



Cisco Cyber Vision

TDM Overview for Cyber Vision 5.4

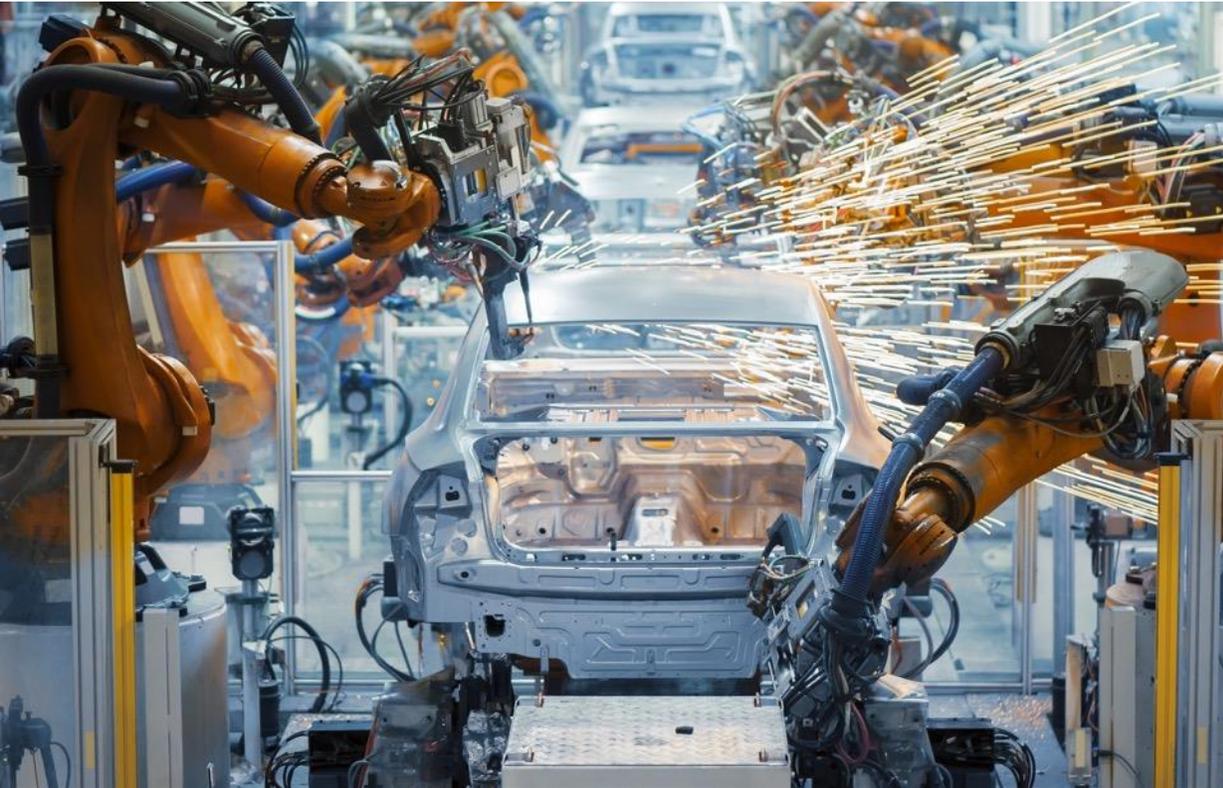
January 2026

Topics covered

- 1 Introduction
- 2 Architecture
- 3 Deployment
- 4 Performance
- 5 The Cyber Vision Workflow
- 6 Integrations
- 7 Licensing
- 8 Administration Features

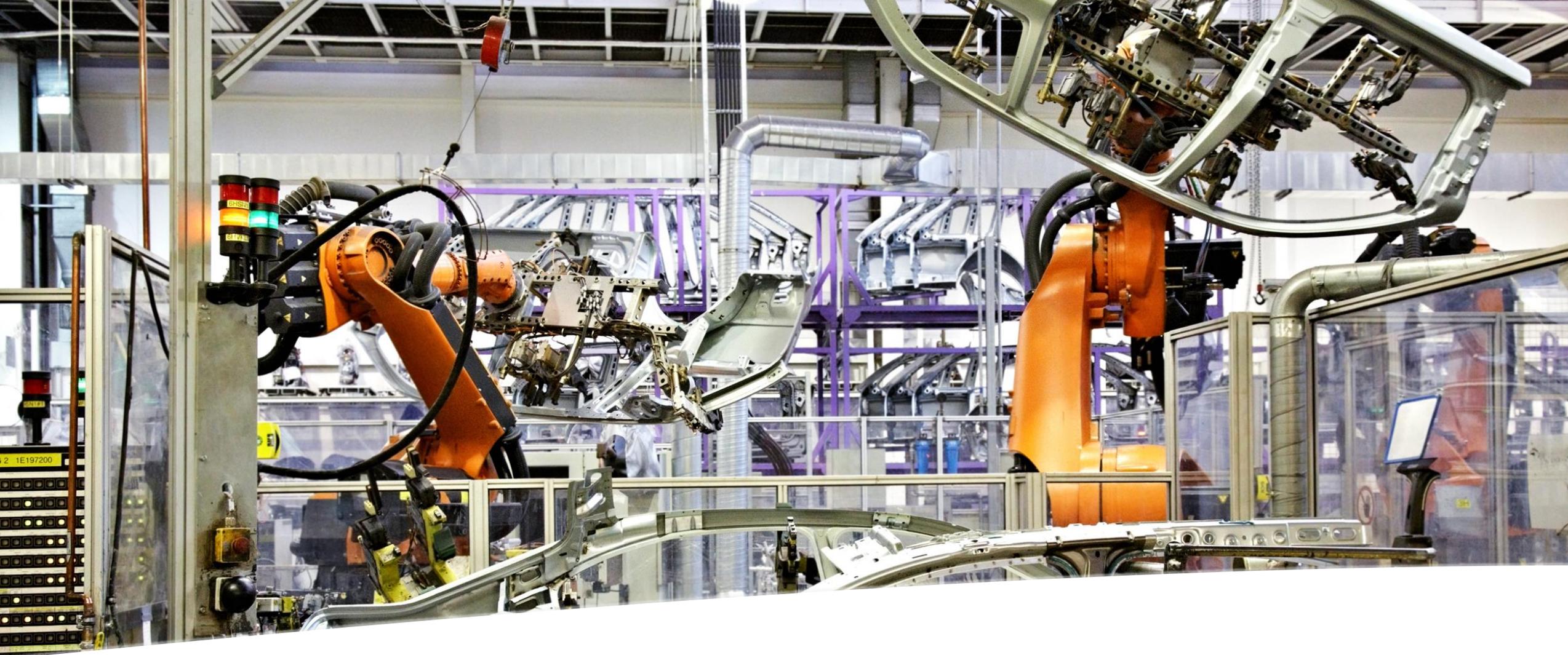


Industry Digitization Increases the Threat Landscape



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

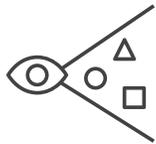
The role of IT is expanding to help secure industrial operations



IT's pain point: Lack of visibility into industrial control networks and connected devices

Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT



Visibility

OT asset inventory
Communication maps



Security Posture

Device vulnerabilities
Risk scoring to prioritize action



Zone Segmentation

Automate segmentation below
the IDMZ to protect operations

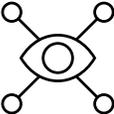
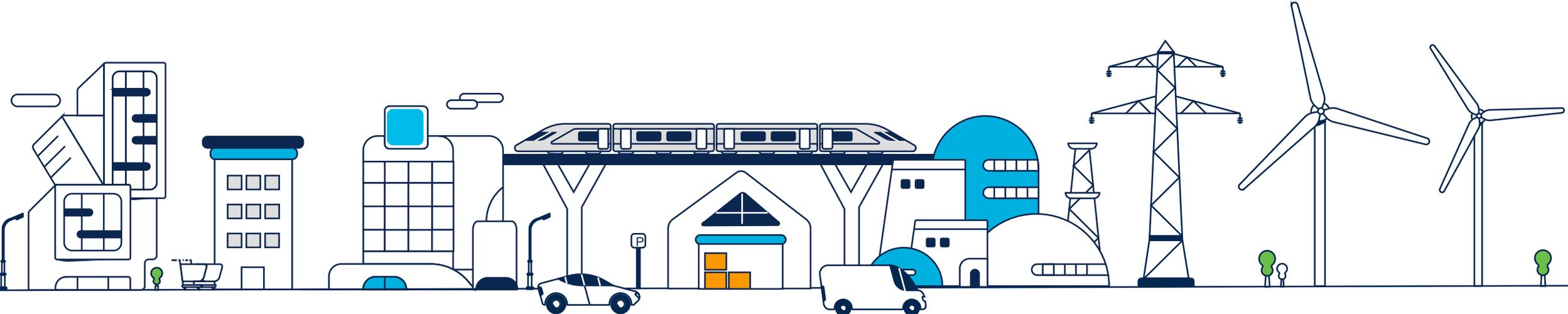


Secure Remote Access

Control risks from remote users
with zero-trust network access

OT security and secure remote access you can deploy at scale

Securing industrial operations starts with OT visibility



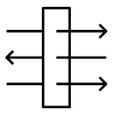
Identify OT assets and their communications



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 Industrial Threat Defense

Visibility

OT Asset Visibility and Security Posture

Cisco Cyber Vision

Network embedded visibility sensor

CV Switch

CV Router

Protection

Zero Trust Security for OT

Secure remote access (ZTNA)

Cisco Secure Equipment Access

Network embedded ZTNA gateway

IEC 62443 zone segmentation

Cisco Secure Firewall

Cisco ISE

Cyber Vision

Conduit

Zone-1

Zone-2

Network enforced segmentation

Response

Cross-Domain Detection, Investigation & Response

splunk >
a **CISCO** company

Visibility across the entire attack chain

Network as a fabric to secure OT at scale

Cyber Vision Architecture

Cisco Cyber Vision: Unique 2-Tier Architecture

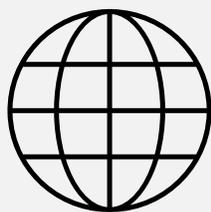
OT visibility that can be deployed at scale



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

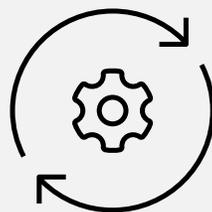
The role of the Cyber Vision Sensor

Collects Industrial Network Traffic



Captures industrial network flows (passive) and queries devices (active). Stores data locally in case the Center is not accessible

Decodes Industrial Protocols (DPI)



Understands most OT and IT communication protocols to analyze packet payloads and extract meaningful information

Sends Metadata to the Cyber Vision Center



Sends metadata to the Center for storage, analysis and visualization. This only adds 3 to 5% extra traffic to the network

Cisco Cyber Vision portfolio

Center

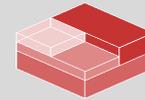
Hardware Appliance

UCS based servers with Hardware RAID

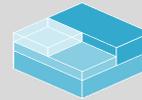


- CV-CNTR-M6N
- 24 core CPU
 - 128 GB RAM
 - 3.2TB drives

Software Appliance Virtual Machines



VMware
ESXi OVA



HyperV
VHD



Nutanix
HAV



Amazon Web
Services



Microsoft
Azure



Google Cloud

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



IE3300, IE3400,
and IE3500
Switches



IE3400HD and IE3500HD
IP67 Switch



Catalyst IR1101
Cellular Router



Catalyst IR1800
Cellular Router



Catalyst IR8300
Multiservice Router



Catalyst IE9300
Rugged Switches



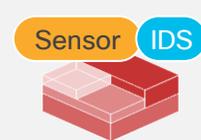
Catalyst 9300/9400
Aggregation Switches

Network Sensors

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



x86 or ARM64 compute
running Docker



x86 Compute
running VMWare



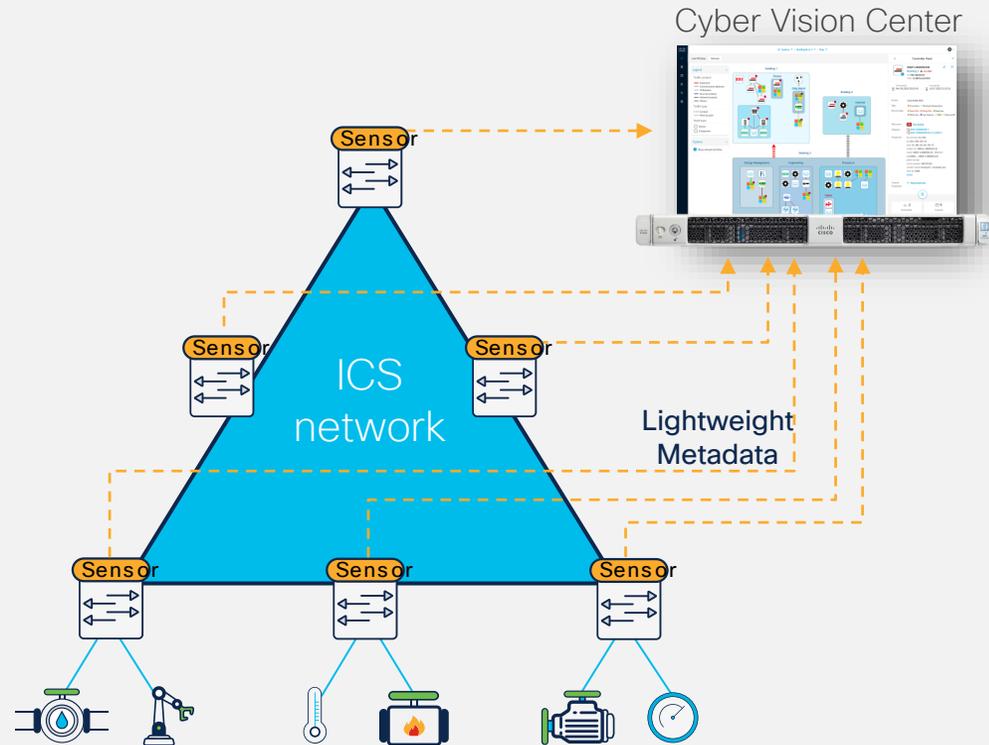
Cisco IC3000
Industrial Compute

Hardware Sensor

DPI and active discovery via SPAN to support brownfield

Cisco Cyber Vision

Visibility built into your network infrastructure

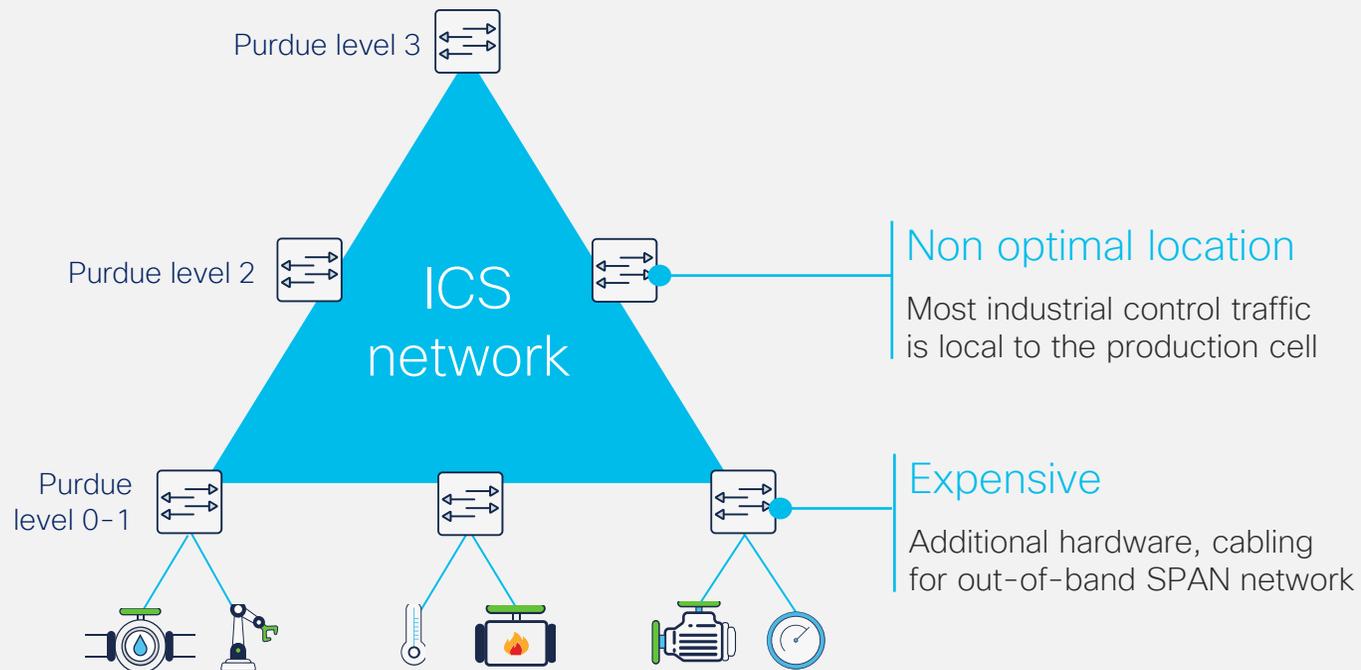


- ✓ Visibility sensor is a software feature running in select Cisco switches and routers
- ✓ No additional appliances needed
- ✓ No need for an out-of-band collection network
- ✓ Active discovery requests see pass NAT and firewall boundaries
- ✓ Centralized deployment and management
- ✓ No impact on network performance

The Cisco industrial network lets you see everything that connects to it

Why is a network-sensor important?

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



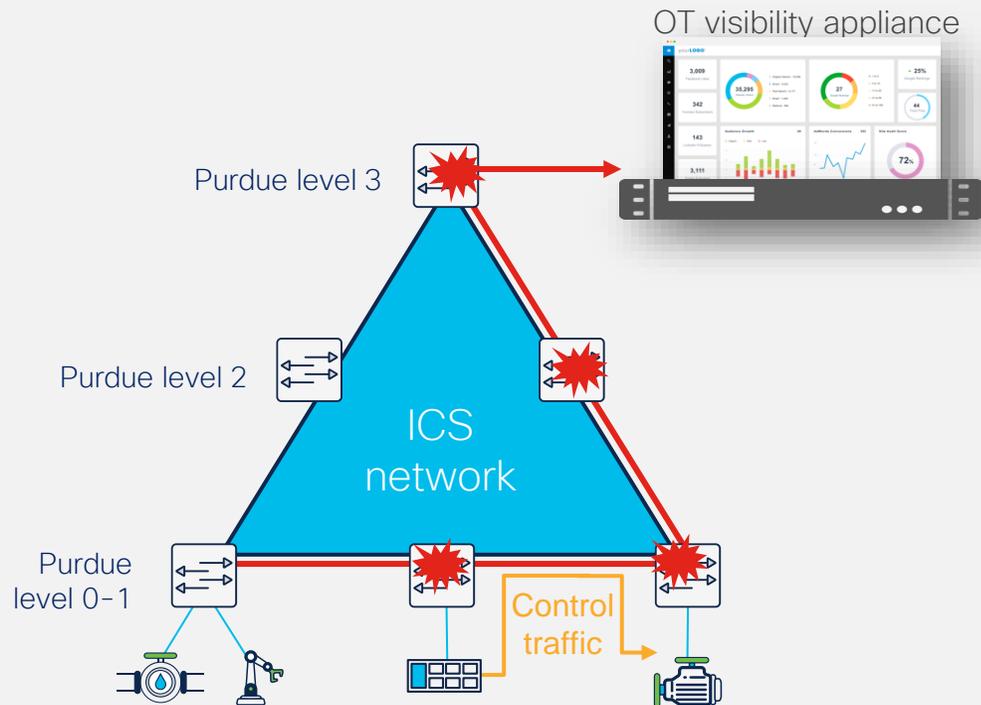
DPI location matters!

- Mirroring traffic at the aggregation layer results in visibility to North-South traffic only
- Mirroring traffic at the cell layer requires an expensive out-of-band SPAN network

Sensors embedded in the network see everything that attaches to it

Why is a network-sensor important?

RSPAN is not a viable option for control system networks



RSPAN introduces Jitter!

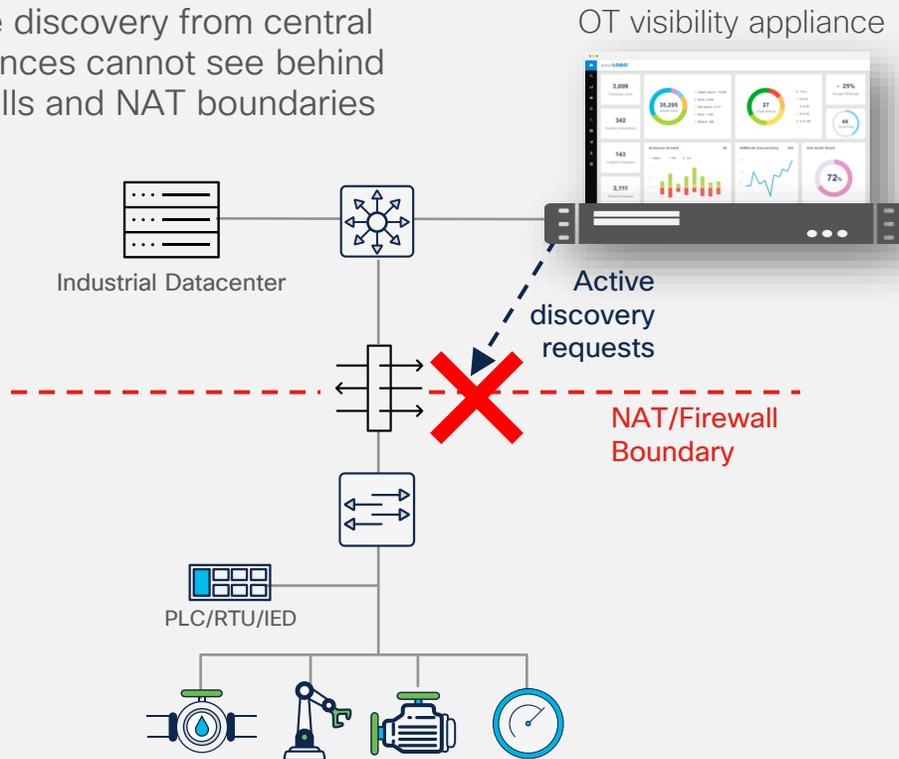
- Head-of-line blocking caused by Inline SPAN traffic negatively impacts time-sensitive control loop
- RSPAN in LANs is detrimental to control system performance

Sensors generate lightweight metadata that does not congest QoS queues

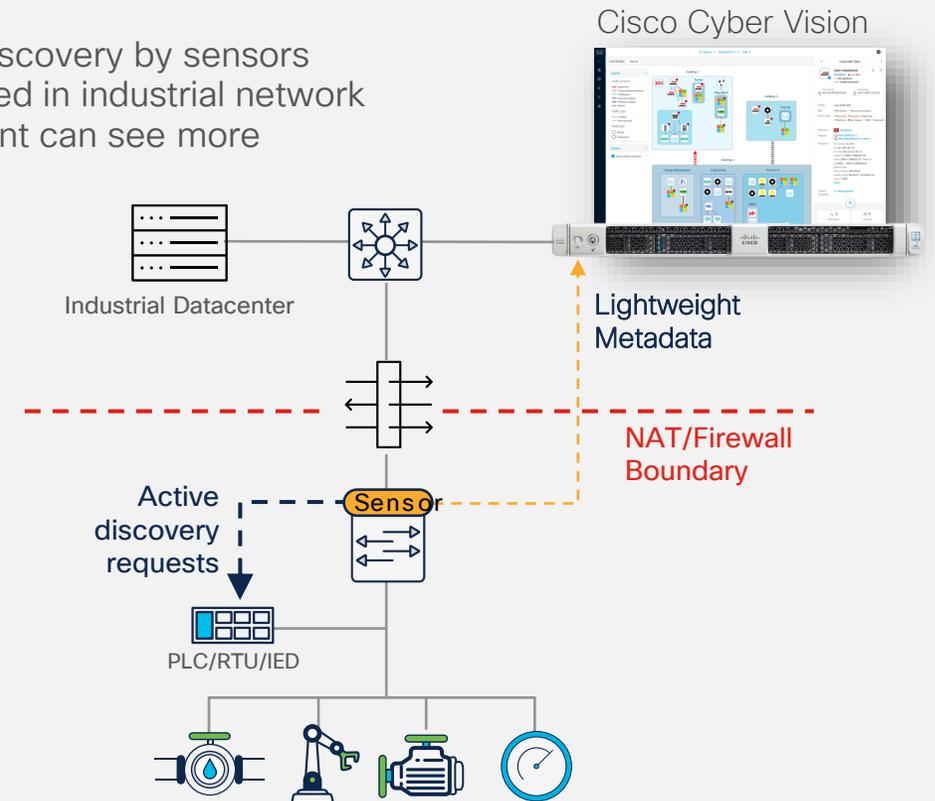
Why is a network-sensor important?

Distributed edge active discovery gives you 100% visibility

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



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



Sensors embedded in the network can see more

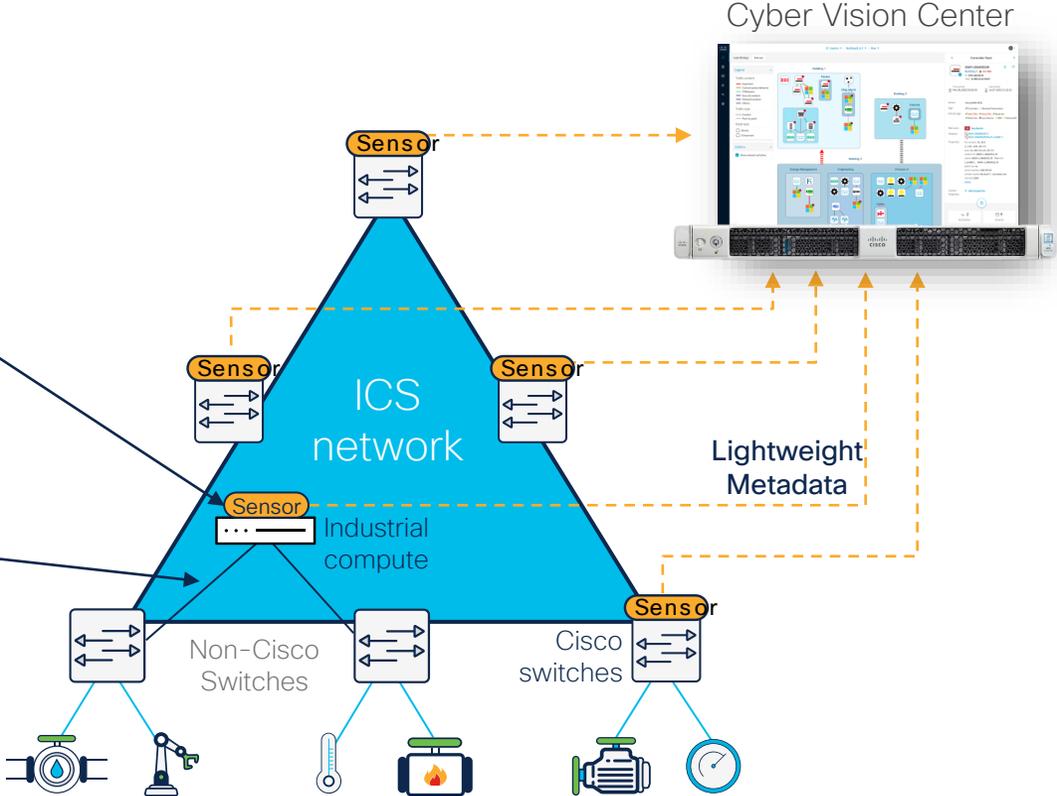
Cyber Vision hardware-sensor connects legacy switches to the OT security infrastructure

Hardware sensor
has low TCO

Low-cost appliance to deploy
everywhere DPI cannot be embedded

Only 1-hop of SPAN traffic

No need for additional network resources to
collect traffic and send data to the console



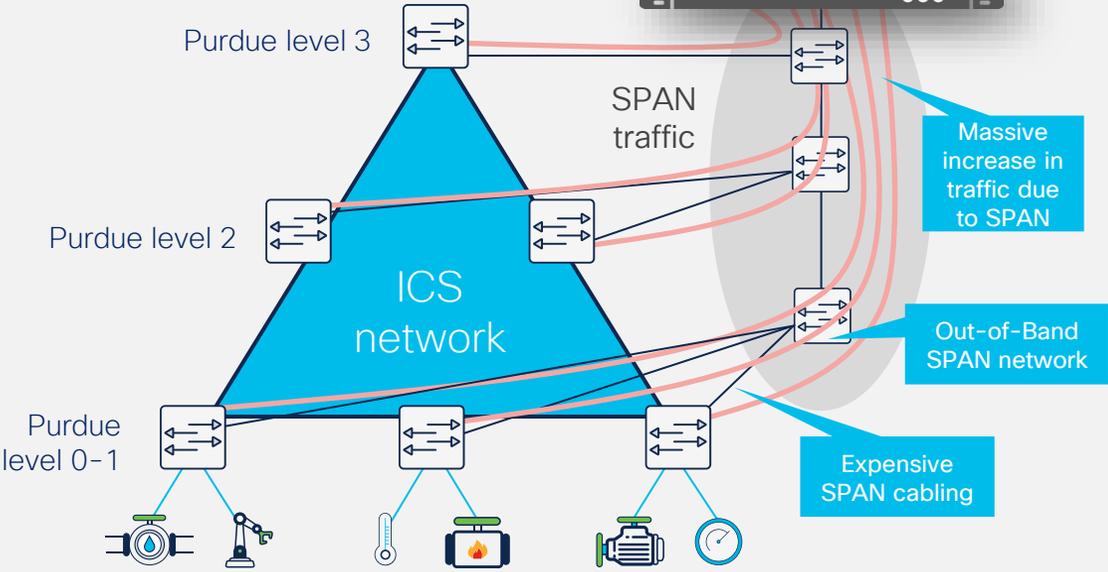
Cisco Cyber Vision works great with third-party switches



Cyber Vision scalable architecture

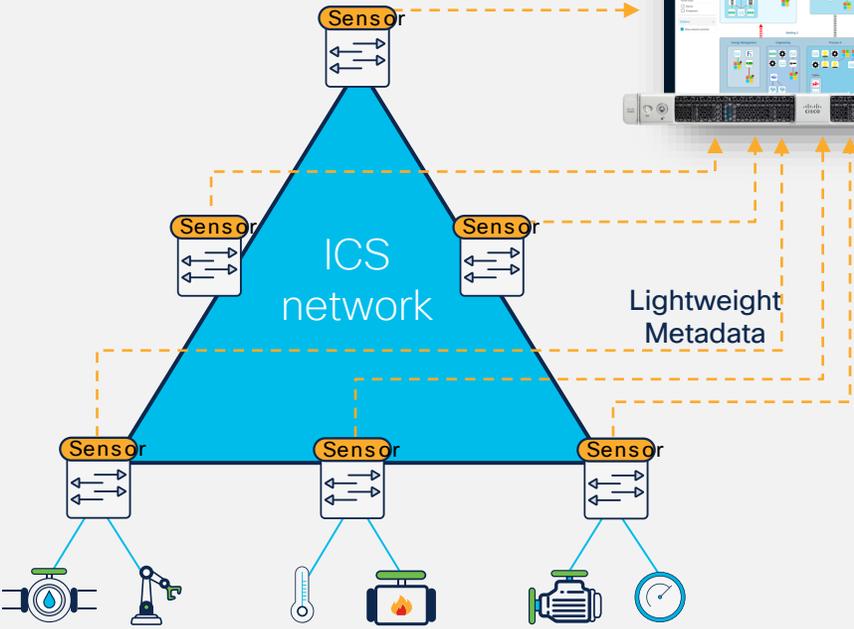
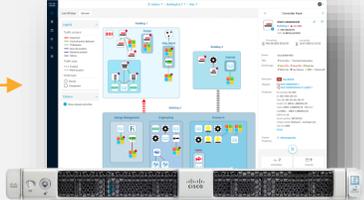
SPAN based solutions incur huge additional hidden-costs

OT visibility appliance



Your network sees everything that attaches to it, eliminating the need for SPAN

Cyber Vision Center



On-Center Sensor offers extra deployment flexibility

Central DPI and IDS capabilities

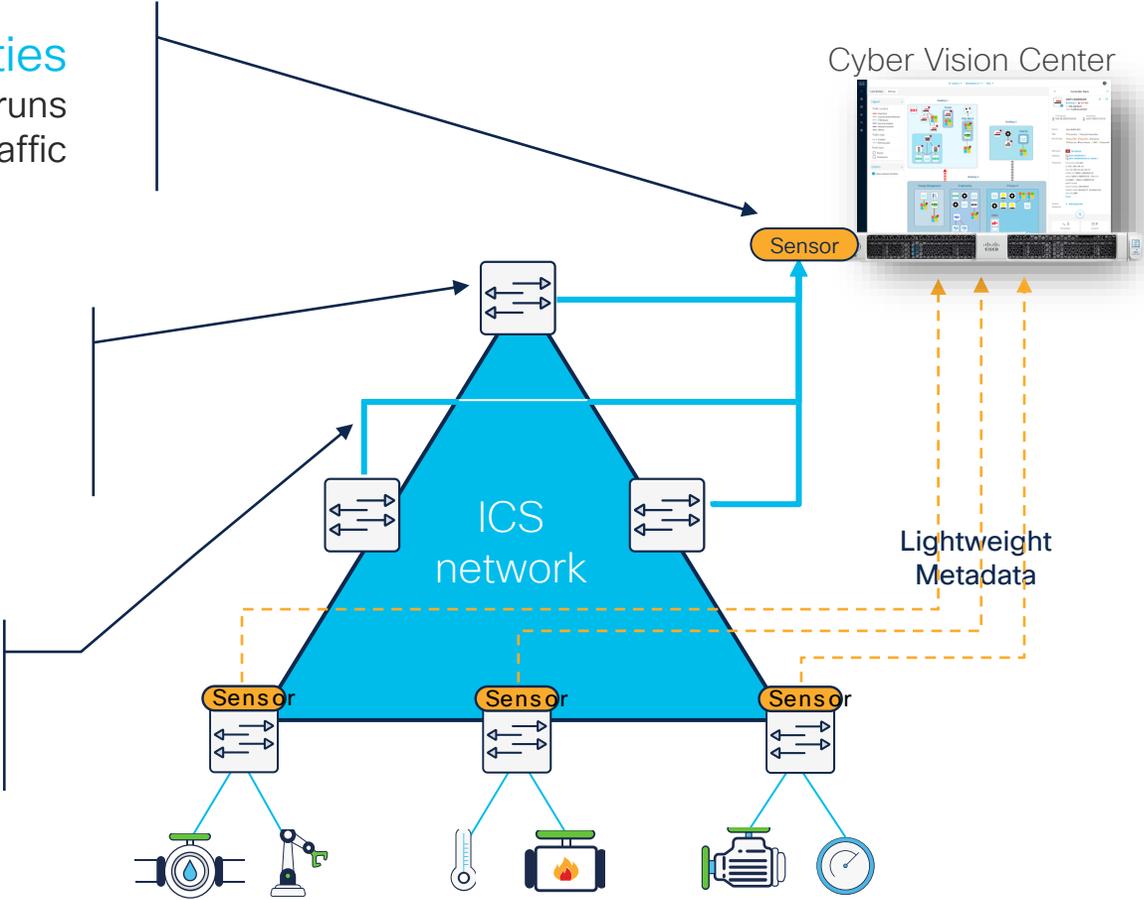
Sensor built into the Cyber Vision Center runs DPI and IDS on raw industrial network traffic

Collect traffic from the datacenter

Needs only 1-hop SPAN from the aggregation switch to the Cyber Vision Center

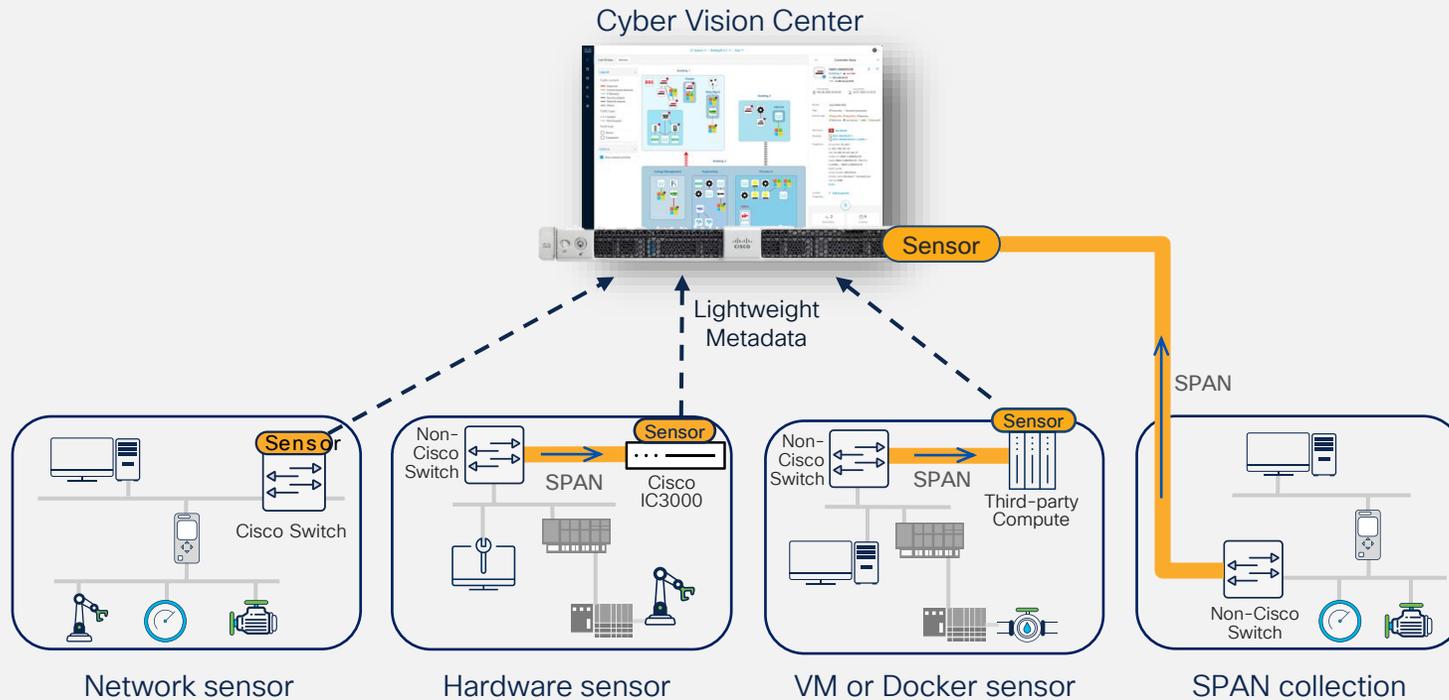
Leverage existing SPAN infrastructures

Makes deployment super easy if the collection network is already in place



Cisco Cyber Vision

Implementing OT visibility at the lowest TCO

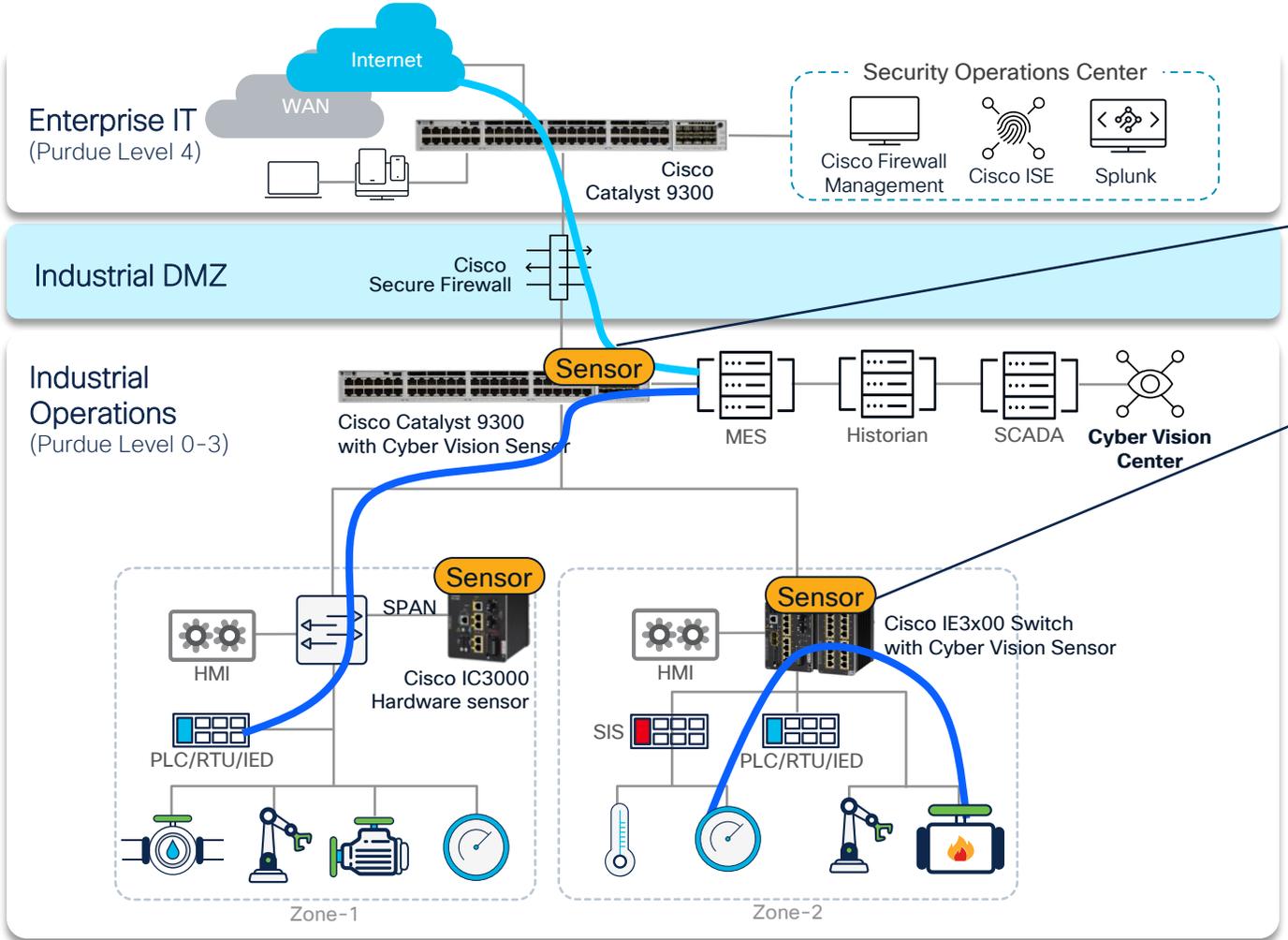


- **Network sensors** embedded in Cisco networking for simple and highly scalable deployments
- **Hardware or Virtual sensors** capturing traffic on any switch with a single hop SPAN to support brownfield deployments
- **On-Center sensor** to leverage existing SPAN infrastructures, or collect traffic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

Cyber Vision scales across brownfield and greenfield environments

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!

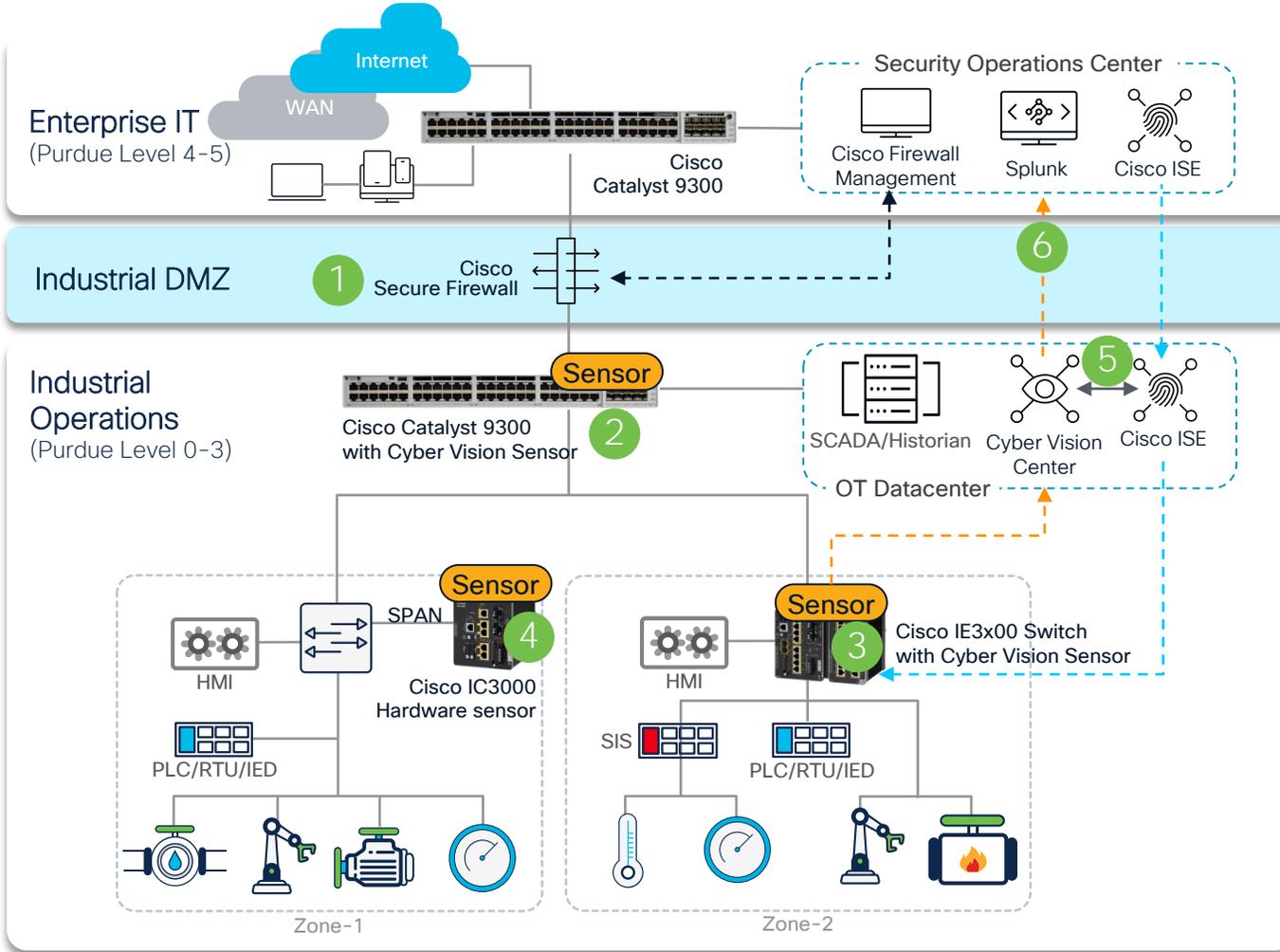
Rule of thumb: All flows must go through at least one sensor. Every networking equipment should have a sensor.

Cisco Cyber Vision in Manufacturing

IT

IT/
OT

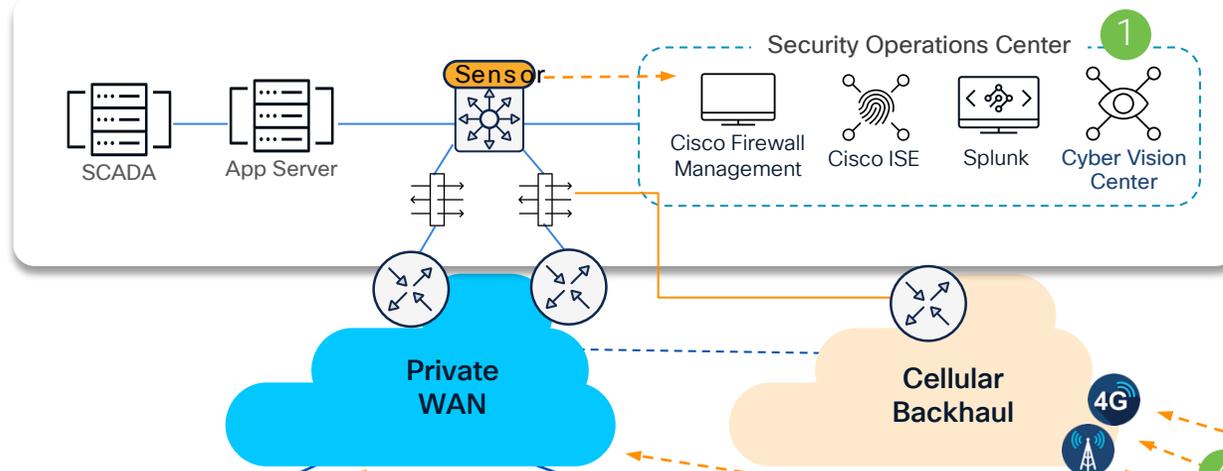
OT



- 1 Isolate IT and OT by installing an industrial DMZ with Cisco Secure FW
- 2 Create macro-segmentation zones in the Catalyst 9300 switches and deploy Cyber Vision sensors with Snort IDS.
- 3 Cyber Vision sensors deployed within segments across IE3x00 switches
- 4 Cyber Vision hardware-sensors deployed via one-hop SPAN to gain visibility on non-Cisco switches
- 5 Build zones and conduits in Cyber Vision and share with ISE for micro segmentation
- 6 Cyber Vision shares details on OT devices and events with SOC to build informed security policies and investigate threats across domains

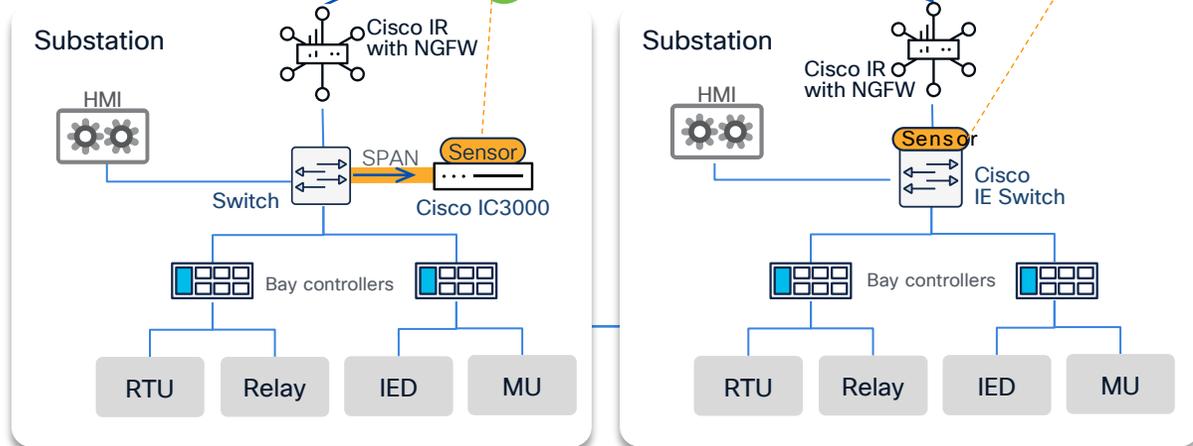
Cisco Cyber Vision in Electric Utilities

Data Center / Control Center

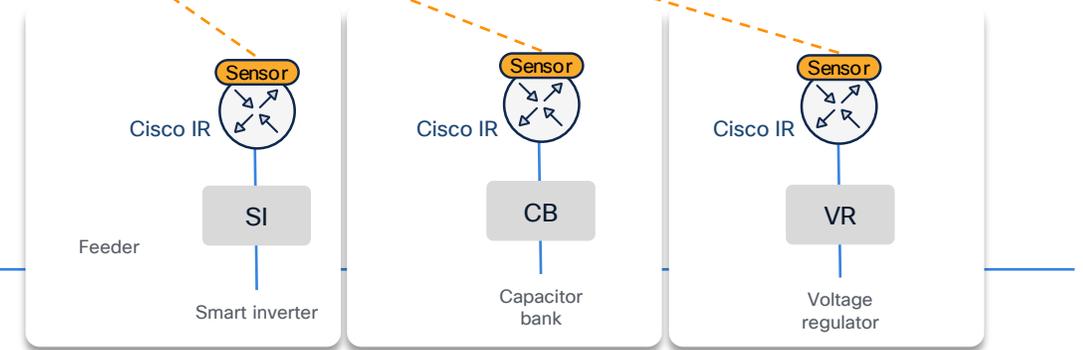


- 1 Cyber Vision Center deployed at Control center
- 2 Cyber Vision Sensor embedded in IE3x00 switches or deployed via one-hop SPAN on Cisco IC3000 in transmission substations
- 3 Cyber Vision Sensor embedded in Cisco Industrial Routers in the distribution grid
- 4 Application-flow streamed from sensors to center over utility private WAN connecting transmission substations and over cellular backhaul from the distribution grid

Transmission Grid

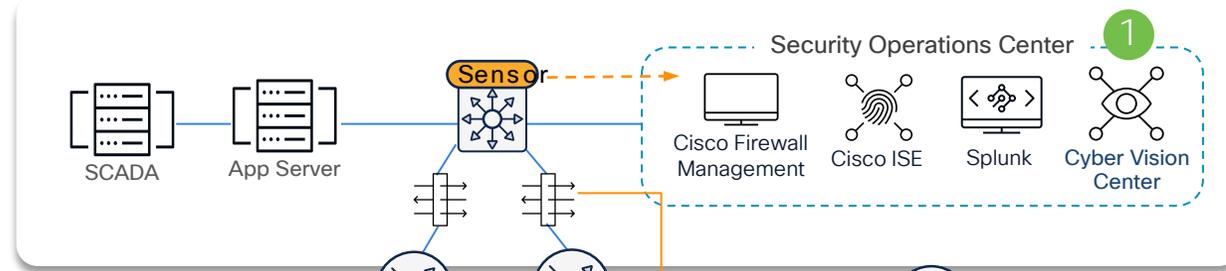


Distribution Grid

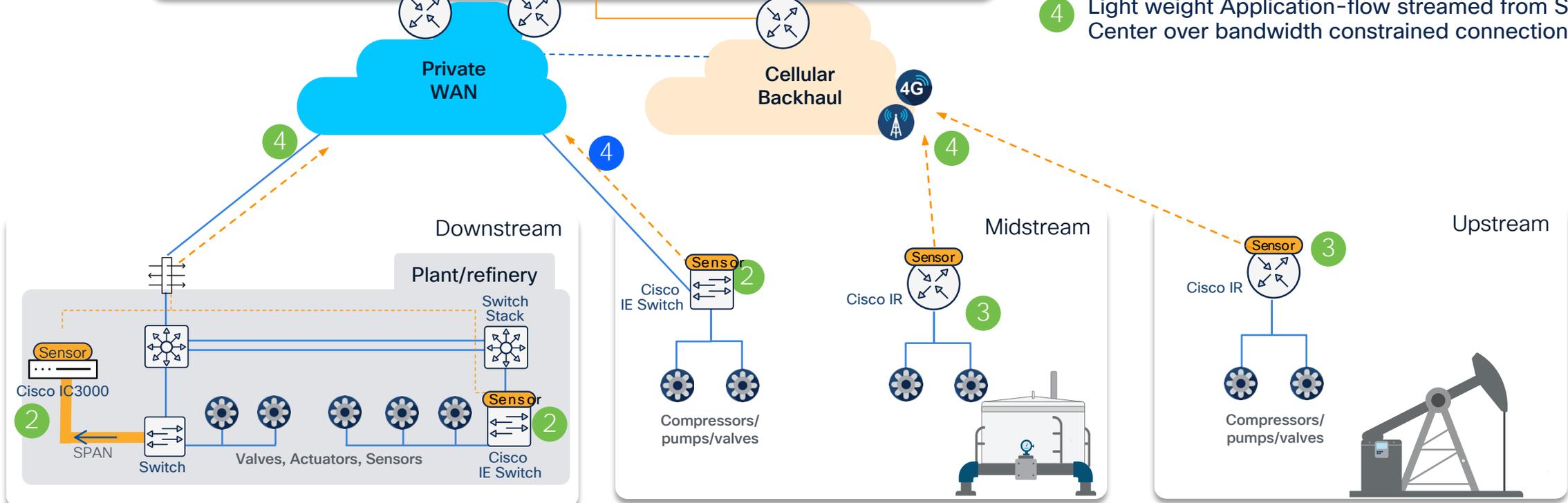


Cisco Cyber Vision in Oil and Gas

Data Center / Control Center



- 1 Cyber Vision Center deployed at Control center
- 2 Cyber Vision Sensor embedded in IE3x00 switches or deployed via one-hop SPAN on Cisco IC3000 in Downstream, Midstream and Upstream
- 3 Cyber Vision Sensor embedded on directly on Cisco Industrial Routers for distributed applications
- 4 Light weight Application-flow streamed from Sensors to Center over bandwidth constrained connections



Where to place the Cyber Vision Center?

Plant-based industries



Manufacturing, Water treatment...

One Center per plant in Level 3
Gives local IT/OT teams visibility and operational insights on their assets

One Global Center at HQ
Gives SOC & CISO teams aggregated visibility across all sites

Infrastructure-based industries



Grid substations,
Roadways, Pipelines...

One Center per Control Center
Gives IT/OT teams visibility and operational insights across all distributed assets

Distributed Edge Asset Discovery



Cyber Vision offers comprehensive asset discovery technologies



Passive Discovery
Leveraging deep
packet inspection (DPI)



Broadcast Active
Discovery



Unicast Active
Discovery

Passive + Active asset discovery

Passive Discovery

- Builds visibility by listening to network traffic
- No interaction with industrial assets
- Edge sensors see cell traffic without SPAN networks

Active Discovery - Optional

- Learns the ICS protocols at play from passive discovery
- Sensors send hello requests to discover silent devices
- Gets comprehensive details on every asset



Closed-loop
enabling 100%
visibility without
disruption

Distributed Edge Active Discovery Features

Features



Enabled by user, fully passive by default



Closed loop control - Passive collection informs active discovery



Wake up broadcast messages



Active discovery performed by the sensor



Active discovery using S7, S7Plus, Profinet, EtherNet/IP, DNP3, SNMP, ICMPv6, WMI, etc.

Benefits



No risk of disrupting industrial assets



Assets are not flooded with ARP requests. Cyber Vision does not scan networks.



Discover silent devices. 100% visibility



Passes firewalls and NAT boundaries. 100% visibility

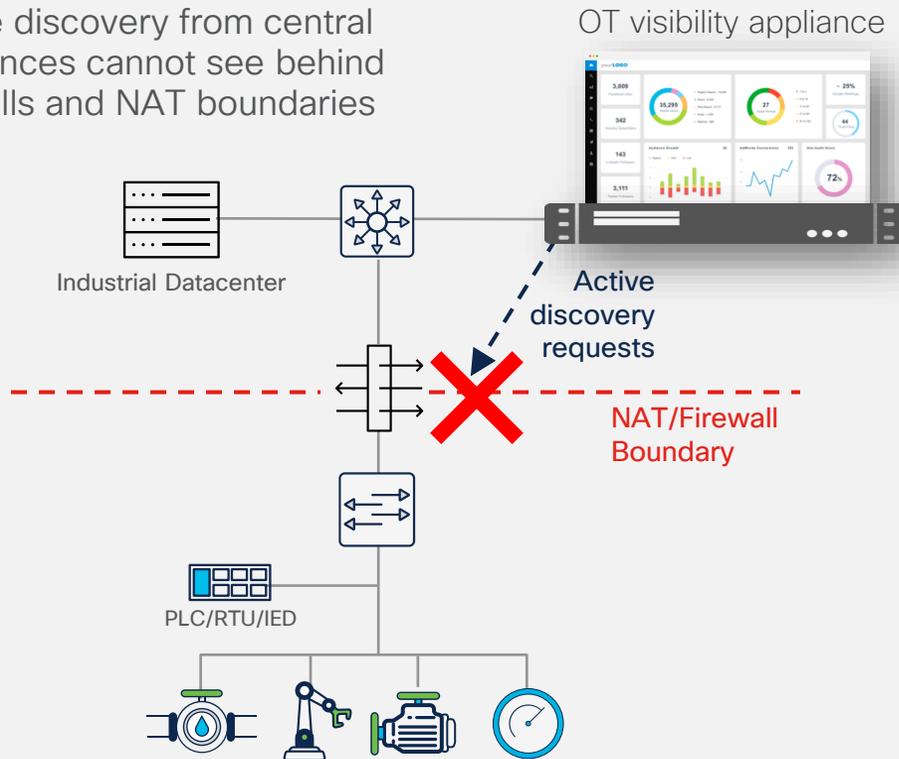


100% visibility of Rockwell, Schneider, Siemens assets and Windows machines

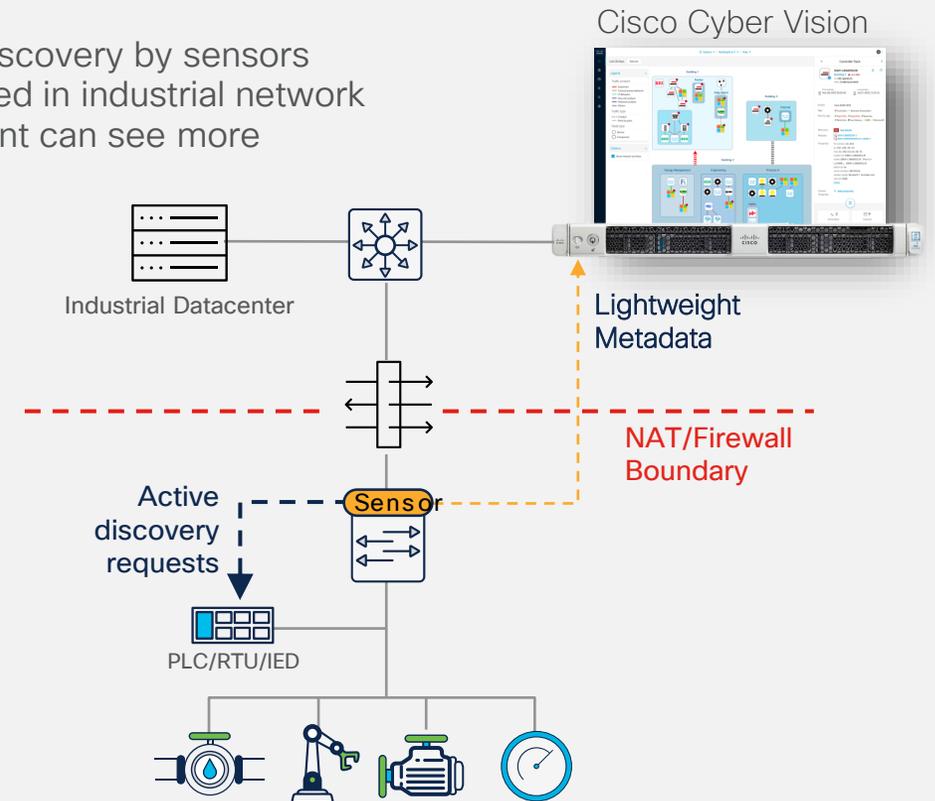
Why is a network-sensor important?

Distributed edge active discovery gives you 100% visibility

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



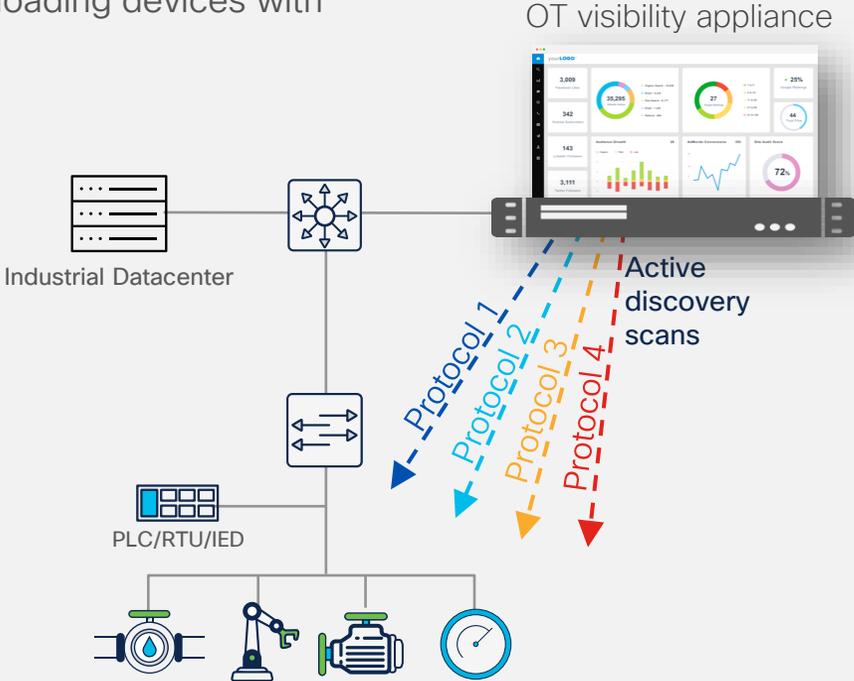
Active discovery by sensors embedded in industrial network equipment can see more



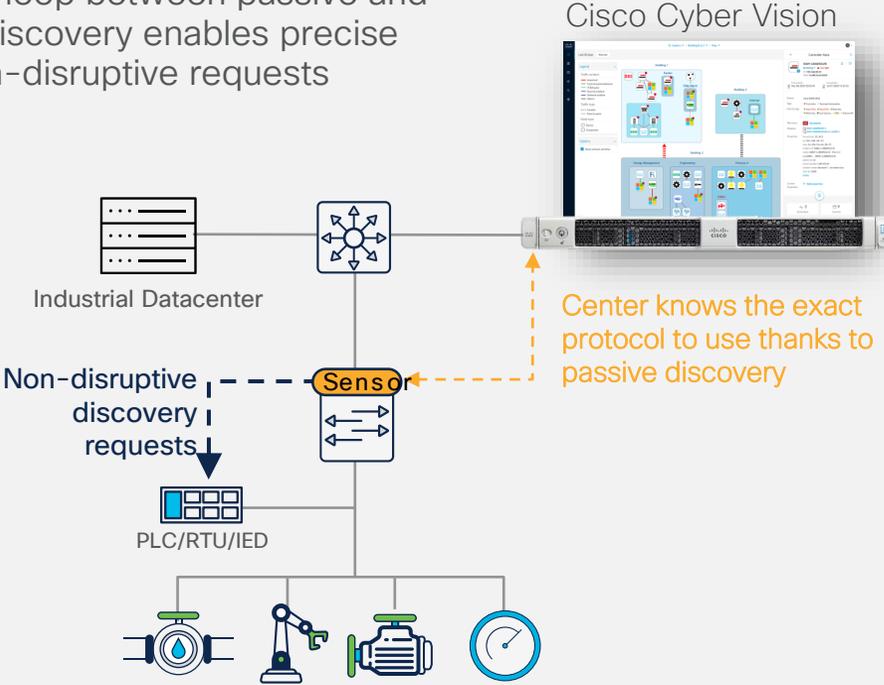
Sensors embedded in the network can see more

Closed-loop control makes active discovery safe

Basic active discovery solutions scan networks overloading devices with ARP requests

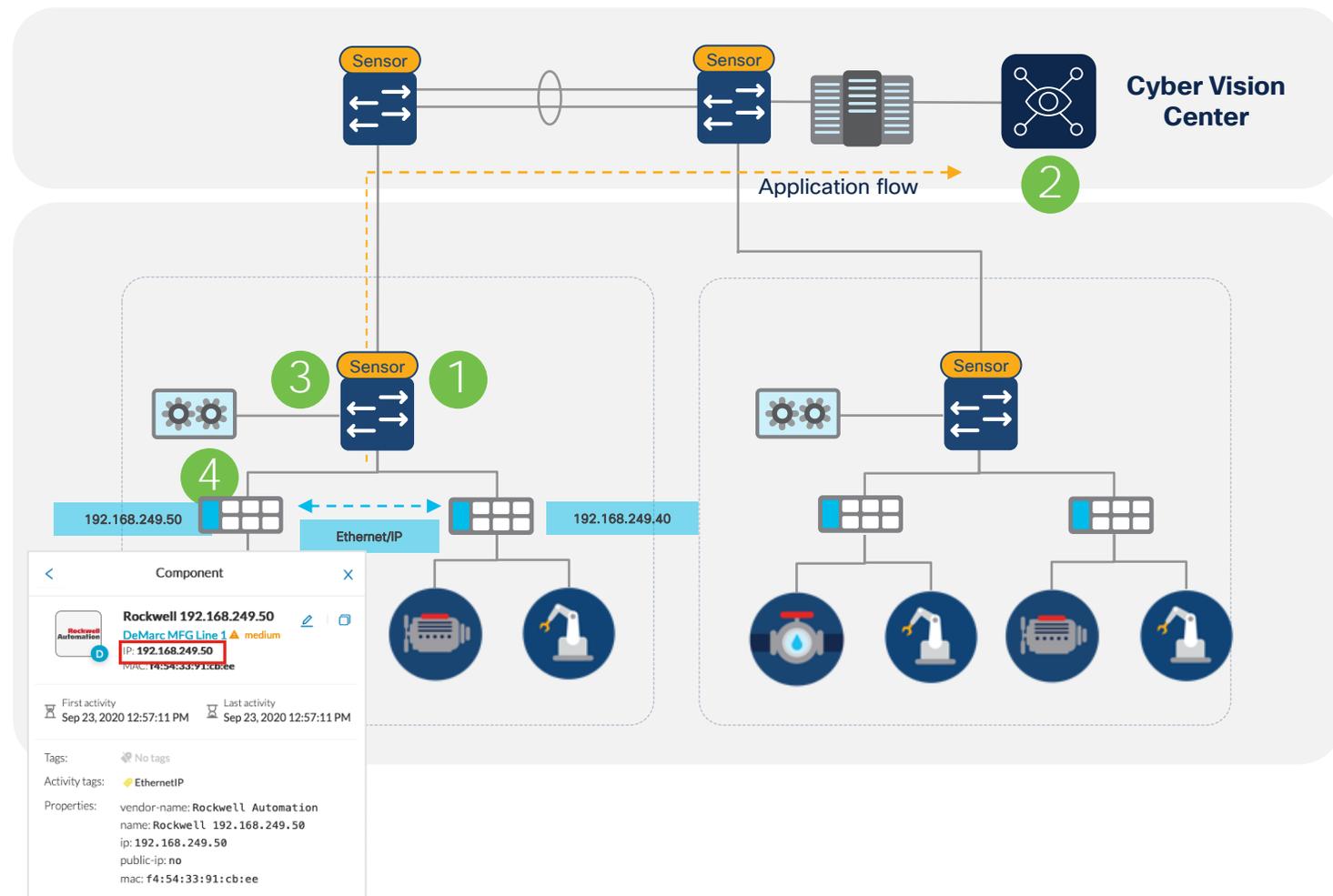


Closed-loop between passive and active discovery enables precise and non-disruptive requests



Active Discovery Closed Loop Control

- 1 Sensor observes known protocol (i.e. Ethernet/IP)
- 2 Center has limited knowledge about device due to limited identity information in traffic
- 3 Center instructs Sensor to perform an active discovery with observed protocol (i.e. Ethernet/IP)
- 4 Device responds with identity information and Sensor sees response



Cyber Vision active discovery keeps you in control

- You choose!
 - Some or all protocols
 - Some or all sensors
- Cannot be activated by accident



Active Discovery Activation

- Choose mode during Sensor install
- No accidental activation of active discovery
- Enabled per protocol via sensor configuration template
- Full user control over discovery traffic

Configure Active Discovery

Please select an application type. If you want to enable Active Discovery on the application, select "Passive and Active Discovery". You will have to add some network interfaces parameters.

Passive only
 Passive and Active Discovery

Add Active Discovery configuration

Use collection interface
[+ New network interface](#)

IP address*

IP address interface used to do Active Discovery and/or SEA

Prefix length*

Like 24, 16 or 8

VLAN number*

Use 1 by default

Network interfaces

- 192.168.170.99/24 VLAN#1 [delete](#)

Unicast Active Discovery

- Cyber Vision Sensors can send unicast messages to devices or broadcast based on configuration
- Unicast discovery offers better visibility compared to broadcast discovery and is not as limited by network architecture or sensor placement
- Enables advanced discovery inquiries such as backplane configurations

Defining Active Discovery Profiles

Step 1: Creating Policies

A policy includes a set of protocols

- Policy1
 - Protocol A with its parameters
 - Protocol B with its parameters
- Policy2
 - Protocol A with its parameters
 - Protocol B with its parameters
 - Protocol C with its parameters
- ...

Step 2: Creating Profiles

Defining where / what / when

A profile is defined by:

- A policy which defined protocols to use
- Some targets for unicast:
 - From one or several preset(s)
 - From a list of IPs
- One or several sensors to use
- A schedule

Creating Active Discovery Policies

Define and configure protocols which could be used in a profile

- Selection of Broadcast and Unicast protocols
- Configuration of each protocol
- Retries
- Security parameters

✕ Create a policy

* Name:

Broadcast configuration

<input type="checkbox"/> Beckhoff	<input type="checkbox"/> EtherNet/IP	<input type="checkbox"/> ICMPv6
<input type="checkbox"/> Profinet	<input type="checkbox"/> SiemensS7	<input type="checkbox"/> BACnet
<input type="checkbox"/> HiDiscovery	<input type="checkbox"/> ABB NetConfig	<input type="checkbox"/> Codesys
<input type="checkbox"/> SiemensLogo	<input type="checkbox"/> SSDP	<input type="checkbox"/> WSDiscovery

Unicast configuration

▼

Advanced settings

Broadcast retry:

Unicast timeout (in seconds):

Broadcast timeout (in seconds):

Creating Active Discovery Profiles

- Configure targets
 - Sensor to use
 - List of IPs to discover
- Configure schedule
 - Reoccurring
 - Run once

CREATE AN ACTIVE DISCOVERY PROFILE ✕

* Name:

* Discovery policy:

Target ⓘ Clear all targets

IPs from presets:

IP targets ⓘ:
[+Add a target IP](#)

* Sensors:
 Use all sensors available ⓘ

Schedule

Schedule periodic discoveries:

Time Range ⓘ: →

* Frequency:

Schedule Reoccurring or Run Once

Schedule Active Discovery to run based on day of the week and time of day

OR

Choose Run once to save and trigger a discovery to occur within 30 seconds

Schedule

Schedule periodic discoveries:

Time Range: Thursday Mar 16th 2023 02:00 PM → End Time (optional)

* Frequency: Select a frequency

- Hourly
- Daily
- Weekly
- Monthly

Paint-Active1-unicast-daily

Target:

- Preset: Paint

Discovery Policy: Active1-unicast

Sensors: All sensors are selected

Scheduling: **Scheduled**

Start time: March 11, 2023 10:00 AM

Periodicity: Weekly

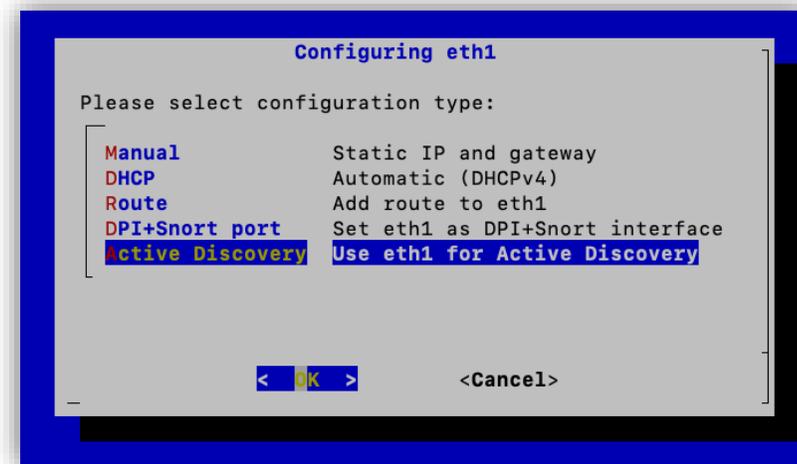
Actions:

[Edit](#) [Delete](#)

[Run once](#) [Pause scheduling](#)

Active Discovery Support for Center Interfaces

- Center network interfaces can be configured as active discovery sensors:
 - CLI 'sbs-netconf'
 - Cannot use eth0 or DPI interfaces
 - Support untagged (access) and tagged traffic (trunk)
 - Support all protocols (broadcast and unicast)
 - For unicast discovery through a routed network, use manual static routes on the active discovery interface (default gateway or static routes set on eth0 do not work)
 - IP configuration done



<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Update status	Location	Health status	Processing status	Active Discovery
<input type="checkbox"/>	FCH2424Y025	FCH2424Y025	172.16.43.211	5.1.1			Disconnected	Disconnected	Enabled
<input type="checkbox"/>	CENTER-ETH1						Running	Normally processing	Enabled

ACTIVE DISCOVERY CONFIGURATION

From here you can configure Active Discovery

Add Active Discovery configuration

+ New network interface

IP address*
192.168.69.102
IP address interface used to do Active Discovery

Prefix length*
24
Like 24, 16 or 8

VLAN number*
0
Use 0 to disable 802.1Q tagging

Network interfaces

No interfaces configured yet

Add Cancel

Configuring SNMP active discovery policies

Version	Level	Auth	Encryption
SNMPv1 (fallback when v2c failed)	noAuthNoPriv	Community String	
SNMPv2c	noAuthNoPriv	Community String	
SNMPv3	noAuthNoPriv	Username	
SNMPv3	AuthNoPriv	MD5 or SHA	
SNMPv3	AuthPriv	MD5 or SHA	AES or DES

Unicast configuration

SNMPv3

Enable

* Retry attempts: * Timeout (in seconds):

User-based security model configuration

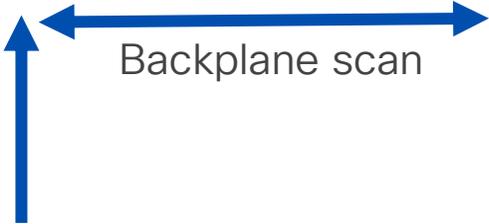
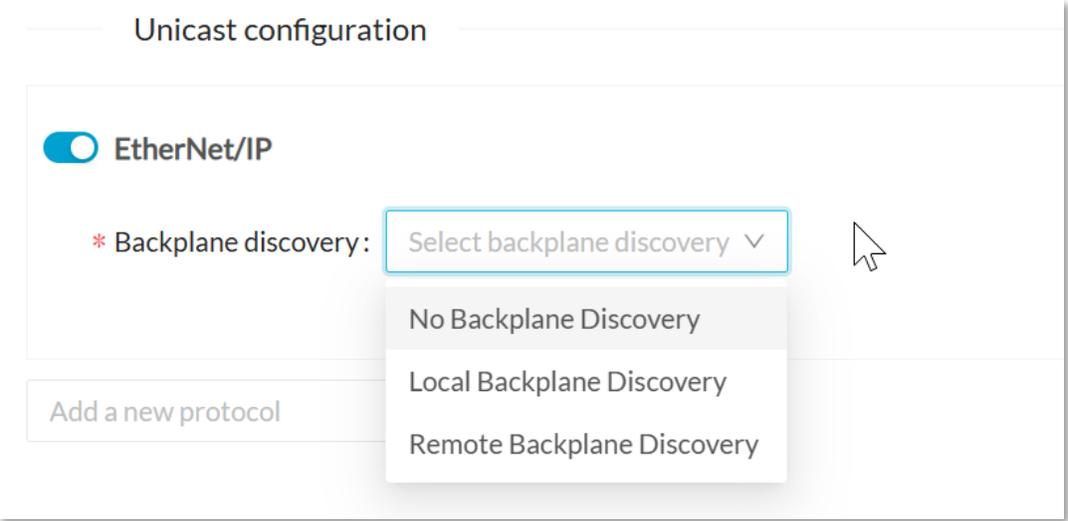
* Security type:

* Username:

* Authentication type: * Authentication password:

* Privacy type: * Privacy password:

Configuring ENIP active discovery policies



Backplane scan

Sensor (EtherNet/IP)
Unicast Active Discovery

Configuring WMI active discovery policies

Unicast configuration

WMI

Enable

* Retry attempts

* Timeout (in seconds)

* Username

* Password

Cancel Save

Windows administrator or users with WMI permissions. The administrator is the only one who can collect installed KBs

WMI: information collected

wmi-caption: **Microsoft Windows 10 Pro**

wmi-name: **WMILAB1001LOC**

wmi-organization: **escalation**

wmi-os-arch: **64-bit**

wmi-os-serial: **00331-10000-00001-AA673**

wmi-proc-architecture: **x64**

wmi-proc-name: **Intel(R) Xeon(R) Platinum 8260 CPU @ 2.40GHz**

wmi-service-pack-major-version: **0**

wmi-service-pack-minor-version: **0**

wmi-windows-build-number: **18362**

wmi-windows-sku: **48**

wmi-caption: **Microsoft Windows 10 Enterprise**

wmi-kb-list: **KB5005699 (Security Update)**

wmi-last-update: **3/8/2023**

wmi-name: **WMILAB1003LOC**

wmi-organization: **escalation**

wmi-os-arch: **64-bit**

wmi-os-serial: **00329-00000-00003-AA417**

wmi-proc-architecture: **x64**

wmi-proc-name: **Intel(R) Xeon(R) Platinum 8260 CPU @ 2.40GHz**

wmi-service-pack-major-version: **0**

wmi-service-pack-minor-version: **0**

wmi-windows-build-number: **19044**

wmi-windows-sku: **4**

wmi-caption: **Microsoft Windows Server 2016 Standard**

wmi-kb-list: **KB3192137 (Update)**

wmi-last-update: **9/12/2016**

wmi-name: **WMILAB201601LOC**

wmi-organization: **escalation**

wmi-os-arch: **64-bit**

wmi-os-serial: **00376-30000-00299-AA135**

wmi-proc-architecture: **x64**

wmi-proc-name: **Intel(R) Xeon(R) Platinum 8260 CPU @ 2.40GHz**

wmi-service-pack-major-version: **0**

wmi-service-pack-minor-version: **0**

wmi-windows-build-number: **14393**

wmi-windows-sku: **7**

Configuring Siemens S7 active discovery policies

Unicast configuration

SiemensS7

SiemensS7plus

S7 and S7plus for Unicast just needs to be enabled without further configuration

Siemens S7: information collected

s7-bootloaderref: **Boot Loader**

s7-bootloaderver: **V 2.2.1**

s7-fwver: **V 2.9.4**

s7-hwref: **6ES7 515-2RM00-0AB0**

s7-hwver: **1**

s7-modulename: **PLC_1**

s7-moduleref: **6ES7 515-2RM00-0AB0**

s7-modulever: **1**

s7-plcname: **PLC_1**

s7-serialnumber: **S C-M6DA37302020**

s7-bootloaderref: **Boot Loader**

s7-bootloaderver: **A 10.12.9**

s7-fwver: **V 2.6.12**

s7-hwref: **6ES7 315-2EH13-0AB0**

s7-hwver: **3**

s7-modulename: **CPU 315-2 PN/DP**

s7-moduleref: **6ES7 315-2EH13-0AB0**

s7-modulever: **3**

s7-plcname: **SIMATIC 300**

s7-serialnumber: **S C-V1R583472007**

snmp-sys-descr: **Siemens, SIMATIC S7, CPU315-2 PN/DP, 6ES7 315-2EH13-0AB0 , HW: 3, FW: V2.6.12, S C-V1R58347200**

Cyber Vision Global Center



Addressing the needs of all personas



Local OT Operator

Gain operational insights to ensure production uptime



Local IT/SecOps

Identify security risks to reduce attack surface



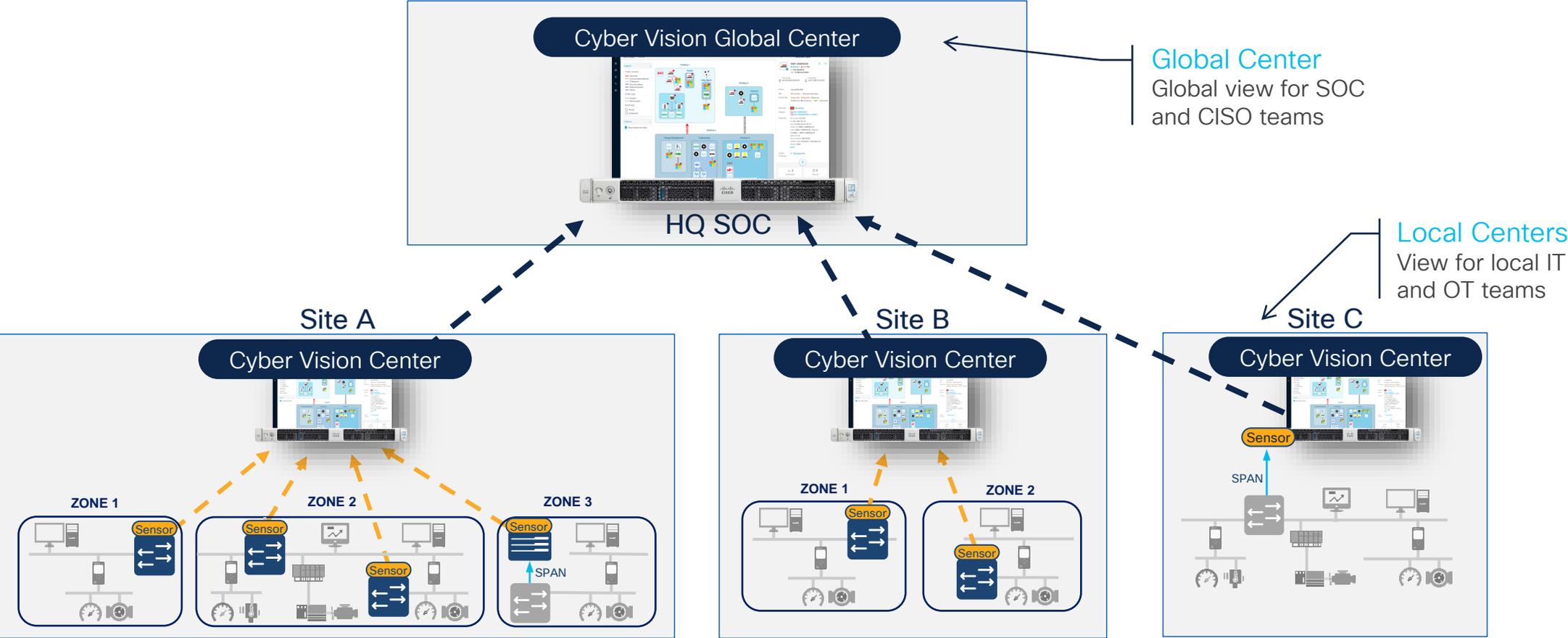
CISO Team

Aggregate data from all sites to drive governance and compliance

Cyber Vision's 3-Tier architecture offers aggregated views for large industrial organizations

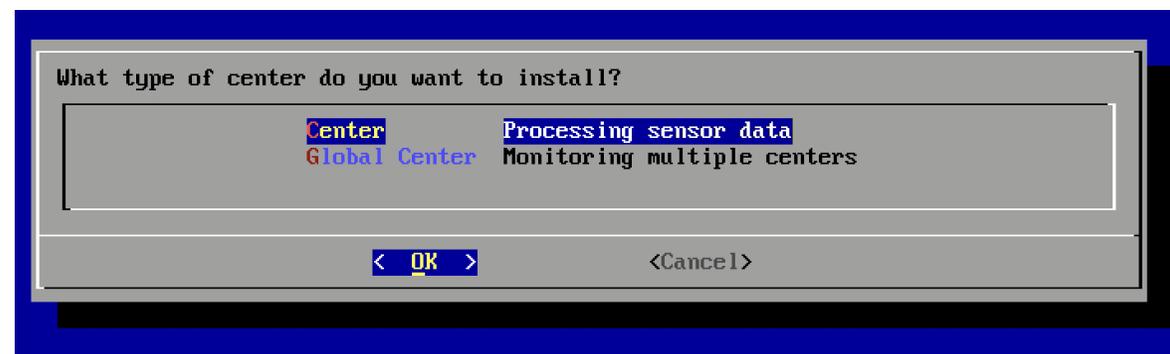
Cisco Cyber Vision Global Center

Global visibility on all sites from a central console



Select Center type during install

- Center
 - System with Sensors directly connected
 - Can be stand-alone or registered to a Global Center
- Global Center
 - System that receives data from Centers
 - No sensors can be registered to a Global Center
 - Select this role to have the install be the Global Center



Applies to Cyber Vision 4.1 and above

Global Center: Multi-site large scale deployments

- Global visibility
 - Asset inventory
 - Vulnerabilities
 - Activities
 - Global Center Presets to view data per site and across sites
- Centralized management
 - Centralized KDB updates
- Used in conjunction with Center with Global Center role
- Sensors can not be registered directly to a Global Center

Brownfield Global Center migration

- Migrate standalone center deployment to global without data loss
- Improved data synchronization between local and global centers allows for easy enrollment/unenrollment

System management

From this page you can manage centers and sensors.

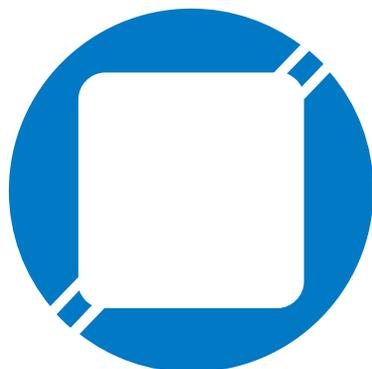
[Register a Center](#) Fingerprint: `b238559590a410c66a59082d934461669a53ca012b636e6f937233931592563c`

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
+	Center 159	10.2.3.159	SBS: 4.1.0+202202021811 KDB: 20220202	Synchronization delay: 1 sec	24 days 9 hrs 15 mins 3 secs	Connected	Unenroll
+	Center 160b	10.2.3.160	SBS: 4.1.0+202202021811 KDB: 20220202	Synchronization delay: 1 sec	24 days 9 hrs 14 mins 55 secs	Connected	Unenroll
+	Center 161	10.2.3.161	SBS: 4.1.0+202202021811 KDB: 20220202	Enrolled	24 days 7 hrs 43 mins 29 secs	Connected	Unenroll

Talos Threat Intelligence Built-in



Cisco Talos



Threat Intelligence

Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts and engineers.



Incident Response

Cisco Talos Incident Response provides a full suite of proactive and reactive services to help you prepare, respond and recover from a breach. With Talos IR, you have direct access to the same threat intelligence available to Cisco.

Actionable Intel



Insurance

Cisco Talos

The world's largest private threat intelligence team
and official developer of Snort signature files

Snort engine spots intrusions, malware and malicious traffic

- Denial of Service
- C2 and Botnet Communication
- Lateral Movement through Windows exploits
- Malware traffic
- Browser Exploit
- PLC Exploits

Superior ICS vulnerability detection

- Manually curated list of ICS vulnerabilities based on CERT and vendors information
- Talos research discovering over 200 vulnerabilities per year, 40% on ICS

Cyber Vision IDS licensing

- Snort IDS functionality included with Advantage licenses at no additional cost
 - Includes Snort Community signatures and the ability to install custom signatures
- Talos Subscriber Rule Set requires optional license
 - Available as an option to Advantage licenses only
 - Includes “shared object rules”; partially vendor-specific more complex, pre-compiled, binary rule set
- Cyber Vision IDS runs from select sensors
 - Cisco IC3000, IR8300, Catalyst 9300/9400, Docker sensors
 - Cyber Vision Center
- Signature rules updated every week
 - Included in the Cyber Vision Knowledge database available for download to all Cyber Vision customers as part of their subscription

Snort Community Rule Set

- Included with Cyber Vision Advantage license
- 4.070 rules, 440 activated*
- New rules may be added 30 days after release

Talos Subscribers Rule Set

- Available as an option to Advantage licenses only
- 51.322 rules, 4.376 shared-object, 6.176 activated*
- New rules added immediately as they are made available
- Superior detection of emerging threats

Snort Rules Management

SNORT

From this page, you can configure which Snort rules are deployed on the Cisco Cyber Vision sensors. You can also load your own custom Snort rules and manage the state of specific Snort rules. By default, Cisco Cyber Vision uses pub ruleset. The subscriber rule set requires advantage licensing and a platform specific IDS license per enabled sensor which may require additional licensing.

Use subscriber rules:

Categories

Category	Download rules	Status
Browser		<input checked="" type="checkbox"/>
Deleted		<input type="checkbox"/>
Experimental-DoS		<input type="checkbox"/>
Experimental-Scada		<input type="checkbox"/>
Exploit-Kit		<input checked="" type="checkbox"/>
File		<input checked="" type="checkbox"/>
Malware-Backdoor		<input checked="" type="checkbox"/>
Malware-CNC		<input checked="" type="checkbox"/>

Import custom rules

 IMPORT CUSTOM RULES FILE

Specific rule

Rule sid:

- Manage and maintain Snort rules deployed on supported Sensors
- Deploy custom Snort rules
- Enable/Disabled specific rules



Immediately detect malicious traffic

The screenshot displays the Cisco Cyber Vision interface. On the left is a dark navigation sidebar with icons for Explore, Reports, Events, Monitor, Search, and Admin. The main content area has a top search bar with a filter for 'severity: Critical'. Below the search bar, there are tabs for 'Dashboard' and 'List', with 'List' being the active tab. The page title is '1 Event'. A table lists one event with the following details:

Time	Severity	Category	Description
December 18, 2025 2:09:55.444 PM	critical	Signature based Detection	Snort alert on UDP id 44037 with signature A Network Trojan was detected from 192.168.0.12 → 212.166.210.80

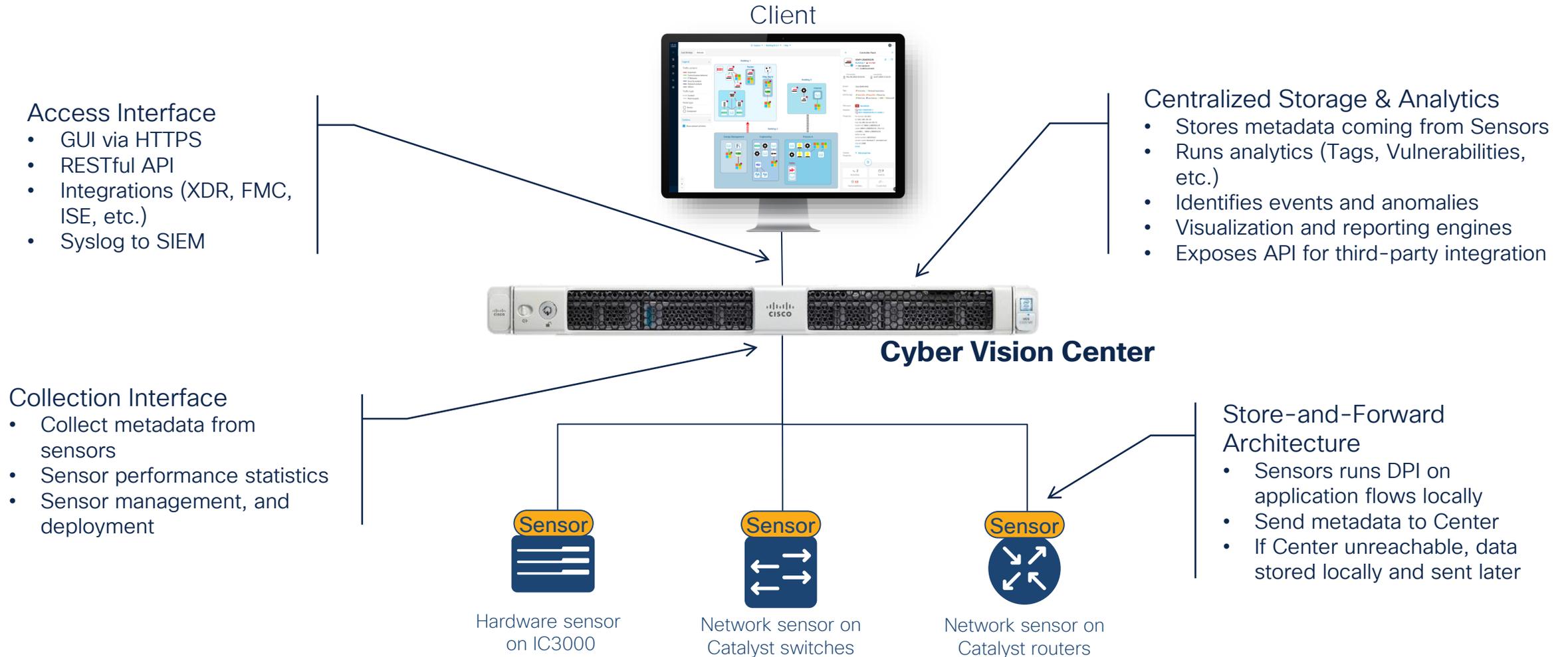
Below the table, the event details are expanded under the heading 'Snort Event':

- Occured at: 03/13-08:06:16.819867
- Sensor: -
- Gid: 1
- Signature ID: 44037
- Priority: 1
- Rule: 1:44037:4 (Revision 4)
- Classification: A Network Trojan was detected
- In network interface: /data/tmp/uploads/c650e4057f8bb0b61b64982ae609c624
- Message: INDICATOR-COMPROMISE DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com - WannaCry
- From: 192.168.0.12:62805
- To: 212.166.210.80:53 (64:80:99:D8:5D:4C -> A4:08:F5:E1:03:EC)
- Protocol: UDP
- Direction: C2S
- Ethernet type: 0x800
- Service: unknown
- VLAN: 0
- Related data: [Download data](#)

- Snort and signature-based detections allow identification of malicious traffic
- Information is being augmented with additional metadata

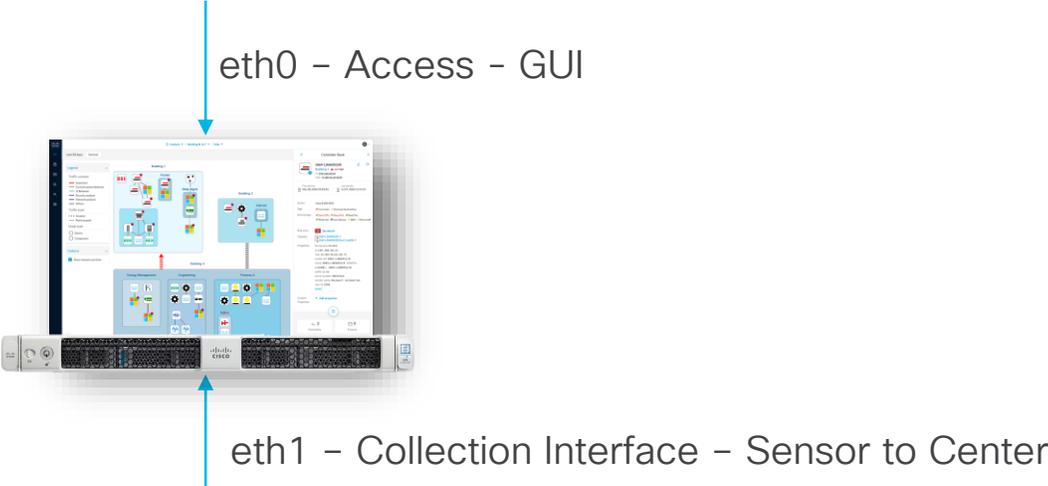
Cyber Vision Center Deployment

Cisco Cyber Vision Center deployment

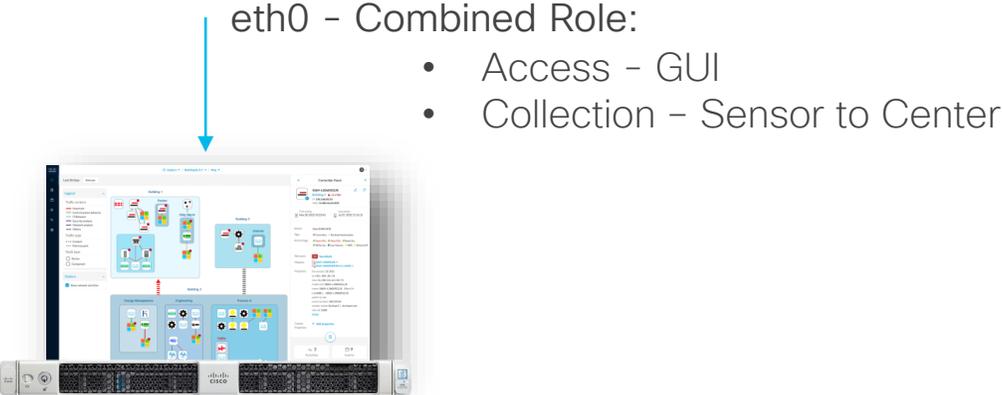


Single or Dual interface

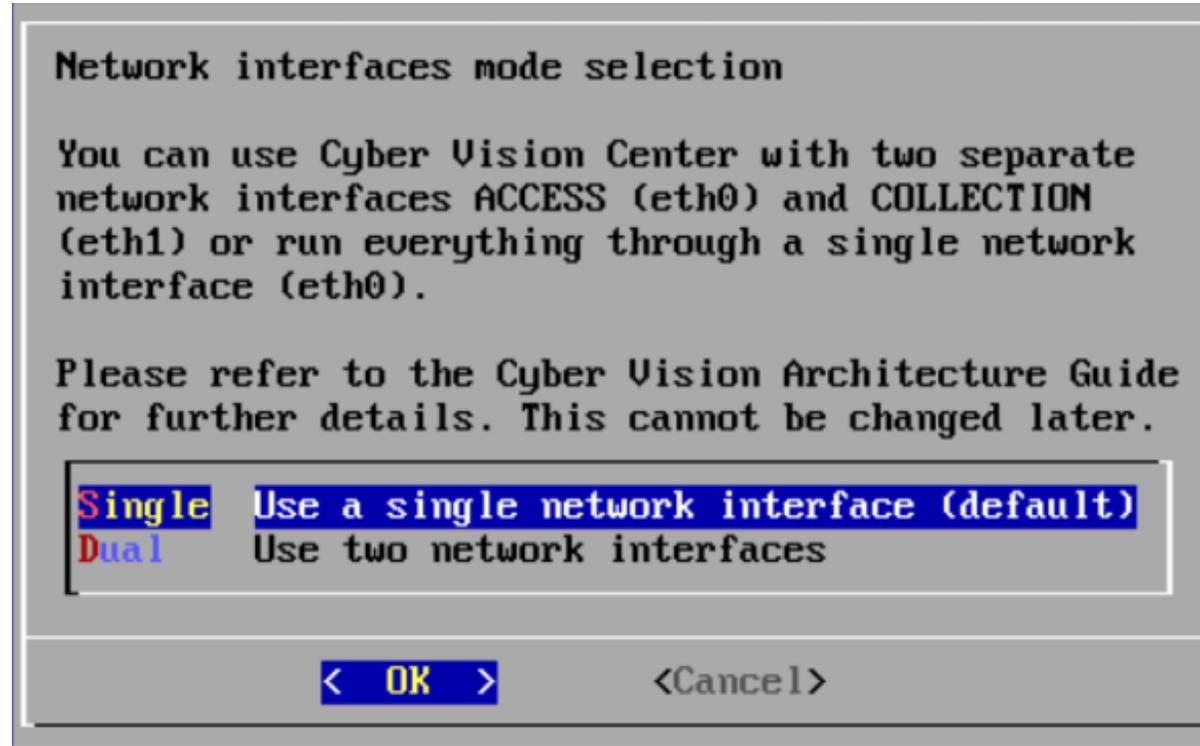
2 interfaces



1 interface



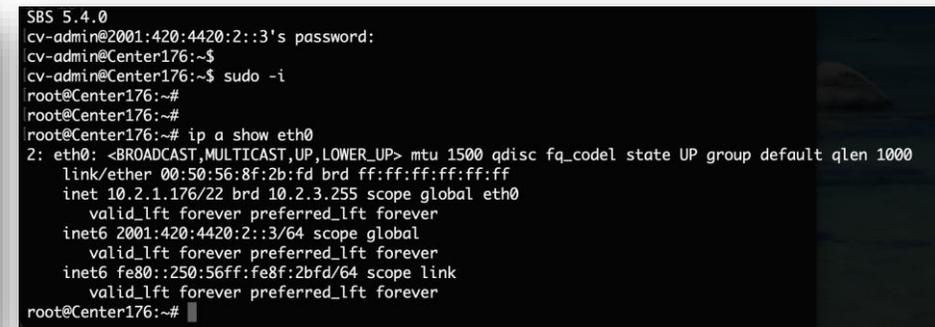
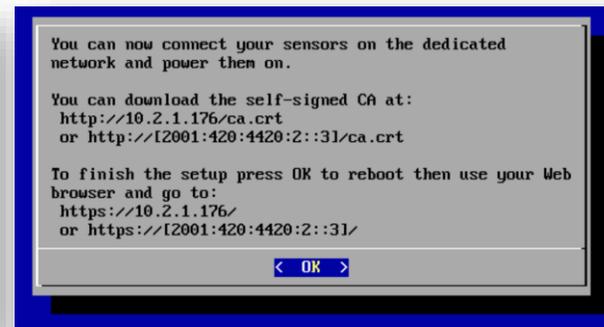
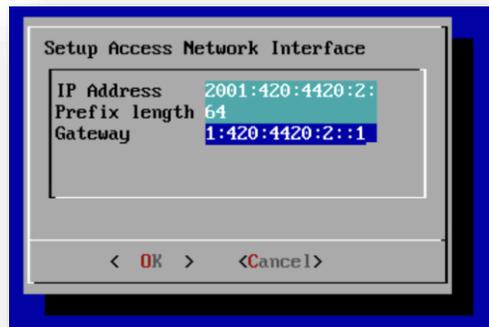
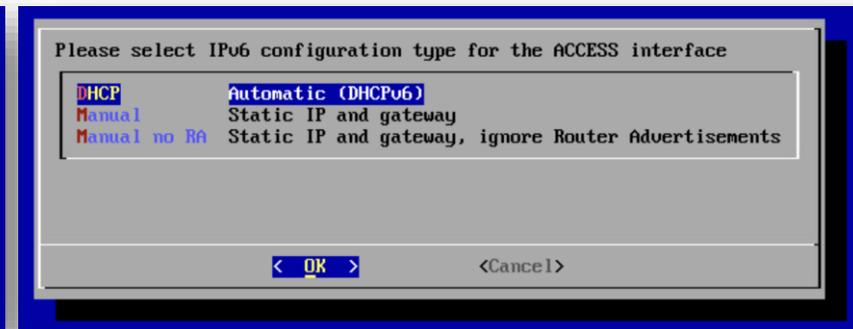
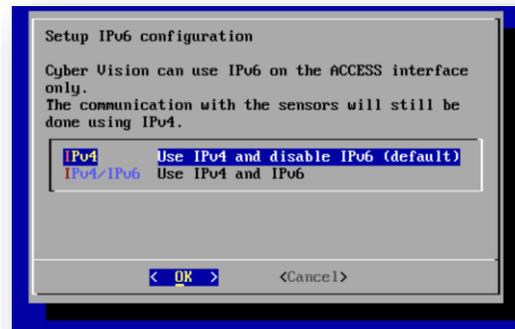
Single or Dual interface selection during install



IPv6 – Support for Administrative Services [1/2]

With v5.4 IPv6 support has been added for all administrative services of the center:
Web-UI, Integrations (syslog, ISE, LDAP), Licensing (direct):

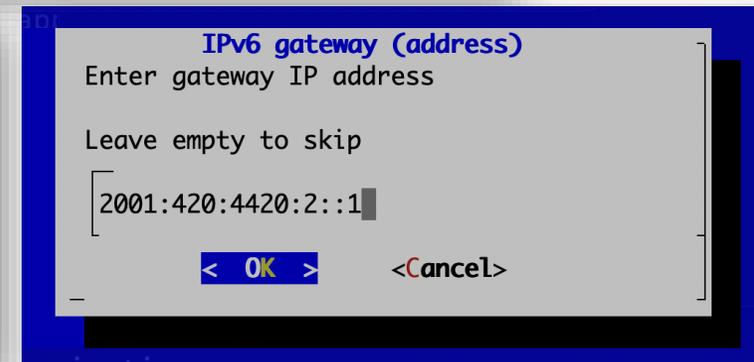
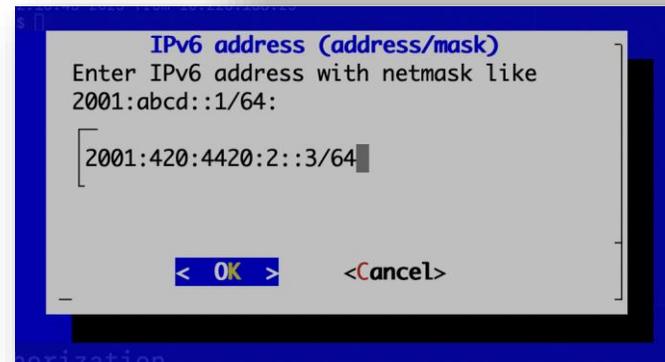
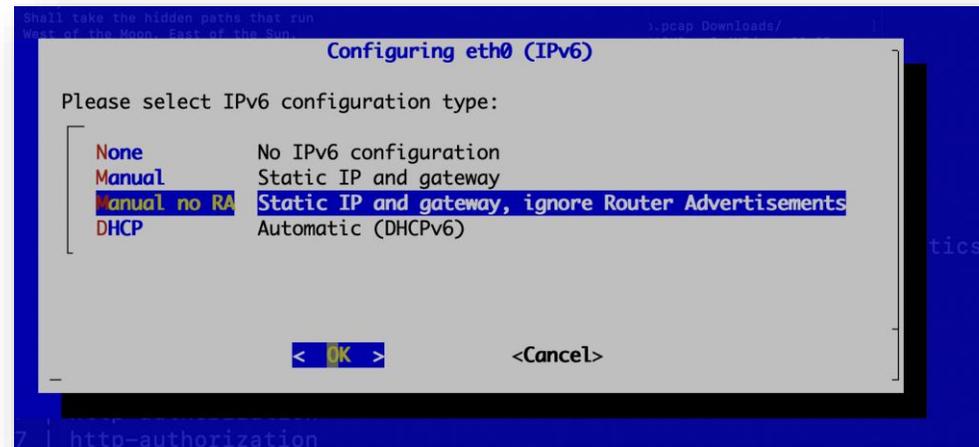
IPv6 configuration during installation:



IPv6 – Support for Administrative Services [2/2]

Change Center IP configuration post-installation

IPv6 configuration using “sbs-netconf” on Center CLI:



On Center DPI and IDS

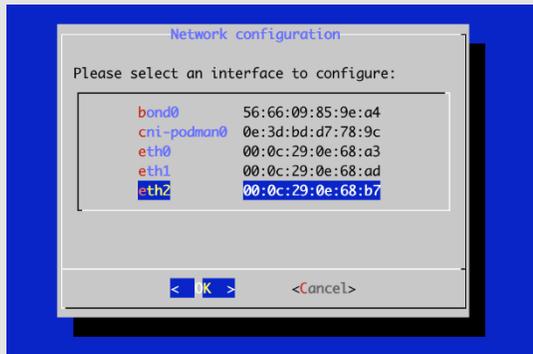
To enable DPI / IDS on Center interface(s):

1) Log into console of center (ie. hypervisor console or ssh)

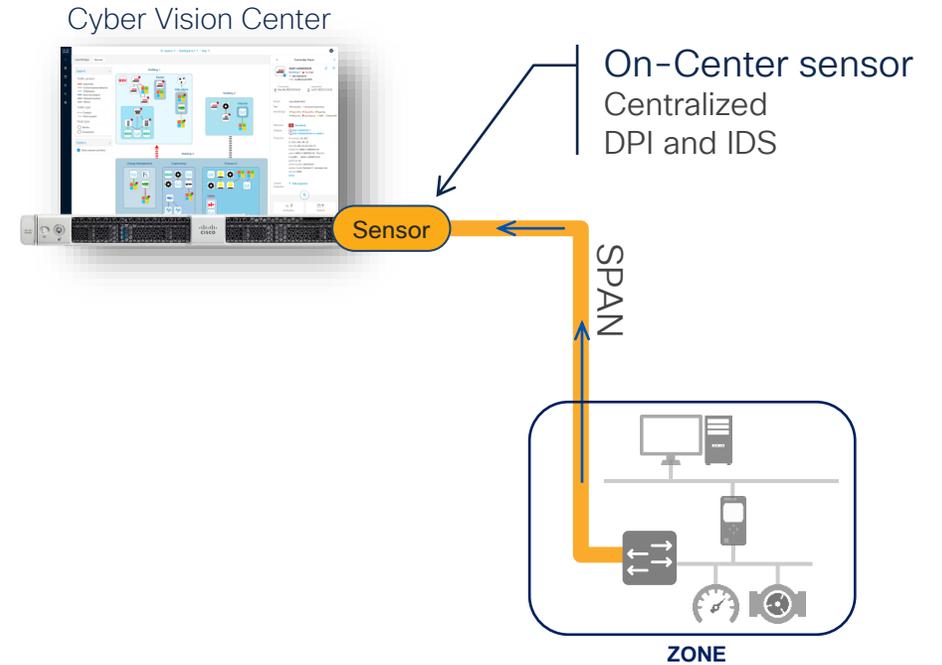
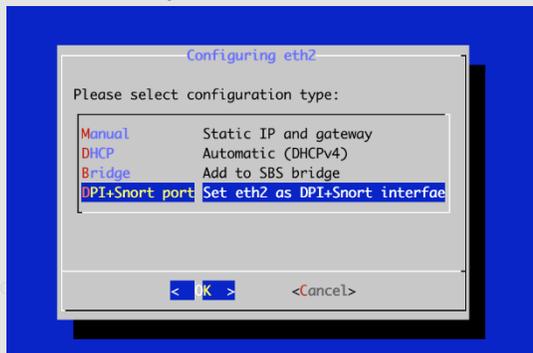
2) Type sbs-netconf command to enter interface setup

```
root@Center# sbs-netconf
```

3) Select interface wish to enable DPI/IDS on:



4) Select DPI+Snort port to enable DPI and IDS on the selected interface:



- Supports up to 4 physical interfaces max with 1 Gbps per interface
- 300,000 pps

Disabling IDS on Center Interface

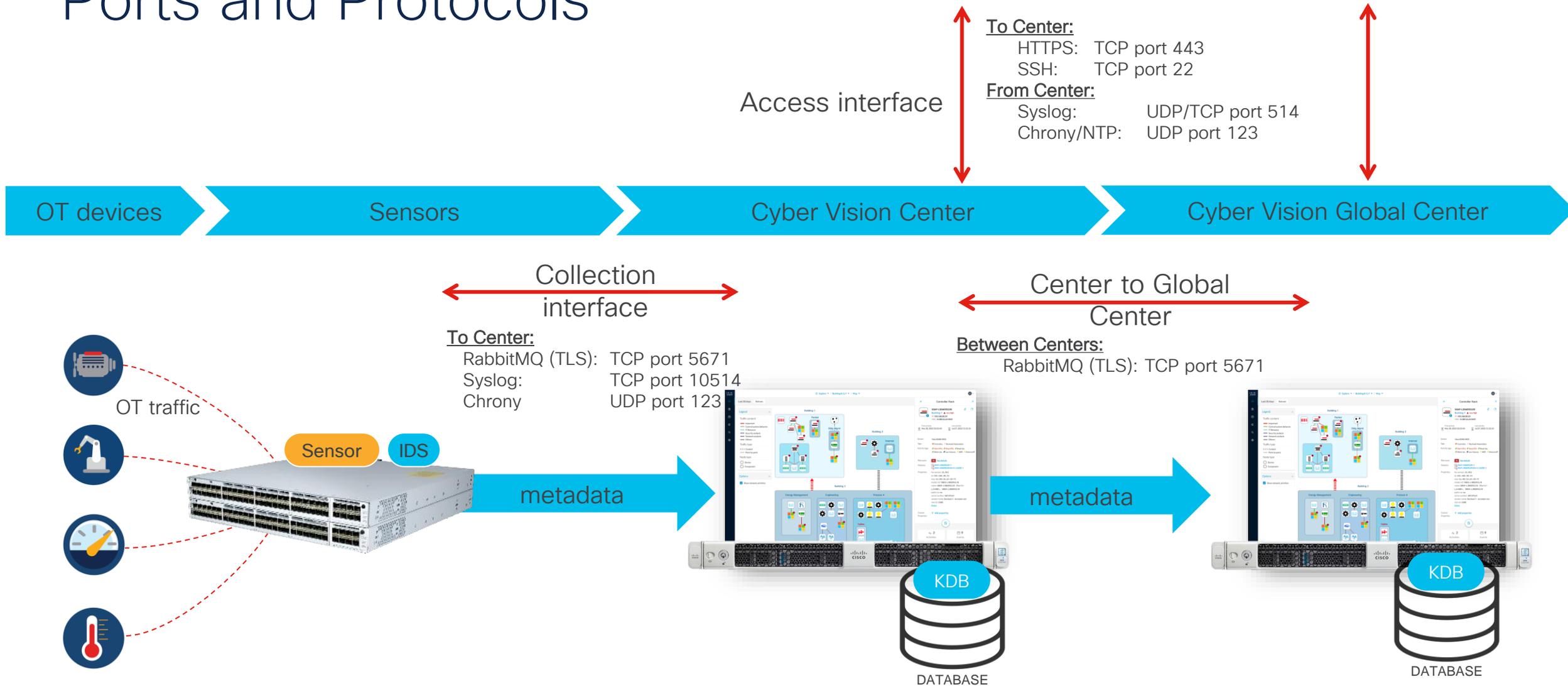
Note: Since v5.3 IDS can be disabled on the Center DPI interfaces from the sensor explorer.

The screenshot shows the 'Sensor Explorer' interface. On the left, there is a table titled 'Folders and sensors (5)'. The table has columns for Label, Serial Number, IP Address, Version, Update status, and Location. The 'Update status' column contains icons: a red 'x' for Docker 01, a green checkmark for Docker 02, a green checkmark for Docker 03, a green checkmark for MyIE3400-01, and a green checkmark for CENTER-ETH2.

On the right, the detailed view for 'CENTER-ETH2' is shown. It includes fields for Label, Serial Number, IP address, Version, System date, Deployment, Active Discovery, Capture mode, and Template. Below these fields is the 'System Health' section, which shows Status: Running, Processing status: Normally processing, and Uptime: N/A. At the bottom of the detailed view, there are several buttons: 'Start Recording', 'Move to', 'Capture mode', 'Disable IDS' (highlighted with a red box), and 'Uninstall'.

<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Update status	Location
<input type="checkbox"/>	Docker 01			5.3.0		
<input type="checkbox"/>	Docker 02			5.3.0		
<input type="checkbox"/>	Docker 03					
<input type="checkbox"/>	MyIE3400-01	FOC2417V07Z	192.168.49.136	5.3.0		
<input type="checkbox"/>	CENTER-ETH2					

Ports and Protocols



CV-CNTR-M6N

Item	Specifications
Form factor	1RU Cisco UCS C225 M6N Rack Server
Processors	AMD 2.85GHz 7443P with 24 cores
Memory	Eight 16GB RDIMM SRx4 3200MHz
RAID	Software enabled RAID will provide RAID 1 or RAID 10 depending on number of drives
Internal storage	Two or Four 1.6 TB NVMe Extreme Perf. High Endurance drives
Embedded network interface cards (NICs)	Dual 10GBASE-T Intel x710 Ethernet ports
Power supplies	Redundant Cisco UCS 1050W AC Power Supply for Rack Server

CV-CNTR-M6N Center Appliance
UCS C225 based Rack Server



Access Interface:
User access to Cyber Vision GUI
API access for integrations
Syslog export

Collection Interface:
Connection to Cyber Vision
Sensors

Dual Redundant PSUs

Optional network interface cards for the UCS C225 M6N

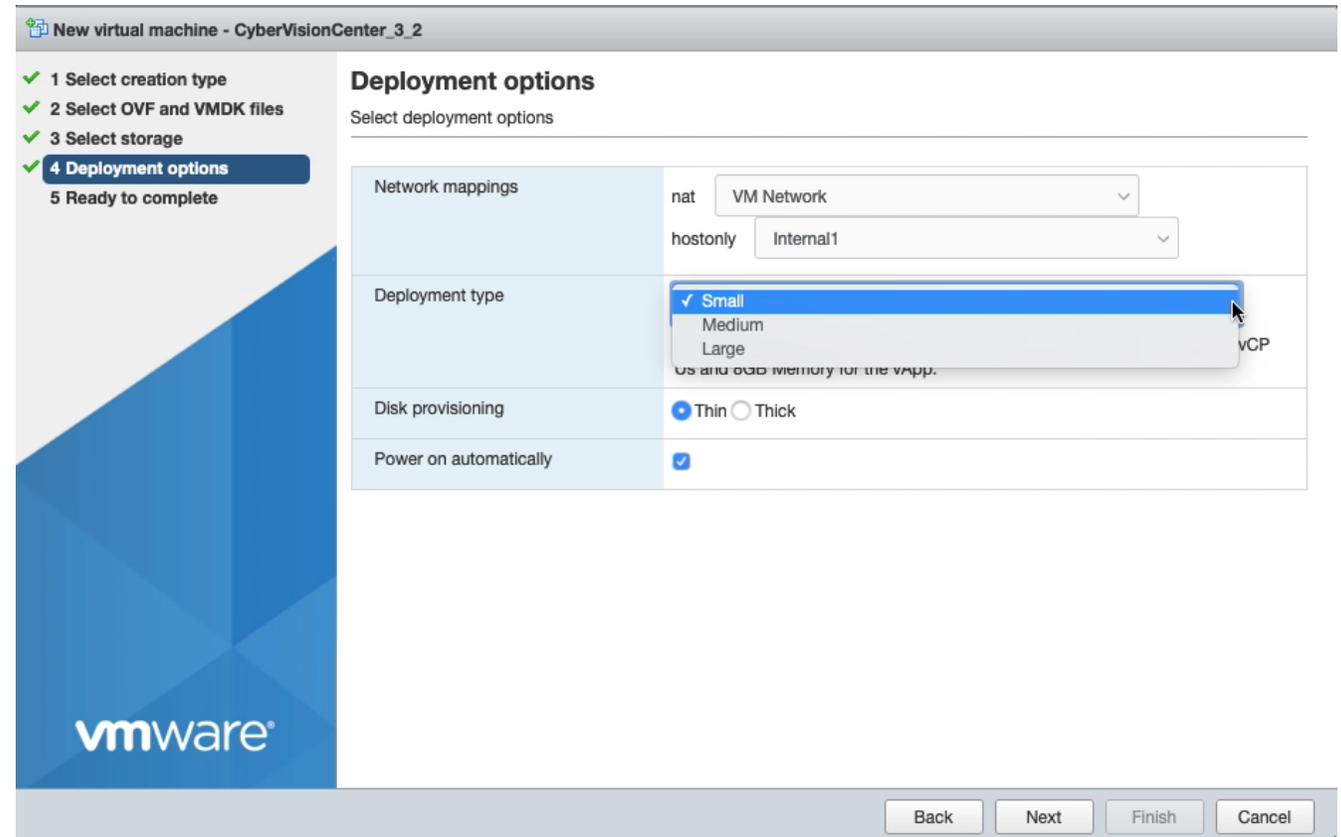
- The CV-CNTR-M6N appliance can support **1 additional** network interface card
- PCIe Card – **Choose 1 card MAX**
 - UCSC-PCIE-IRJ45=
 - 4x 1 Gigabit Ethernet Copper (RJ45) Interfaces
 - UCSC- P-ID10GC=
 - 2x 10 Gigabit Ethernet Interfaces – RJ45*
 - UCSC-PCIE-ID10GF=
 - 2x 10 Gigabit Ethernet Interfaces – SFP+*
 - UCSC-PCIE-IQ10GF=
 - 4x 10 Gigabit Ethernet Interfaces – SFP+*

* It is recommended to only leverage 1 Gbps per interface and 4 total interfaces when used for DPI/IDS functionality

Cyber Vision Center on a Virtual Machine

Template based deployment

- Small – 8 vCPU, 16 GB memory
 - 2000 Components
 - 20 sensors
- Medium – 10 vCPU, 32 GB memory
 - 15,000 Components
 - 50 sensors
- Large – 16 vCPU, 64 GB memory
 - 50,000 Components
 - 150 Sensors



Cyber Vision Center on Cloud servers



Google Cloud Platform



No hardware to
install or maintain



On-prem Center and
Cloud Global Center



Easy Center install for
POC or small sites

JSON template overview

```
{
  "name": "centerType",
  "type": "Microsoft.Common.DropDown",
  "label": "Center type",
  "placeholder": "",
  "defaultValue": "Global Center",
  "toolTip": "Choose the center type",
  "constraints": {
    "allowedValues": [
      {
        "label": "Center",
        "value": "Standalone"
      },
      {
        "label": "Center with Global Center",
        "value": "Local Center"
      },
      {
        "label": "Global Center",
        "value": "Global Center"
      }
    ],
    "required": true
  },
  "visible": true
},
{
  "name": "fqdn",
  "type": "Microsoft.Common.TextBox",
  "label": "FQDN name",
  "toolTip": "Enter the FQDN name",
  "defaultValue": "Center",
  "constraints": {
    "required": true,
    "regex": "^[a-z0-9A-Z-]{5,50}$",
    "validationMessage": "The FQDN name contains non authorized characters"
  }
}
```

Basics Virtual Machine Settings **Cyber Vision Settings** Review + create

Configure Cyber Vision * ⓘ

Cyber Vision configuration

Keyboard layout * ⓘ

Center type * ⓘ

FQDN name * ⓘ

Webapp TLS certificate * Generate an autosigned certificate with the FQDN
 Use a custom certificate

DNS servers

i If no servers are provided, the default provider is OpenDNS: 208.67.222.222, 208.67.220.220

NTP servers

Authorized networks

i If no networks are provided, the default value is to authorize everything (0.0.0.0/0)

Cyber Vision FIPS Compliance

Cyber Vision FIPS compliant version

- Federal Information Processing Standards (FIPS) required for Federal agencies in the USA to deploy Cyber Vision
 - Cyber Vision complies with FIPS 140-3 as of version 5.2
- Dedicated FIPS build
 - Cannot switch from non-FIPS to FIPS version
 - Can't upgrade to FIPs from non-FIPS
 - Can't downgrade from FIPs to non-FIPS
 - Only active discovery versions of sensor are supported
 - Can deploy without configuring or leveraging active discovery
 - Must use FIPS version of Center with FIPS version of sensors
 - Unique download on Cisco.com
- KDB updates can only be applied via command line (no UI)

Cyber Vision Sensors Deployment

Easy sensor provisioning and management

Configure Cyber Vision IOx sensor app

The device requires additional parameters. Some parameters have been pre-filled. Please complete the remaining fields.

Cisco device: IE-3400-8P2S

Capture IP address*

Capture prefix length*

Like 24, 16 or 8

Capture VLAN number*

Collection IP address*

Collection prefix length*

Like 24, 16 or 8

Collection gateway

Collection VLAN number*

Sensors can easily be installed, configured and managed centrally from the Cyber Vision Center using the sensor management extension.

Sensor and host software version compatibility matrix

Platform	Minimum Version	Recommended Version
Cisco IC3000	1.5.2	1.5.2
Cisco Catalyst IE3400	17.6.x	17.9.6a / 17.12.5 / 17.15.3
Cisco Catalyst IE3300 10G	17.6.x	17.9.6a / 17.12.5 / 17.15.3
Cisco Catalyst IE3300	17.12.x	17.12.5 / 17.15.3
Cisco Catalyst IE3500	17.18.x	17.18.x
Cisco Catalyst IE9300	17.12.x	17.12.5 / 17.15.3
Cisco IR1101	17.6.x	17.9.6 / 17.12.4 / 17.15.3
Cisco IR1800	17.6.x	17.9.6 / 17.12.4 / 17.15.3
Cisco Catalyst IR8300	17.9.x	17.9.6 / 17.12.4 / 17.15.3
Cisco Catalyst 9300, 9400	17.6.x	17.9.6a / 17.12.5 / 17.15.3
Docker Sensor	Ubuntu 20, 22 Docker 27.0	Ubuntu 24.04 Docker 27.x
VM Sensor	VMWare v6.x (x86)	VMWare v6.x (x86)

Simplifying sensor deployments

The screenshot shows the Cisco Management jobs interface. The left sidebar contains navigation options: System, Data Management, Network Organization, Sensors, Users, Events, API, License, LDAP Settings, Snort, Risk score, Integrations, and Extensions. The main content area is titled "Management jobs" and displays a table of jobs with their progress and duration.

Jobs	Steps	Duration
Single deployment (FJC2406E0U0)	✓ — ✓ — ✓	35s
Single removal (FJC2406E0U0)	✓	12s
Single redeployment (FJC2406E0U0)	✓ — ✓ — ✓ — ✓	1m 17s
Single redeployment (FCW2445P61X)	Prepare Logs	1m 49s
Single redeployment (FCW2445P61X)	Serial number is different, updating it.	1m 45s
Single removal (FCW23070H7B)	✗	0s
Single removal (FCH2348Y0CU)	✗	0s
Single deployment (FCW2445P61X)	✓ — ✓ — ✓	1m 28s
Single removal (FCW2445P61X)	✗	0s
Single redeployment (FCW2445P61X)	✓ — ✓ — ✗ —	1m 24s

- Enhanced sensor deployment diagnostics
- Easily identify where deployments have failed and why

Sensor Explorer enables sensor management at scale

Folders and sensors (4)

Filter 0 Selected Move selection to More Actions

Label	IP Address	Version
IR		4.0.3 - 4.1.0
Catalyst		4.1.0+202202251419
Hardware Sensor		4.1.0+202202251451
IE		4.1.0+202202251419

Folders organize groups of sensors to allow for easy navigation between groups and bulk actions

Sensor Explorer

Back to Sensor Explorer

Catalyst

Edit Delete

Folders and sensors (2)

Filter 0 Selected Move selection to More Actions

As of: Feb 28, 2022 10:35 AM

Label	IP Address	Version	Health status	Processing status	Active Discovery	Uptime
CAT9300Stack	192.168.105.20	4.1.0+202202251419	Connected	Normally processing	Unavailable	28 minutes
CAT9400	192.168.105.17	4.1.0+202202251419	Connected	Normally processing	Unavailable	29 minutes

CAT9300Stack

Label: CAT9300Stack

Serial Number: FJC2406SOST

IP address: 192.168.105.20

Version: 4.1.0+202202251419

System date: Feb 28, 2022 10:35:58 AM

Deployment: Sensor Management Extension

Active Discovery: Unavailable

Capture mode: All

System Health

Status: Connected

Processing status: Pending data

Uptime: 29 minutes

Go to statistics

Start Recording

Move to

Capture mode

Redeploy

Enable IDS

Uninstall



Bulk Sensor Actions

- Filter on sensors list
- Create folders to group sensors
- Move sensors to folders
- Delete folders

The 'CREATE FOLDER' dialog box contains the following fields and buttons:

- Folder name * (text input field)
- Location (text input field)
- Description (text input field)
- Ok (blue button)
- Cancel (white button with blue border)

The 'Sensor Explorer' interface shows a list of sensors with the following columns: Label, Serial Number, and Location. Two sensors are selected, and the 'More Actions' menu is open, showing 'Delete folders' and 'Update sensors' options.

Label	Serial Number	Location
<input checked="" type="checkbox"/>	RTP-DIST-CAT9300	
<input checked="" type="checkbox"/>	RTP-L1-BAK-IE3400	PERF2
<input type="checkbox"/>	RTP-L1-COOL-IE3400	PERF3

The 'MOVE SELECTION TO' dialog box is displayed over the Sensor Explorer interface. It contains the following elements:

- Destination: (dropdown menu)
- OK (grey button)
- Cancel (white button with blue border)

The background interface shows a list of folders and sensors with the following columns: Label, Serial Number, and Location. One folder is selected.

Label	Serial Number	Location
<input checked="" type="checkbox"/>	NIT	
<input type="checkbox"/>	NTR	

Global credentials

The screenshot displays the Cisco Sensor Explorer interface. On the left, a navigation sidebar includes 'System', 'Data Management', 'Network Organization', and 'Sensors'. The 'Sensors' section is expanded, and 'Sensor Explorer' is highlighted with a red box and a blue circle labeled '1'. The main area is titled 'Sensor Explorer' and contains a toolbar with 'Install sensor', 'Manage Cisco devices' (highlighted with a red box and blue circle '2'), and 'Organize'. Below the toolbar, a 'More Actions' dropdown menu is open, showing 'Update Cisco devices' and 'Manage credentials' (highlighted with a red box and blue circle '3'). A table with columns 'Label' and 'IP Address' is partially visible. On the right, a 'SET GLOBAL CREDENTIALS' dialog box is open, containing a text description and two input fields for 'Login' and 'Password', both marked with an asterisk. The dialog has 'Save' and 'Cancel' buttons at the bottom.

System

Data Management

Network Organization

Sensors

Sensor Explorer

Management jobs

PCAP Upload

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remote

Install sensor

Manage Cisco devices

Organize

Update Cisco devices

Manage credentials

Filter 0 Selected MOVE SELECTION TO More Actions

Label	IP Address
-------	------------

SET GLOBAL CREDENTIALS

You can define "global credentials" which can be used as default credentials when deploying a new Cisco device. When you update these "global credentials" it affects both new and deployed sensors.

Login *

Password *

Save Cancel

CLI to disable Sensor Management Extension

- Stop Sensor management extension from attempting to connect to hosting platform
- Will need to re-enable to update existing sensors or deploy new sensors
- Will see extension as disabled

```
cv-admin@CVCenterBeta:~$ sudo sbs-extension cmd sensor-management disable
Disabling, do not interrupt...
sensor-management-main
sensor-management-postgres
sensor-management-influxdb
Extension has been disabled
```

Name

[DISABLED] Cyber Vision sensor management

UPDATE CISCO DEVICES

 Error while loading sensor management extension

<input type="checkbox"/>	Label 	IP	Version	Target
--------------------------	---	----	---------	--------

No updatable sensor has been found.

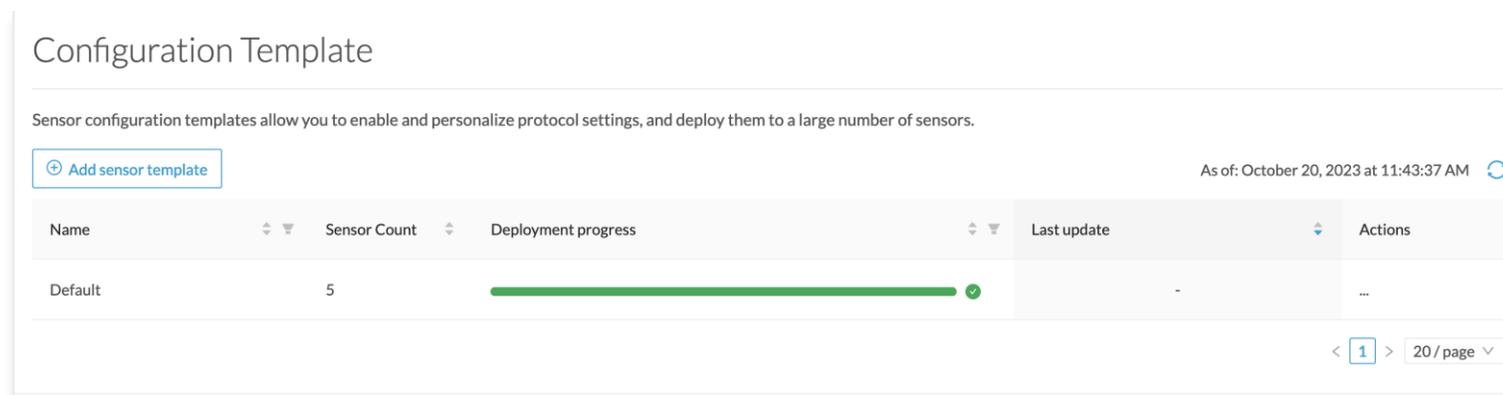
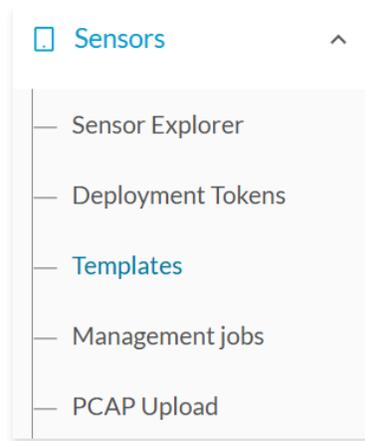
CLI to enable Sensor Management Extension

- Start sensor management extension from CLI

```
cv-admin@CVCenterBeta:~$ sudo sbs-extension cmd sensor-management enable
Enabling, do not interrupt...
run script wrote to stdout:
sensor-management-postgres
sensor-management-influxdb
sensor-management-main
Extension has been enabled
```

Sensor Configuration Template

- Simplifies configuration of multiple sensors across the infrastructure
 - Easily configure protocols and ports to use
- Default template assigned to all sensors at first
 - Can have multiple templates
- See status of template deployments



Sensor Configuration Template Wizard

- Enable/Disable protocols
- Modify ports assigned to specific protocols

CREATE SENSOR TEMPLATE

1 Basic information | 2 Protocol configuration | 3 Select sensors | 4 Summary

Search for protocol name, category, port number, port protocol type... Display modified only

Protocol	Category	Port Mapping
<input checked="" type="checkbox"/> ARP	Network	N/A
<input checked="" type="checkbox"/> Bacnet	BMS	N/A
<input checked="" type="checkbox"/> BACnetVLC	BMS	UDP 47808
<input checked="" type="checkbox"/> BeckhoffAMS	General	TCP 48898
<input checked="" type="checkbox"/> BFD	General	UDP 3734
<input checked="" type="checkbox"/> BoschRCP	General	TCP 1756

Previous Next



Sensor Configuration Template Wizard

- Selectively deploy to a single sensor or multiple sensors

CREATE SENSOR TEMPLATE ×

Basic information ✓ Protocol configuration ✓ **3 Select sensors** 4 Summary

0 Selected [Filters](#) [Select All](#) [Unselect All](#) As of: October 20, 2023 at 11:53:51 AM [↻](#)

<input type="checkbox"/>	Label	IP	Folder	Template	Template Deployment Status	Version	Location	Health Status	Processing Status	Active Discovery	Uptime
<input type="checkbox"/>	CEll1	192.168.6.10	BehrensHome	Default	deployed	4.3		Disconnected	Disconnected	Unavailable	N/A
<input type="checkbox"/>	FCH2409Y01 2	192.168.6.151	BehrensHome	Default	deployed	4.3		Disconnected	Disconnected	Disabled	N/A
<input type="checkbox"/>	FCW23370H4 Q	192.168.2.100	BehrensHome	Default	deployed	4.3		Disconnected	Disconnected	Unavailable	N/A
<input type="checkbox"/>	FDO254412V 1			Default	deployed	4.3		Disconnected	Disconnected	Unavailable	N/A
<input type="checkbox"/>	FOC2330V0G N	192.168.6.20		Default	deployed	4.3		Disconnected	Disconnected	Enabled	N/A

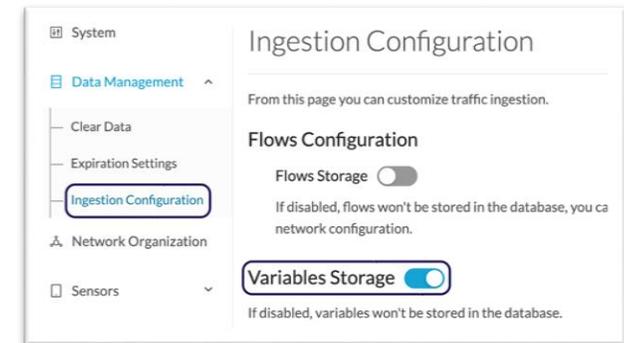
6 Records < 1 > 10 / page

Sensor Configuration Template Wizard

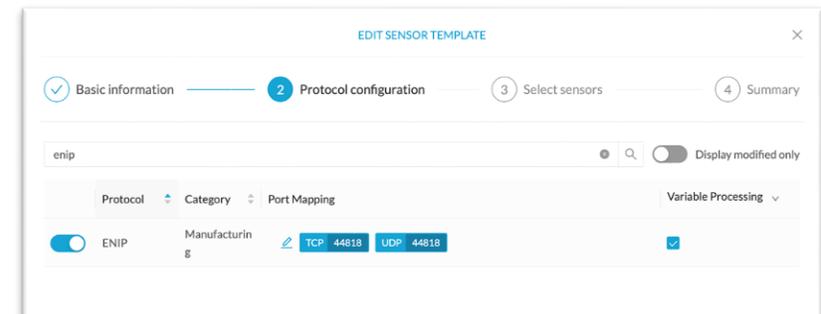
Note: Variable processing is disabled by default in release v5.3.0

- Enable/Disable variable processing as per use-case requirements
- Enabling the processing requires two steps.

1) Activate the “Variables Storage” in the CV Center

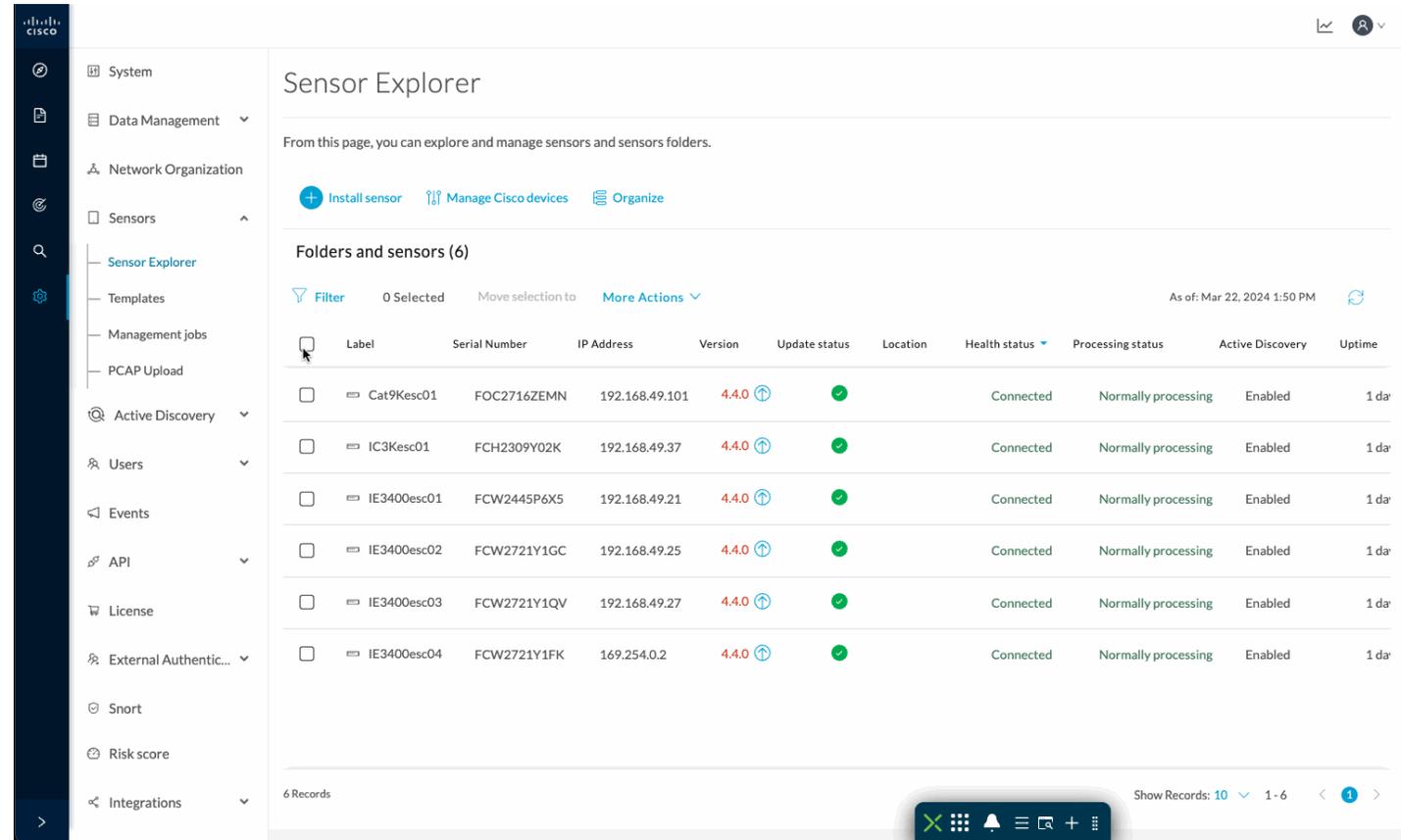


2) Activate the “Variable Processing” for each protocol in the sensor template



Sensor Auto-Update

- User decides which sensors to include into auto-update process
- Sensor collects update file and will be updated, supervised by the center



The screenshot displays the Cisco Sensor Explorer interface. On the left is a navigation sidebar with options like System, Data Management, Network Organization, Sensors, Templates, Management jobs, PCAP Upload, Active Discovery, Users, Events, API, License, External Authentic..., Snort, Risk score, and Integrations. The main content area is titled 'Sensor Explorer' and includes instructions, action buttons (Install sensor, Manage Cisco devices, Organize), and a table of sensors.

From this page, you can explore and manage sensors and sensors folders.

[+ Install sensor](#) [Manage Cisco devices](#) [Organize](#)

Filters and Actions: Filter (0 Selected), Move selection to, More Actions

As of: Mar 22, 2024 1:50 PM

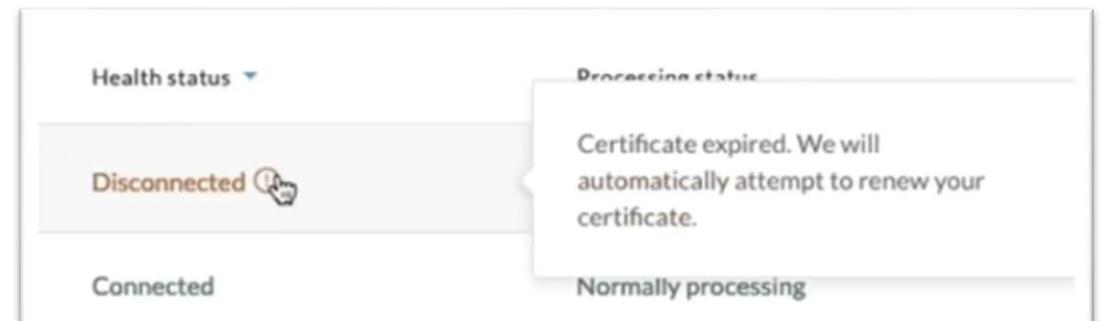
	Label	Serial Number	IP Address	Version	Update status	Location	Health status	Processing status	Active Discovery	Uptime
<input type="checkbox"/>	Cat9Kesc01	FOC2716ZEMN	192.168.49.101	4.4.0	⬆️	🟢	Connected	Normally processing	Enabled	1 da
<input type="checkbox"/>	IC3Kesc01	FCH2309Y02K	192.168.49.37	4.4.0	⬆️	🟢	Connected	Normally processing	Enabled	1 da
<input type="checkbox"/>	IE3400esc01	FCW2445P6X5	192.168.49.21	4.4.0	⬆️	🟢	Connected	Normally processing	Enabled	1 da
<input type="checkbox"/>	IE3400esc02	FCW2721Y1GC	192.168.49.25	4.4.0	⬆️	🟢	Connected	Normally processing	Enabled	1 da
<input type="checkbox"/>	IE3400esc03	FCW2721Y1QV	192.168.49.27	4.4.0	⬆️	🟢	Connected	Normally processing	Enabled	1 da
<input type="checkbox"/>	IE3400esc04	FCW2721Y1FK	169.254.0.2	4.4.0	⬆️	🟢	Connected	Normally processing	Enabled	1 da

6 Records | Show Records: 10 | 1-6 | 1

Certificate renewal enhancement for Sensors

Automated sensor certificate renewal

- 35 days before certificate expiration date, system will attempt to renew it automatically
 - Renewal is done on center side and new provisioning package is automatically sent to sensor
-
- CLI commands:
 - 'sbs-sensor-cert list' to list certificate to renew (or: --all)
 - 'sbs-sensor-cert renew' to renew certificate: -i <sensor id> (or: -a all)



Zero-Touch-Provisioning of Sensors (ZTP)

Allow **deployment** of many sensors **programmatically and at scale** using:

- Cisco Catalyst SD-WAN Manager (formerly vManage)
- Ansible: several playbooks available to use the ZTP provisioning ([Public GitHub repo](#))
- API routes available for custom implementation

The screenshot shows a web interface for managing deployment tokens. A modal window titled "Add new deployment tokens" is open. It contains the following fields and controls:

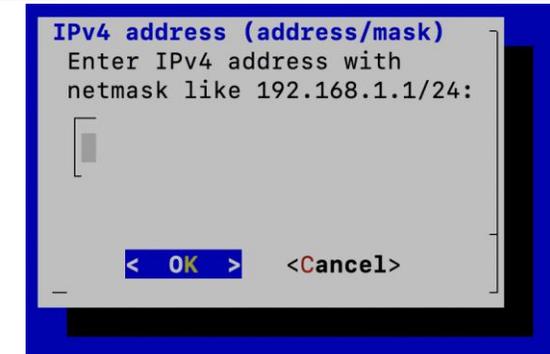
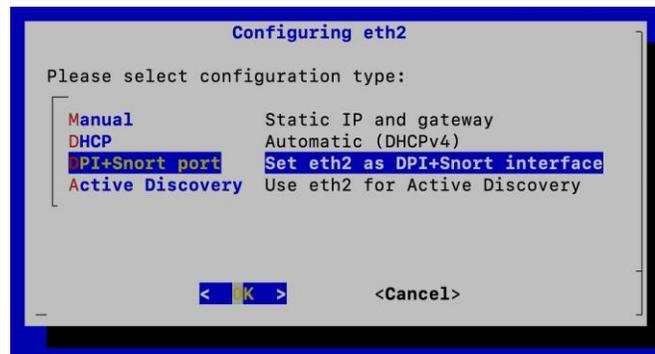
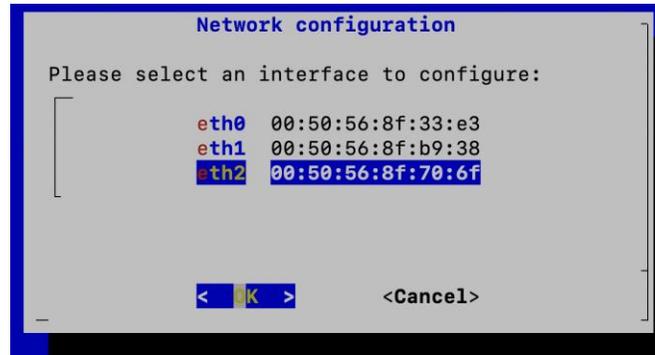
- Name:** Deployment01
- Number of uses:** 4
- Expiration time:** 2025-05-01
- Enabled:** A toggle switch that is currently turned on.
- Buttons:** "Cancel" and "Create".

Name	Tokens	Status	Creation Date	Expiration Date	Usages	
Deployment01	Image	Token				
	cviox-aarch64.tar	Show				
	cviox-active-discovery-aarch64.tar	Show				
	cviox-active-discovery-ic3000-x86-64.tar	Show	Enabled	May 27, 2024	May 1, 2025	0/4
	cviox-active-discovery-x86-64.tar	Show				
	cviox-ic3000-x86-64.tar	Show				
	cviox-x86-64.tar	Show				

ERSPAN Support on Center DPI Interface

Note: In addition to the SPAN capabilities of sensors, Cyber Vision supports ERSPAN on the Center interface starting from v5.3

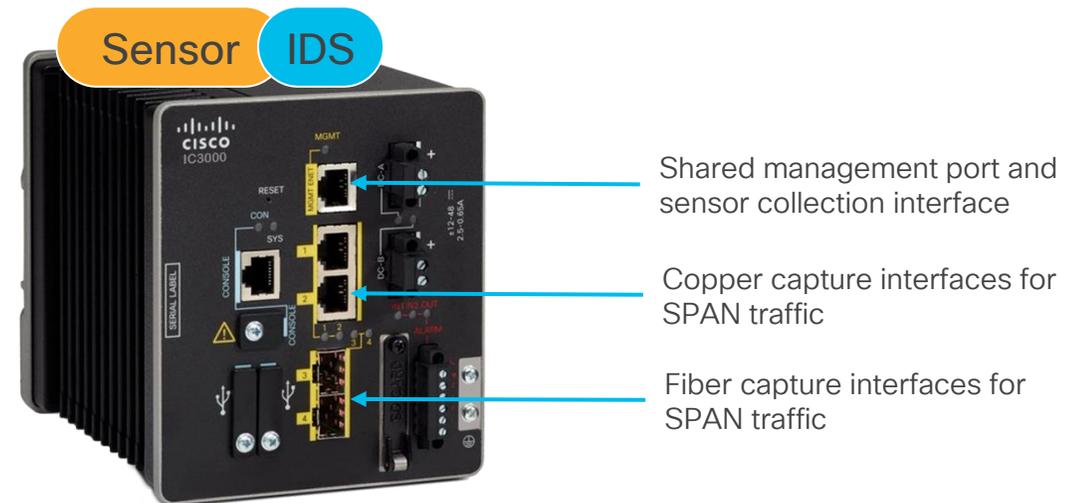
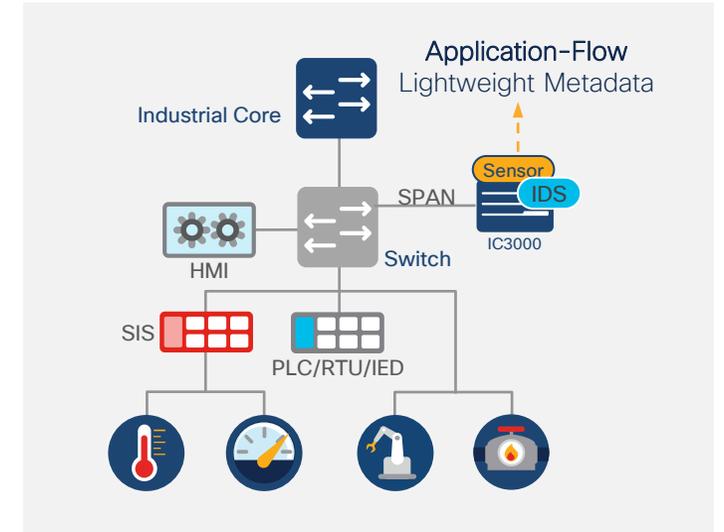
Change the network configuration using 'sbs-netconf' on the commandline of the center:



Cyber Vision hardware-sensor

Cisco IC3000 Industrial Compute

- SPAN based solution to support brownfield: traffic capture and DPI on non-Cisco switches
- Can aggregate SPAN traffic from multiple switches using the 4 capture interfaces
- Lightweight Metadata from Sensor to Center eliminates need for dedicated span network
- Supports Snort IDS with Advantage licenses (Talos subscriber rules available as an option)
- Supported PPS: see [Performance Figures](#)
- Starting 4.3, it leverages same sensor application as other platforms for improved performance and simpler configuration using Sensor templates



Cyber Vision network-sensor

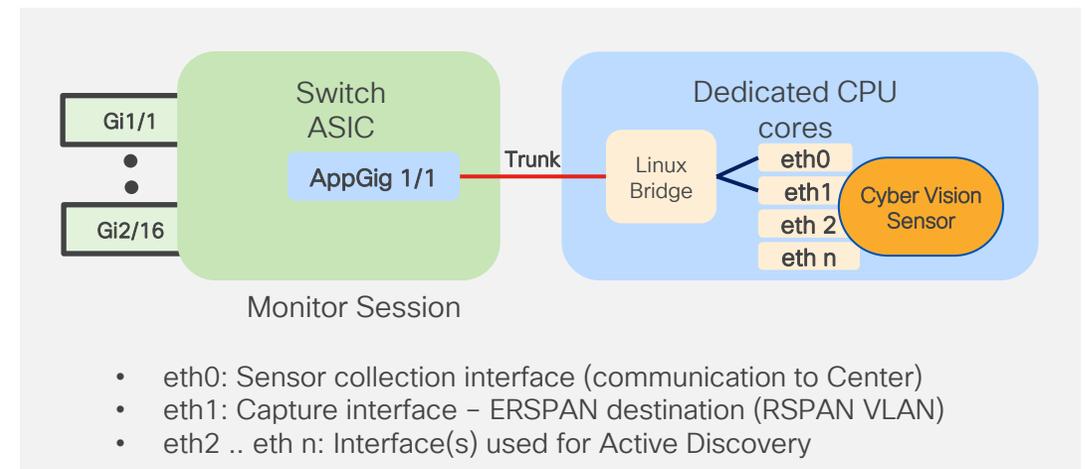
Cisco Catalyst IE3300, IE3400, and IE3500 Rugged Series Switches

- Catalyst IE3300 (see: [version requirements](#))
 - 1GE uplink PIDs manufactured after March 2023 (VID 06+) using Cyber Vision 4.2+
 - All 10GE uplink PIDs
- Catalyst IE3400 and IE3500 (see: [version requirements](#))
- Sensor is an IOx app running on a dedicated core
 - No impact on performance
 - Eliminates the need for SPAN
 - Supported PPS: [see Performance Figures](#)
 - Requires SD Card for application hosting
- Traffic flowing through switch ports is copied to embedded Cyber Vision Sensor for DPI using internal ERSPAN session between IOS dataplane and IOx
- Best deployed as Access switch where ICS assets connect to the network

Cyber Vision Sensor runs on IOx using dedicated cores of switch CPU



Traffic flowing through switch ports is copied to embedded Cyber Vision Sensor for DPI



Cyber Vision network-sensor

L3NAT on IOx

- IOS v17.14 introduces “l3nat-iox” command
- CV sensor will share its IP with the platform

CV center IP: 192.168.49.10
IE3400 management IP: 192.168.49.28

1. Create a collection VLAN (ex: 2507)
2. Add an IP to that VLAN

Example:

```
interface Vlan2507
 ip address 169.254.0.1 255.255.255.252
```

3. Configure sensor eth0 in the collection vlan:

Example:

```
Vlan: 2507
IP: 169.254.0.2
```

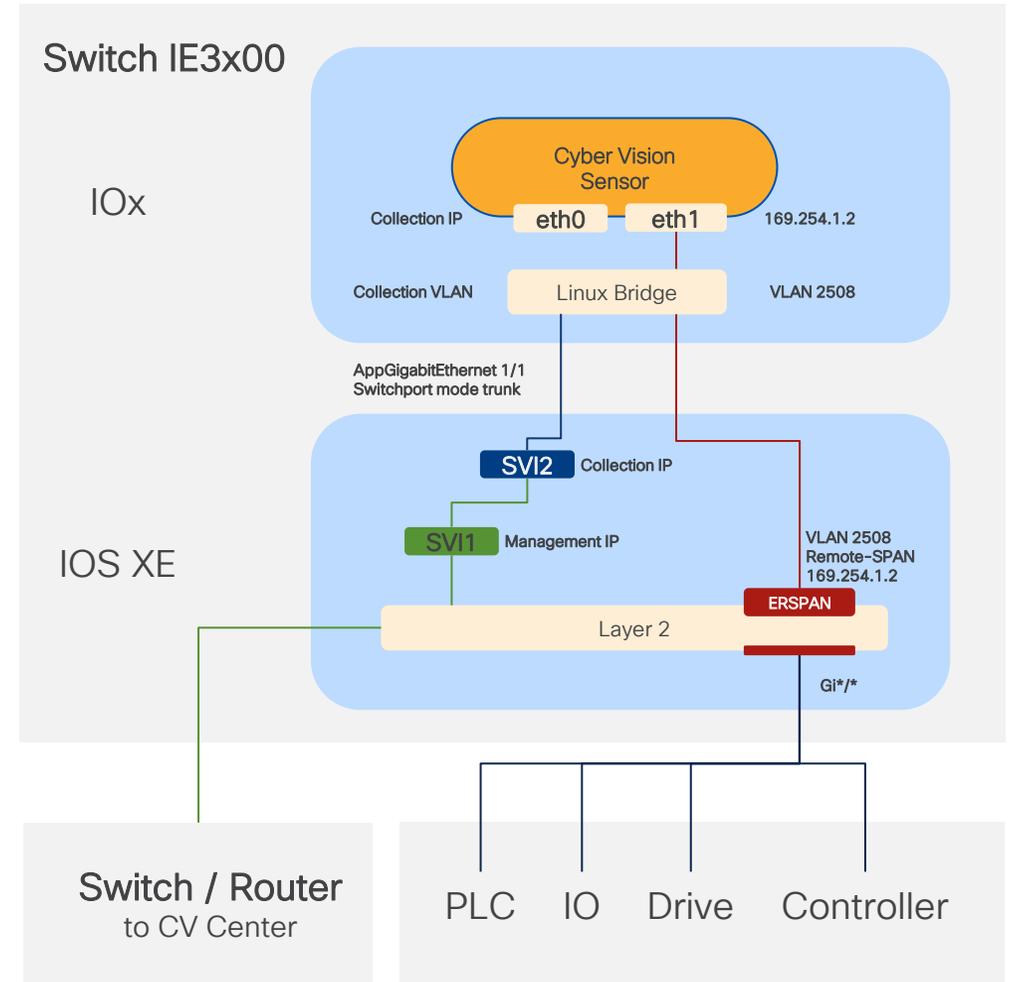
4. Create the new l3nat-iox config

app-ip <Sensor Coll_IP> svi-ip <Switch Mgmt_IP> app-name CCV-ONPREM server-ip <CV Center_IP>

Example:

```
l3nat-iox
 app-ip 169.254.0.2 svi-ip 192.168.49.28 app-name CCV-ONPREM server-ip 192.168.49.10
```

LIMITATION: Active discovery UNICAST only.



IE3x00 Sensor deployment

```
Switch(config)#monitor session 1  
source interface Gi1/3 – 10
```

Example leveraging physical interfaces

```
Switch(config)# monitor session 1  
destination remote vlan 998
```

Remote Span VLAN for sensor capture interface

```
Switch(config)# monitor session 1  
destination format-erspan  
172.16.0.30
```

ERSPAN Format – IP Address of sensor capture interface

Deploy IOx App

Cisco Cyber Vision Center will deploy the Cisco Cyber Vision IOx sensor application to your device. Please provide the IP address, port number, admin user and password to connect:

IP address: *

192.168.3.2

Port: *

Like 443 or 8443

443

User: *

admin

Password: *

••••••

Capture IP address: *

172.16.0.30

Capture subnet mask: *

Like 24, 16 or 8

24

Capture VLAN number: *

998

Collection IP address: *

192.168.6.30

Collection subnet mask: *

Like 24, 16 or 8

24

Collection gateway: *

192.168.6.1

Collection VLAN number: *

6

Capture mode:

Optional

+ Deploy

Cancel



IE3500 Sensor deployment – Monitoring Session

Note: The sensor on IE3500 is configured like for IE3400, except for the monitoring session!

Configuration example:

```
monitor session 1 type erspan-source
source interface Gi1/4 , Gi1/10
header-type 3
destination
erspan-id 2
mtu 9000
ip address 169.254.1.2
origin ip address 169.254.1.1
```

```
IE3500Perf#show monitor session all
Session 1
-----
Type                : ERSPAN Source Session
Status              : Admin Enabled
Source Ports        :
    Both             : Gi1/11
Destination IP Address : 169.254.1.2
MTU                  : 9000
Destination ERSPAN ID : 2
Origin IP Address    : 169.254.1.1
ERSPAN header-type   : 3

IE3500Perf#
```

Cyber Vision network-sensor

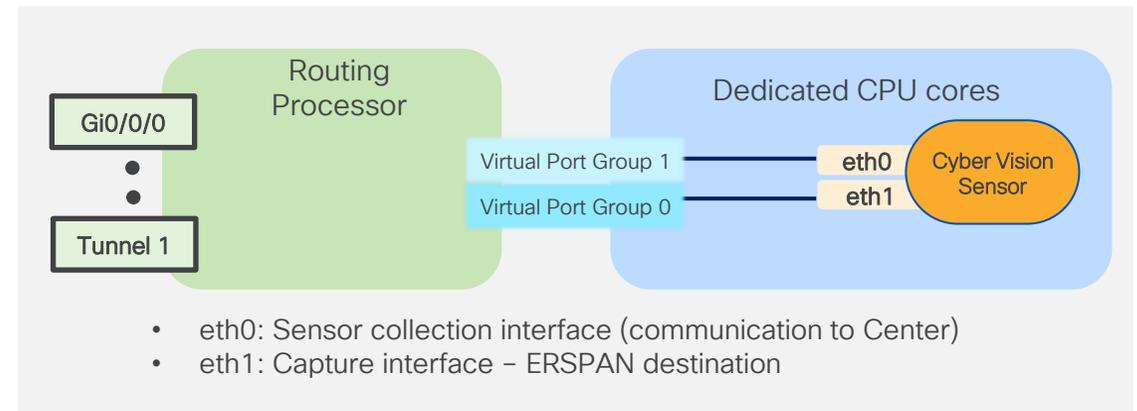
Cisco Catalyst IR1101/IR1800 Rugged Router

- Sensor is an application running in IOx on dedicated cores (no impact on performance)
- Embedded DPI eliminates the need for SPAN
- Traffic flowing through the router is copied to embedded Cyber Vision Sensor for DPI using internal ERSPAN session between IOS dataplane and IOx
 - Only traffic flowing through routed interfaces (GE and Tunnel) is subject to DPI
 - Locally switched traffic between LAN FE ports is not copied to Sensor
- Supported PPS: see [Performance Figures](#)
- Supported on base platform
- Storage required for Store & Forward and packet capture functionalities
 - IR1101: IRM-1100-SPMI + IR1100-SSD-100GB
 - IR1800: IRM-SSD-100G

Cyber Vision Sensor runs on IOx using dedicated cores of router CPU



Traffic flowing through routed interfaces is copied to embedded Cyber Vision Sensor for DPI



IR1101/IR18xx – Monitor configuration

```
Router(config)#monitor session 1 type  
erspan-source
```

Configure ERSPAN monitor session

```
Router(config-mon-erspan-src)# source  
interface tunnel 1
```

```
Router(config-mon-erspan-src)#  
no shut
```

Leverage Tunnel Interface as monitor source and no shut the source

```
Router(config-mon-erspan-src)#  
destination
```

```
Router(config-mon-erspan-src-dst)#  
erspan-Id 1
```

Set ERSPAN ID

```
Router(config-mon-erspan-src-dst)#  
mtu 1464
```

ERSPAN MTU

```
Router(config-mon-erspan-src-dst)#  
IP address 169.254.1.2
```

destination for ERSPAN (Capture IP Address of sensor application)

```
Router(config-mon-erspan-src-dst)#  
Origin IP address 169.254.1.1
```

Source for ERSPAN (IR1101 Interface IP)

Cyber Vision network-sensor

Cisco Catalyst IR8300 Rugged Router

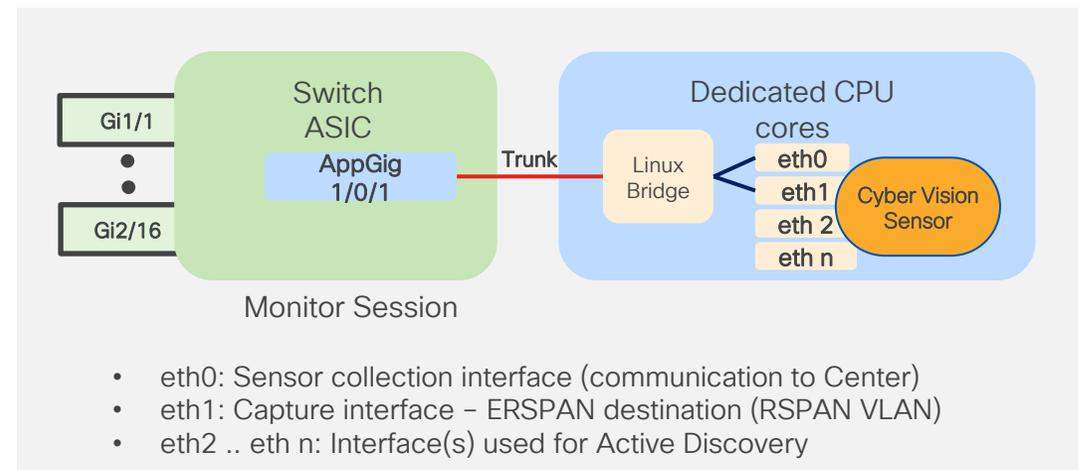
- Runs on Catalyst IR8300
 - see: [version requirements](#)
- Sensor is an application running in IOx on dedicated cores (no impact on performance)
- Supports Snort IDS with Advantage licenses (Talos subscriber rules available as an option)
- Typical deployment: Aggregation switch with multiple routing interfaces
- Supported PPS: see [Performance Figures](#)
- Storage (SSD or SD) required to support Store & Forward and packet capture functionalities
 - 100GB SSD: IRM-SSD-100G



Cyber Vision network-sensor

Cisco Catalyst IE9300 Rugged Series Switches

- Support for Catalyst IE9300 (see: [version requirements](#))
- Embedded DPI eliminates the need for SPAN
- Sensor is an application running in IOx on dedicated cores (no impact on performance)
- Traffic flowing through switch ports is copied to embedded Cyber Vision Sensor for DPI using internal ERSPAN session between IOS dataplane and IOx
- Supported PPS: see [Performance Figures](#)
- Can be deployed as access, aggregation, or as an out of band SPAN aggregation sensor
- Requires SD Card for application hosting

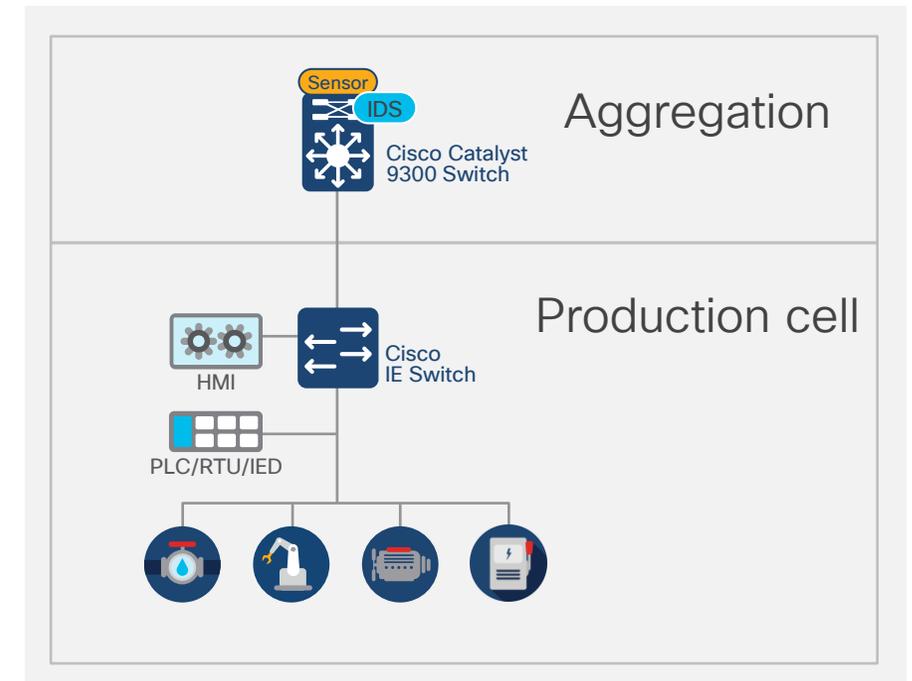


Cyber Vision network-sensor

Cisco Catalyst 9300/9300X/9400

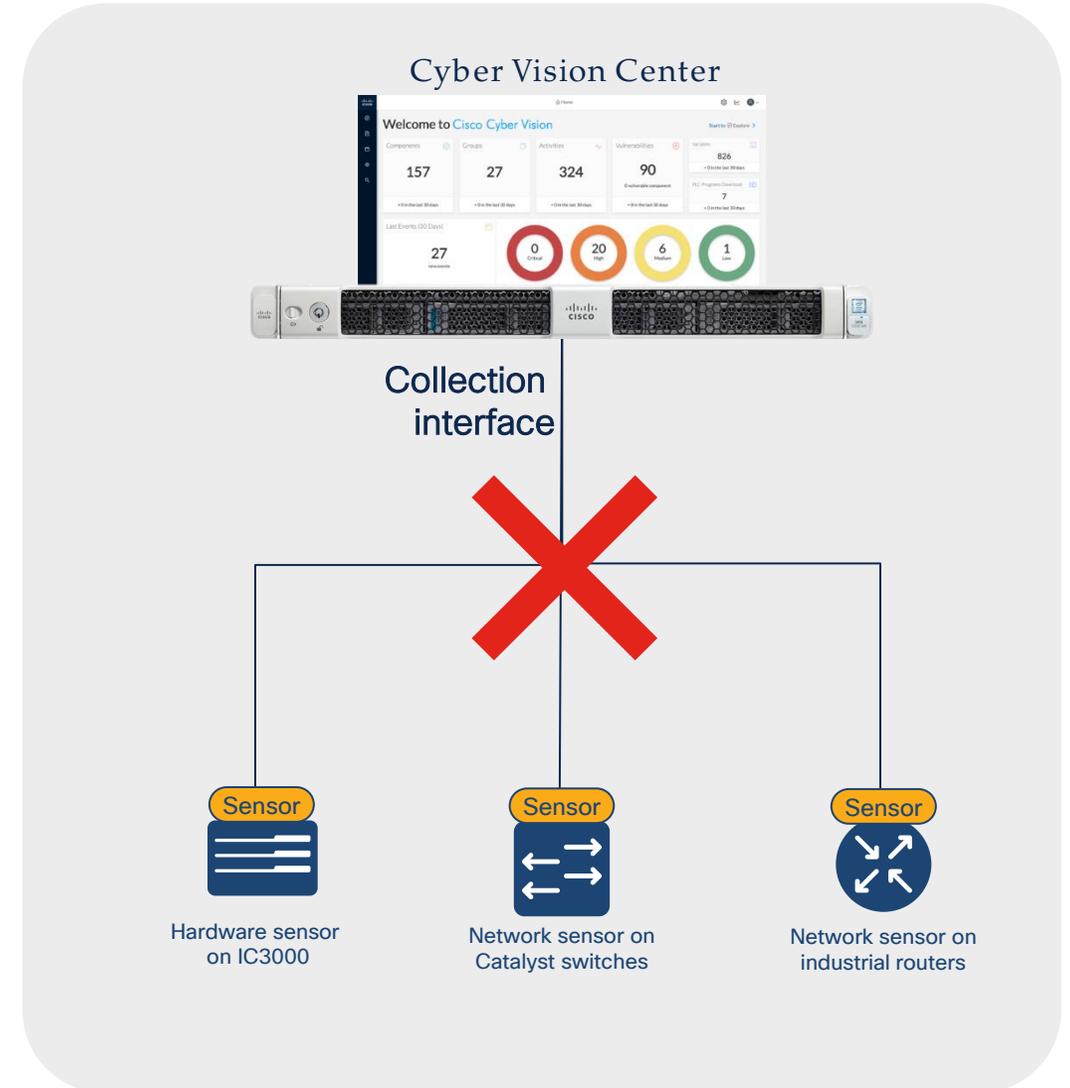
- Can be deployed as access, aggregation, core or as an out of band SPAN aggregation sensor
- Sensor is an application running in IOx
- Leverages ERSPAN to receive traffic from switch
- Supports Snort IDS with Advantage licenses (Talos subscriber rules available as an option)
- Supported PPS: see [Performance Figures](#)
- Catalyst 9300 and 9400
 - see: [version requirements](#)
 - Must support application hosting (DNA Advantage License required)
 - Does not require SSD to run Cyber Vision since version 4.4
 - SSD-240G needed for Store & Forward and packet capture functionalities
 - If no SSD disk is available, sensor is installed on bootflash. The disk-size needs to be set to “minimal-size”, for example:

```
app-resource docker  
run-opts 1 "--tmpfs /tmp:rw,size=128m"
```



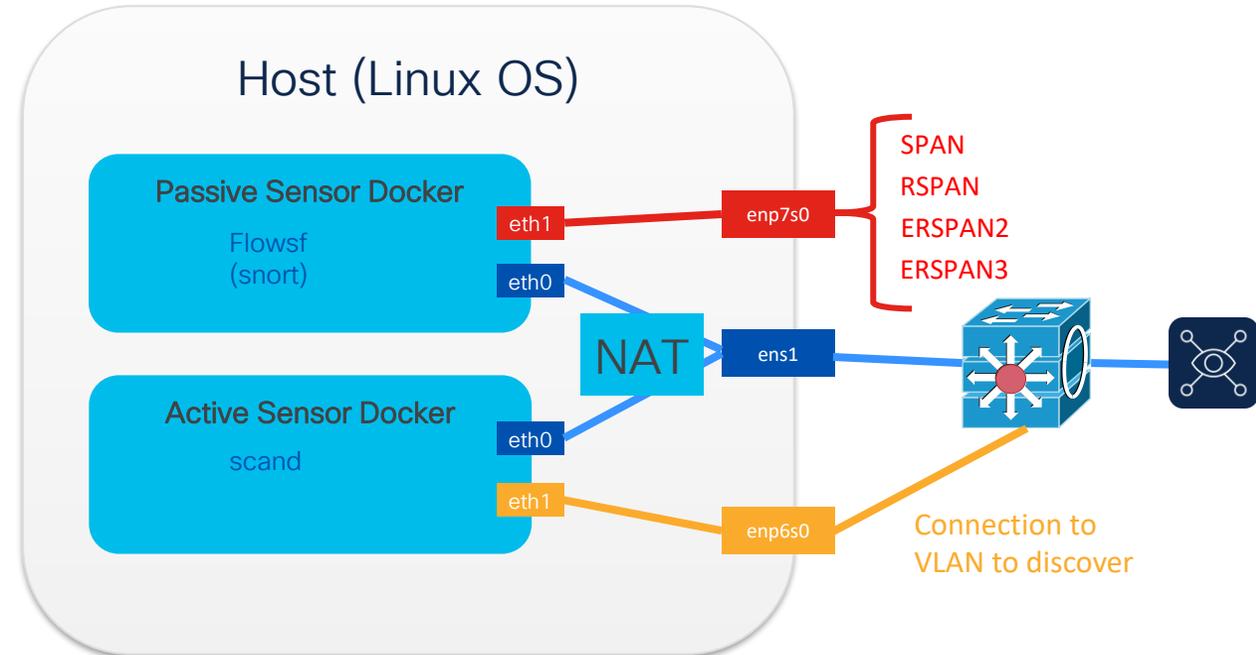
Store and Forward

- Sensor stores DPI data locally when connection to Center is lost
- Uploads data to Center when connection returns
- Eliminate loss of monitoring data



Cyber Vision Docker Sensor

- SPAN based solution to support brownfield: traffic capture and DPI on non-Cisco switches
- Lightweight Metadata from Sensor to Center eliminates need for dedicated span network
- Available for x86 and arm64 platforms
- All sensor features are supported: DPI, Active Discovery, and Snort IDS
- Scalability depends on the available resource on host



eth1 Docker interface will require an IP address in case of ERSPAN configuration

eth1 Docker interface will require an IP on each VLAN to discover

Cyber Vision Docker Sensor – Technical Summary

- Compatible with aarch64 and x86-64 devices
 - Ubuntu 24.04 recommended (also tested and verified with v22.04 and v20.04)
 - Docker for MacOS or Windows not supported for production environments
- Minimum of 1GB dedicated memory required
 - 2GB recommended (4GB if using the Snort IDS engine)
 - CPU and Memory allocation should be restricted
- Docker sensor host requires 2 network interfaces at the minimum (see previous slide)
 - Network interface must support promiscuous mode (“macvlan passthru” mode)
 - Interfaces specified in configuration files must exist on Docker host
- Required network communication
 - Host to CV Center ports: 443/80
 - Docker container instance to Center ports: 5671, 10514
- Storage allocation of Docker instance will grow over time

Cyber Vision Docker Sensor – Deployment

- The Cyber Vision Center is hosting a Docker registry
- After configuring the sensor, the Center will provide a docker-compose definition
- If Active Discovery is enabled, there will be two Docker instances
- Using the docker-compose definition, the sensor can be instantiated on the Docker host by pulling the image(s) from the Center, and register itself after starting

Deployment Phases:

1. Create Deployment Token and scope its reusability across sensor deployments
2. Configure the sensor in the Center (optionally configure Active Discovery)
3. Review and download the resulting docker-compose definition file
4. Instantiate the Docker container(s) using the compose file
5. The Docker instance will use the provided token to register itself in the Cyber Vision Center

Docker Sensor – Deployment Phase 1

Create Deployment Token and scope its reusability across sensor deployments

The screenshot shows the 'Add new deployment tokens' dialog box. The dialog has a title bar with a close button. Below the title bar, there is a 'From this' section with an '+ Add' button. The main form contains three required fields: 'Name' with the value 'Deployment01', 'Number of uses' with the value '4', and 'Expiration time' with the value '2025-05-01' and a calendar icon. Below these fields is an 'Enabled' toggle switch that is currently turned on. At the bottom of the dialog are 'Cancel' and 'Create' buttons.



The screenshot shows the 'New sensor' menu. At the top, there is a '+ New sensor' button and a 'Manage' icon. Below this, there are two main sections: 'Cisco IOx' and 'Other'. Under 'Cisco IOx', there are three options: 'Manual install', 'Install via extension', and 'Install via extension'. Under 'Other', there is a 'Docker sensors' option. At the bottom of the menu, there is a 'Docker01' option.

Docker Sensor – Deployment Phase 2

Configure the sensor in the Center

Sensor Application

Sensor Application

Name*
MyDockerSensor01

Deployment Token*
Phase 1 (4/25) [Create deployment token](#)

Sensor Mode*
Passive and Active Discovery

Collection Configuration

Container(s) will reach the center using NAT

Center is behind NAT



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](#)

Provide Name, Token, Sensor Mode

Provide interface configuration based on traffic type selected.



Docker Sensor – Deployment Phase 3

Optionally configure Active Discovery

Active Discovery

Common configuration:

Active Discovery Interface*

e.g. eth2

Target interface:

CIDR* <input type="text" value="192.168.66.12/24"/> <small>e.g. 192.168.1.1/24</small>	VLAN <input type="text" value="66"/> <small>1-4095</small>		+ Add a new target
CIDR* <input type="text" value="192.168.69.12/24"/> <small>e.g. 192.168.1.1/24</small>	VLAN <input type="text" value="69"/> <small>1-4095</small>		

Configure the Active Discovery interface of the standalone docker instance.

Docker Sensor – Deployment Phase 4

Review and download the resulting docker-compose configuration file

```
Docker Compose

Please ensure that this configuration really fits to your hardware, especially resources allocations

Download Docker Compose file Copy

1  services:
2    ccv-sensor-1:
3      image: center162.443/sensor
4      container_name: ccv-sensor-1
5      restart: always
6      pull_policy: always
7      environment:
8        - SERIAL_NUMBER=MyDockerSensor01-enp6s0.40
9        - PROVISIONING_TOKEN=
10     2Vuc29yMDEtZW5wNmMwLjQwIiwIY2VudG
11     _cj0c2Y07RE0-u1ekT8
12     - ERSPAN_TYPE=2
13     cap_add:
14       - NET_ADMIN
15     networks:
16       ccv-network-0-collection: {}
17       ccv-network-capture-1:
18         ipv4_address: 192.168.40.22
19     volumes:
20       - ccv-volume-1:/data
21     ccv-sensor-2:
22       image: center162.443/sensor
23       container_name: ccv-sensor-2
24       restart: always
25       pull_policy: always
26       environment:
27         - SERIAL_NUMBER=MyDockerSensor01-enp7s0
28         - PROVISIONING_TOKEN=
29     DhHWuKh4YedVemQ
30     cap_add:
```

Review the docker-compose file. Please make sure, that all the settings are valid. Double-check especially the interfaces settings and the Tokens provided.

Docker Sensor – Deployment Phase 5

Instantiate the docker container(s) using the compose file (**green**)

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 <sensor-name> /bin/bash</code>	Provides CLI access to the running docker instance.
Stopping a docker sensor	<code>docker stop <sensor-name></code>	Stopping a running docker container.
Listing all docker container instances	<code>docker ps -a</code>	Comprehensive list of all instantiated containers on the host.
Start/Stop an existing docker sensor	<code>docker start <sensor-name></code> <code>docker stop <sensor-name></code>	Change the state of operation of an existing instance of a docker sensor.
Remove an instance	<code>docker rm -fv <sensor-name></code>	Remove a specific docker container instance.
Check the logs	<code>docker compose logs</code>	Will return the runtime logging of a container instance.

Docker Sensor – Deployment Phase 6

The Docker instance will use the provided token to register itself in the center

Check the sensor management page on the CV Center to check on the operational status of the Docker sensor.

<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Update status	Location	Health status	Processing status
<input type="checkbox"/>	Docker01	Docker01		5.1.0			Connected	Normally pro
<input type="checkbox"/>	Docker02-active	Docker02-active		5.1.0			Connected	Normally pro

Docker01

Label: Docker01

Serial Number: Docker01

IP address: -

Version: 5.1.0+202410032313

System date: Oct 14, 2024 5:56:42 PM

Deployment: Docker (Zero Touch Provisioning)

Active Discovery: Unavailable

Capture mode: All

Template: Default

System Health

Status: **Connected**

Processing status: **Normally processing**

Uptime: 3 days

[Go to statistics](#)

[Start Recording](#)

[Move to](#)

[Download package](#) [Capture mode](#)

[Disable IDS](#) [Uninstall](#)

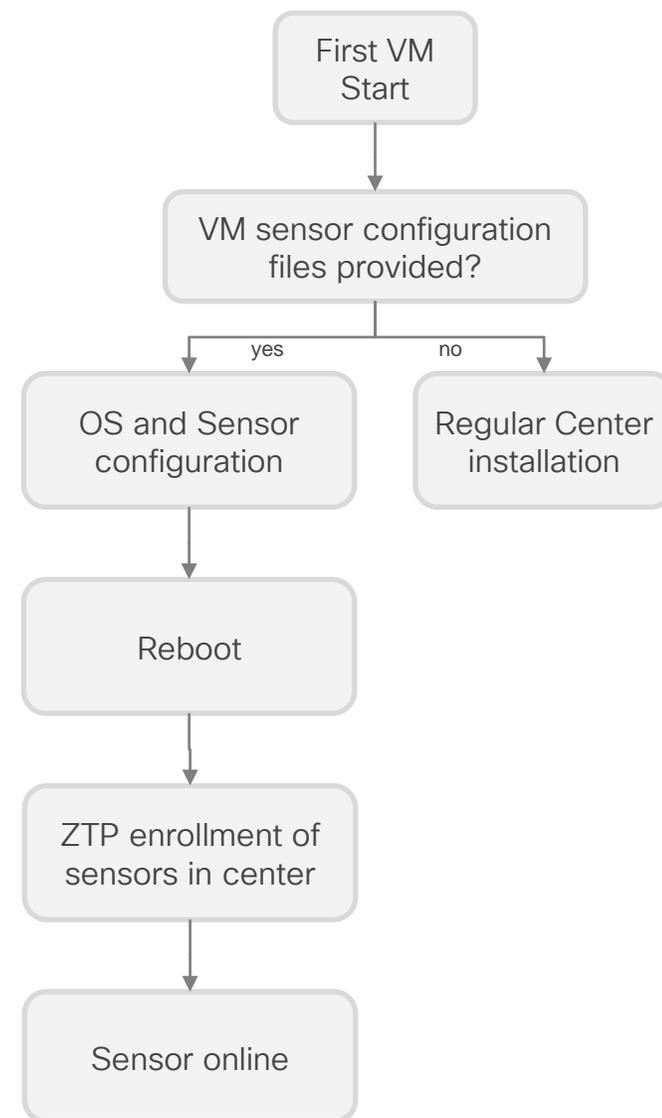
[Update](#)

Cyber Vision VM Sensor – Technical Summary

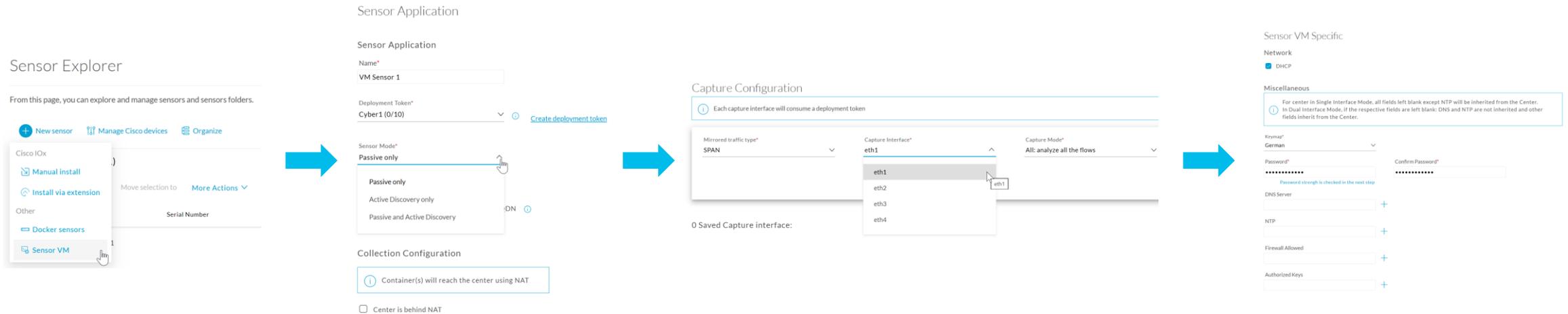
- Compatible with x86-64 devices
 - VMWare v6.x required
 - Minimum of 4GB dedicated memory required (8GB recommended)
 - Minimum of 2 dedicated CPU cores required
- Required network communication
 - Host to CV Center ports: 443/80
 - VM instance to Center ports: 5671, 10514
- Storage allocation of instance will grow over time

Cyber Vision VM Sensor – Deployment Process

- **Targeted scenario:** sensor deployments similar to Docker sensor deployments
- Sensors deployed as VM, leveraging the same base-image as a center deployment
- Same minimum technical requirements like for VM based center deployment for the virtualization stack
- Initialization process:
 - Create image for VM deployment in the center, following the process of creating new sensor
 - Provide image to your hypervisor
 - VM verifies on boot, if VM sensor configuration files were provided
 - If no sensor configuration was provided, setup will proceed to install center
 - If sensor configuration was provided,
 - OS and sensor instances are configured
 - VM rebooted
 - Automatic ZTP enrollment on center
 - Sensors change into “online” operation mode



Cyber Vision VM Sensor – Deployment Process



- The network interfaces are pre-determined by the standard interfaces of the image vs. the host interfaces in a docker-based setup.
- The configuration finishes with the ability to download an .iso image. This image needs to be provided during initialization of the VM to parametrize the starting instance with the configurational choices made.
- With the configuration file provided, the booting sensor VM will automatically onboard itself to the center.

SEA Agent Integration

Single integrated IOx App for Cyber Vision and SEA

- As of Cyber Vision 5.3, the SEA Agent can be integrated in the Cyber Vision Sensor
- The integrated application is deployed on the network from Cyber Vision Center
- Cyber Vision Center integrates with SEA cloud for token exchange to authenticate the SEA Agent
- Users log into SEA and the Cyber Vision Center independently with Single Sign-On
- Docker deployments are not supported. See [datasheet](#) for the list of supported platforms

The screenshot displays the 'Secure Equipment Access' configuration page. It includes a 'Configuration' section with fields for Region (Europe), Organization Name (ccv team), Organization ID (f90be2a2), API Key ID (ccv team), and API Key Secret. Below this is the 'SEA proxy configuration' section with radio buttons for 'Use the Center as Proxy' (selected), 'Direct', and 'Proxy Form'. A 'Reset' button and an 'Enable SEA' button are also visible.

The lower part of the screenshot shows a table titled 'Folders and sensors (1)'. The table has columns for Label, Serial Number, IP Address, Version, Update status, Location, Health status, Processing status, Active Discovery, and Secure Equipment Access. A single sensor is listed with the label 'IE-3400-8T2S+FOC2417V07Z', IP address 192.168.49.136, version 5.3.0, and a green checkmark in the Update status column. Below the table, there is a section for 'Network Device Name', 'SEA Agent Installed By', 'SEA Agent Connection', and 'Agent Version'. The installed by is 'Cyber Vision' and the connection status is 'Up' with a green checkmark.

Label	Serial Number	IP Address	Version	Update status	Location	Health status	Processing status	Active Discovery	Secure Equipment Access
IE-3400-8T2S+FOC2417V07Z	FOC2417V07Z	192.168.49.136	5.3.0	✔		Connected	Normally processing	Enabled	Enabled

Network Device Name	SEA Agent Installed By	SEA Agent Connection	Agent Version
IE-3400-8T2S+FOC2417V07Z	Cyber Vision	✔ Up	0.85-06210c

Performance

Cisco Cyber Vision scale - Center

Per Cyber Vision Center	CV-CNTR-M6N
Max number discovered components	50,000
Max number of flows stored	16 million
Max number of sensors managed	300

Per Global Center	CV-CNTR-M6N
Max number of registered Centers	20
Max number of components synced	150,000



Cisco Cyber Vision scale – Sensors

Platform	Max packet per second	Max number of flows stored
IC3000	12,000	15,000
IE3300/IE3400	12,000	12,000
IE3500	13,000	12,000
IR1101/IR1835	13,200	16,500*
IR8300	15,000	16,500*
IE9300	13,000	12,000
Catalyst 9300/9400	30,000	21,000
Center DPI	300,000	Match Center

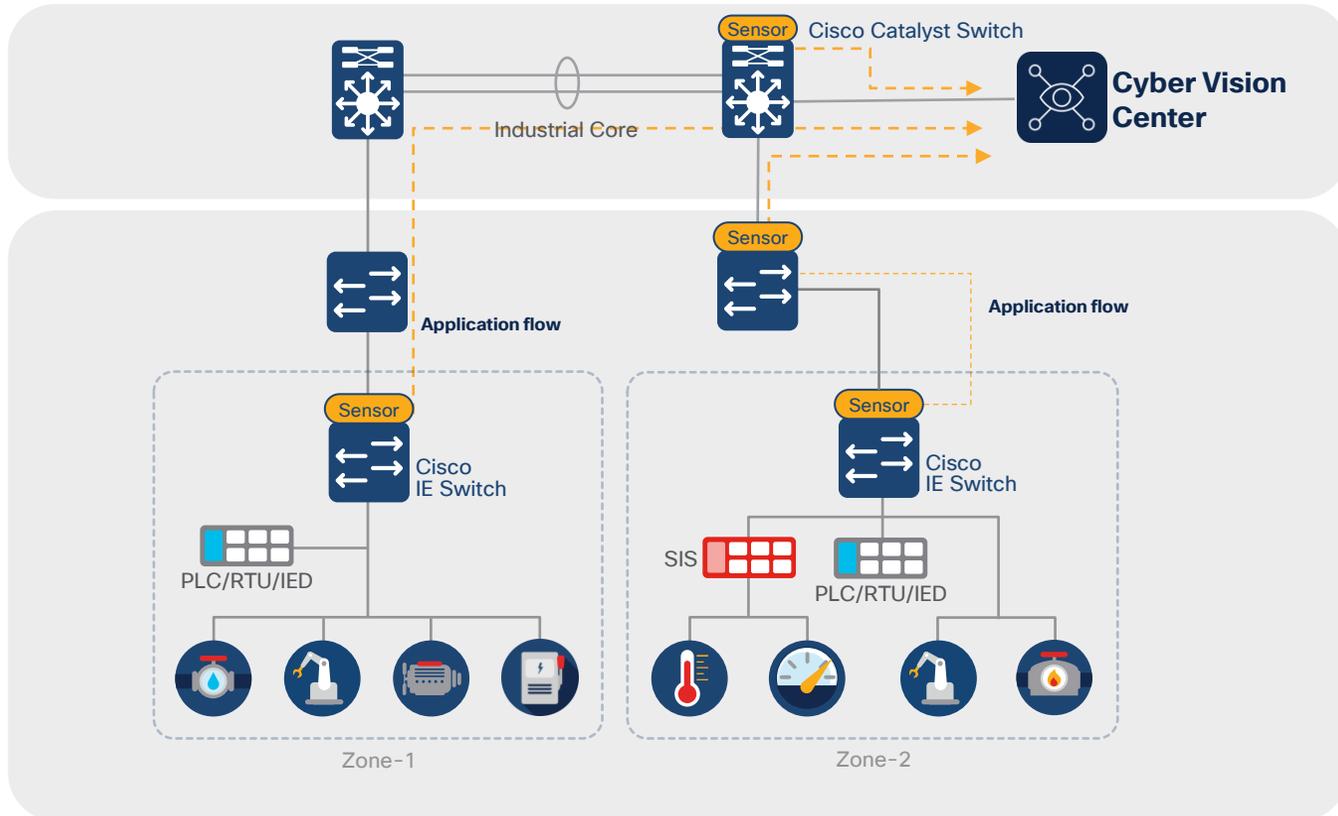
12,000 pps @ average packet size of 750 bytes ~ 70 Mbps

12,000 pps @ average packet size of 1500 bytes ~ 140 Mbps

* With 100GB SSD installed – storage required to support Store and Forward

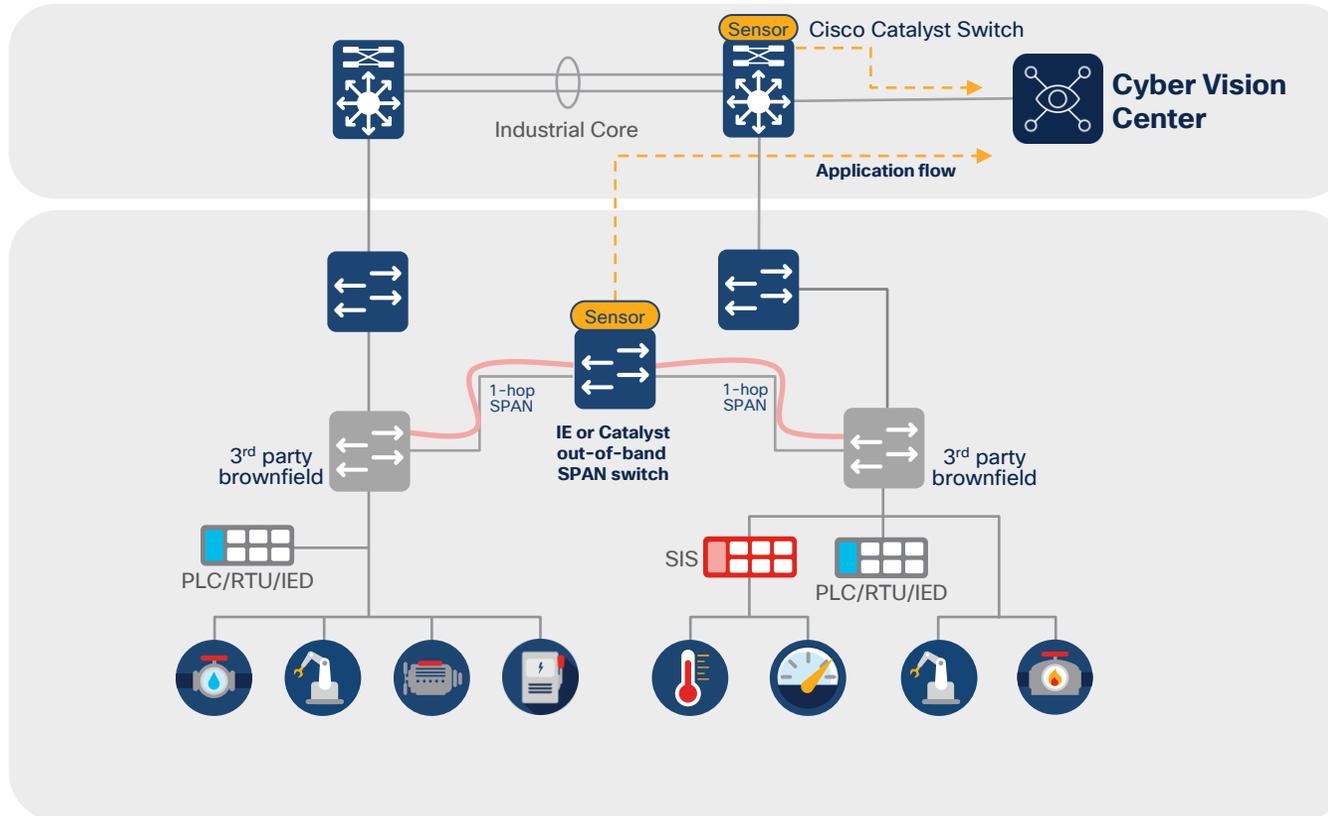


Embedded Sensor



- Embedded Sensor on IE3400 and Catalyst 9300 to capture traffic directly on switches where traffic is passing
- Enables full visibility without requiring additional cabling
- Environment and Scale deciding factor for IE3400 or Catalyst 9300

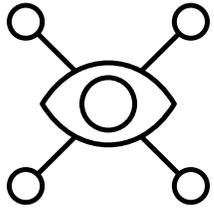
Out-of-Band Collection



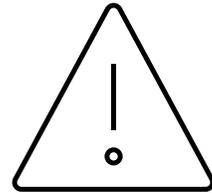
- Embedded Sensor on IE3400 and Catalyst 9300 can be leveraged as out of band sensor
- Enables aggregation of multiple SPAN sessions from across infrastructure
- Environment and scale are deciding factors for IE3400 or Catalyst 9300
- Unlike other solutions that require SPAN all the way to the monitoring appliance, the Cyber Vision solution for brownfield has lower TCO because it leverages the existing network and only requires 1-hop of SPAN traffic

The Cyber Vision Workflow

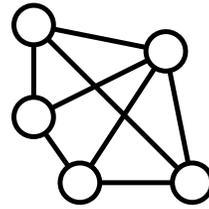
You cannot secure what you don't know



List all the assets you are defending



Spot vulnerabilities to patch



Identify asset communication issues



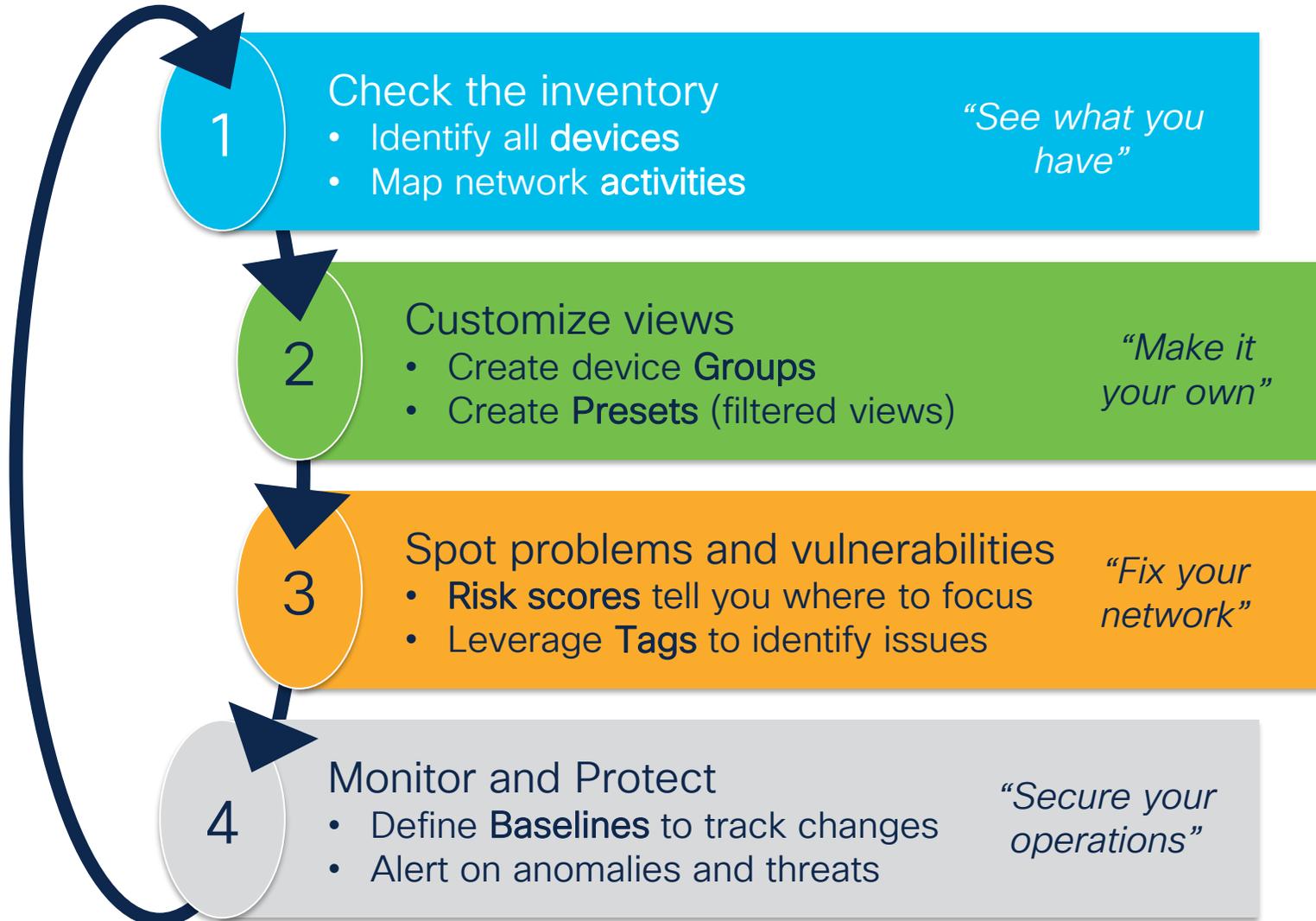
Detect bypass or leaks in the IDMZ



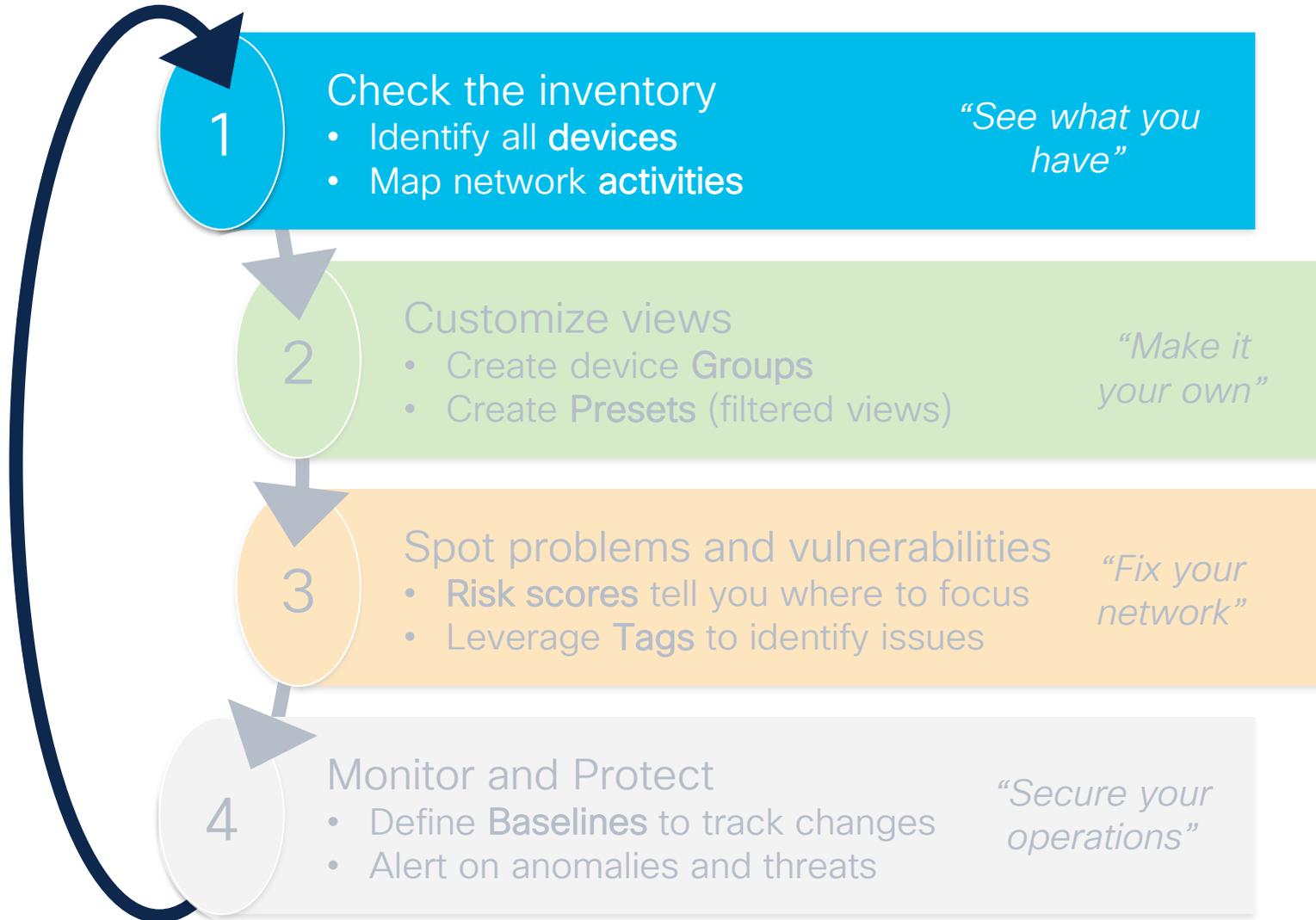
Build compliance reports

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

The Cyber Vision Workflow



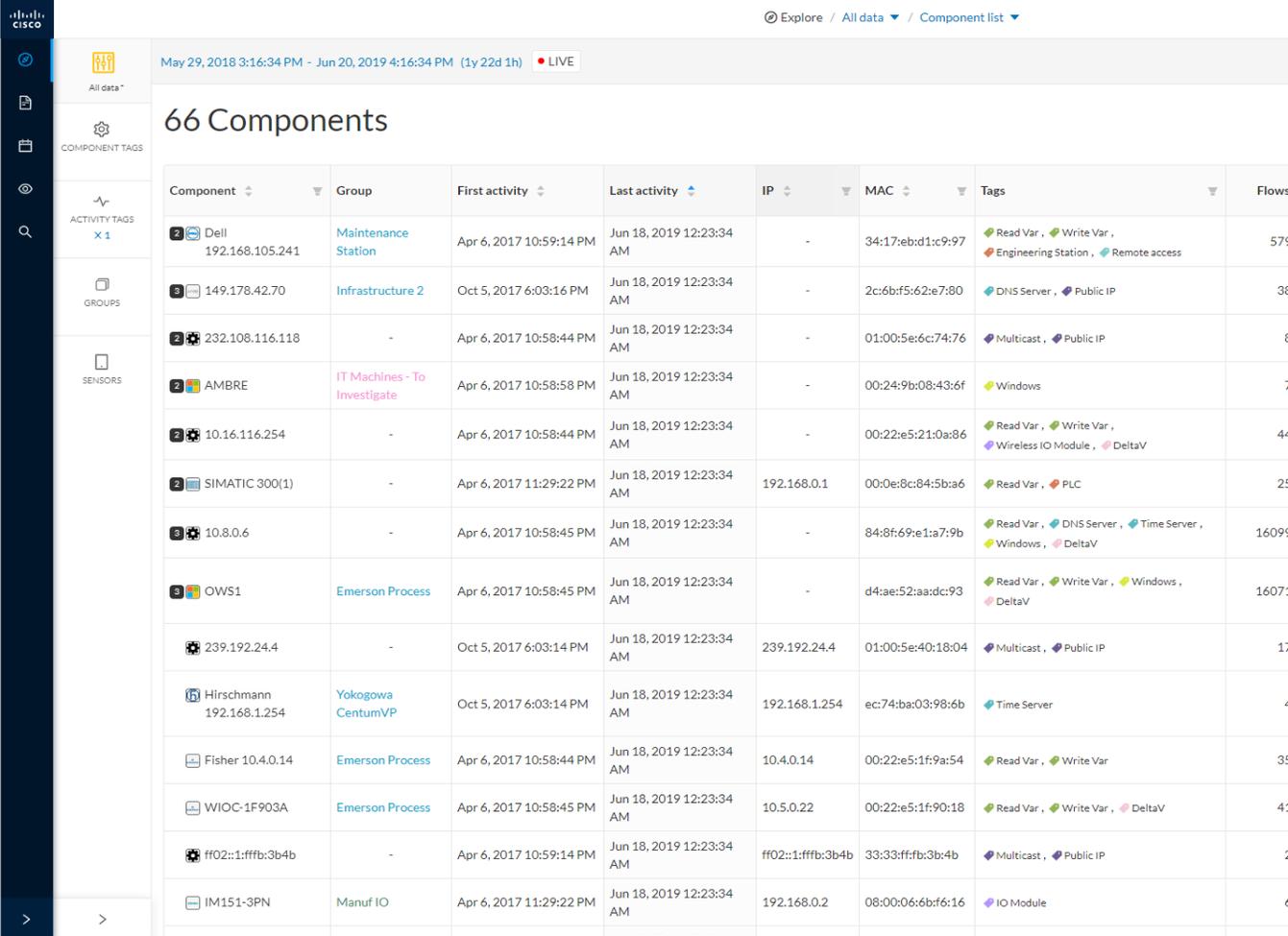
The Cyber Vision Workflow



Comprehensive asset inventory

- Automatically maintain a detailed list of all OT and IT equipment
- Immediate access to software and hardware characteristics
- Track rack-slot components
- Tags make it easy to understand asset functions and properties

Track industrial assets to protect throughout their life cycles



May 29, 2018 3:16:34 PM - Jun 20, 2019 4:16:34 PM (1y 22d 1h) LIVE

66 Components

Component	Group	First activity	Last activity	IP	MAC	Tags	Flows
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	-	34:17:eb:d1:c9:97	Read Var, Write Var, Engineering Station, Remote access	579
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6b:f5:62:e7:80	DNS Server, Public IP	38
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	01:00:5e:6c:74:76	Multicast, Public IP	8
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:34 AM	-	00:24:9b:08:43:6f	Windows	7
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	00:22:e5:21:0a:86	Read Var, Write Var, Wireless IO Module, DeltaV	4
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.1	00:0e:8c:84:5b:a6	Read Var, PLC	25
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	84:8f:69:e1:a7:9b	Read Var, DNS Server, Time Server, Windows, DeltaV	16099
OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4:ae:52:aa:dc:93	Read Var, Write Var, Windows, DeltaV	1607
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	239.192.24.4	01:00:5e:40:18:04	Multicast, Public IP	17
Hirschmann 192.168.1.254	Yokogawa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	192.168.1.254	ec:74:ba:03:98:6b	Time Server	4
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	10.4.0.14	00:22:e5:1f:9a:54	Read Var, Write Var	35
WIOC-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	10.5.0.22	00:22:e5:1f:90:18	Read Var, Write Var, DeltaV	41
ff02::1:fffb:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	ff02::1:fffb:3b4b	33:33:ff:fb:3b:4b	Multicast, Public IP	2
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.2	08:00:06:6b:f6:16	IO Module	6

Detailed information on assets

The screenshot displays the Cisco Duo interface for a specific asset. At the top, the asset is identified as a 'PLC' from 'Munich' with IP '192.168.249.50' and MAC 'f4:54:33:91:cb:ee'. It shows activity dates from Sep 10, 2020 to Jan 19, 2022. A summary bar indicates 4 activities, 42 events, and 10 vulnerabilities. Below this, the 'Properties' section is divided into 'Normalized Properties' and 'Other Properties'. The 'Normalized Properties' section lists details like 'fw-version: 31.11, 31.011', 'ip: 192.168.249.50', 'mac: f4:54:33:91:cb:ee', and 'name: 1769-L16ER/B LOGIX5316ER, SecDemo_LinePLC, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)'. The 'Other Properties' section includes 'enip-cpuname: SecDemo_LinePLC', 'enip-devicetype: ProgrammableLogicController, GeneralPurposeDiscreteIO', and 'enip-version: 31.11, 31.011'. At the bottom, a '4 Components' table lists the following data:

Component	First activity	Last activity	IP	MAC	Tags	Vulnerabilities	Flows	VLAN ID	Sensor
1769-L16ER/B LOGIX5316ER	Sep 10, 2020 3:36:38 PM	Jan 19, 2022 2:00:01 AM	192.168.249.50	f4:54:33:91:cb:ee	Controller	10	-10	-	
SecDemo_LinePLC	Sep 10, 2020 3:36:41 PM	Jan 19, 2022 2:00:01 AM	192.168.249.50	f4:54:33:91:cb:ee	Controller	10	-10	-	
24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)	Sep 10, 2020 3:36:41 PM	Jan 19, 2022 2:00:01 AM	192.168.249.50	f4:54:33:91:cb:ee	No tags	0	-10	-	
1769-L16ER/B LOGIX5316ER	Sep 10, 2020 3:36:37 PM	Jan 19, 2022 2:00:01 AM	192.168.249.50	f4:54:33:91:cb:ee	Controller, Rockwell Automation	10	-20	-	

Insights on risks, vulnerabilities, communications, variables, etc.

Tags to easily understand characteristics, activities, and threats

Asset characteristics, version and network configuration

Control logic properties

Rack slot component details

Operational insights for OT teams

- Detailed asset properties
- Communication maps
- PLC program changes
- Variable accesses

Monitor the integrity of your industrial process

Component

SIMATIC 300(1)
 IP: 192.168.0.1
 MAC: 00:0e:8c:84:5b:a6

First activity: Apr 6, 2017 11:29:22 PM
 Last activity: May 26, 2019 12:21:13 AM

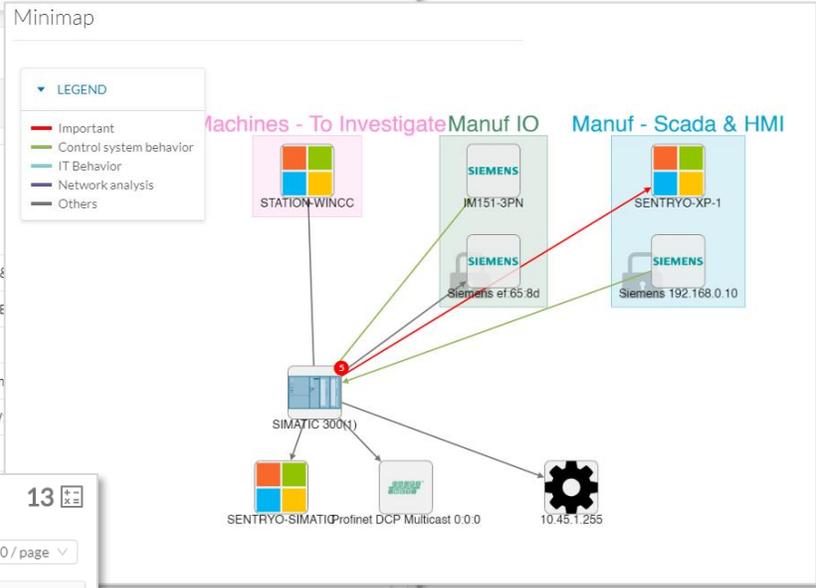
24 Flows, 51 Events, 5 Vulnerabilities, 13 Variables

Basics Security Activity Automation

Properties Tags

Properties

Vendor-Name: Siemens AG A&D ET
 Model-Name: CPU 315-2 PN/DP
 Fw-Version: V 2.5.0
 Hw-Version: 3
 Model-Ref: 6ES7 315-2EH13-0AB0
 Serial-Number: S C-V1R583472007
 Name: SIMATIC 300(1)



Variables accesses

13

Variable	Types	Accessed by	First access	Last access
> M 2.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
▼ M 2.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	Siemens 192.168.0.10	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	SENTRYO-XP-1	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M 8.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M 8.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M 8.2	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM



Operational insights for security analysts

- Access the full history of all communication flows
- View detailed properties and content statistics for each flow
- View live information or go back in time for forensic search

Flows

From	Source Port	To	Destination Port	First activity	Last activity	Tags	Packets	Bytes
Siemens 192.168.105.120	102	PLC_1	49158	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
PLC_1	102	Dell 192.168.105.241	1613	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	Program Upload, Start CPU, Stop CPU, Read Var, Write Var ...1+	0	0 B
PLC_3	102	PLC_1	49159	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
Siemens 192.168.105.120	102	PLC_1	49158	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
Siemens 192.168.105.120	0	PLC_1	0	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	ARP	0	0 B
PLC_3	0	PLC_1	0	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	ARP	0	0 B
PLC_1	102	Dell 192.168.105.241	1611	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	Program Upload, Read Var, Write Var, S7Plus	0	0 B

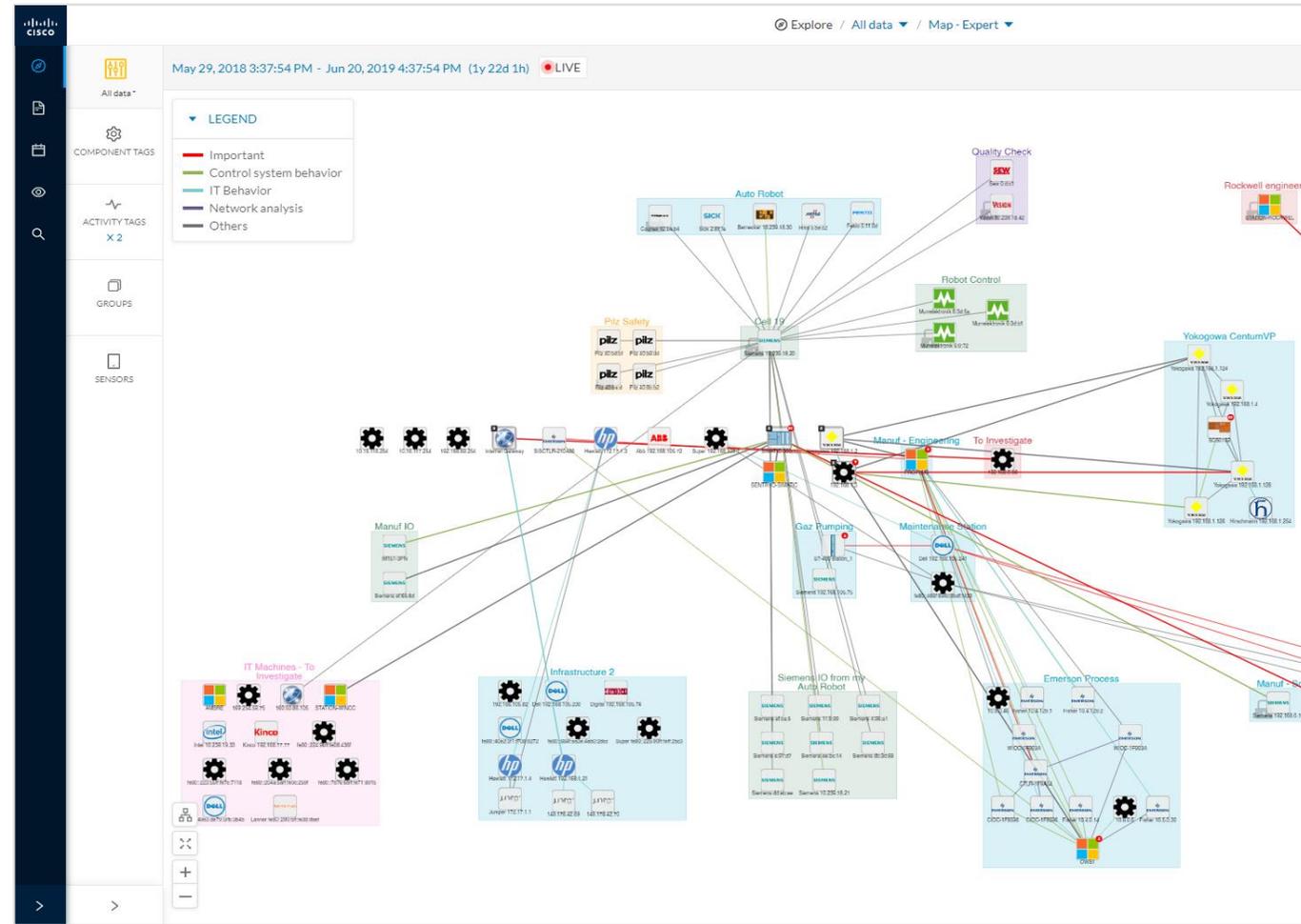
Content Statistics

Property	Value	Occurrences
emerson-udp-event	setvar	7
emerson-udp-function	KeepAlive	1
emerson-udp-function	Message	7
emerson-udp-var-name	PID1/MODE	1
emerson-udp-var-name	PID1/SP	6
emerson-udp-var-scope	CV	6
emerson-udp-var-scope	TARGET	1
emerson-udp-var-value	49.52	1
emerson-udp-var-value	49.97	1
emerson-udp-var-value	69.97	1
emerson-udp-var-value	70	1
emerson-udp-var-value	70.41	1
emerson-udp-var-value	72	1
emerson-udp-var-value	AUTO	1
ipv4-ttl	128	1
ipv4-ttl	64	1

Detailed communication maps

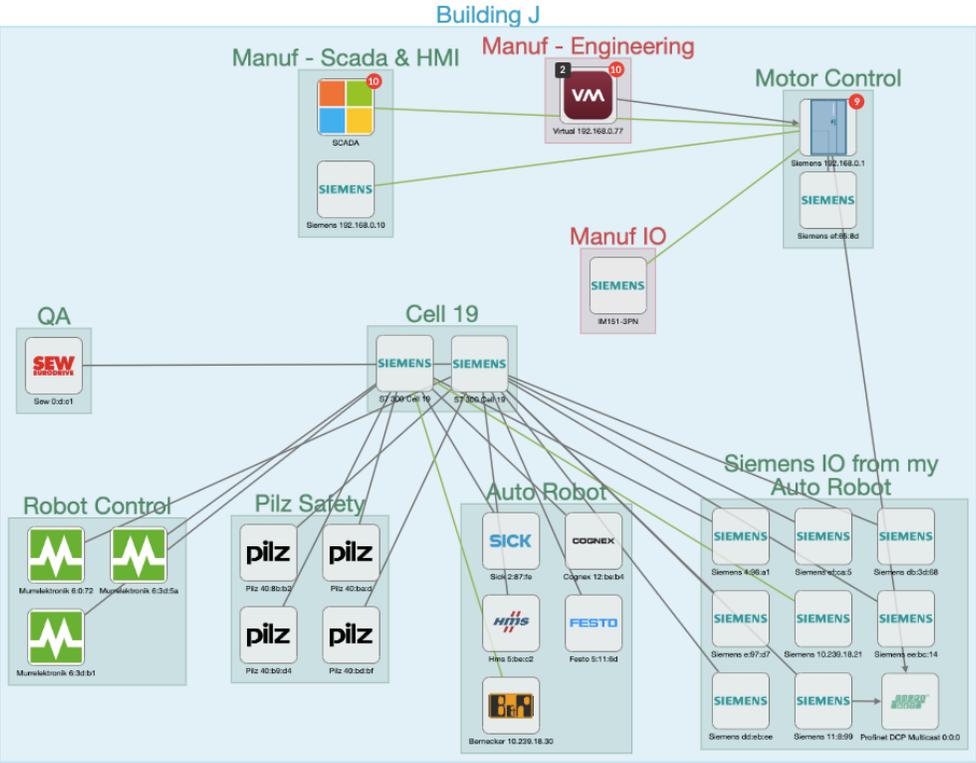
- Identify all relations between assets including application flows
- Pinpoint IDMZ leaks, shadow IT, and rogue remote access activities
- Spot unwanted communications, intrusions, and abnormal behaviors
- Tags make it easy to understand the content of each communication flow
- View live information or go back in time

Monitor industrial network hygiene and drive segmentation



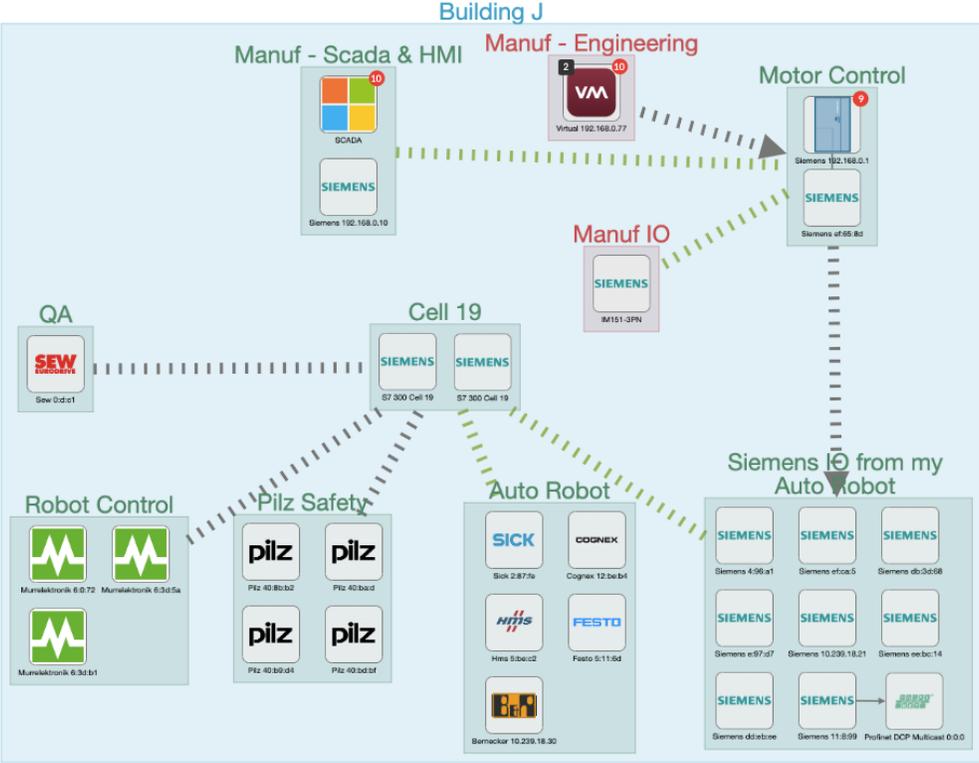
Aggregated activities match ISA/IEC 62443 conduits

Unaggregated



View all asset relationships

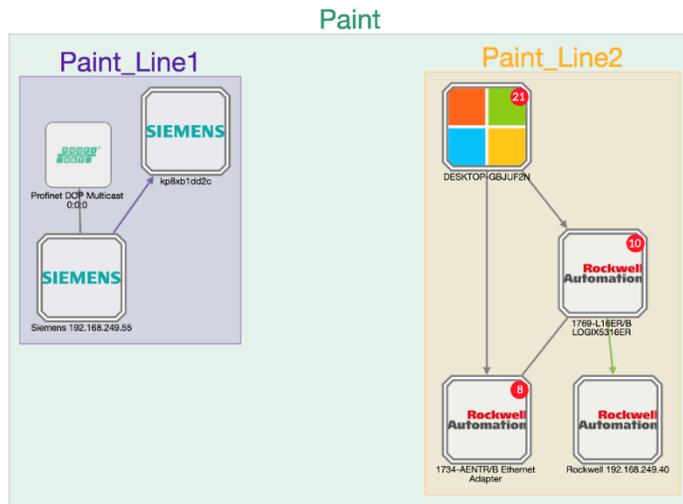
Aggregated



Easily browse and filter conduits including sub-zones

Aggregated components match the physical inventory

Map view



Double-border icons indicate a device with multiple components

ID Cards

Controller Rack

1769-L16ER/B LOGIX53...
Paint_Line2 high
IP: 192.168.249.50
MAC: f4:54:33:91:cb:ee

First activity: Apr 28, 2021 11:48:40 AM
Last activity: Apr 28, 2021 11:48:46 AM

Sensor: -

Tags: Controller, Rockwell Automation

Activity tags: Read Var, Write Var, Low Volume, CIP-IO, EthernetIP

Risk score: 80% See details

Modules:
Rockwell 192.168.249.50
Rockwell 192.168.249.50
Rockwell 192.168.249.50
Rockwell 192.168.249.50
24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)
Rockwell 192.168.249.50
1769-L16ER/B LOGIX5316ER
SecDemo_LinePLC | 1769-L16ER/B LOGIX5316ER
Rockwell 192.168.249.50

Properties:
fw-version: 31.011
ip: 192.168.249.50
mac: f4:54:33:91:cb:ee
model-ref: 24VDC 16PT INPUT & 16PT OUTPUT, 1769-L16ER/B LOGIX5316ER
name: Rockwell 192.168.249.50, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01), 1769-L16ER/B LOGIX5316ER...
... show more

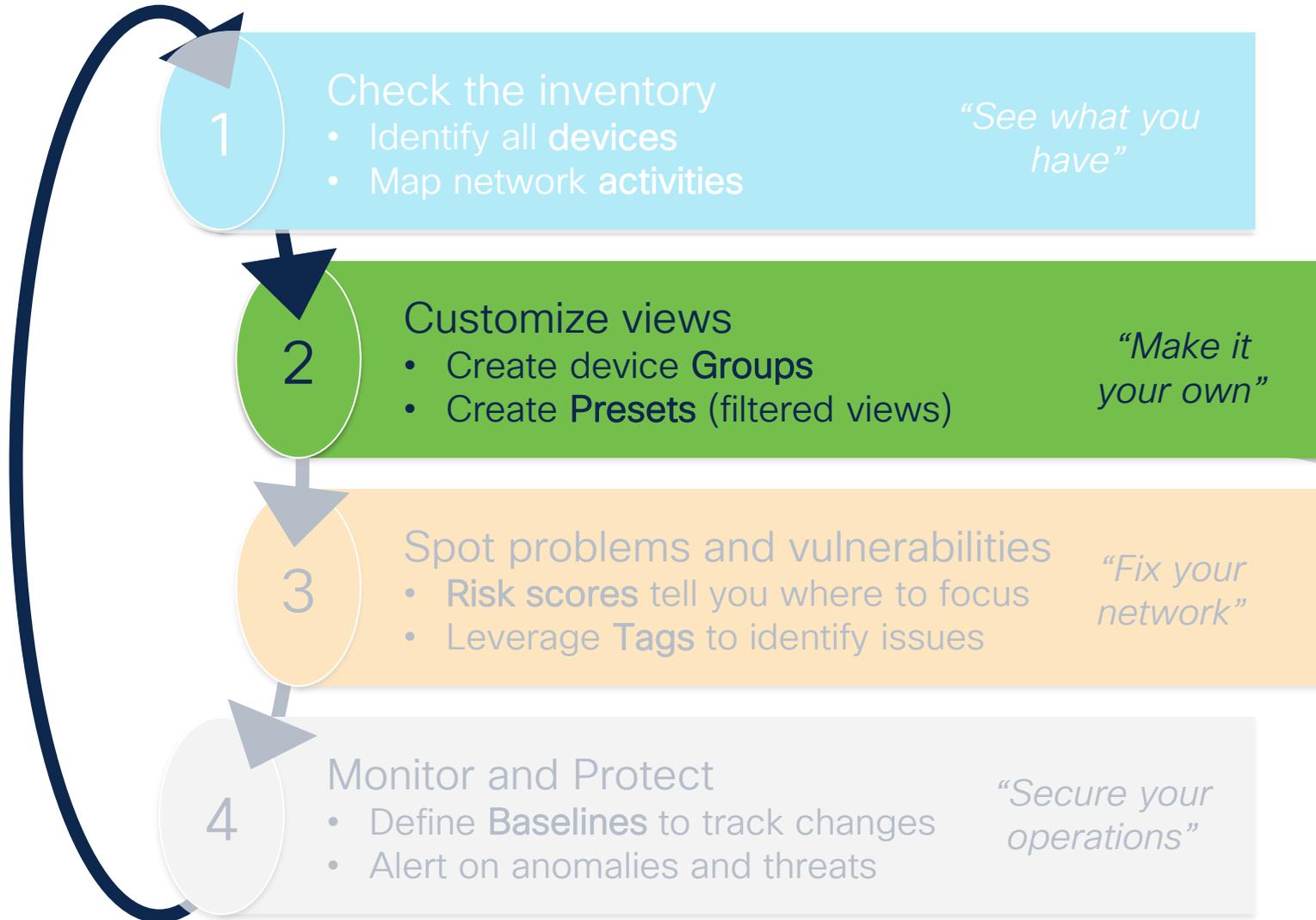
Technical Sheets

8 Components

Component	First activity	Last activity	IP	MAC	Tags	Vulnerabilities	Flows	VLAN ID	Sensor
1756-L55/A 1756-M12/A LOGIX5555 (Port1-Link00)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	Controller	2	-10	-	
1756-OB16/A DCOU ISOL (Port1-Link04)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	
1756-IB16/A DCIN ISOL (Port1-Link03)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	
1756-IB16/A DCIN ISOL (Port1-Link02)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	
1756-OB16/A DCOU ISOL (Port1-Link05)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	
SUBSTATION-119-PLC01	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	9	-10	-	
1756-ENBT/A (Port1-Link01)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	9	-10	-	
Rockwell 192.168.0.200	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	

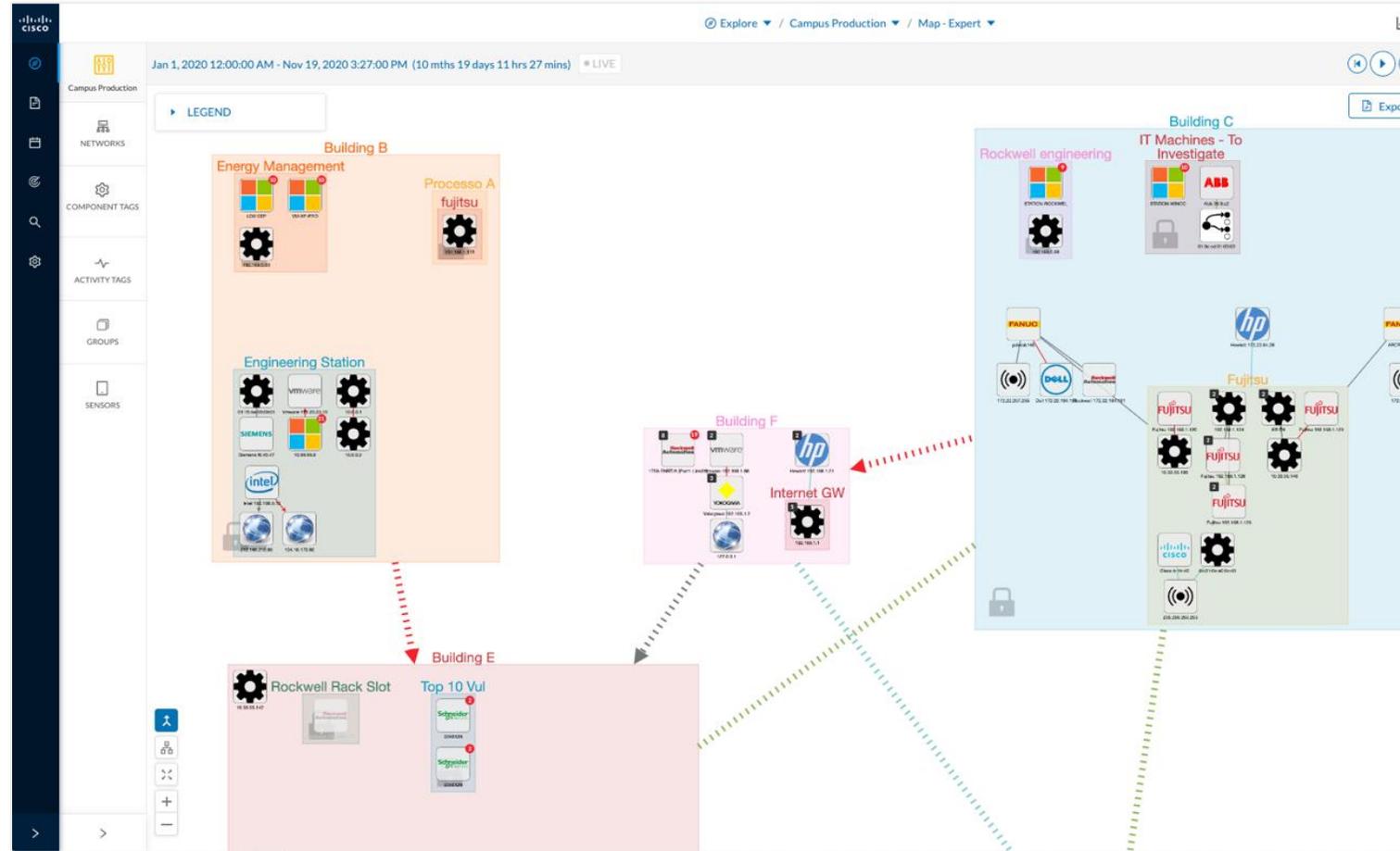
Easily list the components of a device. Click on a component to view more details

The Cyber Vision Workflow



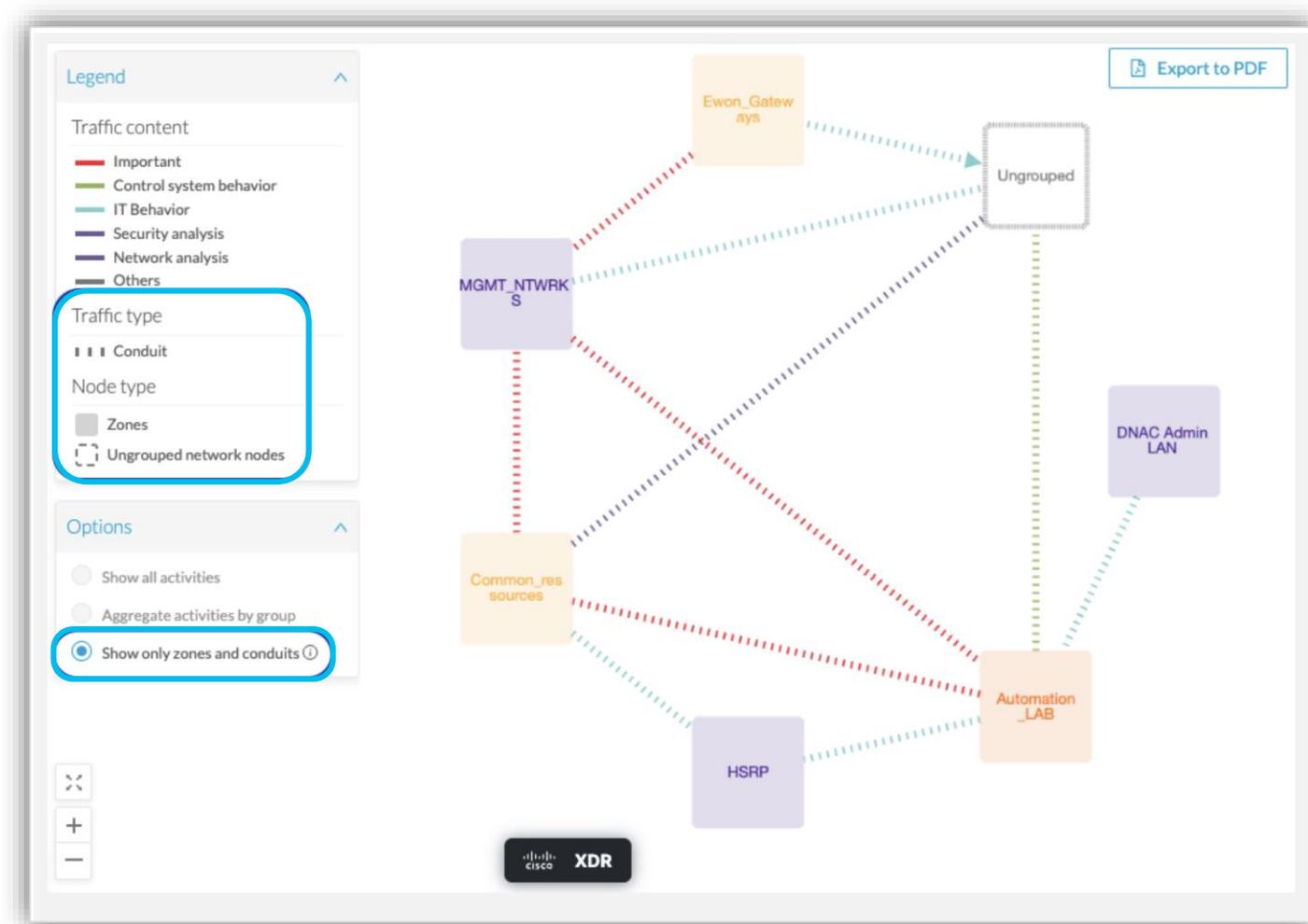
Group assets to define zones and conduits

- Organize your map to match the business and processes
 - Groups and Nested groups
 - Multi-faceted views
 - Quick drilldown
- Enables IT/OT collaboration to define security policies
- Group information shared with IT security tools such as Cisco ISE



“Zones and Conduits” visualization

Easily review your **network segmentation** by focusing on **zone-to-zone communications**



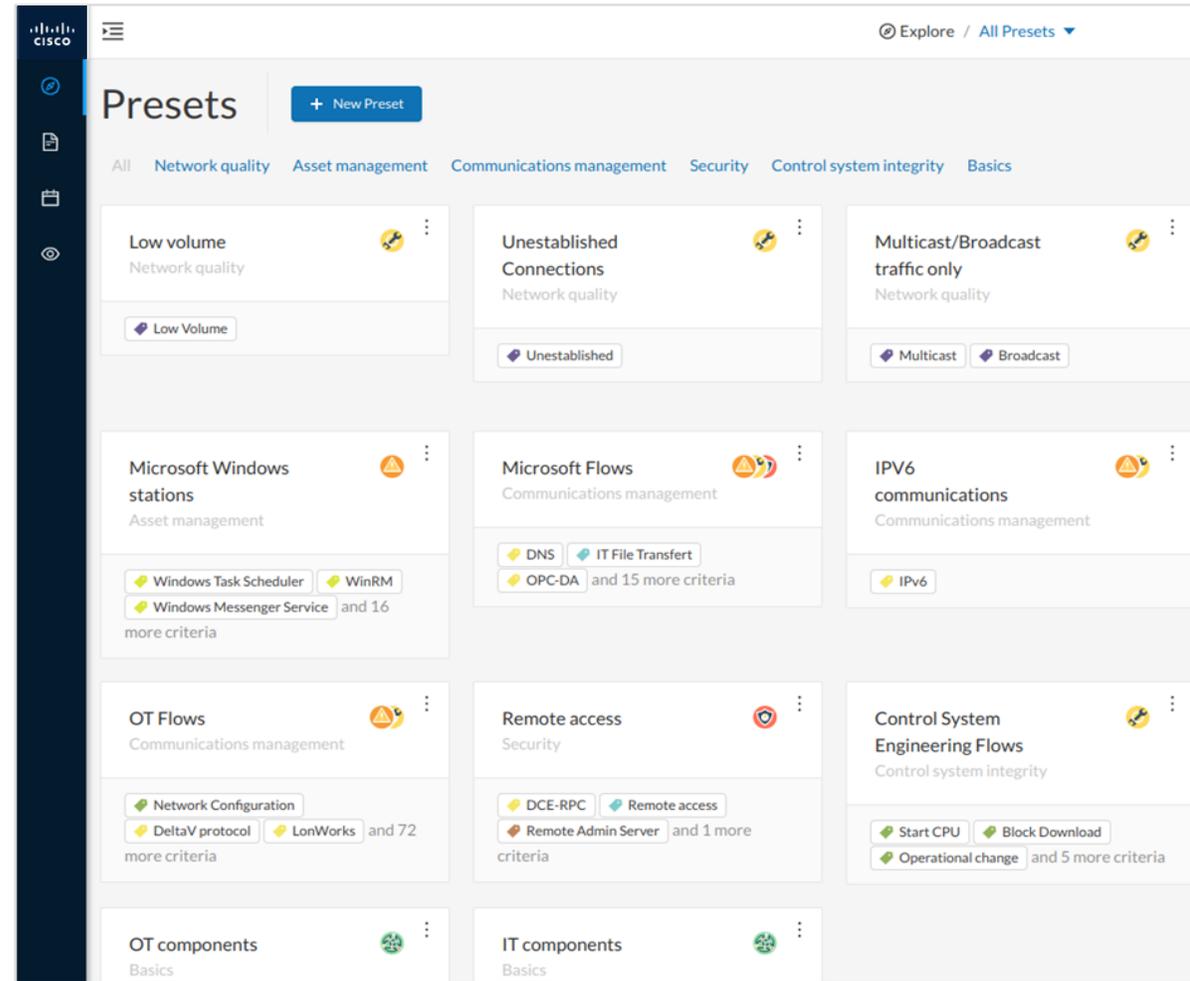
Custom properties to document the organization

- Add detailed information for each group
- Enables IT/OT collaboration
 - Document OT characteristics
 - Describe security policies
 - List organizational info
- All properties are shared with IT security tools
 - Cyber Vision feeds SOC with even more OT context

The screenshot displays the Cisco Cyber Vision interface. On the left, a navigation pane shows 'Campus Production' with sub-panels for NETWORKS, COMPONENT TAGS, ACTIVITY TAGS, GROUPS, and SENSORS. The main area shows a map of 'Campus Production' with a 'LEGEND' and a 'QA' tag. A 'CUSTOM PROPERTIES' dialog box is open, showing 'Group properties' for 'John Doe at 510-5517'. The dialog has a 'Label' field with a dropdown menu and a 'Value' field with a list of options: 'Default labels', 'Accountable organization(s)', 'Safety designation', 'Applicable security requirements', 'Applicable security policies', 'User labels', and '+ Add new label ...'. The background map shows a 'Gas Compression' group with various components like PLCs and pumps, and a 'Maintenance Station' with a Dell server. On the right, a 'Group' panel for 'Gas Compression' shows its parent group 'Building E', description 'Siemens compressor on 1st floor of building E', components 'Controller', 'SCADA Station', activity tags like 'Program Upload', 'Start CPU', 'Stop CPU', 'Read Var', 'Write Var', 'Broadcast', 'ARP', 'Profinet', 'Profinet DCP', 'S7Plus', and custom properties 'Accountable organization(s): John Doe at 510-5517'. At the bottom right, summary statistics show 4 Activities, 45 Events, 28 Vulnerabilities, and 5 Components.

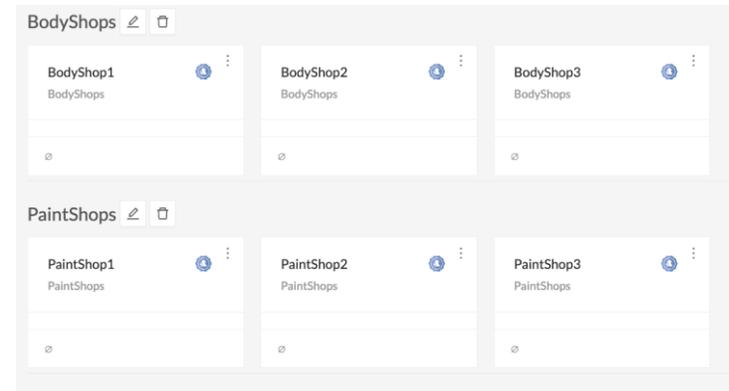
Easily dive into your data with preset views

- Presets are smart filters based on Tags, Groups, Sensors you want to track
 - Preset per site, per production line
 - Preset per asset type, per vendor
 - Preset per behavior types
- Deep-dive into very large datasets with ease
- Share presets with other users to show your discoveries & enable collaboration
- System has predefined presets and the ability for users to create their own
- Use RBAC to manage permissions to access presets



Structure your Presets using Preset Categories

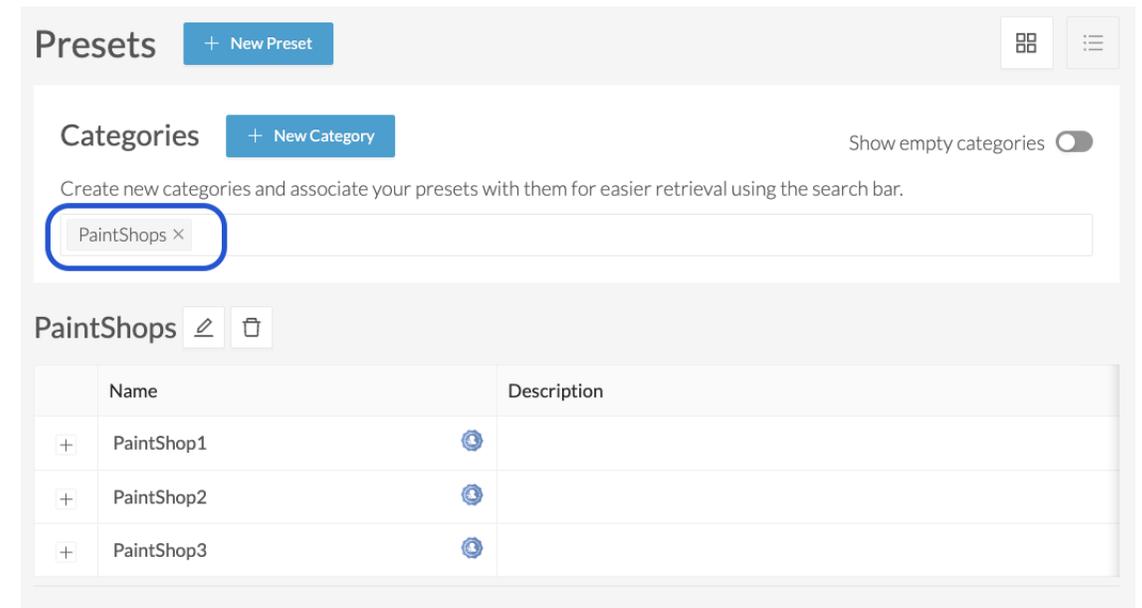
- Too many different and structurally different presets may defy their purpose to provide easy navigation through data
- Leverage **Preset Categories** to aggregate long and diverse lists of presets to categories



The image shows a dashboard with two main sections. The top section is titled 'BodyShops' and contains a table with columns 'Name' and 'Description'. The bottom section is titled 'PaintShops' and contains a table with columns 'Name' and 'Description'.

BodyShops	
Name	Description
+ BodyShop1	
+ BodyShop2	
+ BodyShop3	

PaintShops	
Name	Description
+ PaintShop1	
+ PaintShop2	
+ PaintShop3	



Preset Filters

- Leverage Subnet or VLAN ID as part of preset filter
- Criteria Search enables to quickly find matching tags, groups or sensors

NETWORKS ^

IP address/Subnet mask - *Optional*
Set an IP address. Ex: 192.168.1.0/24

192.168.1.0/24

VLAN ID - *Optional*
Set a number. Ex: 12

12

+ Add X Cancel

Criteria [Select all](#) | [Reject all](#) | [Default](#)

Ether | 🔍

2 criteria found

NETWORKS ▾

COMPONENT TAGS ▾

ACTIVITY TAGS ^

- EtherCAT
- EthernetIP (77)

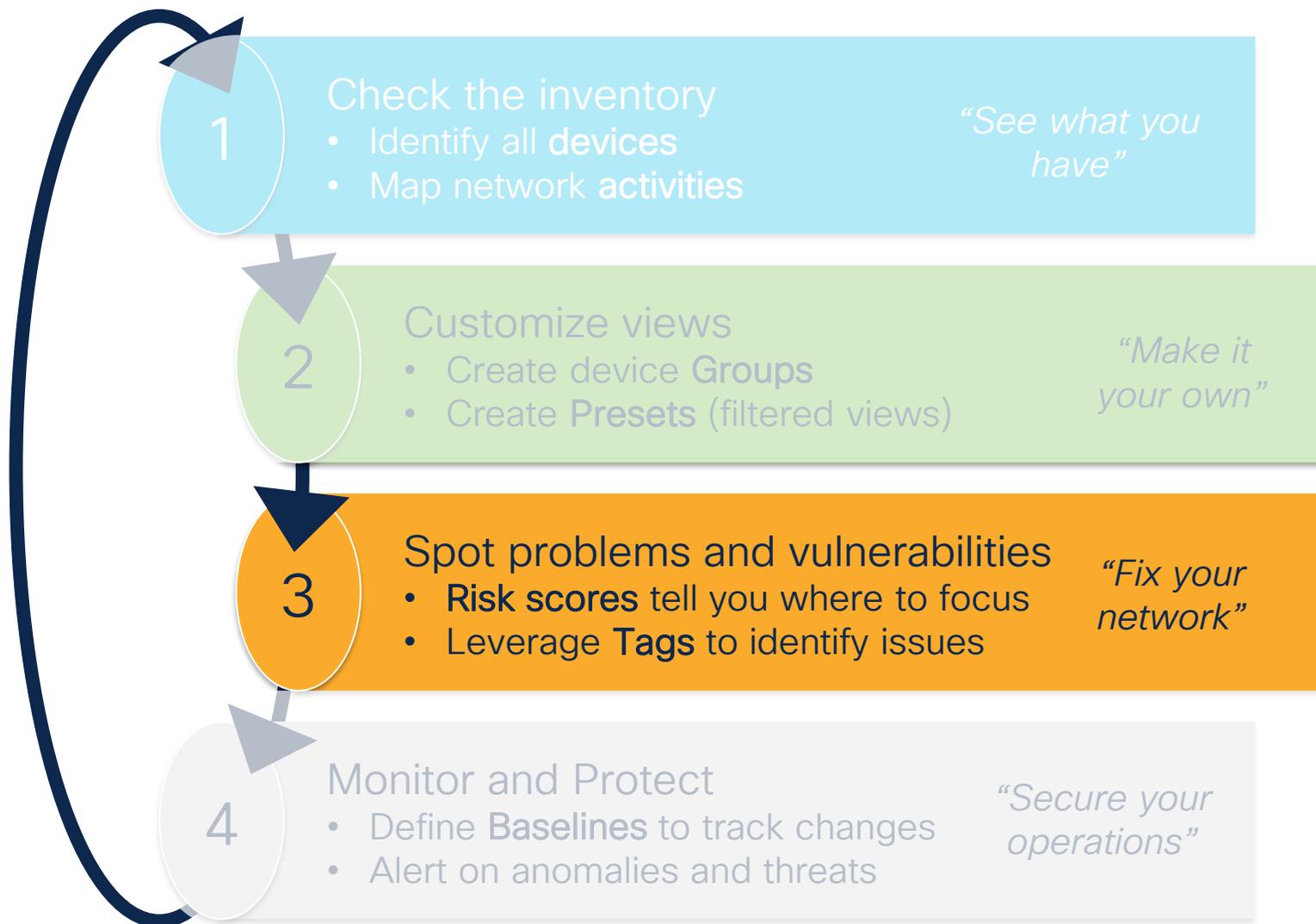
Export views to share insights

- Export your custom views to Excel or PDF
- Use Cyber Vision data to build your own reports and compliance statements
- Share with your teams the list of vulnerabilities to be fixed
- Export data for risk analysis in third party tools

The image displays three screenshots from the Cisco Cyber Vision interface, each with a callout box highlighting an export option:

- Export lists of assets in a Preset to CSV:** A screenshot of the '104 Component' view. A table lists components with columns for Component, Group, First activity, Last activity, IP, MAC, and Tags. An 'Export to CSV' button is highlighted in a red box.
- Export flow details to CSV:** A screenshot of the 'Flows' view. A table lists flow details with columns for Component, Port, Direction, Component, Port, Protocol, First activity, Last activity, Tags, Packets, and Bytes. An 'Export to CSV' button is highlighted in a red box.
- Export maps and dashboards to PDF:** A screenshot of the 'General Map' view. It shows a network diagram with various nodes and connections. An 'Export to PDF' button is highlighted in a red box.

The Cyber Vision Workflow



Investigate problematic assets and communications

- Asset characteristics and communications are automatically translated to Tags
- A common language whatever the vendor reference
- Users do not need to be protocol experts to understand what is going on
- New tags can be added via RESTful API

Cyber Vision tags helps identify devices and activities to investigate

The screenshot displays the Cyber Vision interface with two main sections: Component Tags and Activity Tags. Both sections use a tree view with expandable categories and checkboxes for individual tags.

COMPONENT TAGS

- Components without tags
- Device - Level 0-1
 - IO Module (3)
 - Wireless IO Module (2)
- Device - Level 2
 - Citect Alarm Server
 - Citect IO Server
 - Citect Report Server
 - Citect Trend Server
 - Engineering Station (3)
 - Master
 - PLC (9)
 - SCADA Station (3)
 - Slave
 - Train
- Device - Level 3-4
 - Admin Server (1)
 - DNS Server (2)
 - Database Server
 - Email Server
 - File Transfer Server
 - HTTP Client
 - Historian
 - Host Config Server (3)
 - Key Management Server
 - License Management Server
 - Log Server

ACTIVITY TAGS

- Activities without tags
- Control system behavior
 - Block Download
 - Control action (1)
 - Controller Info
 - Controller Name
 - Data Push
 - Device Init (1)
 - Diagnostics
 - Emergency Brake
 - Firmware Download
 - Firmware Update
 - Force Variable
 - Heartbeat
 - Hot Reboot
 - Insert Program
 - Installed Modules
 - Memory Formatting
 - Network Configuration
 - Operational change
 - PLC Clock
 - PLC Reservation
 - Password Change
 - Program Download (4)
 - Program Upload (2)
 - Programming CPU
- IT behavior
 - Active Directory Replication
 - Admin (1)
 - Antivirus
 - Authentication (1)
 - Database
 - Email
 - Host Config (11)
 - IT File Sync
 - IT File Transfer
 - Key management
 - License Management
 - Log
 - Net Management (3)
 - Net Routing
 - Ping (10)
 - Power Management
 - Printer Management
 - Procedure Call
 - Proxy
 - Remote access (1)
 - Streaming
 - Time Management (9)
 - VPN
 - Web (3)
 - Windows DFS Replication
 - Windows Discovery
- Network analysis
 - Port Scan
 - Port Scan Target
 - Public IP (19)
- Software
 - Active Directory
 - CodeSys
 - DFS
 - Lotus notes
 - Microsoft Exchange
 - NSIS
 - NetLogon
 - PI Osisoft
 - WINS
 - WMI
 - WinRM
 - Windows (10)
 - Windows Audio
 - Windows CSP
 - Windows Connection Mar
 - Windows DTCping
 - Windows File Protection
 - Windows Messenger Serv
 - Windows Network DDE
 - Windows Plug and Play
 - Windows SCM
 - Windows SecondaryLogon
 - Windows Task Scheduler
 - Windows WebClient
 - Windows WebDav

Enhanced visibility on malicious traffic

Explore / 192.168.0.subnet / Activity list

Last 1 day (May 23, 2021 11:43:26 PM – May 24, 2021 11:43:26 PM) Refresh

30 Activities [New data](#) [Export to CSV](#)

1 2 > 20 / page

Device	Device	First activity	Last activity	Tags	Flows	Packets	Volume
STATION	VM-XP-PRO	Oct 11, 2019 11:39:57 AM	May 24, 2021 12:32:16 PM	Program Download , Start CPU , Stop CPU , Unite	~10	91036	6.59 MB
Virtual 192.168.0.77	Siemens 192.168.0.1	Oct 11, 2019 10:59:49 AM	May 24, 2021 12:32:16 PM	ARP , S7	~10	1255	109 kB
IE11WIN7	DESKTOP-GBJUF2N	May 26, 2021 12:14:06 AM	May 26, 2021 12:19:04 AM	Insecure , Authentication , Procedure Call , Exception , Low Volume , Netbios , Netbios Name Service , SMB , SNORT Policy Violation	~20	234	35.6 kB
1756-L55/A 1756-M12 /A LOGIX5555 (Port1-L ink00)	STATION-WINCC	Oct 11, 2019 11:23:14 AM	May 24, 2021 12:32:16 PM	Read Var , Write Var , ARP , EthernetIP	~10	29239	1.46 MB
192.168.0.255	VM-XP-PRO	Oct 11, 2019 11:39:57 AM	May 24, 2021 12:32:16 PM	Insecure , Broadcast , Low Volume , Netbios , SMB	~10	4	972 B

- 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

Activity tags associated with events detected by the Snort IDS

Provides more precise context to understand malicious activities

Identify vulnerabilities to assess risks

- Quickly spot vulnerabilities
 - Dashboard based on Presets
 - Drill down by site, zone, tag, vendor, sensor...
- Easily identify affected components
- Links to quickly pivot to component view
- Additional context for impact and remediation

Explore / 192.168.1 subnet / Vulnerabilities

Jan 1, 2020 12:00:00 AM - Nov 19, 2020 3:27:00 PM (10 mths 19 days 11 hrs 27 mins) LIVE

192.168.1 subnet
My preset

Active baseline: No active baseline
Active Discovery: Disabled
This preset is filtered with keywords «192.168.1»

Criteria
Select all Reject all Default

Search criteria

NETWORKS
COMPONENT TAGS

- Components without tags
- Device - Level 0-1
- Device - Level 2
- Device - Level 3-4
- Network analysis
- Software
- System

ACTIVITY TAGS
GROUPS
SENSORS

73 Vulnerabilities

10 most matched vulnerabilities

Vulnerability severity legend: NONE (green), LOW (yellow), MEDIUM (orange), HIGH (red), CRITICAL (black)

Vulnerability title	CVE	CVSS score	Affected components
Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and Configuration Protocol	CVE-2017-2680	6.5 (v3)	3 components
Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability	CVE-2017-12741	7.5 (v3)	3 components
Denial-of-Service Vulnerability in Profinet Devices	CVE-2019-10936	7.5 (v3)	3 components
Yokogawa CENTUM 'BKHOdeq.exe' Stack Based Buffer Overflow Vulnerability	CVE-2014-0783	9.0 (v2)	2 components
Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Packet Storm	CVE-2014-3888	8.3 (v2)	2 components
Schneider Electric Modicon Modbus Protocol Multiple Authentication Bypass Vulnerabilities	CVE-2017-6032	5.3 (v3)	2 components
Yokogawa CENTUM 'BKESimmgr.exe' Stack Based Buffer Overflow Vulnerability	CVE-2014-0782	0.0 (v2)	2 components
Vulnerabilities in SIMATIC-1200 and SIMATIC S7-1500 CPU families	CVE-2019-10943	7.5 (v3)	2 components
Schneider Electric Modicon Modbus Protocol - Multiple Authentication Bypass Vulnerabilities	CVE-2017-6034	9.8 (v3)	2 components

9 Total vulnerable components for 192.168.1 subnet

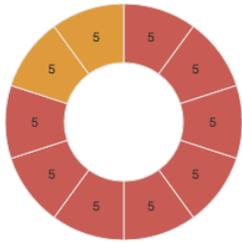
Export detected vulnerabilities

Detected vulnerabilities can be exported for offline review, audit and documentation.

Last 1 day (May 27, 2024 6:34:49 PM – May 28, 2024 6:34:49 PM) [Refresh](#)

[New data](#)

10 most matched vulnerabilities



- CVE-2022-20856 • Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Famil... 5 affected devices
- CVE-2022-20722 • Cisco IOx Application Hosting Environment Vulnerabilities 5 affected devices
- CVE-2022-20919 • Cisco IOS and IOS XE Software Common Industrial Protocol Request... 5 affected devices
- CVE-2022-20726 • Cisco IOx Application Hosting Environment Vulnerabilities 5 affected devices
- CVE-2022-20719 • Cisco IOx Application Hosting Environment Vulnerabilities 5 affected devices
- CVE-2022-20679 • Cisco IOS XE Software IPSec Denial of Service Vulnerability 5 affected devices
- CVE-2022-20718 • Cisco IOx Application Hosting Environment Vulnerabilities 5 affected devices
- CVE-2022-20915 • Cisco IOS XE Software IPv6 VPN over MPLS Denial of Service Vulnerability 5 affected devices
- CVE-2022-20724 • Cisco IOx Application Hosting Environment Vulnerabilities 5 affected devices
- CVE-2022-20722 • Cisco IOx Application Hosting Environment Vulnerabilities 5 affected devices

9 vulnerable devices on All data preset

Vulnerability severity legend: NONE LOW MEDIUM HIGH CRITICAL

74 Vulnerabilities

[Export to CSV](#)

< 1 2 3 4 > 20 / page

Vulnerability title	CVE	CVSS score	Affected devices
Cisco IOx Application Hosting Environment Vulnerabilities	CVE-2022-20721	4.9 (v3.1)	5 devices
Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family DHCP Processing Denial of Service Vulnerability	CVE-2022-20847	7.5 (v3.1)	5 devices
Cisco IOx Application Hosting Environment Vulnerabilities	CVE-2022-20725	4.8 (v3.1)	5 devices

Drive vulnerability remediation

- Automatically spot software & hardware vulnerabilities
- Access comprehensive information on vulnerability severities and solutions
- Track vulnerability acknowledgements
- Built-in vulnerability database curated by Cisco Research Teams always up to date

Enforce cybersecurity best practices

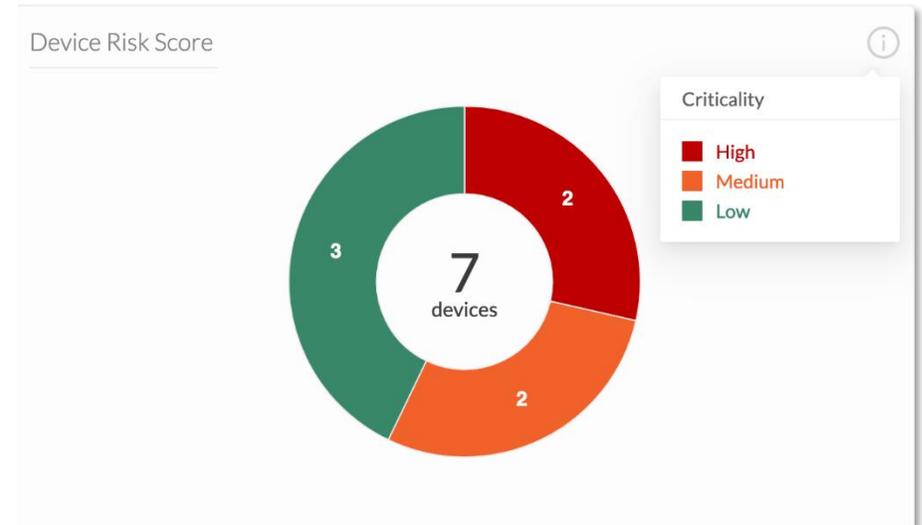
The screenshot displays a network security dashboard for a device named "SIMATIC 300(1)". The device is identified as "[Manheim] Folding P..." with a "very low" risk score. Key details include IP: 192.168.0.1 and MAC: 00:0e:8c:84:5b:a6. The dashboard shows activity logs, tags (Read Var, Controller), and activity tags (Network Configuration, Read Var, Ping, Broadcast, Low Volume, Multicast, ARP, Profinet, Profinet DCP, S7). A summary panel on the right shows 6 Activities, 20 Events, 16 Vulnerabilities, and 0 Credentials. The main content area is titled "Vulnerabilities" and lists two entries:

- Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability** (CVE-2017-12741): Several industrial products are affected by a vulnerability that could allow remote attackers to conduct a Denial-of-Service (DoS) attack. **Score CVSS: 7.8**. Solution: Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available. Published on November 23, 2017. Identified on this component on April 6, 2017. Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0). Links: Siemens Security Advisory.
- SIMATIC S7-300 and S7-400 CPUs Denial of Service and Information Disclosure Vulnerabilities** (CVE-2016-9158): Successful exploitation of these vulnerabilities could lead to a denial-of-service condition or result in credential disclosure. **Score CVSS: 7.8**. Solution: Siemens provides firmware version V3.X.14 for S7-300 CPUs that resolves CVE-2016-9158. Published on December 16, 2016. Identified on this component on April 6, 2017. Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0). Links: www.siemens.com, ics-cert.us-cert.gov, www.securityfocus.com.

At the bottom, there is a checkbox for "Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and".

Risk scoring helps focus on what's important

- Guides non-expert users to devices they should deal with first
- A first step in security management to help make urgent decisions
- Provides simple information on the security posture



Defining the Cyber Vision risk scores

- Risk = Likelihood x Impact
- Likelihood
 - Activity tags (some communications create more risks)
 - Exposure to external IP addresses
 - Discovered vulnerabilities
- Impact
 - Device tags (some devices can create more damages)
 - User-defined industrial impact for groups

Impact	Critical	High	High	High	High
	high	negligible	Significant	High	High
	limited	negligible	negligible	Significant	Significant
	No impact	negligible	negligible	negligible	negligible
		Minimal	Significant	High	Maximal
		Likelihood			

Source: EBIOS

Define impact of Activities to Risk Score

- Configure what length of time activities impact calculated risk score

Risk score

From this page, you can choose the time range that will be used to compute your devices risk scores

Select a time range

30 days

7 days

30 days

Custom

 Save

 Reset to default

Quickly identify “Riskiest” devices

Create presets based on risk thresholds and convert to baselines

Sort and filter risks in your lists of devices

The screenshot displays the Cisco ISE Device List interface. On the left, the 'Criteria' panel is open, showing a 'RISK SCORE' filter with a range from 55 (Min) to 100 (Max). The main table shows 50 filtered devices. The 'Risk score' column is highlighted with a red box, showing scores ranging from 35 to 69. The table columns include Device, Group, First activity, Last activity, IP, MAC, Risk score, and Tags.

Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags
SCS0102	Building K	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:32:15 PM	192.168.1.5 (+ 1 other)	00:00:64:8c:86:34 (+ 1 other)	69	Controller, Time Server
Fisher 10.5.0.22	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:32:15 PM	10.5.0.22	00:22:e5:1f:90:18	44	Controller, DeltaV
Fisher 10.4.0.14	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:32:15 PM	10.4.0.14	00:22:e5:1f:9a:54	44	Controller, DeltaV
10.4.0.30	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:32:15 PM	10.4.0.30 (+ 1 other)	00:22:e5:21:0a:86	44	Controller, Time Server, DeltaV
Yokogawa 192.168.1.126	Fujitsu	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:32:15 PM	192.168.1.126	00:00:64:8c:bb:08 (+ 1 other)	44	Controller
Fisher 10.5.0.18	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:32:15 PM	10.5.0.18	00:22:e5:1f:b0:20	44	Controller, DeltaV
Fisher 10.4.129.2	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:32:15 PM	10.4.129.2	00:22:e5:04:45:44	43	Net Management Server
Fisher 10.4.129.1	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:32:15 PM	10.4.129.1	00:22:e5:12:4c:90	43	Net Management Server
192.168.1.123	fujitsu	Mar 11, 2020 8:21:58 PM	May 24, 2021 12:32:15 PM	192.168.1.123 (+ 1 other)	4c:52:62:33:f5:39	38	Email Server
Hirschmann 192.168.1.254	Building K	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:32:15 PM	192.168.1.254	ec:74:ba:03:98:6b	35	Time Server
Yokogawa 192.168.1.128	Fujitsu	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:32:15 PM	192.168.1.128	00:00:64:8c:ba:90 (+ 1 other)	35	Time Server

Reducing a device risk score

Device: SCS0102, Building K, very high. IP: 192.168.1.4 (+ 1 other), MAC: 00:00:64:8c:86:08 (+ 1 other).

First activity: Oct 11, 2019 11:06:52 AM. Last activity: May 24, 2021 12:32:15 PM.

Activities: 7, Events: 40, Vulnerabilities: 15.

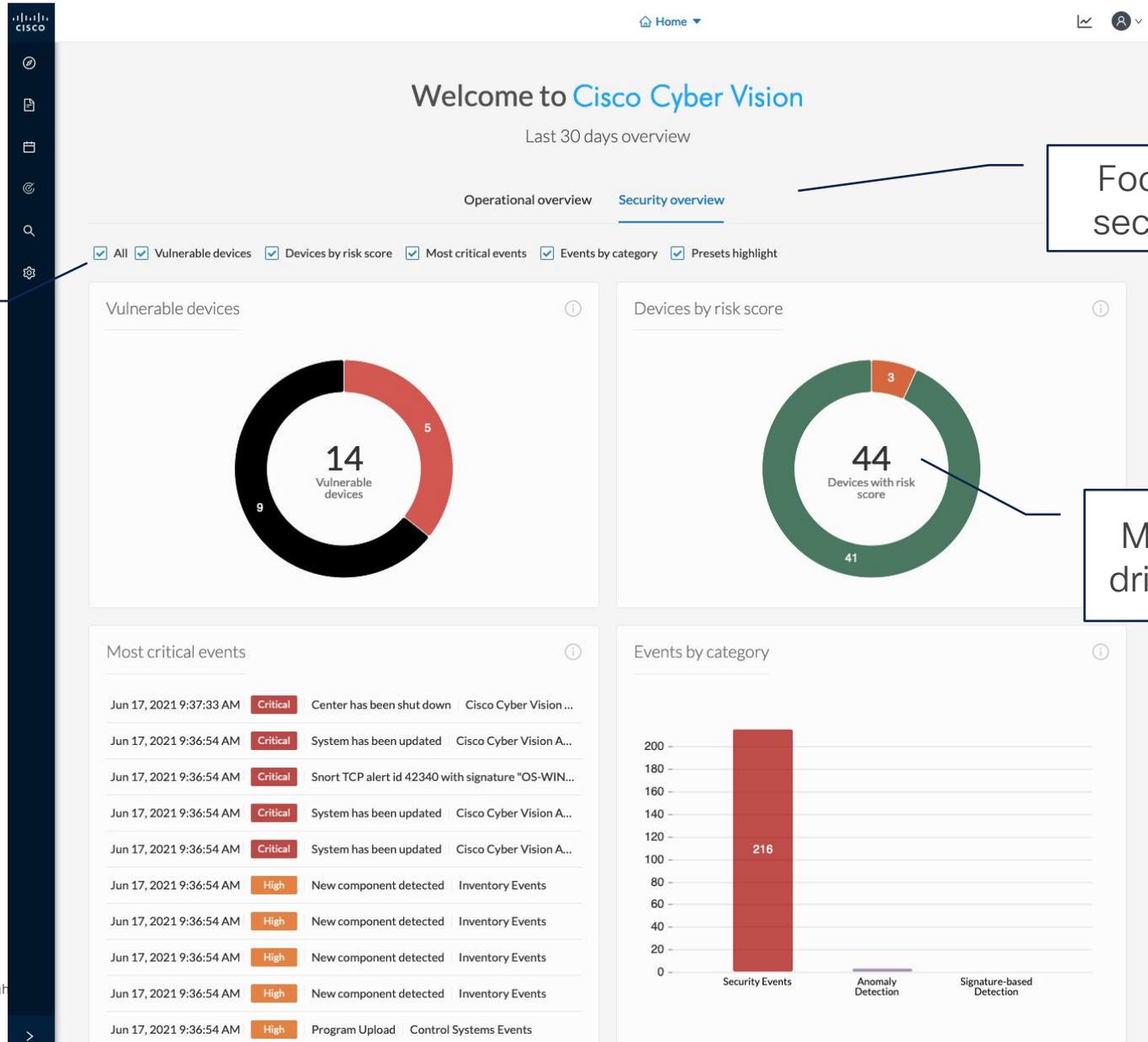
Risk score: 69. Achievable risk score: 44. The best achievable score is 44. It can be reached by patching all vulnerabilities and removing insecure traffic.

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%	Path Traversal Vulnerability in Yokogawa CENTUM CVE-2020-5609 CVSS score: 9.8 Successful exploitation of these vulnerabilities could allow a remote unauthenticated attacker to see ...show more See details

Understand where you are, and where you could be

Understanding what impacts the score

Customizable dashboards to surface information



Choose widgets to customize home

Focus on OT or security insights

Monitor risks and drive improvement

Home ▼ 📄 👤

Welcome to Cisco Cyber Vision

Last 30 days overview

Operational overview Security overview

All Protocol distribution Most critical events Presets highlight

Protocol distribution

Protocol	Count
ARP	66
Others	60
Netbios	25
DeltaV proto...	23
IPv6	21
VNET/IP	19

Most critical events

Timestamp	Severity	Event Description	Source
Jun 17, 2021 9:36:54 AM	Critical	System has been updated	Cisco Cyber Vision A...
Jun 17, 2021 9:36:54 AM	Critical	System has been updated	Cisco Cyber Vision A...
Jun 17, 2021 9:36:54 AM	Critical	Snort TCP alert id 42340 with signature "OS-WIN...	
Jun 17, 2021 9:37:33 AM	Critical	Center has been shut down	Cisco Cyber Vision ...
Jun 17, 2021 9:36:54 AM	Critical	System has been updated	Cisco Cyber Vision A...
Jun 17, 2021 9:36:54 AM	High	New component detected	Inventory Events
Jun 17, 2021 9:36:54 AM	High	Program Upload	Control Systems Events
Jun 17, 2021 9:36:54 AM	High	New component detected	Inventory Events
Jun 17, 2021 9:36:54 AM	High	New component detected	Inventory Events
Jun 17, 2021 9:36:54 AM	High	New component detected	Inventory Events

Presets highlights

☆ Edit favorite presets

Preset	Risk score	Last precomputation	Devices	Vulnerabilities	Events
All Controllers	26.5	Jun 17, 2021 9:46:41 AM	14	94	2098
Broadcast traffic only	12	Jun 17, 2021 9:46:47 AM	30	158	2289
IT Activities	16	Jun 17, 2021 9:46:47 AM	36	169	5343
IT Devices	25	Jun 17, 2021 9:46:49 AM	23	94	5242
Internet Activities	12	Jun 17, 2021 9:46:45 AM	0	0	1779
OT Devices	28	Jun 17, 2021 9:46:46 AM	21	128	1000

Focus on OT or security insights

Ability to pin specific presets to home dashboard

Quickly identify "Riskiest" presets

Counters per preset

Easily spot important IT security information

Security Insights

Devices with external communication | DNS requests | HTTP requests | SMB Tree names | Flows with no tag

1 / 1 Device selected | Clear selection

<input checked="" type="checkbox"/>	Device	Risk Score	IP	MAC
<input checked="" type="checkbox"/>	Router 44:b6:be:42:xx:xx	60	10.90.11.100 (+ 1 other)	44:b6:be:42:e7:40 (+ 3 others)

Security Insights

Devices with external communication | DNS requests | HTTP requests | SMB Tree names | Flows with no tag

The flow storage policy can affect this feature. Please ensure you've enabled the flow storage for networks you want to monitor.

Top 5 DNS requests

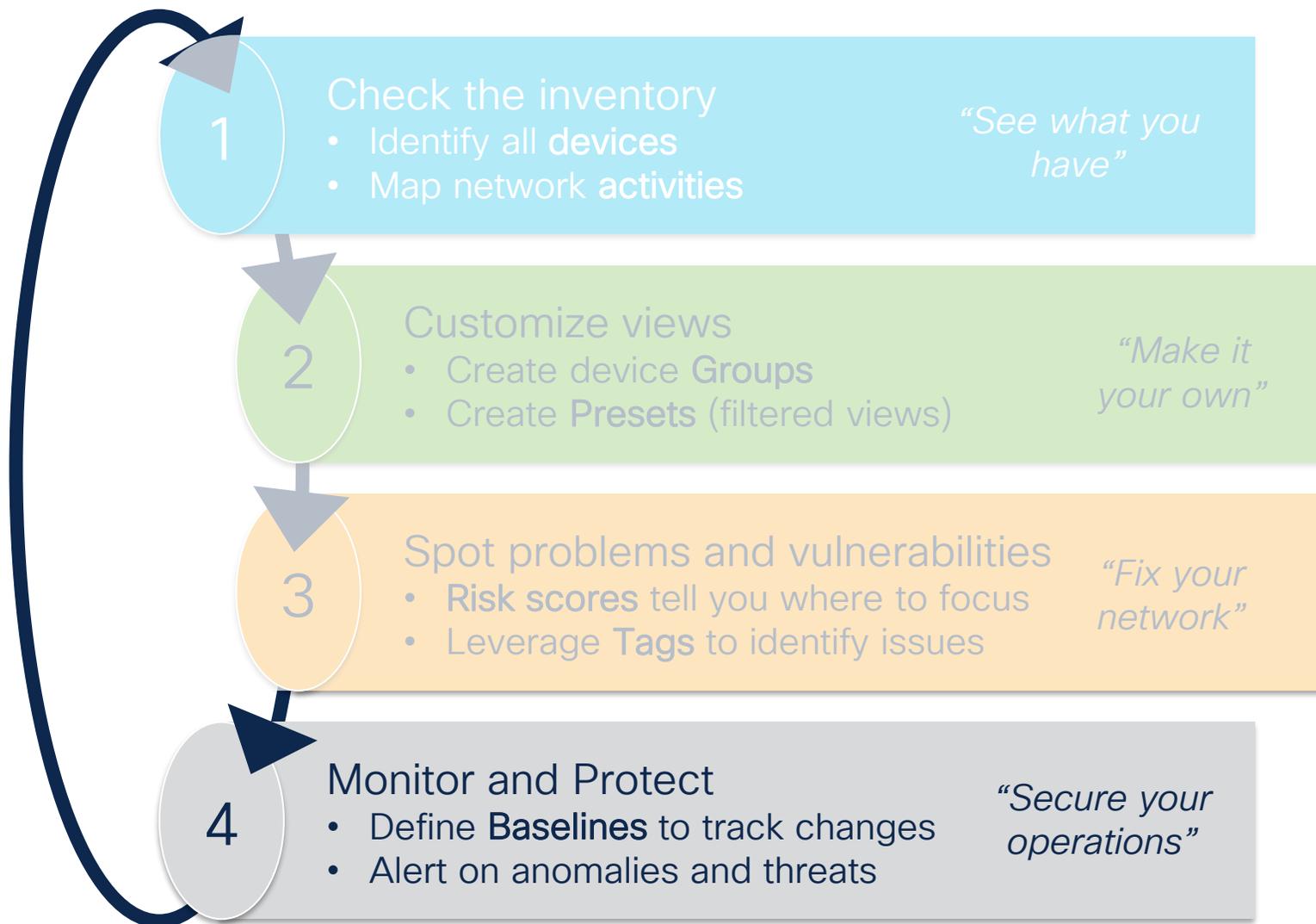
Domain	Requests
pool.ntp.org	701 requests by 4 components
ntp.org.local	44 requests by 4 components
secureprotocolengine-test.intel.com	11 requests by 1 component
api.gridsmart.com	10 requests by 1 component
dns.msftncsi.com	5 requests by 1 component

Rare 5 DNS requests

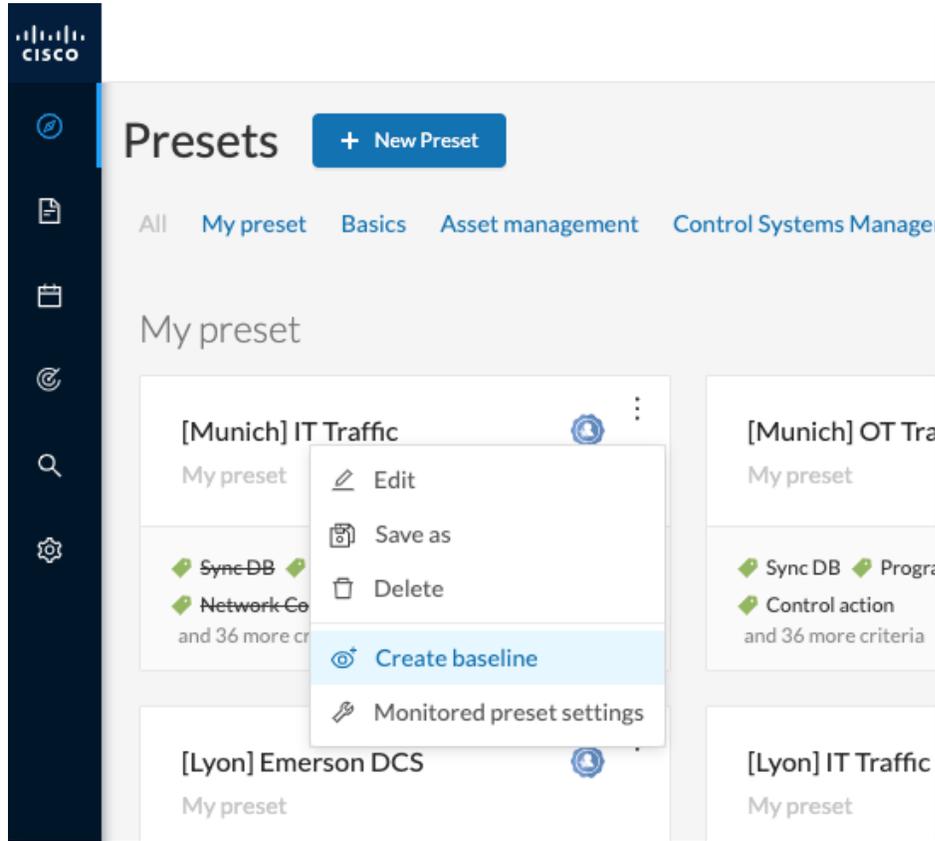
Domain	Requests
dns.msftncsi.com	5 requests by 1 component
api.gridsmart.com	10 requests by 1 component
secureprotocolengine-test.intel.com	11 requests by 1 component
ntp.org.local	44 requests by 4 components
pool.ntp.org	701 requests by 4 components

- External Communication
- Top / Rare DNS requests
- Top / Rare HTTP requests
- Top / Rare SMB usage
- Unclassified “strange” flows

The Cyber Vision Workflow



Identify changes to environment using baselines



Leverage presets to focus monitoring on parts of the environment

- Create presets to fine tune the dataset you want to monitor
- Create baselines for each preset to monitor various states (production/maintenance)
- Set frequency checks and event severity by baseline

What is a Baseline?

It is a snapshot of the production system, letting users define what “normal” is. Cyber Vision detects changes to trigger alerts.

Advanced Options for Baselines

MONITORED PRESET SETTINGS

Check interval (in seconds)*
How often do you want to check the state of this Preset?
10 Enforce check interval

Monitored baseline
Please select the baseline you want to monitor
daeckste_baseline

Events severity
Please select the appropriate severities for this Preset

Severity Type	Severity Level			
	low	medium	high	very high
Differences detected	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Anomaly reported	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Difference acknowledged & included	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Difference acknowledged but not included (keep warning)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Component or Activity removed from baseline	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Advanced settings
Please select the types of differences you want to be alerted about

Components behaviors

- New component
- New tag
- New variable access

Properties behaviors

- New property
- Property update

Activities behaviors

- New activity
- New tag

- Created baselines have the options to define custom settings for:
 - Frequency for checking for deviations
 - Security event severity threshold
 - Components behavior
 - Properties behavior
 - Activities behavior

Baselines highlight abnormal behaviors

- Cyber Vision behavior modeling automatically triggers alerts on deviations to the baselines
 - New and modified assets
 - New activities between assets
 - Variable changes
 - Program modifications
- Accept changes to continuous monitoring or trigger alerts to investigate changes
- Provide feedback on anomalies to give context to security analysts

The screenshot displays the Cisco Cyber Vision interface for a 'Utilities Baseline'. It includes a summary of 37 components (7 new, 2 changed), a table of component details, a network map, and a detailed view of a changed activity.

Status	Component	Group	First activity
NEW	104.26.11.240	-	Jul 15, 2021 2:58:12
NEW	Lantronix 192.168.119.211	Enterprise Network	Jul 15, 2021 2:58:12
NEW	173.36.224.109	-	Jul 15, 2021 2:58:12
NEW	171.70.168.183	-	Jul 15, 2021 2:58:12
NEW	Microsoft 192.168.119.210	Enterprise Network	Jul 15, 2021 2:58:12
CHANGED	Beckwith 10.0.0.57	Station Bus Network	Jul 14, 2021 8:29:56
CHANGED	Cisco 192.168.119.166	Enterprise Network	Jul 14, 2021 8:30:56
-	Rockwell a3:0:cb	Enterprise Network	Jul 14, 2021 8:30:56
-	Rockwell a4:21:c2	Enterprise Network	Jul 14, 2021 8:30:56

Changed Activity

Rockwell 192.168.249.50
Paint Line 2 ▲ high
 IP: 192.168.249.50
 MAC: f4:54:33:91:cb:ee

Rockwell 192.168.249.40
Paint Line 2 ▲ high
 IP: 192.168.249.40
 MAC: f4:54:33:9b:77:76

First activity: Apr 24, 2020 11:04:08 AM
 Last activity: Apr 27, 2020 10:26:37 AM

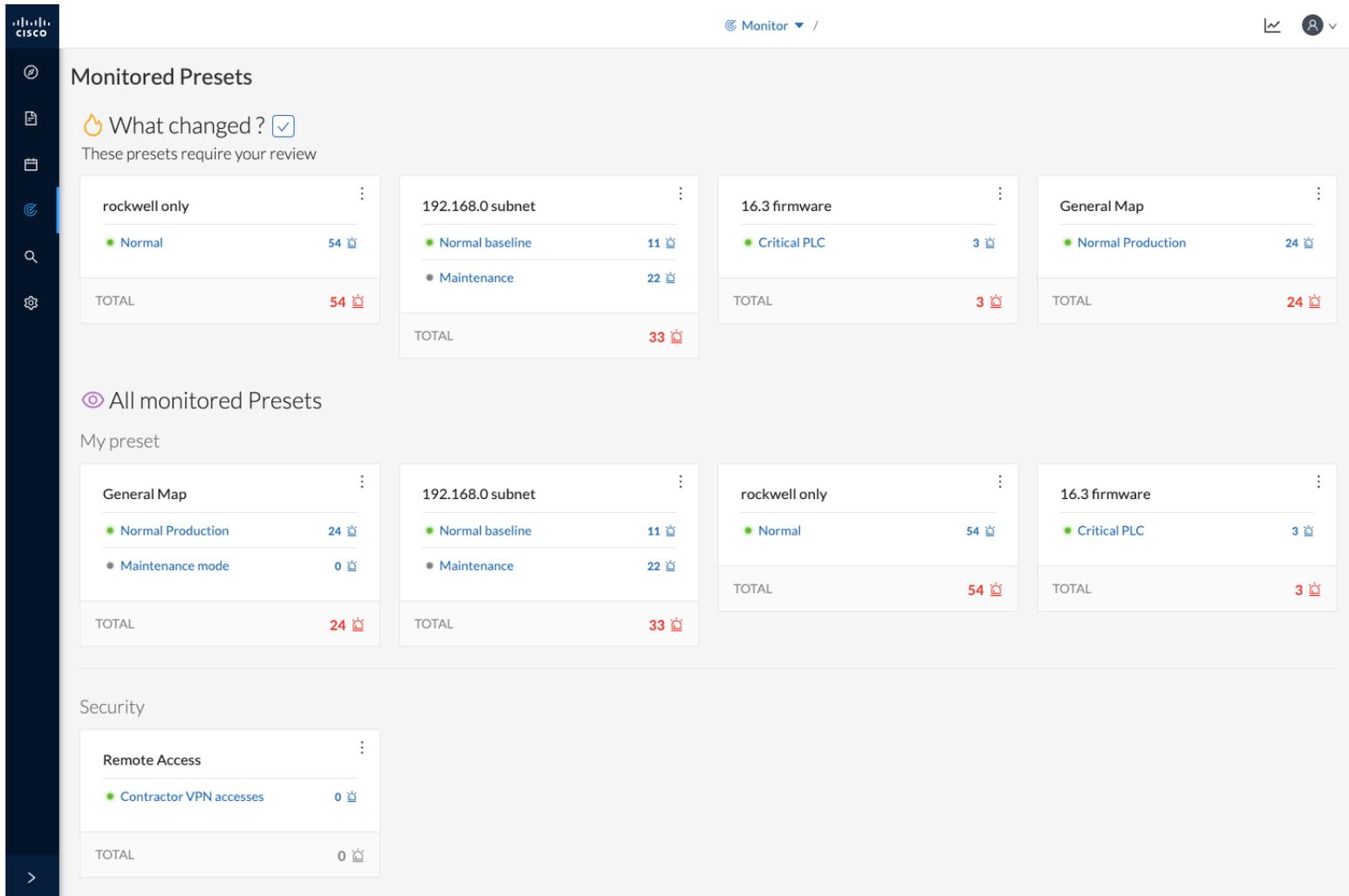
Tags: Read Var, Write Var, EthernetIP

Variables: (1 difference)
 SYNC_NEW1 read Rockwell 192.168.249.50
 SYNC write Rockwell 192.168.249.50
 SYNC read Rockwell 192.168.249.50

Buttons: Acknowledge differences, Report differences, Remove and keep warning, Individual acknowledgment

Summary: 2 Flows, 0 Event, 396127 Packets, 0 Volume

Set advanced detection strategies



Baseline per sensor or group of devices

- Monitor specific production lines, asset types, industrial sites

Baseline per behavior

- Remote connections
- DNS activities
- SMB negotiations
- Encrypted traffic
- OT devices detected
- Control systems behaviors
- or any other behavior tagged by DPI

Minimize false positives

- Create different baselines for production and maintenance states

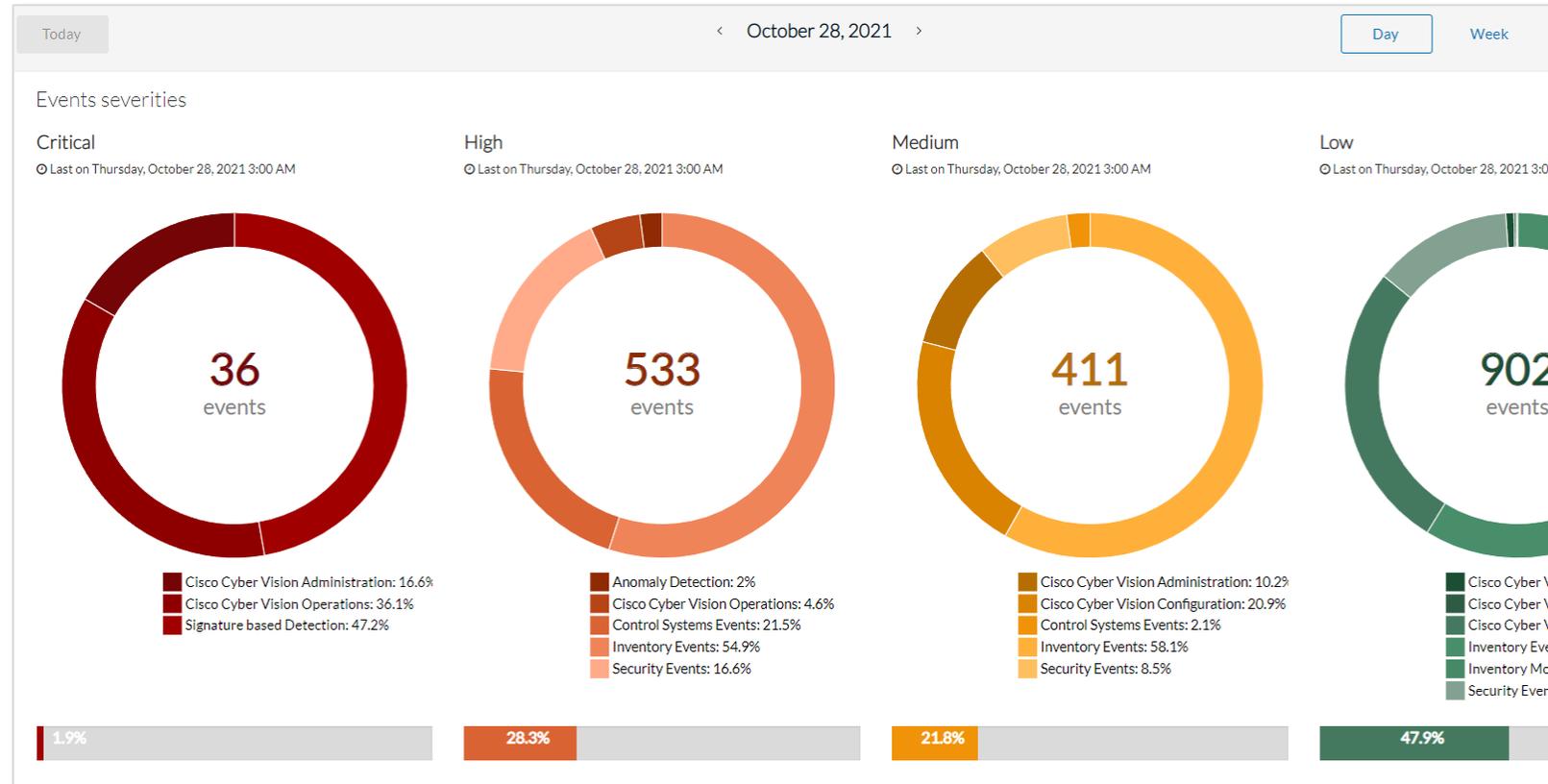
Events: The high-level overview

Easily track everything happening within the industrial network

- Security events (vulnerabilities, port scan, protocol exception...)
- Signature-based detection (Snort IDS)
- Control systems events (variable changes, program upload, stop/start CPU...)
- Asset inventory (New or modified asset...)
- Changes to the Cyber Vision platform (user login, config changes...)

All events automatically sorted by criticality levels

All events can be exported to SIEM and SOC via Syslog



Easily filter and search Events to ease investigations

The screenshot shows the Cisco Security Center interface. At the top right, there is a navigation menu with 'Events' selected. Below this is a search bar containing the text 'snort X' and a search icon. A red arrow points to the search bar. Below the search bar is a notification: 'The events storage is limited to 10000 events per category (see categories)'. The main content area shows 'Dashboard' and 'List' tabs, with 'List' selected. Below this, it says '1 Event'. A table with columns 'Time', 'Severity', 'Category', and 'Description' displays one event. The event details are expanded below the table, showing a 'Snort Event' with various attributes.

Events

snort X Search events

The events storage is limited to 10000 events per category (see categories)

Dashboard List

1 Event

Time	Severity	Category	Description
December 9, 2025 5:23:01.477 PM	critical	Signature based Detection	Snort alert on UDP id 44037 with signature A Network Trojan was detected from 192.168.0.12 → 212.166.210.80

Snort Event

- Occured at: 03/13-08:06:16.819867
- Sensor: -
- Gid: 1
- Signature ID: 44037
- Priority: 1
- Rule: 1:44037:4 (Revision 4)
- Classification: A Network Trojan was detected
- In network interface: /data/tmp/uploads/3755765419bec09a7a0b4c3bdd33cbab
- Message: INDICATOR-COMPROMISE DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - WannaCry
- From: 192.168.0.12:62805
- To: 212.166.210.80:53 (64:80:99:D8:5D:4C -> A4:08:F5:E1:03:EC)
- Protocol: UDP
- Direction: C2S
- Ethernet type: 0x800
- Service: unknown
- VLAN: 0
- Related data: [Download data](#)

Rich context added to all events

The screenshot shows the Cisco ICSM event viewer interface. At the top, there are filters for 'category' (Control Systems Events) and 'severity' (high). A search bar is present with the text 'Search an event'. The main area displays a list of events for 'January' with a 'Live' indicator and 'Auto-follow' checkbox. A navigation bar shows '115' events and a calendar view with dates 1, 2, 3, 8, 9, 10, 11, 12. The selected event is expanded to show details:

- Event:** 01/19/2022 02:00:01 Control Systems Events New program has been uploaded, flow from Dell 10.4.0.6 ((Lyon) Windows Stations) to Dell 10.4.0.6 ((Lyon) Windows Stations) | IP: 10.4.0.6 | MAC: 84:8f:69:e1:a7:9b to 84:8f:69:e1:a7:9b
- Flow:** Source port: 1110, Destination port: 502
- Component source:** Group: Munich, Industrial impact: none, Group description: Munich Parent Group, Device: Vmware 192.168.249.114, Name: Vmware 192.168.249.114, MAC: 00:0c:29:c7:c8:76, IP: 192.168.249.114, Tag: Engineering Station
- Component destination:** Group: Munich, Industrial impact: none, Group description: Munich Parent Group, Device: 1769-L16ER/B LOGIX5316ER, Name: 1769-L16ER/B LOGIX5316ER, MAC: f4:54:33:91:cb:ee, IP: 192.168.249.50, Tags: Controller, Rockwell Automation, 10 vulnerabilities detected

Click to see communications details

Click to see device details

Filter Events based on Category and Time

The screenshot shows a date selection interface with tabs for Day, Week, Month, Year, and Custom. The current date is December 9, 2025. A calendar for December 2025 is displayed, with the 9th highlighted. The calendar shows days from 30 to 10. A 'Today' button is at the bottom.

Su	Mo	Tu	We	Th	Fr	Sa
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

The screenshot shows a search events interface with a search bar and a list of filter fields: ip, mac, category, severity, group, and network. A blue 'D' icon is next to the category field.

Search events

ip:

mac:

category:

severity:

group:

network:

Cyber Vision gives OT context to security analysts



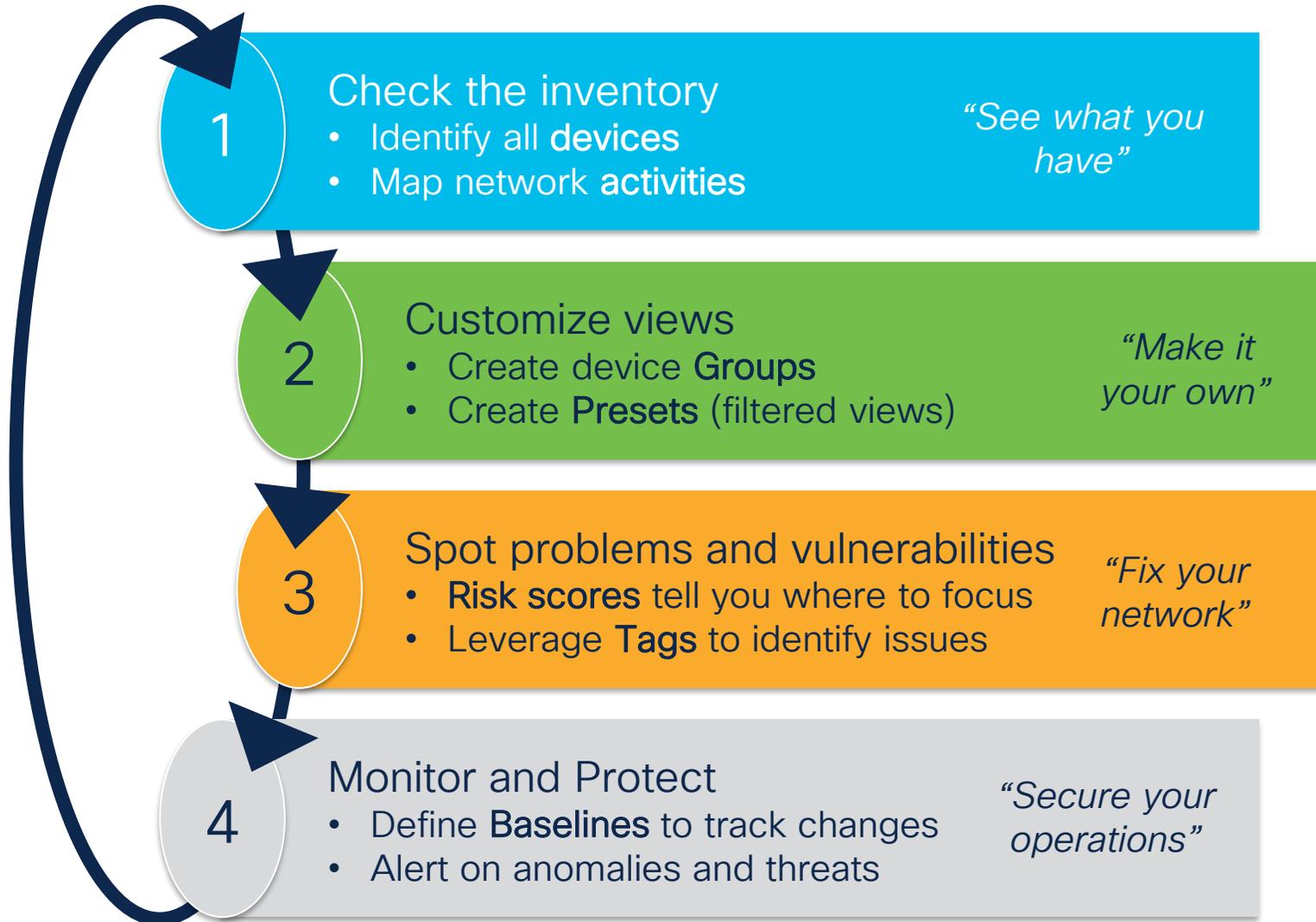
Local OT teams can:

- Acknowledge detected anomalies by providing detailed feedback
- Report anomalies to trigger investigations by security experts

SOC analysts have:

- Detailed technical information on assets, activities and flows
- Security events enriched with context
- Feedback from OT teams to better qualify issues

The Cyber Vision Workflow



Reporting Extension

Cyber Vision Reports

- Executive presentable **PDF** and **Word** documents generated
- **Preset-based** filter
- **Header customization** using company logo
- Public APIs available to **schedule** and download reports
- **Modular sections** - user decides what to include/not include in the report
- One click generation of **new versions** of same report

Security Posture Reports

- Helps organizations demonstrate they have a **handle on risk** with respect to **cyber insurance** and **standard compliance**
- Supports IT teams to **justify investment** into Cyber Vision to their management
- Enables Security Assessment and Managed Service Providers to deliver **white-label reports** to end customers, using a customizable logo
- Allows cyber security teams to **track progress** of risk through historical reports

CISCO

Key Findings

Filter Criteria: -

This report is an automated summary that captures all the vulnerabilities, risky activities, and security events found on the devices in the - by Cisco Cyber Vision on September 24th, 2023 at 8:04 am UTC

Risk score	Devices	Vulnerable Devices	Events(over the last 30 days)
45.0	34	7	323

Security Insights

Severity	Findings
Critical	46 critical and high severity vulnerabilities found on 7 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

Page 3

CISCO

Name	CVSS Score	Severity	Number of affected devices
ns Products CVE-2017-Service Vulnerability	7.5	High	4
ce Vulnerability in	7.5	High	4
of Service Vulnerabilities devices using the PROFINET onfiguration Protocol	6.5	Medium	4
Protection in the Web page of Siemens Industrial	6.5	Medium	4
Controllers			
CVE-2019-6568 Denial Of Service Vulnerability in Web-server of Industrial Products - Siemens	7.5	High	3

Page 22

NIS2 related information for Posture Reports

- “Risk Zone” included in report
- New section for DNS servers
- Total devices and external domains added

Executive Summary

Filter Criteria: All data Preset

Introduction

Cybersecurity risk management is the process of identifying, assessing, and taking steps to reduce cyber risks to an acceptable level. It involves understanding the potential cyber threats to an organization's information assets and systems, evaluating the likelihood and impact of these threats, and implementing appropriate measures to mitigate them.

Key elements of cybersecurity risk management include:

- **Identifying Assets:** Cataloguing what needs to be protected.
- **Threat Assessment:** Determining the potential cyber threats.
- **Vulnerability Analysis:** Identifying weaknesses in systems and controls that could be exploited by threats.
- **Risk Assessment:** Estimating the potential impact and likelihood of threats exploiting vulnerabilities.
- **Risk Mitigation:** Implementing controls to protect against identified risks.
- **Monitoring and Review:** Continuously monitoring the security posture and reviewing the risk management process to adapt to new threats.

This report is an automated summary that captures all the vulnerabilities, risky activities, and security events found on the devices in the **All data Preset** by Cisco Cyber Vision on **May 28th, 2024 at 4:57 pm UTC**

Key Findings

Risk score	Total Devices	Vulnerable Devices	Events(over the last 30 days)
45	46	9	332

You are in a medium-risk zone. Resolving vulnerabilities is recommended, especially as individual devices might have very high scores.

Security Insights

Severity	Findings
Critical	50 critical and high severity vulnerabilities found on 9 devices
Critical	4 device(s) have a risk score >= 70
High	2 device(s) found communicating with external networks

Device Inventory Report

- Generate detailed reports on your device inventory to share with key stakeholders and document compliance reports
- Report highlights risks and events per asset
- Available as Word document or PDF
- Can include all assets or only specific presets
- Can be configured to have only an Executive Summary and/or the detailed list of devices

Create new report

1 General 2 Settings

* Name

Alphanumeric characters or hyphen(-), underscore(_) only (max 40)

Description

0 / 256

* Type

Security Posture

Security Posture

Remote Access

Device Inventory

Download Report Device Inventory

Upload

Cisco logo is the default logo in the report. Upload an SVG, PNG, or JPG image of max 200KB to customize the report header

General Settings

* Preset

All data

Table of content:

At least 1 section must be selected to generate a report

Executive Summary Preset Details

Introduction Risk Score filter

Risk Profile Networks filter

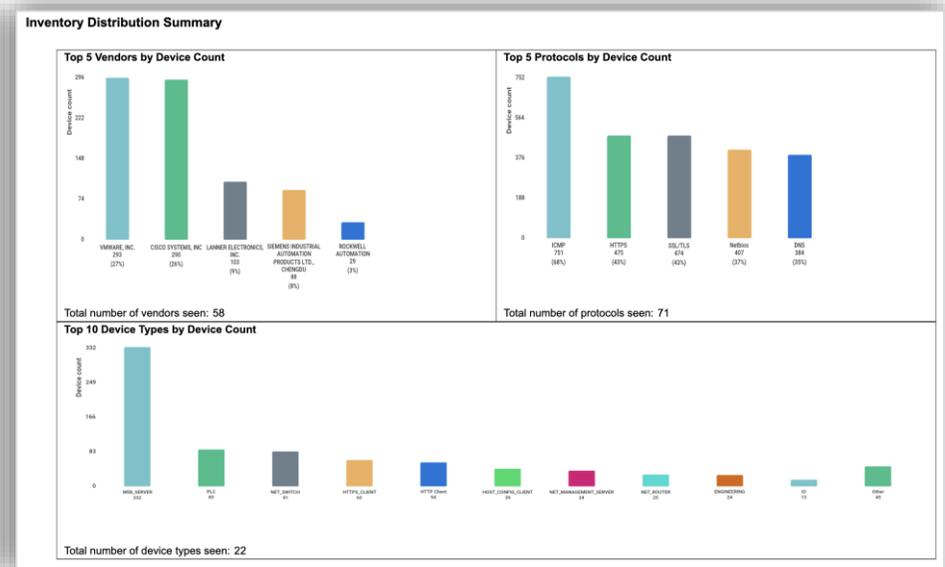
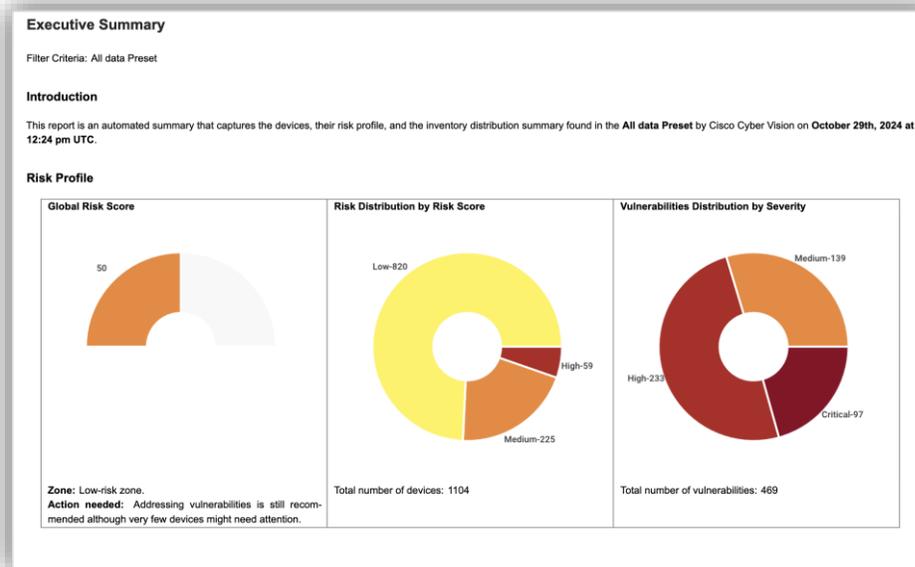
Inventory Distribution Summary Device Tags filter

Top Severity Events Activity Tags filter

External Communications Groups filter

Device Inventory List Sensors filter

Configuration



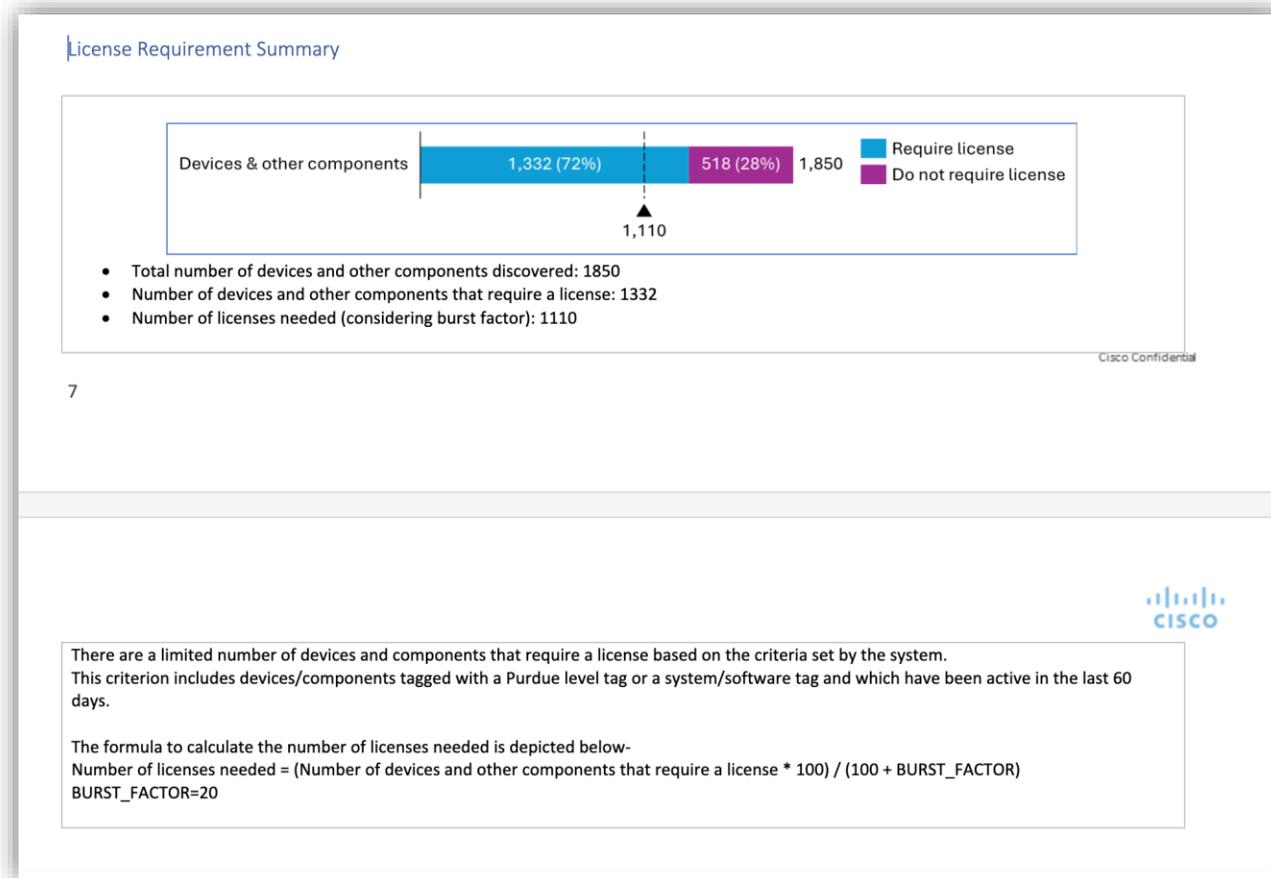
Report example



Device Inventory Report: Licensed Devices



- The Device Inventory Report highlights the Cyber Vision license requirement for your environment.



Remote Access Reports

* Type

Security Posture

Security Posture

Remote Access

Device Inventory

- Report to highlight presence of remote/external access
- Helps detect industrial gateways from vendors such as eWON and Moxa, and remote access software such as AnyDesk and TeamViewer

Cisco Cyber Vision Remote Access Report

March 14, 2024, 1:41 pm UTC

Remote Access Gateways

Filter Criteria: All data Preset

Cisco Cyber Vision has identified the following devices as Remote Access Gateways. These devices may provide access to users to control other OT or IT devices in the network remotely. It is recommended that only authorized users are provided access to selected devices, as needed.

Device Name	Device IP	Mac Address	Vendor	Group
ewon3	192.168.234.22	00:03:27:57:a5:d4	Ewon Inc.	NET_REMOTE_ACCE

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 is trying to access internal devices. The table below depicts those devices that have attempted to run a DNS query for any of these domains, indicating that these devices may have been remotely accessed.

Device Name	Device IP	Group	Domain Name	Count	Latest Timestamp (UTC)
THINKCENTER	192.168.0.72	-	de-fra-anx-r048.router.teamviewer.com	1	2024-03-14 01:40 PM
THINKCENTER	192.168.0.72	-	udp.ping.teamviewer.com	3	2024-03-14 01:39 PM
THINKCENTER	192.168.0.72	-	client.teamviewer.com	2	2024-03-14 01:39 PM
THINKCENTER	192.168.0.72	-	router16.teamviewer.com	1	2024-03-14 01:39 PM
THINKCENTER	192.168.0.72	-	whatsnew.teamviewer.com	1	2024-03-14 01:39 PM
THINKCENTER	192.168.0.72	-	de-muc-anx-r005.router.teamviewer.com	1	2024-03-14 01:39 PM
THINKCENTER	192.168.0.72	-	router13.teamviewer.com	1	2024-03-14 01:39 PM
10.2.1.59	10.2.1.59	-	ntp.talk2m.com	6	2024-03-14 07:51 AM
10.2.1.59	10.2.1.59	-	device.talk2m.com	5	2024-03-14 07:51 AM

Reports Creation and Management

The screenshot displays the Cisco Reports management interface. At the top, there is a navigation bar with the Cisco logo, a 'Reports' dropdown menu, and a 'Go to Cyber Vision beta' button. Below the navigation bar, the main content area is titled 'Generate and manage your reports' and shows '3 Reports'. A '+ Create and run a Report' button is visible. The reports are listed in a table with columns for Name, Preset, Type, Created by, Last Modified, Status, Last Run, and Actions. The table contains three rows: 'DeviceReport', 'Remote Access report', and 'Security Posture report'. The 'Security Posture report' row has an open context menu with options: 'Run Again', 'Edit', 'Duplicate', and 'Delete'. The 'Last Run' column for the 'Security Posture report' shows 'Oct 28, 2024, 11:12 AM' with a refresh icon. The 'Status' column for all reports shows 'Success' with a green dot icon. The 'Actions' column for each report has a three-dot menu icon.

Name	Preset	Type	Created by	Last Modified	Status	Last Run	Actions
DeviceReport	Essential data	Device Inventory	admin@cisco.com	Jan 9, 2025, 9:54 AM	Success	Jan 9, 2025, 9:54 AM	...
Remote Access report	All data	Remote Access	admin@cisco.com	Oct 28, 2024, 3:40 PM	Success	Oct 28, 2024, 3:40 PM	...
Security Posture report	All data	Security Posture	admin@cisco.com	Oct 28, 2024, 11:12 AM	Success	Oct 28, 2024, 11:12 AM	Run Again Edit Duplicate Delete

Reports Creation Wizard

Create new report

1 General 2 Settings

* Name

Alphanumeric characters or hyphen(-), underscore(_) only (max 40)

Description

0 / 256

* Type

Security Posture

This report is an automated summary that captures all the vulnerabilities, risky activities, and security events found on the devices in the selected preset by Cisco Cyber Vision

Customer logo

[Upload](#)

Cisco logo is the default logo in the report. Upload an SVG, PNG, or JPG image of max 200KB to customize the report header

* Format

Create new report

General 2 Settings

* Preset

All data

Table of content:

At least 1 section must be selected to generate a report

- Key Findings
 - Security Insights
 - Top 5 most matched vulnerabilities
 - Top 5 Vendors seen
 - Top 5 Protocols seen
- Security Events seen in {presetName} Presets
- Risky devices in {presetName} Presets
 - Devices with high risk scores
 - Devices with unacknowledged vulnerabilities
 - Devices with acknowledged vulnerabilities
- Risky communications in {presetName} Presets
 - Top 5 most accessed external URLs/IP addresses
 - Top 5 devices accessing the most external URLs/IP addresses
 - Devices that have been remotely accessed
 - Unsecure protocols used by devices
 - Devices using clear text credentials
- Vulnerabilities in {presetName} Presets

[Cancel](#) [Back](#) [Save and Run](#)

Extending IT security to your OT environment

Cyber Vision has the OT information the SOC needs

Visibility

Provides **OT context**, asset inventory and communications map to your SOC

Vulnerabilities

Identify asset vulnerabilities and **assess risks** before they are exploited

Intrusions

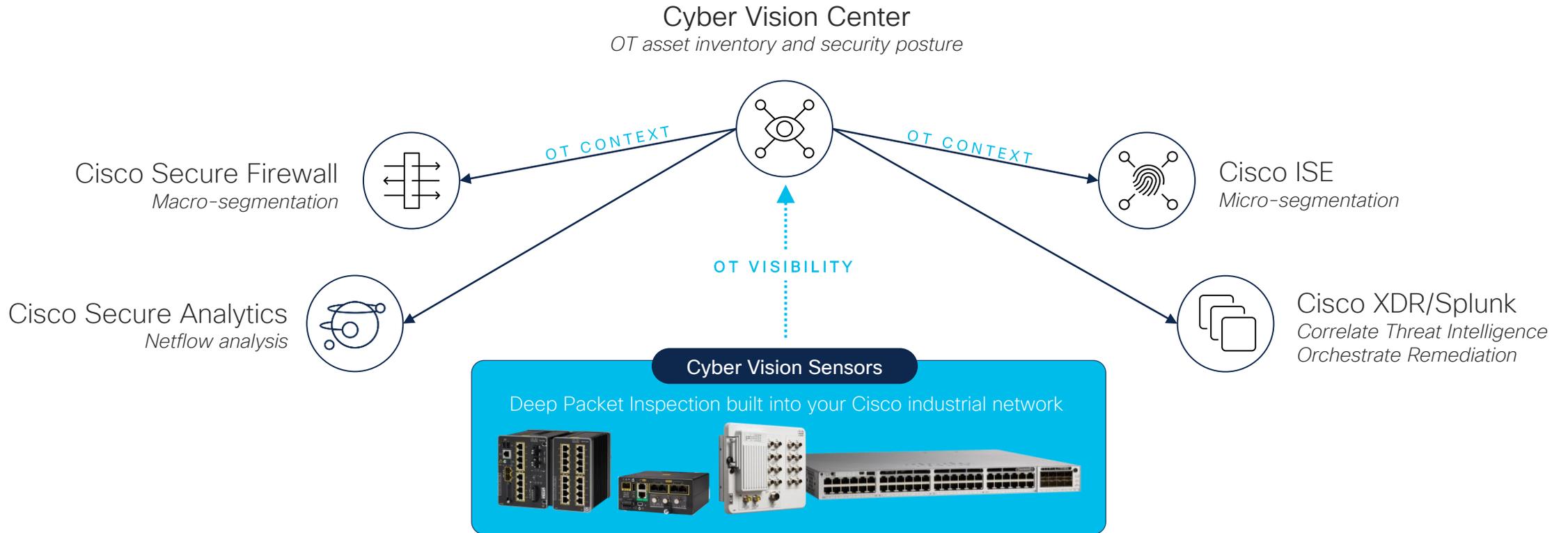
Leverages Talos signatures to detect known and emerging **IT attacks**

Anomalies

Monitor mode detects **malicious behaviors** and unknown attacks

OT events and context shared with your SIEM and IT security platforms

Extend IT security to your industrial settings



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

Integrations and customization via RESTful API

- Access data about components and communication flows available in Cyber Vision
- Leverage sandboxed application hosting to automate functions and integrations
- Modify tag assignment, presets and groups programmatically
- Define custom analyzers for unknown traffic in environment
- Enable bulk acknowledgements of vulnerabilities

API

From this page, you can create, edit and delete authentication tokens. Tokens can be used with the more information.

Name	Token	Status
SampleToken	Hidden (show)	Enabled

Integrate data from Cyber Vision
into additional tools

API Explorer

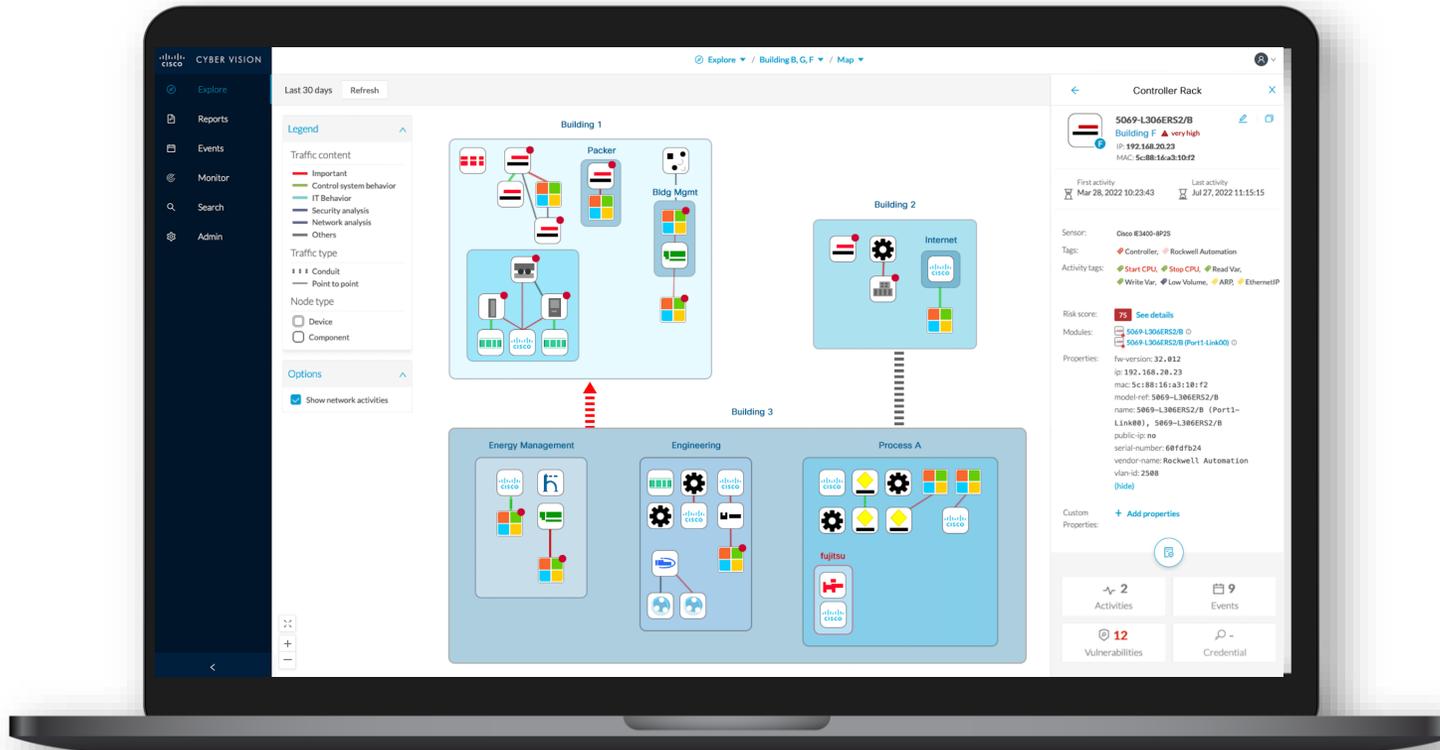
- Building API calls now super easy!
 - Automated documentation
 - Code generation
 - Test-case creation
- Leverage Cyber Vision data to create custom feeds to your tools
- Sample scripts are provided
 - Grouping assets into zones
 - Creating profiling rules
 - and more...

The screenshot displays the Cisco API Explorer interface. On the left is a dark sidebar with the Cisco logo and a navigation menu containing: System, Data management, Sensors, Users, Events, API (highlighted), Token, Documentation, License, LDAP Settings, PxGrid, SNORT, Integrations, and Extensions. The main content area is titled "Cisco Cyber Vision center v3 API. 0.1" and shows the base URL as "/api/3.0/" and the JSON file as "cisco-cyber-vision-api-v3.json". A "Schemes" dropdown menu is set to "HTTPS". Below this, several API endpoints are listed with their methods and descriptions:

- Activities**: Activities are an aggregation of flows between components.
- Baselines**: A baseline is used for monitor mode. They represent a snapshot of the network.
- BaselineDifferences**: In monitor mode, these routes allow to retrieve and review differences between the actual network activity and the baseline description.
- Components**: Components are logical nodes of the network.
- GET /components**: Component list.
- GET /components/{id}**: Get details of one or many components.
- PATCH /components/{id}**: Partial update of a component.
- GET /components/{id}/credentials**: Credential list of a component.
- GET /components/{id}/flows**: Flow list of a component.
- GET /components/{id}/flows/tags**: Flow tag list of a component.
- POST /components/{id}/label**: Set the custom name of a component.
- DELETE /components/{id}/label**: Delete the custom name of a component.

Automating OT network segmentation

Leveraging Visibility to Drive Segmentation



IEC-62443 virtual segmentation

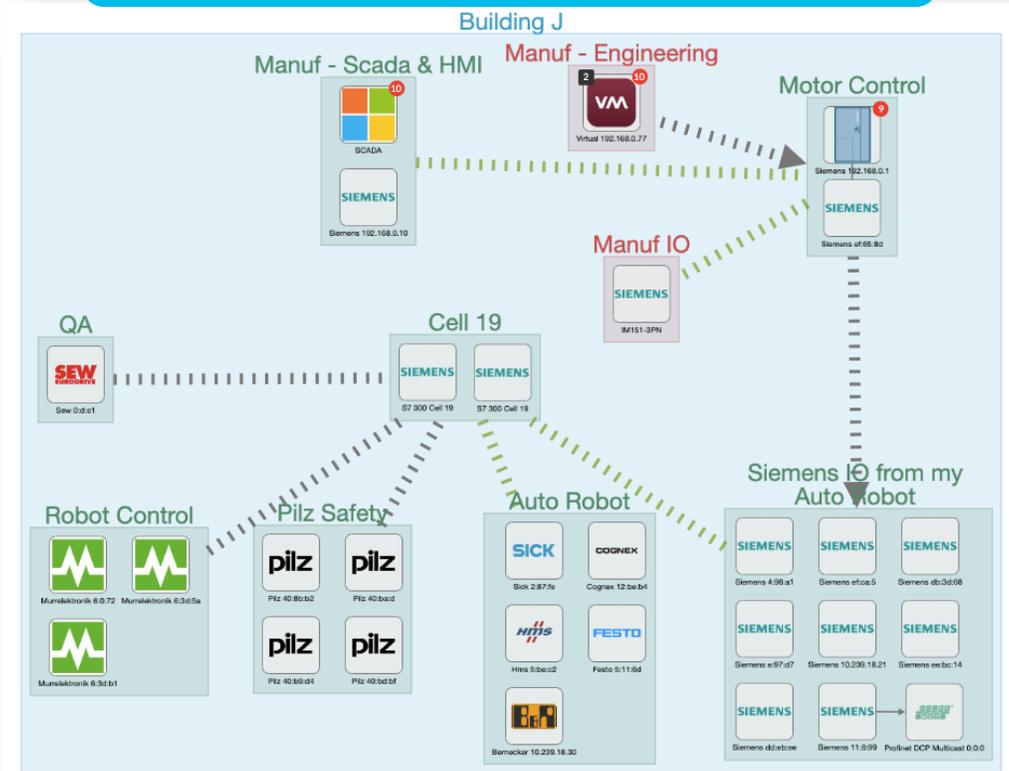
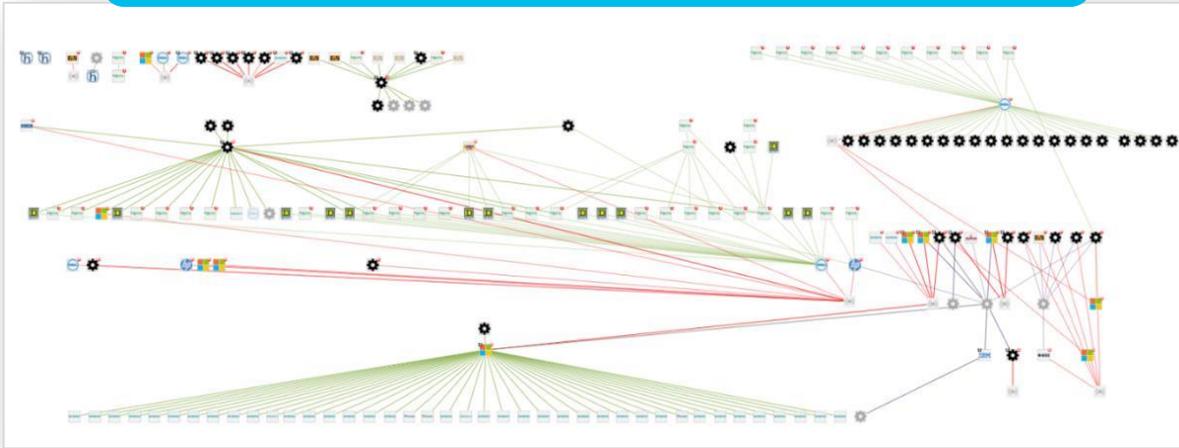
- ✓ Group OT assets into zones
- ✓ Visualize conduits
- ✓ Identify traffic violations
- ✓ Share context with other platforms to enforce segmentation

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

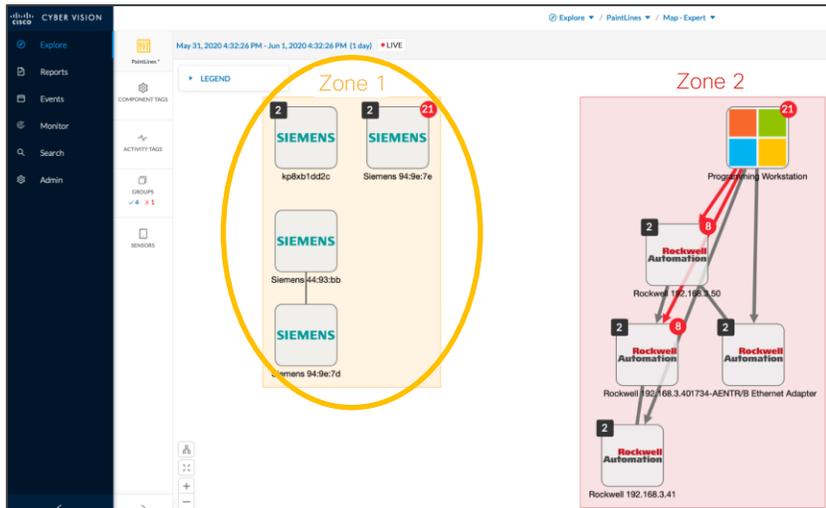
Automated Segmentation **Informed by Visibility**



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	✗	✗	✓	✓

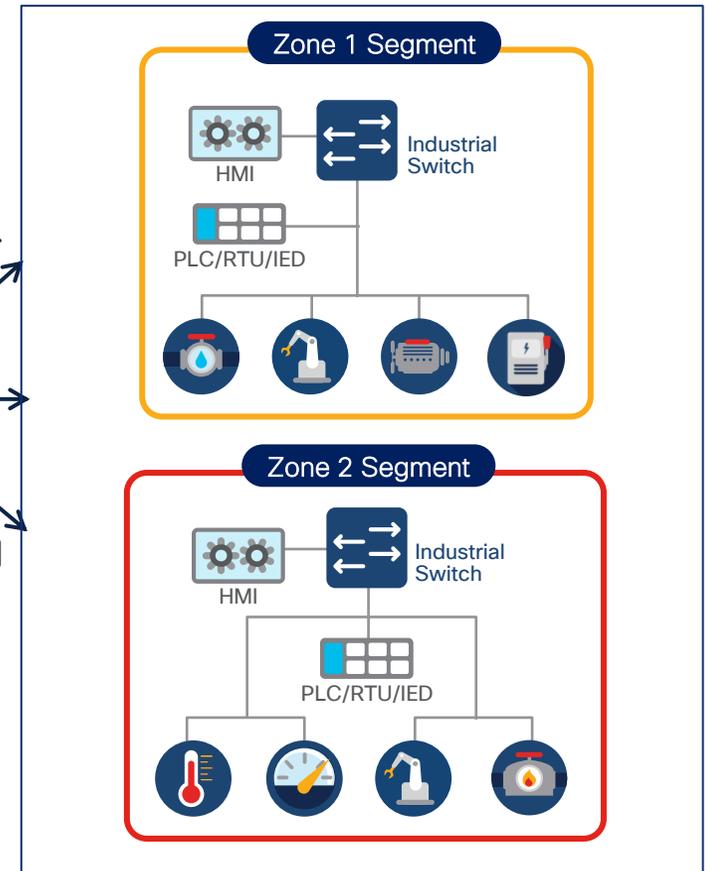
Cisco Firewall Policy Rules
or
Cisco ISE Policy Matrix

dACL

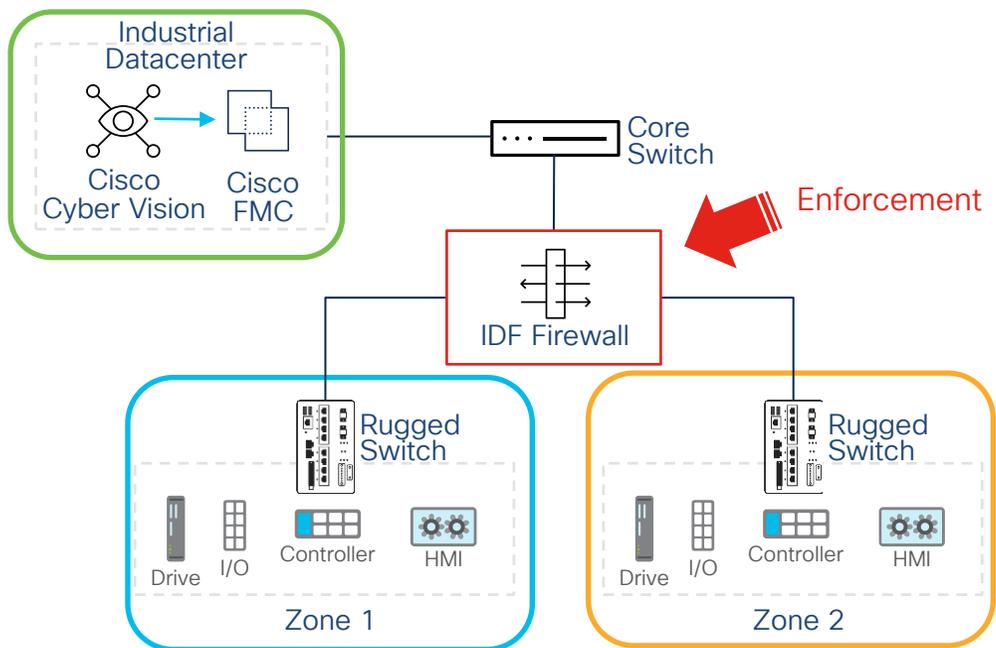
SGT

VLAN

Segmentation of industrial network



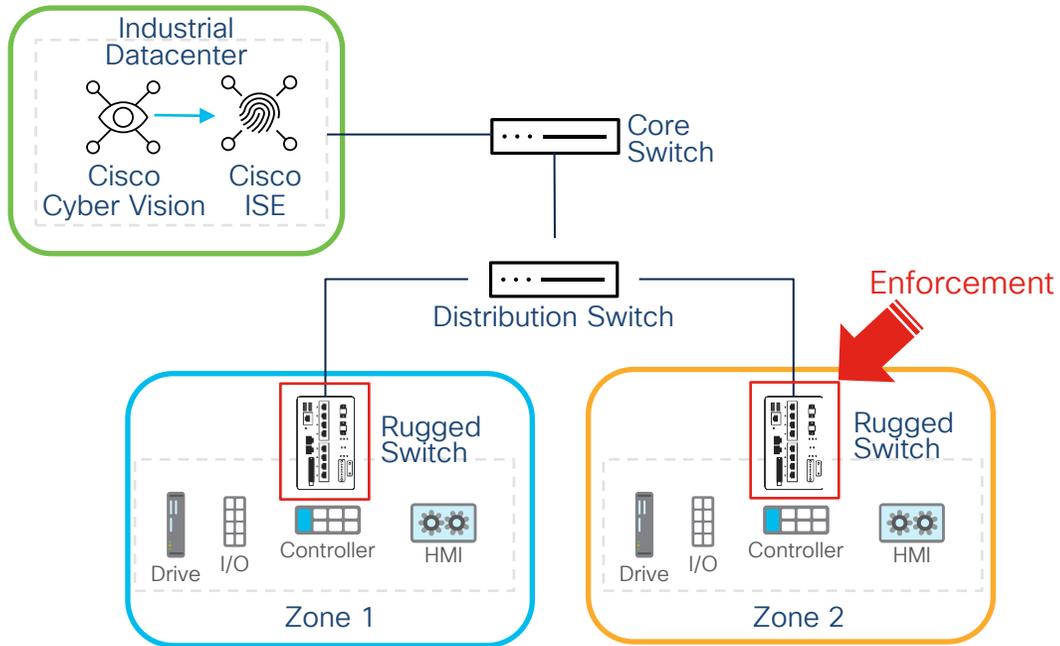
Automated Segmentation **Enforced using Firewalls**



- 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

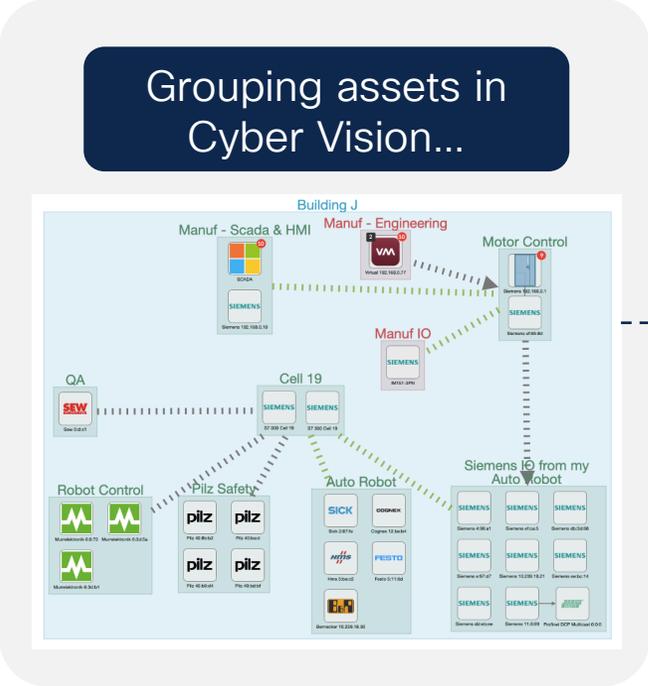
Automated Segmentation **Enforced using Switches**



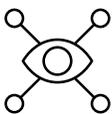
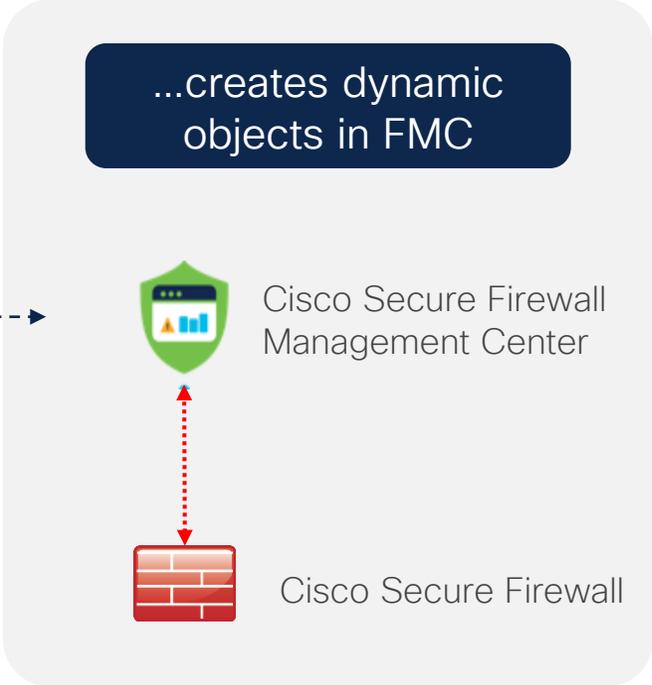
- Cisco Identity Services Engine (ISE) receives devices' profiles from Cyber Vision and associates a network access policy to each
- Policies are pushed to network switches for enforcement at the port level
- Network switches allow/deny assets to communicate based on their profile, not their IP address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

Network access policies automatically updated when OT modifies Cyber Vision groups

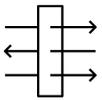
Visibility drives segmentation with Cisco Secure Firewalls



CSDAC



Cisco Cyber Vision
Gain full visibility into assets, and group them according to their role in the industrial process



Cisco Secure Firewall
Automatically update firewall rules to segment industrial networks based on Cyber Vision groups

Simplifying network segmentation with dynamic firewall rules informed by OT visibility

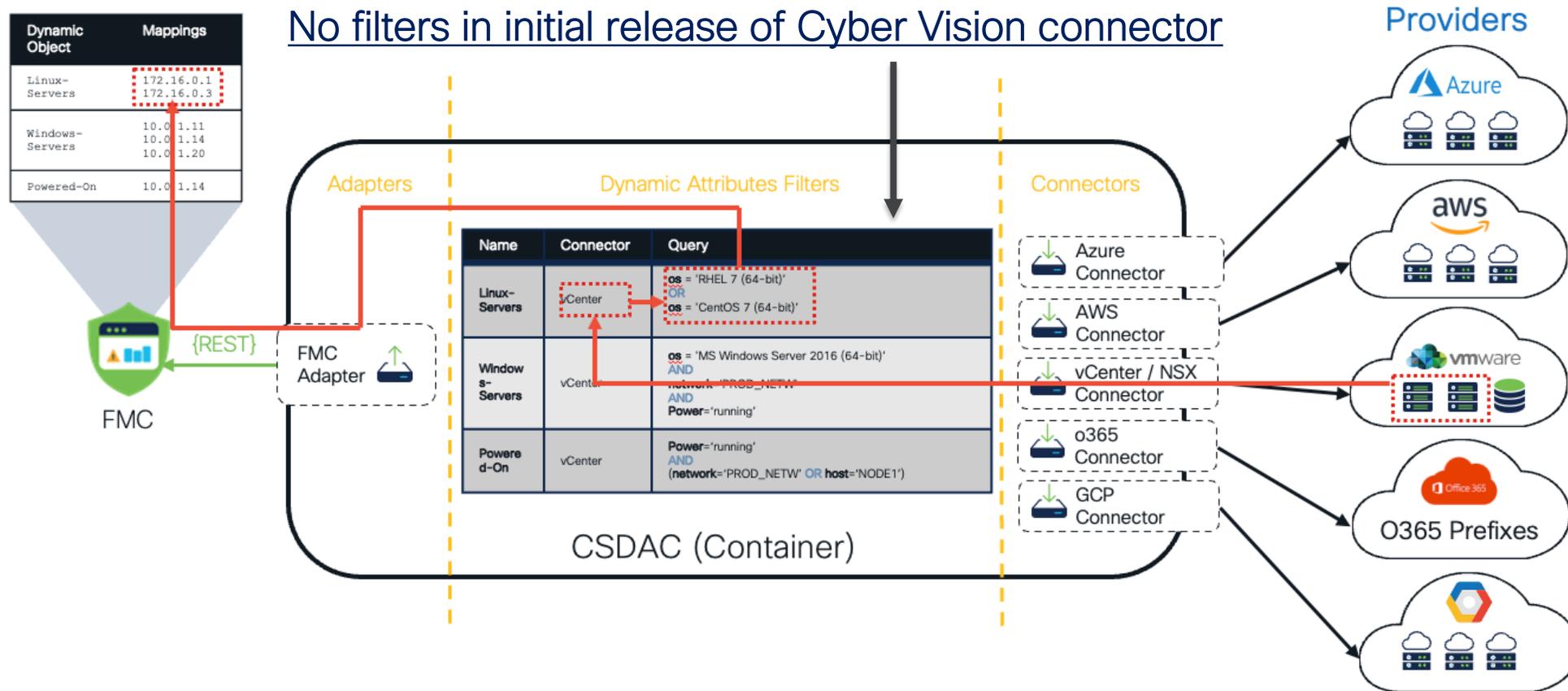
What is CSDAC?

Cisco Secure Dynamic Attributes Connector

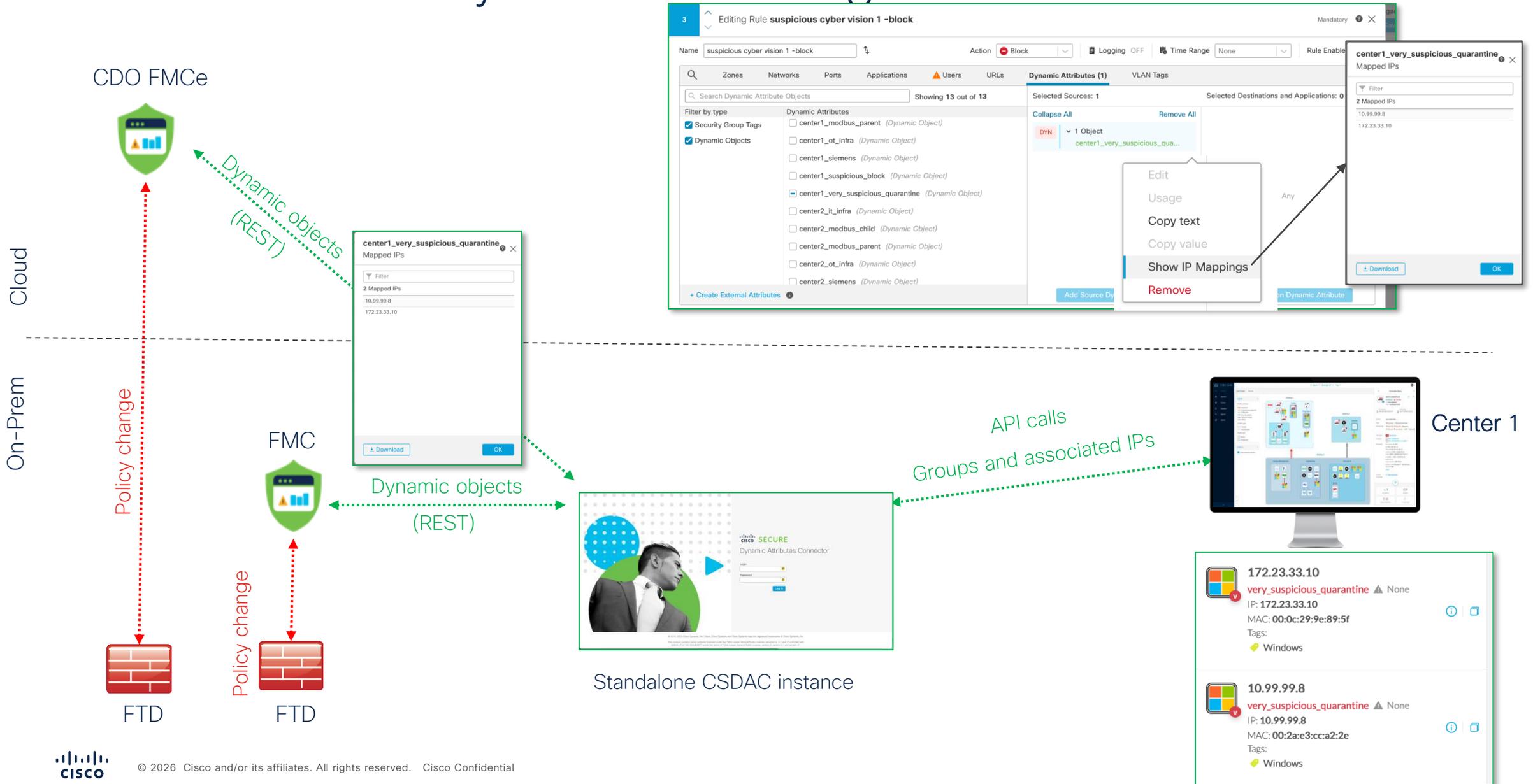
- CSDAC is a Middleware engine (docker container based)
 - It translates API calls from third party elements into dynamic objects for use in FTD access control policy
 - Its available as 1) standalone 2) embedded in FMC (7.4) or FMCe (CDO)
- Primarily used for Cloud and Public Feed Connectors
- Cyber Vision integration is available using a connector
 - Allows for dynamic input to FMC access control policy from Cyber Vision assets
 - No filters in CSDAC - it acts as passthrough
 - Multiple Cyber Vision systems can be connected

Cisco Secure Dynamic Attributes Connector (CSDAC)

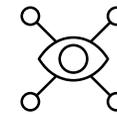
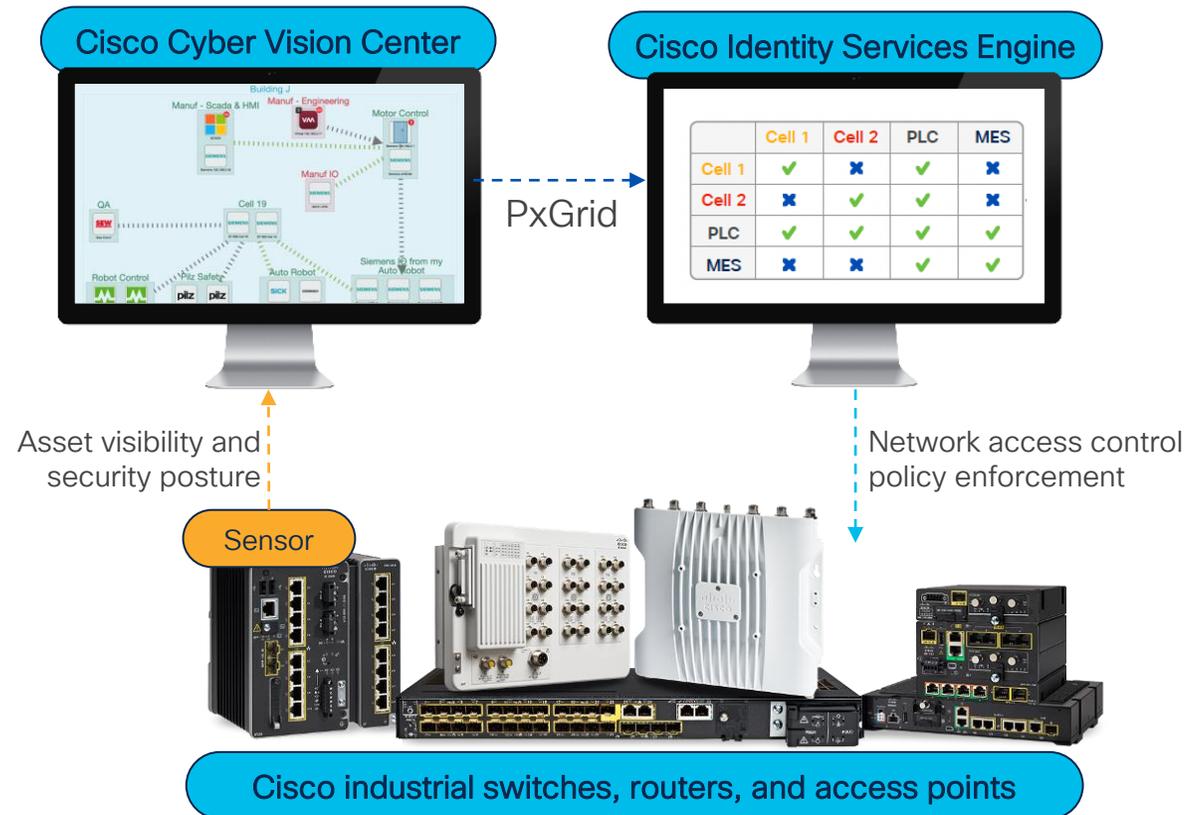
Immediate visibility of object changes. No policy deployment is required.



Cisco CSDAC: Cyber Vision integration



Visibility drives micro-segmentation with Cisco ISE



Cisco Cyber Vision

Gain full visibility into assets, and group them according to their role in the industrial process



Cisco Identity Services Engine

Automatically update access control policies for the network to enforce zero-trust segmentation based on Cyber Vision groups

Enforcing network access policies for each device connected to the industrial networks

Integration with Cisco Identity Services Engine (ISE)

E4:90:69:9E:EF:7D

MAC Address: E4:90:69:9E:EF:7D
Username: E4-90-69-9E-EF-7D
Endpoint Profile: Austin_Plant_Profiler
Current IP Address: 192.168.119.39
Location: Location → All Locations

Applications | **Attributes** | Authentication | Threats | Vulnerabilities

General Attributes

Description

Static Assignment: false

Endpoint Policy: Austin_Plant_Profiler

Static Group Assignment: false

Identity Group Assignment: Austin_Plant_Profiler

Custom Attributes

Attribute Name	Attribute Value
assetGroup	Root > Austin_Plant
assetDeviceType	Controller
assetId	101
assetIpAddress	192.168.119.39
assetMacAddress	04:90:69:9e:ef:7d
assetName	192.168.119.39
assetProductid	1769-L36ERM/A LOGIX5336ERM
assetProtocol	CIP
assetSerialNumber	0x04052C7
assetSwRevision	28.011
assetVendor	Rockwell Automation/Allen-Bradley
ip	192.168.119.39

Devices in ISE get attributes from Cyber Vision

Production Matrix
Populated cells: 36

Destination	Plant 16/0010	Cell1 17/0011	Cell2 18/0012	LinePC 21/0015
Source				
Plant 16/0010	Permit IP	Deny IP	Deny IP	Permit IP
Cell1 17/0011	Deny IP	Permit IP	Deny IP	Permit IP
Cell2 18/0012	Deny IP	Deny IP	Permit IP	Permit IP
LinePC 21/0015	Permit IP	Permit IP	Permit IP	Permit IP

TrustSec policy to enforce zone segmentation

Enrich endpoint attributes in ISE with rich context from Cyber Vision

Assign SGTs based on Cyber Vision grouping for dynamic policy assignment to endpoints

Enforce segmentation through dynamic assignment of VLAN, dACLs or TrustSec

Device information can be sent to ISE based on user selection and filtering of network.

Cyber Vision and ISE enable dynamic segmentation of industrial networks

Cyber Vision - Attributes via pxGrid

ISE attribute	Cisco Cyber Vision property	Description
IOTASSET Library		
assetId	ID	Cyber Vision Component ID
assetName	Name	Component name
assetIpAddress	IP	Component IP address
assetMacAddress	Mac	Component MAC address
assetVendor	Vendor-name	Component manufacturer (IEEE OUI)
assetProductId	Model-ref	Manufacturer product ID
assetSerialNumber	Serial-number	Manufacturer serial number
assetSwRevision	Fw-version	Component firmware version
assetHwRevision	Hw-version	Component hardware version
assetProtocol	Protocols	All Protocols concatenated in one string
Custom Attributes		
assetModelName	Model-name	Manufacturer model name
assetOsName	OS-name	Operating system name
assetProjectName	Project-name	Project name (from PLC program)
assetProjectVersion	Project-version	Project version (from PLC program)
assetGroup	Group	Component group in Cyber Vision
assetGroupPath	Group Path	Component group path in Cyber Vision (Nested Groups)
assetCustomName	Custom Name	Custom Name assigned to component by user

ISE Integration – Custom properties [1/2]

Starting from v5.4 ISE integration supports defining and provisioning up to 4 custom properties.

Custom device attributes created and added via UI or API

Device: Line1 | 5069-L310ER/A
SGT4122 | None
IP: 172.16.10.1 (+ 1 other)
MAC: 5c:88:16:be:5a:6d (+ 1 other)

First activity: Oct 8, 2024 4:28:22 PM
Last activity: Oct 30, 2025 6:19:47 PM

Tags: IO Module, Controller, Rockwell Automation, Unestablished, Insecure, Net Management, Web, Active Discovery, ...10+

Custom properties:
Network: Line-1
Location: Building-111
Service: Line-1

PxGrid integration configuration

PxGrid configuration

Node Name: SRV01CENTER

Host Name: isetraining.ccvtraining.net

IP Address: 10.2.1.130

Client certificate: Import PxGrid certificate

P12 password

Custom attributes to sync to ISE

ccvCustom1	Location
ccvCustom2	Service
ccvCustom3	Network
ccvCustom4	GPS

PxGrid integration configuration

Enables synchronization of custom variables from Cyber Vision device to ISE asset. Ex: choosing "my-variable-key" as the key for ccvCustom1 makes its value visible in ISE as ccvCustom1.

Custom attributes to sync to ISE

ccvCustom1	Location
ccvCustom2	Service
ccvCustom3	Network
ccvCustom4	GPS

Custom attributes selection complete. It is not possible to add more than 4 values.



ISE Integration – Custom properties [2/2]

Use mapped and provisioned CV attributes in ISE

Cyber Vision

Custom attributes to sync to ISE ⓘ

ccvCustom1	Location	⊗
ccvCustom2	Service	⊗
ccvCustom3	Network	⊗
ccvCustom4	Select a property	

DEVICE CUSTOM PROPERTIES

Properties:

Network	Line-1	✎	🗑
Location	Building-111	✎	🗑
Service	Line-1	✎	🗑

+ Add new property



ISE

Endpoint Custom Attributes

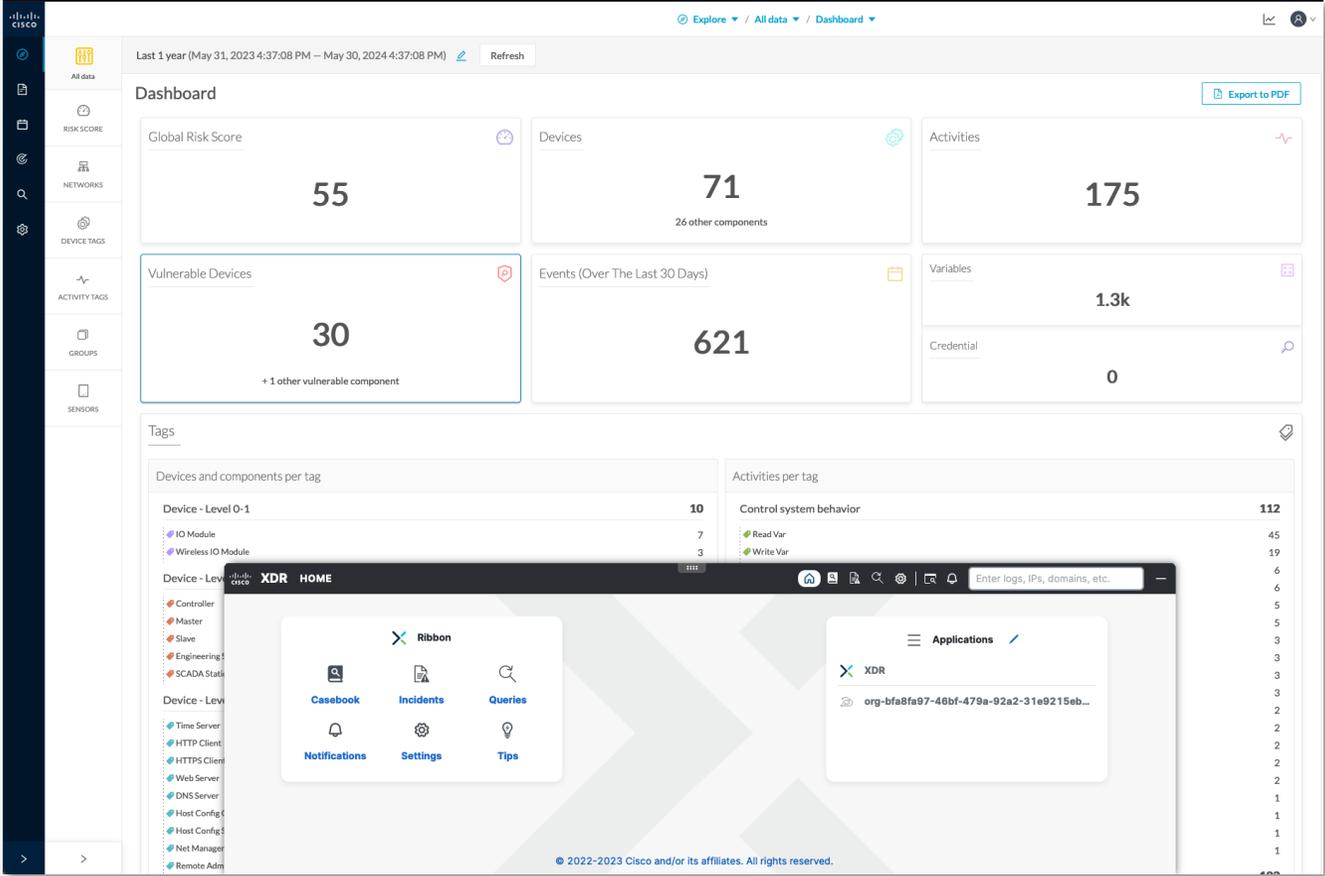
Attribute Name	Type	
ccvCustom1	String	🗑
assetGroup	String	🗑
assetProjectVersion	String	🗑
assetSource	String	🗑
assetOsName	String	🗑
assetGroupPath	String	🗑
assetCustomName	String	🗑
assetProjectName	String	🗑
assetModelName	String	🗑
ccvCustom2	String	🗑
ccvCustom3	String	🗑 +

Custom Attributes

ccvCustom2	Line-1	assetOsName	-
ccvCustom1	Building-111	assetGroupPath	SGT4122
assetGroup	SGT4122	assetCustomName	-
ccvCustom3	Line-1	assetProjectName	-
assetSource	CCV	assetModelName	-
assetProjectVersion	-		

Providing OT context to the SOC

Investigation & Orchestration with Cisco XDR



Leverage Cyber Vision Observables to:

Create and **manage incidents** in Cisco XDR

Create and **orchestrate playbooks**

Launch investigations in Talos, Umbrella, Secure Endpoint, Threat Grid, etc.

XDR Ribbon in Cyber Vision for investigations and remediation orchestration



Promote Cyber Vision events to Cisco XDR

View events in Cyber Vision

Launch investigation in XDR

April 2, 2024 11:40:55 AM critical Control Systems Events

Stop CPU command has been detected from 192.168.105.241 (192.168.105.241) | IP: 192.168.105.241 | MAC: 34:17:eb:d1:c9:97 to 192.168.105.112 (192.168.105.112) | IP: 192.168.105.112 | MAC: 28:63:36:85:b3:32

source	destination	Flow	Source component	Destination component
 192.168.105.241	 192.168.105.112	Source port: 1613 Destination port: 102	Device: 192.168.105.241 Name: 192.168.105.241 MAC: 34:17:eb:d1:c9:97 IP: 192.168.105.241 Tag: Engineering Station	Device: 192.168.105.112 Name: 192.168.105.112 MAC: 28:63:36:85:b3:32 IP: 192.168.105.112 Tag: Controller Vulnerabilities detected: 32

[Report to XDR](#)

Threat Response Investigate Snapshots Incidents Intelligence

Create New Incident Investigate This Incident Change Status Link Reference Download

Find ...

Control system event: Stop CPU command has been detected from...

Control system event: Stop CPU command has been detected from 192.168.249.114 to 192.168.249.502
New - Created by Cisco Cyber Vision on 2021-05-26T04:30:49.867Z

Summary Observables Timeline Sightings Linked References (0)

Seen at 2021-05-26T04:30:27.661Z

Source: Cisco Cyber Vision
Sensor: Network Sensor
IP Address
device

Confidence: High
Severity: High
Environment: Global
Resolution: N/A

DESCRIPTION

Name	Source	Destination
DESKTOP-GBJUF2N	1769-L168/B LOGIX5316ER	
Vendor VMware, Inc.	Rockwell Automation	
Mac 00:0e:29:c7:c8:76	14:54:33:91:eb:ee	
IP 192.168.249.114	192.168.249.50	
Tags	WINDOWS, ENGINEERING PLC, ROCKWELL_AUTOMATION	

TARGETS

IP Address 192.168.249.50

OBSERVABLES RELATED TO SIGHTING (1)

IP Address 192.168.249.114

RELATIONS (1)

IP Address 192.168.249.114 Connected To IP Address 192.168.249.50

KEY PROPERTIES

Categories: Investigation
Disc. Method: Cisco Cyber Vis...
Intend. Effect: Select...
Confidence: High
TLP: Amber

192.168.249.50 IP Address

Add to current Investigation
Investigate in Threat Response
Create Judgement
Talos Intelligence
Search for this IP
Umbrella
IP view for 192.168.249.50

Promote event to Cisco XDR

Events generated in Cyber Vision for process anomalies, signatures and control system can be promoted

Investigate the threat with enrichment from Cisco and 3rd party security products

Cisco XDR Ribbon on Cyber Vision

The screenshot shows the Cisco Cyber Vision dashboard. On the left is a sidebar with navigation options: All data, Basics, Criteria, RISK SCORE, NETWORKS, DEVICE TAGS, ACTIVITY TAGS, GROUPS, and SENSORS. At the bottom of the sidebar, the 'XDR' ribbon is highlighted with a red box. A blue arrow points from this ribbon to the XDR HOME interface shown in the adjacent screenshot. The main dashboard area displays a 'Dashboard' with several widgets: Global Risk Score (60), Devices (5), Vulnerable Devices (2), and Events (Over The Last 30 Days) (28). Below these are 'Tags' and a table of 'Devices and components per tag'.

Device	Count
Device - Level 2	4
Controller	2
Engineering Station	2
Device - Level 3-4	1
DNS Server	1
System	2

Create and manage **incidents**,
Launch **investigations**,
Orchestrate **playbooks**...
...directly from Cyber Vision

The screenshot shows the 'XDR HOME' interface. It features a central 'Ribbon' with icons for Casebook, Incidents, Queries, Notifications, Settings, and Tips. To the right, there is an 'Applications' section with a search bar and a list of applications, including one with ID 'org-bfa8fa97-46bf-479a-92a2-31e9215eb...'. A search bar at the top right is labeled 'Enter logs, IPs, domains, etc.'. The footer contains the copyright notice: '© 2022-2023 Cisco and/or its affiliates. All rights reserved.'

Investigate OT events with Cisco XDR

The screenshot shows the Cisco Cyber Vision interface. At the top, it displays device information for 'IM151-8-CPU' with IP 192.168.1.40 and MAC 00:1b:1b:23:eb:3b. Below this, there's a section for 'Observables on Page' which lists 9 IP addresses, including 192.168.1.40, 192.168.1.10, 172.16.0.51, 172.16.0.1, 192.168.105.241, 192.168.105.112, 192.168.105.150, and 192.168.105.120. Buttons for 'Add 19 Observables to Case' and 'Run Investigation' are visible at the bottom of this list.

Pivot from Cyber Vision to XDR to investigate observables...

...pull details from Umbrella, FTD, Talos, AMP, Stealthwatch, etc.

The screenshot shows the Cisco XDR Threat Response interface. The top navigation bar includes 'Threat Response', 'Investigate', 'Snapshots', 'Incidents', 'Intelligence', and 'Modules'. Below the navigation, there are buttons for 'New Investigation', 'Assign to Incident', and 'Snapshots...'. The main content area shows investigation details for IP 208.67.222.222, including a 'Sightings' graph and a 'Judgements (1) Verdicts (1)' table. The table shows a judgement from Umbrella with a disposition of 'Unknown' and a reason of 'Neutral Cisco Umbrella r'. A context menu is open over the IP address, showing options like 'Copy to Clipboard', 'Create Judgement', 'Add to New Case', 'Talos Intelligence', 'Threat Grid', and 'Umbrella IP view for 208.67.222.222'.



Response Orchestration with XDR Workflows

Orchestration out of the 'box'

- 75 workflows published by Cisco as of Fall 2022
- More being released on a frequent basis

▶ Move Computer to Secure Endpoint Triage group

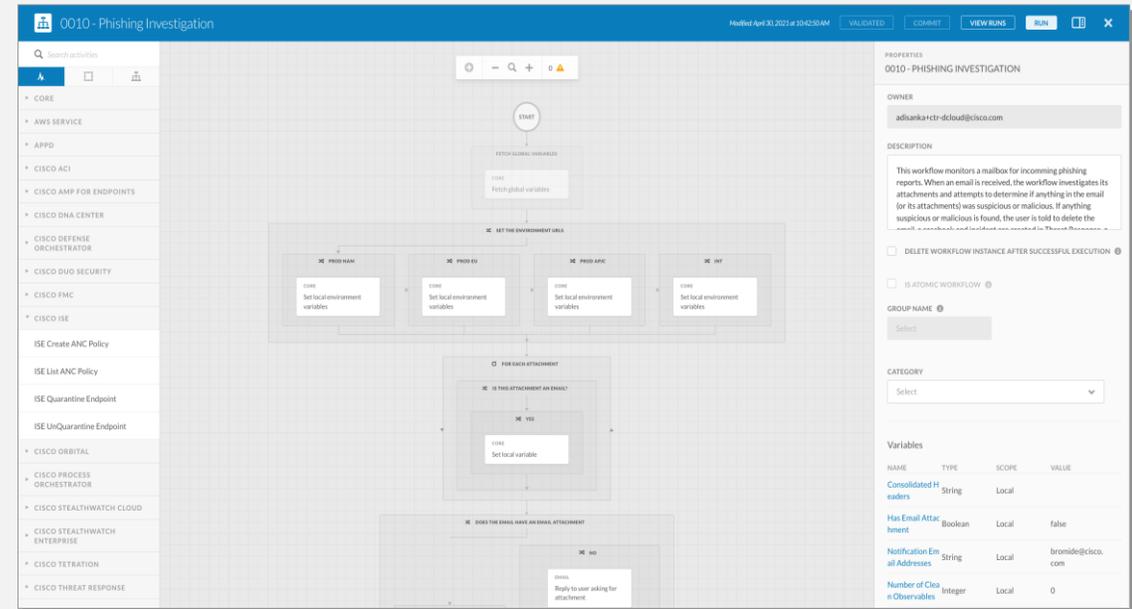
▶ Submit URL to Secure Malware Analytics

▶ Take Orbital forensic snapshot

▶ Take forensic snapshot and isolate

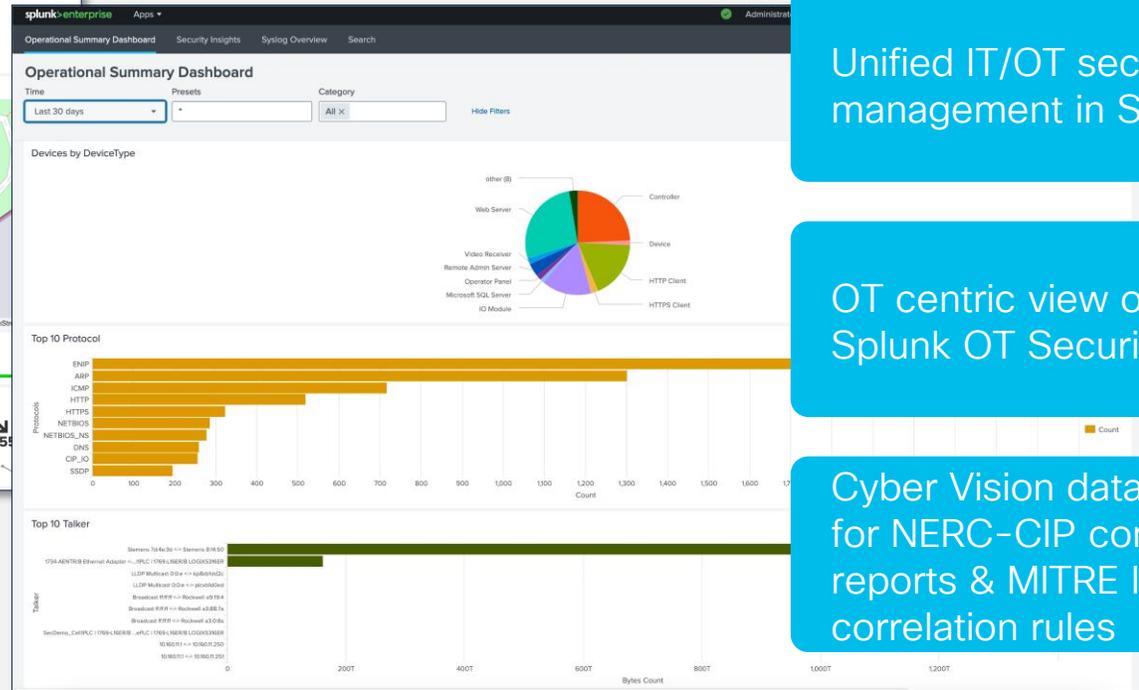
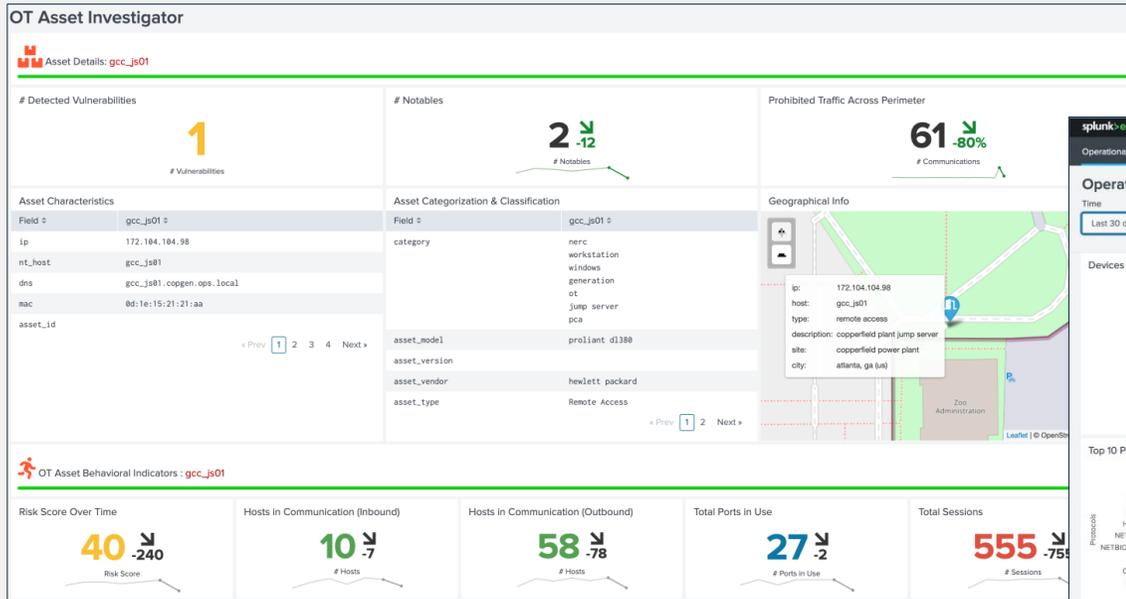
▶ Secure Endpoint host isolation with tier 2 approval

Custom orchestration workflows



Build your own workflows with our low-to no-code, drag-and-drop canvas

Splunk Integration



Unified IT/OT security events management in Splunk SIEM

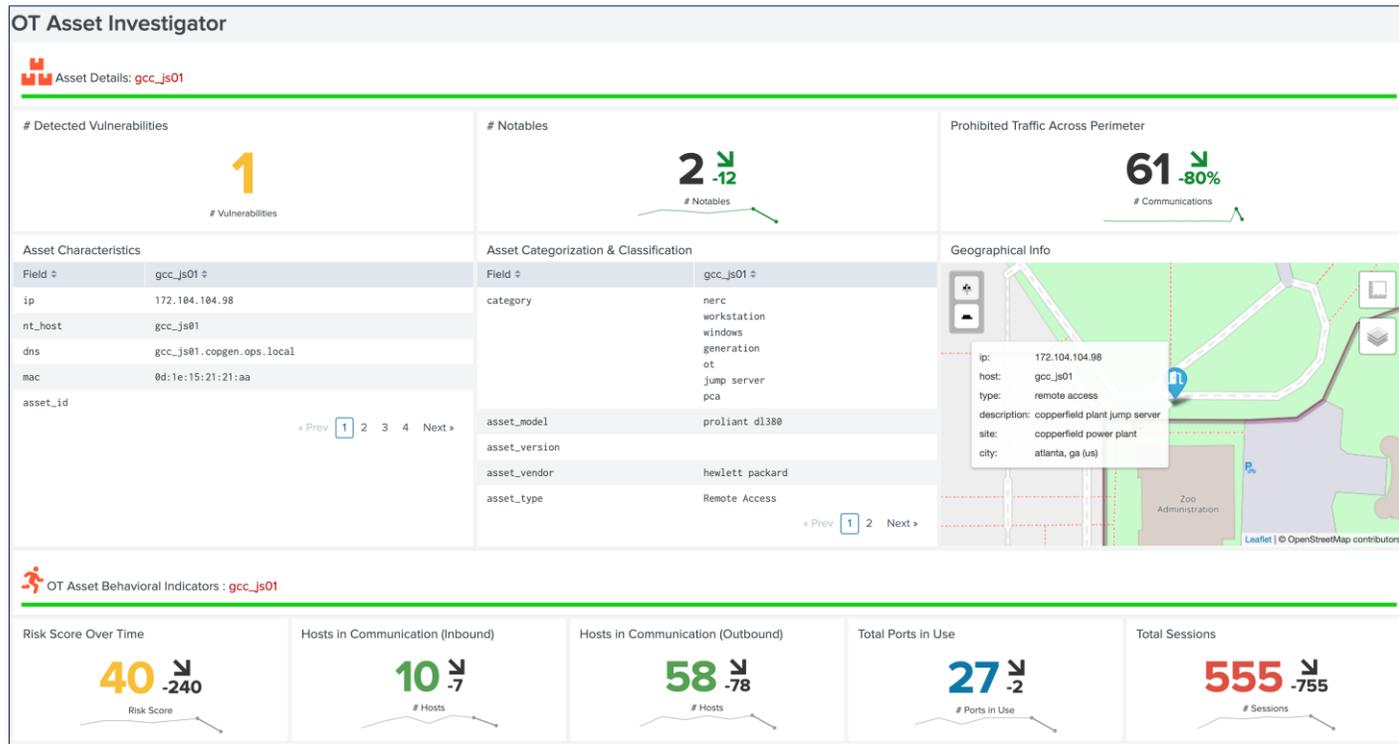
OT centric view of assets in Splunk OT Security Add-on

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

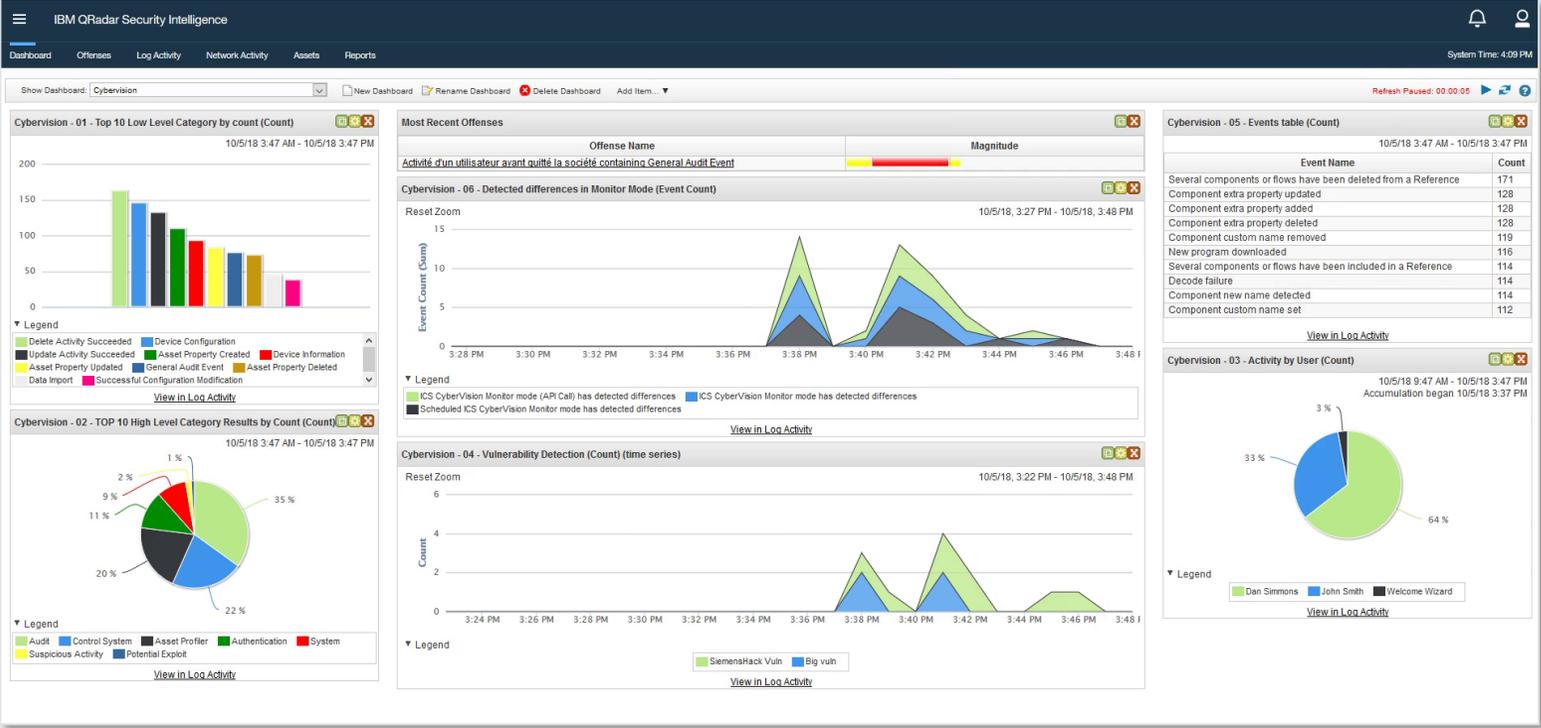


Splunk's OT Security Add On



- Expands Splunk's capabilities across IT and OT environments
- OT centric view of assets
- NERC CIP compliance reporting
- MITRE ICS correlation rules
- Integration with enterprise security
- Cyber Vision data can feed Splunk OT Security Add On
- Splunk OT Security Add On managed and supported directly by Splunk

QRadar Integration



Correlate OT and IT events to quickly remediate threats

Focus on real threats using Machine Learning and pre-defined analytics rules

Automatically discover and monitor OT infrastructure, vulnerabilities and traffic

Syslog integration with free app in X-Force App Exchange



Extending OT visibility to your CMDB



OT asset	OT asset type	IP Address	Manufacturer	Discovery source	Most recent discovery	First discovered	Created
Fisher 10.4.0.22_3769f785-3d84-526c-adf3...	DCS	10.4.0.22	Fisher-Rosemount Systems Inc.	ImportSet	2021-11-16 07:11:23	2021-11-16 07:11:23	2021-11-16 07:11:23
CIOC-1F8596_05a42461-5609-59c0-9ad6-f990...	DCS	10.5.0.18	Fisher-Rosemount Systems Inc.	ImportSet	2021-11-16 07:11:23	2021-11-16 07:11:23	2021-11-16 07:11:23
WIOC-1F903A_a6a44472-310b-5464-ab0e-a596...	DCS	10.5.0.22	Fisher-Rosemount Systems Inc.	ImportSet	2021-11-16 07:11:23	2021-11-16 07:11:23	2021-11-16 07:11:23
169.254.255.255_404ae9c7-9139-50dd-b8ba...	DCS	169.254.255.255	Broadcast	ImportSet	2021-11-16 07:11:26	2021-11-16 07:11:06	2021-11-16 07:11:06
CIOC-1F8596_29ff142-fbb7-5095-8cdd-758f...	DCS	10.4.0.18	Fisher-Rosemount Systems Inc.	ImportSet	2021-11-16 07:11:23	2021-11-16 07:11:23	2021-11-16 07:11:23
Asustek 10.20.102.1	OT Control System	10.20.102.1	ASUSTek COMPUTER INC.	ImportSet	2021-11-16 07:11:21	2021-11-16 07:11:21	2021-11-16 07:11:21
Zat 10.20.100.108	OT Control System	10.20.100.108	ZAT a.s.	ImportSet	2021-11-16 07:11:08	2021-11-16 07:11:08	2021-11-16 07:11:08
Rockwell 192.168.249.40_5c1a73e0-7e60-58...	PLC	192.168.249.40	Rockwell Automation	ImportSet	2021-11-16 07:11:23	2021-11-16 07:11:23	2021-11-16 07:11:23
PLC_1_23932f8f-b37a-53ff-a21d-fddb893268f	PLC	192.168.105.112	Siemens AG	ImportSet	2021-11-16 07:11:22	2021-11-16 07:11:22	2021-11-16 07:11:22
S7-400 station_1_35dee2c8-8e27-5de8-8587...	PLC	192.168.105.115	Siemens AG	ImportSet	2021-11-16 07:11:23	2021-11-16 07:11:23	2021-11-16 07:11:23
SIMATIC 300(1)_38cd1aa2-896c-5786-85b2-2...	PLC	192.168.0.1	Siemens AG	ImportSet	2021-11-16 07:11:07	2021-11-16 07:11:07	2021-11-16 07:11:07
PLC_3_618b4e27-5a50-5554-9bfa-58f800a1ec8	PLC	192.168.105.130	Siemens AG	ImportSet	2021-11-16 07:11:08	2021-11-16 07:11:08	2021-11-16 07:11:08
Siemens 192.168.0.10_8c0372a7-d433-5ac2...	SCADA Server	192.168.0.10	Siemens AG	ImportSet	2021-11-16 07:11:23	2021-11-16 07:11:23	2021-11-16 07:11:23

Integrated with ServiceNow Operational Technology Management suite

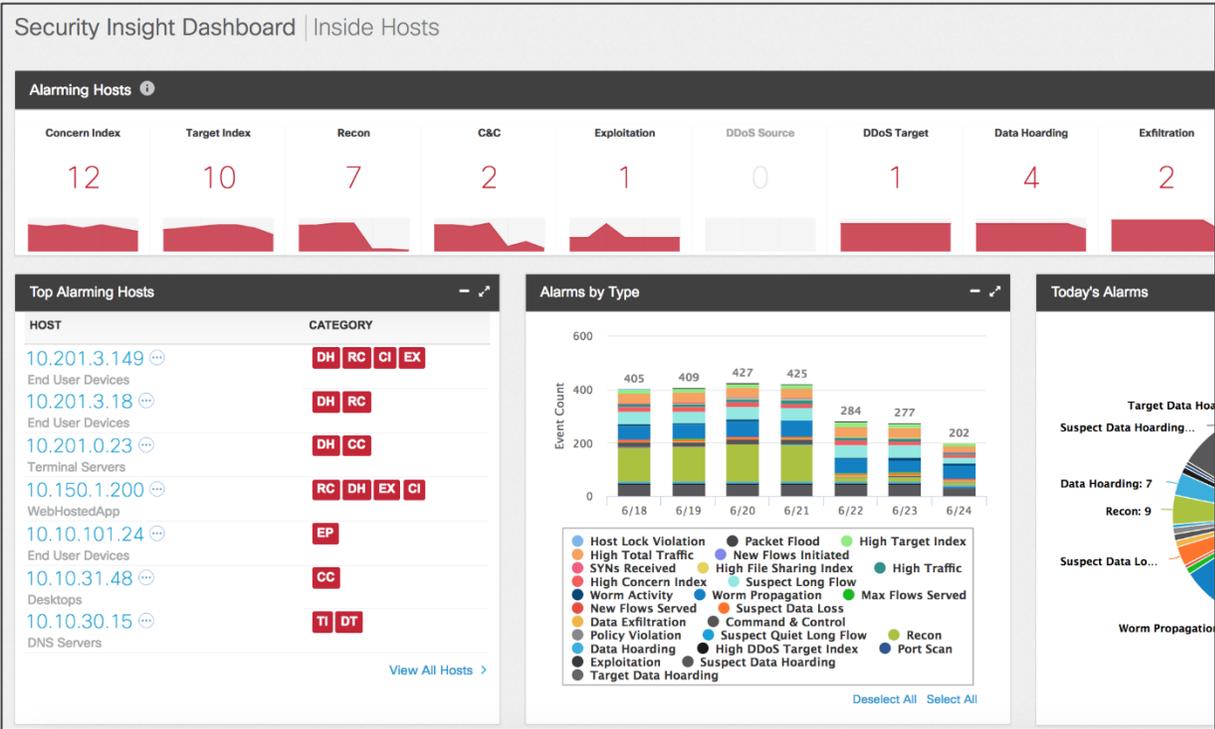
Gain visibility to OT assets along with IT devices in your CMDB

Extend your existing service management workflows to OT assets

Integrate with ServiceNow Operational Technology Management suite



Cisco Secure Analytics + Cyber Vision



Enrich hosts information in Cisco Secure Analytics with rich context from Cyber Vision

Easily identify flows mapped to industrial endpoints with Cyber Vision informed host-group attributes

Create alert policies to identify and alert on inter-zone communications

Cyber Vision helps Secure Analytics investigate and detect threats in industrial networks



Secure Analytics Dynamic Host Groups

Component: 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)

First activity: Apr 24, 2020 11:04:11 AM

Last activity: Apr 24, 2020 11:04:11 AM

Tags: No tags, Activity tags: EthernetIP

Properties:

- vendor-name: Rockwell Automation
- enip-name: 24VDC 16PT INPUT & 16PT OUTPUT
- enip-vendor: Rockwell Automation/Allen-Bradley
- enip-version: 31.11
- enip-productcode: 0x474
- enip-status: Owned, AtLeastOneIOConnectionInRunMode
- enip-devicetype: GeneralPurposeDiscreteIO
- enip-location: Port1-Link01
- enip-serial: 00000000
- enip-vendor: Rockwell Automation
- name: 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)
- ip: 192.168.249.50
- public-ip: no
- mac: f4:54:33:91:cb:ee



Host Group Automation

Host Report | 192.168.119.50

Alarm Categories:

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data
0	0	0	0	0	0	0	

Host Summary:

Host IP: 192.168.119.50

Host Groups:

- Paint Line 2, B.LOGIX5316ER (Port1-Link00), B.LOGIX5316ER
- 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01), Rockwell 192.168.119.50,00000000,60771949|31.11

Traffic by Peer Host Group (last 12 hours):

- Paint Line...
- Rockwell 1...
- 60b98f99
- 5.15
- Rockwell 1...
- B Ethernet...
- Multicast
- Catch All

Cyber Vision identifies attributes of assets via industrial Deep Packet Inspection

Dynamic Host Groups are created, and devices as assigned via Host Group Automation API

Secure Analytics Relationship Policies

Policy Management | Relationship Policy Cancel Save Actions

NAME *
Paint Line 1 to Paint Line 2

DESCRIPTION

HOST GROUP - SIDE 1 * **HOST GROUP - SIDE 2 ***

+ Paint Line 1 × + Paint Line 2 ×

MAP OR DIAGRAM NAME

TRAFFIC BY SERVICES AND APPLICATIONS

+ All Services
All Applications

Relationship Events (1) Select Events

EVENT	POLICY NAME	MAP OR DIAGRAM NAME	HOST GROUPS	TRAFFIC BY SERVICES	TRAFFIC BY APPLICATIONS	STATUS	ACTIONS
Ex. Relationship High Traffic	Filter Policy Name	Filter Map or Diagram Name	Ex. "Inside Hosts"	Ex. "https"	Ex. "Corporate Email"	Ex. "On"	
Relationship New Flows	Paint Line 1 to Paint Line 2		Paint Line 1 ↔ Paint Line 2	All Services	All Applications	<input checked="" type="checkbox"/> On	Delete

50 items per page 1 - 1 of 1 items 1 / 1

Create custom alerts based on attributes from Cyber Vision including Groups – ie. Paint Line 1 should never talk to Paint Line 2



Cyber Vision is a key pillar to securing your OT

**Detects
IT security
events in OT**

**Generates
actionable
alarms on OT
events**

**Reduces the
number of
“false alarms”**

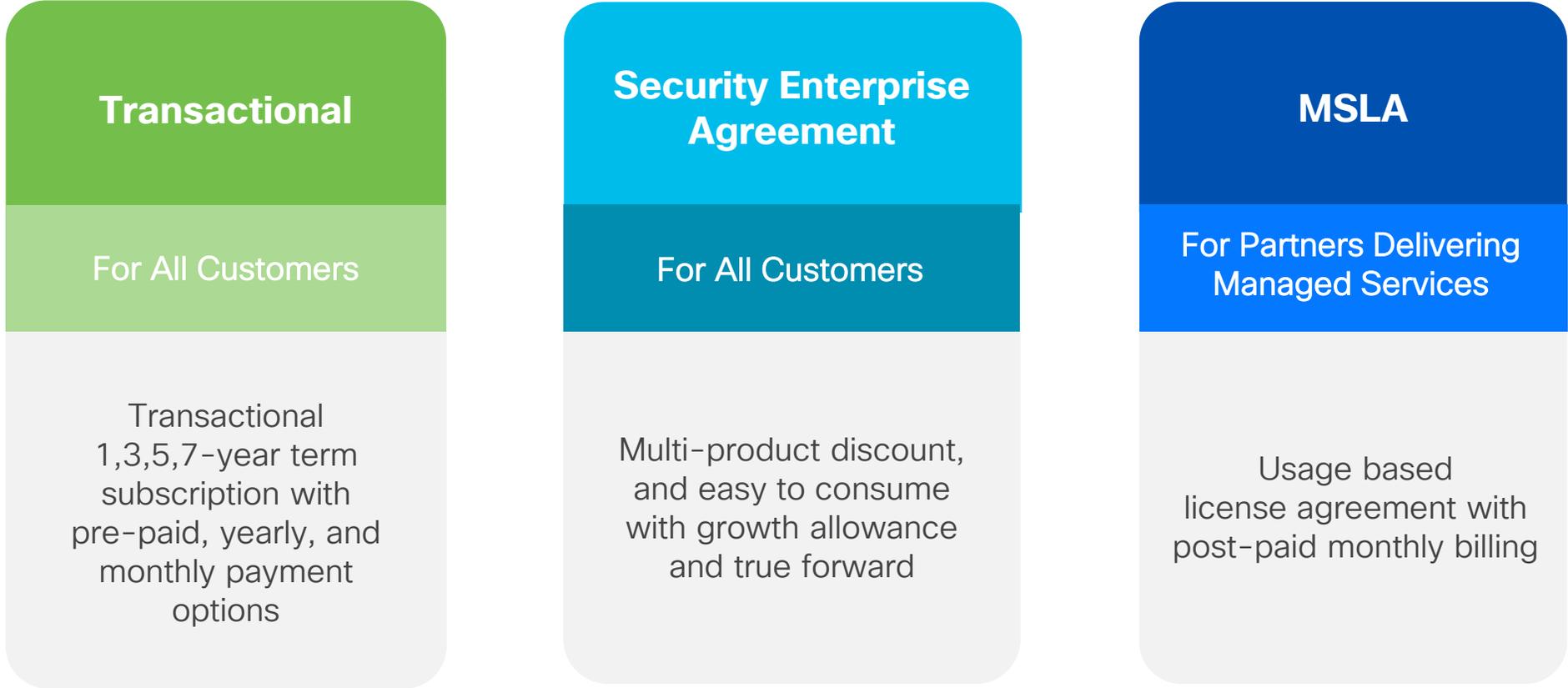
**Scales to very
large industrial
networks**

**Enables
effective IT/OT
collaboration**

Extend your IT security infrastructure to your OT domain

Cyber Vision Licensing

Cyber Vision Buying Options



Software Licensing Overview

Licensing is a recurring subscription model based on:

- Essential or Advantage tiers
- Number of endpoints monitored
- Terms of 1, 3, 5 or 7 years on a pre-paid term basis
- Optional Talos subscription signatures (quantity must match the number of sensors where IDS is enabled)
- No cost for either the Center or Sensor software

About Cyber Vision Endpoints

A licensed “endpoint” is defined by two characteristics:

1) Any device which contains at least one component with one of the following tags

- “Device - Level 0-1” OR
- “Device - Level 2” OR
- “Device - Level 3-4” OR
- “Software” OR
- “System”

2) Seen by Cyber Vision within the last 60 days

You can apply filters to exclude specific devices from Cyber Vision and save on the license count

In case device count exceeds license, Cyber Vision will still list new devices, up to a 20% threshold

Pricing per monitored endpoints allows for free and unlimited number of Sensors and Centers

Cyber Vision License Tiers

Cyber Vision Essentials

INVENTORY

- Device inventory
- Identify communication patterns
- Generate inventory reports

VULNERABILITY

- Identify device vulnerabilities
- Generate vulnerability reports

ACTIVITIES

- Track control system events
- Generate device activity reports

RESTful API

- REST API programming interface

Cyber Vision Advantage

Includes Essentials features, plus:

SECURITY POSTURE

- Device Risk Scoring
- Security posture, remote access reports

INTRUSION DETECTION

- Snort IDS on supported sensors
- Talos community signatures (New rules may be added 30 days after release)

BEHAVIOR MONITORING

- Create baselines for asset behaviors
- Alerts on deviations

SECURE REMOTE ACCESS

- Zero Trust Network Access (ZTNA), powered by Cisco Secure Equipment Access

ADVANCED INTEGRATION

- Cisco XDR integration
- pxGrid integration with ISE
- SIEM integration – Splunk, QRadar
- ServiceNow OT Management integration

Talos subscriber rules for Cyber Vision IDS

Requires Cyber Vision Advantage. Licensed per IDS enabled sensor.

ENHANCES ADVANTAGE IDS WITH:

- Talos subscription signatures, specifically curated for industrial networks
- Immediate rules availability
- 15x more rules compared to community signatures

Cyber Vision Ordering Guide: <https://salesresources.cisco.com/Link/Content/DCJpXgQqcFdd98hGgBq6p84MTHdj>



Cyber Vision is an “Add-On Suite” in Security EA 3.0

Full Commit Suites

Solution	Protection	Zero Trust	Cloud & Network Security	Security Platform & Response
Suites	 User Protection	 Duo	 Umbrella	 Secure Endpoint <i>(AMP for Endpoints)</i>
	 Cloud Protection	 Identity Services Engine (ISE)	 Secure Access	 Secure Network & Cloud Analytics <i>(Stealthwatch)</i>
	 Breach Protection	 Secure Workload <i>(Tetration)</i>	 Secure Web Appliance (WSA)	 Extended Detection & Response (XDR)
	 User & Breach Protection (Combination)		 Secure Firewall (NGFW)	 Secure Email <i>(Email Security)</i>
				 Vulnerability Management <i>(Kenna)</i>

Add-On Suites (Partial Commit only)

- Secure Client Premier (AnyConnect Apex)
- Threatgrid (Advanced, Cloud, Content, Feeds)
- Web Application Firewall (WAF)
- IoT Secure Equipment Access (SEA)
- Cloud Delivered Firewall Management (NGFW & NGIPS, Umbrella, FTDv, ASAv, ML)
- Cyber Vision**
- Secure Email Threat Defense
- Cloudlock
- Secure Cloud DDoS Protection
- SAL (Logging & Analytics)
- AMP Private Cloud (AMP virtual private cloud)
- Cisco Talos Incident Response

Requirements

- Meet requirements for Security EA 3.0
- 25 Cyber Vision licenses minimum

Customer Benefits for Cyber Vision Enrollment

- Inherit 5-20% discount from Qualifying suite
- Annual True Forward
- Annual payments
- Co-termination
- Fixed Price (for true forward consumption)
- Flexibility to expand when ready

MSLA: Licensing for managed services providers

Configure Utility Mode

The Utility mode is available to customers that choosed the Smart software Manager Satellite transport mode with a Managed Service License Agreement (MSLA) program.

In Utility mode, the Smart Agent keeps track of the usage of licensing entitlements in units of time. The Smart Agent sends license usage reports to a licensing satellite or server every four hours. The usage reports are forwarded to a billing server and the customer is sent a monthly bill for their license usage.

Utility mode: Enabled

Customer informations

Customer ID: * Id	Customer name: * name
Customer street: * street	Customer city: * city
Customer state: * state	Customer country: * country
Customer postal code: * 12345	

[Activate Post-paid Usage Subscription](#)

Reserved	In Use	Status
100	30	Authorized

- Simplify licensing for managed services
- Uses a postpaid licensing model for Essentials, Advantage and IDS licenses
- Available from 3.2.2
- Additional information can be found [here](#)

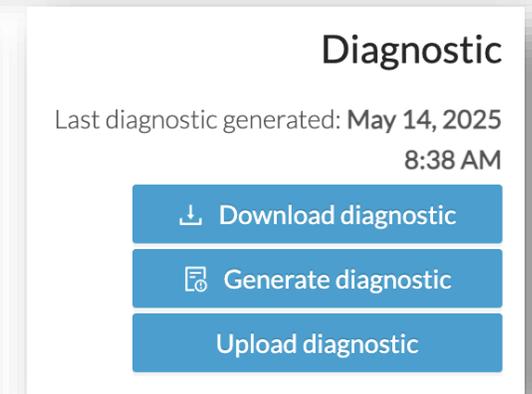
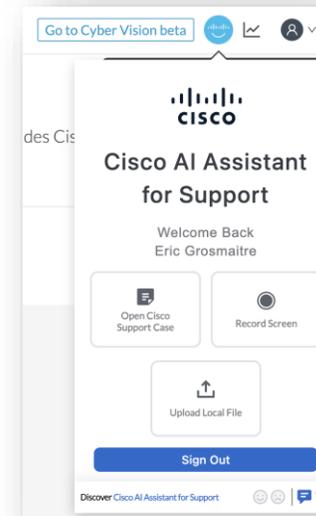
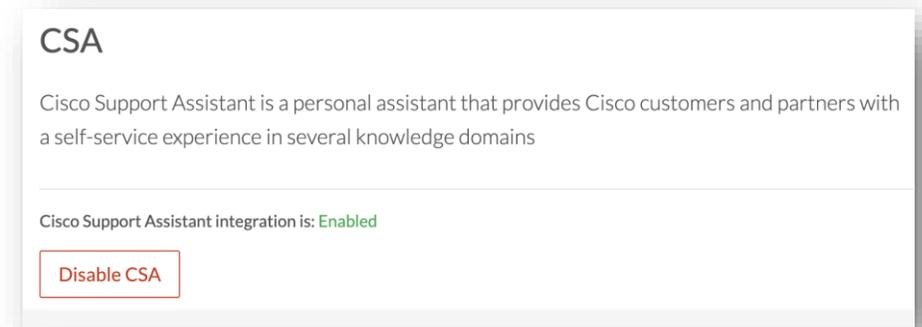
Administration Features

Cisco Support Assistant in Cyber Vision

Cisco Support Assistant becomes available in CV Center with v5.3.0. This feature allows to easily open a support case, upload related files and record screens.

Note:

- The feature needs to be enabled (Admin->Integrations->CSA)
- To use the feature, you need to provide a login to “Cisco AI Assistant” service
- Automatically upload a diagnostic bundle file from the “System Statistics center page” of CV to the technical support case



Supported Syslog Formats

With version v5.3, the list of supported syslog formats is restricted to CEF:

* Format: RFC3164/CEF

- Standard - *Deprecated*
- Standard/CEF
- RFC3164 - *Deprecated*
- RFC3164/CEF

Syslog configuration

* Protocol: * Host:

* Port:

Save configuration Cancel

* Format:

- CEF
- CEF Extended Time Precision

Cyber Vision Center Queue – Status Monitoring

Internal queues are being monitored, and their status is reported, including global center synchronization queues. The queue count is an important metric to monitor and to determine the workload and potential backpressure on your CV center setup.

System Health

Service Status

This section displays the status of specific Cyber Vision Services and Extensions. Periodic checks are performed to assess the status of each service and extension. If any part extension is down, this information will be reported here.

🕒 Last updated: Jun 13, 2025, 6:00 PM

Name	Type
sbs-marmotd.service	Service

Queue Status

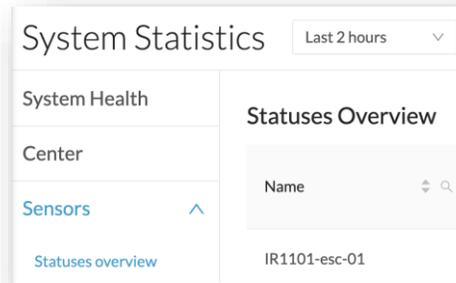
This section displays the status of the queues. Periodic checks are performed to monitor the messages dropped from the queues. If any queue is dropping message then that reported here.

Name	Count	Last Drop Time
ccv.queue.events	64	Jun 13, 2025, 6:13 PM
ccv.queue.burrow_results	4259	Jun 13, 2025, 6:16 PM



Sensor data collection report

- Starting with v5.4 the center provides an overview of the current sensor data collection at “System Statistics / Sensor / Statuses Overview”



- Examples:
 - Zero-valued rows suggest technical/configurative issues. For instance, dysfunctional monitoring session
 - Missing or wrong dates suggest incorrect time-sync status.

Name	Product ID	Components	Activities	Unicast Activities	Current Time
ir1101-esc-03	IR1101-K9	0	0	0	Nov 3, 2025
ir1101-esc-02	IR1101-K9	58	24	0	Nov 3, 2025
IR1101-esc-01	IR1101-K9	59	51	2	Nov 3, 2025

Line1	IE-3400-8T2S	82	126	27	Nov 3, 2025
MainSwitch	C9300-24T	96	132	36	Nov 3, 2025
Line2	IE-3400-8T2S	75	110	28	Nov 3, 2025
Common	IE-3400-8T2S	87	133	32	Nov 3, 2025

Cyber Vision Knowledge Database

Includes:

- List of vulnerabilities manually curated for industrial devices
- Snort rules to detect malware and intrusions
- List of tags and associated rules (component tags, flow/activity tags)
- Icons (vendor icons, specific device front panel icons)

The Cyber Vision KDB is updated every week
Updates included with the Cyber Vision subscription

Role Based Access Control

- Assign users to 1 of 4 default system roles
 - **Admin** – Full Access – has access to the Admin page and can set users roles
 - **Product** – has access to the sensor panel and the events panel in the Admin page
 - **Operator** – has access to the Monitor mode and can edit groups and acknowledge vulnerabilities
 - **Auditor** – has access to the Map and Events pages
- Restrict access to appropriate information and functions

CREATE A NEW USER ×

Firstname ^{*}: Lastname ^{*}:

Email ^{*}:

Password ^{*}: Confirm password ^{*}:

Suggested password:
f;yEahV3s)PR7y3V  

Role ^{*}:
 ^

- Admin
- Product
- Operator
- Auditor**

Custom User Roles

- Create roles to customize read/write access to different parts of Cyber Vision
- Minimum default access is read-only for the Explore page
- Easy role creation by duplicating and modifying existing roles

From this page, you can create Cisco Cyber Vision user roles, edit and delete them.

[ADMIN](#) [AUDITOR](#) [OPERATOR](#) [PRODUCT](#) [NEW ROLE](#) [+](#)

Role Name

Role Description

Search/Add existing permission: [+](#) Add New Permissions [?](#)

Administrative Rights ?	read	write		read	write
Active Discovery	<input type="checkbox"/>	<input type="checkbox"/>	API	<input type="checkbox"/>	<input type="checkbox"/>
Center Certificate	<input type="checkbox"/>	<input type="checkbox"/>	Data Management	<input type="checkbox"/>	<input type="checkbox"/>
Events	<input type="checkbox"/>	<input type="checkbox"/>	Events Settings	<input type="checkbox"/>	<input type="checkbox"/>
Explore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Extensions	<input type="checkbox"/>	<input type="checkbox"/>
External Authentication	<input type="checkbox"/>	<input type="checkbox"/>	Integrations	<input type="checkbox"/>	<input type="checkbox"/>
License	<input type="checkbox"/>	<input type="checkbox"/>	Monitor	<input type="checkbox"/>	<input type="checkbox"/>
Network Organization	<input type="checkbox"/>	<input type="checkbox"/>	Reports	<input type="checkbox"/>	<input type="checkbox"/>
Risk Score	<input type="checkbox"/>	<input type="checkbox"/>	Secure X	<input type="checkbox"/>	<input type="checkbox"/>
Security Settings	<input type="checkbox"/>	<input type="checkbox"/>	Sensors	<input type="checkbox"/>	<input type="checkbox"/>
SNMP	<input type="checkbox"/>	<input type="checkbox"/>	Snort	<input type="checkbox"/>	<input type="checkbox"/>
System	<input type="checkbox"/>	<input type="checkbox"/>	User Admin	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability Management	<input type="checkbox"/>	<input type="checkbox"/>			

SAML 2.0 Support for Authentication

SAML 2.0 added with v5.3 as an option for centralized authentication

External Authentication

LDAP **Single Sign-On**

From this page, you can manage Cisco Cyber Vision SSO settings.

[+ New Settings](#)

EDIT SSO SETTINGS

Configurations **Role Mapping**

Default roles ⓘ

Product 5568bb76-5d75-41ab-ba1d-1d7bddffe6e!

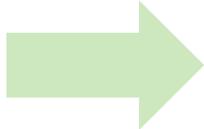
Operator

Auditor

Custom roles ⓘ

ADMIN-SSO f9c22980-d84f-4b30-bb50-0c0d!

[OK](#) [Cancel](#)



CISCO

Cisco Cyber Vision

Cybersecurity for IoT

[Login with SSO](#)

or

[Login with Credentials](#)

English (US)

EDIT SSO SETTINGS

Configurations **Role Mapping**

* Role Attribute ⓘ Email Attribute ⓘ

groups

Upload XML File ⓘ

* Upload

[Upload Idp Metadata](#)

sts.windows.net.xml

Manual Configuration

[Go to Cyber Vision beta](#)

Signed in as **testericCCV@ciscoitindp.onmicrosoft.com**

[My Settings](#)

[Logout](#)



LDAP integration for User Authentication

- Secure connection to LDAP servers using TLS certificates
- Supported AD: Windows Server 2012, 2016, 2019, 2022
- Redundant LDAP servers are supported
- Custom and default roles can be mapped to AD groups
- Default Admin Role is local only but custom roles with admin access can be created and mapped to LDAP groups
- The LDAP search filter is editable so CV can interact with Microsoft LDS or any other LDAP with a custom schema
- \$user is mandatory as it's the variable taken from the login form

EDIT LDAP SETTINGS

Settings Role Mapping

LDAP over TLS/SSL Use self signed certificate

* Primary Server Address * Primary Server Port

Secondary Server Address Secondary Server Port

* Base DN ⓘ

* Search Filter ⓘ
Example: (&(sAMAccountName=\$user)(objectClass=user)) or (&(uid=\$user)(objectClass=user))

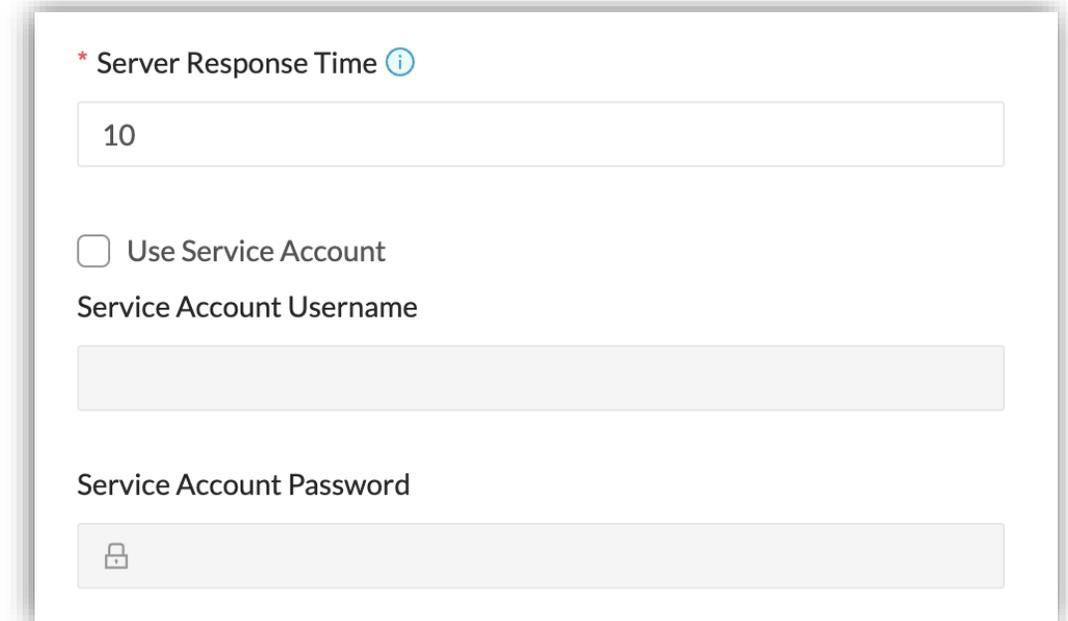
* Server Response Time ⓘ

LDS Support (Lightweight Directory Services) [1/2]

- Base DN: flexible definition of search scope
 - For example: DC=local,DC=lab-autom,OU=lab-users
 - Valid for Microsoft Active Directory and LDS
- Search Filter:
 - In Microsoft AD each object (user, group) has an attribute “SAMAccountName”.
 - For Microsoft AD a common search filter is:
(&(sAMAccountName=\$user)(objectClass=user))
 - In LDS: the object structure is customizable
 - The search filter can be defined depending on the use case, for example:
“(&(uid=\$user)(objectClass=user))”

LDS Support (Lightweight Directory Services) [2/2]

- Server response time
 - Configurable timeout
- User Service Account
 - Can be necessary to browse AD or LDS objects
 - Service account which has read permission on directory objects.



* Server Response Time ⓘ

10

Use Service Account

Service Account Username

Service Account Password

🔒

The screenshot shows a configuration panel for LDS Support. It features a text input field for 'Server Response Time' containing the value '10'. Below this is a checkbox labeled 'Use Service Account', which is currently unchecked. Underneath the checkbox are two more text input fields: 'Service Account Username' and 'Service Account Password'. The password field has a lock icon on the left side, indicating it is a secure field.

User security settings

- Define password lifetimes and reuse

🕒 Passwords lifetime

ADMINISTRATORS

Lifetime password in days :

Warning days before password expiration :

Grace days before password expiration :

USERS

Lifetime password in days :

Warning days before password expiration :

Grace days before password expiration :

🔒 Passwords blocking

Number of authorized failed login attempts :

Time, in minutes, before authorizing new attempts :

🔄 Passwords reuse limitation

Time interval before a password can be reused (between 0 and 365 days) :

Cyber Vision Center SNMP monitoring

- SNMP used for remote monitoring of Cyber Vision Centers
 - SNMP v2c
 - SNMP v3
- Cyber Vision metrics exposed:
 - CPU
 - Load
 - RAM
 - Swap
 - Traffic for all physical interfaces
 - Data storage
 - Packets statistics

SNMP Global Configuration

SNMP protocol allows remote monitoring of network and equipment.

This page allows you to configure the configuration used by the SNMP agents on this center and on connected sensors.

Note that changing the configuration on this page does not automatically replace the configuration used on sensors.

SNMP agent

Configuration

Monitoring hosts (IPv4):

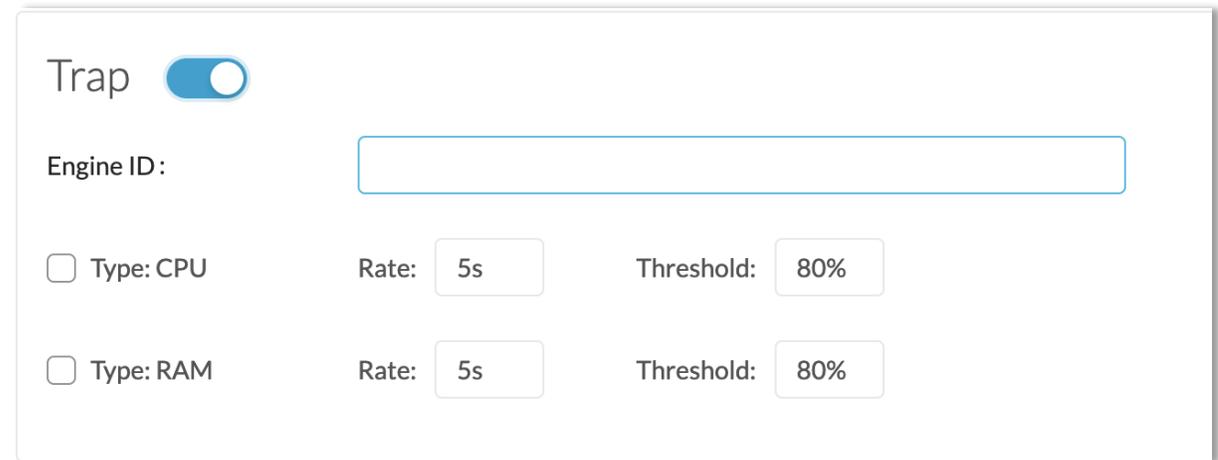
Version: 3 2c

Security type:

Username:

SNMP traps

- Traps let Cyber Vision send unrequested messages to the SNMP manager
- Traps can be activated for
 - RAM
 - CPU
- Rate and Threshold can be customized



The screenshot shows a configuration panel for SNMP traps. At the top, the word "Trap" is followed by a blue toggle switch that is turned on. Below this, there is a label "Engine ID:" followed by an empty text input field. Underneath, there are two rows of configuration options. The first row has a radio button labeled "Type: CPU", a "Rate:" field with a dropdown menu showing "5s", and a "Threshold:" field with a dropdown menu showing "80%". The second row has a radio button labeled "Type: RAM", a "Rate:" field with a dropdown menu showing "5s", and a "Threshold:" field with a dropdown menu showing "80%".

Extension modules

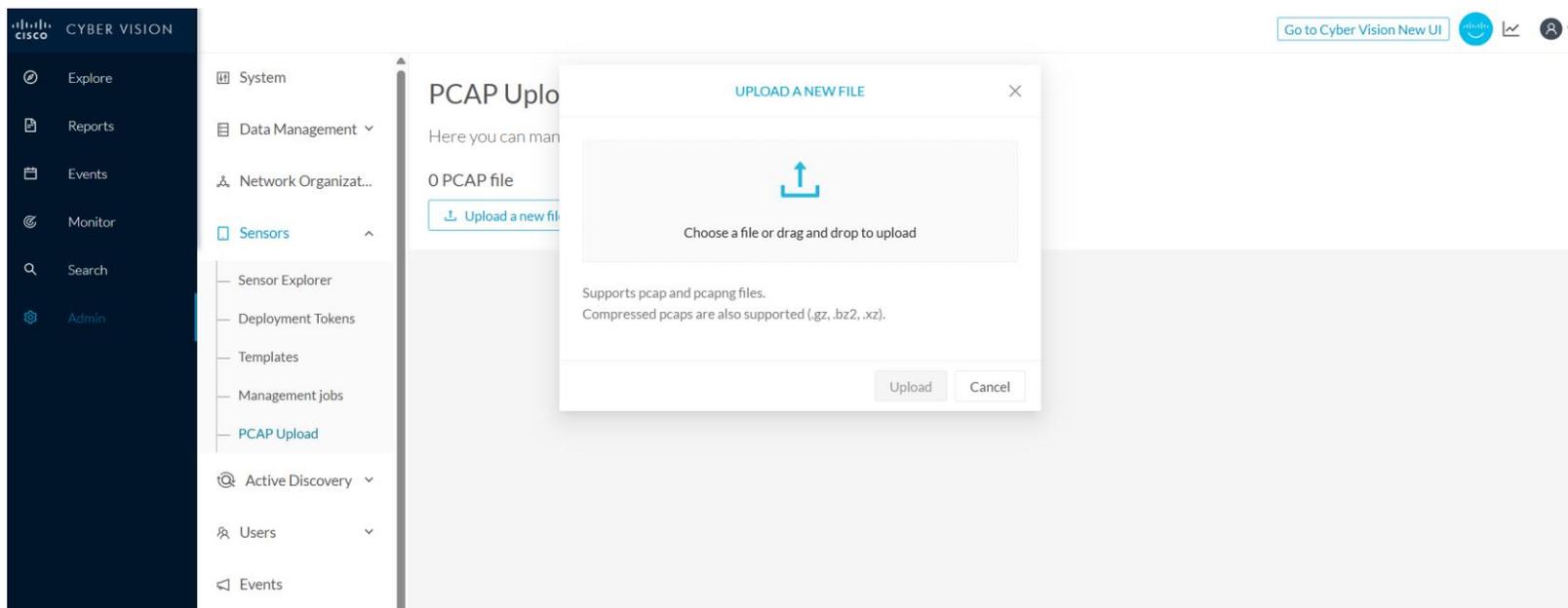
The screenshot displays the 'Extensions' management interface in Cisco Cyber Vision. The left sidebar contains navigation items: Explore, Reports, Events, Monitor, Search, Admin, System, Data Management, Network Organization, Sensors, Active Discovery, Users, Events, API, License, External Authentication, Snort, Risk score, Integrations, Extensions (highlighted), Web Server Certificate, and SNMP. The main content area is titled 'Extensions' and includes a description: 'From this page, you can manage Cyber Vision Extensions. Extensions are optional add-ons to Cyber Vision Center which provide more features, such as the management of new device types, additional detection engines, or integrations with external services.' Below the description is a link to 'Import a new extension file'. A table lists the installed extensions:

Name	Version	Actions
Cyber Vision Reports Management	5.4.0	Update Remove
Cyber Vision sensor management	5.4.0	Update Remove

Extensions add additional features independent of software release cycle

- Cyber Vision Sensor Management enables simplified IOx based sensor deployments
- Cyber Vision Reports Management provides ability to create customizable reports including the Security Posture Report

PCAP ingestion through Center UI



- Enables to use/demonstrate Cyber Vision with customer provided packet captures (PCAP)
- PCAP Upload at Admin->Sensors
- Ability to automatically create matching preset and rewrite packet timestamps to time of import

PCAP recording on Center interface

Starting with v5.4 PCAP recordings of the Center interfaces are now possible from the CV Center GUI.

- The system statistics UI for the center support recording a PCAP for a specific network interface on the center.
- The user interface will provide the current operational status of the recording.
- Once completed, it provides the link to download the PCAP.

The screenshot displays the 'System Statistics' page in the CV Center GUI. The page is divided into several sections:

- System Health:** Shows the system ID as VMWare-42 0f 35 95 53 f9 61 a6-49 64 d7 f7 3b 00 00 bb. Other details include Version: 5.4.0 (build 202510282303), Uptime: 3d 23h 43m 4s, System date (UTC): Nov 3, 2025 5:19 PM, Ingestion status: active, and SNMP: disabled.
- PCAP Capture (Initial State):** Shows the interface set to 'eth0' and the filter set to 'host smartreceiver.cisco.com'. A 'Start Capture' button is visible. Below this, it indicates the last capture was on Oct 30, 2025 3:40:18 PM and provides a 'Download (36.1 KB)' link.
- PCAP Capture (Running State):** Shows the interface as 'eth0' and the filter as 'e.g: tcp, udp, port 443, host 10.0.0.1'. A 'Stop Capture' button is visible. Below this, it indicates the capture has been running since Nov 3, 2025 6:16:17 PM and has a size of 962.4 KB.
- PCAP Capture (Completed State):** Shows the interface as 'eth0' and the filter as 'e.g: tcp, udp, port 443, host 10.0.0.1'. A 'Start Capture' button is visible. Below this, it indicates the last capture was on Nov 3, 2025 6:22:48 PM and provides a 'Download (1.1 MB)' link.

Network Organization Configuration

- Define IT/OT/External networks
- Specify if public IP addresses are used in your private network
- Make risk scoring more accurate
- Have an accurate view of which devices are internal/external
 - Can leverage subnets to define these networks
 - If it's not defined as internal, is considered external
 - Most specific subnet is what system matches

EDIT A NETWORK ×

IP address / subnet VLAN ID (optional)

10.176.25.0/24 1625

Network name

OT1

Network Type

OT Internal ▼

Use a device engine option for this network range

- This IP range is deployed several time. The device engine will not use the IP property of network components in it to create devices. ⓘ
- Do not group component seen by different sensors. For this IP range, the device engine will only use components from one sensor to create devices. ⓘ

Cancel Save

− 192.168.0.0/16	192.168/16 private network	OT Internal		
192.168.10.0/24	Line1	OT Internal		

External Component Handling

- Communication from/to a device which is not defined by an internal network will result in reduced data stored
 - Internal Device (IP, MAC), Source Port (TCP/UDP), External Device (IP), Destination Port (TCP/UDP), DNS/HTTP, Protocol/Service, Hostname, volume of traffic

Define Data Expiration Settings

- Configure report storage settings in Cyber Vision Center

Expiration Settings

From this page you can set the expiration time of data. Expired data is removed on daily-basis.

You will be notified through an event when data is deleted from the database.

Reports

The reports should be removed from the system if their creation date is older than 6 months

Change reports expiration:

The oldest report should be hidden from the system when there are more than 10 versions of the same report

Change maximum versions limit:

 Save

Clear Data

- Flexibly clear data from Cyber Vision Center
- Select specific components based on Type, Subnet, VLAN and recent activity

Clear Data

From this page, you can manage data stored in Cisco Cyber Vision. You can clear your database to optimize the Center performances.

Select a type of data

All data
Remove all data from the database (components, activities, groups, flows, variables, events, baselines). The configuration is not dropped.

Components selection
Remove selected components and associated data. If several criteria are selected, only components matching ALL criteria will be removed.

Component Type: IT OT

IP Subnet:

VLAN:

Inactive since:

Creation time: →

Activities, Flows and Variables
Remove all activities, flows and variables from the database, they will not be available anymore. Important: note that monitoring will be impacted.

Flows and Variables
Remove all flows and variables from the database, they will not be available anymore. Important: note that monitoring will be impacted.

Variables
Remove all variables from the database, they will not be available anymore. Important: note that variables monitoring will be impacted.

Purge Components originating from a VLAN

With version v5.3, the center supports removing components originating from a specific VLAN:

Clear Data

From this page, you can manage data stored in Cisco Cyber Vision. You can clear your database to optimize the Center performances.

Select a type of data

All data

Remove all data from the database (components, activities, groups, flows, variables, events, baselines). The configuration is not dropped.

Components selection

Remove selected components and associated data. If several criteria are selected, only components matching ALL criteria will be removed.

Component Type: IT OT

IP Subnet:

VLAN:

Inactive since:

Creation time: →

Configurable Flow Storage

- Flow storage not enabled by default
 - Provides ability to optimize what information is stored
- Enables ability to aggregate Flow details for optimal performance

Ingestion Configuration

From this page you can customize traffic ingestion.

Flows Configuration

Flows Storage

If disabled, flows won't be stored in the database, you can enable storage and adjust settings in your network configuration.

Please note flow storage can consume system resources and impact the Center performance.

Select All OT

Deselect All IT

Network Name	IP Address / subnet	VLAN ID	Network Type
<input type="checkbox"/> 10/8 private network	10.0.0.0/8		OT Internal
<input type="checkbox"/> IPv4 link local	169.254.0.0/16		OT Internal
<input type="checkbox"/> 172.16/12 private network	172.16.0.0/12		OT Internal
<input type="checkbox"/> 192.168/16 private network	192.168.0.0/16		OT Internal
<input type="checkbox"/> FC00::/7 IPv6 local unicast	fc00::/7		OT Internal
<input type="checkbox"/> IPv6 link local	fe80::/10		OT Internal
<input type="checkbox"/> Others			External

L2 Flow Storage

L2 flows are defined by communication between endpoints without IP addresses.

Flows Aggregation

Cisco Cyber Vision stores every individual network flow that has been seen by the sensors with full details (including the client/server ports for each flow).

For some TCP/UDP based protocols, the client port is dynamically generated by the client and thus Cisco Cyber Vision will store multiple similar copies of the flow for each spotted client port. When enabling flow aggregation, Cisco Cyber Vision will instead discard the client port, thus limiting the number of flows in the database.

Only the following protocols are concerned by flow aggregation: DNS, NTP, SSH, SNMP, Syslog, RabbitMQ, HTTP(S), IEC104, EtherNet/IP.

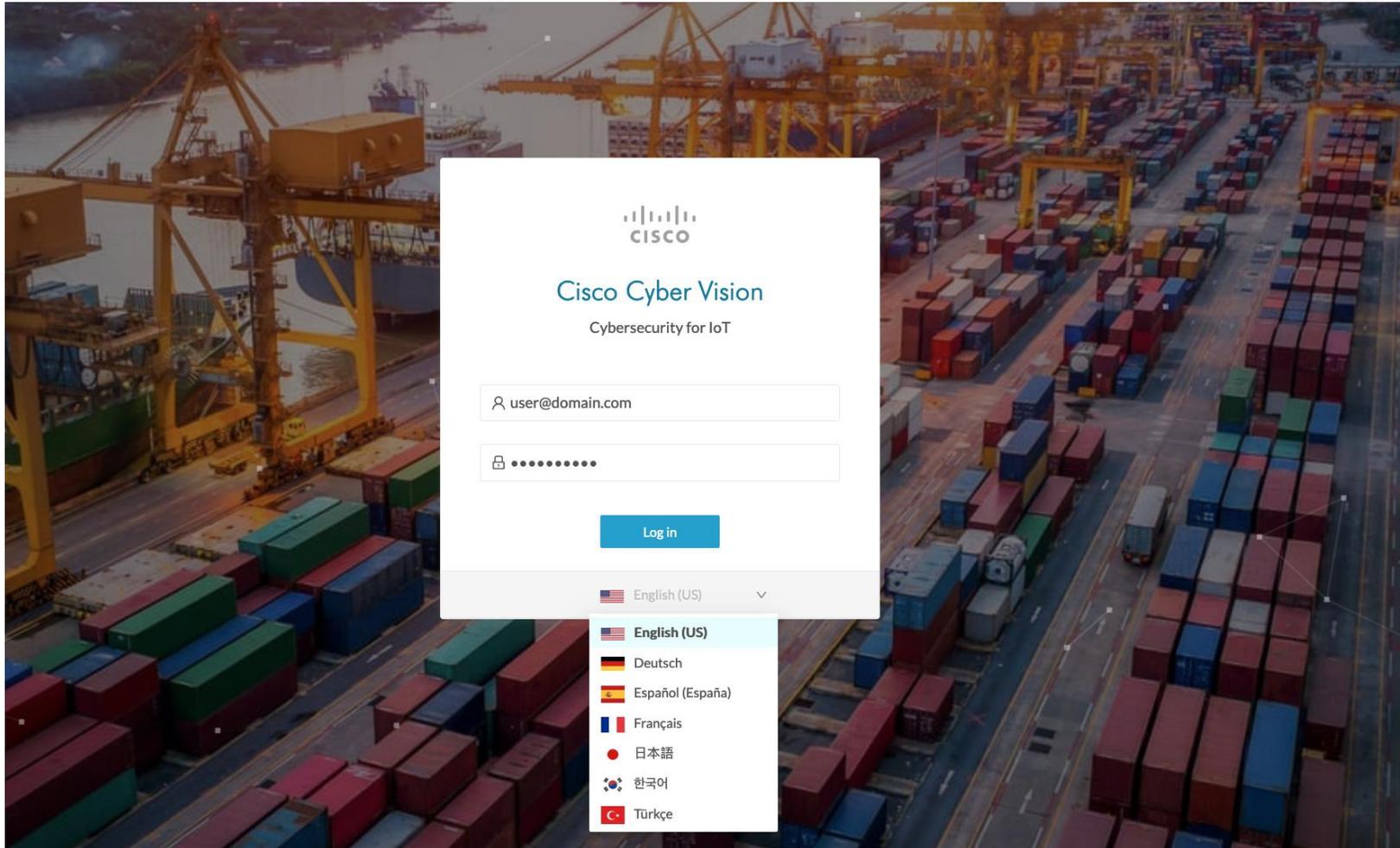
Flows for other protocols are always stored with full details.

Port scan detection

Variables Storage

If disabled, variables won't be stored in the database.

Multiple UI languages



User interface available in:

- English
- German
- Spanish
- French
- Japanese
- Korean
- Turkish

Putting it all together

Protect your industrial operations with Cisco

Best of Cybersecurity

Comprehensive capabilities



Best of OT Networking

Deep understanding of industrial requirements



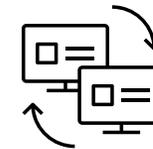
OT Visibility



Zero Trust
Network Access



Network
Segmentation



Cisco + Splunk
SOC of the future



Threat Intelligence &
Incident Response

From OT visibility to Cross-Domain Detection, Investigation, and Remediation



Learn more on Cisco Industrial Security



Get all the solution details
cisco.com/go/IoTSecurity



Sales tools on SalesConnect
cs.co/IoTSecurity



Leverage our Industrial Security CVDs
www.cisco.com/go/iotcvd



Learn about our promotions and offers
www.cisco.com/go/iotoffers

