

OT Security Assessment with Cyber Vision

cisco Live !

Best Practices and Lessons Learnt from the Field.

Jay Adusupalli
Technical Leader, CX APJC

Session ID: BRKIOT-2073

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

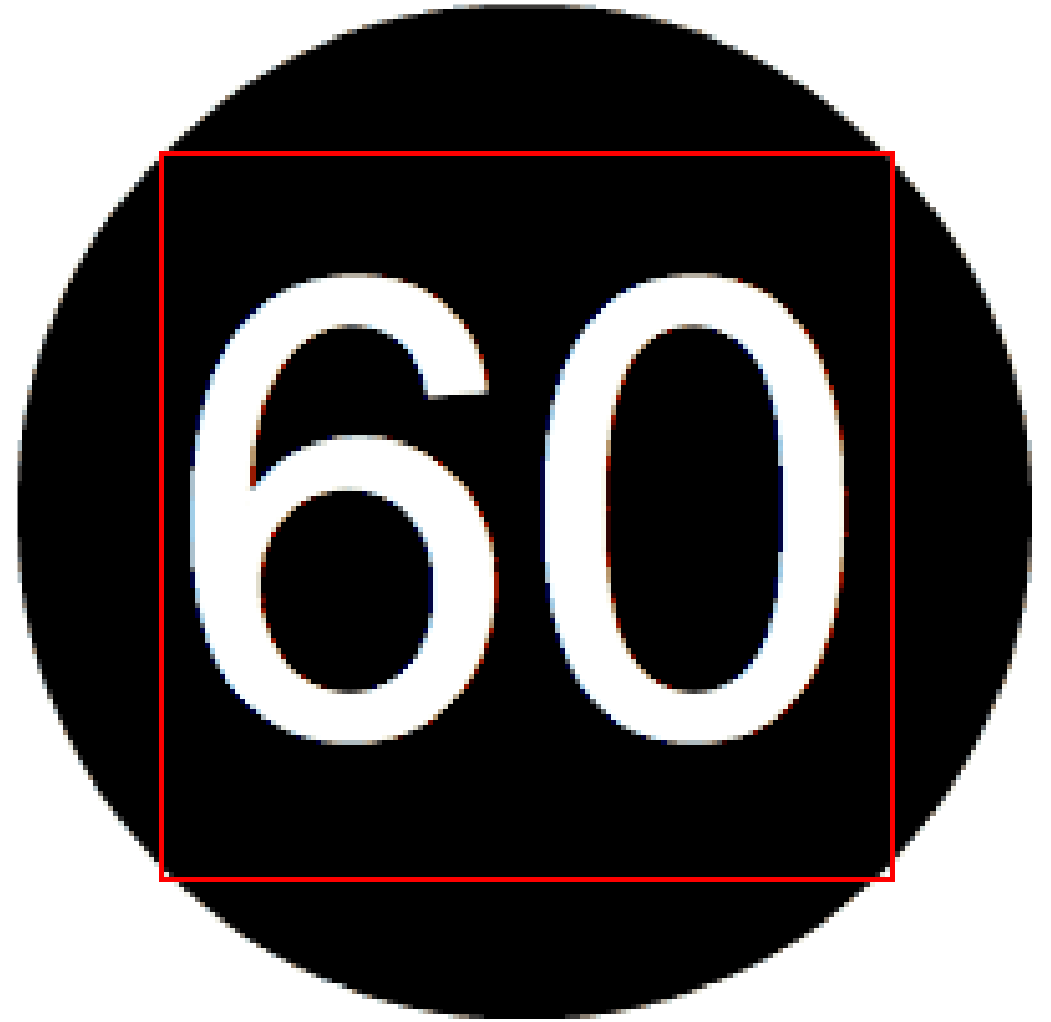
Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-2073>



**You have
seconds!**



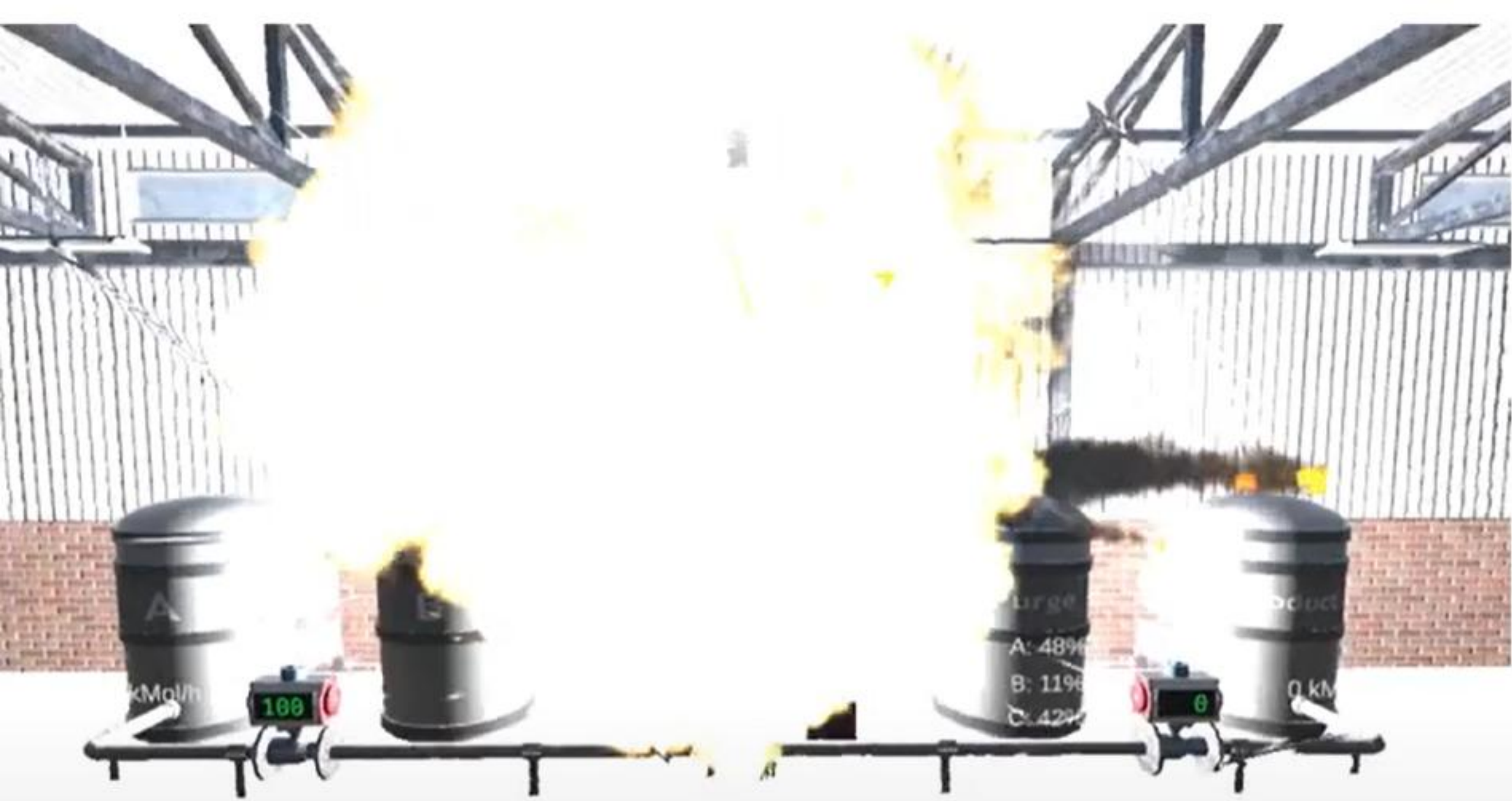




Reduce input “A” manually and cut down external connections.



To manage a cyber attack, the option is to **modify B and D** rather than reduce **A**. This aligns with common cybersecurity best practices where modifying or strengthening specific controls or configurations (such as network segmentation, access policies, or security group settings) is more effective than simply reducing a parameter A without context.



Agenda

- 01 The Threat Landscape
- 02 Why an OT Assessment?
- 03 Assessment Workflow
- 04 Lessons learnt from the field
- 05 The future of Industrial Security

The Threat Landscape

OT Cybersecurity Threats have escalated dramatically

Adversaries present target awareness



Lower Entry Barriers

Adversaries demonstrate growing awareness of OT as an effective attack vectors



Diverse Threat Actors

State-sponsored groups, cyber criminals and hacktivists target industrial operations.



Ransomware Surge

Ransomware Attacks against industrial organizations have increased 87% Year on Year



Manufacturing Focus

Manufacturing remains top target.

Japan's Ransomware Surge:

68 Incidents Target Critical Infrastructure in 2025

Dramatic Incident Increase

Japan experienced 68 ransomware cases during first half 2025, representing 1.4-fold increase.

Manufacturing Sector Dominance

Manufacturing sector experienced highest number of incidents at 18.2% of total cases.

SME Primary Targets

Organizations with capital under 1 billion yen made up 69% of all cases.

Qilin Emerges Leader

Qilin ransomware group emerged as most active with eight confirmed victim organizations.

UAT-5918

APT Targeting Taiwan's Critical Infrastructure

Talos assesses with high confidence that UAT-5918 is an advanced persistent threat group targeting entities in Taiwan.

UAT-5918 deploys web shells across discovered sub-domains and internet-accessible servers to open multiple entry points.

UAT-5918's tooling and TTPs overlap substantially with several APT groups including Volt Typhoon and Flax Typhoon.

Why do an Assessment?

Typical issues found in industrial networks

Unauthorized remote access by third parties

OT network fully connected to IT Default credentials to log into systems

Security Patches not installed Unknown devices

Flat/Unsegmented Networks Bad Firewall or Switch configuration

Firmware uploaded over FTP without Signature

Multiple Time Servers DNS queries to Amazon Windows XP SMBv1

Unnecessary network communications

Decommissioned assets still connected IPv6 traffic in IPv4 networks

Devices in the wrong VLAN Malware or Virus activities

Program Upload over VPN during the night

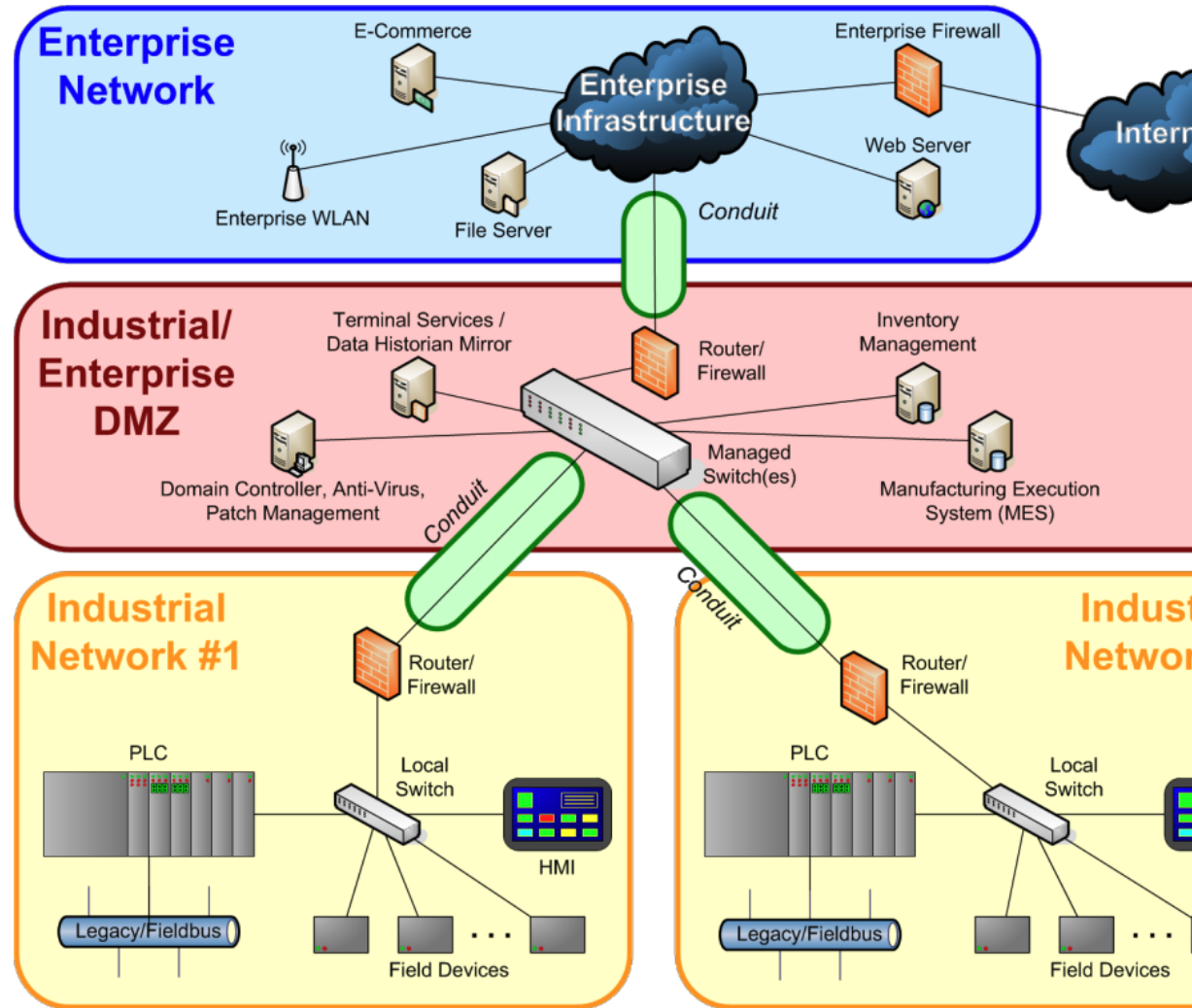
Intensifying Regulatory and Compliance Pressures on Critical Infrastructure

- **Global and Regional Standards Tighten**
 - NIST 800-82, IEC 62443, NERC CIP, EU NIS2 now mandate higher OT security
- **Transportation & Utilities Rules**
 - TSA directives drive security upgrades for pipelines, rail, aviation
- **Sector-Specific Compliance**
 - FDA rules in healthcare, CFATS for chemical plants
- **Compliance as Investment Driver**
 - Regulation spurs layered defences, segmentation, ZTNA adoption
- **Harmonization Trends**
 - Governments, ISA, NIST work to unify resilience frameworks

Prerequisites to implementing ISA/IEC 62443

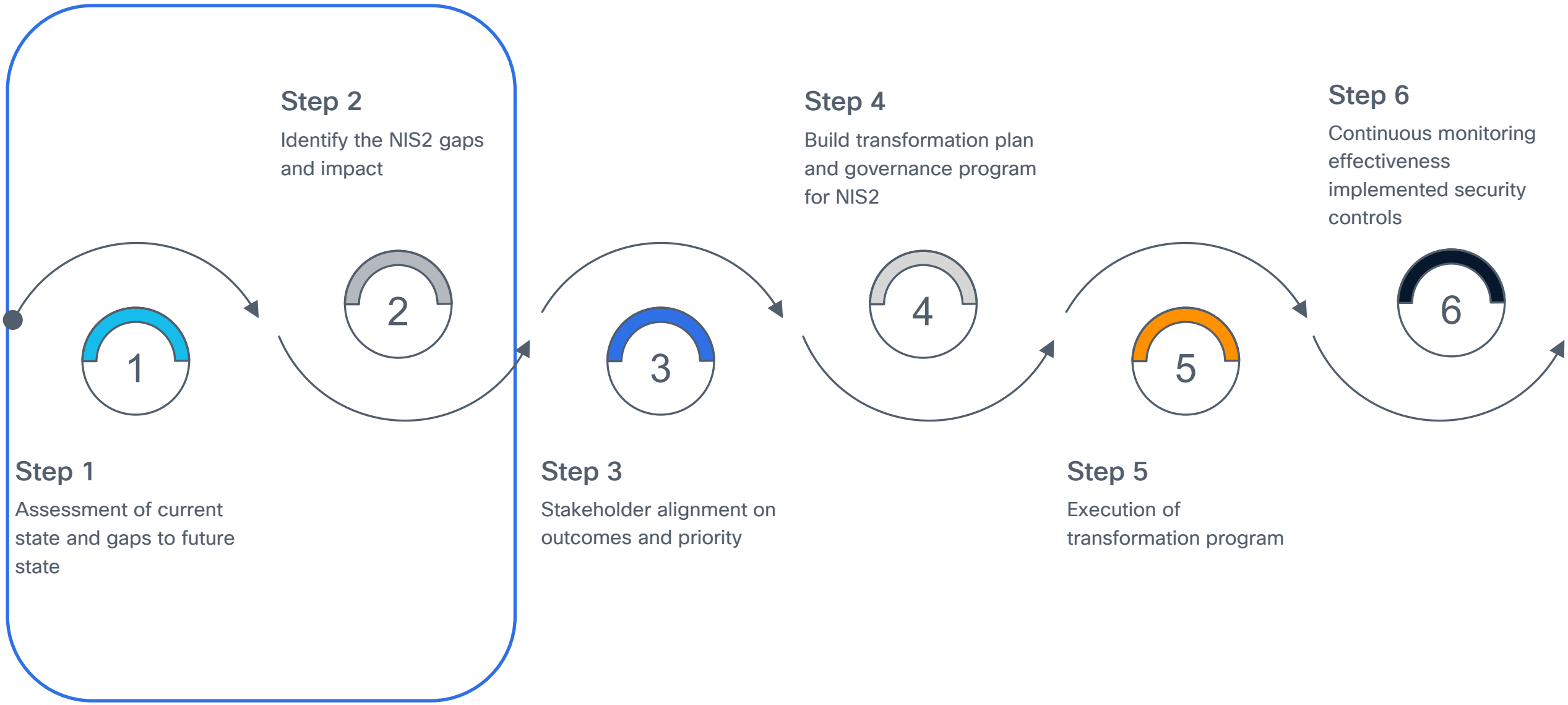
- OT Security Assessment based on IEC 62443-3-2 to understand:
 - What to protect (System under Consideration)
 - The right security level to achieved (Target-SL)
 - Where information flows
 - How systems and devices interact
 - Group assets that share common security requirements into zones & conduits
- Asset owner's policies & procedures
 - Determine the Target Security Level

ISA/IEC 62443 Zones and Conduits



- **Zone:** Collection of entities that represent a partitioning of a System under Consideration (SUC)
- **Conduit:** connecting a zone with another zone or with the outside that share common security requirements

Step 1&2 in NIS2 Customer journey



Cyber Vision Assessment

You cannot secure what you don't know



Most customers don't have accurate asset inventory

55% have no or low confidence that they know all devices in their network

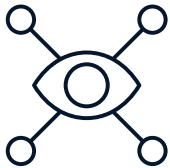


Blind to what their assets are communicating with

ICS equipment deployed over the years without strict security policies

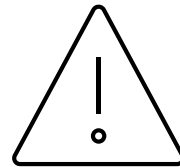
Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT



Visibility

OT asset inventory
Communication patterns



Security Posture

Device vulnerabilities
Risk scoring



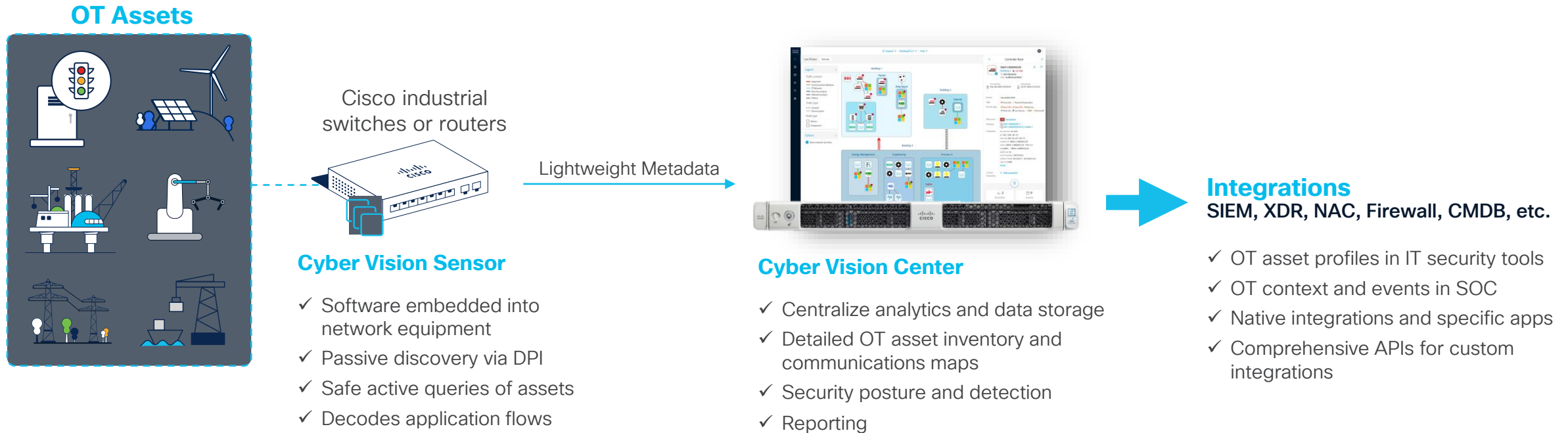
Operational Insights

Track process/device modifications
Record control system events

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

Cisco Cyber Vision: Unique 2-Tier Architecture

OT Visibility that can be deployed at scale



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

The Cyber Vision Workflow

OT Assessment

Step1. “See what you have”

Comprehensive asset inventory

[illegible]

Detailed information on assets

4 Activities

42 Events

10 Vulnerabilities

Controller, Rockwell Automation

Start CPU, Stop CPU, Diagnostics, Read Var, Write Var, Low Volume, CIP-IO, EthernetIP, Umas (hide)

Properties

Components

Tags

Normalized Properties

Other Properties

4 Components

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

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

Tags to easily understand characteristics, activities, and threats

Asset characteristics, version and network configuration

Control logic properties

Rack slot component details

Operational insights for OT teams

Component



SIMATIC 300(1)

IP: 192.168.0.1

MAC: 00:0e:8c:84:5b:a6

24

Flows

51

Events

5

Vulnerabilities

-

Credential

13

Variables

First activity

Apr 6, 2017 11:29:22 PM

Last activity

May 26, 2019 12:21:13 AM

Read Var

PLC

Add to group

Create group

Basics

Security

Activity

Automation

Properties

Tags

Properties

Vendor-Name: Siemens AG A&D ET

Model-Name: CPU 315-2 PN/DP

Fw-Version: V 2.5.0

Hw-Version: 3

Model-Ref: 6ES7 315-2EH13-0AB0

Serial-Number: S C-V1R583472007

Name: SIMATIC 300(1)

Ip: 192.168.0.1

Public-IP: no

Mac: 00:0e:8c:84:5b:a6

S7-Bootloaderref: Boot Loader

Vendor: Siemens AG A&D ET

S7-Hwref: 6ES7 315-2EH13-0AB0

S7-Rack: 0

Name-Vendorip: Siemens 192.168.0.1

S7-Serialnumber: S C-V1R583472007

S7-Hwver: 3

S7-Plcname: SIMATIC 300(1)

Name-S7-Plc: SIMATIC 300(1)

S7-Modulever: 3

S7-Slot: 2

S7-Bootloaderver: A 10.12.9

S7-Moduleref: 6ES7 315-2EH13-0AB0

S7-Modulename: CPU 315-2 PN/DP

S7-Fwver: V 2.5.0

Minimap

LEGEND

Important

Control system behavior

IT Behavior

Network analysis

Others

Machines - To Investigate

Manuf IO

Manuf - Scada & HMI

STATION-WINCC

SIEMENS IM151-3PN

Siemens et 65.8d

SENTRYO-XP-1

Siemens 192.168.0.10

SIMATIC 300(1)

SENTRYO-SIMATIC

Profinet DCP Multicast 0.0.0

10.45.1.255

Variables accesses

13

< 1 > 20 / page

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

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKIOT-2073



Operational insights for security analysts

Flows

< 1 > 40 / page

From	Source Port	To	Destination Port	First activity	Last activity	Tags	Packets	Bytes
Siemens 192.168.105.120	102	PLC_1	49158	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0B
PLC_1	102	Dell 192.168.105.241	1613	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	Program Upload , Start CPU , Stop CPU , Read Var , Write Var ...1+	0	0B
PLC_3	102	PLC_1	49159	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0B
Siemens 192.168.105.120	102	PLC_1	49158	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	No tags	0	0B
Siemens 192.168.105.120	0	PLC_1	0	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	ARP	0	0B
PLC_3	0	PLC_1	0	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	ARP	0	0B
PLC_1	102	Dell 192.168.105.241	1611	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	Program Upload , Read Var , Write Var , S7Plus	0	
PLC_1	102	Dell 192.168.105.241	1614	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	Read Var , Write Var , S7Plus	0	
PLC_1	102	Dell 192.168.105.241	1612	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	Read Var , Write Var , S7Plus	0	
PLC_1	102	Dell 192.168.105.241	1614	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	Read Var , Write Var , S7Plus	0	
Siemens 192.168.105.150	49162	PLC_1	102	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	Read Var , Write Var , S7Plus	0	
Siemens 192.168.105.150	49163	PLC_1	102	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	No tags	0	
PLC_1	102	Dell 192.168.105.241	1613	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	Program Upload , Start CPU , Stop CPU , Read Var , Write Var ...1+	0	
Siemens 192.168.105.150	0	PLC_1	0	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	ARP	0	
PLC_1	0	Siemens 192.168.105.150	0	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	ARP	0	

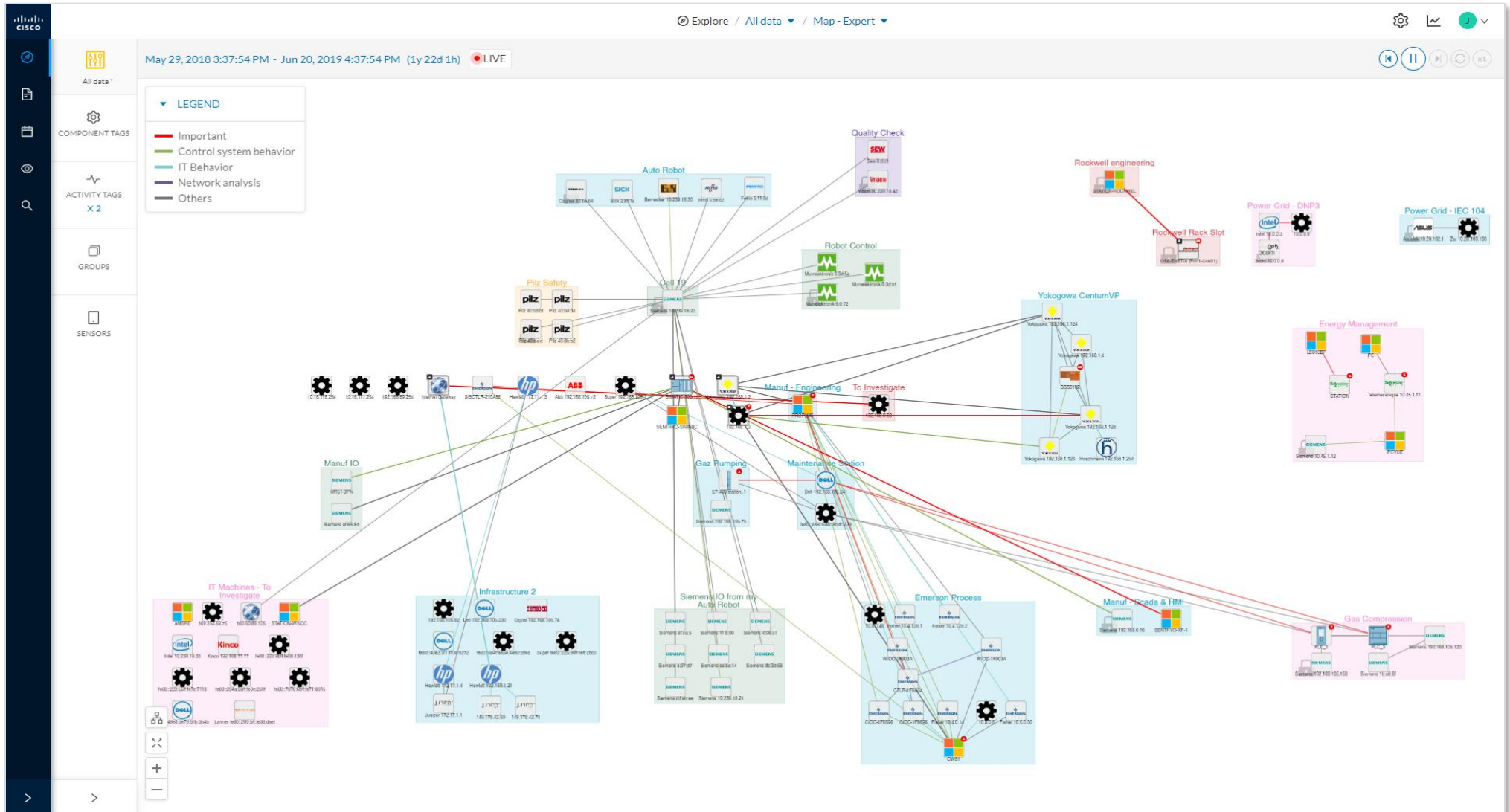
Content Statistics

< 1 > 40 / page

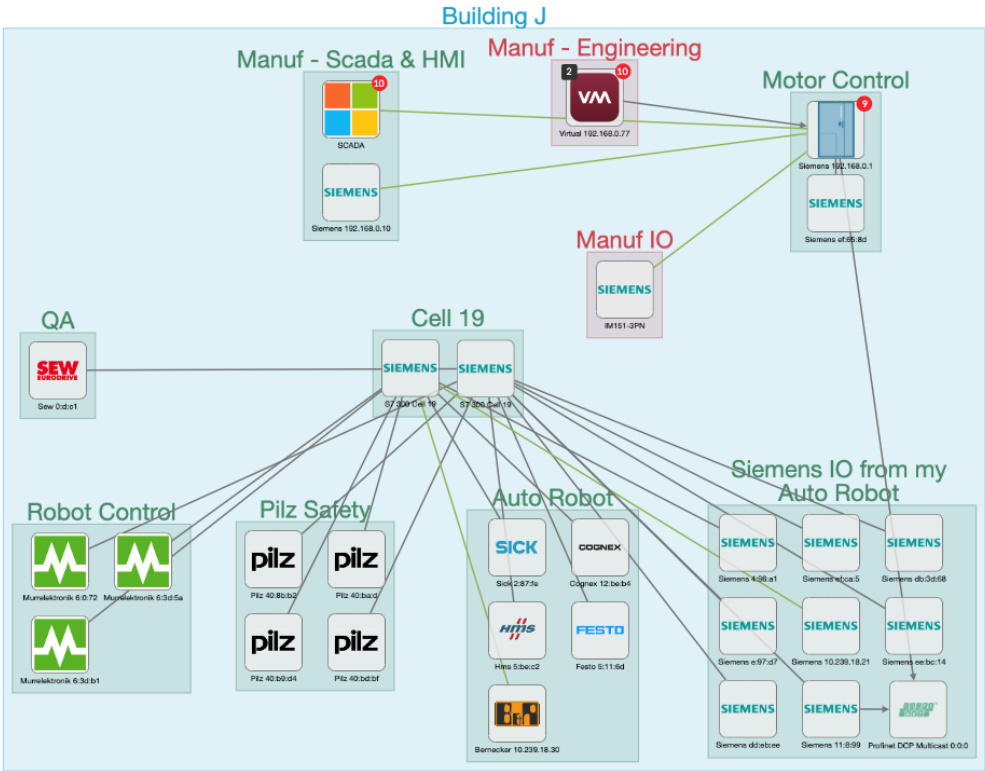
Property	Value	Occurrences
emerson-udp-event	setvar	7
emerson-udp-function	KeepAlive	1
emerson-udp-function	Message	7
emerson-udp-var-name	PID1/MODE	1
emerson-udp-var-name	PID1/SP	6
emerson-udp-var-scope	CV	6
emerson-udp-var-scope	TARGET	1
emerson-udp-var-value	49.52	1
emerson-udp-var-value	49.97	1
emerson-udp-var-value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

< 1 > 40 / page

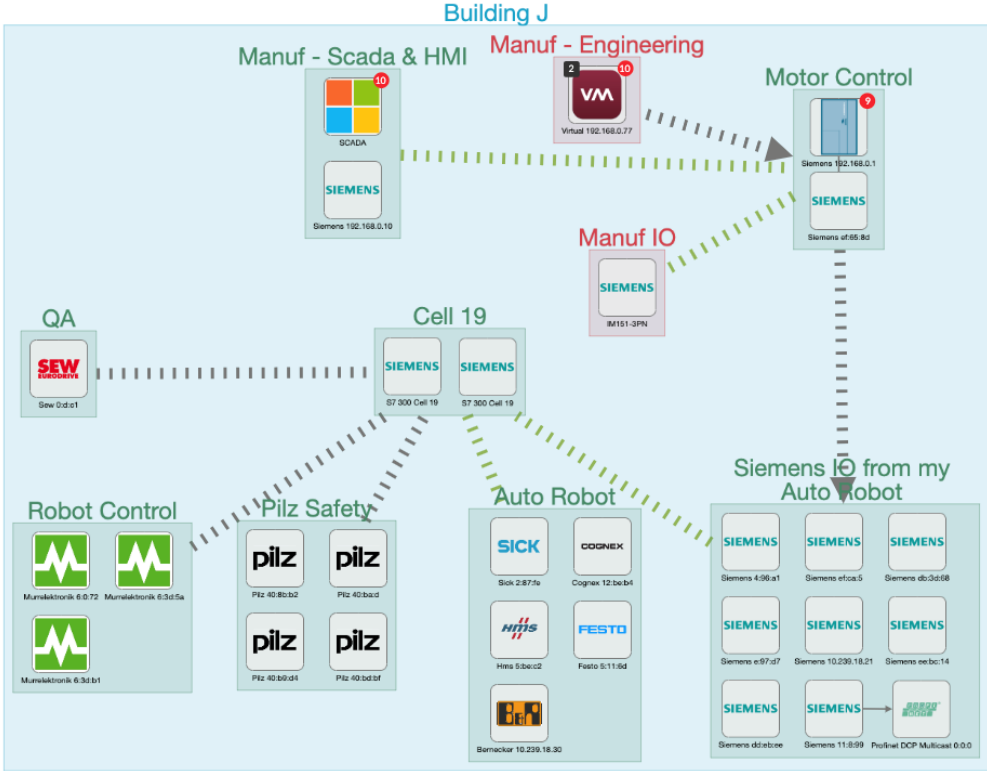
Detailed communication maps



Aggregated activities match ISA/IEC 62443 conduits

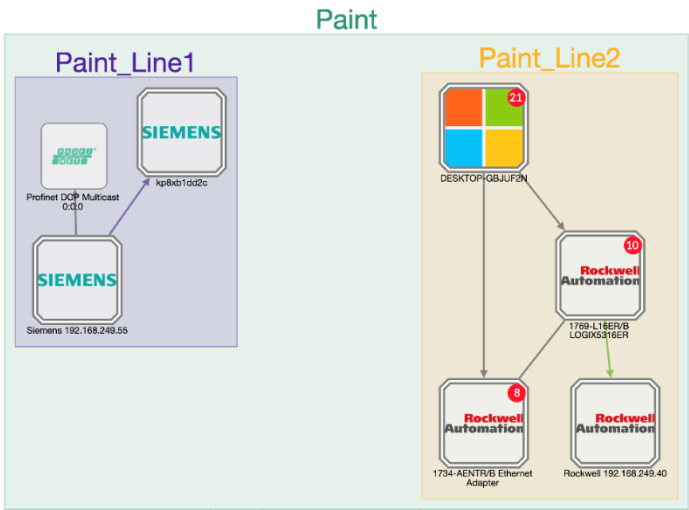


View all asset relationships

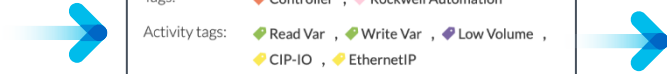


Easily browse through conduits

Aggregated components match the physical inventory



Double-border icons indicate a device with multiple components



Controller Rack

1769-L16ER/B LOGIX53...

Paint_Line2 high

IP: 192.168.249.50

MAC: f4:54:33:91:cb:ee

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

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

Sensor: -

Tags: Controller, Rockwell Automation

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

Risk score: 80% See details

Modules:

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

Properties:

fw-version: 31.011

ip: 192.168.249.50

mac: f4:54:33:91:cb:ee

model-ref: 24VDC 16PT INPUT & 16PT OUTPUT, 1769-L16ER/B LOGIX5316ER

name: Rockwell 192.168.249.50, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01), 1769-L16ER/B LOGIX5316ER...

... show more



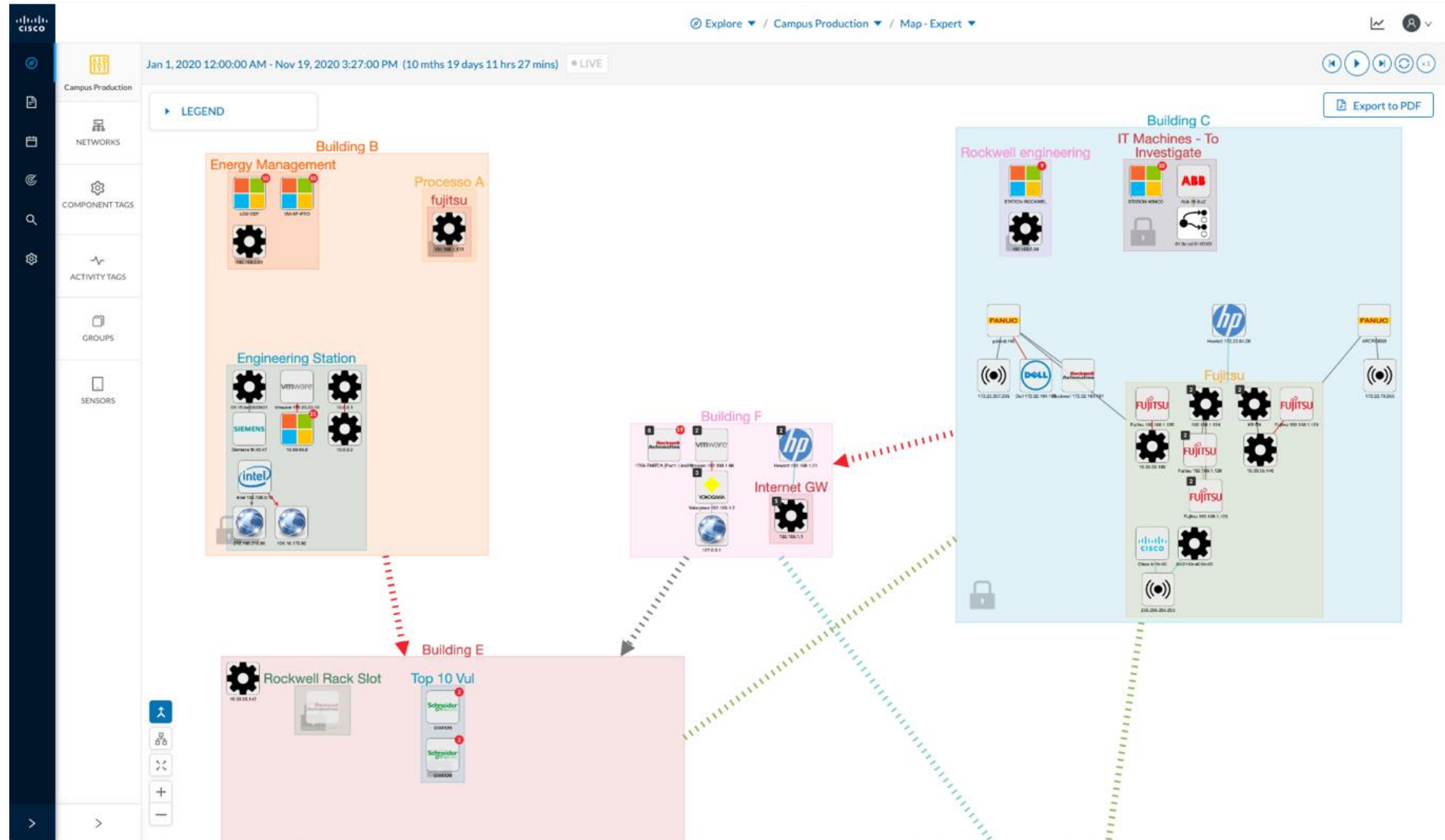
8 Components

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

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

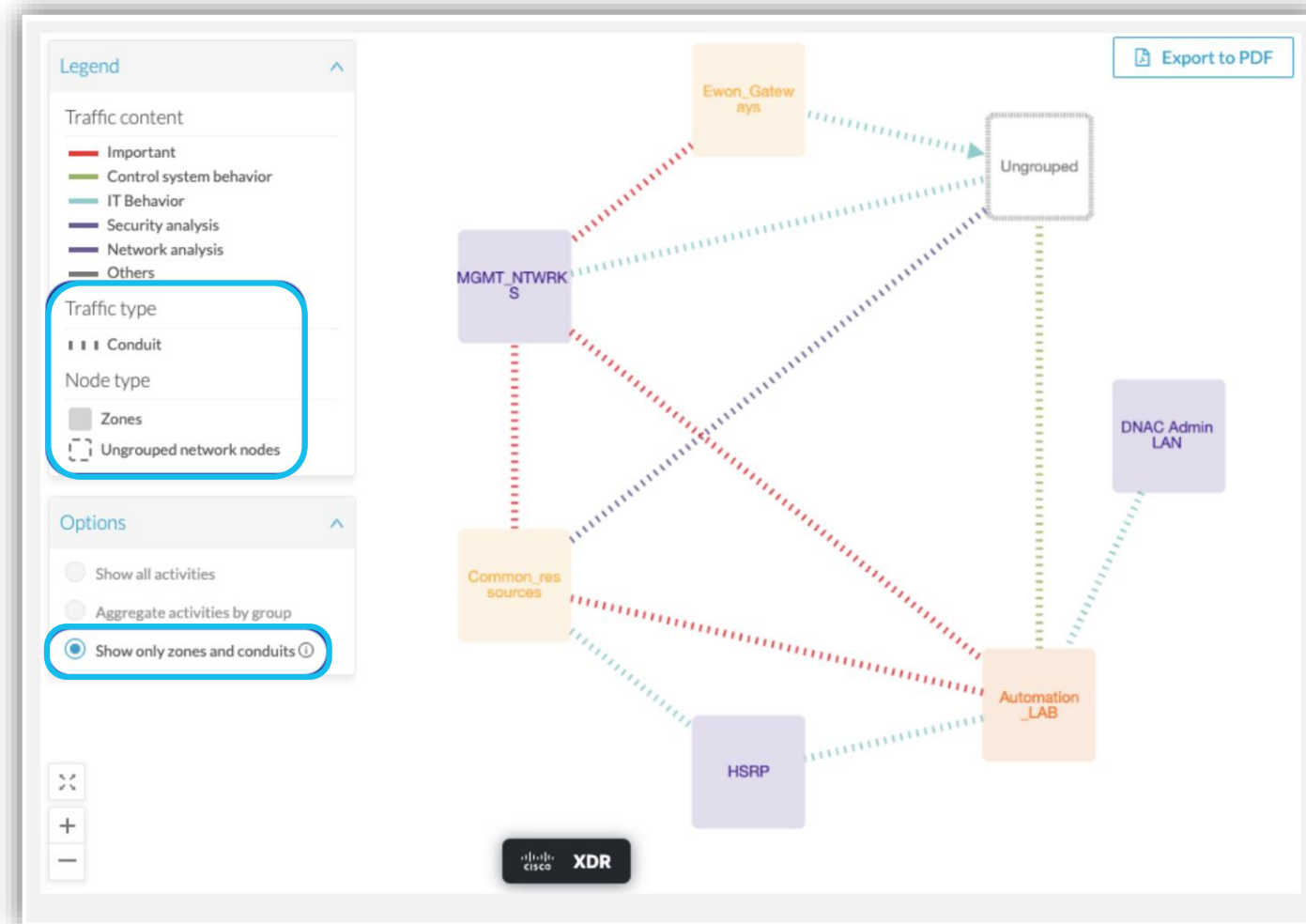
Step 2. “Make it your own”

Group assets to define zones and conduits

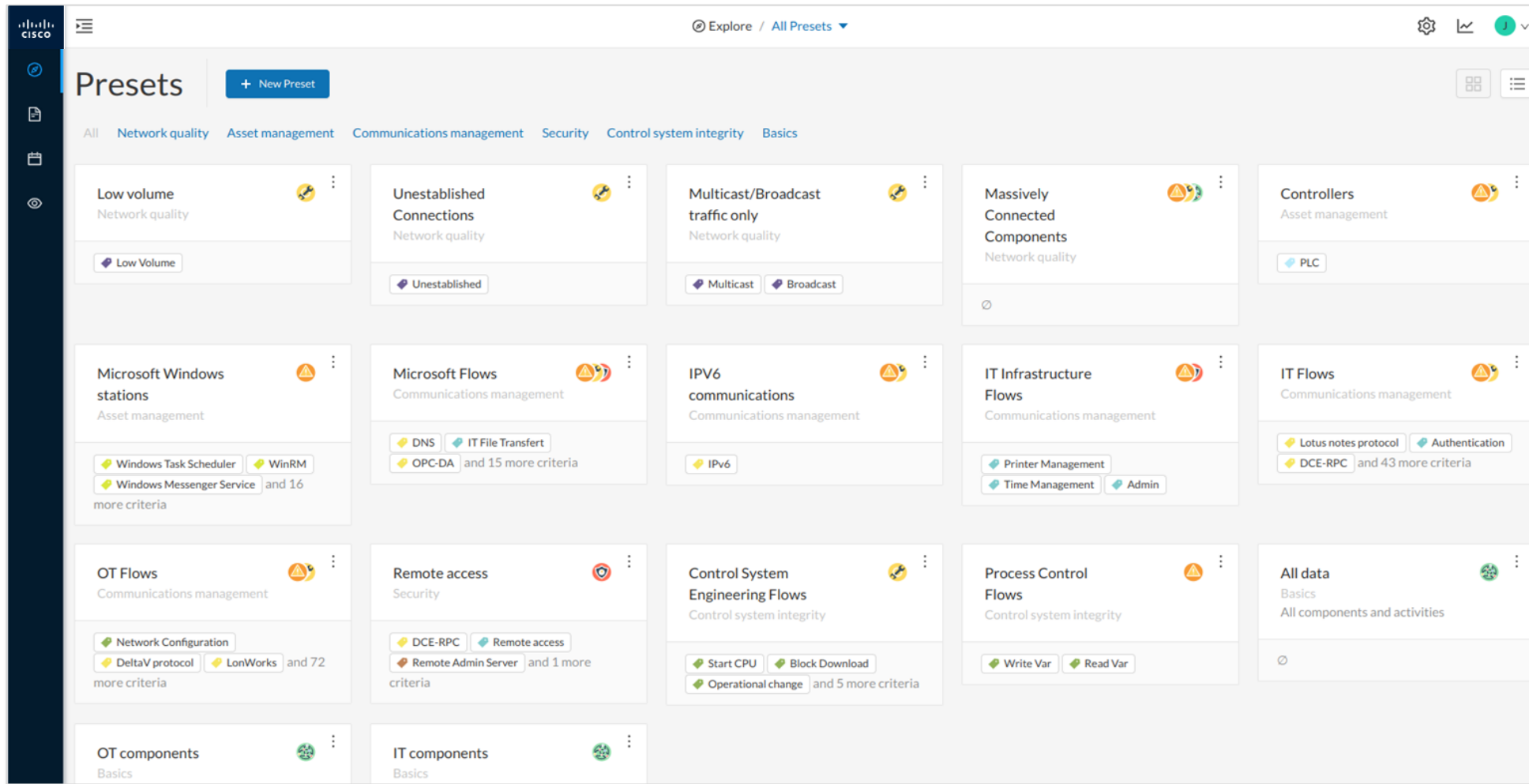


“Zones and Conduits” visualization

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



Easily dive into your data with preset views



Step 3. “Fix your Network”

Investigate problematic assets and communications

COMPONENT TAGS

☐ Components without tags

☐ Device - Level 0-1

- ☐ IO Module (3)
- ☐ Wireless IO Module (2)

☐ Device - Level 2

- ☐ Citect Alarm Server
- ☐ Citect IO Server
- ☐ Citect Report Server
- ☐ Citect Trend Server
- ☐ Engineering Station (3)
- ☐ Master
- ☐ PLC (9)
- ☐ SCADA Station (3)
- ☐ Slave
- ☐ Train

☐ Device - Level 3-4

- ☐ Admin Server (1)
- ☐ DNS Server (2)
- ☐ Database Server
- ☐ Email Server
- ☐ File Transfer Server
- ☐ HTTP Client
- ☐ Historian
- ☐ Host Config Server (3)
- ☐ Key Management Server
- ☐ License Management Server
- ☐ Log Server

☐ Network analysis

- ☐ Port Scan
- ☐ Port Scan Target
- ☐ Public IP (19)

☐ Software

- ☐ Active Directory
- ☐ CodeSys
- ☐ DFS
- ☐ Lotus notes
- ☐ Microsoft Exchange
- ☐ NSIS
- ☐ NetLogon
- ☐ PI Osisoft
- ☐ WINS
- ☐ WMI
- ☐ WinRM
- ☐ Windows (10)
- ☐ Windows Audio
- ☐ Windows CSP
- ☐ Windows Connection Manager
- ☐ Windows DTCping
- ☐ Windows File Protection
- ☐ Windows Messenger Service
- ☐ Windows Network DDE
- ☐ Windows Plug and Play
- ☐ Windows SCM
- ☐ Windows SecondaryLogon
- ☐ Windows Task Scheduler
- ☐ Windows WebClient
- ☐ Windows Workstation

ACTIVITY TAGS

☐ Activities without tags

☐ Control system behavior

- ☐ Block Download
- ☐ Control action (1)
- ☐ Controller Info
- ☐ Controller Name
- ☐ Data Push
- ☐ Device Init (1)
- ☐ Diagnostics
- ☐ Emergency Brake
- ☐ Firmware Download
- ☐ Firmware Update
- ☐ Force Variable
- ☐ Heartbeat
- ☐ Hot Reboot
- ☐ Insert Program
- ☐ Installed Modules
- ☐ Memory Formatting
- ☐ Network Configuration
- ☐ Operational change
- ☐ PLC Clock
- ☐ PLC Reservation
- ☐ Password Change
- ☐ Program Download (4)
- ☐ Program Upload (2)
- ☐ Programming CPU

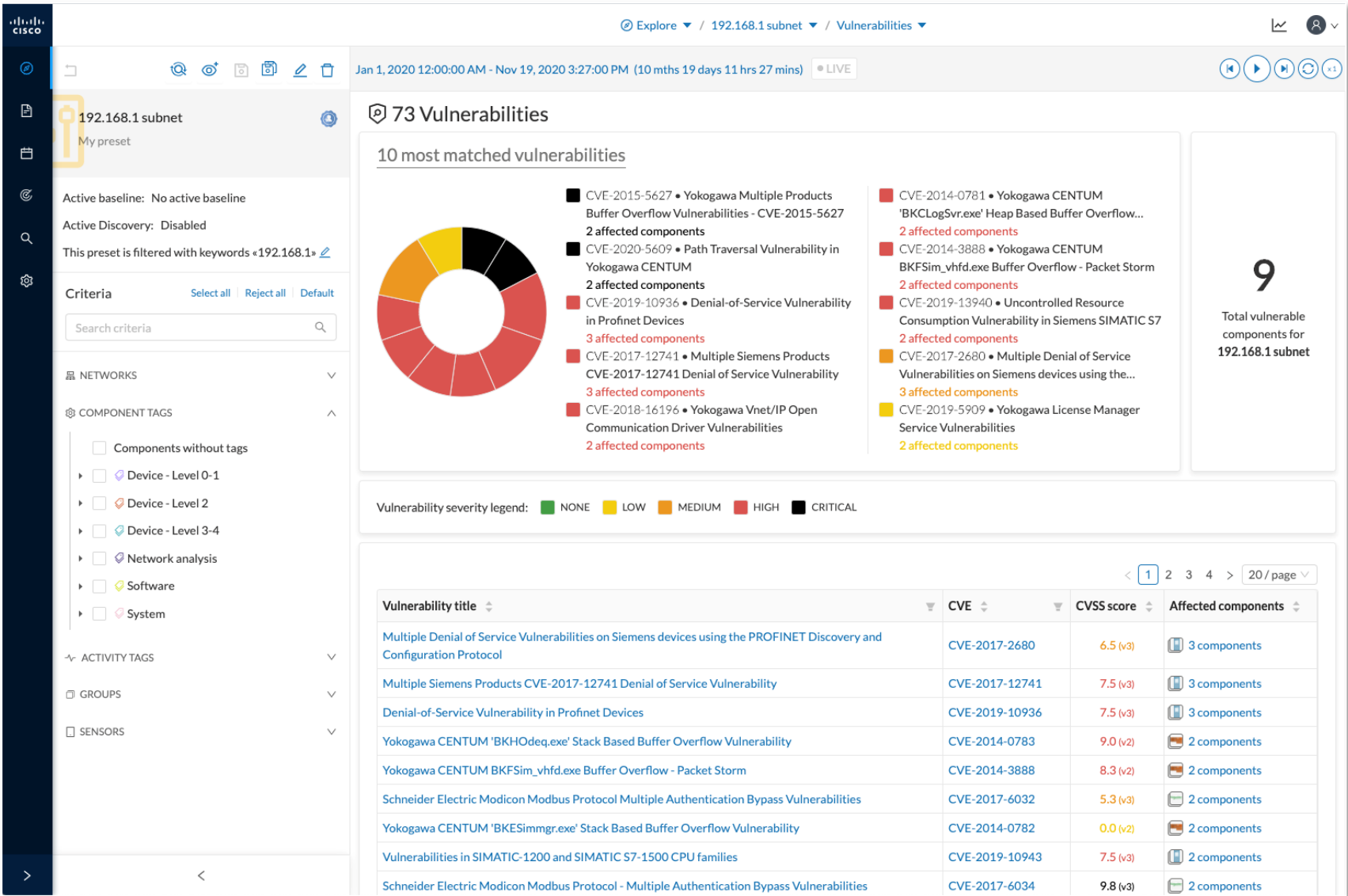
☐ IT behavior

- ☐ Active Directory Replication
- ☐ Admin (1)
- ☐ Antivirus
- ☐ Authentication (1)
- ☐ Database
- ☐ Email
- ☐ Host Config (11)
- ☐ IT File Sync
- ☐ IT File Transfer
- ☐ Key management
- ☐ License Management
- ☐ Log
- ☐ Net Management (3)
- ☐ Net Routing
- ☐ Ping (10)
- ☐ Power Management
- ☐ Printer Management
- ☐ Procedure Call
- ☐ Proxy
- ☐ Remote access (1)
- ☐ Streaming
- ☐ Time Management (9)
- ☐ VPN
- ☐ Web (3)
- ☐ Windows DFS Replication
- ☐ Windows Discovery

☐ Network analysis

- ☐ Authentication Error
- ☐ Broadcast (81)

Identify vulnerabilities to assess risks



Drive vulnerability remediation

Device



SIMATIC 300(1)
[Manheim] Folding P... very low
IP: 192.168.0.1
MAC: 00:0e:8c:84:5b:a6

First activity
Aug 2, 2019 7:32:37 AM

Last activity
Jan 19, 2022 2:00:01 AM

Tags

Read Var, Controller

Activity tags

Network Configuration, Read Var, Ping, Broadcast, Low Volume, Multicast, ARP, Profinet, Profinet DCP, S7 (hide)

6 Activities

20 Events

16 Vulnerabilities

Credential

Variable

Basics

Risk score

Security

Activity

Automation

Vulnerabilities

Credentials

Vulnerabilities

16

☐ Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability
CVE-2017-12741
Several industrial products are affected by a vulnerability that could allow remote attackers to conduct a Denial-of-Service (DoS) attack.
Solution
Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.
Published on November 23, 2017
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0)
Links
[Siemens Security Advisory](#)

☐ SIMATIC S7-300 and S7-400 CPUs Denial of Service and Information Disclosure Vulnerabilities
CVE-2016-9158
Successful exploitation of these vulnerabilities could lead to a denial-of-service condition or result in credential disclosure.
Solution
Siemens provides firmware version V3.X.14 for S7-300 CPUs that resolves CVE-2016-9158.
Published on December 16, 2016
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0)
Links
[www.siemens.com](#)
[ics-cert.us-cert.gov](#)
[www.securityfocus.com](#)

☒ Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and

7.8
score CVSS
Access Vector: Network
Access Complexity: Low
Authentication: None Required
Confidentiality impact: None
Integrity impact: None
Availability impact: Complete
Acknowledge?
Explain why OK

7.8
score CVSS
Access Vector: Network
Access Complexity: Low
Authentication: None Required
Confidentiality impact: None
Integrity impact: None
Availability impact: Complete
Acknowledge?
Explain why OK

Quickly identify “Riskiest” devices

Create presets based on risk thresholds and convert to baselines

Sort and filter risks in your lists of devices

Site Data

My preset

Description:

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

Active baseline: No active baseline

Active Discovery: Disabled

Criteria

Select all Reject all Default

Search criteria

RISK SCORE

Min

55

Max

100

+ Add X Cancel

NETWORKS

DEVICE TAGS X2

ACTIVITY TAGS

GROUPS

SENSORS

Last 1 year (May 24, 2020 4:51:22 PM — May 24, 2021 4:51:22 PM) Refresh

50 Devices (filtered) New data

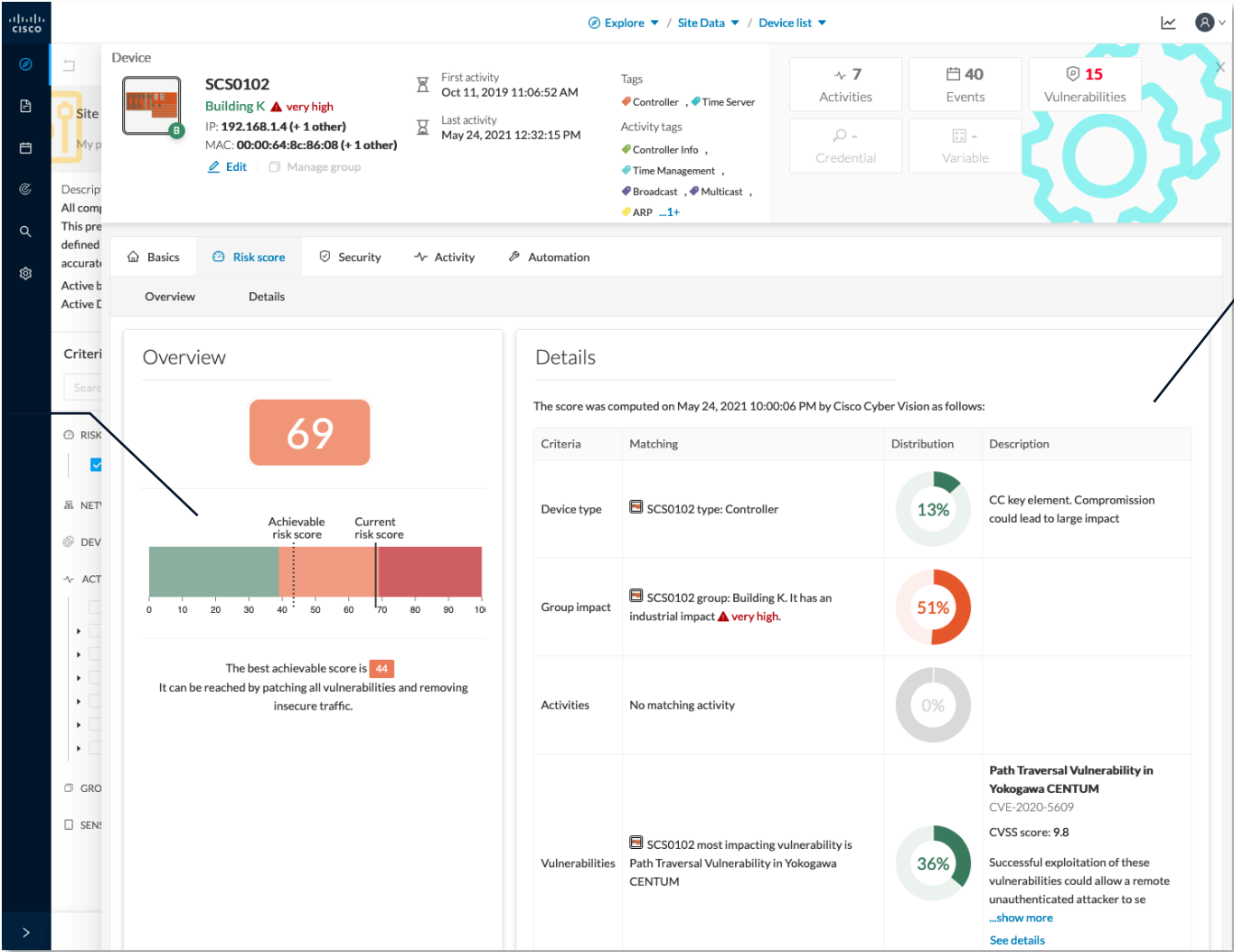
Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags
SCS0102	Building K	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:32:15 PM	192.168.1.5 (+ 1 other)	00:00:64:8c:86:34 (+ 1 other)	69	Controller , Time Server
Fisher 10.5.0.22	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:32:15 PM	10.5.0.22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

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKIOT-2073

Reducing a device risk score

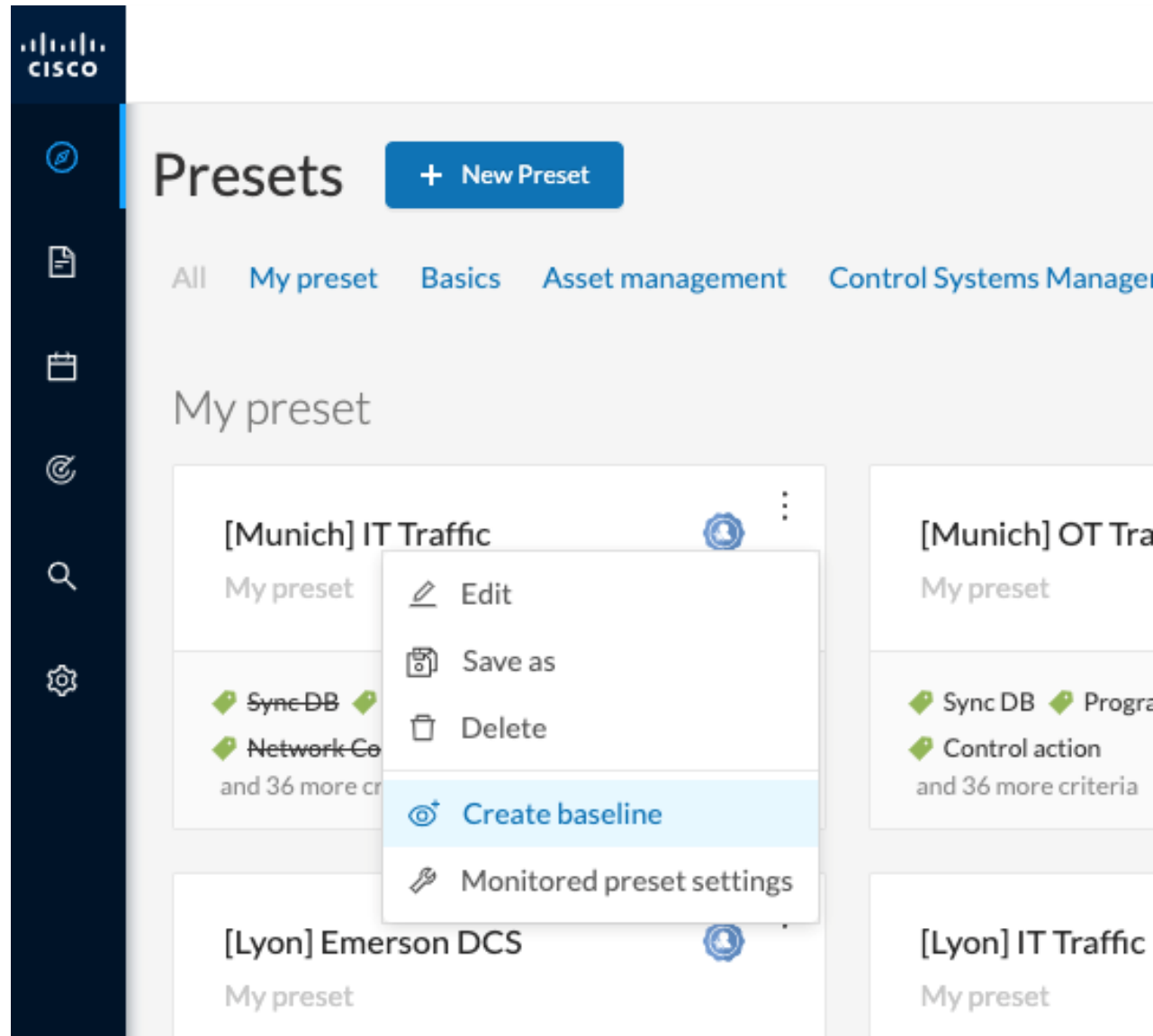
Understand where you are, and where you could be



Understanding what impacts the score

Step 4: Secure your Operations”

Identify changes to environment using baselines



Baselines highlight abnormal behaviors

Utilities

see on [Explore](#)

Utilities Baseline

7 new components

6 new activities

2 changed components

1 changed activity

Created with data seen between:
Jul 14, 2021 2:57:06 PM - Jul 15, 2021 2:57:06 PM

Last check: Jan 19, 2022 11:24:48 PM

Description: Utilities Baseline

Active criteria

GROUPS

Broadcast-Components

Packet-replay

Utilities Demo

City Substation

Process Bus Network

Station Bus Network

Control Center

Enterprise Network

Devices without groups

SENSORS

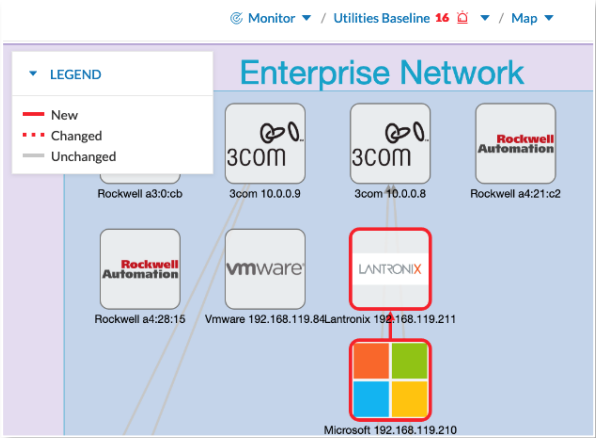
SENSORVM-INT17283

37 Components

7 new

2 changed

Status	Component	Group	First activity
NEW	104.26.11.240	-	Jul 15, 2021 2:58:12 PM
NEW	Lantronix 192.168.119.211	Enterprise Network	Jul 15, 2021 2:58:12 PM
NEW	173.36.224.109	-	Jul 15, 2021 2:58:12 PM
NEW	171.70.168.183	-	Jul 15, 2021 2:58:12 PM
NEW	Microsoft 192.168.119.210	Enterprise Network	Jul 15, 2021 2:58:12 PM
CHANGED	Beckwith 10.0.0.57	Station Bus Network	Jul 14, 2021 8:29:50 PM
CHANGED	Cisco 192.168.119.166	Enterprise Network	Jul 14, 2021 8:30:56 PM
-	Rockwell a3:0:cb	Enterprise Network	Jul 14, 2021 8:30:56 PM
-	Vmware 192.168.119.50	Enterprise Network	Jul 14, 2021 8:30:56 PM



Changed Activity

Rockwell Automation

Rockwell Automation

Rockwell 192.168.249.50

Paint Line 2 ▲ high

IP: 192.168.249.50

MAC: f4:54:33:91:cb:ee

Rockwell 192.168.249.40

Paint Line 2 ▲ high

IP: 192.168.249.40

MAC: f4:54:33:9b:77:76

First activity

Apr 24, 2020 11:04:08 AM

Last activity

Apr 27, 2020 10:26:37 AM

Tags:

Read Var

Write Var

EthernetIP

Variables: (1 difference)

SYNC_NEW1 read Rockwell 192.168.249.50

SYNC write Rockwell 192.168.249.50

SYNC read Rockwell 192.168.249.50

Acknowledge differences

Report differences

Remove and keep warning

Individual acknowledgment

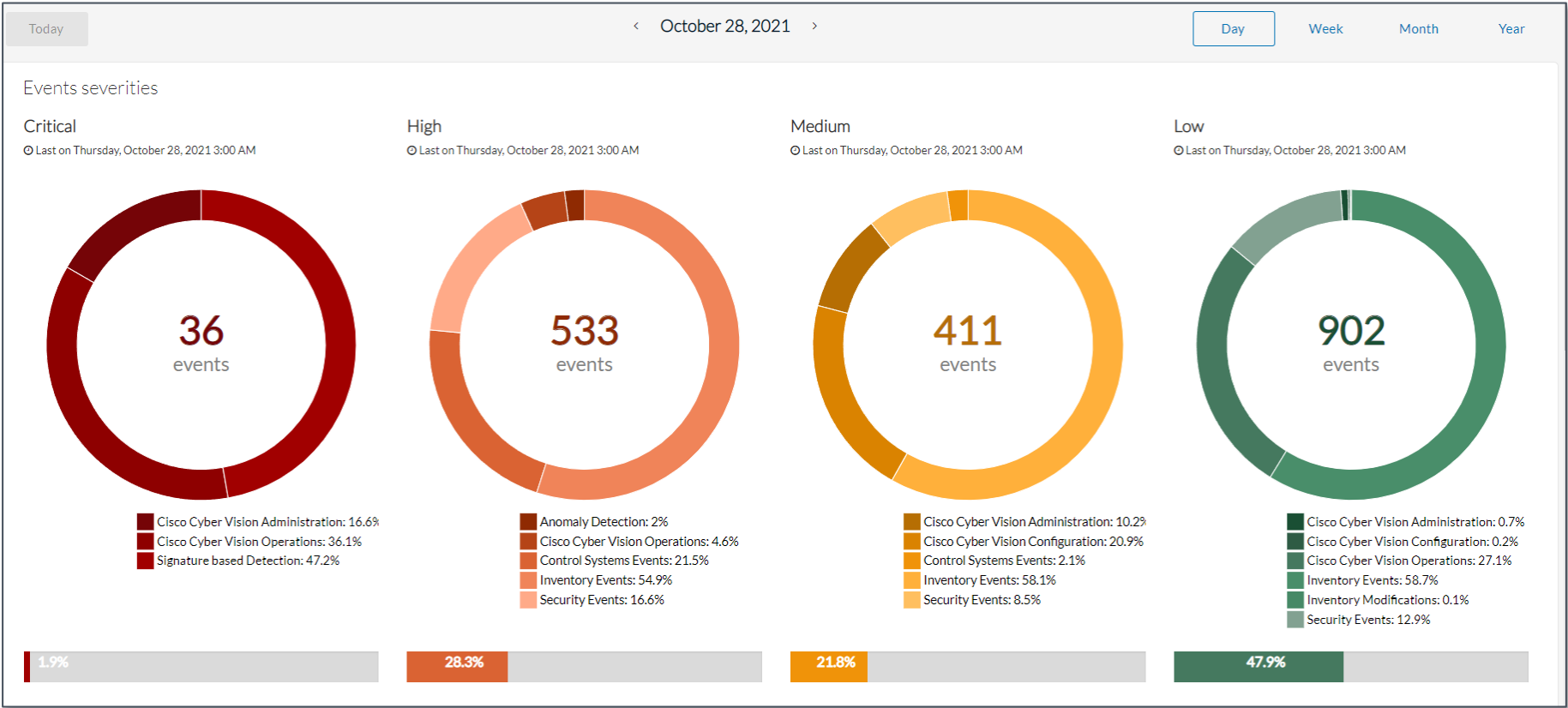
2 Flows

- Event

396127 Packets

- Volume

Events: The high-level overview



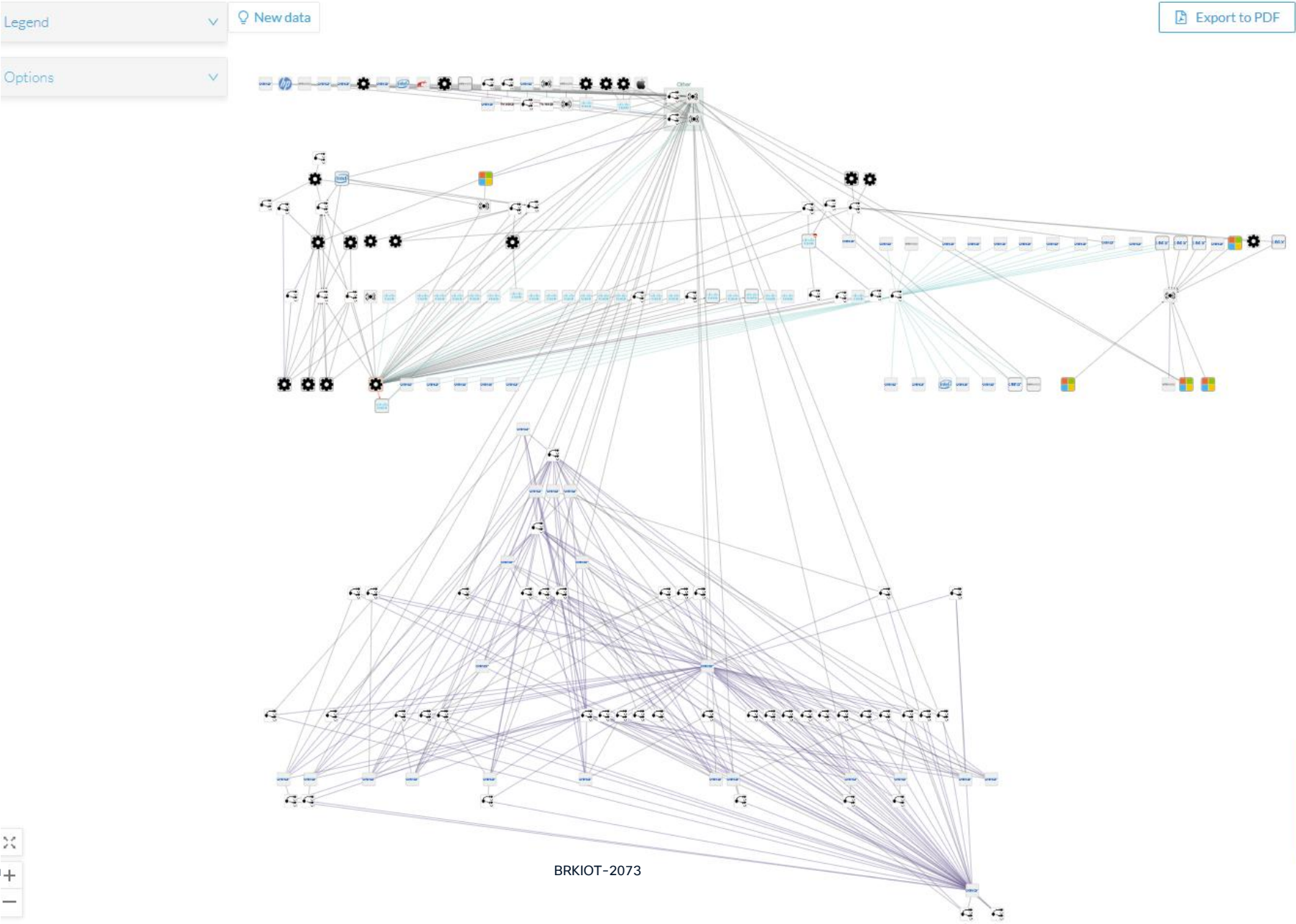
Best Practices & Lessons Learnt



“the flat network chaos”

when every device was in an inclusive /16 network

Communication Map Spaghetti!



Best Practices and Recommendations

- **Short Term:** Disable Chatty Protocols (Activity Tags)
- **Medium Term:** Use the Cyber Vision communication map as a **blueprint for segmentation**.

- ☒ IPv6 (13)
- ☐ ISL
- ☐ Iteris
- ☐ Iteris Veolcity data
- ☐ ITS DSRC
- ☐ KiTraffic
- ☐ LACP
- ☐ Link Layer Discovery Protocol
- ☒ LLMNR (24)



“the black box acquisition”

Offline PCAP Analysis and Asset Inventory

PCAP Upload

Here you can manage PCAP uploads.

6 PCAP files

[Upload a new file](#)

12 Devices and 8 other components [New data](#)

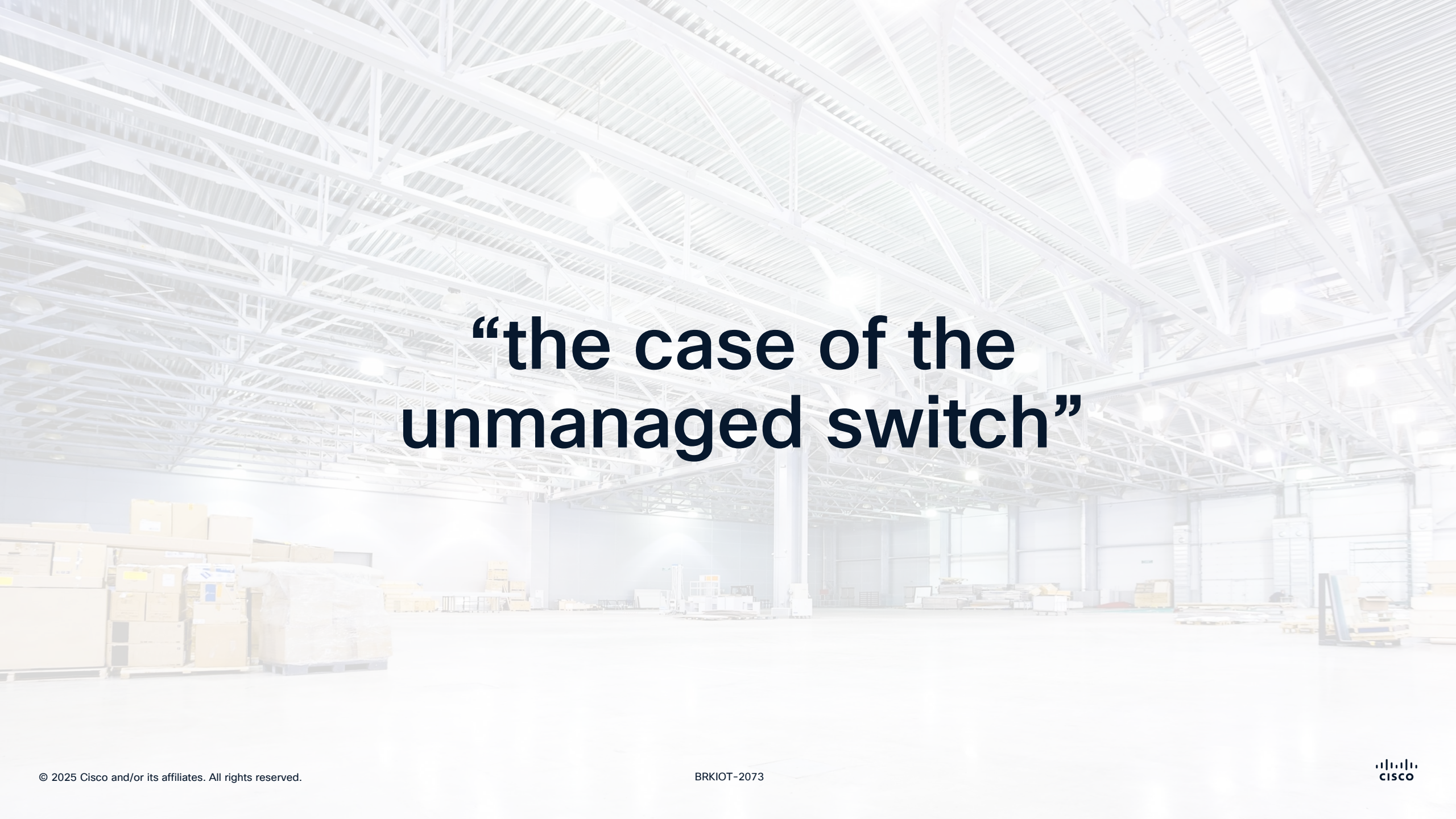
☐	Device	First activity	Last activity	IP	MAC	Risk score	External Communication
☐	 scada-VLIPC	Sep 28, 2025 8:40:28 AM	Sep 28, 2025 1:57:14 PM	192.168.0.103 (+ 1 other)	00:a0:45:b1:5d:c9	55	Yes
☐	 192.168.0.2	Sep 28, 2025 8:40:22 AM	Sep 28, 2025 1:54:43 PM	192.168.0.2	00:0c:29:1b:f9:cf (+ 1 other)	50	No
☐	 192.168.0.3	Sep 28, 2025 8:44:21 AM	Sep 28, 2025 1:48:04 PM	192.168.0.3	00:a0:45:b2:c4:cd	45	No
☐	 x-PC	Sep 28, 2025 9:02:33 AM	Sep 28, 2025 3:02:33 PM	172.27.224.70 (+ 1 other)	00:0c:29:9d:9e:9e (+ 1 other)	45	No

Best Practices and Recommendations

- **Short Term:** Contain and Remediate the external communicating device.
- **Medium Term:** Before any integration, deploy a firewall and segment the old network internally.
- **Long Term:** Make Assessment a mandatory step in M&A due diligence process for all future acquisitions.

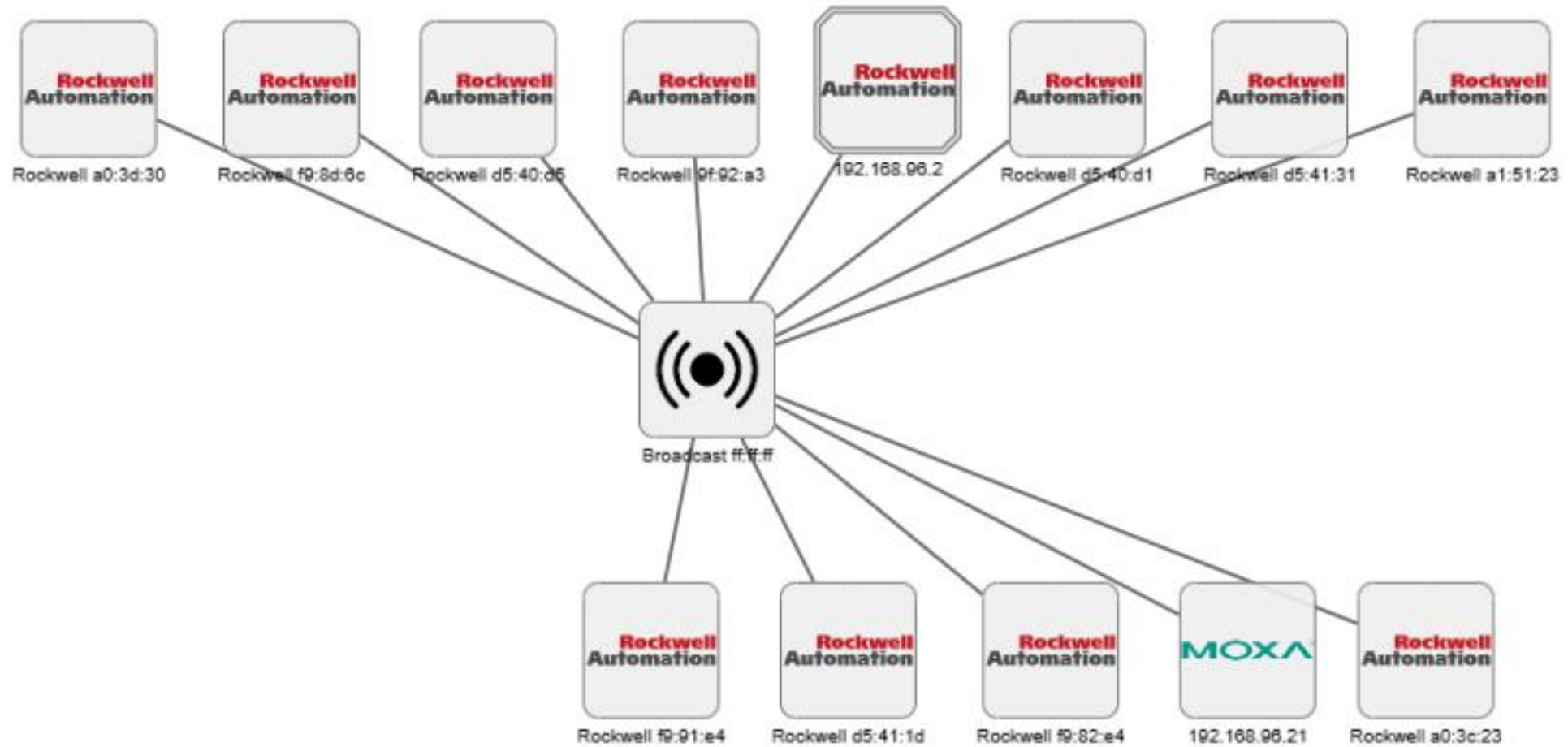
2 External Communications

Direction	Internal IP	External IP	Server Port	Hostname	Protocol	Received by device
Outbound	192.168.0.103	8.8.4.4	53		DNS	70 B
Outbound	192.168.0.103	8.8.8.8	53		DNS	70 B



“the case of the unmanaged switch”

Limited Visibility on the Network Communications



Active Discovery Activation

- **Active Discovery:** . Closed-loop between passive and active discovery enables precise and non-disruptive requests.

Active Discovery policies

From this page you can manage the Active Discovery policies.

2 Discovery policies

+ Create policy

Name

EthIP

Unicast configuration

☒ EtherNet/IP

☒ Backplane discovery

EthIP

Broadcast configuration

Beckhoff - Disabled	EtherNet/IP - Enabled	ICMPv6 - Disabled
Profinet - Disabled	SiemensS7 - Disabled	BACnet - Disabled
HiDiscovery - Disabled	ABB NetConfig - Disabled	Codesys - Disabled
SiemensLogo - Disabled	SSDP - Disabled	



Sensor (EtherNet/IP)
Unicast Active Discovery

Backplane scan

BRKIOT-2073

Active Discovery Properties Discovery

Flow



192.168.20.192

IP: 192.168.20.192

Port: 45896

MAC: 52:54:00:61:05:d7



1756-EN2T/D

IP: 192.168.20.22

Port: 44818

MAC: 5c:88:16:ef:d1:2e

 First activity
Feb 9, 2022 3:00:57 PM

 Last activity
Feb 9, 2022 3:00:57 PM

Tags

Active Discovery,

Low Volume, EthernetIP

Basics

PropertiesContent StatisticsTags

Properties

enip-command: ListIdentity

enip-event: Equipment

enip-name: 1756-EN2T/D

enip-serial: 0114f91d

enip-status-ra-major: RUN

enip-vendor: Rockwell Automation/Allen-Bradley

ethertype: IPv4

enip-devicetype: CommunicationsAdapter

enip-location: Endpoint

enip-productcode: 0xa6

enip-status: AtLeastOneIOConnectionInRunMode

enip-status-ra-minor: ???

enip-version: 11.001

protocol: UDP

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKIOT-2073



Active Discovery Backplane Scanning

Properties

enip-cip-class: Connection Manager Object

enip-devicetype: ProgrammableLogicController

enip-location: Port1-Link00

enip-productcode: 0x5c

enip-status: AtLeastOneIOConnectionInRunMode,ReservedBits12-15:0x3

enip-status-ra-minor: RUN

enip-version: 32.051

protocol: TCP

enip-cip-request: true

enip-event: Equipment

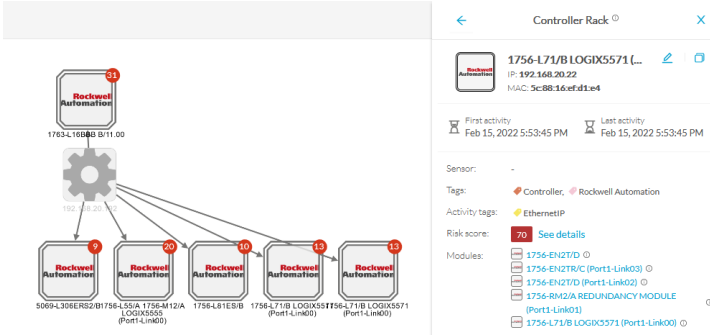
enip-name: 1756-L71/B LOGIX5571

enip-serial: 0115289b

enip-status-ra-major: REM

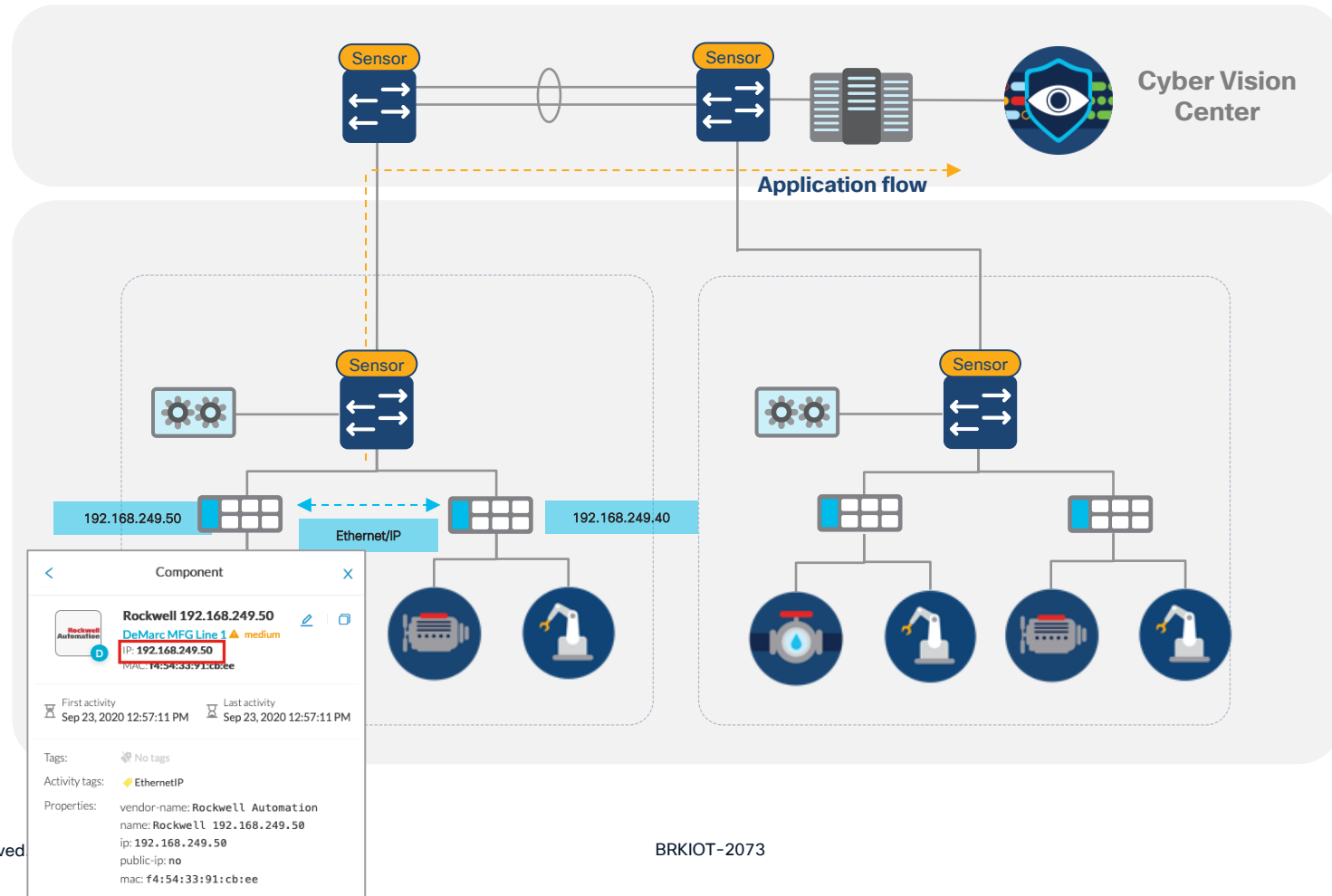
enip-vendor: Rockwell Automation/Allen-Bradley

ethertype: IPv4



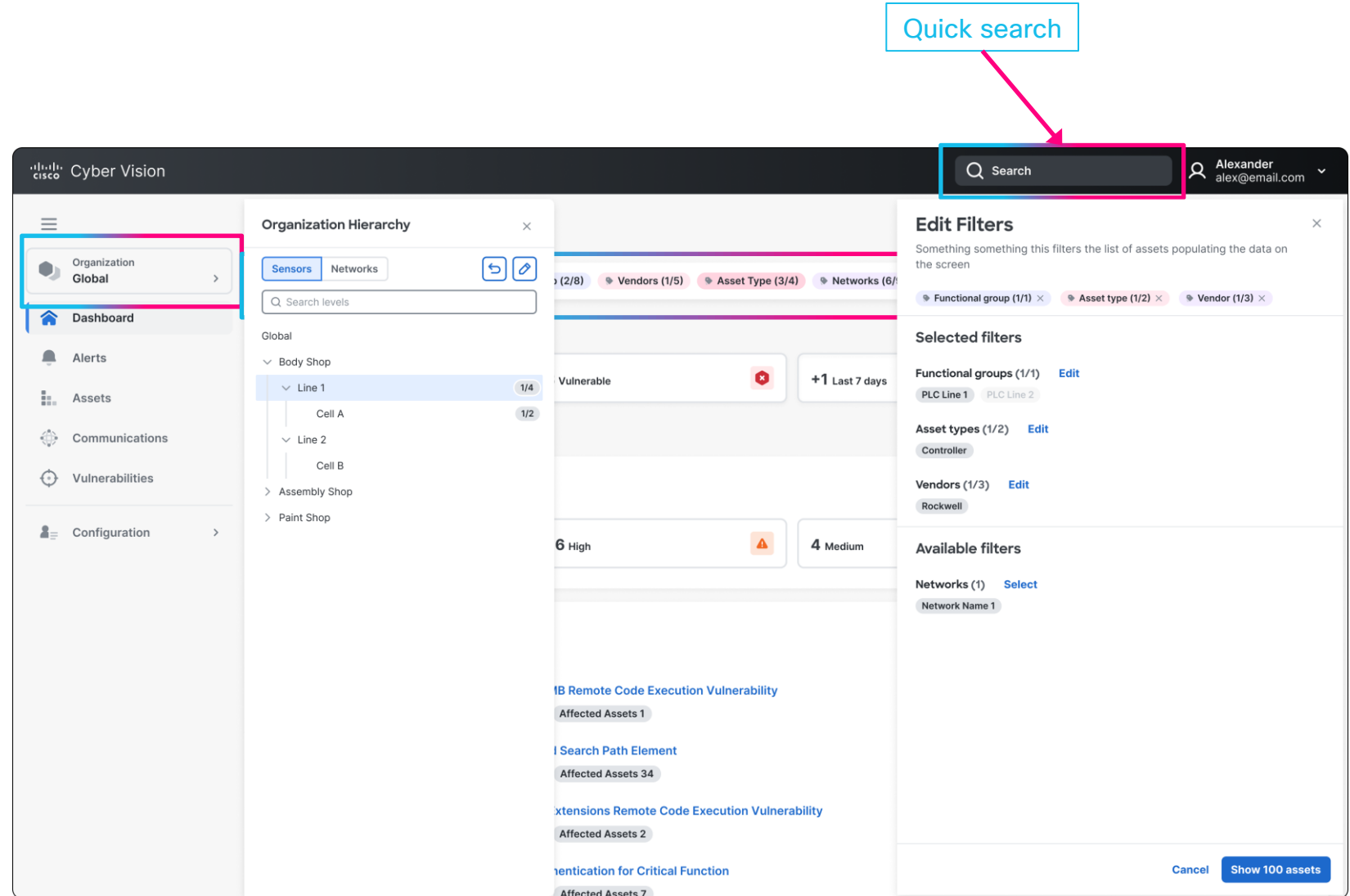
Best Practices for Active Discovery

- **Subnet Access:** Sensor must have an IP Address in the target subnet/VLAN and directly accessible from sensor
- **Unicast Discovery:** Target subnet/VLAN must be directly accessible or reachable via a gateway/route.

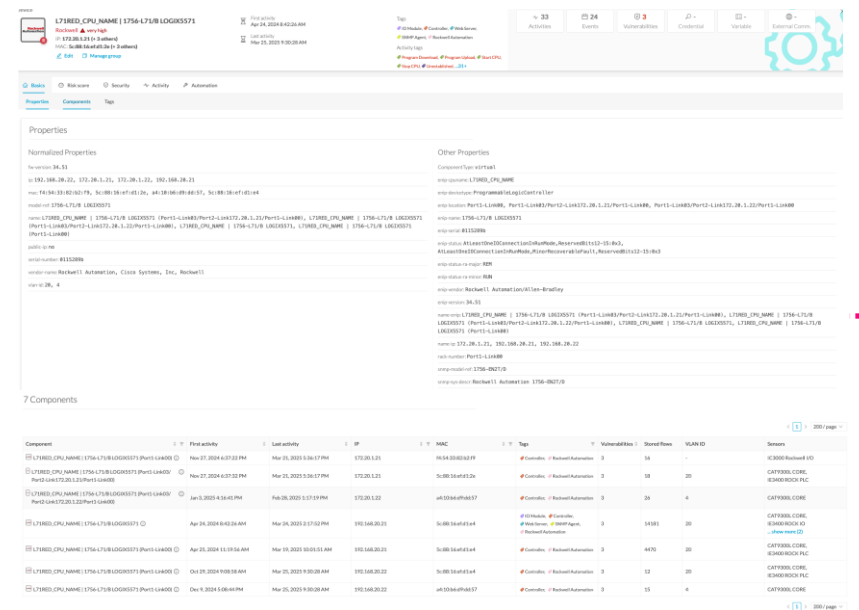


Cyber Vision Updates: Simplified Navigation

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

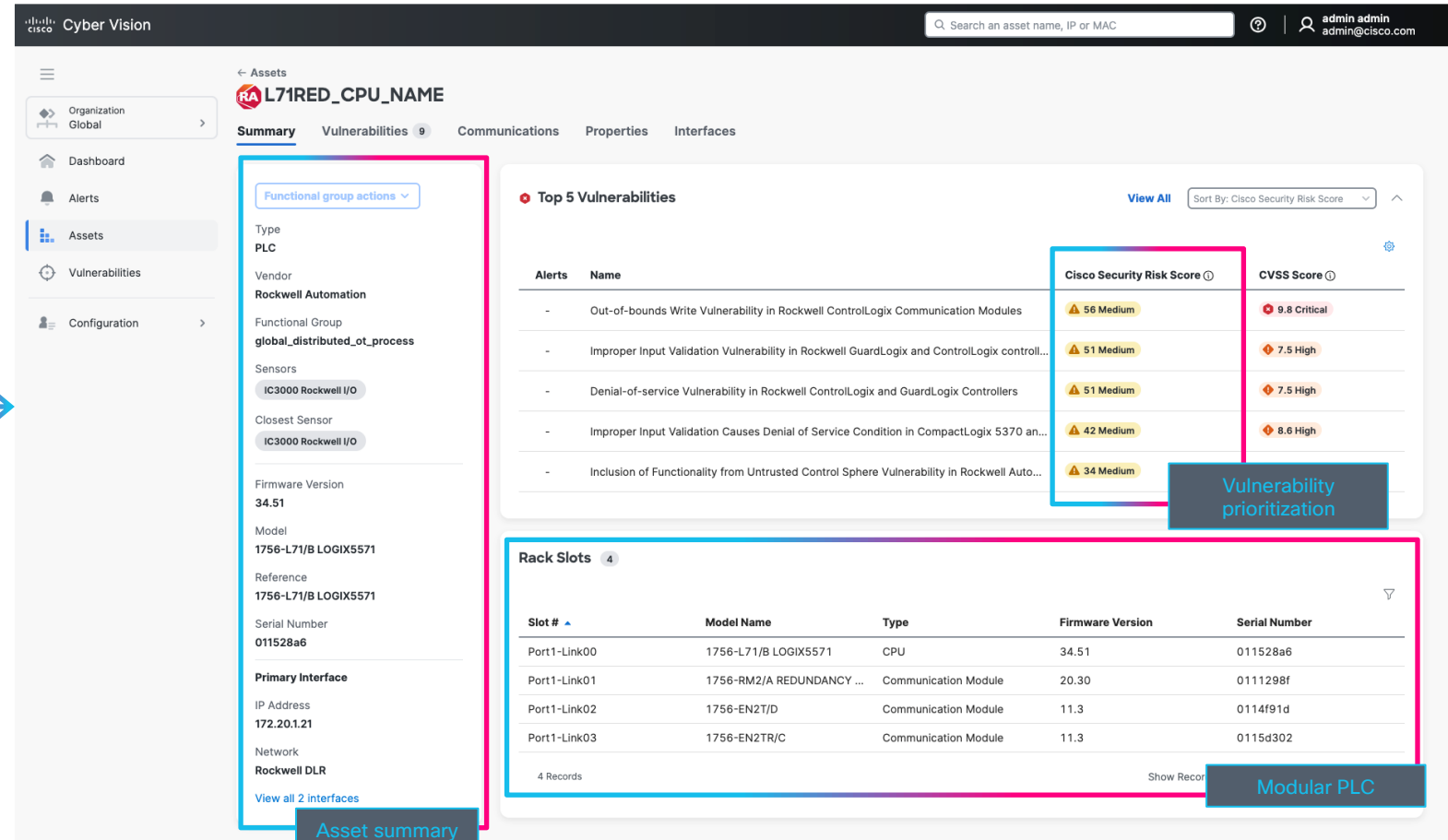


CyberVision Updates: Asset details: Focus on what matters



The old interface shows a complex asset details page for 'L71RED_CPU_NAME (1756-L71/B LOGIX5571)'. It includes a 'Properties' tab with 'Normalized Properties' and 'Other Properties'. A large table at the bottom lists 'Components' with columns for Component, First activity, Last activity, IP, MAC, Tag, Vulnerabilities, and Sensors. The table contains multiple rows of data for different components and their associated activities and vulnerabilities.

Devices can be made off **multiple components** and seen through different routers / firewalls which creates **complexity**



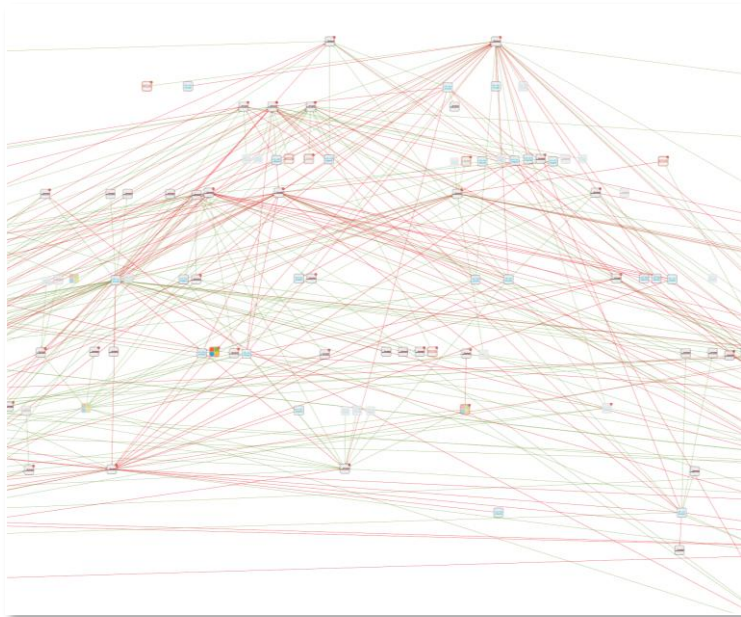
The new interface shows a streamlined asset details page for 'L71RED_CPU_NAME'. It includes a 'Summary' tab with a 'Functional group actions' dropdown. A 'Top 5 Vulnerabilities' table lists vulnerabilities with their names, Cisco Security Risk Score, and CVSS Score. A 'Rack Slots' table lists slots with their model names, types, firmware versions, and serial numbers. The interface is more focused on providing meaningful information and is easier to navigate.

Alerts	Name	Cisco Security Risk Score	CVSS Score
-	Out-of-bounds Write Vulnerability in Rockwell ControlLogix Communication Modules	56 Medium	9.8 Critical
-	Improper Input Validation Vulnerability in Rockwell GuardLogix and ControlLogix controll...	51 Medium	7.5 High
-	Denial-of-service Vulnerability in Rockwell ControlLogix and GuardLogix Controllers	51 Medium	7.5 High
-	Improper Input Validation Causes Denial of Service Condition in CompactLogix 5370 an...	42 Medium	8.6 High
-	Inclusion of Functionality from Untrusted Control Sphere Vulnerability in Rockwell Auto...	34 Medium	

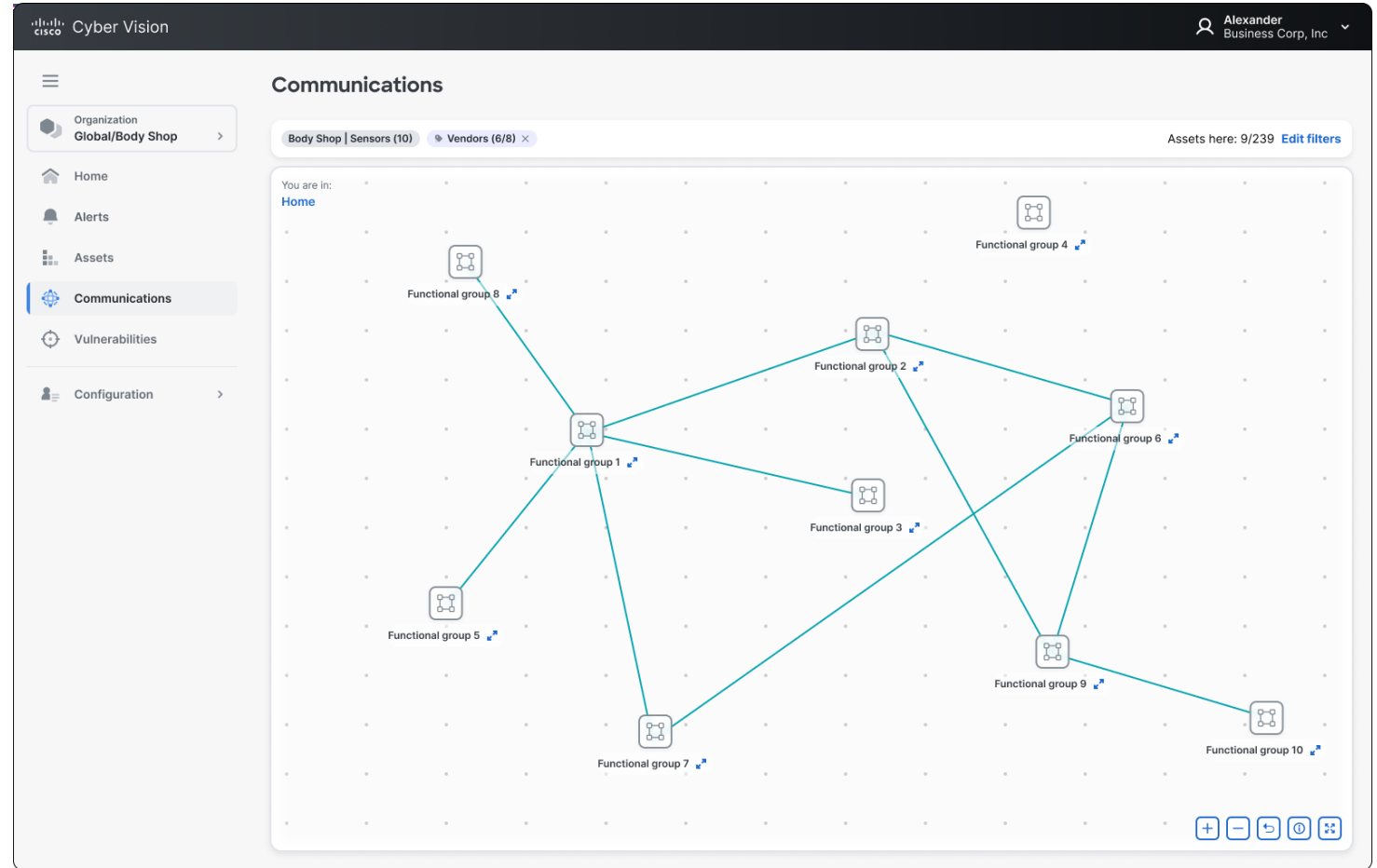
Slot #	Model Name	Type	Firmware Version	Serial Number
Port1-Link00	1756-L71/B LOGIX5571	CPU	34.51	011528a6
Port1-Link01	1756-RM2/A REDUNDANCY ...	Communication Module	20.30	0111298f
Port1-Link02	1756-EN2T/D	Communication Module	11.3	0114f91d
Port1-Link03	1756-EN2TR/C	Communication Module	11.3	0115d302

New UI only surface **meaningful information**

Cyber Vision Updates: AI-driven asset clustering

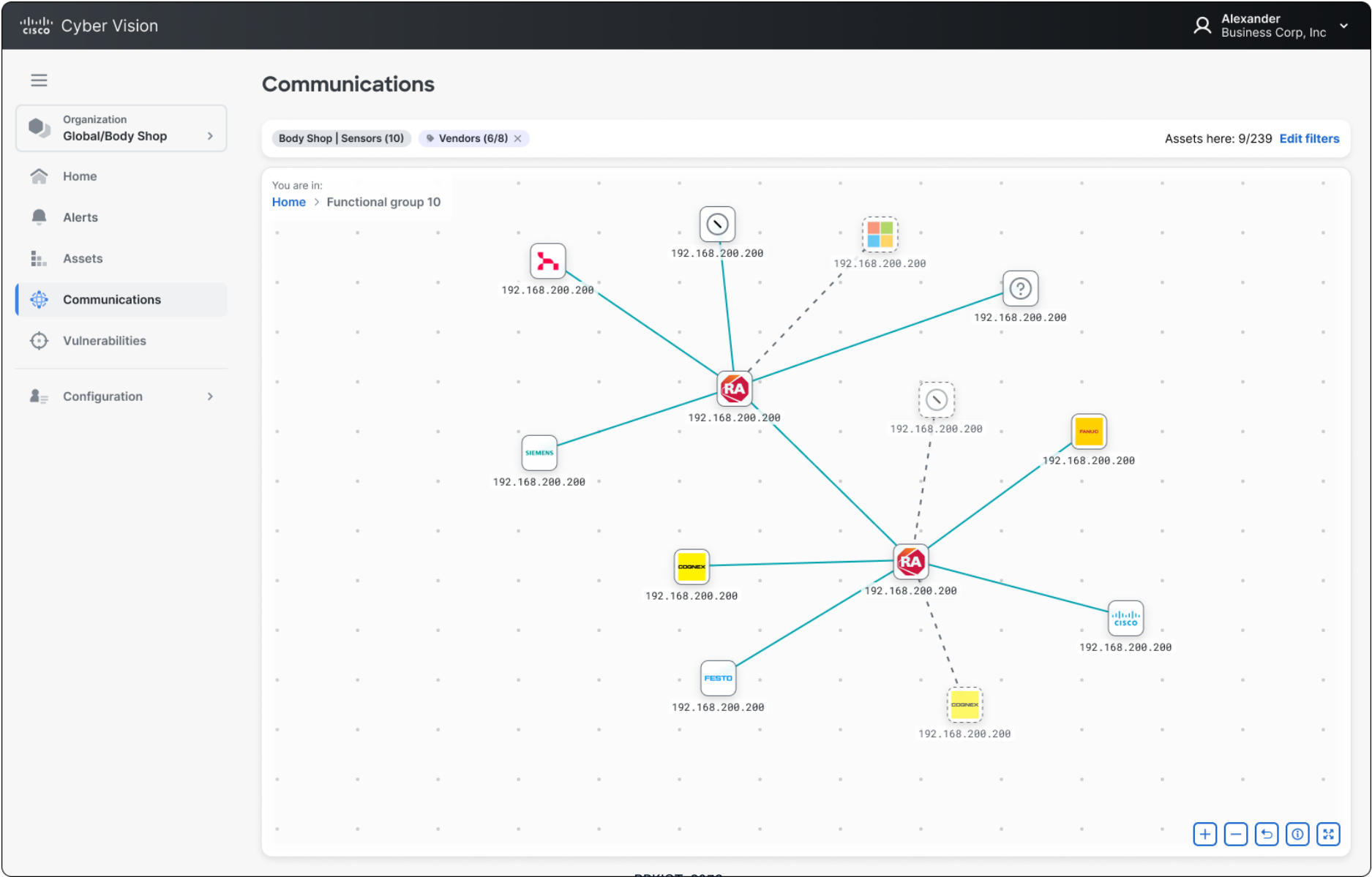


OT asset inventory projects highlight flat, unsegmented networks



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

Cybervision Updates: Internal group communication

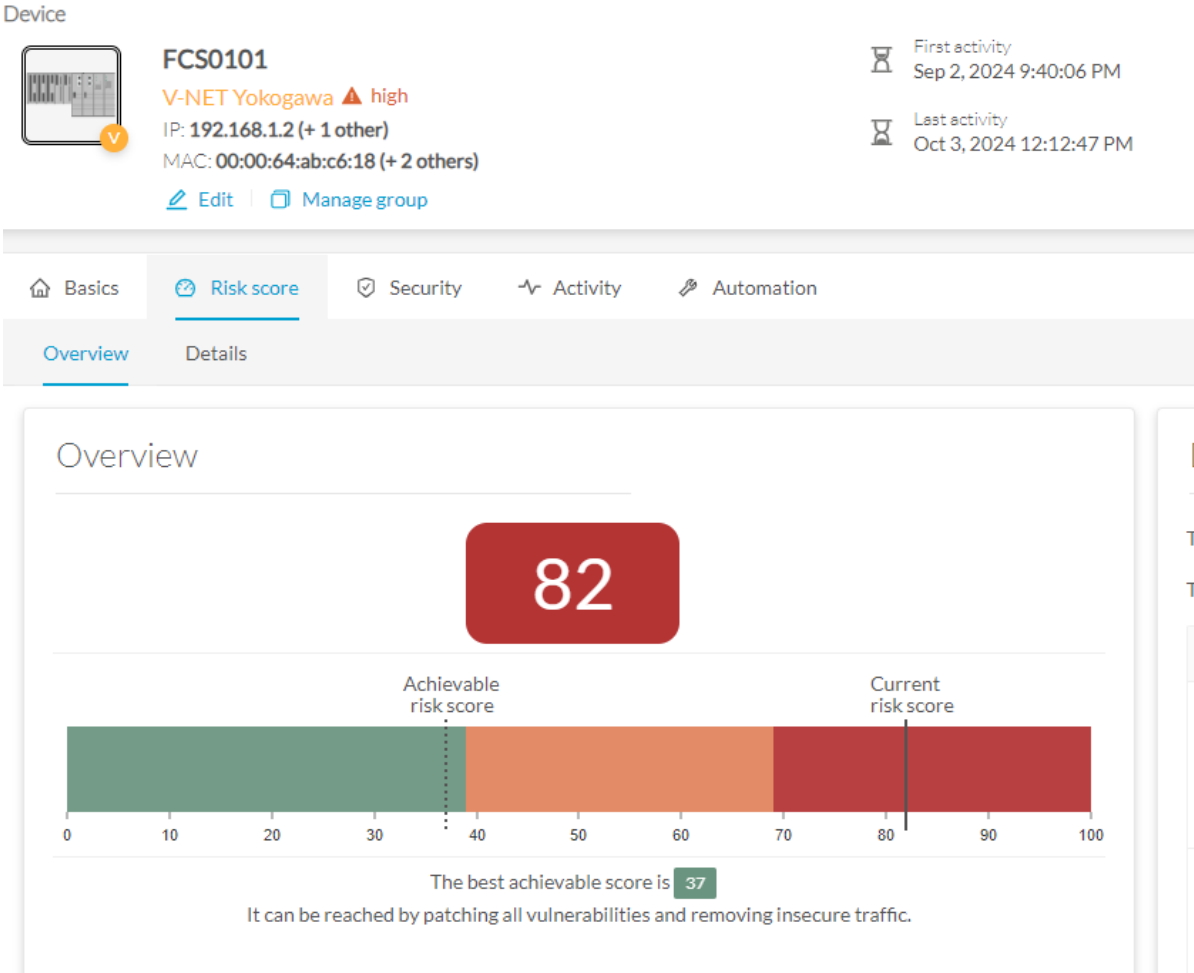




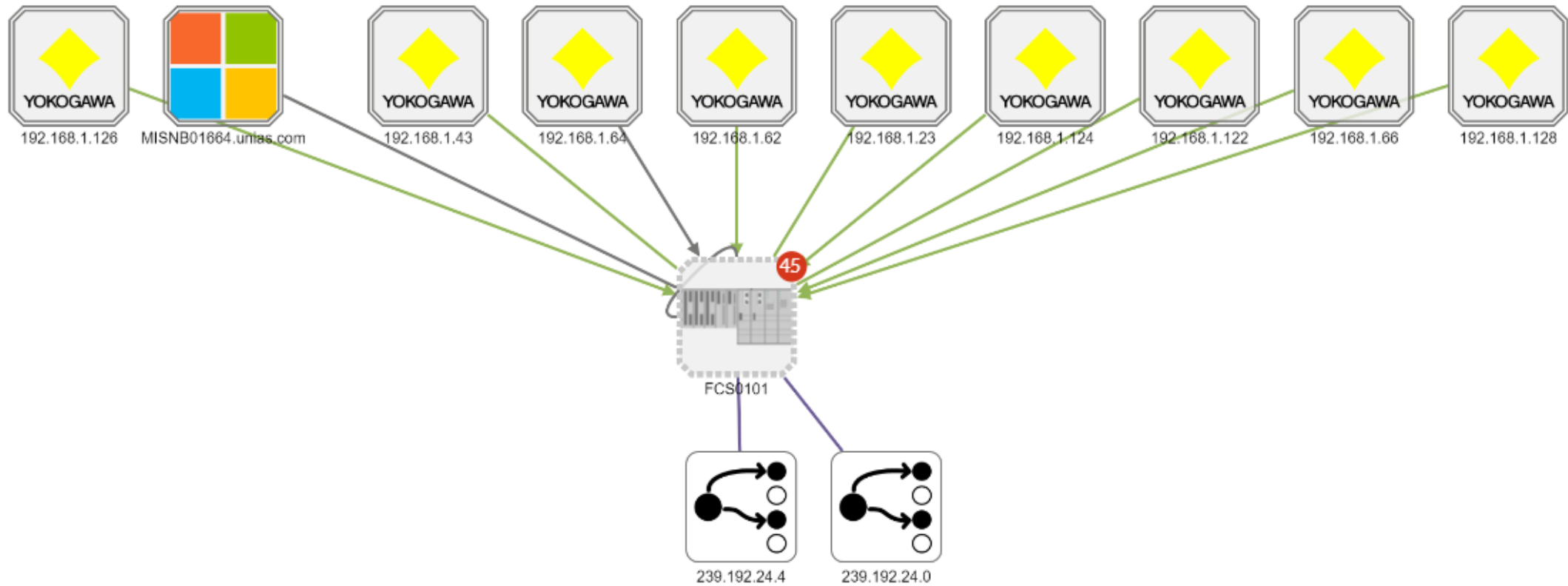
“the un-patchable, Critical PLC”

Vulnerability Findings

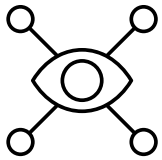
CVE	CVSS score
CVE-2021-44228	10 (v3.1)
CVE-2020-11897	10 (v3)
CVE-2020-11896	10 (v3)
CVE-2022-21194	9.8 (v3.1)
CVE-2022-23402	9.8 (v3.1)
CVE-2020-5608	9.8 (v3)
CVE-2020-5609	9.8 (v3)
CVE-2019-5909	9.8 (v3)



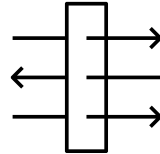
Communication Map



Segmentation Phases



Virtual Segmentation



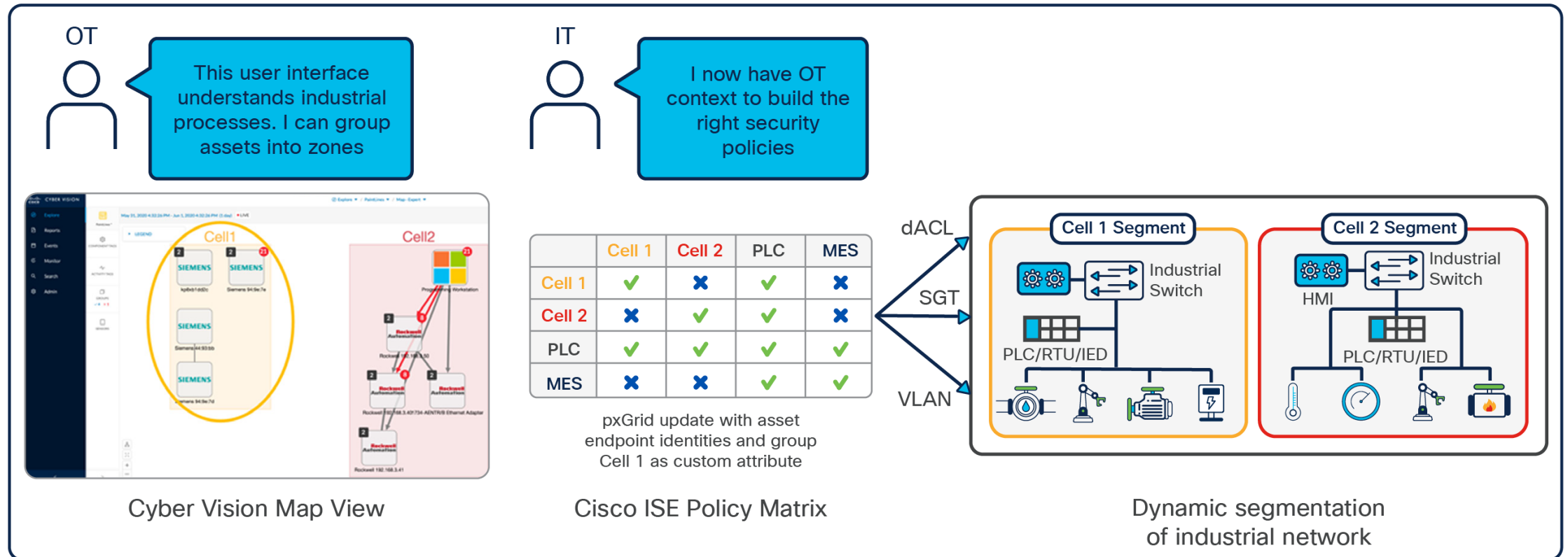
Macro Segmentation

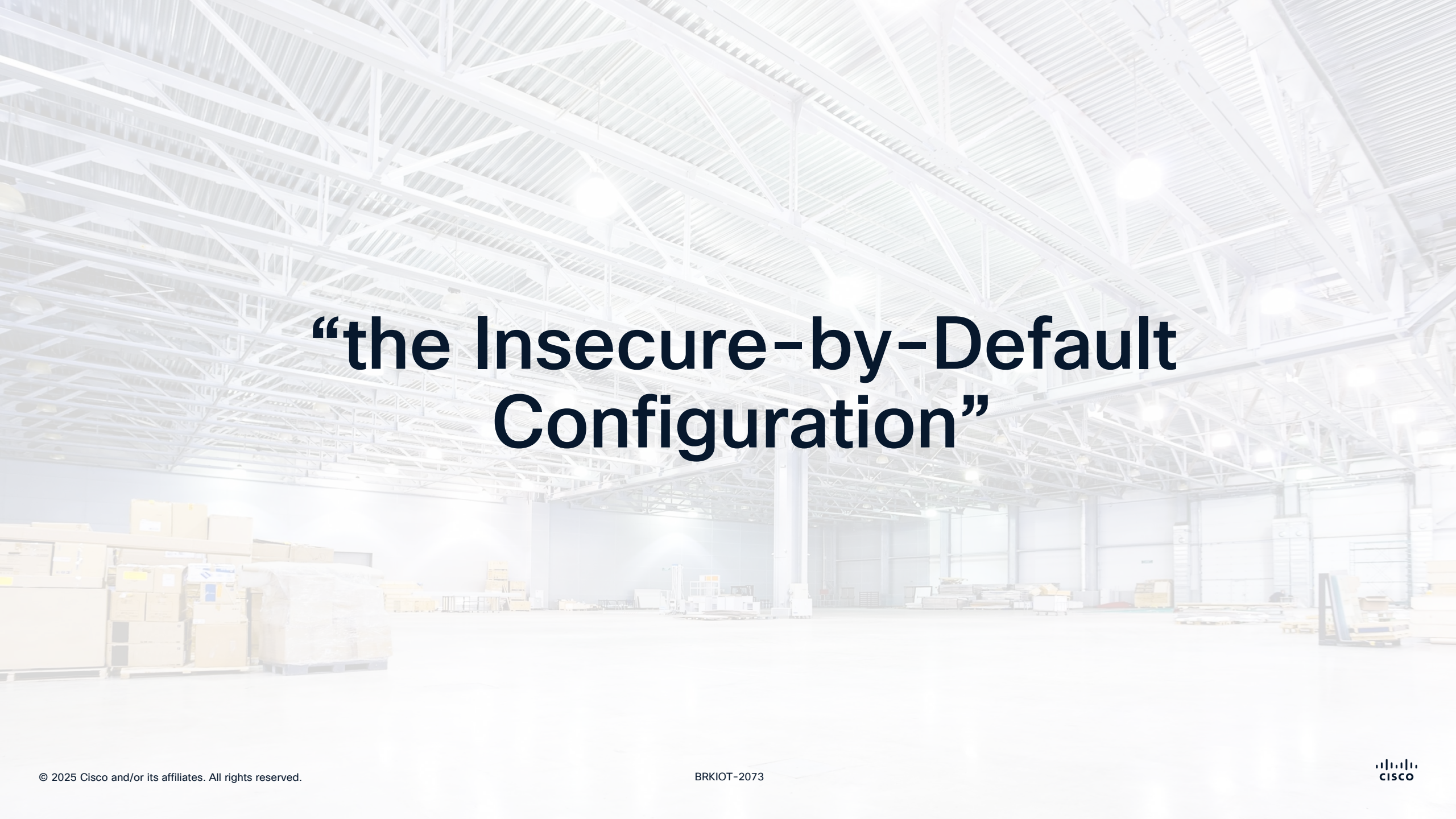


Micro Segmentation

Best Practices and Recommendations

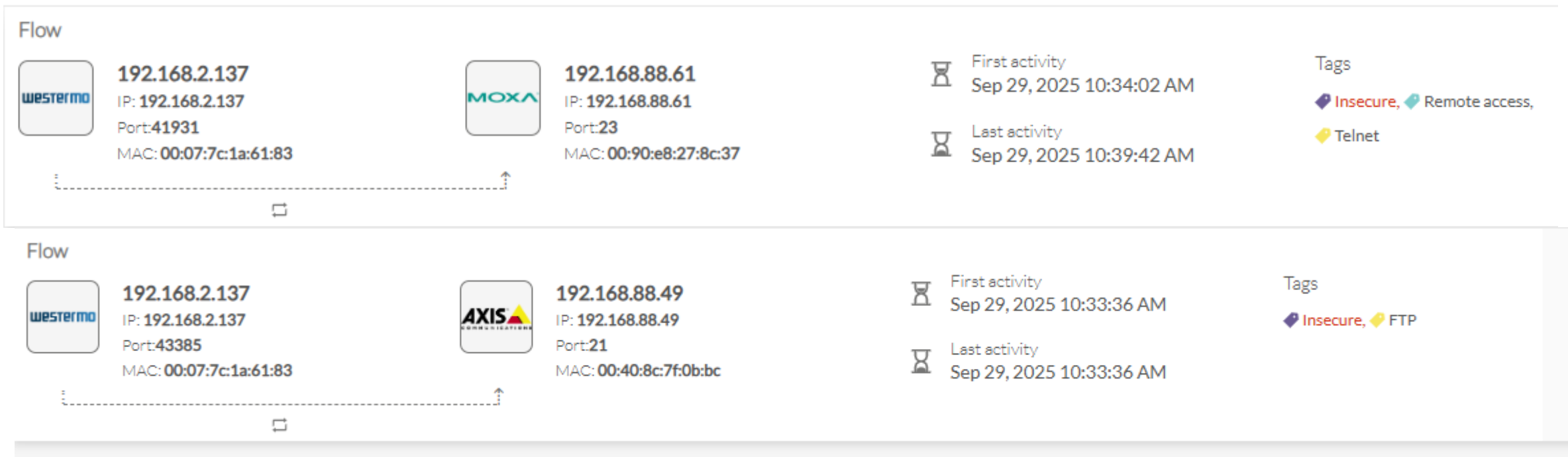
- **Short Term:** Implement virtual patching via switch ACL or Firewall Rules that allows traffic PLC's IP address to its communication peers.
- **Medium Term:** Implement Micro-Segmentation using ISE TrustSec
- **Long Term:** Develop a formal lifecycle management program for OT Assests. Monitor for any violation attempts.





“the Insecure-by-Default Configuration”

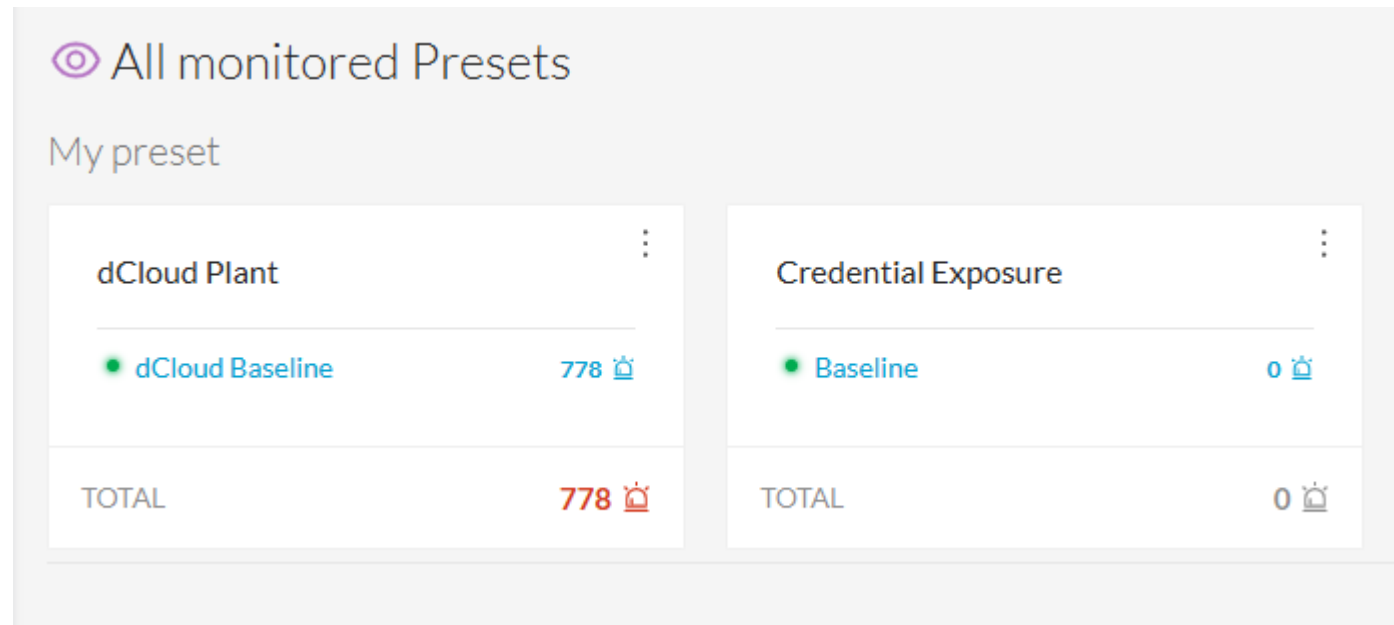
Credential Discovery & Insecure Protocol Analysis



Credential
1

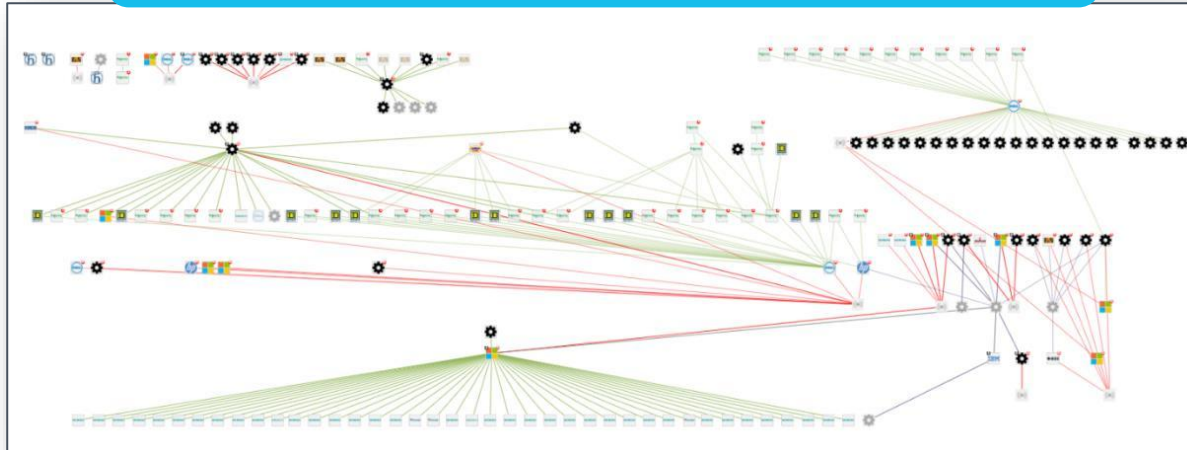
Best Practices for Insecure-by-Default Configurations

- **Immediate:** Identify an alternate, more secure service (ssh instead of telnet, sftp/scp instead of ftp)
- **Mid-Term:** Create and enforce a mandatory security hardening checklist for all devices. Also should include changing default credentials before a device is put into production.
- **Govern & Monitor (Long-Term):** Use Cyber Vision to continuously monitor for the use of insecure protocols and credential leakage. Automate alerts for any occurrence

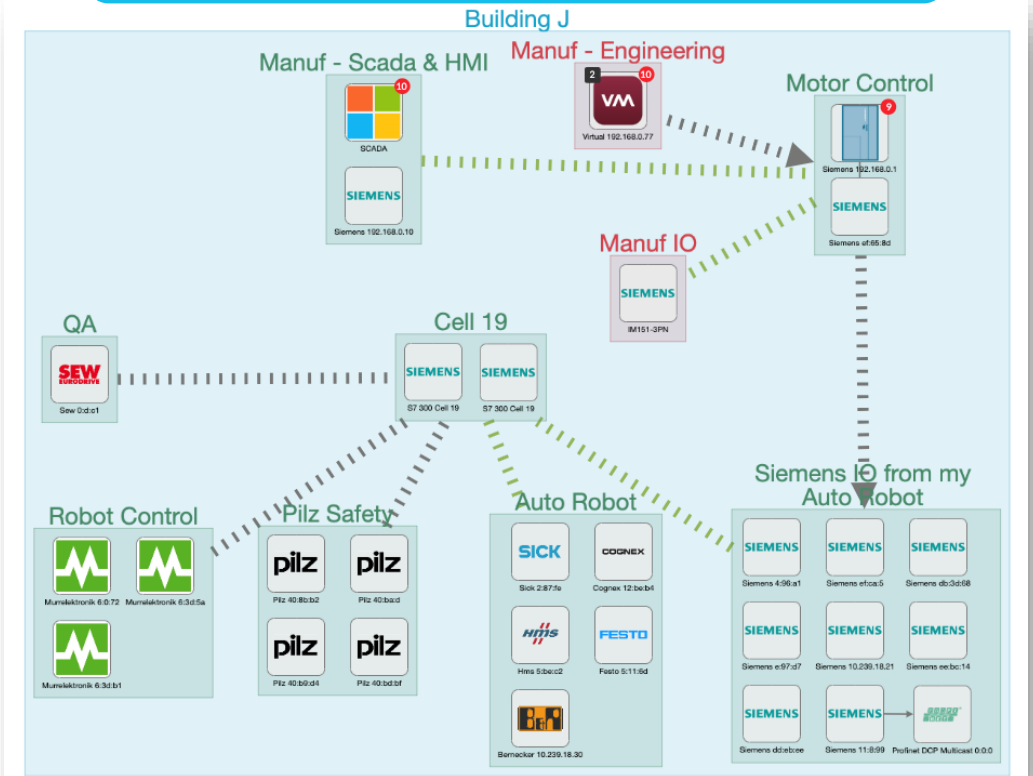


Driving Segmentation with Visibility: Virtual Segmentation

Cyber Vision discovers all connected assets...

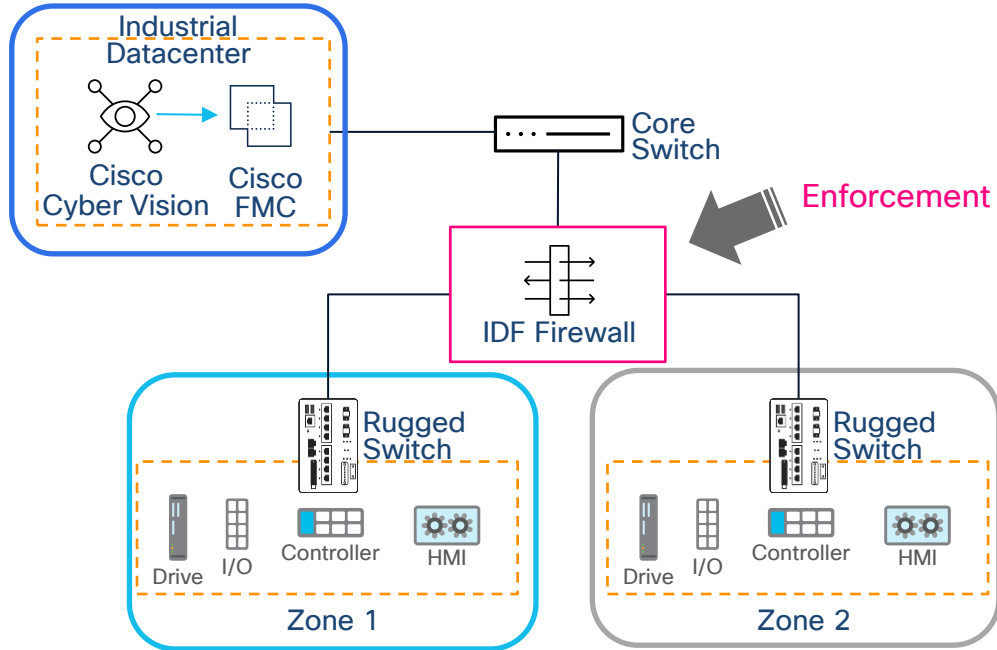


...and groups them into logical zones



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

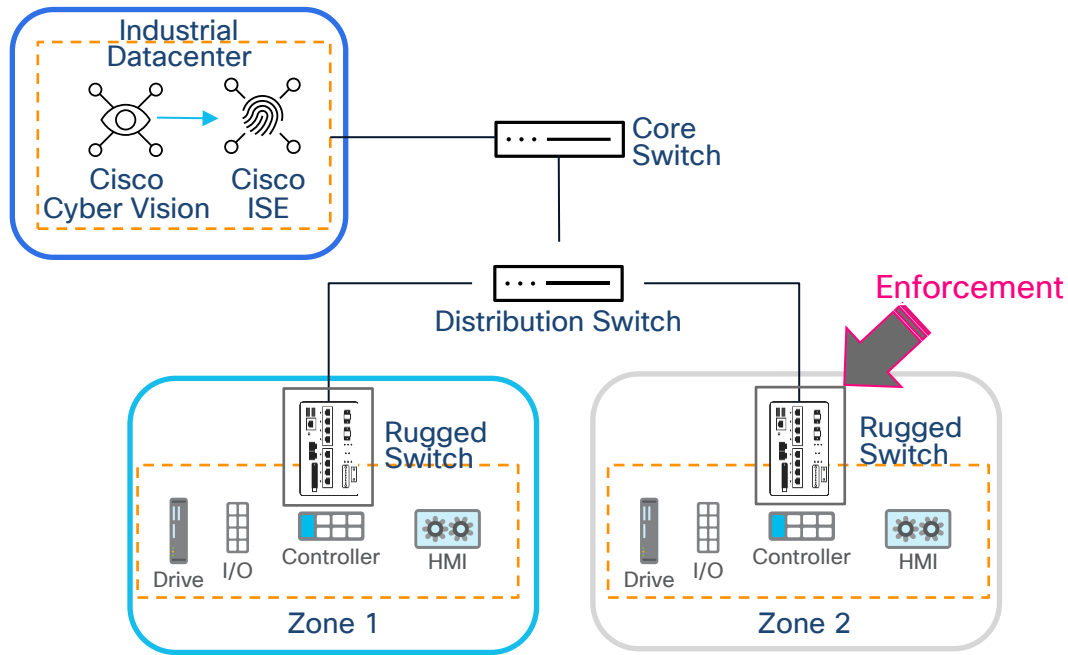
Macro Segmentation Enforced using Firewalls



- 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

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

Trustsec enables micro-segmentation

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

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

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

Endpoint Profile: Austin_Plant_Profiler

Current IP Address: 192.168.119.39

Location: Location → All Locations

Applications

Attributes

Authentication

Threats

Vulnerabilities

General Attributes

Description

Static Assignmentfalse

Endpoint PolicyAustin_Plant_Profiler

Static Group Assignmentfalse

Identity Group AssignmentAustin_Plant_Profiler

Custom Attributes

Attribute NameAttribute Value

x

Attribute Name

Attribute Value

assetGroupRoot > Austin_Plant

assetDeviceTypeController

assetId101

assetIpAddress192.168.119.39

assetMacAddresse4:90:69:9e:ef:7d

assetName192.168.119.39

assetProductId1769-L36ERM/A LOGIX5336ERM

assetProtocolCIP

assetSerialNumber0x604052C7

assetSwRevision28.011

assetVendorRockwell Automation/Allen-Bradley

ip192.168.119.39

Production Matrix

Populated cells: 36

EditAddClearDeployVerify DeployMonitor All - OffImportExportViewShowman

Destination	Plant16/0010	Cell117/0011	Cell218/0012	LinePLC21/0015
Source				
Plant16/0010	Permit IP	Deny IP	Deny IP	Permit IP
Cell117/0011	Deny IP	Permit IP	Deny IP	Permit IP
Cell218/0012	Deny IP	Deny IP	Permit IP	Permit IP
LinePLC21/0015	Permit IP	Permit IP	Permit IP	Permit IP

TrustSec policy to enforce zone segmentation

Enrich endpoint attributes in ISE with rich context from Cyber Vision

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

Enforce segmentation through dynamic assignment of VLAN, dACLs or TrustSec

Cyber Vision and ISE enable dynamic segmentation of industrial networks



**“the unauthorized late-
night program change”**

Deep Packet Inspection

 OT-WRKST07	51191	→	 Cisco 10.207.1.2	102	TCP	Jun 1, 2022 6:07:44 AM	Jun 1, 2022 6:07:57 AM	<div><div>Program Download,</div><div>Block Download,</div><div>Read Var,</div><div>Write Var,</div><div>S7Plus</div></div>	243	90.7 kB
 Cisco 10.207.0.5 2	51191	→	 Siemens 10.207.1.2	102	TCP	Jun 1, 2022 6:07:44 AM	Jun 1, 2022 6:07:57 AM	<div><div>Program Download,</div><div>Block Download,</div><div>Write Var,</div><div>S7Plus</div></div>	122	53.2 kB
 OT-WRKST07	49898	→	 Cisco 10.207.1.2	102	TCP	May 31, 2022 7:00:18 PM	Jun 1, 2022 5:51:38 AM	<div><div>Force Variable,</div><div>Notify Var,</div><div>Read Var,</div><div>Write Var,</div><div>S7Plus</div></div>	765854	95.3 MB

Best Practices for Unauthorized Changes to Controllers

- **Short-Term:** Immediately restrict workstation access for the contractor. Restore PLC from a last known good backup
- **Mid-Term:** Implement a strict change management policy for all PLC modifications. Cisco ISE can enforce RBA to ensure only authorized engineers on authorized devices can perform program downloads..
- **Govern & Monitor (Long-Term):** Use CyberVision to create a baseline of normal behavior. Configure a high-priority alert to be sent to both OT and Security Teams anytime this event occurs.

Control Systems Events

Label	Severity Level				Syslog export	Database storage
	 low	 medium	 high	 very high		
New program downloaded	☐	☐	☐	☒	☒	☒
New program uploaded	☐	☐	☐	☒	☒	☒



**“the initial foothold of an
attack”**

IDS for OT

+	September 29, 2025 10:40:56.068 AM	critical	Security Events	Port scan over TCP between 192.168.2.22 (192.168.2.22) IP: 192.168.2.22 MAC: 00:07:7c:1a:61:83 and 192.168.88.50 (192.168.88.50) IP: 192.168.88.50 MAC: 00:05:e4:01:24:d3
+	September 29, 2025 10:40:56.068 AM	critical	Security Events	Port scan over TCP between 192.168.2.22 (192.168.2.22) IP: 192.168.2.22 MAC: 00:07:7c:1a:61:83 and 192.168.88.95 (192.168.88.95) IP: 192.168.88.95 MAC: 00:0a:dc:5b:27:a0
+	September 29, 2025 10:40:56.068 AM	critical	Security Events	Port scan over TCP between 192.168.2.22 (192.168.2.22) IP: 192.168.2.22 MAC: 00:07:7c:1a:61:83 and 192.168.88.51 (192.168.88.51) IP: 192.168.88.51 MAC: 00:d0:c9:bd:2e:57
+	September 29, 2025 10:40:56.068 AM	critical	Security Events	Port scan over TCP between 192.168.2.22 (192.168.2.22) IP: 192.168.2.22 MAC: 00:07:7c:1a:61:83 and 192.168.88.115 (192.168.88.115) IP: 192.168.88.115 MAC: 00:40:9d:28:ee:0d
+	September 29, 2025 10:40:56.068 AM	critical	Security Events	Port scan over TCP between 192.168.2.22 (192.168.2.22) IP: 192.168.2.22 MAC: 00:07:7c:1a:61:83 and 192.168.88.30 (192.168.88.30) IP: 192.168.88.30 MAC: 00:1c:06:01:d4:23
+	September 29, 2025 10:40:56.068 AM	critical	Security Events	Port scan over TCP between 192.168.2.22 (192.168.2.22) IP: 192.168.2.22 MAC: 00:07:7c:1a:61:83 and 192.168.88.49 (192.168.88.49) IP: 192.168.88.49 MAC: 00:40:8c:7f:0b:bc
+	September 29, 2025 10:40:56.068 AM	critical	Security Events	Port scan over TCP between 192.168.2.21 (192.168.2.21) IP: 192.168.2.21 MAC: 00:07:7c:1a:61:83 and 192.168.88.60 (192.168.88.60) IP: 192.168.88.60 MAC: 00:90:e8:26:40:23
+	September 29, 2025 10:40:56.068 AM	critical	Security Events	Port scan over TCP between 192.168.2.22 (192.168.2.22) IP: 192.168.2.22 MAC: 00:07:7c:1a:61:83 and 192.168.88.60 (192.168.88.60) IP: 192.168.88.60 MAC: 00:90:e8:26:40:23
+	September 29, 2025 10:40:56.068 AM	critical	Security Events	Port scan over TCP between 192.168.2.22 (192.168.2.22) IP: 192.168.2.22 MAC: 00:07:7c:1a:61:83 and 192.168.88.75 (192.168.88.75) IP: 192.168.88.75 MAC: 00:80:63:b5:b6:bb

Best Practices for IDS Alerts

- **Short-Term:** Isolate the compromised host from the network. Reset the engineer's credentials.
- **Mid-Term:** Enforce stricter segmentation between IT and OT networks.
- **Govern & Monitor (Long-Term):** Integrate CyberVision alerts with a SIEM/SOAR platform., e.g., Cisco XDR

XDR

XDR is a cloud-native, built-in platform that connects our Cisco Secure portfolio and your infrastructure. It allows you to radically reduce dwell time and human-powered tasks.

Configuration

If you activate this option users will be able to authenticate and benefit from XDR integration's features:

- Create incidents from the events page for these categories of events:
 - Anomaly Detection
 - Control Systems Events
 - Signature based Detection
- Activate XDR Ribbon and benefit from the associated features

Moreover, without requiring XDR authentication, users will have access to the 'Investigate' button on the Cyber Vision technical sheet for components, which will direct them to Cisco Threat Response (CTR).

Region

Enable XDR

Promote Events to Cisco XDR

April 2, 2024 11:40:55 AM

critical

Control Systems Events

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

source



192.168.105.241

destination



192.168.105.112

Flow

Source port: 1613
Destination port: 102

Source component

Device: 192.168.105.241
Name: 192.168.105.241
MAC: 34:17:eb:d1:c9:97
IP: 192.168.105.241
Tag: Engineering Station

Destination component

Device: 192.168.105.112
Name: 192.168.105.112
MAC: 28:63:36:85:b3:32
IP: 192.168.105.112
Tag: Controller
Vulnerabilities detected: 32

Report to XDR

View events in Cyber Vision

Launch investigation in XDR

Threat Response

Investigate

Snapshots

Incidents

Intelligence

Create New Incident

Investigate This Incident

Change Status

Link Reference

Download

Find ...

0 / 50

Sort/Filter: 6

Control system event: Stop CPU com...

Cisco Cyber Vision - 2021-05-26T04:30:50.175Z

Short: Attempted Information Leak fro...

Cisco Cyber Vision - 2021-05-26T04:25:31.206Z

Security Intelligence event - IP_Reput...

NGFW Event Service - 2021-01-12T17:17:41.117Z

Security Intelligence event - IP_Reput...

NGFW Event Service - 2021-01-12T17:12:05.193Z

Security Intelligence event - IP_Reput...

NGFW Event Service - 2021-01-12T17:12:02.934Z

Security Intelligence event - IP_Reput...

NGFW Event Service - 2021-01-12T17:12:02.931Z

Security Intelligence event - IP_Reput...

ngfw_event_service - 2020-04-06T16:43:32.309Z

Security Intelligence event - IP_Reput...

ngfw_event_service - 2020-04-06T16:43:32.309Z

Security Intelligence event - IP_Reput...

ngfw_event_service - 2020-04-06T16:43:32.309Z

Security Intelligence event - IP_Reput...

ngfw_event_service - 2020-04-06T16:43:32.287Z

Security Intelligence event - IP_Reput...

ngfw_event_service - 2020-03-31T19:23:04.676Z

Security Intelligence event - IP_Reput...

ngfw_event_service - 2020-03-31T19:12:34.460Z

Security Intelligence event - IP_Reput...

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

Control system event: Stop CPU command has been detected from 192.168.249.114 to 192.168.249.50:502
New - Created by Cisco Cyber Vision on 2021-05-26T04:30:49.867Z

Summary

Observables

Timeline

Sightings

Linked References (0)

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

JSON

Add Assignees

No one is assigned - assign yourself

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

KEY PROPERTIES

Categories: Investigation

Disc. Method: Cisco Cyber Visi...

Intend. Effect: Select ...

Confidence: High

TLP: Amber

DESCRIPTION

Source

Destination

Name: DESKTOP-GJUF2N

1769-L16ER/B LOGIX5316ER

Vendor VMware, Inc.

Rockwell Automation

Mac 00:0c:29:c7:c8:76

f4:54:33:91:cbee

IP 192.168.249.114

192.168.249.50

Tags WINDOWS, ENGINEERING PLC, ROCKWELL_AUTOMATION

TARGETS

IP Address 192.168.249.50

OBSERVABLES RELATED TO SIGHTING (1)

IP Address 192.168.249.114

RELATIONS (1)

IP Address 192.168.249.114 Connected To IP Address 192.168.249.50



“Man-in-the-Middle”

Alert for new Device -1 mac: e4:5f:01:3f:cb ip : 10.202.2.2

June
July
2

07/14/2022 17:12:43 Inventory Events New property "vendor-name : Raspberry Pi Trading Ltd" detected to  Raspberry 10.202.2.2 (⚙️ Telemecanique 10.202.2.2) | IP : 10.202.2.2 | MAC : e4:5f:01:3f:37:cb



Raspberry 10.202.2.2

See Technical sheet

Properties

Device: ⚙️ Telemecanique 10.202.2.2
Name : Raspberry 10.202.2.2
MAC : e4:5f:01:3f:37:cb
IP : 10.202.2.2

New properties detected
vendor-name : Raspberry Pi Trading Ltd

07/14/2022 17:12:43 Inventory Events New component detected on the network:  Raspberry 10.202.2.2 (⚙️ Telemecanique 10.202.2.2) | IP : 10.202.2.2 | MAC : e4:5f:01:3f:37:cb



Raspberry 10.202.2.2

See Technical sheet

Properties

Device: ⚙️ Telemecanique 10.202.2.2
Name : Raspberry 10.202.2.2
MAC : e4:5f:01:3f:37:cb
IP : 10.202.2.2

07/14/2022 17:12:43 Inventory Events Found an initial name "Raspberry 10.202.2.2" for the component  Raspberry 10.202.2.2 (⚙️ Telemecanique 10.202.2.2) | IP : 10.202.2.2 | MAC : e4:5f:01:3f:37:cb



Raspberry 10.202.2.2

See Technical sheet

Properties

Device: ⚙️ Telemecanique 10.202.2.2
Name : Raspberry 10.202.2.2
MAC : e4:5f:01:3f:37:cb
IP : 10.202.2.2

Alert for new Device -2 mac: e4:5f:01:3f:cb ip : 10.202.2.3

July 2

07/14/2022 17:12:43 Inventory Events New property "vendor-name : Raspberry Pi Trading Ltd" detected to Raspberry 10.202.2.3 (Telemecanique 10.202.2.3) | IP:10.202.2.3 | MAC:e4:5f:01:3f:37:cb



Properties

Device: Telemecanique 10.202.2.3

Name : Raspberry 10.202.2.3

MAC : e4:5f:01:3f:37:cb

IP : 10.202.2.3

[See Technical sheet](#)

New properties detected

vendor-name : Raspberry Pi Trading Ltd

07/14/2022 17:12:43 Inventory Events New component detected on the network: Raspberry 10.202.2.3 (Telemecanique 10.202.2.3) | IP:10.202.2.3 | MAC:e4:5f:01:3f:37:cb



Properties

Device: Telemecanique 10.202.2.3

Name : Raspberry 10.202.2.3

MAC : e4:5f:01:3f:37:cb

IP : 10.202.2.3

[See Technical sheet](#)

07/14/2022 17:12:43 Inventory Events Found an initial name "Raspberry 10.202.2.3" for the component Raspberry 10.202.2.3 (Telemecanique 10.202.2.3) | IP:10.202.2.3 | MAC:e4:5f:01:3f:37:cb



Properties

Device: Telemecanique 10.202.2.3

Name : Raspberry 10.202.2.3

MAC : e4:5f:01:3f:37:cb

IP : 10.202.2.3

[See Technical sheet](#)

gust
nber

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKIOT-2073


cisco

Timeline

2:00 PM

3:00 PM

4:00 PM

5:00 PM

6:00 PM

7:00 PM

161

ve ▶ 5:00 PM

o-follow ☐

96

◀ 1 2 3 ... 15 16 17 ▶

16:10:12.975	Control Systems Events	New program has been downloaded, flow from	 OT-WRKST02 (🔒 ot-wrkst02) IP: 10.202.0.52 MAC: 00:50:56:9e:27:0a to
16:10:12.975	Control Systems Events	New program has been downloaded, flow from	 Cisco 10.202.0.52 (🔒 ot-wrkst02) IP: 10.202.0.52 MAC: 4c:5d:3c:b4:48:45 to
16:12:43.083	Inventory Events	New component detected on the network:	 Cisco 10.202.5.201 (🔒 kali-raspberry-pi) IP: 10.202.5.201 MAC: 4c:5d:3c:b4:48:44
16:14:43.156	Inventory Events	New component detected on the network:	 kali-raspberry-pi (🔒 kali-raspberry-pi) MAC: e4:5f:01:3f:37:cb
16:32:13.886	Inventory Events	New component detected on the network:	 170.72.78.228 (🔒 170.72.78.228) IP: 170.72.78.228 MAC: 4c:5d:3c:b4:48:46
16:32:13.886	Inventory Events	New component detected on the network:	 138.199.14.84 (🔒 138.199.14.84) IP: 138.199.14.84 MAC: 4c:5d:3c:b4:48:46
16:32:13.886	Inventory Events	New component detected on the network:	 Cisco 10.1.51.85 (🔒 Cisco 10.1.51.85) IP: 10.1.51.85 MAC: 4c:5d:3c:b4:48:46
16:32:13.886	Inventory Events	New component detected on the network:	 52.137.110.235 (🔒 52.137.110.235) IP: 52.137.110.235 MAC: 4c:5d:3c:b4:48:46
16:32:13.886	Inventory Events	New component detected on the network:	 170.72.69.100 (🔒 170.72.69.100) IP: 170.72.69.100 MAC: 4c:5d:3c:b4:48:46
16:32:13.886	Inventory Events	New component detected on the network:	 173.223.217.220 (🔒 173.223.217.220) IP: 173.223.217.220 MAC: 4c:5d:3c:b4:48:46

◀ 1 2 3 4 5 6 7 8 9 10 ▶

17:12:43.791	Inventory Events	New component detected on the network:	 Raspberry 10.202.2.2 IP: 10.202.2.2 MAC: e4:5f:01:3f:37:cb
17:12:43.791	Inventory Events	New component detected on the network:	 Raspberry 10.202.2.3 IP: 10.202.2.3 MAC: e4:5f:01:3f:37:cb
17:13:43.863	Inventory Events	New component detected on the network:	 Cisco 192.168.70.159 IP: 192.168.70.159 MAC: 4c:5d:3c:b4:48:44
17:14:43.939	Inventory Events	New component detected on the network:	 142.250.199.170 IP: 142.250.199.170 MAC: 4c:5d:3c:b4:48:46
17:15:13.980	Inventory Events	New component detected on the network:	 101.53.168.152 IP: 101.53.168.152 MAC: 4c:5d:3c:b4:48:46
17:16:44.188	Inventory Events	New component detected on the network:	 20.42.73.29 IP: 20.42.73.29 MAC: 4c:5d:3c:b4:48:46
17:17:14.229	Inventory Events	New component detected on the network:	 63.140.36.104 IP: 63.140.36.104 MAC: 4c:5d:3c:b4:48:46
17:17:14.229	Inventory Events	New component detected on the network:	 172.217.27.205 IP: 172.217.27.205 MAC: 4c:5d:3c:b4:48:46
17:17:14.229	Inventory Events	New component detected on the network:	 172.217.174.68 IP: 172.217.174.68 MAC: 4c:5d:3c:b4:48:46
17:17:14.229	Inventory Events	New component detected on the network:	 142.250.192.67 IP: 142.250.192.67 MAC: 4c:5d:3c:b4:48:46



“malware execution”

Malware Download and Execution {DPI for OT Protocols}

Device	Device	First activity	Last activity	Tags	Stored flows	Packets	Volume	Events
 192.168.1.2	 192.168.1.88	Sep 28, 2025 1:44:57 PM	Sep 28, 2025 1:52:13 PM	<div><div>Program Download</div><div>Program Upload,</div><div>Start CPU,</div><div>Triconex</div></div>	1	896	144 kB	80

	Time	Severity	Category	Description
+	September 28, 2025 1:52:17.591 PM	critical	Signature based Detection	Malware named TRITON detected by DPIbetween  192.168.1.88 ( 192.168.1.88) IP: 192.168.1.88 MAC: 00:0c:29:28:dd:c5 and  192.168.1.2 ( 192.168.1.2) IP: 192.168.1.2 MAC: 40:00:00:00:00:02
+	September 28, 2025 1:52:17.591 PM	critical	Signature based Detection	Malware named TRITON detected by DPIbetween  192.168.1.2 ( 192.168.1.2) IP: 192.168.1.2 MAC: 40:00:00:00:00:02 and  192.168.1.88 ( 192.168.1.88) IP: 192.168.1.88 MAC: 00:0c:29:28:dd:c5

Best Practices and Recommendations

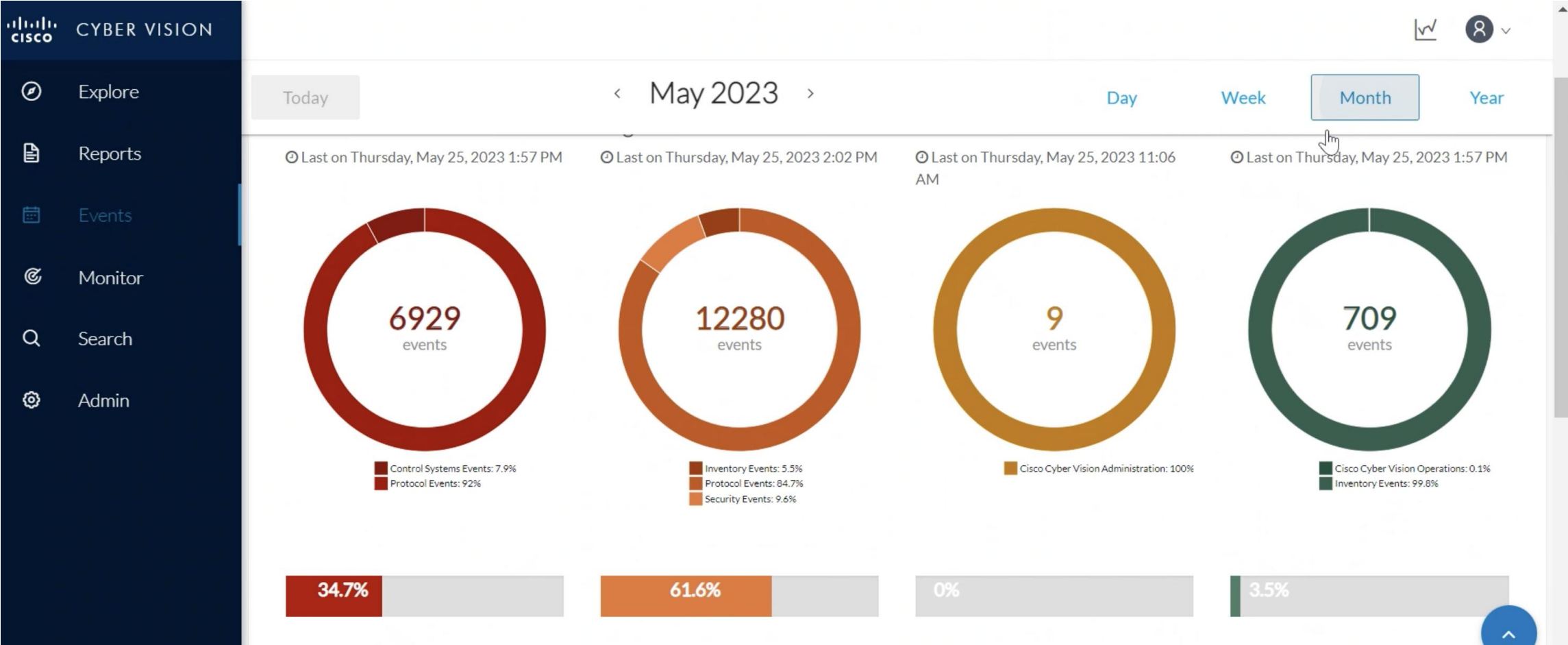
- Contain & Remediate (Short-Term)
- **Isolate, Verify Integrity, Physical Audit**
- **Long-Term:** Implement Zero-Trust Baseline for the Safety Network. Any communication whatsoever, other than the explicitly allowed diagnostic heartbeats should trigger highest possible severity alert,
- **Automated Incident Response**
- **Policy and Training**



“The SOC Integration”

Alert fatigue?

What do you think the problem is with the below image?



IT/OT Converged SOC Operations should be planned!

- Place Sensors Behind Perimeter Devices
 - Use firewalls or adaptive security appliances to filter traffic before sensors
- Understand Network Environment
 - Assess size, complexity, interconnections, traffic types for optimal placement
- Use Appropriate Capture Modes
 - 'Optimal' mode for mostly unicast; 'All' mode if multicast monitoring is needed
- Filter Known False Positives
 - Exclude benign sources like scanners or load balancers to reduce noise
- Gradual Deployment
 - Start small, use groups and presets, then expand to fine-tune alerts

CyberVision Update: Redesigned Alerts to reduce fatigue

The screenshot displays the Cisco CyberVision Alerts page. The top navigation bar includes the Cisco logo, the text 'Cyber Vision', a search bar, and a user profile. The left sidebar contains navigation links for Organization, Dashboard, Alerts, Assets, Vulnerabilities, and Configuration. The main content area is titled 'Alerts' and shows a summary of alert counts: 0 Critical, 3 High, 1 Medium, and 0 Low. Below this, there is a table of alerts with columns for Alert Type, Trigger, Instances, Severity, and Triggered By. The first alert is for 'Severe vulnerabilities in monitored entities' triggered by 'CVE-2023-3595 - Out-of-bounds Write Vulnerability in Rockwell...'. A detailed view of this alert is expanded, showing the CVE description, a table of risk scores, and a link to view the alert summary.

Alert Type	Trigger	Instances	Severity	Triggered By
Severe vulnerabilities in monitored entities	CVE-2023-3595 - Out-of-bounds Write Vulnerability in Rockwell...	1	High	Vulnerability
Severe vulnerabilities in monitored entities	CVE-2023-2262 - PN1649 - Stack-based Buffer Overflow in R...	1	High	Vulnerability
Severe vulnerabilities in monitored entities	CVE-2012-6438 - Rockwell Automation ControlLogix PLC Impr...	1	High	Vulnerability
Prohibited Vendors	ASRock	6	Medium	Property

CVE-2023-3595 - Out-of-bounds Write Vulnerability in Rockwell ControlLogix Communication Modules
1 monitored asset(s) are affected by this vulnerability which has a score $\geq$ the threshold defined in the alert rules

Cisco Security Risk Score	CVSS Score	Attack vector	Exploitability
56 Medium	9.8 Critical	Network	Not available

[View alert summary](#)

Rule Engine

- New rule engine to configure Alert thresholds
- E.g. trigger alert if CVSS score greater than 9 for assets seen by Sensor X

Alert Grouping

- Alerts grouped based on trigger to reduce number of alerts generated
- E.g. one CVE will generate only one alert for every matching asset in the environment

Actionable Alerts

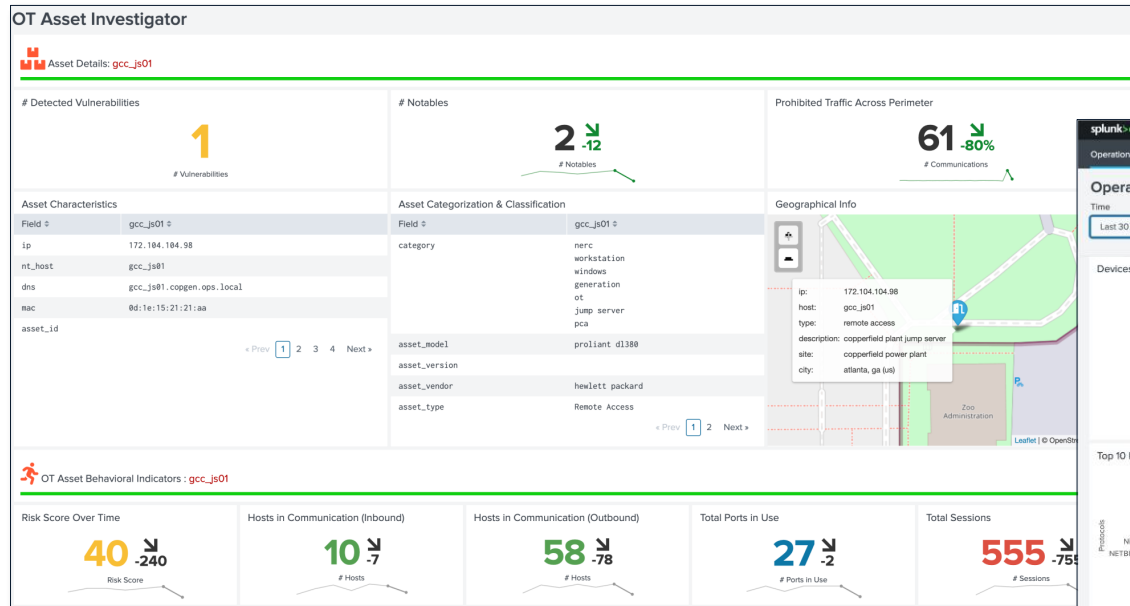
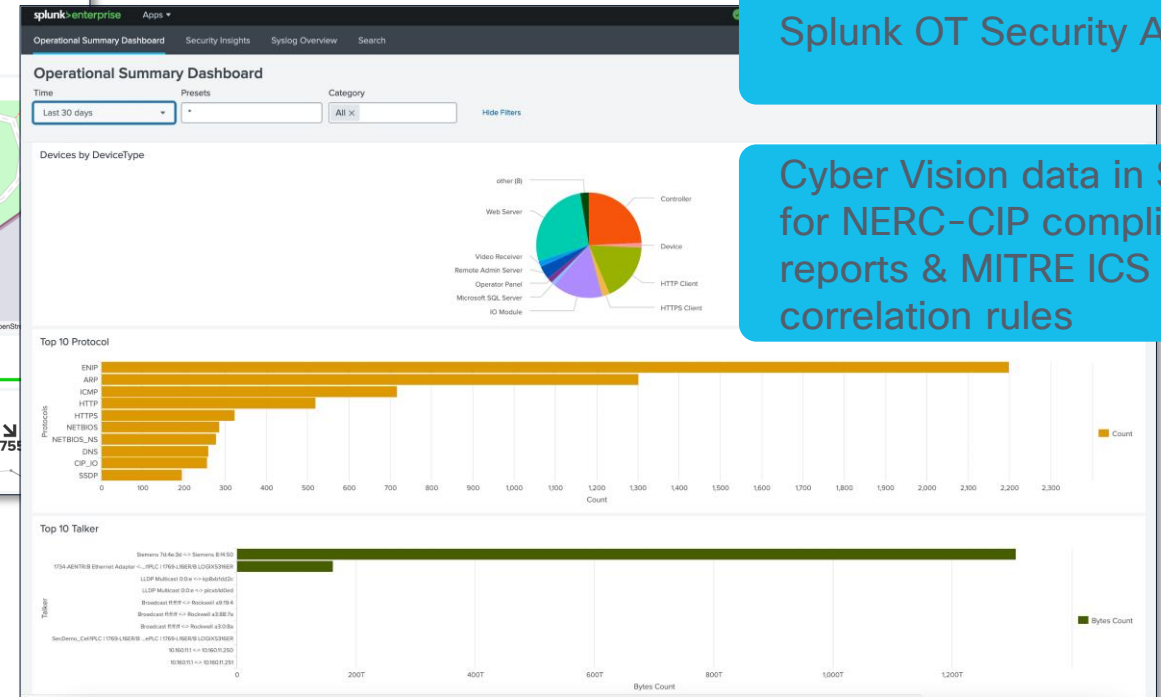
- Can be muted or automatically cleared, thereby reducing noise and focusing on what really matters

SIEM Integration: Splunk

Unified IT/OT security events management in Splunk SIEM

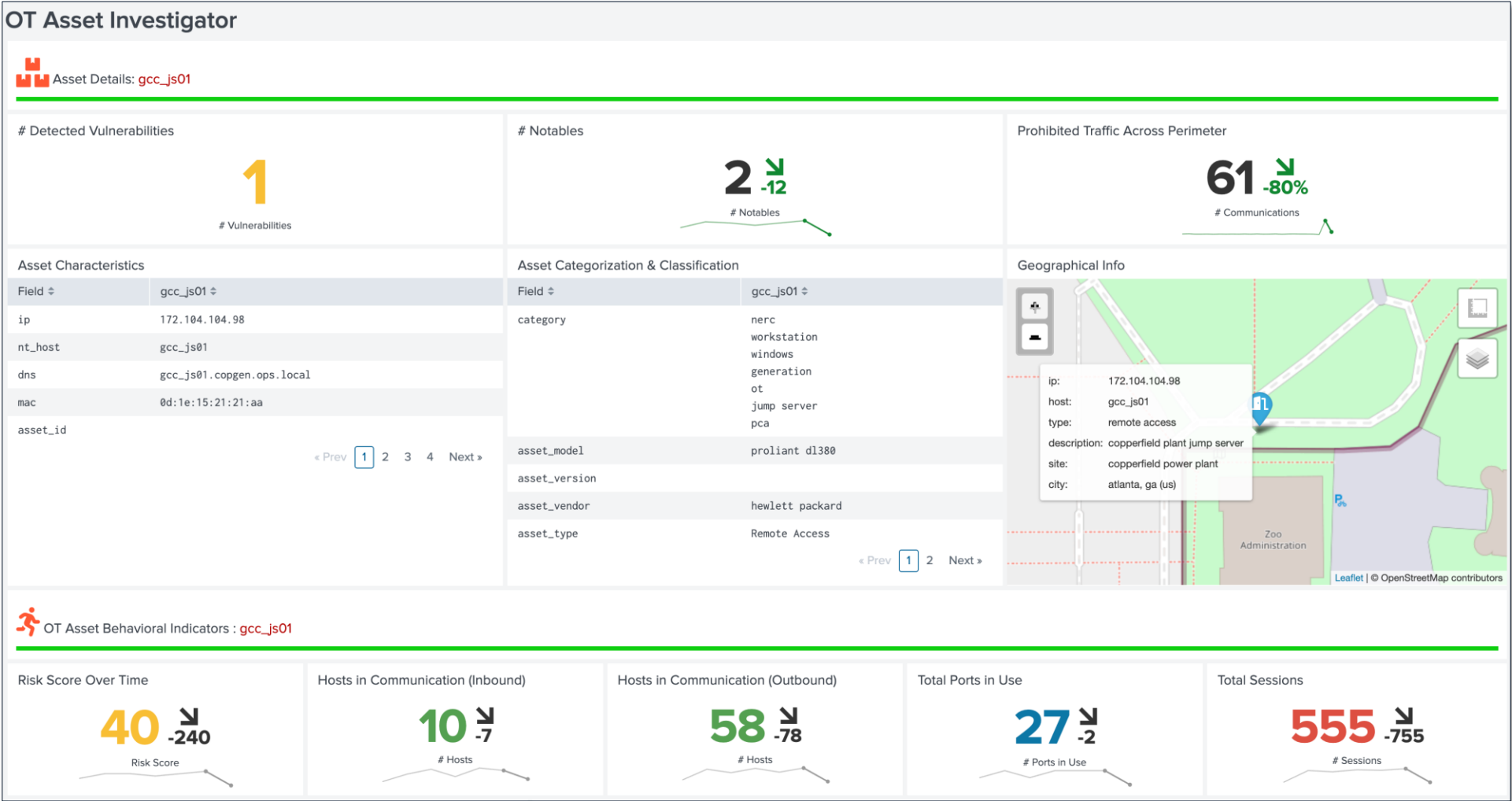
OT centric view of assets in Splunk OT Security Add-on

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

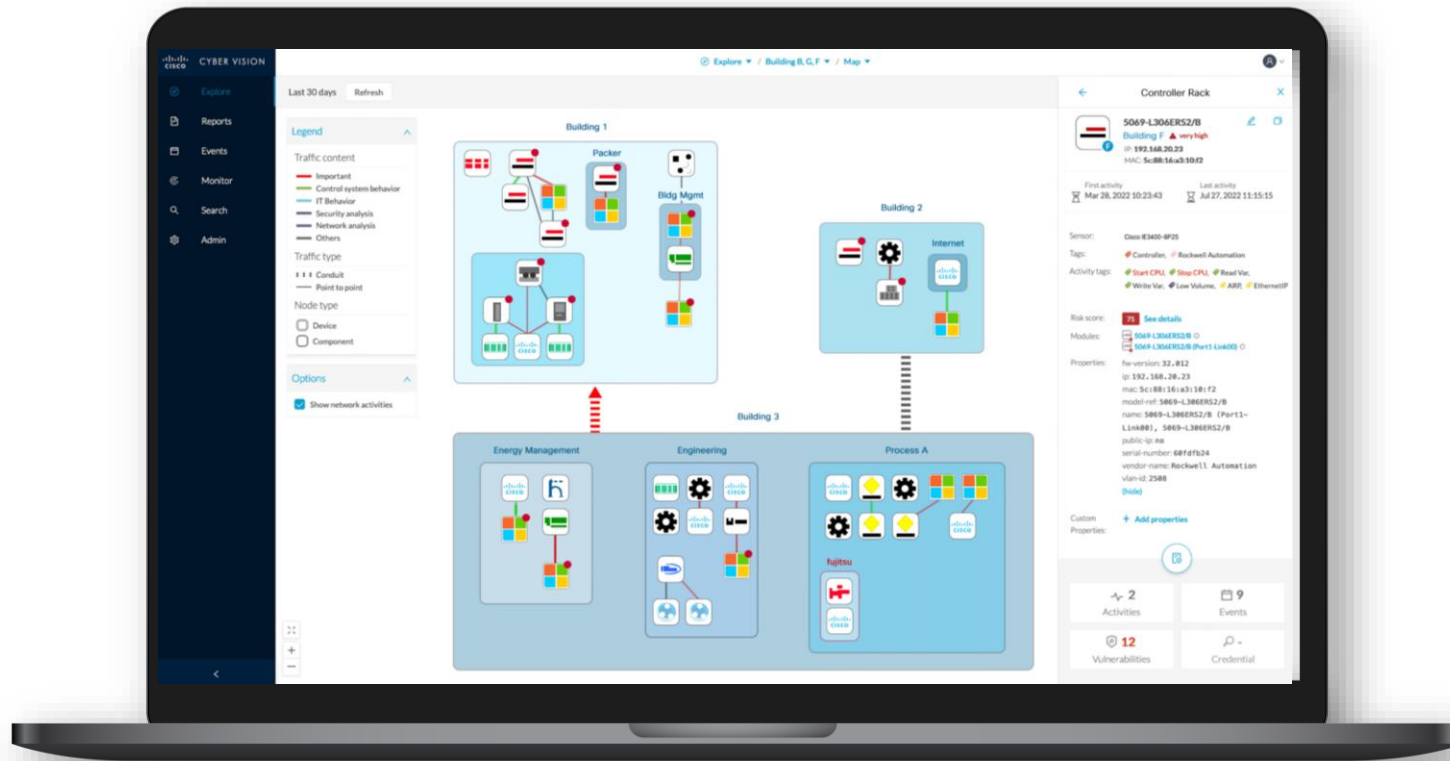
SIEM Integration: Splunk OT Security Add-On





“compliance”

The Journey to ISA/IEC 62443



IEC-62443 virtual segmentation



Group OT assets into zones



Visualize conduits



Identify traffic violations



Share context with other platforms to enforce segmentation

NIS2 related information for Posture Reports

- “Risk Zone” included in report
- DNS Servers and Communication
- Total devices and external domains

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

Preparing for a NERC CIP Audit: Device Inventory Report

Create new report

1 General

2 Settings

Name

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

Description

0 / 256

Type

Security Posture

Security Posture

Remote Access

Device Inventory

Customer logo

Device Inventory

Upload

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

General

2 Settings

Preset

All data

Table of content:

At least 1 section must be selected to generate a report

Executive Summary

Introduction

Risk Profile

Inventory Distribution Summary

Top Severity Events

External Communications

Device Inventory List

Preset Details

Risk Score filter

Networks filter

Device Tags filter

Activity Tags filter

Groups filter

Sensors filter

Executive Summary

Filter Criteria: All data Preset

Introduction

This report is an automated summary that captures the devices, their risk profile, and the inventory distribution summary found in the All data Preset by Cisco Cyber Vision on October 29th, 2024 at 12:24 pm UTC.

Risk Profile

Global Risk Score

50

Zone: Low-risk zone.
Action needed: Addressing vulnerabilities is still recommended although very few devices might need attention.

Risk Distribution by Risk Score

Low-820

High-59

Medium-225

Total number of devices: 1104

Vulnerabilities Distribution by Severity

High-233

Medium-139

Critical-97

Total number of vulnerabilities: 469

Inventory Distribution Summary

Top 5 Vendors by Device Count

Vendor	Count	Percentage
VMWARE INC	281	(27%)
CISCO SYSTEMS INC	276	(26%)
LANCOM ELECTRONICS INC	94	(9%)
SHURE INCORPORATED	73	(7%)
SEWELL AUTOMATION	29	(3%)

Top 5 Protocols by Device Count

Protocol	Count	Percentage
HTTP	101	(38%)
HTTPS	45	(21%)
SSH	43	(20%)
Modbus	40	(27%)
SNMP	34	(22%)

Total number of vendors seen: 58

Total number of protocols seen: 71

Top 10 Device Types by Device Count

Device Type	Count
WEB_BROWSER	104
FILE	45
NET_DEVICE	31
HTTPS_PROXY	24
HTTPS_PROXY	24
NET_DEVICE	19
NET_DEVICE	19
NET_DEVICE	19
NET_DEVICE	19
NET_DEVICE	19

Total number of device types seen: 22

Remote Access Reports

* Type

Security Posture

Security Posture

Remote Access

Device Inventory

Cisco Cyber Vision Remote Access Report

March 14, 2024, 1:41 pm UTC

Remote Access Gateways

Filter Criteria: All data Preset

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

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

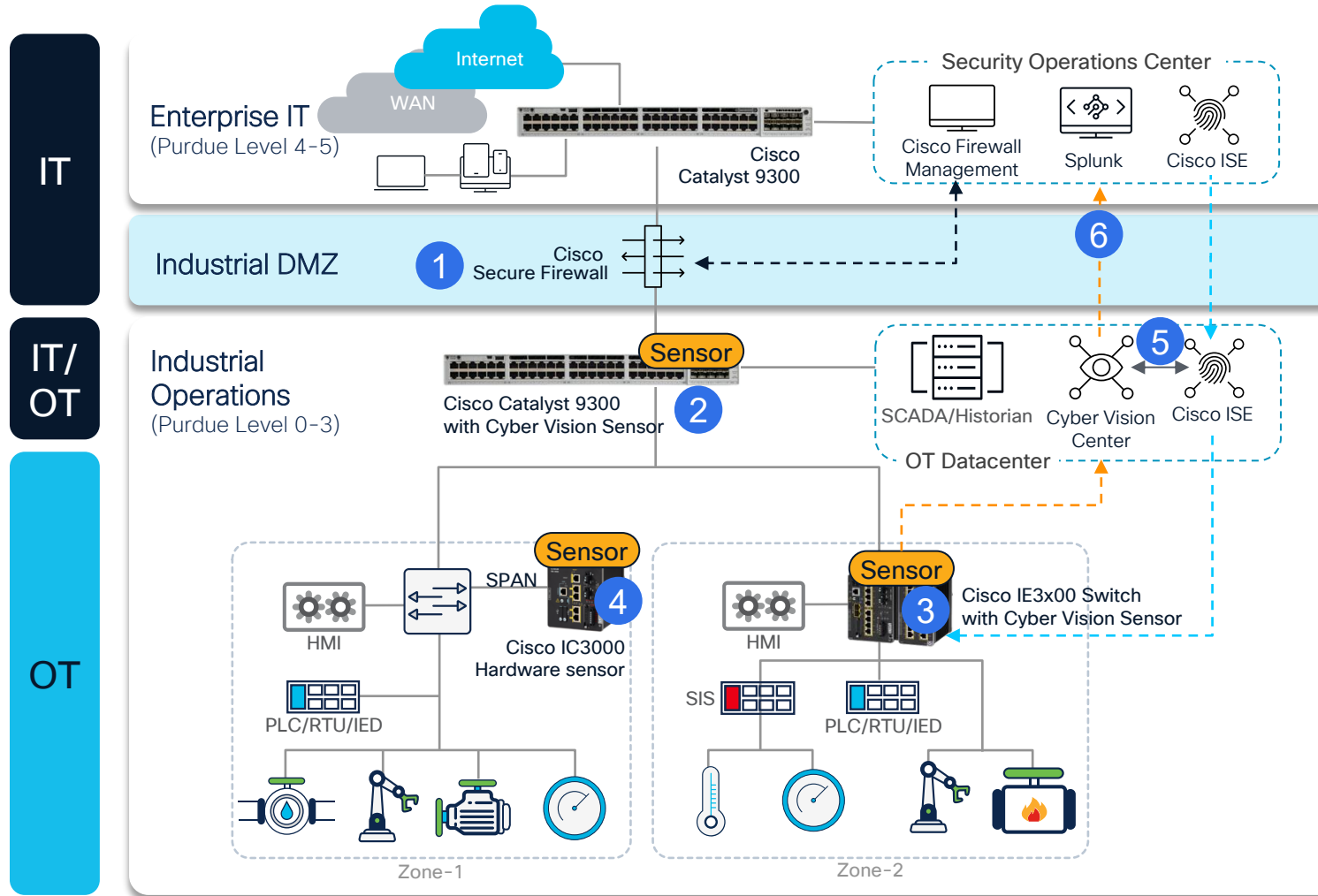
DNS Queries to Remote Access Domain Names

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

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

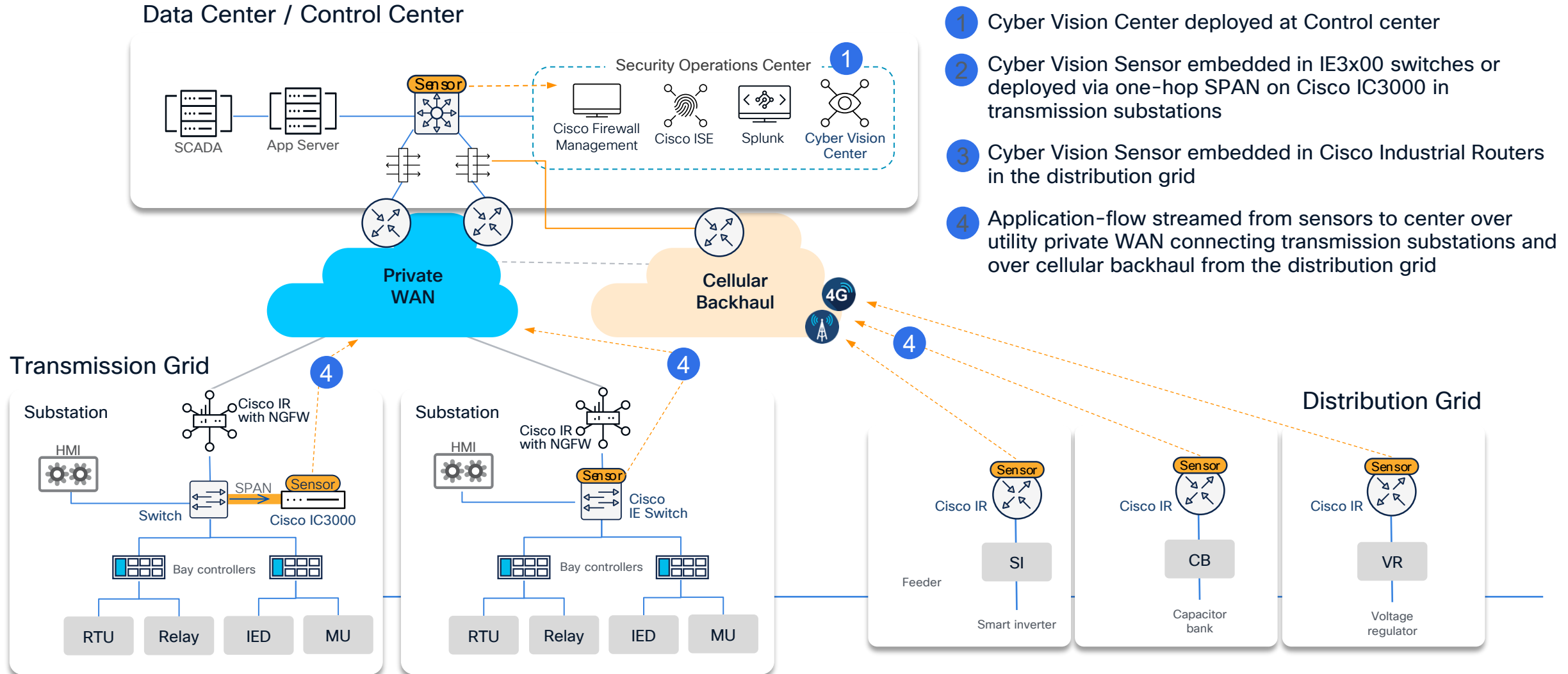
Cyber Vision in Industries

Cisco Cyber Vision in Manufacturing



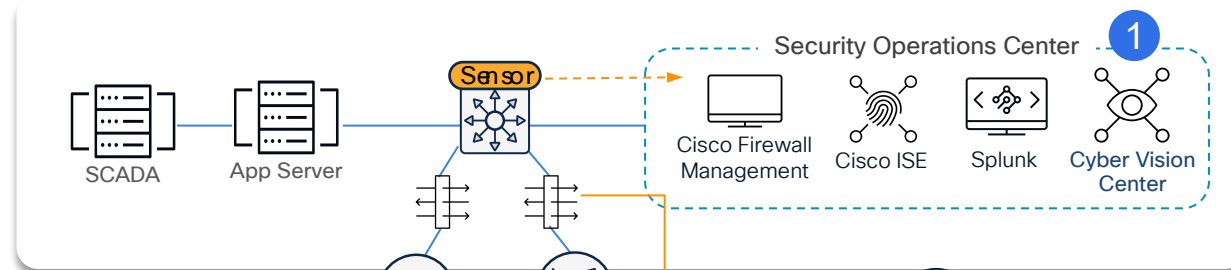
- 1 Isolate IT and OT by installing an industrial DMZ with Cisco Secure FW
- 2 Create macro-segmentation zones in the Catalyst 9300 switches and deploy Cyber Vision sensors with Snort IDS.
- 3 Cyber Vision sensors deployed within segments across IE3x00 switches
- 4 Cyber Vision hardware-sensors deployed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



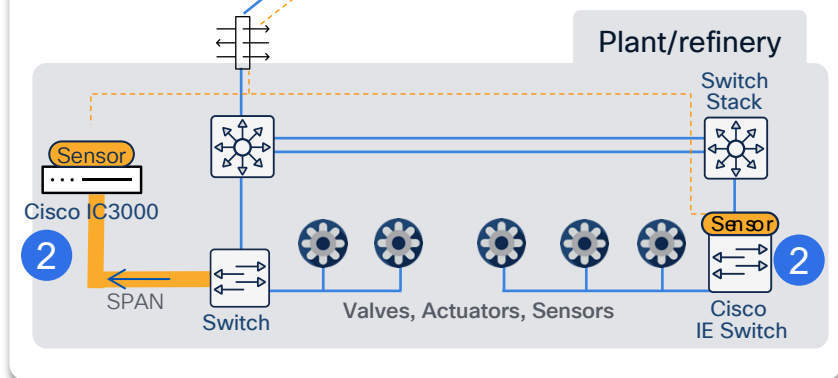
Cisco Cyber Vision in Oil and Gas

Data Center / Control Center

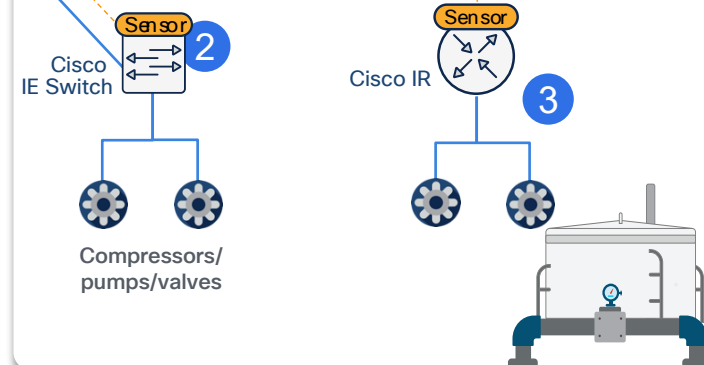


- 1 Cyber Vision Center deployed at Control center
- 2 Cyber Vision Sensor embedded in IE3x00 switches or deployed via one-hop SPAN on Cisco IC3000 in Downstream, Midstream and Upstream
- 3 Cyber Vision Sensor embedded on directly on Cisco Industrial Routers for distributed applications
- 4 Light weight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

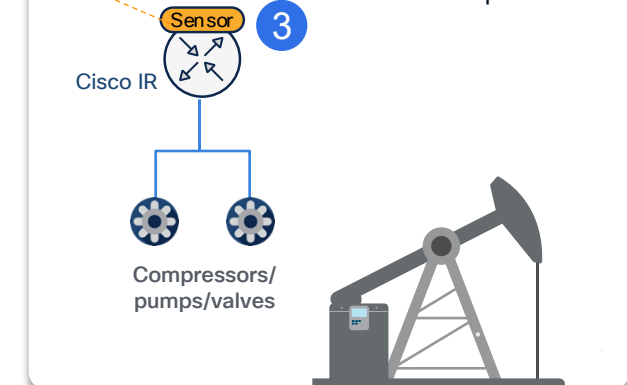
Downstream



Midstream



Upstream



The Future of Industrial Network Security

Industrial Defense Must Embrace IT-OT Convergence for Future Security



- IT and OT integration is central to digital transformation, driving operational efficiency and better data insights.

- As environments grow more interconnected, risks increase, requiring cooperative and unified security strategies.

- Organizations should leverage IT technologies in industrial networks to ensure resilience, reduce complexity, and drive new outcomes.

- Organizations must break down silos and adopt unified security strategies that enable collaboration and prepare them for emerging risks.

IT-OT Integration Drives Operational Excellence and Security Coverage

Performance Priority

Operational excellence leads investment decisions with 36% prioritizing enhanced throughput capabilities

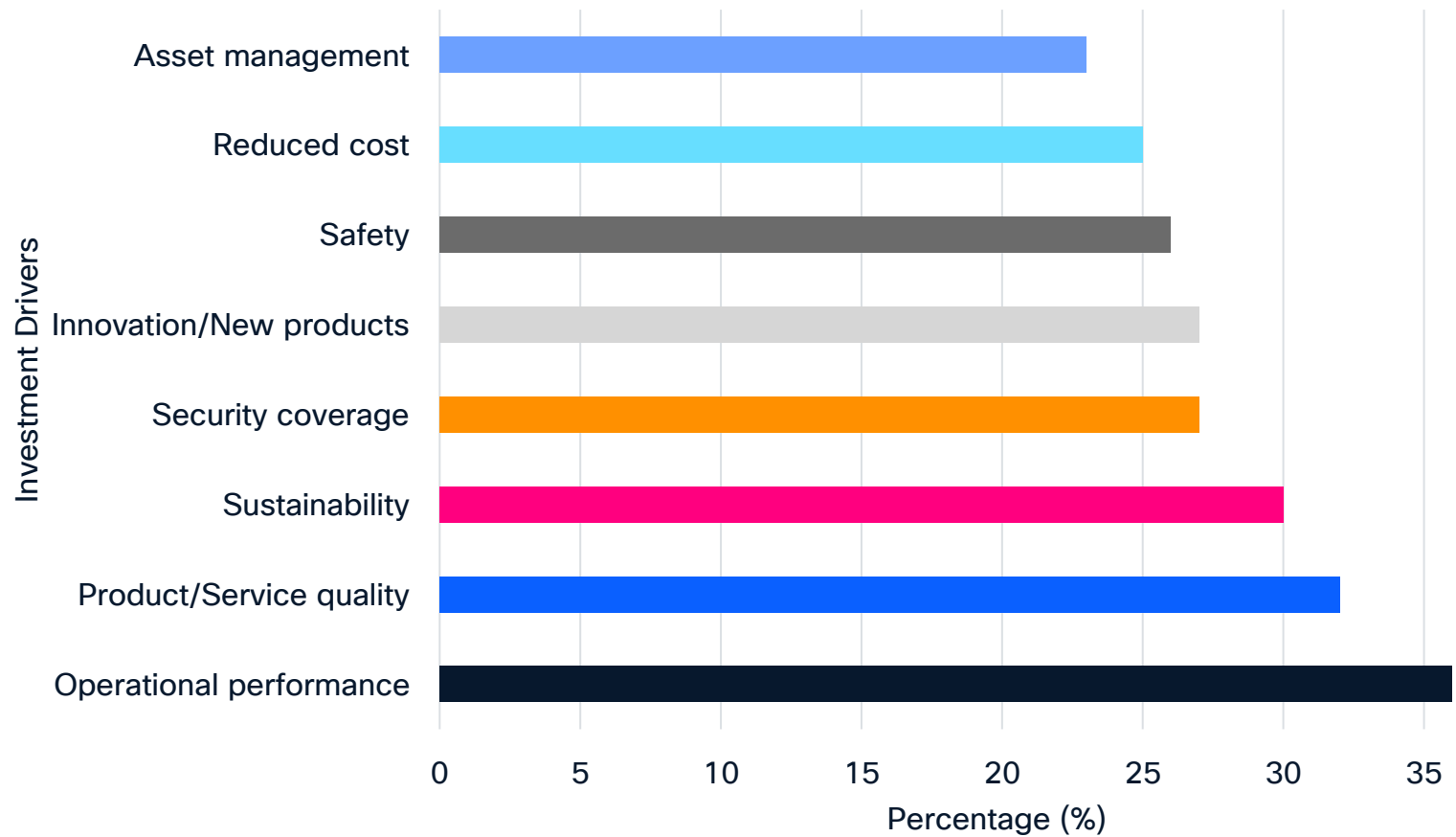
Quality Focus

Product quality drives 32% of integration efforts through predictive issue resolution

Strategic Balance

Security coverage ranks fourth at 27% indicating comprehensive defense modernization approach

Main Drivers for IT-OT Integration Investment in Industrial Defense



Collaborative IT-OT Teams Essential for Industrial Security Maturity

Maturity Paradox

Higher security sophistication increases rather than reduces IT collaboration requirements significantly

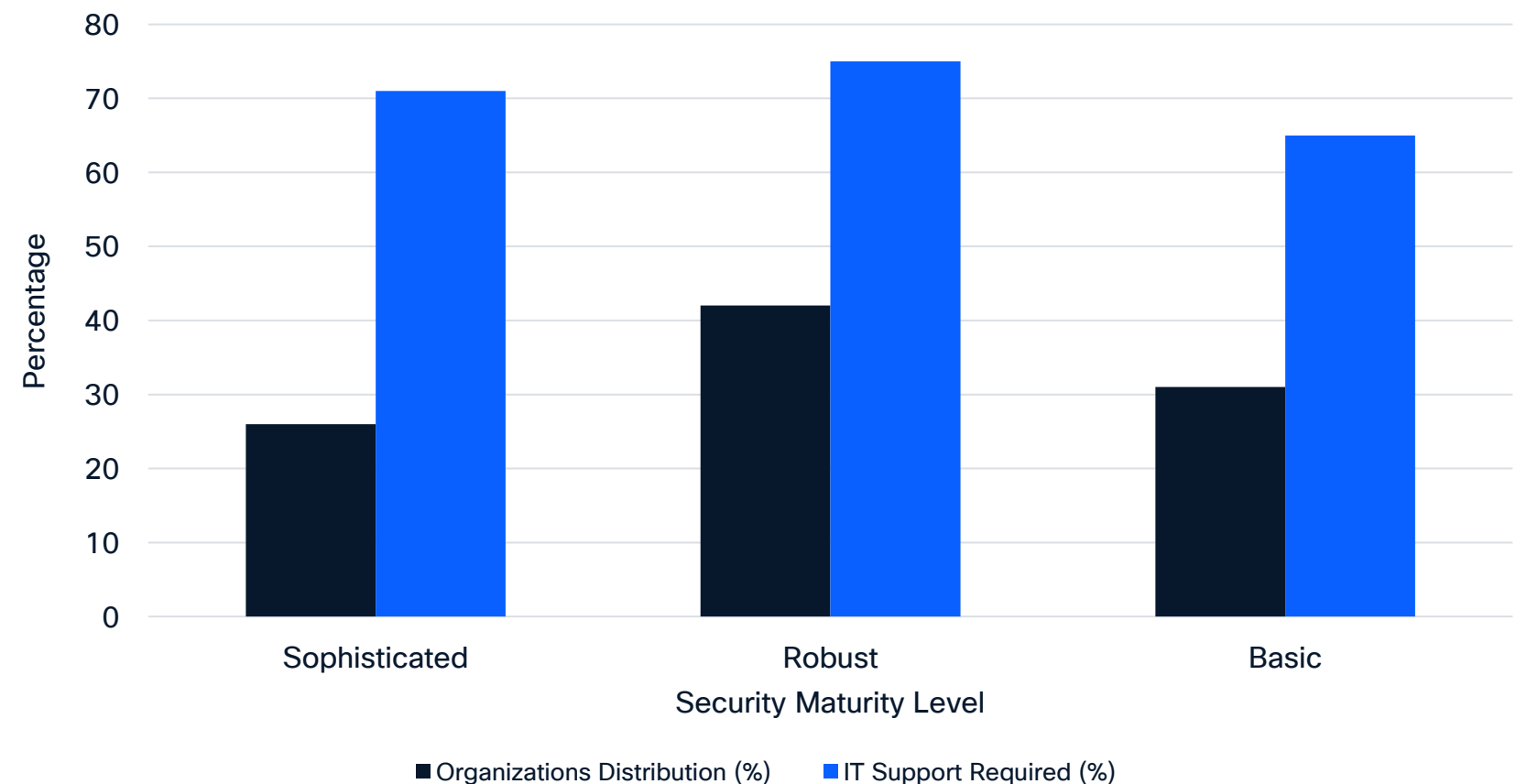
Robust Dependency

Organizations with robust security practices show highest IT support needs at 75%

Universal Integration

Even basic security implementations require substantial 65% IT support for effectiveness

Security Sophistication Levels and IT Support Requirements



Comprehensive Visibility and Segmentation Protect Critical Industrial Assets

Lack of visibility is a significant barrier to implementing an effective industrial security strategy and often leaves critical gaps unaddressed.

50% of OT assets are over 10 years old and their security posture needs to be assessed.

Embedding OT visibility capabilities in the network offers scalable and cost-effective deployment options, enabling organizations to overcome related limitations.

Most OT networks remain unsegmented, leaving critical assets exposed and increasing the likelihood of lateral movement during attacks.

The adaptive enforcement of segmentation policies strengthens operational resilience and aligns with zero trust principles.

Unified Industrial SOC Enables Advanced Threat Detection Across Domains



Isolation No Longer Viable

Managing OT security in isolation is no longer viable as industrial operations increasingly rely on IT and cloud.



Unified Detection Required

Unified threat detection enables organizations to correlate events across all domains and detect patterns and advanced threats that could otherwise go unnoticed.



Best-in-Class Tools Needed

Detecting and responding to modern threats requires best-in-class IT security tools for each task of the security workflow.

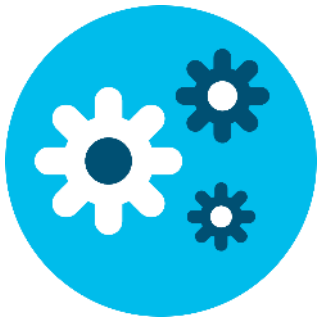


Integrated View is Essential

Organizations need a unified, integrated view of security data from best-in-class IT security tools to enable effective threat detection across IT, OT, and cloud in their SOC.

Cisco Cyber Vision Assessment Services

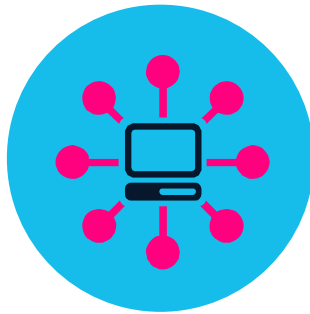
With Cisco's **Assessment Service** you can get a Comprehensive Picture of your Industrial Security Posture



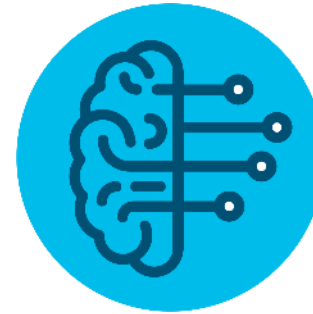
Automated Asset
Inventory



Vulnerability
Detection



Communication
Maps



Actionable
Insights



Detailed
Reports

Services led by Cisco OT Security experts, following a process that is proven to yield results.

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: jadusupa@cisco.com

Thank you

CISCO Live !

