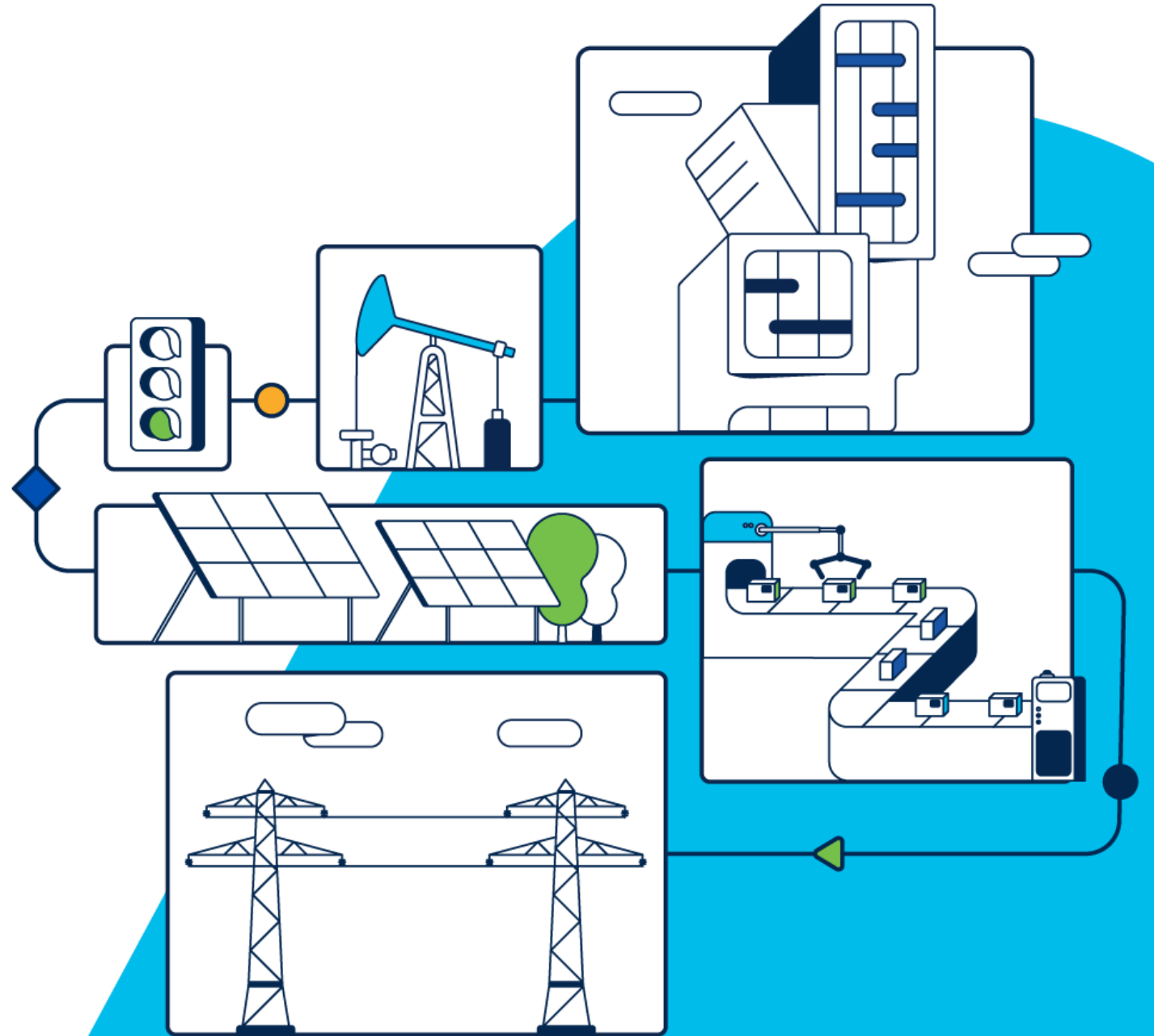




# CISCO Industrial

Bratislava 2026

Peter Malic, Cisco  
Michal Remper, Soitron



# O čom budeme rozprávať

- Cisco Industriálne Portfólio
- OT Security, základné kroky pre zabezpečenie siete
- Cisco Cyber Vision
- Q&A

# Industrial IoT networking portfolio Overview

## Industrial Ethernet switches

DIN-Rail, IP67, and Stackable Rackmount



## Industrial Cybersecurity

Cyber Vision, Secure Equipment Access



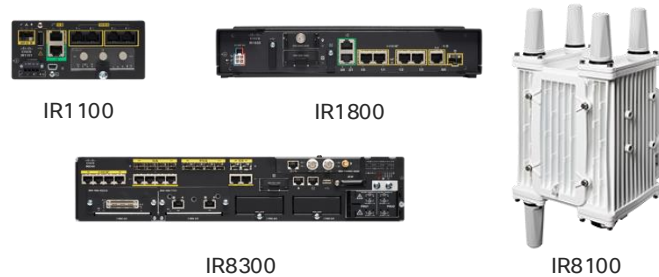
## Industrial Wi-Fi and Ultra-reliable Wireless Backhaul

For outdoor conditions



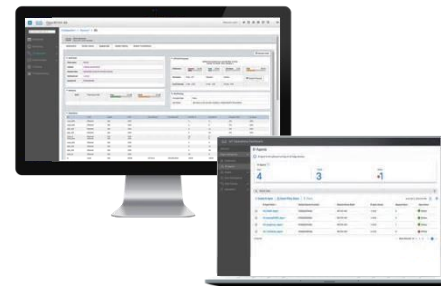
## Industrial Routers

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



## Data Control and Exchange

Edge Intelligence, IOx



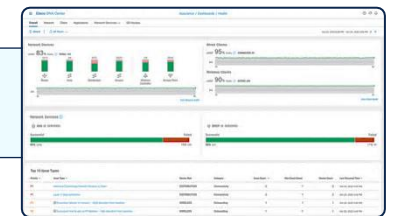
## Embedded Networking

Embedded routers and switches for industrial Makers



## Management and Automation

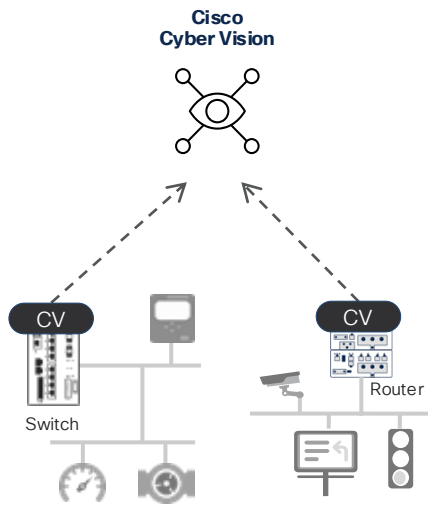
Cisco Catalyst Center, Cisco Catalyst WAN Manager, Field Network Director, IW Service



# Zabezpečenie Siete, 4 Základné Kroky

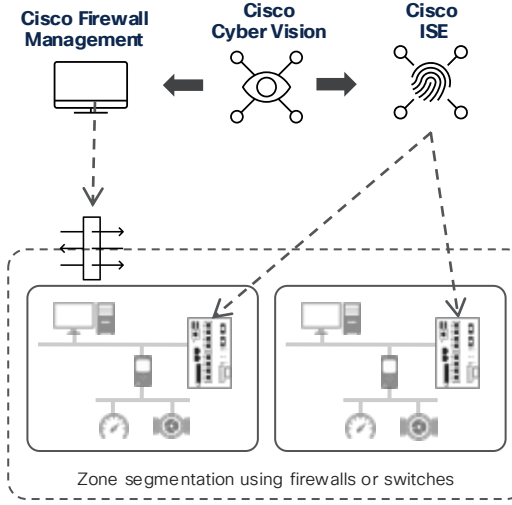
1

Asset Visibility and  
OT Security Posture



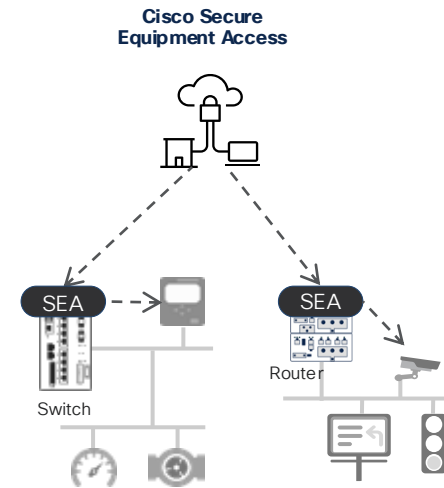
2

Zero Trust  
Segmentation



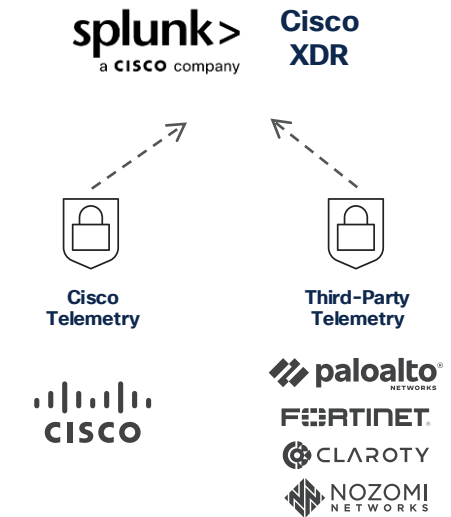
3

Zero Trust Network Access  
(ZTNA) for OT



4

Cross-Domain Detection,  
Investigation & Response



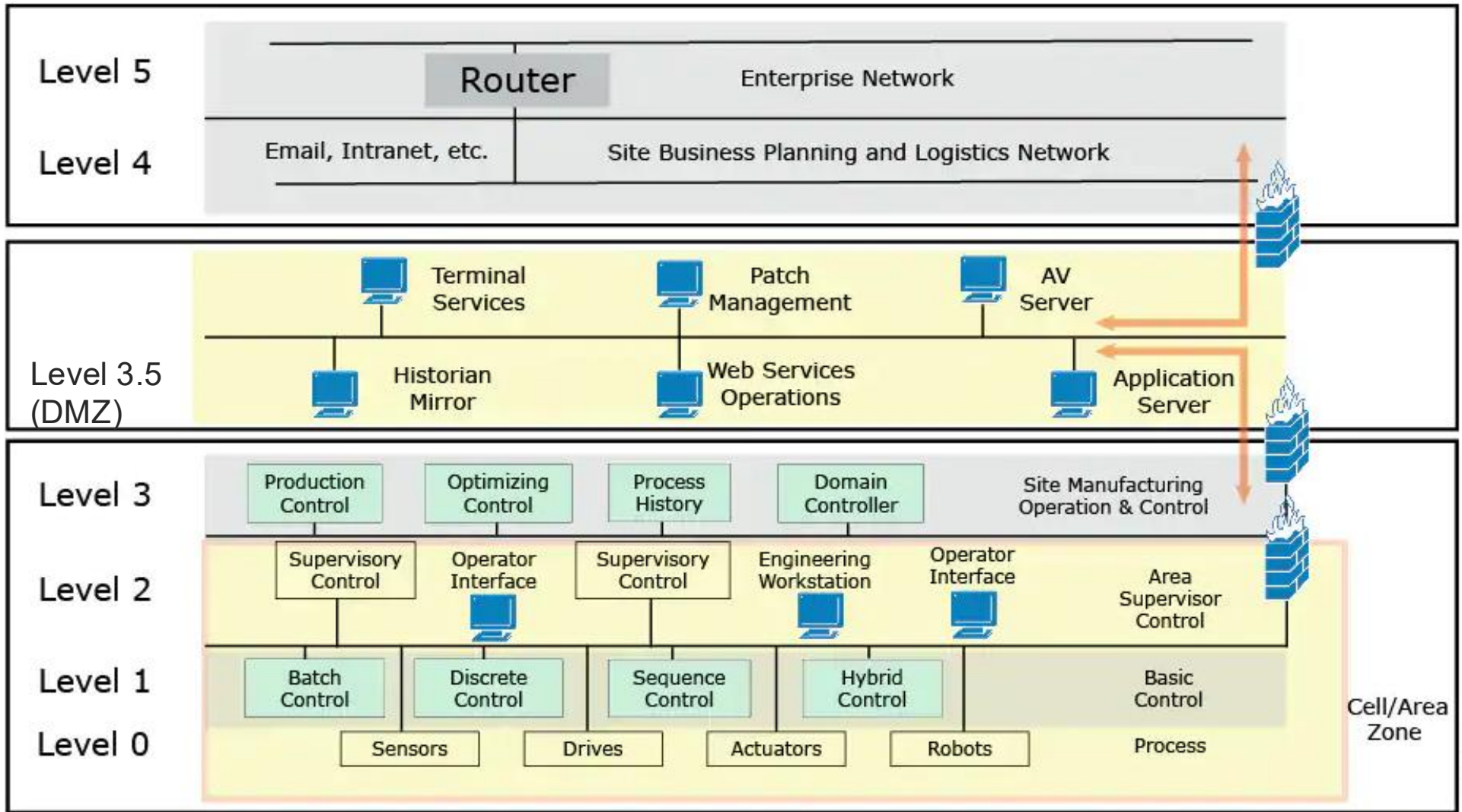
Talos Threat Intelligence

+



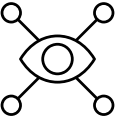
Talos Incident Response

# ISA-95 / CIM (Purdue) Model



Extract from CISCO "Oil and Gas Pipeline Security Reference Document". CIM / ISA model differ in the scope of levels 0-1;

# Čo treba zabezpečiť?



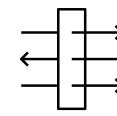
Identify OT assets and their communications



Spot vulnerabilities to patch or protect



Segment networks with access policies



Detect bypass or leaks in the IDMZ

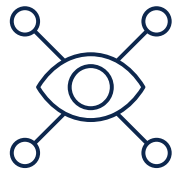


Drive compliance and governance

Visibility helps drive IT/OT collaboration to secure industrial operations

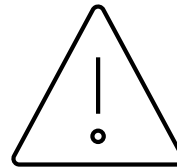
# Cisco Cyber Vision

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" by Rockwell Automation. It includes fields for "First activity" (Apr 14, 2021 11:45:12 AM), "Last activity" (Apr 16, 2021 11:00:01 AM), IP address (192.168.249.50), and MAC address (f4:54:33:91:cb:ee). A "Paint\_Line\_2" tag is marked as "high". A "Tags" section lists "Controller", "Rockwell Automation", "Stop CPU", "Diagnostics", "Read Var", "Write Var", and "Low Volume ...3+". Summary statistics show 14 Flows, 9 Events, 10 Vulnerabilities, and 0 Credentials. A "Minimap" window is overlaid on the right, titled "Communication Map". It features a legend with categories: Important (red), Control system behavior (green), IT Behavior (blue), Network analysis (purple), and Others (grey). The map shows a central "SIMATIC 300(N)" node connected to "STATION-WINCC", "SIEMENS IM151-3PN", "SIEMENS SENTRYO-XP-1", "Siemens ef 65 8d", and "Siemens 192.168.0.10". A red line highlights a path from the central node to the SENTRYO-XP-1 node. Other nodes include "SENTRYO-SIMATIC" and "Profinet DCP Multicast 0.0.0".

# 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. The top section, titled "Vulnerability Detection", shows a search for "192.168.1 subnet" resulting in "73 Vulnerabilities". A donut chart indicates the distribution of these vulnerabilities by severity: 2 Critical (red), 2 High (orange), 3 Medium (yellow), and 66 Low (green). A list of 10 most matched vulnerabilities is provided, including CVE-2015-5627 (Yokogawa Multiple Products Buffer Overflow Vulnerabilities), CVE-2020-5609 (Path Traversal Vulnerability in Yokogawa CENTUM), and CVE-2019-10936 (Denial-of-Service Vulnerability in Profnet Devices). A summary box on the right indicates "9 Total vulnerable components for 192.168.1 subnet".

The bottom section, titled "Risk Scores", shows the risk score for a specific device, "SCS0102 Building K", which is "very high". The current risk score is 69, and the best achievable score is 44. A bar chart compares the current risk score (69) to the achievable risk score (44). The score was computed on May 24, 2021 10:00:06 PM by Cisco Cyber Vision as follows:

Criteria	Matching	Distribution	Description
Device type	SCS0102 type: Controller	13%	CC key element. Compromise could lead to large impact
Group impact	SCS0102 group: Building K. It has an industrial impact very high.	51%	
Activities	No matching activity	0%	
Vulnerabilities	SCS0102 most impacting vulnerability is Path Traversal Vulnerability in Yokogawa CENTUM	36%	CVSS score: 9.8 Successful exploitation of these vulnerabilities could allow a remote unauthenticated attacker to se... <a href="#">show more</a> <a href="#">See details</a>

# 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 the Cisco Cyber Vision interface for Malware Detection. It features a search bar at the top with filters for 'category' (Signature based Detection) and 'severity' (very high). Below the search bar, there are two event cards. The first event, dated 16:12:09.236, is a 'Signature based Detection' with the message 'Snort allow on TCP id 27679 with signature A Network Trojan was detected'. The second event, dated 10:31:27.690, is also a 'Signature based Detection' with the message 'Snort allow on UDP id 44037 with signature A Network Trojan was detected'. Both events include detailed metadata such as 'Occurred at', 'Sensor', 'Action', 'Gid', 'Signature ID', 'Priority', 'Rule', and 'Classification'. A 'DOWNLOAD DATA' link is provided for each event. At the bottom, a network diagram shows the source IP 'Intel 192.168.0.12' and the destination IP '212.166.210.80', with associated MAC and IP addresses for both.

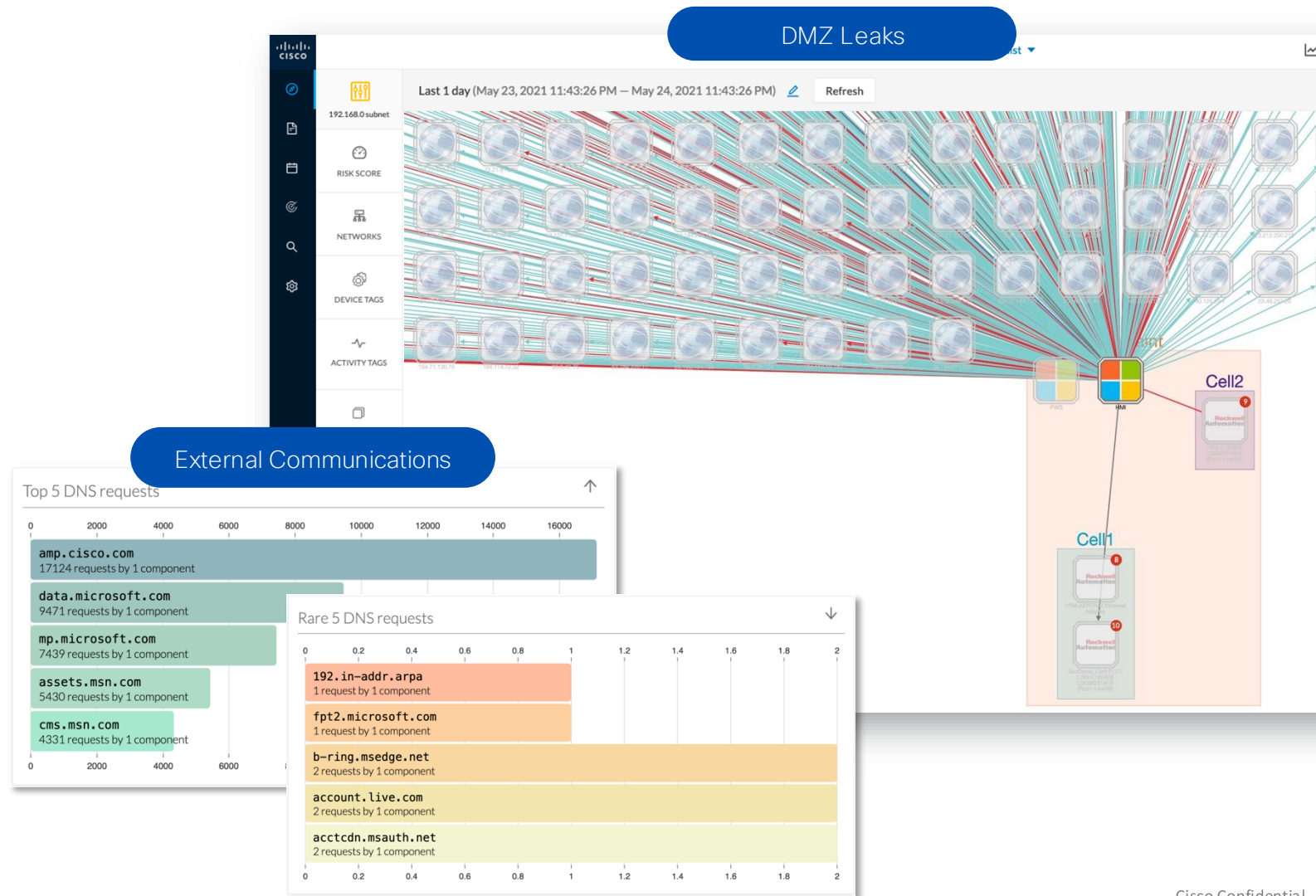
# Visibility into external communications

## Identify DMZ leaks

Filter subnets to identify traffic to external networks and stop unauthorized leaks past the DMZ

## External communications

Identify assets trying to access external servers to spot malware infections, misconfigurations, and unnecessary traffic



# Visibility Reports to help manage risks

## Customizable Reports

Track risk management improvements and show progress to management with historical reports

## Remote Access Reports

Document remote access gateways to engage with operation teams and remove backdoors into the OT network

### Remote Access Reports

#### Key Findings

Filter Criteria: All data Preset

This report is an automated summary that captures a list of all Remote Access Gateways related activities found on the devices in the All data Preset by Cisco Cyber Vision on Feb 8 am UTC

Risk score	Total Devices	Vulnerable Devices
37	4	0

#### Security Insights

Severity	Findings
High	1 devices have been identified as Remote Access Gateways
High	1 devices have been attempted to be remotely accessed
Medium	3 devices have run DNS queries for 3 remote access domains

#### DNS Queries to Remote Access Domain Names

Cisco Cyber Vision maintains a list of known remote access domains that are used whenever a remote user attempts to access internal devices. The table below depicts those devices that have attempted to run a DNS query to these domains, indicating that these devices may have been remotely accessed.

Device Name	Device IP	Group	Domain Name	Count	Latest Timestamp (UTC)
192.168.0.72	192.168.0.72	-	client.teamviewer.com	1	2024-02-06 07:39 AM
192.168.0.72	192.168.0.72	-	de-fra-anx-r048.router.teamviewer.com	1	2024-02-06 07:39 AM
192.168.0.72	192.168.0.72	-	router13.teamviewer.com	1	2024-02-06 07:39 AM

#### Attempted Remote Access Communications

Cisco Cyber Vision maintains a list of known domains that are used whenever a remote user is trying to access internal devices. The table below depicts those internal devices that may have been attempted to be accessed remotely from one of these domains listed next to it.

Device Name	Device IP	Group	Remote Domain Name	Protocols used	Count	Latest Timestamp (UTC)
192.168.0.72	192.168.0.72	-	client.teamviewer.com	TeamViewer (443)	1	2024-02-06 07:39 AM

### Key Findings

Filter Criteria: -

This report is an automated summary that captures all the vulnerability security events found on the devices in the - by Cisco Cyber Vision on Sep 8:04 am UTC

Risk score	Devices	Vulnerable Devices	Events(over the last 24 hours)
45.0	34	7	323

#### Security Insights

Severity	Findings
Critical	46 critical and high severity vulnerabilities found on devices
Critical	4 devices have a risk score > 70
High	3 devices found communicating with external networks
High	47 devices have been remotely accessed
High	2 devices found using 11 unsecured protocols
High	2 devices using clear text passwords

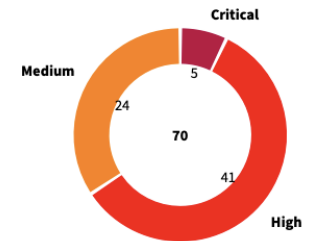
#### Top 5 Vendors seen

Vendor	Number of devices
ABB Oy / Medium Voltage Products	1
Cisco Systems Inc	1
ASIX ELECTRONICS CORP.	1
Quanta Storage Inc.	1

## Security Posture Reports

### Vulnerabilities

Filter Criteria: -



CVE ID	Vulnerability Name	CVSS Score	Severity	Number of affected devices
CVE-2017-12741	Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability	7.5	High	4
CVE-2019-10936	Denial-of-Service Vulnerability in Profinet Devices	7.5	High	4
CVE-2017-2680	Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and Configuration Protocol	6.5	Medium	4
CVE-2022-30694	Missing CSRF Protection in the Web Server Login Page of Siemens Industrial Controllers	6.5	Medium	4
CVE-2019-6568	Denial Of Service Vulnerability in Web-server of Industrial Products - Siemens	7.5	High	3

# 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

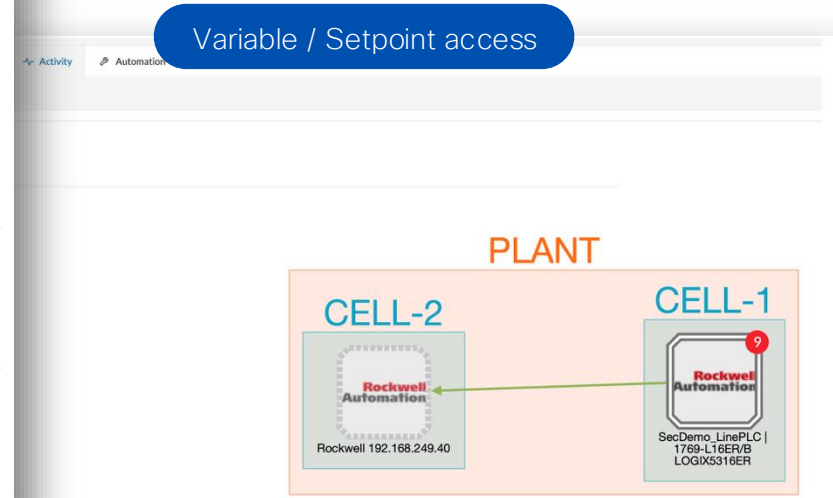
**Control System Activities**

Activity

- PLC\_3**  
Gas Compression ▲ very high  
IP: 192.168.105.130  
MAC: 28:63:36:82:28:96
- Dell 192.168.105.241**  
Maintenance Station ▲ high  
IP: 192.168.105.241  
MAC: 34:17:eb:d1:c9:97

First activity: Apr 6, 2017 10:59:13 PM  
Last activity: Jun 20, 2019 12:22:27 AM

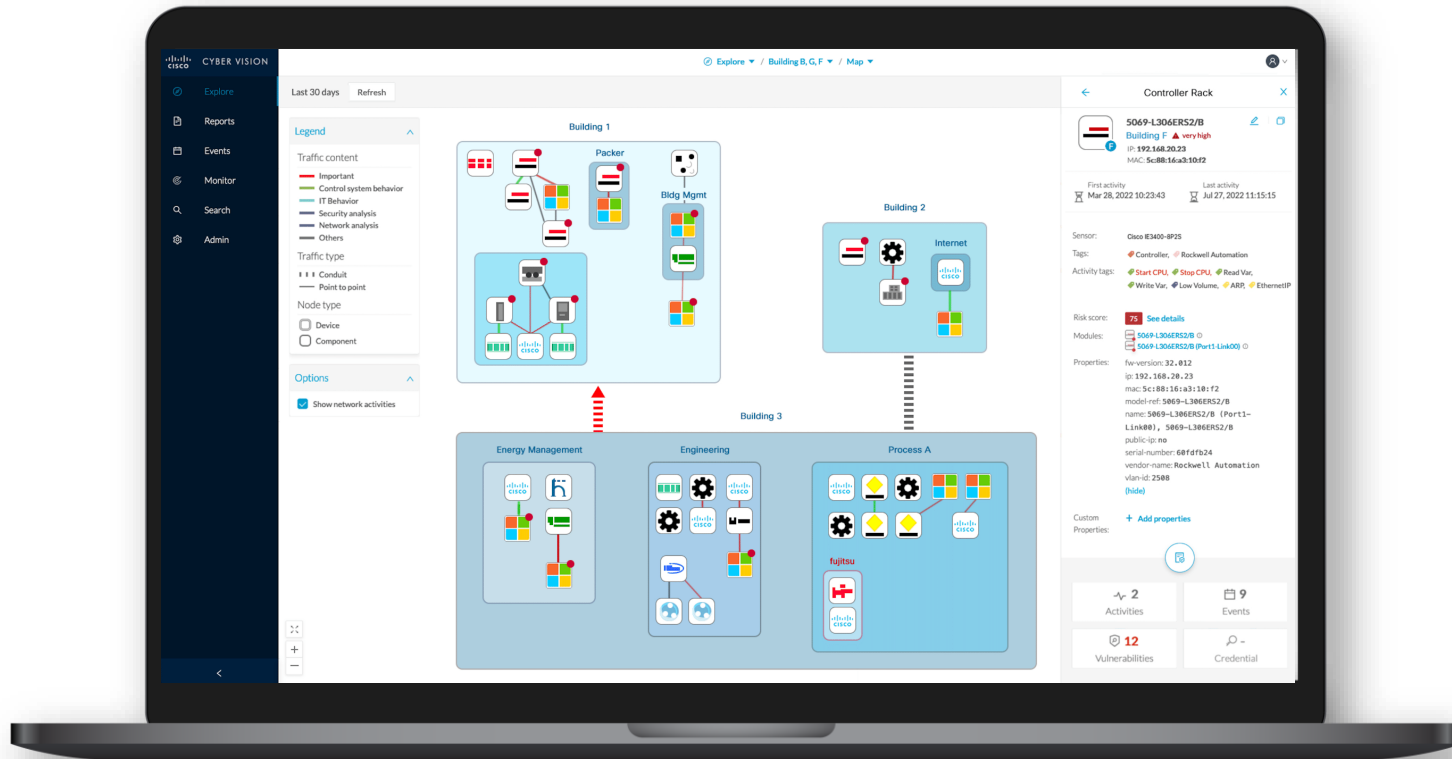
Tags: Program Upload, Start CPU, Stop CPU, Read Var, Write Var, ARP, S7Plus (hide)



Variables accesses

Variable	Protocol	Details	Types	Accessed by
SYNC	enip	Endpoint	READ / WRITE	SecDemo_LinePLC   1769-L16ER/B LOGIXS316ER
SYNC_NEW1	enip	Endpoint	READ	SecDemo_LinePLC   1769-L16ER/B LOGIXS316ER

# Leveraging visibility to drive segmentation



## ISA/IEC-62443 virtual segmentation



Group OT assets into zones



Visualize conduits



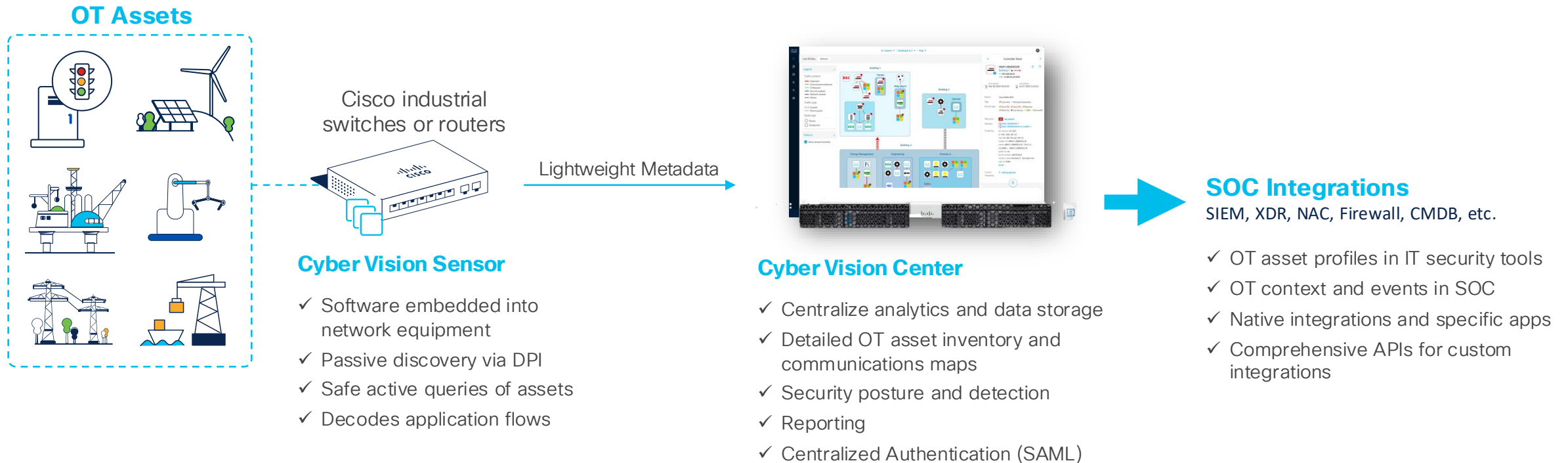
Identify traffic violations



Share context with other platforms to enforce segmentation

# 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



Amazon Web Services



Microsoft Azure

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

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

Sensors

Sensor



Catalyst IE3300, IE3400 and IE3500 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

Sensor

IDS



x86 or ARM64 Compute

Sensor

IDS



IC3000 Industrial Compute

## Network-Sensors

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

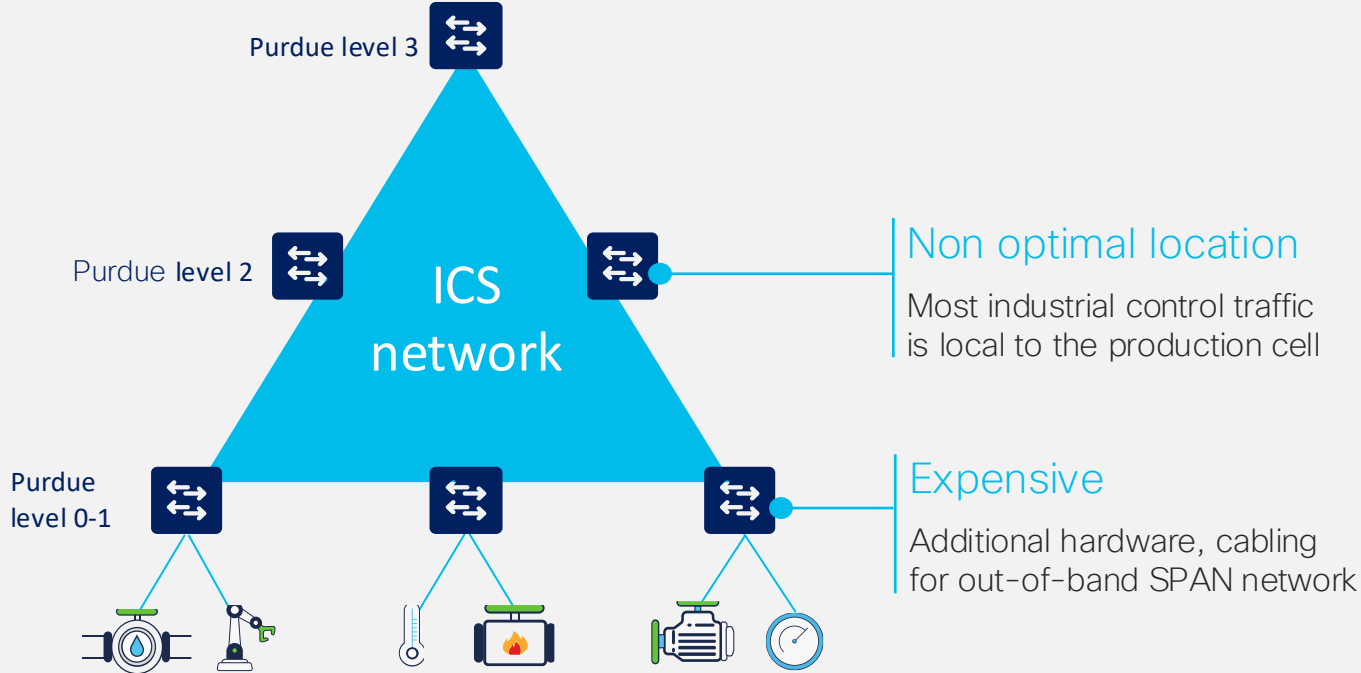
## Docker Sensor Hardware-Sensor

DPI and active discovery via SPAN to support brownfield



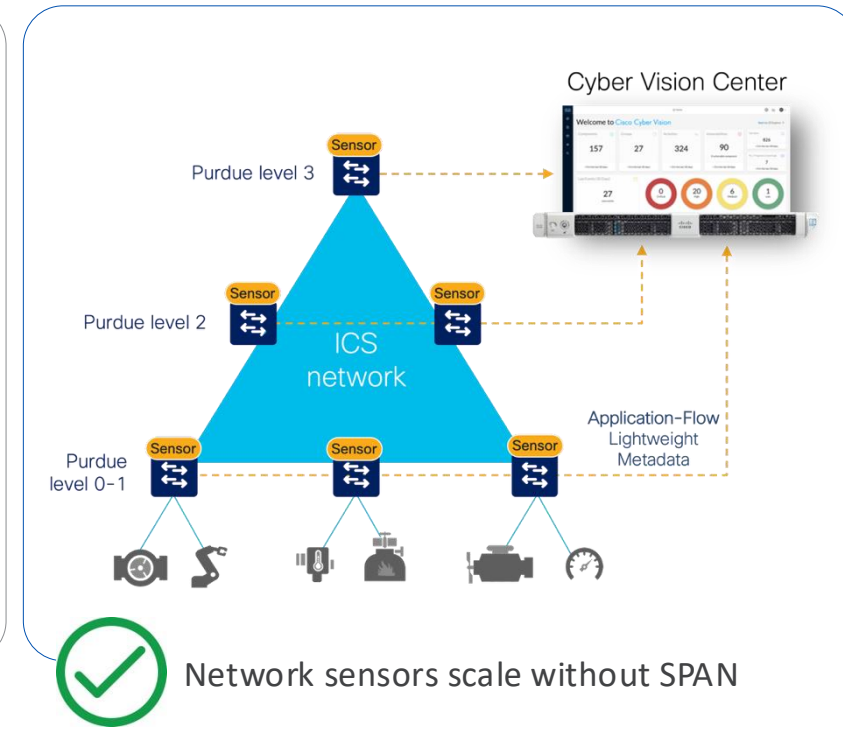
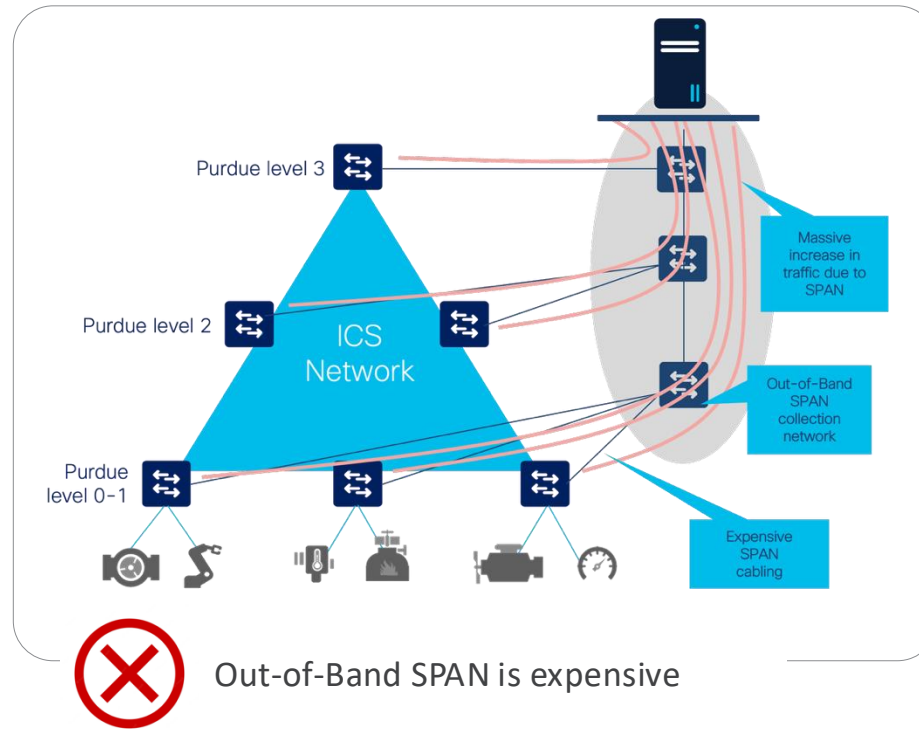
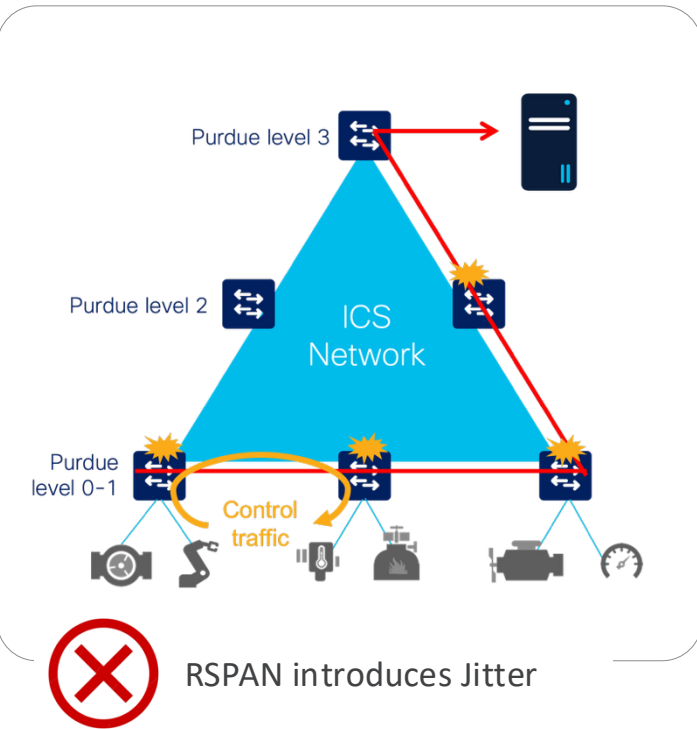
# Why is a network-sensor important?

Most industrial network traffic is East-West, not North-South



Sensors embedded in the network see everything that attaches to it

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



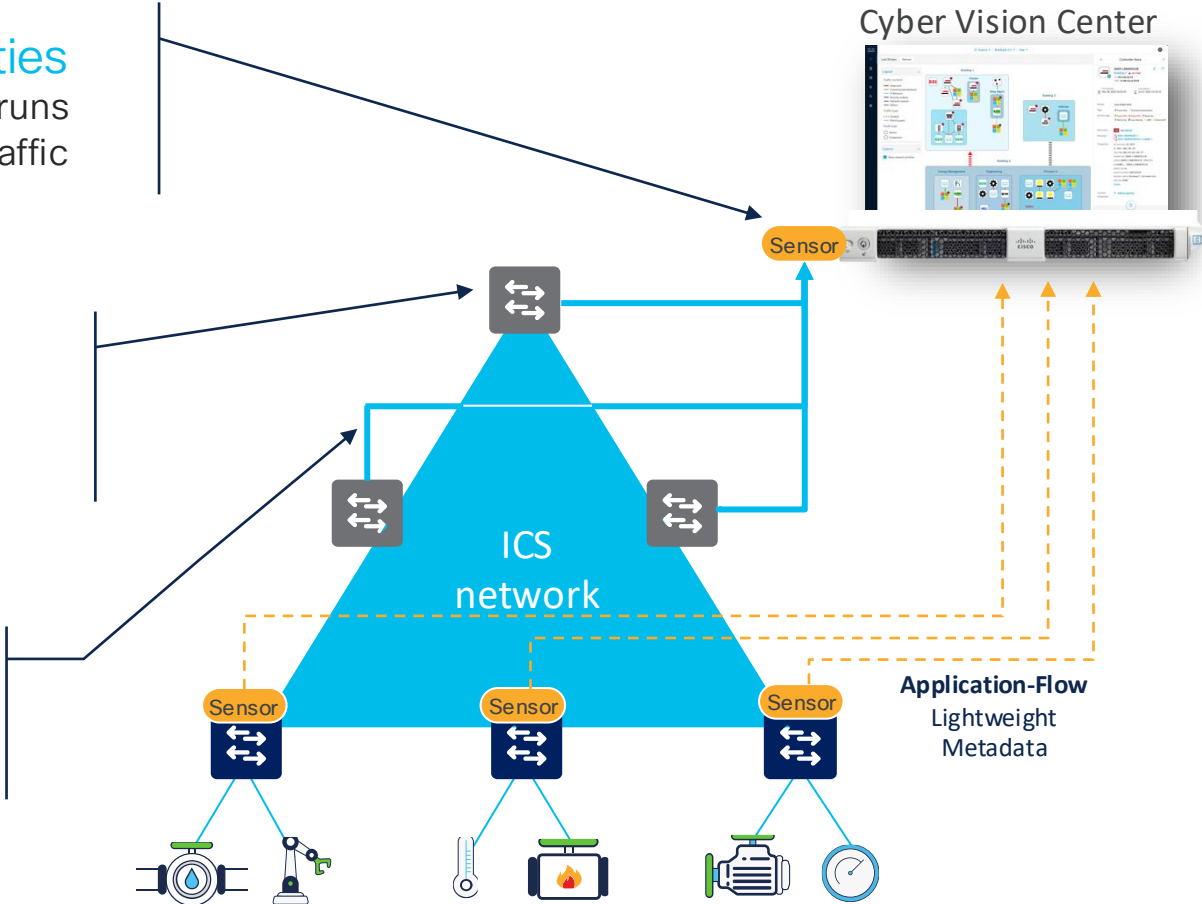
OT visibility sensors embedded into network equipment sees more and is easier to scale

# On-Center Sensor offers extra deployment flexibility

**Central DPI and IDS capabilities**  
Sensor built into the Cyber Vision Center runs DPI and IDS on raw industrial network traffic

**Collect traffic from the datacenter**  
Needs only 1-hop SPAN from the aggregation switch to the Cyber Vision Center

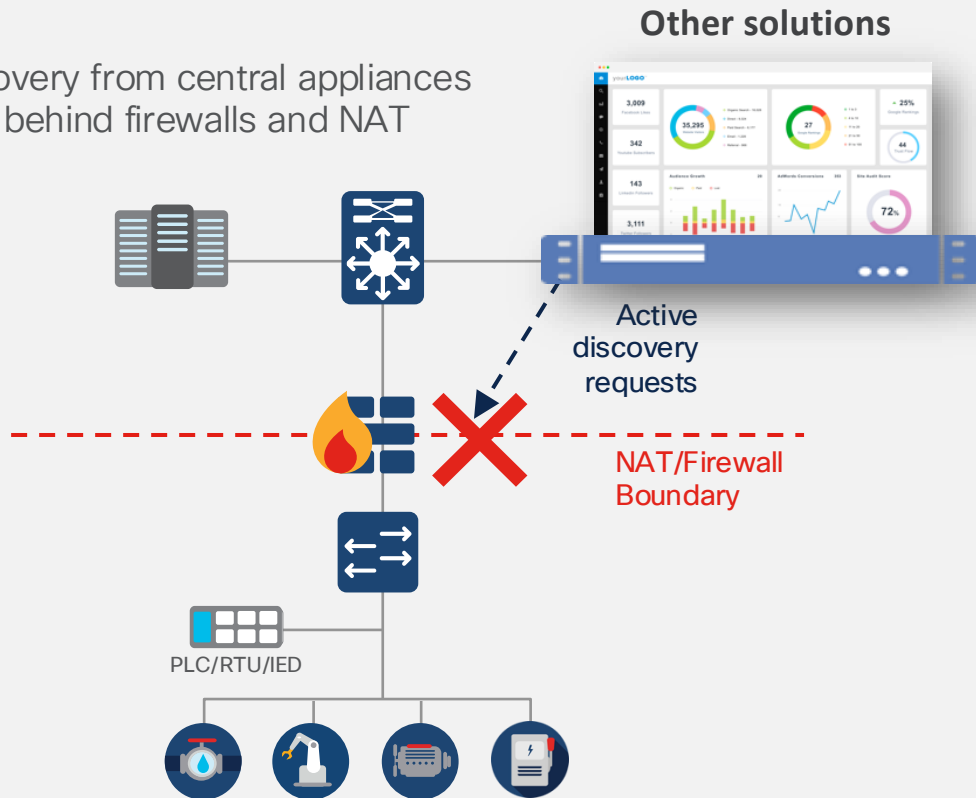
**Leverage existing SPAN infrastructures**  
Makes deployment super easy if the collection network is already in place



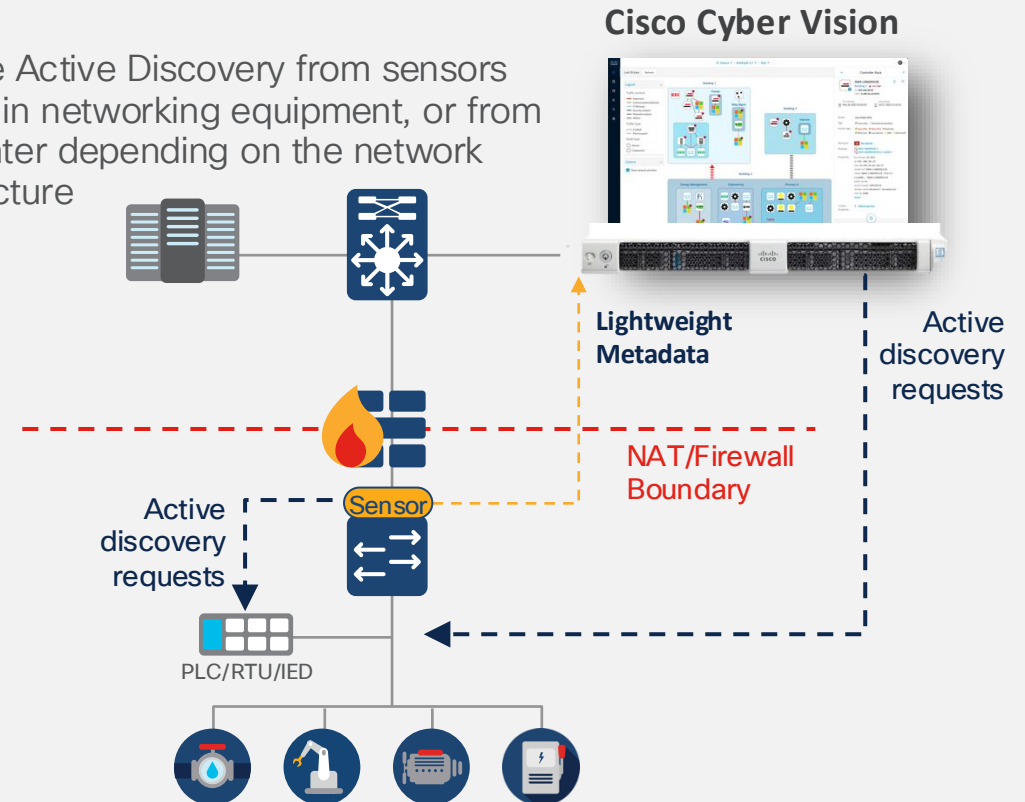
# Why is a network-sensor important?

Sensors embedded in the network can see more

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

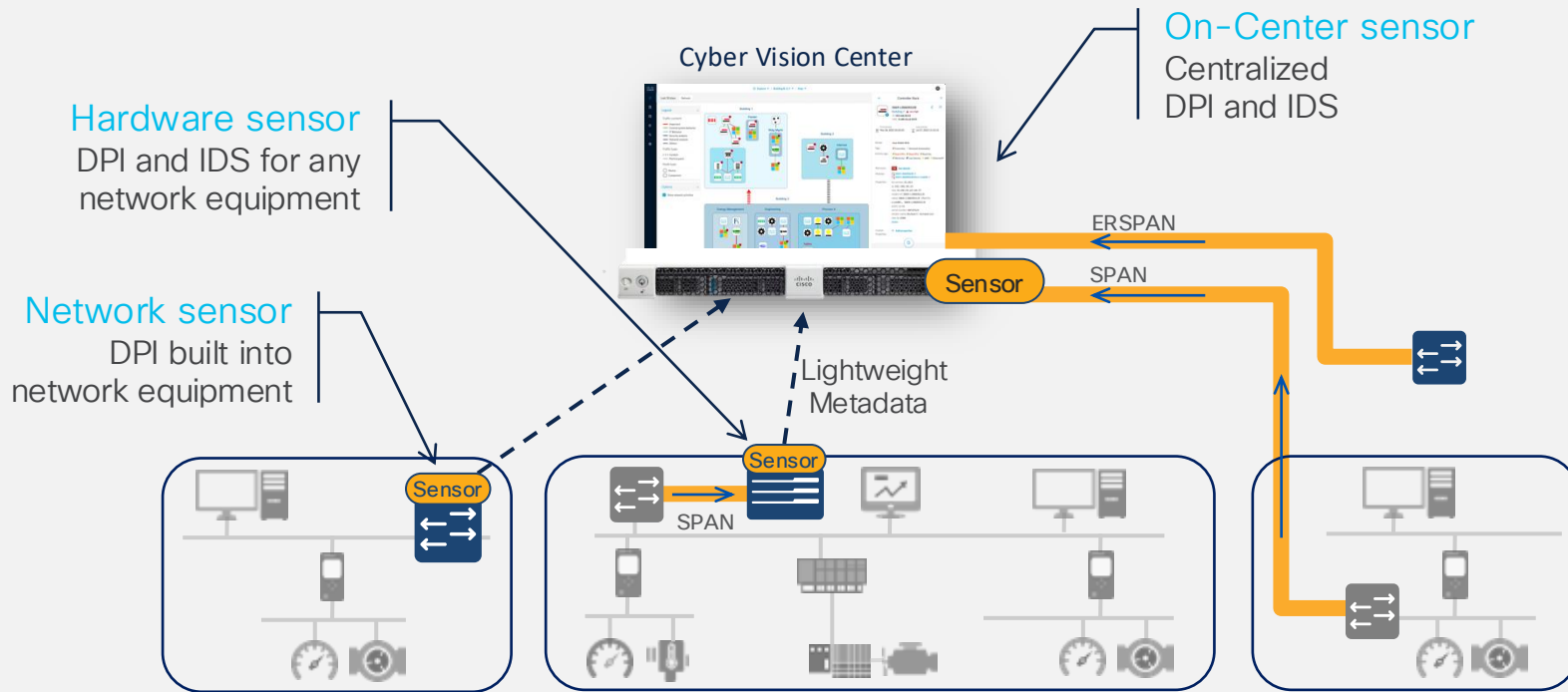


Flexible Active Discovery from sensors hosted in networking equipment, or from the center depending on the network architecture



Active discovery requests are not blocked by NAT and firewall boundaries

# Cyber Vision offers flexible deployment options



- **Network sensors** embedded in Cisco networking for simple and highly scalable deployments
- **Hardware 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, including ERSPAN to the center network interfaces

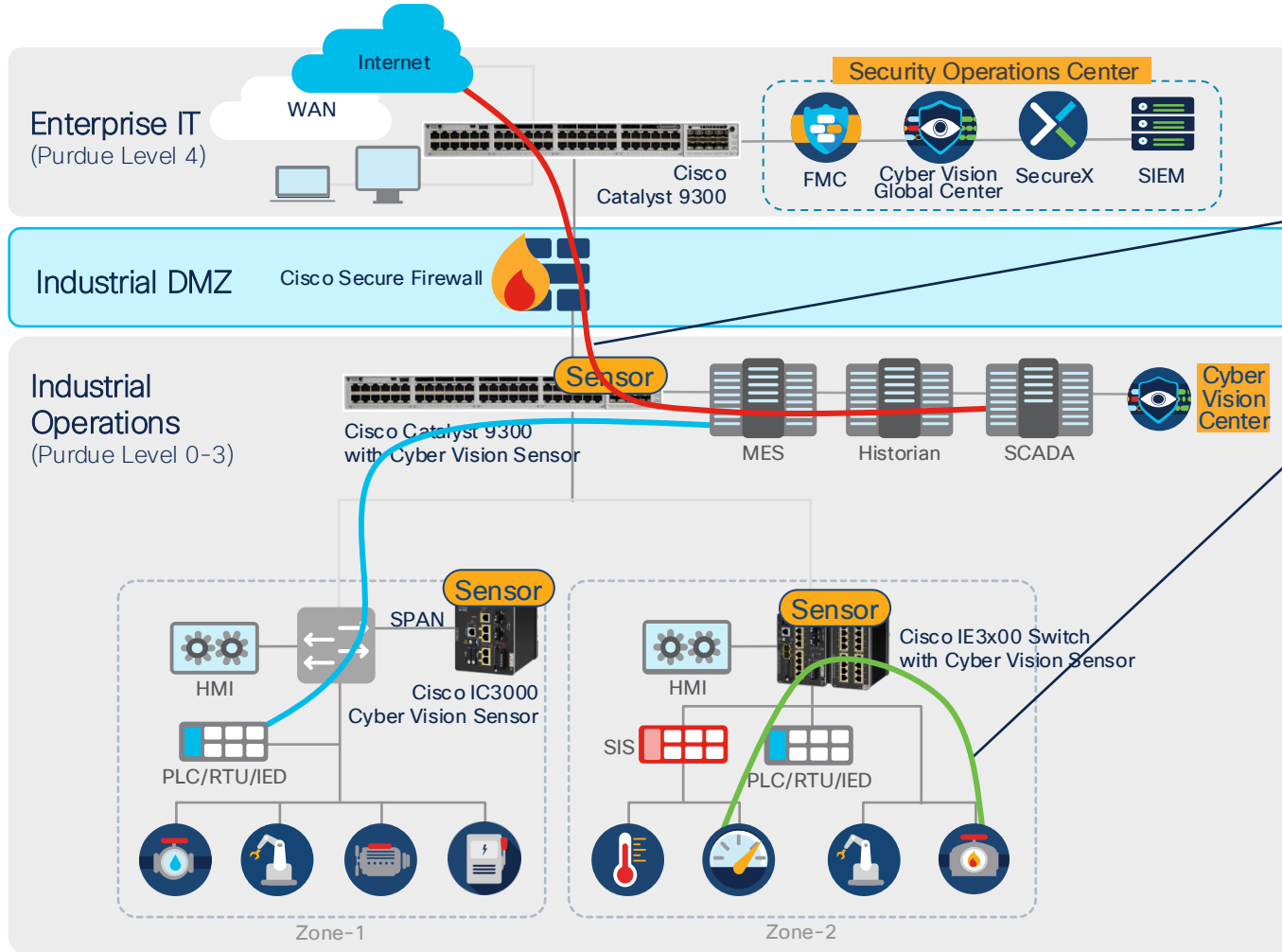
Cyber Vision can mix architectures to best fit your constraints

# 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!

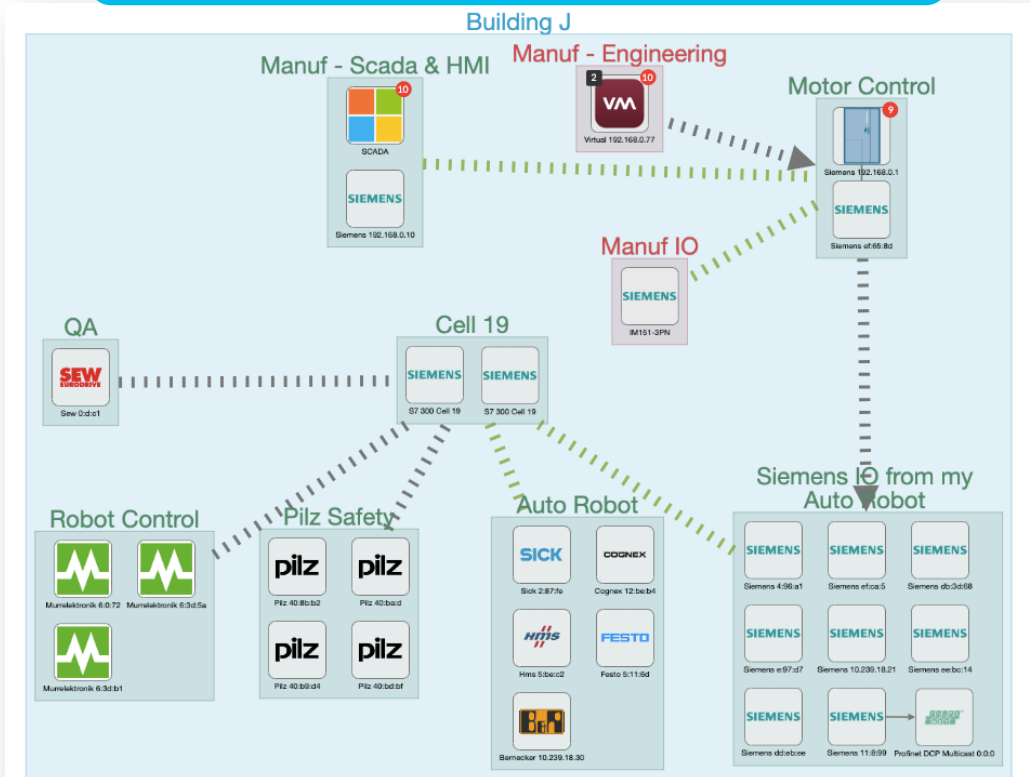
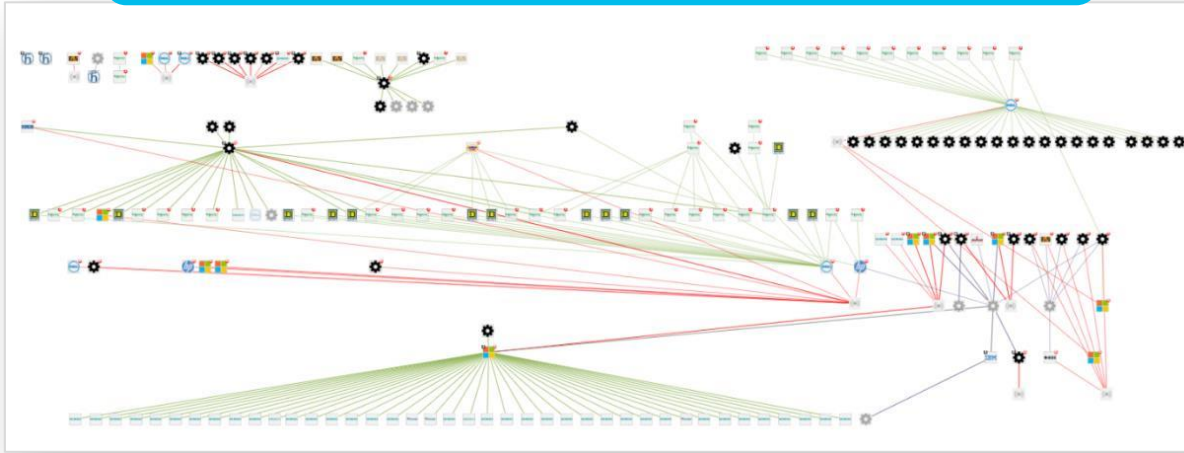
Rule of thumb: All flows must go through at least one sensor. Every networking equipment should have a sensor.

# Leveraging Visibility to Drive Segmentation

Cyber Vision discovers all connected assets...



...and groups them into logical zones



Give OT the tool they need to document ISA/IEC-62443 zones and conduits

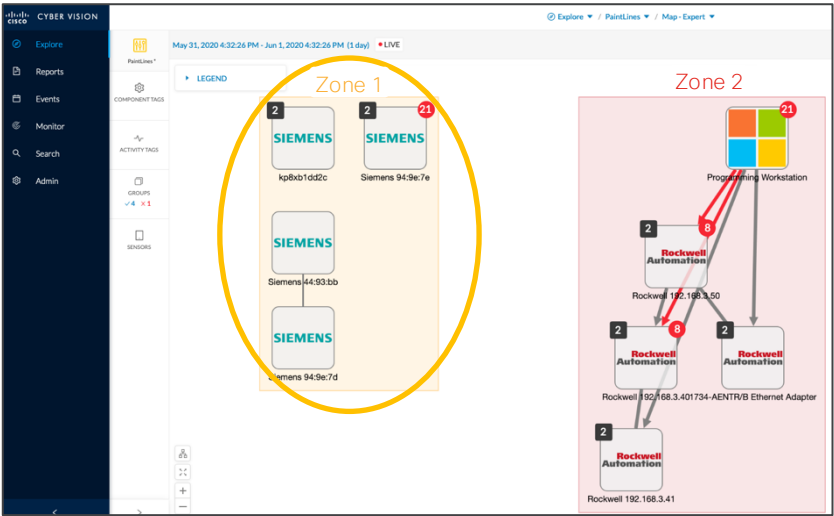
# Automated Segmentation Informed by Visibility



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



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

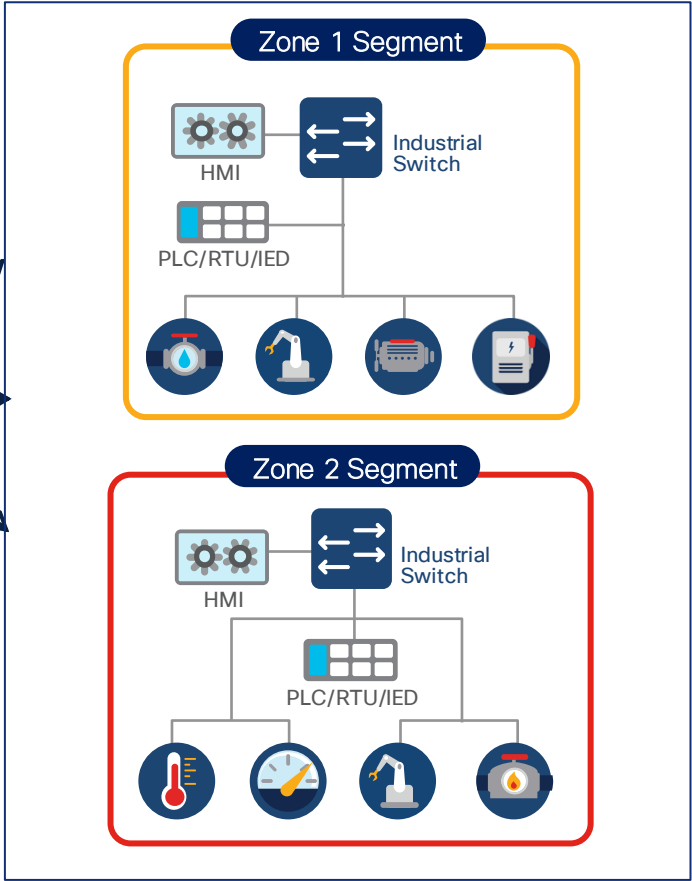


Cisco Cyber Vision Map View

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

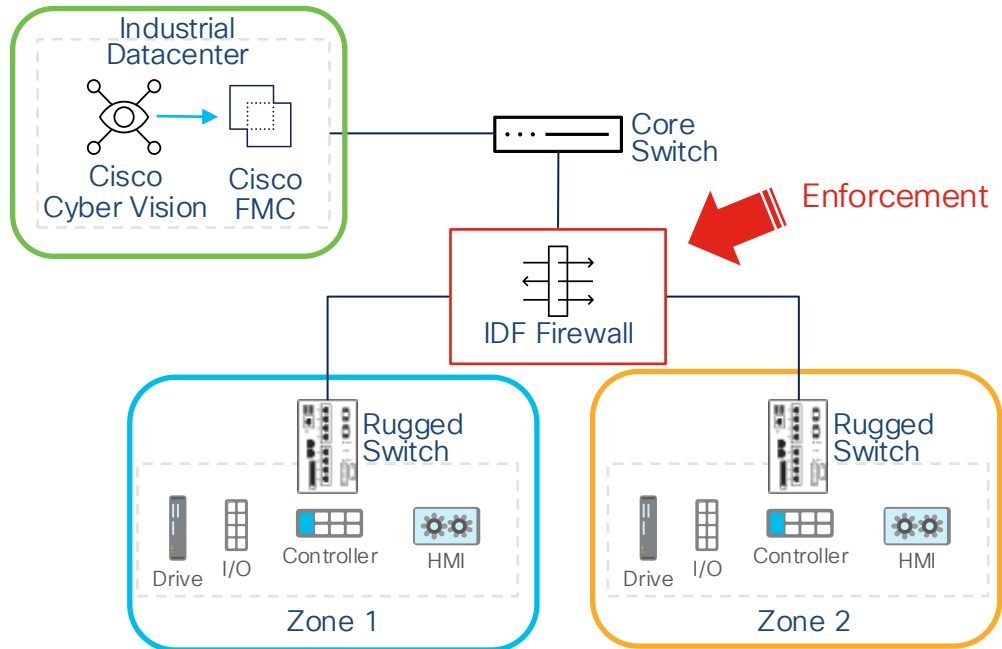
Cisco Firewall Policy Rules or Cisco ISE Policy Matrix

Segmentation of industrial network



dACL  
SGT  
VLAN

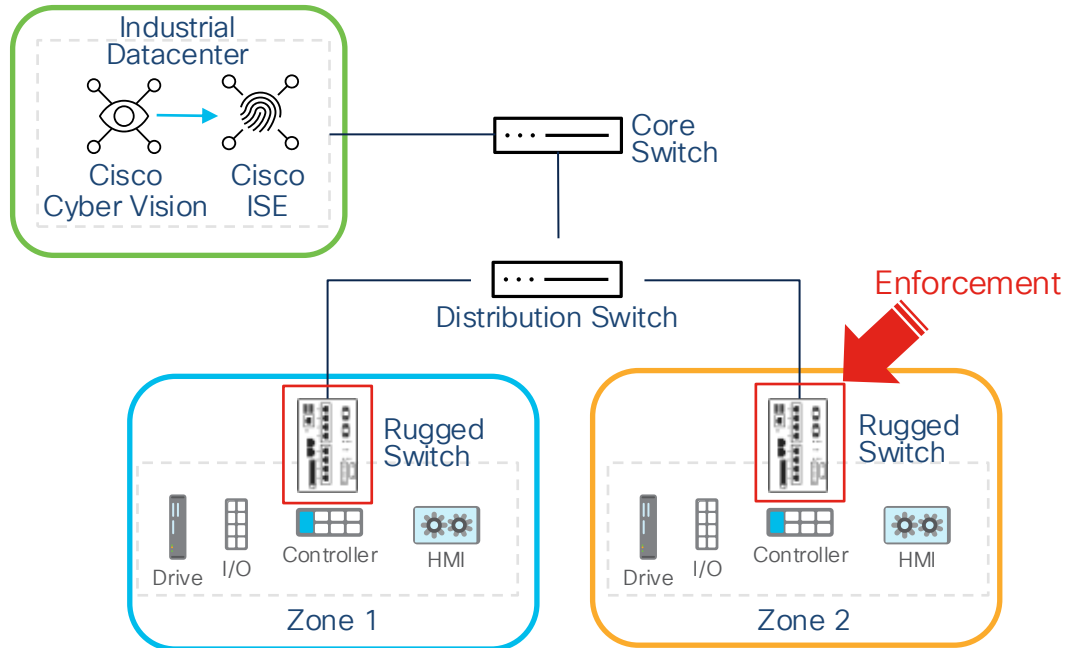
# Automated Segmentation **Enforced using Firewalls**



- All VLANs in the OT network terminate at the firewall installed in the distribution network (IDF)
- Traffic that crosses VLAN boundaries is subject to firewall rules
- Take advantage of application firewall rules such as enabling read only access across zones or denying specific OT commands
- Cisco Firewall Management Center (FMC) centralizes policy definition for all firewalls

Firewall policies automatically updated when OT modifies Cyber Vision groups

# Automated Segmentation **Enforced using Switches**



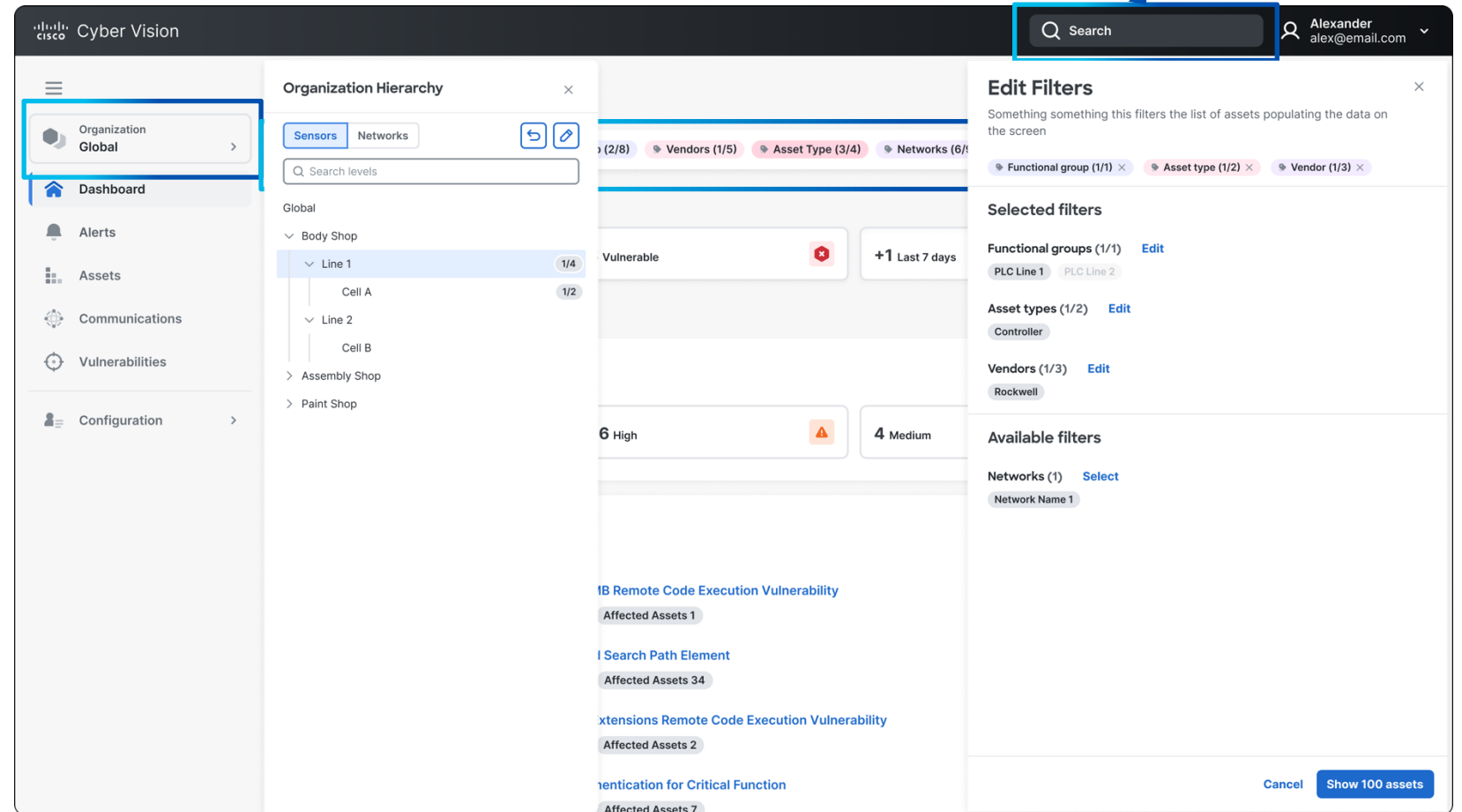
- Cisco Identity Services Engine (ISE) receives devices' profiles from Cyber Vision and associates a network access policy to each
- Policies are pushed to network switches for enforcement at the port level
- Network switches allow/deny assets to communicate based on their profile, not their IP address
- Deny by default is applied to assets not profiled

Network access policies automatically updated when OT modifies Cyber Vision groups

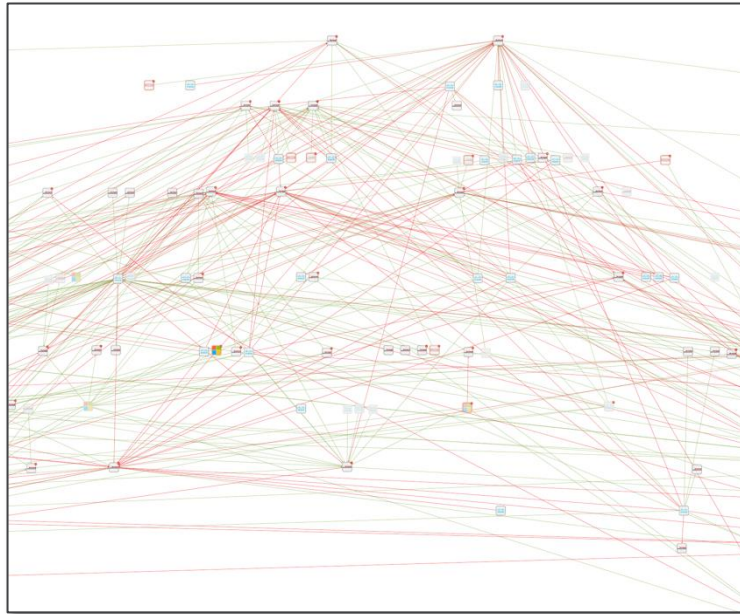
# Simplified Navigation

- **Hierarchy-based** navigation to organize your OT assets based on **subnets** or **sensor** placement
- **Filters** (Active View) to focus on **specific data**
- **Rapidly** find your asset with **Quick search**

Quick search



# AI-driven asset clustering

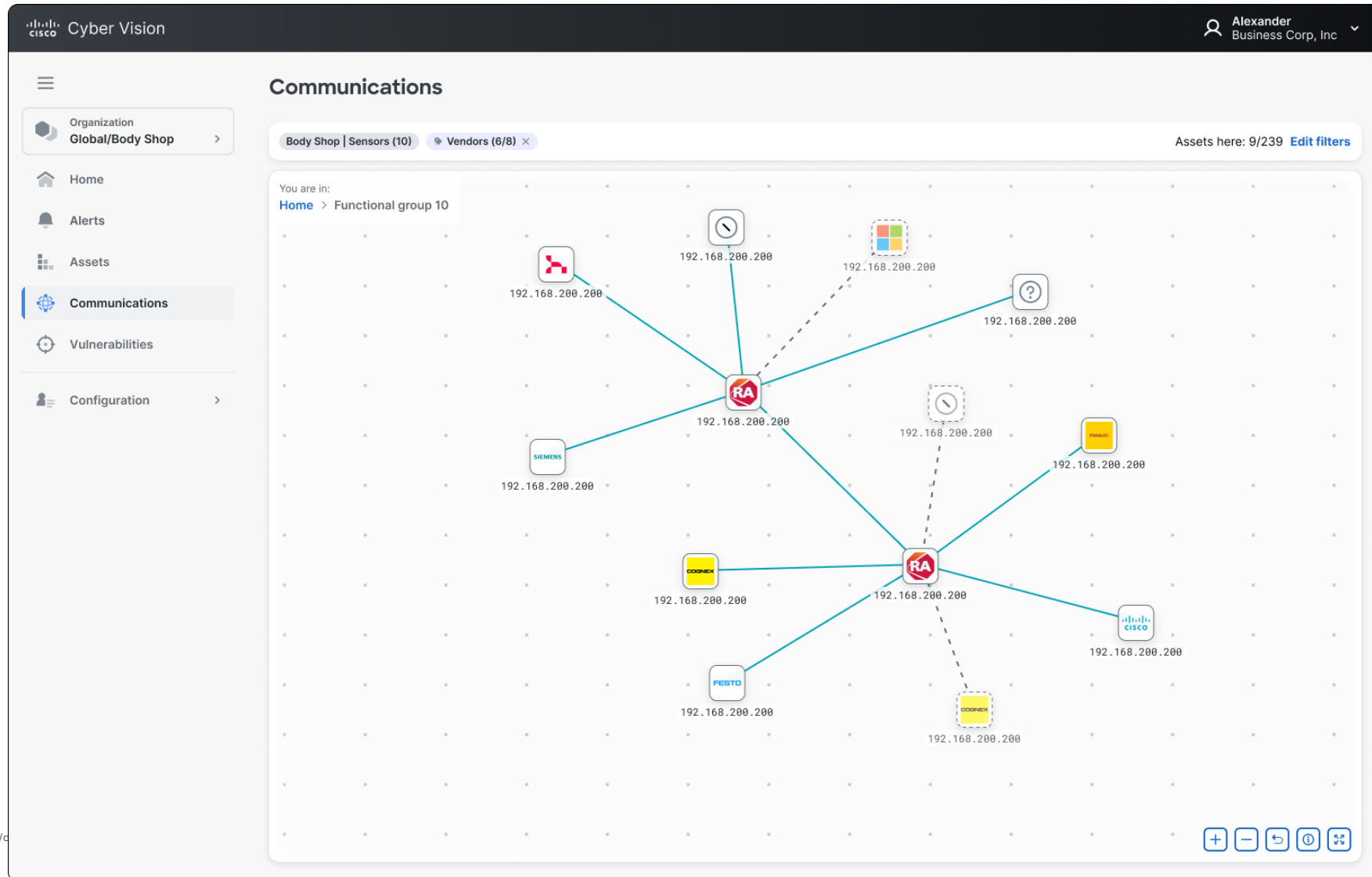


OT asset inventory projects highlight flat, unsegmented networks

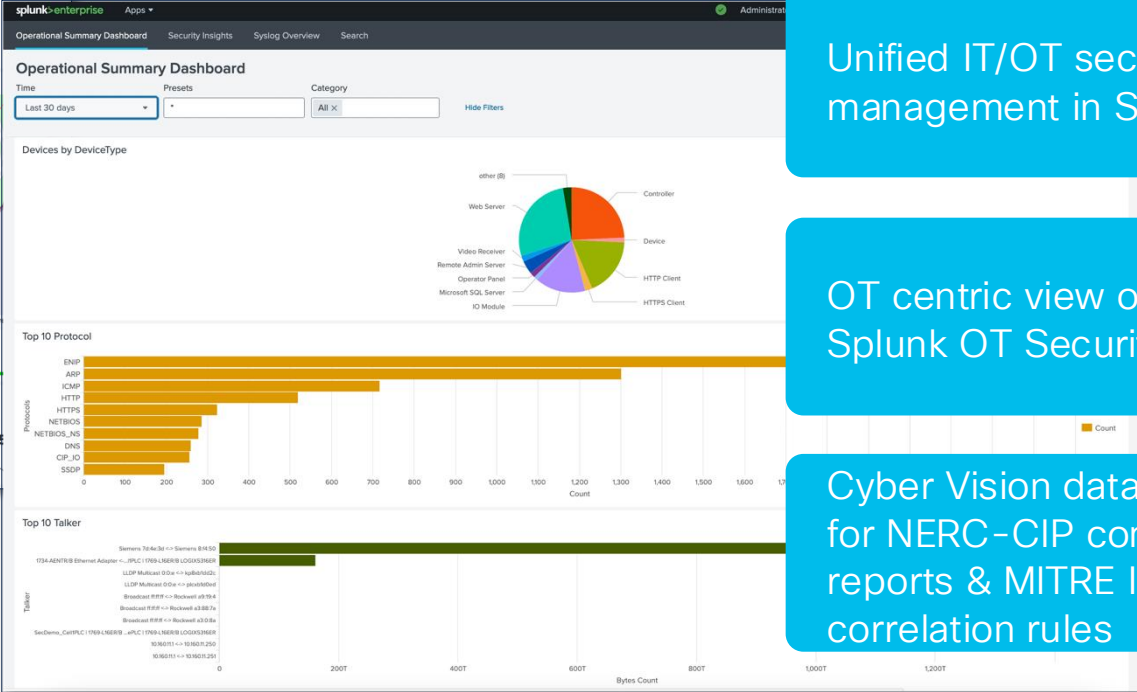
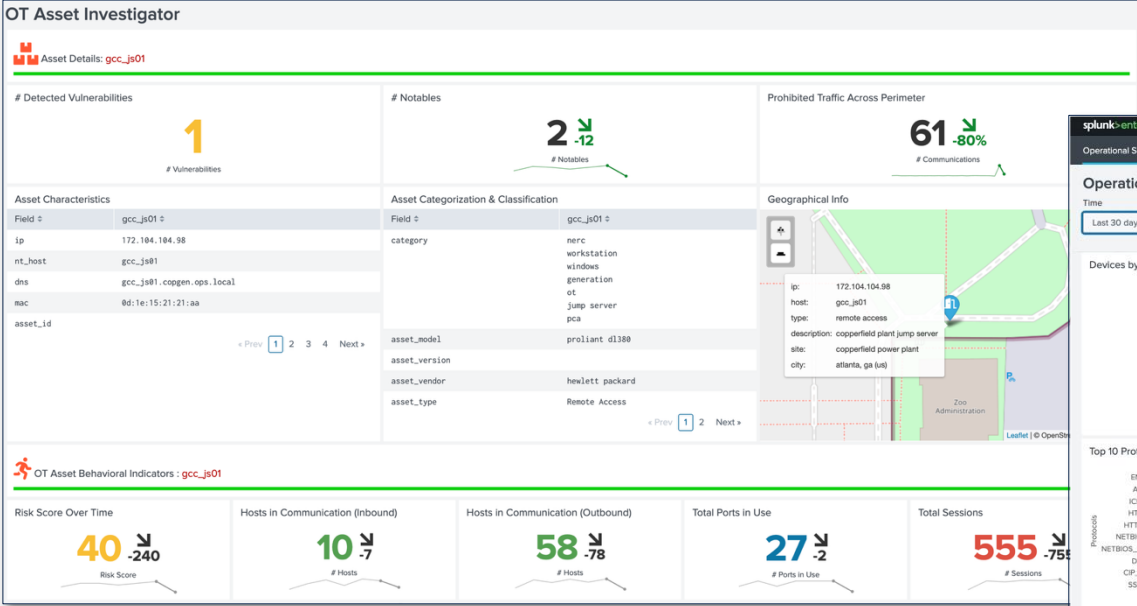


Cisco Cyber Vision ML-driven auto-grouping automatically creates security zones to drive network segmentation using Firewalls or NAC

# Internal group communication



# Splunk Integration



Unified IT/OT security events management in Splunk SIEM

OT centric view of assets in Splunk OT Security Add-on

Cyber Vision data in Splunk for NERC-CIP compliance reports & MITRE ICS correlation rules

## Syslog and REST API integration with Splunk SIEM and OT Security Add-on

