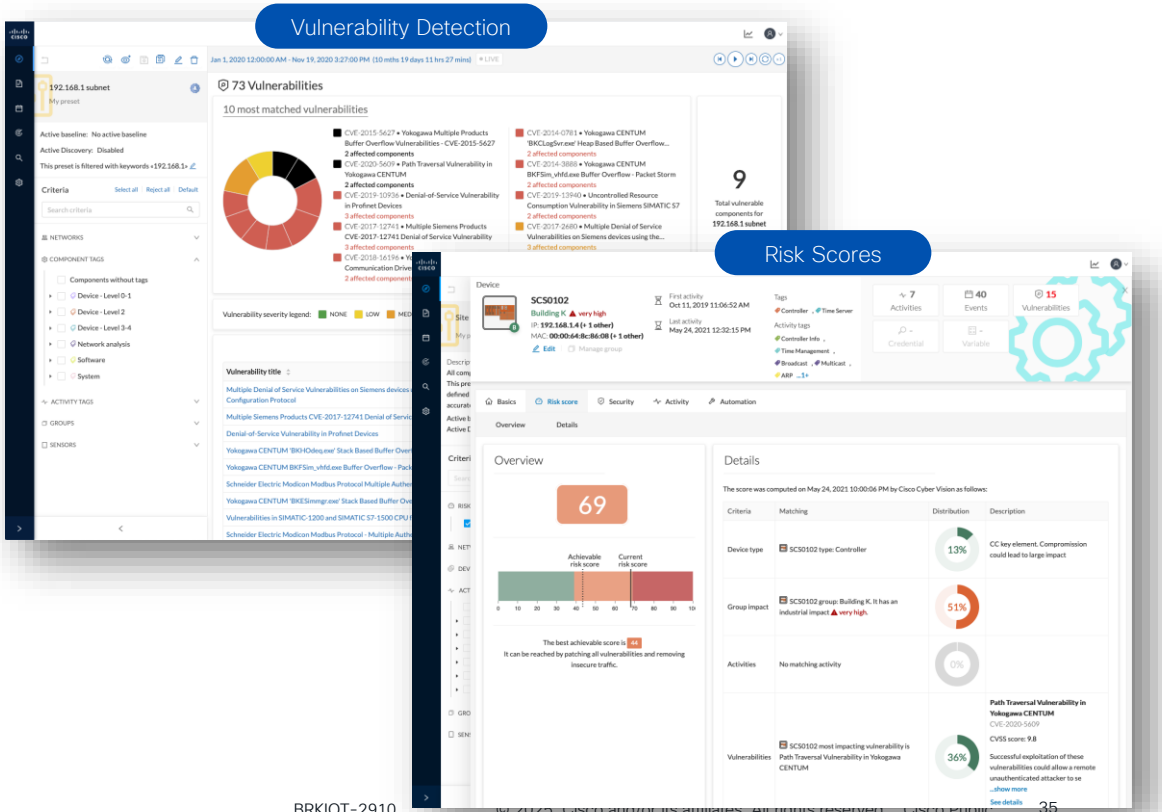
Visibility into the OT security posture

Vulnerability Detection

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

Risk Scoring

Risk scoring for assets, production cells and sites, to help prioritize action and improve governance



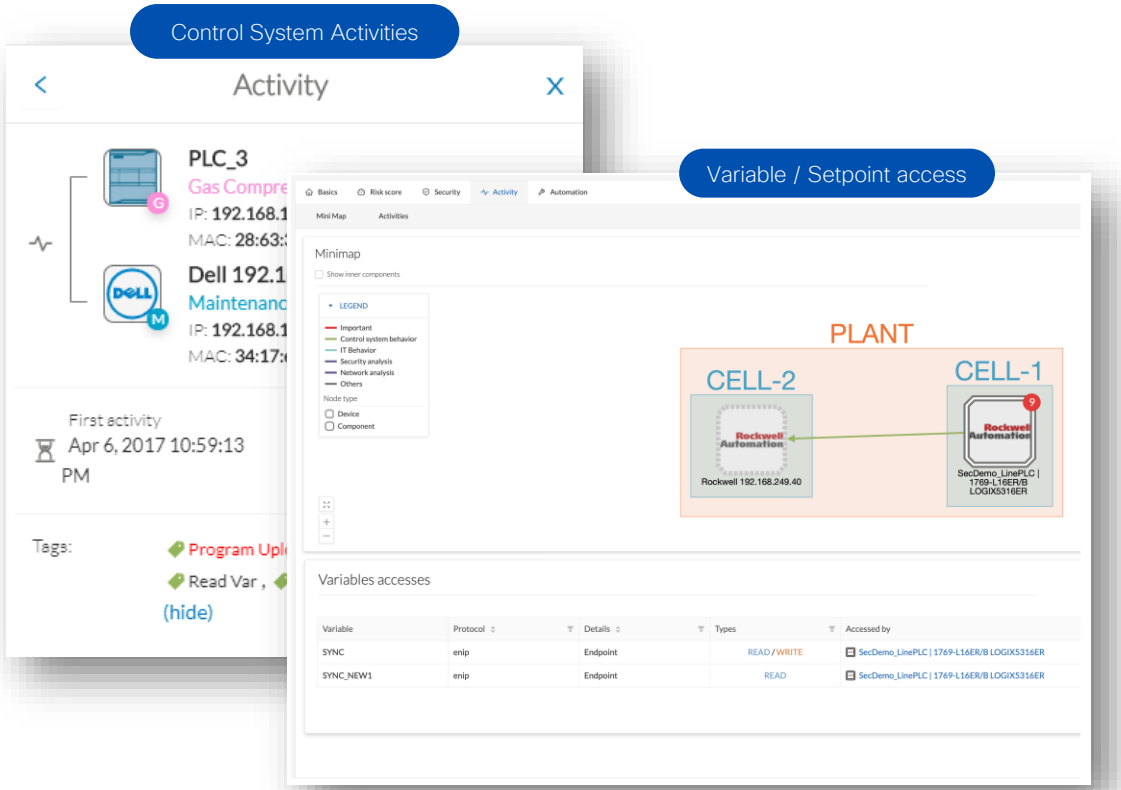
Visibility into operational issues

Control System Activities

Track process modifications
Identify configuration changes
Record control system events

Variable Access

See which variables, objects, setpoints are being accessed or modified to help OT troubleshoot issues



Visibility into threats with Snort IDS and Talos

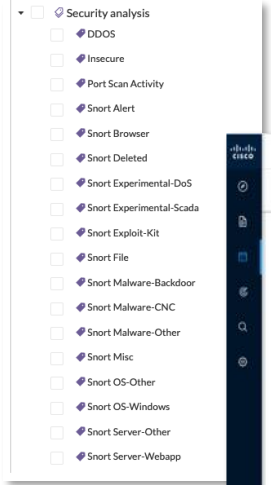
Malware Intrusions

Snort IDS with Talos threat intelligence helps identify malware and intrusions into the OT network

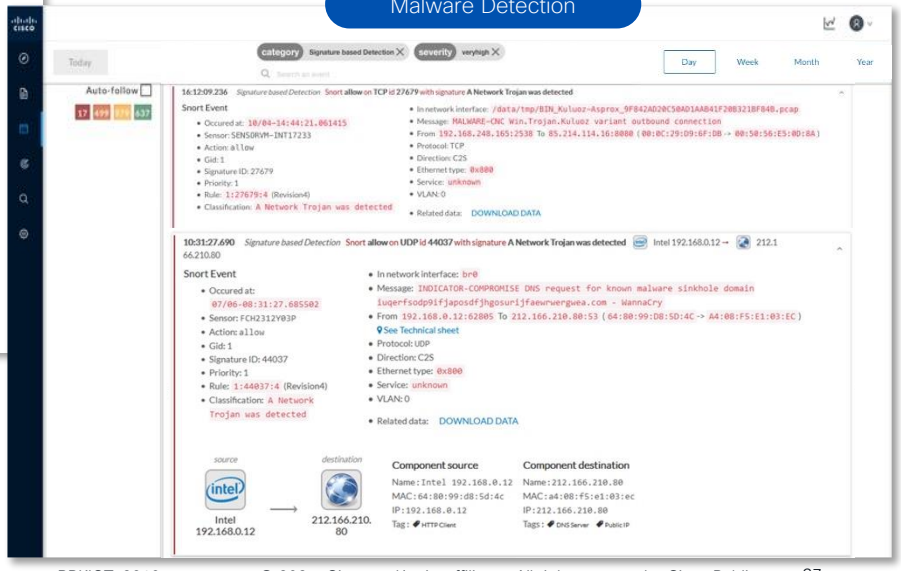
Malicious Traffic

Snort tags automatically associated with network activities to help identify malicious traffic

Malicious Activities



Malware Detection



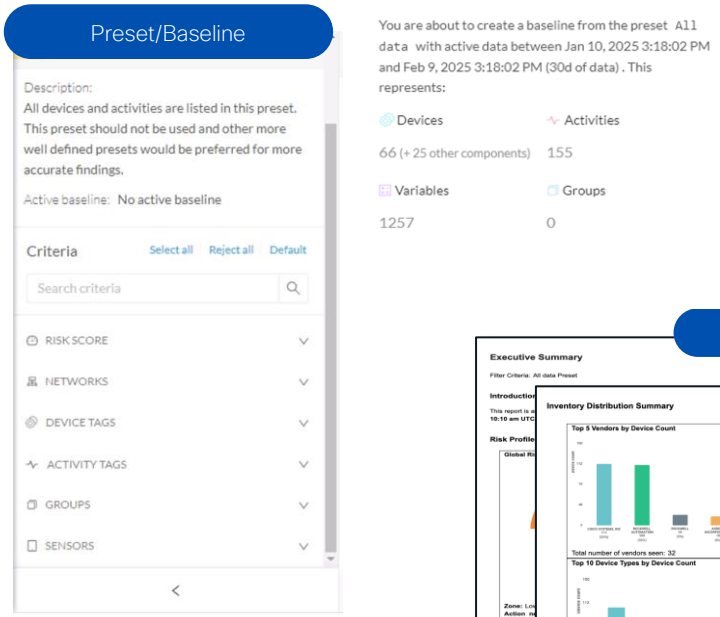
Visibility context with Presets, Baseline & Reporting

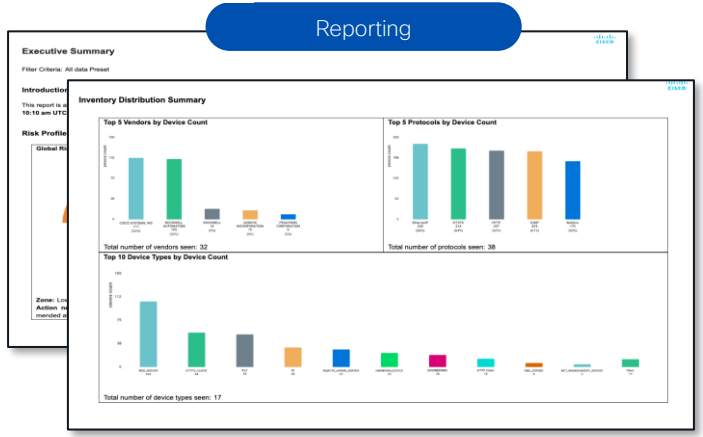
Preset/Baseline

Presets: View a subset of discovered assets and communications, in a dimensional information reduction based on multiple filter criteria
Leverage presets to set baselines

Reporting

Generate Inventory, Remote Access and Security Posture reports, based on Presets
Reports are exportable in docx and pdf formats.





198.18.133.1

Explore - Cisco Cyber Vision

cybercenter/#/

Home

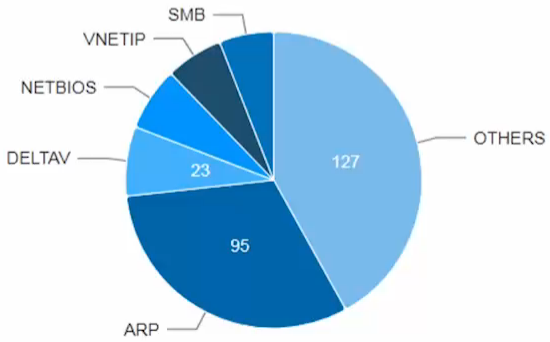
Welcome to Cisco Cyber Vision

Last 30 days overview

Operational overview | Security overview

All | Protocol distribution | Most critical events | Presets highlight

Protocol distribution



Most critical events

Feb 10, 2025 1:00:05 AM	Critical	Sensor 8a29b7ca-fdf3-4e2f-999f-524632f7...
Feb 10, 2025 1:00:05 AM	Critical	Sensor 8e2fb2fe-c4dd-46a6-8e01-27907dc...
Feb 10, 2025 1:00:05 AM	Critical	Sensor 4a7bf983-8b3c-435a-92e6-101363...
Feb 10, 2025 1:00:05 AM	Critical	System has been updated | Cisco Cyber Vis...
Feb 10, 2025 1:00:05 AM	Critical	System has not been updated | Cisco Cyber...
Feb 10, 2025 1:00:05 AM	Critical	System has been updated | Cisco Cyber Vis...
Feb 10, 2025 1:00:05 AM	Critical	Sensor 07fda1d6-7544-4c55-acd4-6d9af63...

Start

12:53 PM
2/10/2025

How Cyber Vision helps with NIS2 compliance

Required NIS2 Measures	Cyber Vision Capabilities
Risk analysis	Risk scores, Security posture reports
Incident prevention	IEC62443 zone segmentation with Cisco ISE
Incident detection & response	Snort IDS with Talos Threat Intel, Splunk & XDR
Vulnerability management	OT asset vulnerability, Cisco VM Risk scores
Cyber hygiene	Asset inventory, Activities, Security insights

Assess OT cyber risks with Cyber Vision to implement best practices

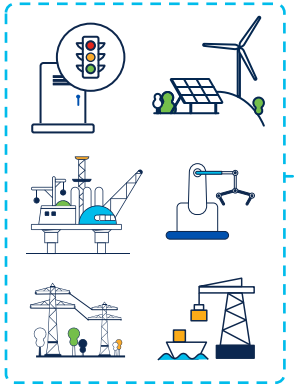
Cyber Vision Architecture

cisco Live!

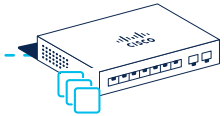
Cisco Cyber Vision: Unique 2-Tier Architecture

OT visibility that can be deployed at scale

OT Assets



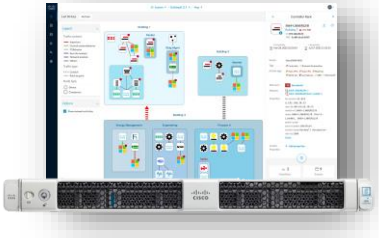
Cisco industrial switches or routers



Cyber Vision Sensor

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

Lightweight Metadata



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 Cyber Vision portfolio

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

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

Catalyst IE3300 and IE3400 Switches

Catalyst IE3400HD IP67 Switch

Catalyst IR1101 Cellular Router

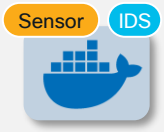
Catalyst IR1800 Cellular Router

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

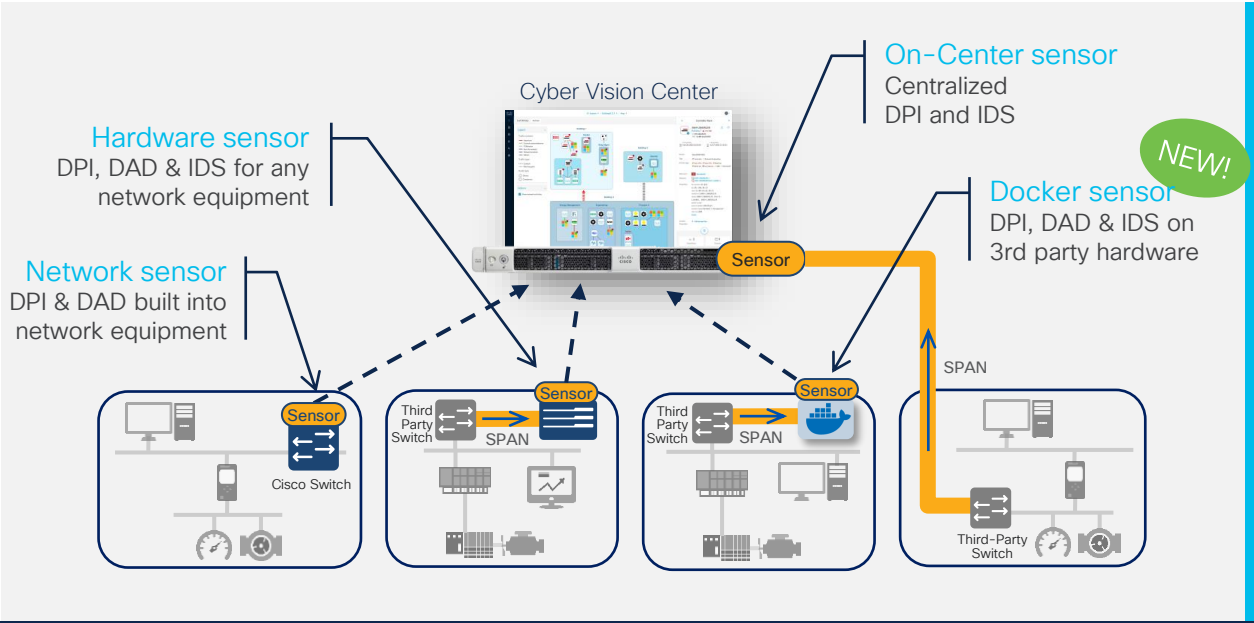


x86 or ARM64 Compute

IC3000 Industrial Compute

Docker Sensor
Hardware-Sensor
DPI and active discovery via SPAN to support brownfield

Easy to deploy in Brownfield and Greenfield environments



- **Network-sensors** embedded in Cisco networking for simple and highly scalable deployments
- **Hardware or Virtual sensors** capturing traffic on any switch with a single hop SPAN to support brownfield deployments
- **On-Center sensor** to leverage existing SPAN infrastructures, or collect traffic within the datacenter

Cyber Vision offers flexible deployment options to best fit your constraints

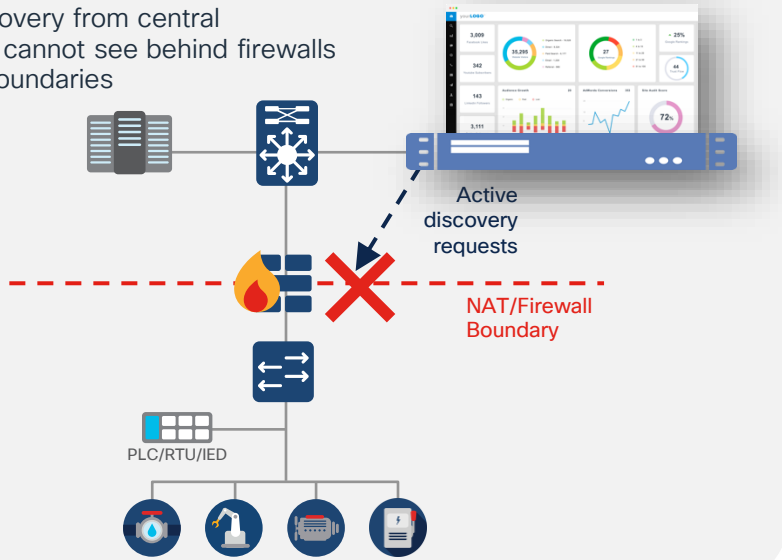
DPI = Deep Packet inspection
DAD = Distributed Active Discovery
IDS = Intrusion Detection System

Why is a network-sensor important?

Sensors embedded in the network can see more

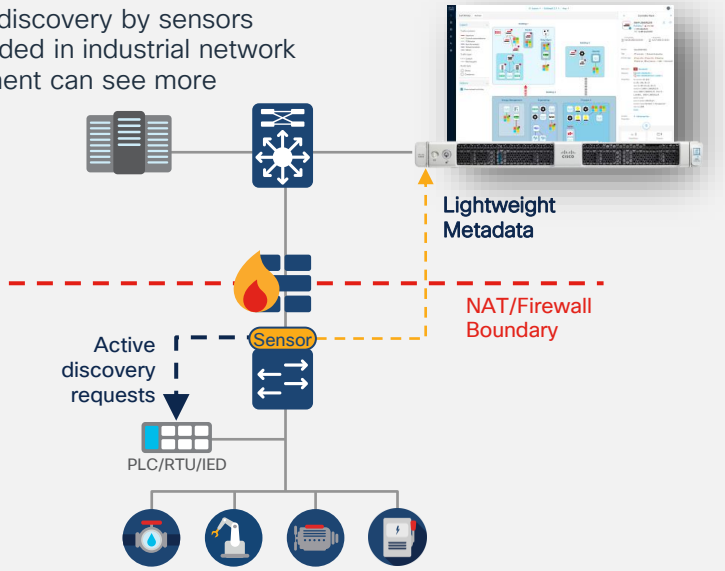
Other solutions

Active discovery from central appliances cannot see behind firewalls and NAT boundaries



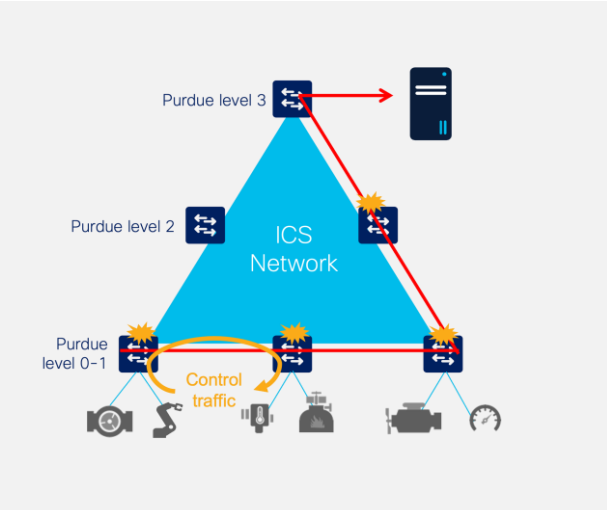
Cisco Cyber Vision

Active discovery by sensors embedded in industrial network equipment can see more

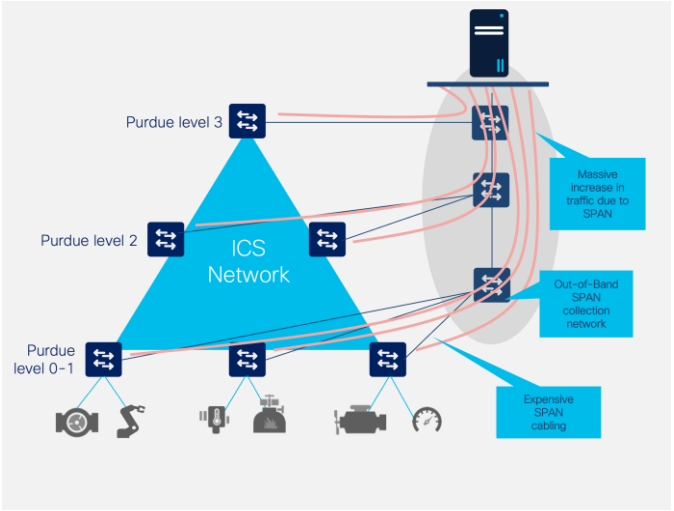


Active discovery requests are not blocked by NAT and firewall boundaries

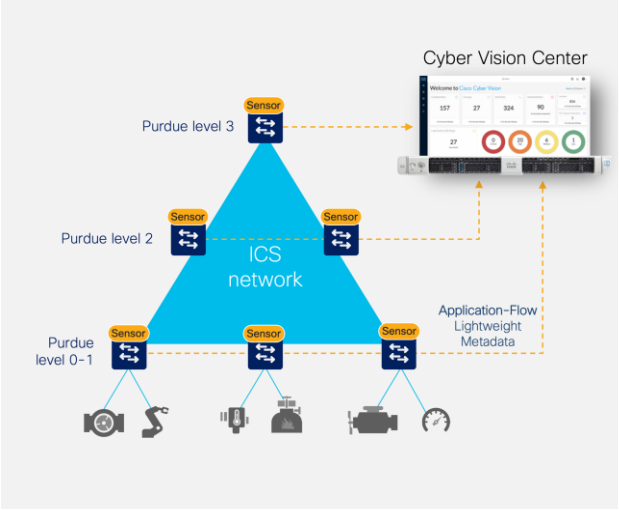
Leverage the network as a sensor to lower cost and complexity



RSPAN introduces Jitter



Out-of-Band SPAN is expensive

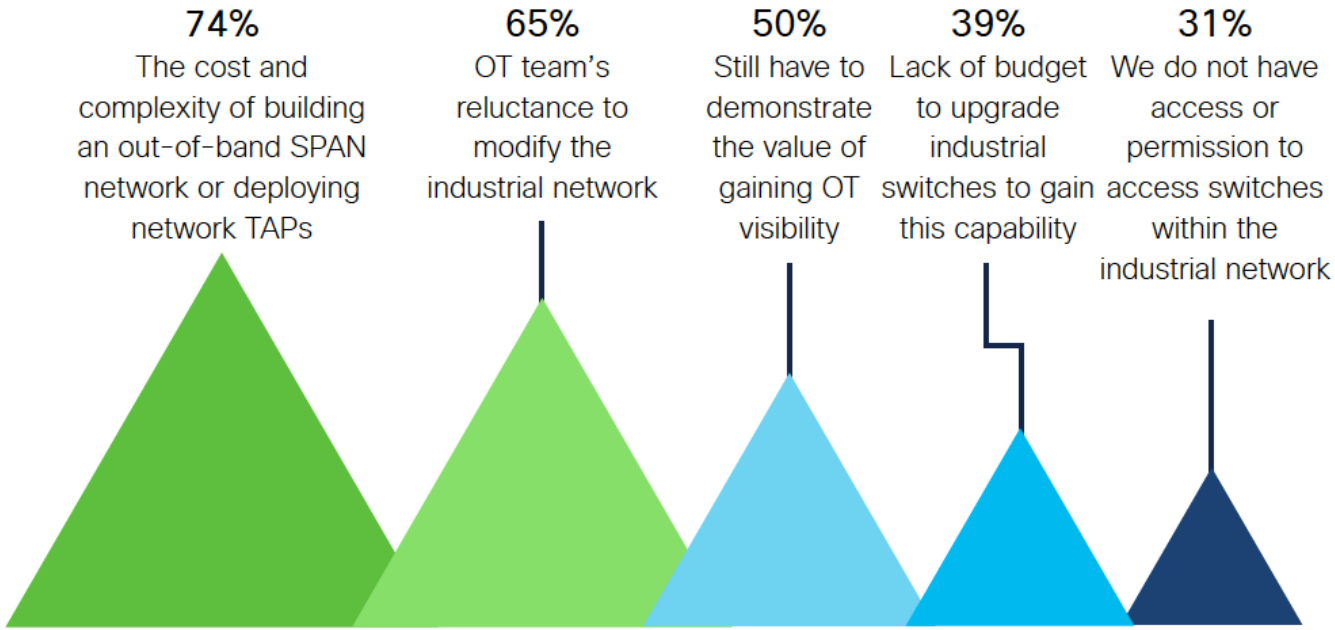


Network sensors scale without SPAN

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

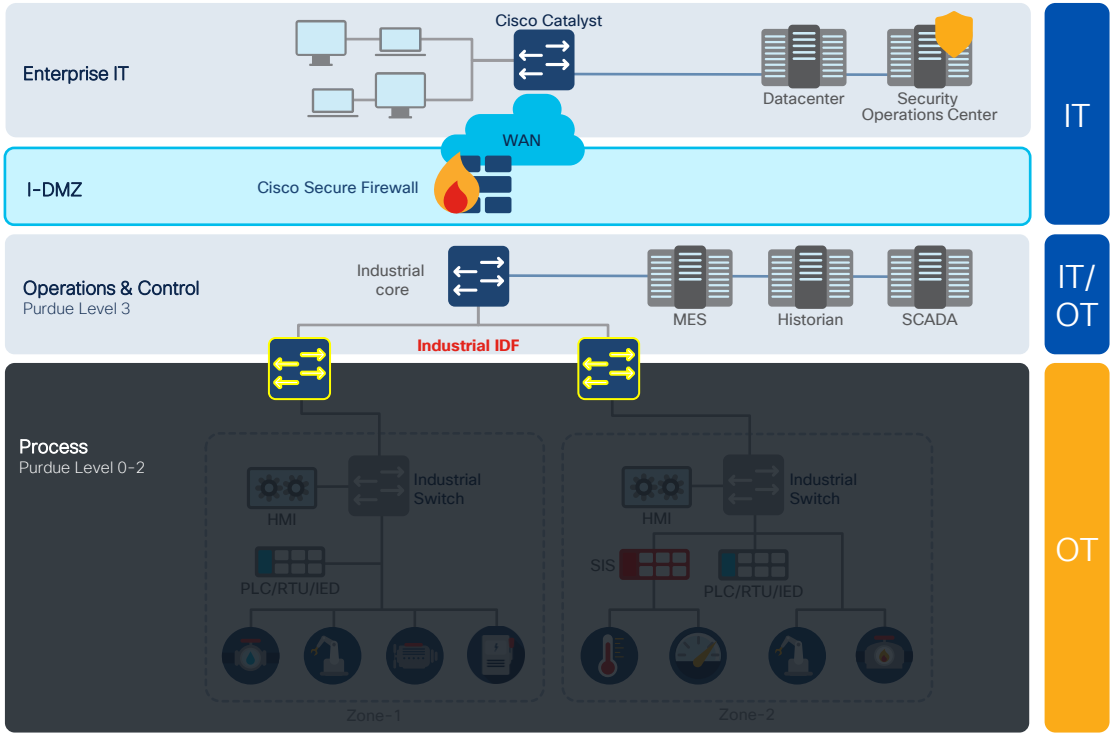
Gartner Peer Insight's Survey

What do you see as the main obstacles?



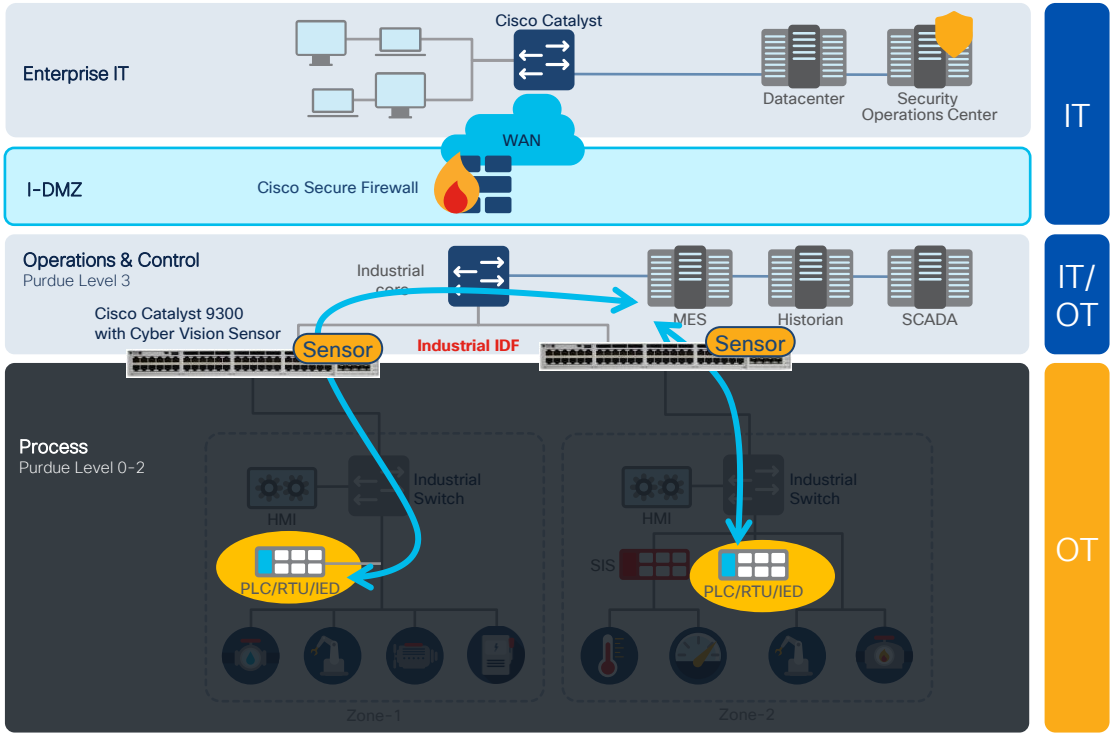
None of these **2%**, Other **1%**

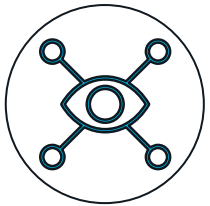
IT has no visibility below the Industrial IDF



How can IT leverage network equipment it owns to gain visibility into OT?

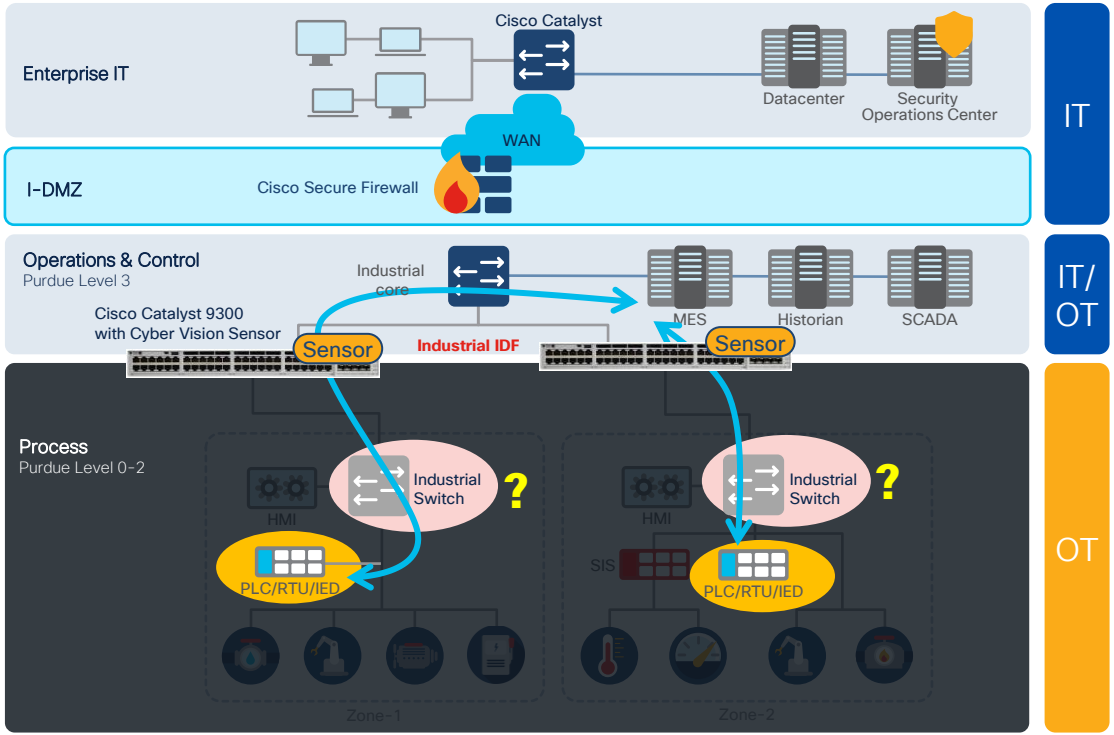
Your Catalyst switches let you turn on the lights





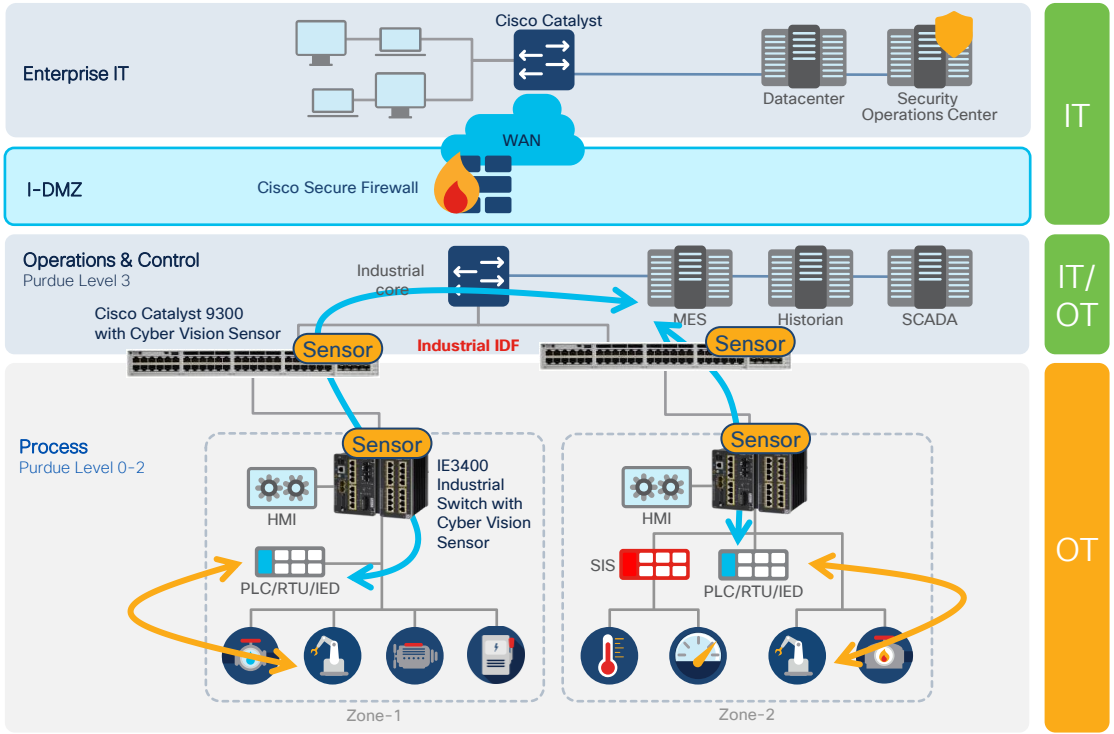
Step-1: Cyber Vision Sensor on Catalyst 9300 gives you visibility to North-South communications to identify key assets

Get OT buy-in by showing the benefits of visibility



Step-2: Work with OT to identify the critical industrial switches that connect these key assets

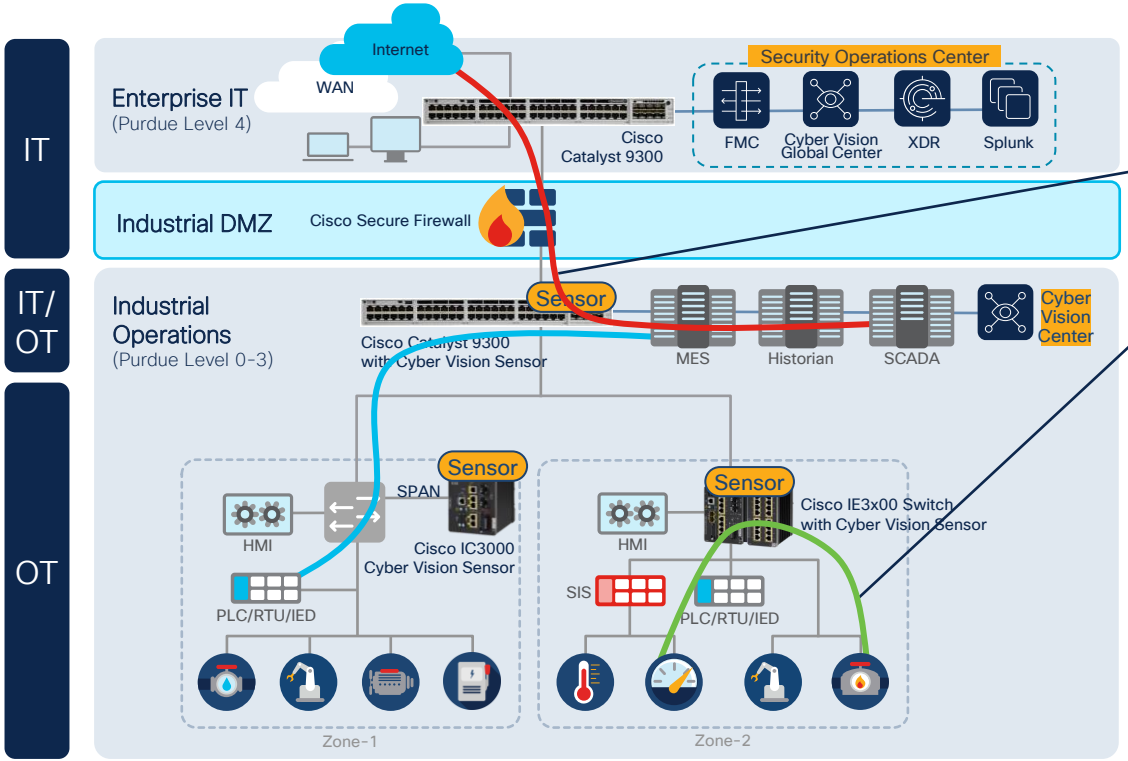
Gain full visibility to improve your security posture



Step-3: Replace critical switches with Cisco IE Switch running Cyber Vision sensor to see the entire OT network

Note: You don't need to replace all industrial switches, just the ones connecting to PLC's

Do you need a Sensor on every switch?



Sensor at aggregation sees North-South traffic

Sensor at the edge sees East-West traffic

Remember: Cyber Vision is licensed per endpoint, not per sensor!

Rule of thumb: All flows must go through at least one sensor. Every networking equipment should have a sensor.

Unified IT/OT security across 20+ flooring factories worldwide

Customer Case Study: CSSIOT-1573
Wed, Feb 12th 12:00 PM - 12:45 PM CET

Giving IT full visibility on all their OT networks to help solve production issues faster and drive collaboration with the line of business

Challenges

- Each factory had different OT network architectures and little/no security practices
- IT had no visibility into any OT networks
- An audit highlighted OT as a huge cyber risk

Results

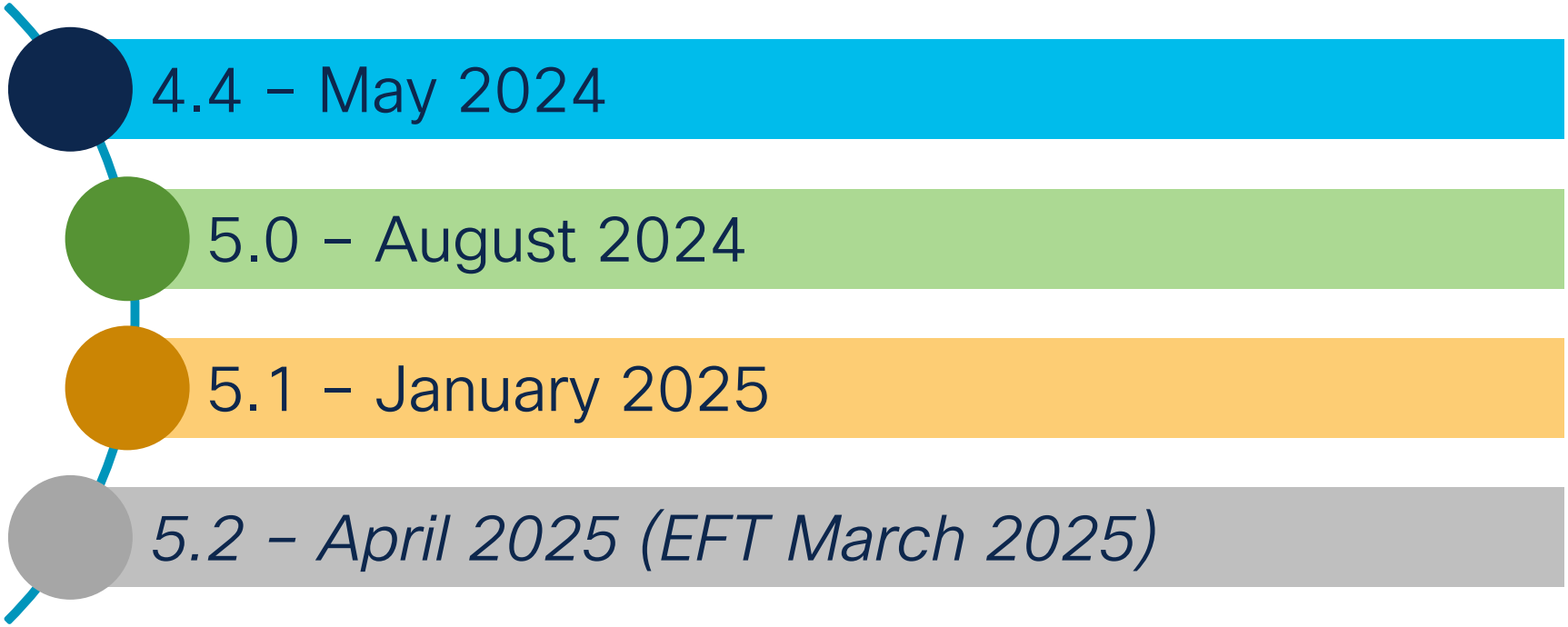
- Standardized OT networks on Cisco IE3x00 switches to improve production performance and lower costs
- Gained 100% visibility into all factories by enabling Cyber Vision sensor on Cisco IE switches
- Created a workstream between IT and OT to drive security improvements and industry 4.0 projects
- IT now has unified IT/OT security with Cyber Vision integrated with Cisco ISE, Secure Firewall and Splunk

https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/unilin-group.html

Feature Spotlight

cisco Live!

What happened since last Cisco Live (Feb 2024)?



Docker Sensor

Platform agnostic

- Support both **arm64** and **x86**
- Tested and validated with **Ubuntu** (20.04 and 22.0) and **Docker 27.0**

Versatility

- Supports **all sensor's features**
  - Passive (DPI)
  - Active Discovery
  - Snort

Scalability

- **Each sensor interface** can use a different **CPU core**
- Fit both **small compute*** for low throughput or **UCS like server** for high bandwidth

** RAM: 1GB minimum, 2GB recommended*

Docker sensor deployment steps

Docker sensor deployment steps

Step 1: Create a deployment token

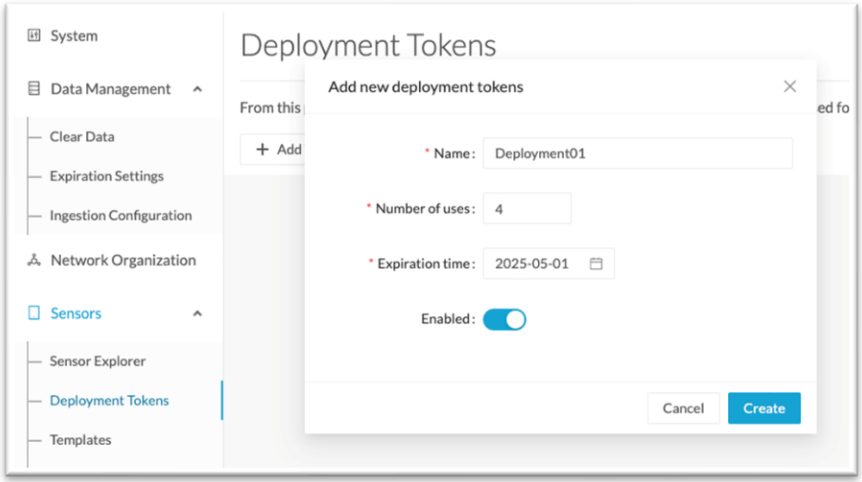
Step 2: Start the Docker wizard

Step 3: Select Sensor type (DPI, Snort, AD)

Step 4: Configure network interfaces

Step 5: Download Docker compose file

Step 6: Start the docker sensor



Docker sensor deployment steps

Step 1: Create a deployment token

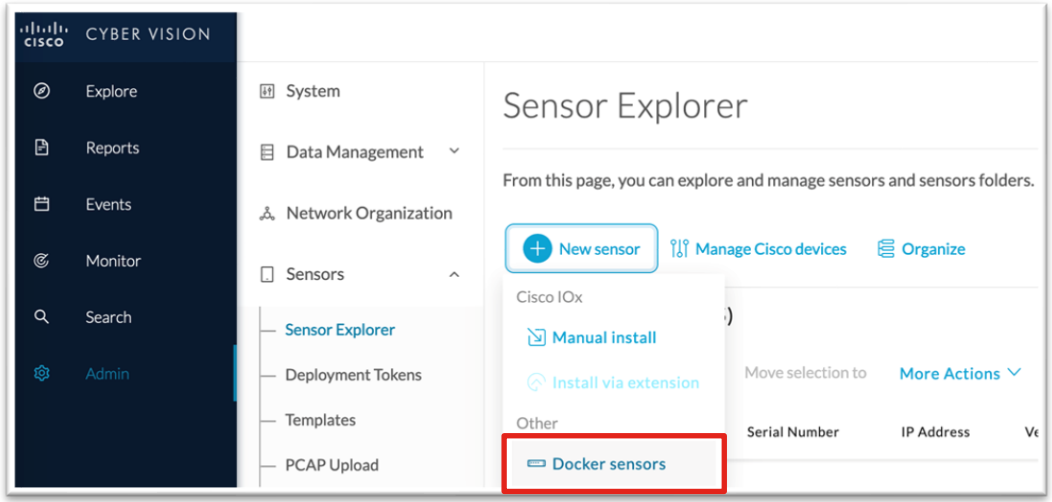
Step 2: Start the Docker wizard

Step 3: Select Sensor type (DPI, Snort, AD)

Step 4: Configure network interfaces

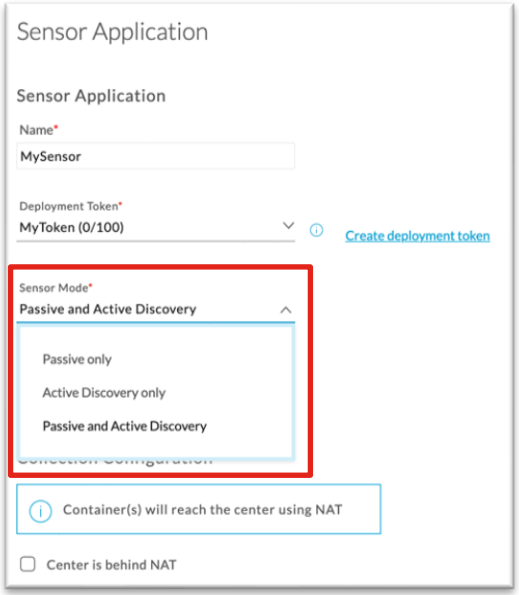
Step 5: Download Docker compose file

Step 6: Start the docker sensor



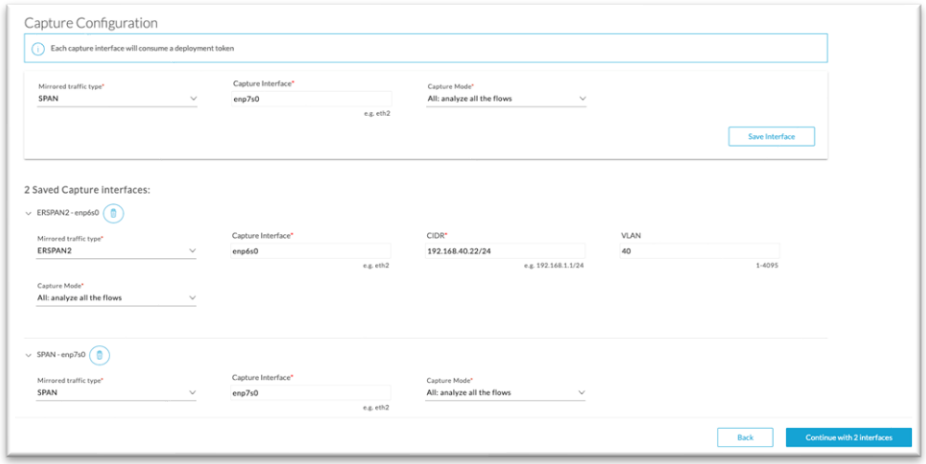
Docker sensor deployment steps

Step 1: Create a deployment token → Step 2: Start the Docker wizard → **Step 3: Select Sensor type (DPI and/or AD)** → Step 4: Configure network interfaces → Step 5: Download Docker compose file → Step 6: Start the docker sensor

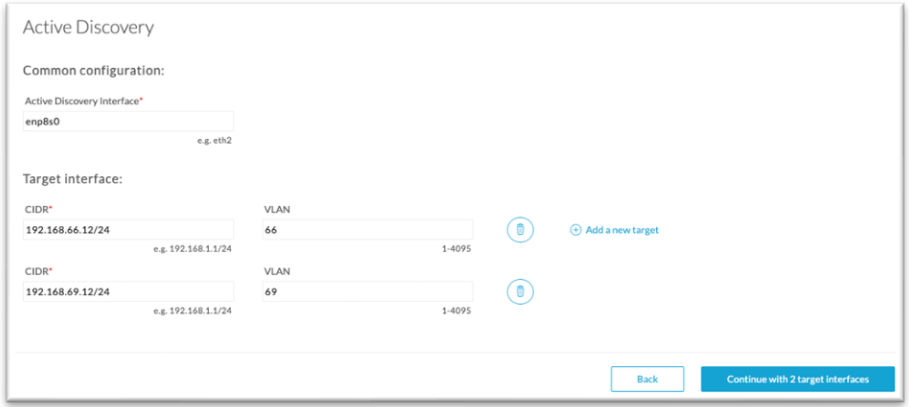


Docker sensor deployment steps

Step 1: Create a deployment token → Step 2: Start the Docker wizard → Step 3: Select Sensor type (DPI and/or AD) → **Step 4: Configure network interfaces** → Step 5: Download Docker compose file → Step 6: Start the docker sensor



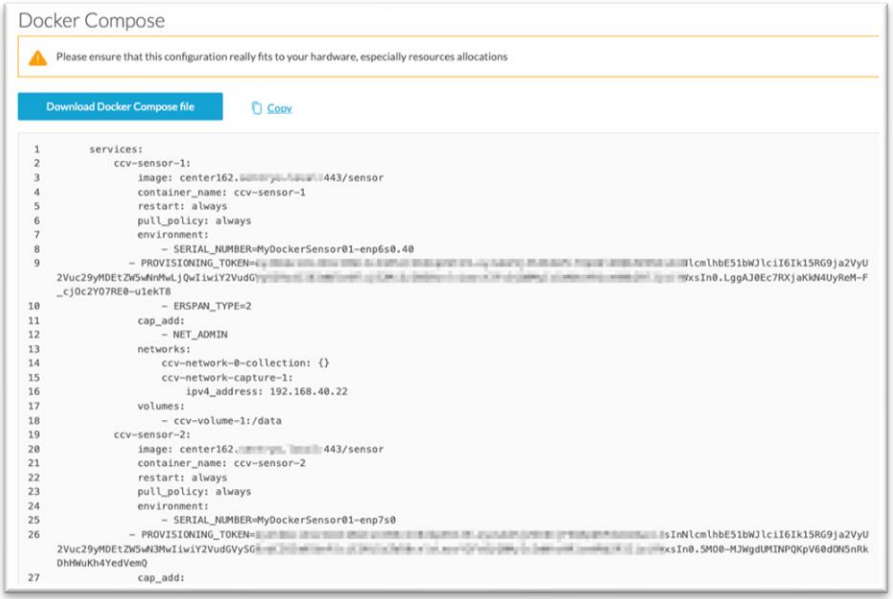
Capture interface configuration



Active Discovery configuration

Docker sensor deployment steps

Step 1: Create a deployment token → Step 2: Start the Docker wizard → Step 3: Select Sensor type (DPI and/or AD) → Step 4: Configure network interfaces → **Step 5: Download Docker compose file** → Step 6: Start the docker sensor



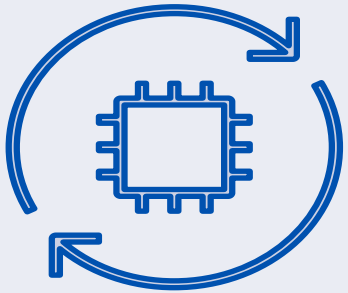
Docker sensor deployment steps

Task	Command	Result
Interactive sensor creation	docker compose up	System will display stderr/stdout of the instance. End with Ctrl+C
Start and run sensor independently	docker compose up -d	System will start the docker container instances to the background and leave them running
Forcefully recreate the docker instance	docker compose up --force-recreate -d	End existing sensor, recreate a new instance and send it to the background.
Interactive access to container instance	docker exec -it <sensor-name> /bin/bash	Provides CLI access to the running docker instance.
Stopping a docker sensor	docker stop <sensor-name>	Stopping a running docker container.
Start/Stop an existing docker sensor	docker start <sensor-name> docker stop <sensor-name>	Change the state of operation of an existing instance of a docker sensor.

Docker sensor limitation

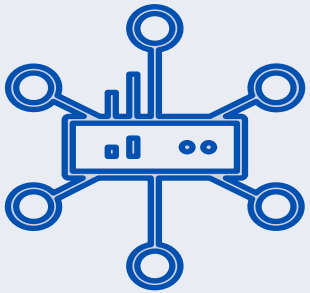
- Active Discovery cannot use sensor’s collection interface
- By default, sensor will run without any resource limitation
- The docker host needs to trust Cyber Vision CA to pull the app

Other sensor enhancements



Sensor app in-place update

Support of Cat9300 without SSD

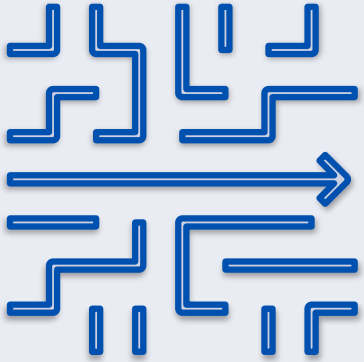


Catalyst SD-WAN Manager support

Cyber Vision New UI/UX (preview)

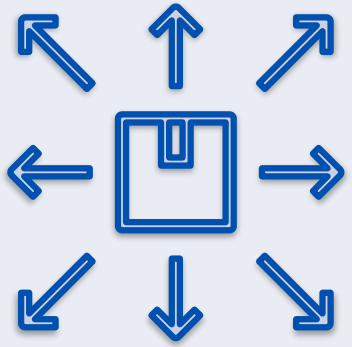
cisco Live!

Goal of this new UI

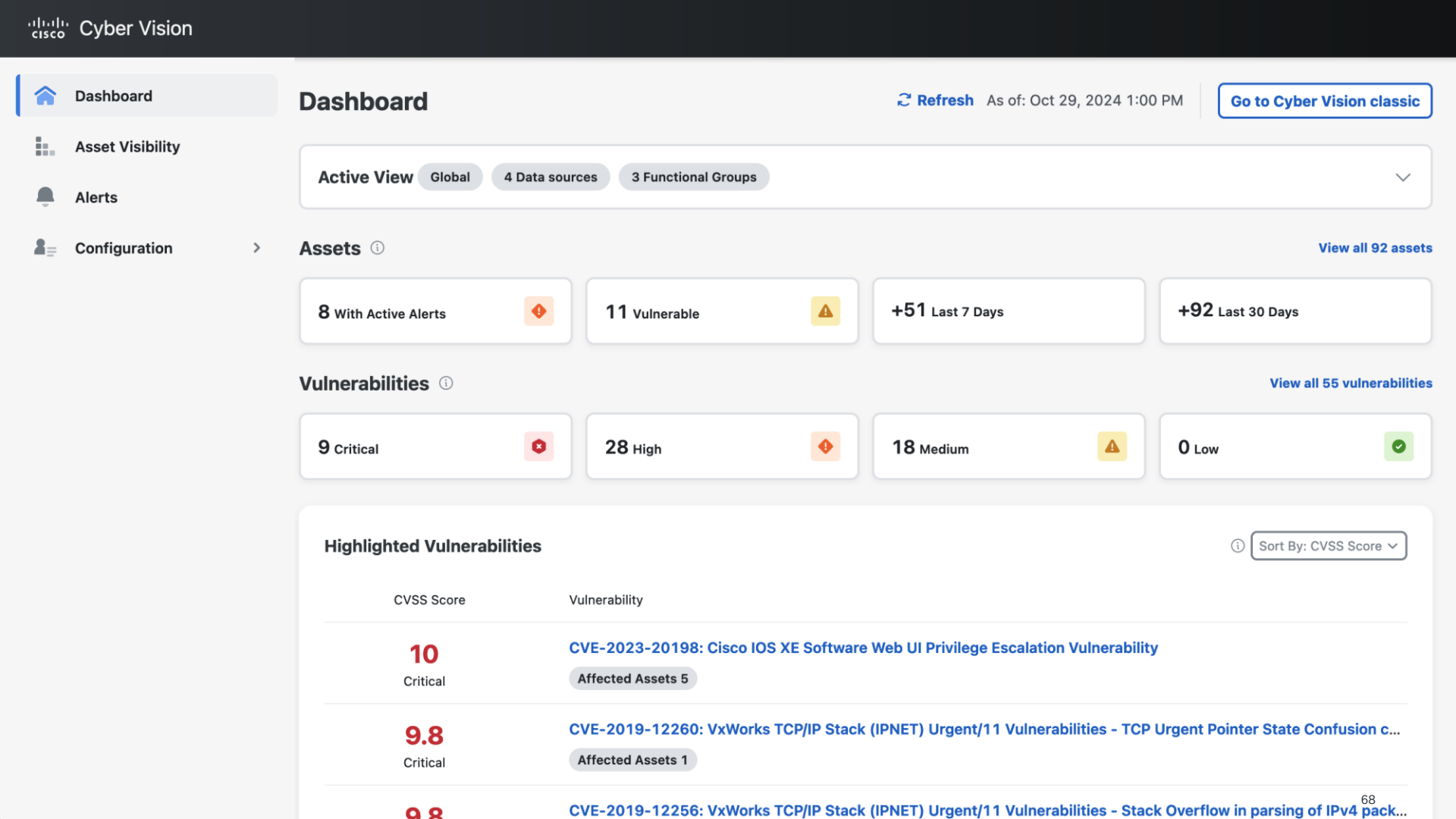


Simplified User Experience (aligned with other Cisco products)

Reduced time-to-value



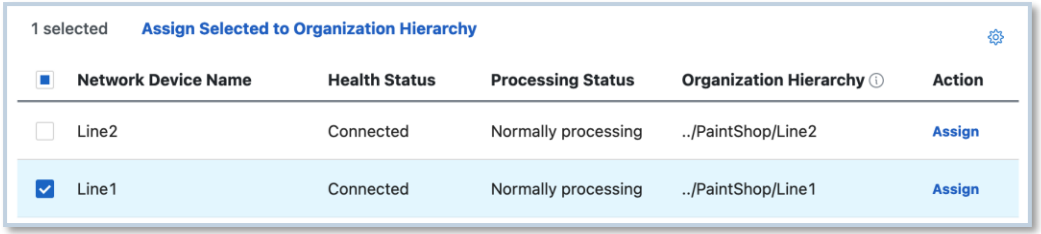
Enhanced scalability

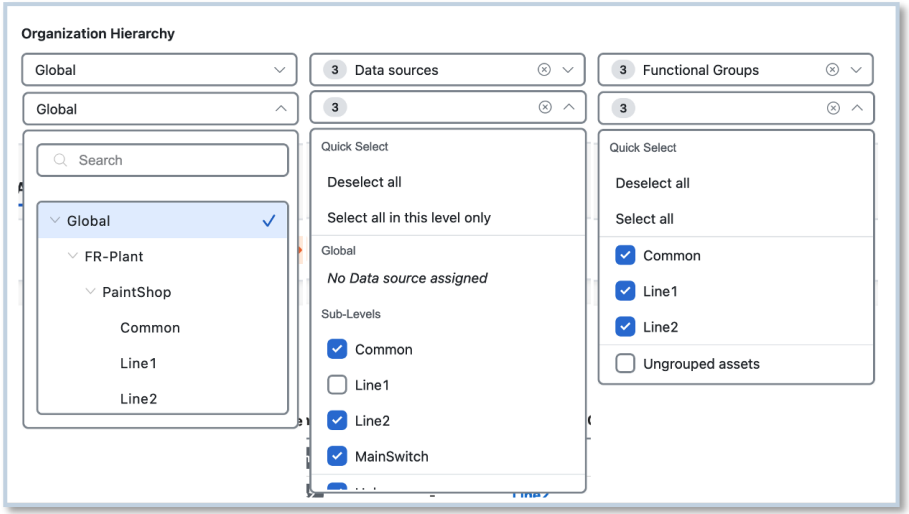

Cyber Vision
Dashboard
Asset Visibility
Alerts
Configuration
Dashboard
Refresh
As of: Oct 29, 2024 1:00 PM
Go to Cyber Vision classic
Active View
Global
4 Data sources
3 Functional Groups
Assets
View all 92 assets
8 With Active Alerts
11 Vulnerable
+51 Last 7 Days
+92 Last 30 Days
Vulnerabilities
View all 55 vulnerabilities
9 Critical
28 High
18 Medium
0 Low
Highlighted Vulnerabilities
Sort By: CVSS Score
CVSS Score
Vulnerability
10
Critical
CVE-2023-20198: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability
Affected Assets 5
9.8
Critical
CVE-2019-12260: VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion c...
Affected Assets 1
9.8
CVE-2019-12256: VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Stack Overflow in parsing of IPv4 pack...

New Beta UI Preview – Viewing Data

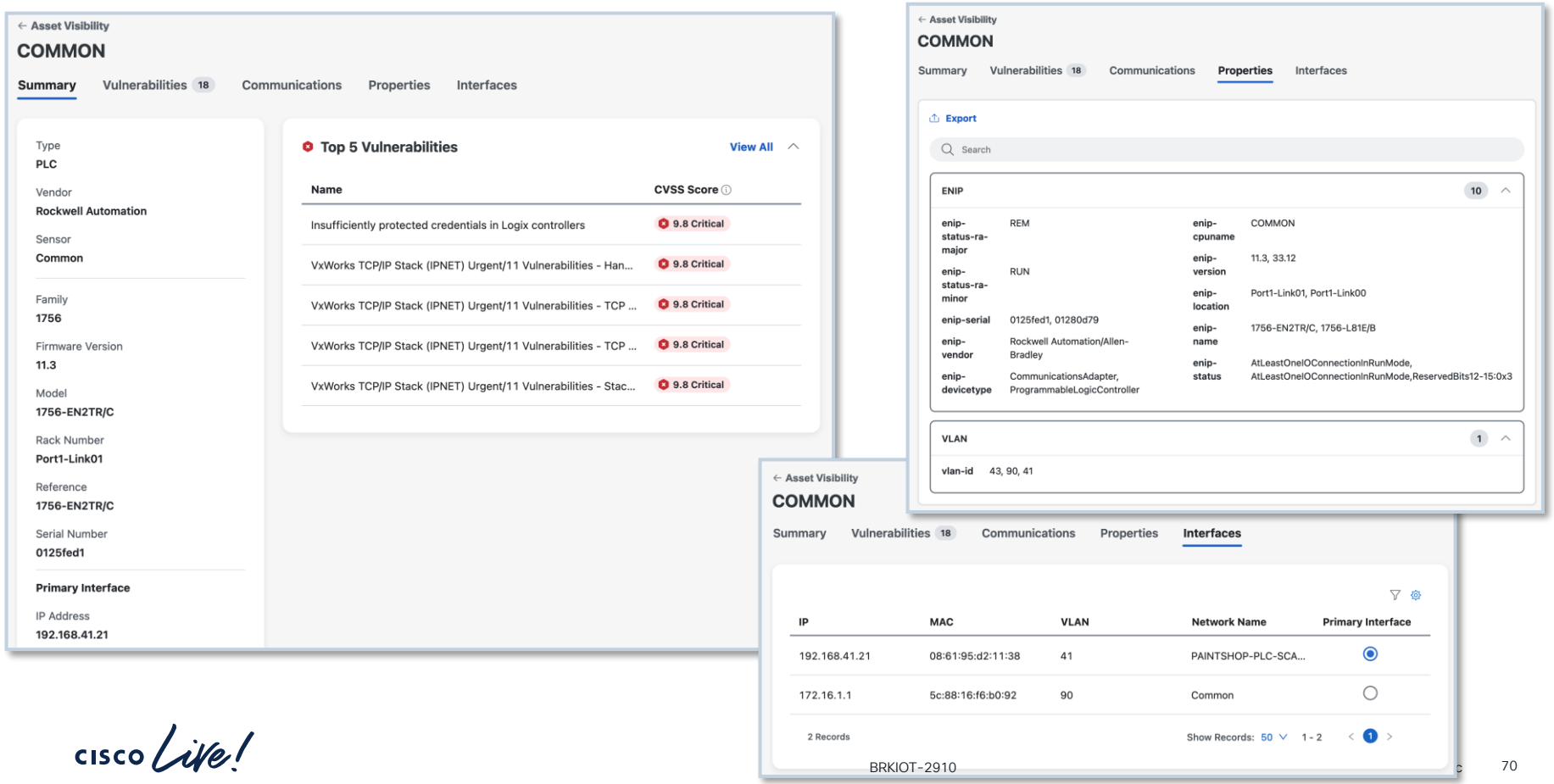
Navigate data displayed by selecting parameters

- Organization Hierarchy is nested selections of data sources
- Each asset has a primary data source (sensor or PCAP)
- Functional Groups are assets auto clustered based on network communications

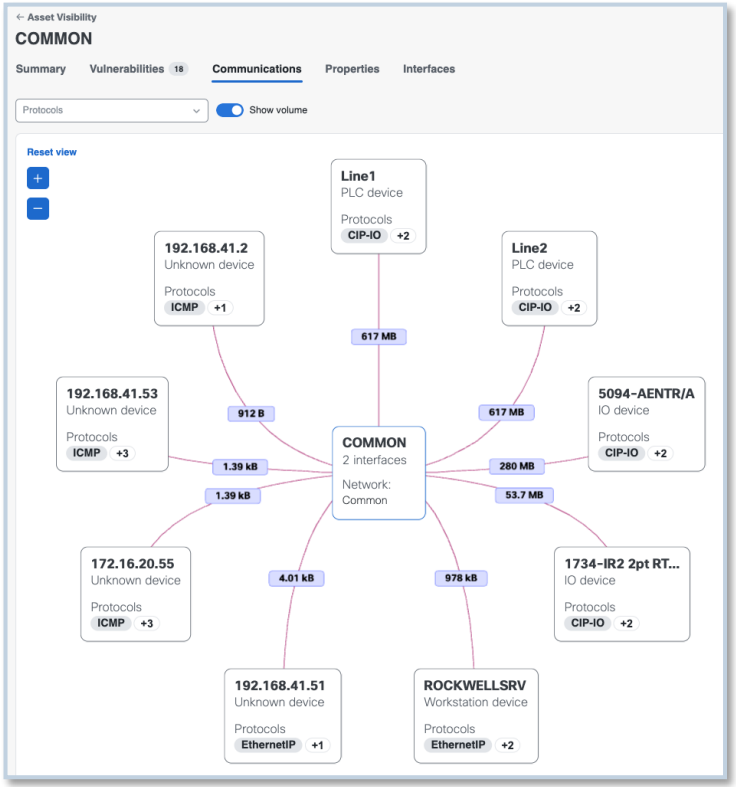


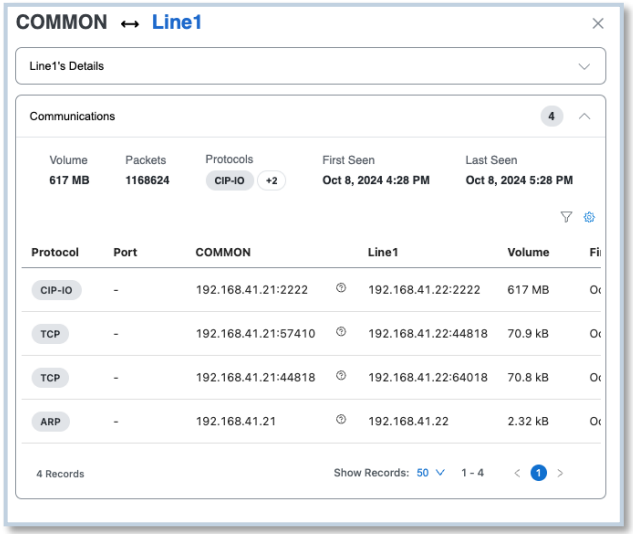


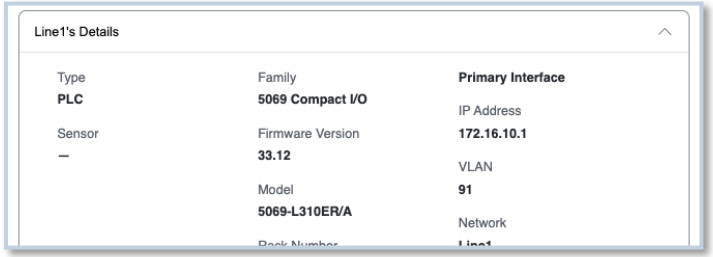
New Beta UI Preview – Assets



New Beta UI Preview – Asset Communications



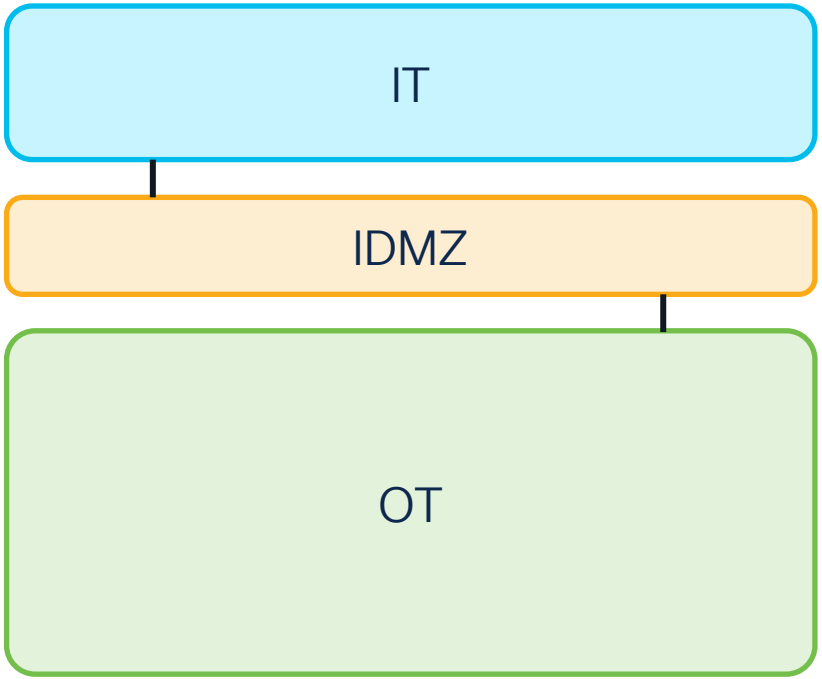




Network Segmentation: ISE & Firewall

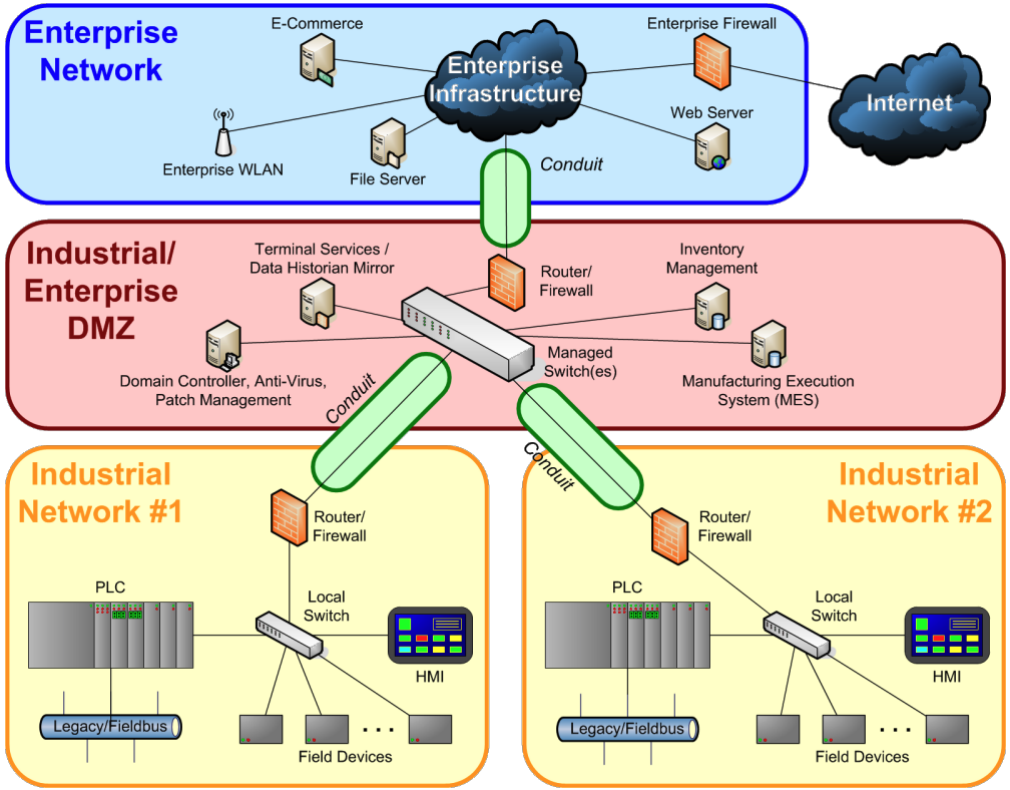
cisco Live!

The Purdue Model



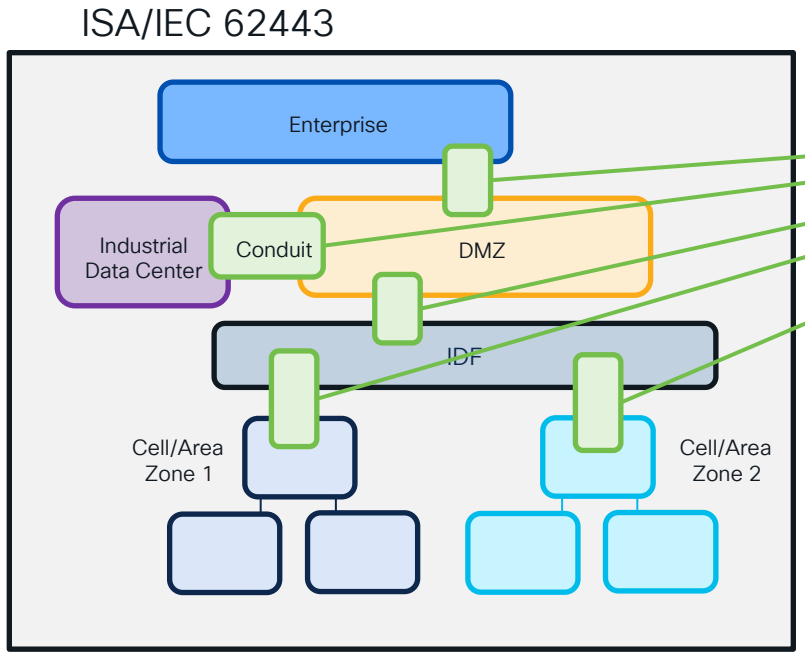
- No direct communication between IT (level 4 & 5) & OT (level 0 – 3)
- IDMZ services (level 3.5) are recommended to be segmented from each other
  - i.e. each service in its own VLAN and terminates at the firewall
- OT consists of site operations zone (level 3) and Cell/Area zone (level 0-2)

IEC 62443 Zones & Conduits



- **Zone**: Collection of entities that represent a partitioning of a System under Consideration (SUC) based on their functional, logical and physical (including location) relationship that share common security requirements
- **Conduit**: Physical or logical grouping of communication channels, intermittent or permanent, between connecting a zone with another zone or with the outside that share common security requirements
- The intent is to identify those assets which share common security characteristics in order to establish a set of common security requirements that reduce cybersecurity risk

The Segmentation Journey – Virtual Segmentation



Virtual Segmentation

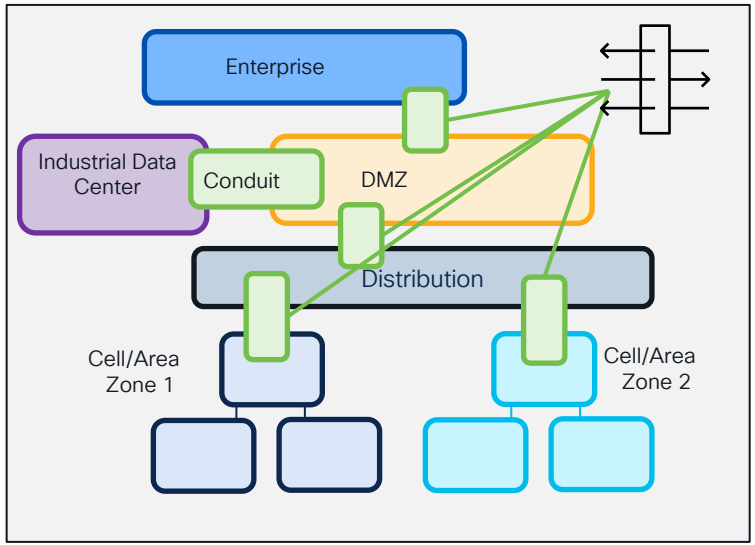
Visualizing the zones and conduits model and reacting to data observed between zones

The Segmentation Journey – Macro and Micro

Macro Segmentation

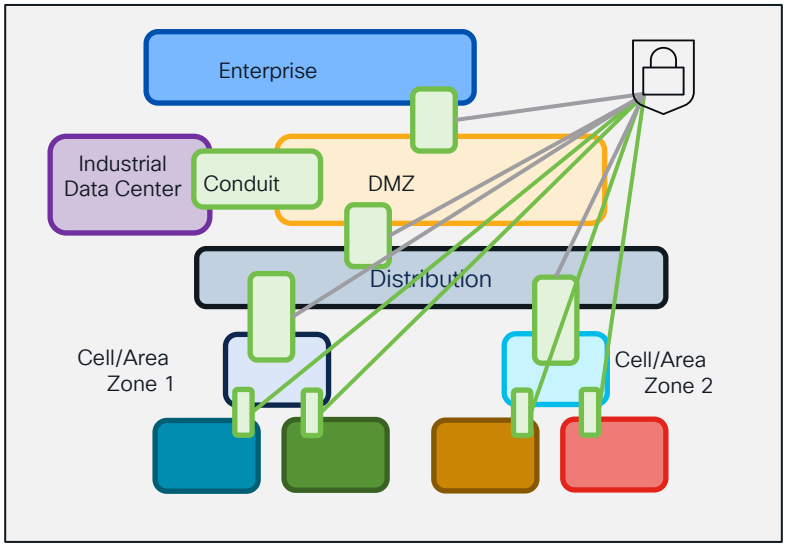
- Policy across “large” zones (between Cell/Area Zones / Production Lines)
- Distribution is typically point of VLAN termination
- Generally done at Firewall level

ISA/IEC 62443



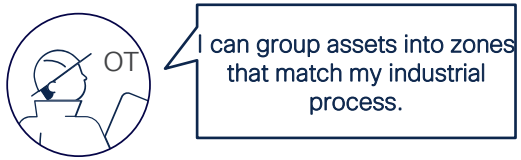
Micro Segmentation

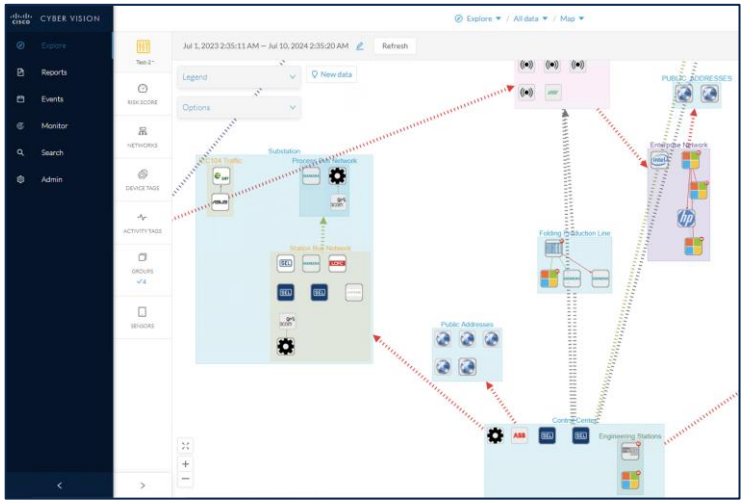
- Pushing policy across “small” zones
- Segmentation within Cell/Area Zones
- It can be done on firewall, switches or routers

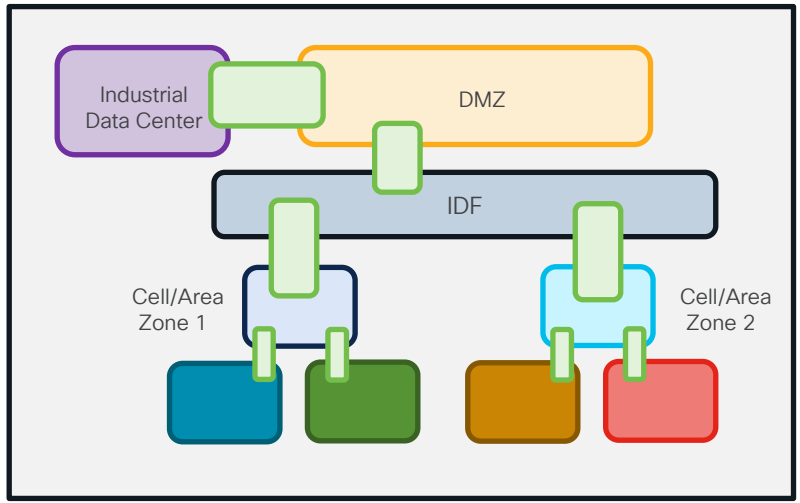


Streamlining OT Segmentation with Cyber Vision Visibility

Endpoint Profile | Activity Tags | Network Flows | Risk Score

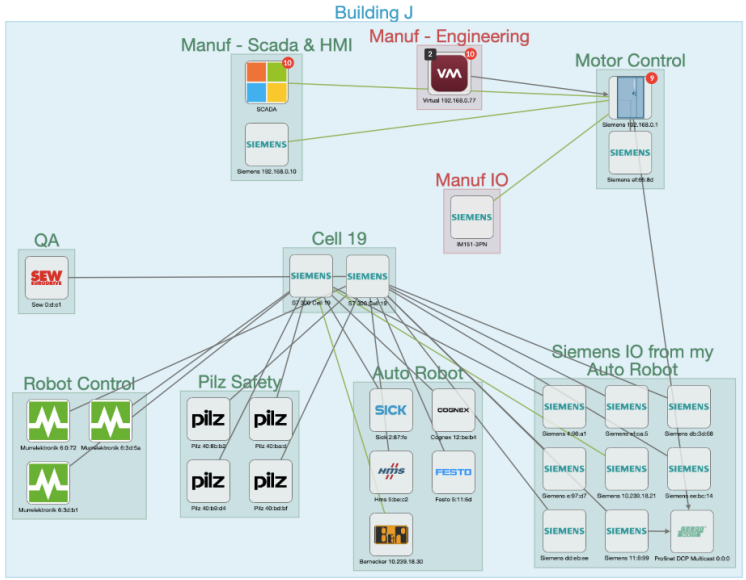






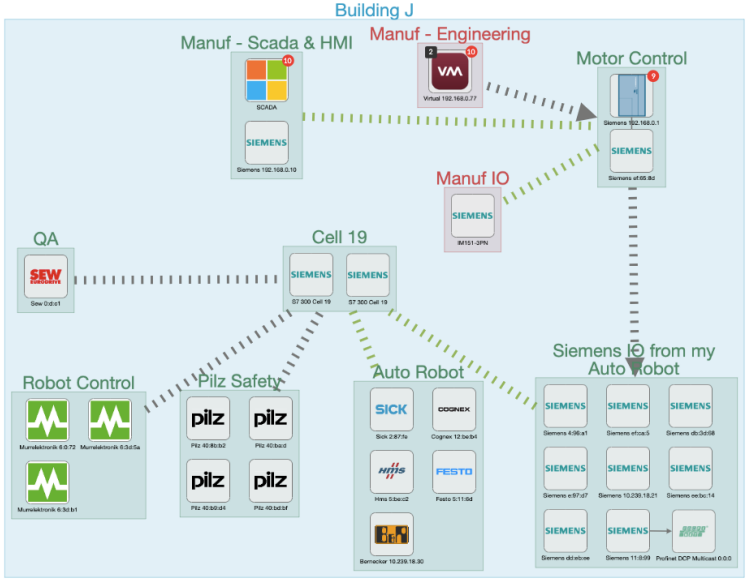
Aggregated activities match IEC62443 conduits

Unaggregated



View all asset relationships

Aggregated

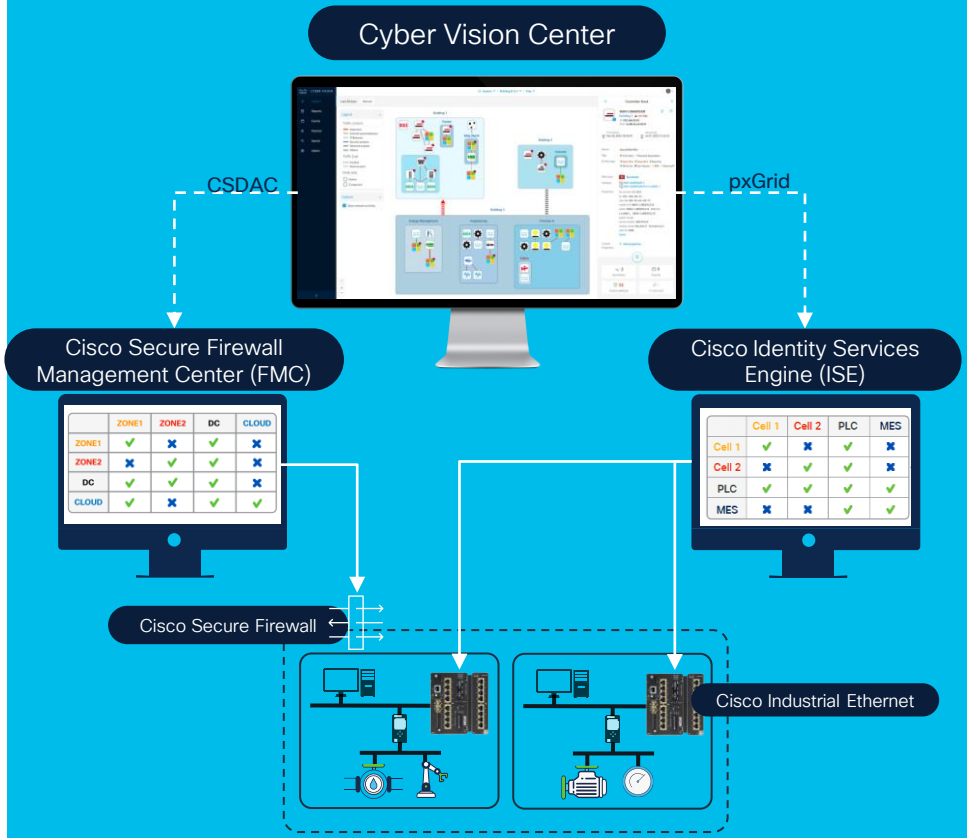


Easily browse through conduits

Cyber Vision Integration for Segmentation

OT visibility drives segmentation to mirror industrial processes

- 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

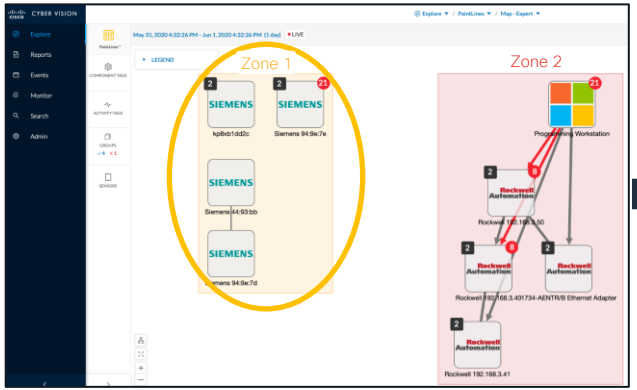


Automated **ISA/IEC-62443** zone segmentation using firewalls or switches

Automated Segmentation **Informed by Visibility**

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	✗	✗	✓	✓

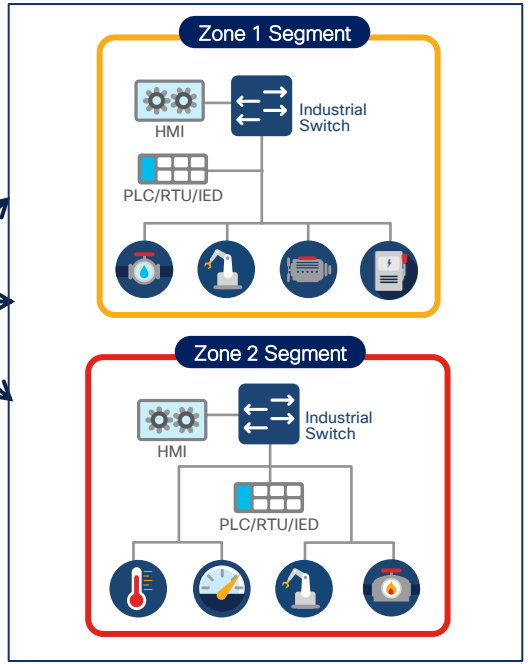
Cisco ISE Policy Matrix

dACL

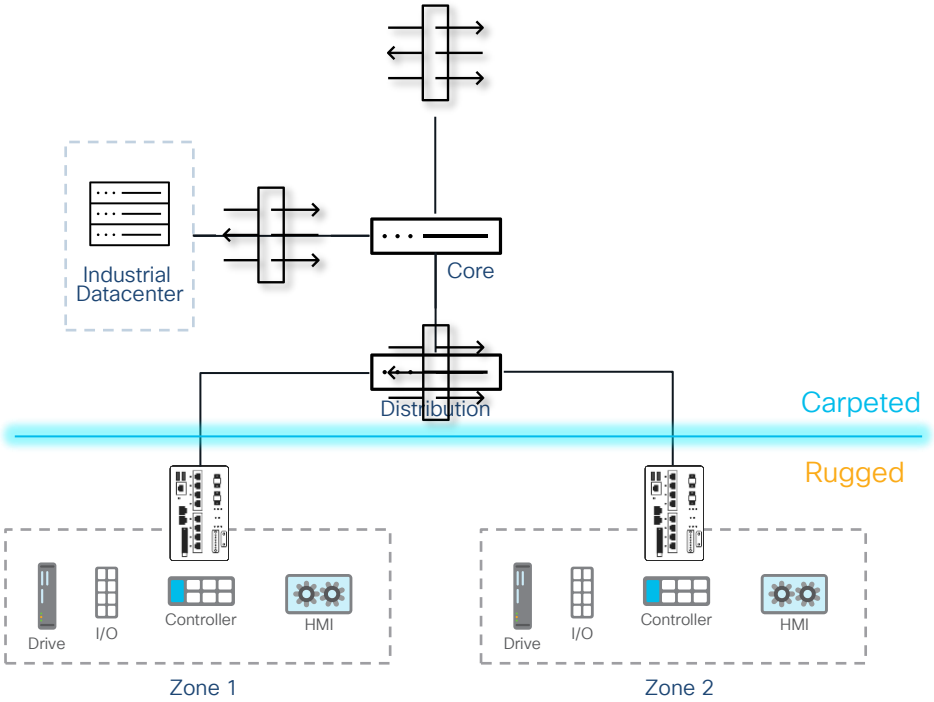
SGT

VLAN

Segmentation of industrial network



Firewalls in Plant Networks



IT / OT Boundary

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

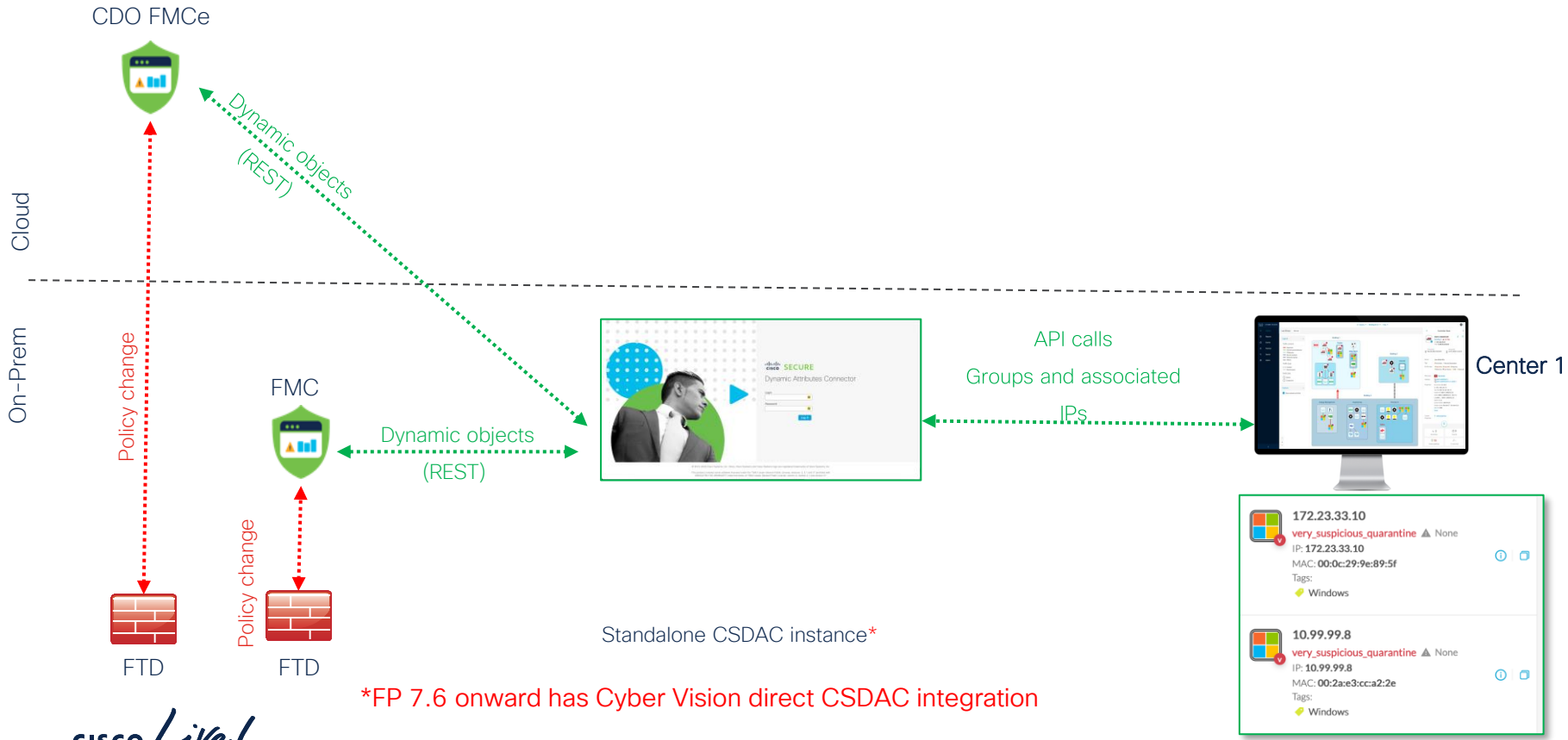
Industrial Data Center

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)

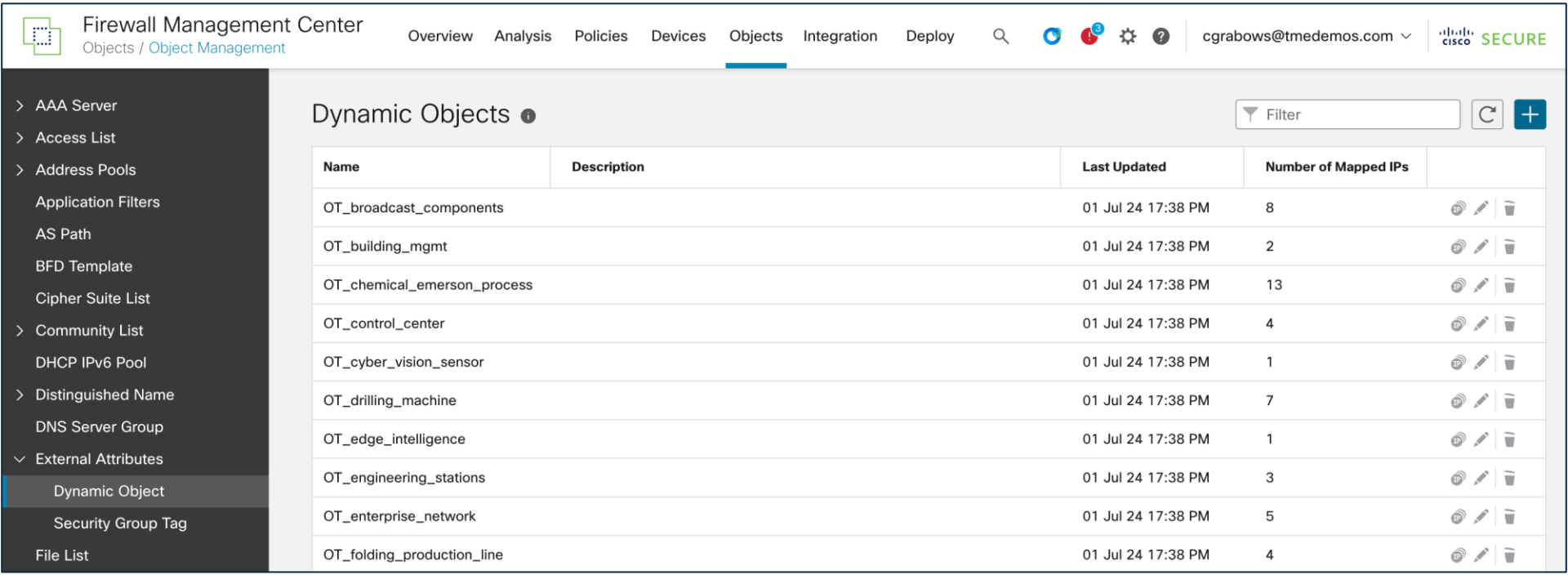
A common deployment model in OT is to terminate VLANs at a firewall. This reduces the need for firewalls per cell

Cisco Secure Dynamic Attributes Connector Cyber Vision Integration



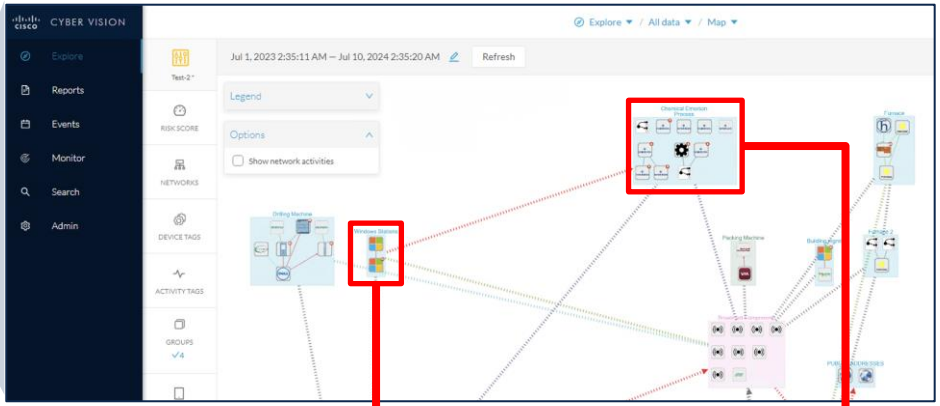
*FP 7.6 onward has Cyber Vision direct CSDAC integration

Cisco Secure Dynamic Attributes Connector Cyber Vision Integration



Firewall Policy with OT Dynamic Objects

Cyber Vision



Firewall policies automatically follow dynamic OT groups.

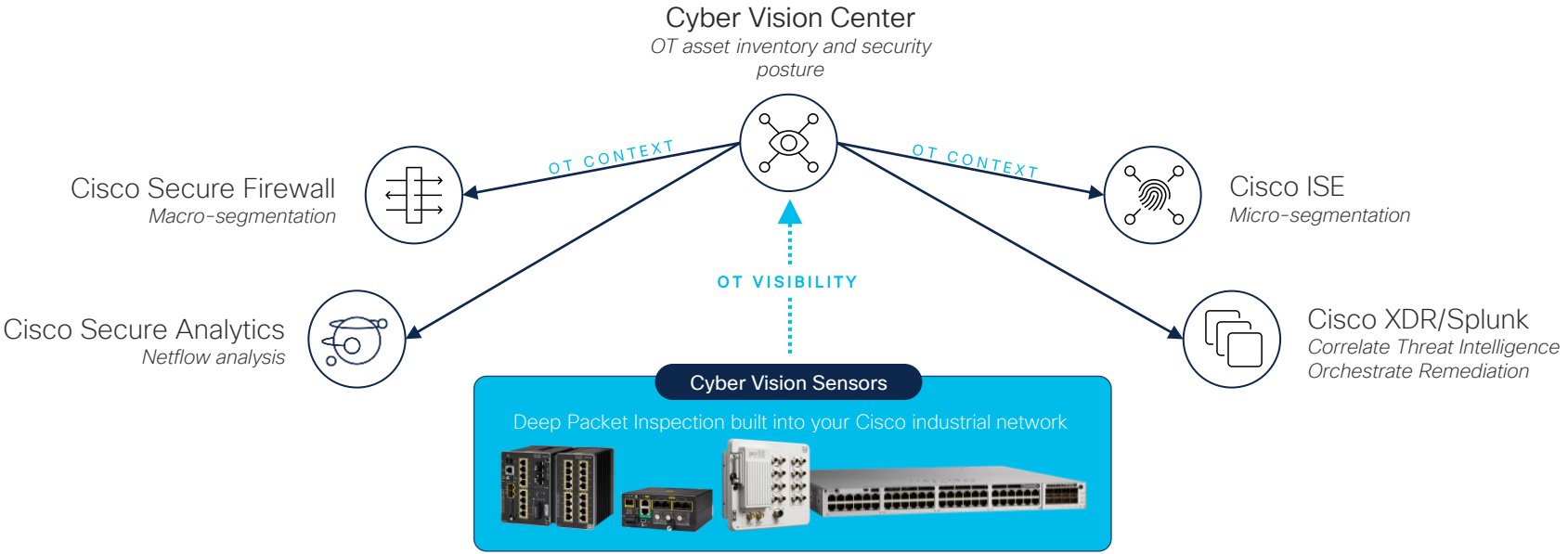
FMC

	Name	Action	Sources	Destinations and Applications
	Mandatory (No rules)			
	Default (1 - 3)			
1	Management Access	Allow	NET Engineering-Range	APP HTTPS, RDP, SSH DYN OT_management_stations
2	Folding Process CTRL	Allow	DYN OT_control_center	APP S7Comm, S7Comm Ack, S7Comm Ack Data DYN OT_folding_production_line
3	New-Rule-#2-ALLOW	Allow	DYN OT_windows_stations	DYN OT_chemical_emerson_process

Cyber Vision Integration Splunk & XDR

cisco Live!

Extend IT security to your industrial settings



The broadest OT security solution on the market • Powered by Talos Threat Intelligence

Cisco XDR

Investigate & remediate the highest priority incidents with greater speed, efficiency, and confidence

Extended

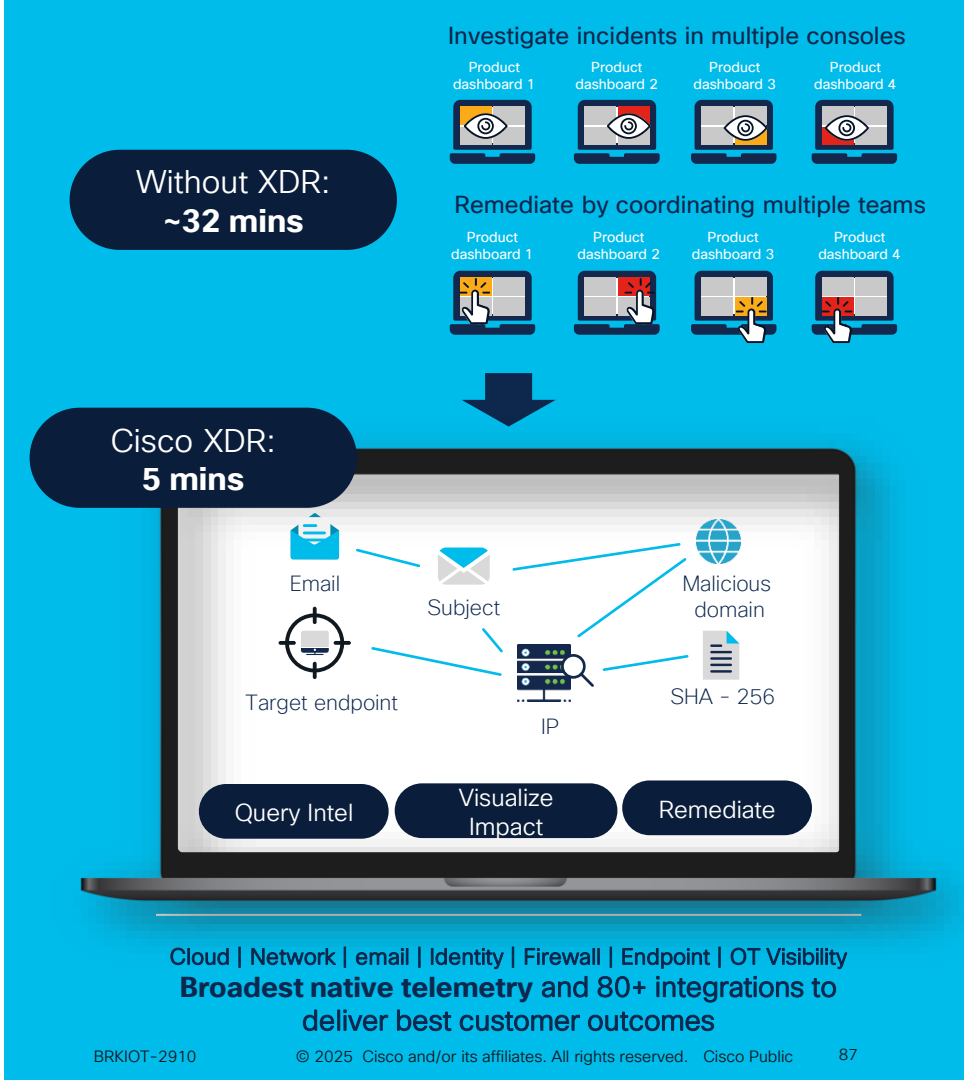
Multi-vector telemetry ingest from network, cloud, endpoint, email, and more from Cisco and 3rd party

Detection

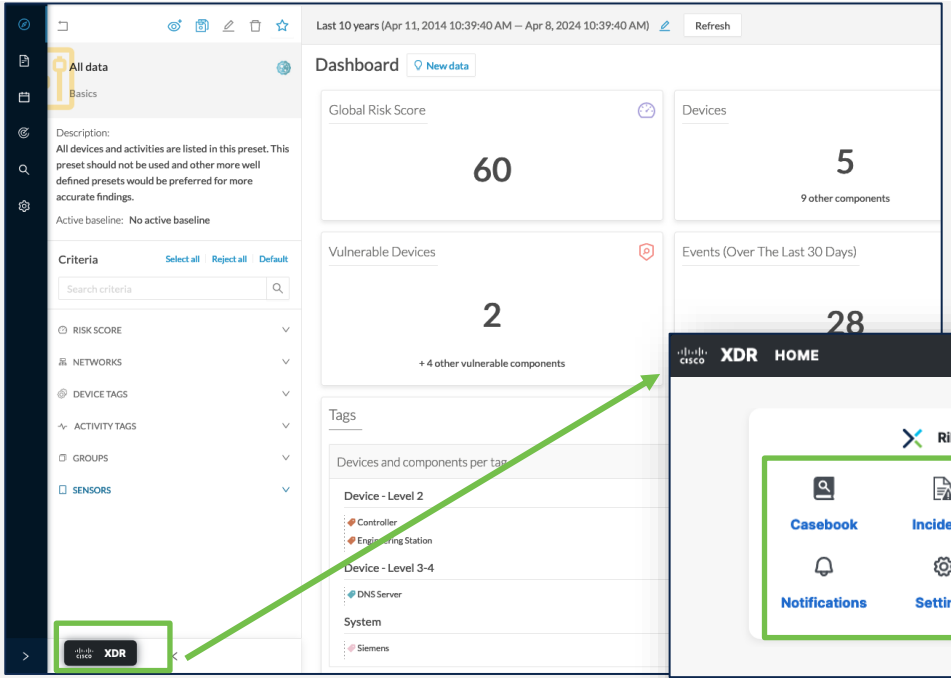
Cross domain alert detections and attack chaining with automated incident prioritization and enrichment

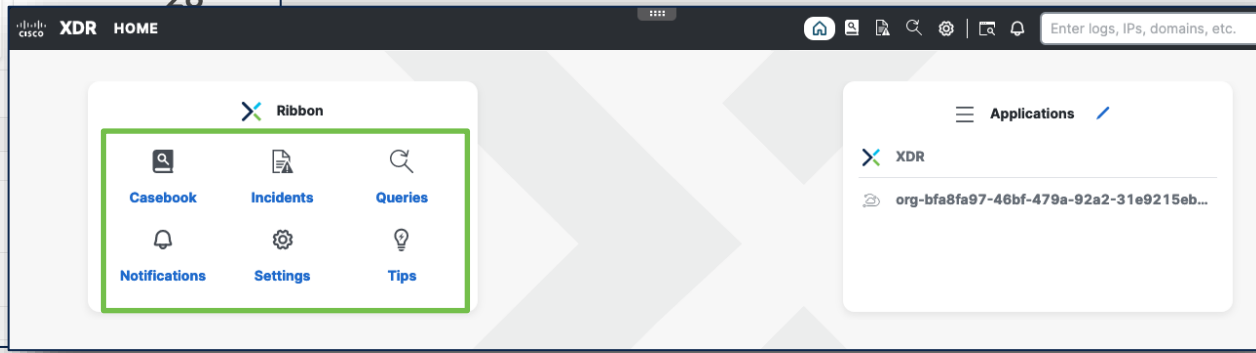
Response

Automated or user triggered responses to block observables using any integrated technology



Cisco XDR Ribbon on Cyber Vision: Investigation & Orchestration

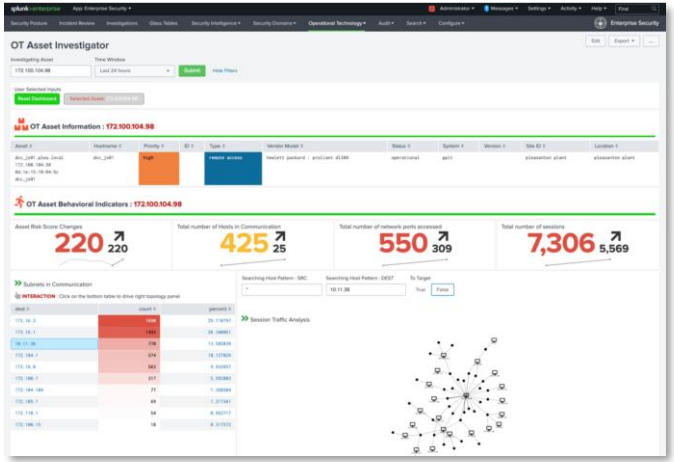


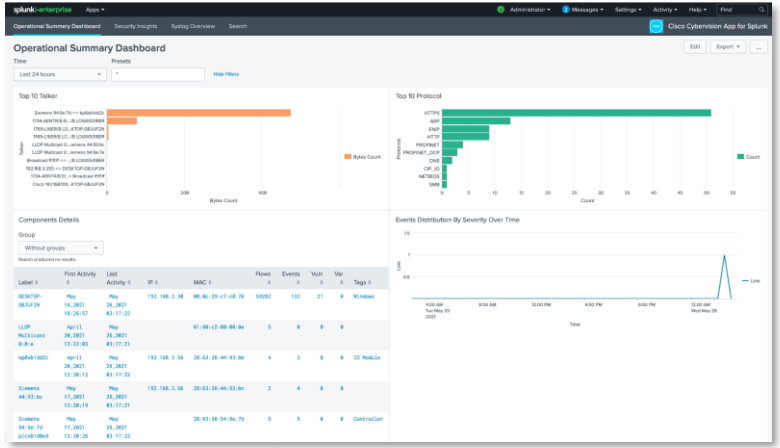


Create and manage incidents,
Launch investigations,
Orchestrate playbooks...

...directly from Cyber Vision

Unified visibility across IT and OT with Splunk





Splunk OT Add-on

Cyber Vision App

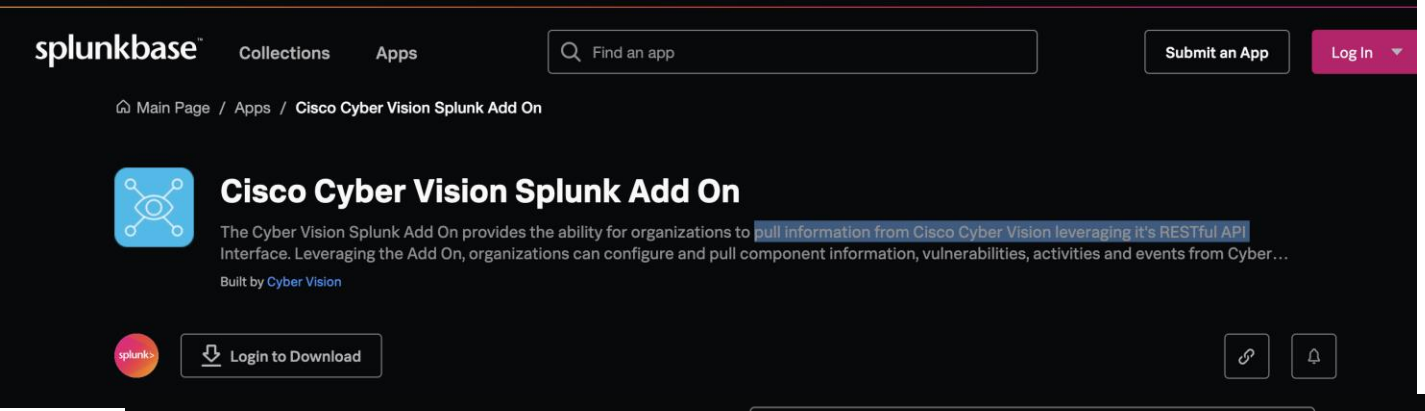
Cyber Vision Center(s)

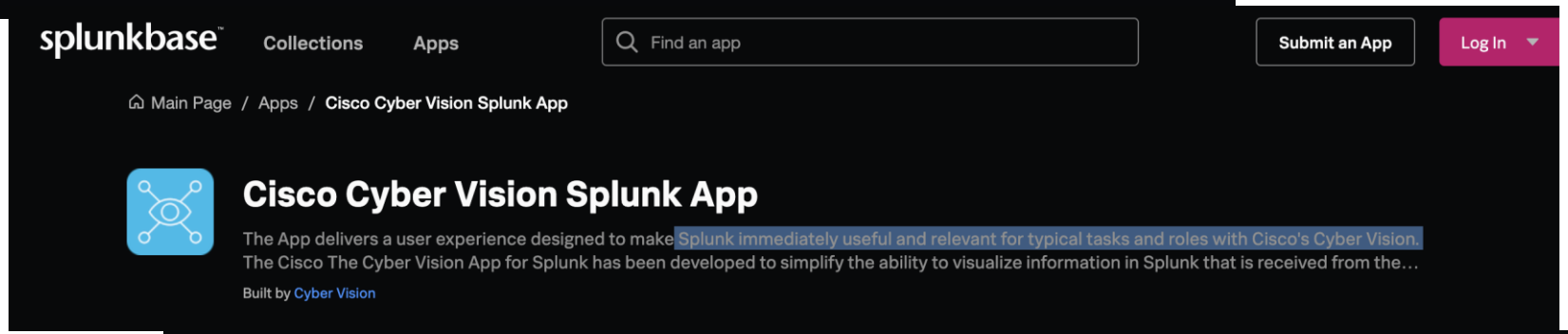
Splunk Enterprise Security

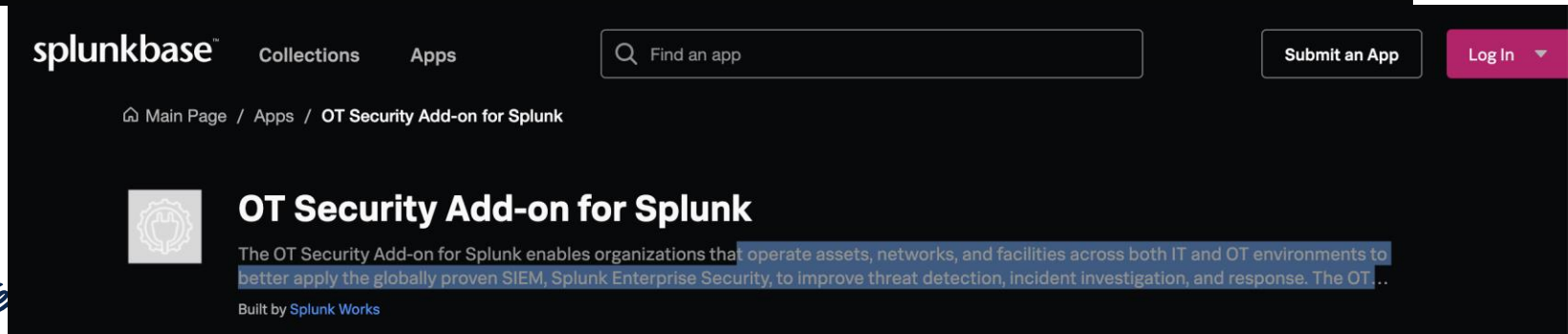
Cyber Vision Add-On

REST API

Splunk base


splunkbase
Collections
Apps
Find an app
Submit an App
Log In
Main Page / Apps / Cisco Cyber Vision Splunk Add On
Cisco Cyber Vision Splunk Add On
The Cyber Vision Splunk Add On provides the ability for organizations to pull information from Cisco Cyber Vision leveraging it's RESTful API Interface. Leveraging the Add On, organizations can configure and pull component information, vulnerabilities, activities and events from Cyber…
Built by Cyber Vision
Login to Download

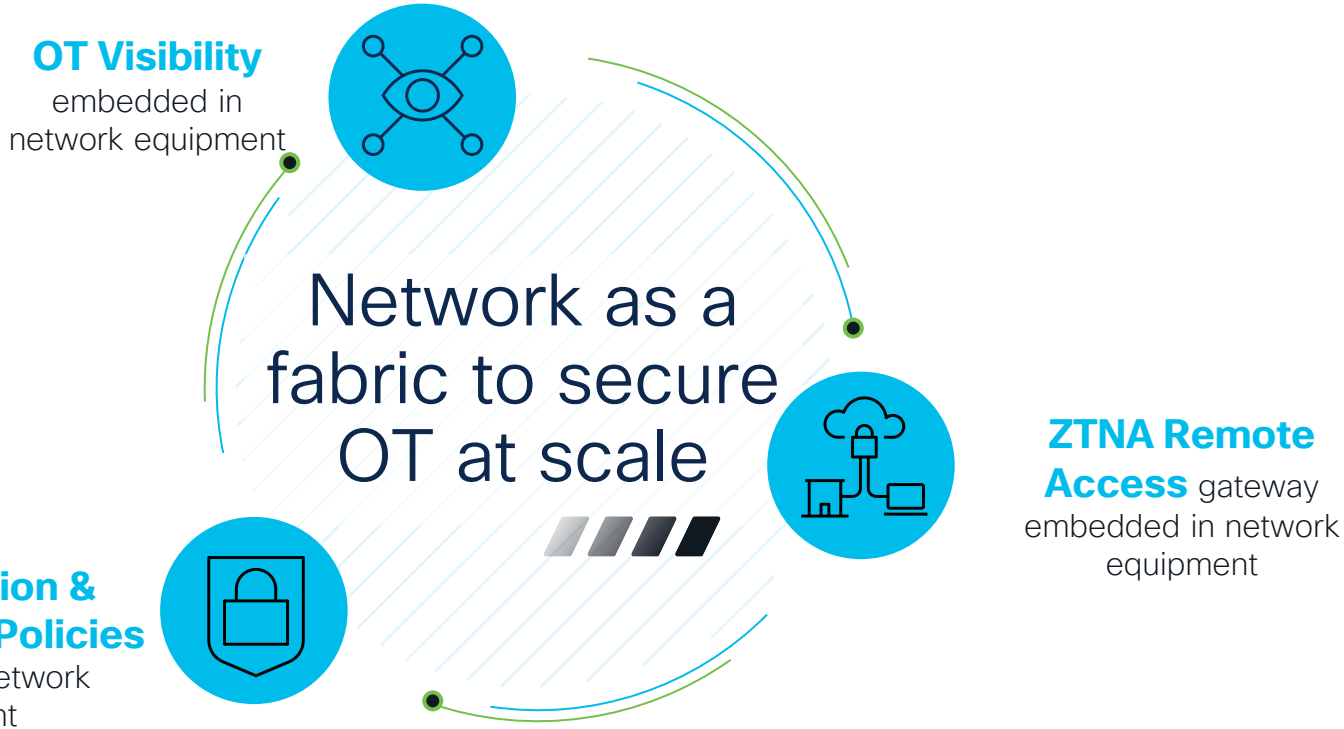

splunkbase
Collections
Apps
Find an app
Submit an App
Log In
Main Page / Apps / Cisco Cyber Vision Splunk App
Cisco Cyber Vision Splunk App
The App delivers a user experience designed to make Splunk immediately useful and relevant for typical tasks and roles with Cisco's Cyber Vision. The Cisco The Cyber Vision App for Splunk has been developed to simplify the ability to visualize information in Splunk that is received from the…
Built by Cyber Vision


splunkbase
Collections
Apps
Find an app
Submit an App
Log In
Main Page / Apps / OT Security Add-on for Splunk
OT Security Add-on for Splunk
The OT Security Add-on for Splunk enables organizations that operate assets, networks, and facilities across both IT and OT environments to better apply the globally proven SIEM, Splunk Enterprise Security, to improve threat detection, incident investigation, and response. The OT…
Built by Splunk Works

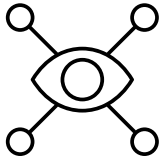
cisco Live

Conclusion

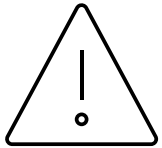
The Cisco Industrial Security Differentiation



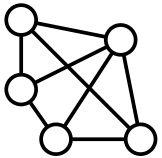
You cannot secure what you cannot see



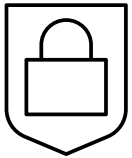
List all the assets you are defending



Spot vulnerabilities to patch



Identify asset communication issues



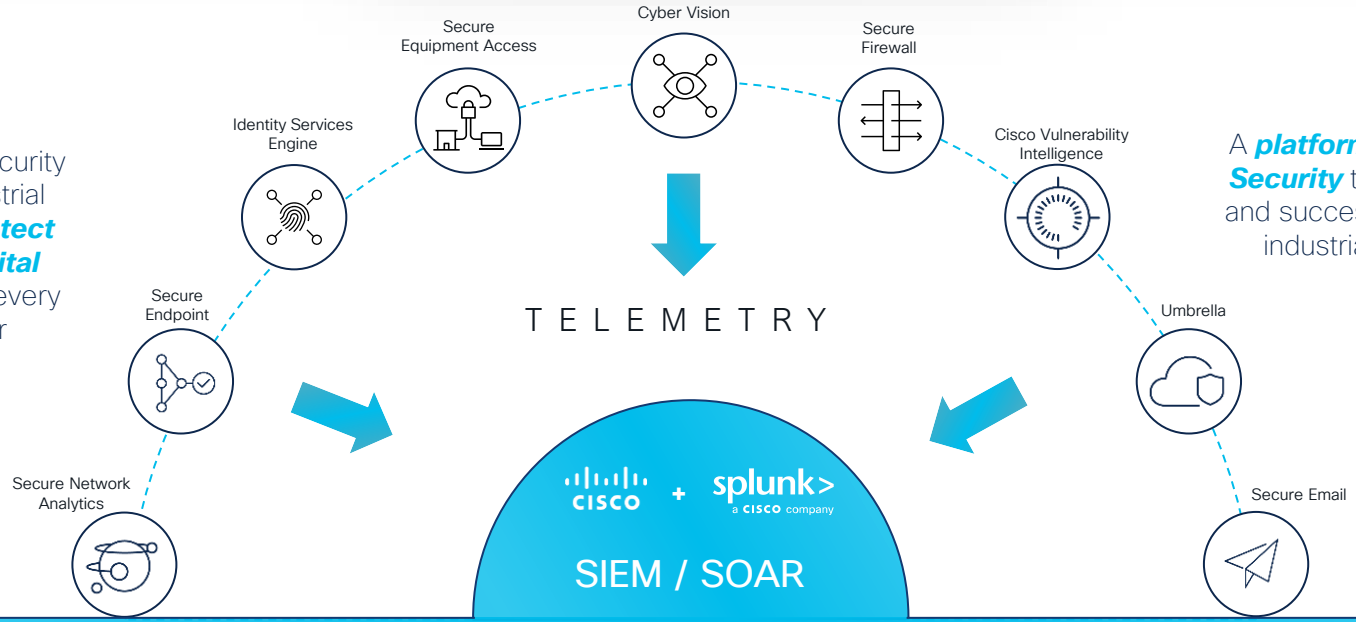
Detect bypass or leaks in the IDMZ

Build compliance reports

Gain visibility into your OT to take corrective actions, segment networks, build security policies and drive best practices

Threat Intelligence — AI — Identity Intelligence

The most comprehensive security solution for industrial customers to ***protect their entire digital footprint*** across every aspect of their organization



A ***platform for OT, IT, and Security*** teams ***to partner*** and successfully defend the industrial environment

AI powered cross-domain security across IT, OT, and Cloud

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

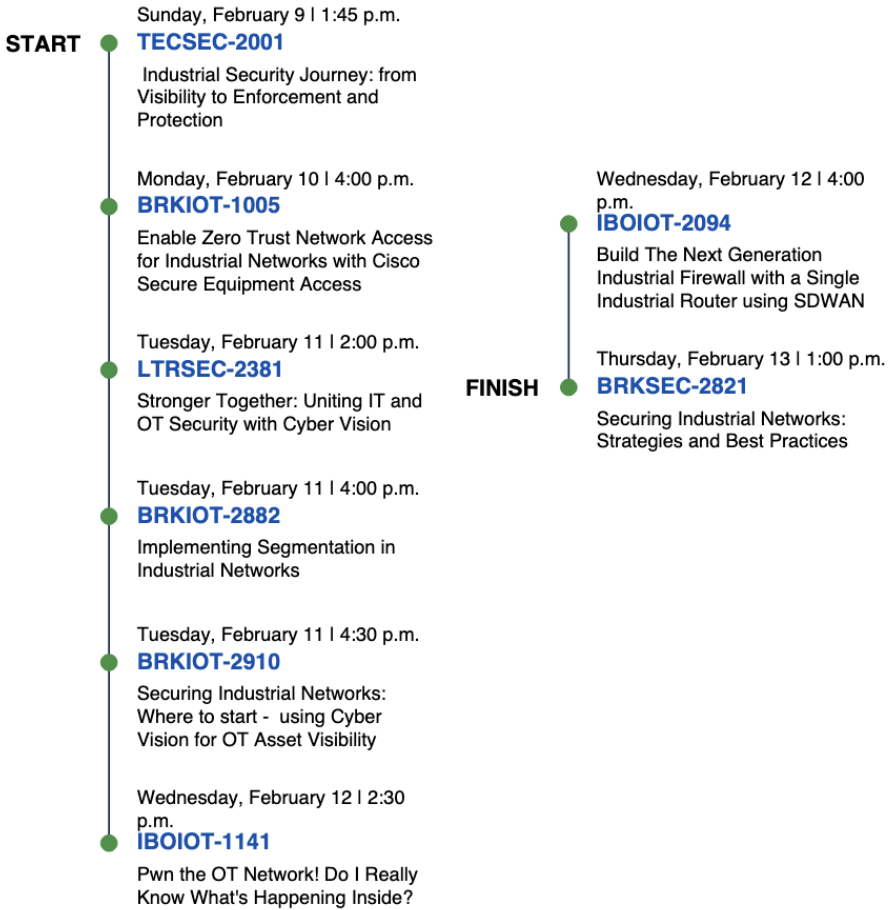
1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Internet of Things

Secure your Industrial IoT Environment

In these industrial IoT environments, the scale and associated attack surface increase exponentially. Also the extreme requirements for performance, availability and visibility raise the need to transform the way of thinking and designing these complex IoT networks, especially when agility and ease of use are a must. Secure network automation and orchestration lead the way and secure network transformation is the core platform for line of business innovation and resilience.



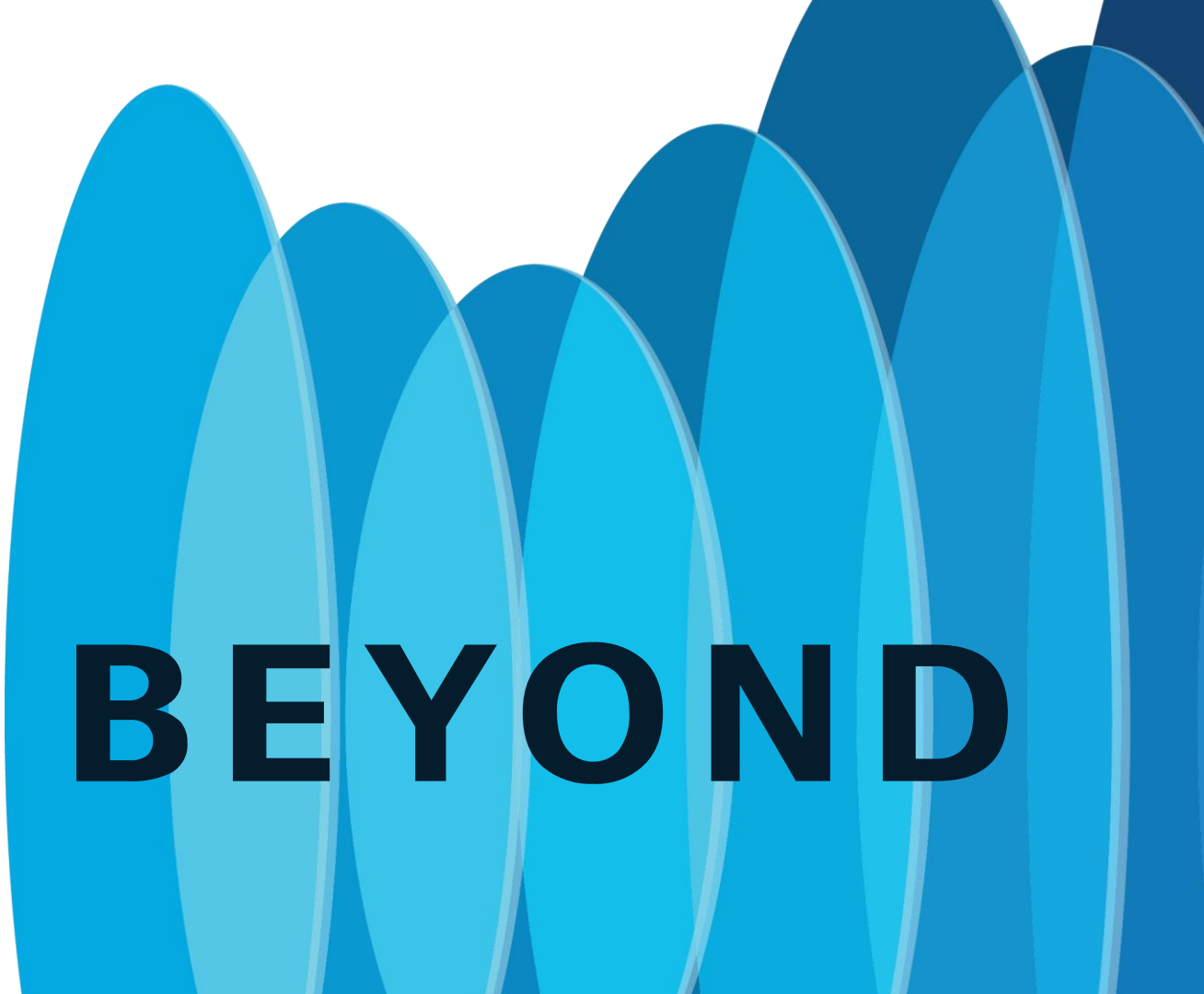
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Thank you

cisco Live!

cisco Live!



GO BEYOND