Cisco Cyber Vision

TDM Overview for Cyber Vision 5.4

January 2026

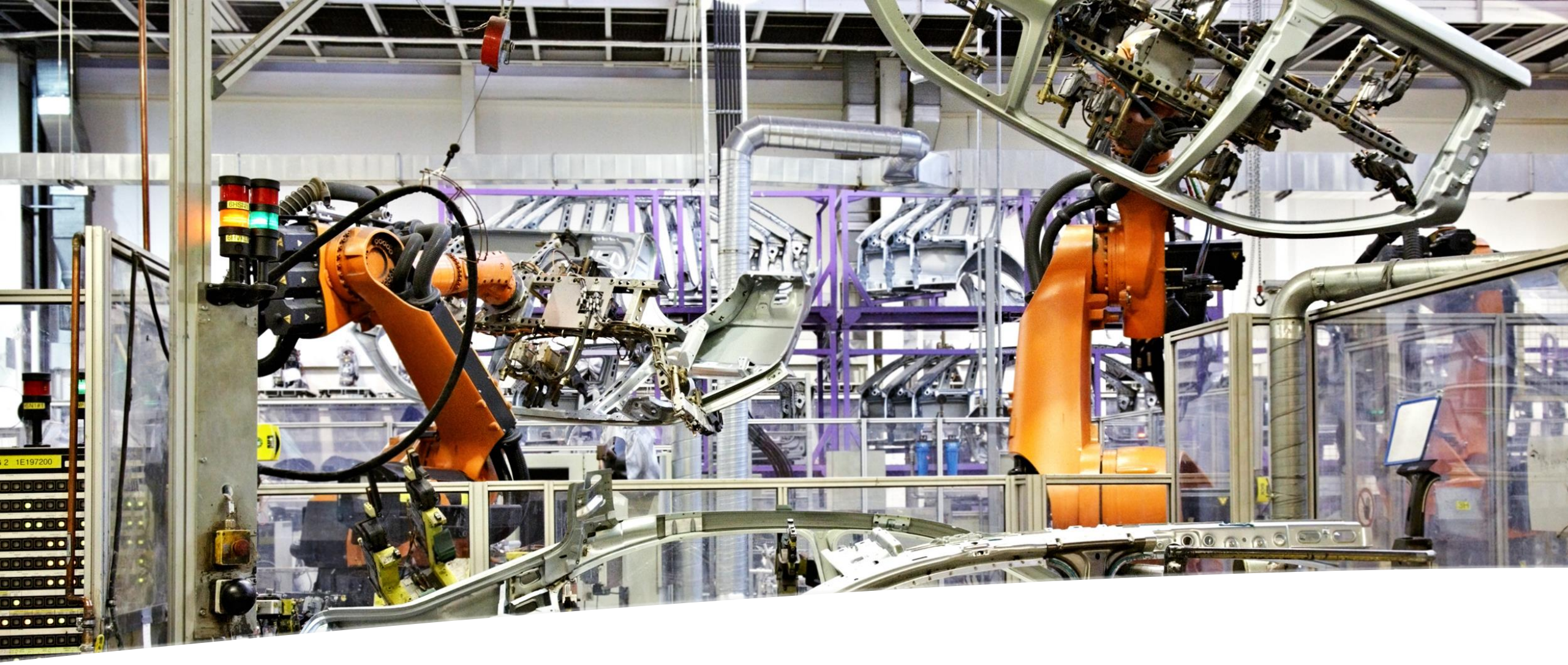
Topics covered

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

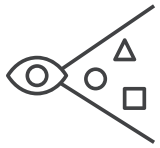
The role of IT is expanding to help secure industrial operations



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

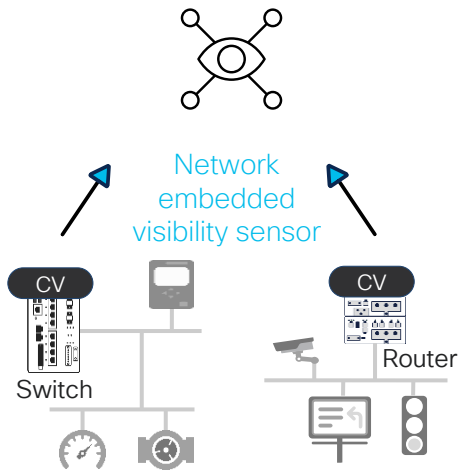
Visibility helps drive IT/OT collaboration to secure industrial operations

Cisco Industrial Threat Defense

Visibility

OT Asset Visibility and Security Posture

Cisco Cyber Vision

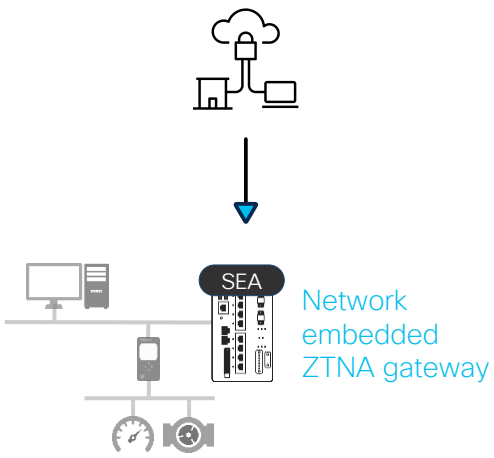


Protection

Zero Trust Security for OT

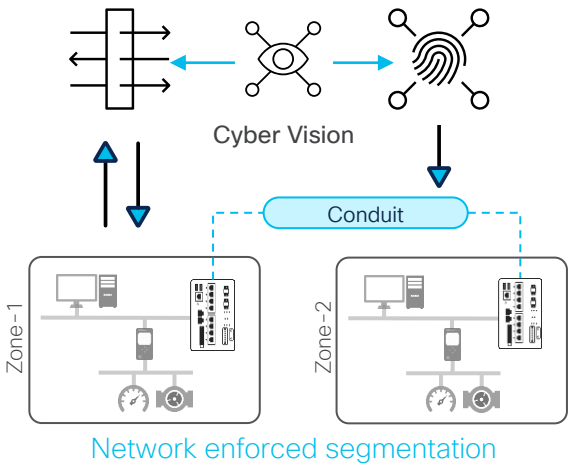
Secure remote access (ZTNA)

Cisco Secure Equipment Access



IEC 62443 zone segmentation

Cisco Secure Firewall **Cisco ISE**

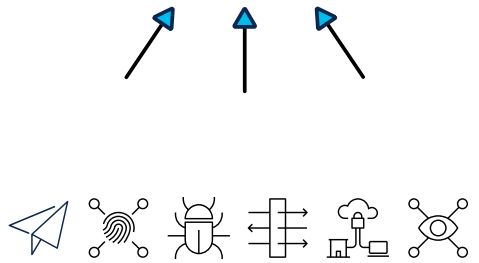


Network enforced segmentation

Response

Cross-Domain Detection, Investigation & Response

splunk> a cisco company



Visibility across the entire attack chain

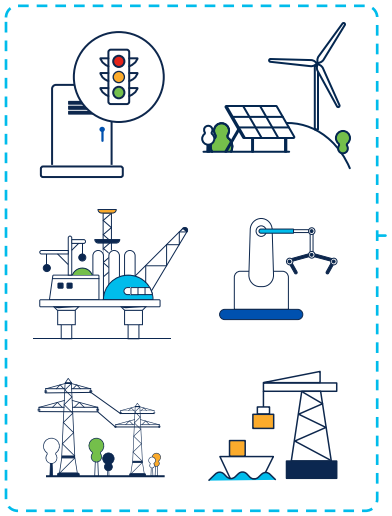
Network as a fabric to secure OT at scale

Cyber Vision Architecture

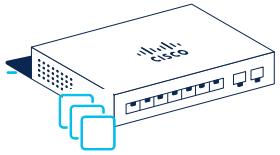
Cisco Cyber Vision: Unique 2-Tier Architecture

OT visibility that can be deployed at scale

OT Assets



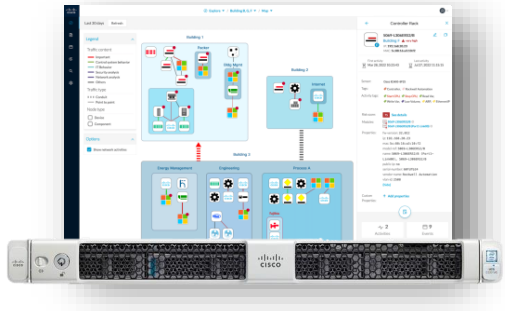
Cisco industrial switches or routers



Lightweight Metadata

Cyber Vision Sensor

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



Cyber Vision Center

- ✓ Centralize analytics and data storage
- ✓ Detailed OT asset inventory and communications maps
- ✓ Security posture and detection
- ✓ Reporting

Integrations

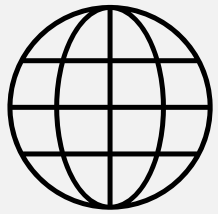
SIEM, XDR, NAC, Firewall, CMDB, etc.

- ✓ OT asset profiles in IT security tools
- ✓ OT context and events in SOC
- ✓ Native integrations and specific apps
- ✓ Comprehensive APIs for custom integrations

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

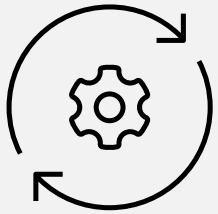
The role of the Cyber Vision Sensor

Collects Industrial Network Traffic



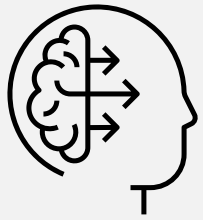
Captures industrial network flows (passive) and queries devices (active). Stores data locally in case the Center is not accessible

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

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

Amazon Web Services

Microsoft Azure

Google Cloud

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

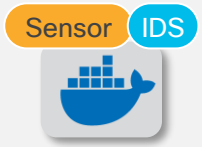
Catalyst IR8300 Multiservice Router

Catalyst IE9300 Rugged Switches

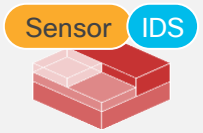
Catalyst 9300/9400 Aggregation Switches

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

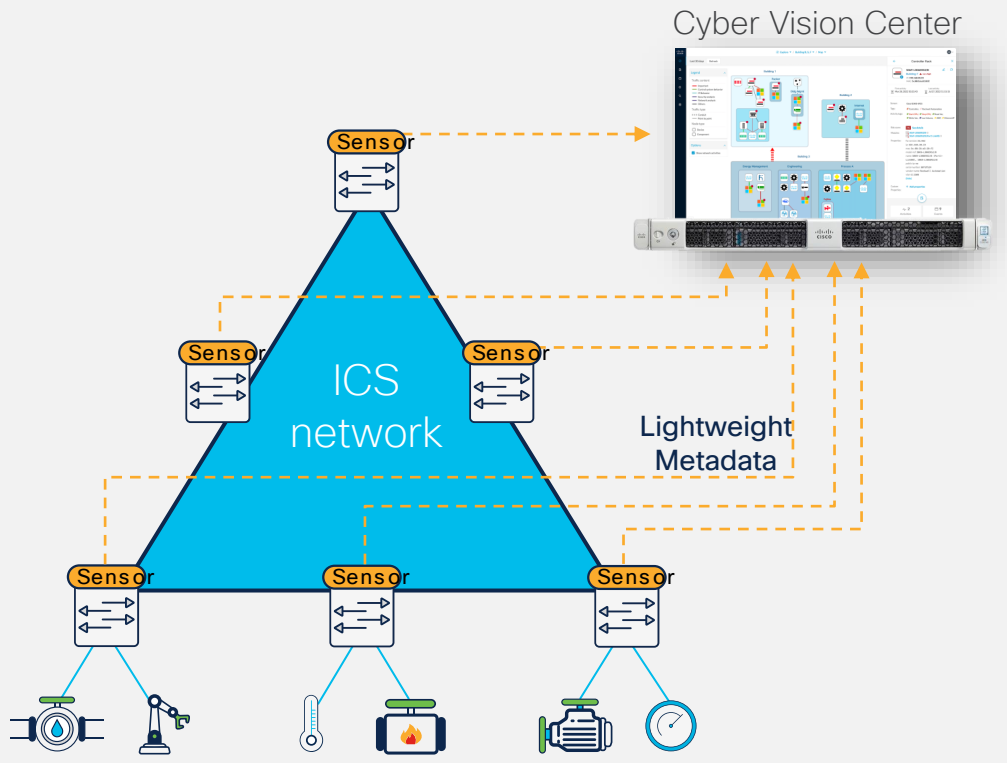
Cisco IC3000 Industrial Compute

Hardware Sensor

DPI and active discovery via SPAN to support brownfield

Cisco Cyber Vision

Visibility built into your network infrastructure

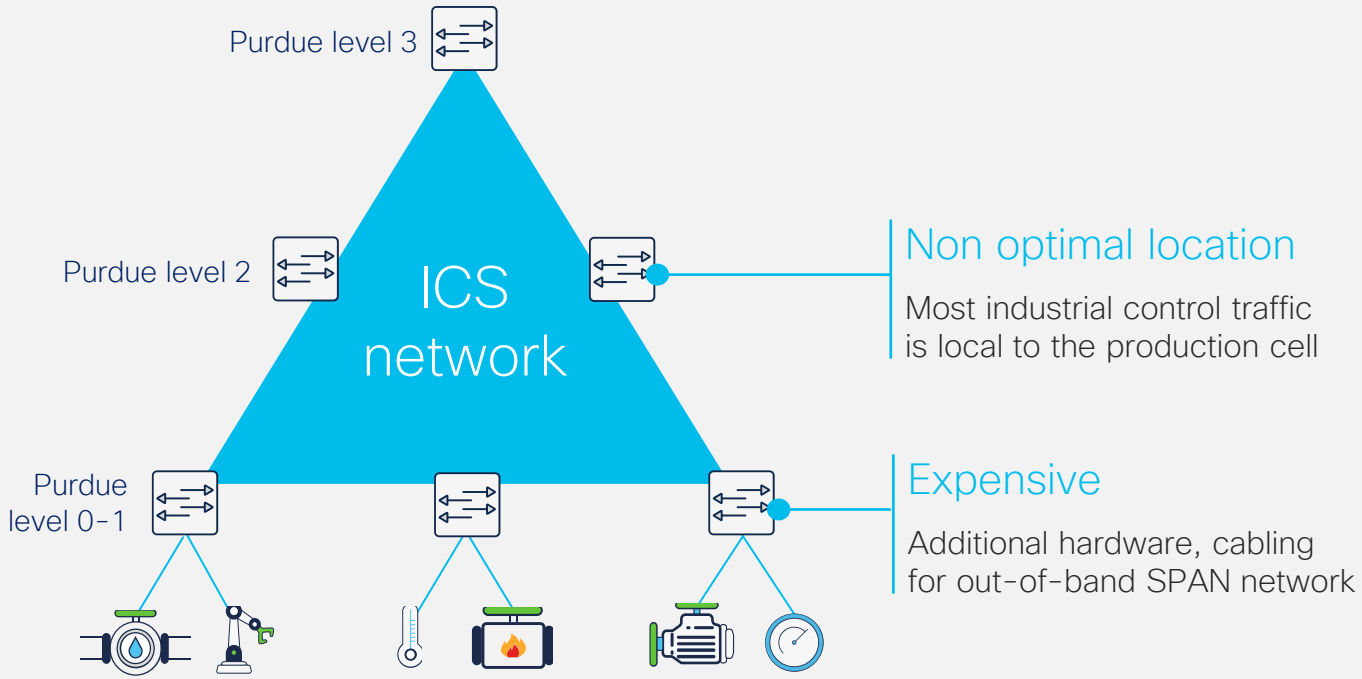


- Visibility sensor is a software feature running in select Cisco switches and routers
- No additional appliances needed
- No need for an out-of-band collection network
- Active discovery requests see pass NAT and firewall boundaries
- Centralized deployment and management
- No impact on network performance

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



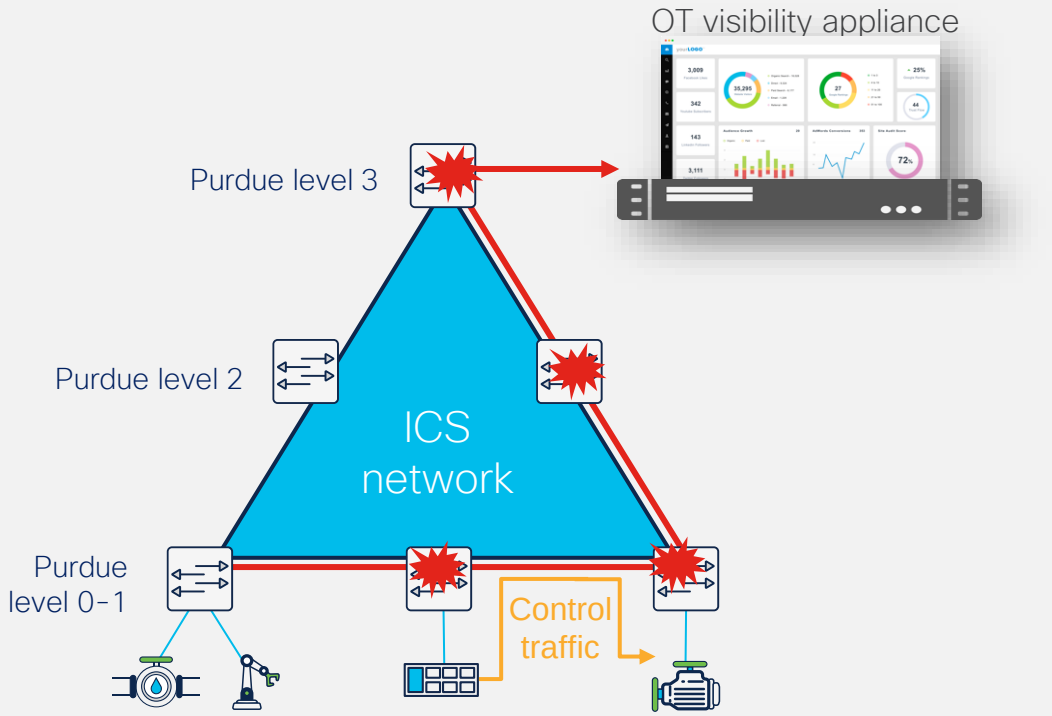
DPI location matters!

- 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!

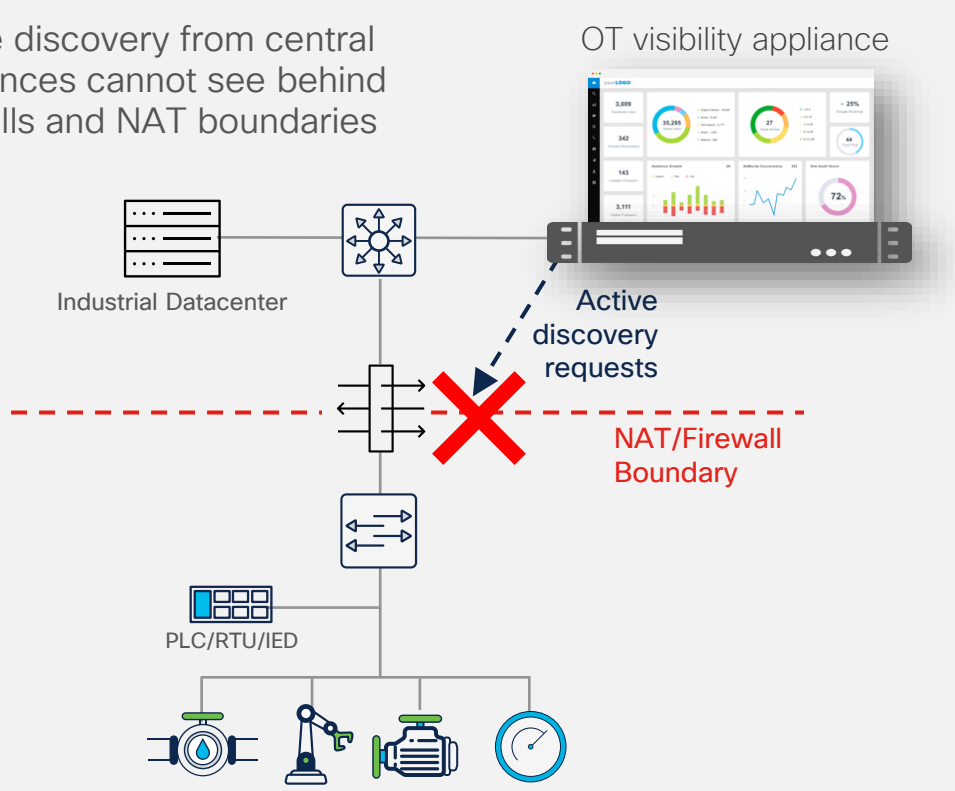
- Head-of-line blocking caused by Inline SPAN traffic negatively impacts time-sensitive control loop
- RSPAN in LANs is detrimental to control system performance

Sensors generate lightweight metadata that does not congest QoS queues

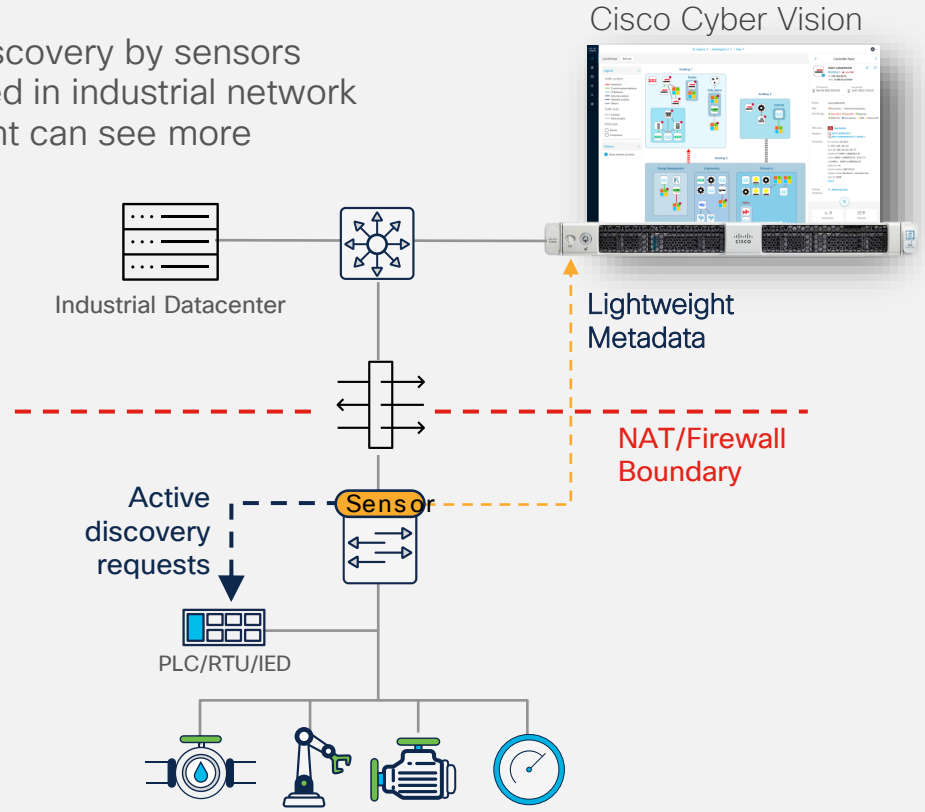
Why is a network-sensor important?

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

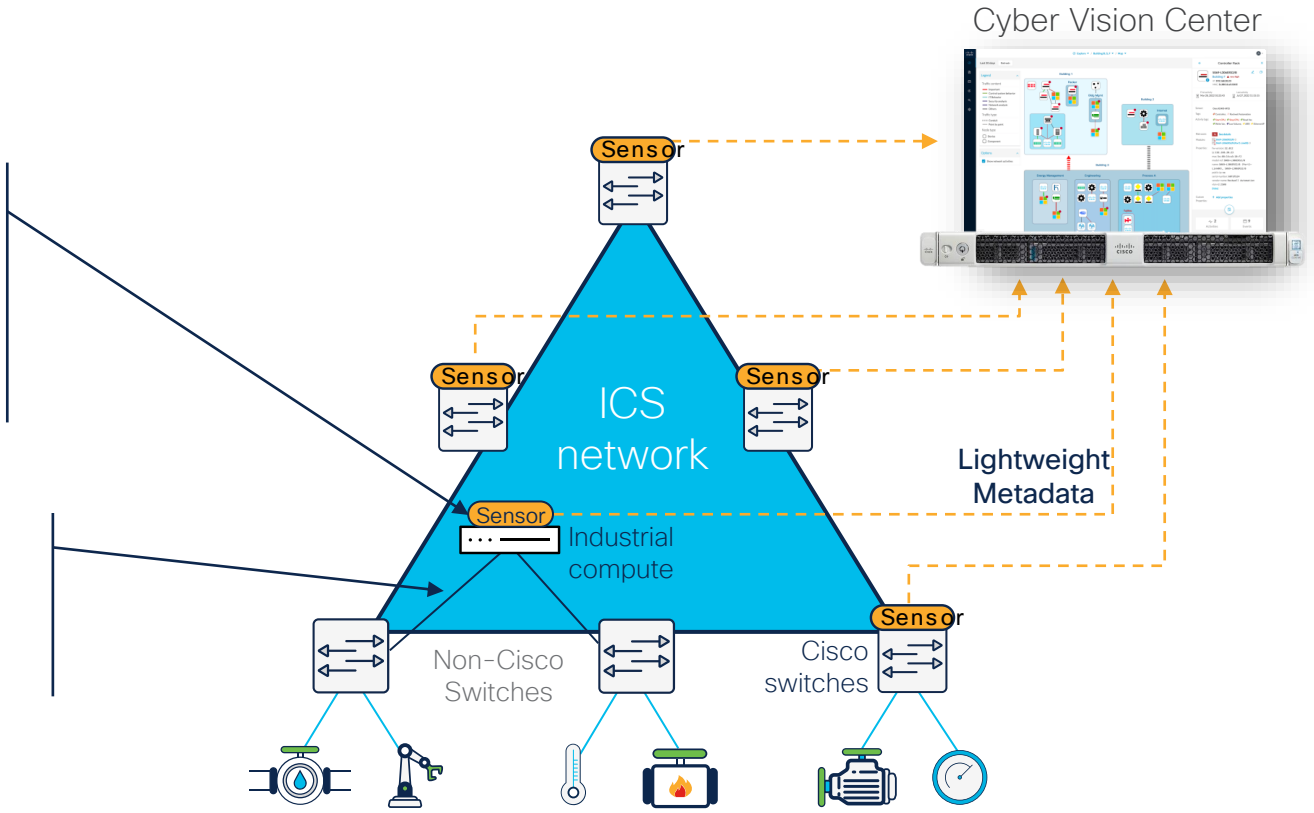
Cyber Vision hardware-sensor connects legacy switches to the OT security infrastructure

Hardware sensor has low TCO

Low-cost appliance to deploy everywhere DPI cannot be embedded

Only 1-hop of SPAN traffic

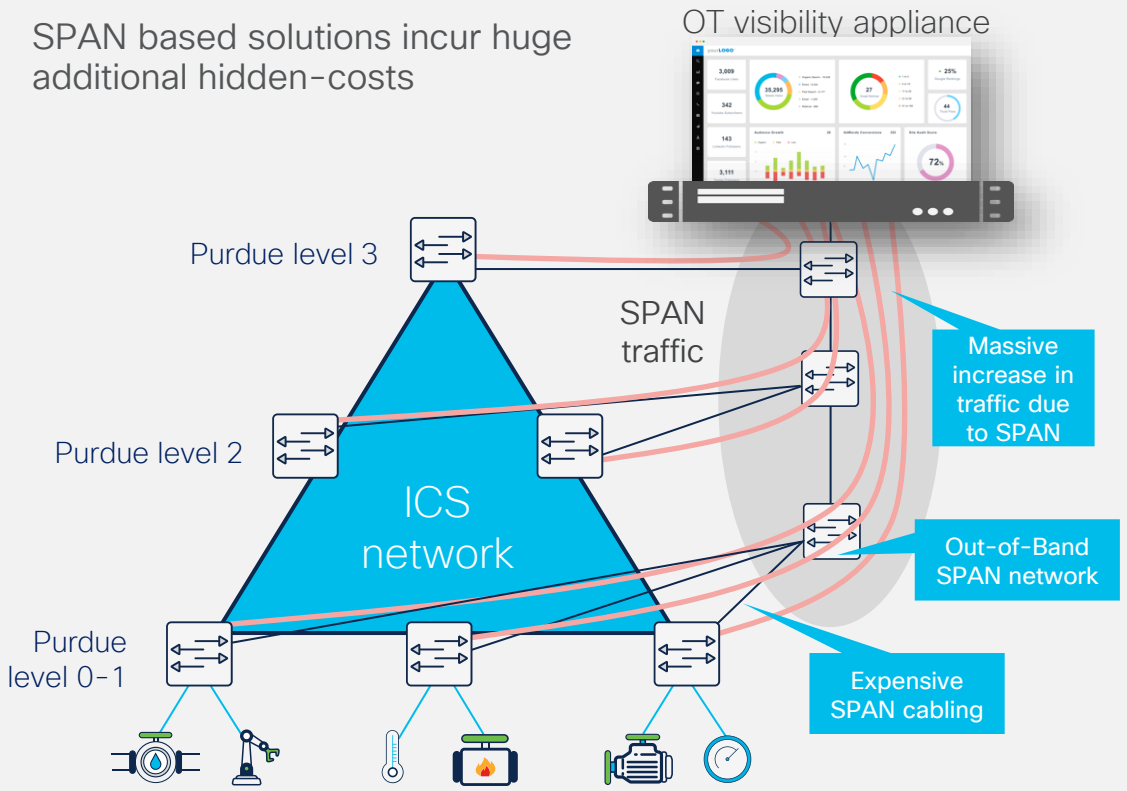
No need for additional network resources to collect traffic and send data to the console



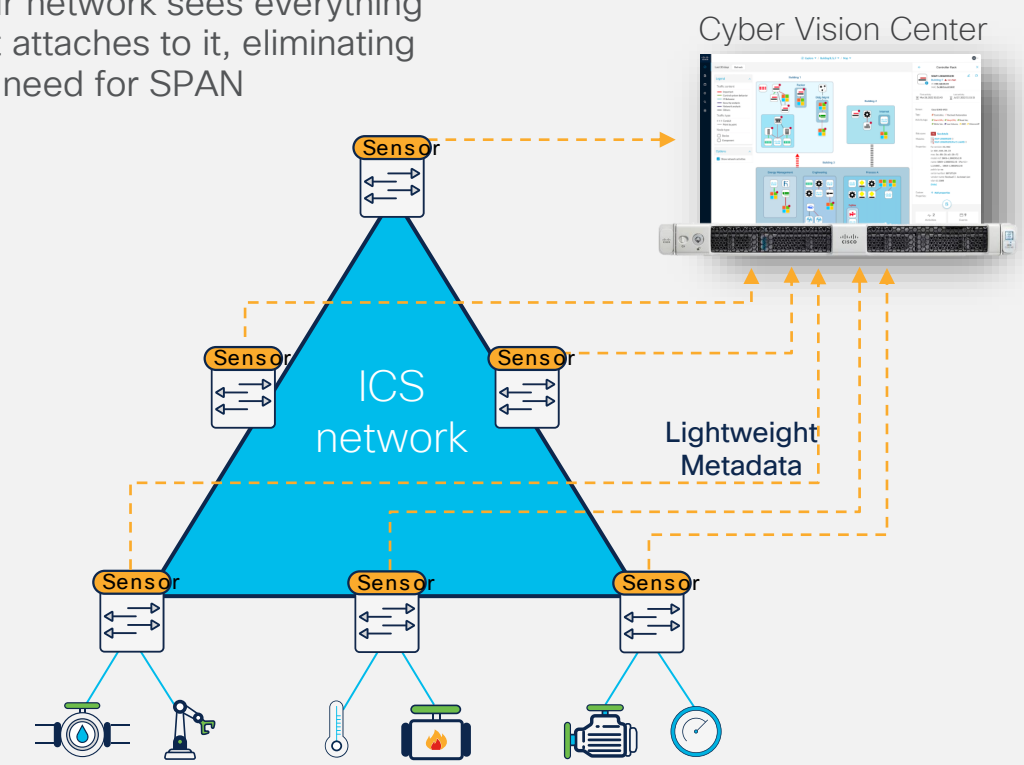
Cisco Cyber Vision works great with third-party switches

Cyber Vision scalable architecture

SPAN based solutions incur huge additional hidden-costs



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



On-Center Sensor offers extra deployment flexibility

Central DPI and IDS capabilities

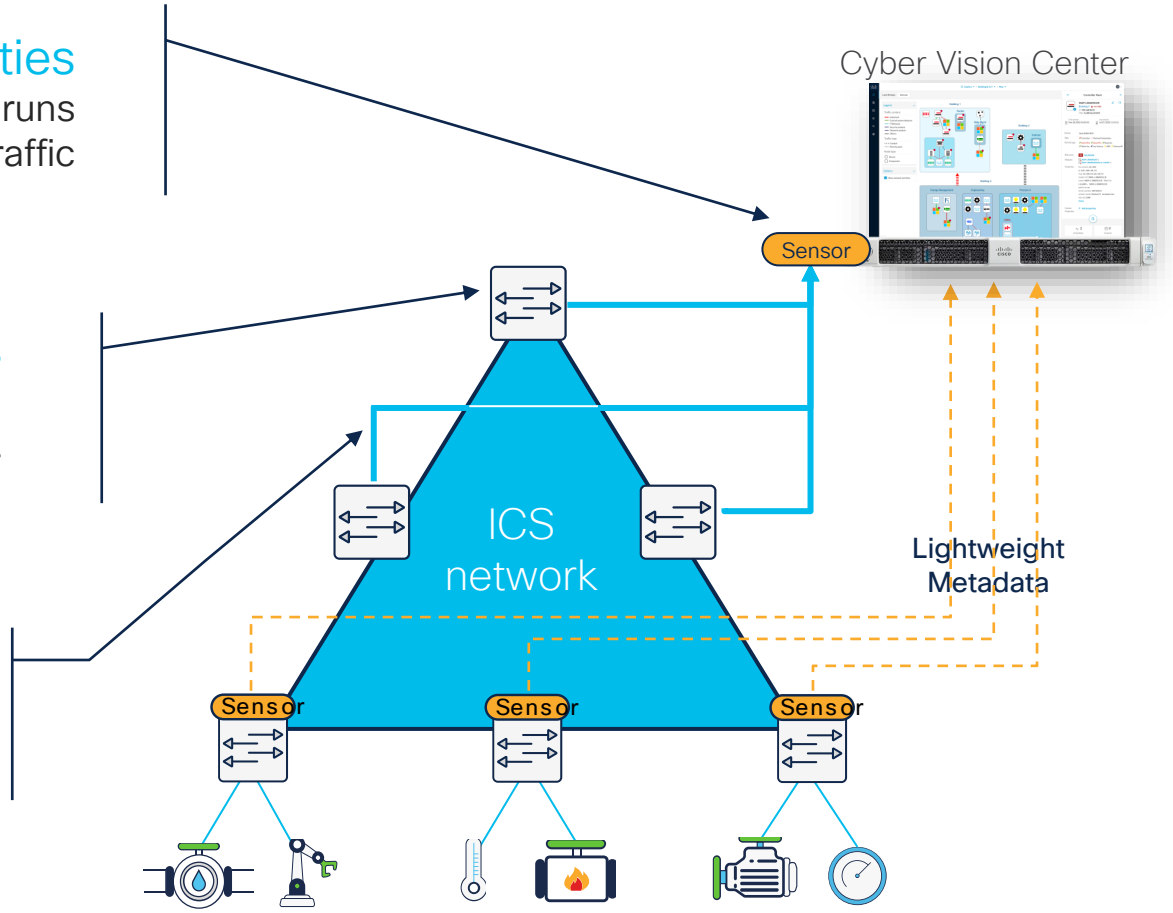
Sensor built into the Cyber Vision Center runs DPI and IDS on raw industrial network traffic

Collect traffic from the datacenter

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

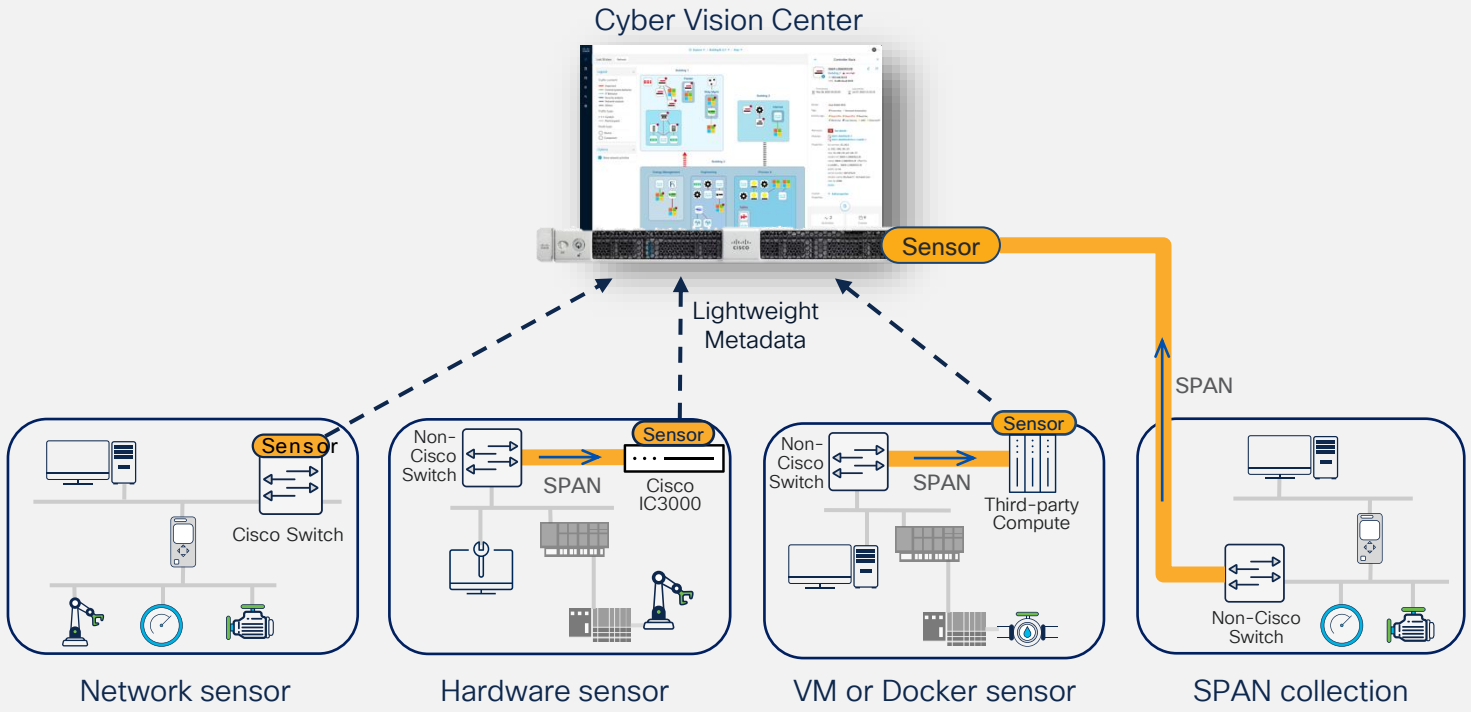
Leverage existing SPAN infrastructures

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



Cisco Cyber Vision

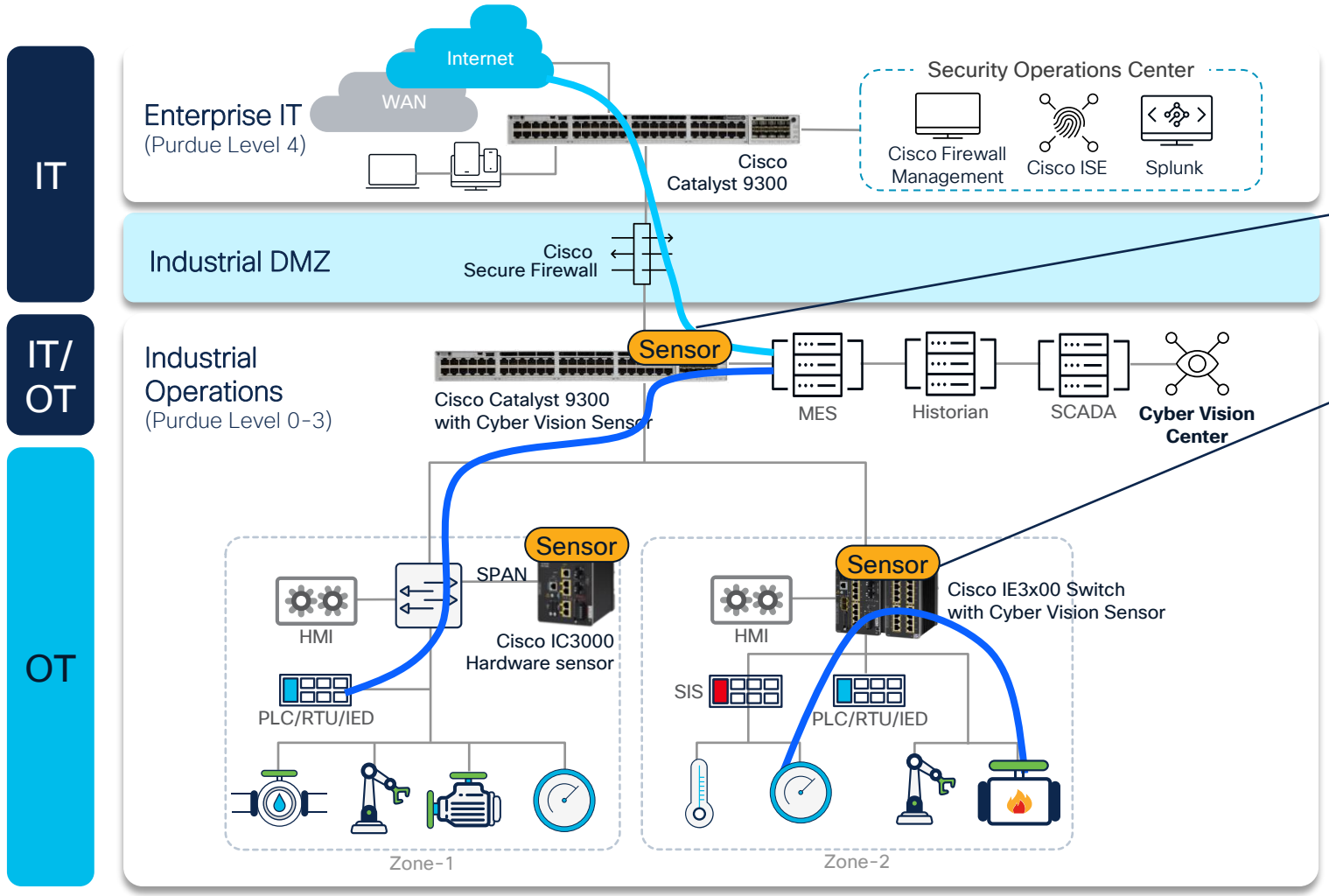
Implementing OT visibility at the lowest TCO



- **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?



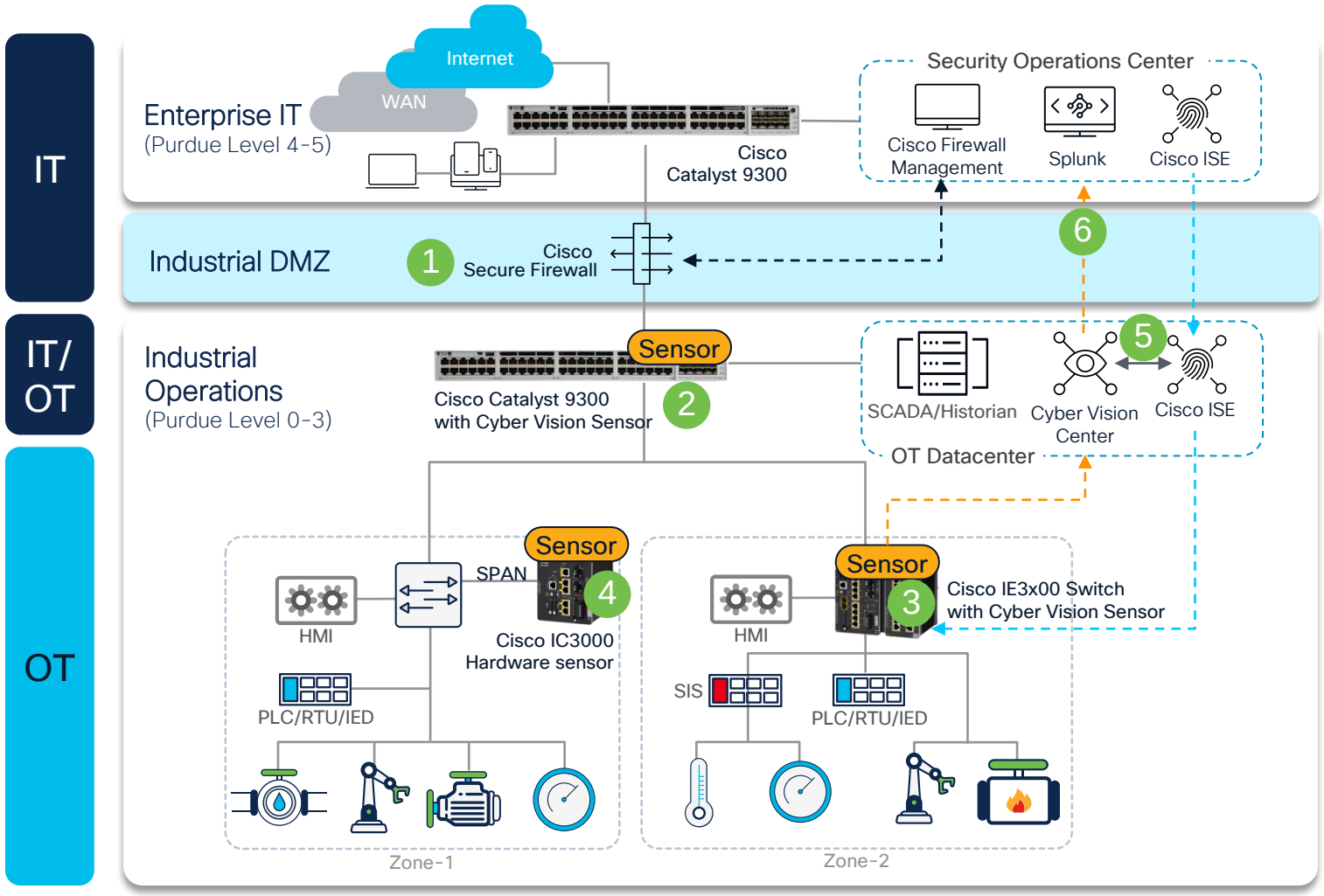
Sensor at aggregation sees North-South traffic

Sensor at the edge sees East-West traffic

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

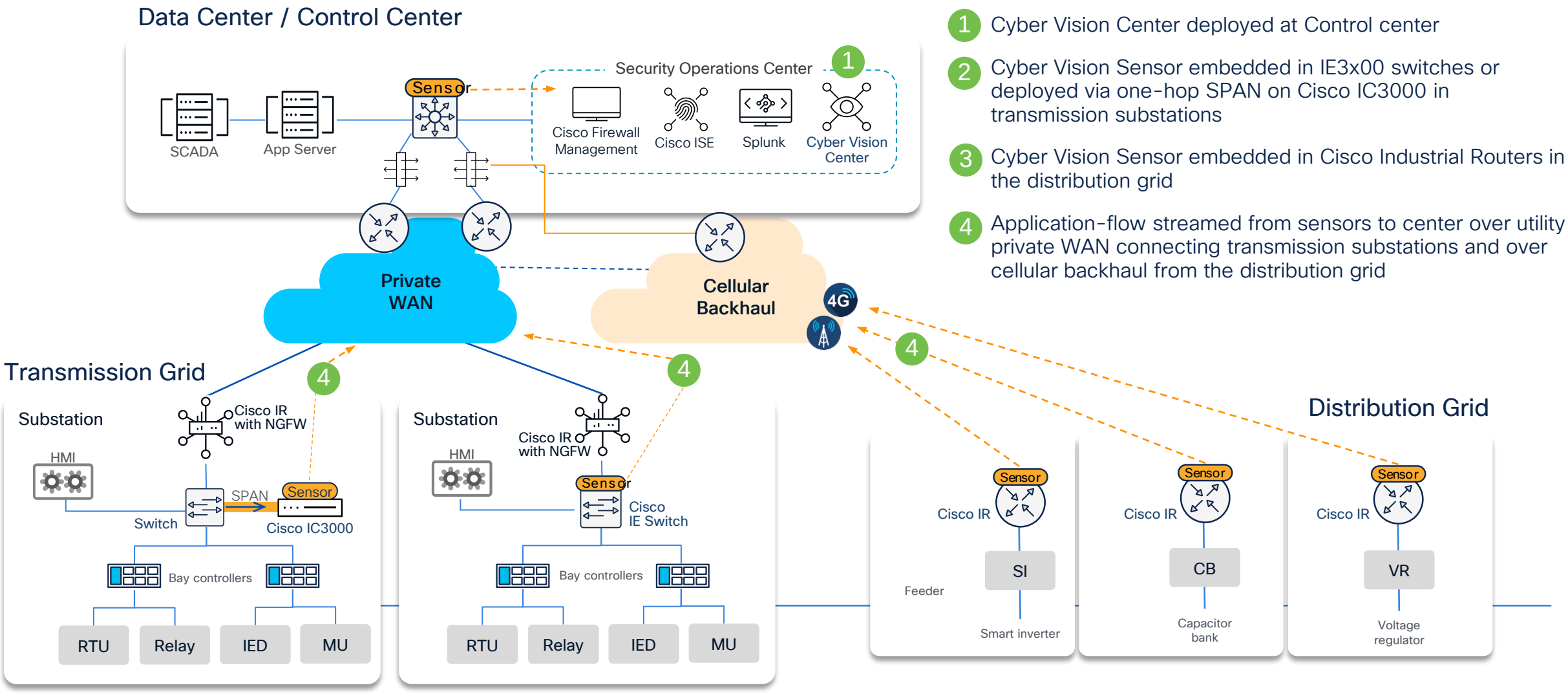
Rule of thumb: All flows must go through at least one sensor. Every networking equipment should have a sensor.

Cisco Cyber Vision in Manufacturing



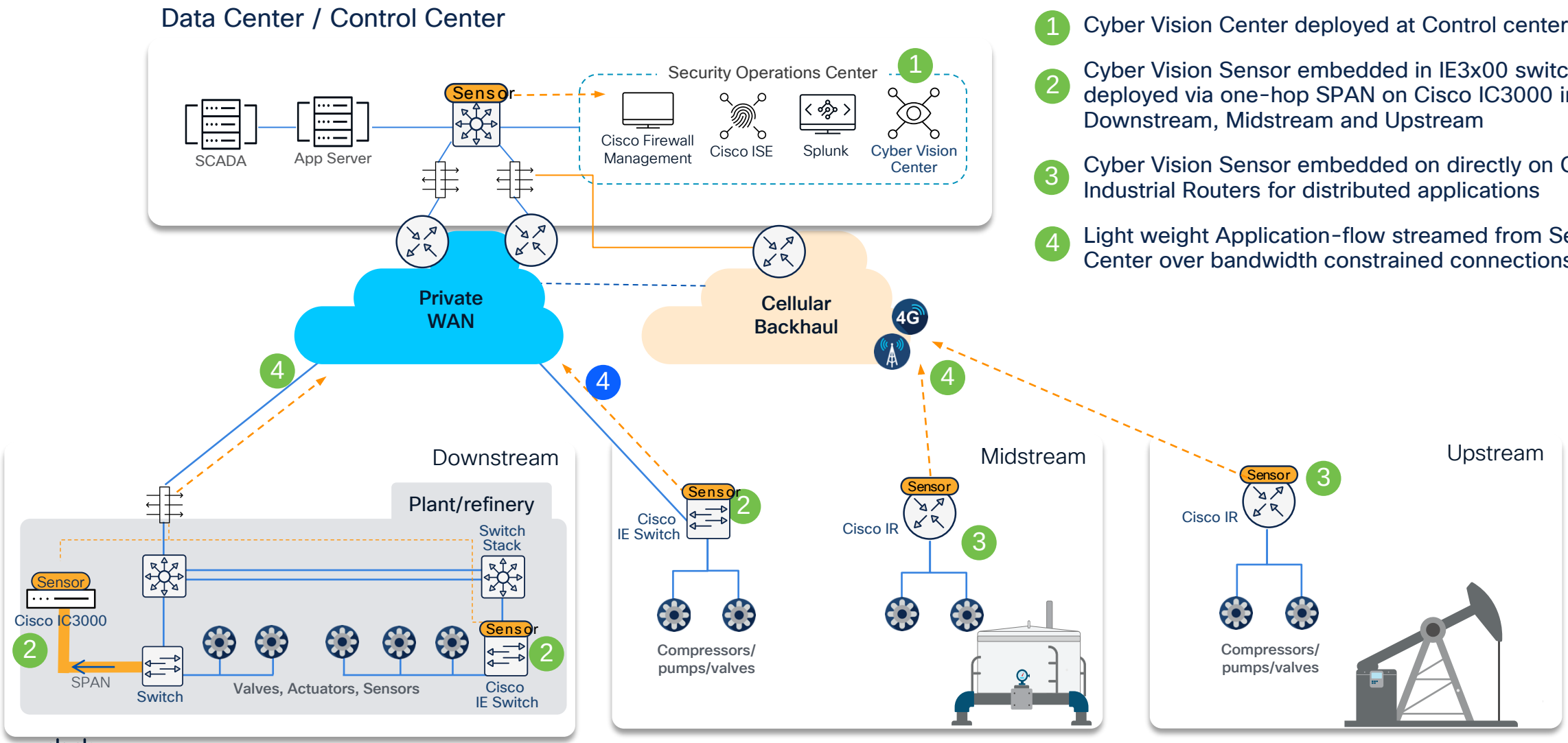
1. Isolate IT and OT by installing an industrial DMZ with Cisco Secure FW
2. Create macro-segmentation zones in the Catalyst 9300 switches and deploy Cyber Vision sensors with Snort IDS.
3. Cyber Vision sensors deployed within segments across IE3x00 switches
4. Cyber Vision hardware-sensors deployed 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



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

Cisco Cyber Vision in Oil and Gas



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

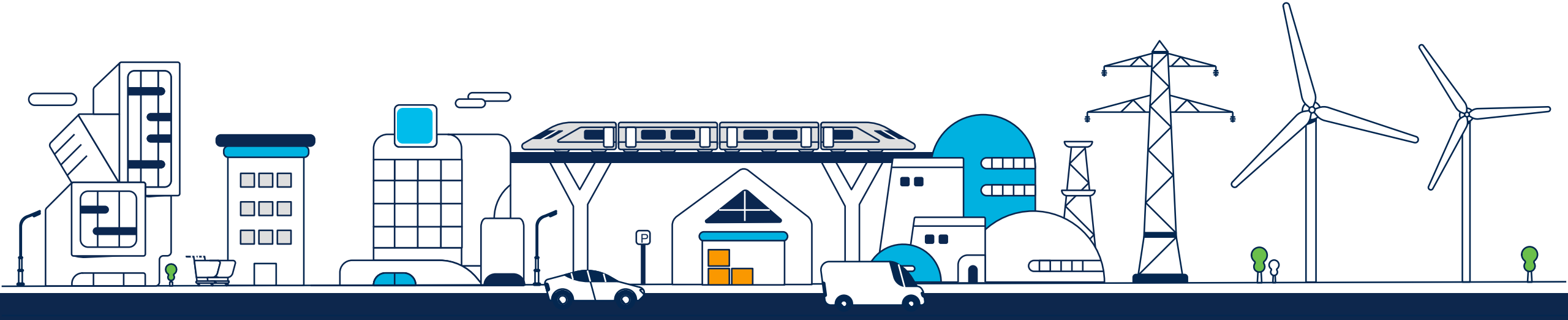
One Global Center at HQ
Gives SOC & CISO teams aggregated visibility across all sites

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

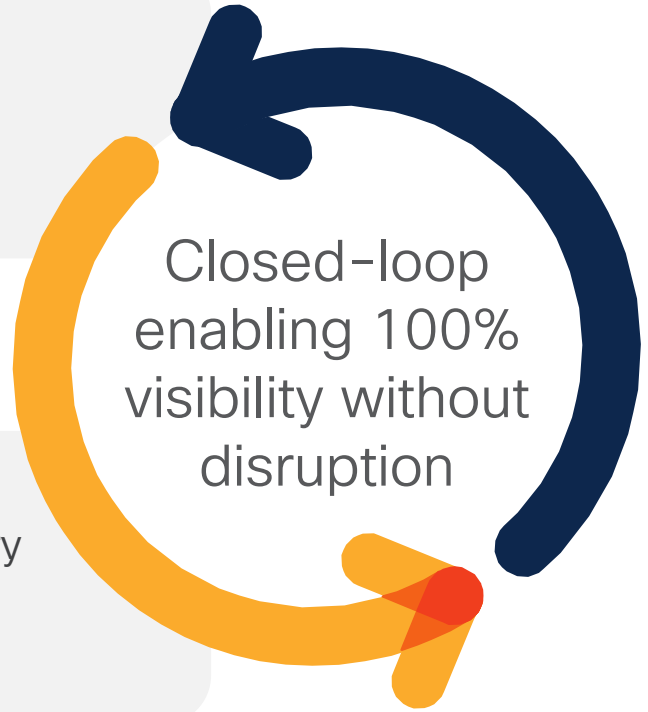
Passive + Active asset discovery

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



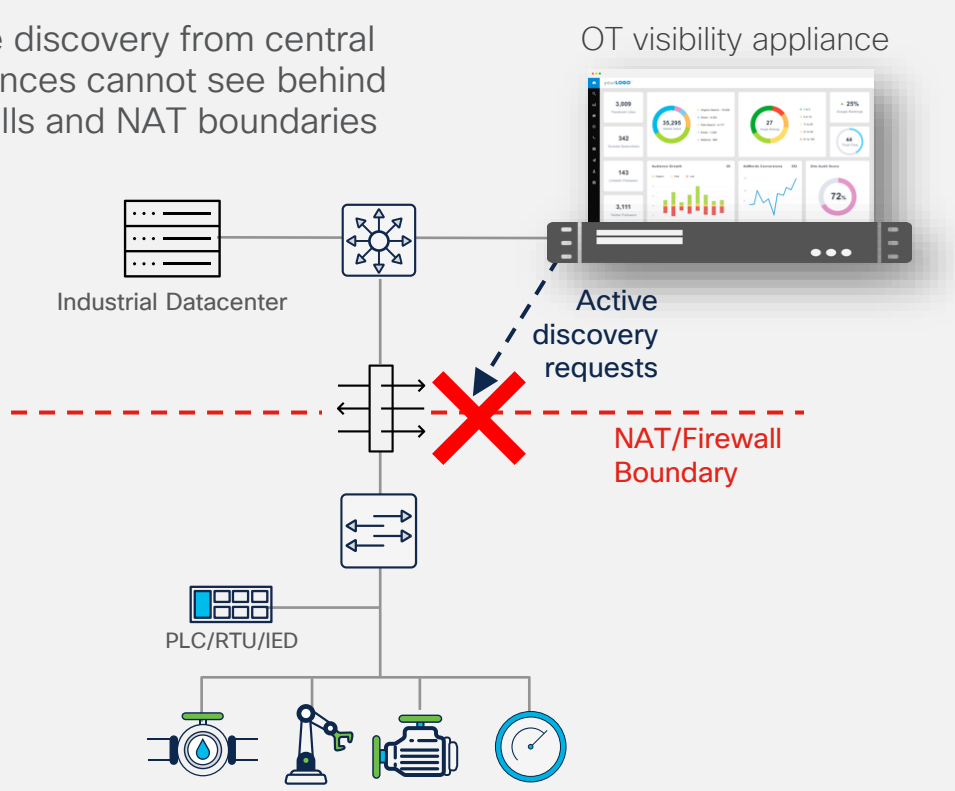
Distributed Edge Active Discovery Features

Features	Benefits
Enabled by user, fully passive by default	No risk of disrupting industrial assets
Closed loop control – Passive collection informs active discovery	Assets are not flooded with ARP requests. Cyber Vision does not scan networks.
Wake up broadcast messages	Discover silent devices. 100% visibility
Active discovery performed by the sensor	Passes firewalls and NAT boundaries. 100% visibility
Active discovery using S7, S7Plus, Profinet, EtherNet/IP, DNP3, SNMP, ICMPv6, WMI, etc.	100% visibility of Rockwell, Schneider, Siemens assets and Windows machines

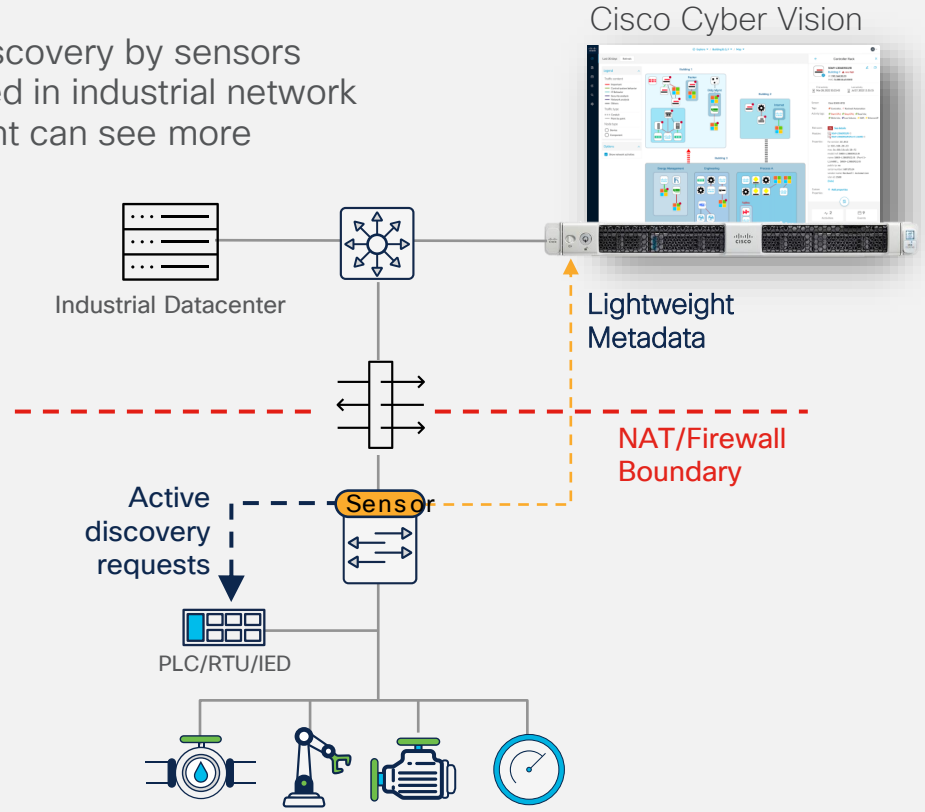
Why is a network-sensor important?

Distributed edge active discovery gives you 100% visibility

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



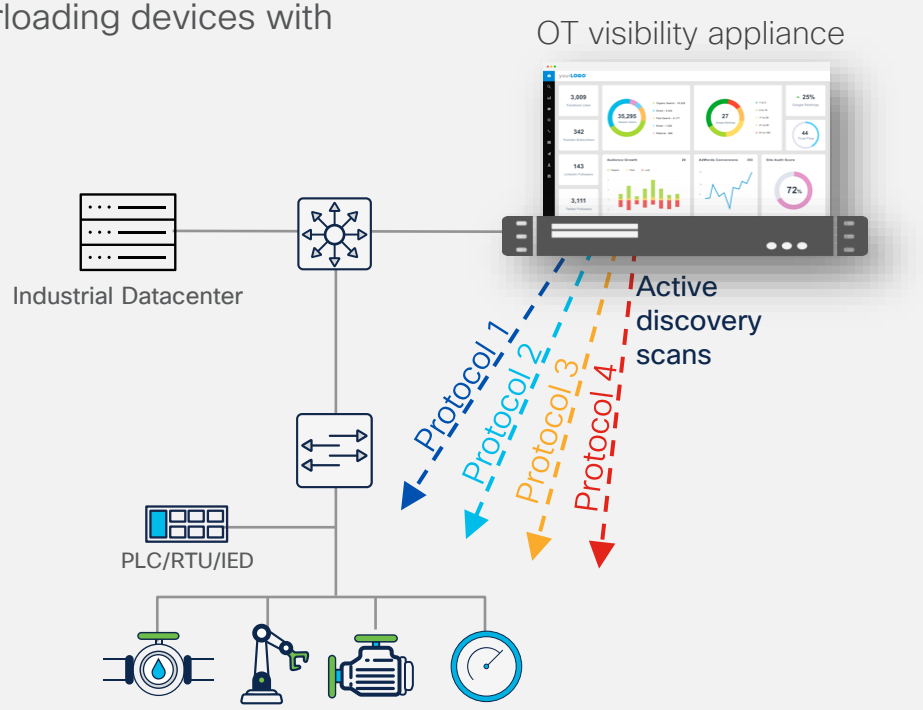
Active discovery by sensors embedded in industrial network equipment can see more



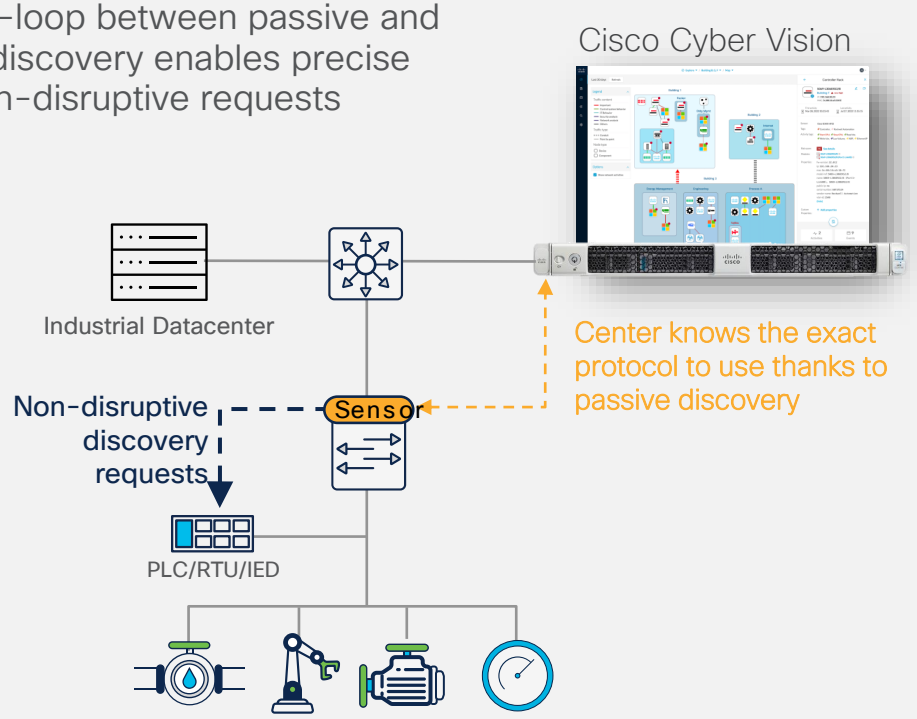
Sensors embedded in the network can see more

Closed-loop control makes active discovery safe

Basic active discovery solutions scan networks overloading devices with ARP requests

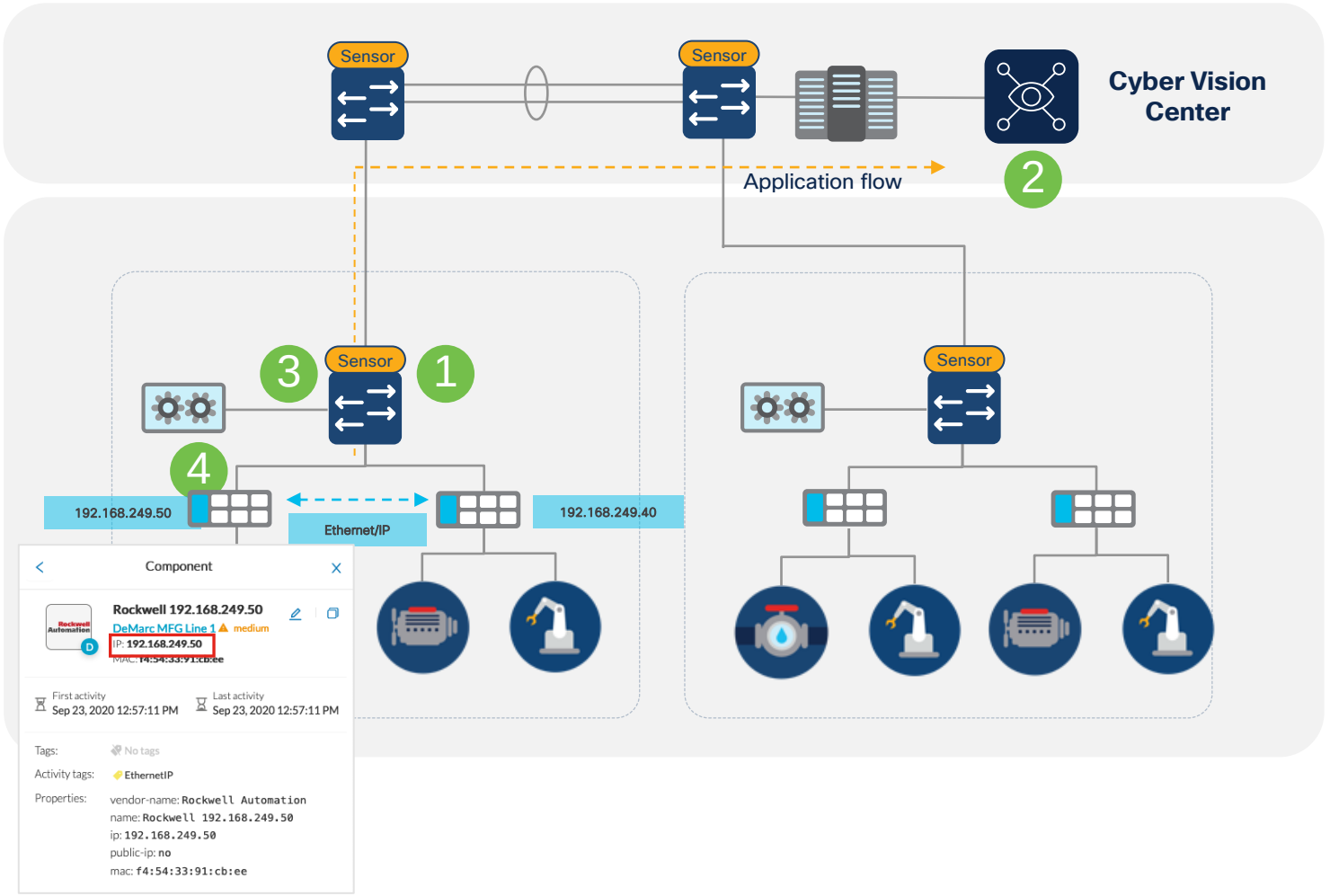


Closed-loop between passive and active discovery enables precise and non-disruptive requests



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

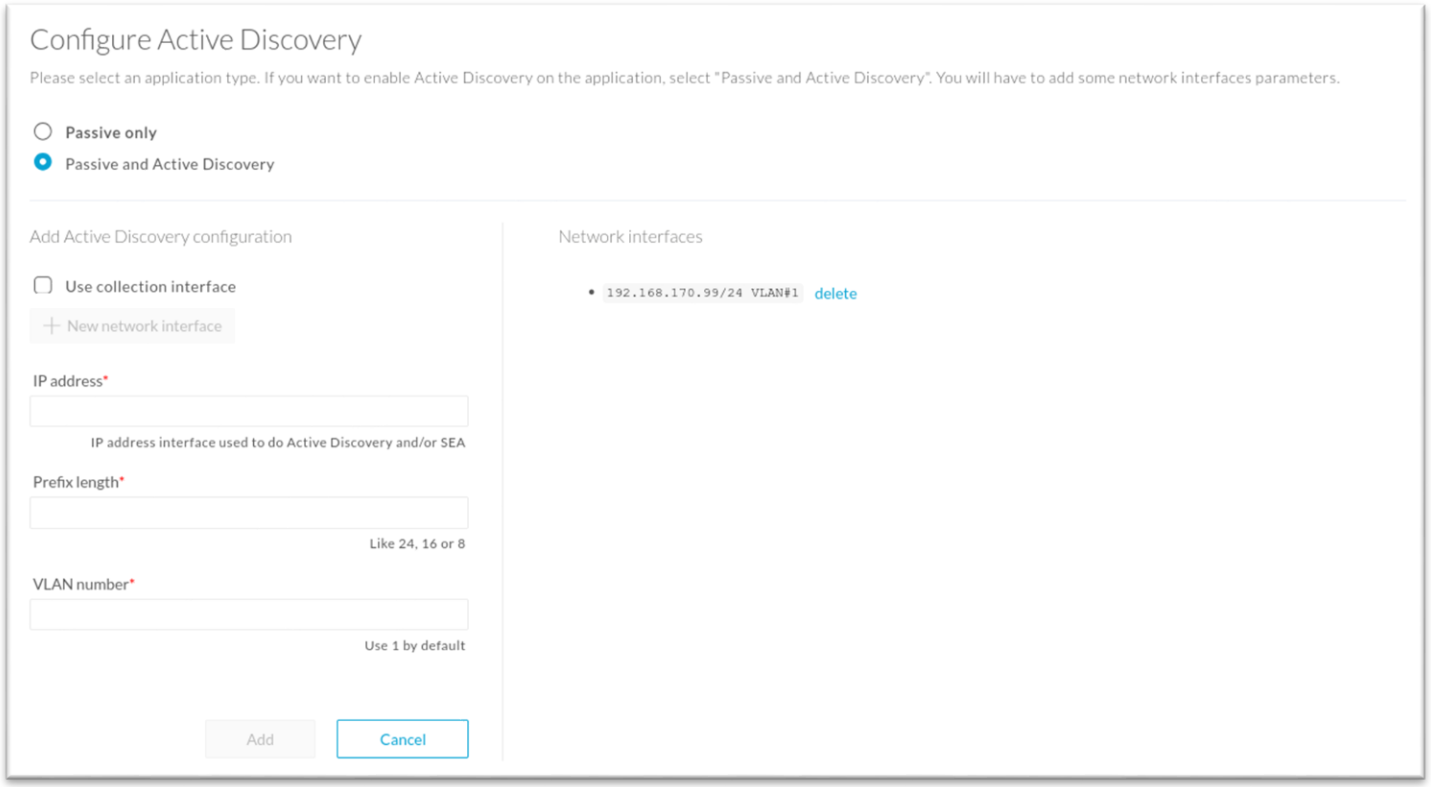


Cyber Vision active discovery keeps you in control

- 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



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

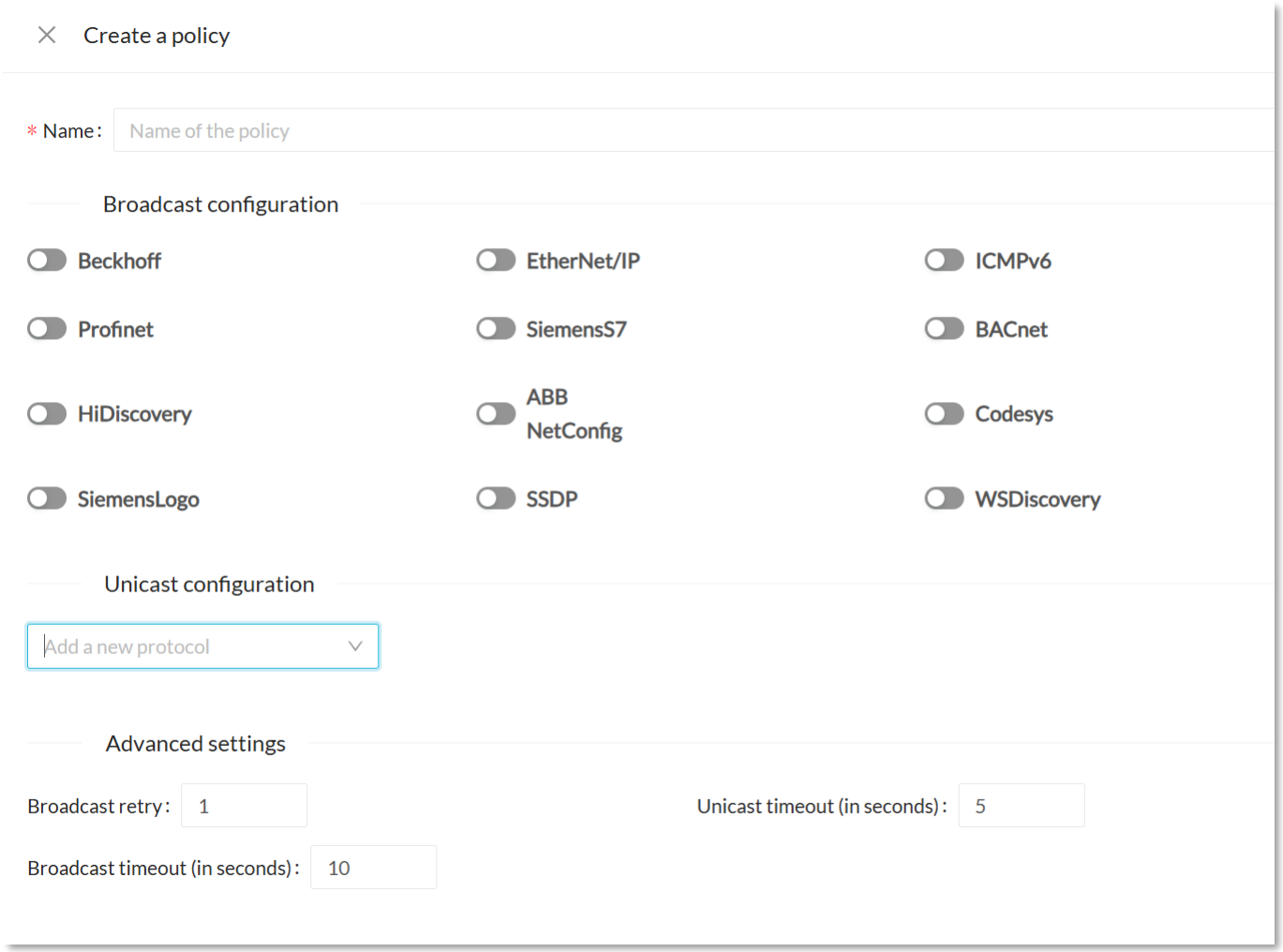
A profile is defined by:

- 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

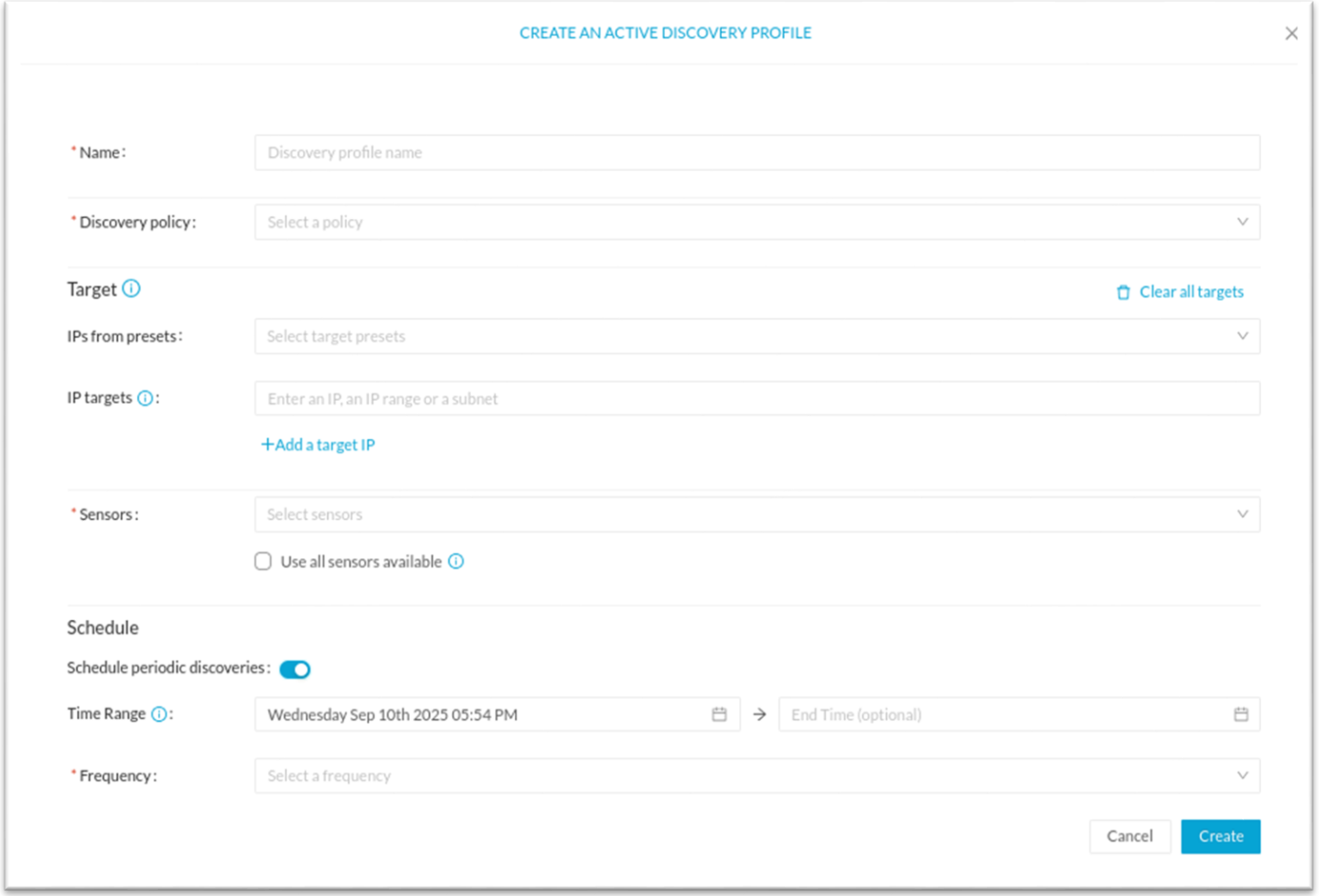
Define and configure protocols which could be used in a profile

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



Creating Active Discovery Profiles

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

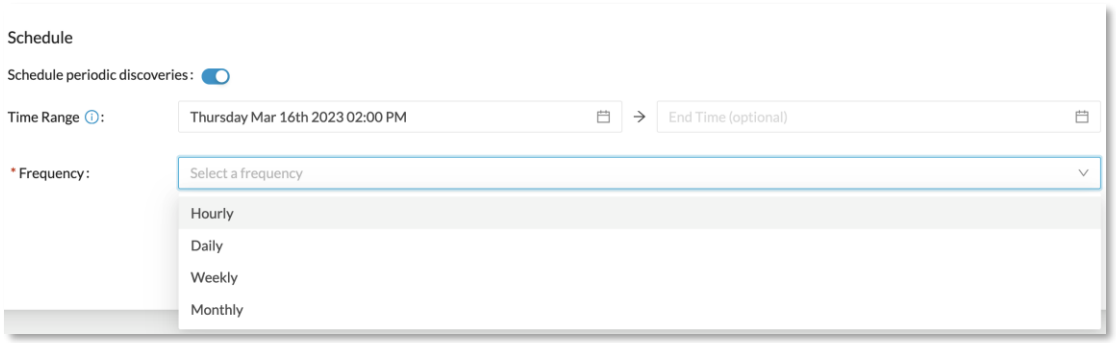


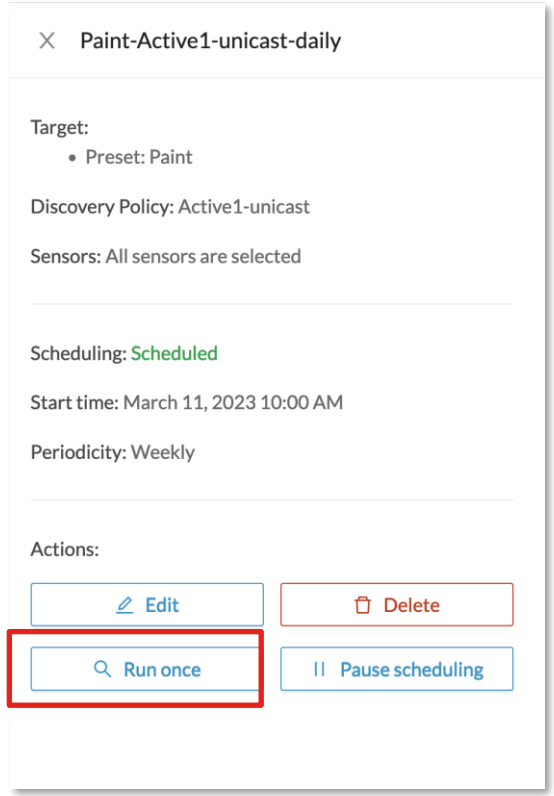
Schedule Reoccurring or Run Once

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

OR

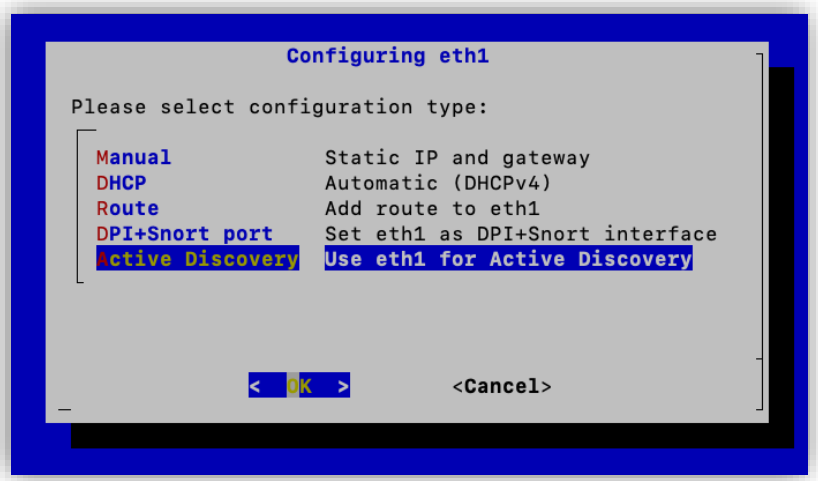
Choose Run once to save and trigger a discovery to occur within 30 seconds

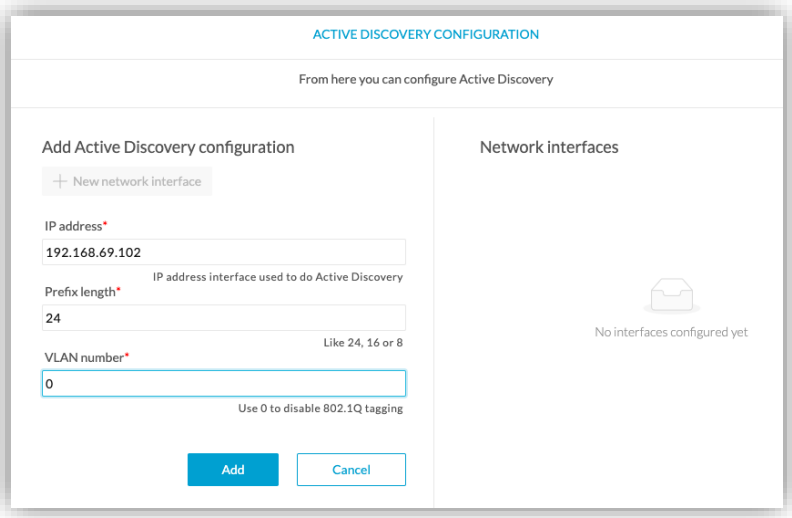


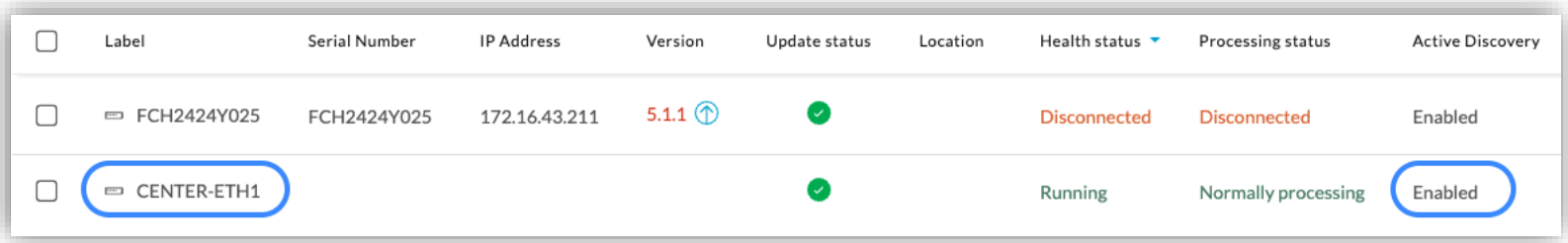


Active Discovery Support for Center Interfaces

- 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

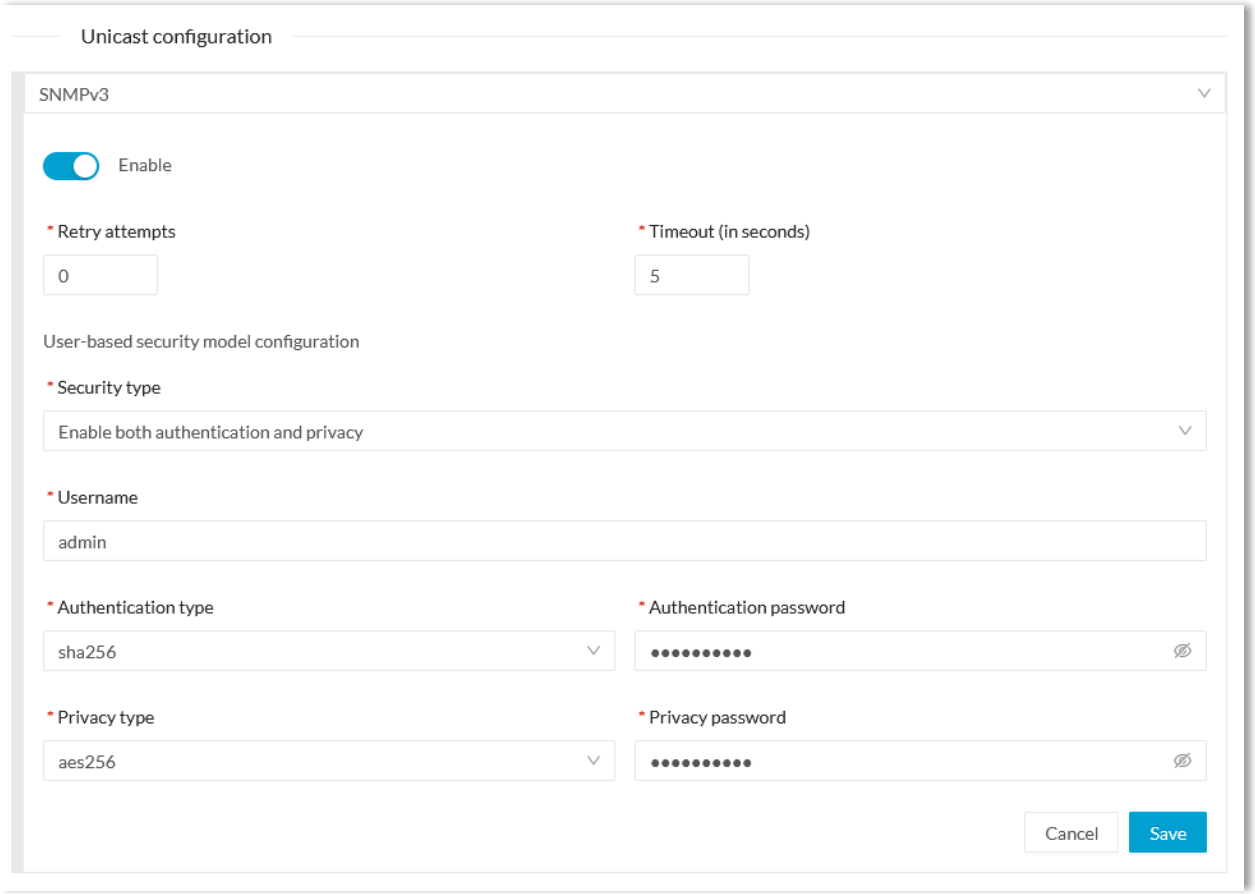




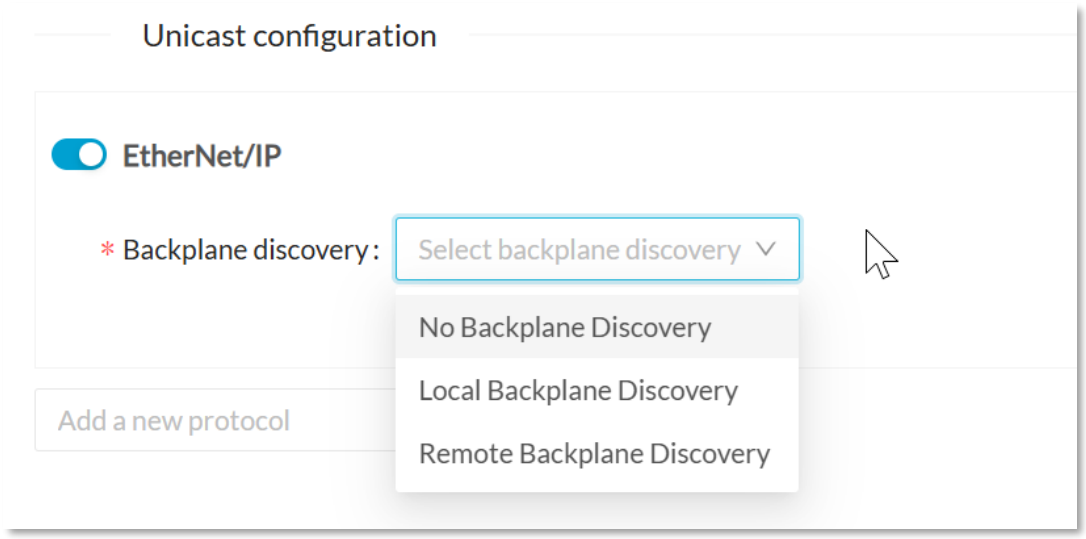


Configuring SNMP active discovery policies

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



Configuring ENIP active discovery policies



Configuring WMI active discovery policies

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 @ 2.40GH**

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**

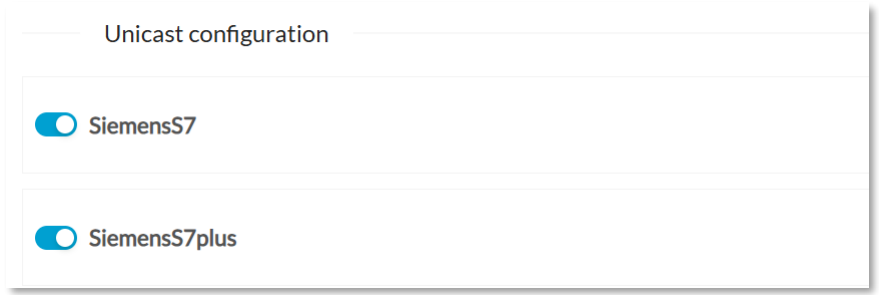
wmi-service-pack-major-version: **0**

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

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

wmi-windows-sku: **7**

Configuring Siemens S7 active discovery policies



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

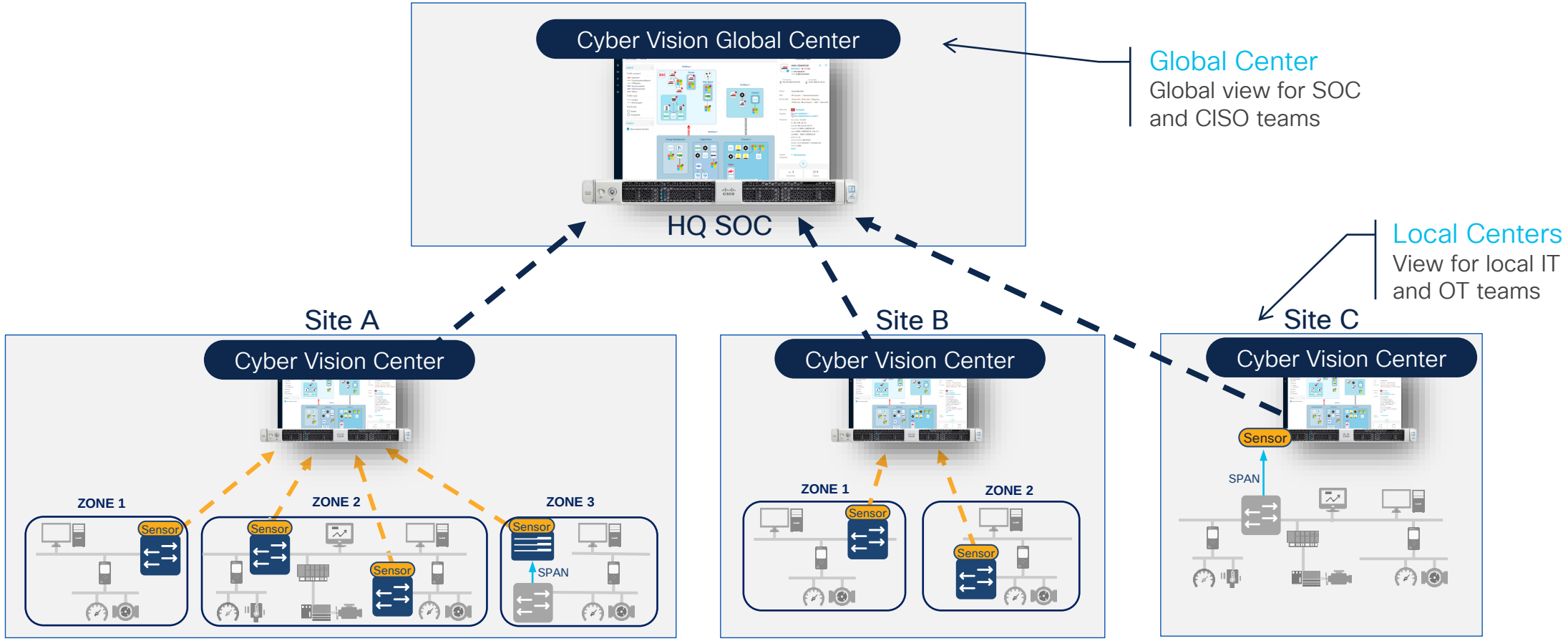
CISO Team

Aggregate data from all sites to drive governance and compliance

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

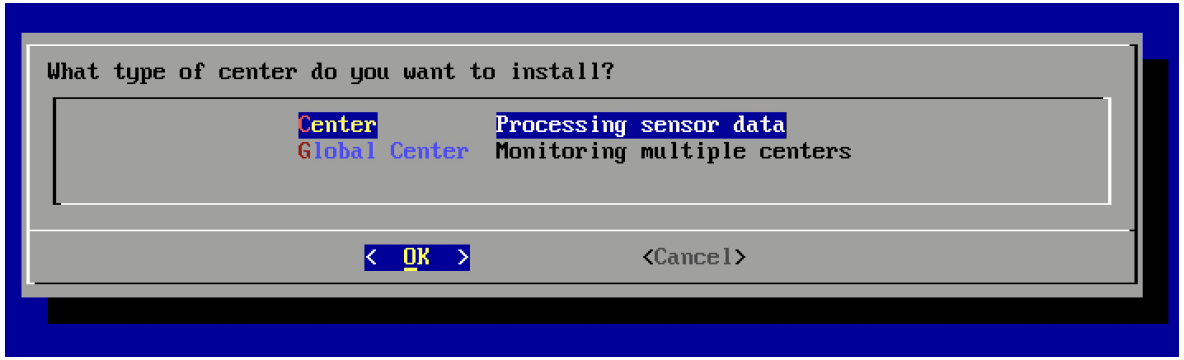
Cisco Cyber Vision Global Center

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



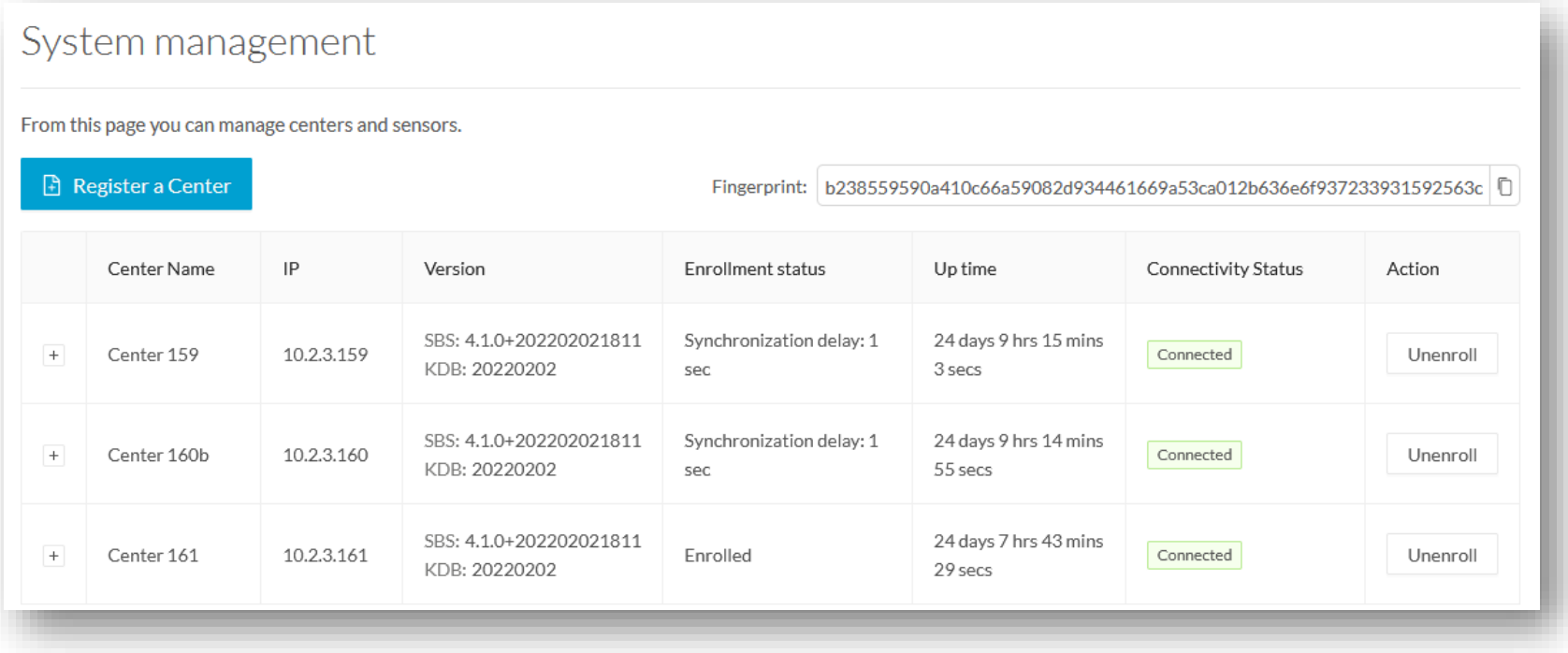
Applies to Cyber Vision 4.1 and above

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



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

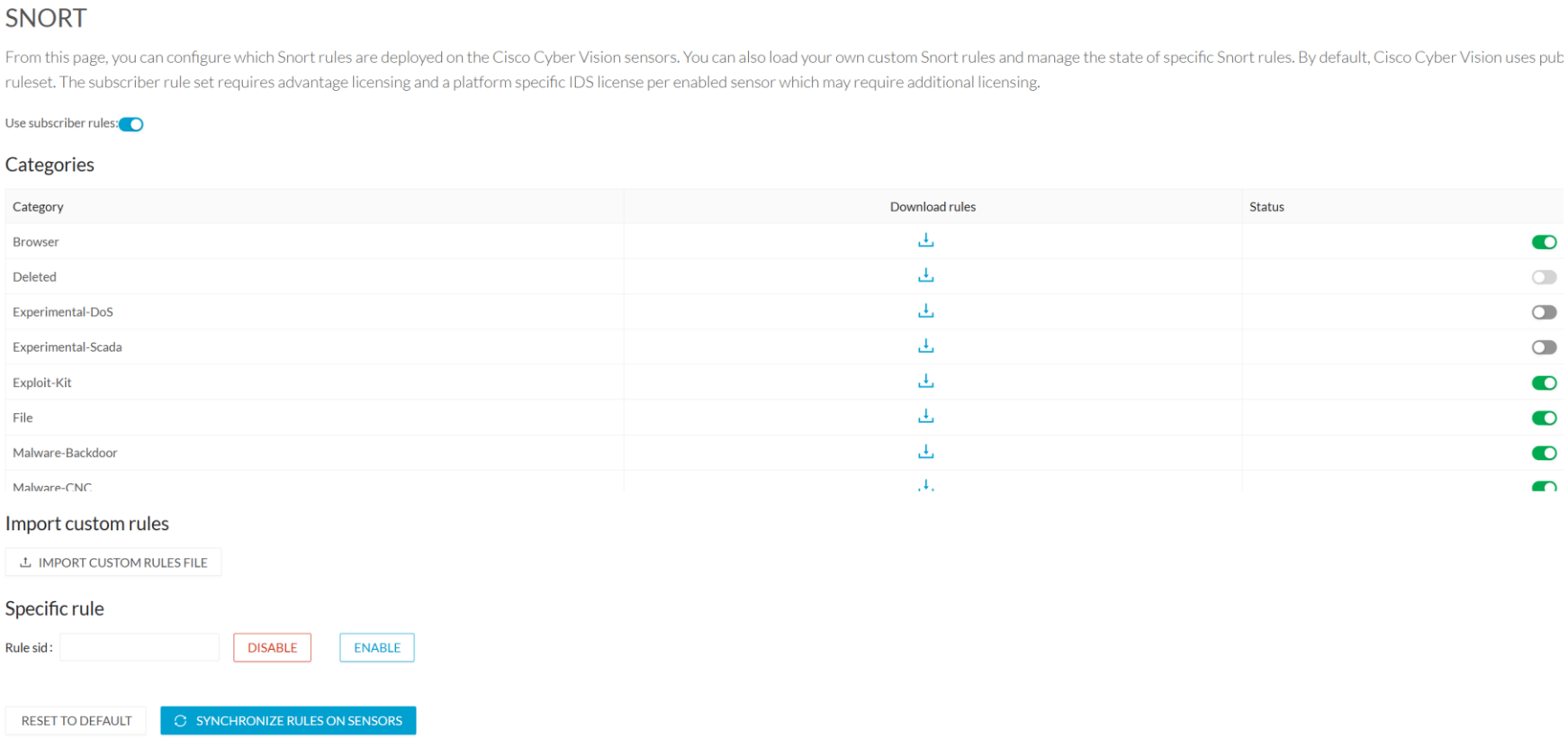
- Included with Cyber Vision Advantage license
- 4.070 rules, 440 activated*
- New rules may be added 30 days after release

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

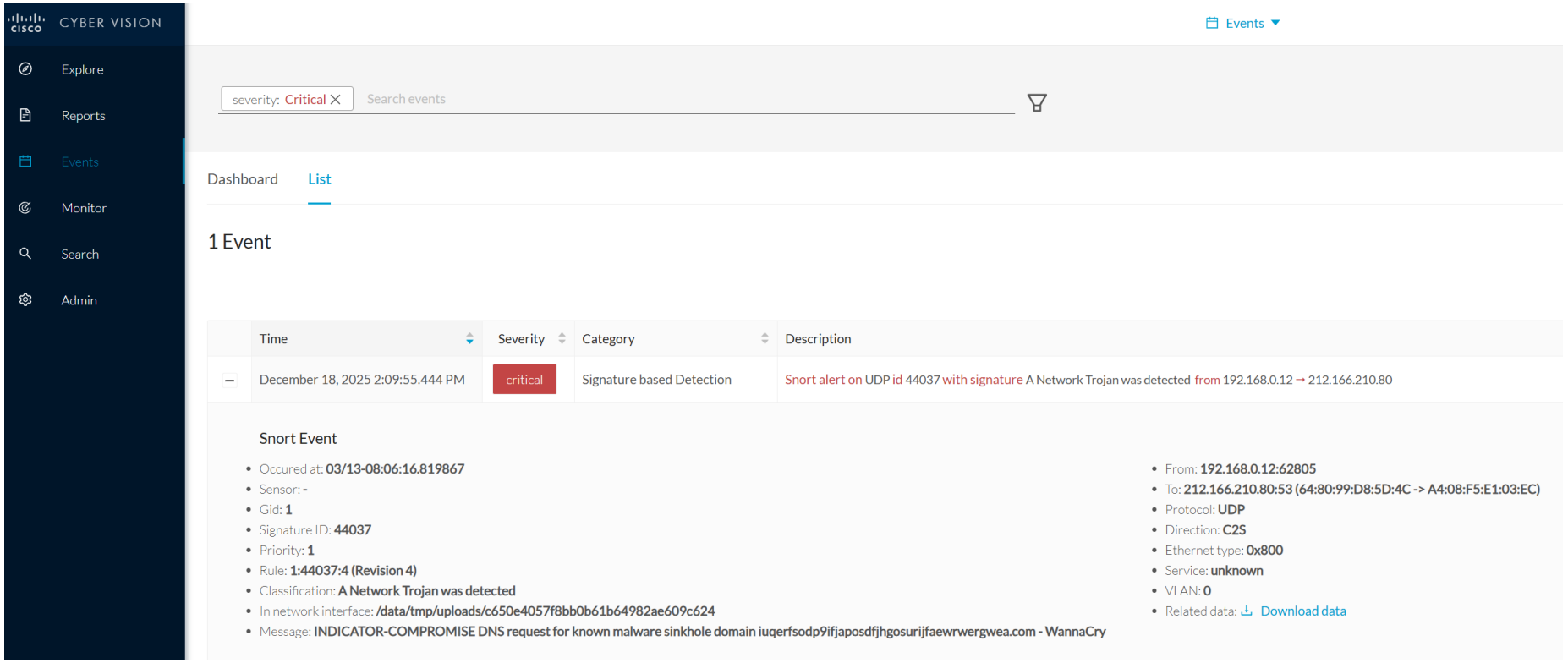
* As of Dec 2025

Snort Rules Management



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

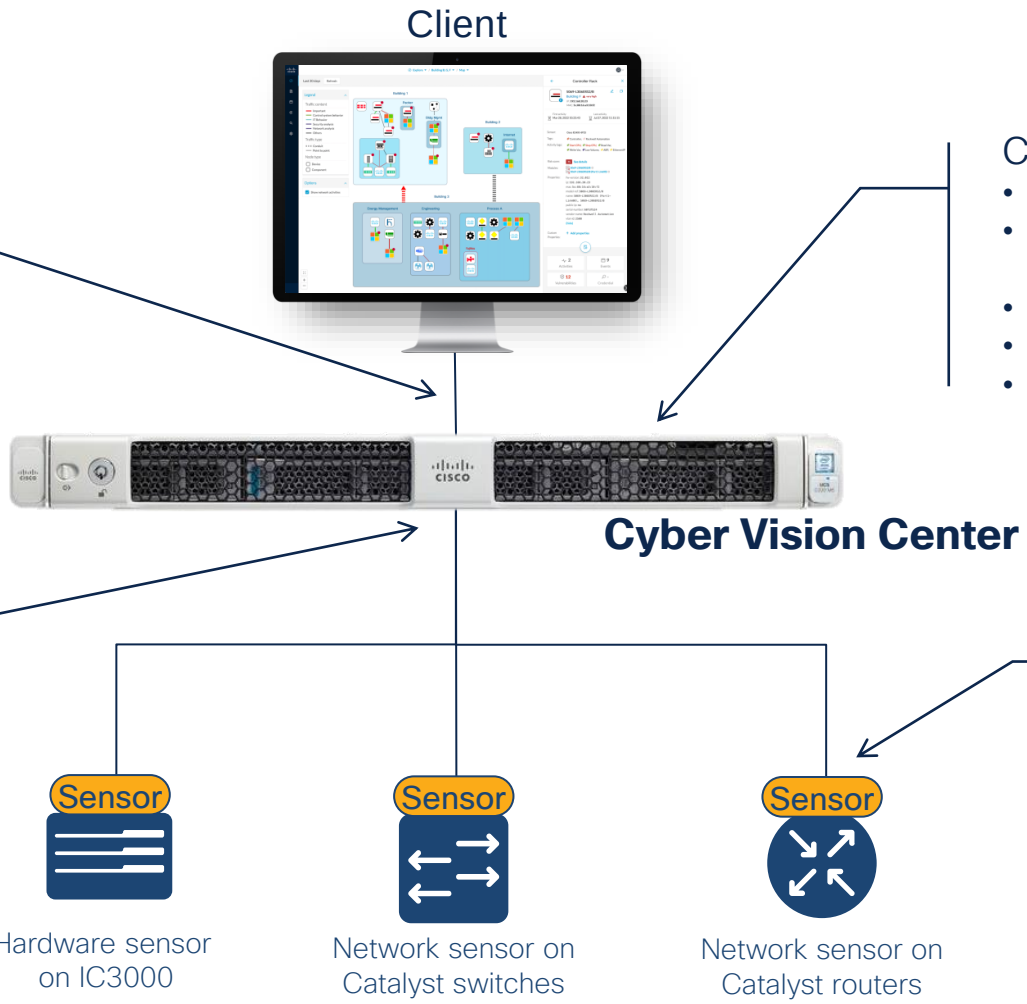
Immediately detect malicious traffic



- 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



Access Interface
- GUI via HTTPS
- RESTful API
- Integrations (XDR, FMC, ISE, etc.)
- Syslog to SIEM

Centralized Storage & Analytics
- Stores metadata coming from Sensors
- Runs analytics (Tags, Vulnerabilities, etc.)
- Identifies events and anomalies
- Visualization and reporting engines
- Exposes API for third-party integration

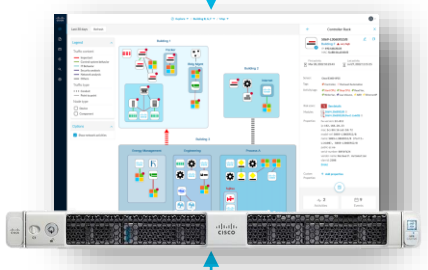
Collection Interface
- Collect metadata from sensors
- Sensor performance statistics
- Sensor management, and deployment

Store-and-Forward Architecture
- Sensors runs DPI on application flows locally
- Send metadata to Center
- If Center unreachable, data stored locally and sent later

Single or Dual interface

2 interfaces

eth0 – Access - GUI

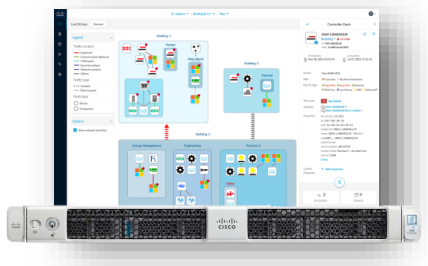


eth1 – Collection Interface – Sensor to Center

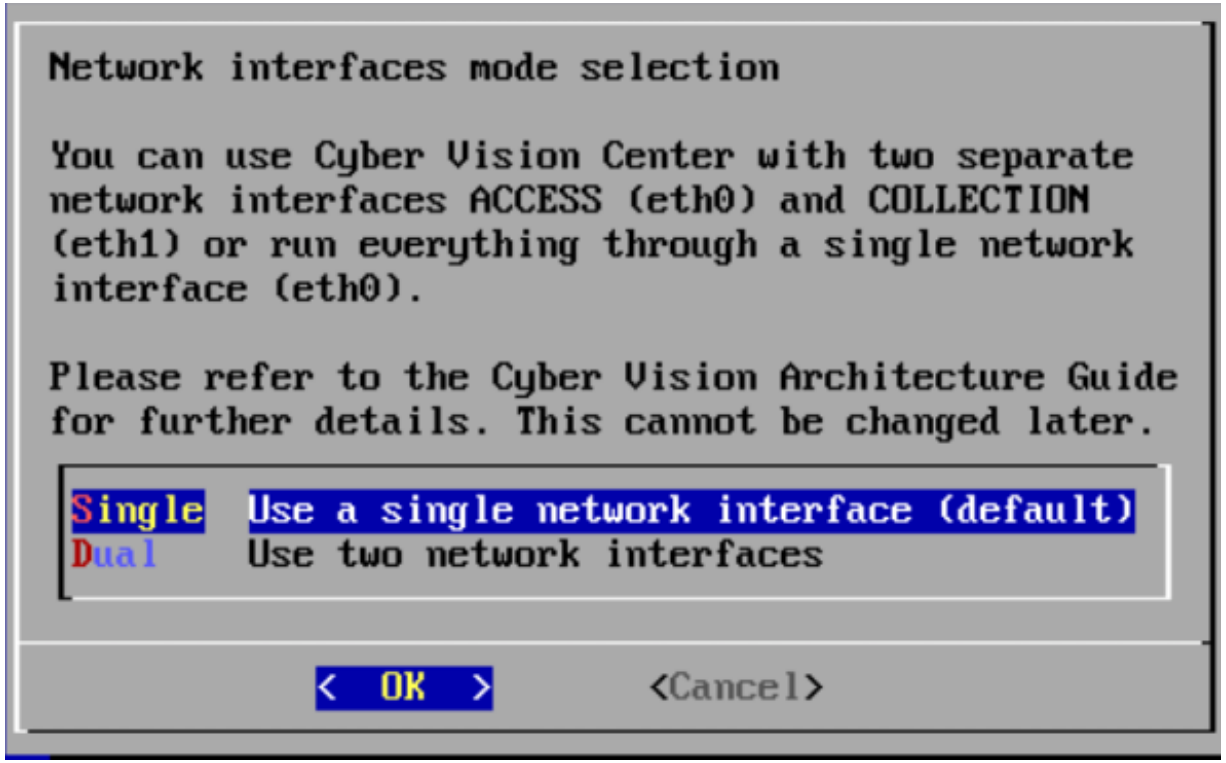
1 interface

eth0 - Combined Role:

- Access - GUI
- Collection – Sensor to Center



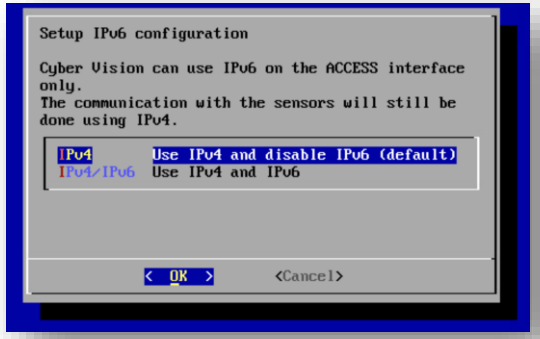
Single or Dual interface selection during install

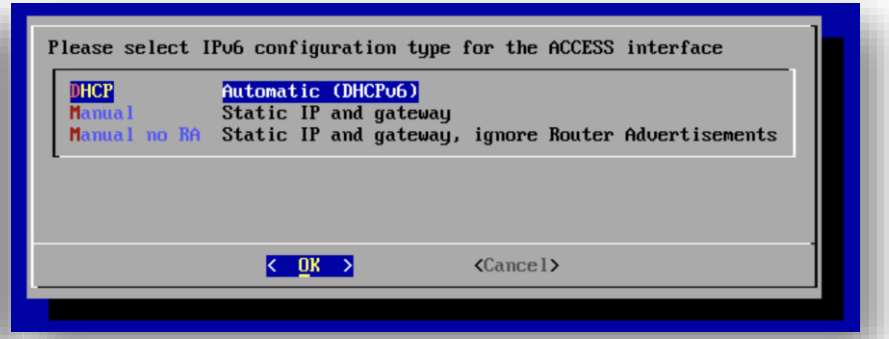


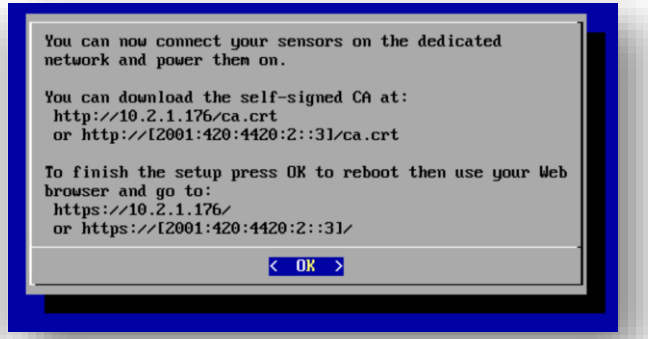
IPv6 – Support for Administrative Services [1/2]

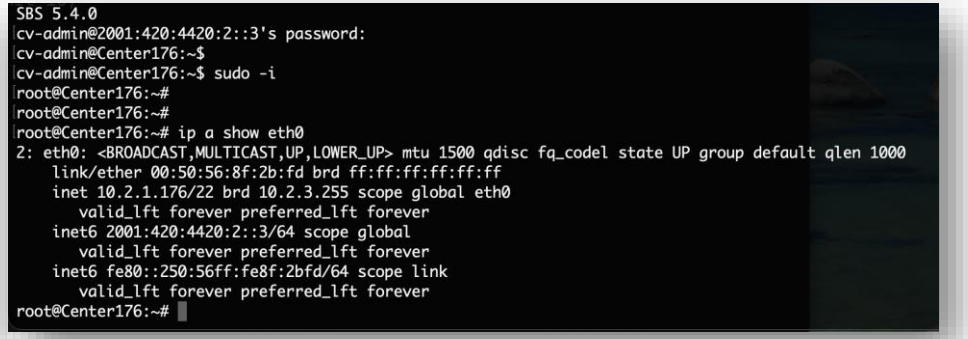
With v5.4 IPv6 support has been added for all administrative services of the center:
Web-UI, Integrations (syslog, ISE, LDAP), Licensing (direct):

IPv6 configuration during installation:





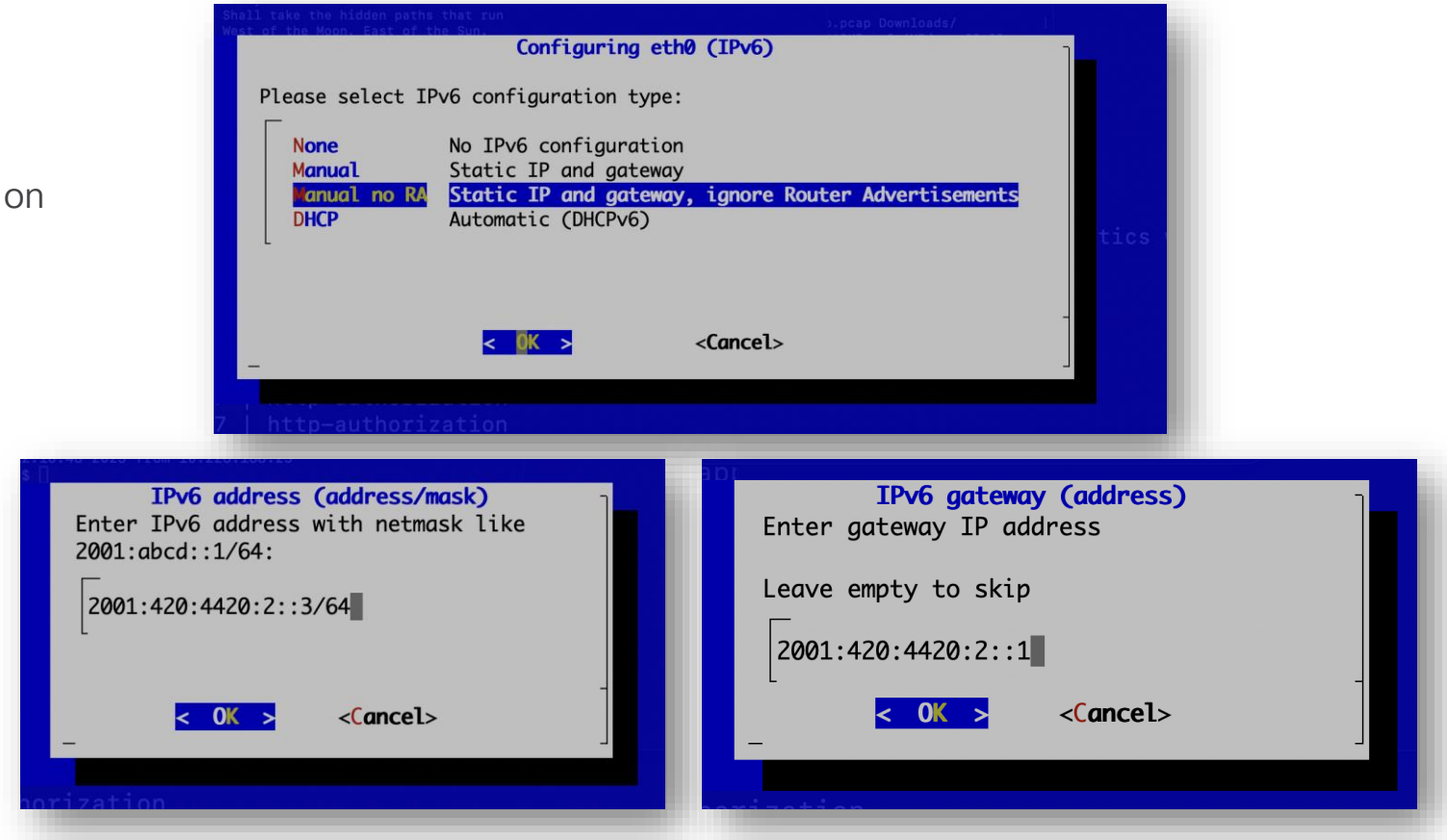




IPv6 – Support for Administrative Services [2/2]

Change Center IP configuration post-installation

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



On Center DPI and IDS

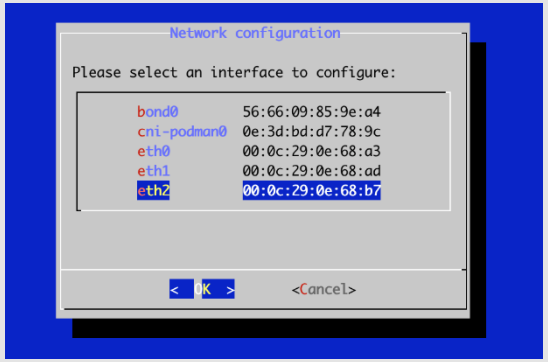
 # To enable DPI / IDS on Center interface(s):

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

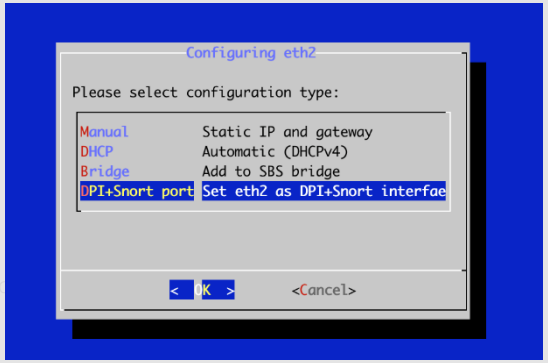
2) Type sbs-netconf command to enter interface setup

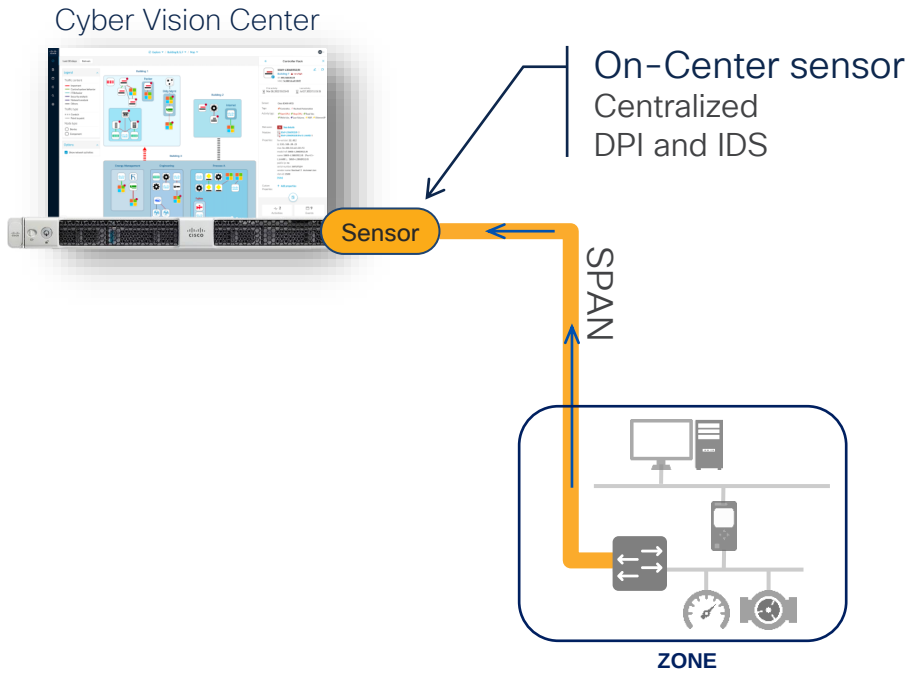
root@Center# sbs-netconf

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



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

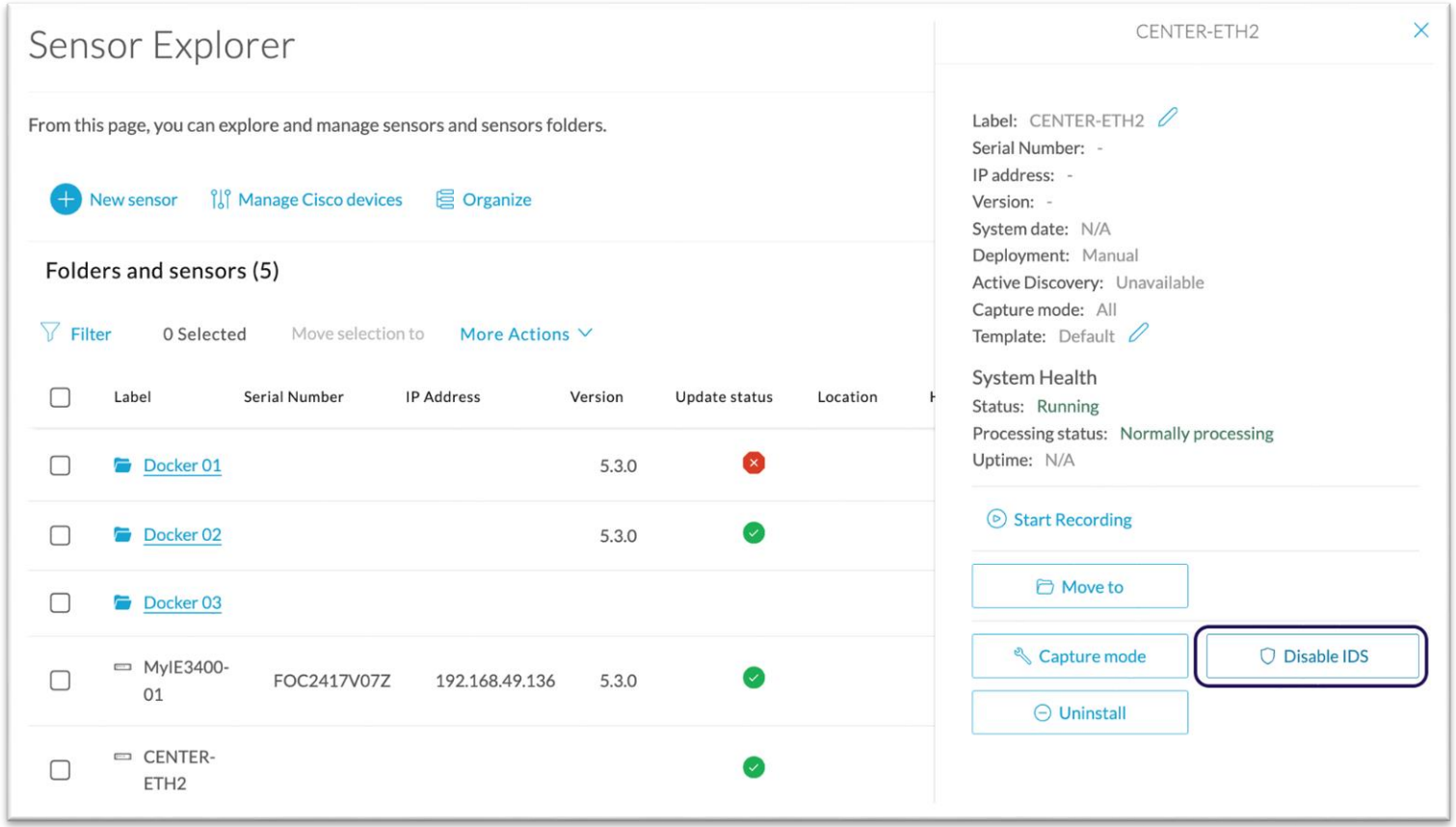




- Supports up to 4 physical interfaces max with 1 Gbps per interface
- 300,000 pps

Disabling IDS on Center Interface

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



Ports and Protocols

Access interface

To Center:
HTTPS: TCP port 443
SSH: TCP port 22
From Center:
Syslog: UDP/TCP port 514
Chrony/NTP: UDP port 123

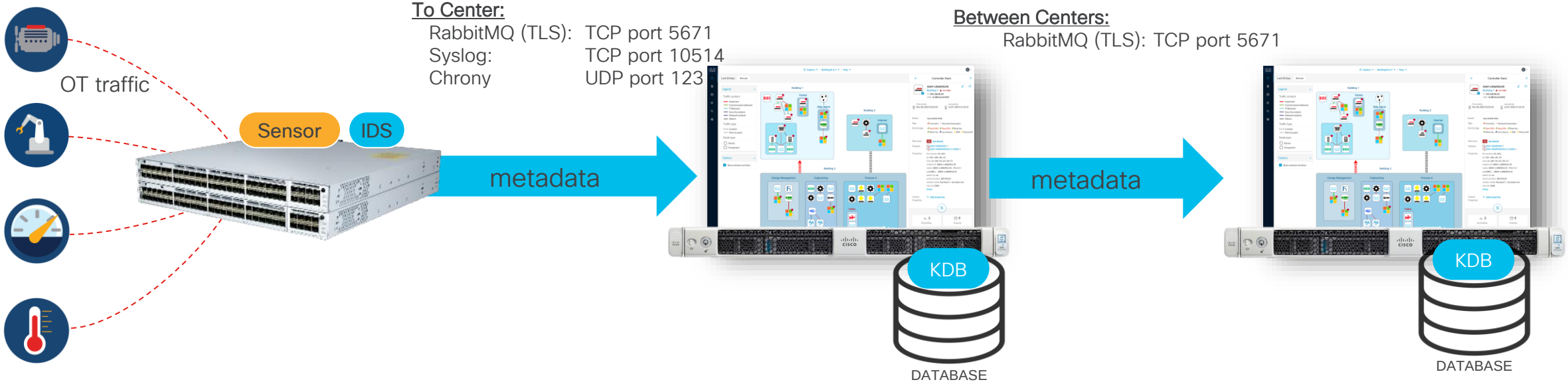
OT devices | Sensors | Cyber Vision Center | Cyber Vision Global Center

Collection interface

To Center:
RabbitMQ (TLS): TCP port 5671
Syslog: TCP port 10514
Chrony UDP port 123

Center to Global Center

Between Centers:
RabbitMQ (TLS): TCP port 5671



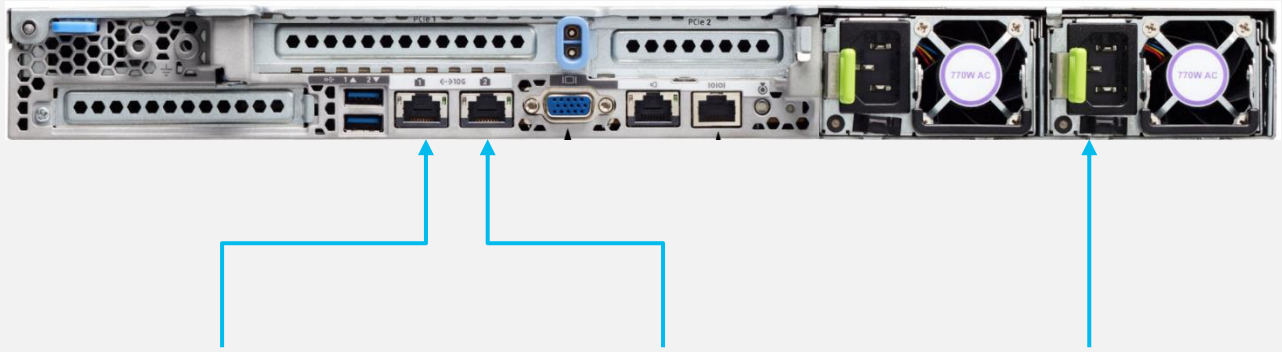
For more details, please refer to the Cyber Vision Architecture Guide available on https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html#Design

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

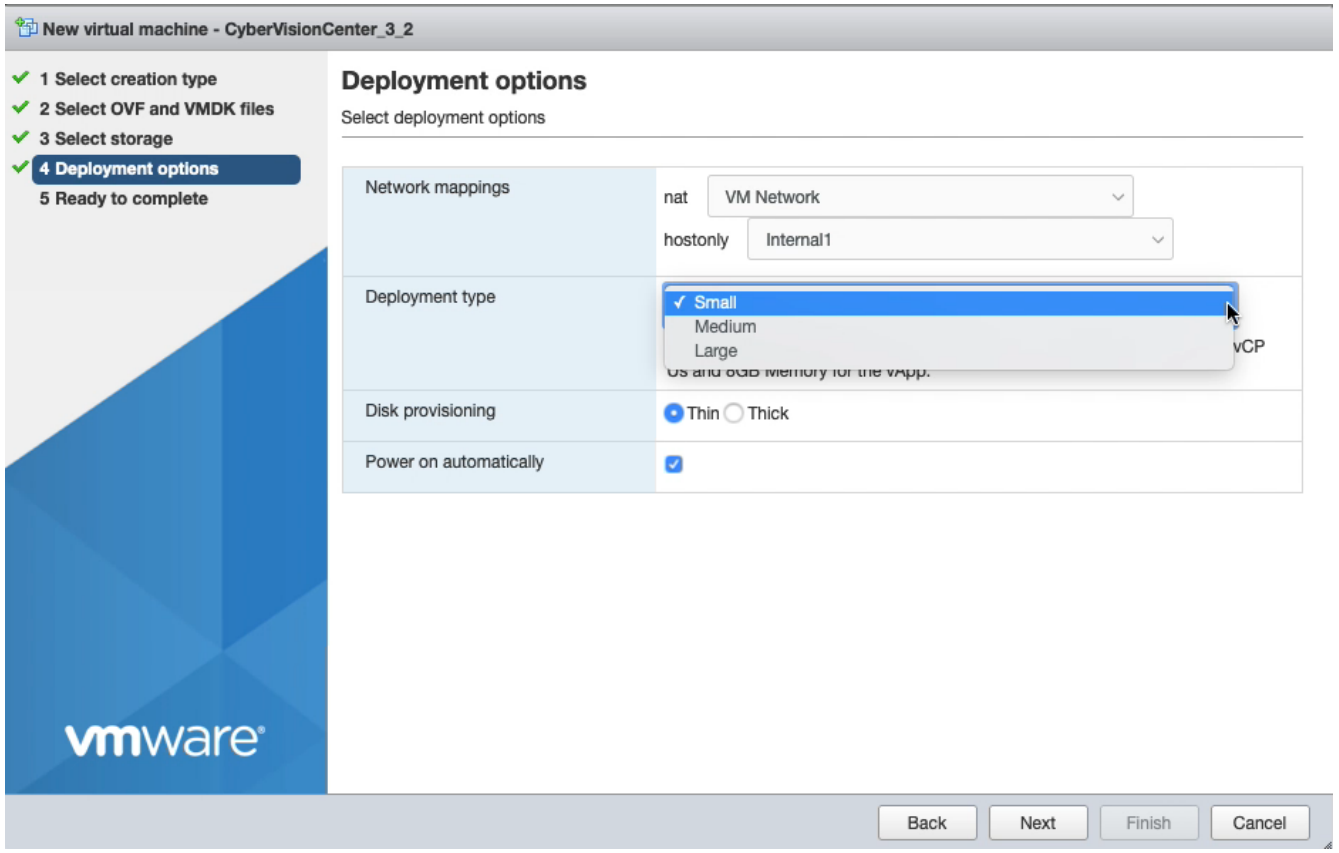
- PCIe Card – **Choose 1 card MAX**
  - UCSC-PCIE-IRJ45=
    - 4x 1 Gigabit Ethernet Copper (RJ45) Interfaces
  - UCSC- P-ID10GC=
    - 2x 10 Gigabit Ethernet Interfaces – RJ45*
  - UCSC-PCIE-ID10GF=
    - 2x 10 Gigabit Ethernet Interfaces – SFP+*
  - UCSC-PCIE-IQ10GF=
    - 4x 10 Gigabit Ethernet Interfaces – 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

amazon web services

Microsoft Azure

Google Cloud Platform

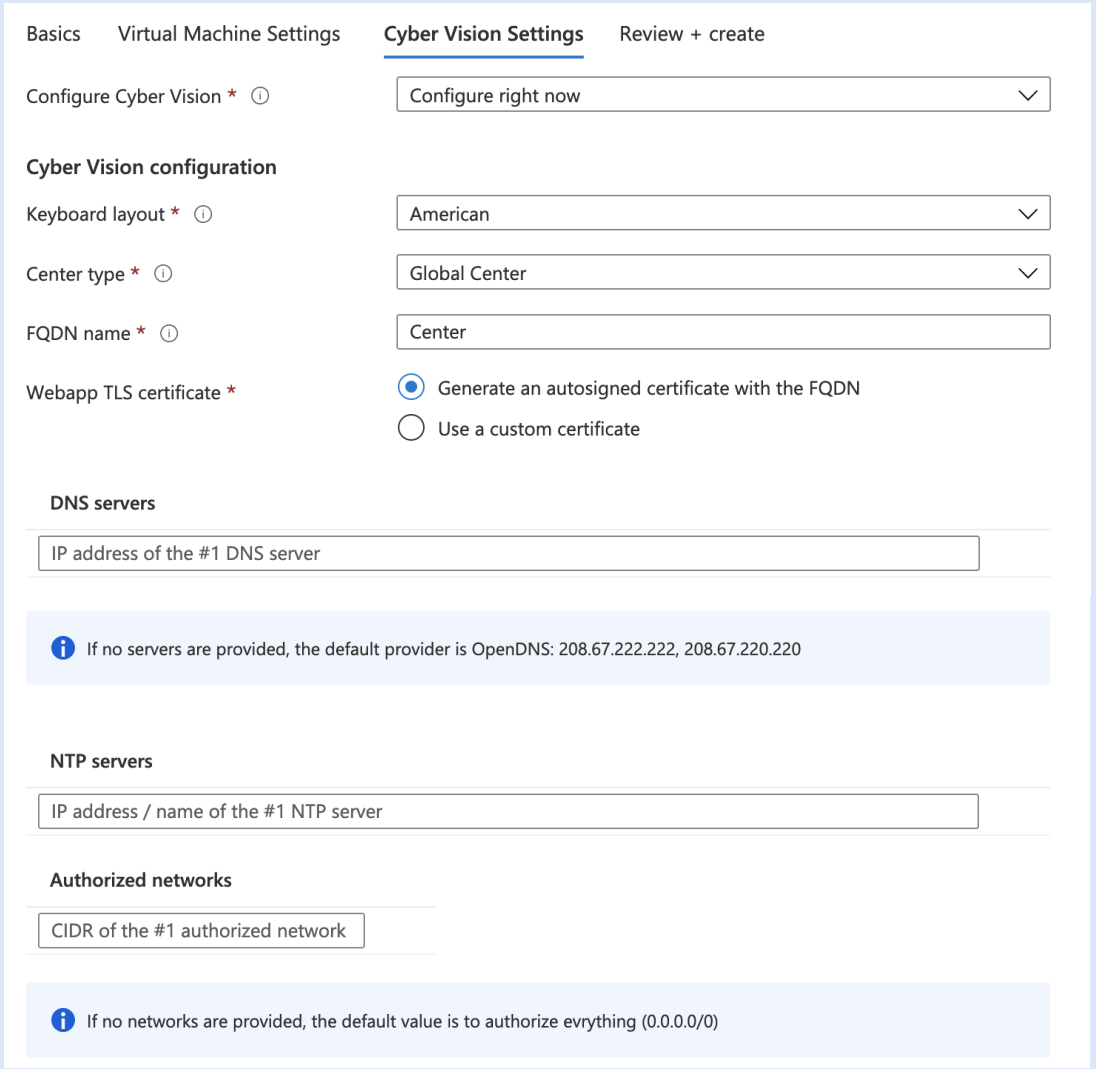
No hardware to install or maintain

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"
    }
```



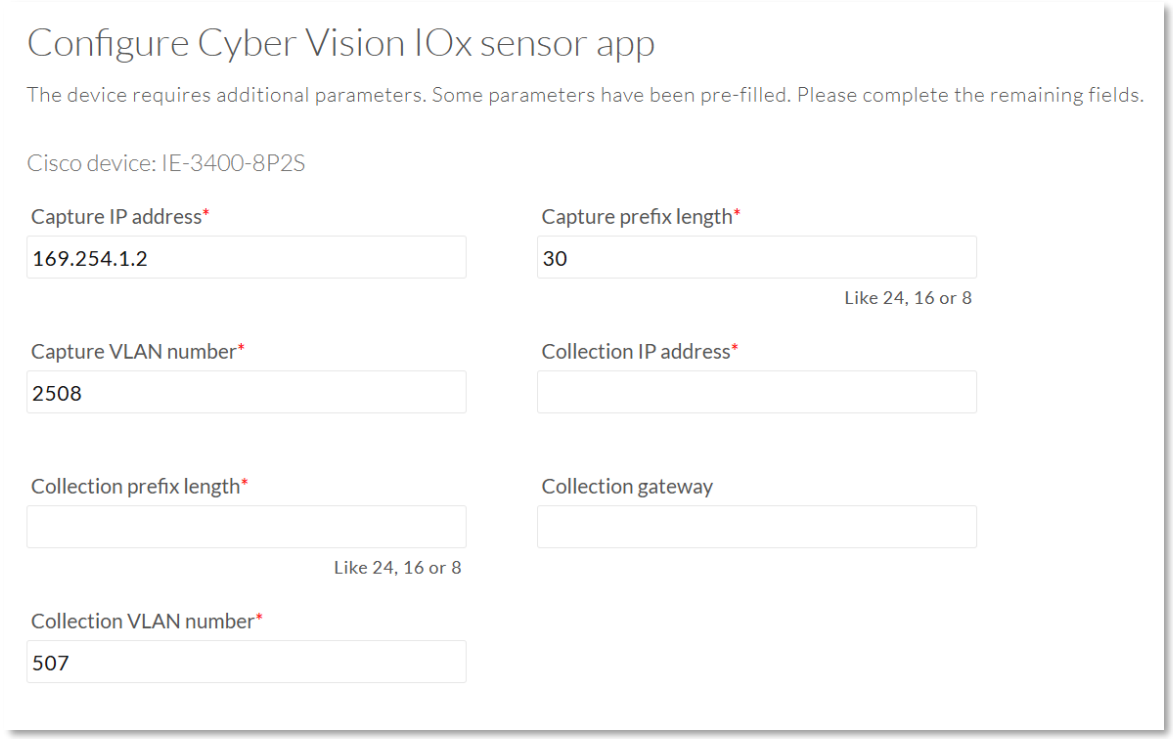
Cyber Vision FIPS Compliance

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

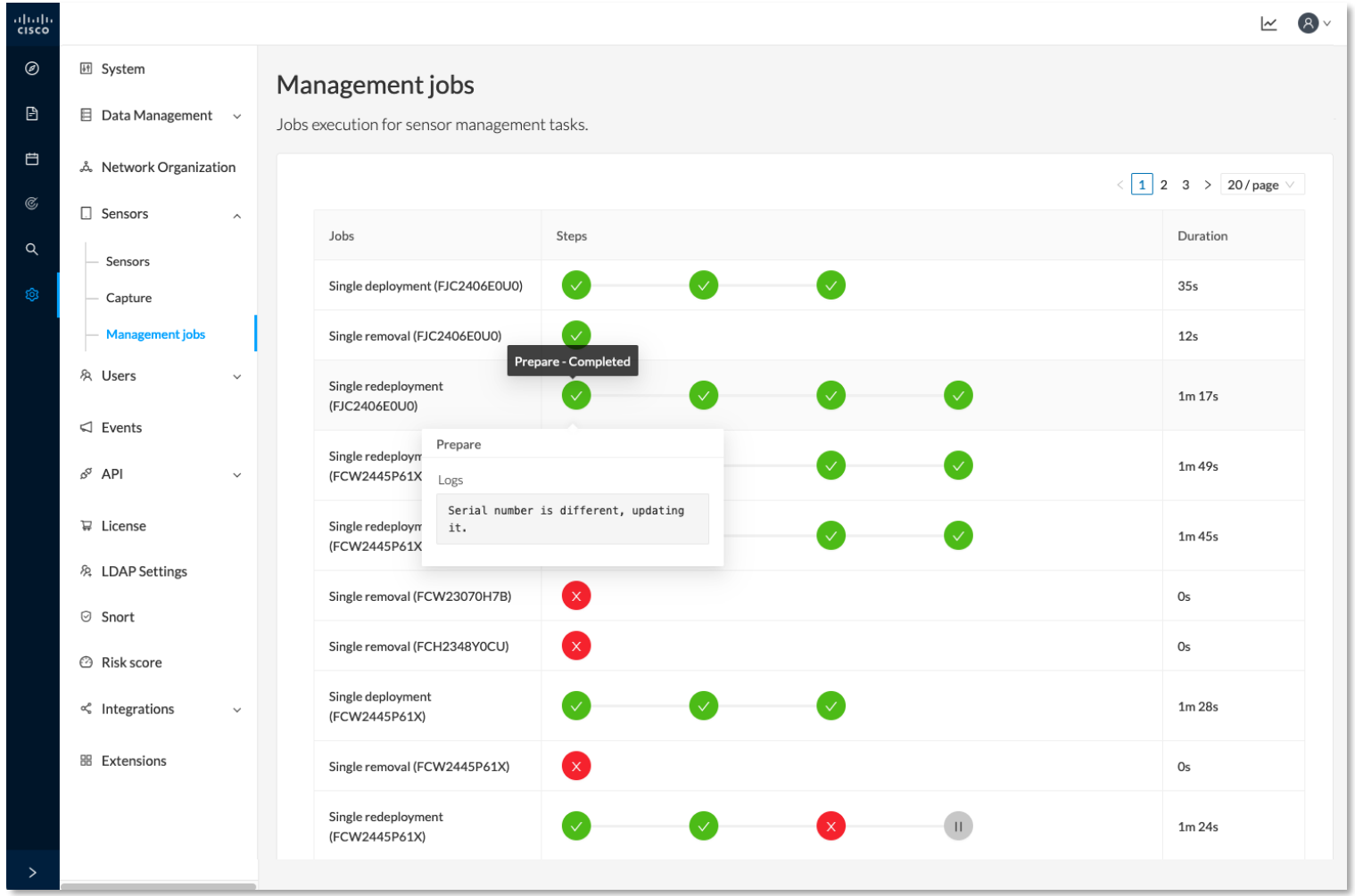


Sensors can easily be installed, configured and managed centrally from the Cyber Vision Center using the sensor management extension.

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)

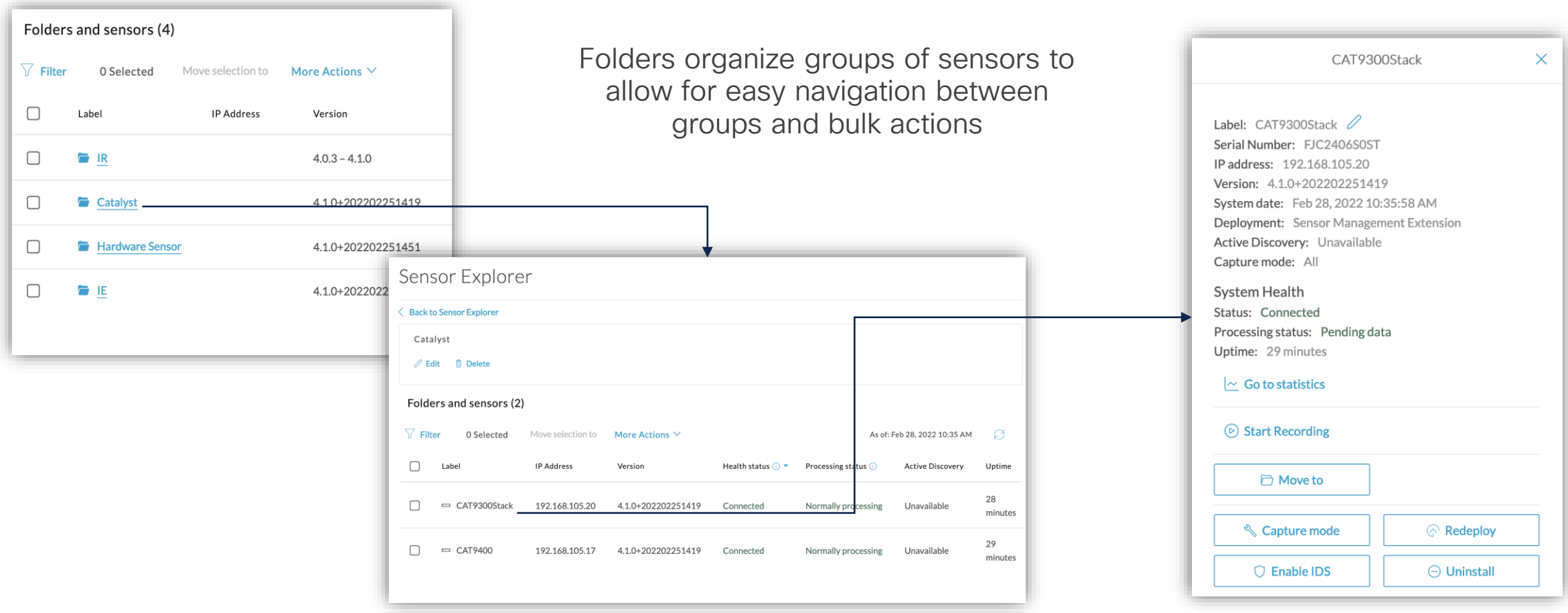
Simplifying sensor deployments



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

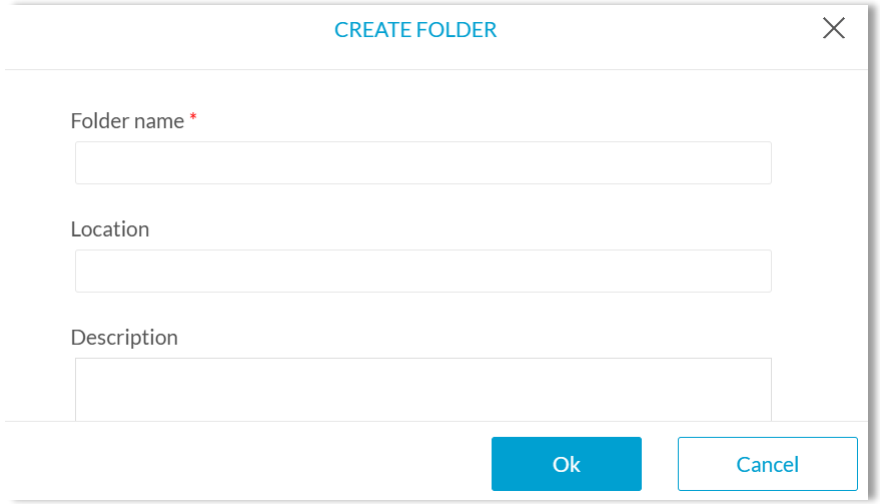
Sensor Explorer enables sensor management at scale

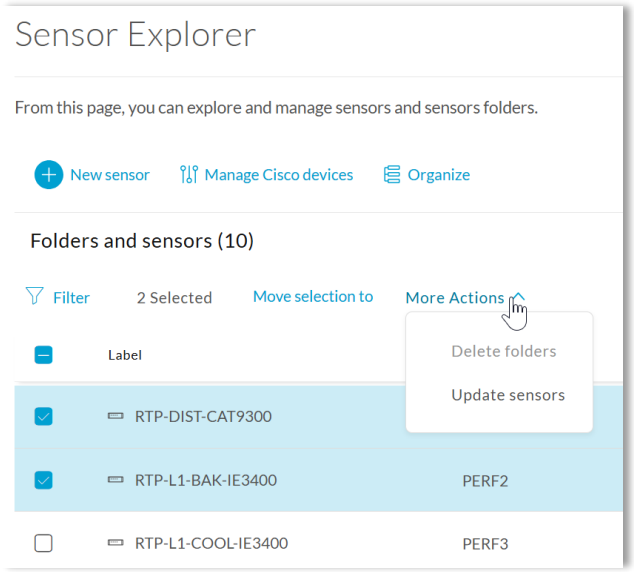
Folders organize groups of sensors to allow for easy navigation between groups and bulk actions

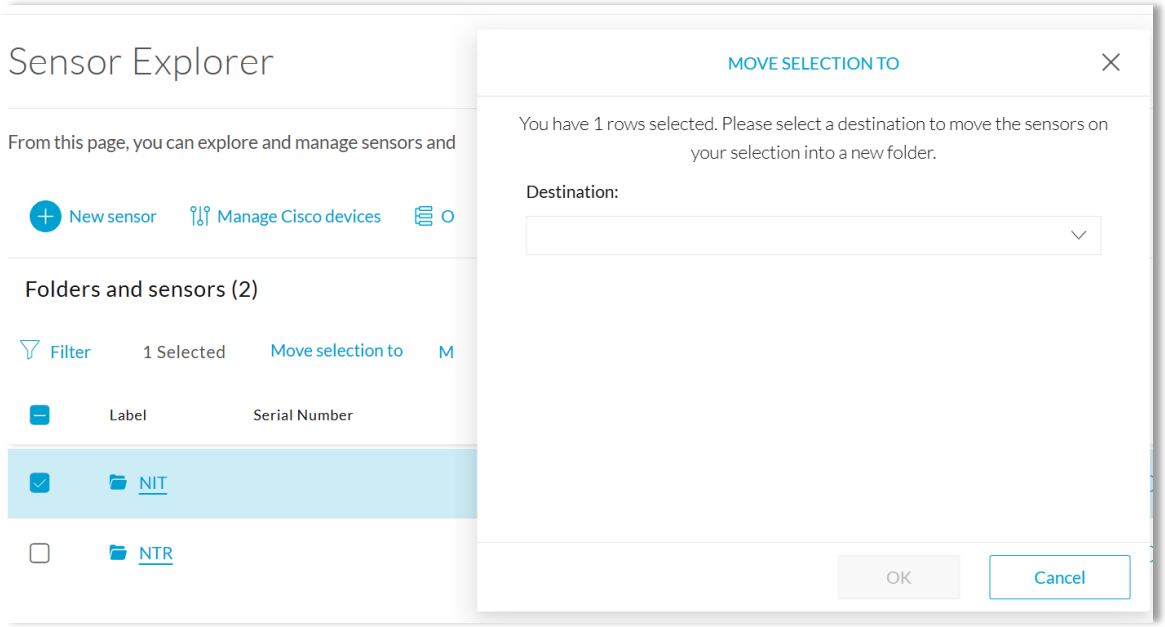


Bulk Sensor Actions

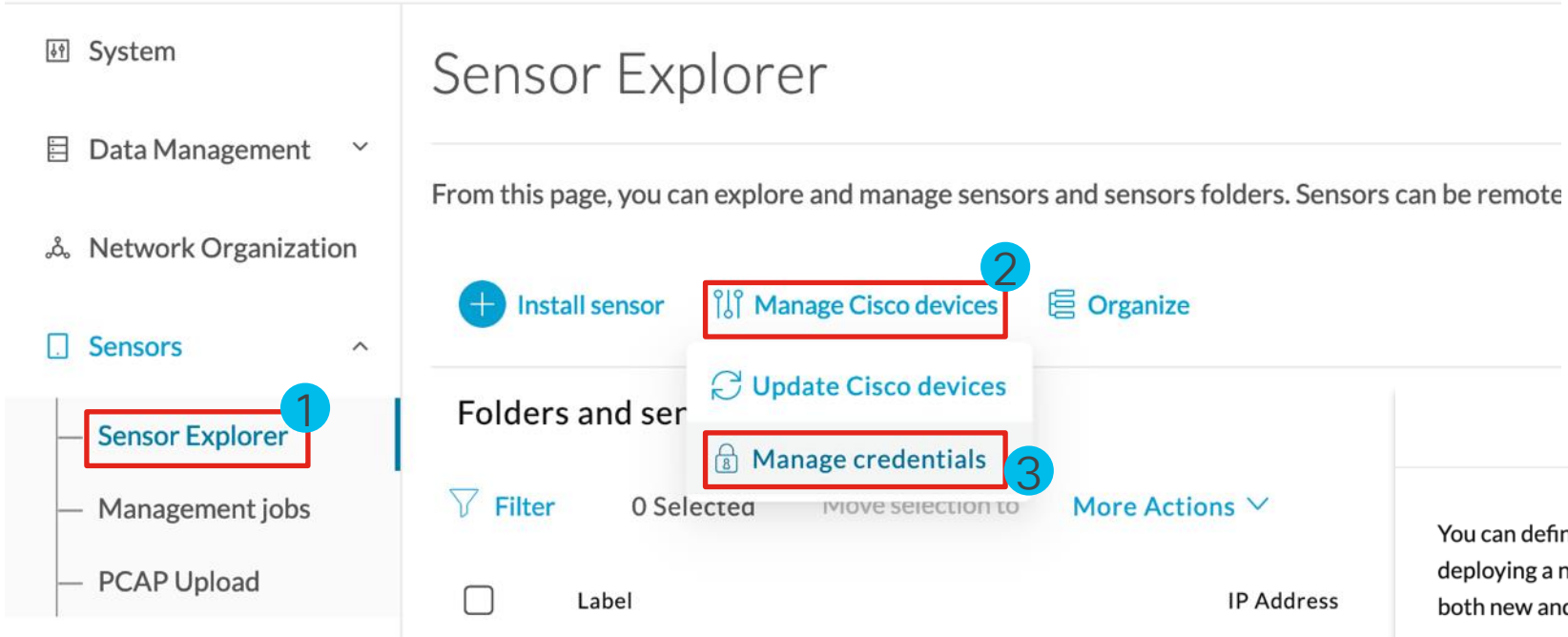
- Filter on sensors list
- Create folders to group sensors
- Move sensors to folders
- Delete folders

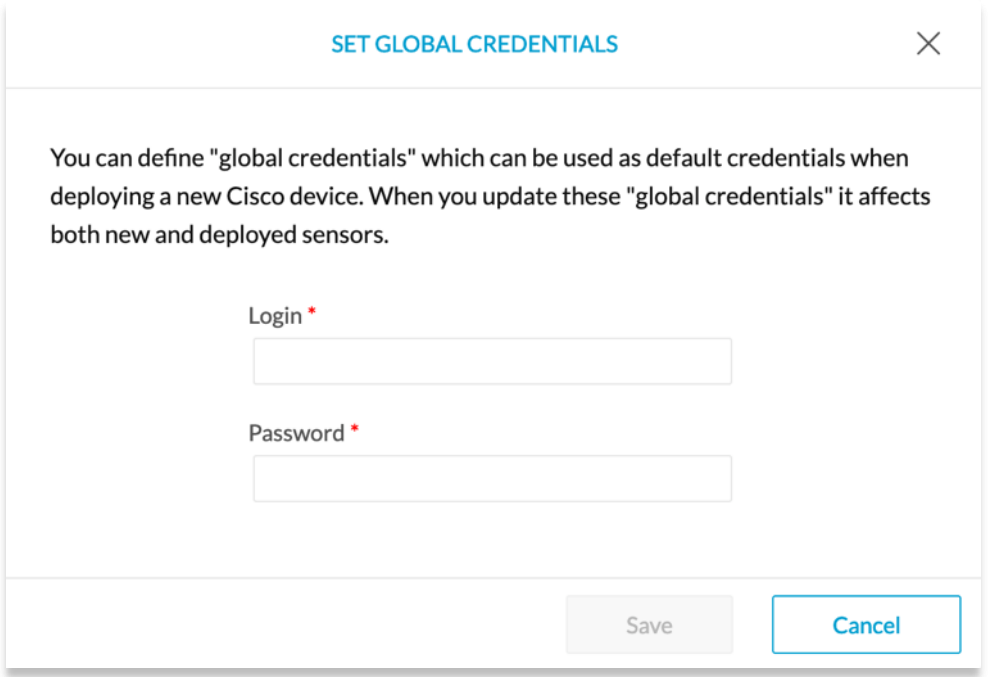






Global credentials

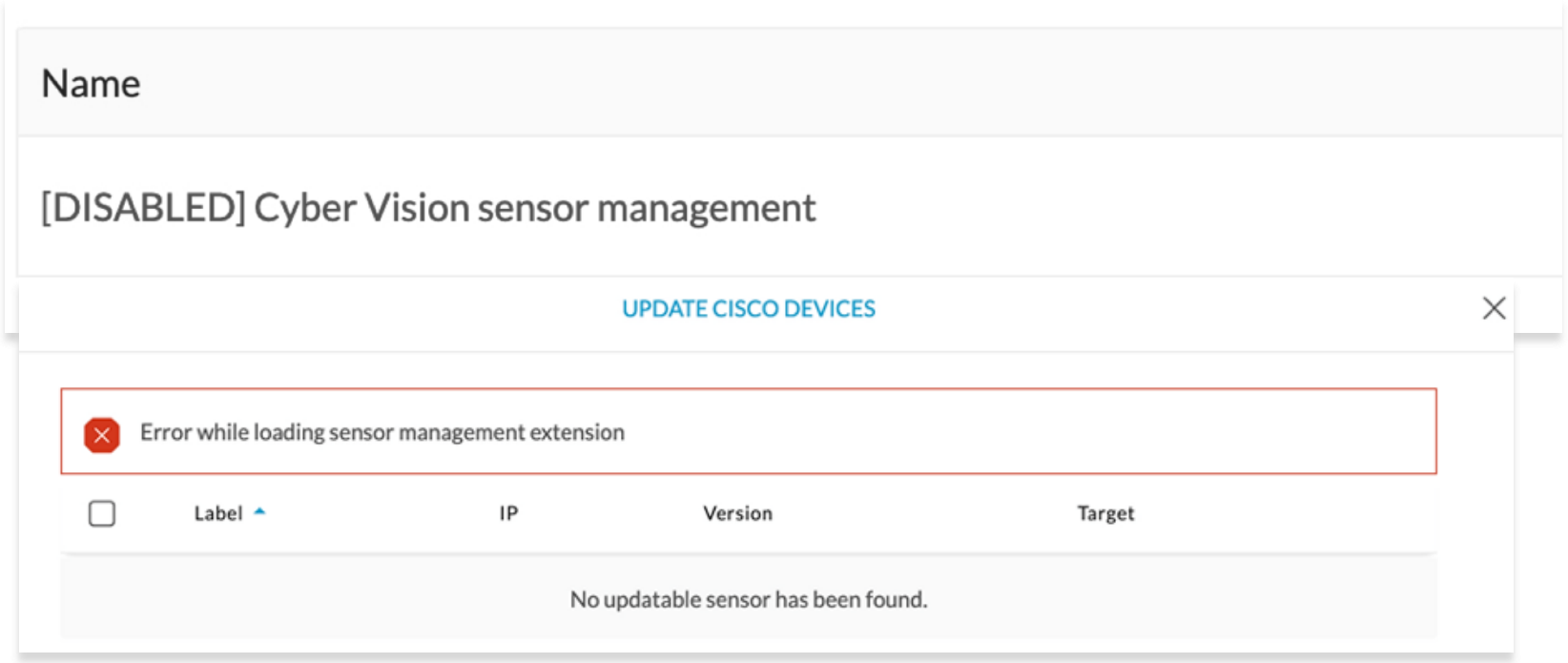




CLI to disable Sensor Management Extension

- 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
```



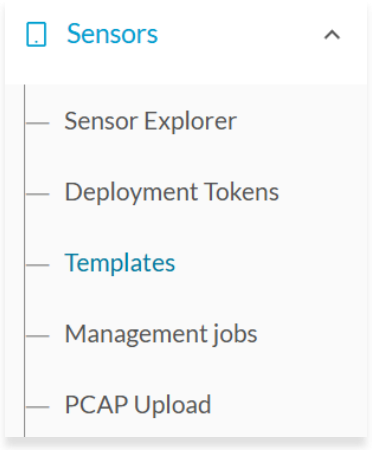
CLI to enable Sensor Management Extension

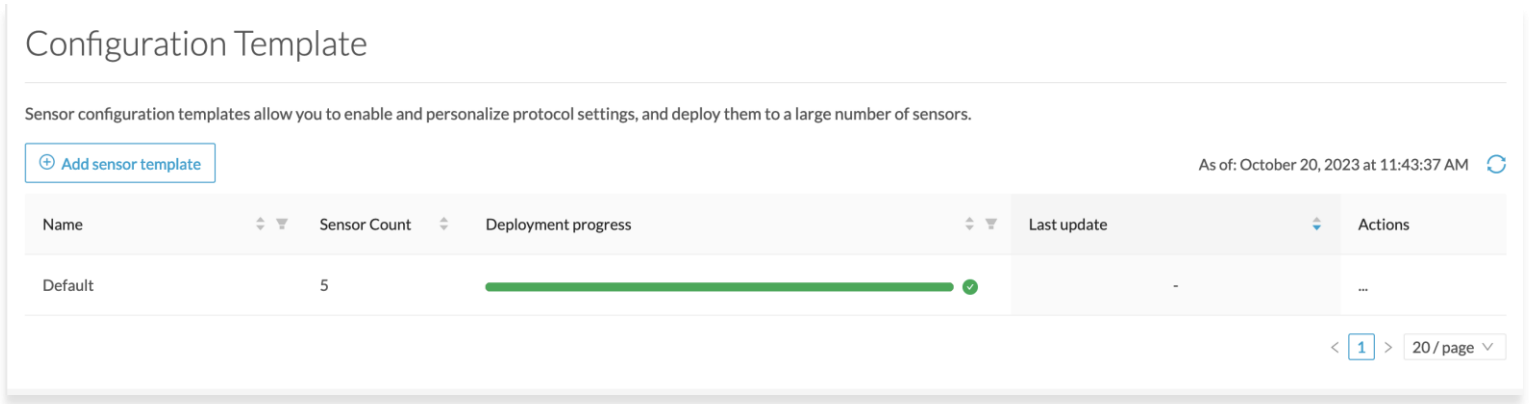
- Start sensor management extension from CLI

```
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

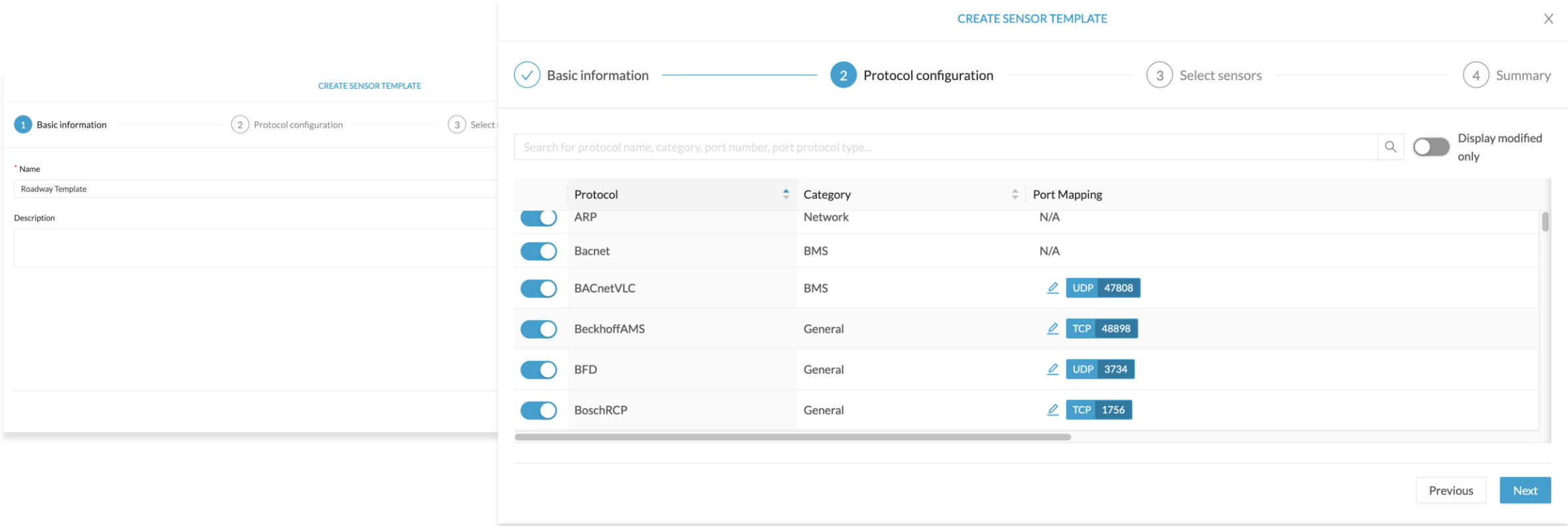
- Simplifies configuration of multiple sensors across the infrastructure
  - Easily configure protocols and ports to use
- Default template assigned to all sensors at first
  - Can have multiple templates
- See status of template deployments





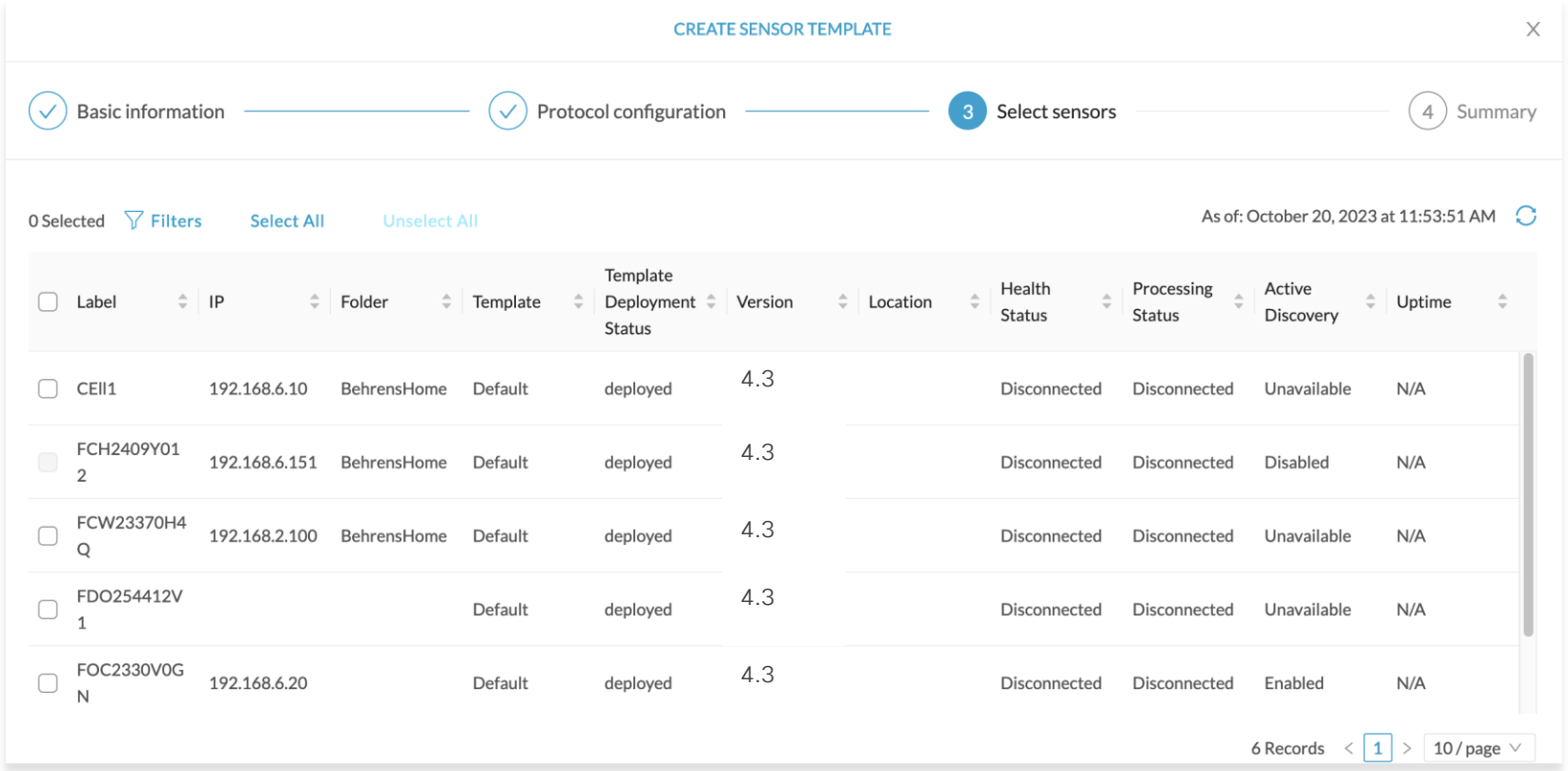
Sensor Configuration Template Wizard

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



Sensor Configuration Template Wizard

- Selectively deploy to a single sensor or multiple sensors

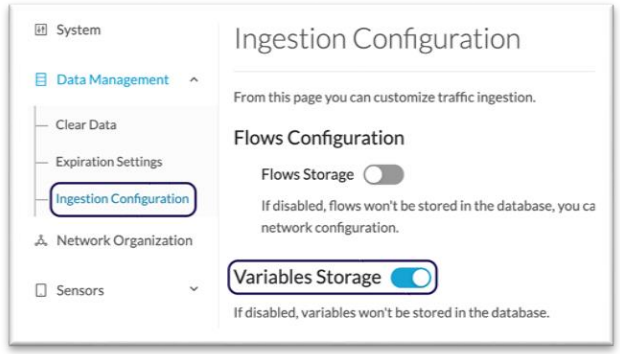


Sensor Configuration Template Wizard

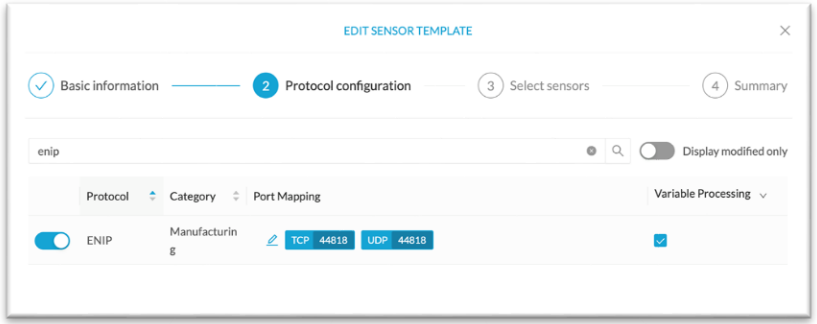
Note: Variable processing is disabled by default in release v5.3.0

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

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

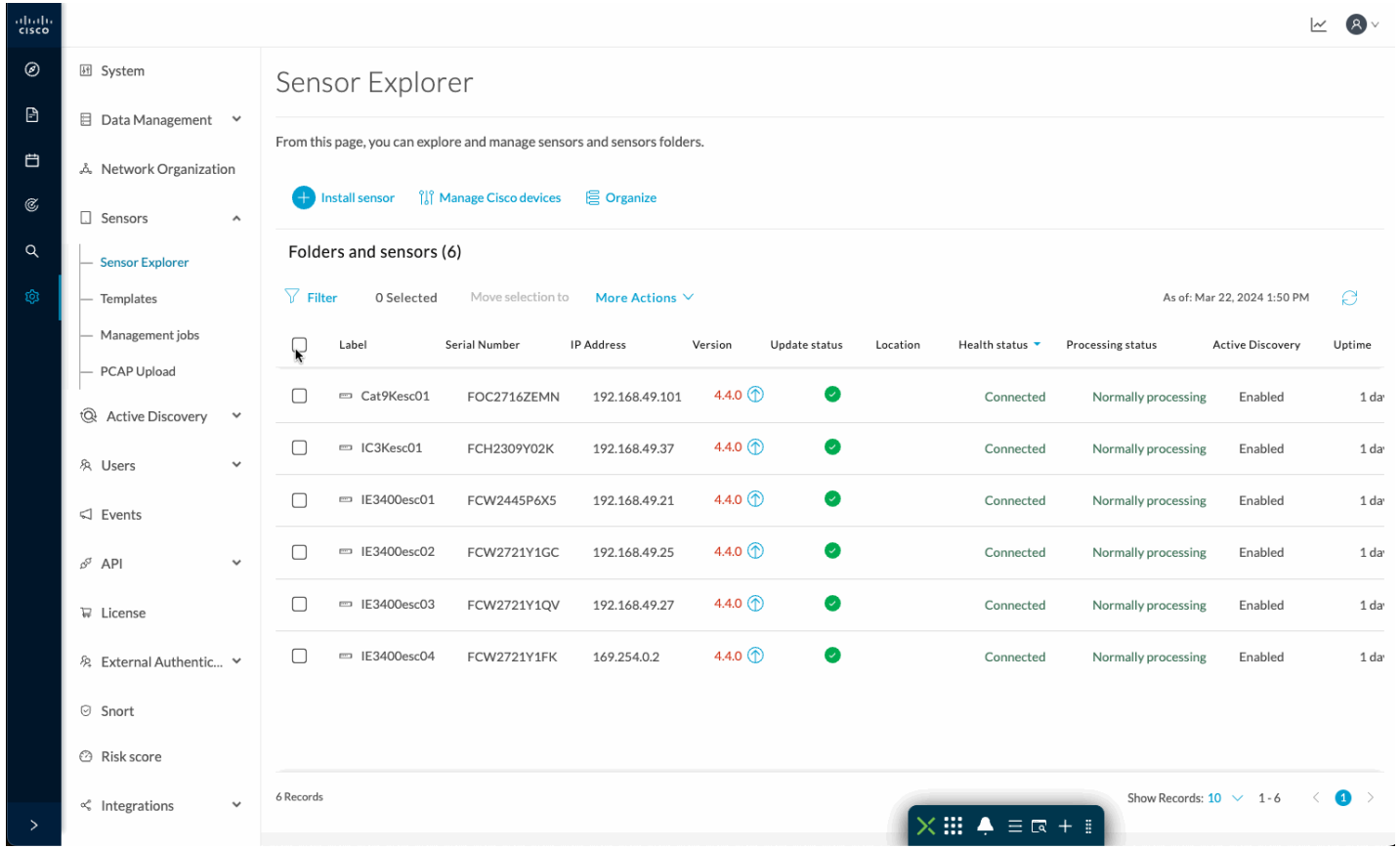


2) Activate the “Variable Processing” for each protocol in the sensor template



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



Certificate renewal enhancement for Sensors

Automated sensor certificate renewal

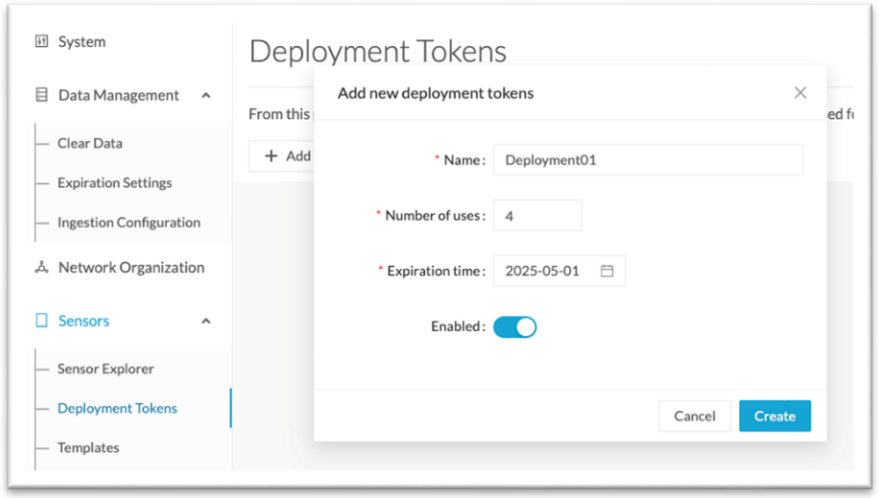
- 35 days before certificate expiration date, system will attempt to renew it automatically
- Renewal is done on center side and new provisioning package is automatically sent to sensor

- 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

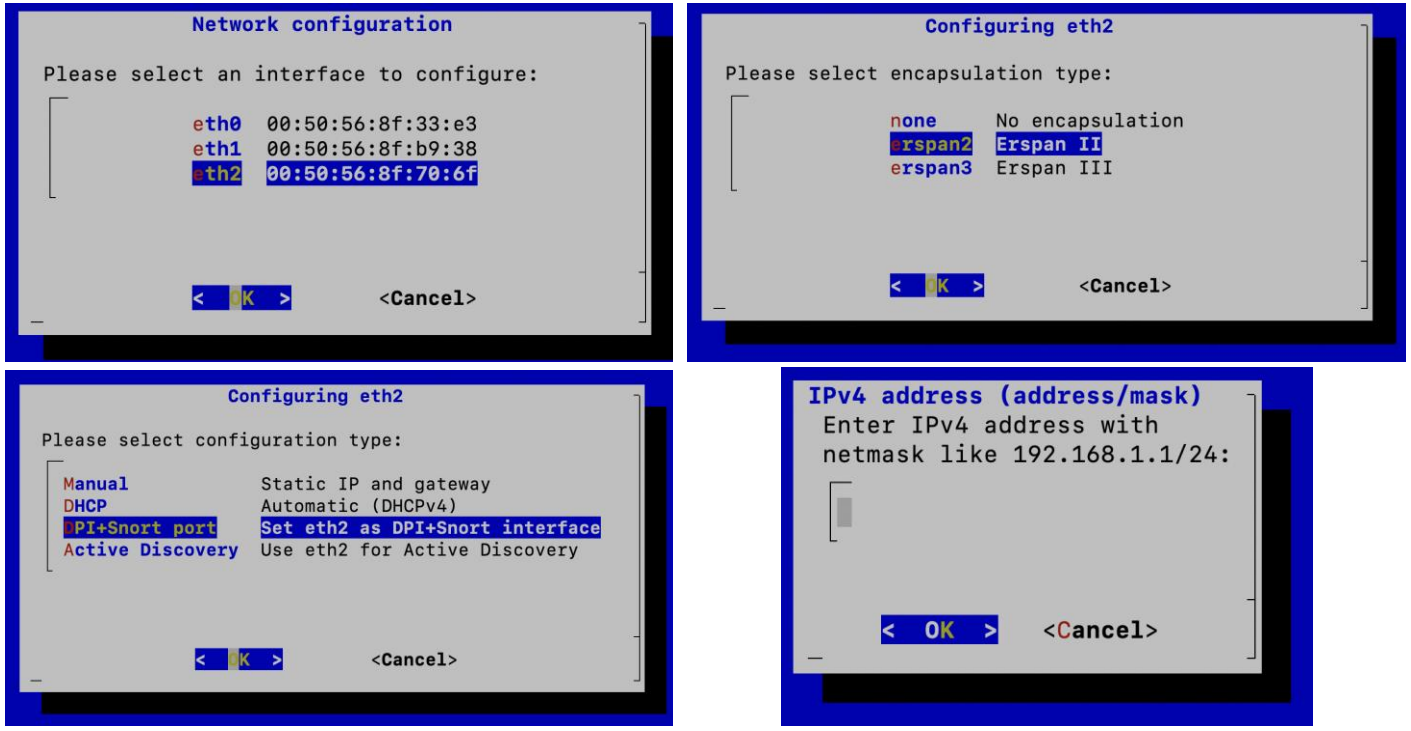


Name	Tokens		Status	Creation Date	Expiration Date	Usages
	Image	Token				
	cviox-aarch64.tar	Show				
	cviox-active-discovery-aarch64.tar	Show				
Deployment01	cviox-active-discovery-ic3000-x86-64.tar	Show	Enabled	May 27, 2024	May 1, 2025	0/4
	cviox-active-discovery-x86-64.tar	Show				
	cviox-ic3000-x86-64.tar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

ERSPAN Support on Center DPI Interface

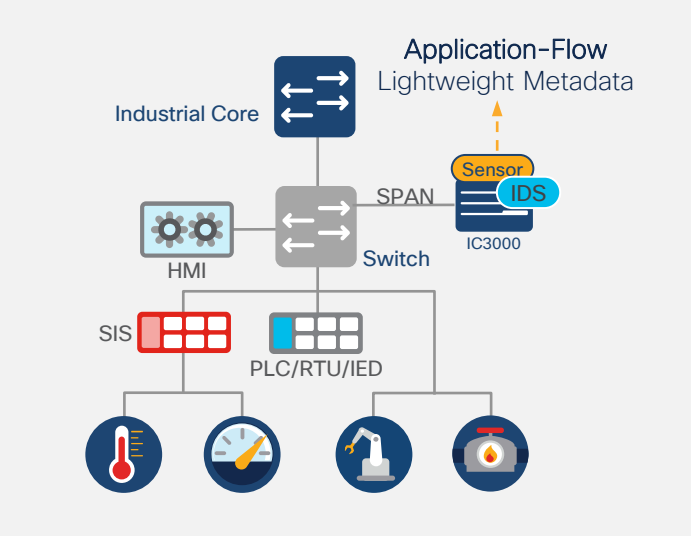
Note: In addition to the SPAN capabilities of sensors, Cyber Vision supports ERSPAN on the Center interface starting from v5.3

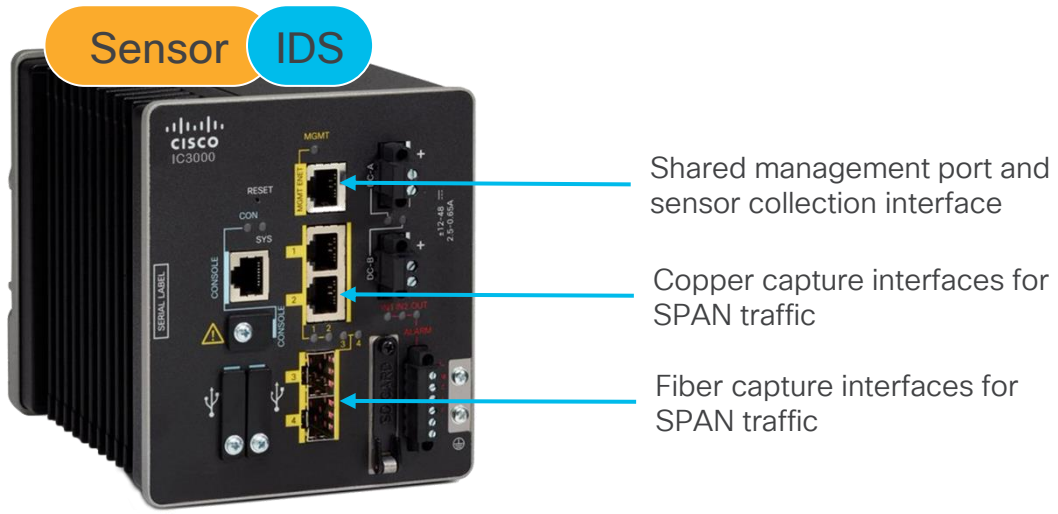
Change the network configuration using ‘sbs-netconf’ on the commandline of the center:



Cyber Vision hardware-sensor
Cisco IC3000 Industrial Compute

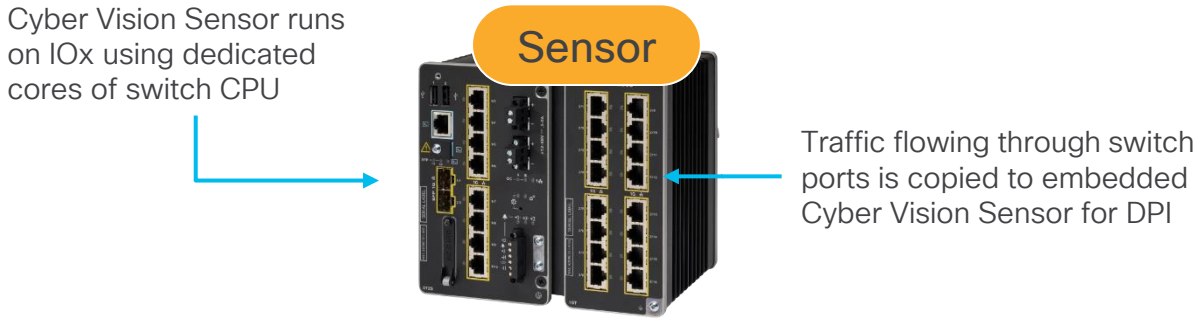
- SPAN based solution to support brownfield: traffic capture and DPI on non-Cisco switches
- Can aggregate SPAN traffic from multiple switches using the 4 capture interfaces
- Lightweight Metadata from Sensor to Center eliminates need for dedicated span network
- Supports Snort IDS with Advantage licenses (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

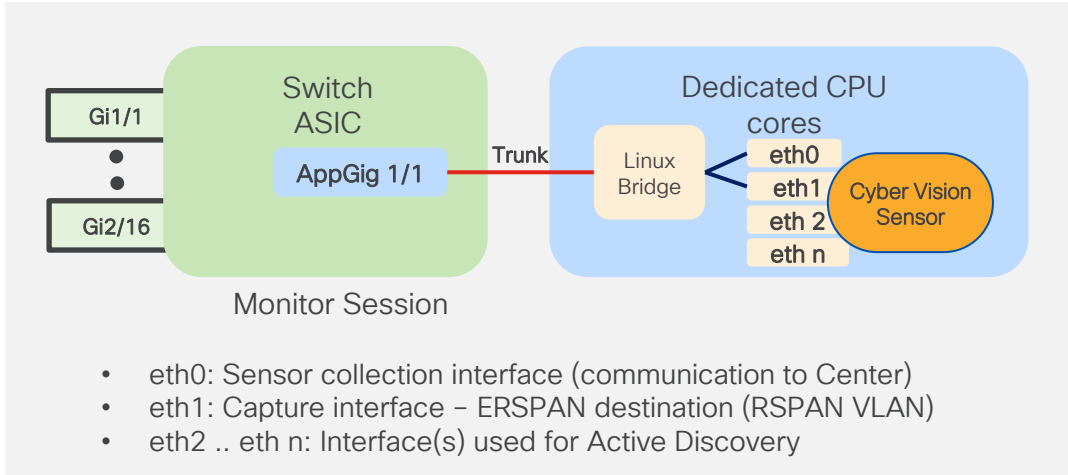




Cyber Vision network-sensor
Cisco Catalyst IE3300, IE3400, and IE3500 Rugged Series Switches

- 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





- eth0: Sensor collection interface (communication to Center)
- eth1: Capture interface – ERSPAN destination (RSPAN VLAN)
- eth2 .. eth n: Interface(s) used for Active Discovery

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

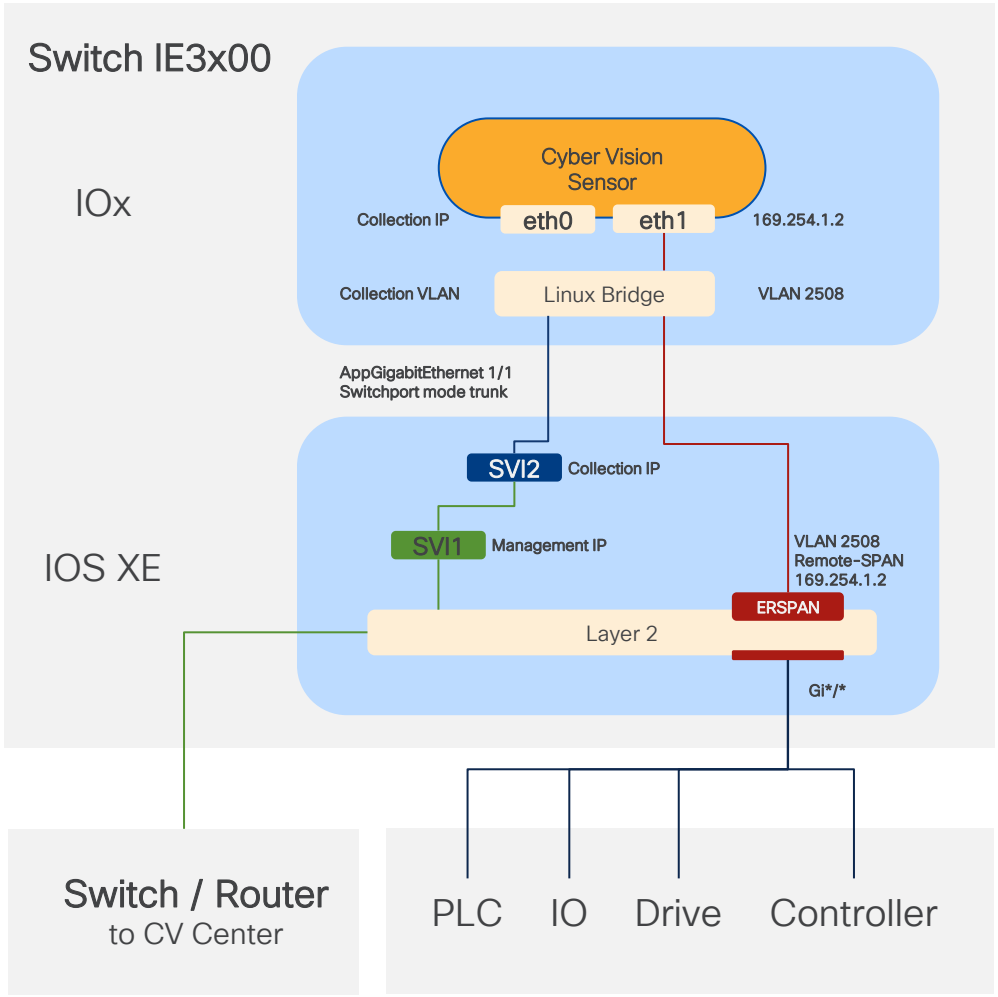
1. Create a collection VLAN (ex: 2507)

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

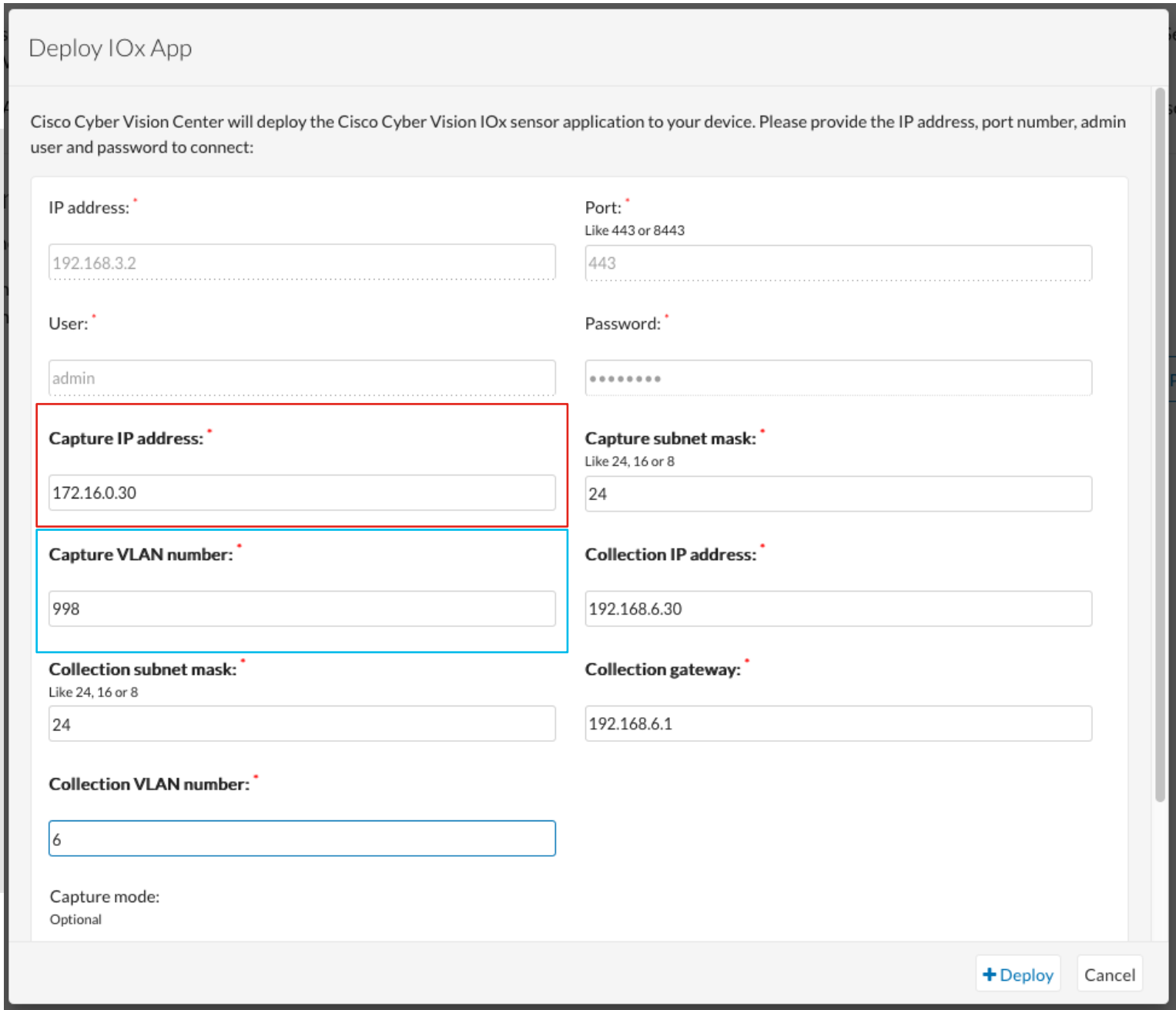
Example leveraging physical interfaces

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



IE3500 Sensor deployment – Monitoring Session

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

Configuration example:

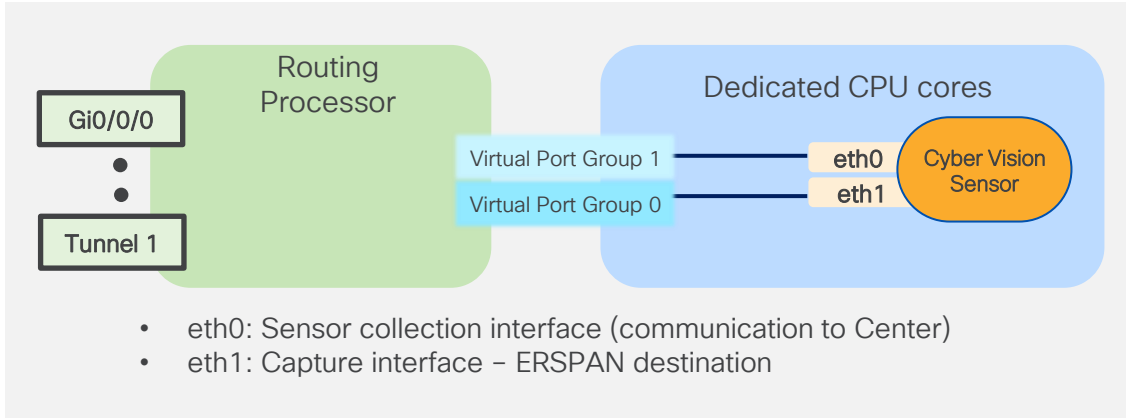
```
monitor session 1 type erspan-source
 source interface Gi1/4 , Gi1/10
 header-type 3
 destination
  erspan-id 2
  mtu 9000
  ip address 169.254.1.2
  origin ip address 169.254.1.1
```

```
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



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

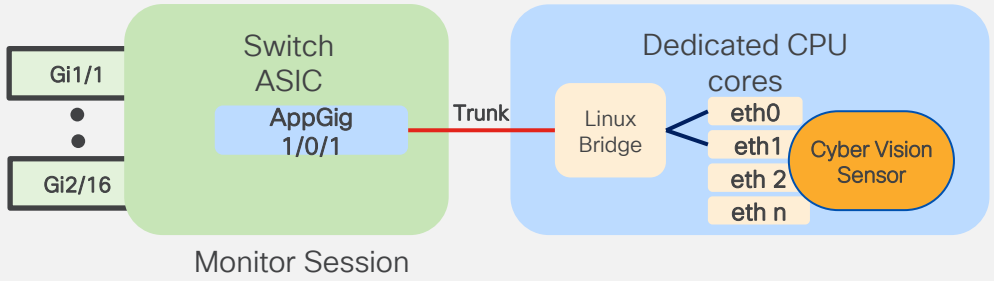
Source for ERSPAN (IR1101 Interface IP)

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

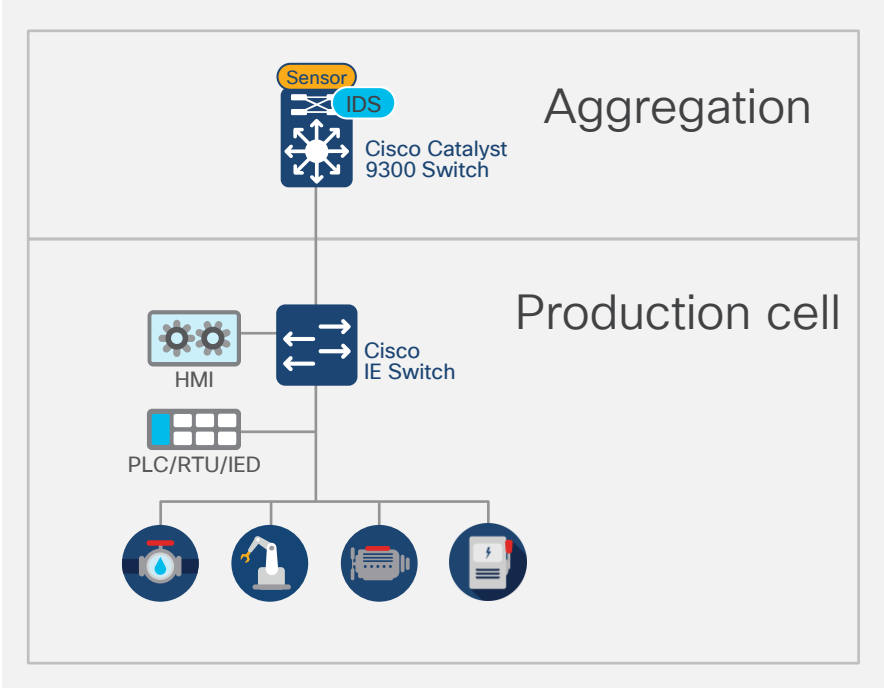


- eth0: Sensor collection interface (communication to Center)
- eth1: Capture interface – ERSPAN destination (RSPAN VLAN)
- eth2 .. eth n: Interface(s) used for Active Discovery

Cyber Vision network-sensor
Cisco Catalyst 9300/9300X/9400

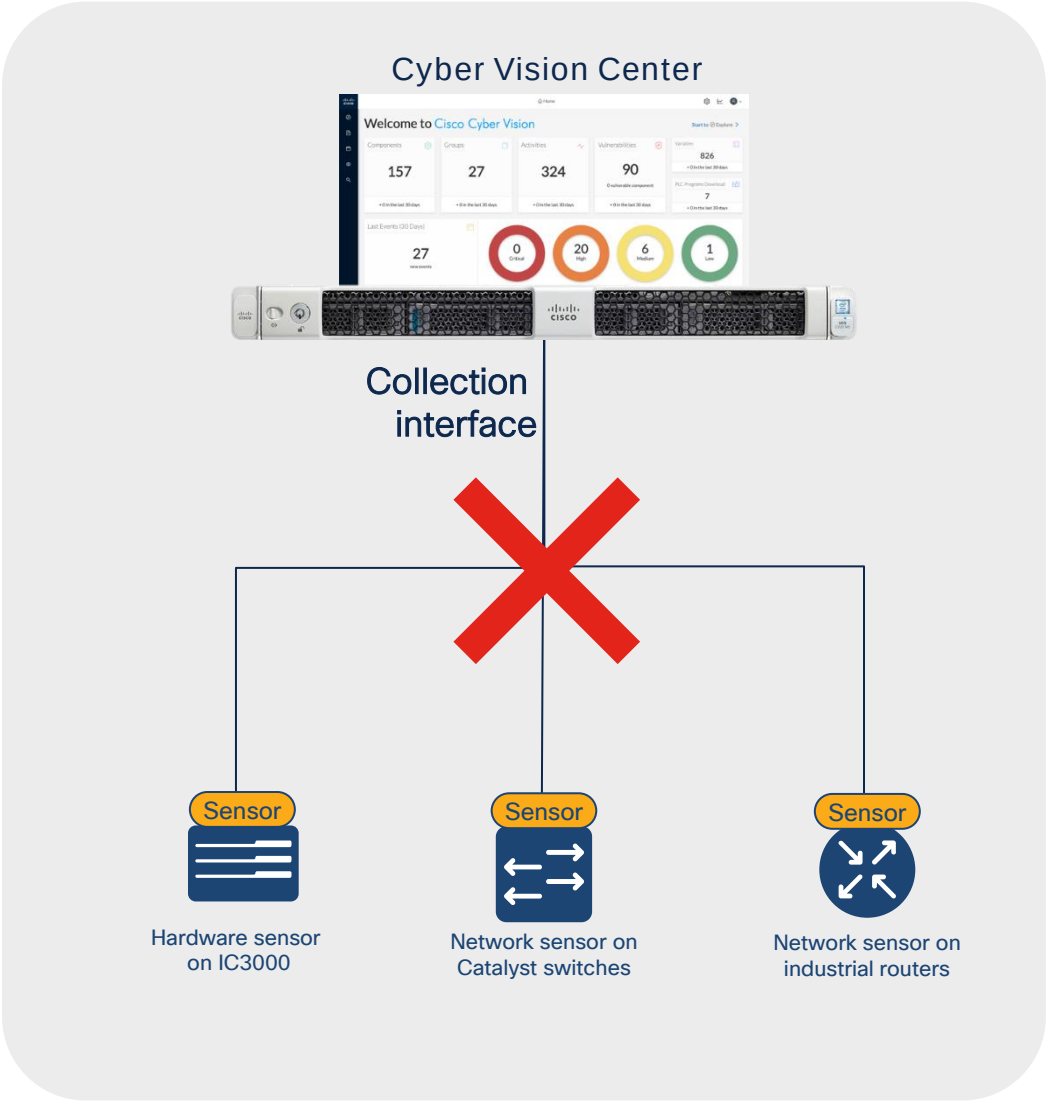
- Can be deployed as access, aggregation, core or as an out of band SPAN aggregation sensor
- Sensor is an application running in IOx
- Leverages ERSPAN to receive traffic from switch
- Supports Snort IDS with Advantage licenses (Talos subscriber rules available as an option)
- Supported PPS: see Performance 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”
```



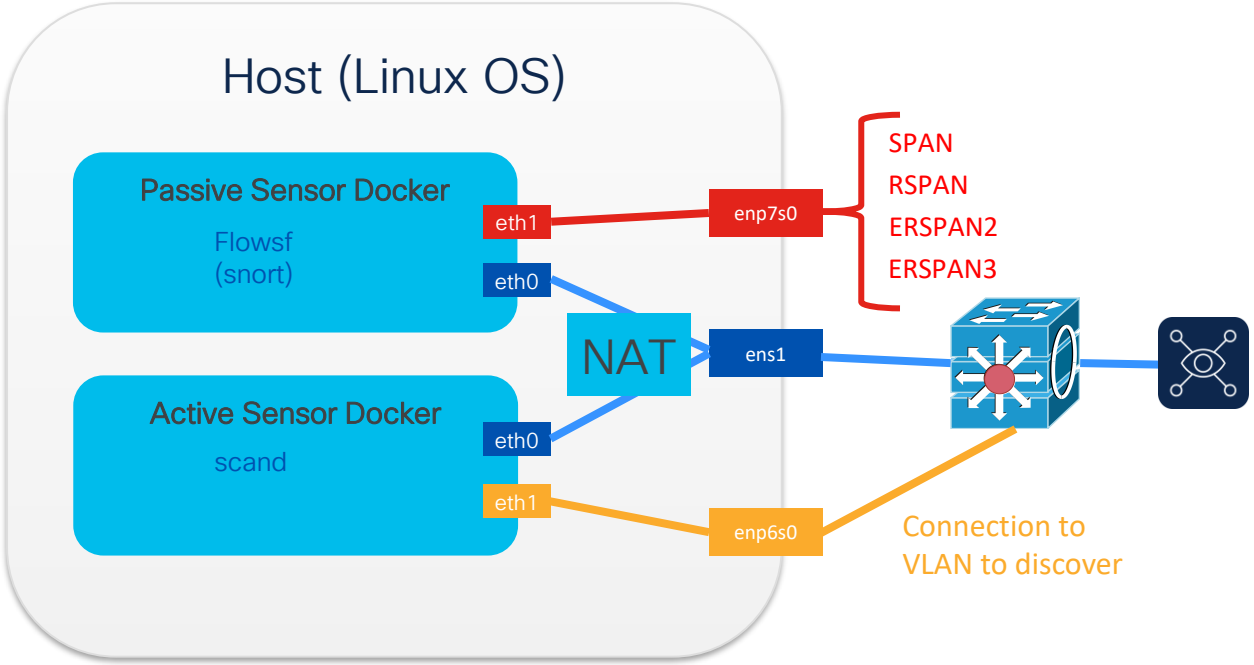
Store and Forward

- 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

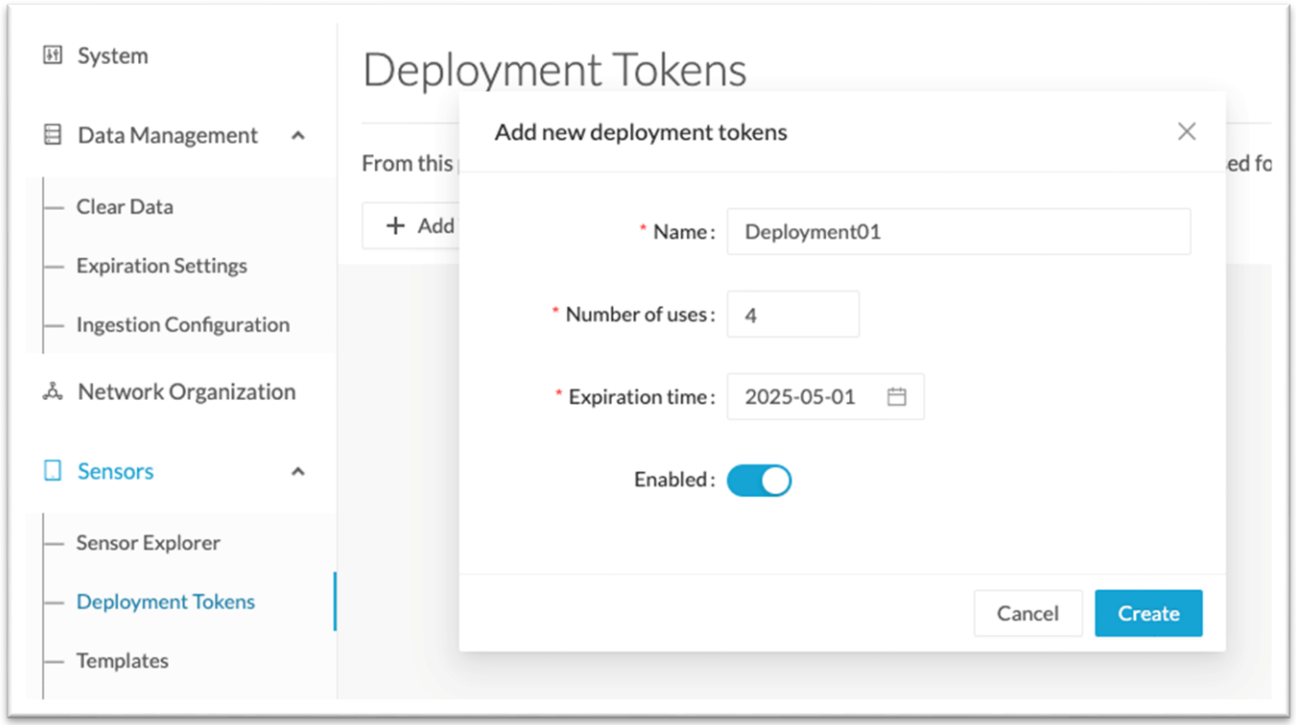
- The Cyber Vision Center is hosting a Docker registry
- After configuring the sensor, the Center will provide a docker-compose definition
- If Active Discovery is enabled, there will be two Docker instances
- Using the docker-compose definition, the sensor can be instantiated on the Docker host by pulling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

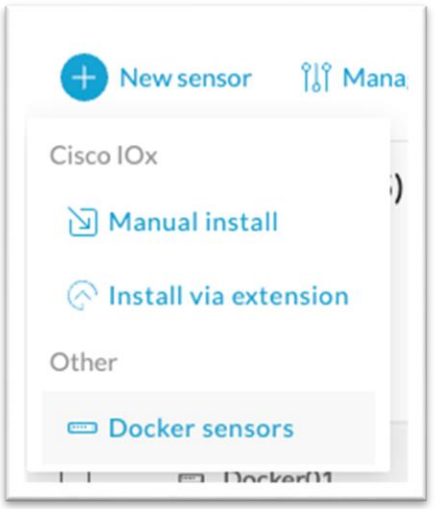
Deployment Phases:

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

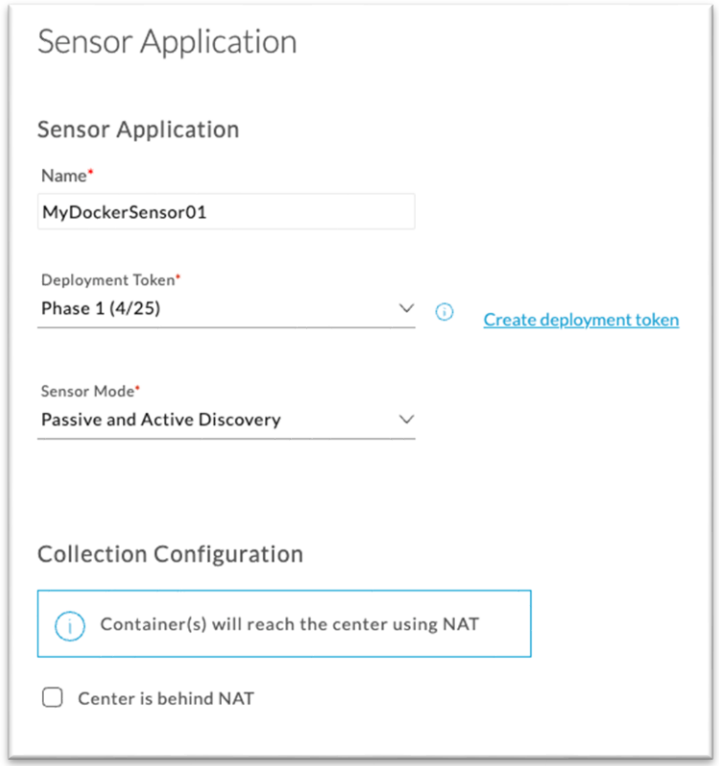
Create Deployment Token and scope its reusability across sensor deployments



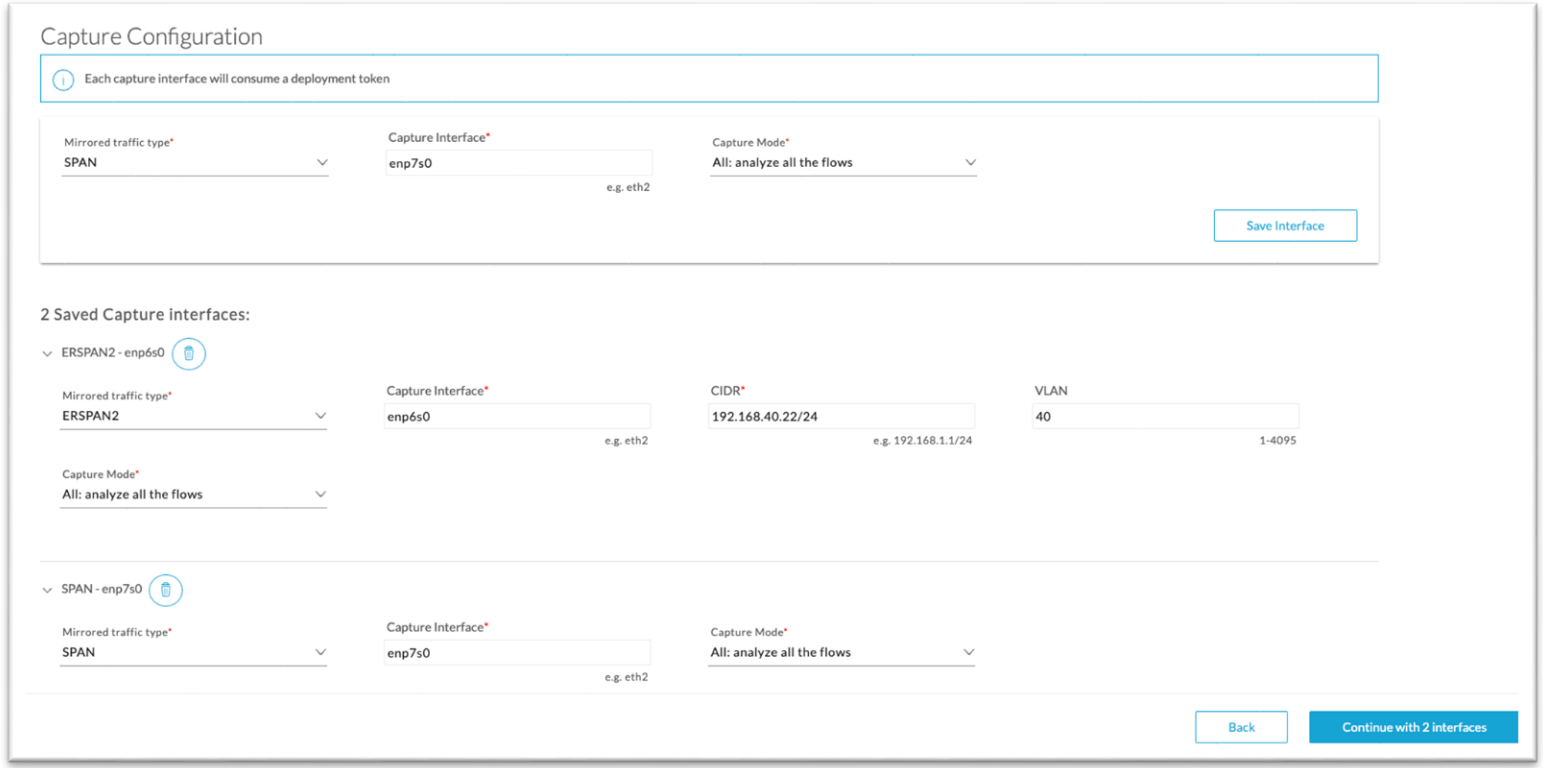


Docker Sensor – Deployment Phase 2

Configure the sensor in the Center



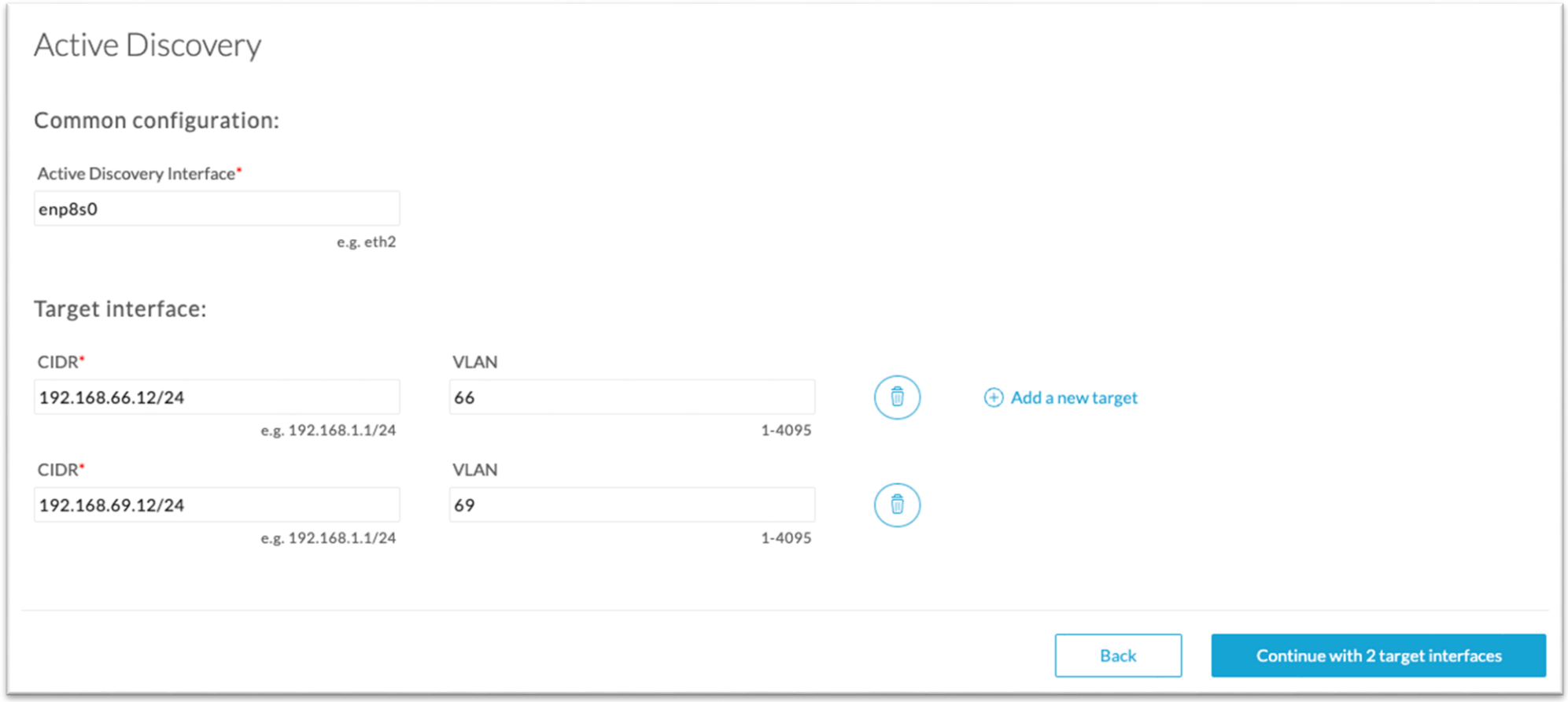
Provide Name, Token, Sensor Mode



Provide interface configuration based on traffic type selected.

Docker Sensor – Deployment Phase 3

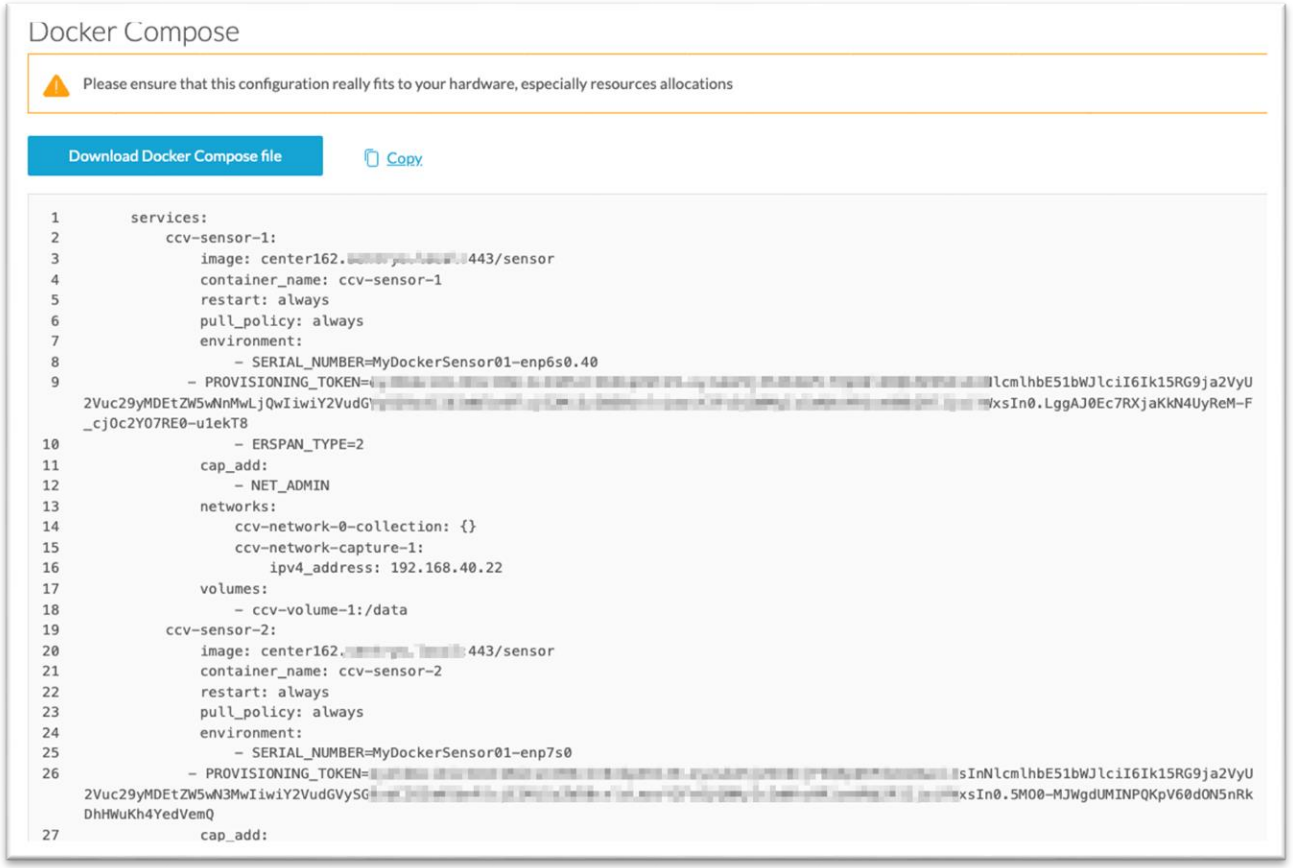
Optionally configure Active Discovery



Configure the Active Discovery interface of the standalone docker instance.

Docker Sensor – Deployment Phase 4

Review and download the resulting docker-compose configuration file



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

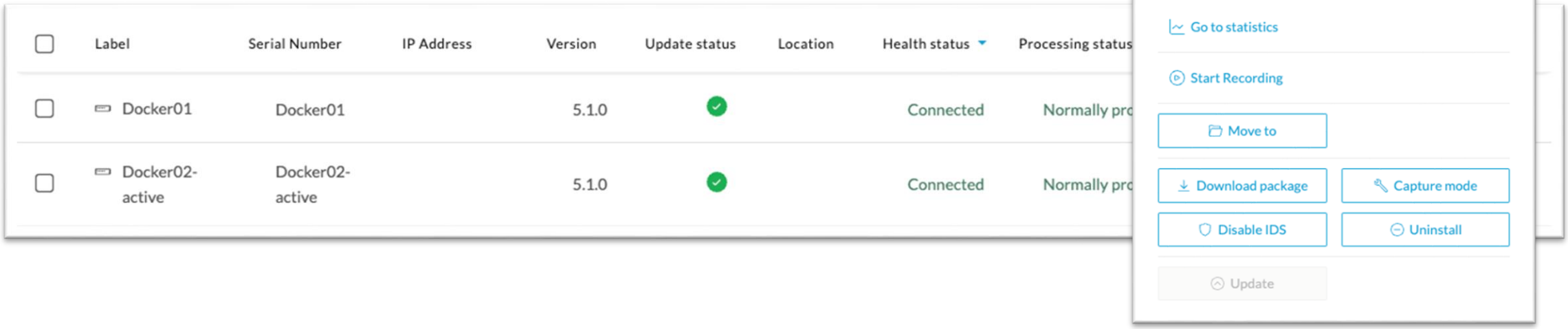
Instantiate the docker container(s) using the compose file (green)

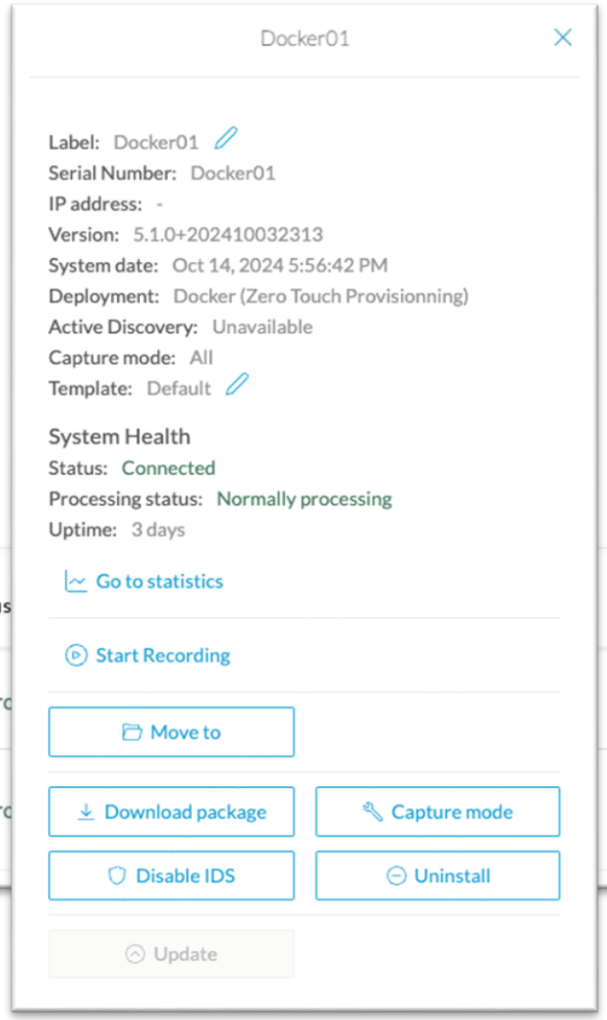
Task	Command	Result
Interactive sensor creation	docker compose up	System will display stderr/stdout of the instance. End with Ctrl+C
Start and run sensor independently	docker compose up -d	System will start the docker container instances to the background and leave them running
Forcefully recreate the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



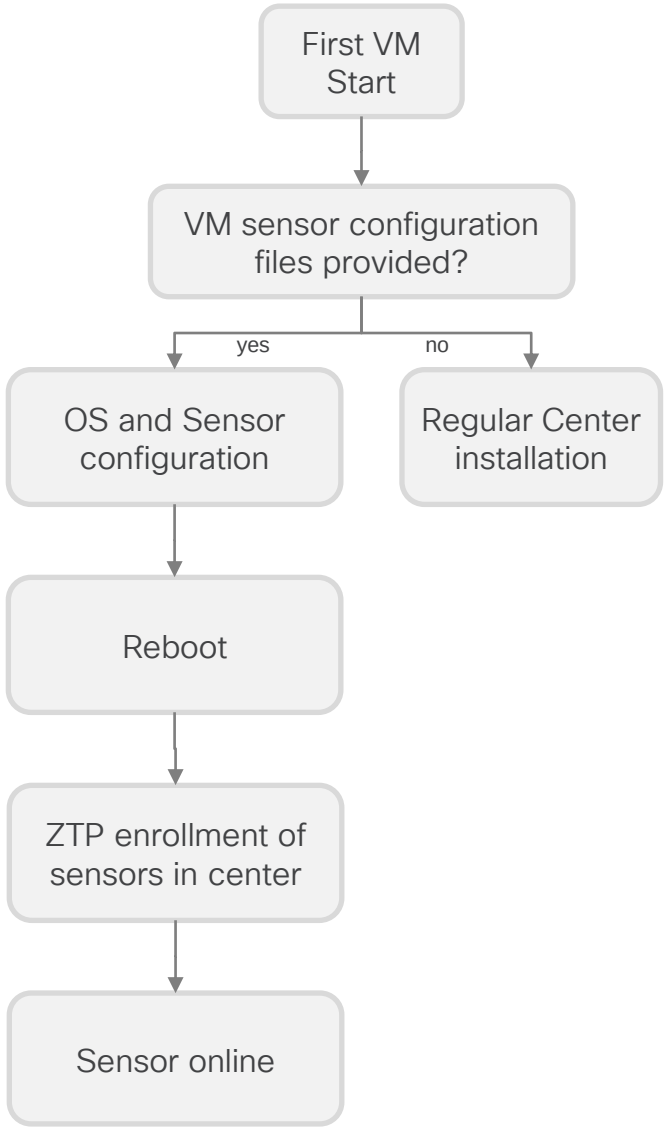


Cyber Vision VM Sensor – Technical Summary

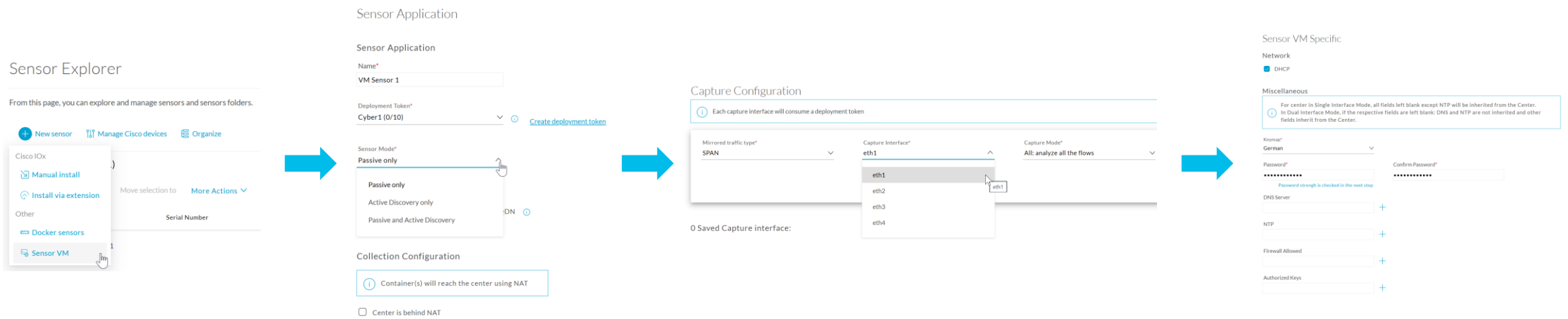
- Compatible with x86-64 devices
  - VMWare v6.x required
  - Minimum of 4GB dedicated memory required (8GB recommended)
  - Minimum of 2 dedicated CPU cores required
- Required network communication
  - Host to CV Center ports: 443/80
  - VM instance to Center ports: 5671, 10514
- Storage allocation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

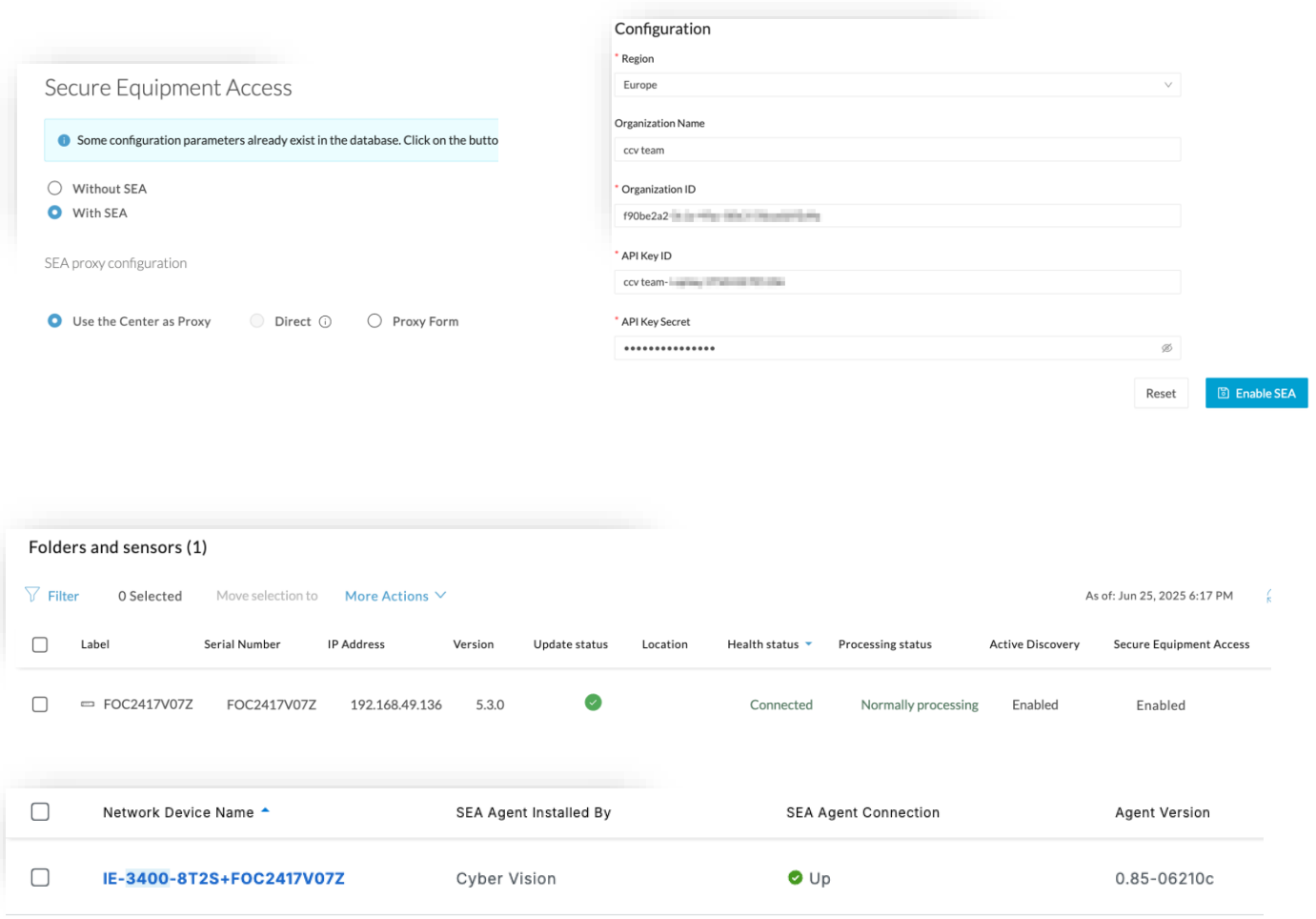


- The network interfaces are pre-determined by the standard interfaces of the image vs. the host interfaces in a docker-based setup.
- The configuration finishes with the ability to download an .iso image. This image needs to be provided during initialization of the VM to parametrize the starting instance 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



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

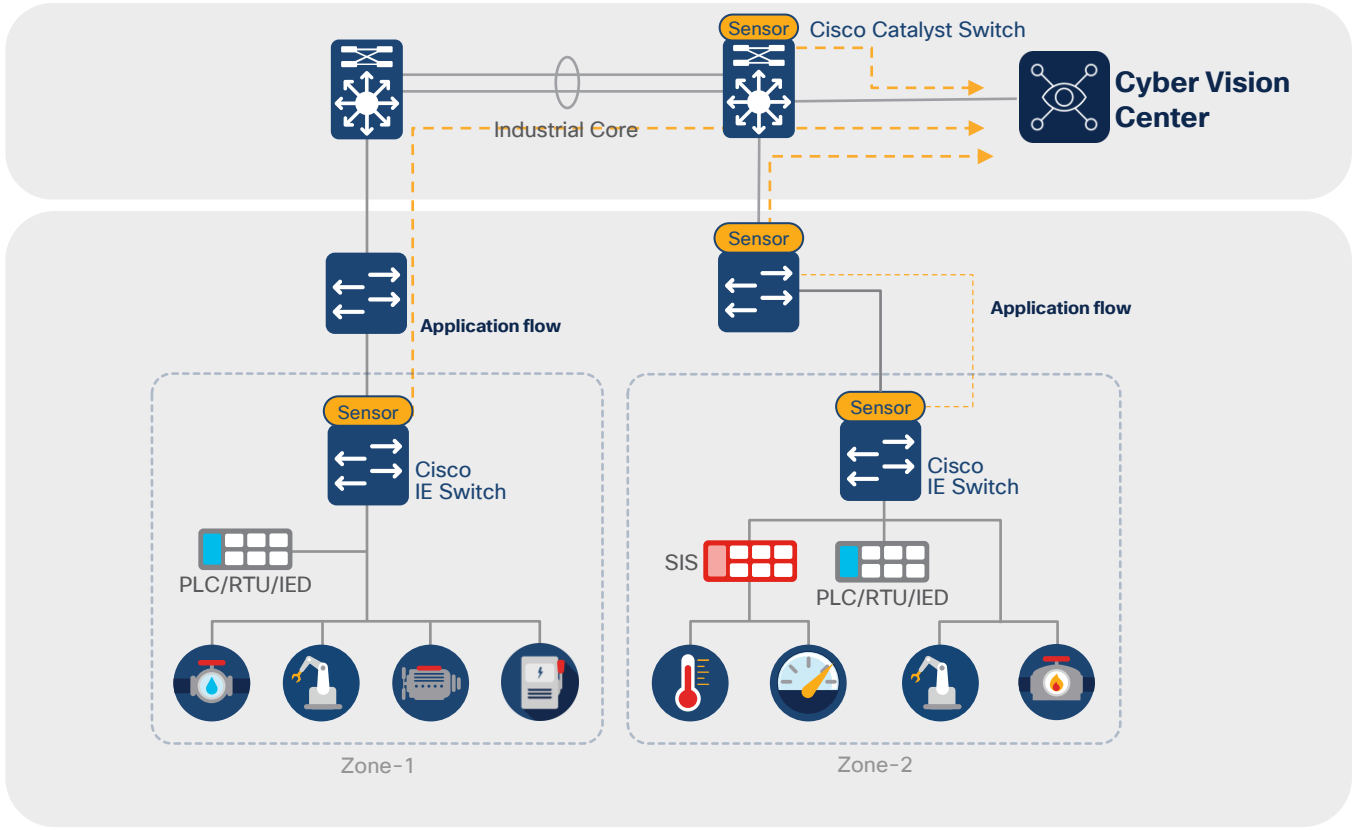
More detail: [Cisco Cyber Vision Datasheet]

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

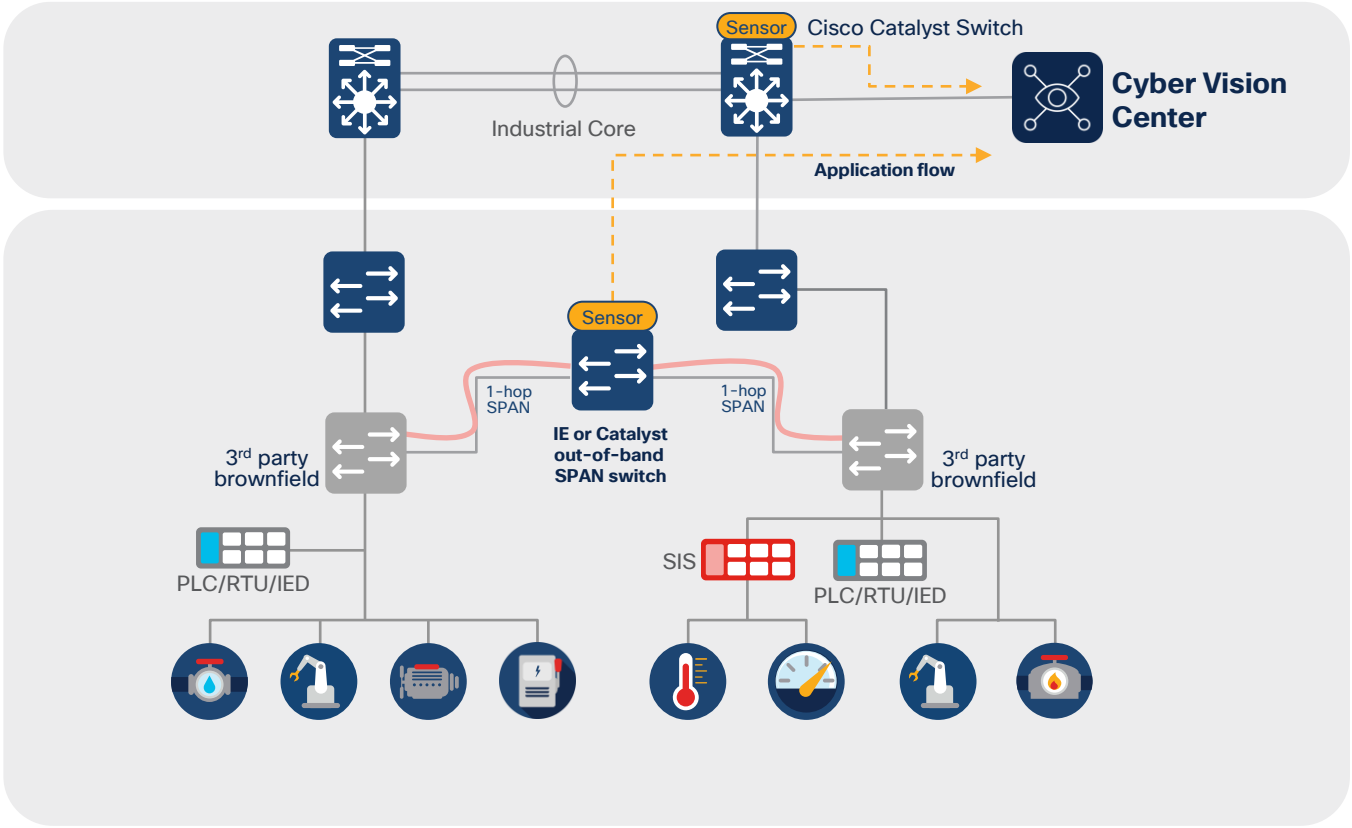
12,000 pps @ average packet size of 750 bytes ~ 70 Mbps
12,000 pps @ average packet size of 1500 bytes ~ 140 Mbps
* With 100GB SSD installed – storage required to support Store and Forward

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

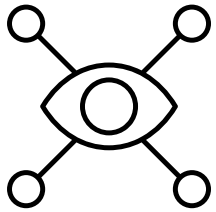
Out-of-Band Collection



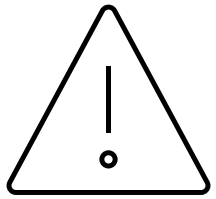
- Embedded Sensor on IE3400 and Catalyst 9300 can be leveraged as out of band sensor
- Enables aggregation of multiple SPAN sessions from across infrastructure
- Environment and scale are deciding factors for IE3400 or Catalyst 9300
- Unlike other solutions that require SPAN all the way to the monitoring 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

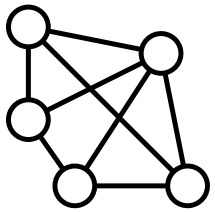
You cannot secure what you don’t know



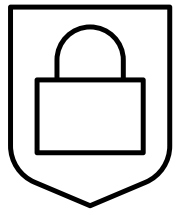
List all the assets you are defending



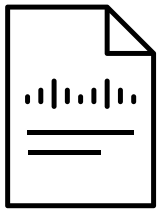
Spot vulnerabilities to patch



Identify asset communication issues



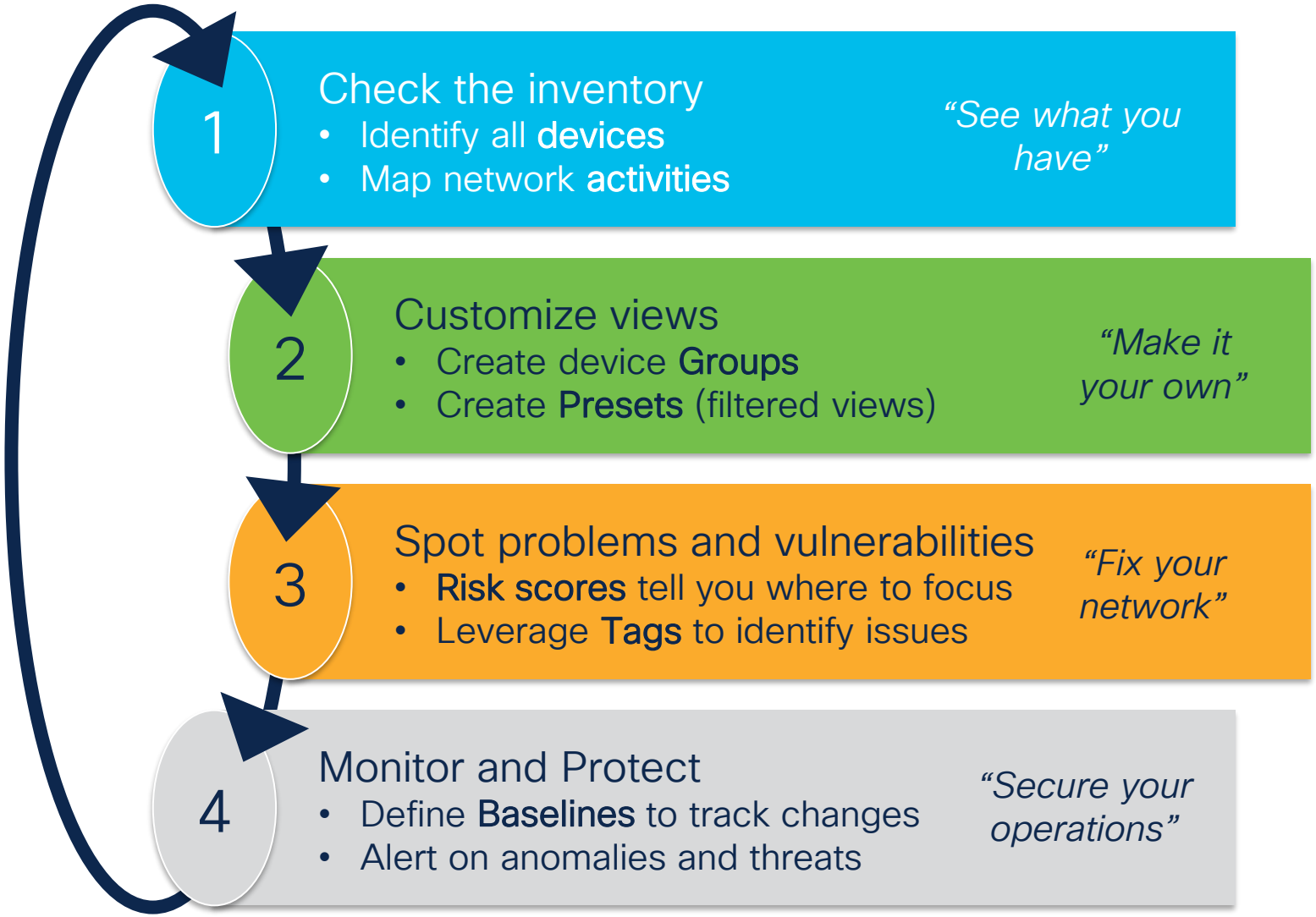
Detect bypass or leaks in the IDMZ



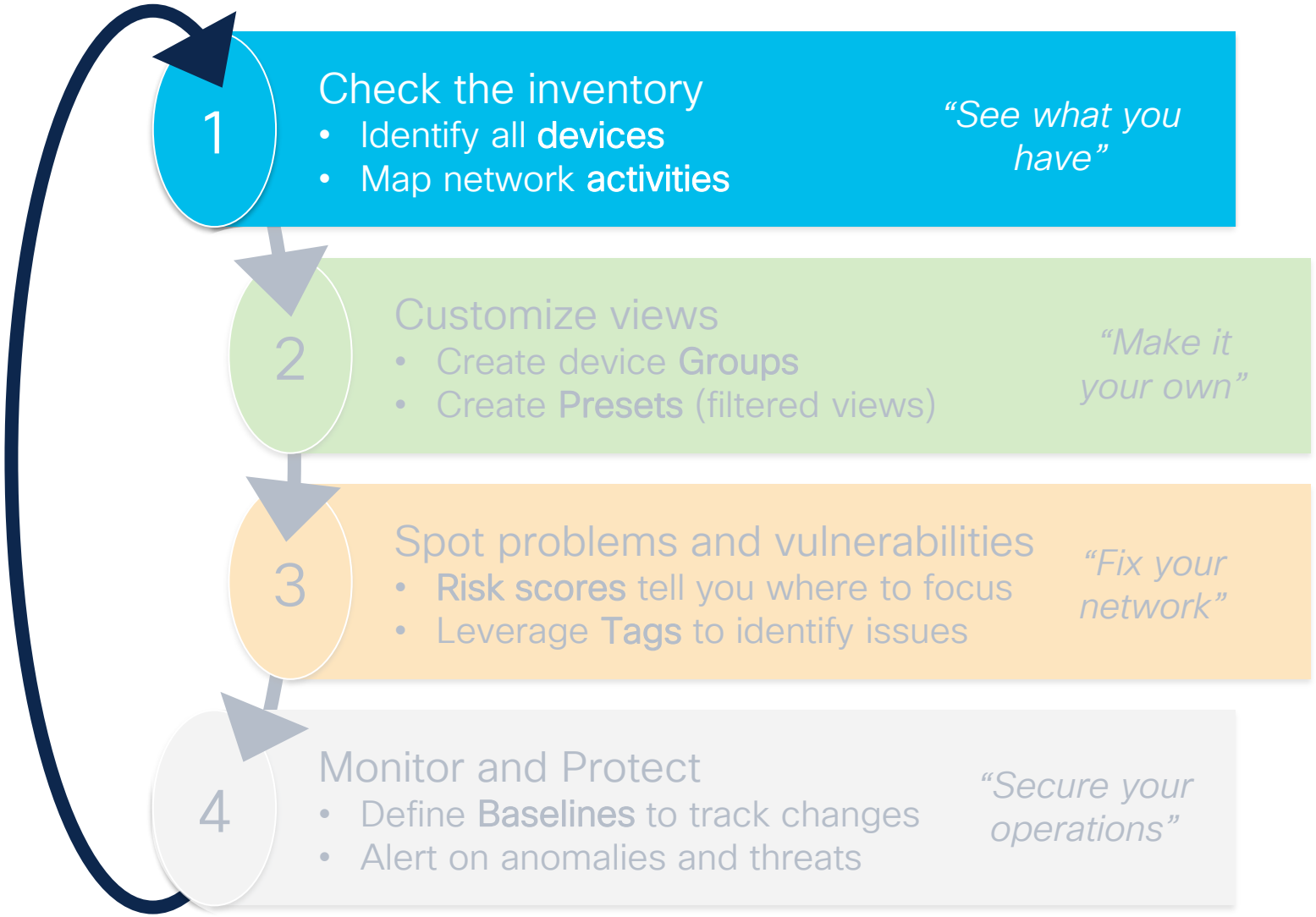
Build compliance reports

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

The Cyber Vision Workflow

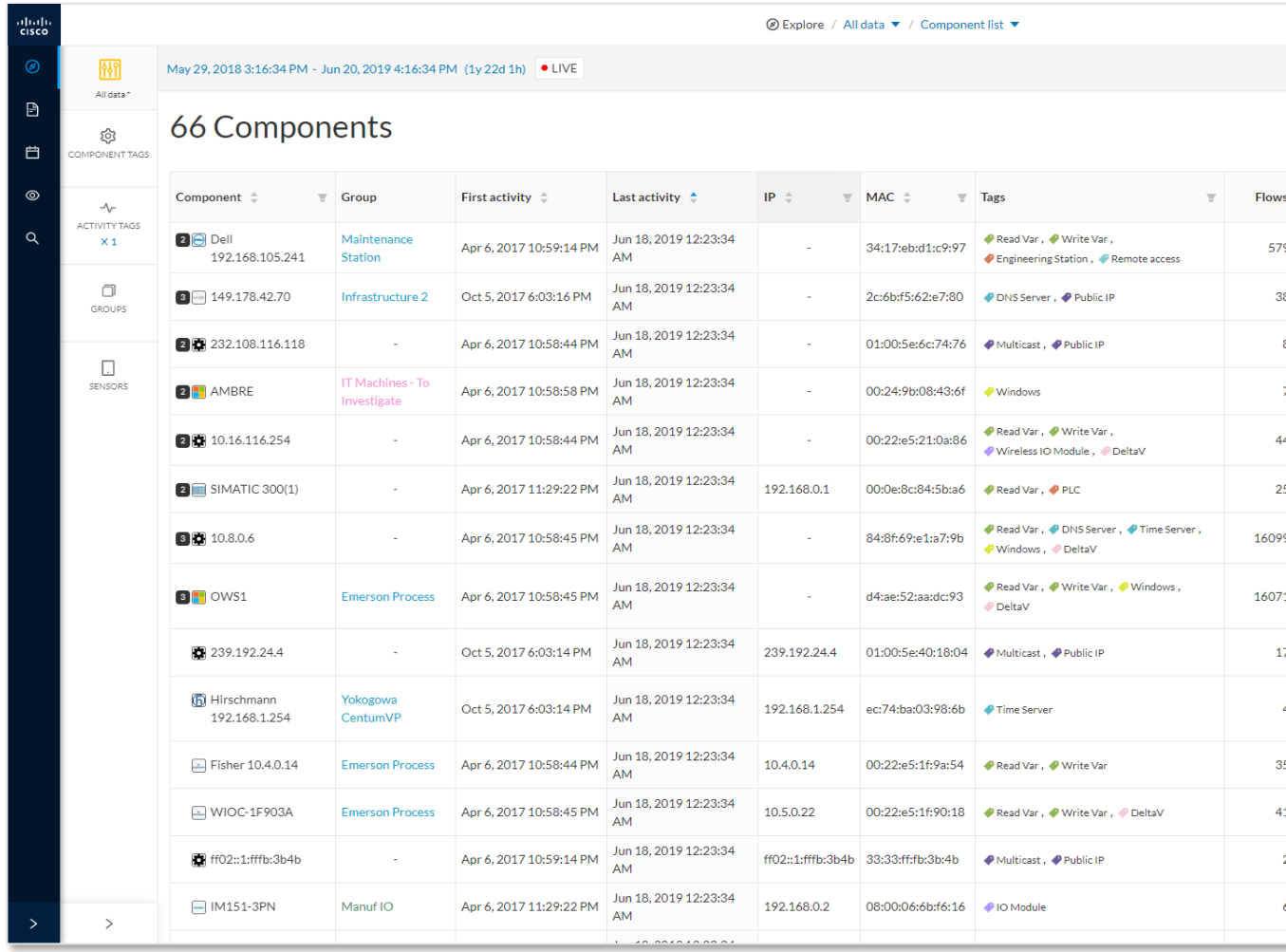


The Cyber Vision Workflow



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

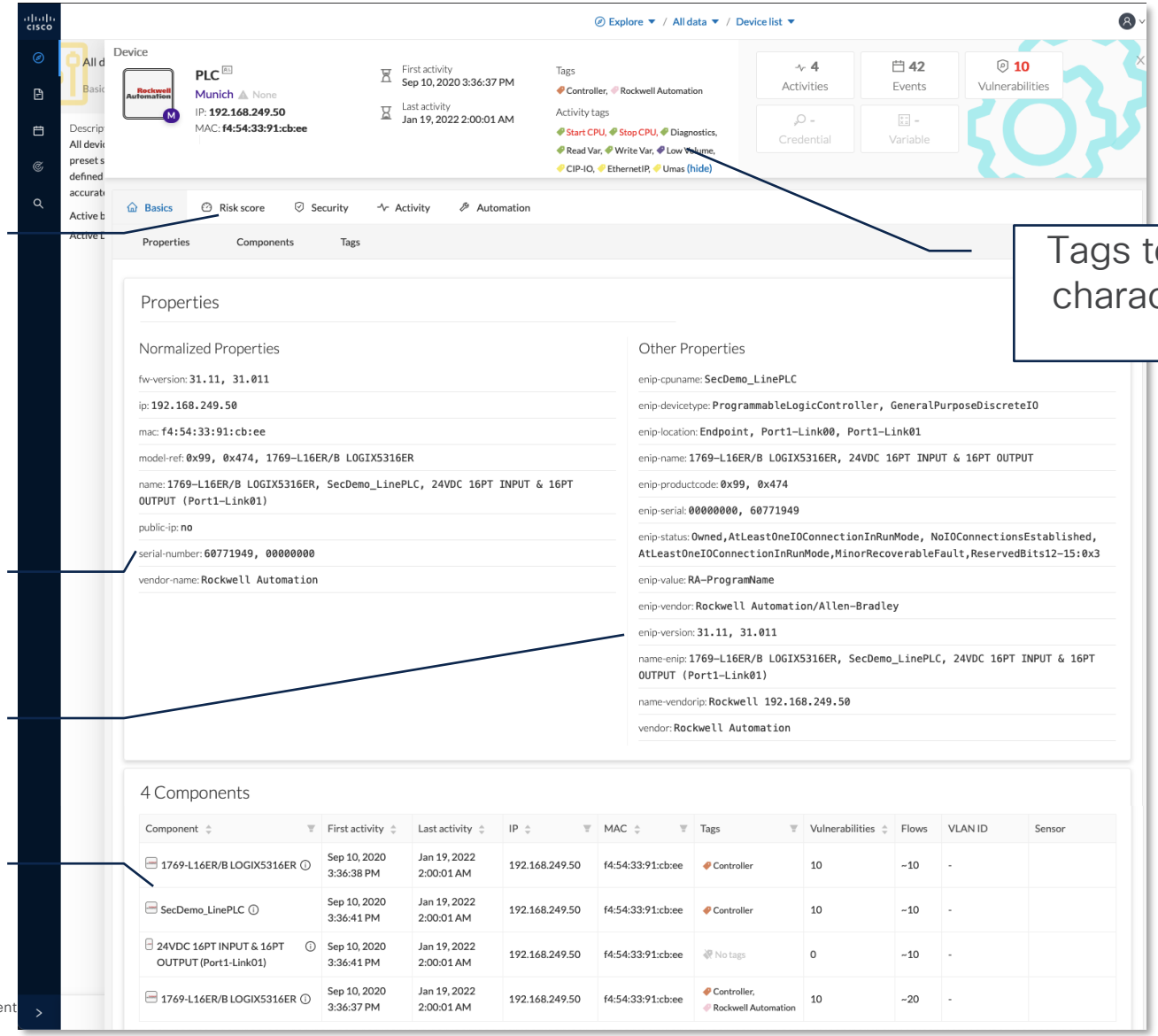
Detailed information on assets

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

Asset characteristics, version and network configuration

Control logic properties

Rack slot component details

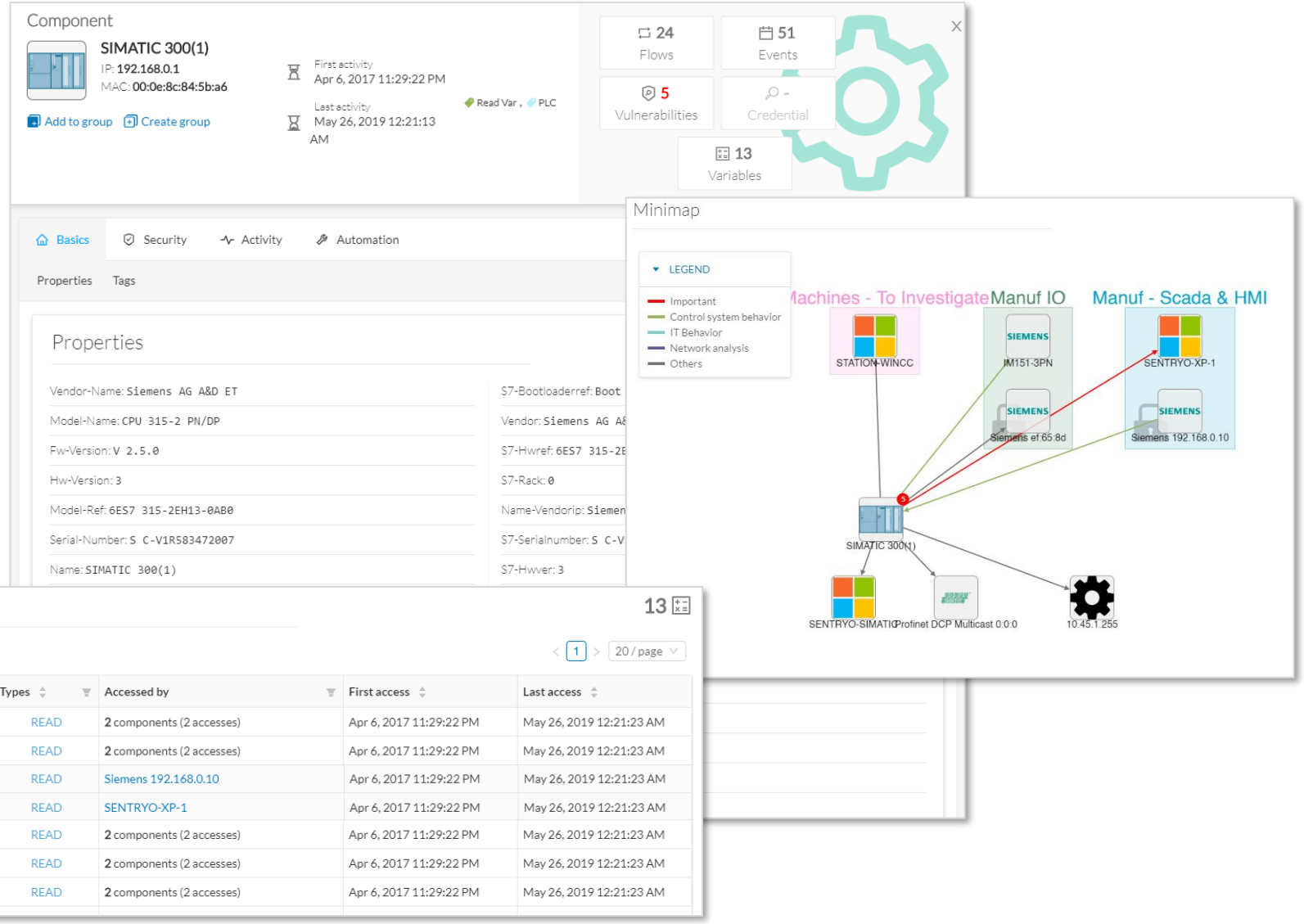


Tags to easily understand characteristics, activities, and threats

Operational insights for OT teams

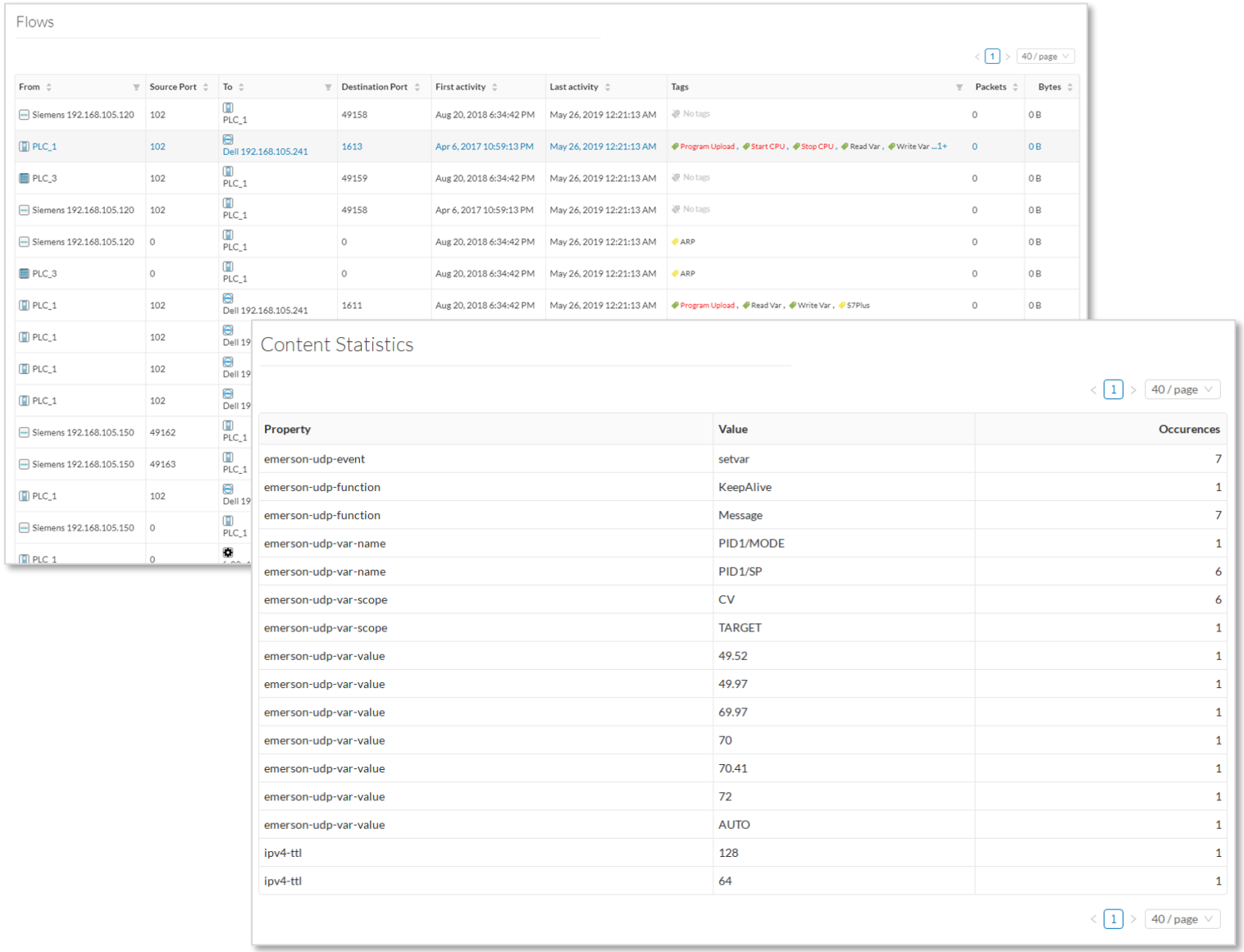
- Detailed asset properties
- Communication maps
- PLC program changes
- Variable accesses

Monitor the integrity of your industrial process



Operational insights for security analysts

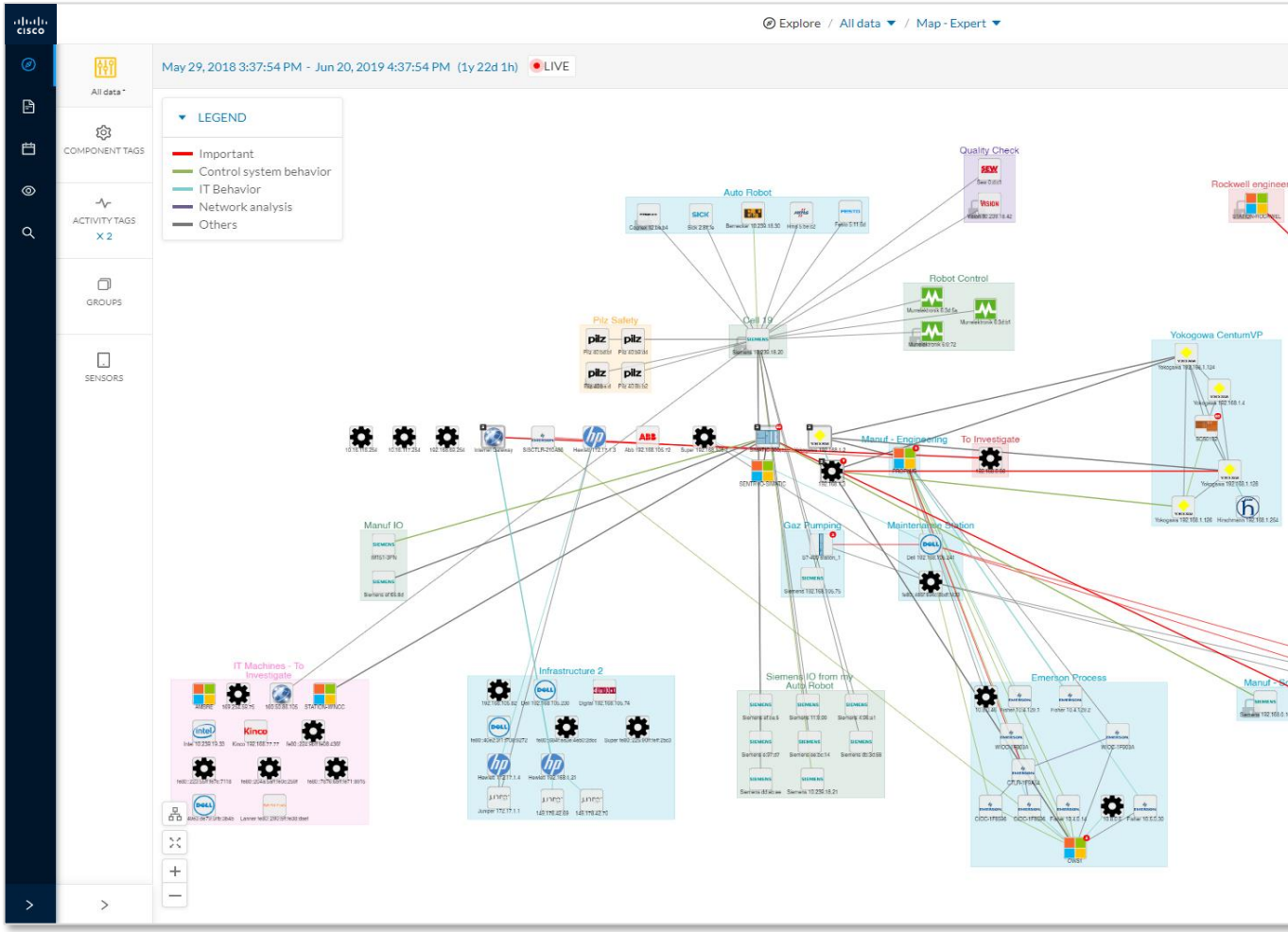
- Access the full history of all communication flows
- View detailed properties and content statistics for each flow
- View live information or go back in time for forensic search



Detailed communication maps

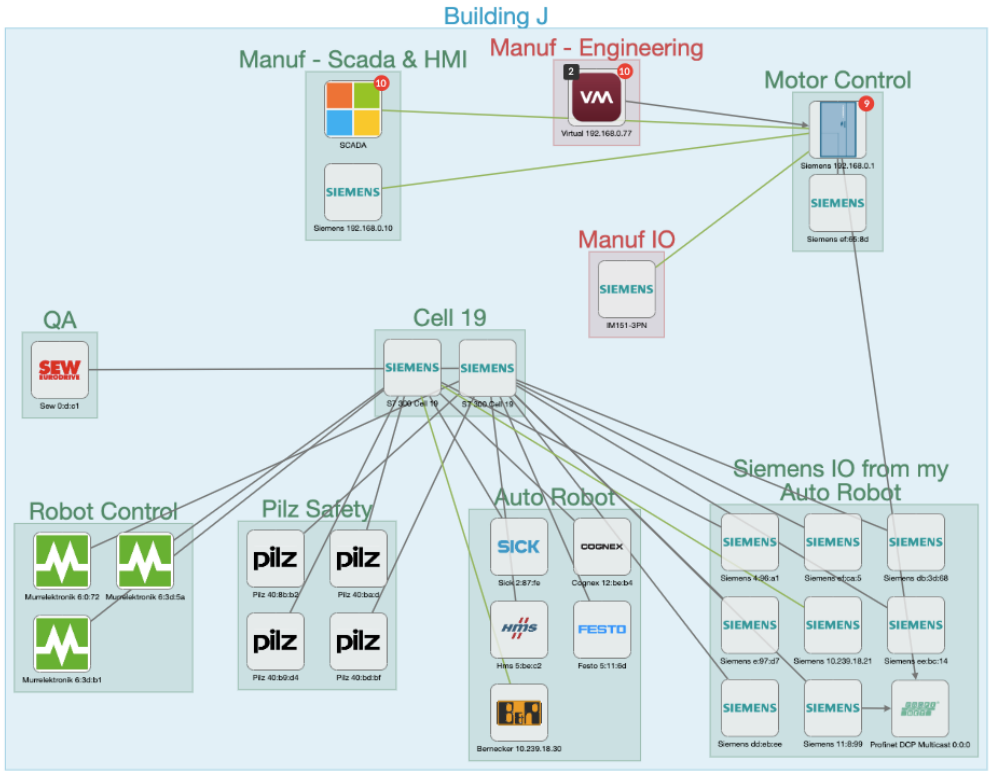
- Identify all relations between assets including application flows
- Pinpoint IDMZ leaks, shadow IT, and rogue remote access activities
- Spot unwanted communications, intrusions, and abnormal behaviors
- Tags make it easy to understand the content of each communication flow
- View live information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

Monitor industrial network hygiene and drive segmentation



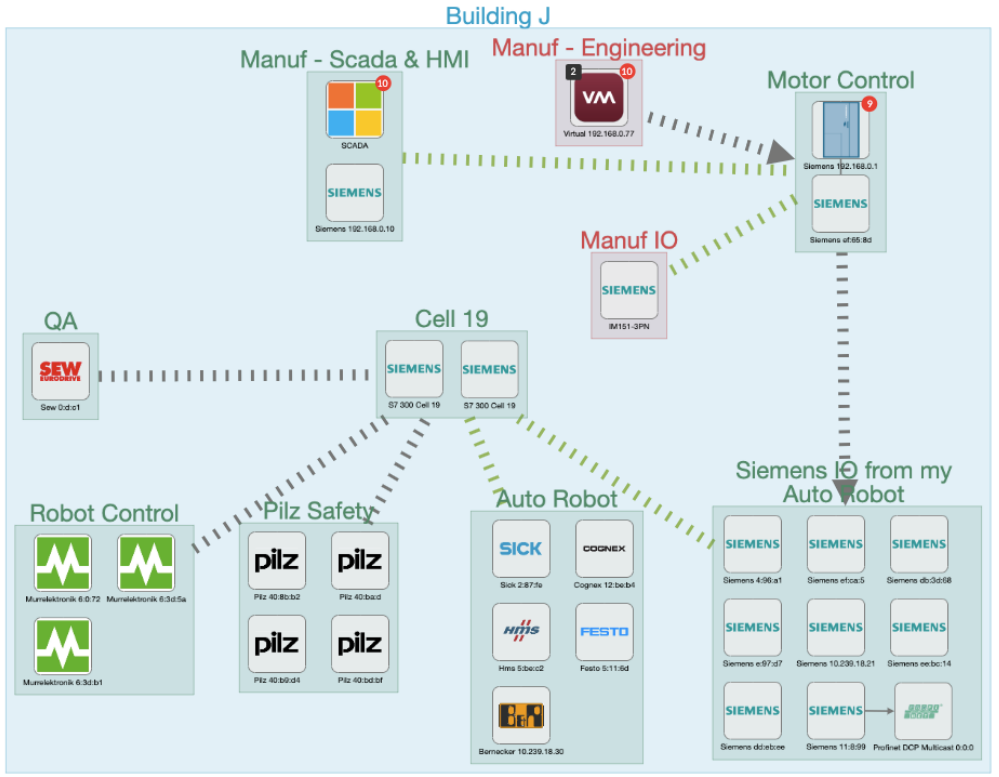
Aggregated activities match ISA/IEC 62443 conduits

Unaggregated



View all asset relationships

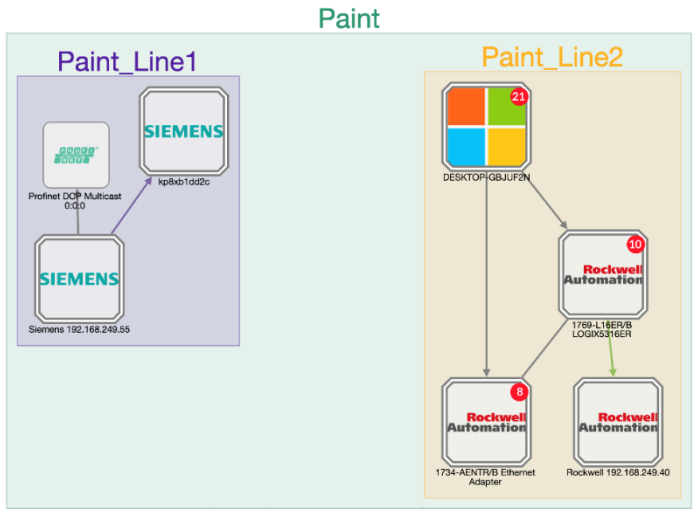
Aggregated



Easily browse and filter conduits including sub-zones

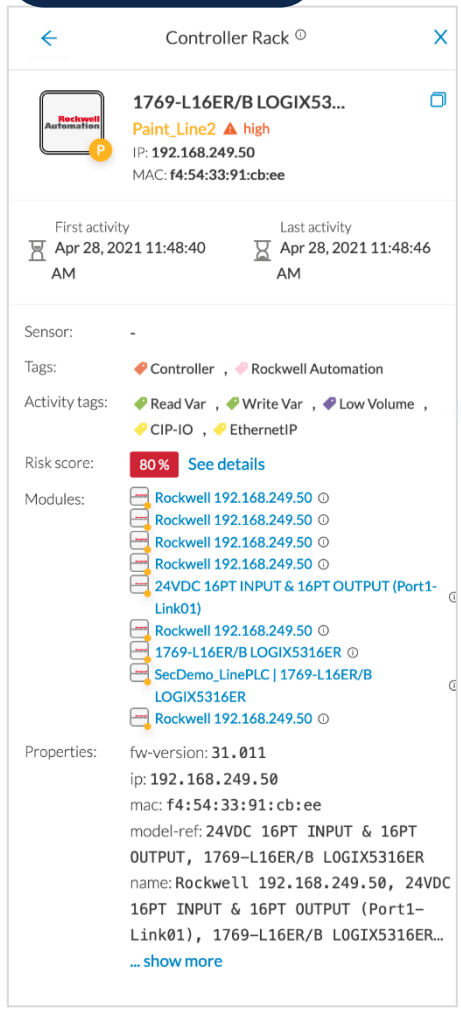
Aggregated components match the physical inventory

Map view

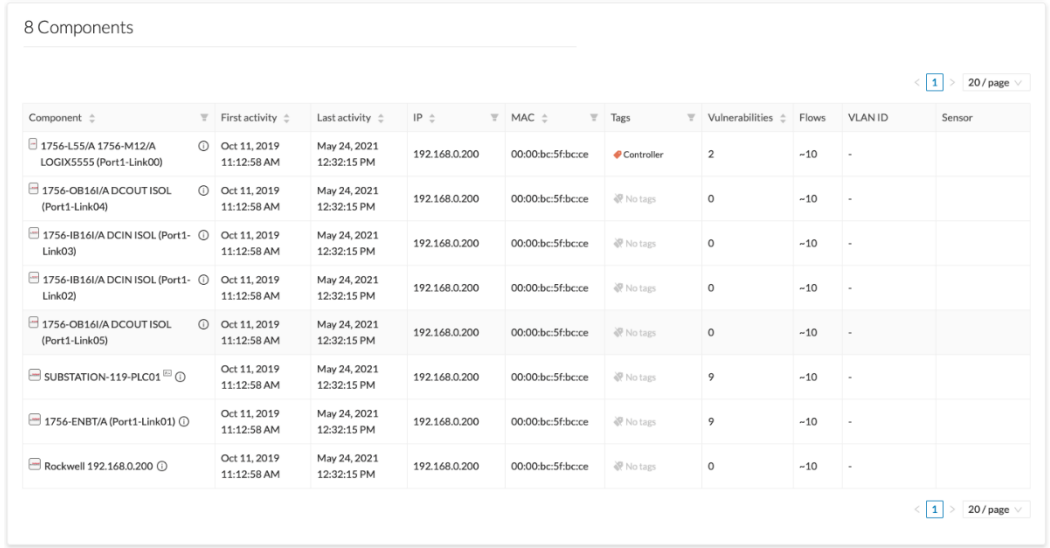


Double-border icons indicate a device with multiple components

ID Cards

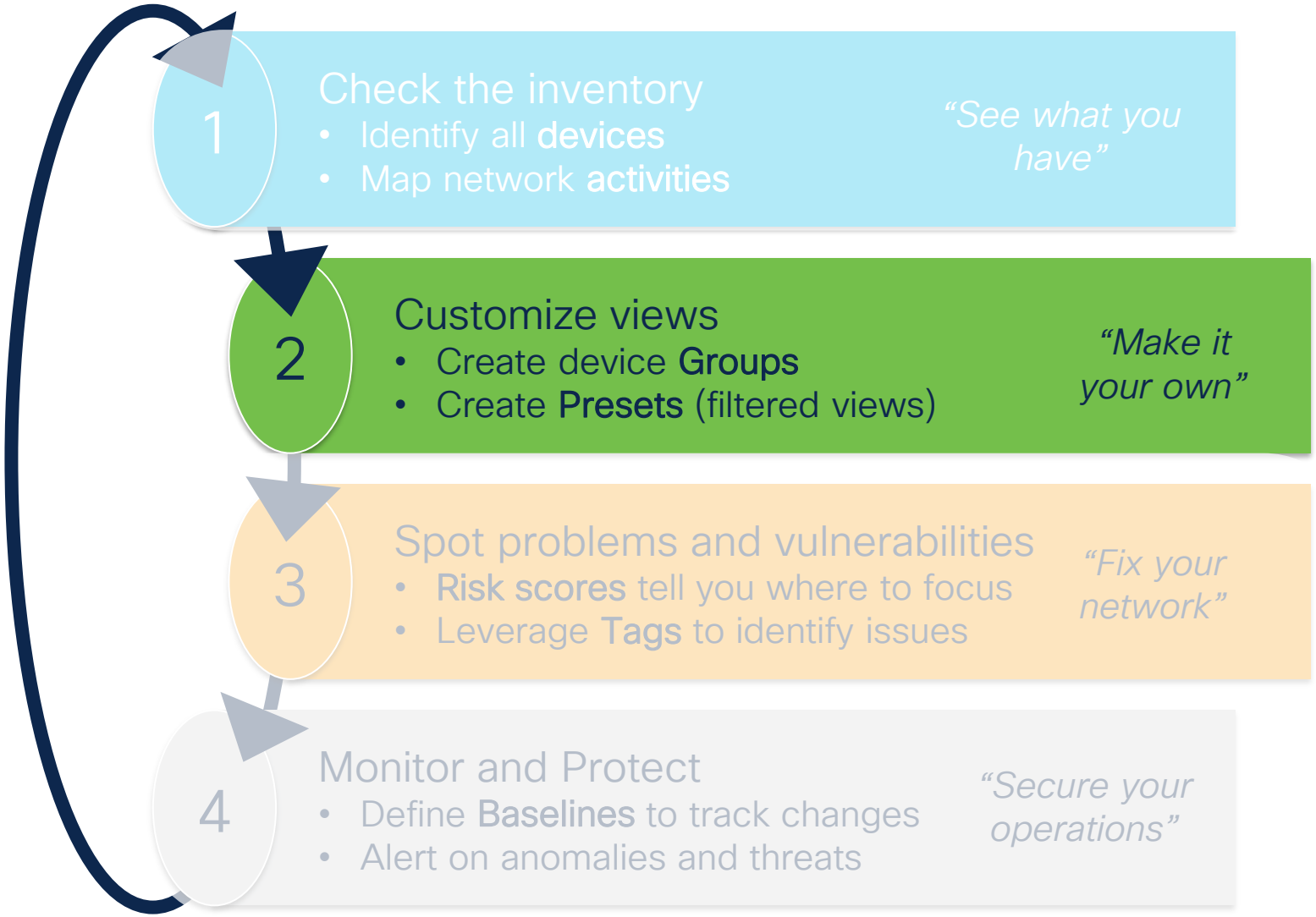


Technical Sheets



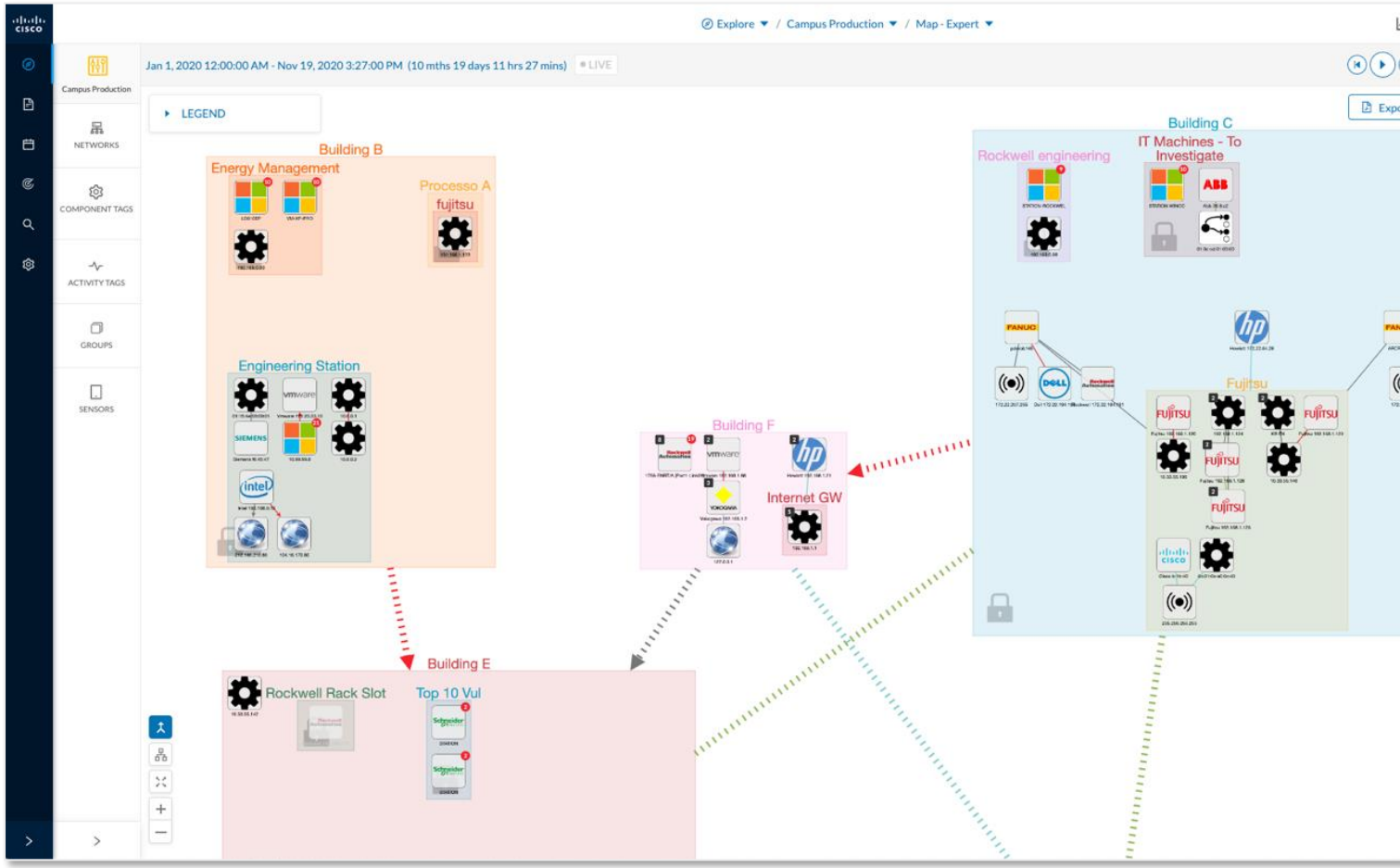
Easily list the components of a device. Click on a component to view more details

The Cyber Vision Workflow



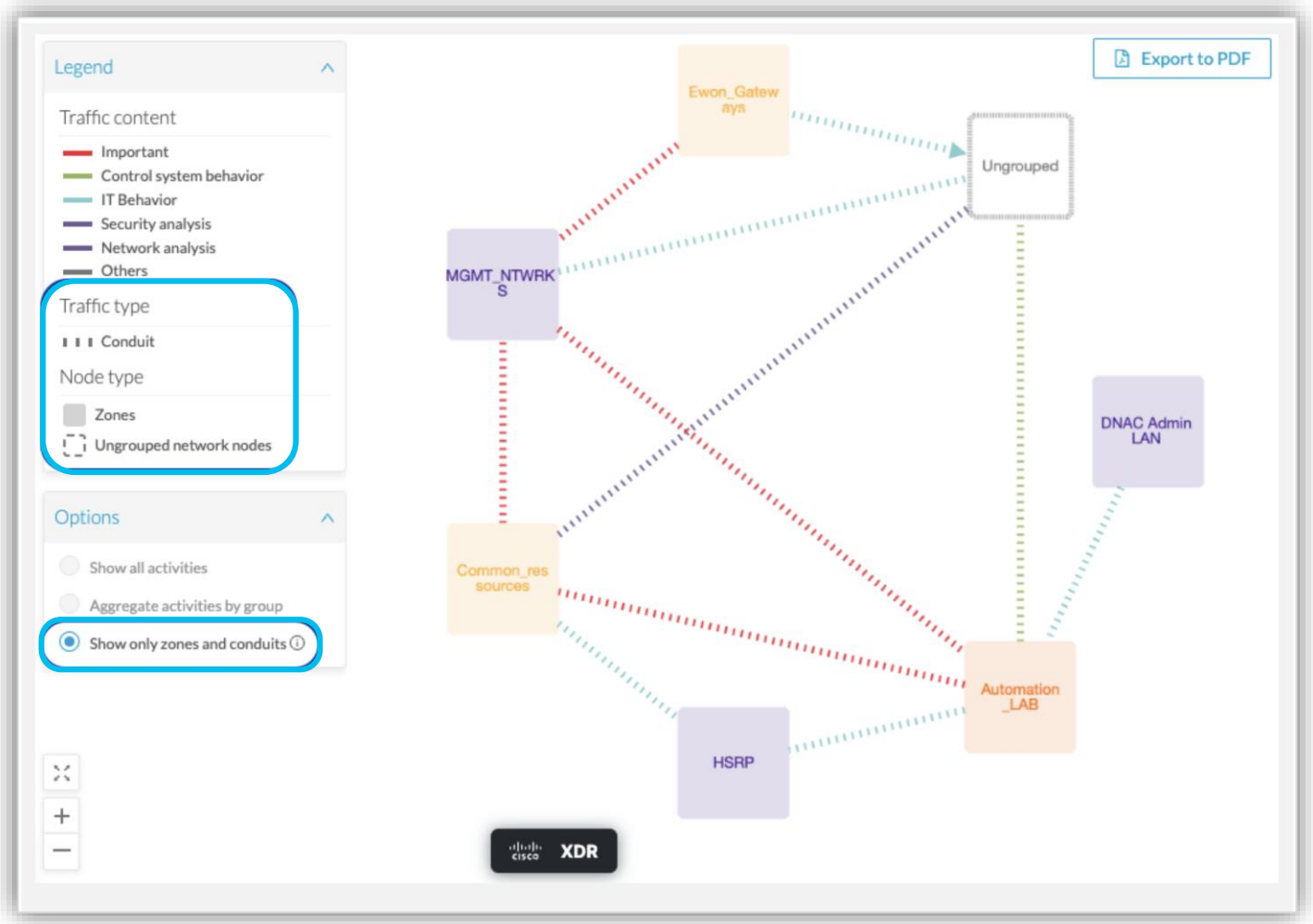
Group assets to define zones and conduits

- 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



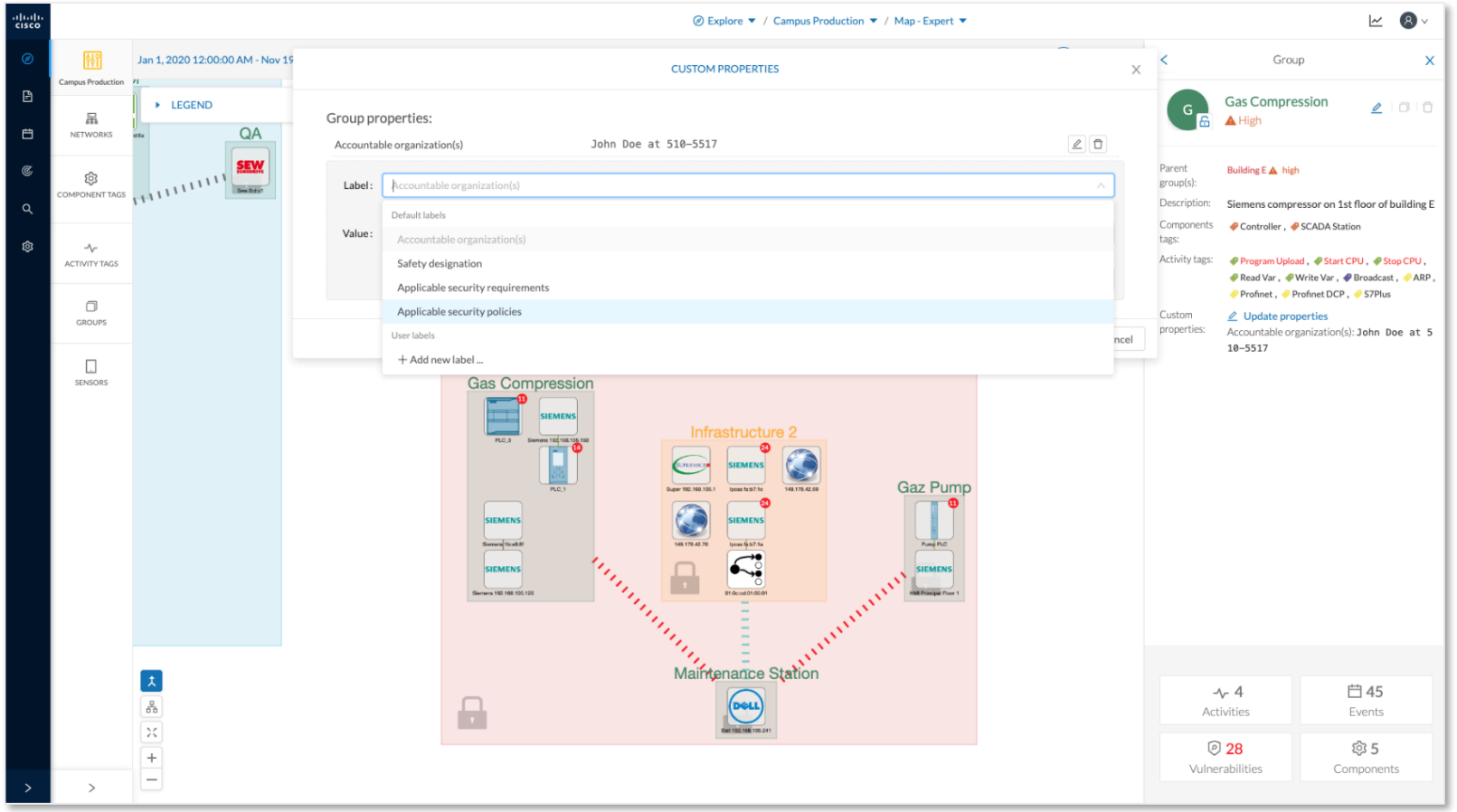
“Zones and Conduits” visualization

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



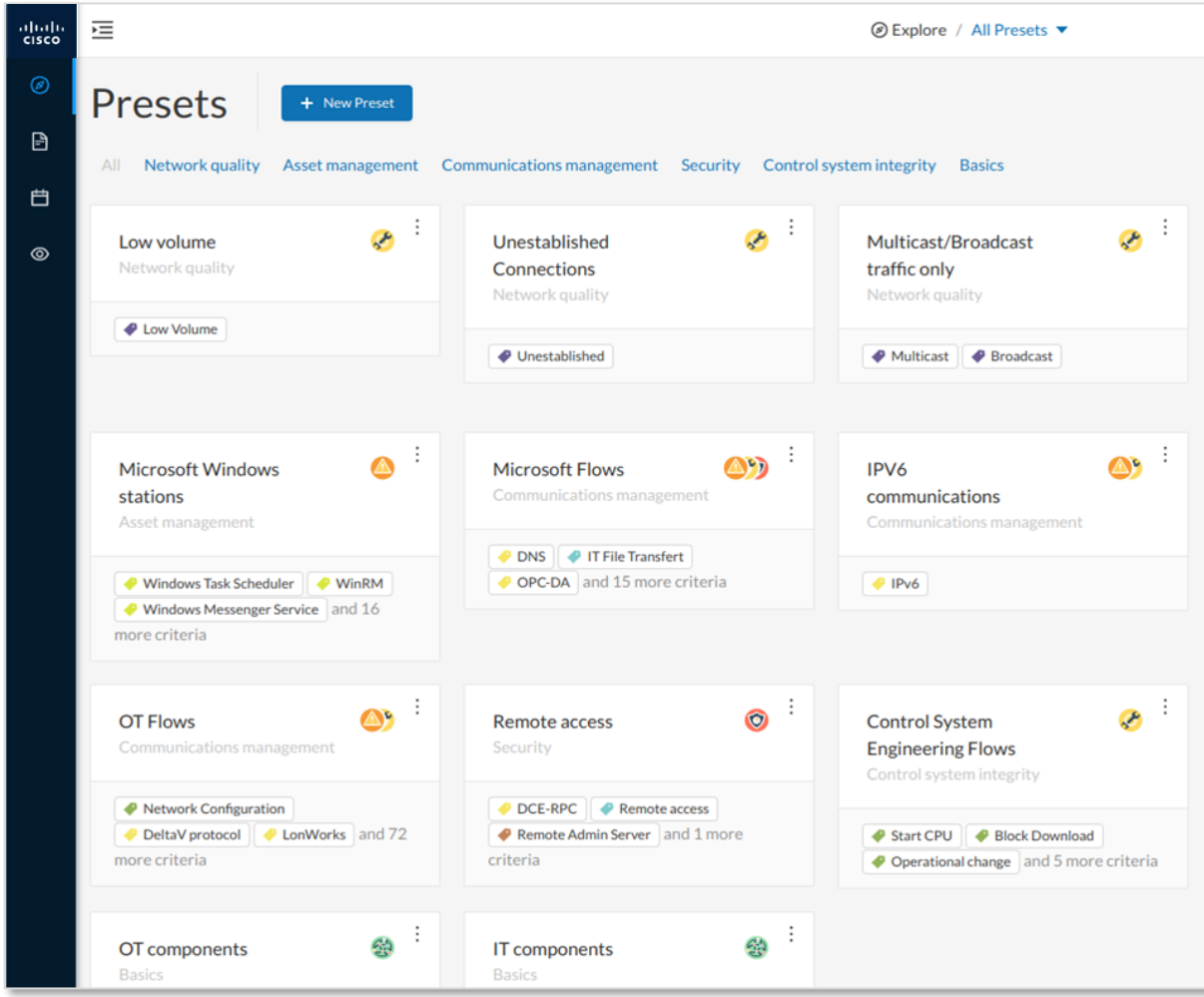
Custom properties to document the organization

- 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



Easily dive into your data with preset views

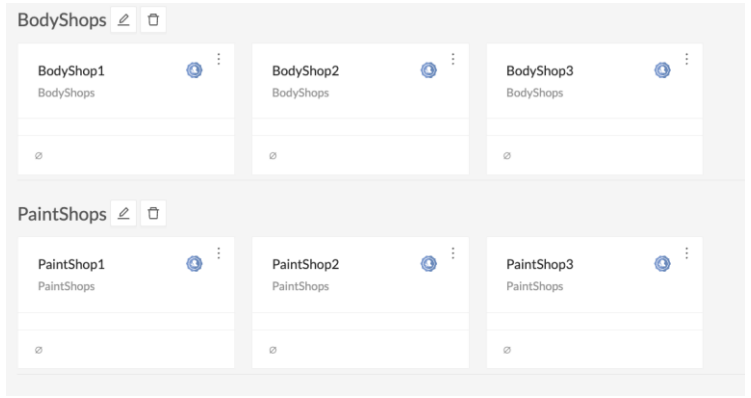
- Presets are smart filters based on Tags, Groups, Sensors you want to track
  - Preset per site, per production line
  - Preset per asset type, per vendor
  - Preset per behavior types
- Deep-dive into very large datasets with ease
- Share presets with other users to show your discoveries & enable collaboration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

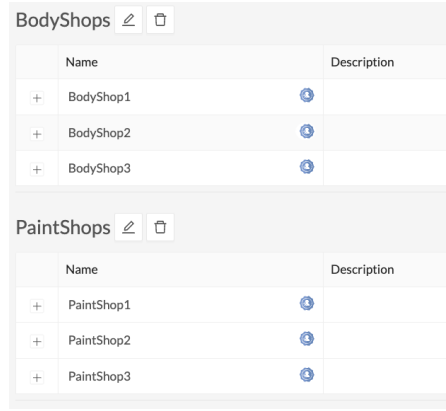


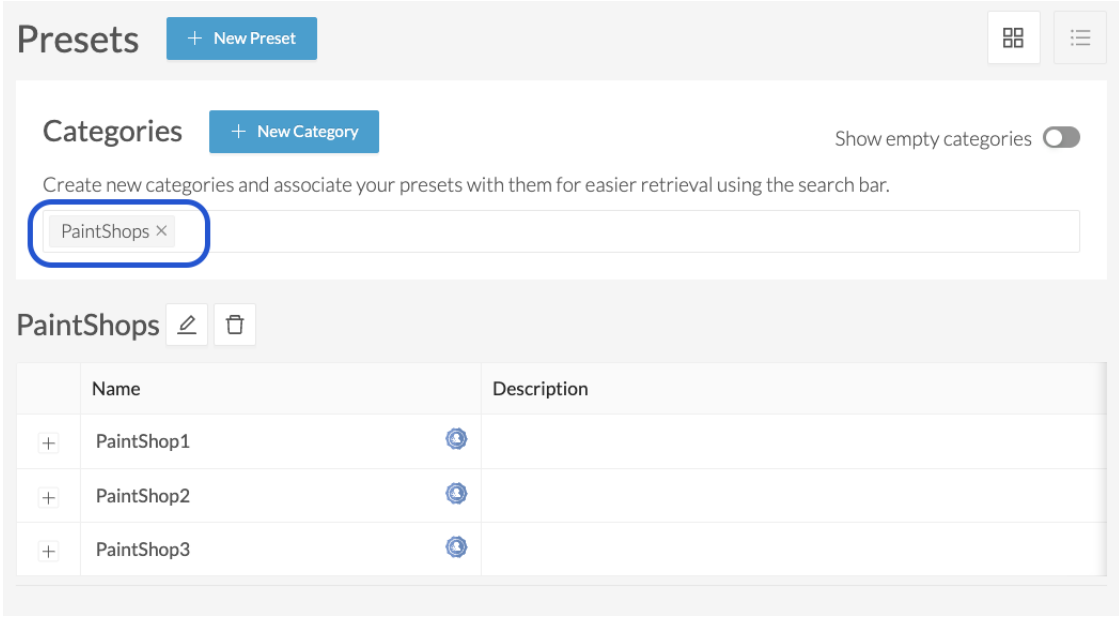
Structure your Presets using Preset Categories

- 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



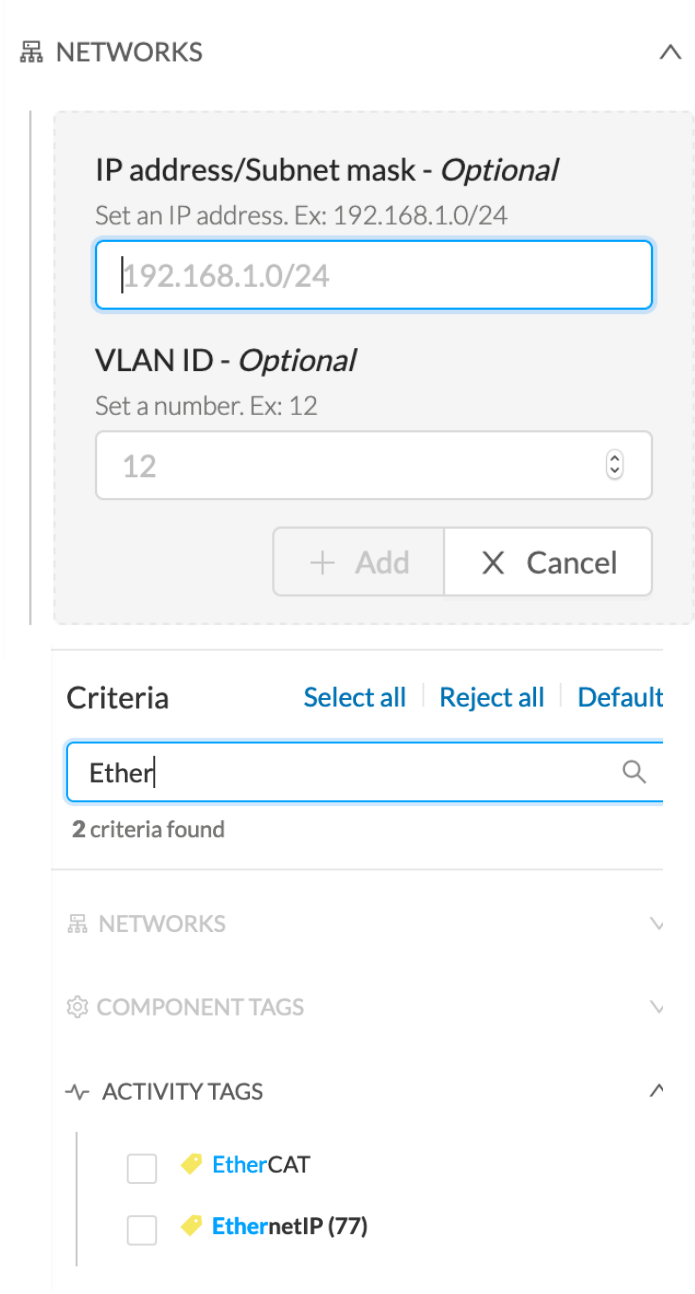




Preset Filters

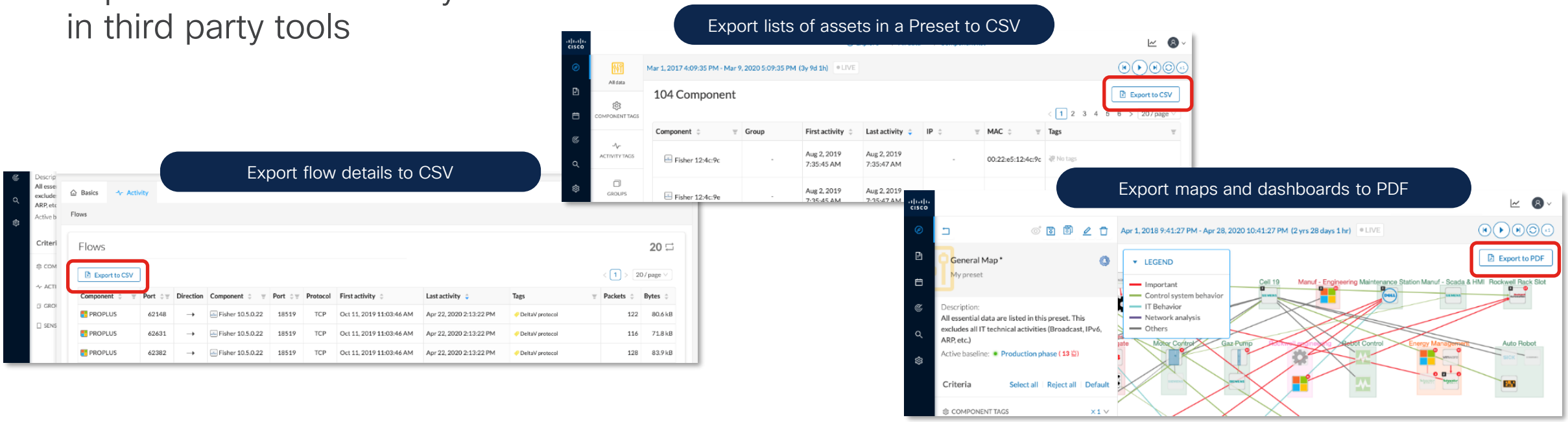
- Leverage Subnet or VLAN ID as part of preset filter

- Criteria Search enables to quickly find matching tags, groups or sensors

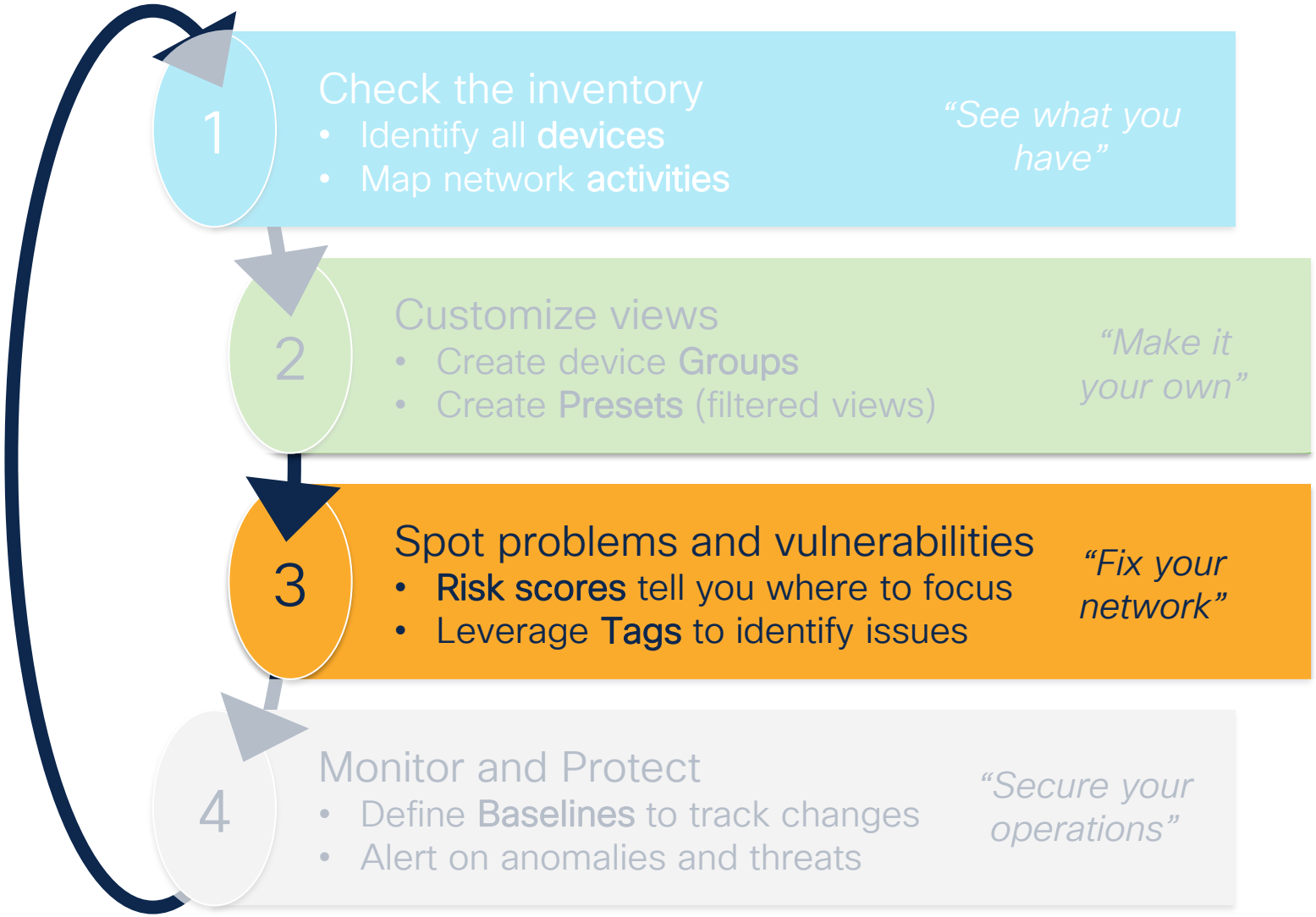


Export views to share insights

- 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



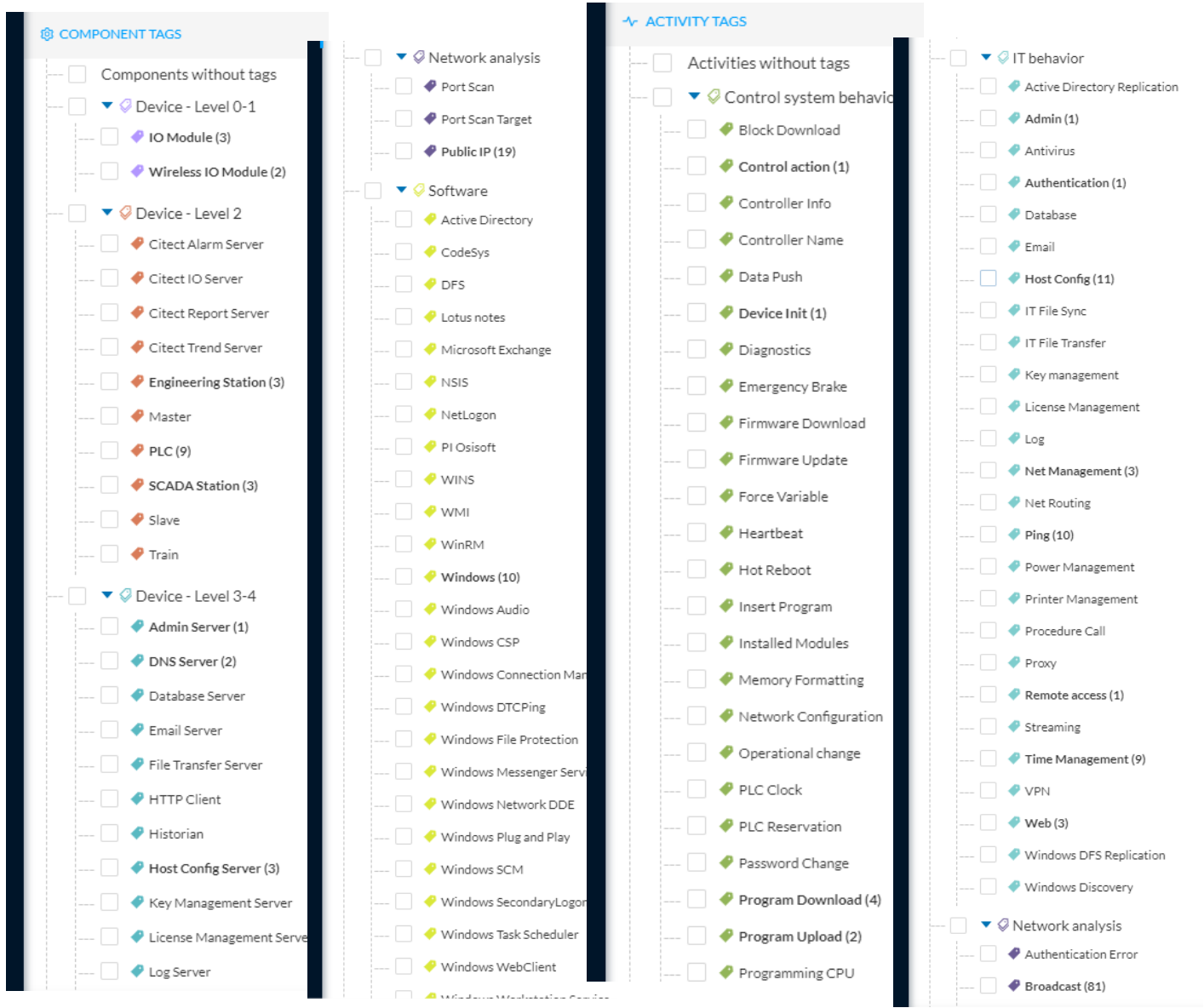
The Cyber Vision Workflow



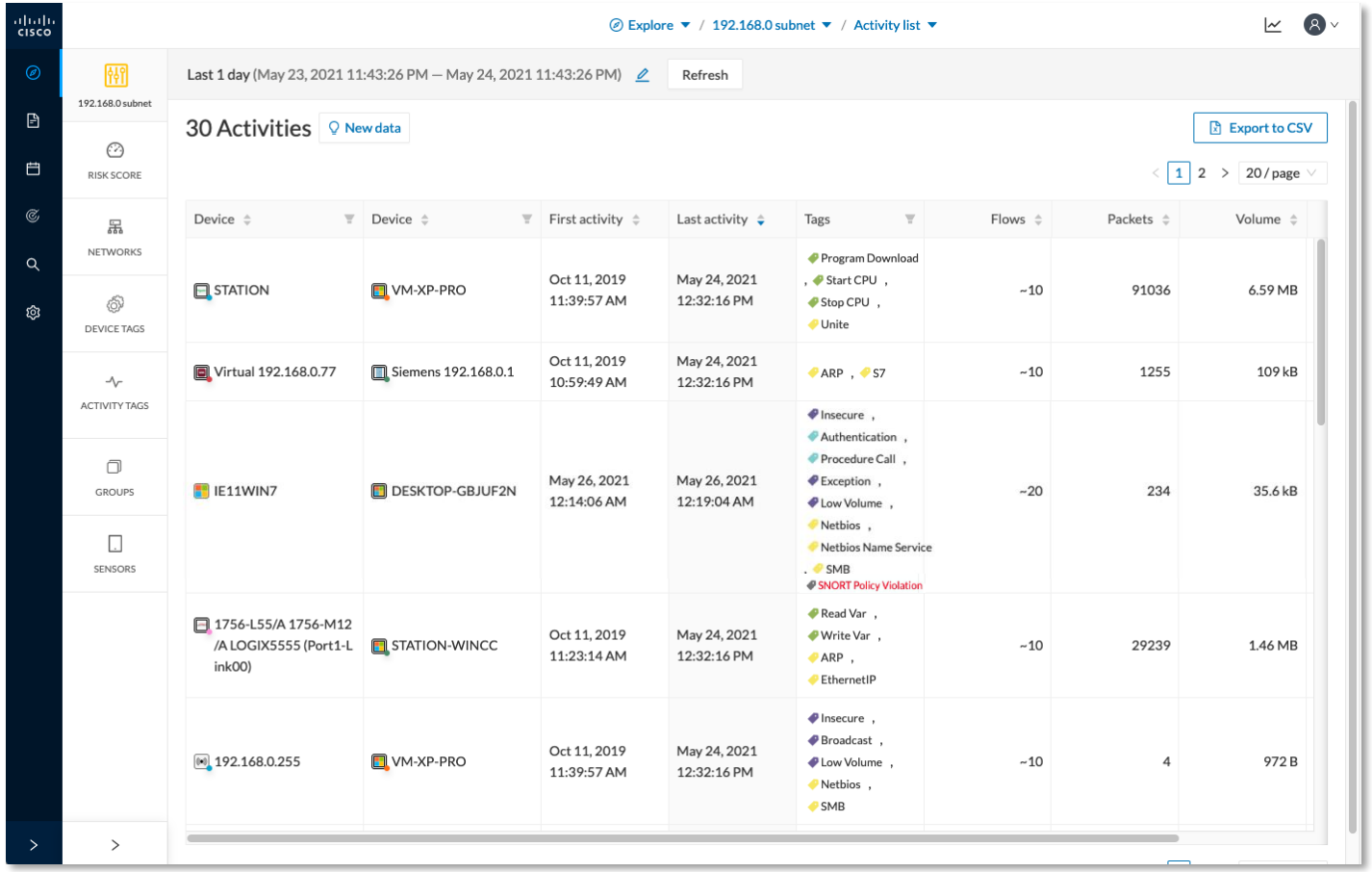
Investigate problematic assets and communications

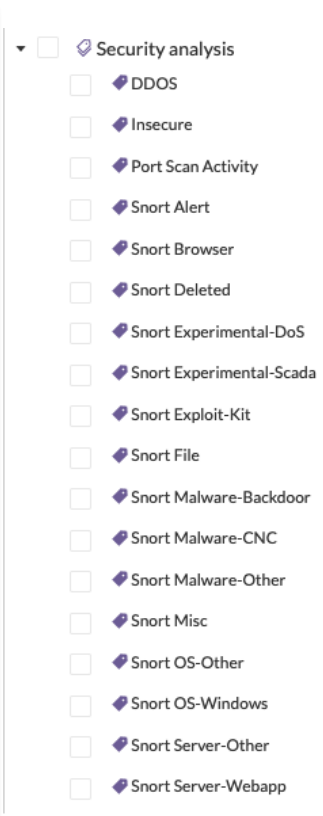
- Asset characteristics and communications are automatically translated to Tags
- A common language whatever the vendor reference
- Users do not need to be protocol experts to understand what is going on
- New tags can be added via RESTful API

Cyber Vision tags helps identify devices and activities to investigate



Enhanced visibility on malicious traffic



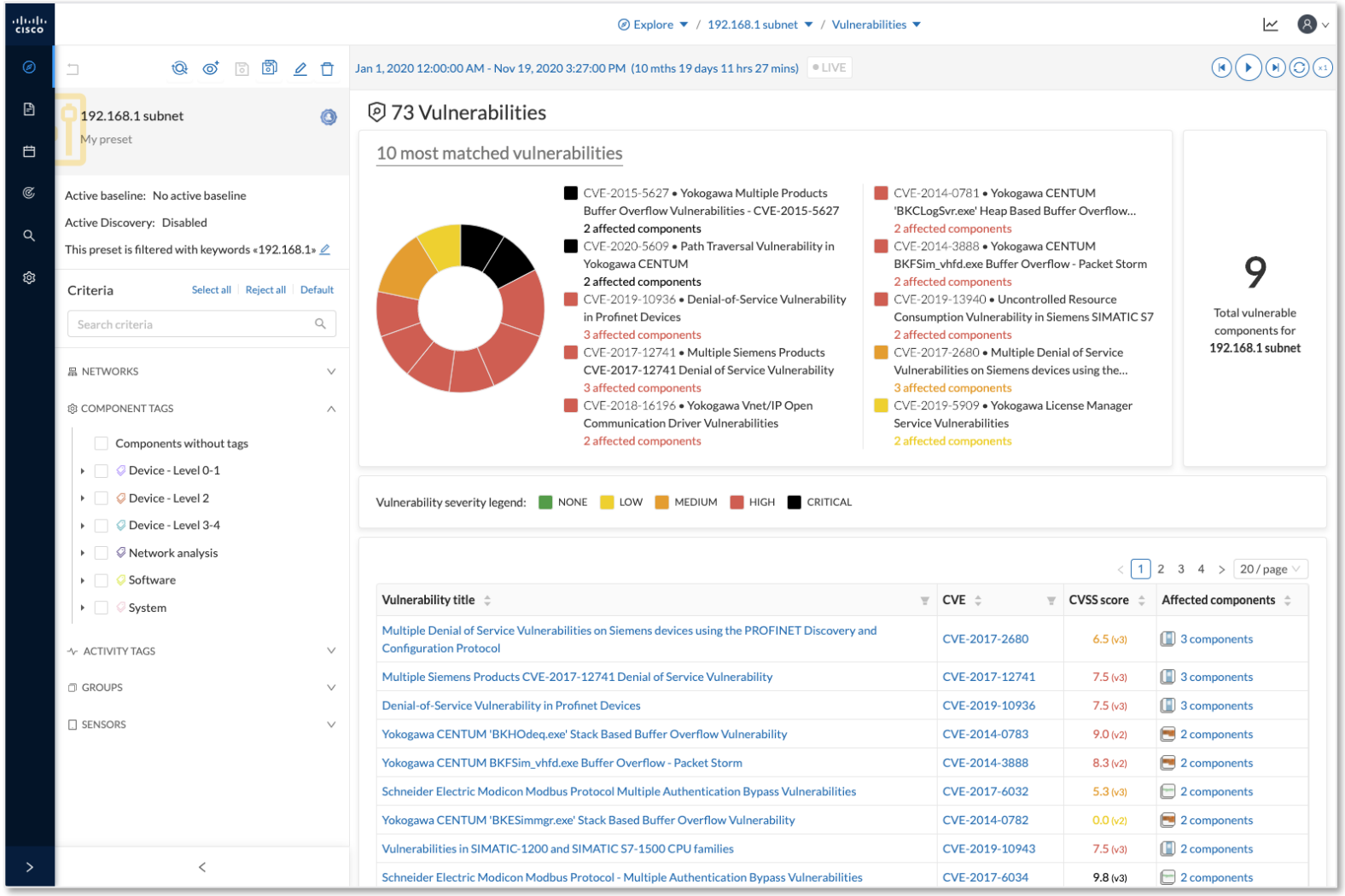


Activity tags associated with events detected by the Snort IDS

Provides more precise context to understand malicious activities

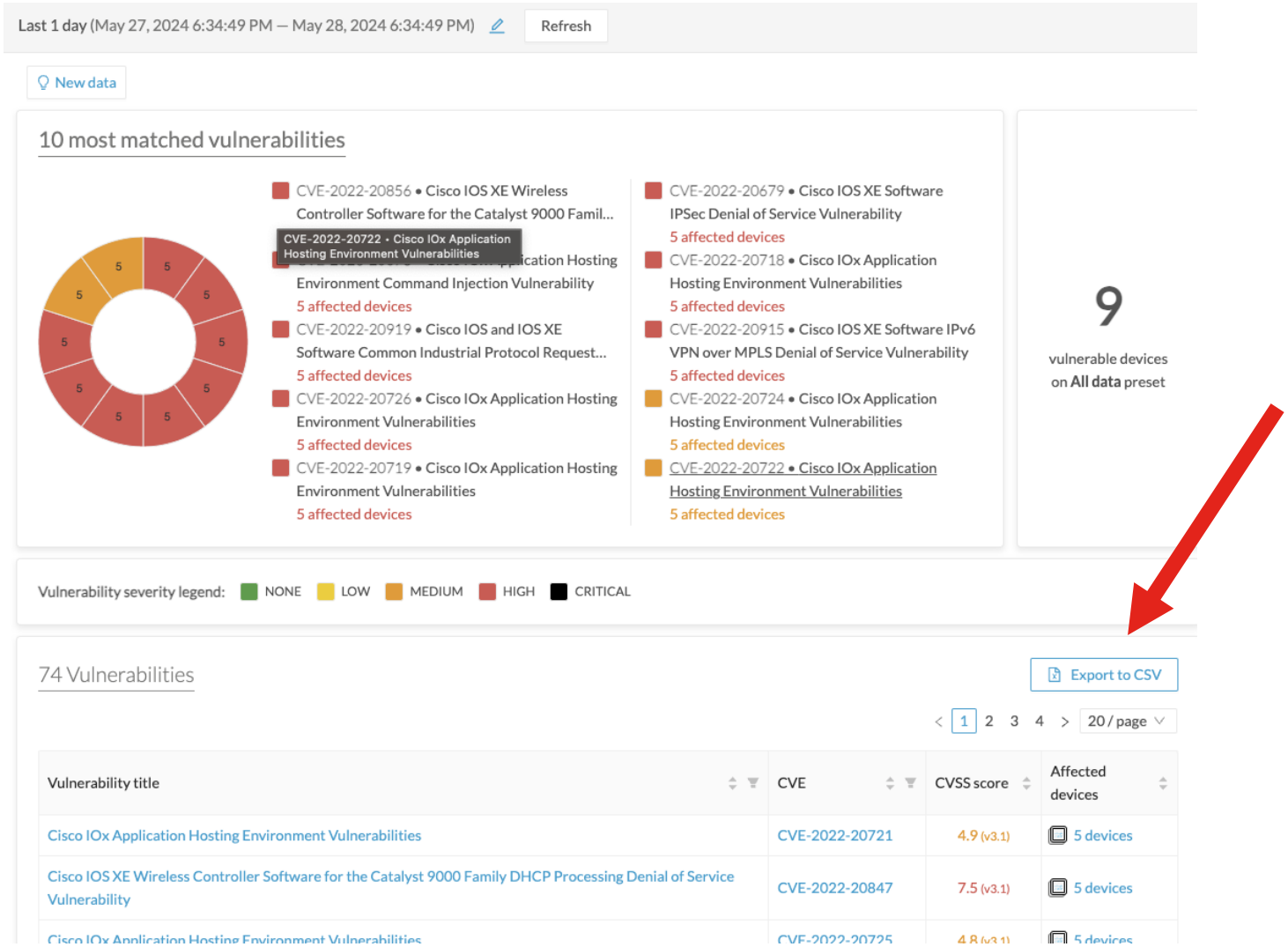
Identify vulnerabilities to assess risks

- 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



Export detected vulnerabilities

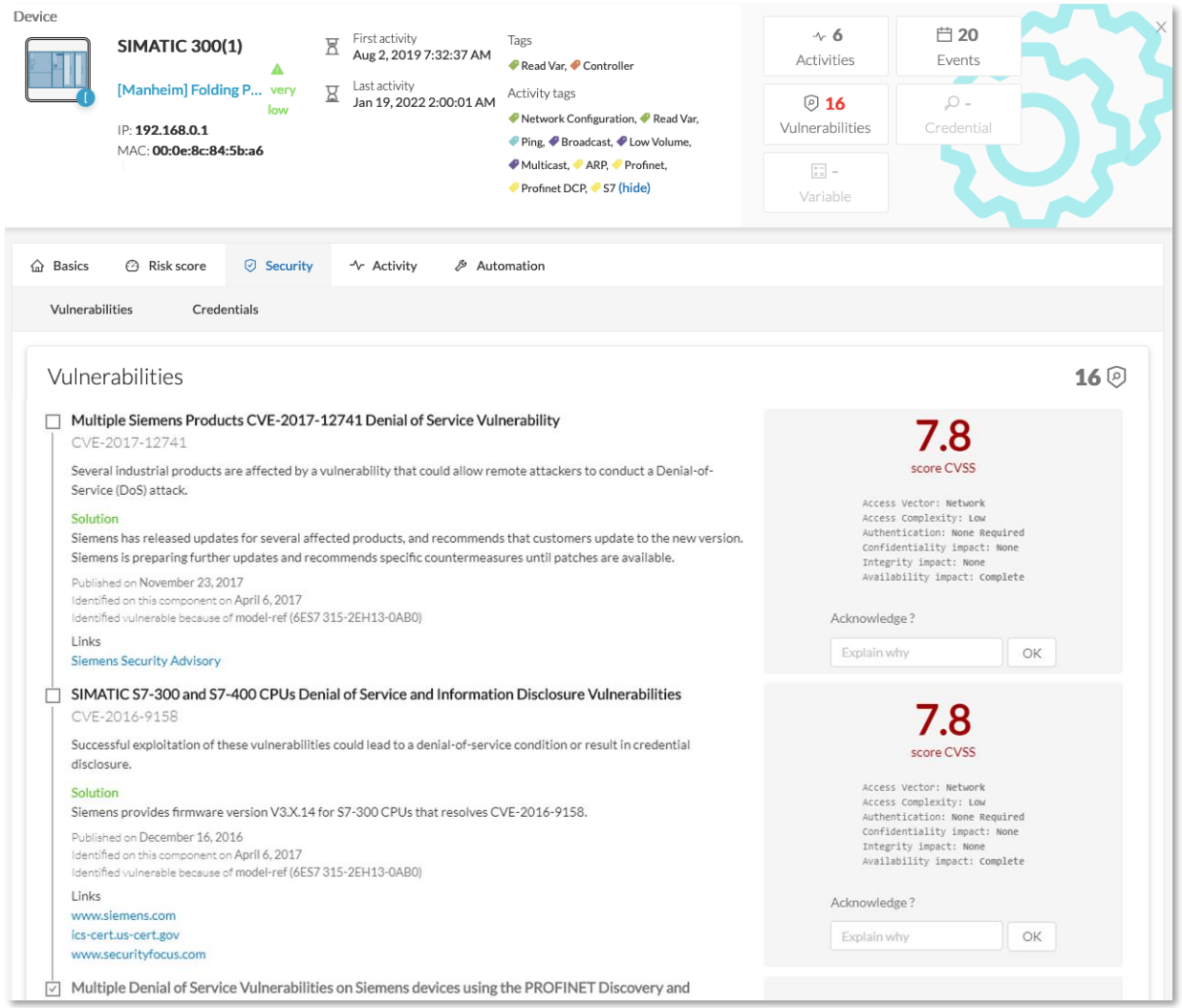
Detected vulnerabilities can be exported for offline review, audit and documentation.



Drive vulnerability remediation

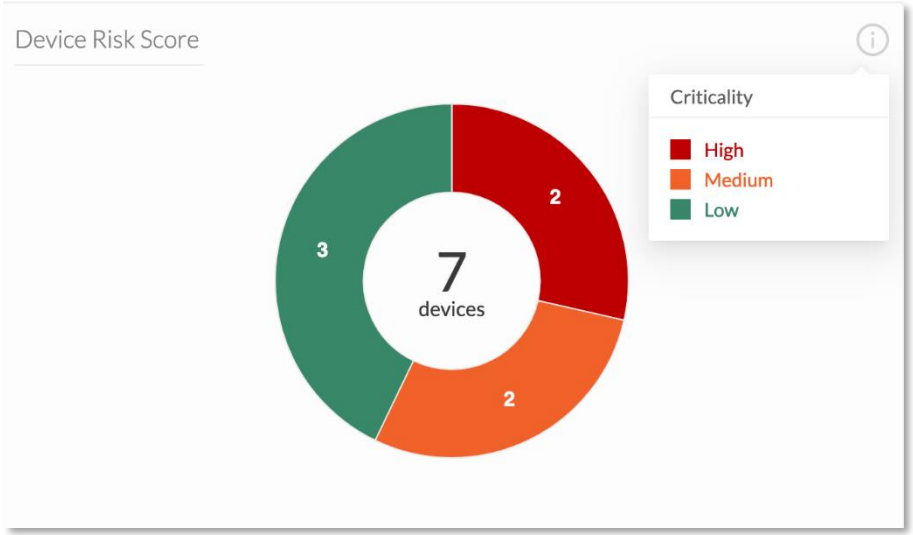
- Automatically spot software & hardware vulnerabilities
- Access comprehensive information on vulnerability severities and solutions
- Track vulnerability acknowledgements
- Built-in vulnerability database curated by Cisco Research Teams always up to date

Enforce cybersecurity best practices



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

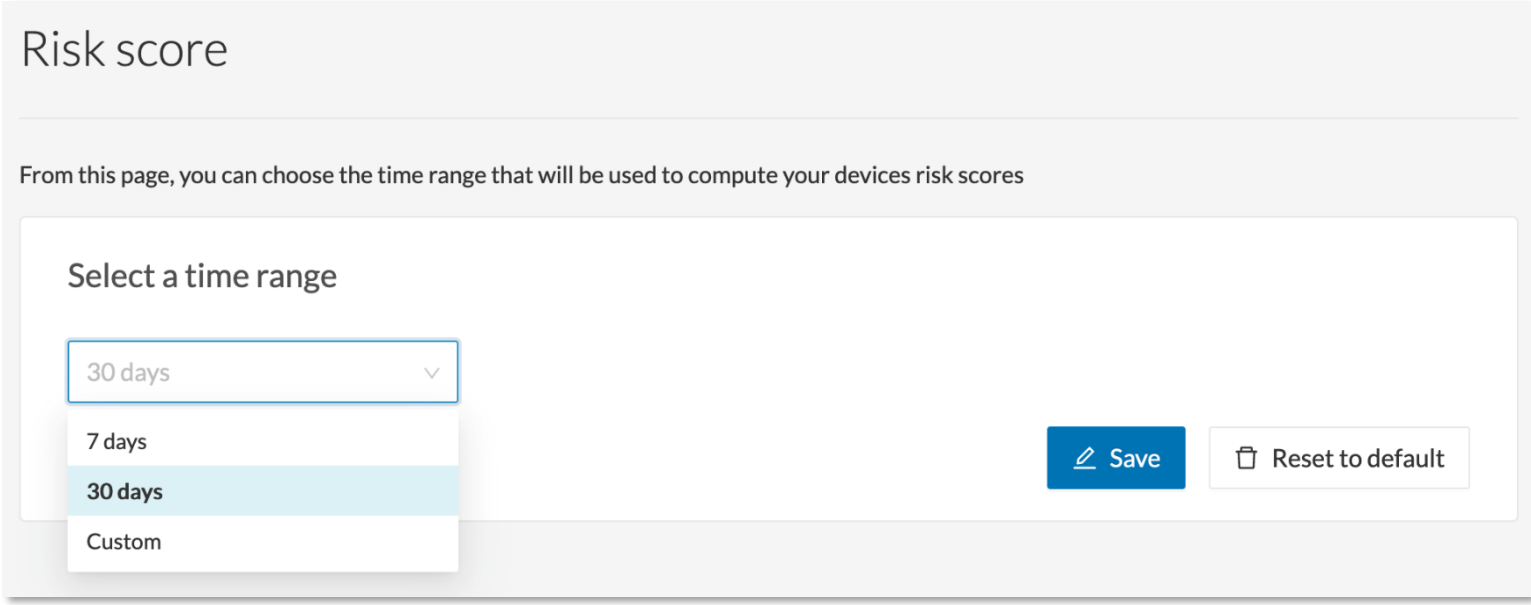
- Risk = Likelihood x Impact
- Likelihood
  - Activity tags (some communications create more risks)
  - Exposure to external IP addresses
  - Discovered vulnerabilities
- Impact
  - Device tags (some devices can create more damages)
  - User-defined industrial impact for groups

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

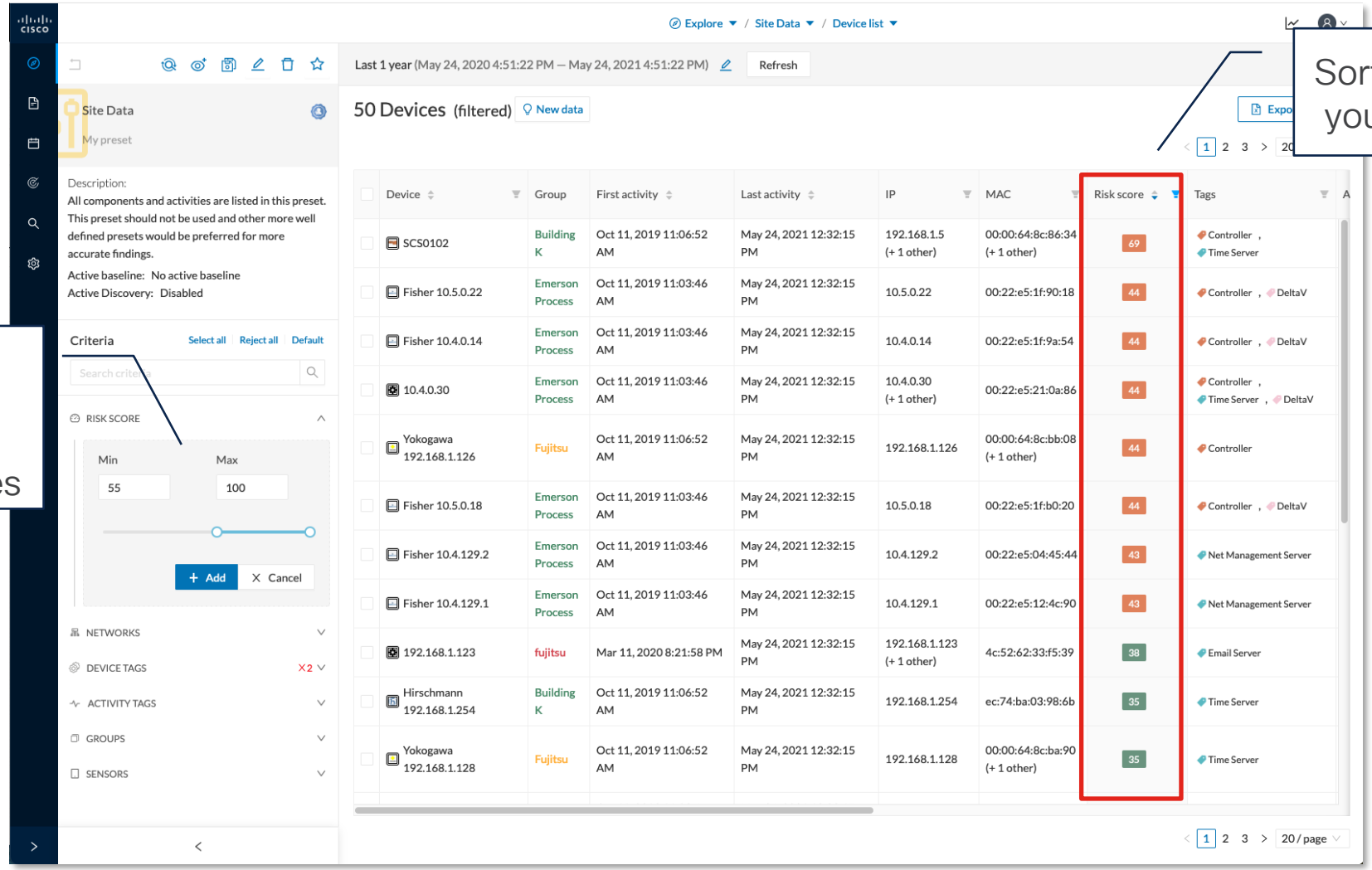
Define impact of Activities to Risk Score

- Configure what length of time activities impact calculated risk score



Quickly identify “Riskiest” devices

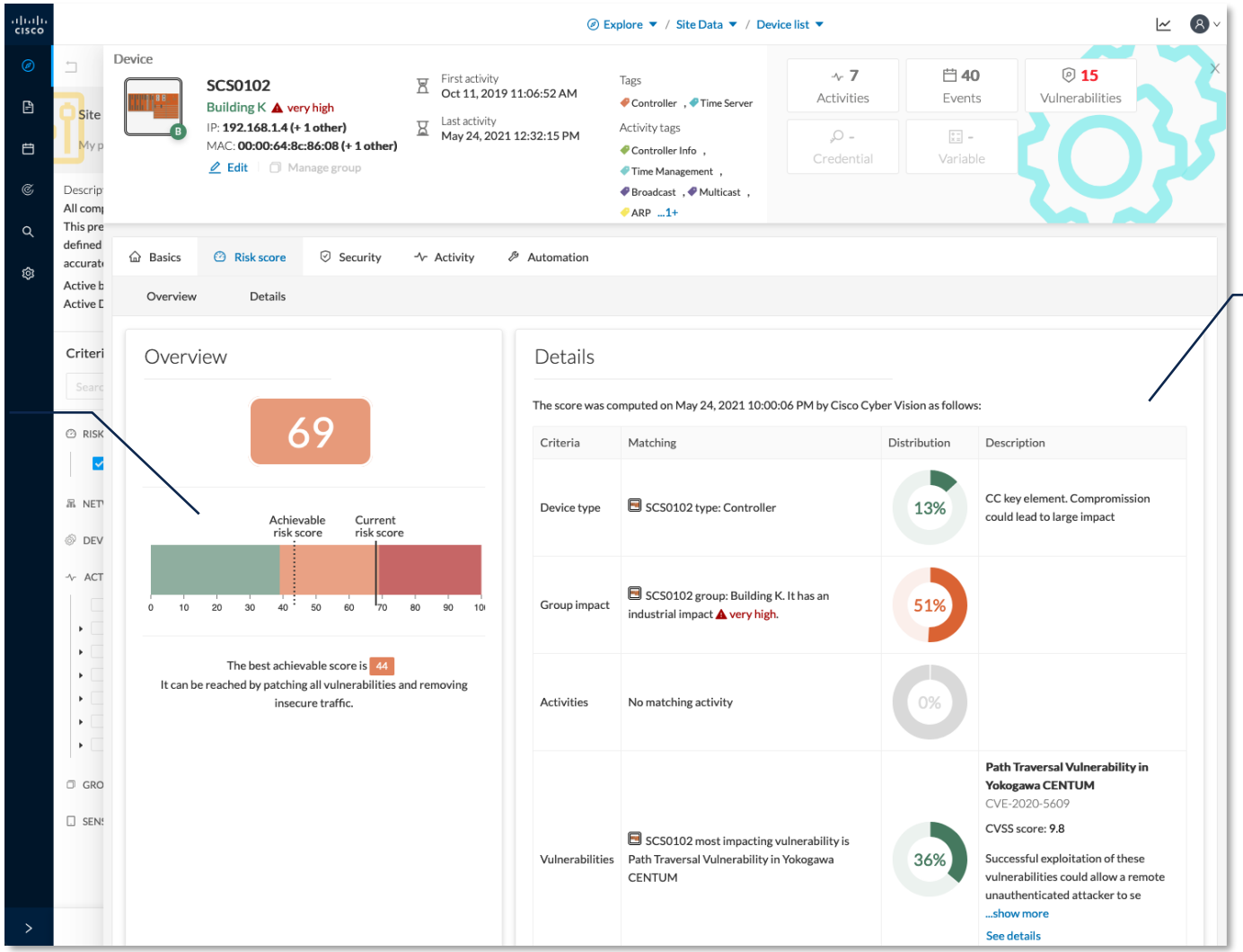
Create presets based on risk thresholds and convert to baselines



Sort and filter risks in your lists of devices

Reducing a device risk score

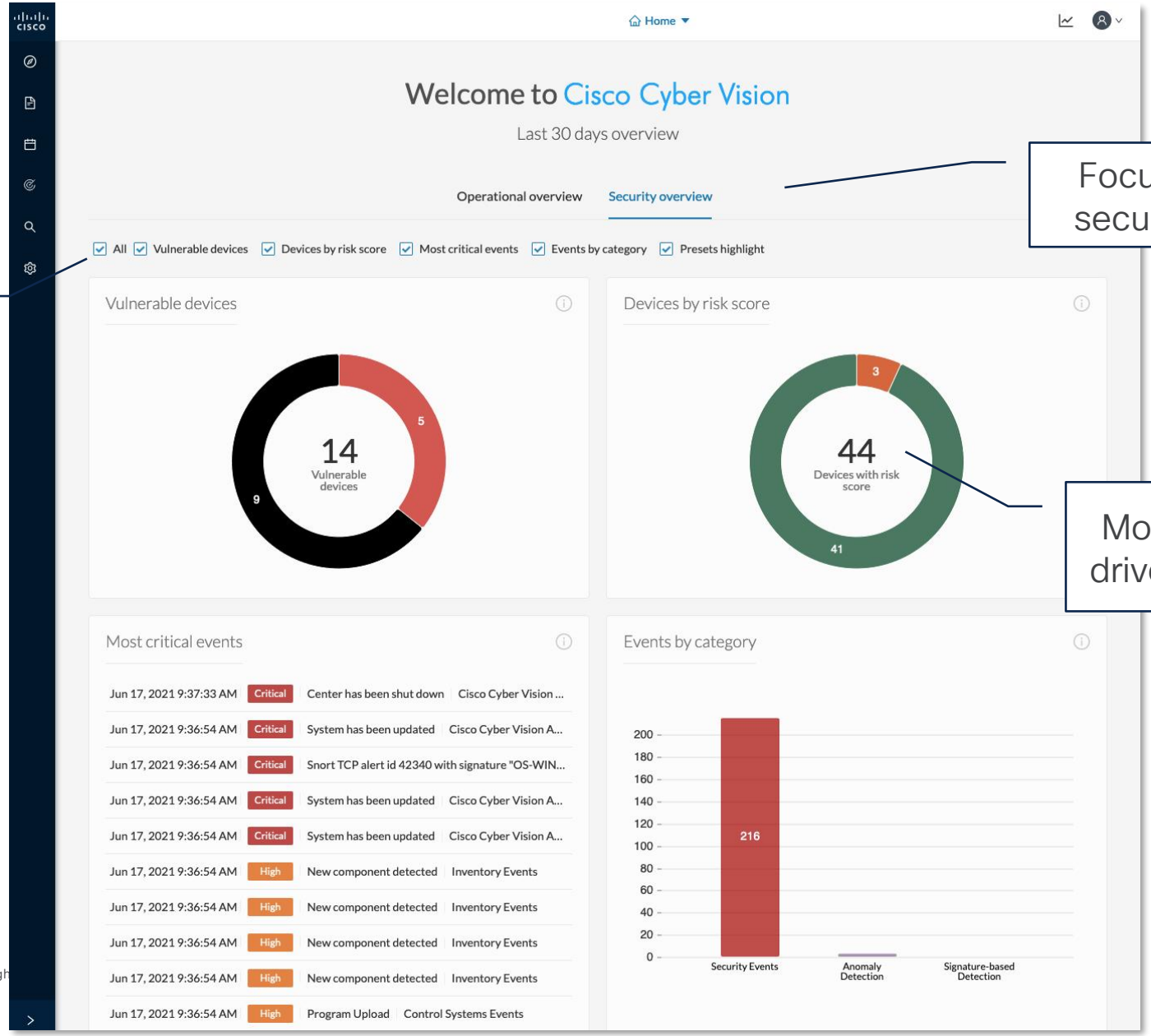
Understand where you are, and where you could be



Understanding what impacts the score

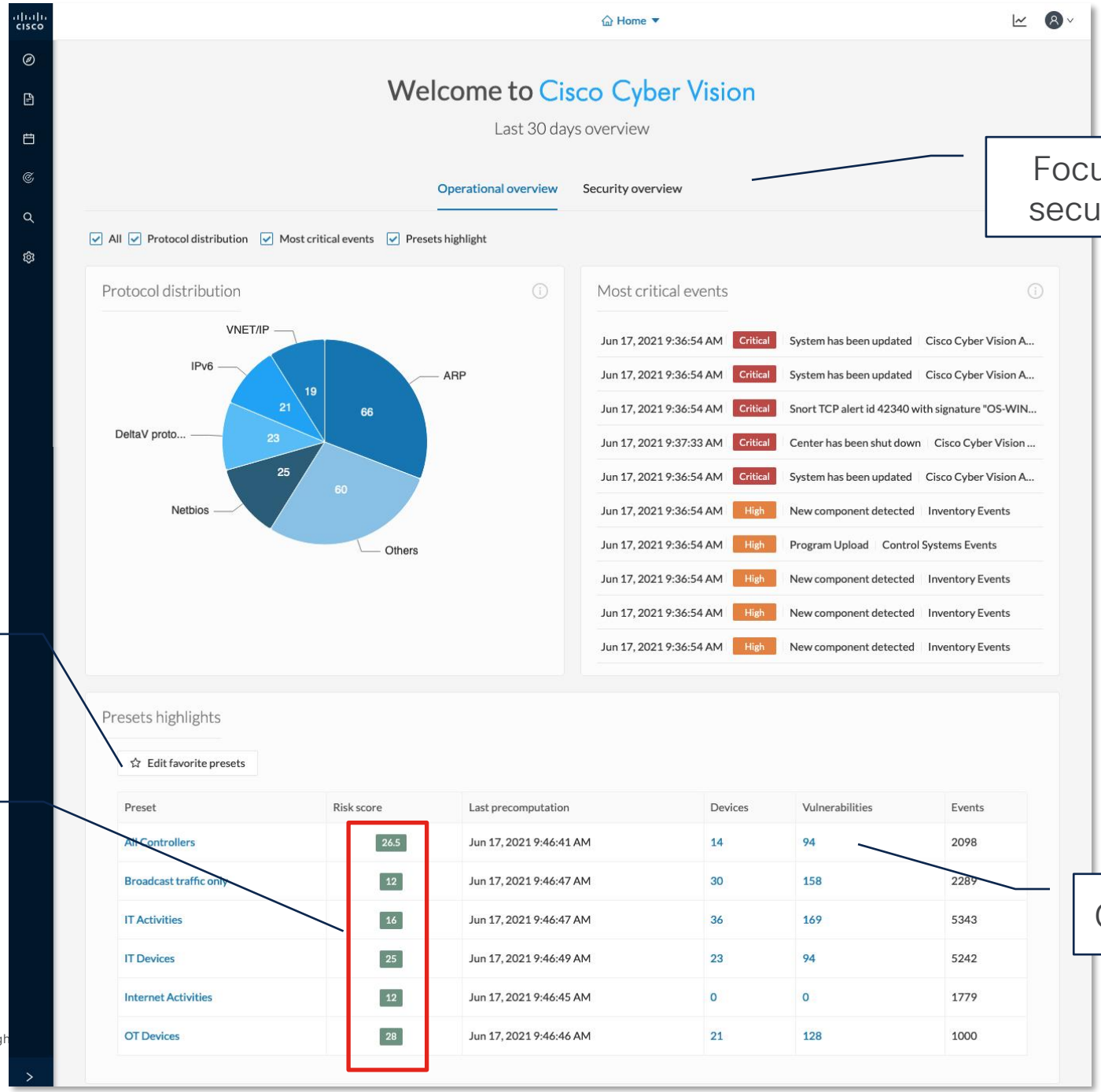
Customizable dashboards to surface information

Choose widgets to customize home



Focus on OT or security insights

Monitor risks and drive improvement



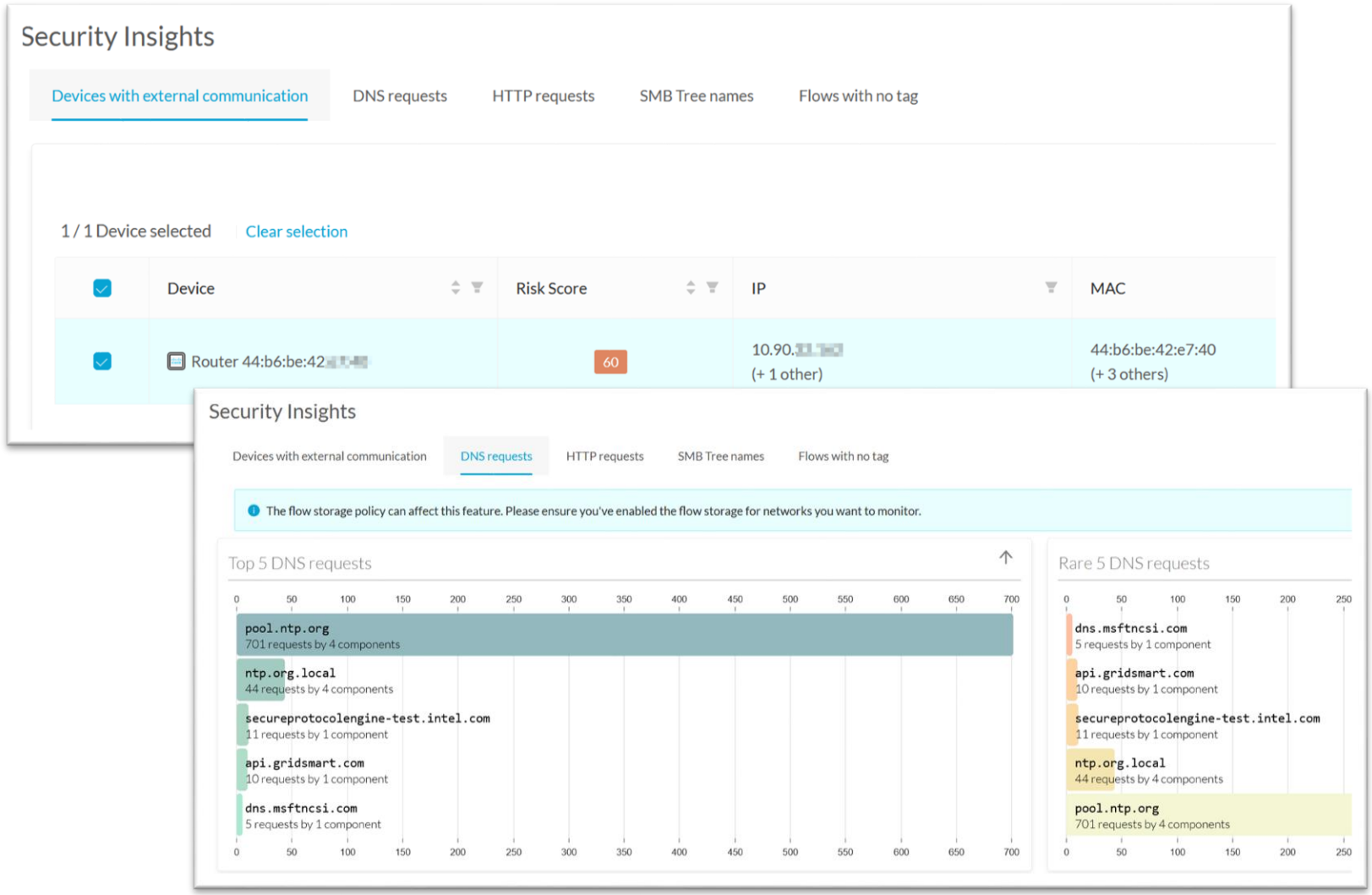
Focus on OT or security insights

Ability to pin specific presets to home dashboard

Quickly identify “Riskiest” presets

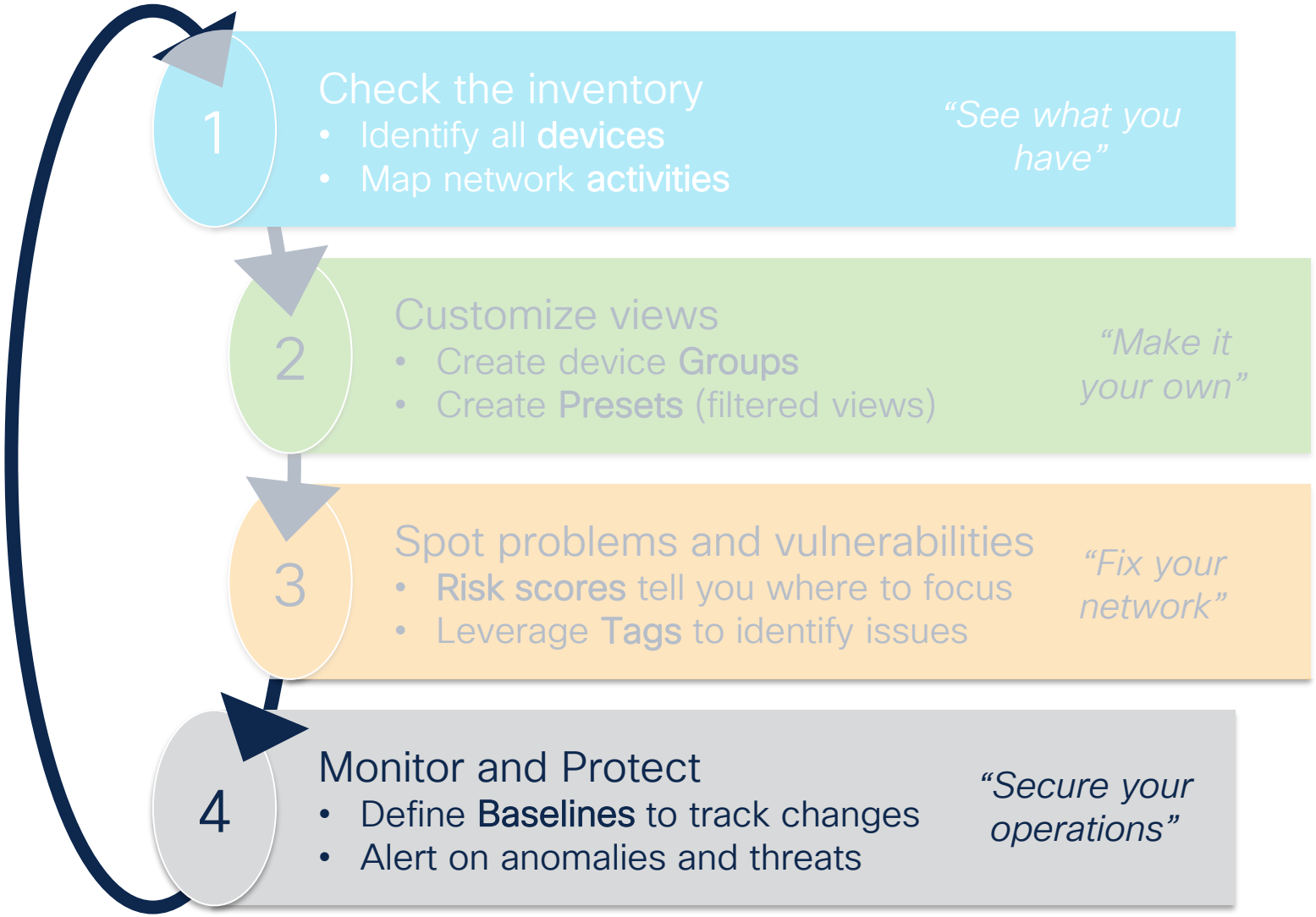
Counters per preset

Easily spot important IT security information

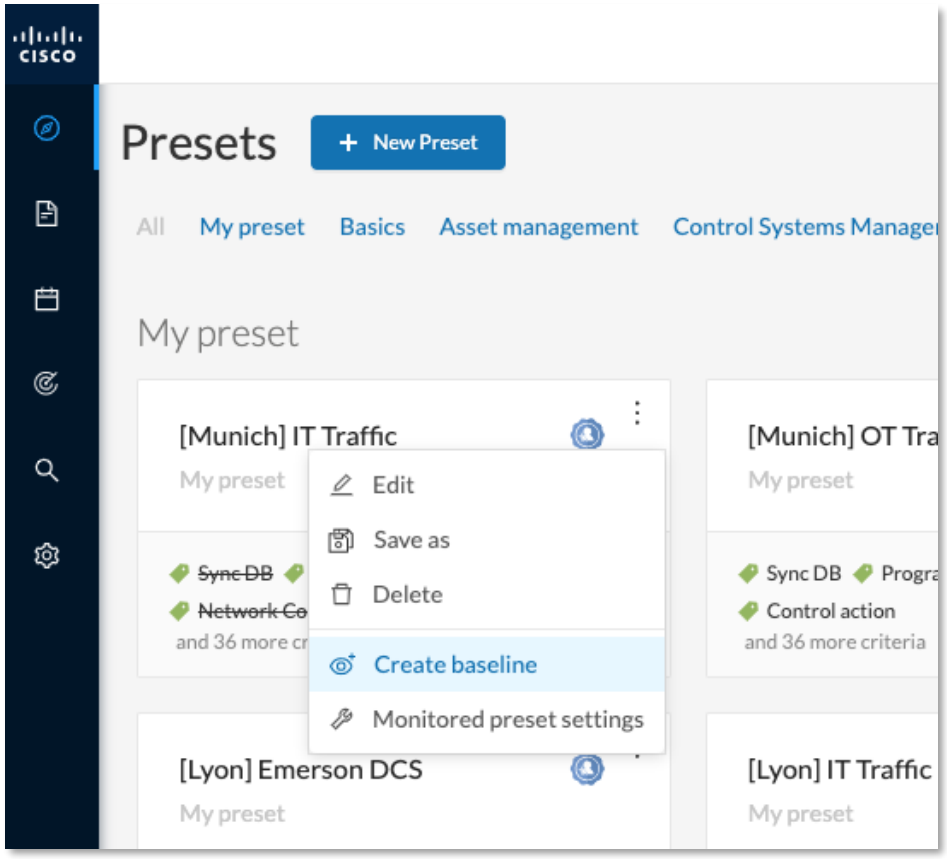


- External Communication
- Top / Rare DNS requests
- Top / Rare HTTP requests
- Top / Rare SMB usage
- Unclassified “strange” flows

The Cyber Vision Workflow



Identify changes to environment using baselines

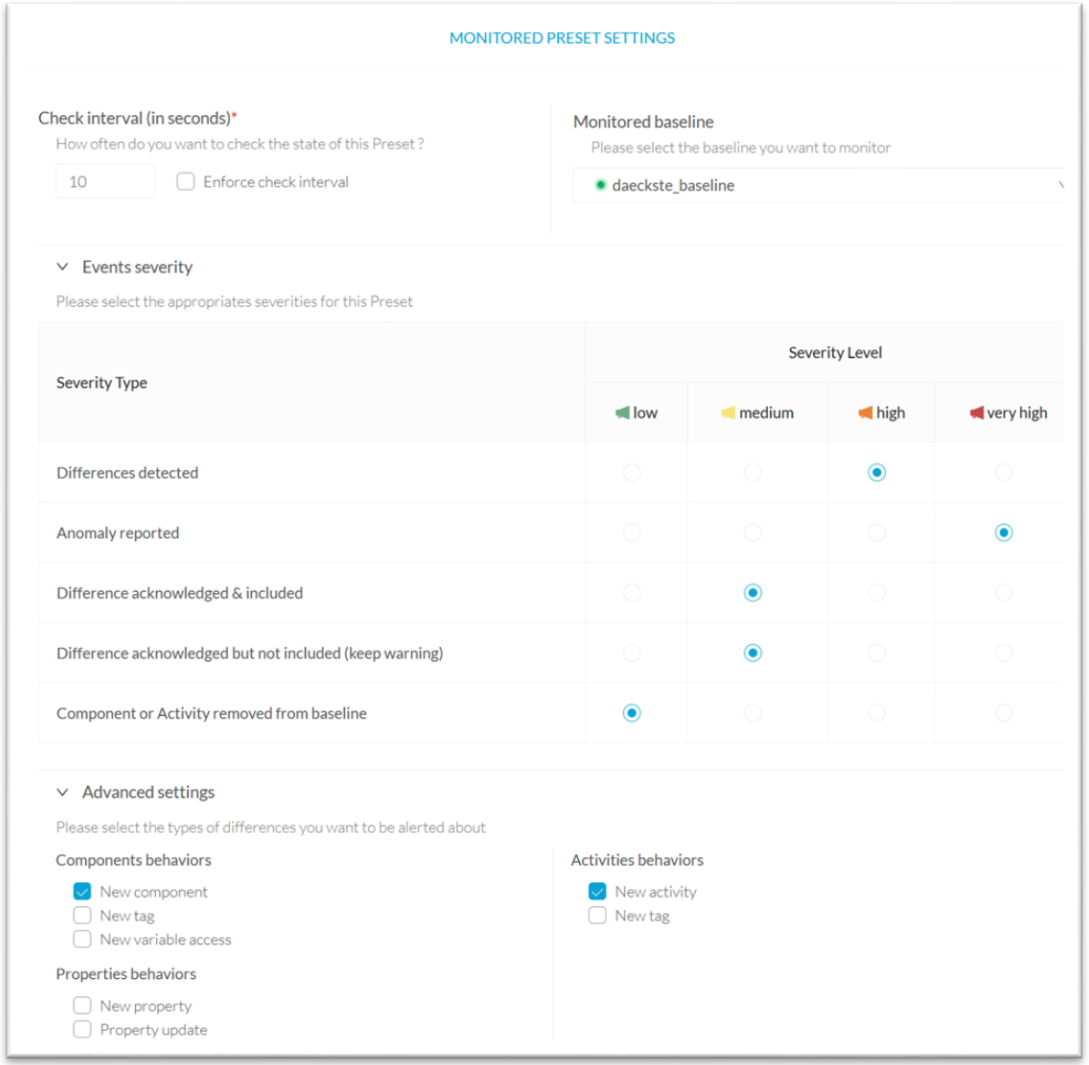


Leverage presets to focus monitoring on parts of the environment

- 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.

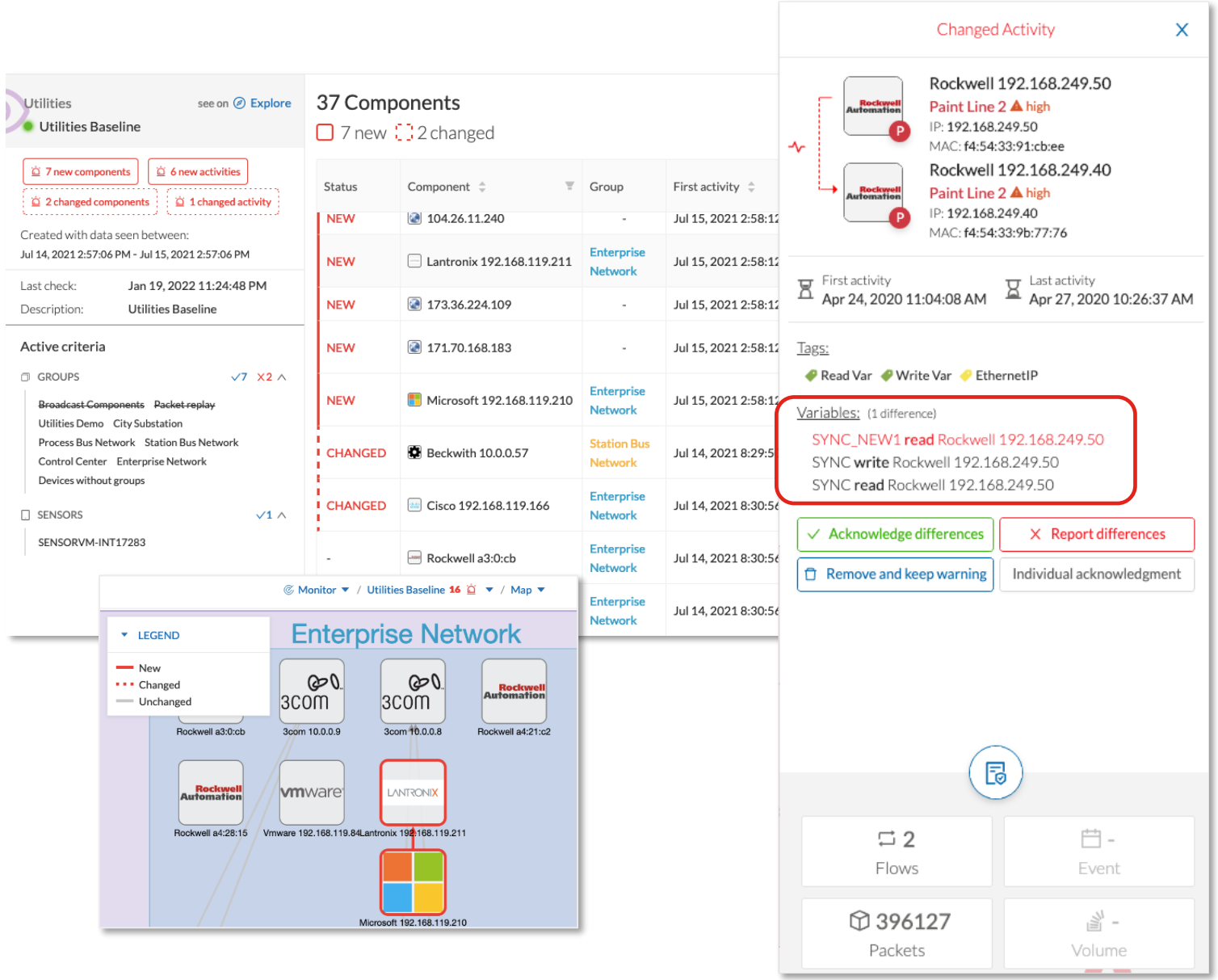
Advanced Options for Baselines



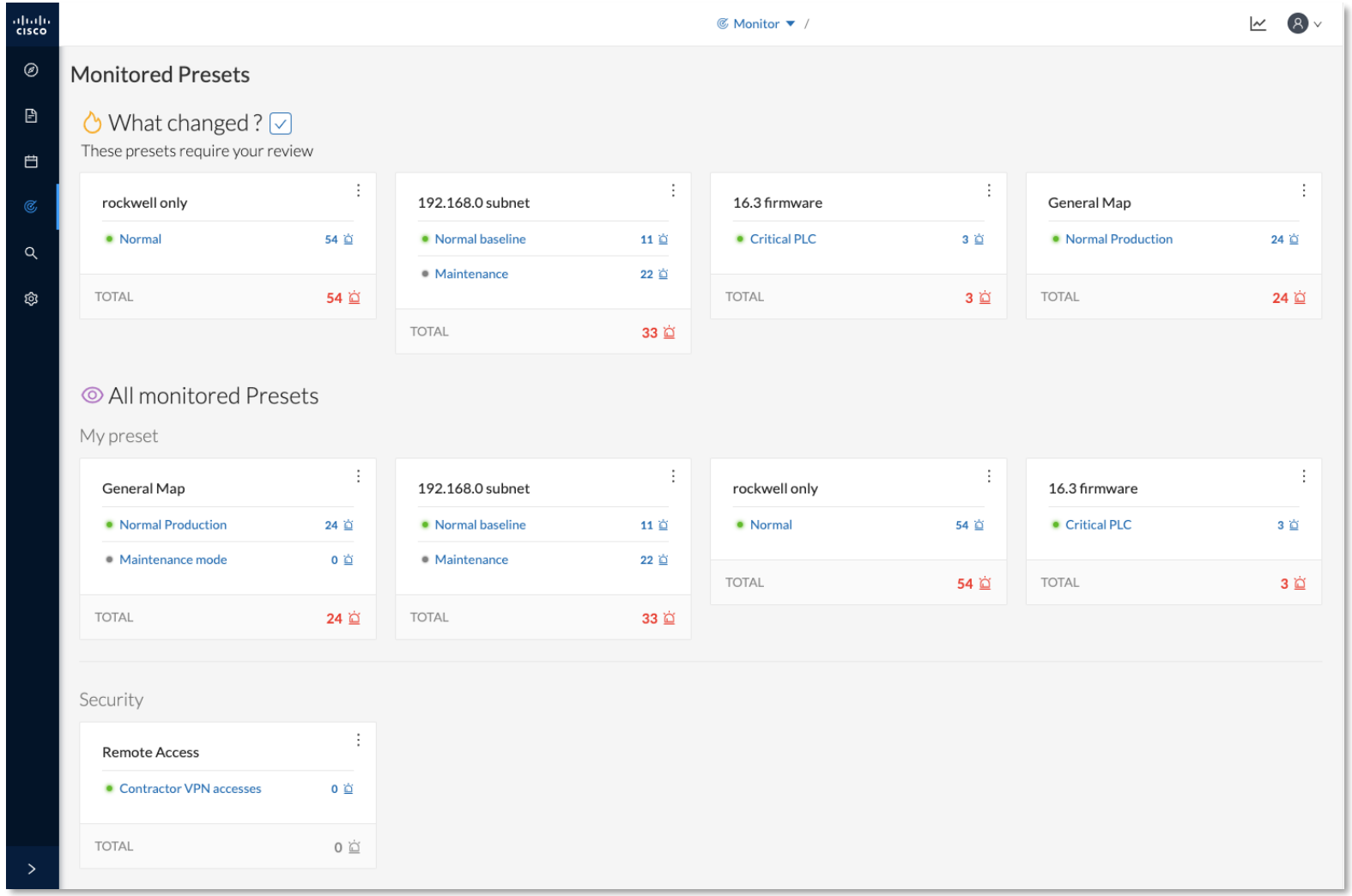
- Created baselines have the options to define custom settings for:
  - Frequency for checking for deviations
  - Security event severity threshold
  - Components behavior
  - Properties behavior
  - Activities behavior

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



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

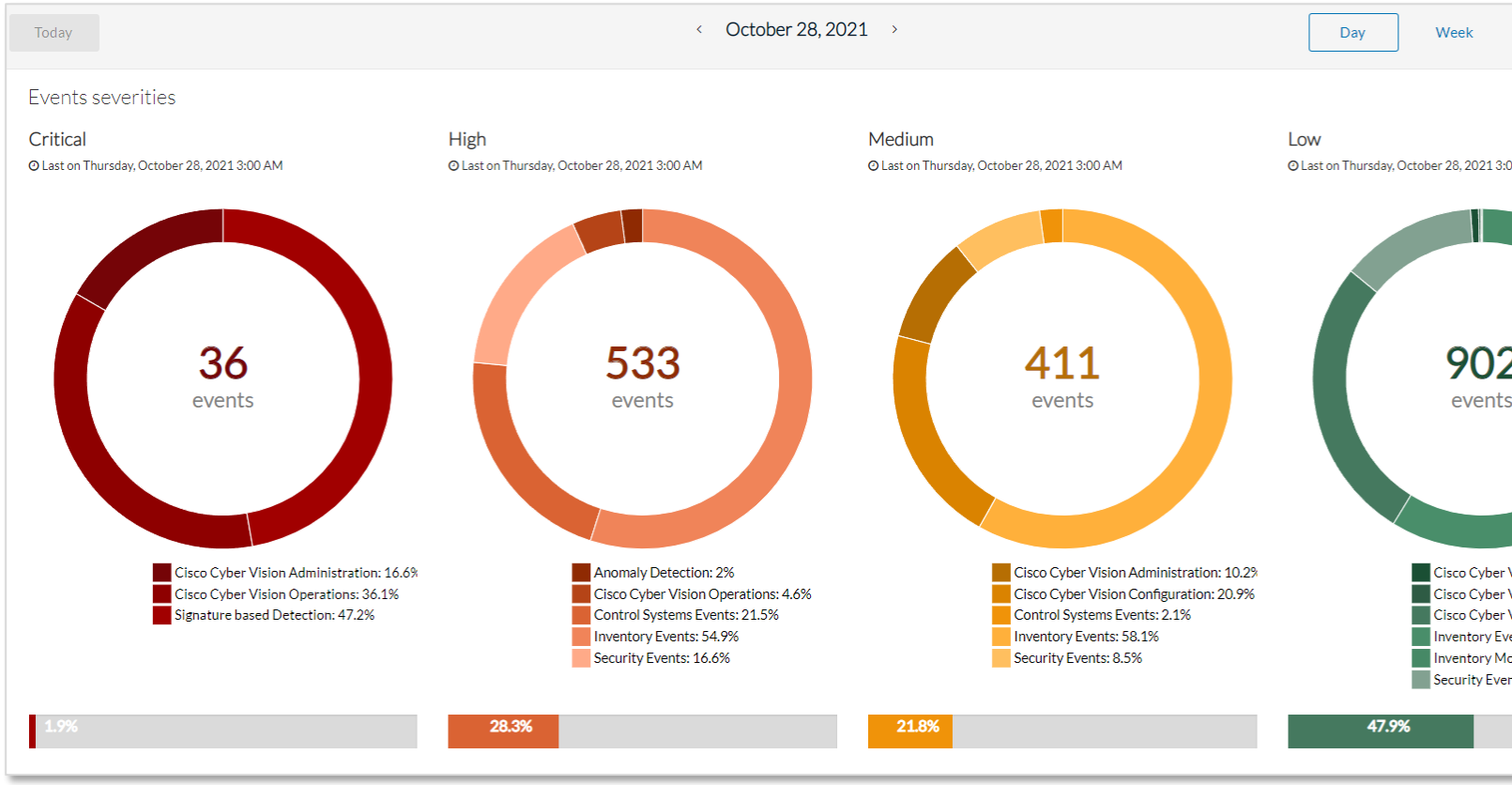
Events: The high-level overview

Easily track everything happening within the industrial network

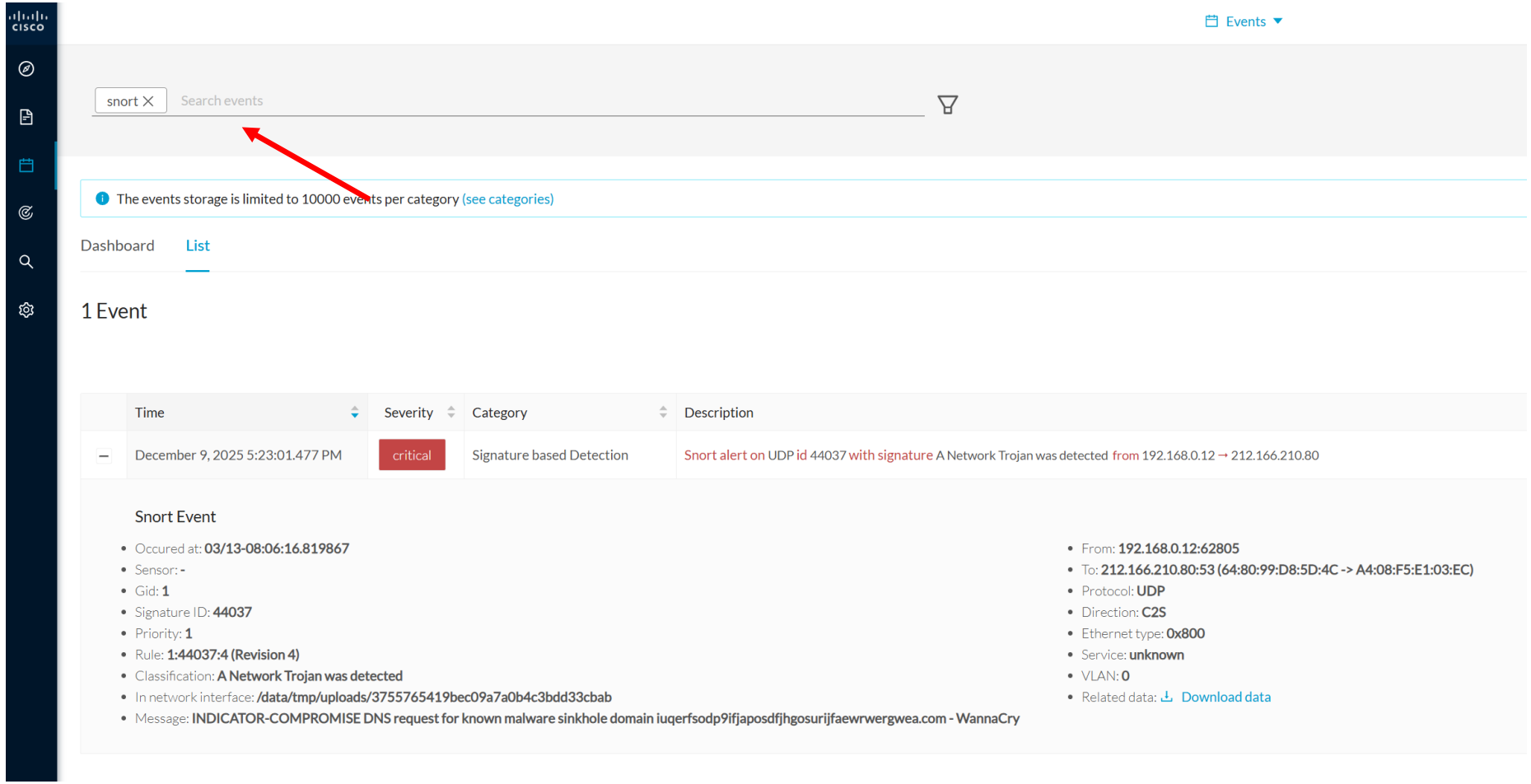
- Security events (vulnerabilities, port scan, protocol exception…)
- Signature-based detection (Snort IDS)
- Control systems events (variable changes, program upload, stop/start CPU…)
- Asset inventory (New or modified asset…)
- Changes to the Cyber Vision platform (user login, config changes…)

All events automatically sorted by criticality levels

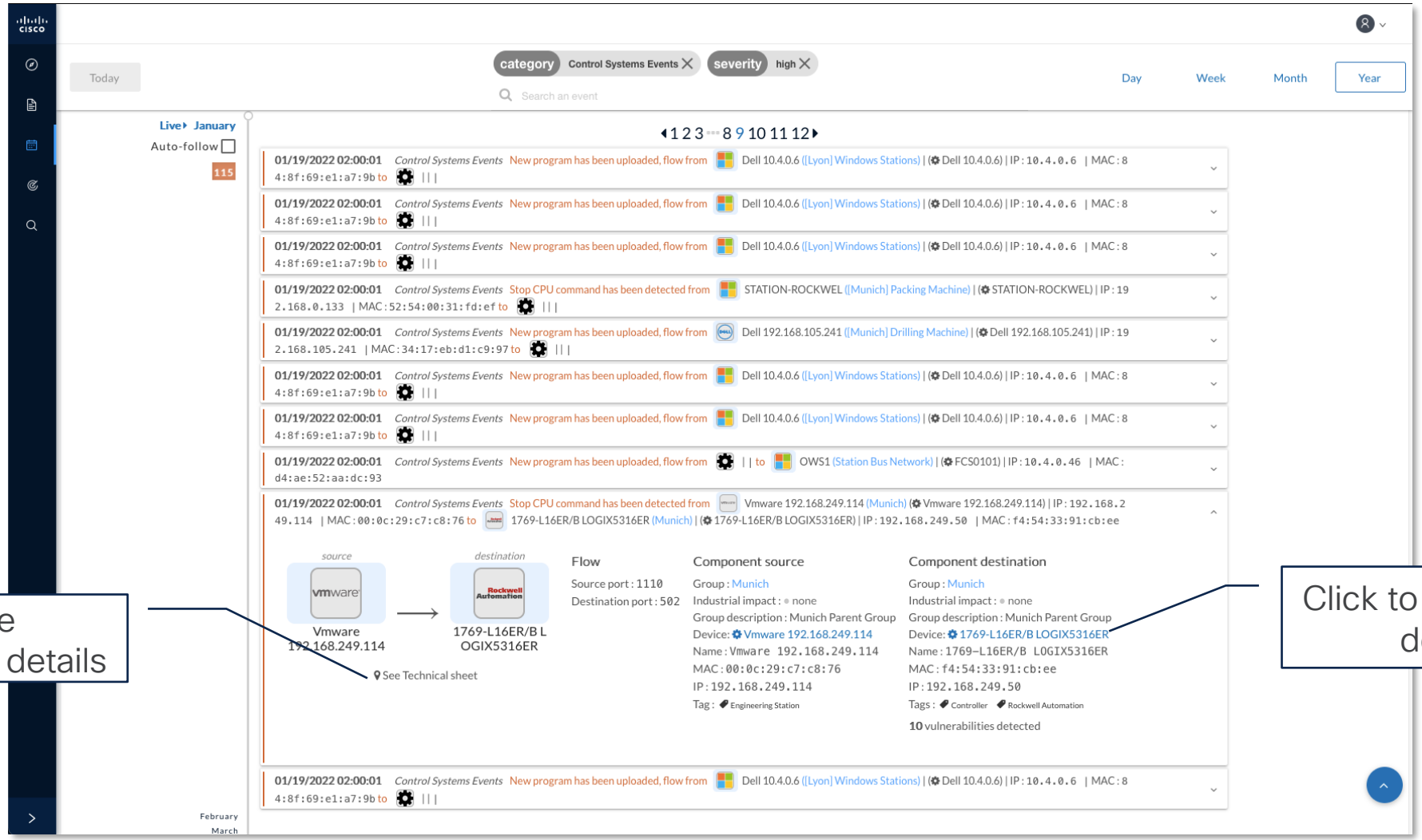
All events can be exported to SIEM and SOC via Syslog



Easily filter and search Events to ease investigations



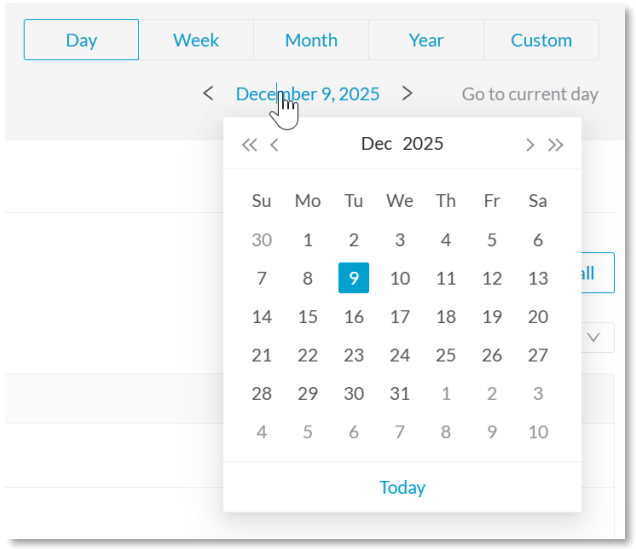
Rich context added to all events

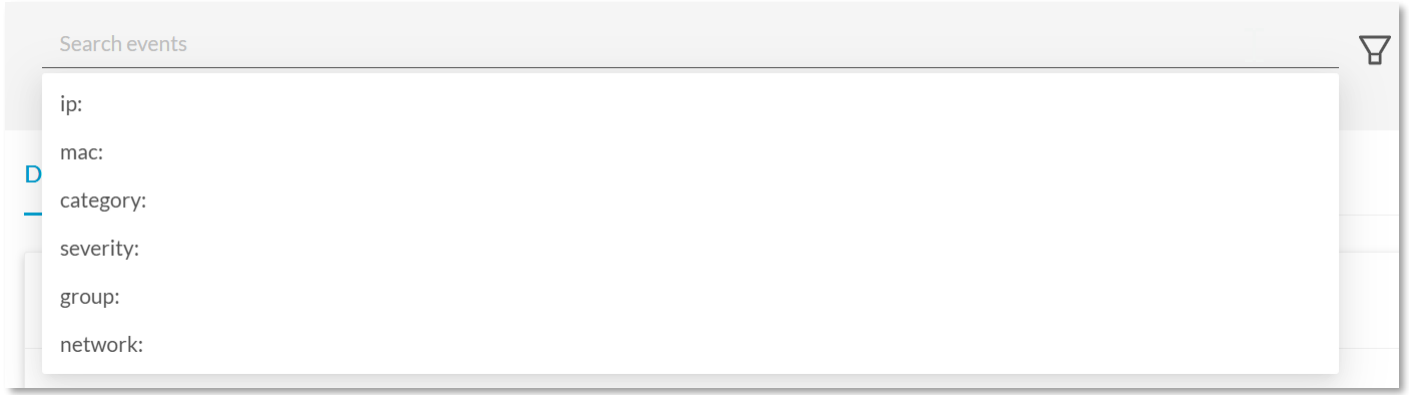


Click to see communications details

Click to see device details

Filter Events based on Category and Time





Cyber Vision gives OT context to security analysts

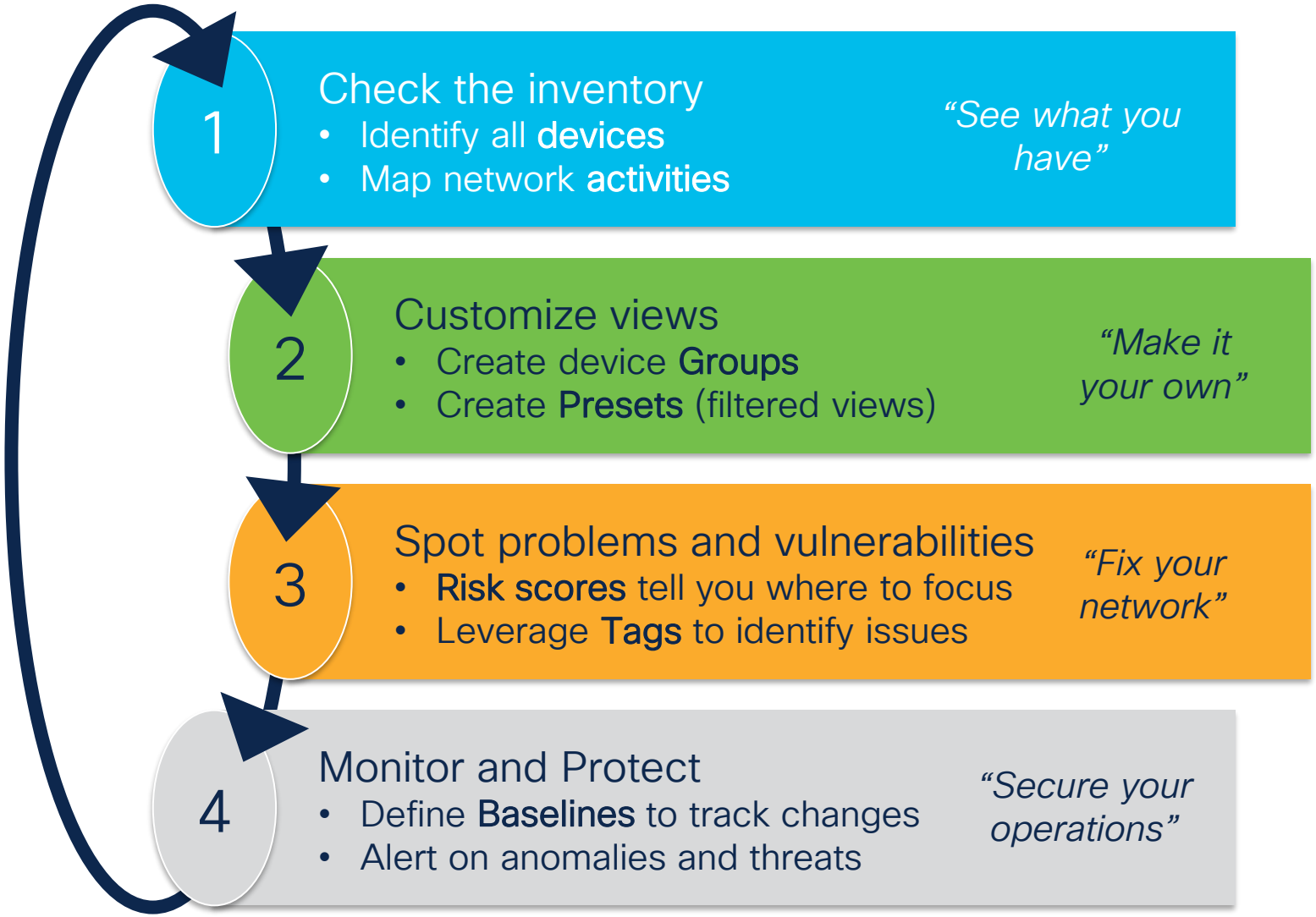
Local OT teams can:

- 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



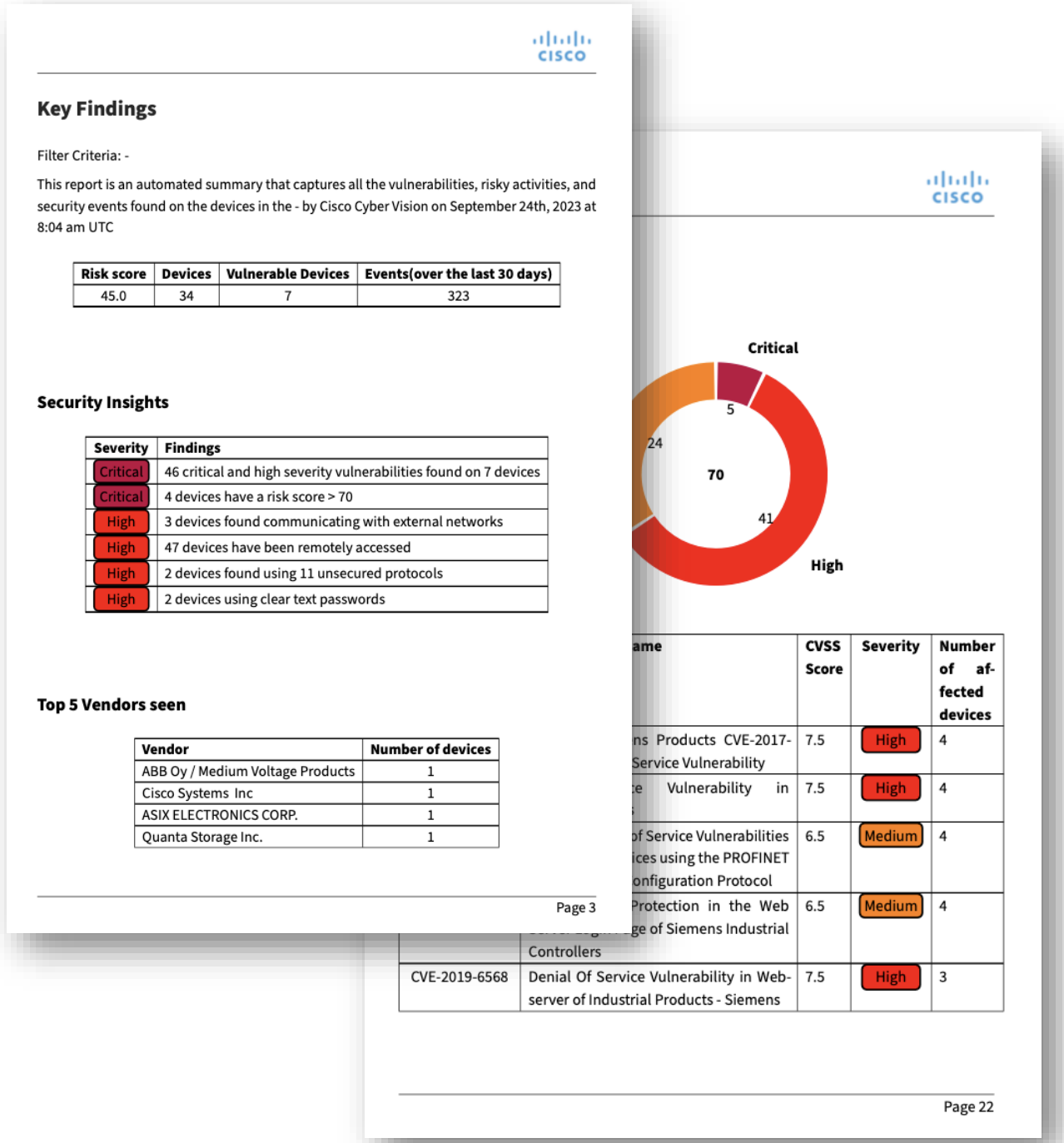
Reporting Extension

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



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

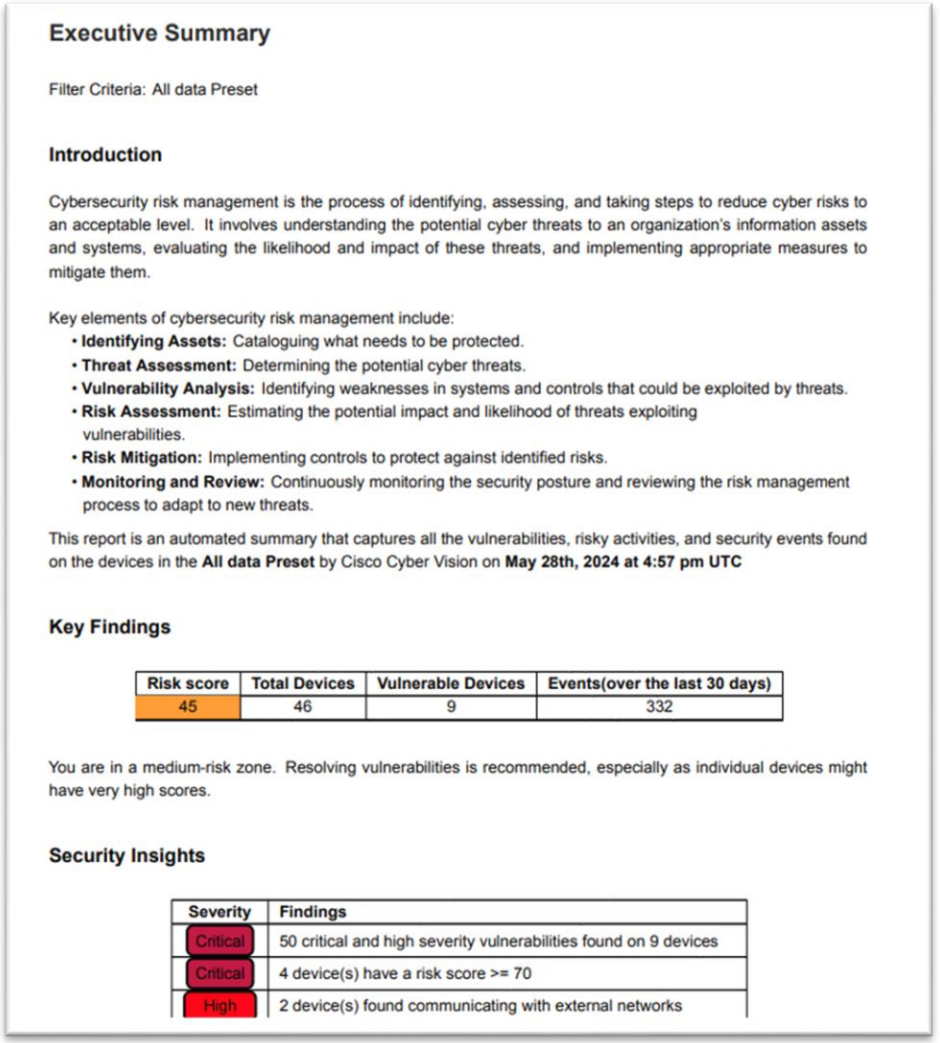
Page 3

	ame	CVSS Score	Severity	Number of af-fected devices
	ns Products CVE-2017-Service Vulnerability	7.5	High	4
	e Vulnerability in	7.5	High	4
	of Service Vulnerabilities ces using the PROFINET onfiguration Protocol	6.5	Medium	4
	Protection in the Web ge of Siemens Industrial Controllers	6.5	Medium	4
CVE-2019-6568	Denial Of Service Vulnerability in Web-server of Industrial Products - Siemens	7.5	High	3

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

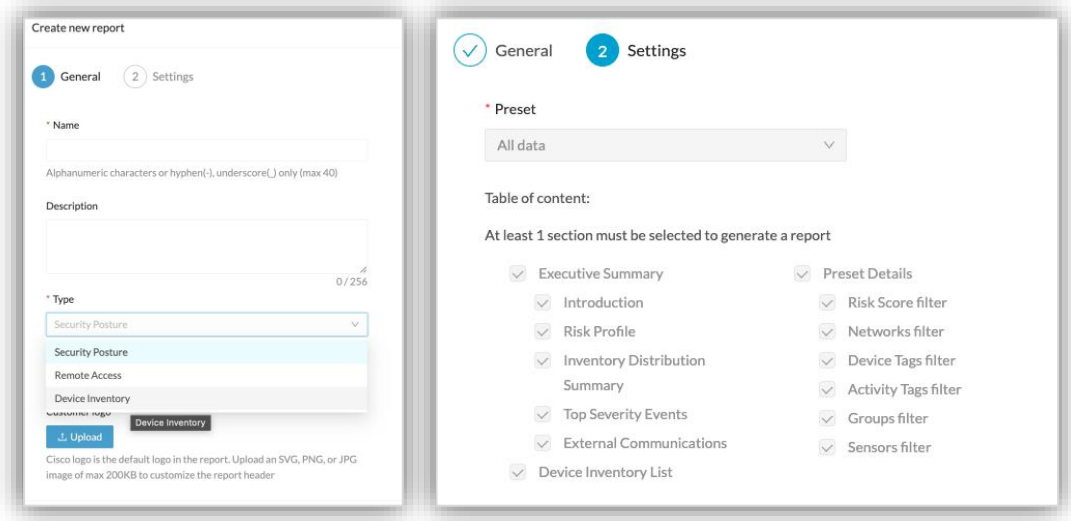
You are in a medium-risk zone. Resolving vulnerabilities is recommended, especially as individual devices might have very high scores.

Security Insights

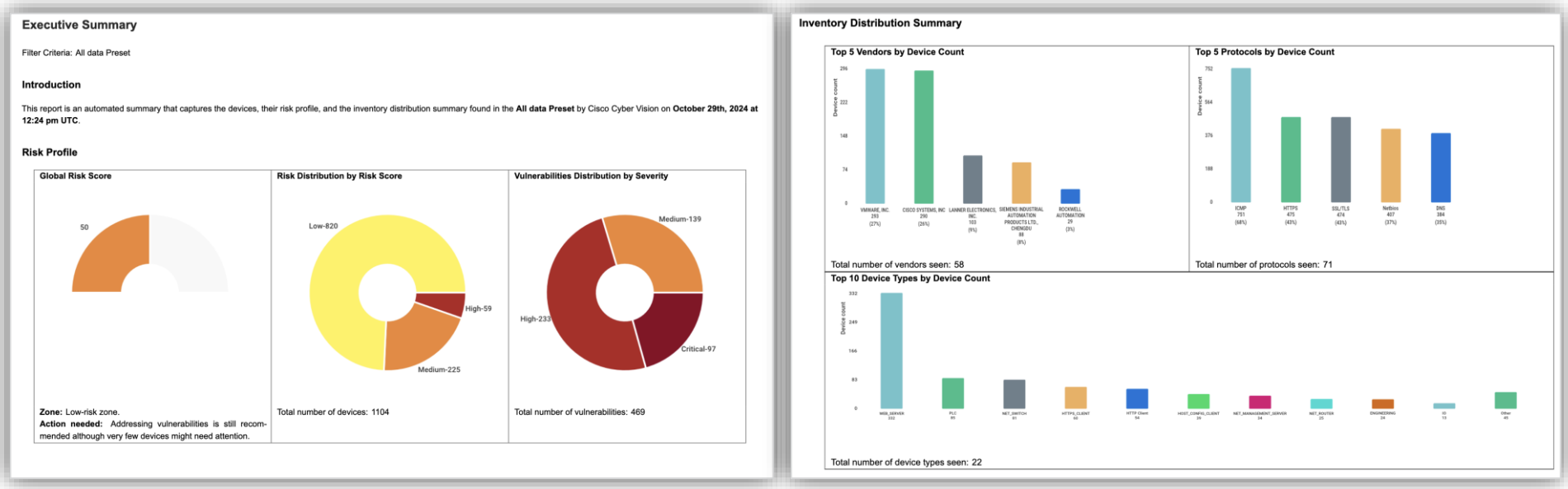
Severity	Findings
Critical	50 critical and high severity vulnerabilities found on 9 devices
Critical	4 device(s) have a risk score >= 70
High	2 device(s) found communicating with external networks

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

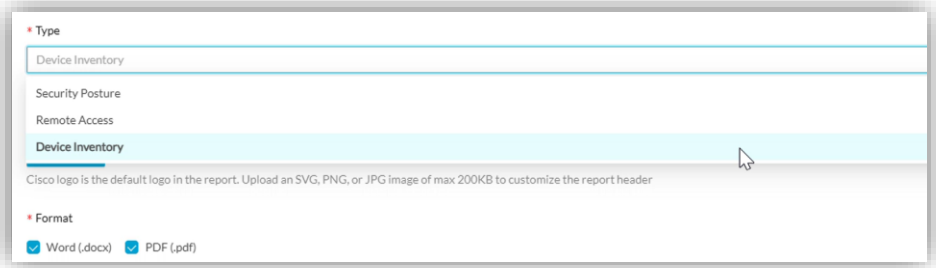


Configuration

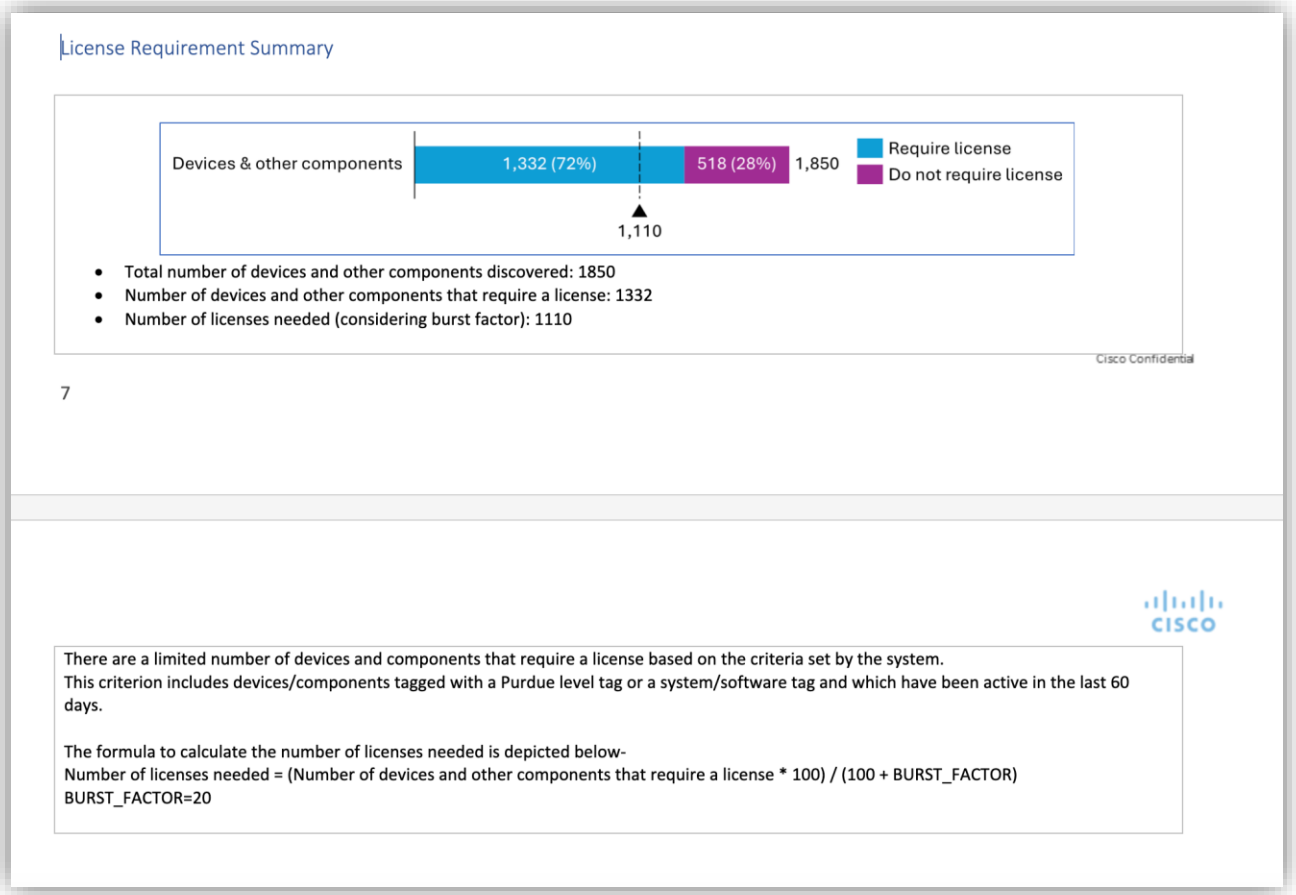


Report example

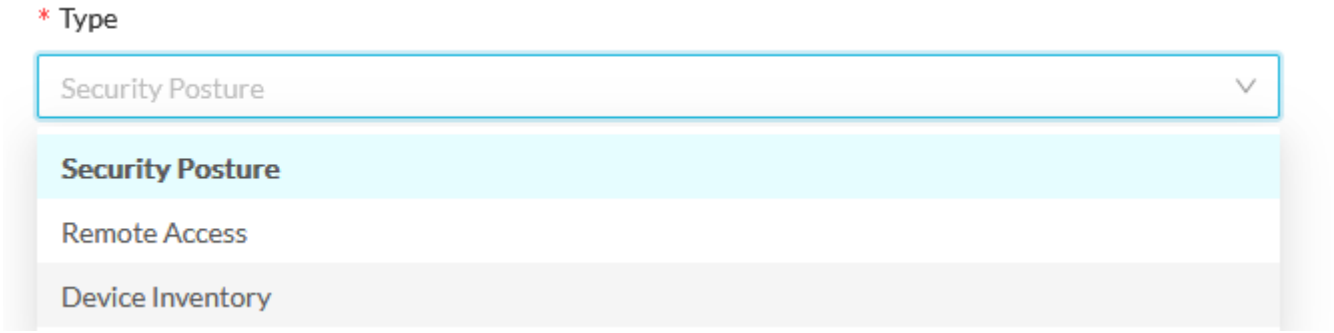
Device Inventory Report: Licensed Devices

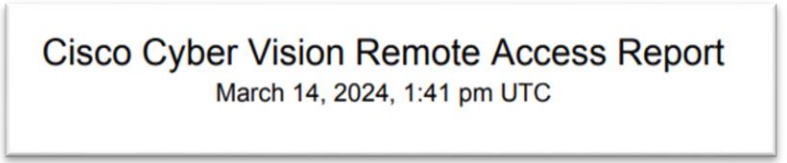


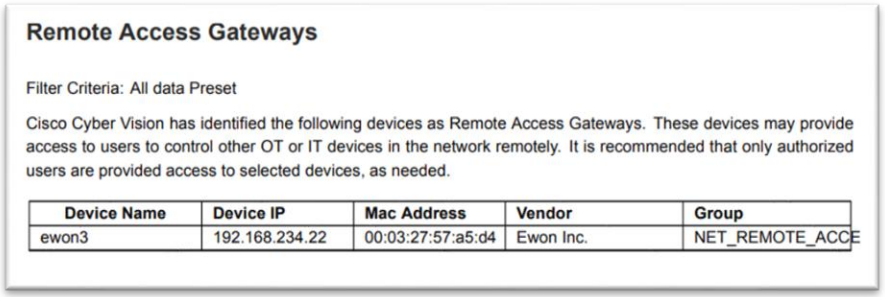
- The Device Inventory Report highlights the Cyber Vision license requirement for your environment.



Remote Access Reports





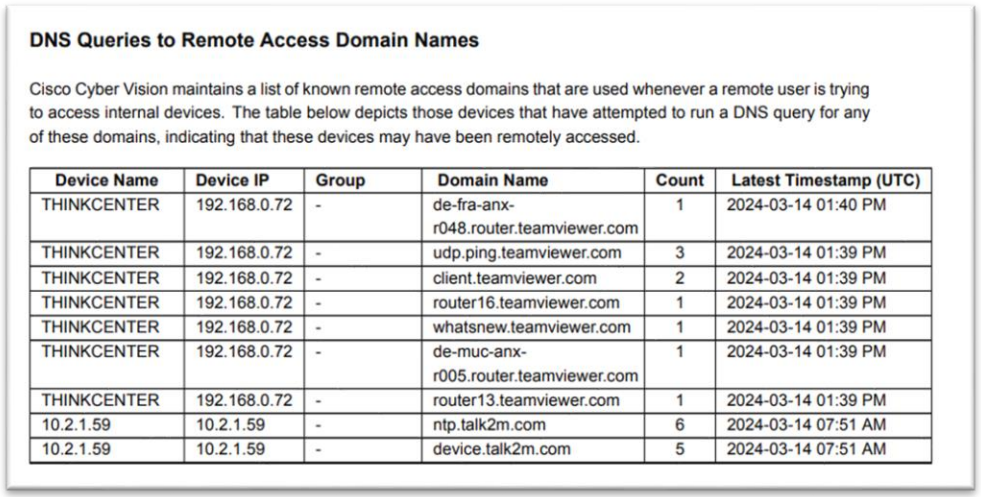


Remote Access Gateways

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



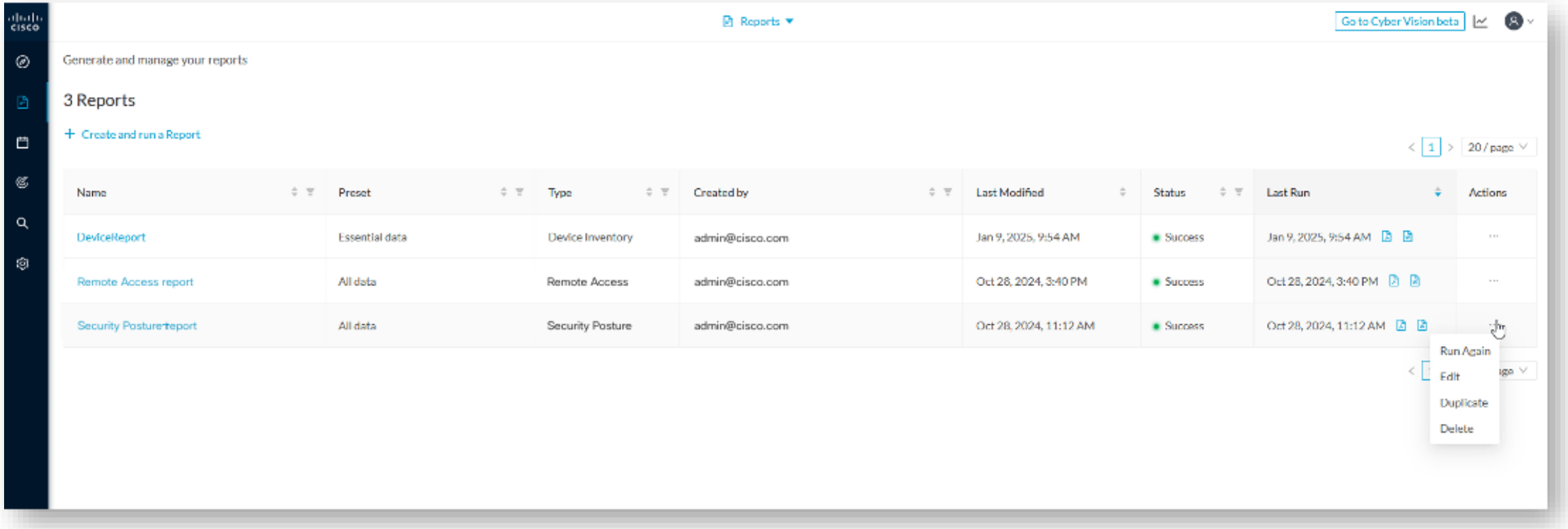
DNS Queries to Remote Access Domain Names

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.

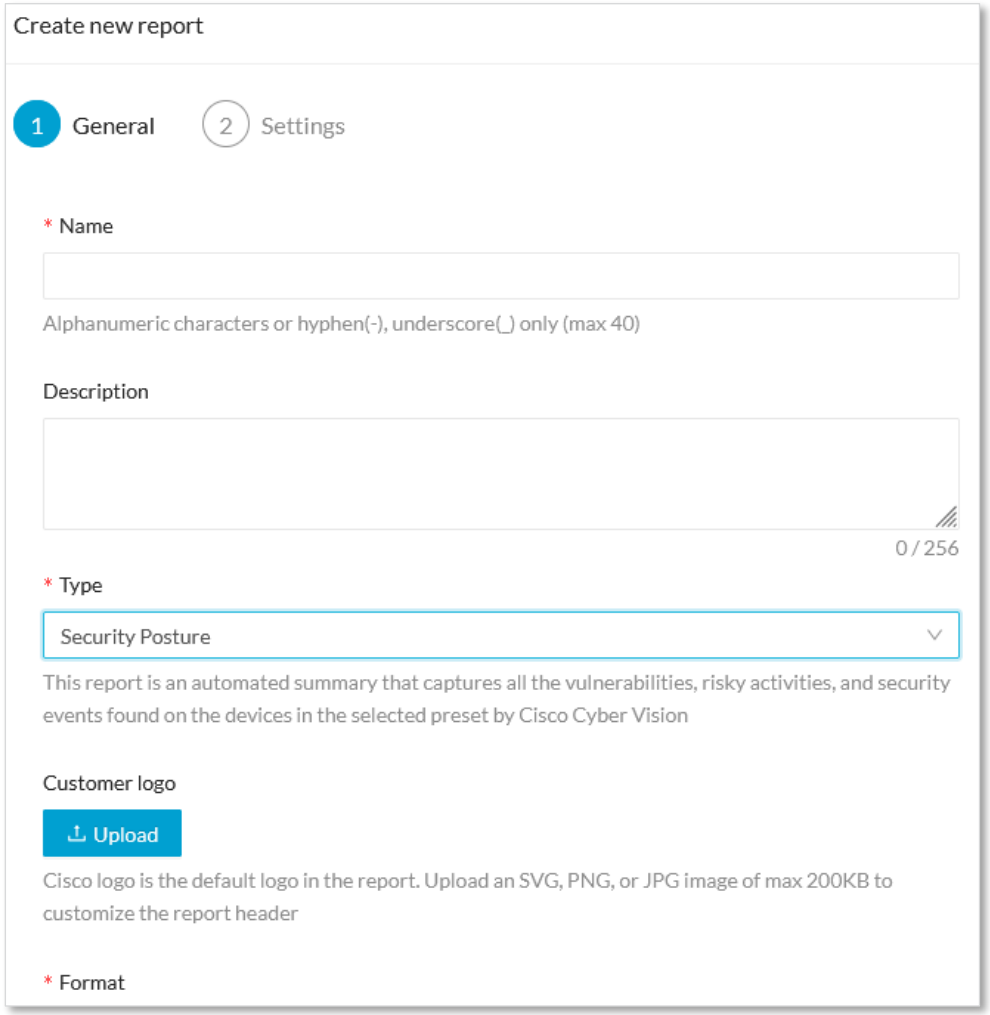
Device Name	Device IP	Group	Domain Name	Count	Latest Timestamp (UTC)
THINKCENTER	192.168.0.72	-	de-fra-anx-r048.router.teamviewer.com	1	2024-03-14 01:40 PM
THINKCENTER	192.168.0.72	-	udp.ping.teamviewer.com	3	2024-03-14 01:39 PM
THINKCENTER	192.168.0.72	-	client.teamviewer.com	2	2024-03-14 01:39 PM
THINKCENTER	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

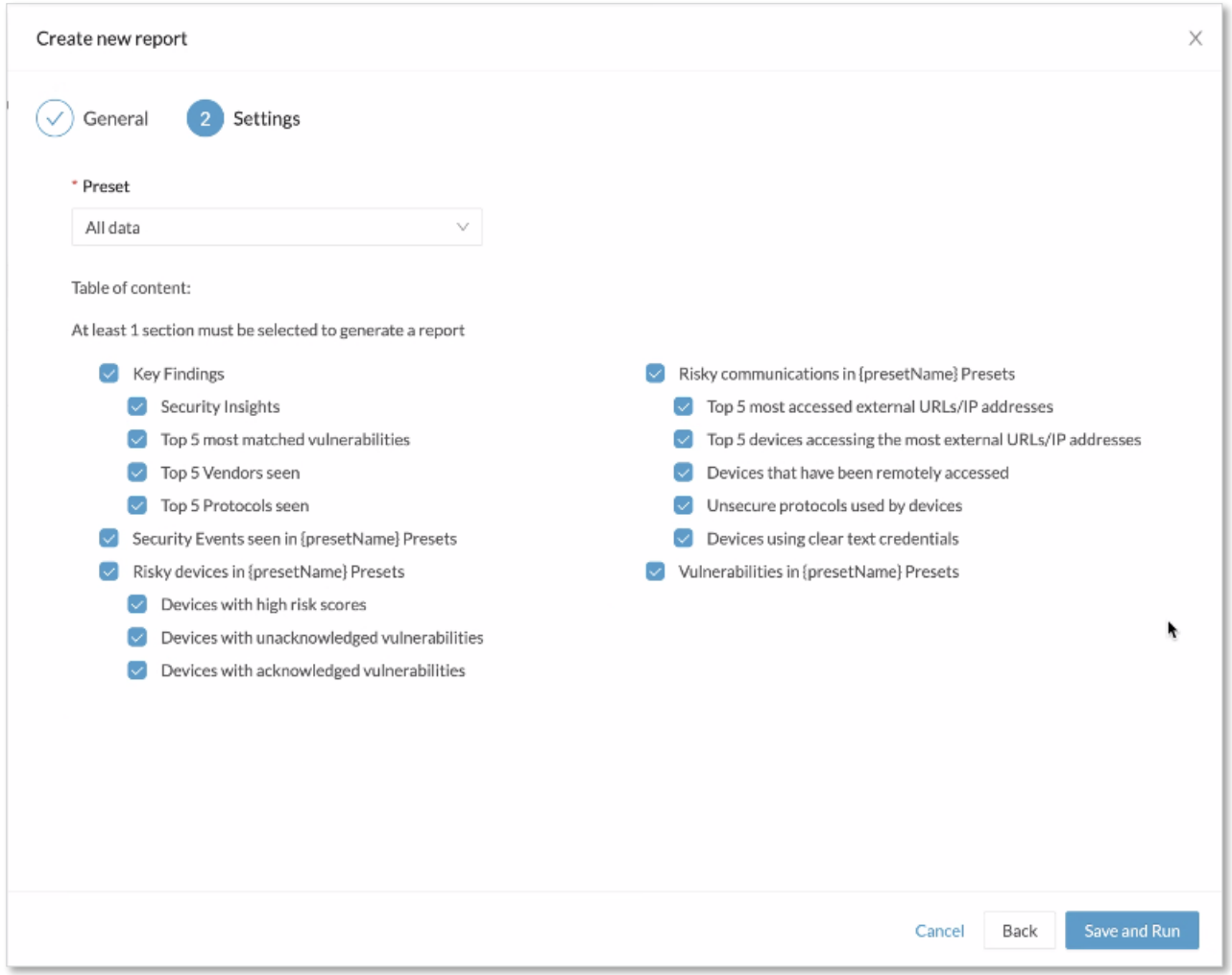
- Report to highlight presence of remote/external access
- Helps detect industrial gateways from vendors such as eWON and Moxa, and remote access software such as AnyDesk and TeamViewer

Reports Creation and Management



Reports Creation Wizard





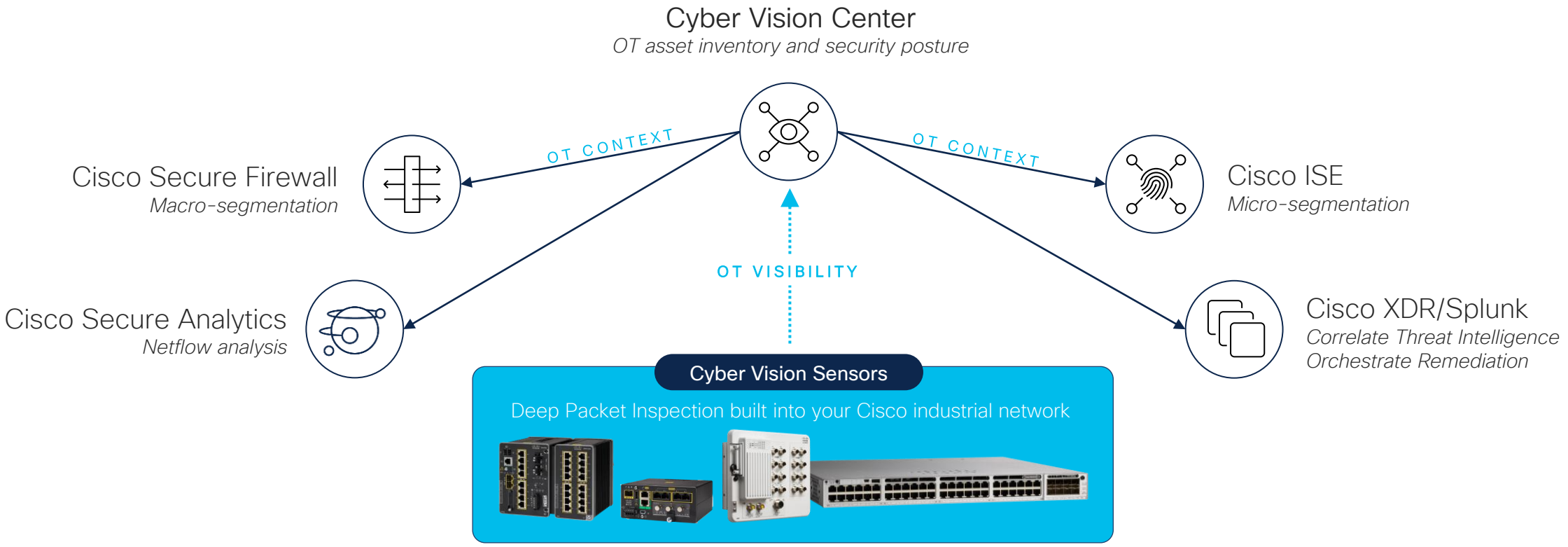
Extending IT security to your OT environment

Cyber Vision has the OT information the SOC needs

Visibility	Vulnerabilities	Intrusions	Anomalies
Provides **OT context**, asset inventory and communications map to your SOC	Identify asset vulnerabilities and **assess risks** before they are exploited	Leverages Talos signatures to detect known and emerging **IT attacks**	Monitor mode detects **malicious behaviors** and unknown attacks

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

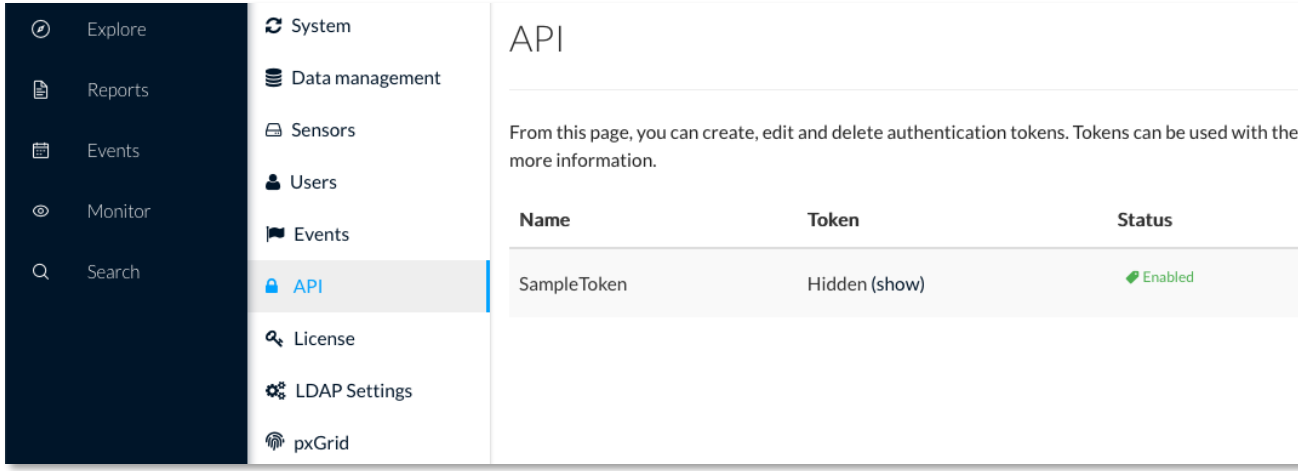
Extend IT security to your industrial settings



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

Integrations and customization via RESTful API

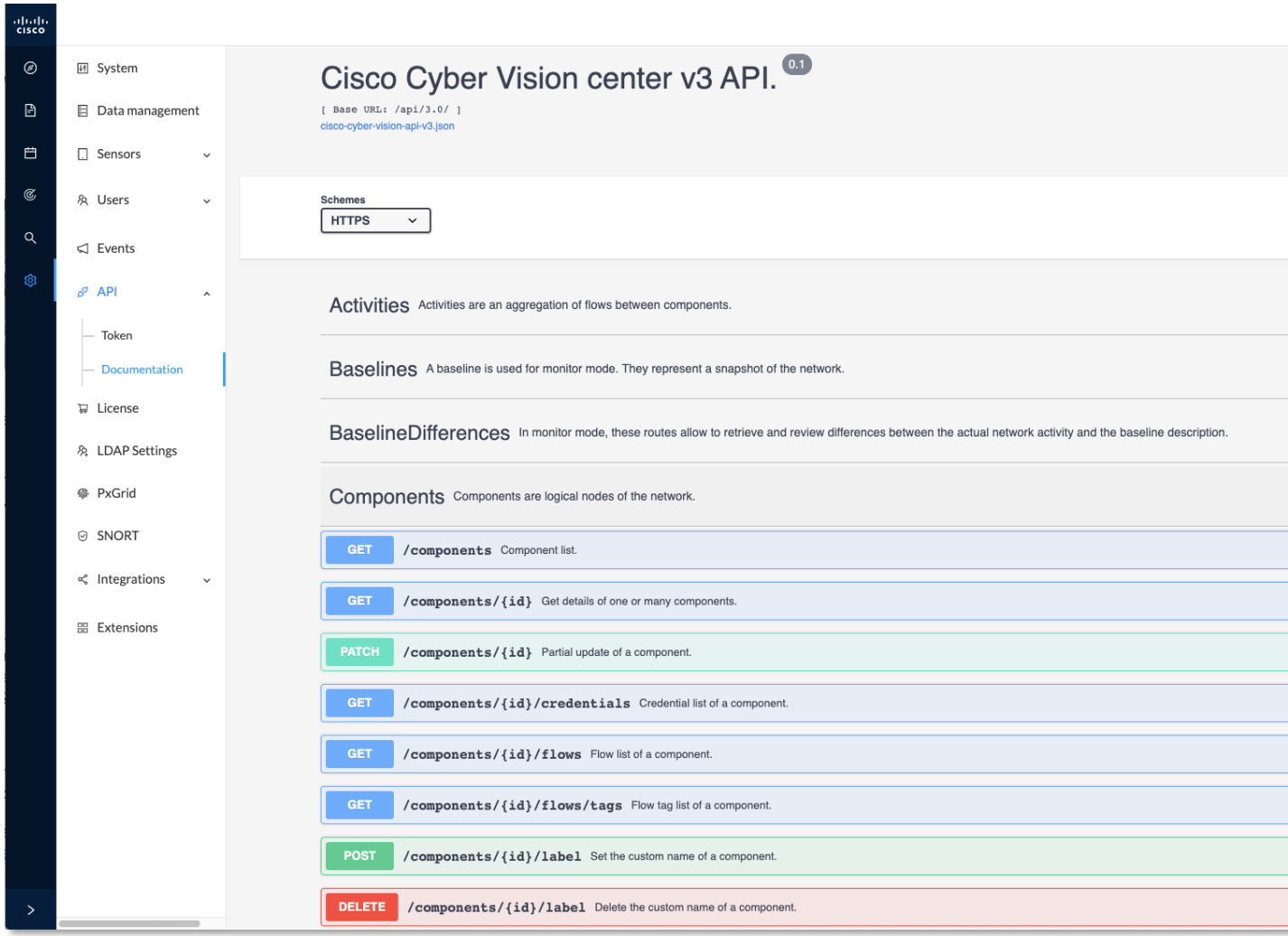
- Access data about components and communication flows available in Cyber Vision
- Leverage sandboxed application hosting to automate functions and integrations
- Modify tag assignment, presets and groups programmatically
- Define custom analyzers for unknown traffic in environment
- Enable bulk acknowledgements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



Integrate data from Cyber Vision into additional tools

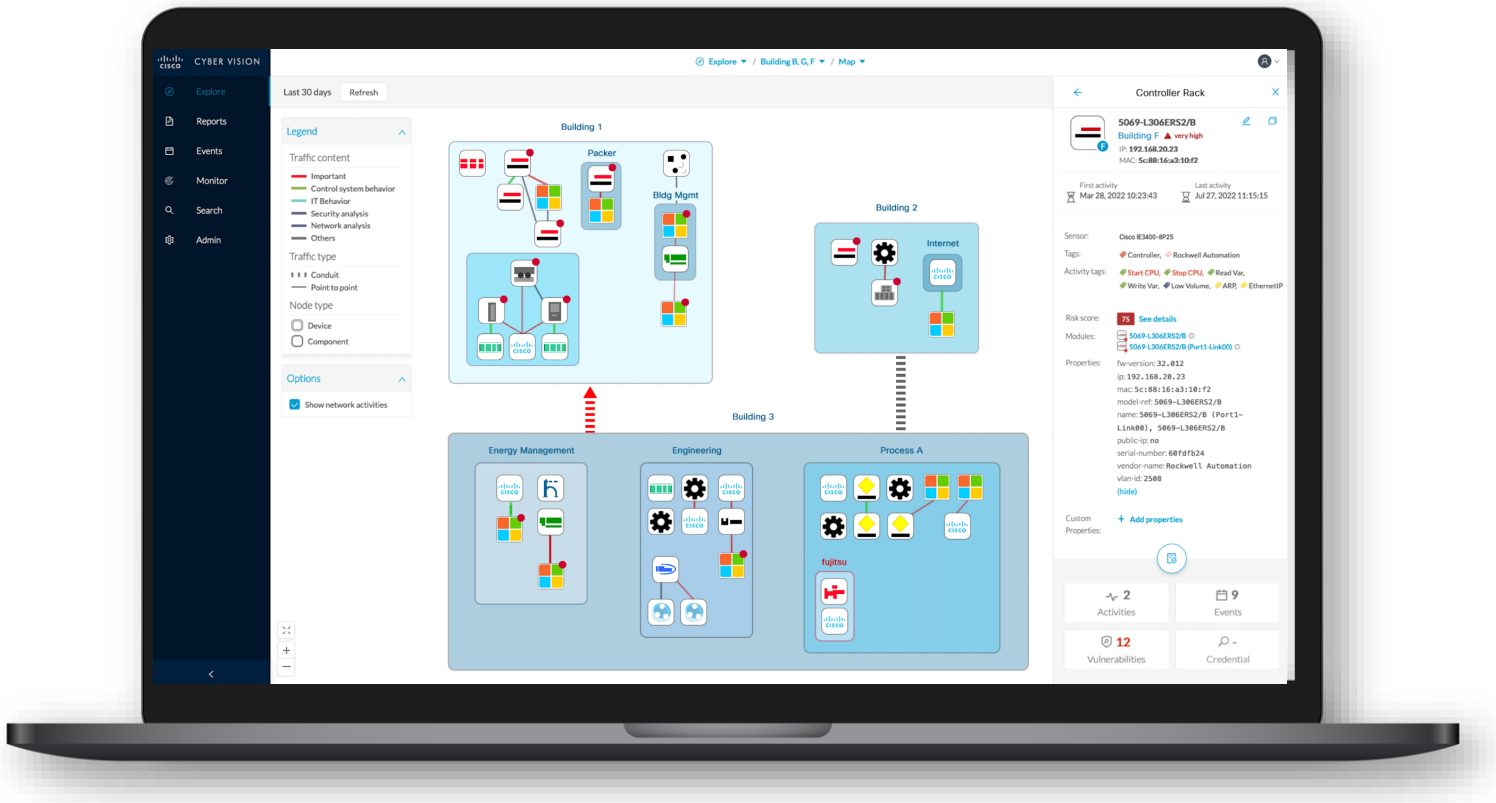
API Explorer

- 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...



Automating OT network segmentation

Leveraging Visibility to Drive Segmentation

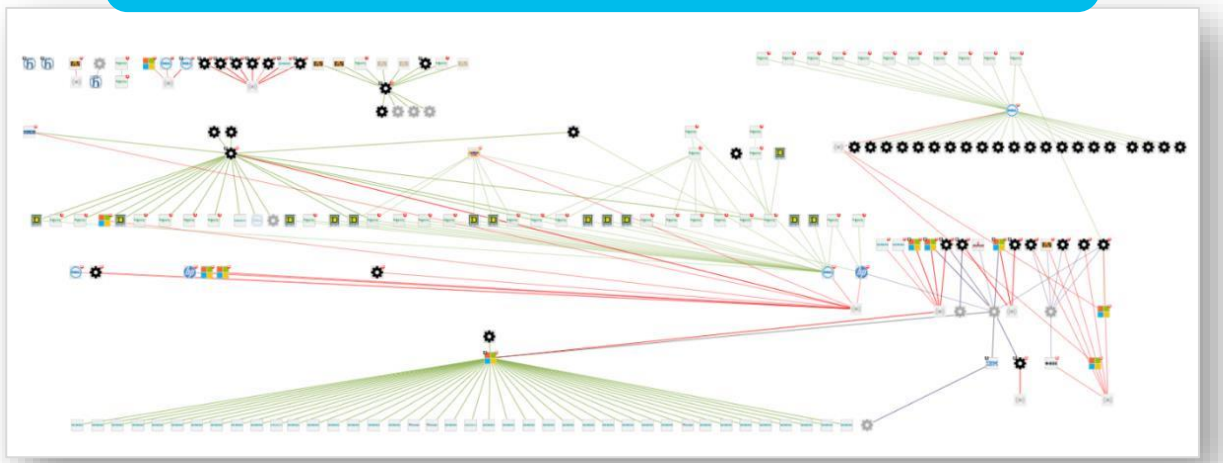


IEC-62443 virtual segmentation

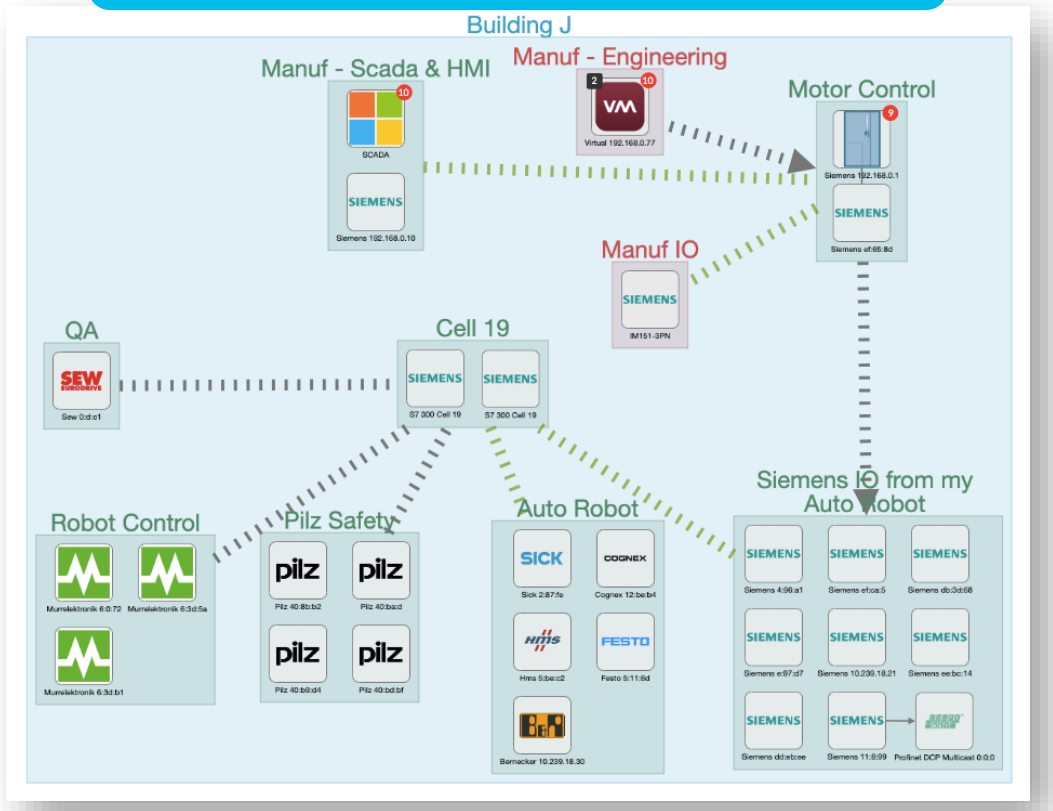
- Group OT assets into zones
- Visualize conduits
- Identify traffic violations
- Share context with other platforms to enforce segmentation

Leveraging Visibility to Drive Segmentation

Cyber Vision discovers all connected assets...



...and groups them into logical zones

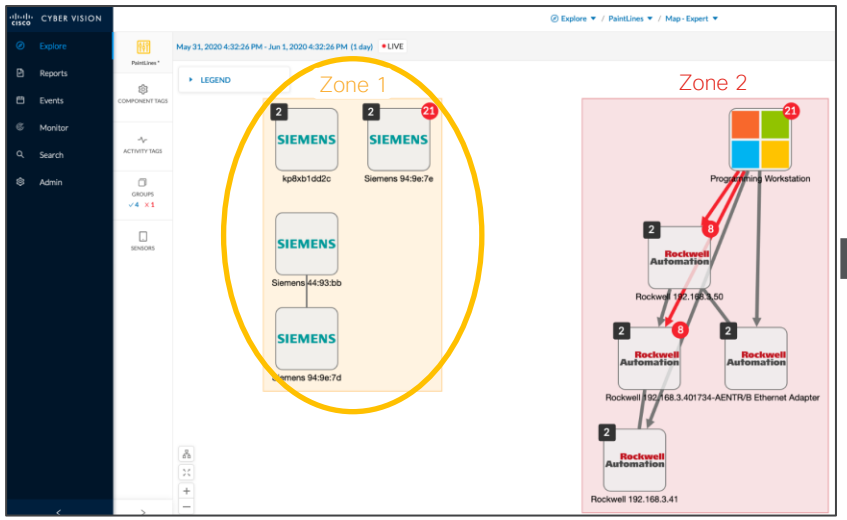


Give OT the tool they need to document ISA/IEC-62443 zones and conduits

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	✗	✗	✓	✓

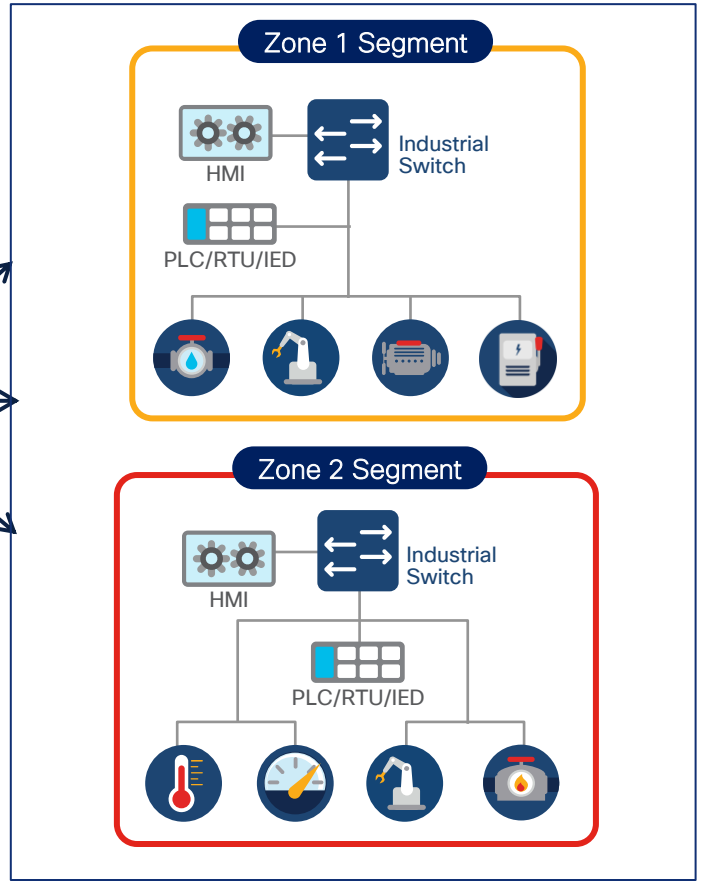
Cisco Firewall Policy Rules
or
Cisco ISE Policy Matrix

dACL

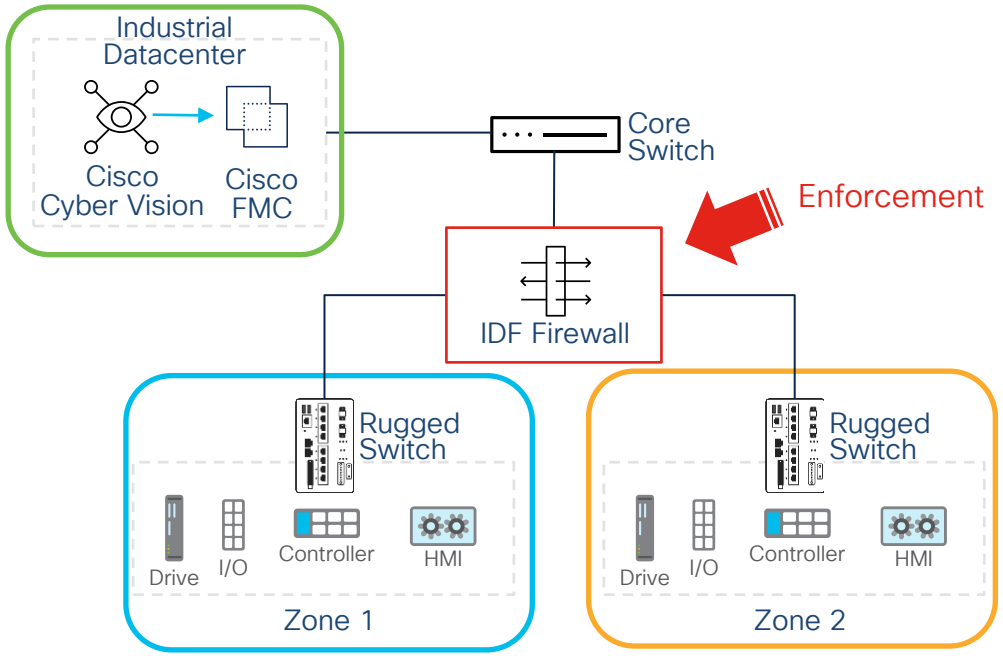
SGT

VLAN

Segmentation of industrial network



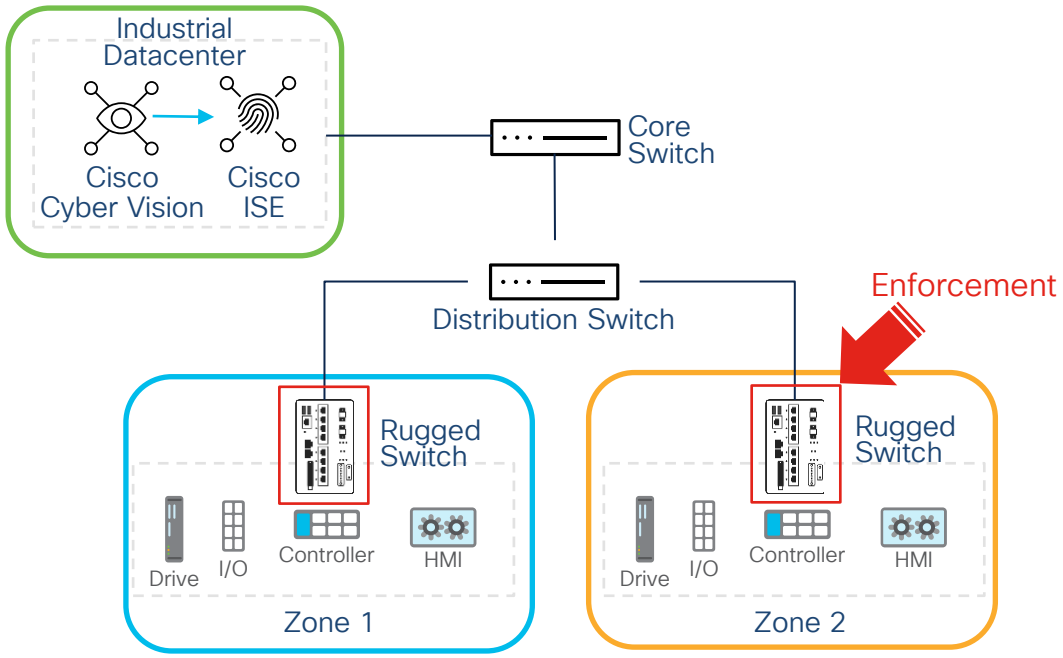
Automated Segmentation **Enforced using Firewalls**



- 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**

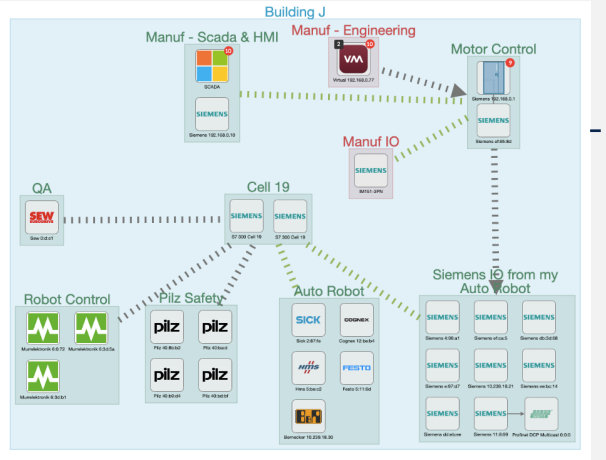


- Cisco Identity Services Engine (ISE) receives devices' profiles from Cyber Vision and associates a network access policy to each
- Policies are pushed to network switches for enforcement at the port level
- Network switches allow/deny assets to communicate based on their profile, not their IP address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

Grouping assets in Cyber Vision...



CSDAC

...creates dynamic objects in FMC

Cisco Secure Firewall Management Center

Cisco Secure Firewall

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

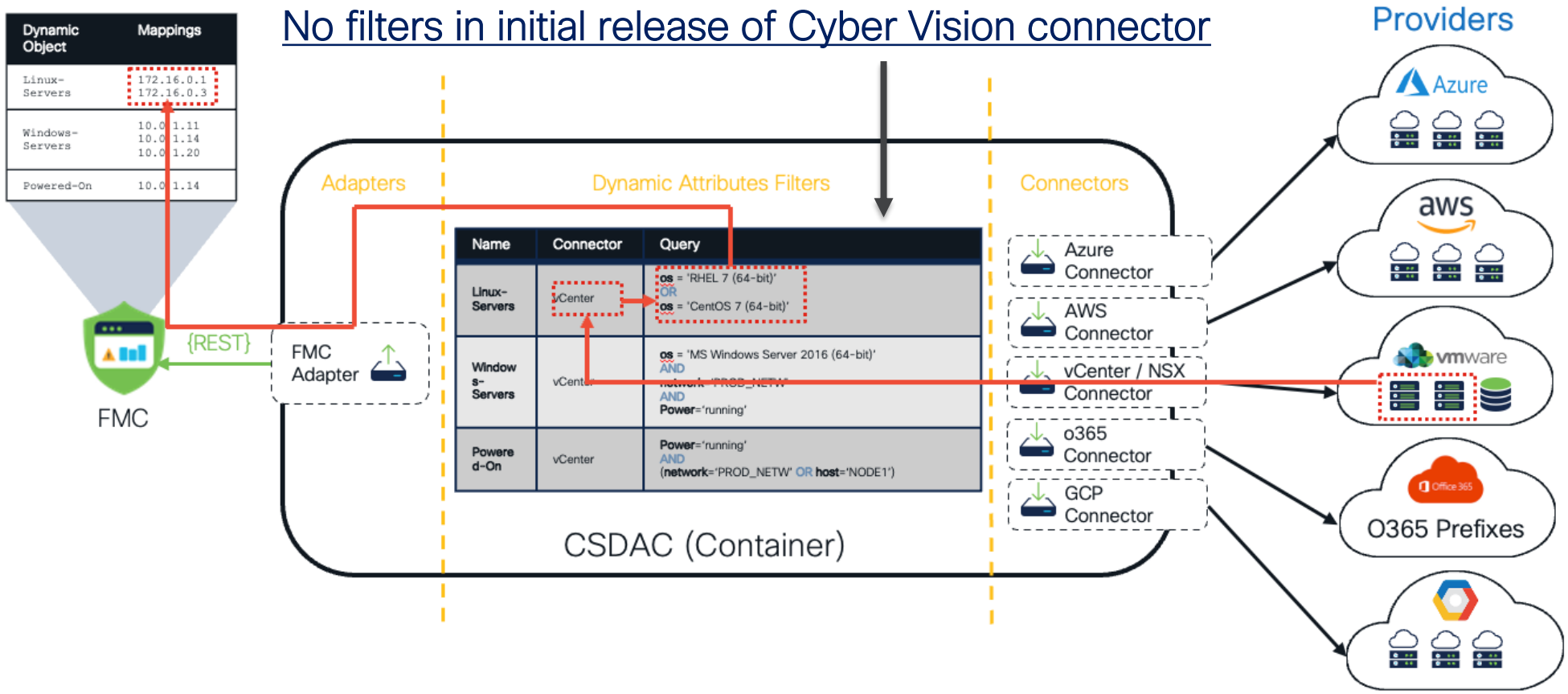
Simplifying network segmentation with dynamic firewall rules informed by OT visibility

What is CSDAC?
Cisco Secure Dynamic Attributes Connector

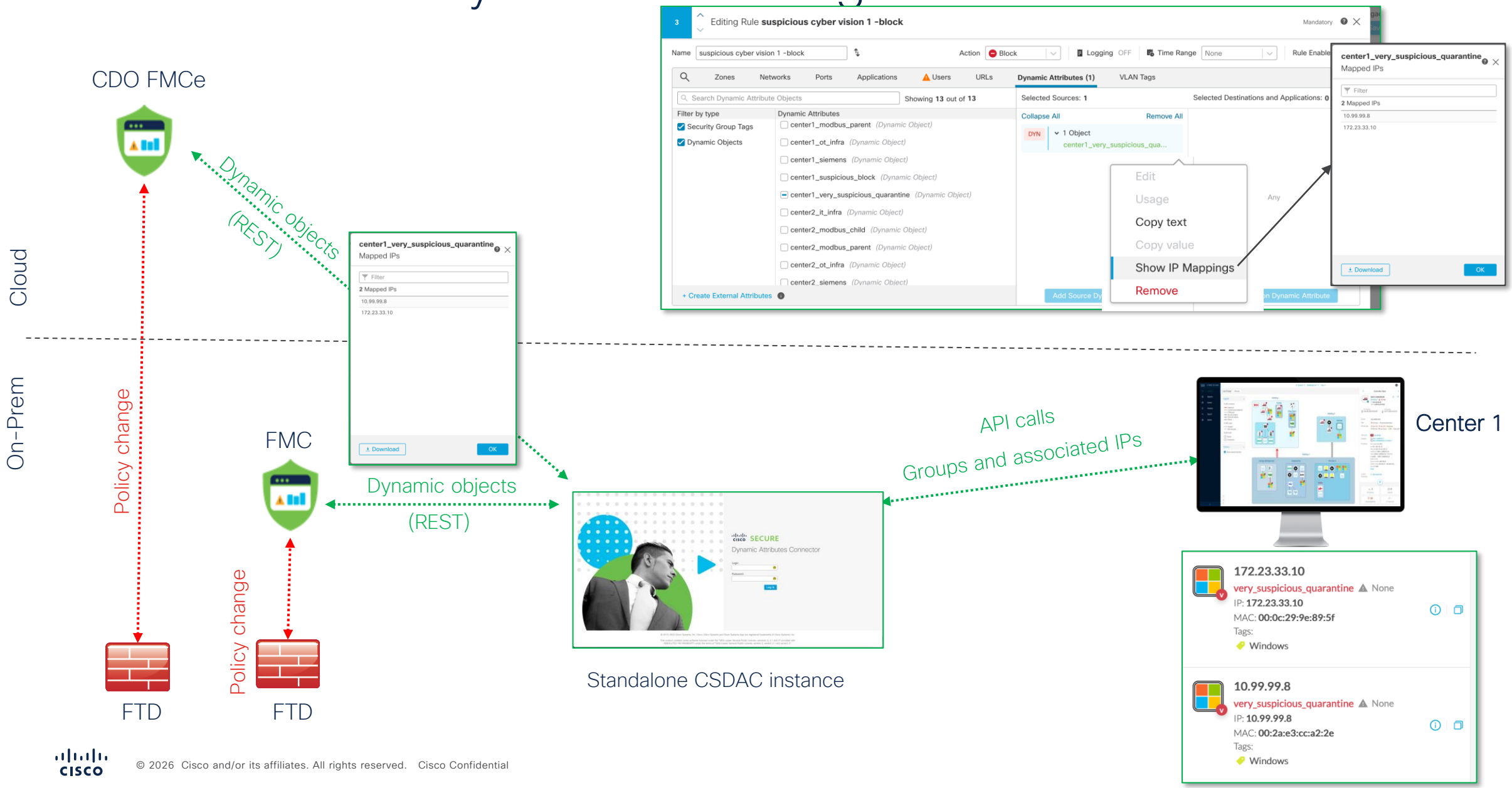
- CSDAC is a Middleware engine (docker container based)
  - It translates API calls from third party elements into dynamic objects for use in FTD access control policy
  - Its available as 1) standalone 2) embedded in FMC (7.4) or FMCe (CDO)
- Primarily used for Cloud and Public Feed Connectors
- Cyber 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)

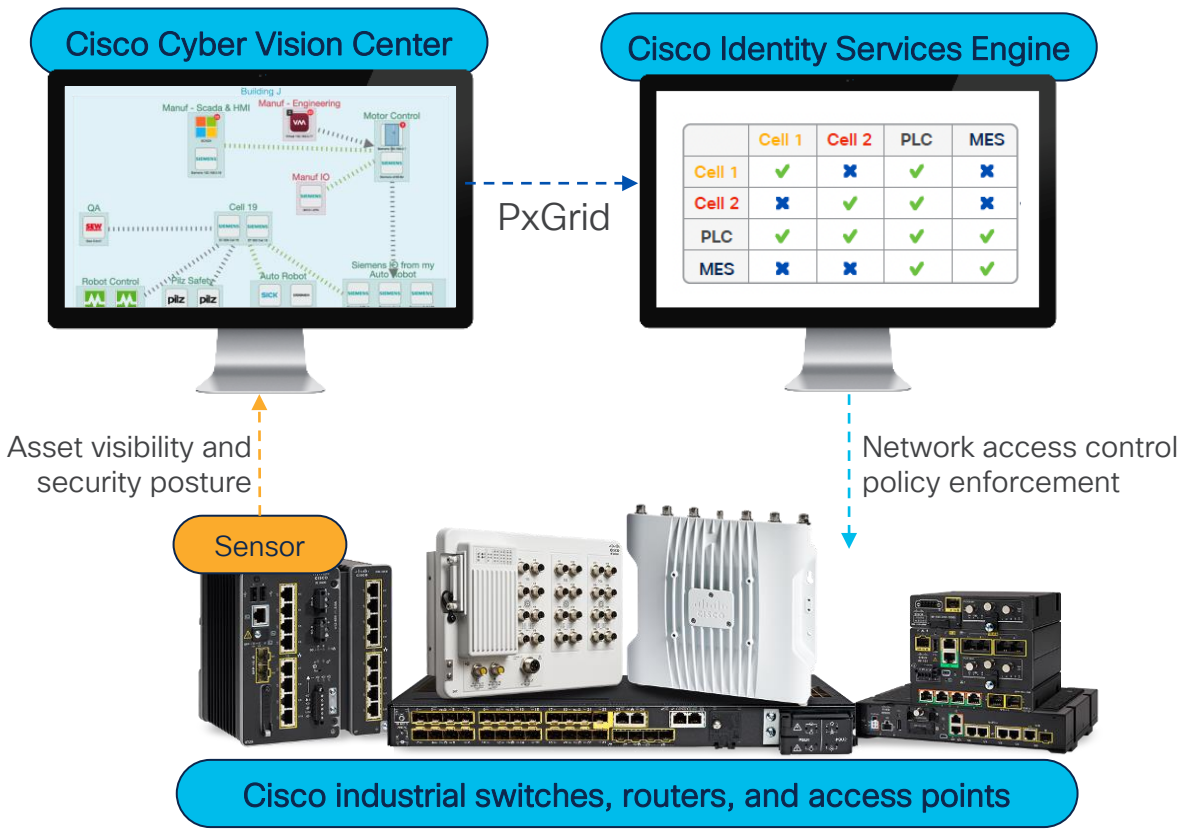
Immediate visibility of object changes. No policy deployment is required.



Cisco CSDAC: Cyber Vision integration



Visibility drives micro-segmentation with Cisco ISE

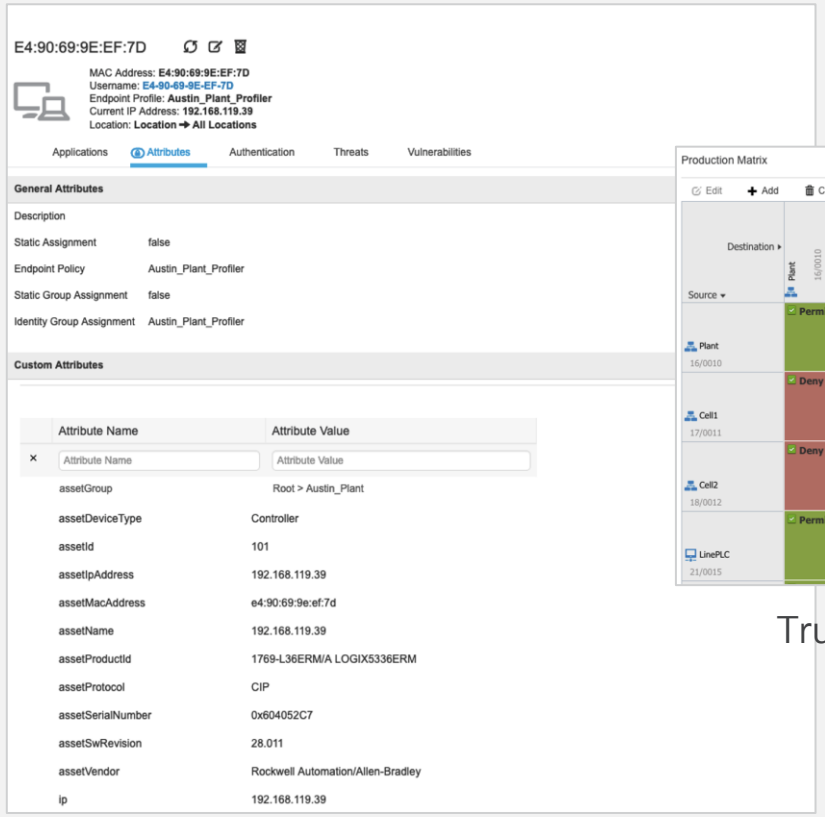


Cisco Cyber Vision
Gain full visibility into assets, and group them according to their role in the industrial process

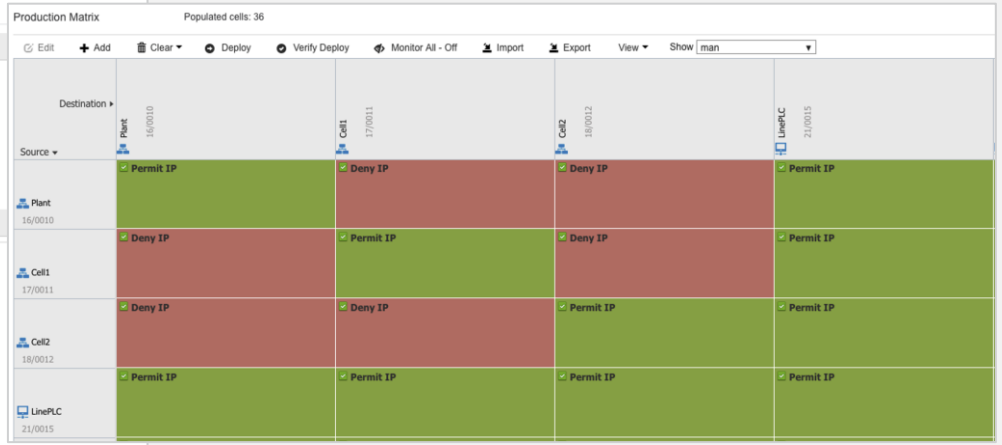
Cisco Identity Services Engine
Automatically update access control policies for the network to enforce zero-trust segmentation based on Cyber Vision groups

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

Integration with Cisco Identity Services Engine (ISE)



Devices in ISE get attributes from Cyber Vision



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

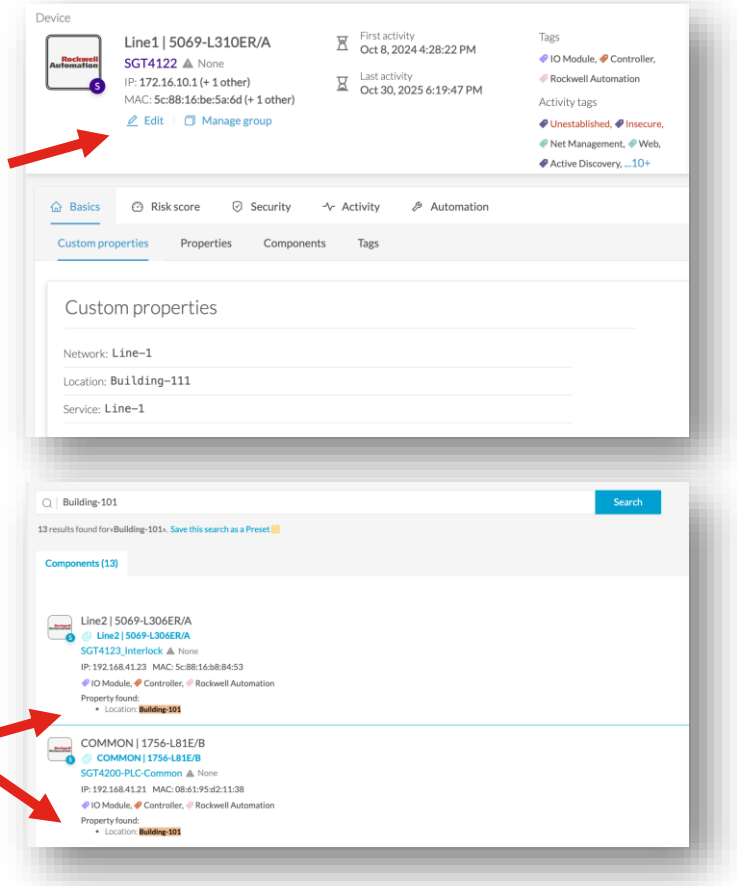
Cyber Vision – Attributes via pxGrid

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

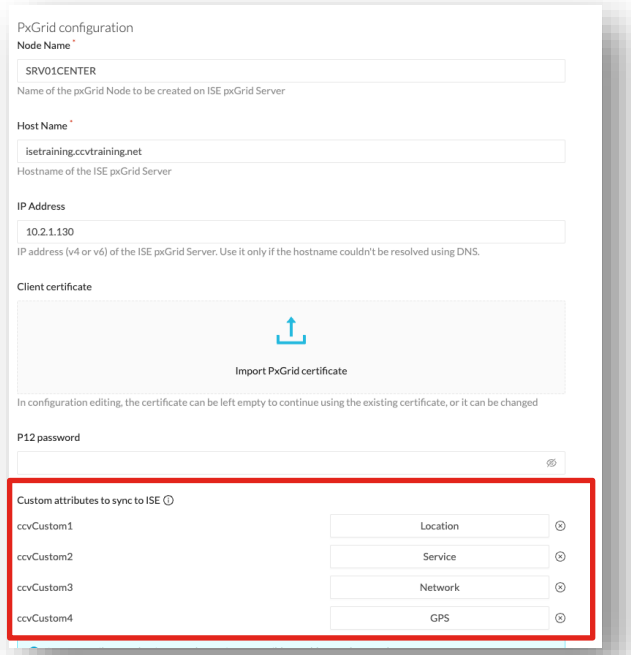
ISE Integration – Custom properties [1/2]

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

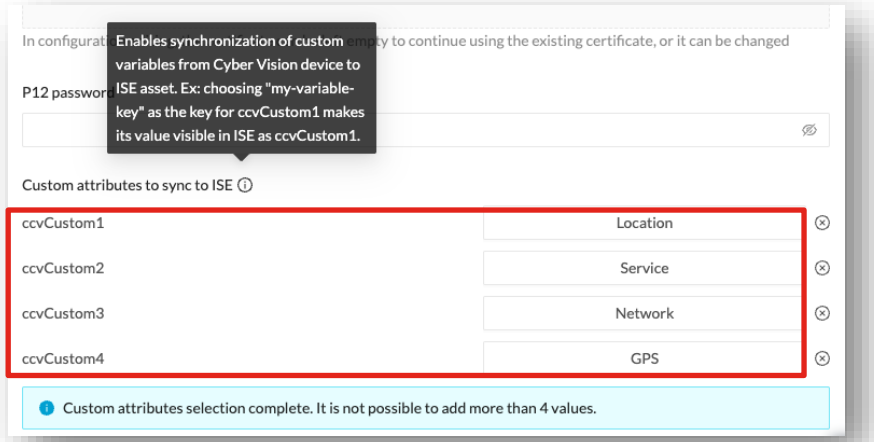
Custom device attributes created and added via UI or API



PxGrid integration configuration



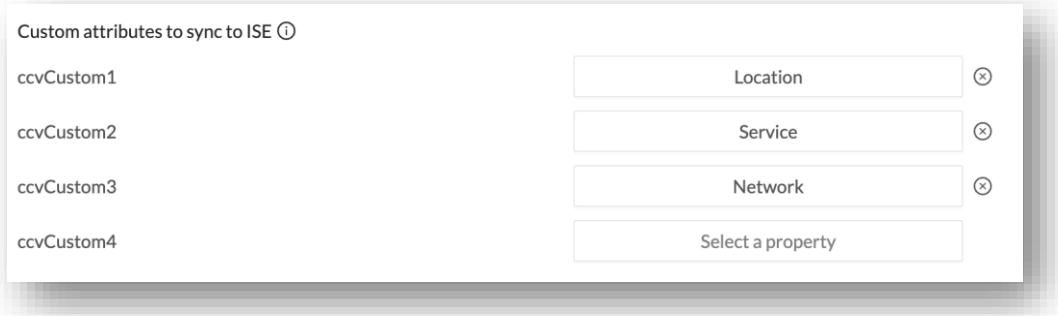
PxGrid integration configuration

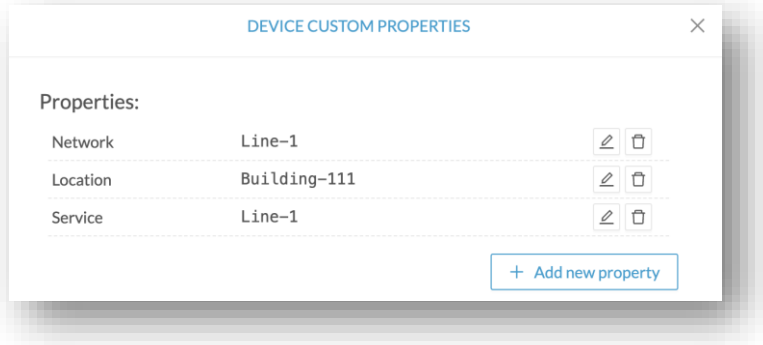


ISE Integration – Custom properties [2/2]

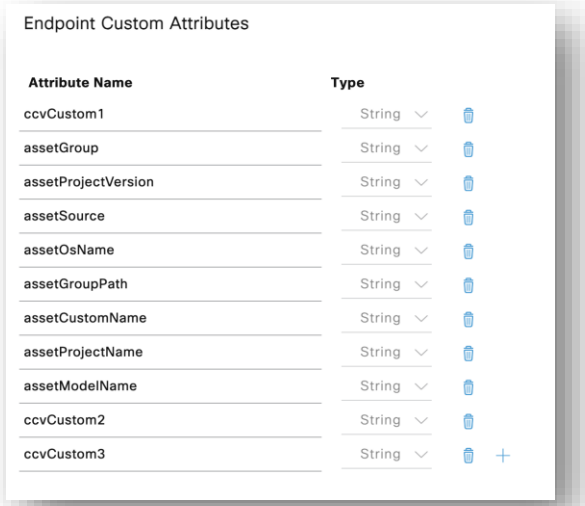
Use mapped and provisioned CV attributes in ISE

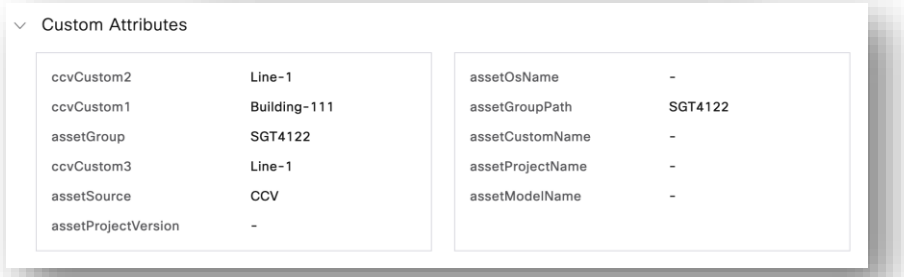
Cyber Vision





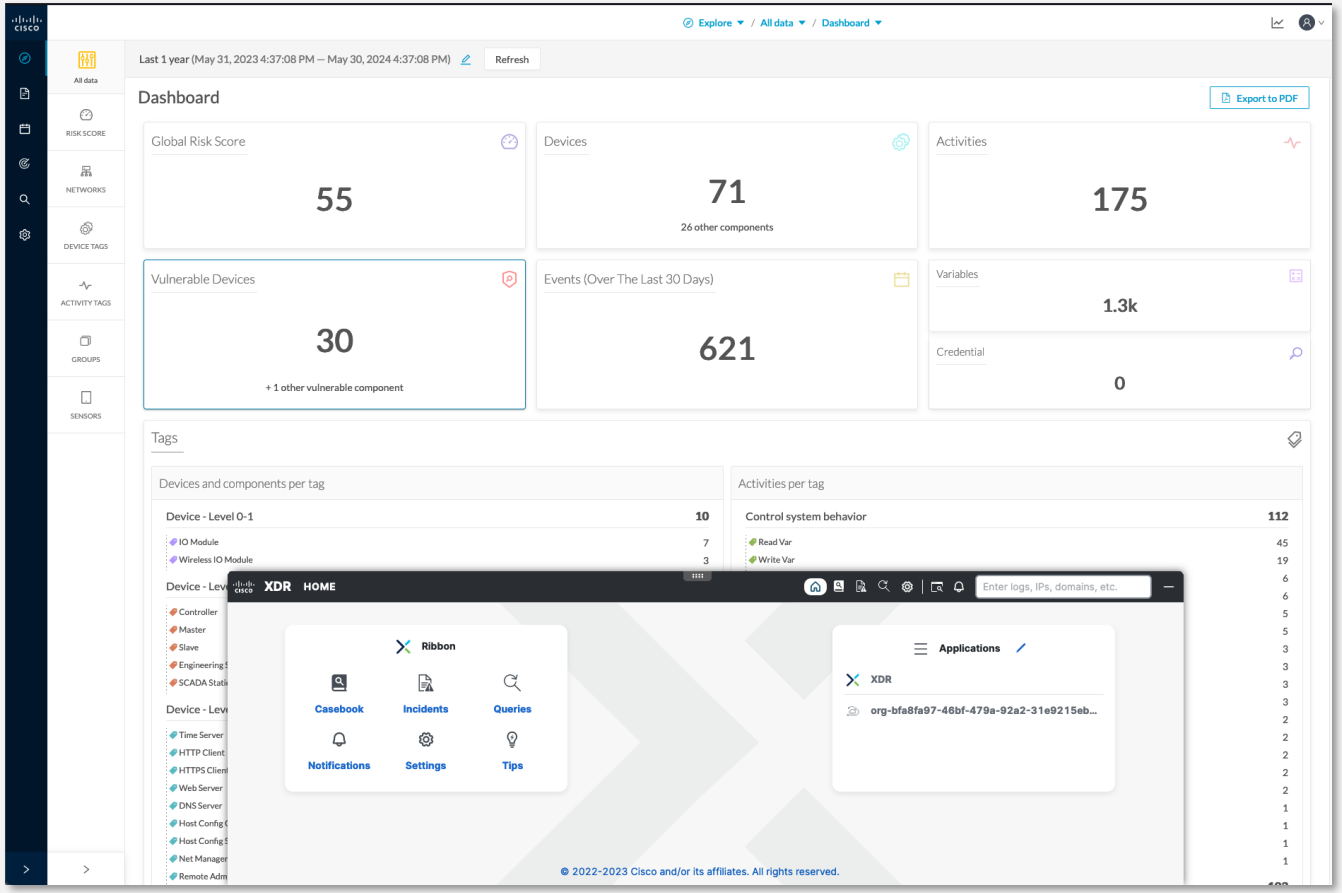
ISE





Providing OT context to the SOC

Investigation & Orchestration with Cisco XDR



Leverage Cyber Vision Observables to:

Create and **manage incidents** in Cisco XDR

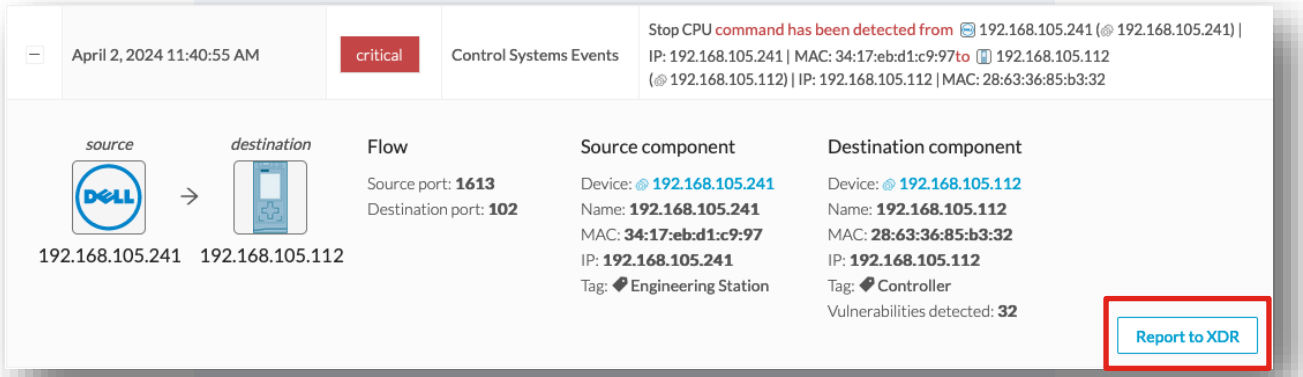
Create and **orchestrate playbooks**

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

XDR Ribbon in Cyber Vision for investigations and remediation orchestration

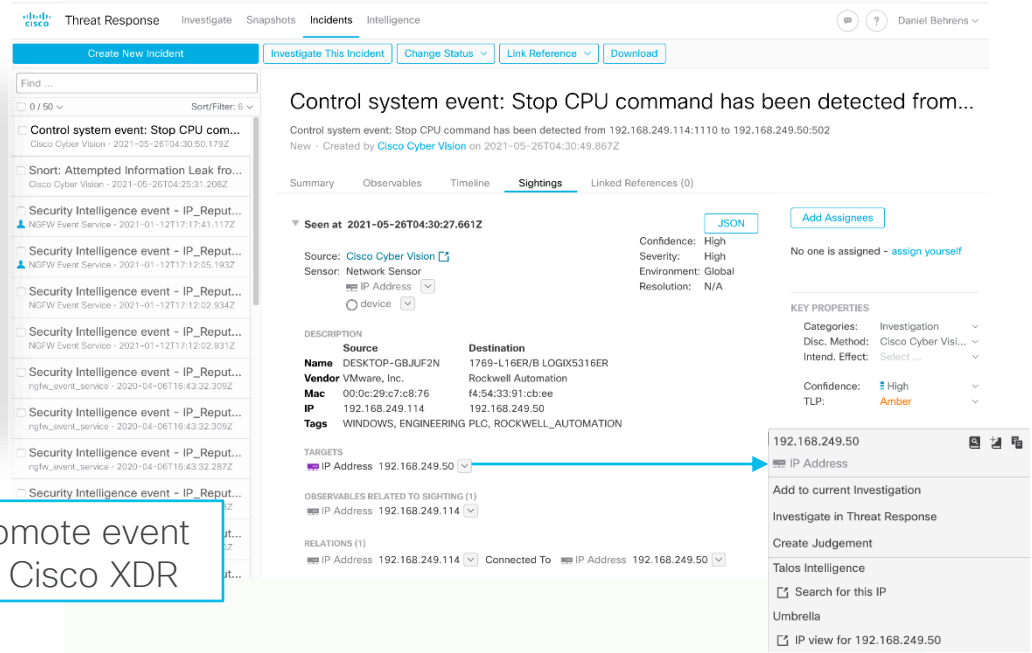
Promote Cyber Vision events to Cisco XDR

View events in Cyber Vision



Promote event to Cisco XDR

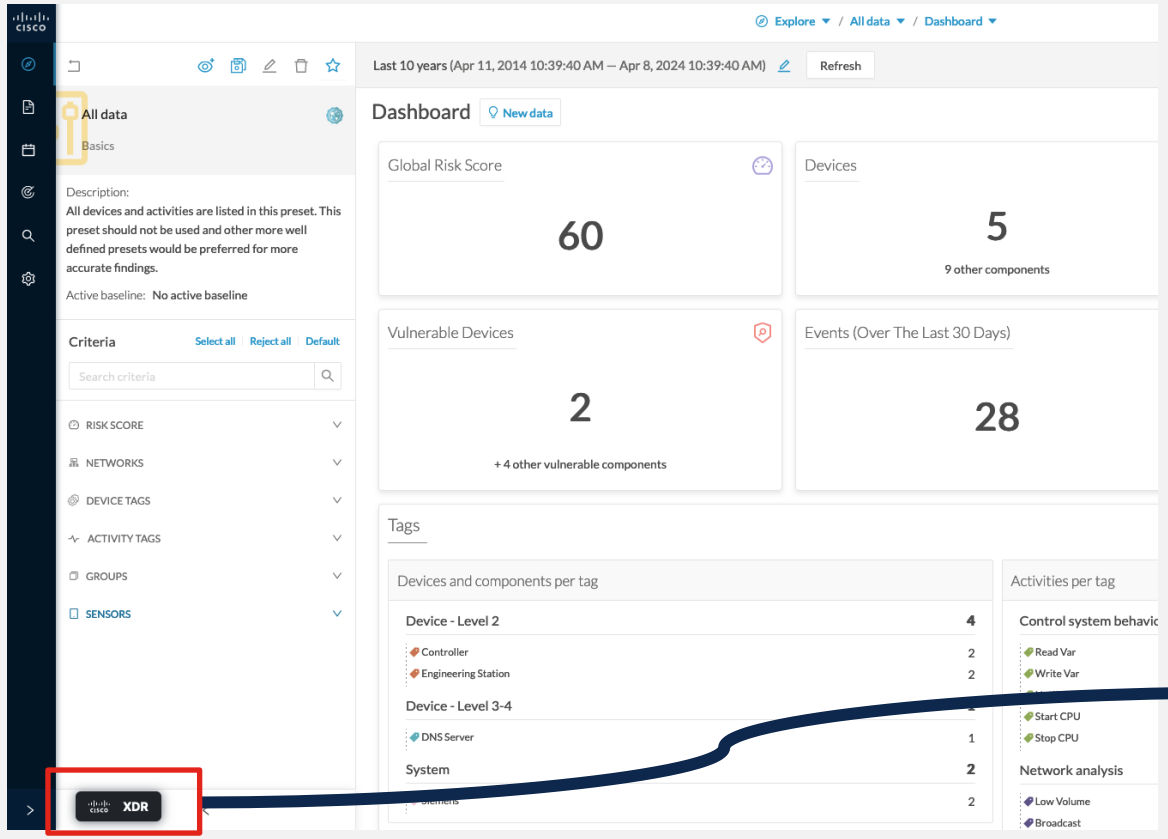
Launch investigation in XDR



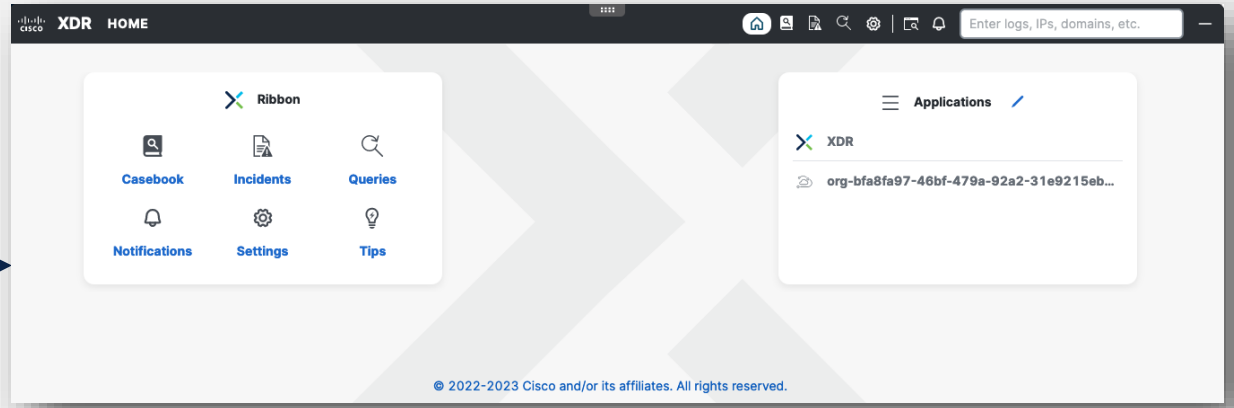
Events generated in Cyber Vision for process anomalies, signatures and control system can be promoted

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

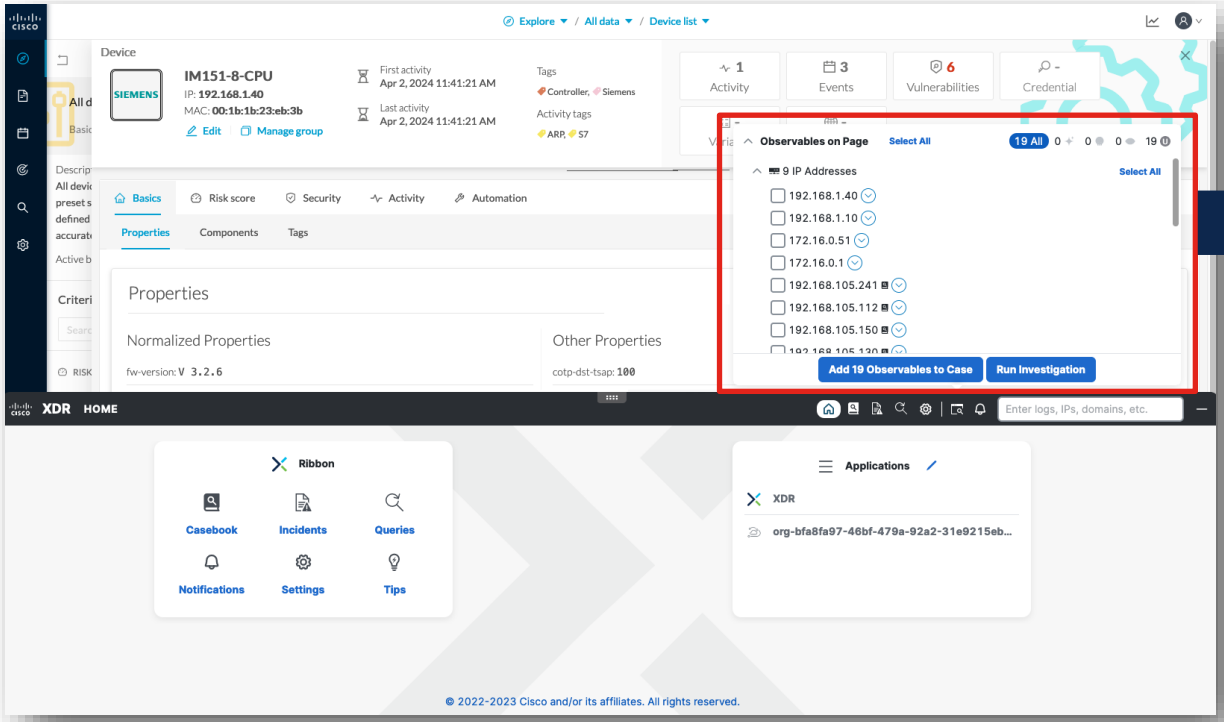
Cisco XDR Ribbon on Cyber Vision



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

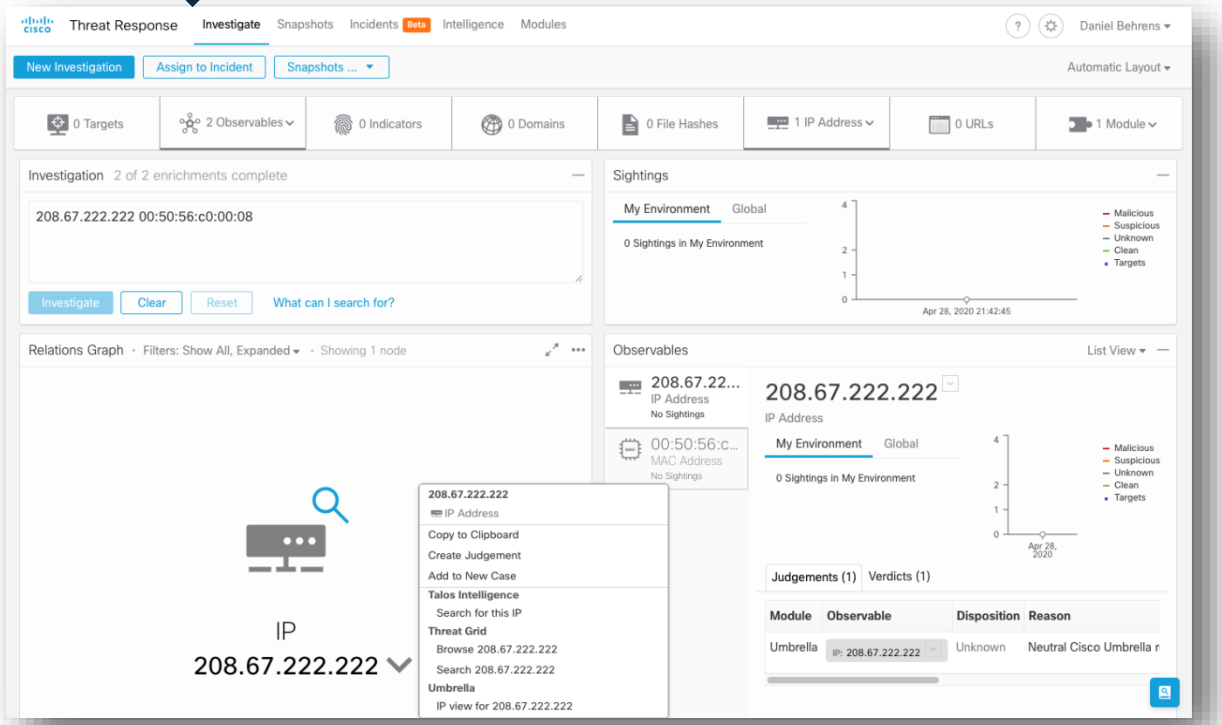


Investigate OT events with Cisco XDR



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

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



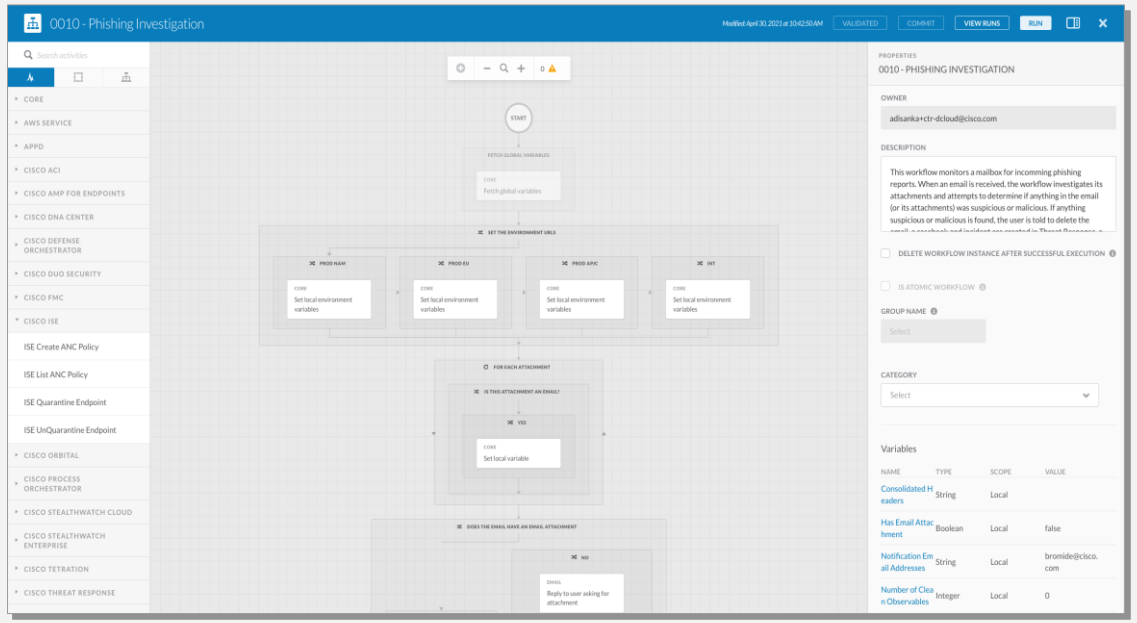
Response Orchestration with XDR Workflows

Orchestration out of the ‘box’

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

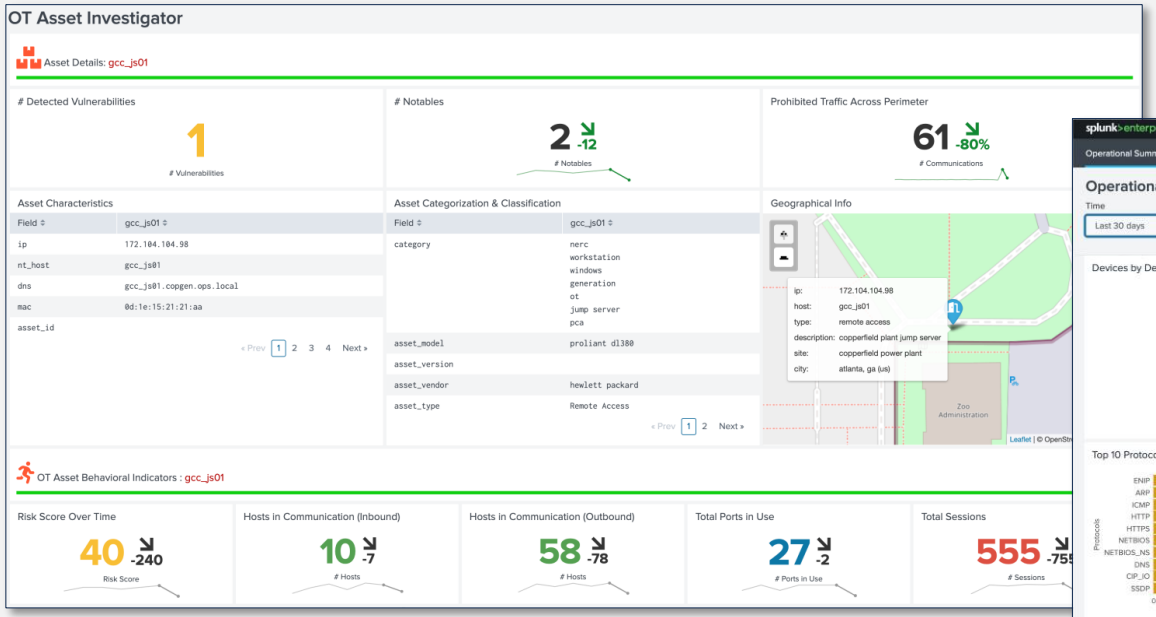
- Move Computer to Secure Endpoint Triage group
- Submit URL to Secure Malware Analytics
- Take Orbital forensic snapshot
- Take forensic snapshot and isolate
- Secure Endpoint host isolation with tier 2 approval

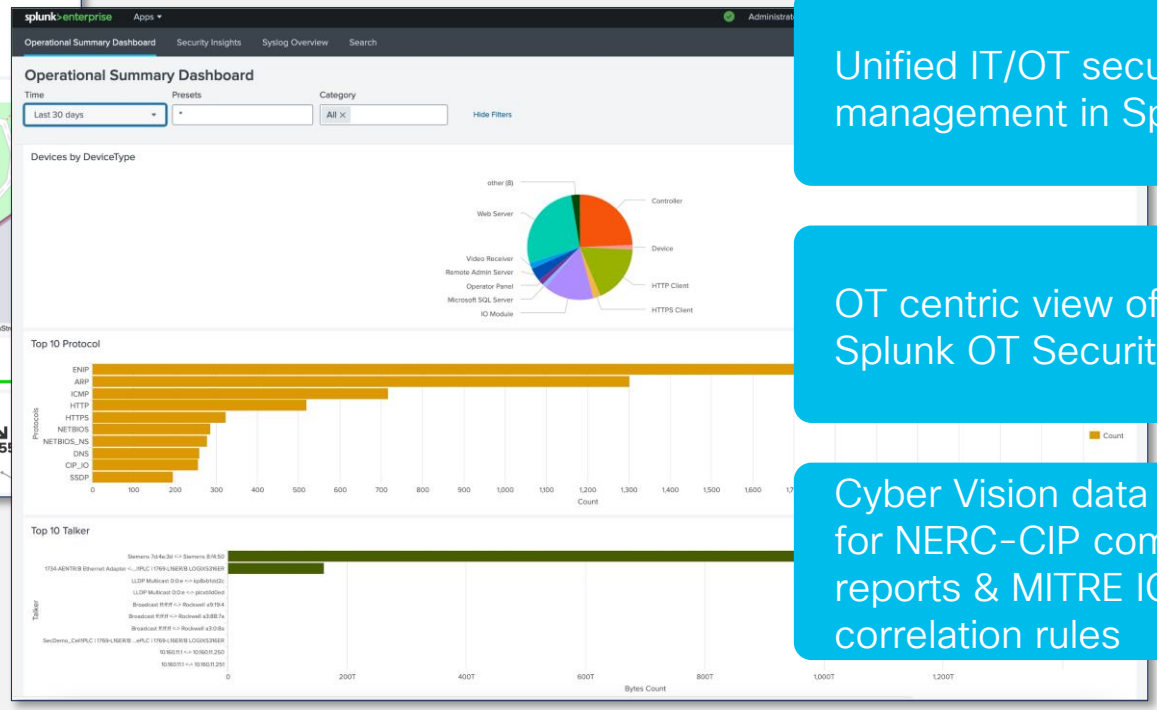
Custom orchestration workflows



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

Splunk Integration





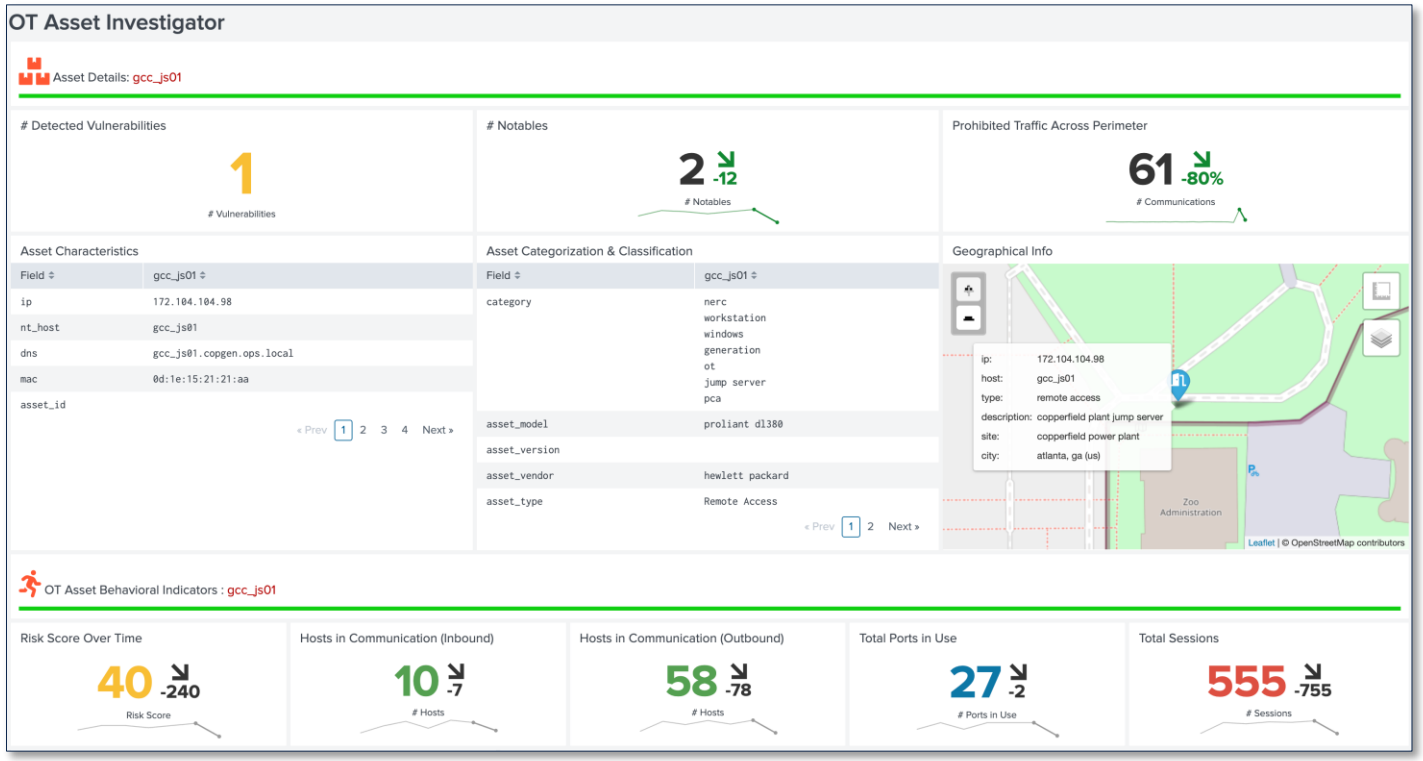
Unified IT/OT security events management in Splunk SIEM

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

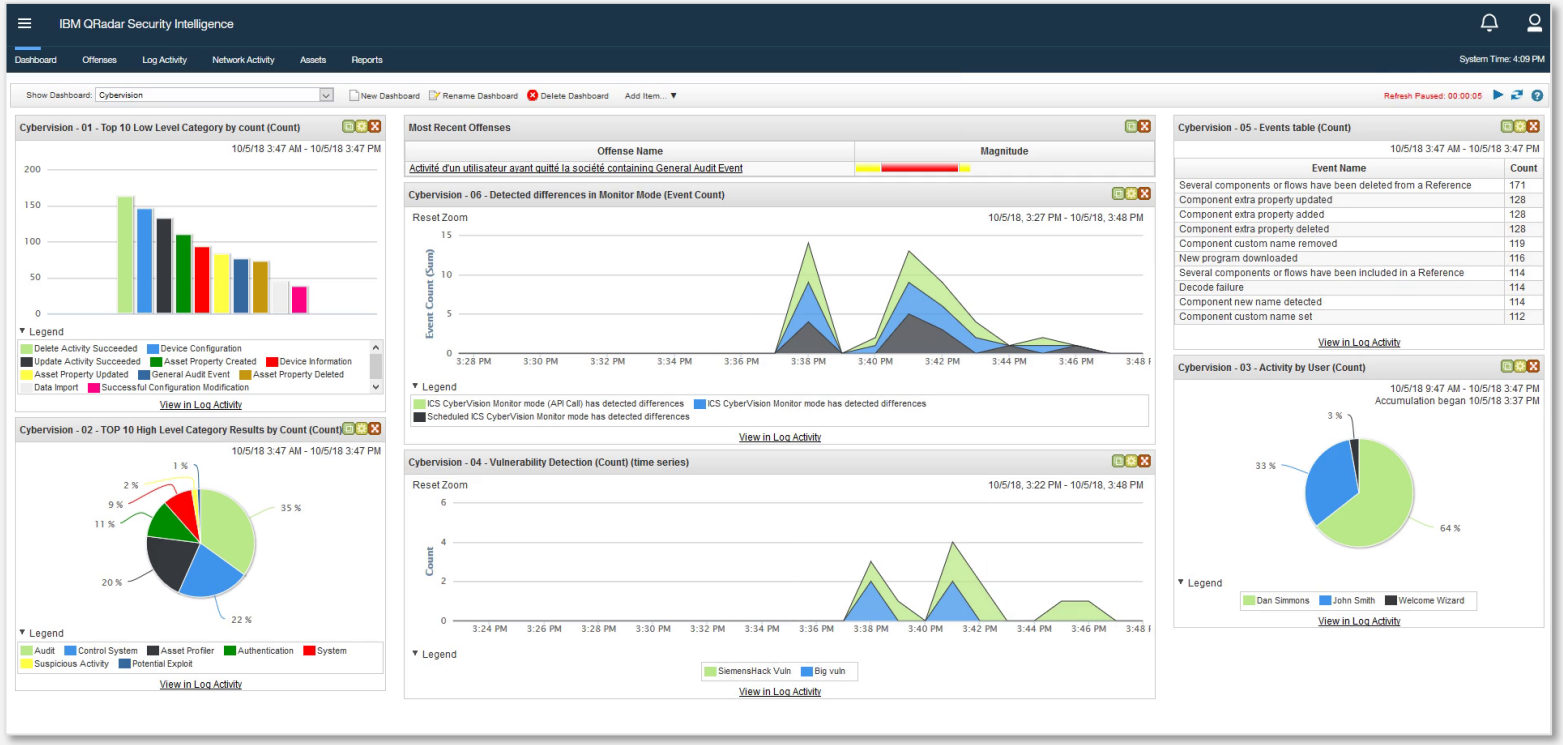
Syslog and REST API integration with Splunk SIEM and OT Security Add-on

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

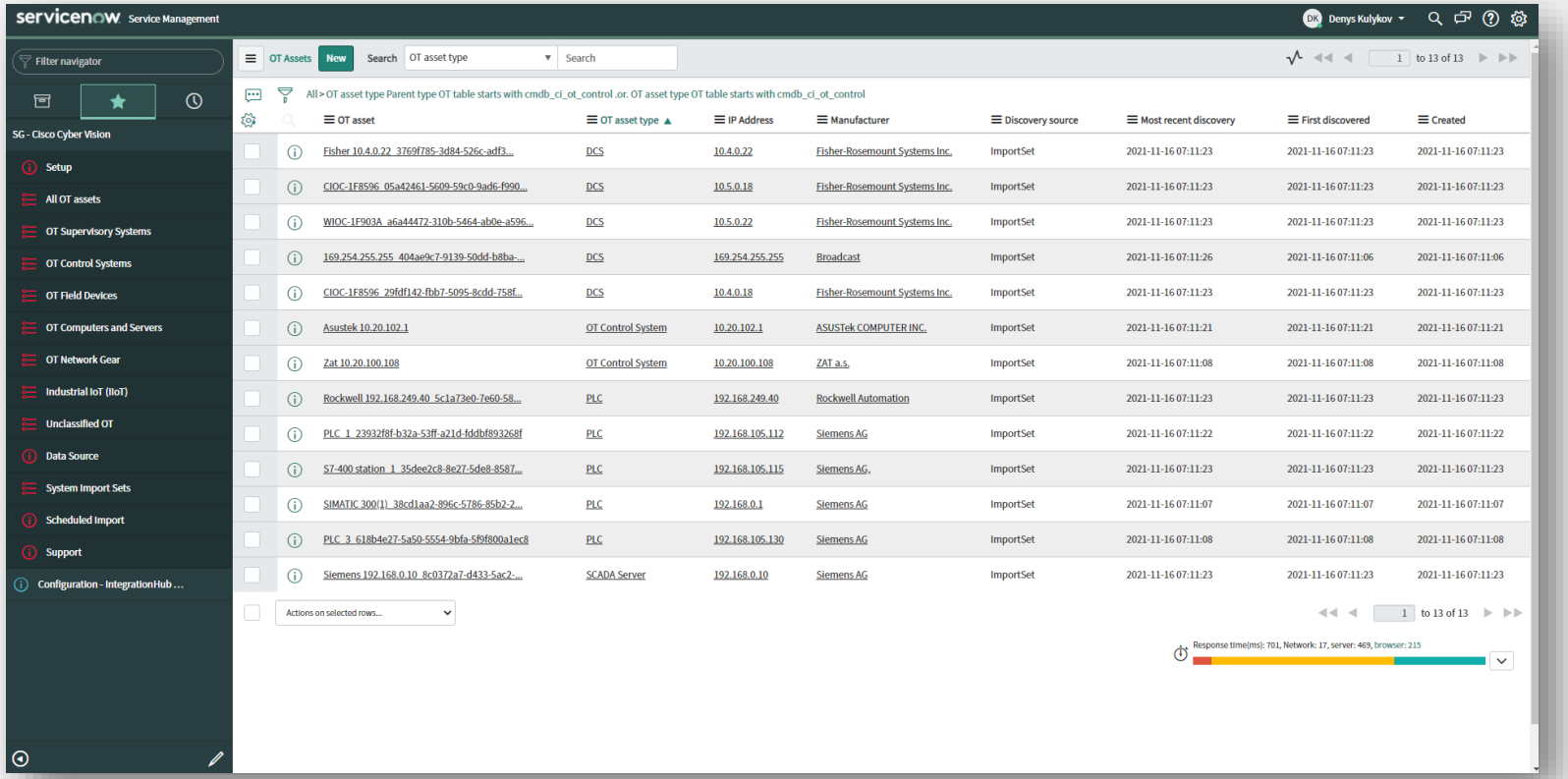
Focus on real threats using Machine Learning and pre-defined analytics rules

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

servicenow



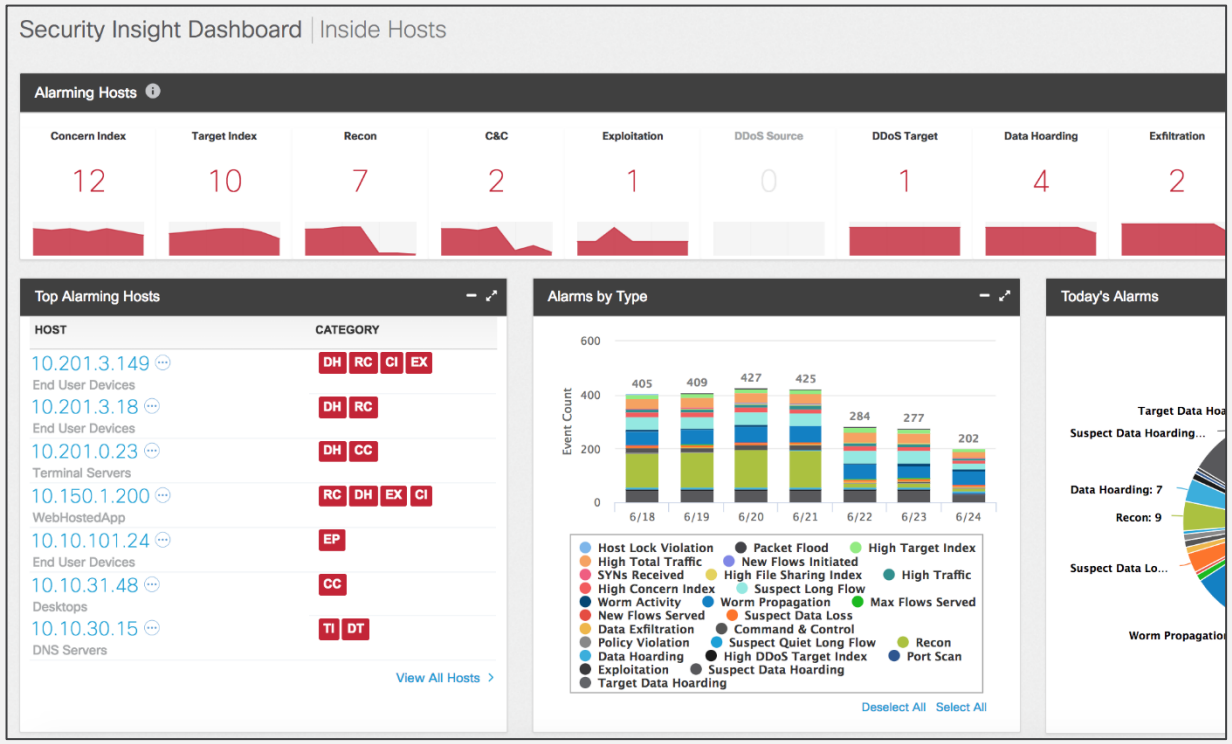
Integrated with ServiceNow Operational Technology Management suite

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



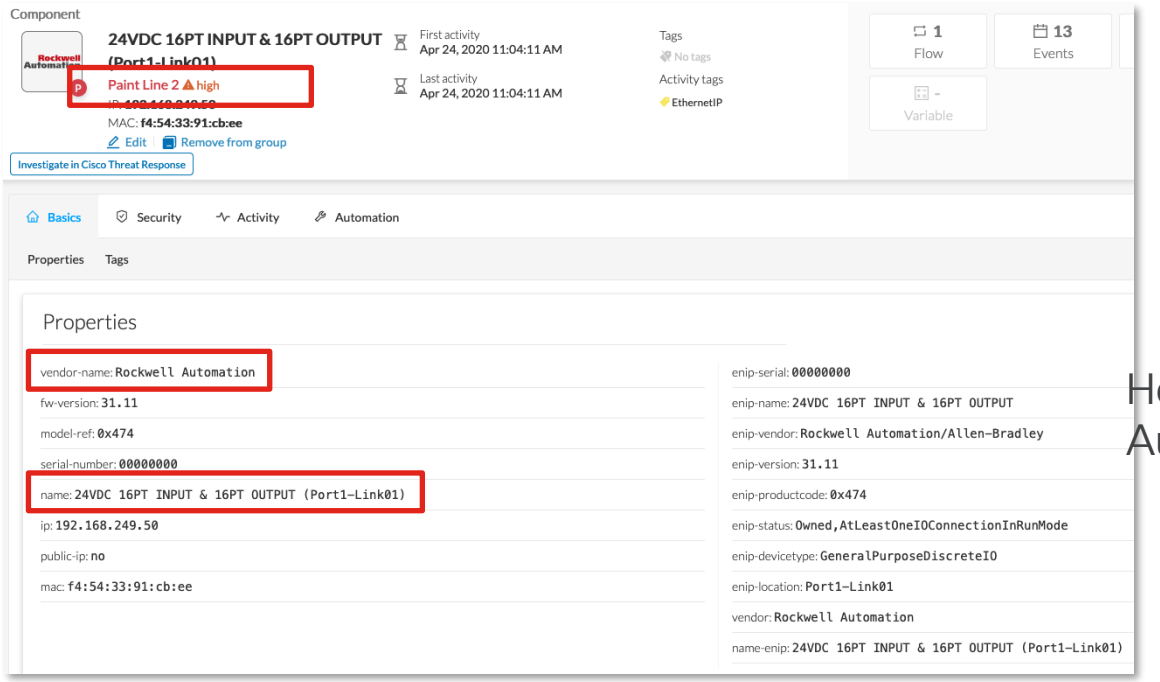
Enrich hosts information in Cisco Secure Analytics with rich context from Cyber Vision

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

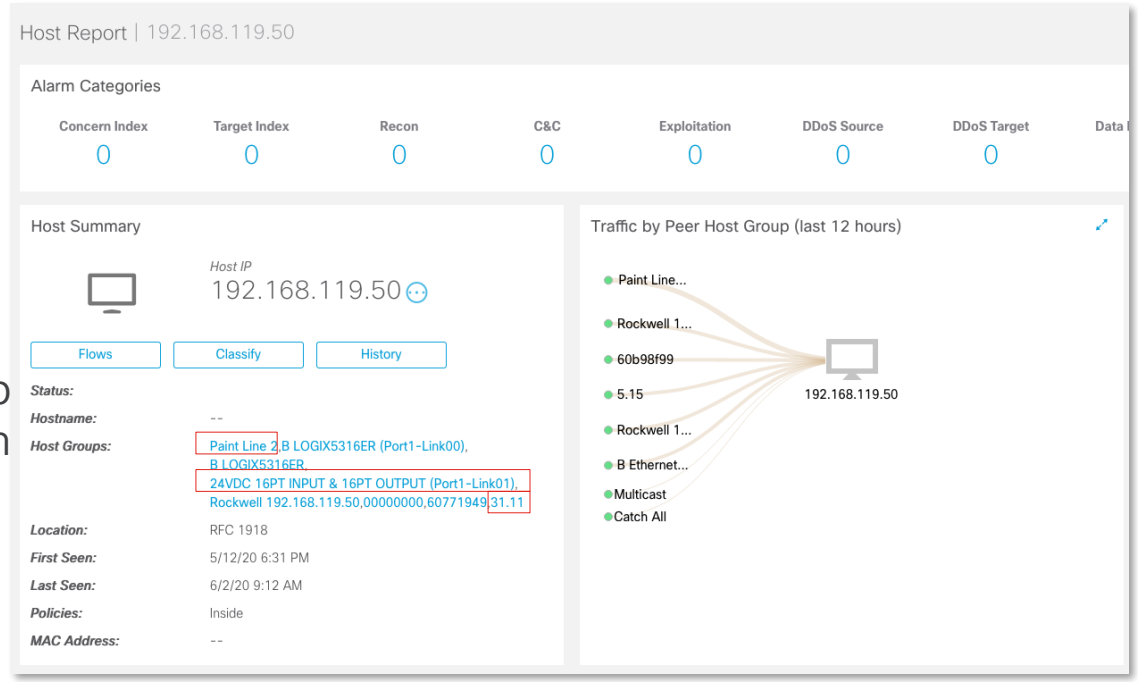
Create alert policies to identify and alert on inter-zone communications

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

Secure Analytics Dynamic Host Groups



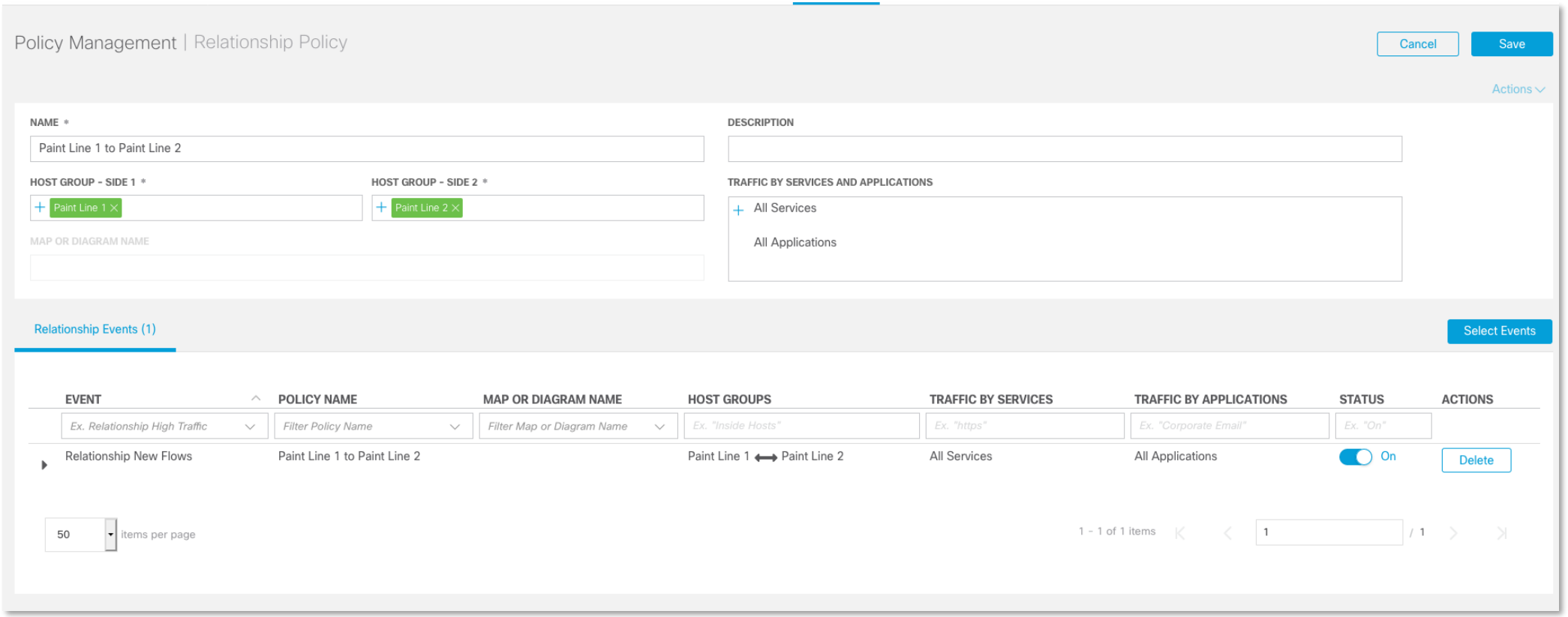
Host Group Automation



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



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

Transactional

For All Customers

Transactional 1,3,5,7-year term subscription with pre-paid, yearly, and monthly payment options

Security Enterprise Agreement

For All Customers

Multi-product discount, and easy to consume with growth allowance and true forward

MSLA

For Partners Delivering Managed Services

Usage based license agreement with post-paid monthly billing

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 licenses come with Standard software support. More details on all available software support levels can be found here.

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 Cloud Protection Breach Protection **User & Breach Protection** (Combination)	Duo **Identity Services Engine (ISE)** **Secure Workload** *(Tetration)*	Umbrella Secure Access **Secure Web Appliance** *(WSA)* **Secure Firewall** *(NGFW)*	**Secure Endpoint** *(AMP for Endpoints)* **Secure Network & Cloud Analytics** *(Stealthwatch)* **Extended Detection & Response** (XDR) **Secure Email** *(Email Security)* **Vulnerability Management** (*Kenna*)

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

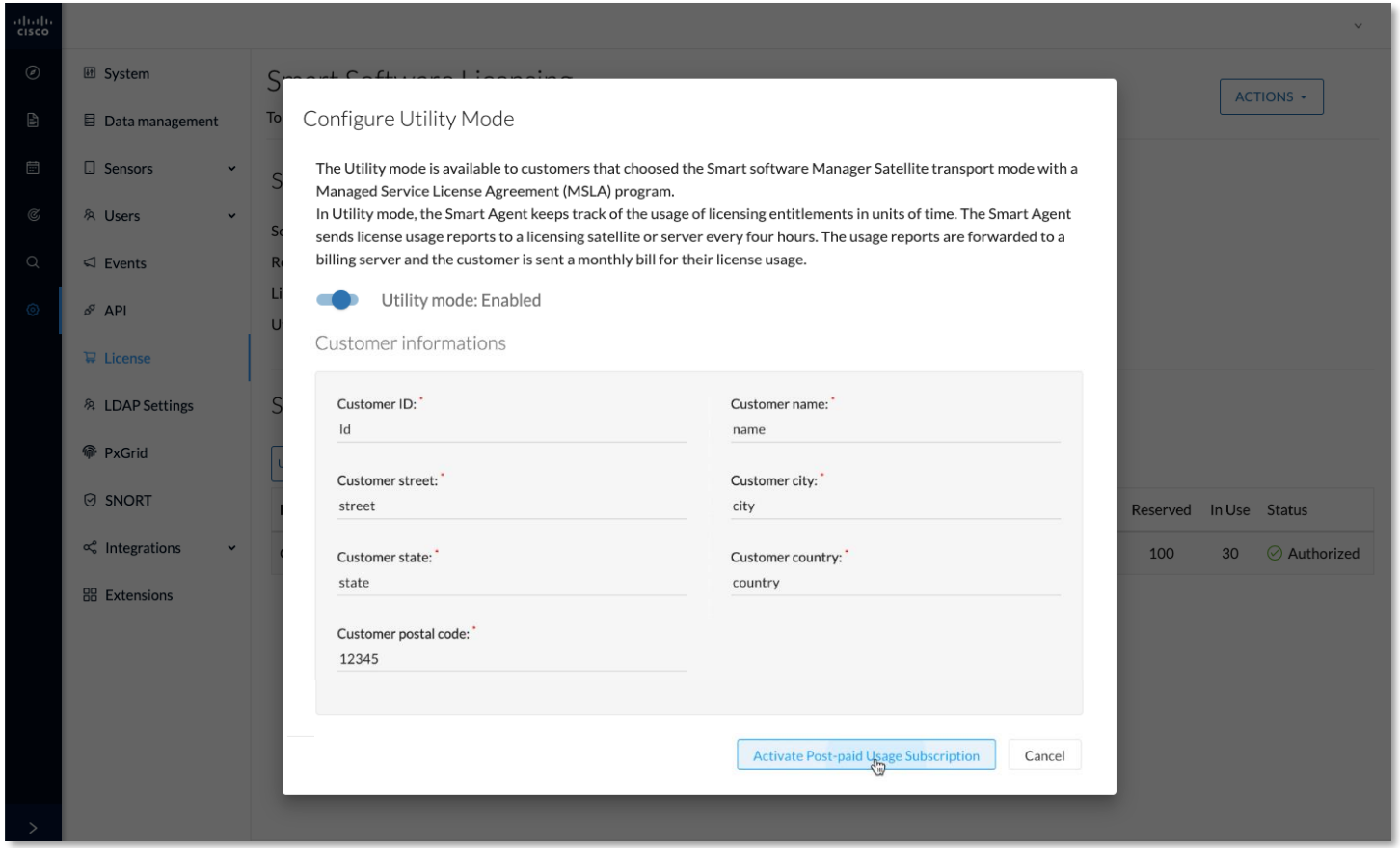
Requirements

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

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



- 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

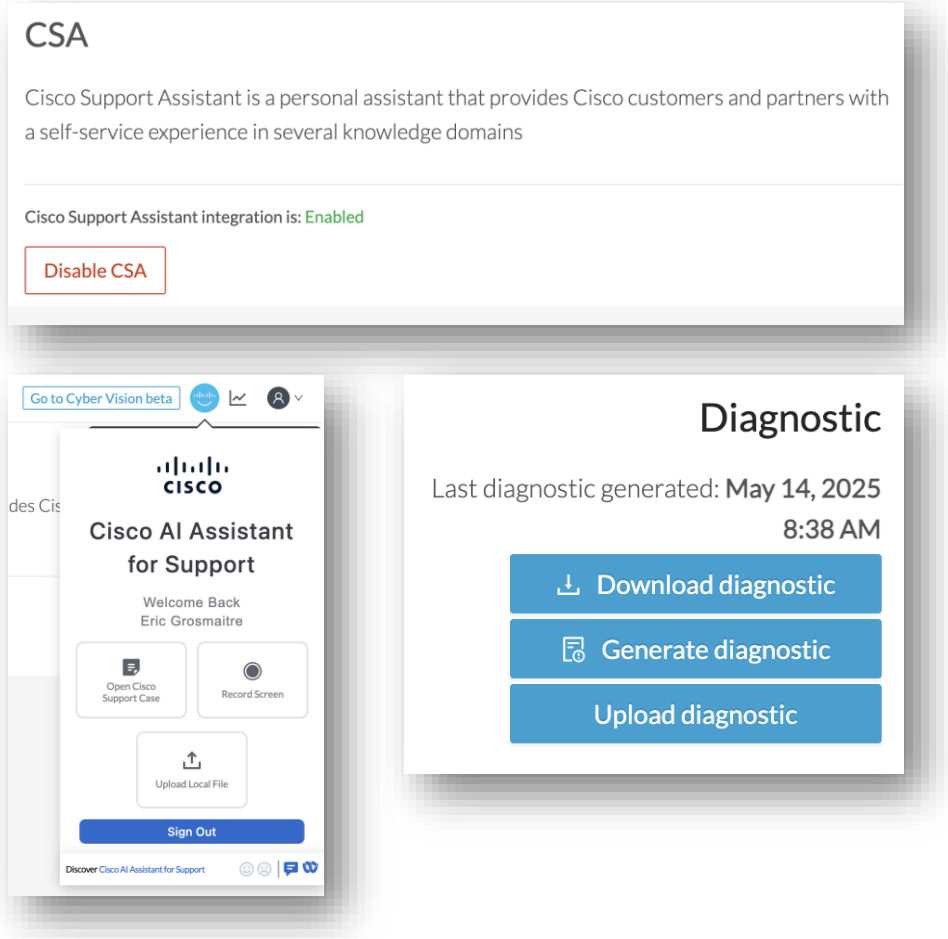
Administration Features

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.

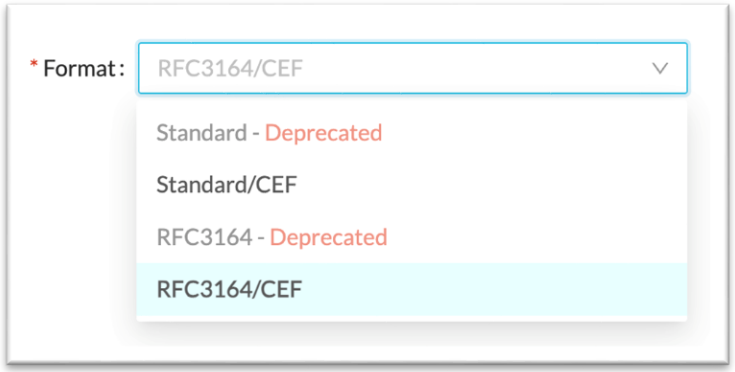
Note:

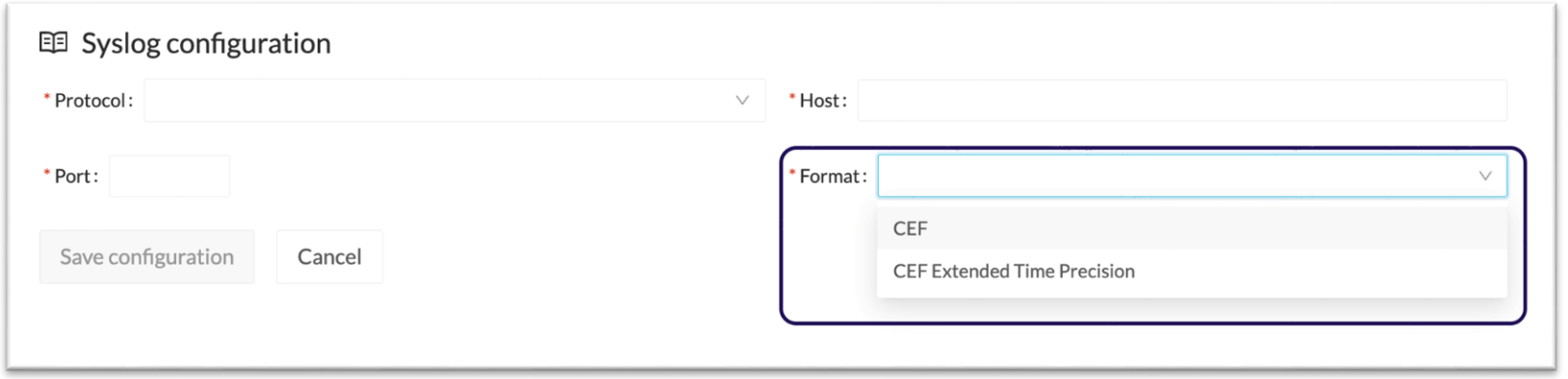
- The feature needs to be enabled (Admin->Integrations->CSA)
- To use the feature, you need to provide a login to “Cisco AI Assistant” service
- Automatically upload a diagnostic bundle file from the “System Statistics center page” of CV to the technical support case



Supported Syslog Formats

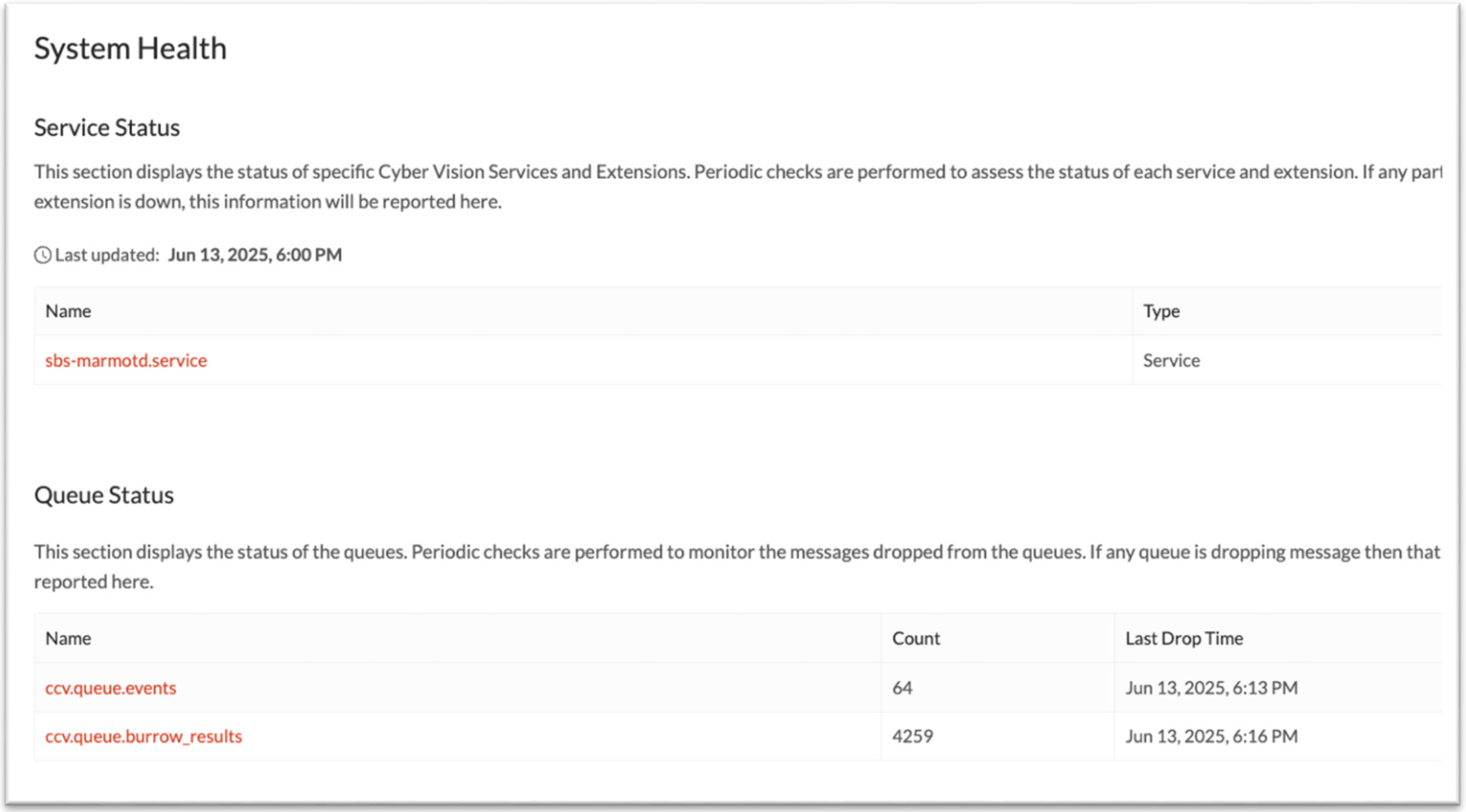
With version v5.3, the list of supported syslog formats is restricted to CEF:





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

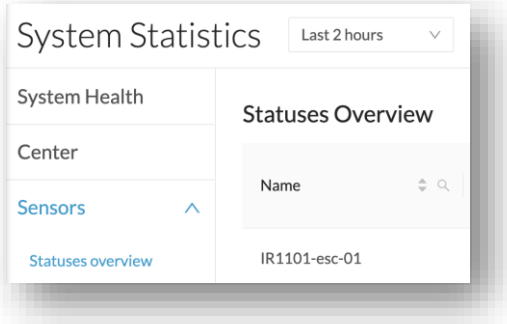
Queue Status

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.

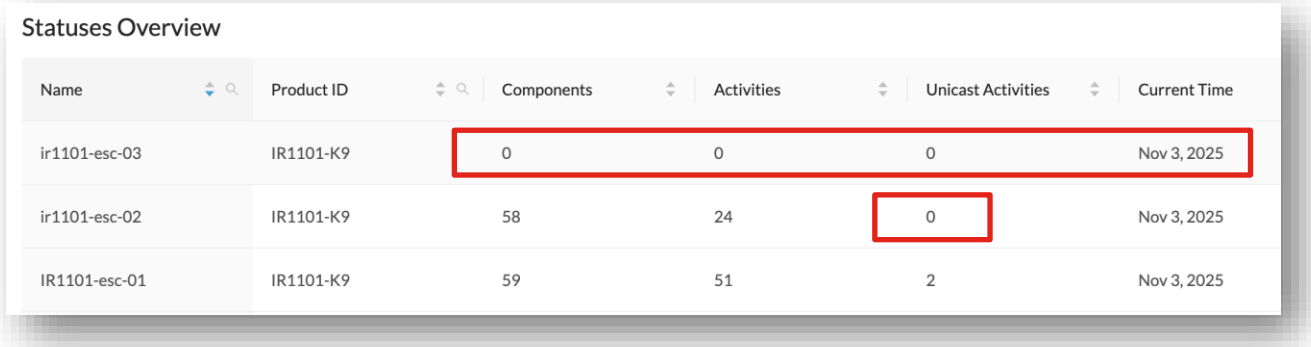
Name	Count	Last Drop Time
ccv.queue.events	64	Jun 13, 2025, 6:13 PM
ccv.queue.burrow_results	4259	Jun 13, 2025, 6:16 PM

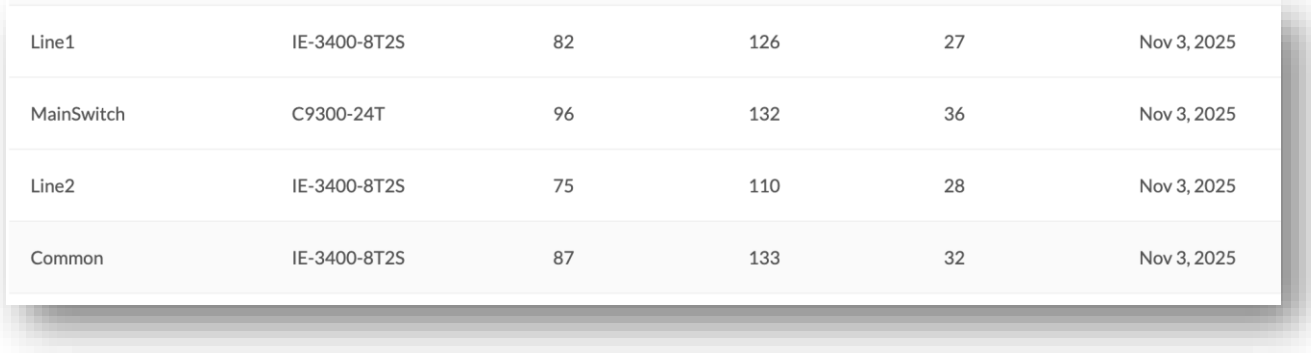
Sensor data collection report

- 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.





Cyber Vision Knowledge Database

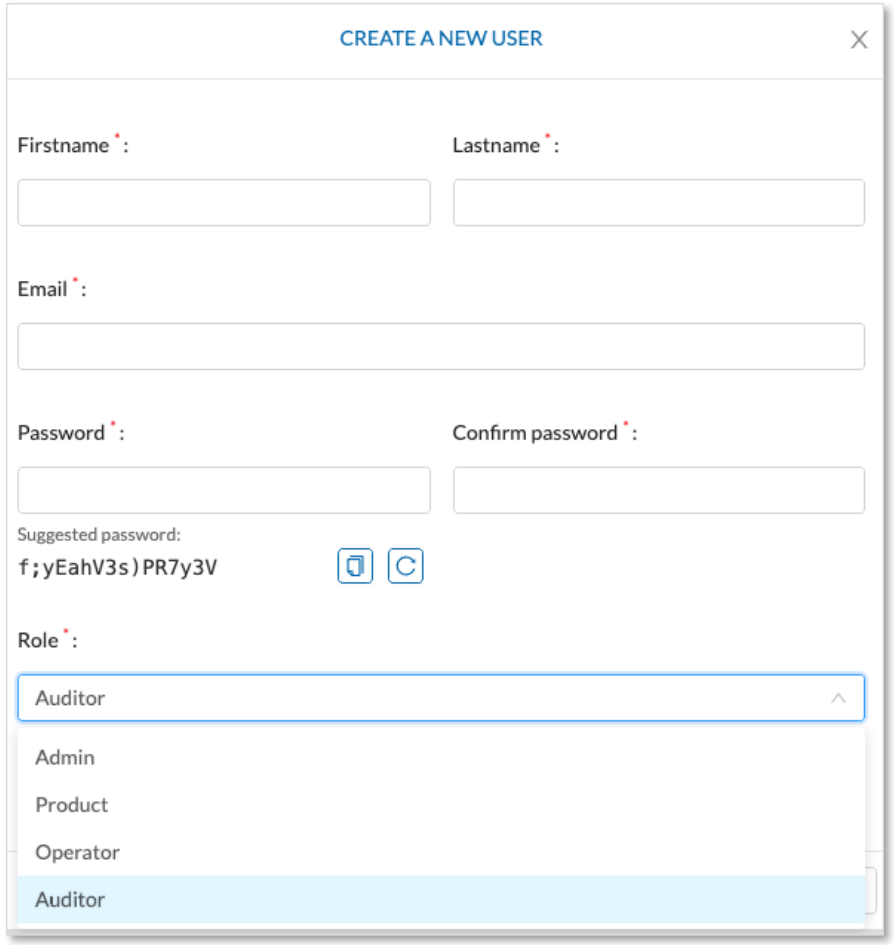
Includes:

- 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

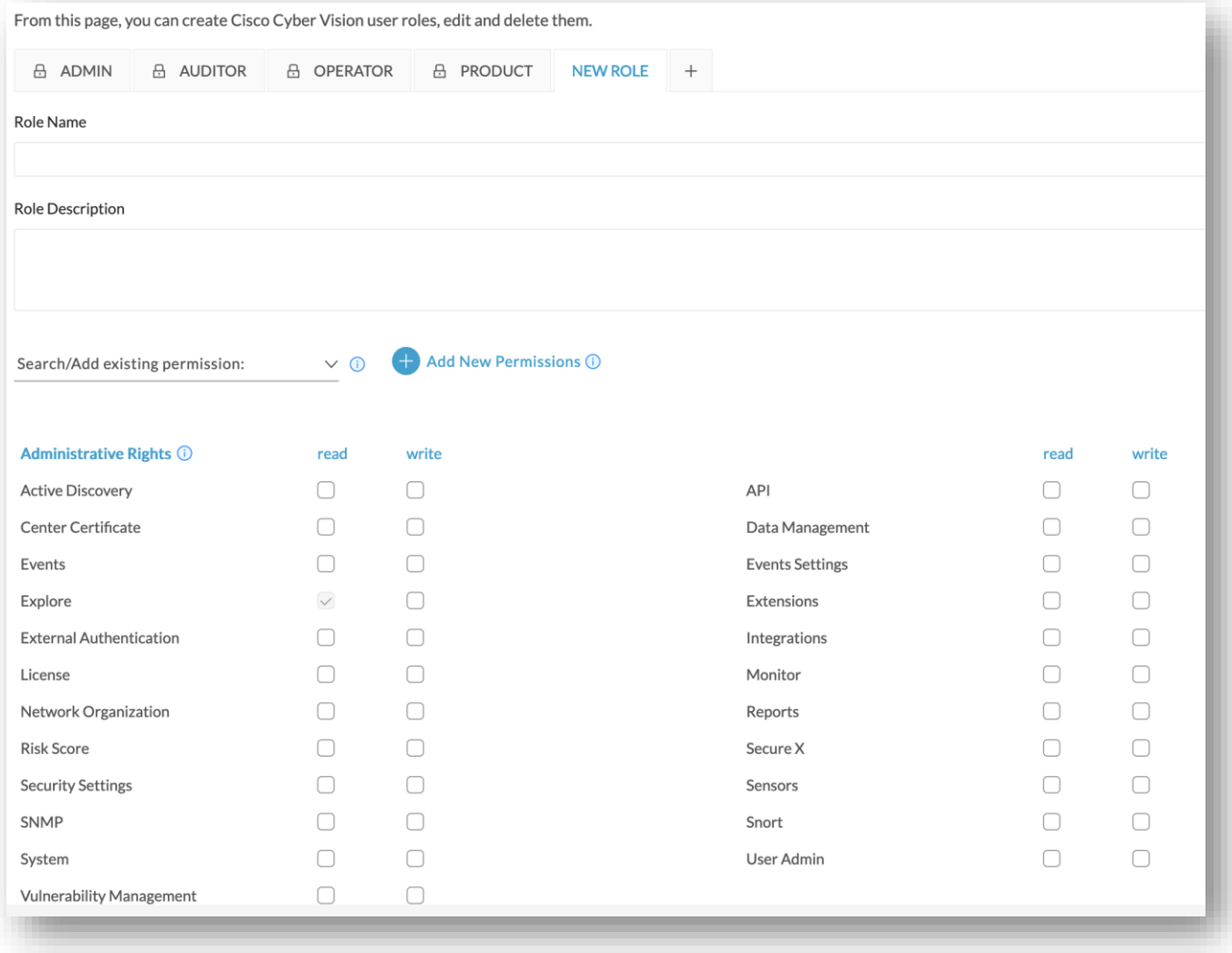
Role Based Access Control

- 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



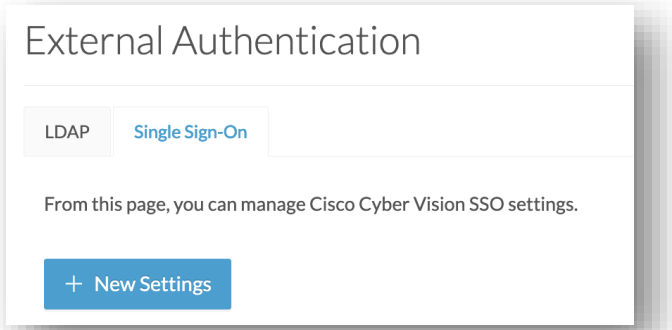
Custom User Roles

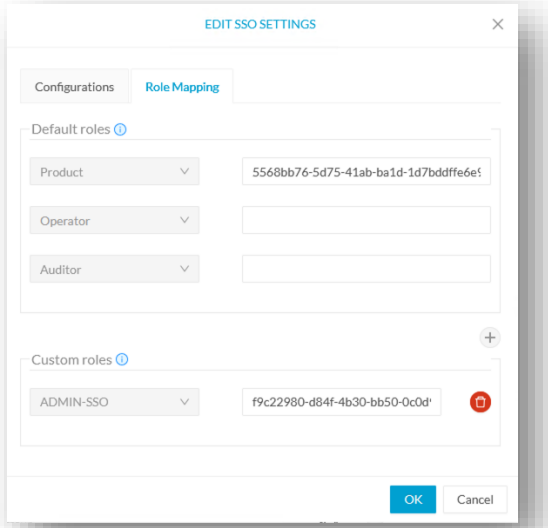
- Create roles to customize read/write access to different parts of Cyber Vision
- Minimum default access is read-only for the Explore page
- Easy role creation by duplicating and modifying existing roles

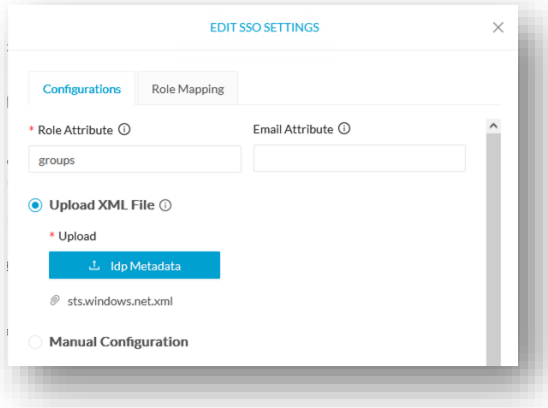


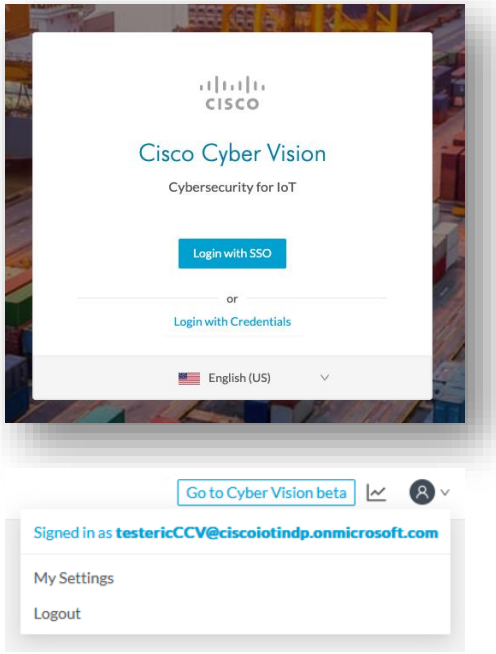
SAML 2.0 Support for Authentication

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



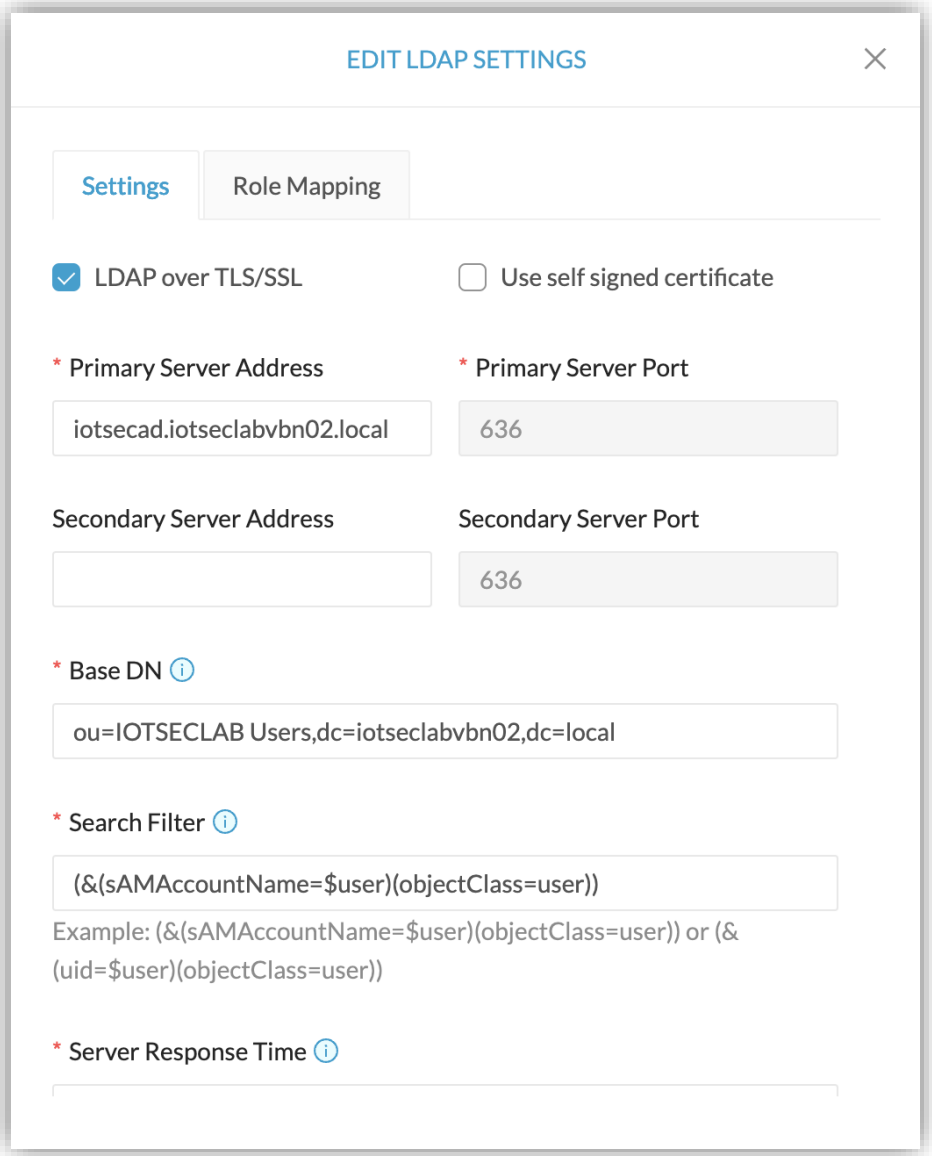






LDAP integration for User Authentication

- 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

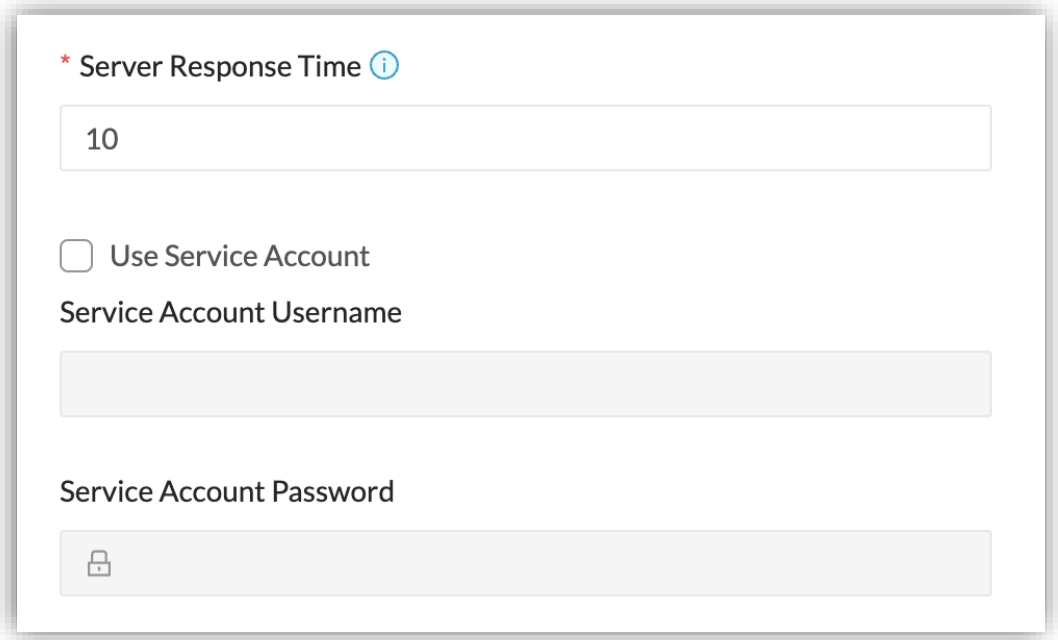


LDS Support (Lightweight Directory Services) [1/2]

- 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))”

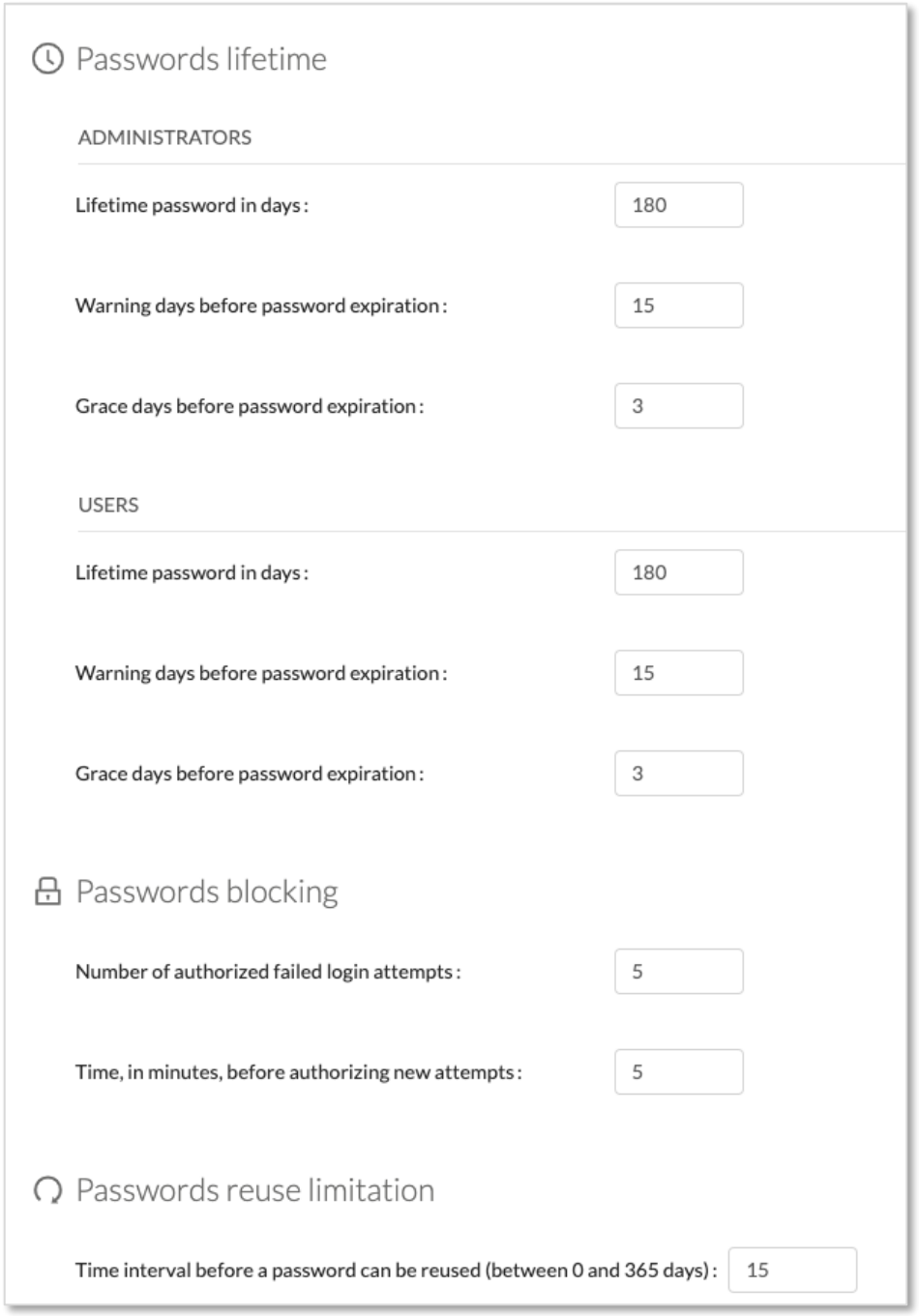
LDS Support (Lightweight Directory Services) [2/2]

- 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.



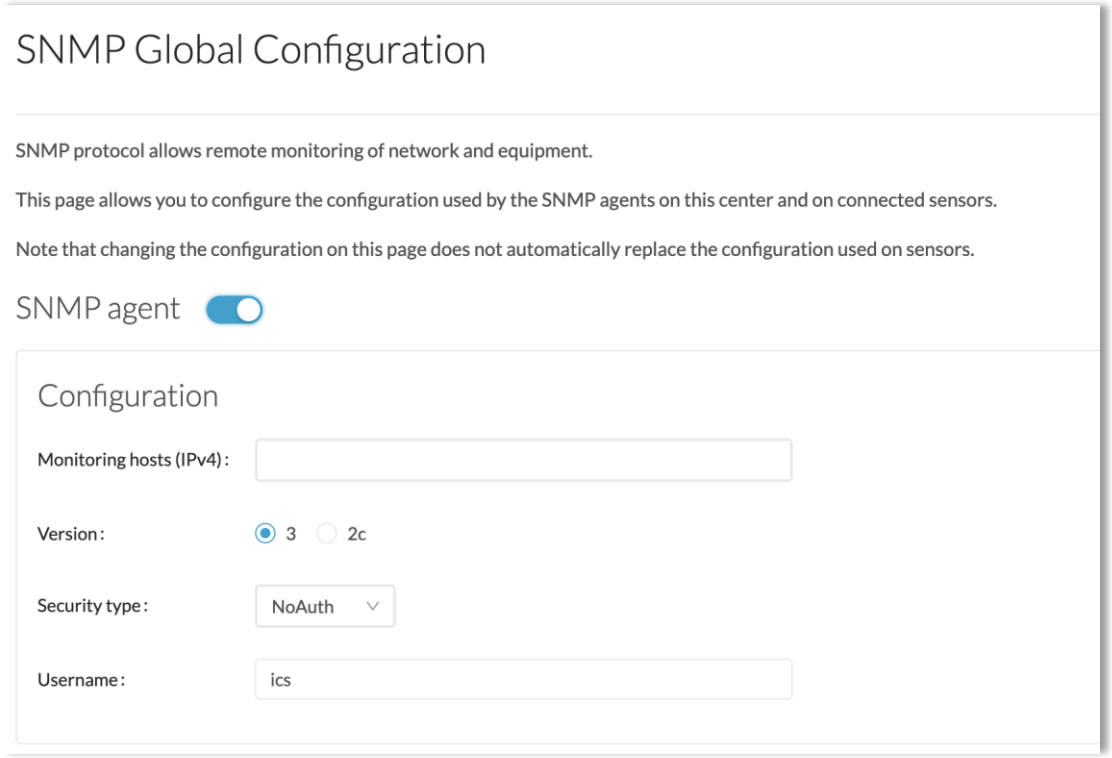
User security settings

- Define password lifetimes and reuse



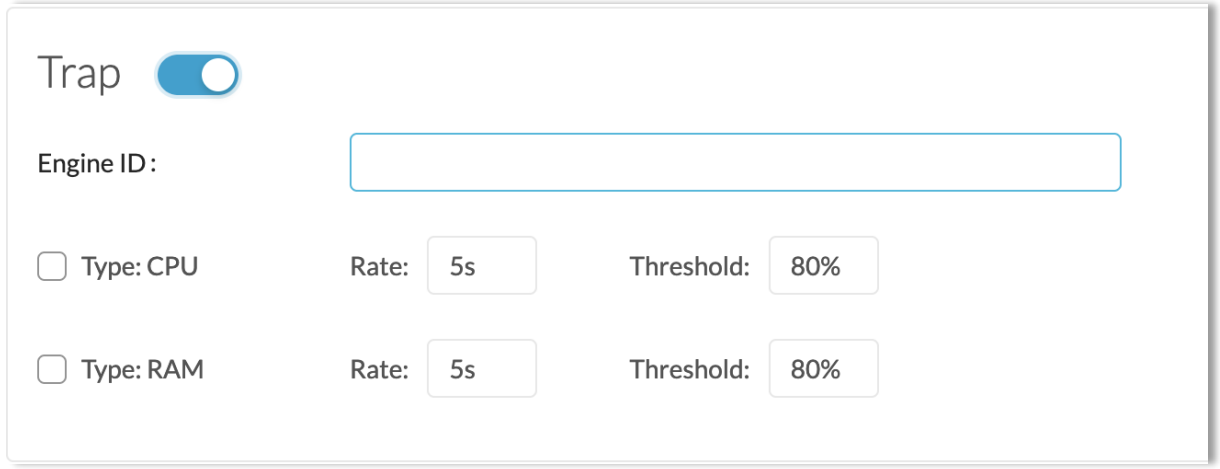
Cyber Vision Center SNMP monitoring

- 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

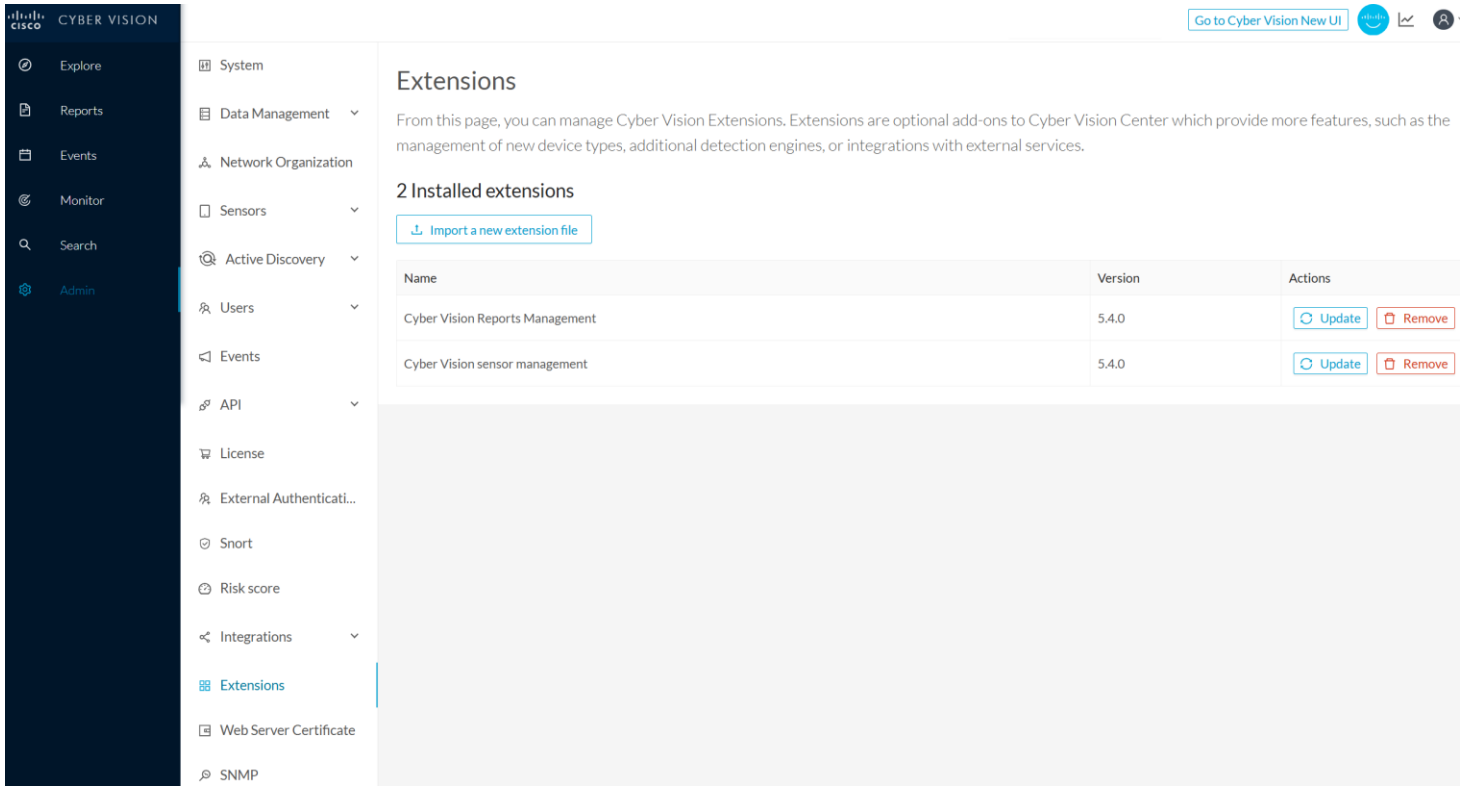


SNMP traps

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



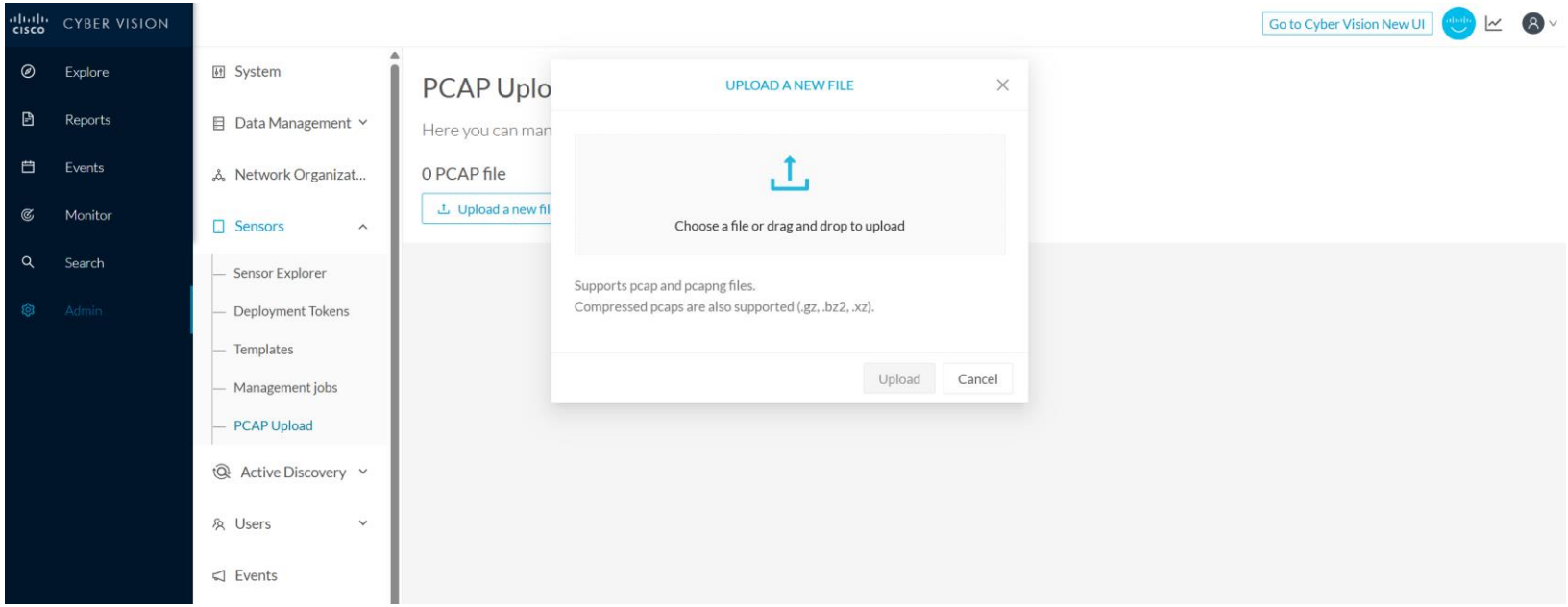
Extension modules



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

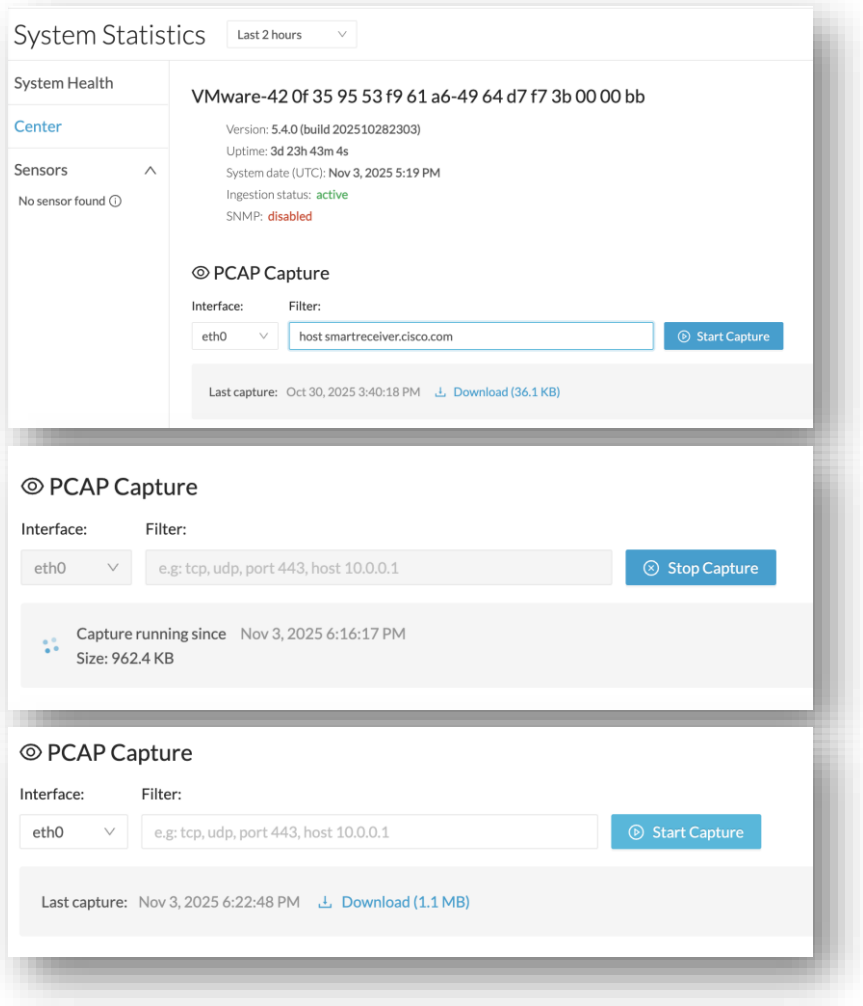


- Enables to use/demonstrate Cyber Vision with customer provided packet captures (PCAP)
- PCAP Upload at Admin->Sensors
- Ability to automatically create matching preset and rewrite packet timestamps to time of import

PCAP recording on Center interface

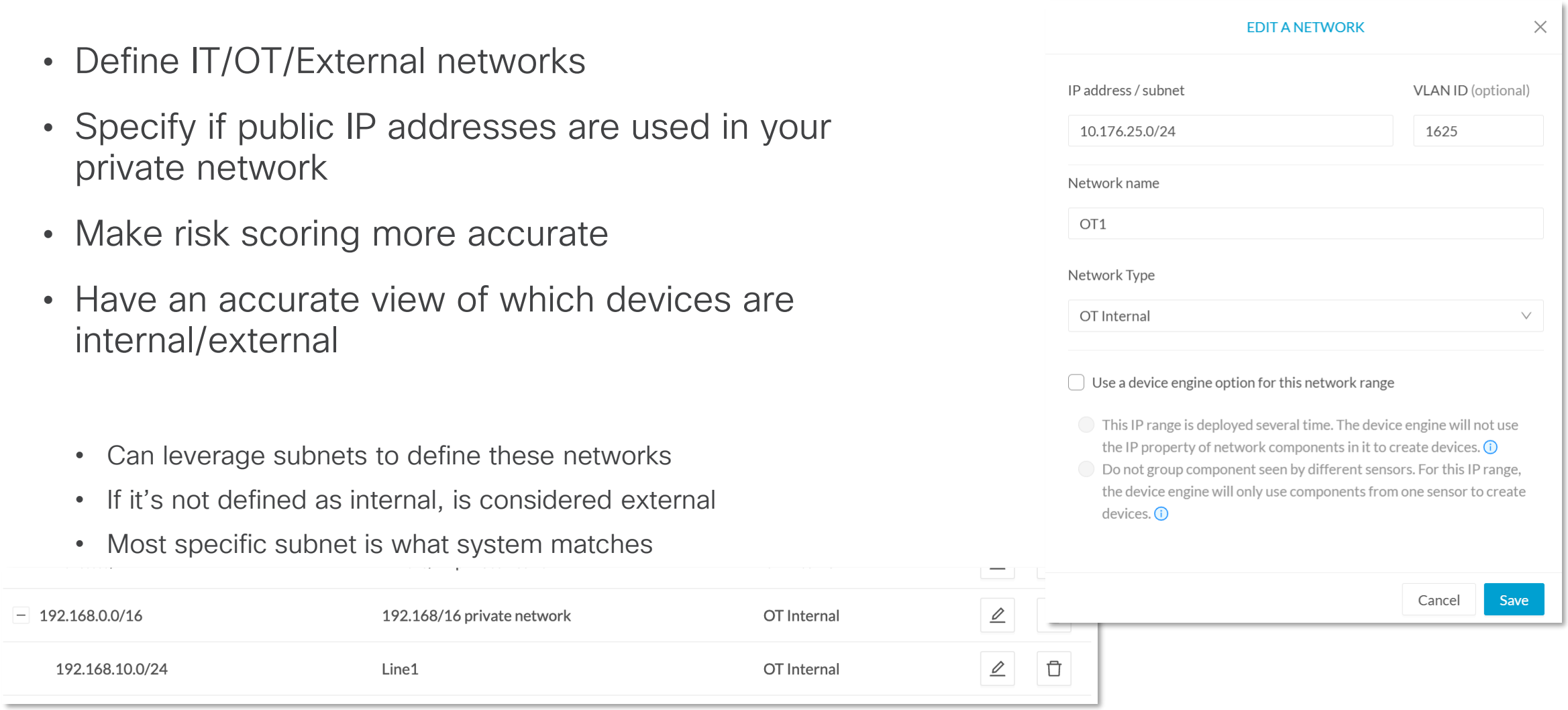
Starting with v5.4 PCAP recordings of the Center interfaces are now possible from the CV Center GUI.

- 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.



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

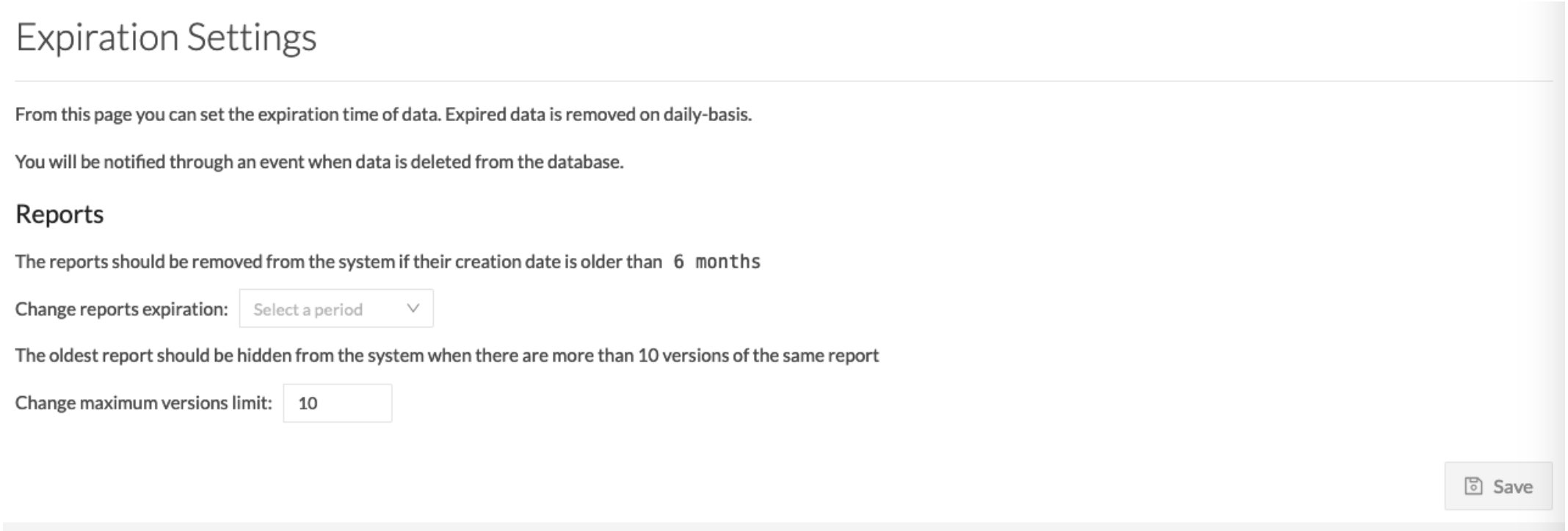


External Component Handling

- 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

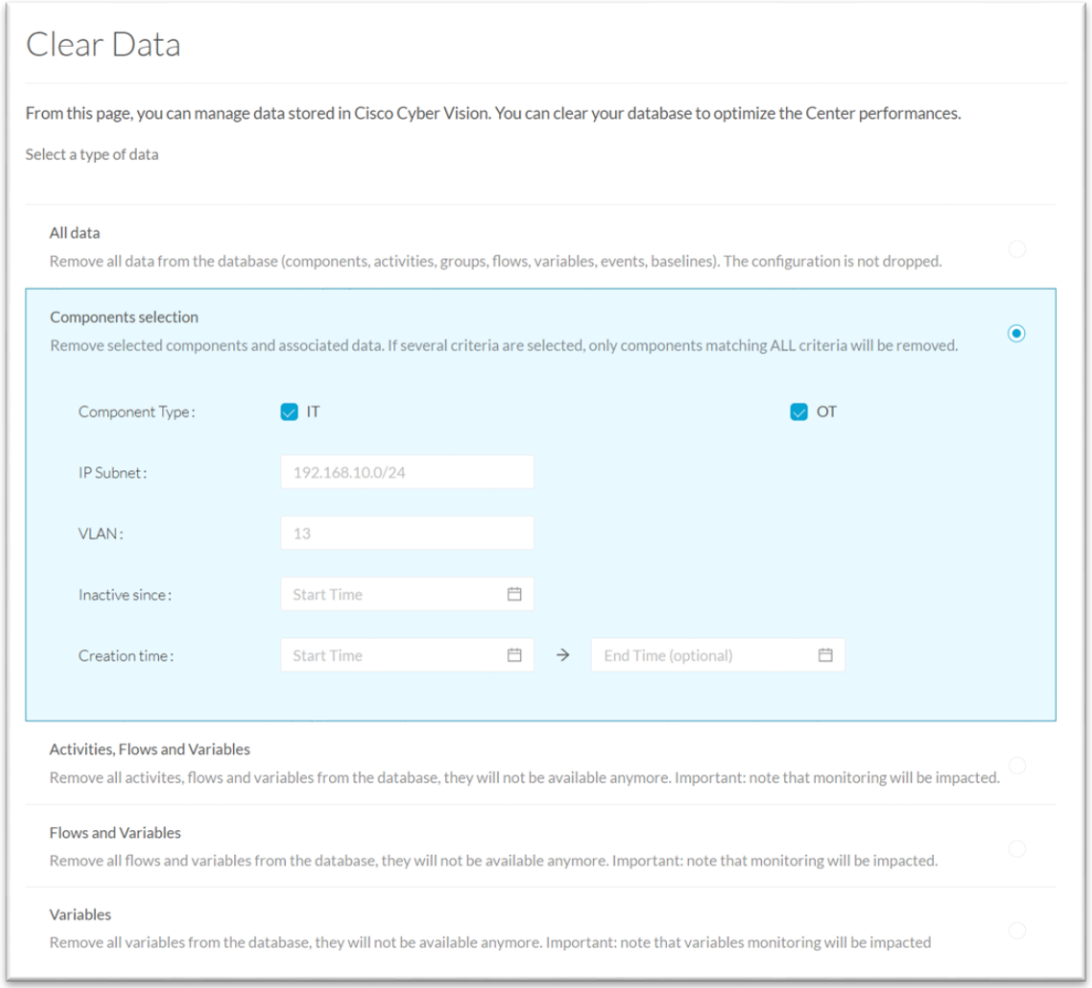
Define Data Expiration Settings

- Configure report storage settings in Cyber Vision Center



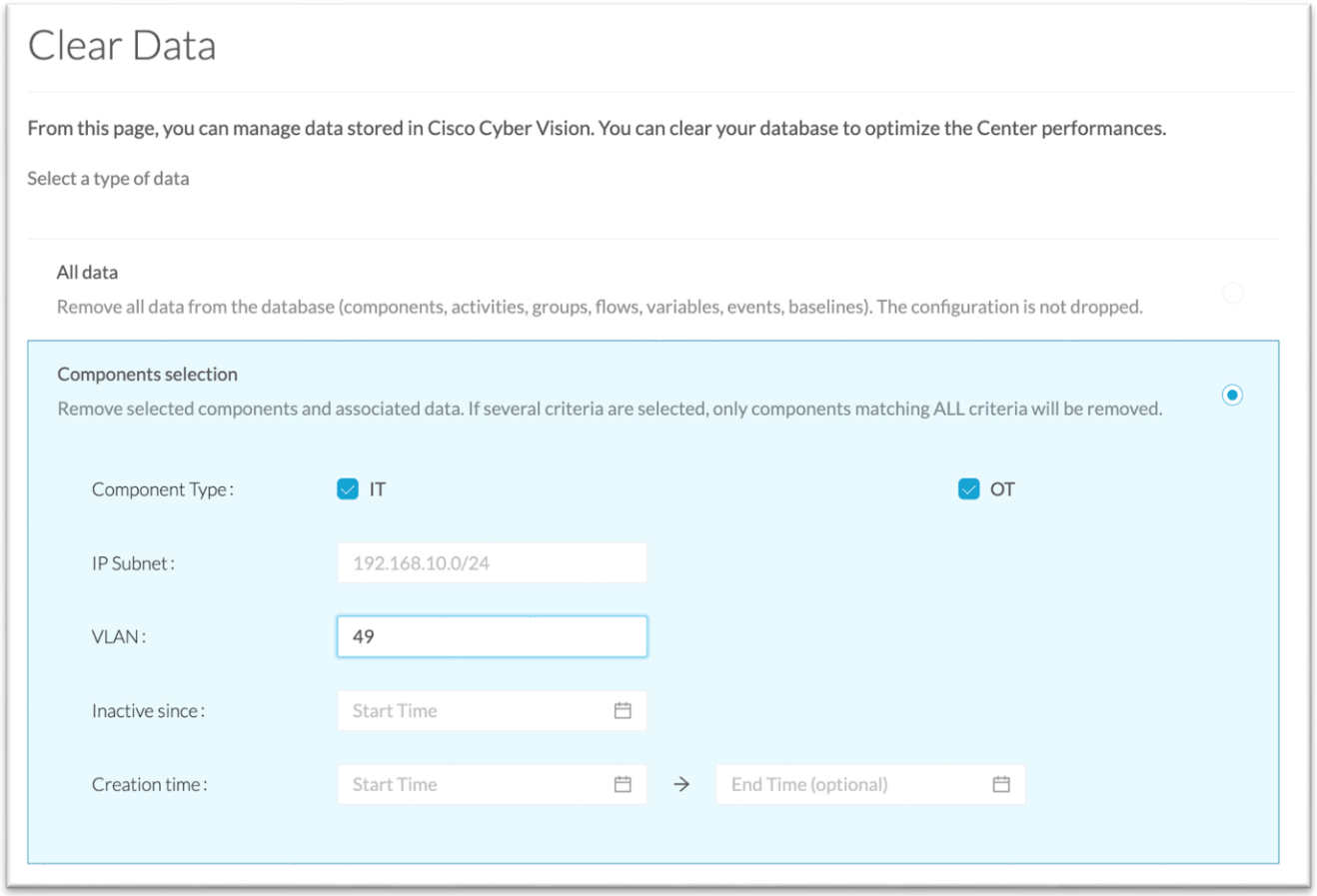
Clear Data

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



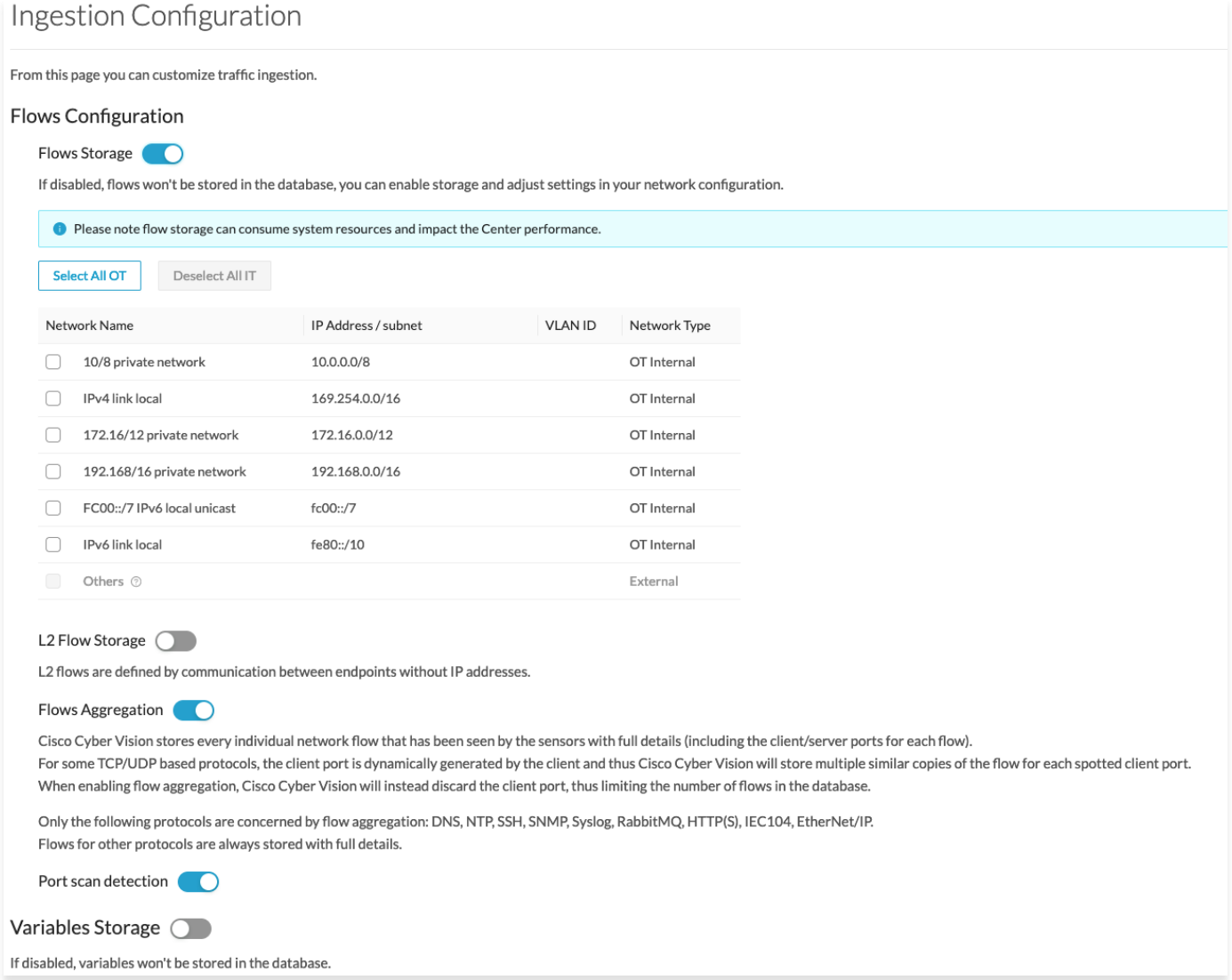
Purge Components originating from a VLAN

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

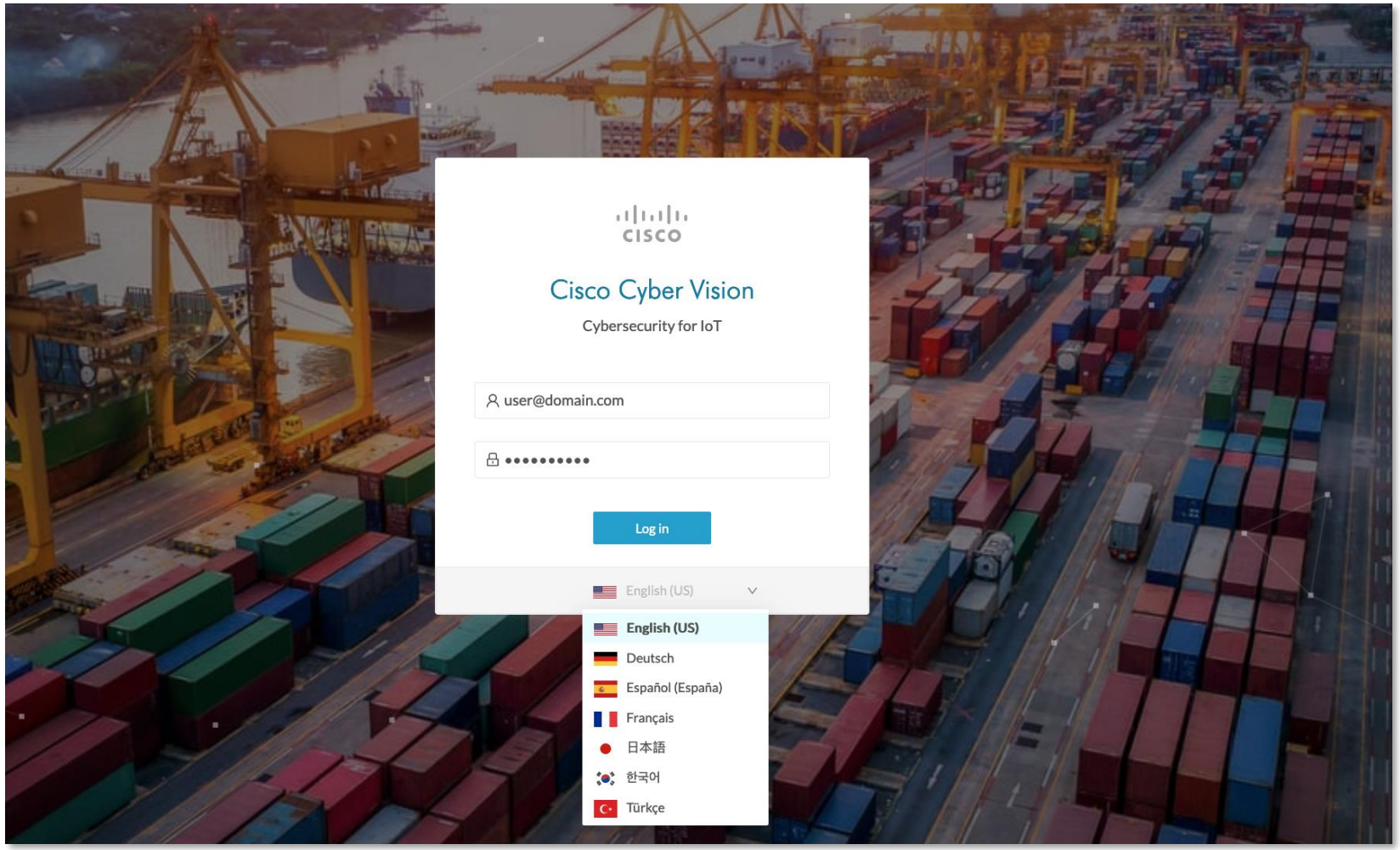


Configurable Flow Storage

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



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

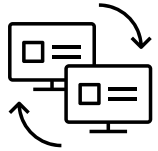
+

Best of OT Networking
Deep understanding of industrial requirements

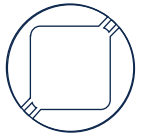
OT Visibility

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


CISCO