Sécurité des réseaux industriels (OT)

Analyse approfondie de Cyber Vision

Florian Bois
Network Security Engineer,
Orange Cyberdefense

Nicolas DEVILLE
IIoT Security Product Manager,
Cisco

16 Septembre 2025

- Do not edit
- How to change the design

- **Quel est le 1er mot qui vous viens à l’esprit lorsque l’on parle de cyber-sécurité industrielle ?**

ⓘ

- The Slido app must be installed on every computer you’re presenting from

slido

- Do not edit
- How to change the design

- Comment jugez vous la sécurité de vos réseaux OT ?

- The Slido app must be installed on every computer you’re presenting from

slido

- **Votre entreprise est-elle impactée par NIS2 ?**

Agenda

01 Les enjeux cyber dans l’OT

02 Etapes de sécurisation des réseaux OT

03 Visibilité : Cisco Cyber Vision

04 Segmentation : ISE & FMC

05 Gestion des accès distant : SEA

06 Surveillance et répons à incident : Splunk

07 Cas clients

Agenda

01 Les enjeux cyber dans l'OT

02 Etapes de sécurisation des réseaux OT

03 Visibilité : Cisco Cyber Vision

04 Segmentation : ISE & FMC

05 Gestion des accès distant : SEA

06 Surveillance et répons à incident : Splunk

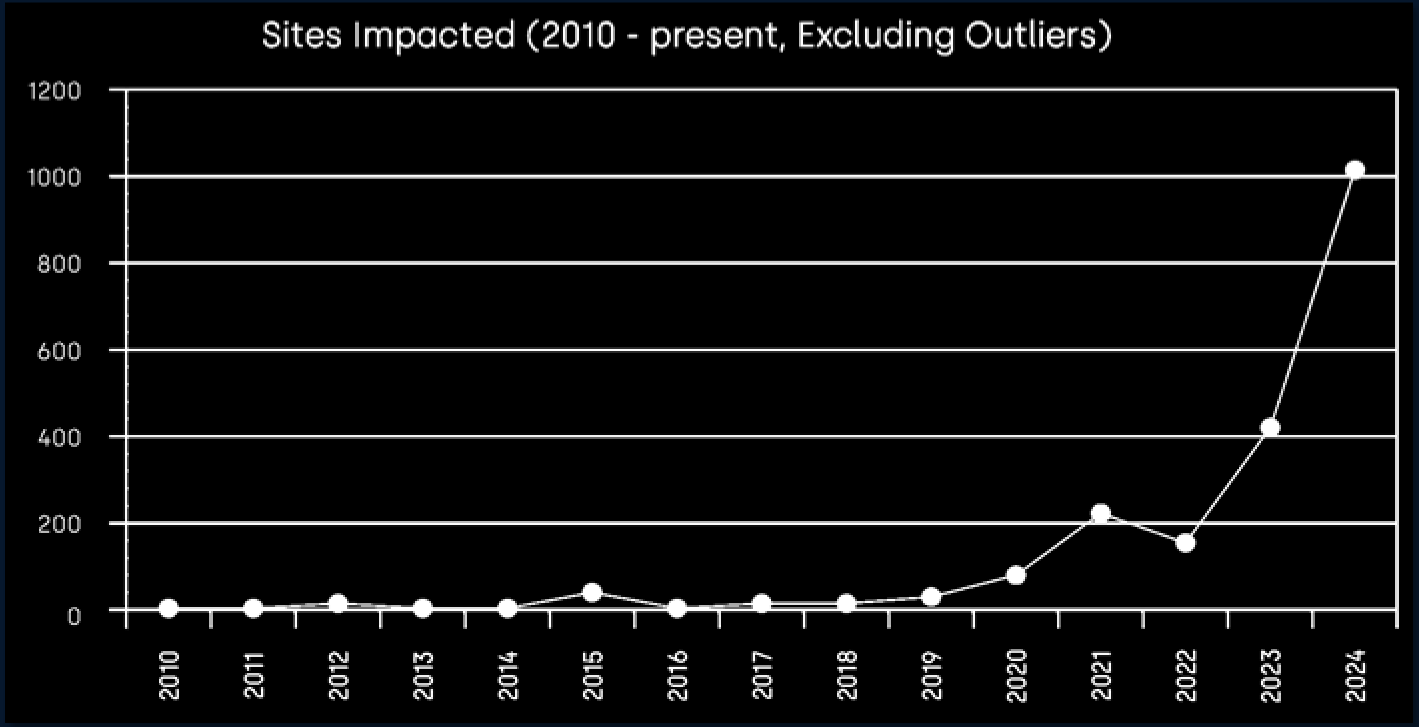
07 Cas clients

The reality of industry digitization

Increased connectivity results in more cyberattacks

2024 saw:

- At least one cyberattack every week against OT assets caused physical consequences in 2024
- 146% increase in sites impacted by cyberattacks with physical consequences
- Nation state attacks have tripled



Waterfall 2025 OT Cyber Security Threat Report

Industrial Security Challenges are scary

- Internet accessible Industrial Control Systems
- Port-forwarding on LTE backdoors
- Legacy Windows devices with known exploits
- More state sponsorship to exploit vulnerabilities

.....

+

AI enhancements have introduced even more threats, and made exploitation easier than ever

- AI Generated code to exploit vulnerabilities (Hacker GPT)
- Remote Access backdoors built into autonomous robots (Unitree Go1 Robot Dogs)
- Adaptive malware bypassing IPS signatures

Common issues in industrial operations

- Lack of OT visibility
- Vulnerable assets
- Lack of segmentation
- Limited OT security skill sets
- Poor access control
- Ineffective workflow between OT and IT

Agenda

01 Les enjeux cyber dans l’OT

02 **Etapes de sécurisation des réseaux OT**

03 Visibilité : Cisco Cyber Vision

04 Segmentation : ISE & FMC

05 Gestion des accès distant : SEA

06 Surveillance et répons à incident : Splunk

07 Cas clients

The journey to secure operational networks

Understand the OT security posture with OT visibility

Limit blast radius with network segmentation

Control risks from remote access to OT assets

Monitor OT networks in the SOC

Agenda

01 Les enjeux cyber dans l’OT

02 Etapes de sécurisation des réseaux OT

03 Visibilité : Cisco Cyber Vision

04 Segmentation : ISE & FMC

05 Gestion des accès distant : SEA

06 Surveillance et répons à incident : Splunk

07 Cas clients

Step #1: Deploying OT Visibility

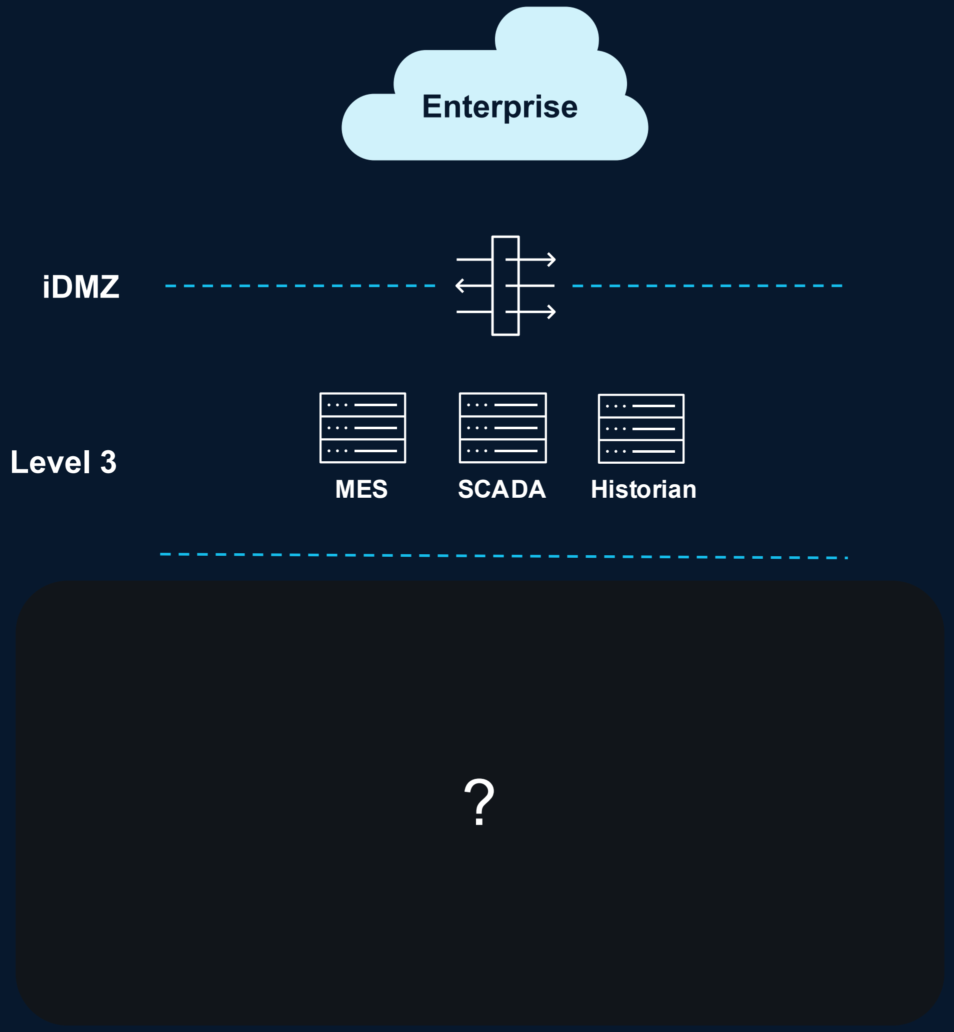
Understand the OT security posture with OT visibility

Limit blast radius with network segmentation

Control risks from remote access to OT assets

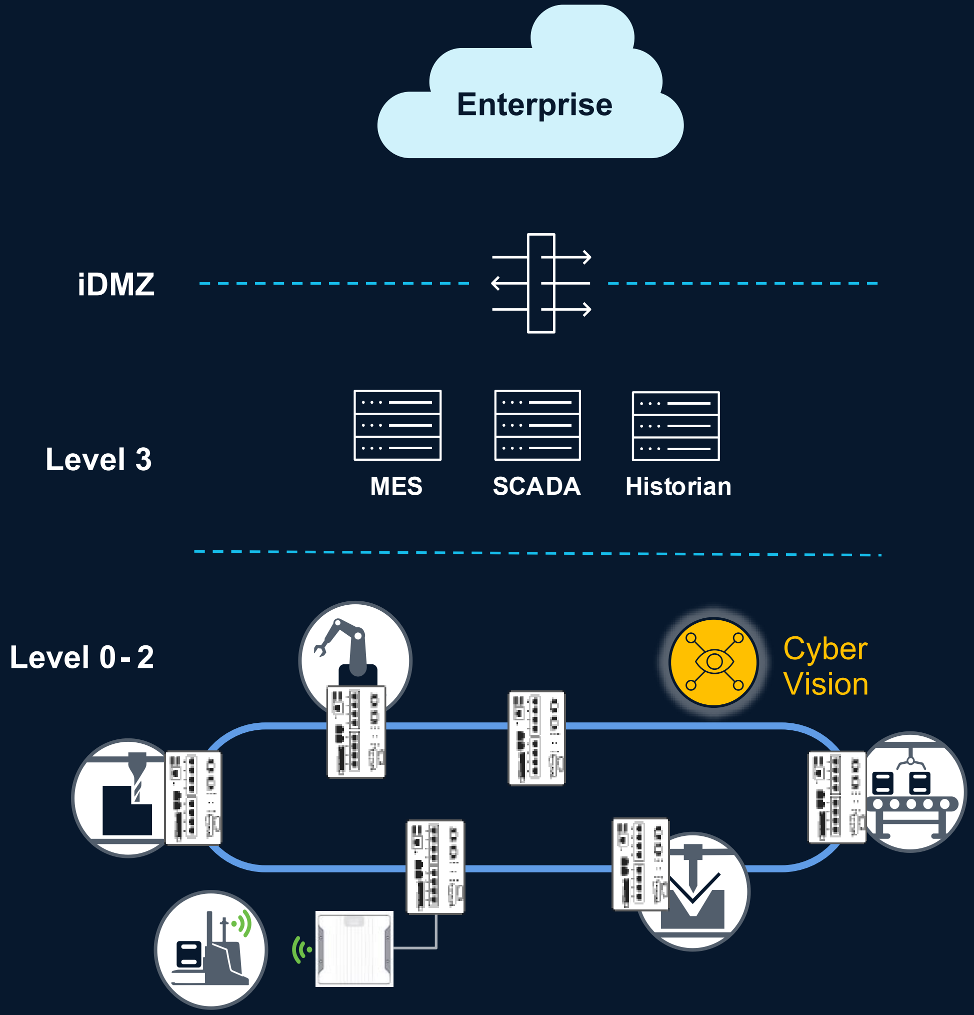
Monitor OT networks in the SOC

Most organizations do not have visibility into their critical assets



Cisco Cyber Vision “turns on the lights” for industries

- Inventory OT assets and their communications
- Spot vulnerabilities to patch or mitigate
- Create access policies to segment networks
- Detect bypass or leaks in the IDMZ
- Drive compliance and governance



Automated discovery of assets, vulnerabilities, and communication across the industrial network

Cisco Cyber Vision

Visibility & Security Platform
for the Industrial IoT

Visibility

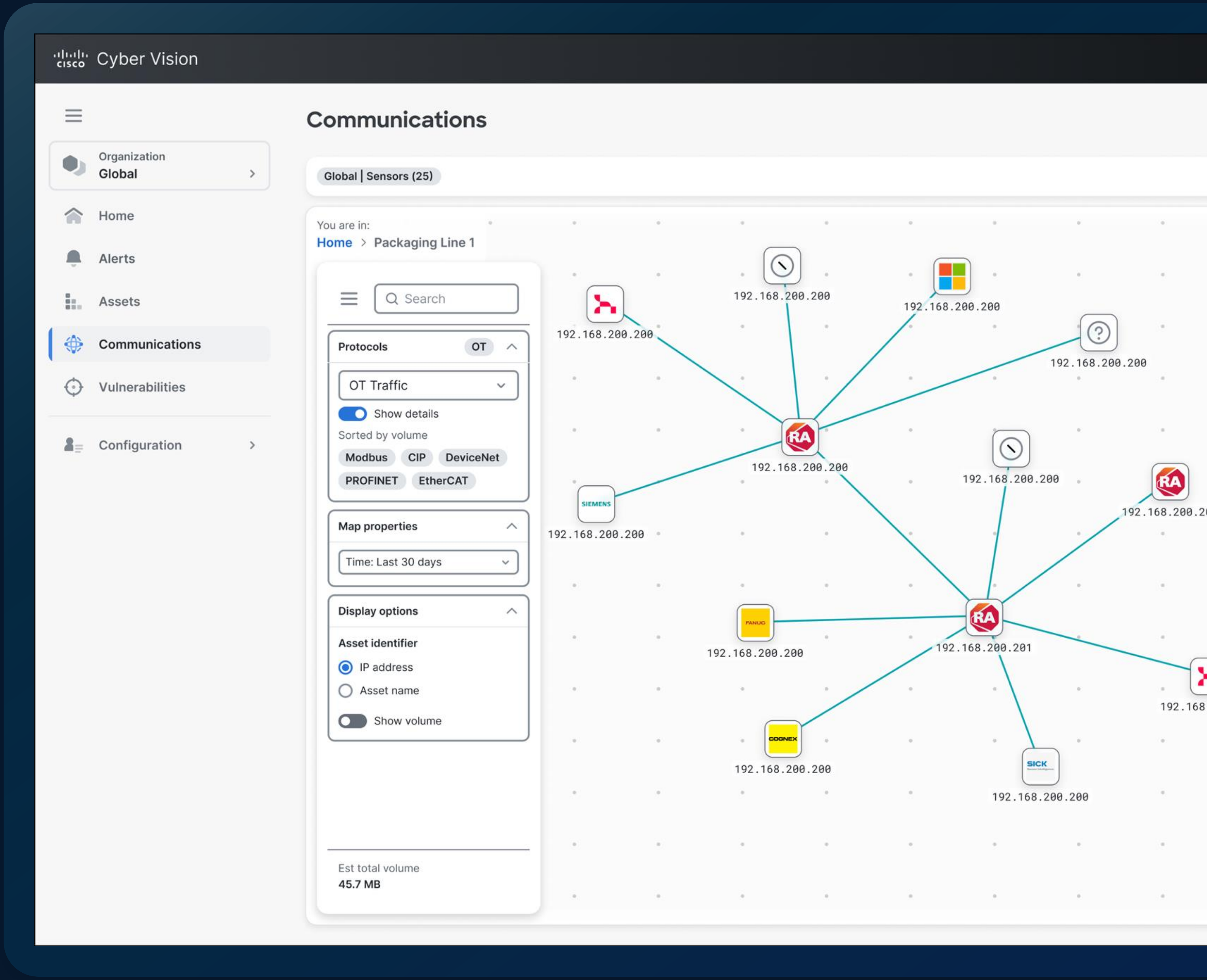
OT asset inventory
Communication patterns

Security Posture

Device vulnerabilities
Risk scoring

Zone Segmentation

Automate segmentation below the IDMZ to protect operations



You are in:
Home > Packaging Line 1

Protocols: OT
OT Traffic
Show details: on
Sorted by volume
Modbus · CIP · DeviceNet · PROFINET · EtherCAT

Map properties
Time: Last 30 days

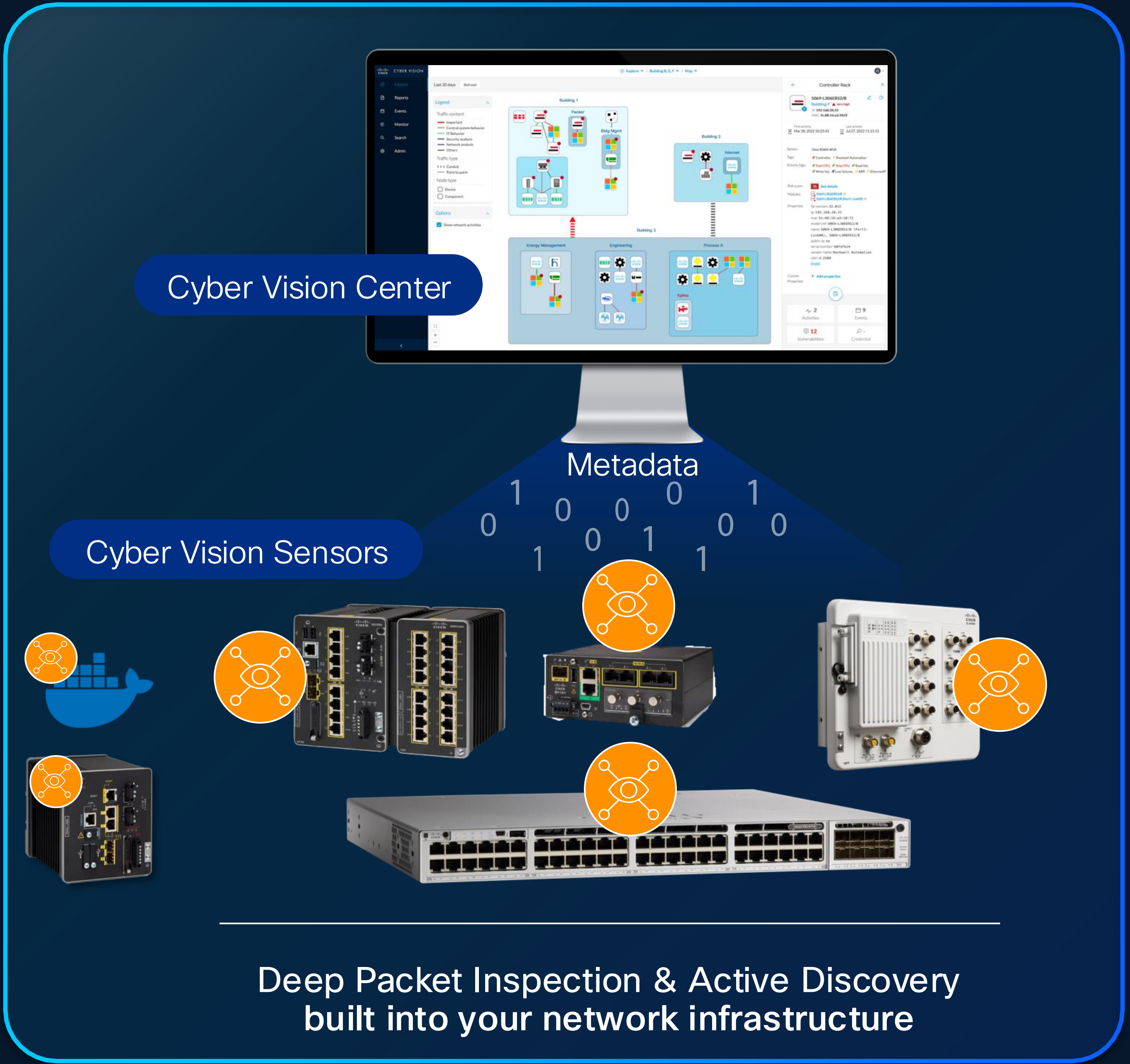
Display options
Asset identifier
● IP address
○ Asset name
Show volume: off

Est total volume
45.7 MB

Cyber Vision

Visibility built-in, not bolted on

Cisco industrial network sees everything, so you gain visibility at scale



Cyber Vision Center

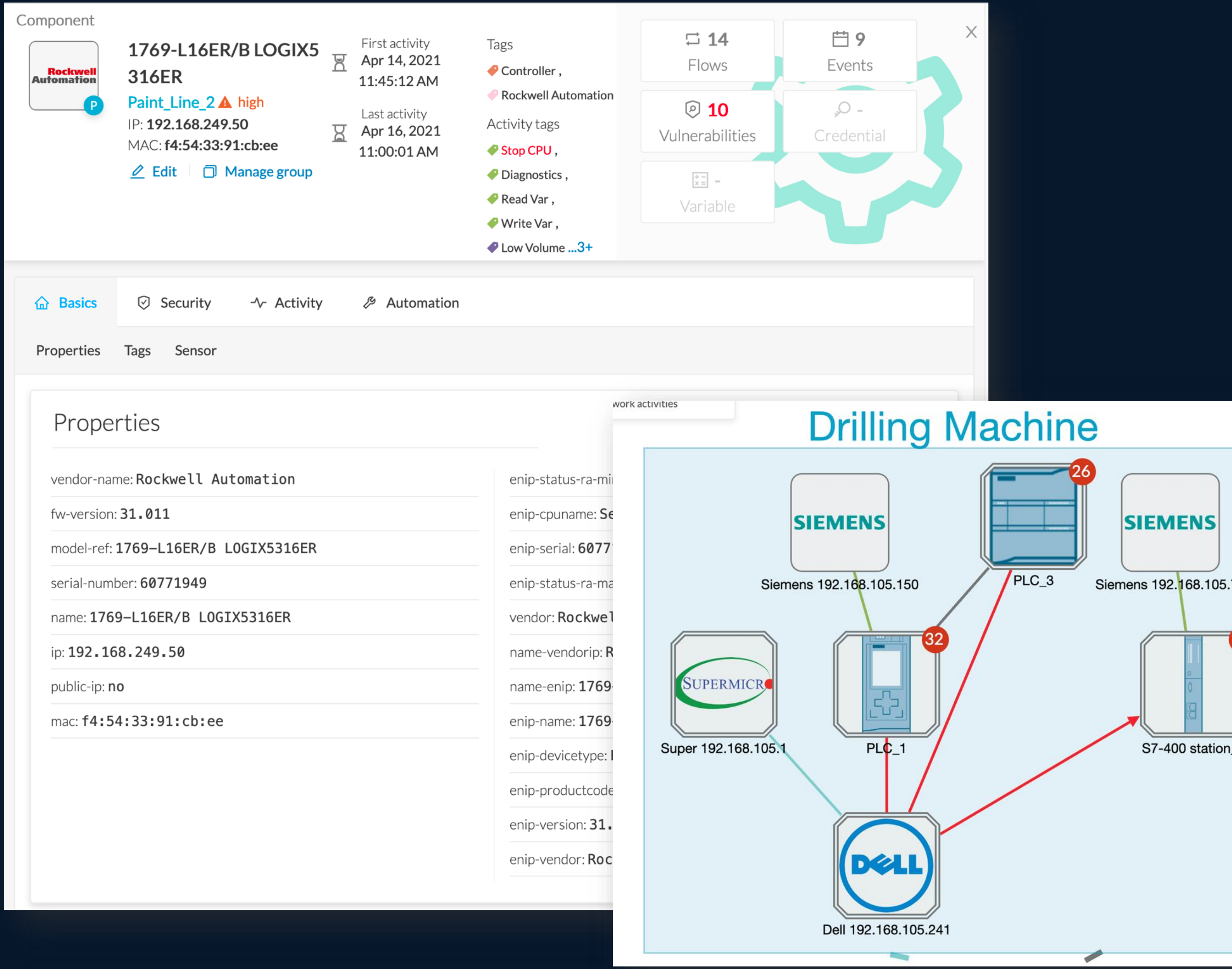
Metadata

Cyber Vision Sensors

Deep Packet Inspection & Active Discovery
built into your network infrastructure

Visibility into connected industrial assets

Understand the identity of all assets in the environment gain insight into network communications



Component

1769-L16ER/B LOGIX5316ER

Paint_Line_2 ⚠ high

IP: 192.168.249.50

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

Edit | Manage group

First activity Apr 14, 2021 11:45:12 AM

Last activity Apr 16, 2021 11:00:01 AM

Tags: Controller , Rockwell Automation

Activity tags: Stop CPU , Diagnostics , Read Var , Write Var , Low Volume ...3+

14 Flows | 9 Events | 10 Vulnerabilities | - Credential | - Variable

Basics | Security | Activity | Automation

Properties | Tags | Sensor

Properties

vendor-name: Rockwell Automation

fw-version: 31.011

model-ref: 1769-L16ER/B LOGIX5316ER

serial-number: 60771949

name: 1769-L16ER/B LOGIX5316ER

ip: 192.168.249.50

public-ip: no

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

enip-status-ra-mi

enip-cpuname: Se

enip-serial: 6077

enip-status-ra-ma

vendor: Rockwel

name-vendorip: R

name-enip: 1769

enip-name: 1769

enip-devicetype: I

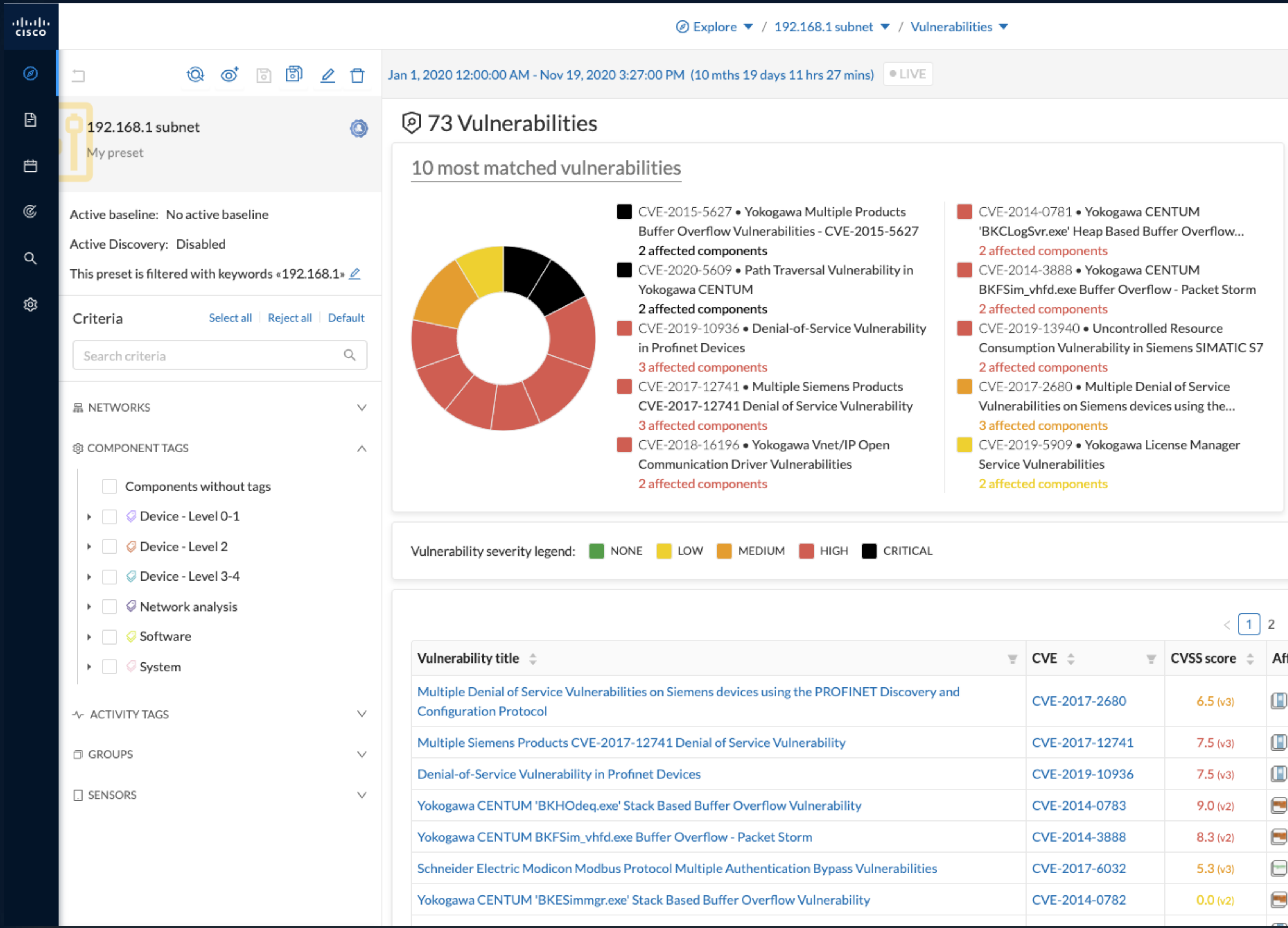
enip-productcode

enip-version: 31.

enip-vendor: Roc

Identify & Track Vulnerabilities

Identify known asset vulnerabilities so you can patch or protect them before they are exploited



Explore ▾ / 192.168.1 subnet ▾ / Vulnerabilities ▾

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

192.168.1 subnet
My preset

Active baseline: No active baseline

Active Discovery: Disabled

This preset is filtered with keywords «192.168.1»

Criteria | Select all | Reject all | Default

Search criteria

NETWORKS

COMPONENT TAGS

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

ACTIVITY TAGS

GROUPS

SENSORS

73 Vulnerabilities

10 most matched vulnerabilities

- ■ CVE-2015-5627 • Yokogawa Multiple Products Buffer Overflow Vulnerabilities - CVE-2015-5627
  2 affected components
- ■ CVE-2020-5609 • Path Traversal Vulnerability in Yokogawa CENTUM
  2 affected components
- 🟥 CVE-2019-10936 • Denial-of-Service Vulnerability in Profinet Devices
  3 affected components
- 🟥 CVE-2017-12741 • Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability
  3 affected components
- 🟥 CVE-2018-16196 • Yokogawa Vnet/IP Open Communication Driver Vulnerabilities
  2 affected components
- 🟥 CVE-2014-0781 • Yokogawa CENTUM 'BKCLogSvr.exe' Heap Based Buffer Overflow...
  2 affected components
- 🟥 CVE-2014-3888 • Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Packet Storm
  2 affected components
- 🟥 CVE-2019-13940 • Uncontrolled Resource Consumption Vulnerability in Siemens SIMATIC S7
  2 affected components
- 🟧 CVE-2017-2680 • Multiple Denial of Service Vulnerabilities on Siemens devices using the...
  3 affected components
- 🟨 CVE-2019-5909 • Yokogawa License Manager Service Vulnerabilities
  2 affected components

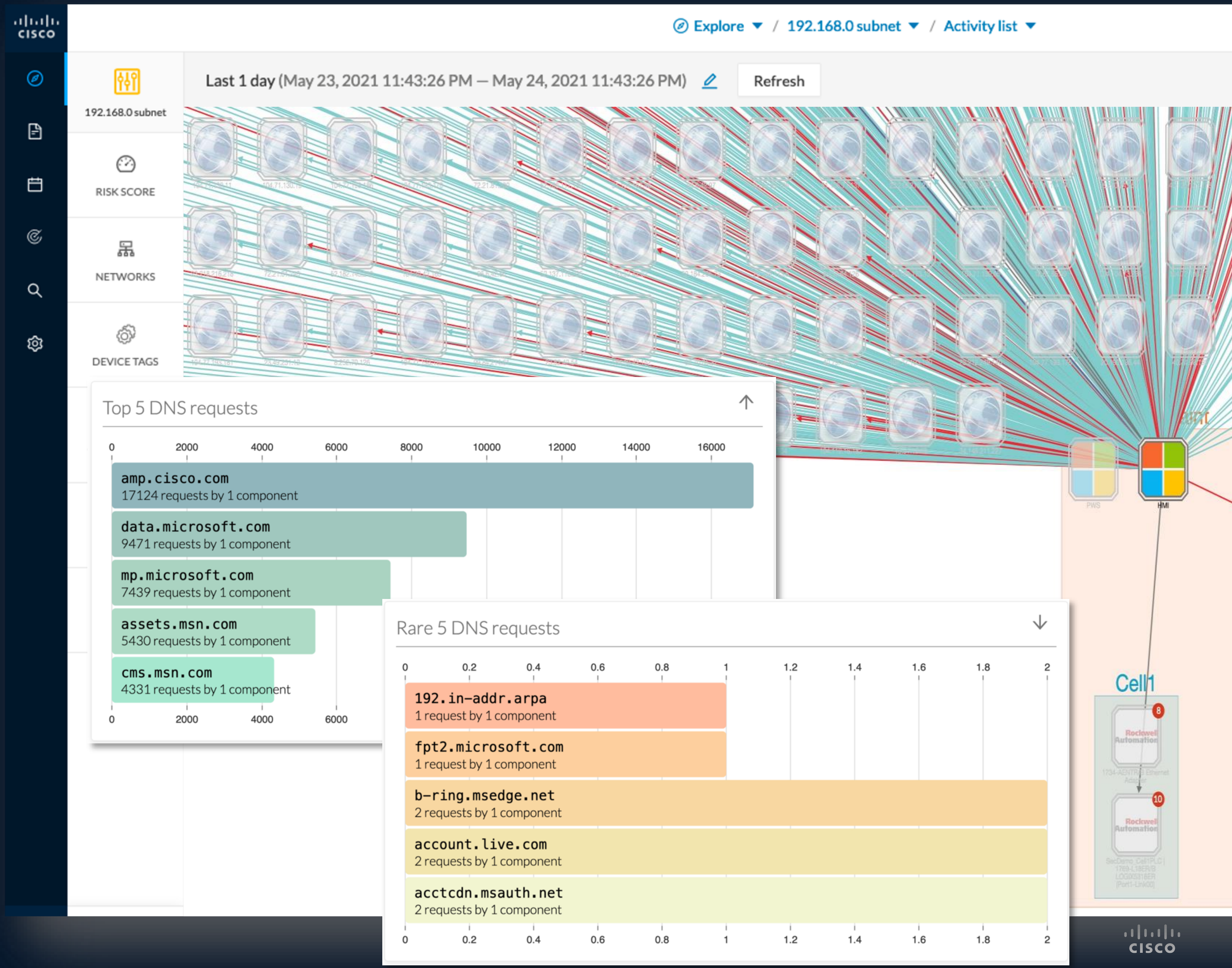
Vulnerability severity legend: 🟩 NONE 🟨 LOW 🟧 MEDIUM 🟥 HIGH ■ CRITICAL

< 1 2

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

Identify & Stop iDMZ Leaks

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



Explore / 192.168.0 subnet / Activity list

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

Refresh

192.168.0 subnet

RISK SCORE

NETWORKS

DEVICE TAGS

Top 5 DNS requests

amp.cisco.com
17124 requests by 1 component

data.microsoft.com
9471 requests by 1 component

mp.microsoft.com
7439 requests by 1 component

assets.msn.com
5430 requests by 1 component

cms.msn.com
4331 requests by 1 component

Rare 5 DNS requests

192.in-addr.arpa
1 request by 1 component

fpt2.microsoft.com
1 request by 1 component

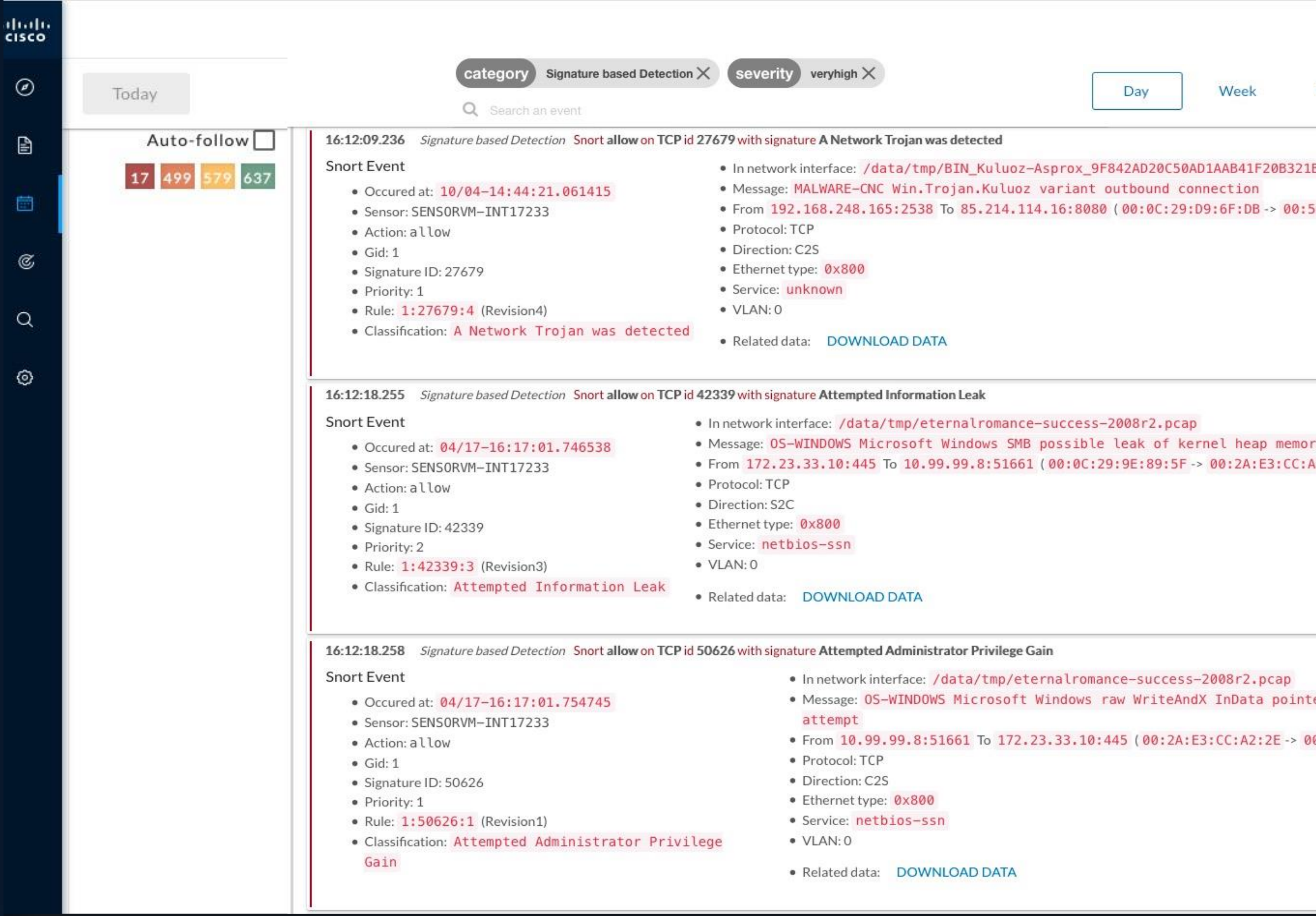
b-ring.msedge.net
2 requests by 1 component

account.live.com
2 requests by 1 component

acctcdn.msauth.net
2 requests by 1 component

Detect Malicious Intrusions

Detect malicious intrusions with Snort IDS and Talos threat intelligence



16:12:09.236 *Signature based Detection* Snort **allow** on TCP id 27679 with signature **A Network Trojan was detected**

Snort Event

- Occured at: `10/04-14:44:21.061415`
- Sensor: SENSORVM-INT17233
- Action: `allow`
- Gid: 1
- Signature ID: 27679
- Priority: 1
- Rule: `1:27679:4` (Revision4)
- Classification: `A Network Trojan was detected`
- In network interface: `/data/tmp/BIN_Kuluoz-Asprox_9F842AD20C50AD1AAB41F20B321E`
- Message: `MALWARE-CNC Win.Trojan.Kuluoz variant outbound connection`
- From `192.168.248.165:2538` To `85.214.114.16:8080` (`00:0C:29:D9:6F:DB` -> `00:5`
- Protocol: TCP
- Direction: C2S
- Ethernet type: `0x800`
- Service: `unknown`
- VLAN: 0
- Related data: DOWNLOAD DATA

16:12:18.255 *Signature based Detection* Snort **allow** on TCP id 42339 with signature **Attempted Information Leak**

Snort Event

- Occured at: `04/17-16:17:01.746538`
- Sensor: SENSORVM-INT17233
- Action: `allow`
- Gid: 1
- Signature ID: 42339
- Priority: 2
- Rule: `1:42339:3` (Revision3)
- Classification: `Attempted Information Leak`
- In network interface: `/data/tmp/eternalromance-success-2008r2.pcap`
- Message: `OS-WINDOWS Microsoft Windows SMB possible leak of kernel heap memor`
- From `172.23.33.10:445` To `10.99.99.8:51661` (`00:0C:29:9E:89:5F` -> `00:2A:E3:CC:A`
- Protocol: TCP
- Direction: S2C
- Ethernet type: `0x800`
- Service: `netbios-ssn`
- VLAN: 0
- Related data: DOWNLOAD DATA

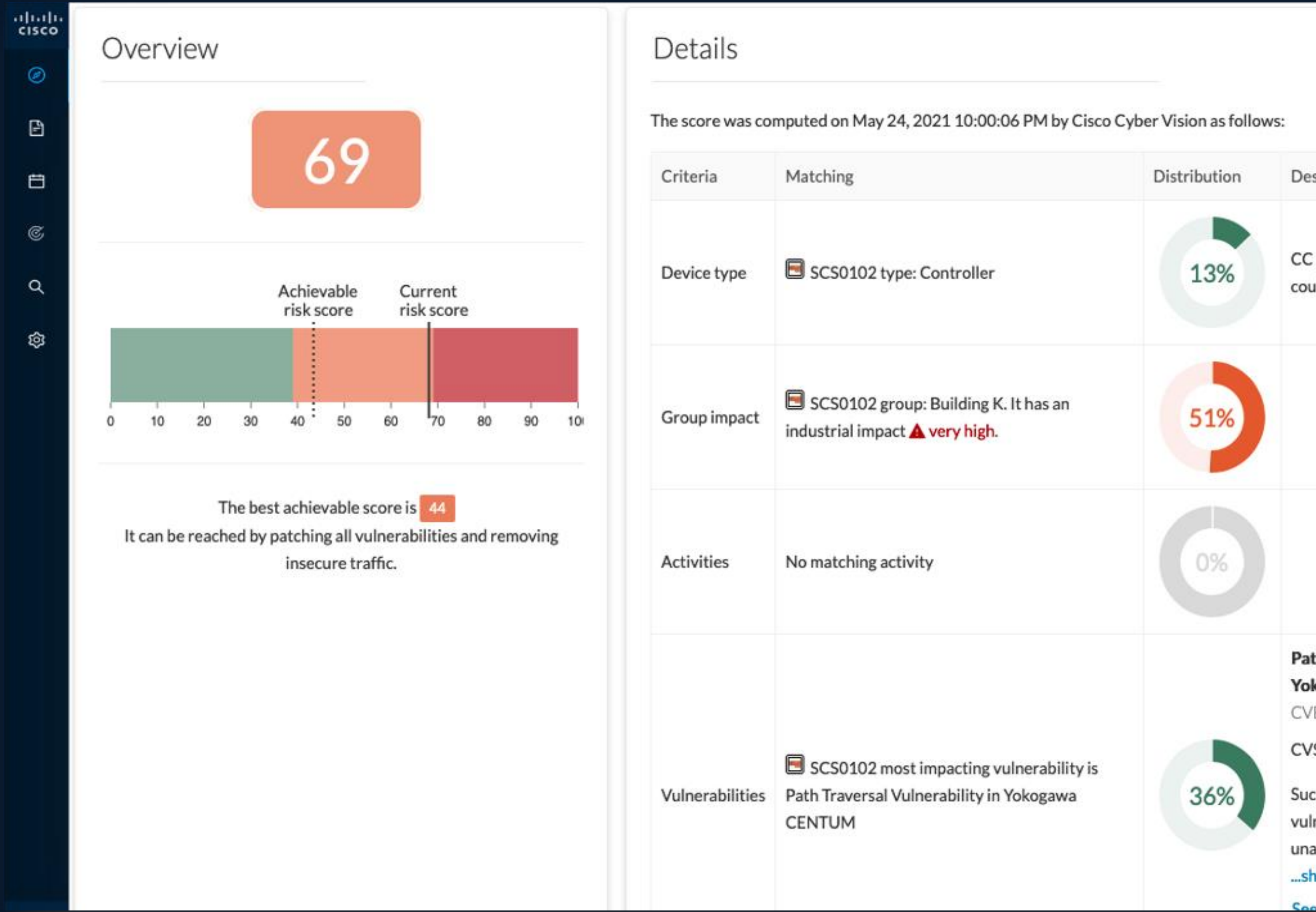
16:12:18.258 *Signature based Detection* Snort **allow** on TCP id 50626 with signature **Attempted Administrator Privilege Gain**

Snort Event

- Occured at: `04/17-16:17:01.754745`
- Sensor: SENSORVM-INT17233
- Action: `allow`
- Gid: 1
- Signature ID: 50626
- Priority: 1
- Rule: `1:50626:1` (Revision1)
- Classification: `Attempted Administrator Privilege Gain`
- In network interface: `/data/tmp/eternalromance-success-2008r2.pcap`
- Message: `OS-WINDOWS Microsoft Windows raw WriteAndX InData pointe attempt`
- From `10.99.99.8:51661` To `172.23.33.10:445` (`00:2A:E3:CC:A2:2E` -> `00`
- Protocol: TCP
- Direction: C2S
- Ethernet type: `0x800`
- Service: `netbios-ssn`
- VLAN: 0
- Related data: DOWNLOAD DATA

Track your Risk Exposure

Asset risk scoring based on impact and likelihood to help you improve compliance



Overview

69

The best achievable score is 44
It can be reached by patching all vulnerabilities and removing insecure traffic.

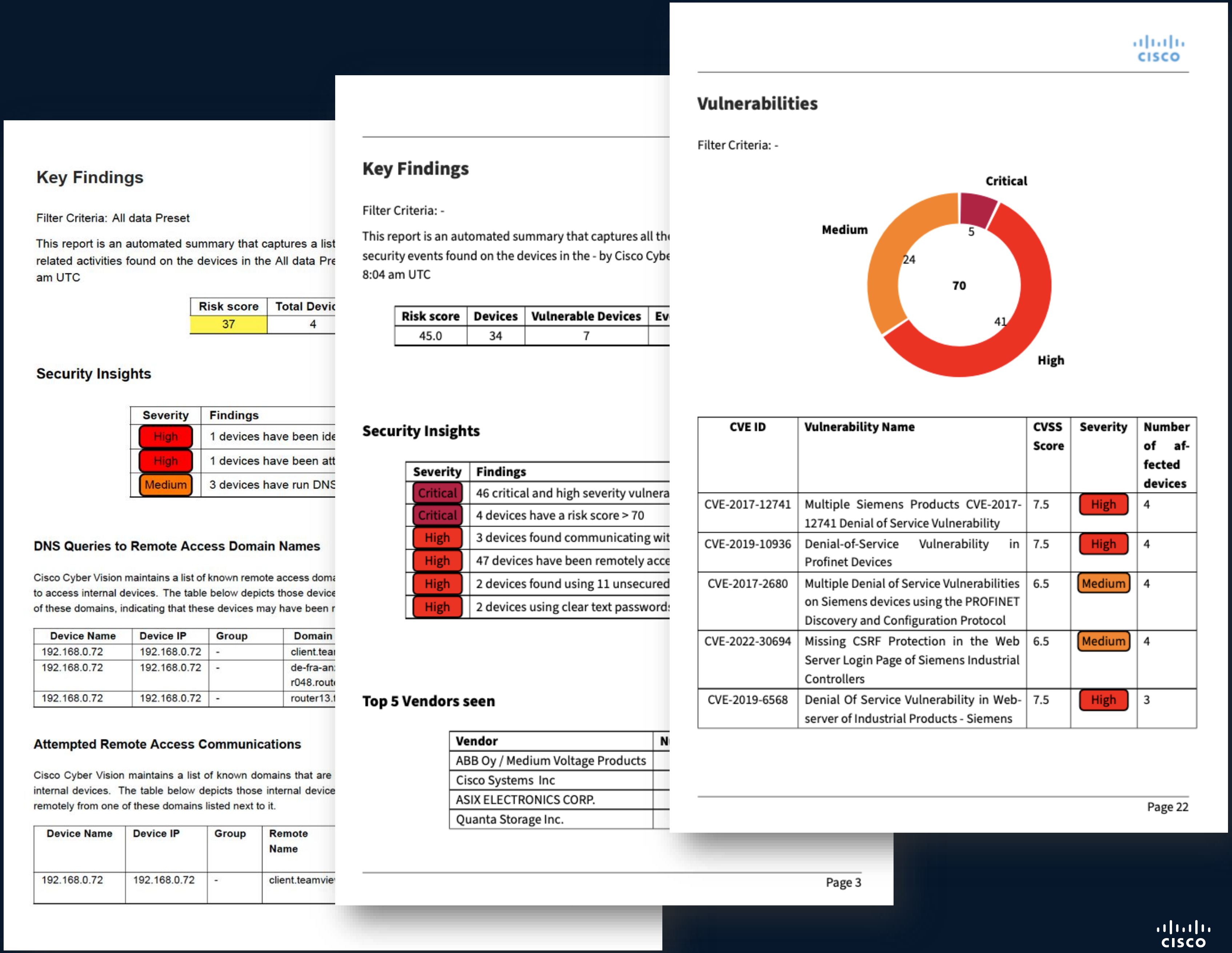
Details

The score was computed on May 24, 2021 10:00:06 PM by Cisco Cyber Vision as follows:

Criteria	Matching	Distribution	Des
Device type	SCS0102 type: Controller	13%	CC cou
Group impact	SCS0102 group: Building K. It has an industrial impact ⚠ very high.	51%	
Activities	No matching activity	0%	
Vulnerabilities	SCS0102 most impacting vulnerability is Path Traversal Vulnerability in Yokogawa CENTUM	36%	Pat Yok CVI CVS Suc vul una ...sh See

Measure Progress with Reports

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



Key Findings

Filter Criteria: All data Preset

This report is an automated summary that captures a list
related activities found on the devices in the All data Pre
am UTC

Risk score	Total Devic
37	4

Security Insights

Severity	Findings
High	1 devices have been ide
High	1 devices have been att
Medium	3 devices have run DNS

DNS Queries to Remote Access Domain Names

Cisco Cyber Vision maintains a list of known remote access doma
to access internal devices. The table below depicts those device
of these domains, indicating that these devices may have been r

Device Name	Device IP	Group	Domain
192.168.0.72	192.168.0.72	-	client.tear
192.168.0.72	192.168.0.72	-	de-fra-an: r048.rout
192.168.0.72	192.168.0.72	-	router13.t

Attempted Remote Access Communications

Cisco Cyber Vision maintains a list of known domains that are
internal devices. The table below depicts those internal device
remotely from one of these domains listed next to it.

Device Name	Device IP	Group	Remote Name
192.168.0.72	192.168.0.72	-	client.teamvie

Key Findings

Filter Criteria: -

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

Risk score	Devices	Vulnerable Devices	Ev
45.0	34	7	

Security Insights

Severity	Findings
Critical	46 critical and high severity vulnera
Critical	4 devices have a risk score > 70
High	3 devices found communicating wit
High	47 devices have been remotely acce
High	2 devices found using 11 unsecured
High	2 devices using clear text password

Top 5 Vendors seen

Vendor	N
ABB Oy / Medium Voltage Products	
Cisco Systems Inc	
ASIX ELECTRONICS CORP.	
Quanta Storage Inc.	

Page 3

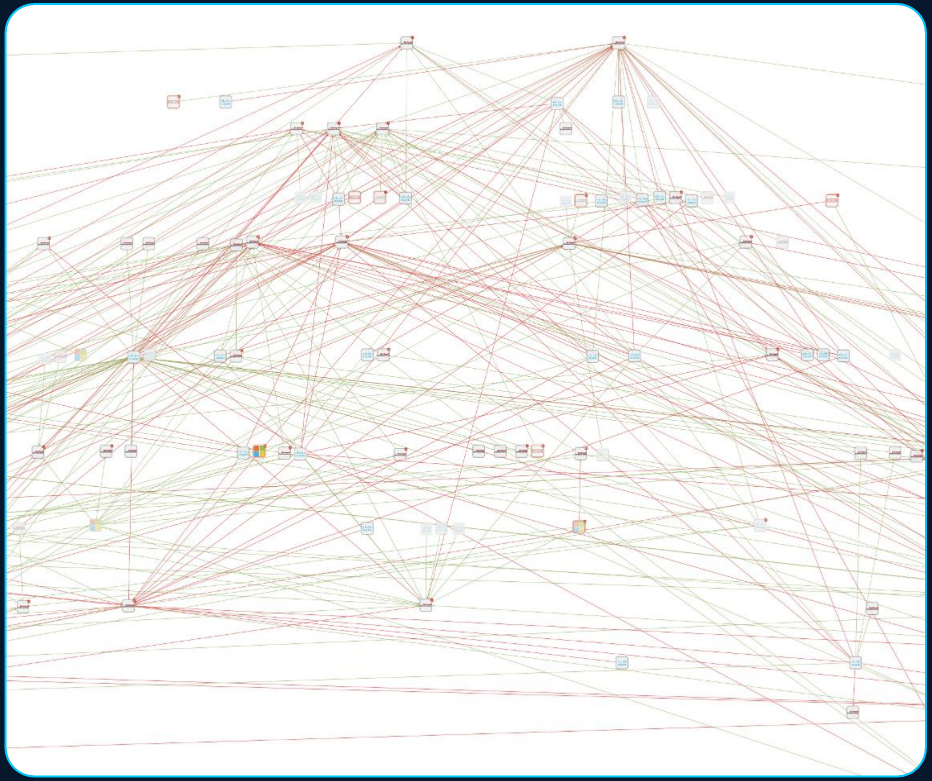
Vulnerabilities

Filter Criteria: -

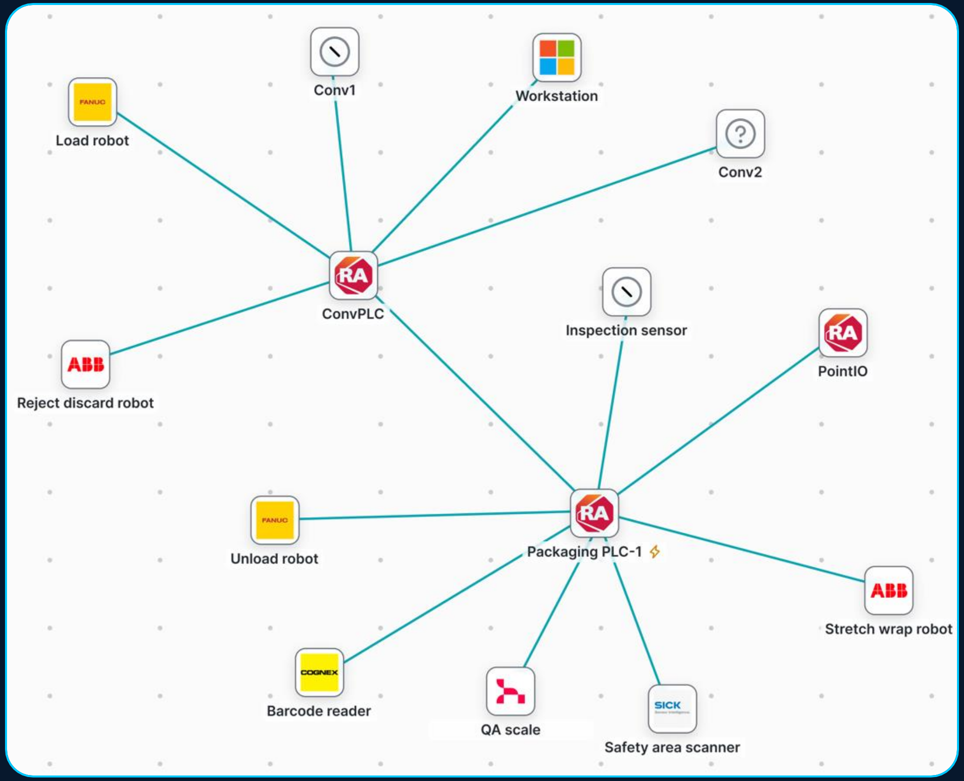
CVE ID	Vulnerability Name	CVSS Score	Severity	Number of affected devices
CVE-2017-12741	Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability	7.5	High	4
CVE-2019-10936	Denial-of-Service Vulnerability in Profinet Devices	7.5	High	4
CVE-2017-2680	Multiple Denial of Service Vulnerabilities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

Page 22

Use AI to streamline network segmentation and protect operations

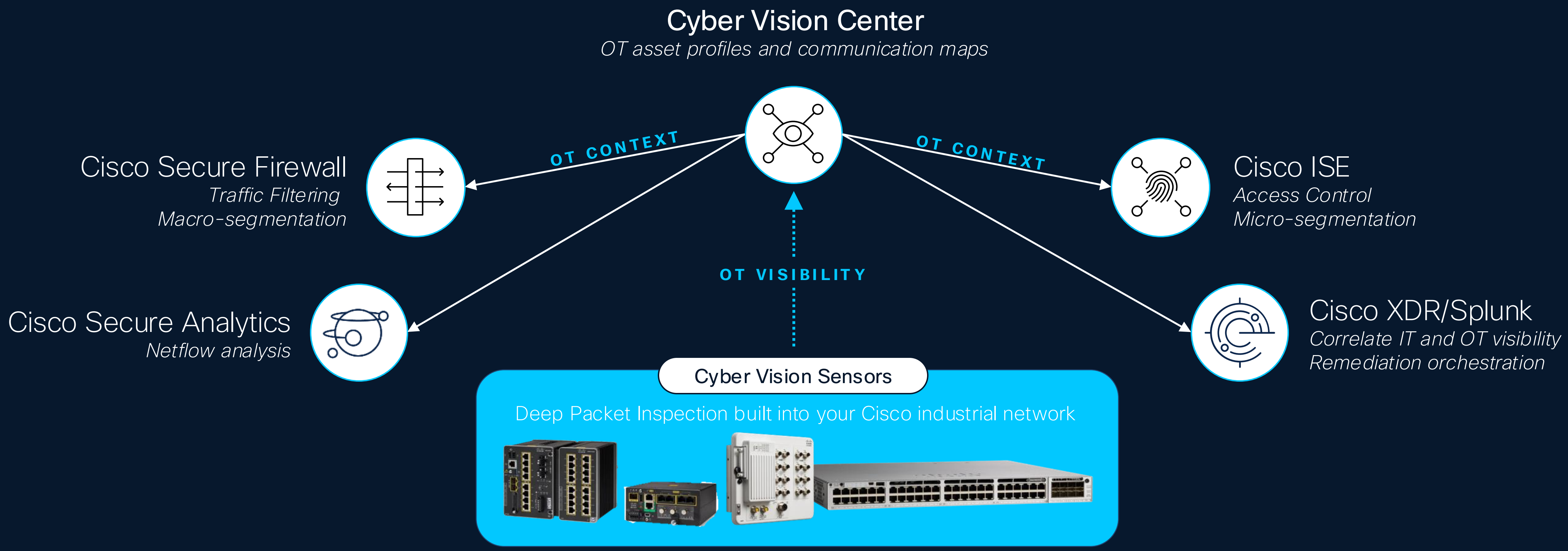


OT asset inventory projects highlight flat, unsegmented networks



Cyber Vision AI-based clustering automatically creates security zones to drive network segmentation using Firewalls or NAC

Cyber Vision extends IT security to your industrial settings



Cyber Vision Center
OT asset profiles and communication maps

OT CONTEXT

OT CONTEXT

OT VISIBILITY

Cisco Secure Firewall
Traffic Filtering
Macro-segmentation

Cisco Secure Analytics
Netflow analysis

Cisco ISE
Access Control
Micro-segmentation

Cisco XDR/Splunk
Correlate IT and OT visibility
Remediation orchestration

Cyber Vision Sensors

Deep Packet Inspection built into your Cisco industrial network

OT context and insights that are foundational to using IT security tools to secure industrial networks

Agenda

01 Les enjeux cyber dans l'OT

02 Etapes de sécurisation des réseaux OT

03 Visibilité : Cisco Cyber Vision

04 Segmentation : ISE & FMC

05 Gestion des accès distant : SEA

06 Surveillance et répons à incident : Splunk

07 Cas clients

Step #2: Network Segmentation

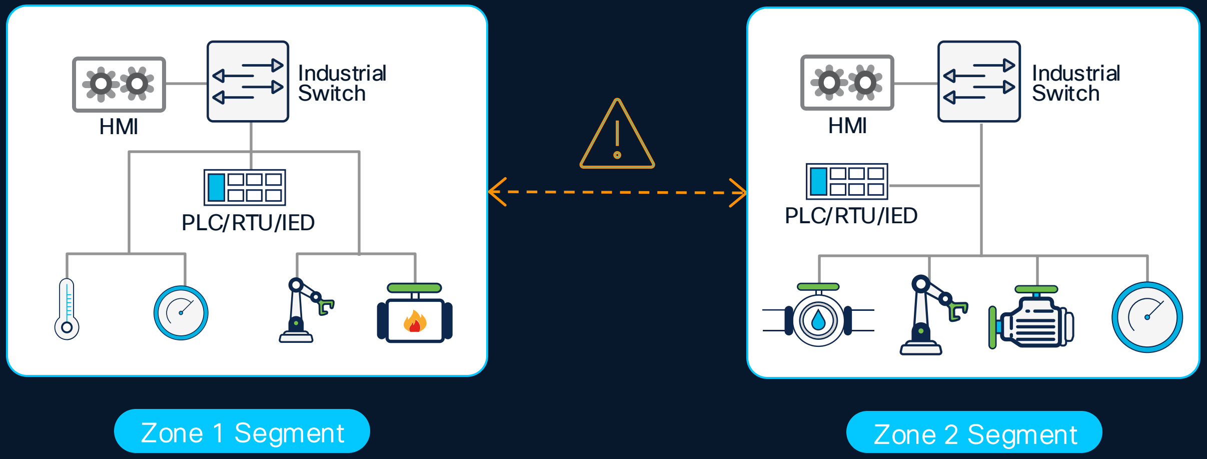
Understand the OT security posture with OT visibility

Limit blast radius with network segmentation

Control risks from remote access to OT assets

Monitor OT networks in the SOC

Preventative measures are required to protect OT networks, not just visibility



⚠ Malware can easily spread through the entire OT network

⚠ An attacker only needs to exploit one of many vulnerabilities to cause serious damage

⚠ Implementing access control can cause downtime due to legitimate process flows getting blocked

First identify what the scope of segmentation is

Use Case #1
Protect the IT / OT Boundary

If the IT network is exploited, there should be no direct path to the critical network

Use the Cisco Secure Firewall to control traffic between IT and OT

Use Case #2
Protect OT from the Industrial Data Center

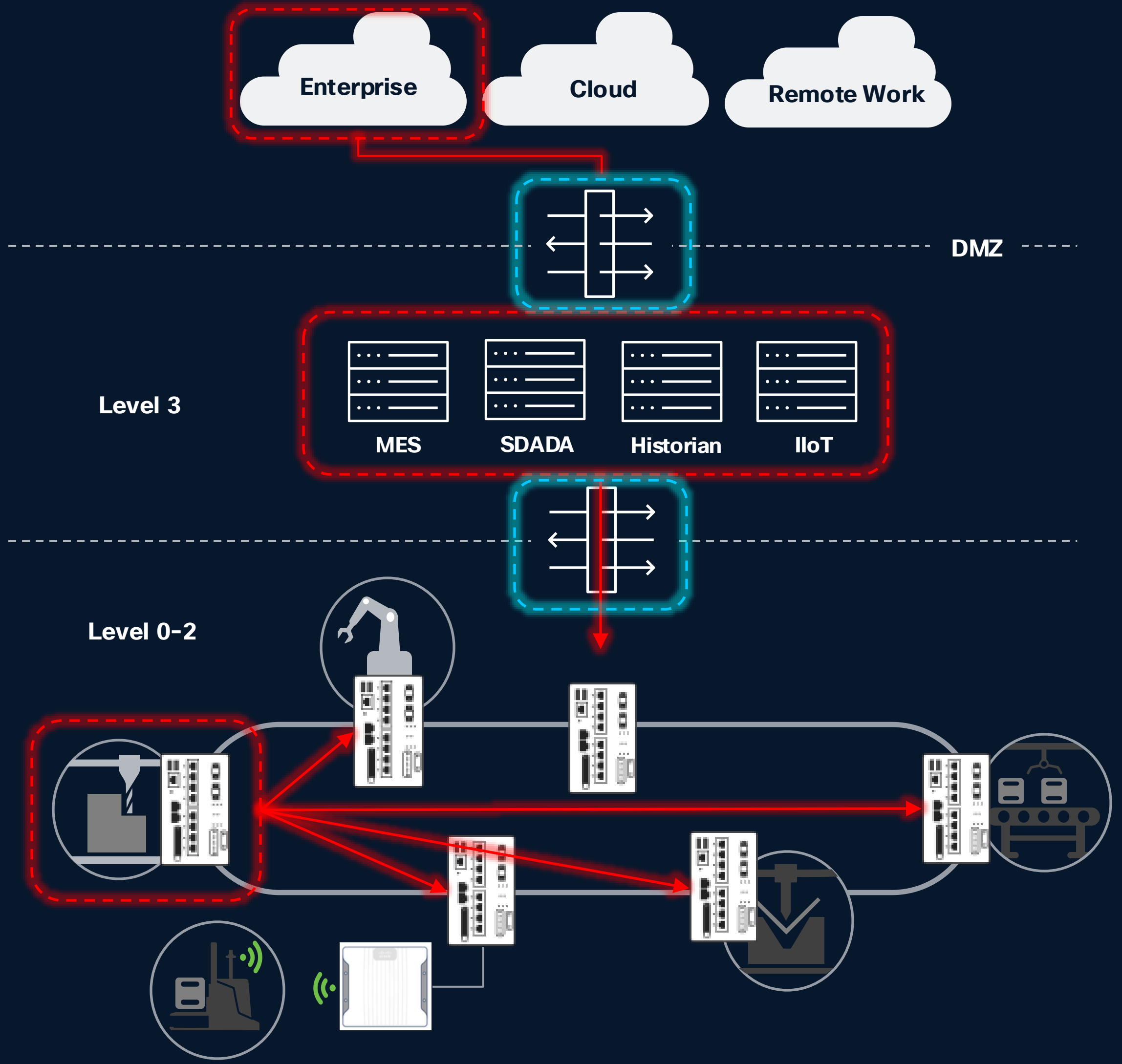
Rising AI investments have expanded the IDC and introduced more ways for attackers to gain a foothold to the network.

Use the Cisco Secure Firewall to protect the OT network from the IDC

Use Case #3
Prevent Lateral Movement in the Control Network

If one process zone is compromised, others should continue to run without interruption.

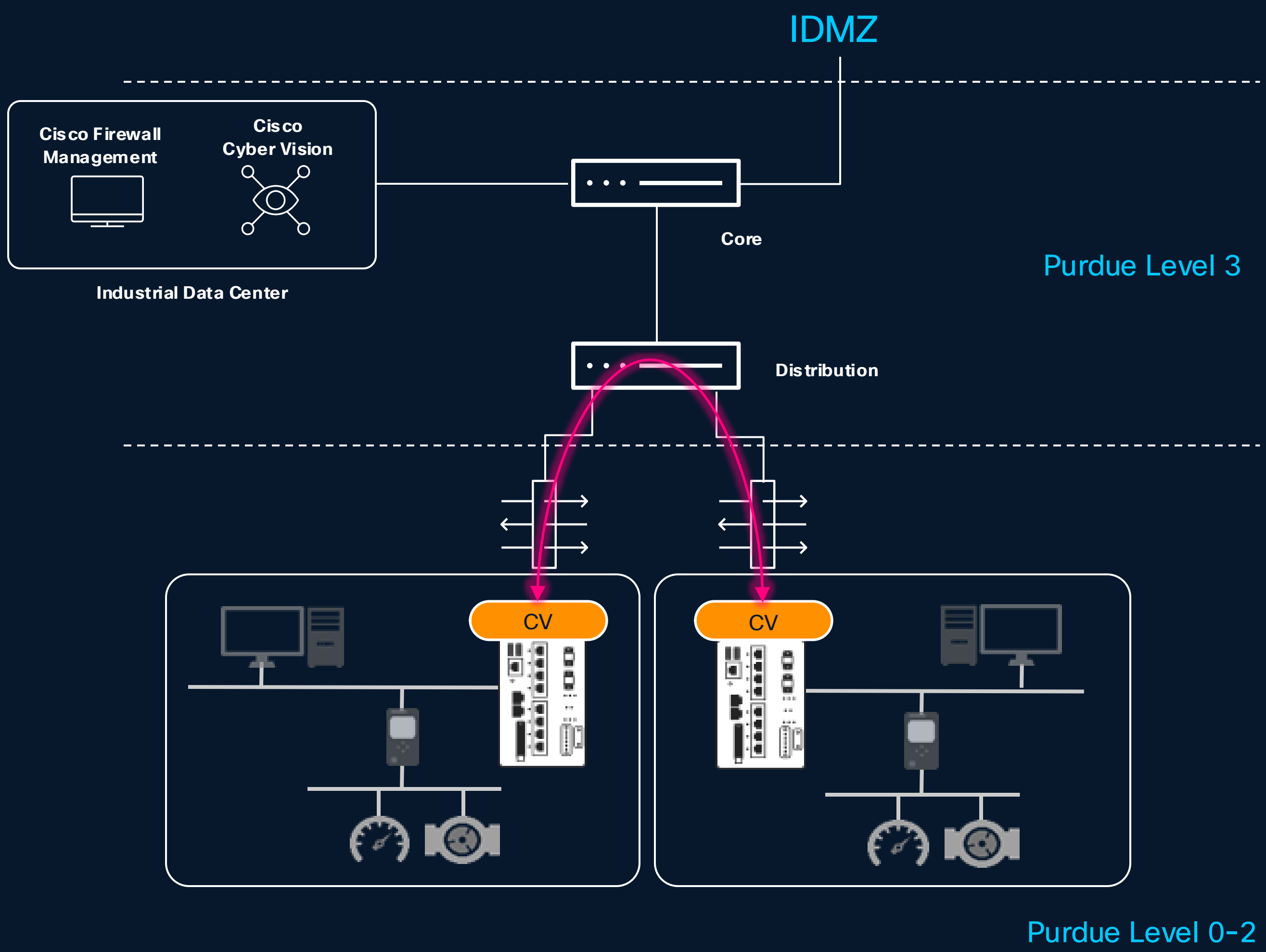
Use Cisco Identity Services Engine and go on the journey to Zero Trust for OT



Securing Plant Networks with Cisco Secure Firewall

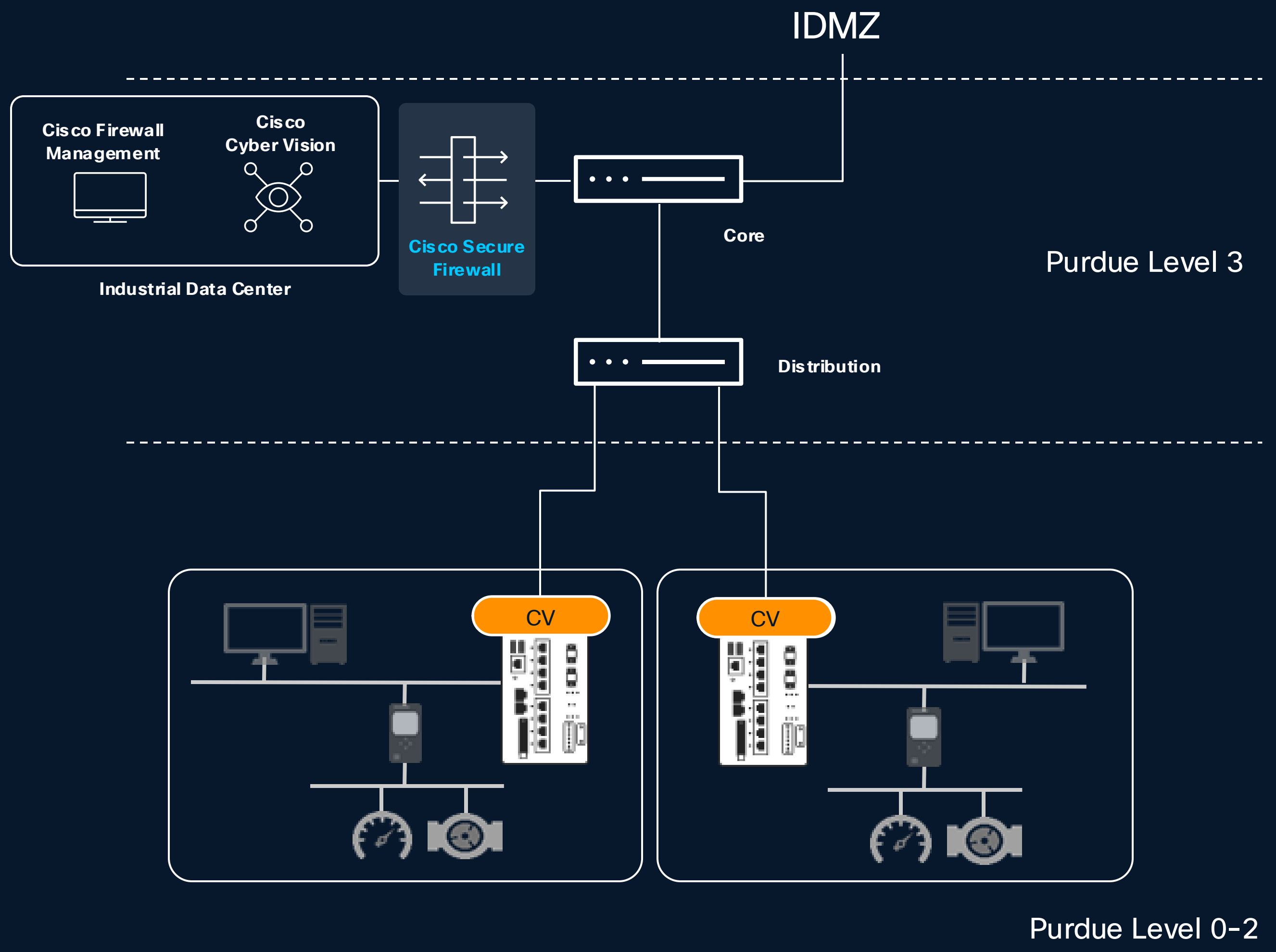
Common OT firewall mistake

Placing firewalls at the edge of every process zone



- If I have 200 cell/area zones, that means 200 new firewalls
  - More hardware to manage
  - More policies to manage
  - Patch management
  - …
- Interzone communication means traffic must flow through two separate firewalls which adds unnecessary latency, especially if traffic is subject to an IPS
- Rugged firewalls are best suited to Intra-zone communication, for once off use cases, and only if advanced protection features are required

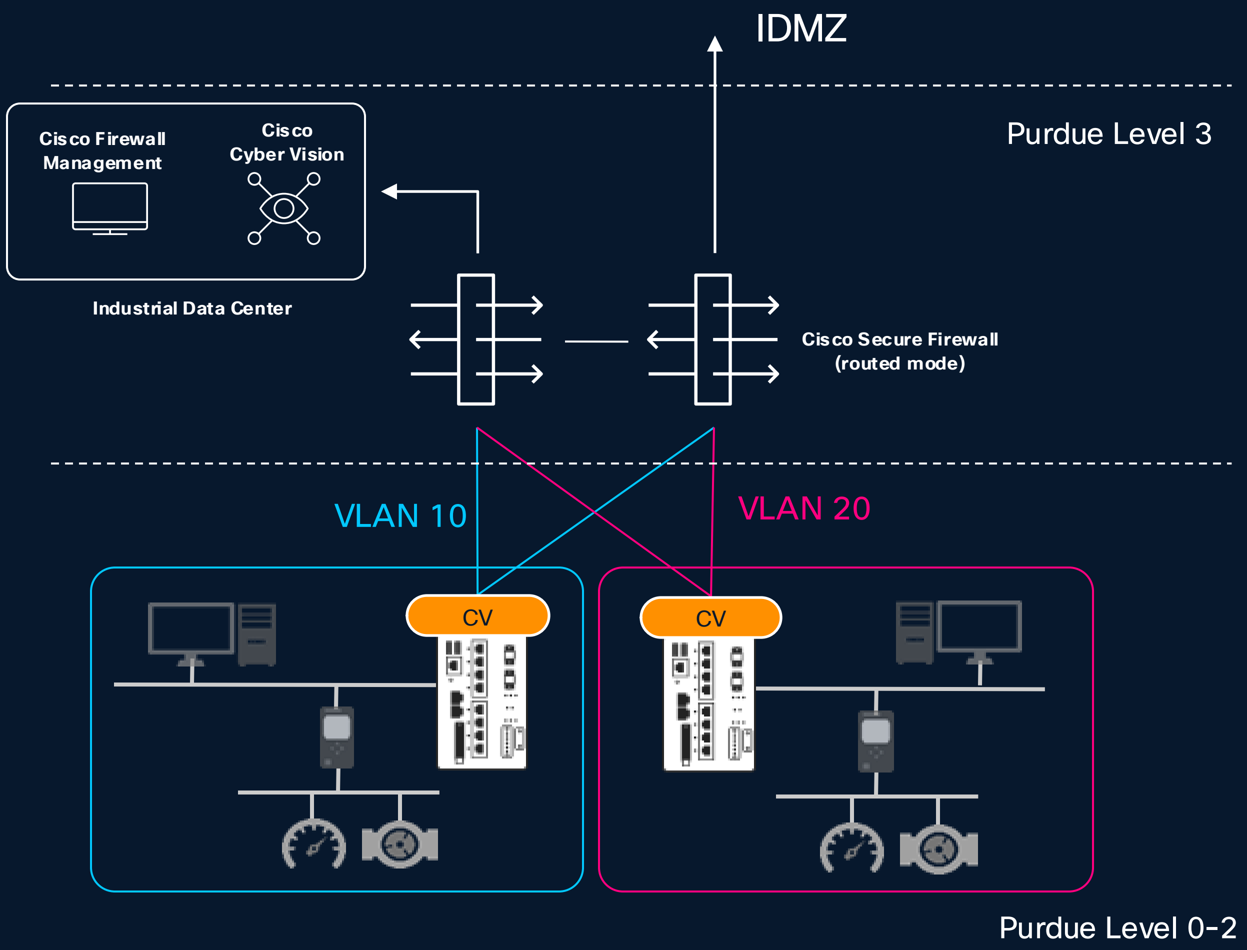
Better approach to OT firewall #1
Cisco Secure Firewall at the industrial data center



- Industrial Data Center (IDC) typically resides below DMZ firewall, meaning no protection between it and the plant floor
- IDC may be exposed to the Internet for modern applications, increasing its attack surface
- Workloads are being moved from the cell/area zones to the IDC, meaning critical traffic will flow back and forth
- It is critical we provide a security barrier between the virtual workloads and the physical devices

Better approach to OT firewall #2

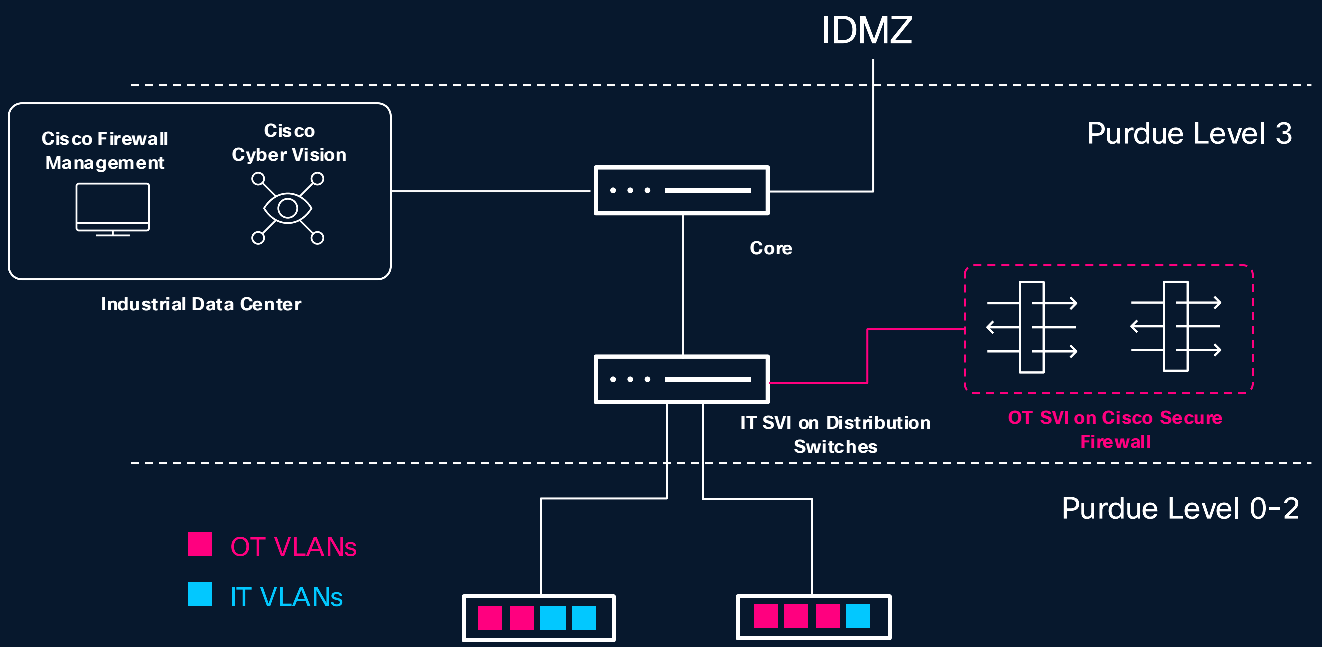
Cisco Secure Firewall as routing point for the OT network



- VLANs are often overlooked for security because by themselves they offer little protection
- Use a firewall to route between VLANs so all routed traffic is subject to firewall enforcement
- Enables you to place a small cluster of firewalls to protect a full plant instead of a unique firewall per zone

Better approach to OT firewall #3

Only terminate critical VLANs at the firewall

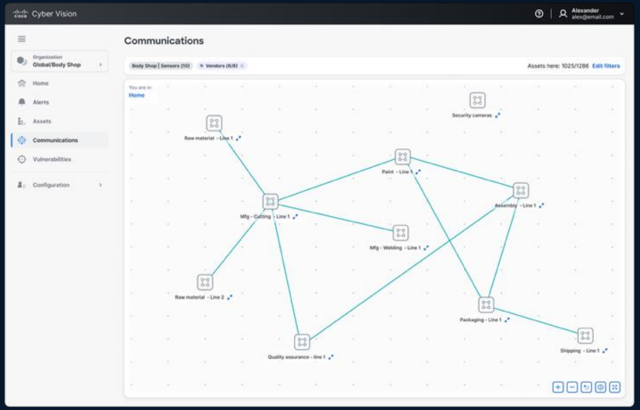


- Many manufacturing plants have a mix of OT and IT / non-critical VLANs within an environment
- Not all traffic needs to traverse a firewall
- Dedicate firewalls for protection of OT assets
- Main goal is to reduce the blast radius. If one zone is compromised, our goal is to limit downtime to that one zone

Enhancing firewall policies with OT context from Cyber Vision

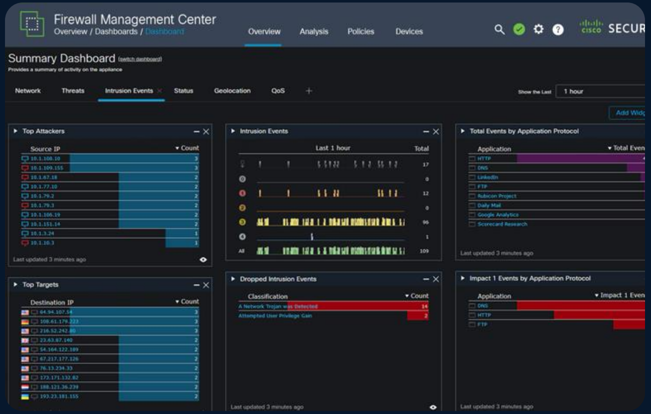
OT

Grouping assets in Cyber Vision



CSDAC

Creates Dynamic Attributes in FMC



Source IP	Count
10.1.108.10	3
10.1.109.155	3
10.1.67.18	2
10.1.77.10	2
10.1.79.2	2
10.1.79.3	2
10.1.106.19	2
10.1.151.14	2
10.1.3.24	1
10.1.10.3	1

	Total
	17
	0
	12
	0
	96
	1
All	109

Destination IP	Count
64.94.107.54	3
108.61.179.223	3
216.52.242.80	3
23.63.87.140	2
54.164.122.189	2
67.217.177.126	2
76.13.234.33	2
173.171.132.82	2
188.121.36.239	2
193.23.181.155	2

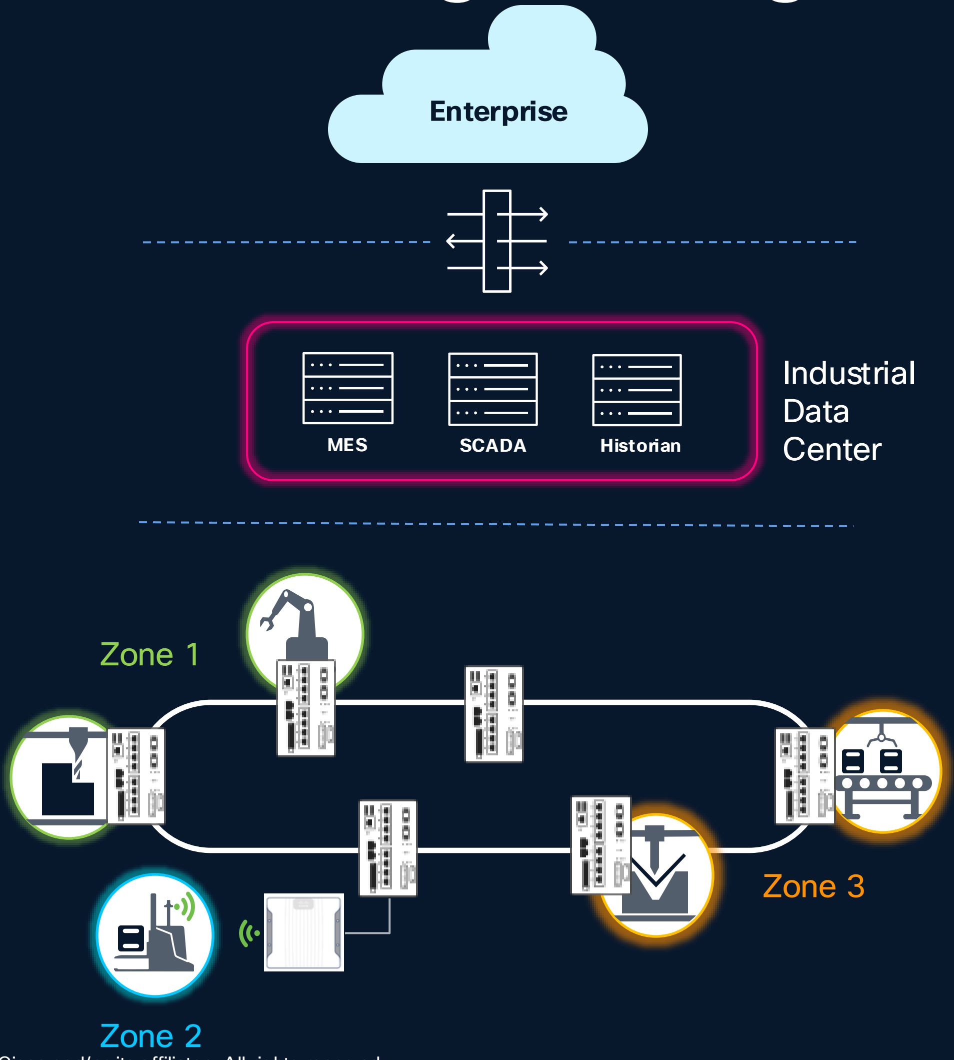
Classification	Count
A Network Trojan was Detected	14
Attempted User Privilege Gain	2

Policies enforced by Cisco Secure Firewall

Zero downtime with OT controlled adaptive firewall rules

Securing Plant Networks with Cisco Identity Services Engine

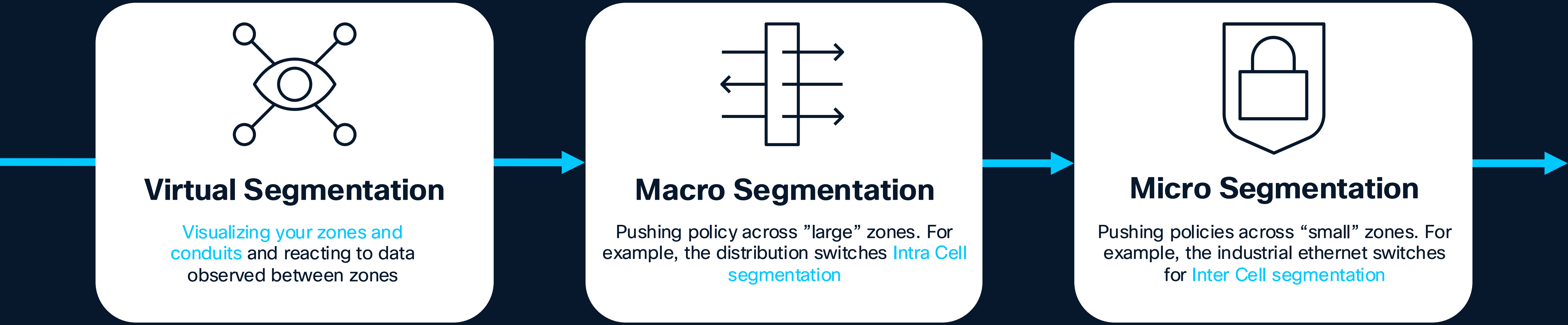
Organizations are adopting the IEC62443 Zones & Conduits Model for segmenting their OT network



- Zones represent a group of devices on based on functional, logical or physical relationships
- Conduits represent the networking equipment used to communicate across zones

The intent is to move from one flat OT network to multiple small OT networks with security controls in between

A journey to implementing micro segmentation in OT



Virtual Segmentation

Visualizing your zones and conduits and reacting to data observed between zones

Macro Segmentation

Pushing policy across ”large” zones. For example, the distribution switches Intra Cell segmentation

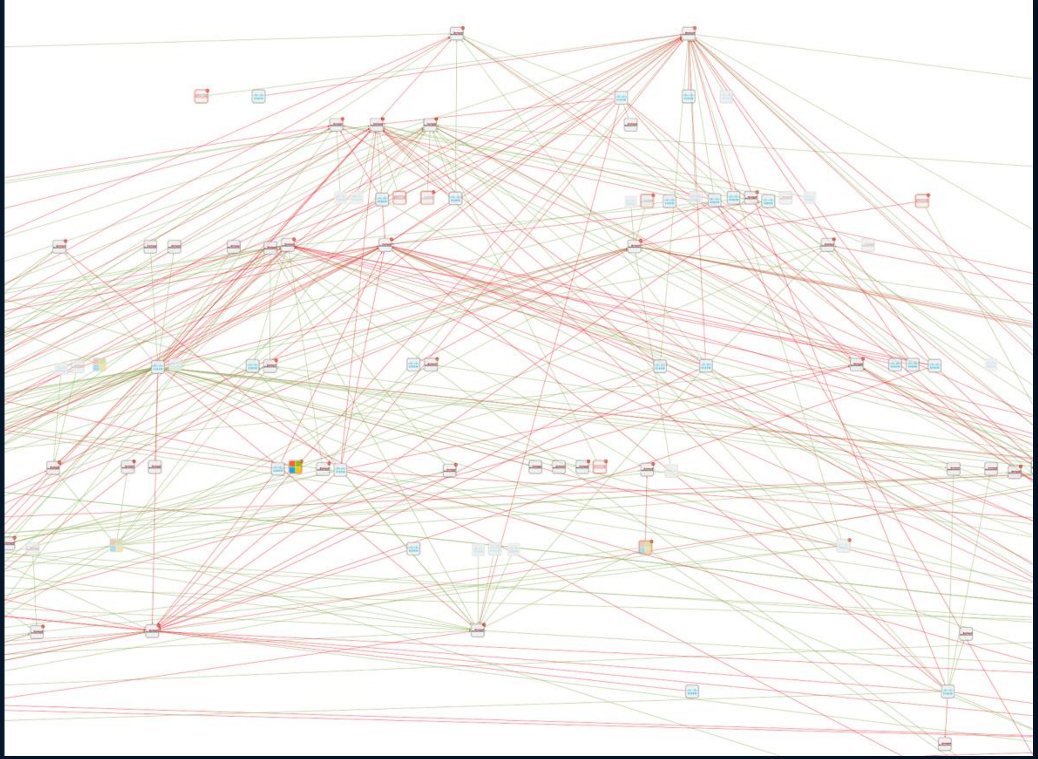
Micro Segmentation

Pushing policies across “small” zones. For example, the industrial ethernet switches for Inter Cell segmentation

A micro segmentation project should never start with micro segmentation. Start with macro and do micro segmentation one zone at a time!

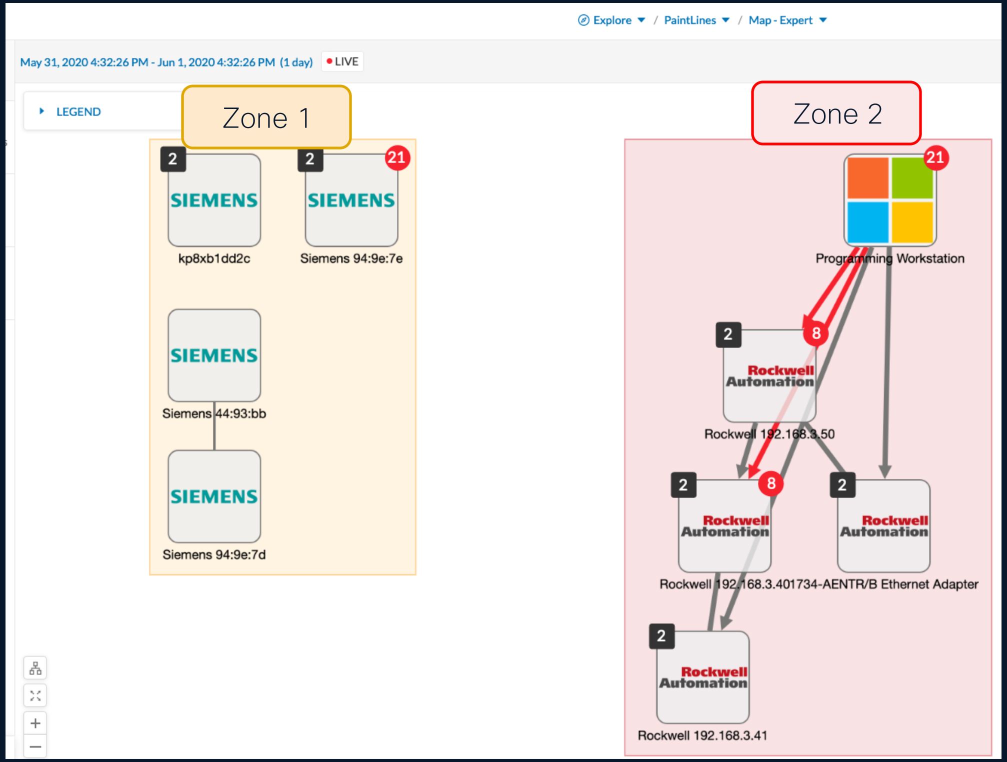
First build your Zones & Conduits in Cyber Vision...

Cyber Vision discovers OT assets...



OT asset inventory projects highlight flat, unsegmented networks

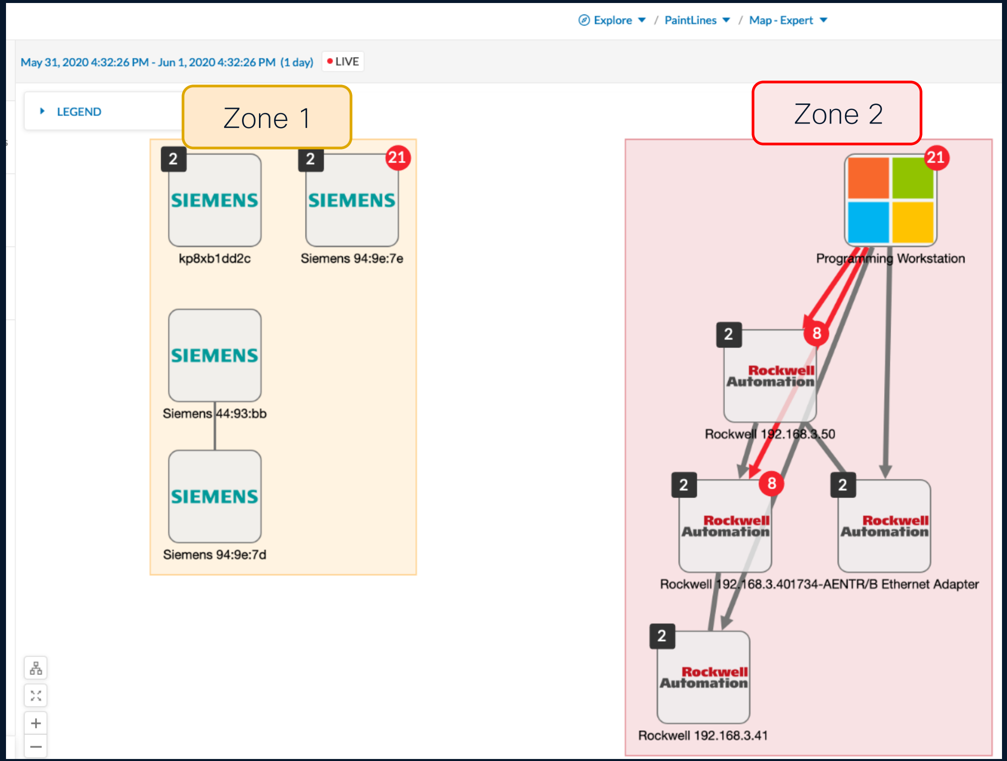
...and groups them into logical zones...

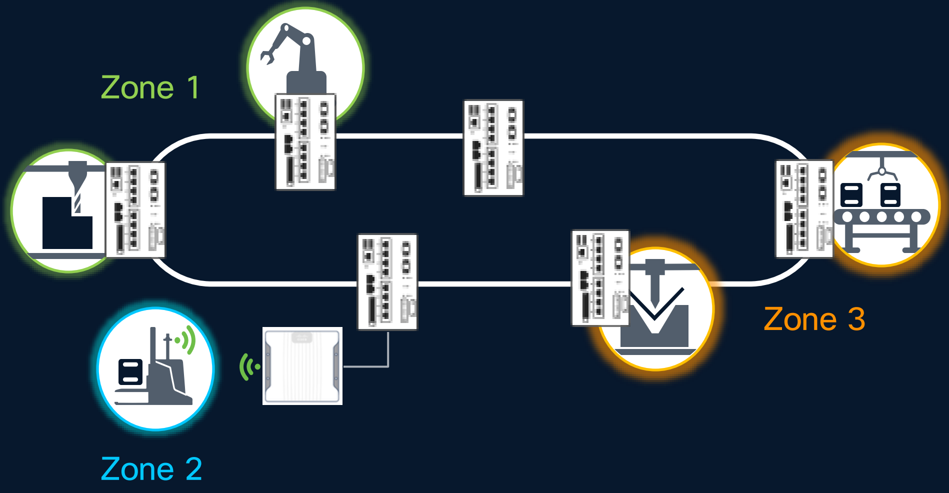


Cyber Vision helps OT teams document security zones to drive segmentation

Securing Plant Networks with Cisco Identity Services Engine

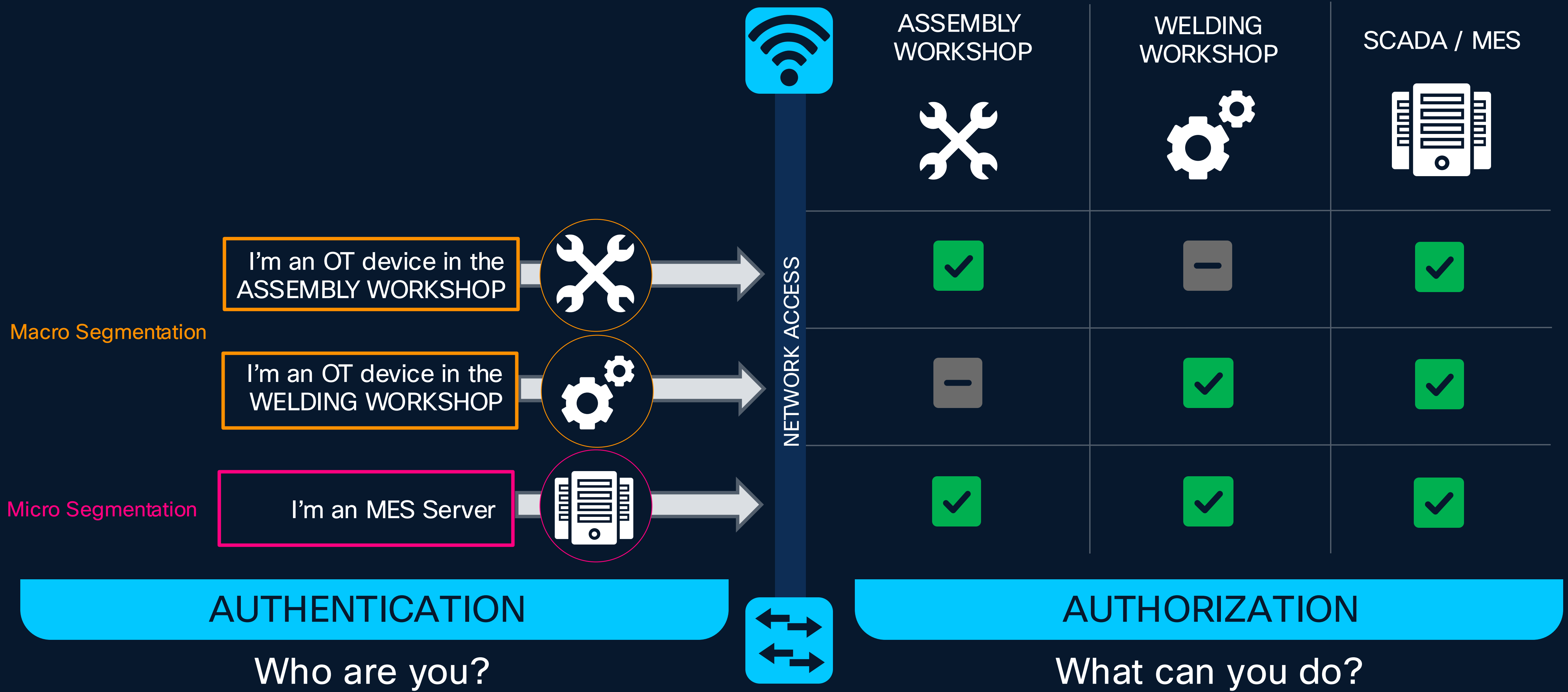
.... then push policy back into the network





Adaptive segmentation enforced by IT, controlled by OT

Cisco TrustSec – Hybrid Macro / Micro Segmentation



Macro Segmentation

Micro Segmentation

	ASSEMBLY WORKSHOP	WELDING WORKSHOP	SCADA / MES
I'm an OT device in the ASSEMBLY WORKSHOP	✓	–	✓
I'm an OT device in the WELDING WORKSHOP	–	✓	✓
I'm an MES Server	✓	✓	✓

AUTHENTICATION

Who are you?

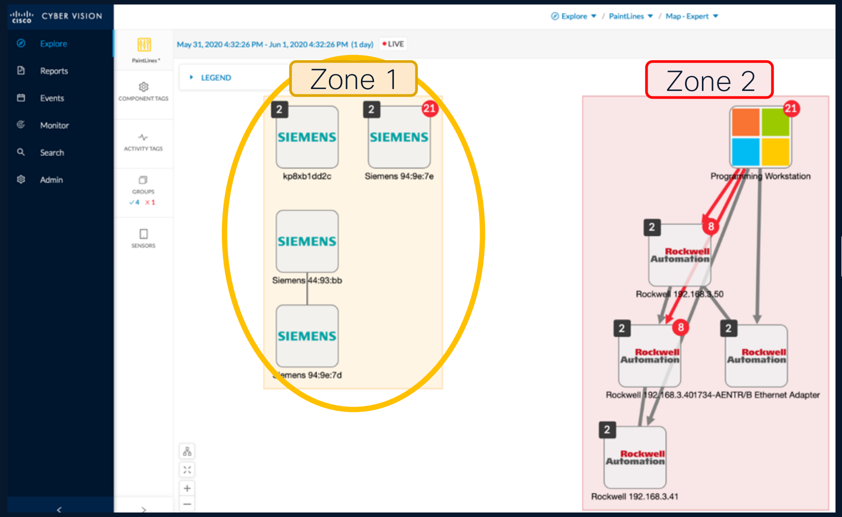
AUTHORIZATION

What can you do?

Segmentation driven by OT Context from Cyber Vision

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

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



Cisco Cyber Vision Map View

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

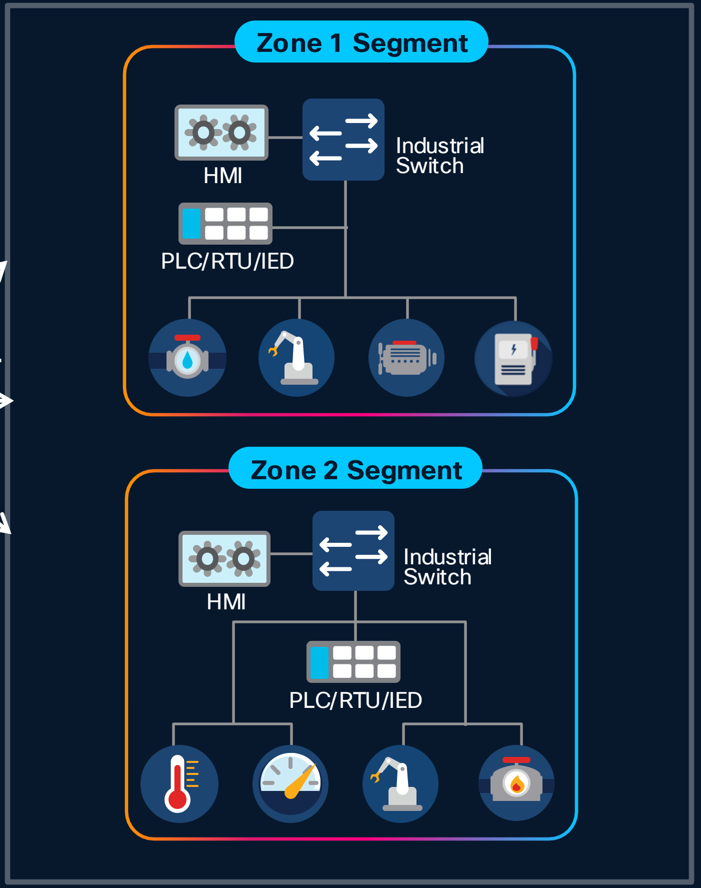
Cisco ISE Policy Matrix

dACL

SGT

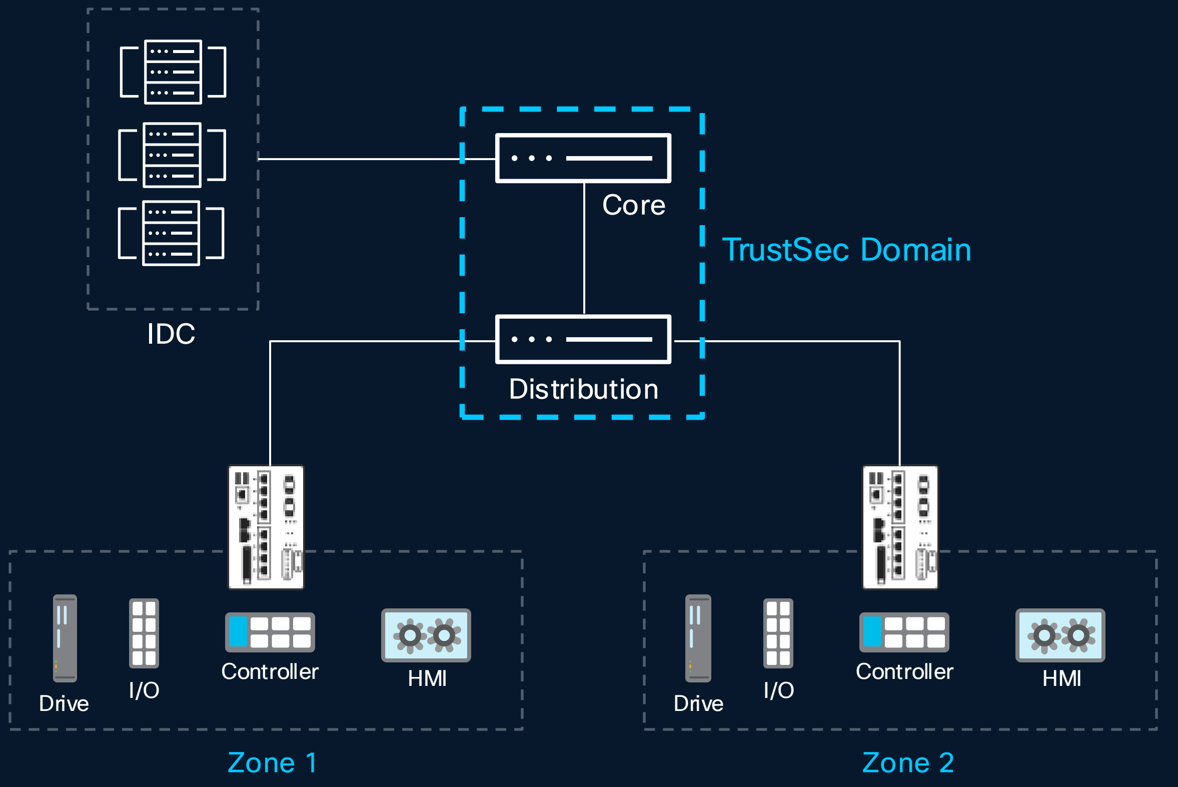
VLAN

Segmentation of industrial network



Debunking TrustSec myths

A full Cisco network is NOT required for TrustSec



- The TrustSec domain will act as the conduit between zones
- All traffic within a zone is free to communicate
- Use Cyber Vision to gain visibility inside the zone
- Use ISE to control traffic between zones

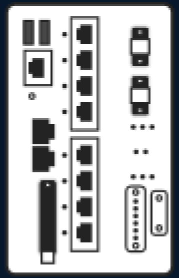
Just because a network can do micro segmentation does not mean you should turn it on immediately

What Devices Support SGT Enforcement?

Enforcement Nodes: Can actively block traffic

Catalyst Switches

Typically used at the distribution & core

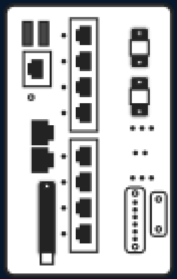


NEW

IE3500, IE3400, IE9300

Typically used at access & aggregation

SXP Speakers: Can share IP to SGT information over SXP but cannot enforce traffic. Used for authentication, not for enforcement



- IE3300
- IE3200
- IE3100
- IE2000

Agenda

01 Les enjeux cyber dans l’OT

02 Etapes de sécurisation des réseaux OT

03 Visibilité : Cisco Cyber Vision

04 Segmentation : ISE & FMC

05 Gestion des accès distant : SEA

06 Surveillance et répons à incident : Splunk

07 Cas clients

Step #3: Secure Remote Access

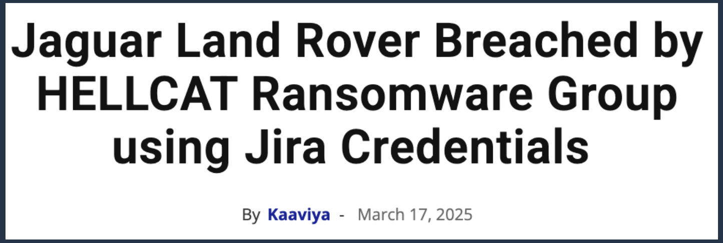
Understand the OT security posture with OT visibility

Limit blast radius with network segmentation

Control risks from remote access to OT assets

Monitor OT networks in the SOC

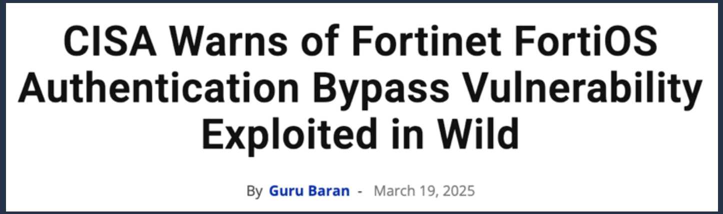
Unsecure OT remote access is a major threat to industrial operations



Jaguar Land Rover Breached by HELLCAT Ransomware Group using Jira Credentials

By **Kaaviya** - March 17, 2025

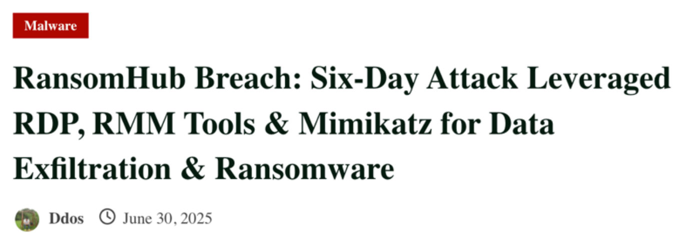
Credential abuse and **social engineering** is the most common way to breach a network



CISA Warns of Fortinet FortiOS Authentication Bypass Vulnerability Exploited in Wild

By **Guru Baran** - March 19, 2025

Vulnerability exploits on edge infrastructure is on the rise. Anything with a public IP address will be attacked.



Malware

RansomHub Breach: Six-Day Attack Leveraged RDP, RMM Tools & Mimikatz for Data Exfiltration & Ransomware

Ddos June 30, 2025

Traditional remote access gateways do not stop the **risk of lateral movement**

OT remote access options are either security backdoors or come with many trade-offs

Ad-Hoc Software

Often installed on operator workstations

Backdoor to IT security policies

Cellular Gateways

Dedicated hardware installed by machine builders

Backdoor to IT security policies

VPN

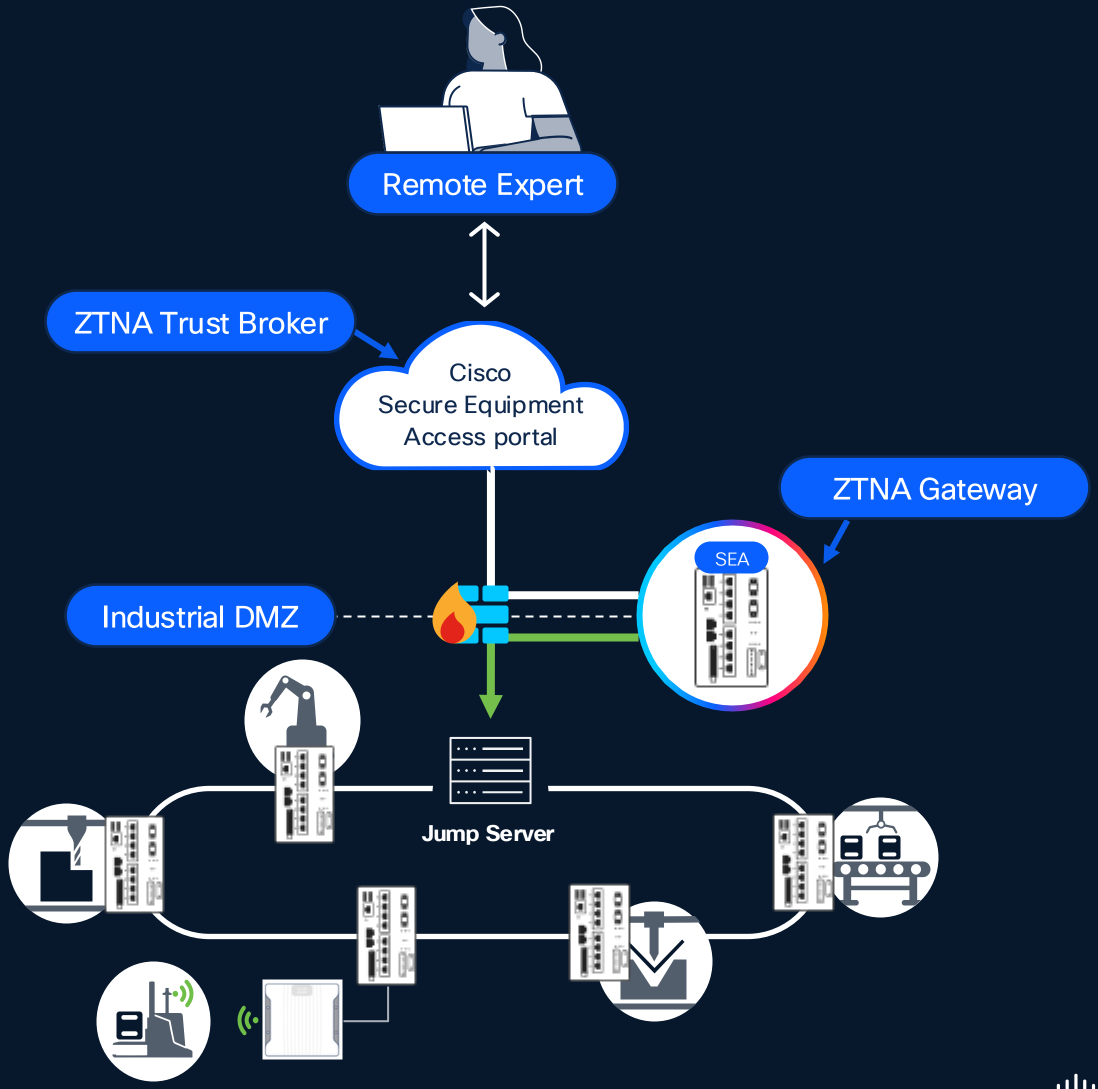
Always-On,
All-or-Nothing access

Need additional controls to deny full network access

Enhance existing Jump Servers with Zero-Trust

Supercharge your existing remote access setup with modern security capabilities

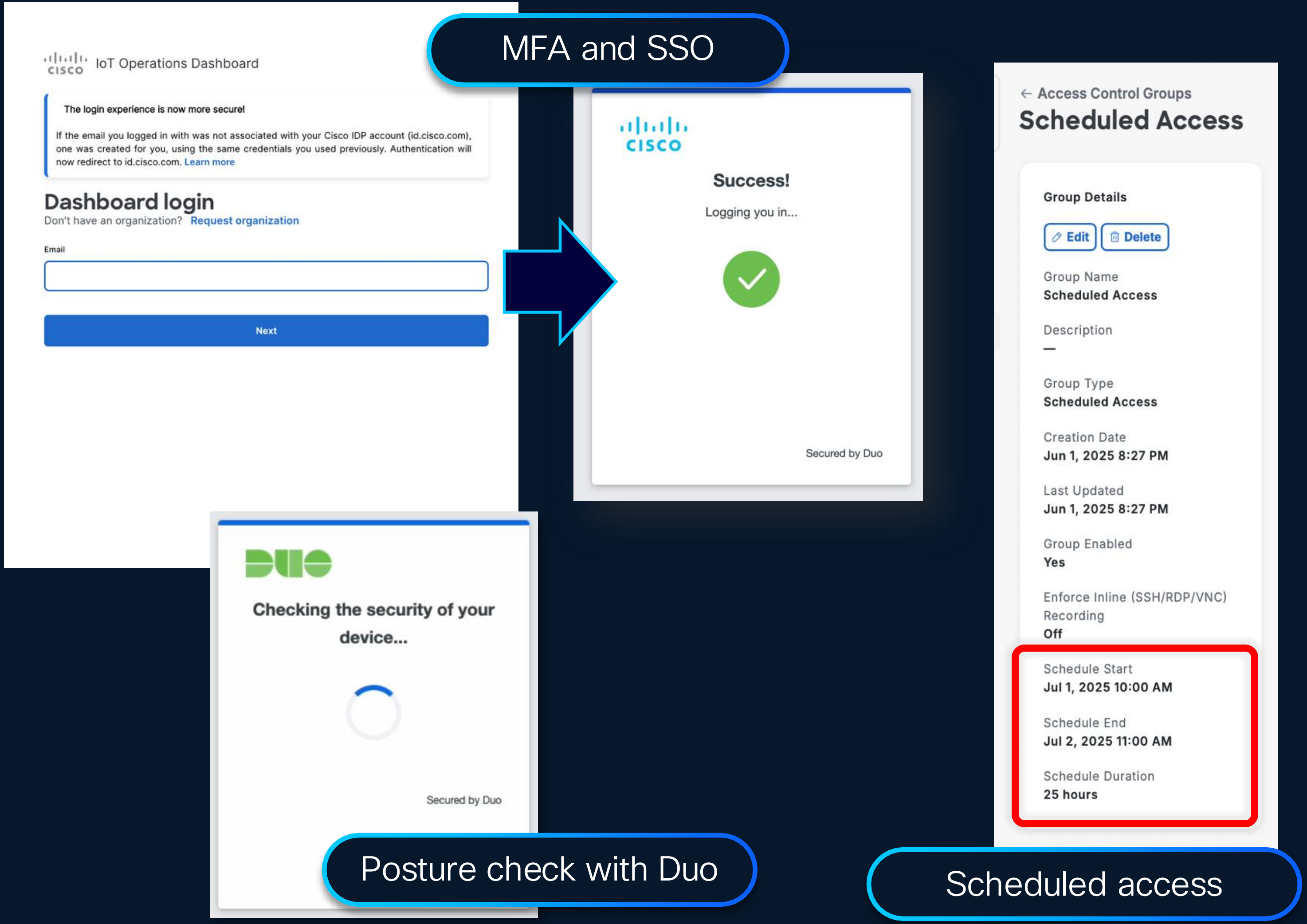
- Keep existing jump servers to maintain workflows and simplify change
- Replace insecure VPNs and enforce robust access control with SEA ensuring only authorized users have access only at specific times
- Gain new control with SEA recording sessions or inspecting file transfer*
- Simplify operations with cloud-based policy management that OT can use



Zero-Trust Security Controls

Ensure only trusted users can connect and when.

- Verify user identities with MFA and SSO, integrating with your IdP
- Prevent malware intrusion by verifying compliance of remote user’s computers using Cisco Duo
- Enforce schedules to allow access only at time of need



IoT Operations Dashboard

The login experience is now more secure!

If the email you logged in with was not associated with your Cisco IDP account (id.cisco.com), one was created for you, using the same credentials you used previously. Authentication will now redirect to id.cisco.com. Learn more

Dashboard login

Don't have an organization? Request organization

Email

Next

MFA and SSO

Success!

Logging you in...

Secured by Duo

Checking the security of your device...

Secured by Duo

Posture check with Duo

← Access Control Groups

Scheduled Access

Group Details

Edit Delete

Group Name
Scheduled Access

Description
—

Group Type
Scheduled Access

Creation Date
Jun 1, 2025 8:27 PM

Last Updated
Jun 1, 2025 8:27 PM

Group Enabled
Yes

Enforce Inline (SSH/RDP/VNC) Recording
Off

Schedule Start
Jul 1, 2025 10:00 AM

Schedule End
Jul 2, 2025 11:00 AM

Schedule Duration
25 hours

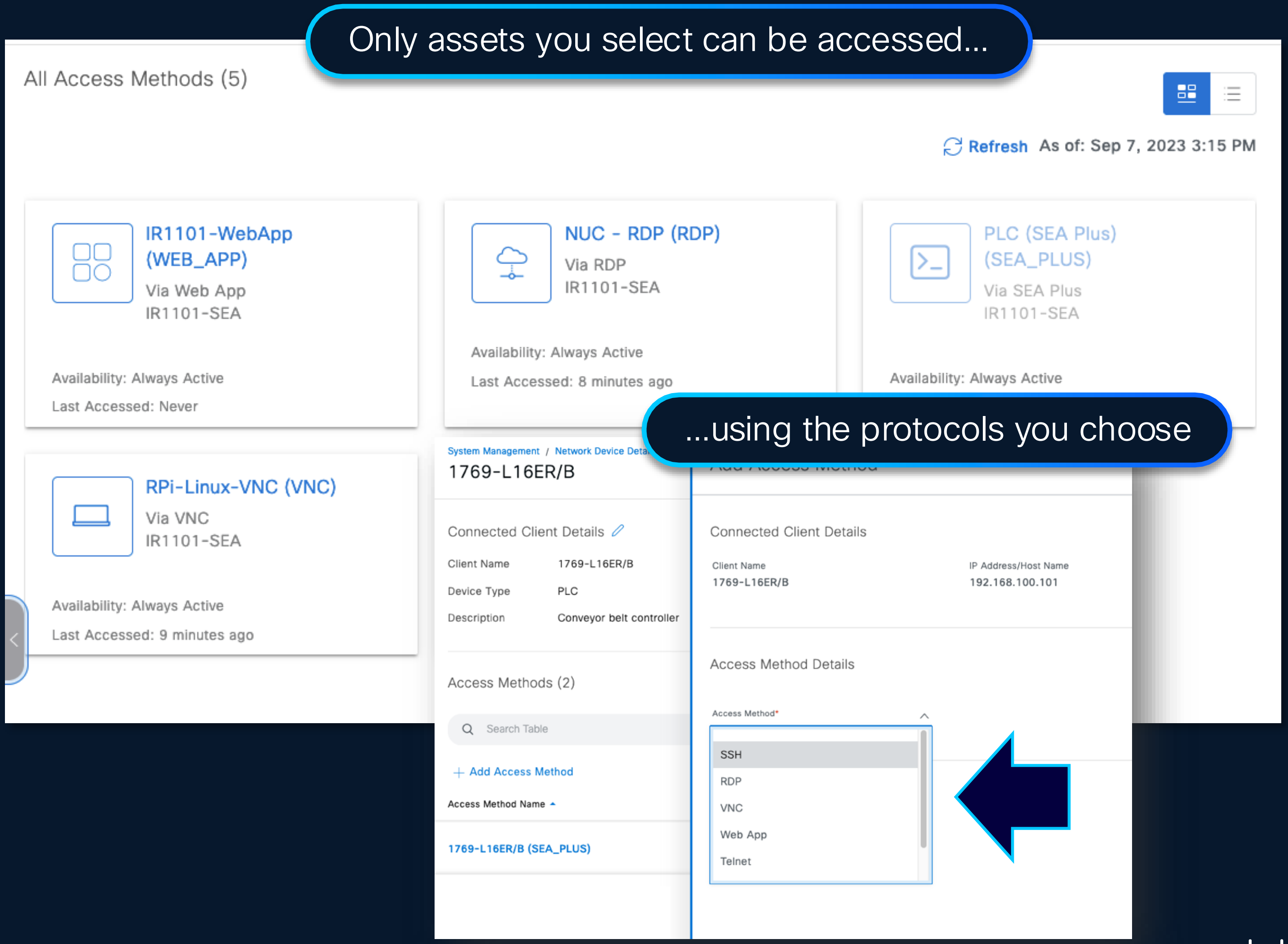
Scheduled access

Cisco Secure Equipment Access

Least Privilege Access Controls

Never expose your entire network and prevent lateral movement.

- Only assets you specify can be accessed by the remote users you choose
- Using only the protocols allowed
- Only on the days and times allowed



Only assets you select can be accessed…

All Access Methods (5)

Refresh As of: Sep 7, 2023 3:15 PM

IR1101-WebApp (WEB_APP)
Via Web App
IR1101-SEA
Availability: Always Active
Last Accessed: Never

NUC - RDP (RDP)
Via RDP
IR1101-SEA
Availability: Always Active
Last Accessed: 8 minutes ago

PLC (SEA Plus) (SEA_PLUS)
Via SEA Plus
IR1101-SEA
Availability: Always Active

RPi-Linux-VNC (VNC)
Via VNC
IR1101-SEA
Availability: Always Active
Last Accessed: 9 minutes ago

…using the protocols you choose

System Management / Network Device Deta

1769-L16ER/B

Connected Client Details

Client Name 1769-L16ER/B
Device Type PLC
Description Conveyor belt controller

Access Methods (2)

Search Table

+ Add Access Method

Access Method Name

1769-L16ER/B (SEA_PLUS)

Connected Client Details

Client Name: 1769-L16ER/B
IP Address/Host Name: 192.168.100.101

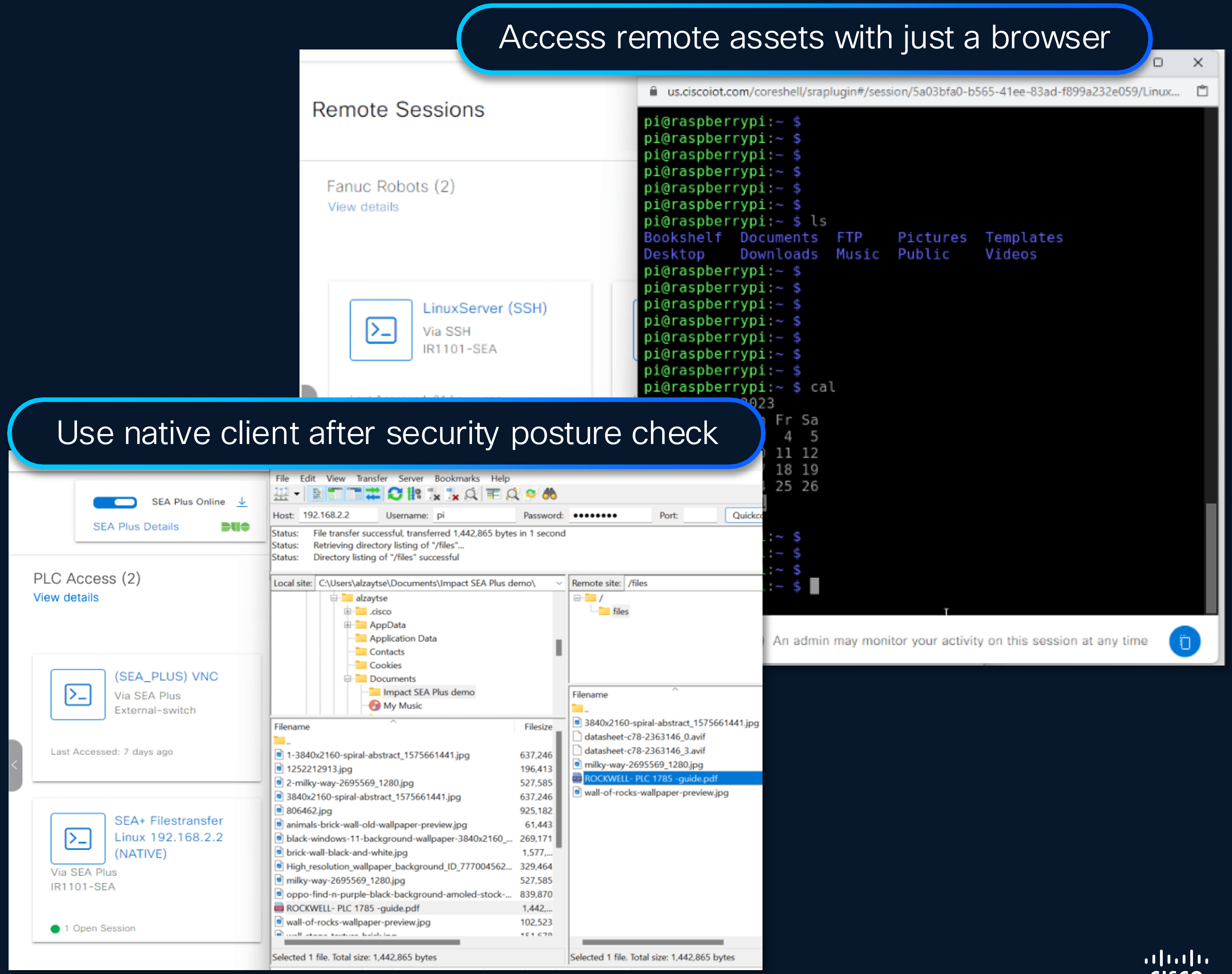
Access Method Details

Access Method*

Clientless and Agent-based Access

Get total control of how users can access assets while offering flexibility and ease of use.

- Clientless: Users only need a browser to access remote assets using RDP, VNC, SSH, Telnet or HTTP(S)
- Agent-based: Use native desktop clients for advanced tasks, only once computer has been verified for compliance with health policies



Access remote assets with just a browser

Use native client after security posture check

us.ciscoiot.com/coreshell/sraplugin#/session/5a03bfa0-b565-41ee-83ad-f899a232e059/Linux...

```
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $ ls
Bookshelf  Documents  FTP    Pictures  Templates
Desktop    Downloads  Music  Public    Videos
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $ cal
              023
                Fr Sa
                 4  5
                11 12
                18 19
                25 26

           :~ $
           :~ $
           :~ $
           :~ $
```

An admin may monitor your activity on this session at any time

Host: 192.168.2.2 Username: pi Password: •••••••• Port:

```
Status:     File transfer successful, transferred 1,442,865 bytes in 1 second
Status:     Retrieving directory listing of "/files"...
Status:     Directory listing of "/files" successful
```

Local site: C:\Users\alzaytse\Documents\Impact SEA Plus demo\

```
alzaytse
  .cisco
  AppData
  Application Data
  Contacts
  Cookies
  Documents
    Impact SEA Plus demo
    My Music
```

Remote site: /files

```
/
  files
```

```
Filename                                                Filesize
..
1-3840x2160-spiral-abstract_1575661441.jpg               637,246
1252212913.jpg                                           196,413
2-milky-way-2695569_1280.jpg                             527,585
3840x2160-spiral-abstract_1575661441.jpg                 637,246
806462.jpg                                               925,182
animals-brick-wall-old-wallpaper-preview.jpg              61,443
black-windows-11-background-wallpaper-3840x2160_...      269,171
brick-wall-black-and-white.jpg                           1,577,...
High_resolution_wallpaper_background_ID_777004562...     329,464
milky-way-2695569_1280.jpg                               527,585
oppo-find-n-purple-black-background-amoled-stock-...     839,870
ROCKWELL- PLC 1785 -guide.pdf                            1,442,...
wall-of-rocks-wallpaper-preview.jpg                      102,523
```

Selected 1 file. Total size: 1,442,865 bytes

```
Filename
..
3840x2160-spiral-abstract_1575661441.jpg
datasheet-c78-2363146_0.avif
datasheet-c78-2363146_3.avif
milky-way-2695569_1280.jpg
ROCKWELL- PLC 1785 -guide.pdf
wall-of-rocks-wallpaper-preview.jpg
```

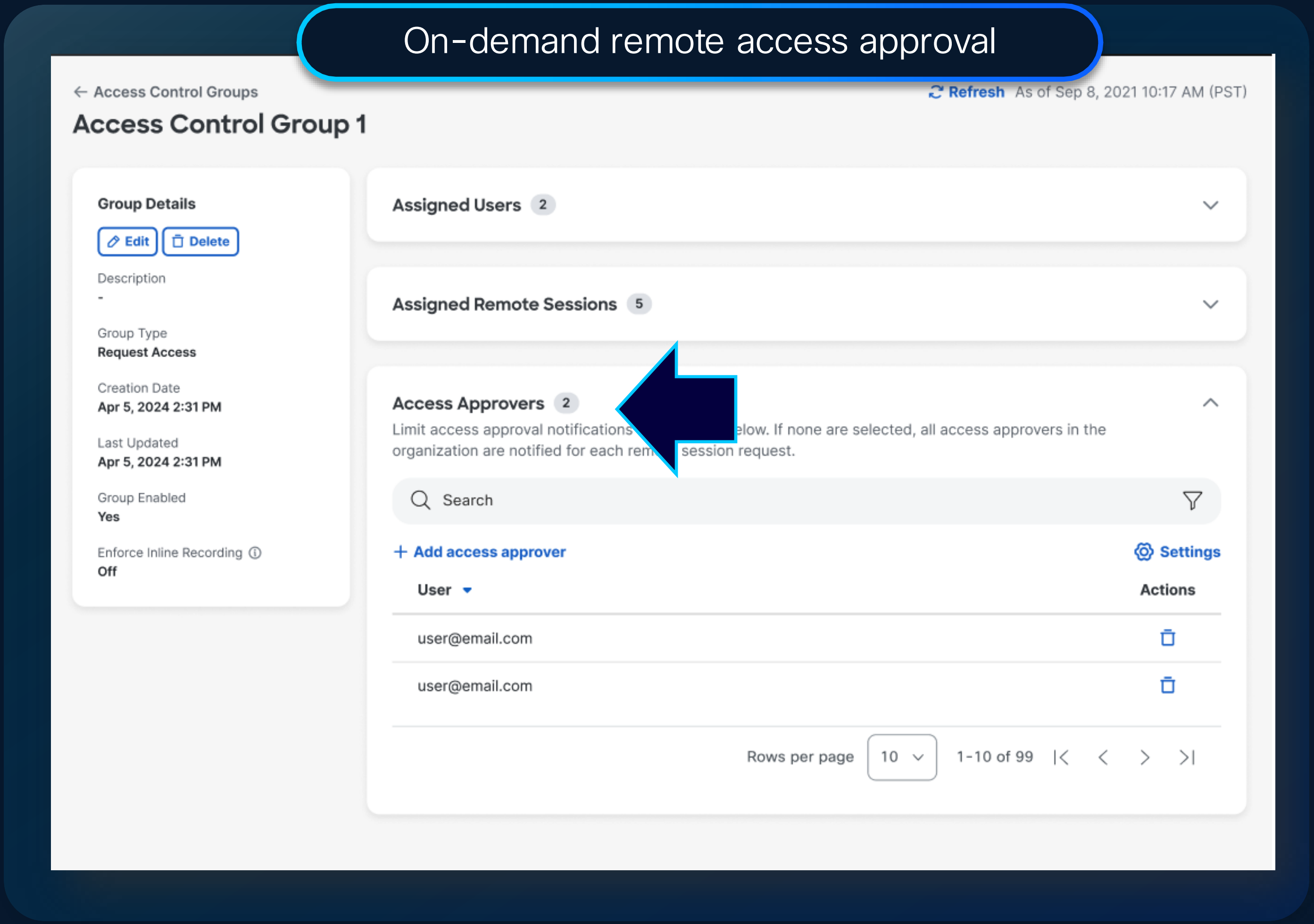
Selected 1 file. Total size: 1,442,865 bytes

Cisco Secure Equipment Access

OT Self-Service: On-Demand Remote Access

Help OT teams seamlessly drive operations with contractors while maintaining controls

- Remote users can request access when they need it. No need to preconfigure ever changing users
- Privileged users receive email notifications to grant access on-demand



On-demand remote access approval

← Access Control Groups

Refresh As of Sep 8, 2021 10:17 AM (PST)

Access Control Group 1

Group Details

Edit | Delete

Description
-

Group Type
Request Access

Creation Date
Apr 5, 2024 2:31 PM

Last Updated
Apr 5, 2024 2:31 PM

Group Enabled
Yes

Enforce Inline Recording ⓘ
Off

Assigned Users 2

Assigned Remote Sessions 5

Access Approvers 2

Limit access approval notifications [illegible] elow. If none are selected, all access approvers in the organization are notified for each rem[illegible] session request.

Search

+ Add access approver | Settings

User ▾	Actions
user@email.com	🗑
user@email.com	🗑

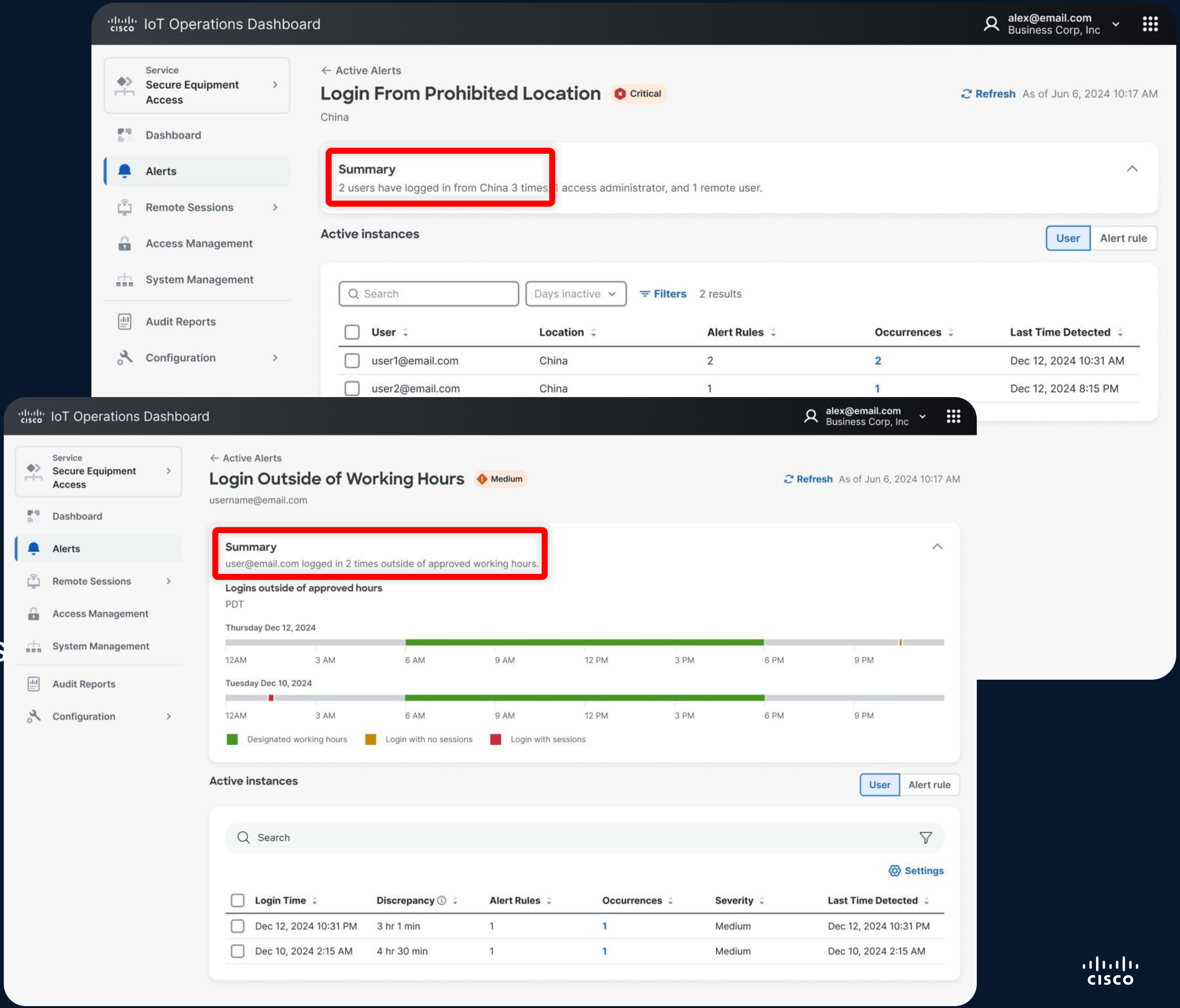
Rows per page 10 | 1-10 of 99

Cisco Secure Equipment Access

Remote User Identity Threat Detection

Detect threats related to remote user identity

- Login from unapproved geolocation
- Login outside working hours
- Auto deactivation of unused accounts



Login From Prohibited Location

Critical

China

As of Jun 6, 2024 10:17 AM

Summary

2 users have logged in from China 3 times. 1 access administrator, and 1 remote user.

Active instances

2 results

□	User	Location	Alert Rules	Occurrences	Last Time Detected
□	user1@email.com	China	2	2	Dec 12, 2024 10:31 AM
□	user2@email.com	China	1	1	Dec 12, 2024 8:15 PM

Login Outside of Working Hours

Medium

username@email.com

As of Jun 6, 2024 10:17 AM

Summary

user@email.com logged in 2 times outside of approved working hours.

Logins outside of approved hours

PDT

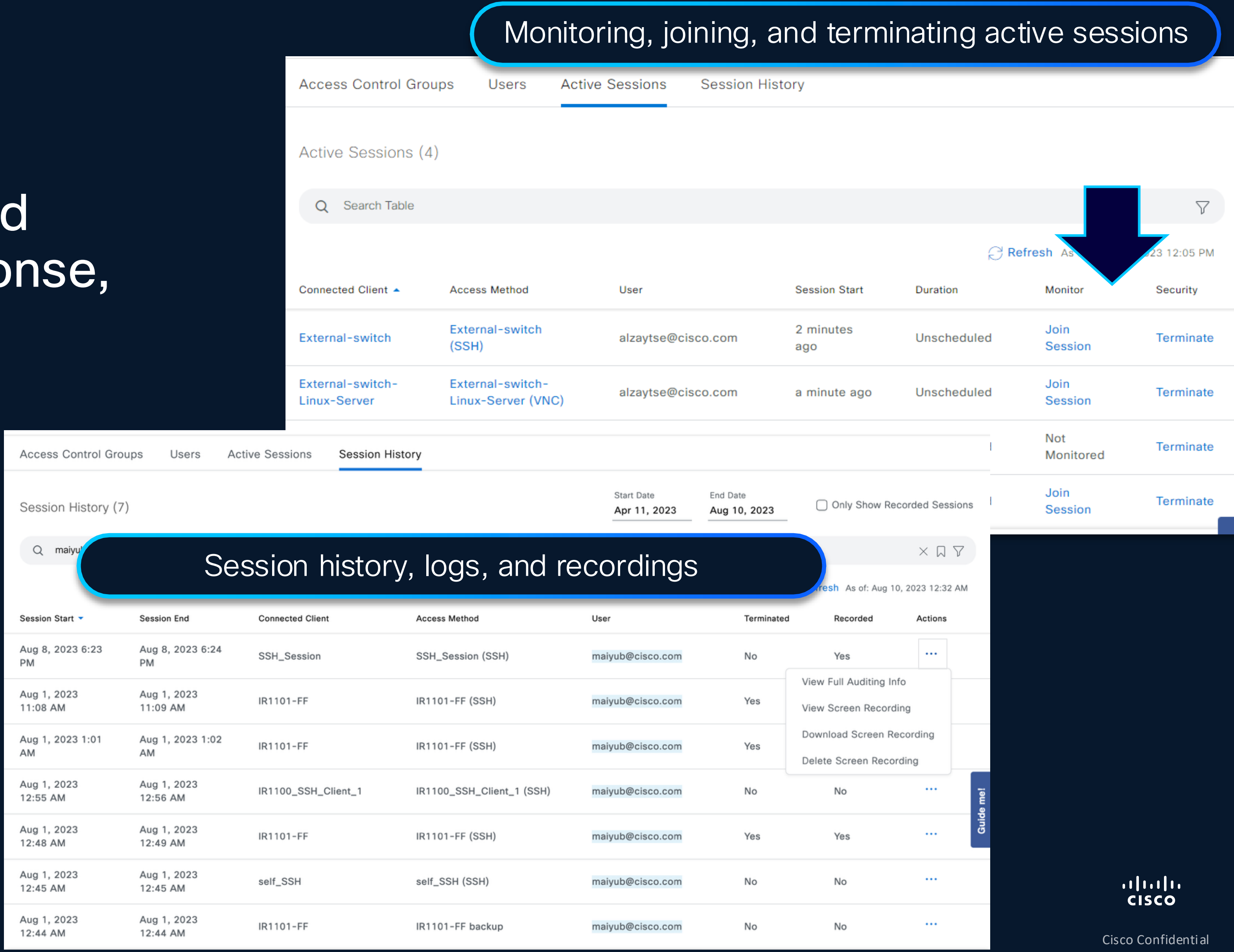
Active instances

□	Login Time	Discrepancy ⓘ	Alert Rules	Occurrences	Severity	Last Time Detected
□	Dec 12, 2024 10:31 PM	3 hr 1 min	1	1	Medium	Dec 12, 2024 10:31 PM
□	Dec 10, 2024 2:15 AM	4 hr 30 min	1	1	Medium	Dec 10, 2024 2:15 AM

Session Recording, Monitoring, and Termination

Real-time visibility on active and past sessions for incident response, investigations, and compliance.

- Monitor active sessions from anywhere in the world
- Terminate remote user session if you detect suspicious activity
- Record or Join sessions for training or audit purposes



Monitoring, joining, and terminating active sessions

Active Sessions (4)

23 12:05 PM

Connected Client	Access Method	User	Session Start	Duration	Monitor	Security
External-switch	External-switch (SSH)	alzaytse@cisco.com	2 minutes ago	Unscheduled	Join Session	Terminate
External-switch-Linux-Server	External-switch-Linux-Server (VNC)	alzaytse@cisco.com	a minute ago	Unscheduled	Join Session	Terminate
					Not Monitored	Terminate
					Join Session	Terminate

Session history, logs, and recordings

Session History (7)

Start Date Apr 11, 2023

End Date Aug 10, 2023

□ Only Show Recorded Sessions

As of: Aug 10, 2023 12:32 AM

Session Start	Session End	Connected Client	Access Method	User	Terminated	Recorded	Actions
Aug 8, 2023 6:23 PM	Aug 8, 2023 6:24 PM	SSH_Session	SSH_Session (SSH)	maiyub@cisco.com	No	Yes	···
Aug 1, 2023 11:08 AM	Aug 1, 2023 11:09 AM	IR1101-FF	IR1101-FF (SSH)	maiyub@cisco.com	Yes		
Aug 1, 2023 1:01 AM	Aug 1, 2023 1:02 AM	IR1101-FF	IR1101-FF (SSH)	maiyub@cisco.com	Yes		
Aug 1, 2023 12:55 AM	Aug 1, 2023 12:56 AM	IR1100_SSH_Client_1	IR1100_SSH_Client_1 (SSH)	maiyub@cisco.com	No	No	···
Aug 1, 2023 12:48 AM	Aug 1, 2023 12:49 AM	IR1101-FF	IR1101-FF (SSH)	maiyub@cisco.com	Yes	Yes	···
Aug 1, 2023 12:45 AM	Aug 1, 2023 12:45 AM	self_SSH	self_SSH (SSH)	maiyub@cisco.com	No	No	···
Aug 1, 2023 12:44 AM	Aug 1, 2023 12:44 AM	IR1101-FF	IR1101-FF backup	maiyub@cisco.com	No	No	···

Agenda

01 Les enjeux cyber dans l’OT

02 Etapes de sécurisation des réseaux OT

03 Visibilité : Cisco Cyber Vision

04 Segmentation : ISE & FMC

05 Gestion des accès distant : SEA

06 Surveillance et répons à incident : Splunk

07 Cas clients

Step #4: Unify IT and OT visibility into the SOC

Understand the OT security posture with OT visibility

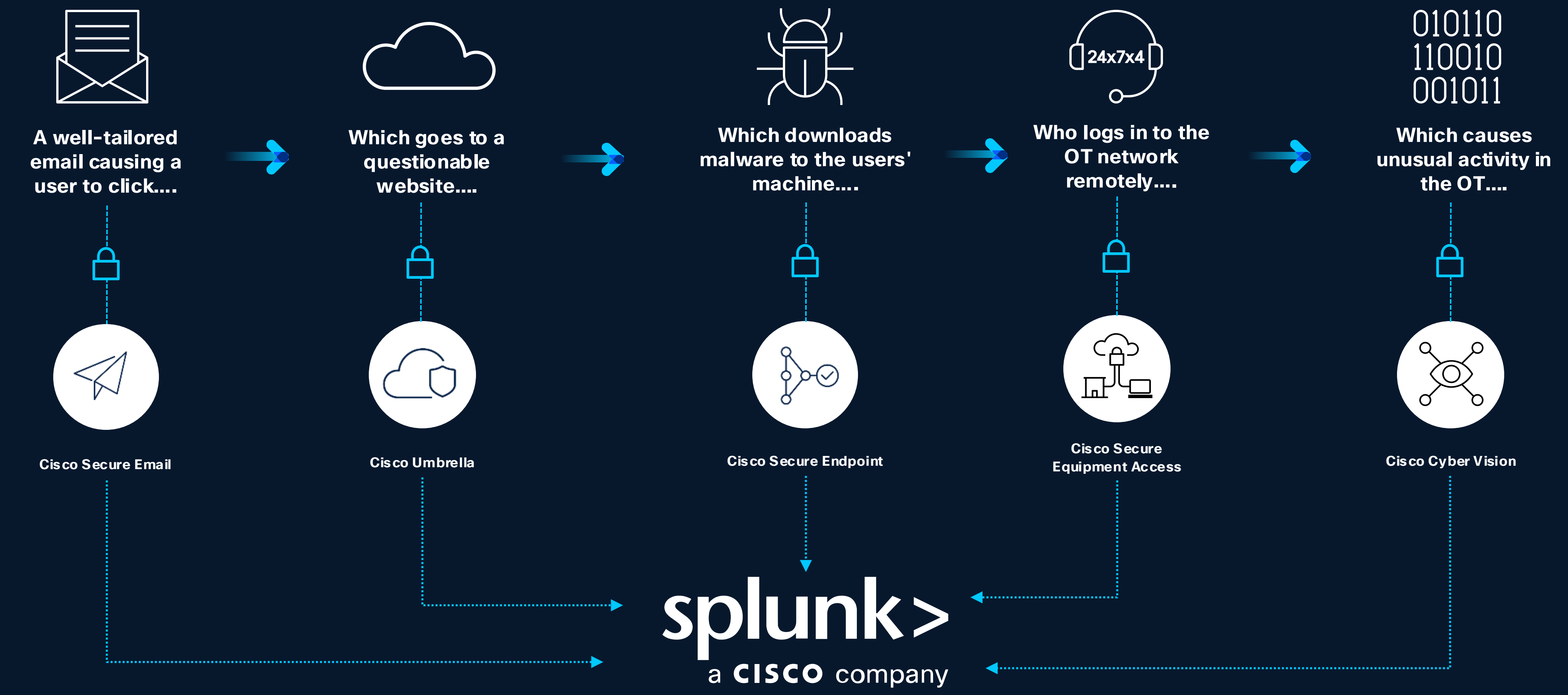
Limit blast radius with network segmentation

Control risks from remote access to OT assets

Monitor OT networks in the SOC

A siloed approach is not enough to secure OT

Detecting threats requires cross-domain visibility



A well-tailored email causing a user to click....

Which goes to a questionable website....

Which downloads malware to the users' machine....

Who logs in to the OT network remotely....

Which causes unusual activity in the OT....

Cisco Secure Email

Cisco Umbrella

Cisco Secure Endpoint

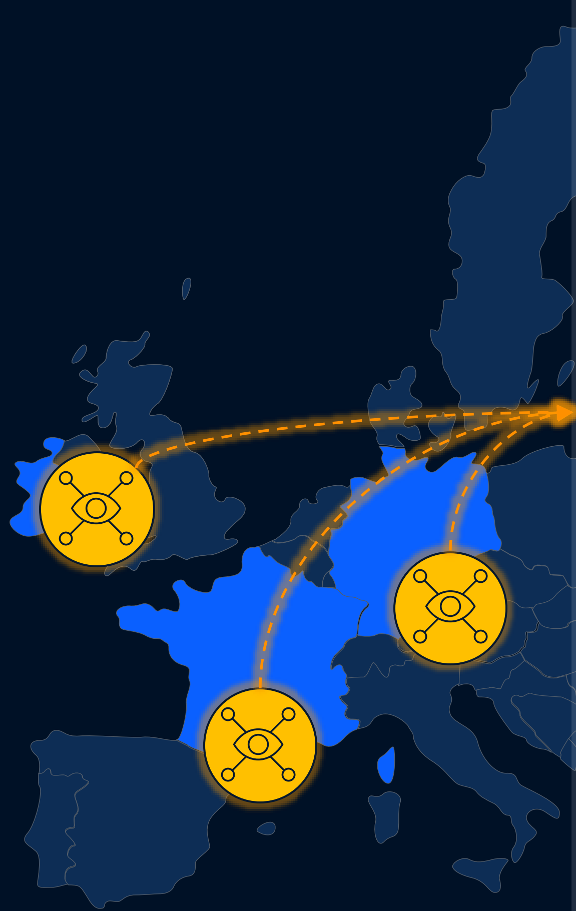
Cisco Secure Equipment Access

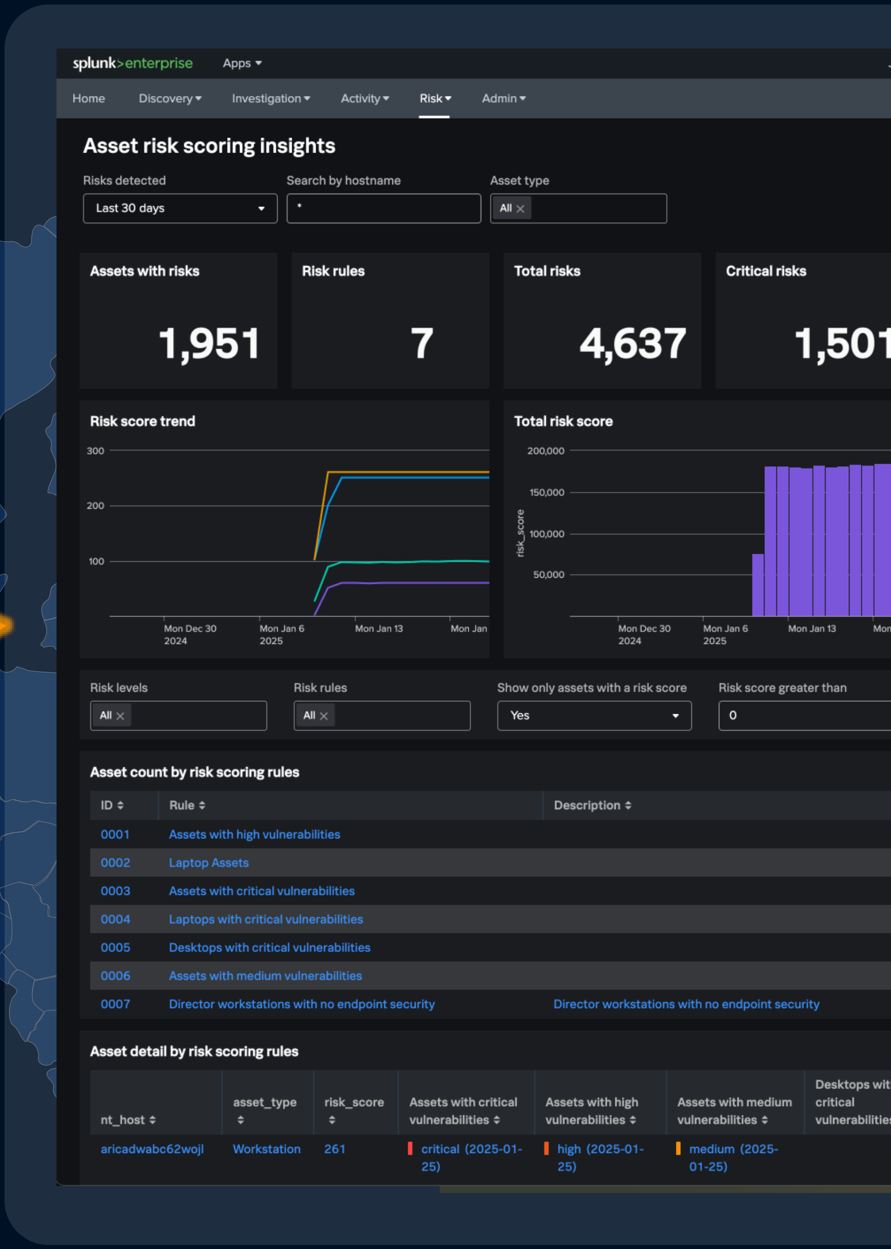
Cisco Cyber Vision

Splunk for OT Security

Detect and remediate threats across IT & OT

- ✓ Unified IT/OT security events management
- ✓ Aggregate all Cyber Vision deployments
- ✓ Schedule reports over email
- ✓ Perimeter Monitoring
- ✓ Risk Based Alerting
- ✓ MITRE ATT&CK ICS correlation rules





Asset risk scoring insights

Risks detected: Last 30 days ▾

Search by hostname: *

Asset type: All ×

Assets with risks	Risk rules	Total risks	Critical risks
1,951	7	4,637	1,501

Risk score trend

Total risk score

Risk levels: All ×

Risk rules: All ×

Show only assets with a risk score: Yes ▾

Risk score greater than: 0

Asset count by risk scoring rules

ID ⇕	Rule ⇕	Description ⇕
0001	Assets with high vulnerabilities	
0002	Laptop Assets	
0003	Assets with critical vulnerabilities	
0004	Laptops with critical vulnerabilities	
0005	Desktops with critical vulnerabilities	
0006	Assets with medium vulnerabilities	
0007	Director workstations with no endpoint security	Director workstations with no endpoint security

Asset detail by risk scoring rules

nt_host ⇕	asset_type ⇕	risk_score ⇕	Assets with critical vulnerabilities ⇕	Assets with high vulnerabilities ⇕	Assets with medium vulnerabilities ⇕	Desktops wit critical vulnerabilitie
aricadwabc62wojl	Workstation	261	🟥 critical (2025-01-25)	🟧 high (2025-01-25)	🟧 medium (2025-01-25)	

Agenda

01 Les enjeux cyber dans l'OT

02 Etapes de sécurisation des réseaux OT

03 Visibilité : Cisco Cyber Vision

04 Segmentation : ISE & FMC

05 Gestion des accès distant : SEA

06 Surveillance et répons à incident : Splunk

07 Cas clients

Case study: Manufacturing

UNILIN: A global leader in the flooring industry

Business drivers

- An audit highlighted OT network as a huge cyber risk
- IT had no visibility into OT network
- IT wanted a solution which was easy to deploy and use and that could integrate with their existing security tool set (Firepower, Stealthwatch, SecureX and Splunk)

Solution

- Chose Cisco IE3x00 switches as the standard network foundation
- Deployed Cyber Vision sensor on Cisco IE switches to gain 100% visibility
- Cyber Vision fully integrated with the IT security tools

Outcome

- IT gets comprehensive OT information in their IT security tools
- OT leverages Cyber Vision for insights into OT processes

https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/unilin-group.html

Case study: Water Utility

Albuquerque Bernalillo County Water Utility Authority

Business drivers

- New requirements set by America's Water Infrastructure Act (AWIA) regulatory compliance
- Aging network and security infrastructure

Solution

- Complete refresh and update of the SCADA network infrastructure with a focus on cybersecurity
- Upgraded to Cisco Catalyst IE3400 and Catalyst 9300 with embedded Cyber Vision Sensor
- Deployed ISA3000 firewalls to protect zones

Outcome

- Increased security with comprehensive visibility on OT assets
- Standardized platforms for IT/OT to share same data and better collaborate. Can now extend Cisco ISE to OT domain.
- Now has to right tools and processes for regulatory compliance with AWIA standards

https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/albuquerque-water-authority.html

Case study: Auto manufacturer

EV auto manufacturer with global operations

Business drivers

- Major outages due to network misconfiguration. No standard on switching platform made it is impossible to troubleshoot
- No visibility into entire ICS environment
- Line builders using same IP address ranges across multiple cells required lots of external NAT devices

Solution

- Standardize on Cisco IE3x00 switches to benefit from
  - L2NAT
  - Profinet & CIP support
  - Modularity of port counts
  - Gigabit Ethernet speeds
- Cyber Vision sensor on IE switches to gain 100% visibility without the high cost of building a SPAN collection network

Outcome

- Standardization of IE switches makes it easy to manage the network
- Increased confidence in uptime in the production environment

Case study: Power utility

CPFL Energia builds resilience and regulatory compliance

Business drivers

- Over 700 substations to monitor and secure
- Very old, unmanaged network infrastructure connecting remote grid assets to their control center using satellite links
- No inventory of connected assets, vulnerabilities and risks
- Had to comply with new local cybersecurity regulations

Solution

- Replaced switches in all substations with Catalyst IE3400 and embedded Cyber Vision Sensor
- One Cyber Vision Center per region and one Global Center in HQ
- Cisco Secure Firewalls to filter traffic in/out of substations

Outcome

- Cyber Vision DPI in IE switches limits traffic from substations to the SOC, saving on satellite links
- OT security events sent to SIEM for security analysts to manage OT security incidents
- Now has detailed information on grid assets and events to comply with local regulatory requirements

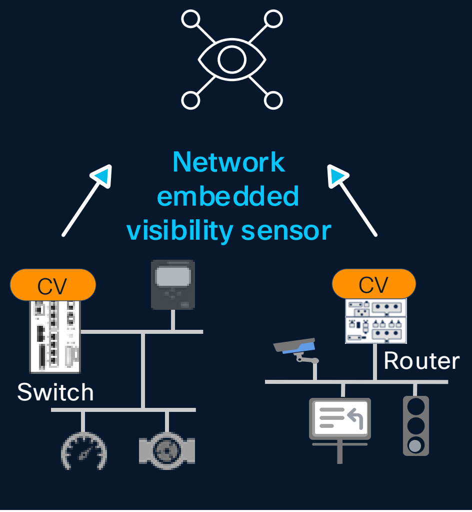
https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/cpfl-energia.html

Conclusion

Putting it All Together... Cisco Industrial Threat Defense

OT Asset Visibility and Security Posture

Cisco Cyber Vision



Zero Trust Security for OT

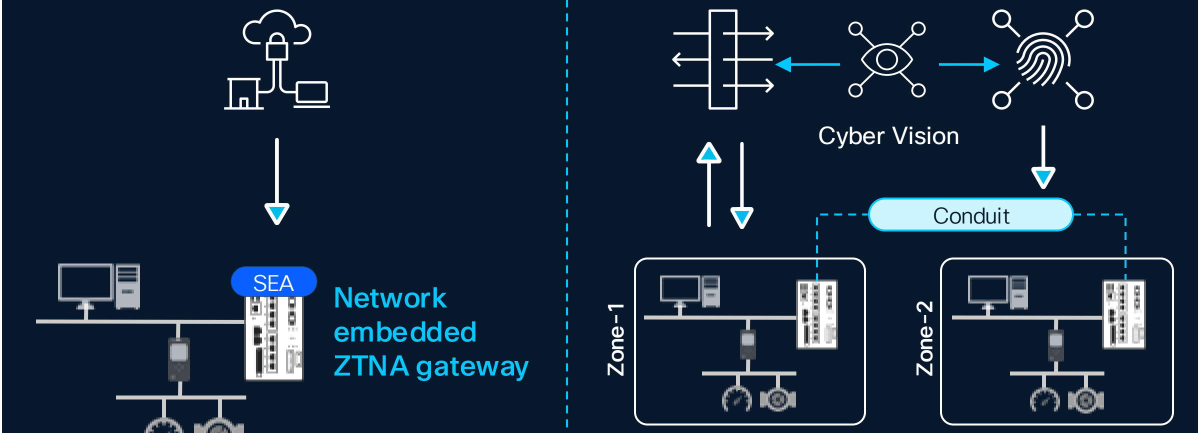
Secure remote access (ZTNA)

Cisco Secure Equipment Access

IEC 62443 zone segmentation

Cisco Secure Firewall

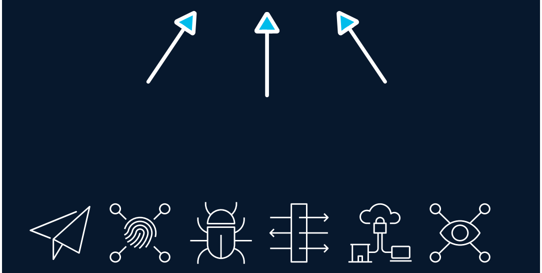
Cisco ISE



Network enforced segmentation

Cross-Domain Detection, Investigation & Response

splunk> a cisco company



Visibility across the entire attack chain

Highly scalable, comprehensive industrial security, embedded in the network

Grow your OT Security business

Help your customers secure their operations

Engage with IoT Sales Specialists to maximize your chances of success
iotsalesglobal@cisco.com

Visit cisco.com/go/iotsecurity

Leverage our Industrial Security Validated Designs (CVD)
www.cisco.com/go/iotcvd

Learn about your options for discounted licenses
www.cisco.com/go/iotoffers

MERCI DE VOTRE ATTENTION !

Sondage de satisfaction

Merci de votre feedback

Scannez-moi

Cyberdefense