



# 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?

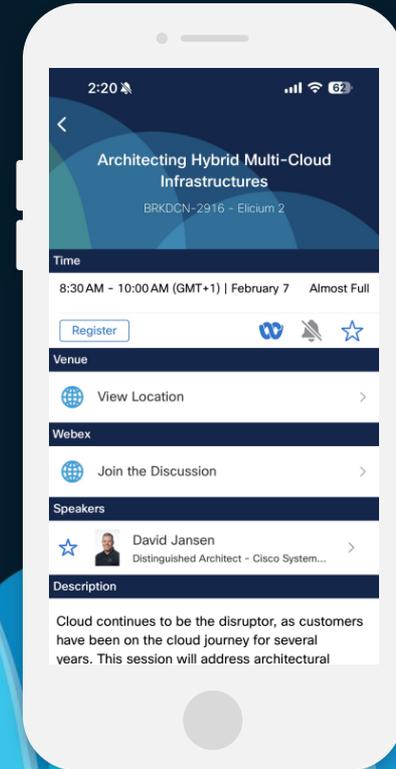
Use the Webex app to chat with the speaker after the session

## 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.

**CISCO** *Live!*



# Your presenters



**Abubakar Maaroo**  
IIoT Solutions Engineer



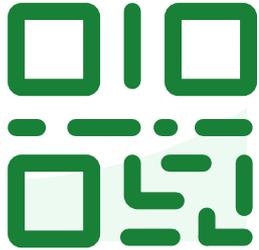
**Nicolas Deville**  
IIoT Security Product Manager

# 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](https://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

① Start presenting to display the poll results on this slide.

slido

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

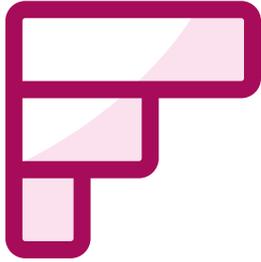


# How would you describe your current Industrial network security?

ⓘ 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?

① 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



# 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, C**

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

Jan 29, 2024

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

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

**Suzuki Motorcycle India breach forces plant shutdown**

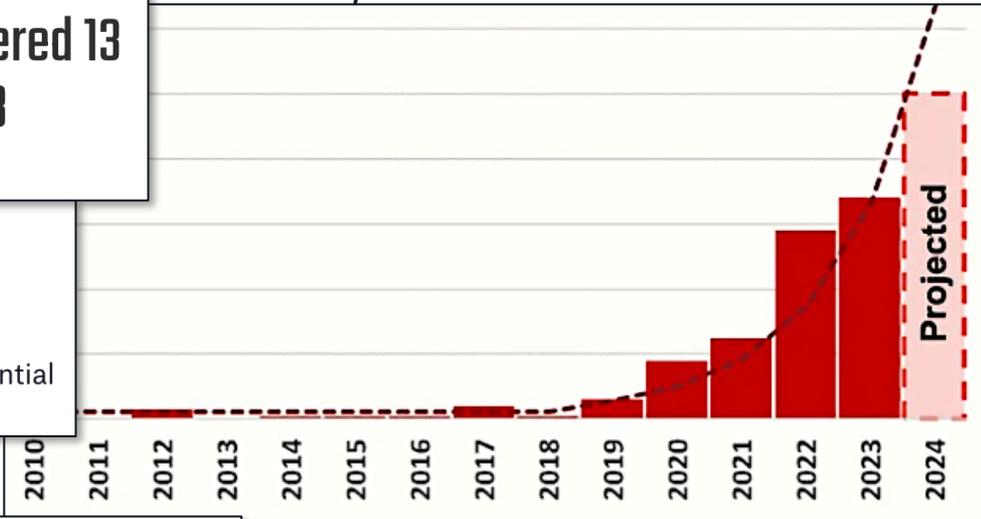
**Simpson Manufacturing Takes Systems Offline Following Cyberattack**

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

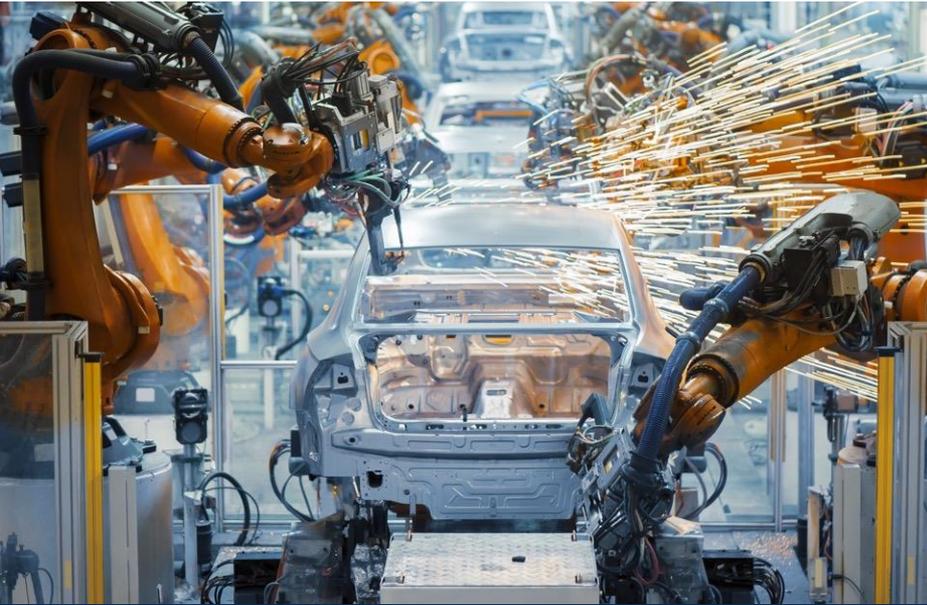
*CISCO Live!*

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

*OT Reported Incidents since 2010*



# Industry Digitization Increases the Threat Landscape



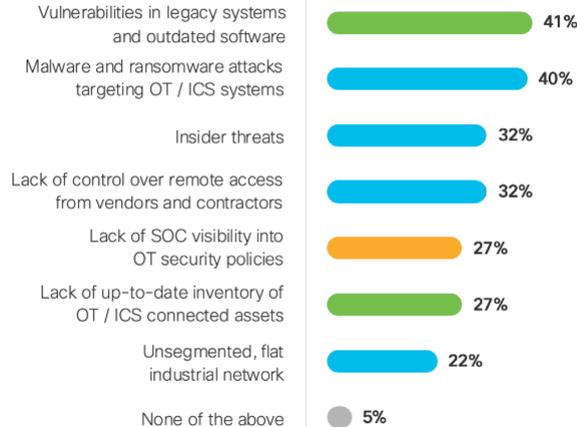
- More connected automation devices
- IoT devices accessing the cloud
- Shadow IT in industrial networks
- Remote access from third parties
- Malware intrusions
- New regulatory requirements

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

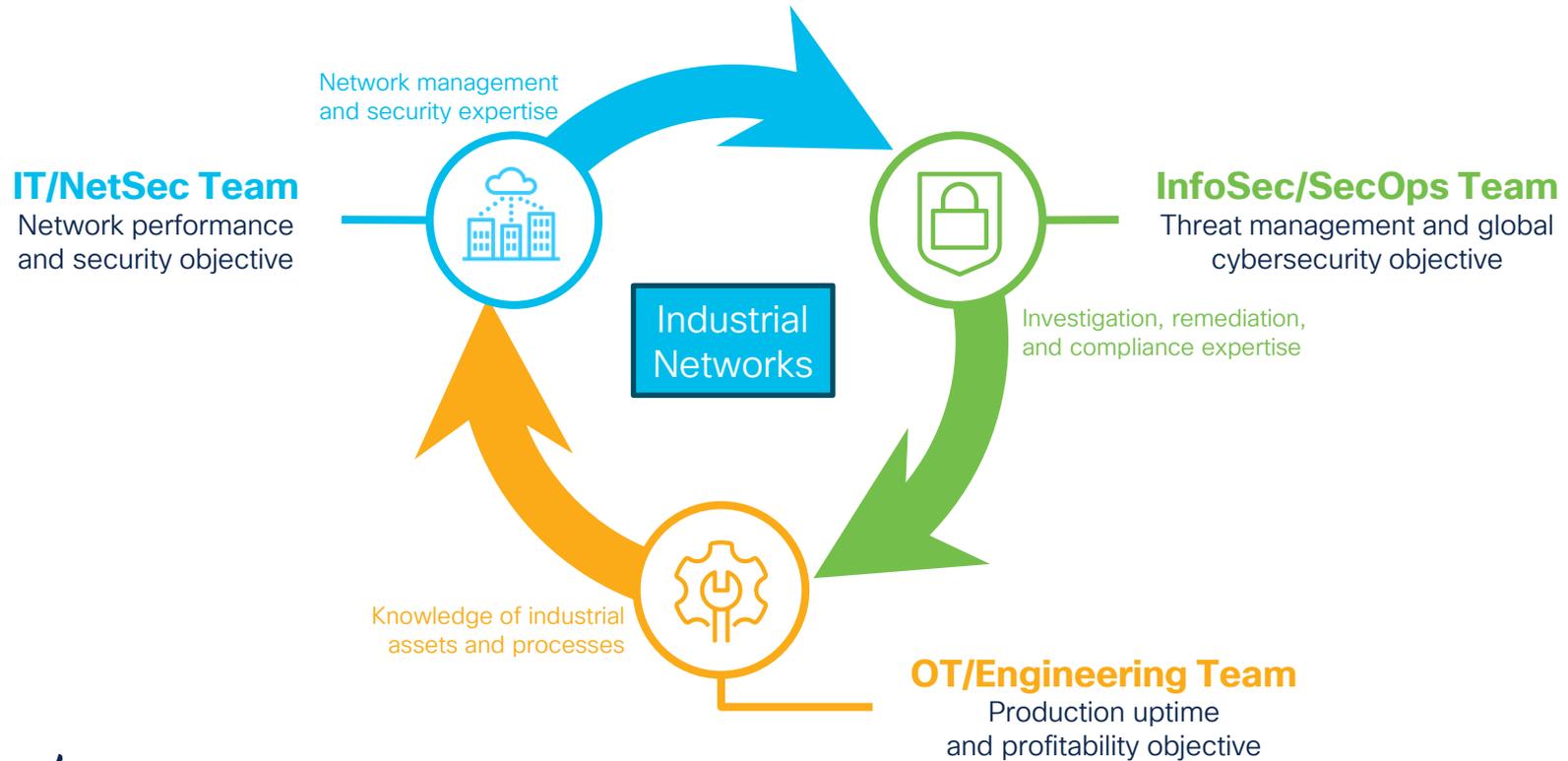
Unnecessary network communications

Decommissioned assets still connected      IPv6 traffic in IPv4 networks

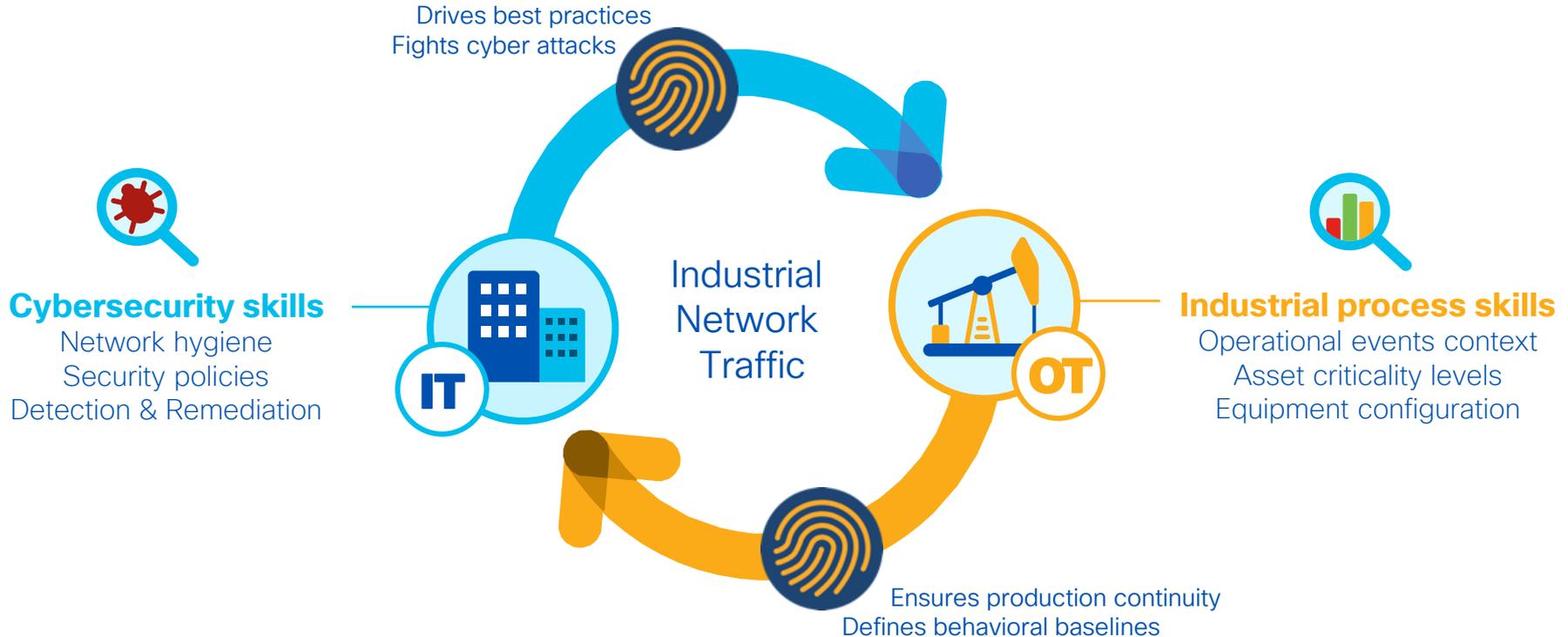
Devices in the wrong VLAN      Malware or Virus activities

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)



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

(Compliance in Law 18th October 2024)

Risk analysis and management  
Incident handling and reporting  
Crisis management  
Policies and procedures

Organizational

Cryptography  
Asset management  
Access control  
Multifactor authentication

Technical

Operational

Cybersecurity best practices  
Workforce trainings  
Vulnerability management  
Supply chain security

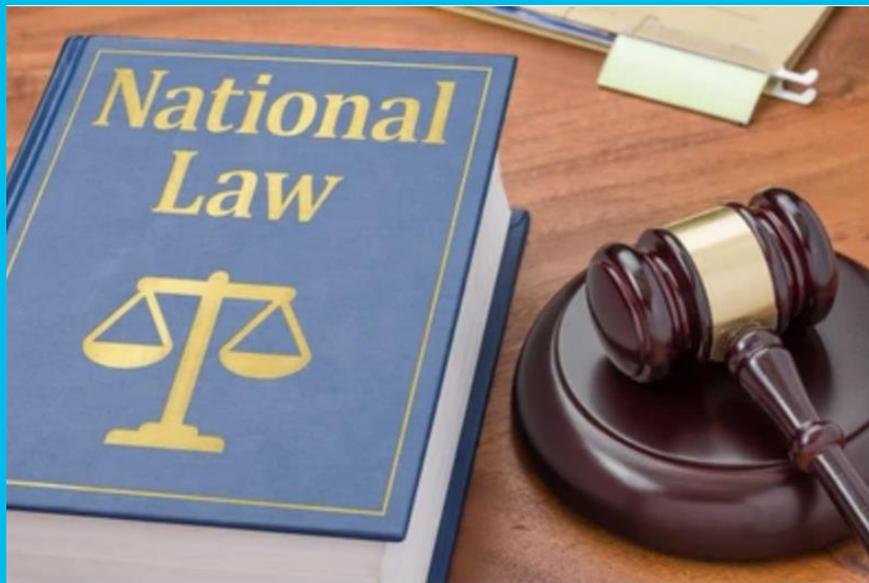
# NIS 2 impacts many more sectors than its predecessor NIS



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 18<sup>th</sup> 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	Fully Transposed	National Cyber and Info Security Agency (NÚKIB)
Denmark	Transposed Early (2023)	Danish Centre 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)

For Reference

# 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 (Limited Updates)	National Cyber Security Centre (NCSC.nl)
Poland	Transposed (Sectoral Delays)	SIPT & 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)

For Reference

# 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?

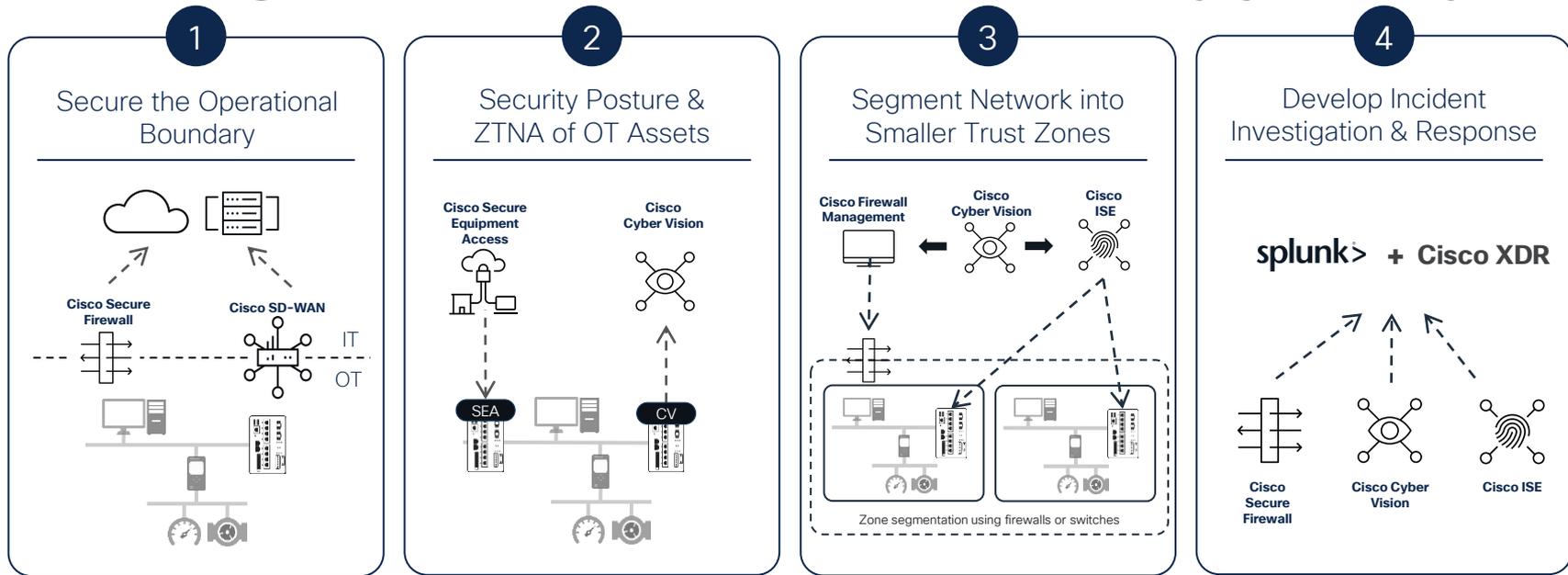
① Start presenting to display the poll results on this slide.

# The Journey to OT Security

CISCO *Live!*



# Enabling a comprehensive OT security journey



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

The screenshot displays the Cisco Cyber Vision interface. At the top, a blue banner reads "Asset Inventory". Below it, a detailed view of a component is shown: "1769-L16ER/B LOGIX5 316ER" from Rockwell Automation. It lists first and last activity dates (Apr 14, 2021 and Apr 16, 2021), IP (192.168.249.50), and MAC (f4:54:33:91:cb:ee) addresses. A "Paint\_Line\_2" tag is highlighted as "high". A summary box on the right shows 14 flows, 9 events, 10 vulnerabilities, and a credential. Below the component view, a "Properties" panel lists details like vendor-name (Rockwell Automation), fw-version (31.011), model-ref (1769-L16ER/B LOGIX5316ER), serial-number (60771949), name (1769-L16ER/B LOGIX5316ER), ip (192.168.249.50), public-ip (no), and mac (f4:54:33:91:cb:ee). To the right, a "Communication Map" shows a central "SIMATIC 300(t)" node connected to several other nodes: "STATION-WINCC", "SIEMENS IM151-3PN", "SIEMENS Siemens et R5 Bd", "SIEMENS SENTRYO-XP-1", and "Siemens 192.168.0.10". A legend indicates that red lines represent "Important" connections, green lines represent "Control system behavior", blue lines represent "IT Behavior", and black lines represent "Network analysis". Other nodes include "SENTRYO-SIMATICProfinet DCP Multicast 0.0.0" and "10.45.1.255".

# 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

The screenshot displays the Cisco Cyber Vision interface. At the top, a blue banner reads "Vulnerability Detection". Below it, a sidebar on the left shows a tree view of assets, including "192.168.1 subnet". The main panel shows "73 Vulnerabilities" with a donut chart and a list of 10 most matched vulnerabilities, such as CVE-2015-5627 and CVE-2014-0761. A "Risk Scores" banner is visible on the right. Below, a detailed view for "SC30102 Building K" shows a risk score of 69. The "Overview" section includes a bar chart comparing "Achievable risk score" (around 40) and "Current risk score" (69). The "Details" section provides a breakdown of risk by criteria, such as "Device type" (13%), "Group impact" (51%), and "Vulnerabilities" (36%).

# 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

The screenshot displays the Cisco Cyber Vision interface. At the top, a blue header reads "Control System Activities". Below it, the "Activity" page shows details for "PLC\_3 Gas Compressor" (IP: 192.168.1.1, MAC: 28:63:...) and "Dell 192.1 Maintenance" (IP: 192.168.1.1, MAC: 34:17:...). A "First activity" timestamp is shown as "Apr 6, 2017 10:59:13 PM". A "Tags" section lists "Program Upload" and "Read Var".

On the right, a "Variable / Setpoint access" window shows a "PLANT" diagram with "CELL-2" and "CELL-1". A green line connects the two cells. Below the diagram is a "Variables accesses" table:

Variable	Protocol	Details	Types	Accessed by
SYNC	enip	Endpoint	READ / WRITE	SecDemo_LinePLC   1769-L16ER/B LOGIX5316ER
SYNC_NEW1	enip	Endpoint	READ	SecDemo_LinePLC   1769-L16ER/B LOGIX5316ER

# 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

- Security analysis
  - DDOS
  - Insecure
  - Port Scan Activity
  - Snort Alert
  - Snort Browser
  - Snort Deleted
  - Snort Experimental-Dos
  - Snort Experimental-Scada
  - Snort Exploit-Kit
  - Snort File
  - Snort Malware-Backdoor
  - Snort Malware-CNC
  - Snort Malware-Other
  - Snort Misc
  - Snort OS-Other
  - Snort OS-Windows
  - Snort Server-Other
  - Snort Server-Webapp

### Malware Detection

The screenshot displays two Snort events in the Cisco Cyber Vision interface. The top event is dated 16:12:09.236 and is categorized as 'Signature based Detection' with a severity of 'veryhigh'. It reports a 'Network Trojan' detected on TCP port 27679. The event details include: Occurred at 16/06/24:44:21.861415; Sensor: SENSORVM-INT17233; Action: allow; Gid: 1; Signature ID: 27679; Priority: 1; Rule: 1:27679:4 (Revision4); Classification: A Network Trojan was detected. The bottom event is dated 10:31:27.690 and is also categorized as 'Signature based Detection' with a severity of 'high'. It reports a 'Network Trojan' detected on UDP port 44037. The event details include: Occurred at 07/06/08:31:27.685502; Sensor: FCH212V93P; Action: allow; Gid: 1; Signature ID: 44037; Priority: 1; Rule: 1:44037:4 (Revision4); Classification: A Network Trojan was detected. Both events show related data such as network interface, message, source and destination IP addresses, protocol, direction, and Ethernet type. A table at the bottom summarizes the component source and destination for the second event.

source	destination	Component source	Component destination
intel 192.168.0.12	212.166.210.80	Name: Intel 192.168.0.12 MAC: 64:80:99:d8:5d:4c IP: 192.168.0.12 Tag: HTTP Client	Name: 212.166.210.80 MAC: a4:08:f5:e1:03:ec IP: 212.166.210.80 Tags: DNS Server, Public IP

# 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.

Preset/Baseline

Description:  
All devices and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline

Criteria Select all Reject all Default

Search criteria

- RISK SCORE
- NETWORKS
- DEVICE TAGS
- ACTIVITY TAGS
- GROUPS
- SENSORS

You are about to create a baseline from the preset All data with active data between Jan 10, 2025 3:18:02 PM and Feb 9, 2025 3:18:02 PM (30d of data). This represents:

Devices 66 (+ 25 other components) 155  
 Activities 155  
 Variables 1257  
 Groups 0

## Reporting

Executive Summary

Filter Criteria: All data Present

Introduction  
This report is available in PDF format.

Risk Profile

Inventory Distribution Summary

Top 5 Vendors by Device Count

Vendor	Count
HP	100
HP-PRINTER	80
HP-PC	20
HP-SCANNER	10
HP-TELEPHONE	5

Top 5 Protocols by Device Count

Protocol	Count
TCP	100
HTTP	80
HTTPS	60
SSH	40
SMTP	20

Total number of vendors seen: 32  
Total number of protocols seen: 38

Top 10 Device Types by Device Count

Device Type	Count
HP-PC	100
HP-PRINTER	80
HP-SCANNER	20
HP-TELEPHONE	10
HP-PC-DESKTOP	5
HP-PC-LAPTOP	5
HP-PC-SERVER	5
HP-PC-SMARTPHONE	5
HP-PC-TABLET	5
HP-PC-WEARABLE	5

Total number of device types seen: 17



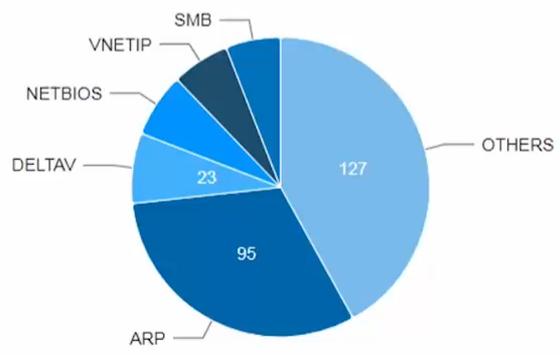
# Welcome to Cisco Cyber Vision

Last 30 days overview

Operational overview Security overview

All  Protocol distribution  Most critical events  Presets highlight

## Protocol distribution

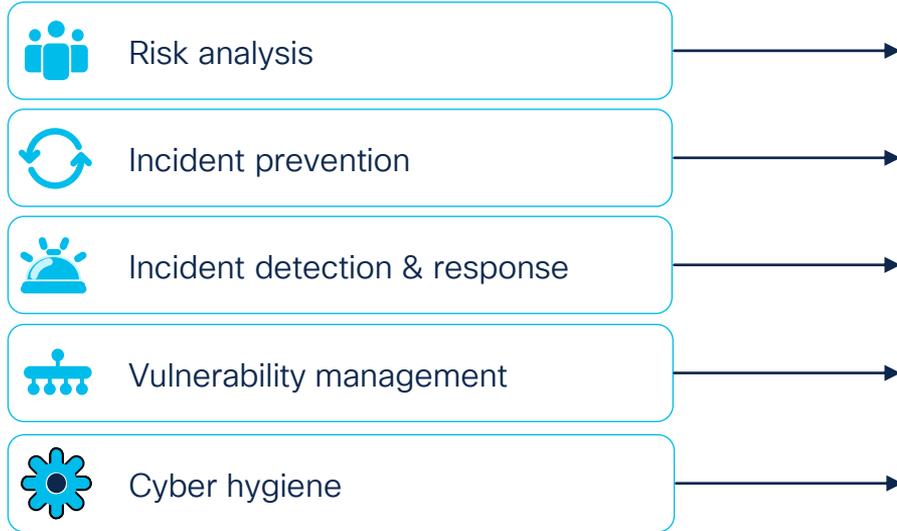


## Most critical events

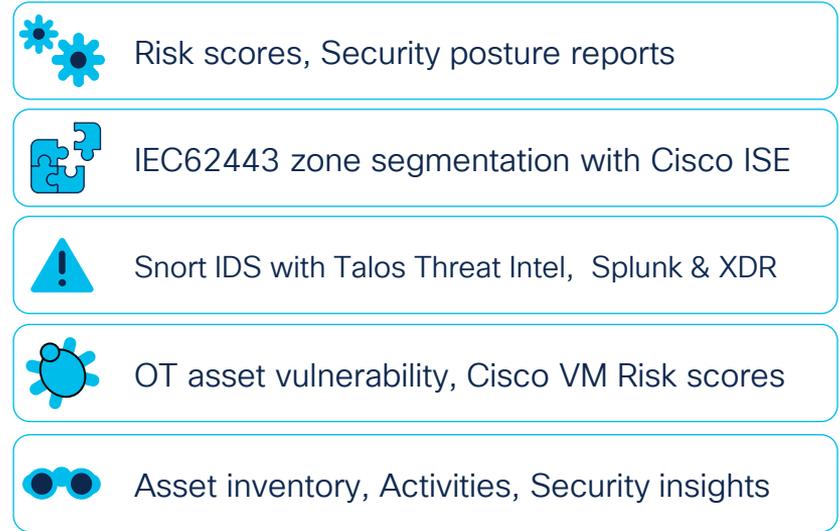
- Feb 10, 2025 1:00:05 AM **Critical** Sensor 8a29b7ca-fdf3-4e2f-999f-524632f...
- Feb 10, 2025 1:00:05 AM **Critical** Sensor 8e2fb2fe-c4dd-46a6-8e01-27907dc...
- Feb 10, 2025 1:00:05 AM **Critical** Sensor 4a7bf983-8b3c-435a-92e6-101363...
- Feb 10, 2025 1:00:05 AM **Critical** System has been updated | 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...

# How Cyber Vision helps with NIS2 compliance

## Required NIS2 Measures



## Cyber Vision Capabilities



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

# Cisco Cyber Vision portfolio

Center

### Hardware Appliance

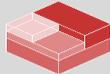
UCS based servers with Hardware RAID



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

### Software Appliance

Virtual Machines



VMWare ESXi OVA



HyperV VHD

**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

**Sensor**

Catalyst IE3300 and IE3400 Switches

**Sensor**

Catalyst IE3400HD 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

### Network-Sensors

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

**Sensor IDS**

x86 or ARM64 Compute

### Docker Sensor

**Sensor IDS**

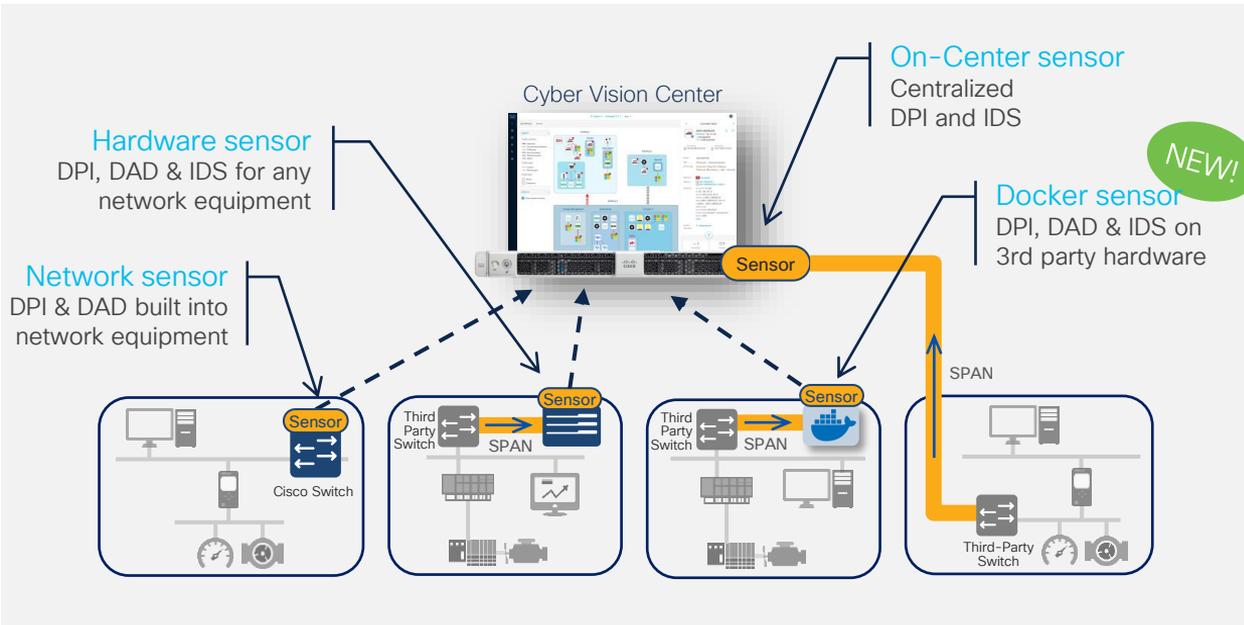
IC3000 Industrial Compute

### Hardware-Sensor

DPI and active discovery via SPAN to support brownfield



# Easy to deploy in Brownfield and Greenfield environments



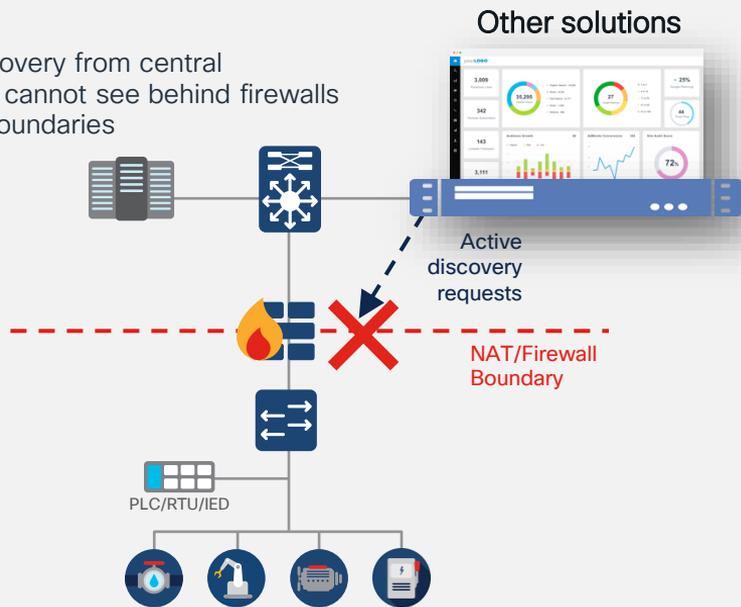
- **Network-sensors** embedded in Cisco networking for simple and highly scalable deployments
- **Hardware or Virtual sensors** capturing traffic on any switch with a single hop SPAN to support brownfield deployments
- **On-Center sensor** to leverage existing SPAN infrastructures, or collect traffic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

Cyber Vision offers flexible deployment options to best fit your constraints

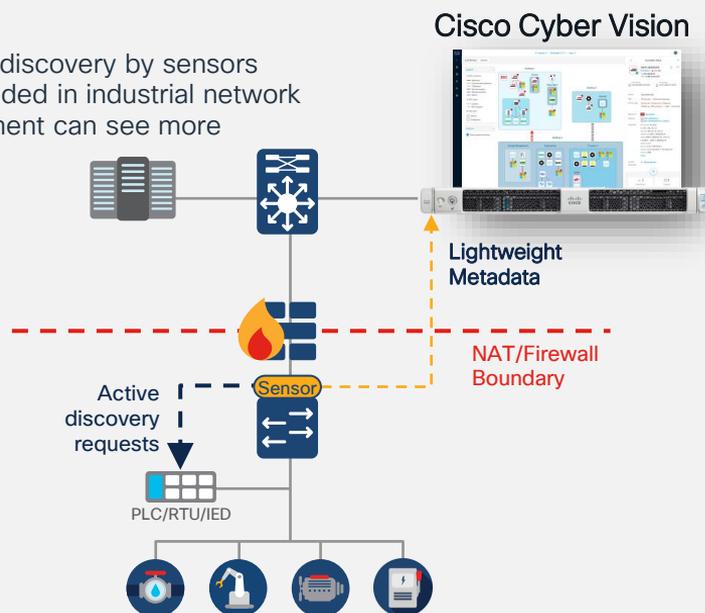
# Why is a network-sensor important?

## Sensors embedded in the network can see more

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

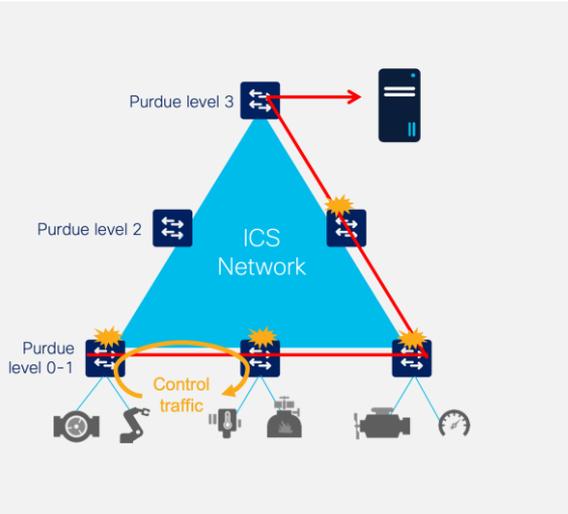


Active discovery by sensors embedded in industrial network equipment can see more

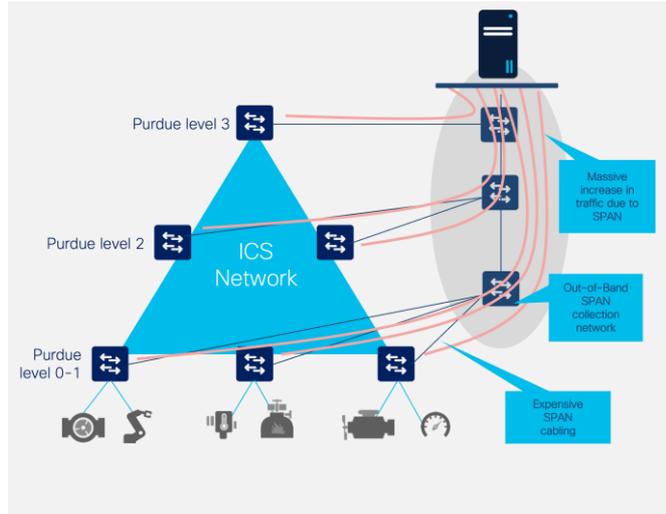


Active discovery requests are not blocked by NAT and firewall boundaries

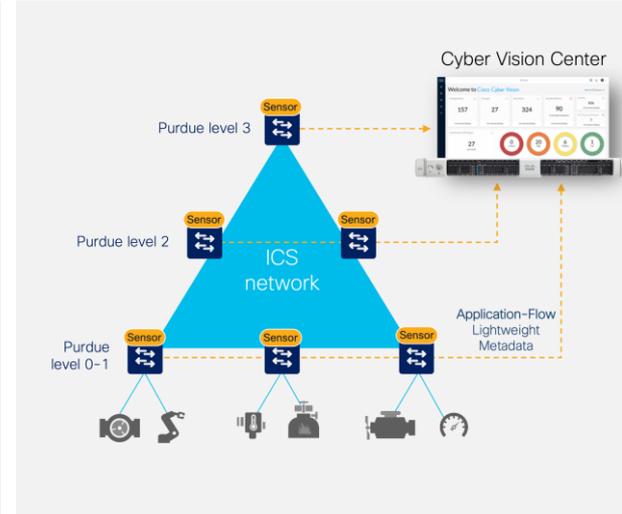
# Leverage the network as a sensor to lower cost and complexity



RSPAN introduces Jitter



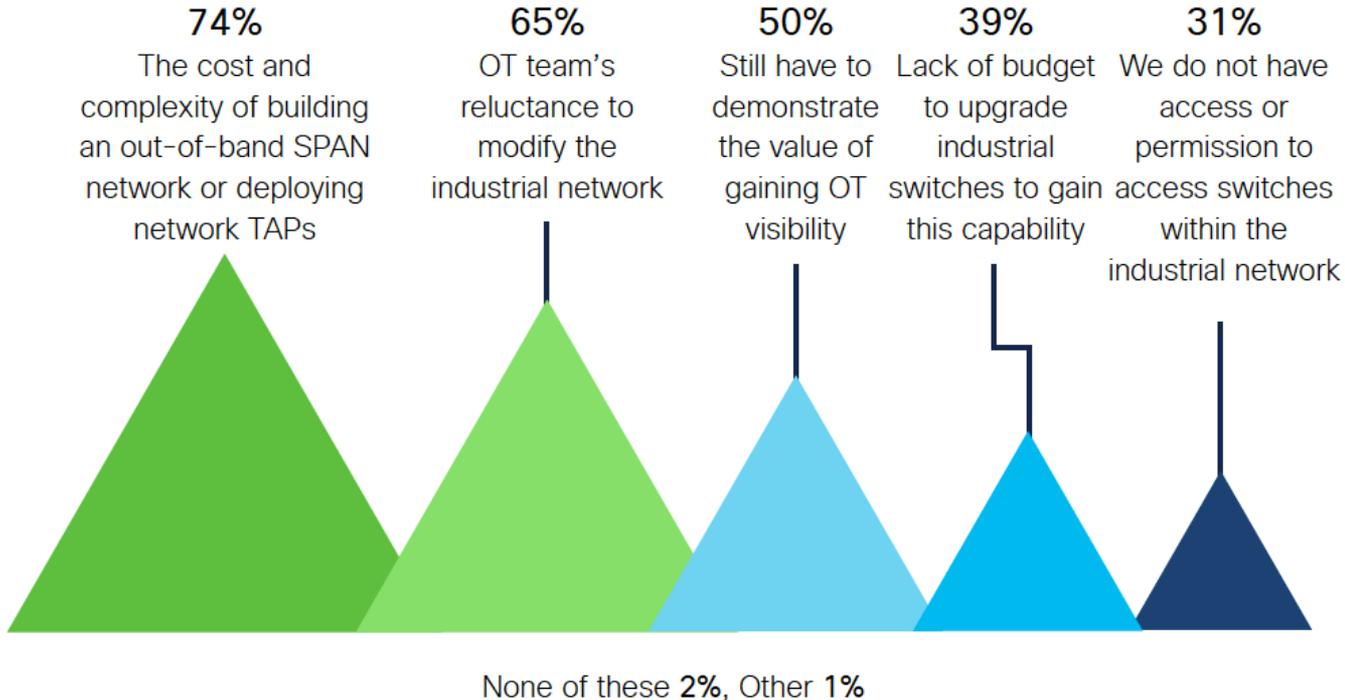
Out-of-Band SPAN is expensive



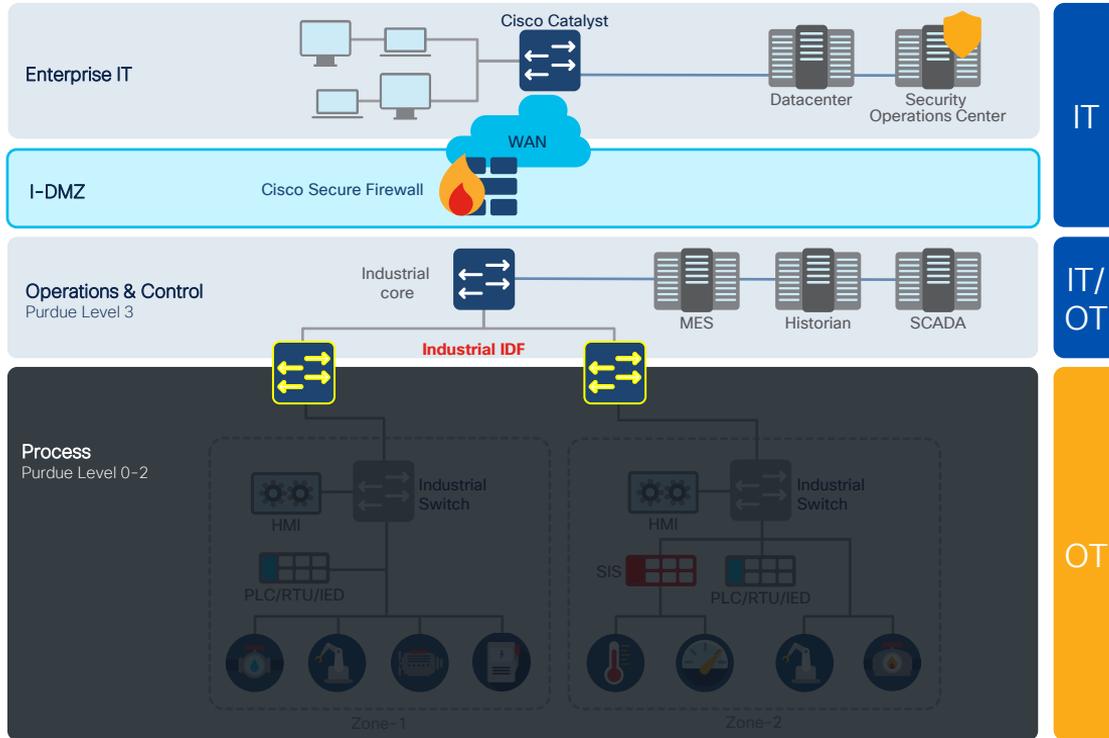
Network sensors scale without SPAN

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

# What do you see as the main obstacles?

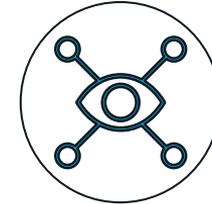
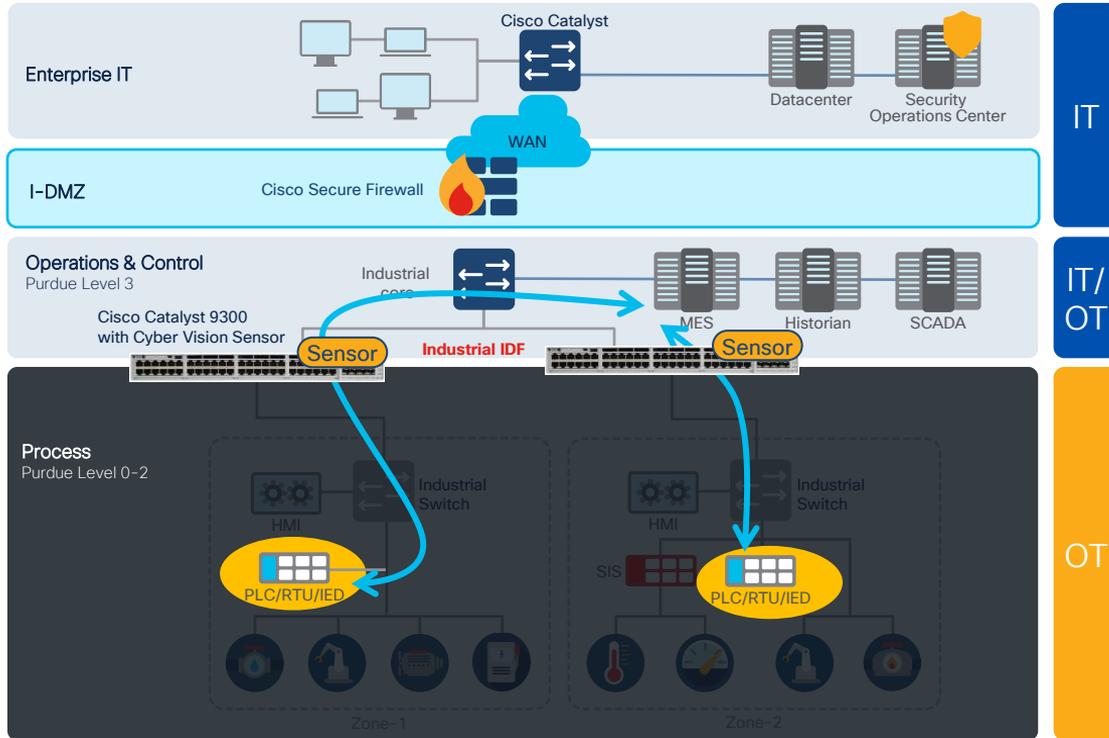


# IT has no visibility below the Industrial IDF



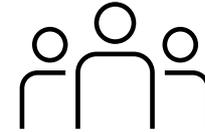
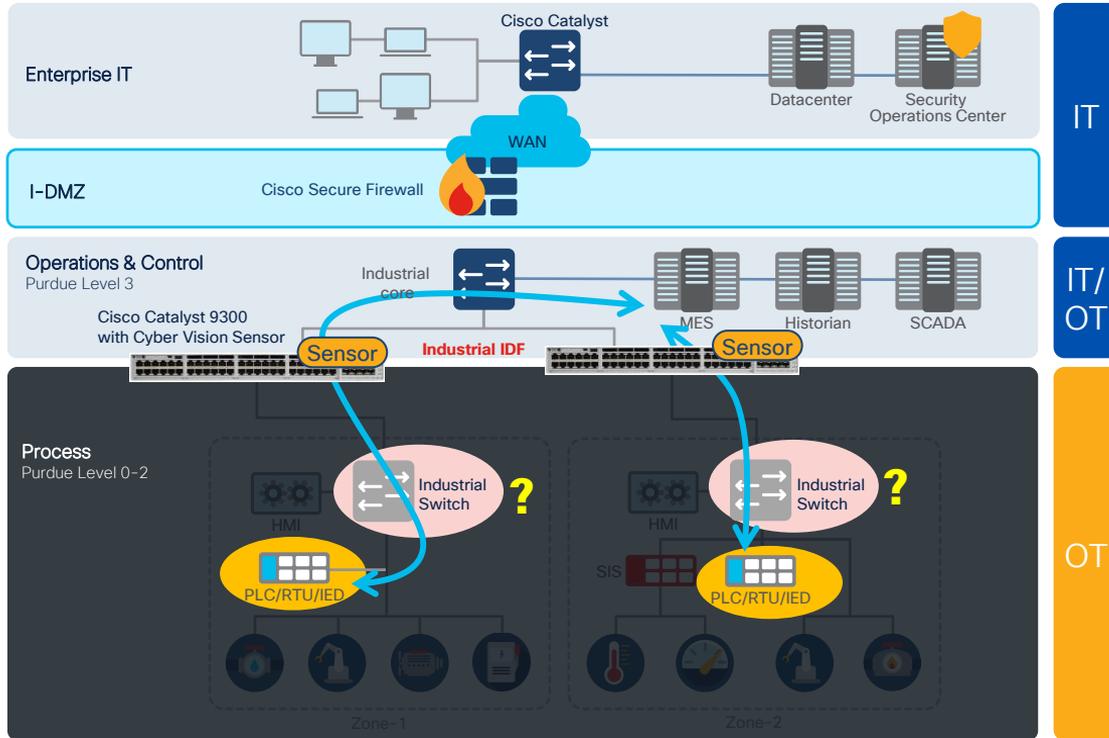
How can IT leverage network equipment it owns to gain visibility into OT?

# Your Catalyst switches let you turn on the lights



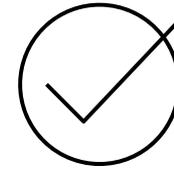
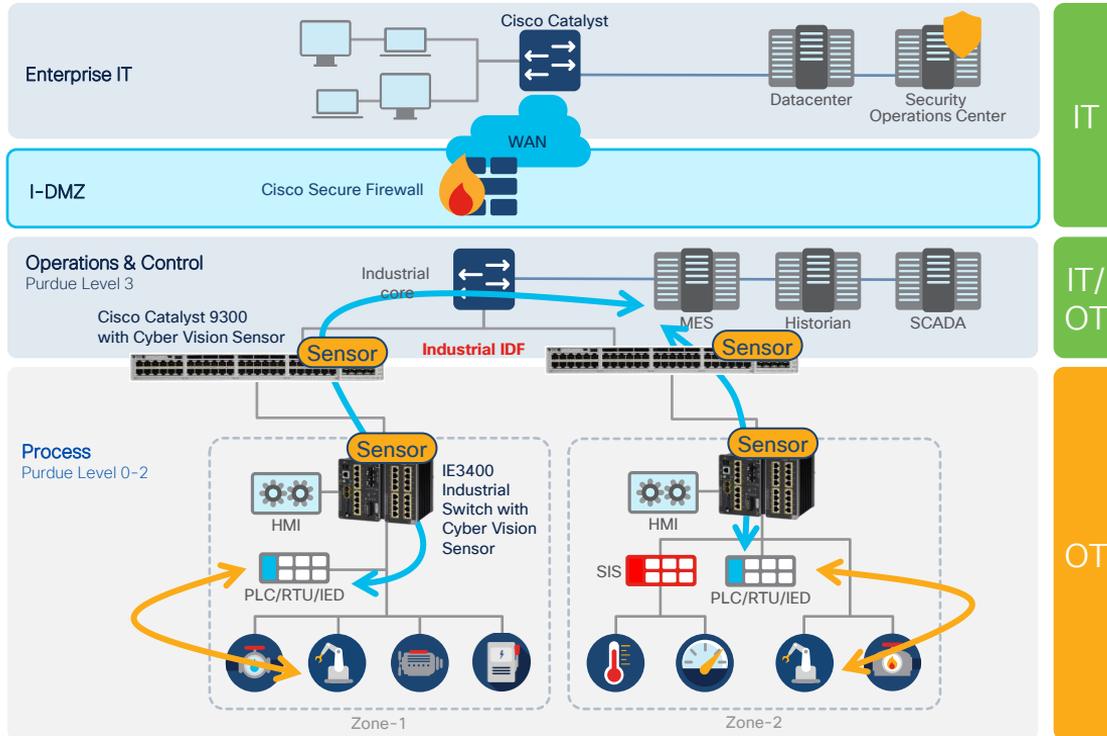
**Step-1:** Cyber Vision Sensor on Catalyst 9300 gives you visibility to North-South communications to identify key assets

# 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

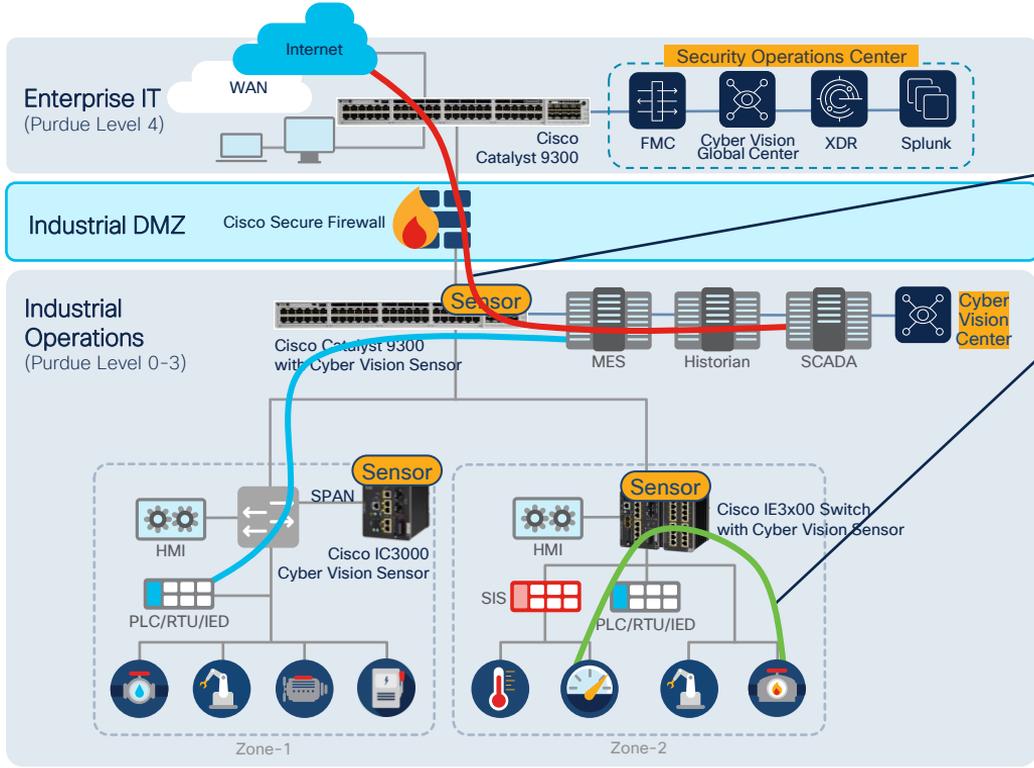


**Step-3:** Replace critical switches with Cisco IE Switch running Cyber Vision sensor to see the entire OT network

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?

IT  
IT/OT  
OT



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

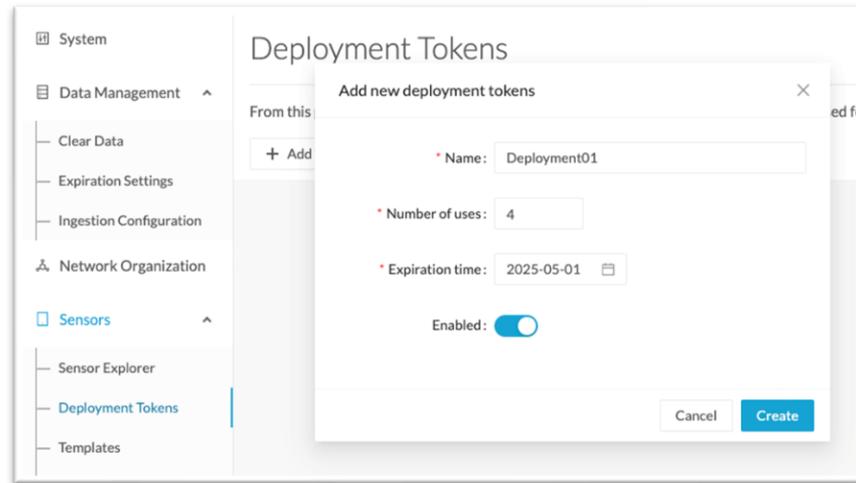
## Scalability

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

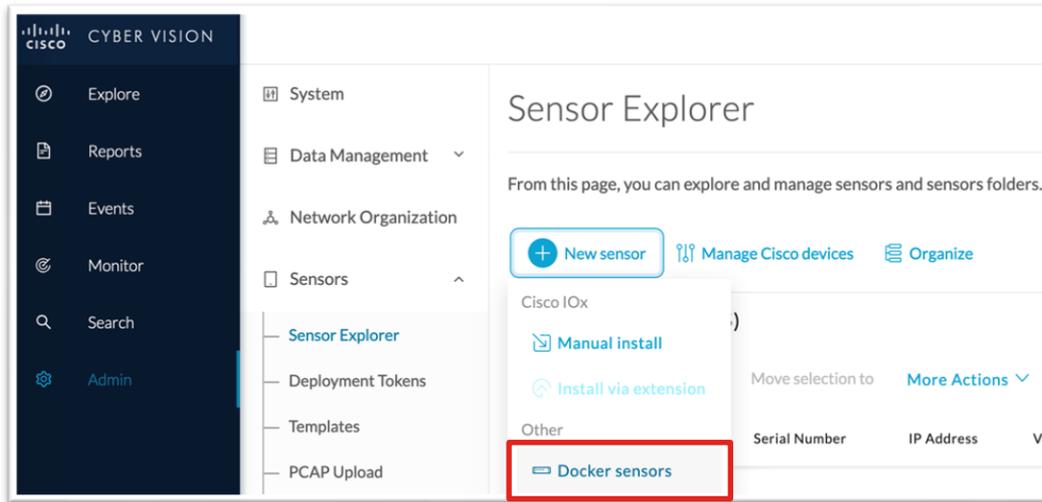
# Docker sensor deployment steps



# Docker sensor deployment steps



# Docker sensor deployment steps



# Docker sensor deployment steps



Sensor Application

Sensor Application

Name\*  
MySensor

Deployment Token\*  
MyToken (0/100) [Create deployment token](#)

Sensor Mode\*  
Passive and Active Discovery

- Passive only
- Active Discovery only
- Passive and Active Discovery

Container(s) will reach the center using NAT

Center is behind NAT

# Docker sensor deployment steps



Capture Configuration

Each capture interface will consume a deployment token

Mirrored traffic type\*  
SPAN

Capture Interface\*  
enp7s0  
e.g. eth2

Capture Mode\*  
All: analyze all the flows

Save Interface

2 Saved Capture interfaces:

ERSPAN2 - enp6s0

Mirrored traffic type\*  
ERSPAN2

Capture Interface\*  
enp6s0  
e.g. eth2

CIDR\*  
192.168.40.22/24  
e.g. 192.168.1.1/24

VLAN  
40  
1-4095

Capture Mode\*  
All: analyze all the flows

SPAN - enp7s0

Mirrored traffic type\*  
SPAN

Capture Interface\*  
enp7s0  
e.g. eth2

Capture Mode\*  
All: analyze all the flows

Back Continue with 2 Interfaces

Capture interface configuration

Active Discovery

Common configuration:

Active Discovery Interface\*  
enp8s0  
e.g. eth2

Target interface:

CIDR\*  
192.168.66.12/24  
e.g. 192.168.1.1/24

VLAN  
66  
1-4095

CIDR\*  
192.168.69.12/24  
e.g. 192.168.1.1/24

VLAN  
69  
1-4095

Back Continue with 2 Target Interfaces

Active Discovery configuration



# Docker sensor deployment steps

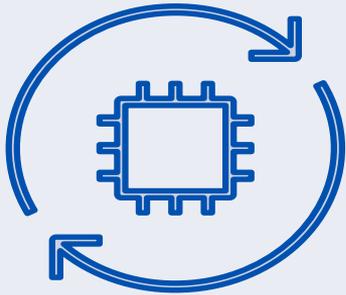


Task	Command	Result
Interactive sensor creation	<code>docker compose up</code>	System will display stderr/stdout of the instance. End with Ctrl+C
Start and run sensor independently	<code>docker compose up -d</code>	System will start the docker container instances to the background and leave them running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

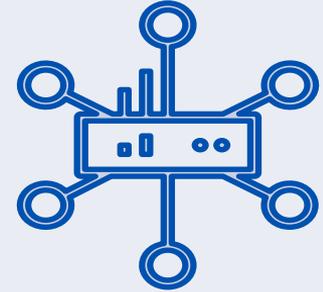
# Other sensor enhancements



Sensor app in-place  
update



Support of Cat9300  
without SSD



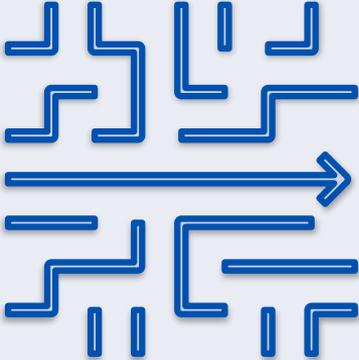
Catalyst SD-WAN  
Manager support

# Cyber Vision New UI/UX (preview)

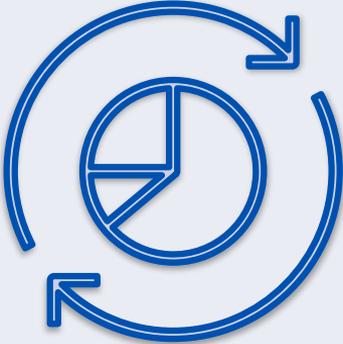
CISCO *Live!*



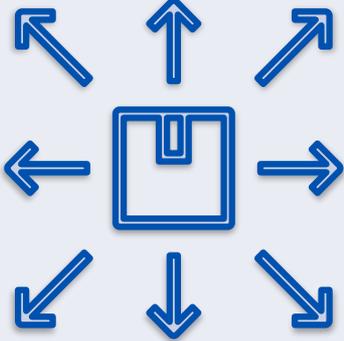
# Goal of this new UI



Simplified User Experience (aligned with other Cisco products)



Reduced time-to-value



Enhanced scalability

- 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 ①

[View all 92 assets](#)

8 With Active Alerts  11 Vulnerable  +51 Last 7 Days +92 Last 30 Days

## Vulnerabilities ①

[View all 55 vulnerabilities](#)

9 Critical  28 High  18 Medium  0 Low 

### Highlighted Vulnerabilities

① Sort By: CVSS Score

CVSS Score	Vulnerability
10 Critical	<a href="#">CVE-2023-20198: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability</a> Affected Assets 5
9.8 Critical	<a href="#">CVE-2019-12260: VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion c...</a> Affected Assets 1
9.8	<a href="#">CVE-2019-12256: VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Stack Overflow in parsing of IPv4 pack...</a>

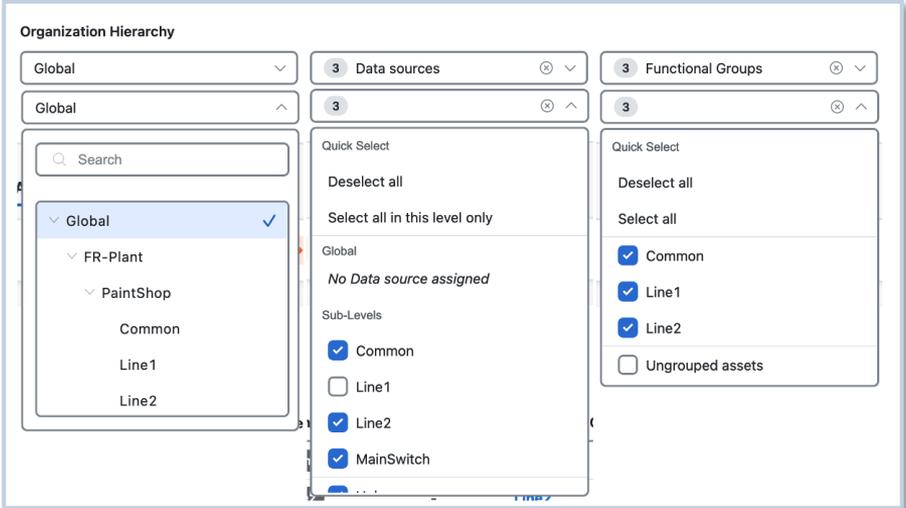
# New Beta UI Preview – Viewing Data

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

1 selected **Assign Selected to Organization Hierarchy** 

<input checked="" type="checkbox"/> Network Device Name	Health Status	Processing Status	Organization Hierarchy <sup>①</sup>	Action
<input type="checkbox"/> Line2	Connected	Normally processing	../PaintShop/Line2	<a href="#">Assign</a>
<input checked="" type="checkbox"/> Line1	Connected	Normally processing	../PaintShop/Line1	<a href="#">Assign</a>



Organization Hierarchy

Global   3 Data sources  3 Functional Groups  3

Global   3  3

Quick Select

Deselect all

Select all in this level only

Global

No Data source assigned

Sub-Levels

Common

Line1

Line2

MainSwitch

Quick Select

Deselect all

Select all

Common

Line1

Line2

Ungrouped assets

# New Beta UI Preview – Assets

← Asset Visibility

## COMMON

Summary Vulnerabilities 18 Communications Properties Interfaces

Type  
PLC

Vendor  
**Rockwell Automation**

Sensor  
**Common**

Family  
**1756**

Firmware Version  
**11.3**

Model  
**1756-EN2TR/C**

Rack Number  
**Port1-Link01**

Reference  
**1756-EN2TR/C**

Serial Number  
**0125fed1**

**Primary Interface**

IP Address  
**192.168.41.21**

**Top 5 Vulnerabilities** View All ^

Name	CVSS Score
Insufficiently protected credentials in Logix controllers	9.8 Critical
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Han...	9.8 Critical
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP ...	9.8 Critical
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP ...	9.8 Critical
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Stac...	9.8 Critical

← Asset Visibility

## COMMON

Summary Vulnerabilities 18 Communications **Properties** Interfaces

[Export](#)

Search

**ENIP** 10 ^

enip-status-ra-major	REM	enip-cpuname	COMMON
enip-status-ra-minor	RUN	enip-version	11.3, 33.12
enip-serial	0125fed1, 01280d79	enip-location	Port1-Link01, Port1-Link00
enip-vendor	Rockwell Automation/Allen-Bradley	enip-name	1756-EN2TR/C, 1756-L81E/B
enip-devicetype	CommunicationsAdapter, ProgrammableLogicController	enip-status	AtLeastOneIOConnectionInRunMode, AtLeastOneIOConnectionInRunMode,ReservedBits12-15:0x3

**VLAN** 1 ^

vlan-id	43, 90, 41
---------	------------

← Asset Visibility

## COMMON

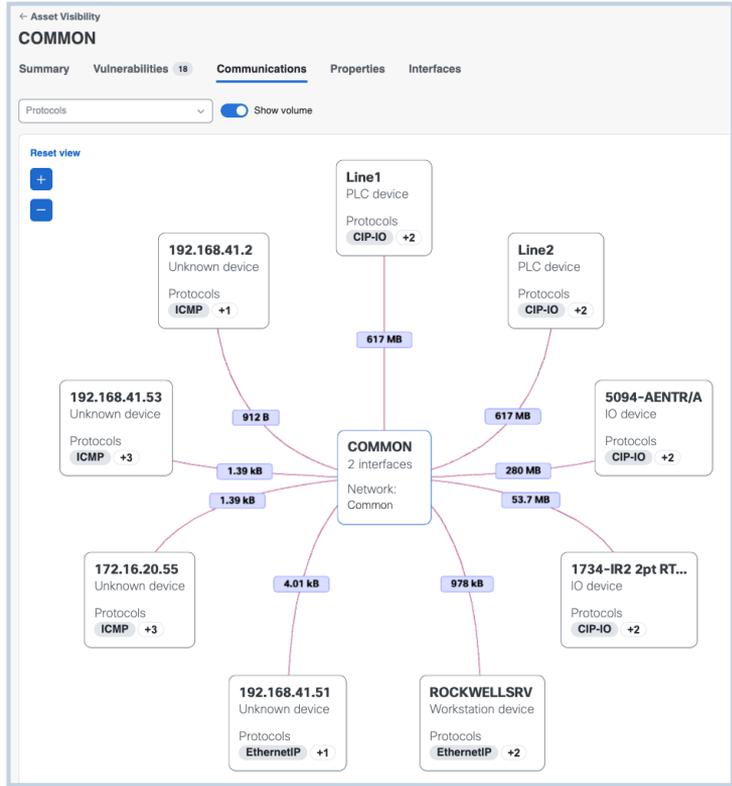
Summary Vulnerabilities 18 Communications Properties **Interfaces**

IP	MAC	VLAN	Network Name	Primary Interface
192.168.41.21	08:61:95:d2:11:38	41	PAINTSHOP-PLC-SCA...	<input checked="" type="radio"/>
172.16.1.1	5c:88:16:f6:b0:92	90	Common	<input type="radio"/>

2 Records Show Records: 50 1 - 2 < 1 >

BRKIOT-2910

# New Beta UI Preview – Asset Communications



COMMON ↔ Line1

Line1's Details

Communications 4

Volume	Packets	Protocols	First Seen	Last Seen
617 MB	1186824	CIP-IO +2	Oct 8, 2024 4:28 PM	Oct 8, 2024 5:28 PM

Protocol	Port	COMMON	Line1	Volume	Fi
CIP-IO	-	192.168.41.21:2222	192.168.41.22:2222	617 MB	Ok
TCP	-	192.168.41.21:57410	192.168.41.22:44818	70.9 kB	Ok
TCP	-	192.168.41.21:44818	192.168.41.22:64018	70.8 kB	Ok
ARP	-	192.168.41.21	192.168.41.22	2.32 kB	Ok

4 Records Show Records: 50 1 - 4

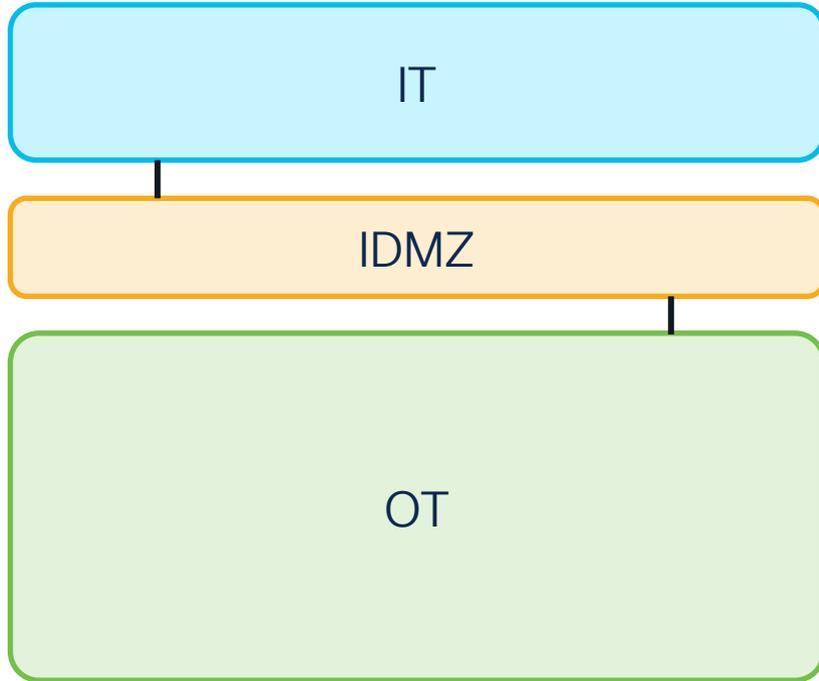
Line1's Details

Type	Family	Primary Interface
PLC	5069 Compact I/O	IP Address
Sensor	Firmware Version	172.16.10.1
-	33.12	VLAN
	Model	91
	5069-L310ER/A	Network
	Back Number	Line1

# Network Segmentation: ISE & Firewall

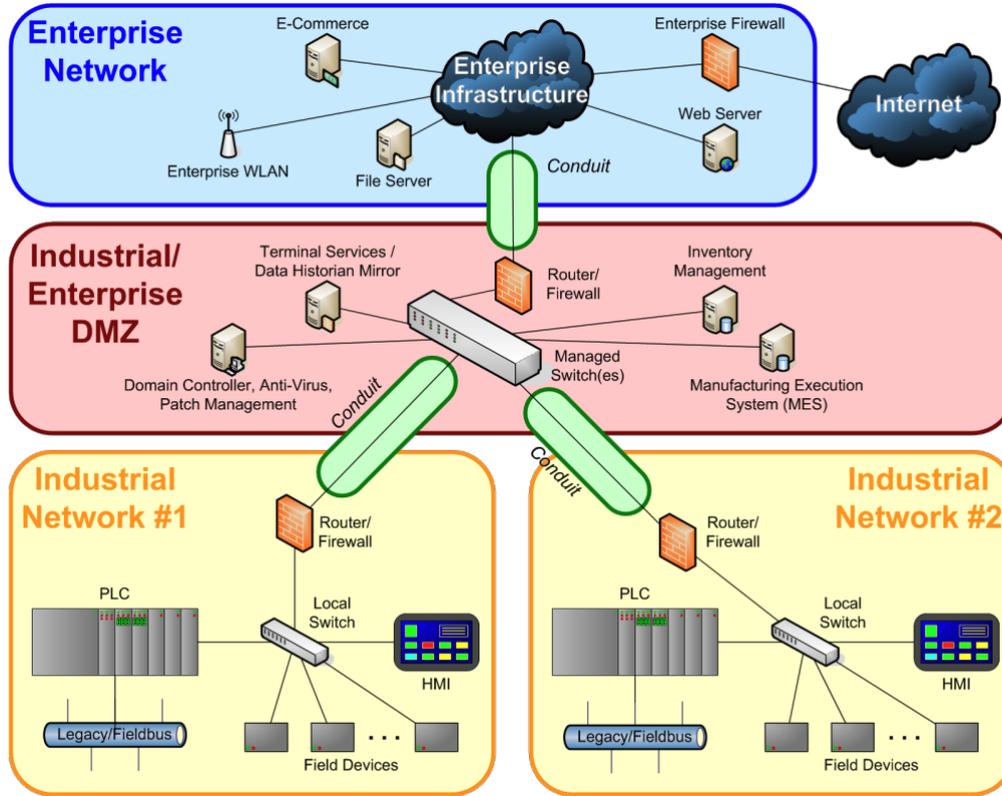


# The Purdue Model



- 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)

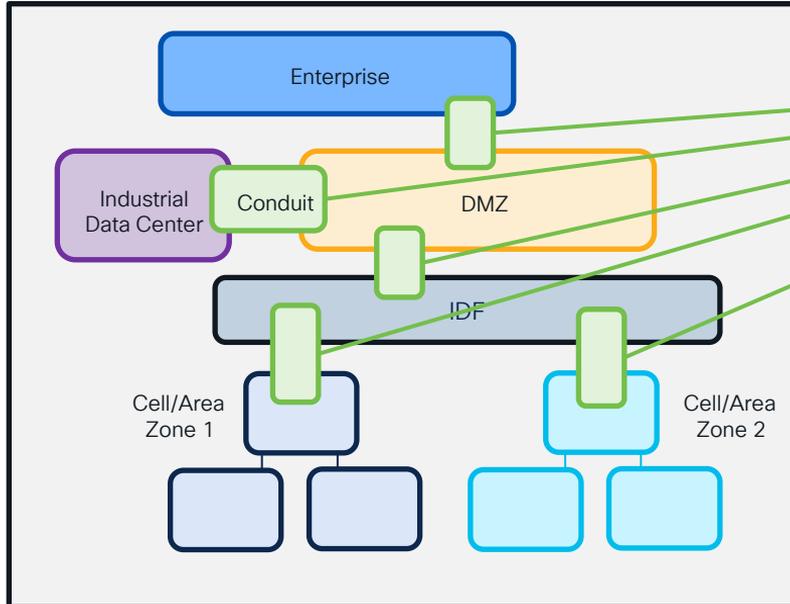
# IEC 62443 Zones & Conduits



- **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

ISA/IEC 62443



## Virtual Segmentation

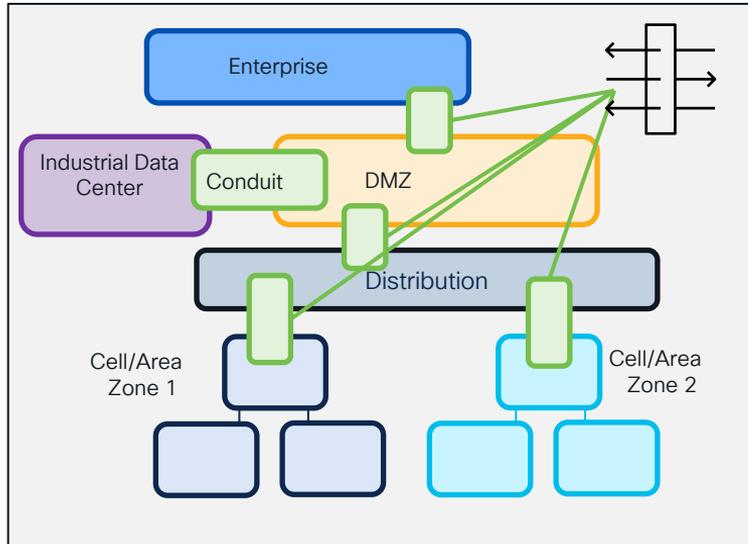
Visualizing the zones and conduits model and reacting to data observed between zones

# The Segmentation Journey – Macro and Micro

## Macro Segmentation

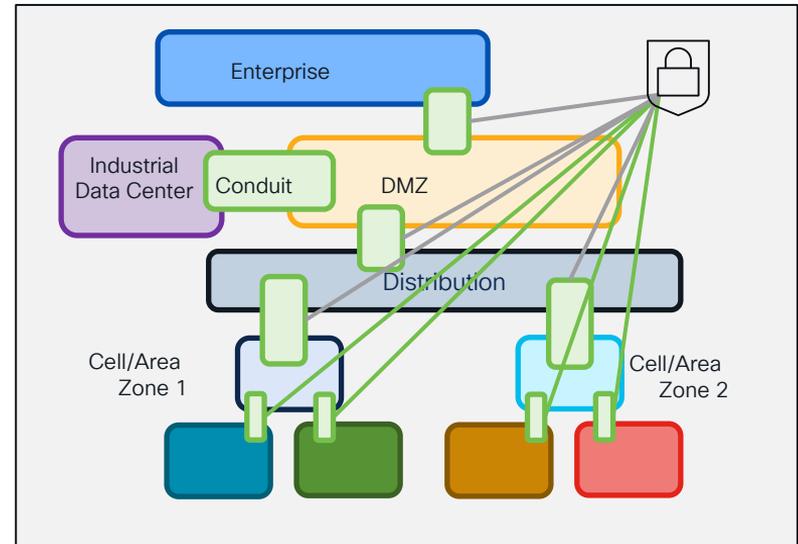
- Policy across “large” zones (between Cell/Area Zones / Production Lines)
- Distribution is typically point of VLAN termination
- Generally done at Firewall level

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

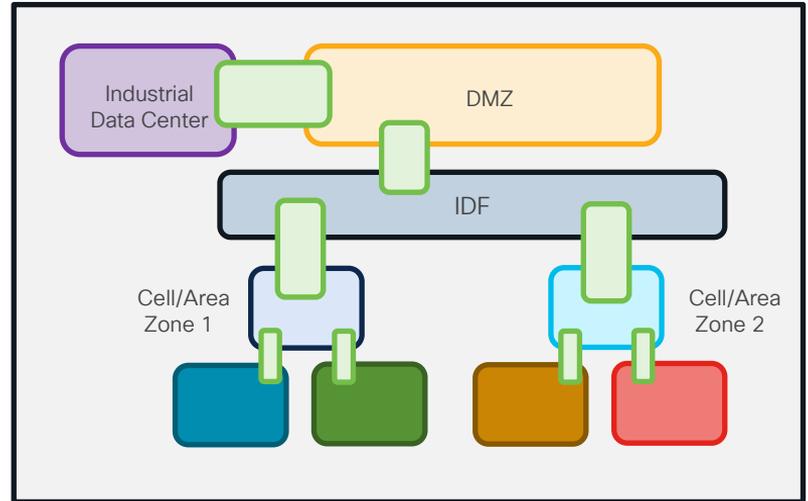
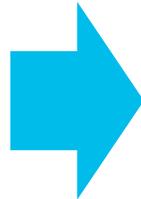
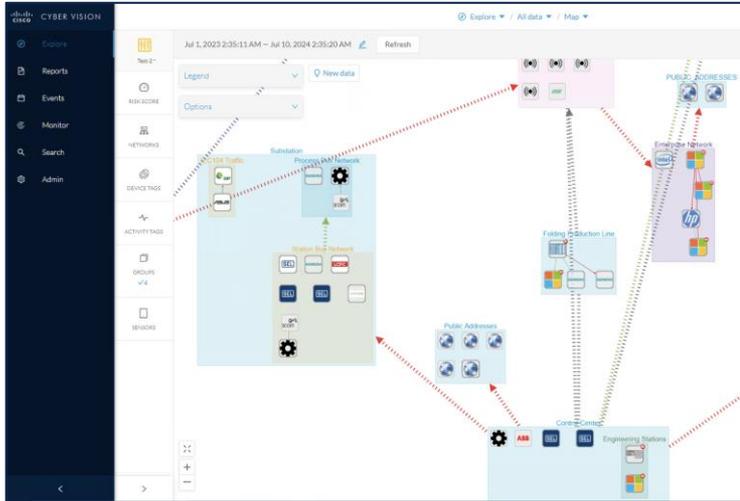
Activity Tags

Network Flows

Risk Score

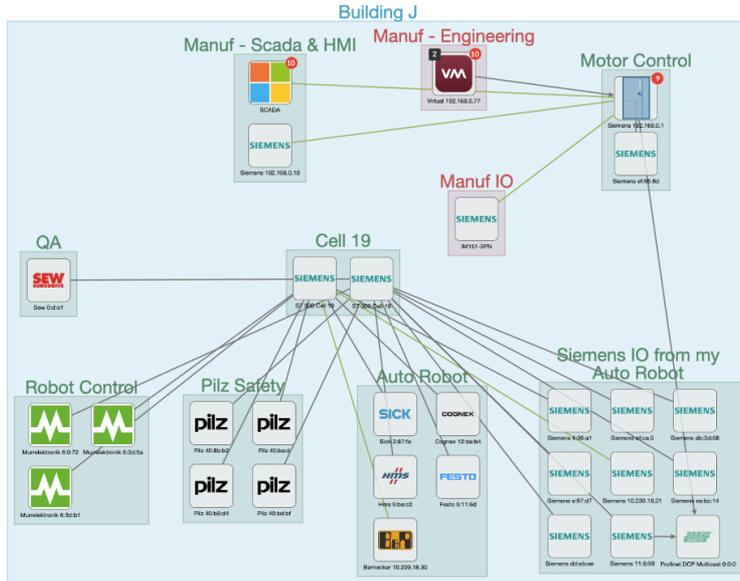


I can group assets into zones that match my industrial process.



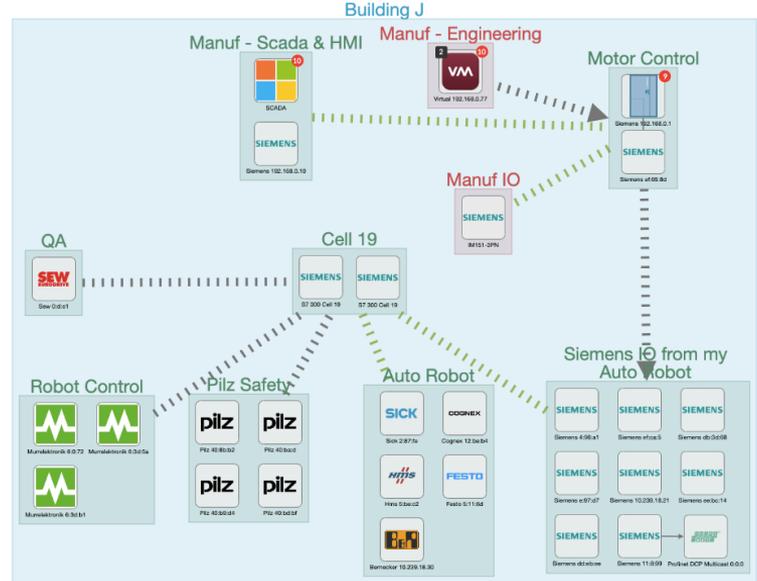
# Aggregated activities match IEC62443 conduits

## Unaggregated



[View all asset relationships](#)

## Aggregated



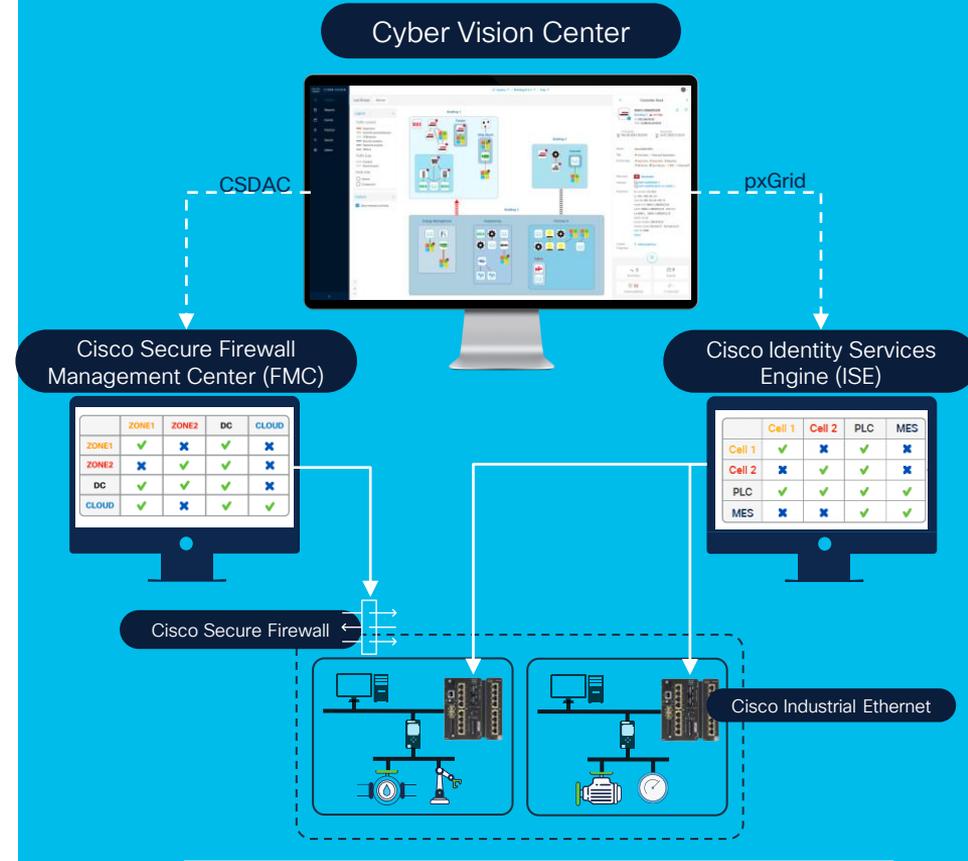
[Easily browse through conduits](#)

# 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

**CISCO** *Live!*



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

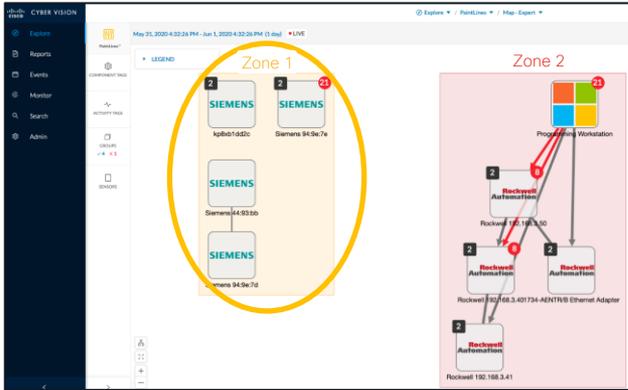
# Automated Segmentation Informed by Visibility



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



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



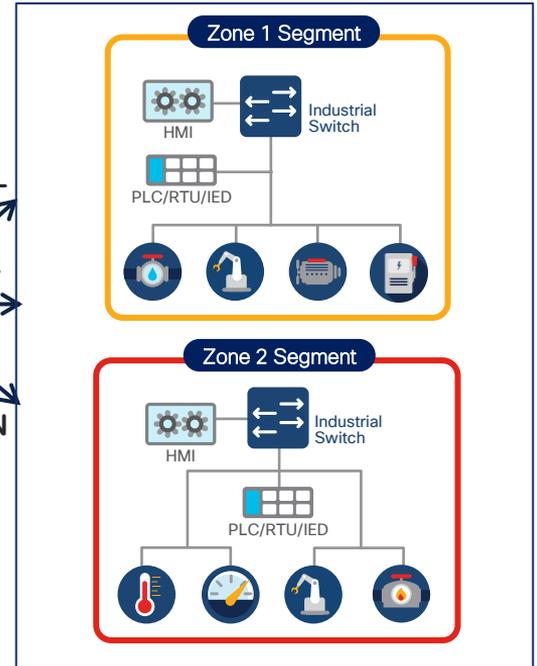
Cisco Cyber Vision Map View

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

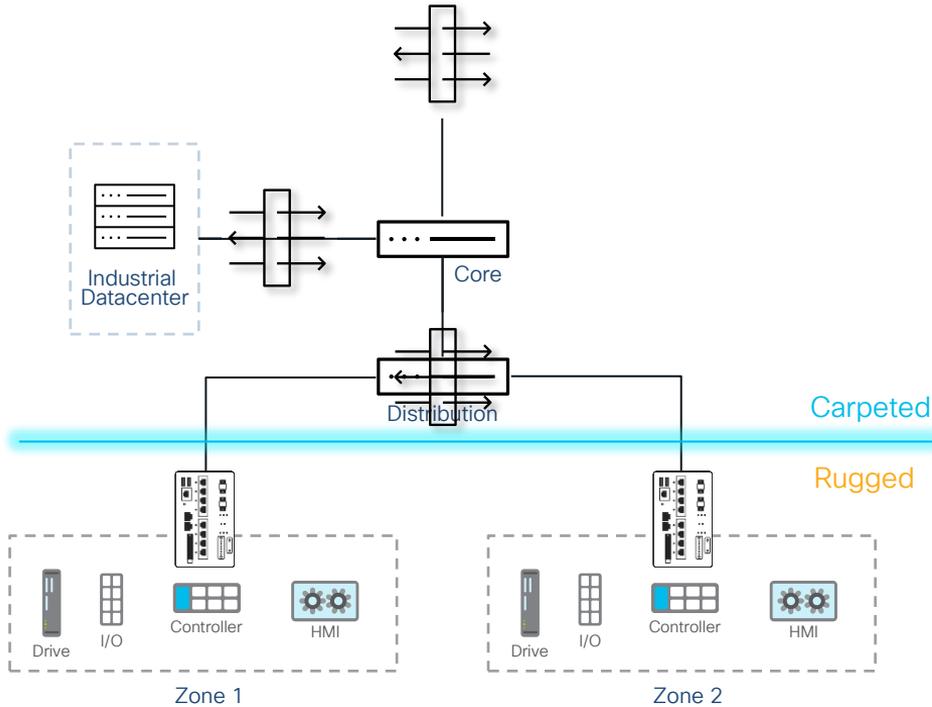
Cisco ISE Policy Matrix

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

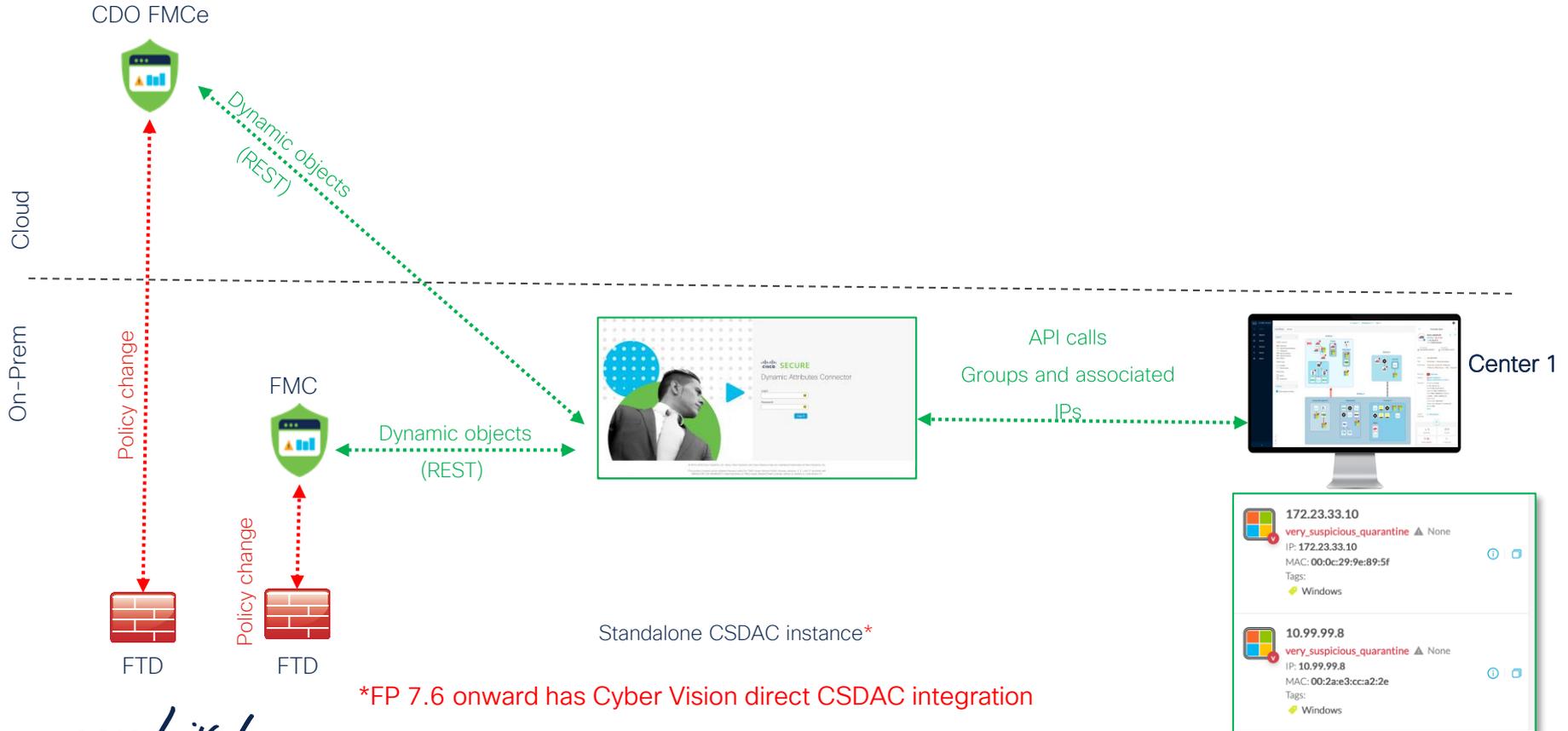
## Industrial Data Center

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 Management Center  
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration Deploy

cgrabows@tmedemos.com

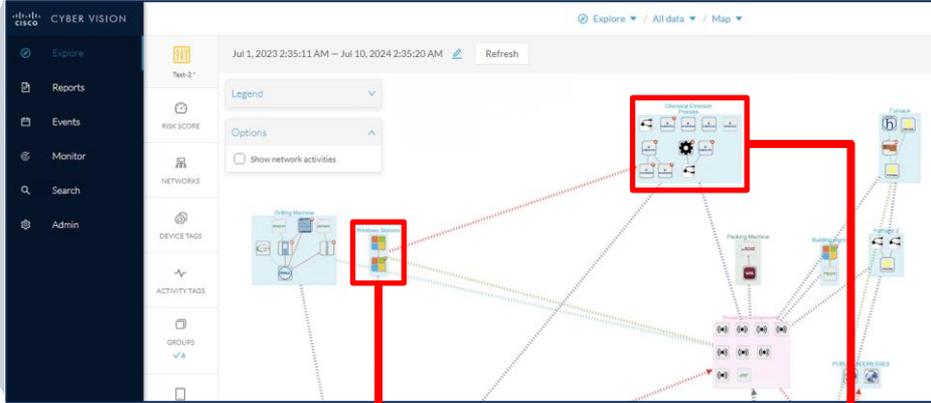
Dynamic Objects

Name	Description	Last Updated	Number of Mapped IPs	
OT_broadcast_components		01 Jul 24 17:38 PM	8	
OT_building_mgmt		01 Jul 24 17:38 PM	2	
OT_chemical_emerson_process		01 Jul 24 17:38 PM	13	
OT_control_center		01 Jul 24 17:38 PM	4	
OT_cyber_vision_sensor		01 Jul 24 17:38 PM	1	
OT_drilling_machine		01 Jul 24 17:38 PM	7	
OT_edge_intelligence		01 Jul 24 17:38 PM	1	
OT_engineering_stations		01 Jul 24 17:38 PM	3	
OT_enterprise_network		01 Jul 24 17:38 PM	5	
OT_folding_production_line		01 Jul 24 17:38 PM	4	

- > AAA Server
- > Access List
- > Address Pools
  - Application Filters
  - AS Path
  - BFD Template
  - Cipher Suite List
- > Community List
- DHCP IPv6 Pool
- > Distinguished Name
- DNS Server Group
- > External Attributes
  - Dynamic Object**
  - Security Group Tag
- File List

# Firewall Policy with OT Dynamic Objects

Cyber Vision



Firewall policies automatically follow dynamic OT groups.



FMC

	Name	Action	Sources	Destinations and Applications
<b>Mandatory (No rules)</b>				
▼ <b>Default (1 - 3)</b>				
<input type="checkbox"/>	1 Management Access	Allow	NET Engineering-Range	APP HTTPS, RDP, SSH; DYN OT_management_stations
<input type="checkbox"/>	2 Folding Process CTRL	Allow	DYN OT_control_center	APP S7Comm, S7Comm Ack, S7Comm Ack Data; DYN OT_folding_production_line
<input type="checkbox"/>	3 New-Rule-#2-ALLOW	Allow	DYN OT_windows_stations	DYN OT_chemical_emerson_process

# Cyber Vision Integration Splunk & XDR

CISCO *Live!*





# 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** Live!

Investigate incidents in multiple consoles

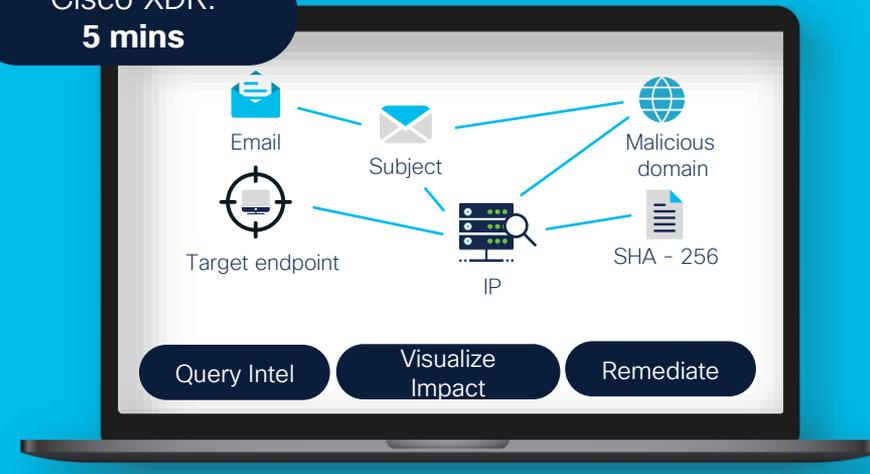


Without XDR:  
~32 mins

Remediate by coordinating multiple teams



Cisco XDR:  
5 mins



Cloud | Network | email | Identity | Firewall | Endpoint | OT Visibility  
**Broadest native telemetry and 80+ integrations to deliver best customer outcomes**

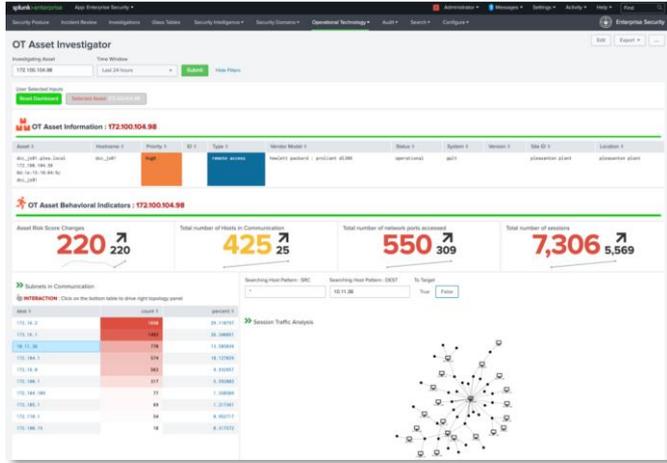
# Cisco XDR Ribbon on Cyber Vision: Investigation & Orchestration

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

...directly from Cyber Vision

The image shows a screenshot of the Cisco XDR interface. On the left, there is a sidebar with navigation options: All data, Basics, Description, Criteria, RISK SCORE, NETWORKS, DEVICE TAGS, ACTIVITY TAGS, GROUPS, and SENSORS. The main dashboard displays several metrics: Global Risk Score (60), Devices (5), Vulnerable Devices (2), and Events (Over The Last 30 Days) (28). A green arrow points from the 'XDR' button in the bottom-left corner of the sidebar to the 'XDR HOME' header of an overlay window. This overlay window, titled 'XDR HOME', features a 'Ribbon' section with six icons: Casebook, Incidents, Queries, Notifications, Settings, and Tips. To the right of the ribbon is an 'Applications' section with a search bar and a dropdown menu.

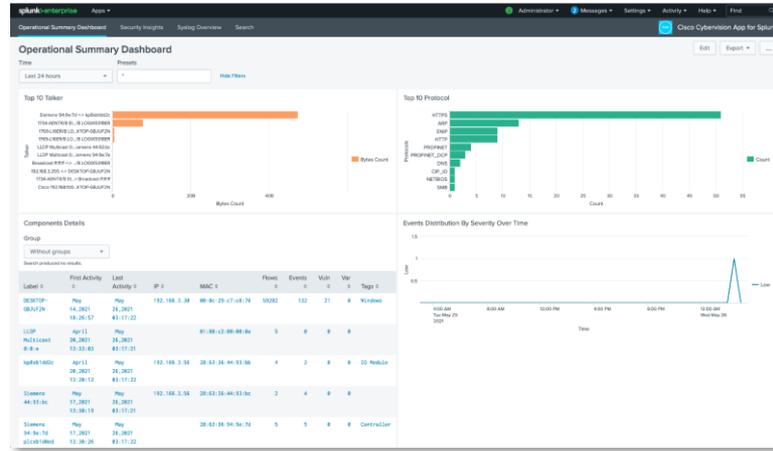
# Unified visibility across IT and OT with Splunk



Splunk OT Add-on

Splunk Enterprise Security

Splunk base

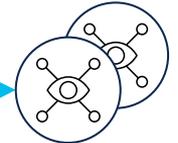


Cyber Vision App

Cyber Vision Add-On

Cyber Vision Center(s)

REST API





## 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 its 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



## 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](#)



## OT Security Add-on for Splunk

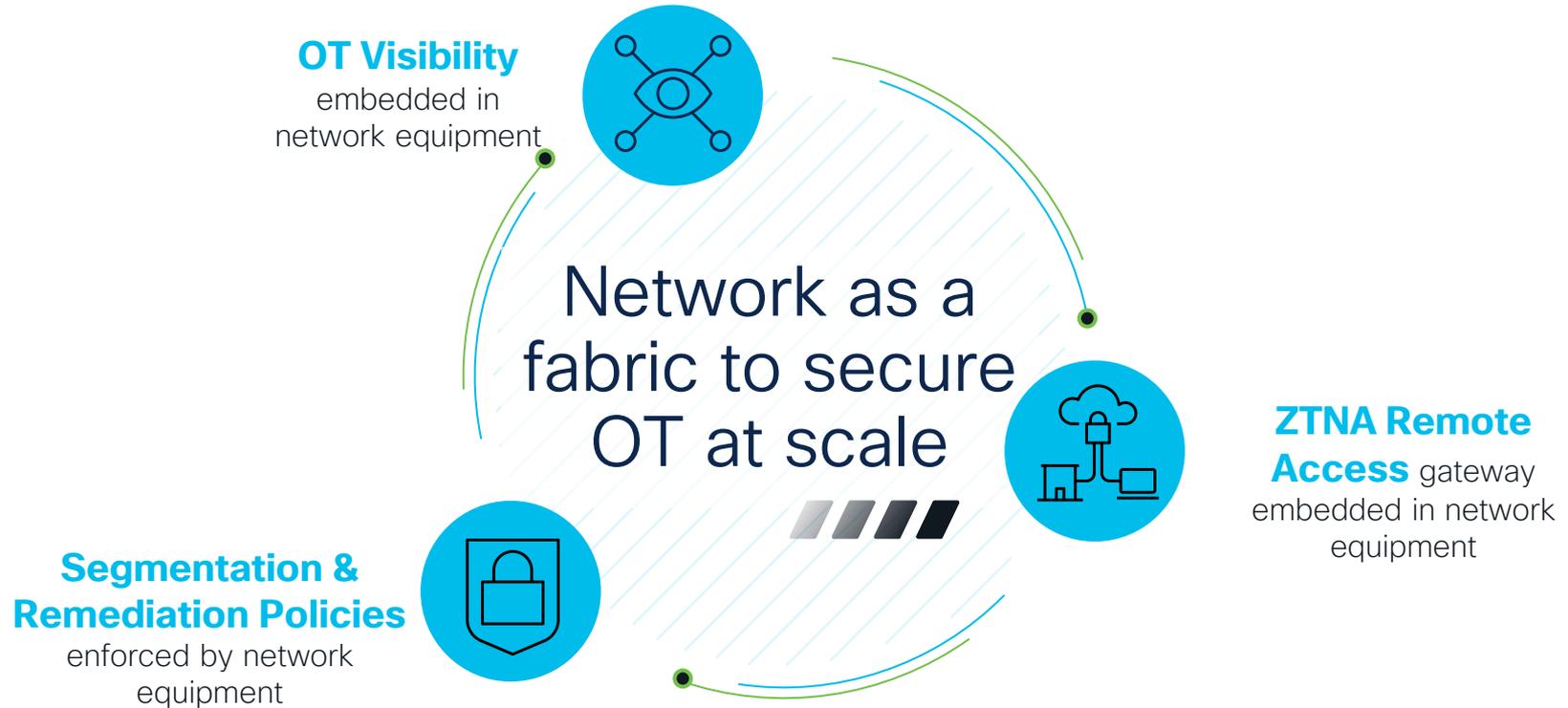
The OT Security Add-on for Splunk enables organizations that operate assets, networks, and facilities across both IT and OT environments to better apply the globally proven SIEM, Splunk Enterprise Security, to improve threat detection, incident investigation, and response. The OT...

Built by [Splunk Works](#)

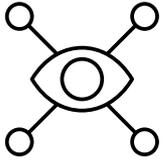
# Conclusion



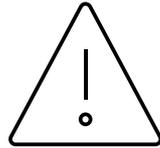
# The Cisco Industrial Security Differentiation



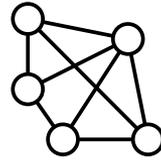
# You cannot secure what you cannot see



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

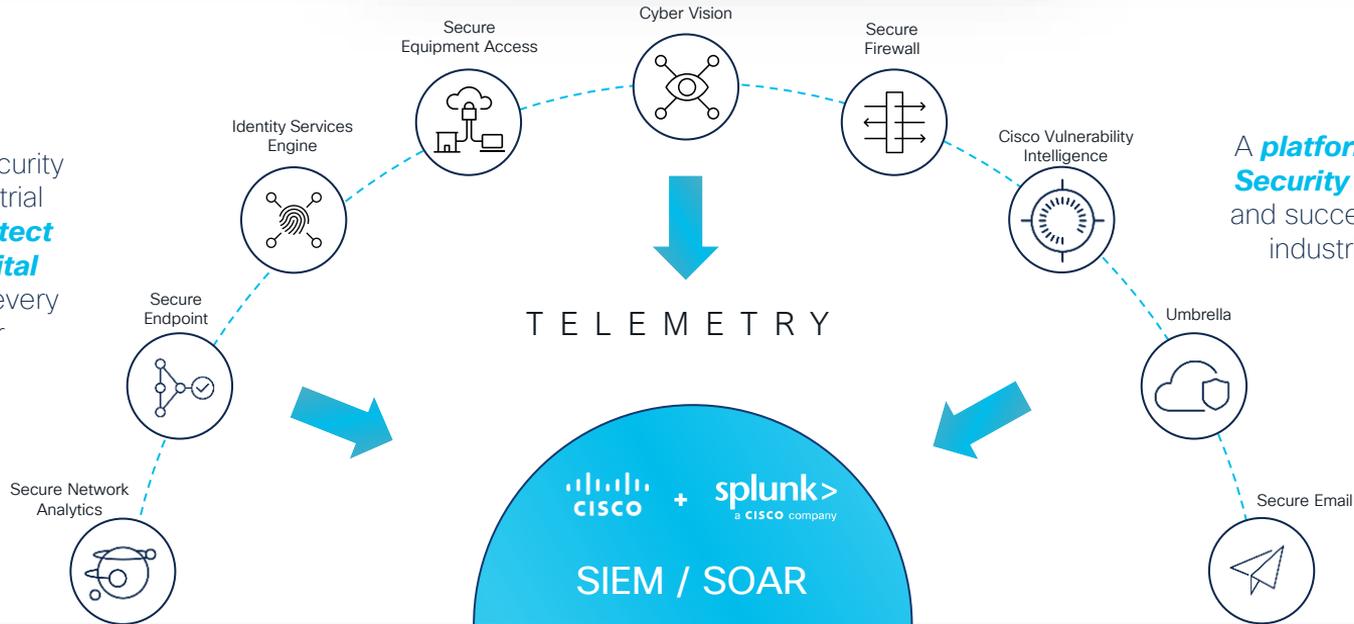
Threat Intelligence

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?

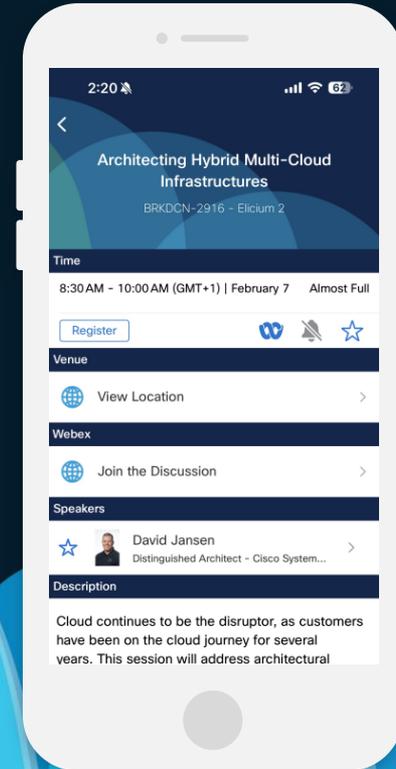
Use the Webex app to chat with the speaker after the session

## 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.

**CISCO** *Live!*



# 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.

START

Sunday, February 9 | 1:45 p.m.

### TECSEC-2001

Industrial Security Journey: from Visibility to Enforcement and Protection

Monday, February 10 | 4:00 p.m.

### BRKIOT-1005

Enable Zero Trust Network Access for Industrial Networks with Cisco Secure Equipment Access

Tuesday, February 11 | 2:00 p.m.

### LTRSEC-2381

Stronger Together: Uniting IT and OT Security with Cyber Vision

Tuesday, February 11 | 4:00 p.m.

### BRKIOT-2882

Implementing Segmentation in Industrial Networks

Tuesday, February 11 | 4:30 p.m.

### BRKIOT-2910

Securing Industrial Networks: Where to start - using Cyber Vision for OT Asset Visibility

Wednesday, February 12 | 2:30 p.m.

### IBOIoT-1141

Pwn the OT Network! Do I Really Know What's Happening Inside?

Wednesday, February 12 | 4:00 p.m.

### IBOIoT-2094

Build The Next Generation Industrial Firewall with a Single Industrial Router using SDWAN

Thursday, February 13 | 1:00 p.m.

### BRKSEC-2821

Securing Industrial Networks: Strategies and Best Practices

FINISH

# 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](https://ciscolive.com/on-demand). Sessions from this event will be available from March 3.



Thank you

CISCO *Live!*



CISCO *Live!*

GO BEYOND

A series of overlapping, vertically-oriented ovals in various shades of blue, ranging from light to dark, positioned on the right side of the image.