Securing Industrial Networks

Strategies and Best Practices

Tilman Taubert
Leader - EMEA IoT Industry Specialists

BRKSEC-2821

ttaubert@cisco:~ $ whoami

- With Cisco since 2018
- 15 Year’s in Consulting/Implementation
  - Long time of that deploying “OT” Networking & Cyber Security
- Manufacturing, Critical Infrastructure / Utilities
- ‘On the fence’ between IT / OT

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.

Session Expectations

What to expect:

- An architecture view of the solution
- Understanding of the products available and their function
- The whole is greater than the sum of the parts

What not to expect:

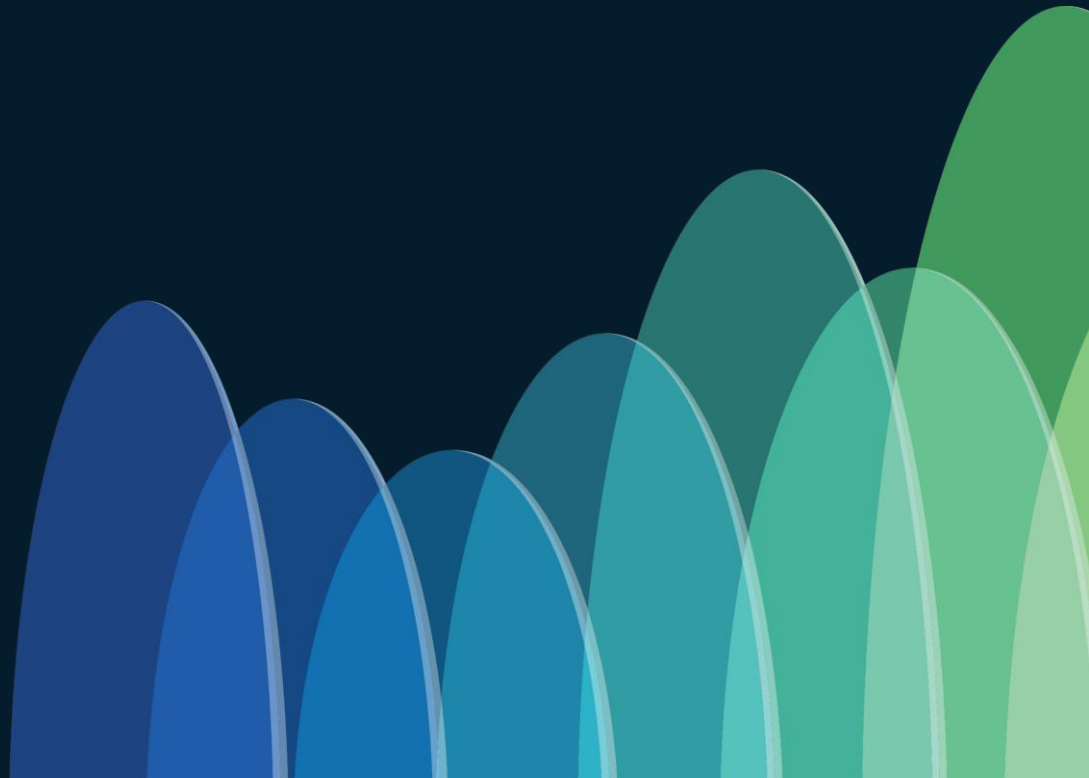
- Deep dive of the different products
- Configuration or implementation guidelines

Session Agenda

- Industrial Security Overview
- Asset Visibility & Security Posture
- Segment network into smaller Zones
- Secure Remote Access
- Detection, Investigation and Response

Overview Demos
(within each section)

Industrial Security



cisco Live!

2024 State of Industrial Networking Report

Firms struggle to keep infrastructure secure

The top challenge for organizations trying to run and maintain industrial infrastructure is cybersecurity: cited by 39% of respondents.

This figure rises to 50% of companies whose revenues exceed $30 billion, suggesting the task of defending against cyberattacks increases as businesses get larger and more complex.

After cybersecurity, the next biggest stumbling blocks all relate to alignment and integration. Firms struggle with a lack of standardization (37%), disparate vendors and partners (36%), and a lack of collaboration with IT colleagues (33%).

1# 39%
Implementing robust cybersecurity measures and mitigating cyber threats

2# 37%
Lack of standardization across industrial infrastructure

3# 36%
Managing multiple vendors, including strategic partners and point solutions

4# 33%
Lack of collaboration and efficiencies with IT

5# 31%
Meeting regulatory compliance requirements

6# 28%
Addressing equipment maintenance and aging infrastructure

7# 25%
Lack of visibility and inventory of connected assets

Q. What are the biggest challenges your company faces in the optimal running and maintenance of its industrial infrastructure? Select all that apply

2024 State of Industrial Networking Report

13

Reality check

Security Challenges in Industrial Environments

Common themes

Antiquated Systems
Unpatched, legacy systems

Technical Debt
Lack of segmentation

OT Security Skills
IT sec ⇔ Ops knowledge

Lack of Visibility
What's out there, who is talking to who, what are they saying

Access Control
Access needs evolving

Change Control
24/7/365 Operations

Business Needs
Real-time Information, no downtime, quick access

Reality check #2

The incident response hierarchy of needs

"During incident response, I operate at the same tempo as the adversary to protect my business assets."

"When my red team emulates a real-world adversary, I detect their intrusion at multiple points along the kill chain."

"I detect hygiene issues and operator activity that does not follow best practices."

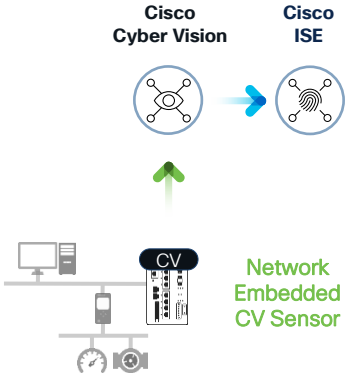
Cybersecurity Programs

Common strategic objectives

1. **Rapid Visibility of IACS System** Threats, ensuring the Ability to Detect both IT and OT malware within the Industrial environment.
2. **Up-to-date complete Inventory** of IACS system Assets with details per Asset.
3. **Mitigate risk from Unpatchable systems**, both IT and OT assets and these assets associated business risk to the operation.
4. Protect Industrial Platform and Applications from Attack. **Protect from** both Known and Unknown **Malware**.
5. **Limit Network Traffic** and Network Path leveraged to get to Critical Industrial Systems.

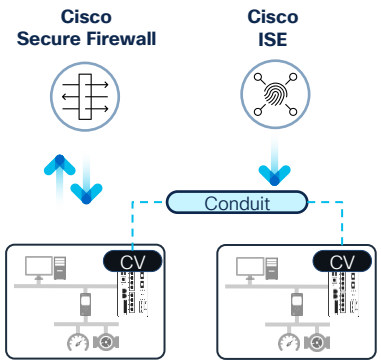
Cisco's Industrial Threat Defense Journey

1 Asset Visibility & Security Posture



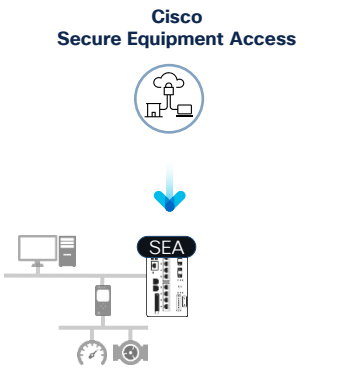
2 Zero Trust for OT

Segment network into smaller Zones
IEC 62443 Zones & Conduits

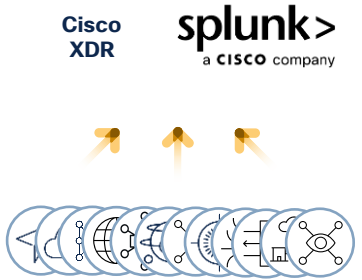


3 Zero Trust for OT

Secure Remote Access

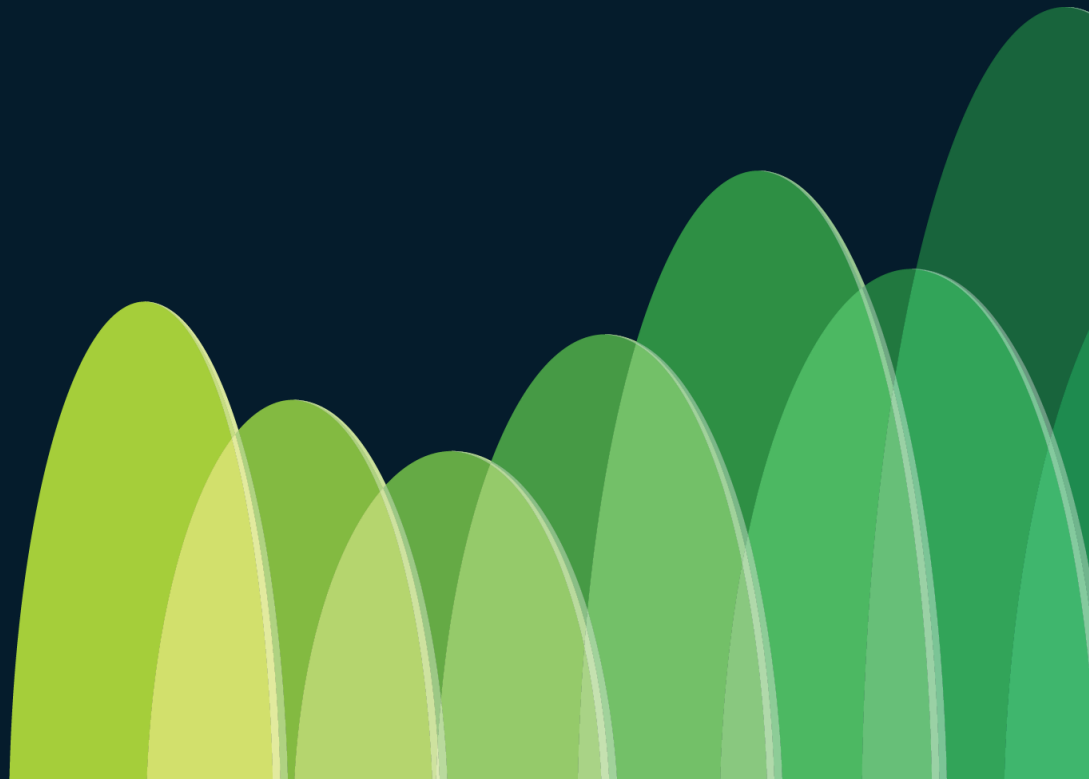


4 Cross-Domain Detection, Investigation & Response



Visibility across the entire attack chain

Asset Visibility & Security Posture



cisco Live!

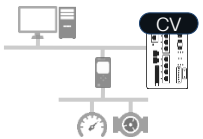
Cisco's Industrial Threat Defense Journey

1

Asset Visibility & Security Posture

Cisco Cyber Vision

Cisco ISE



Network Embedded CV Sensor

2

3

Zero Trust for OT

Segment network into smaller Zones
IEC 62443 Zones & Conduits

Cisco Secure Firewall

Cisco ISE

Secure Remote Access

Cisco Secure Equipment Access

4

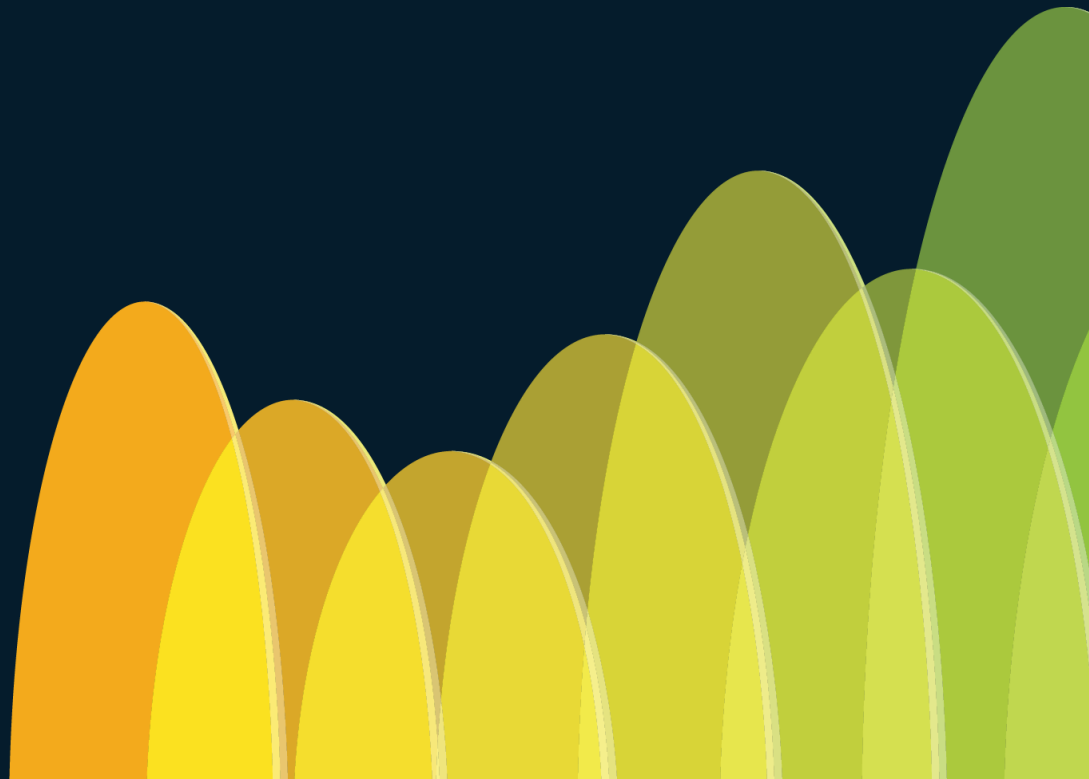
Cross-Domain Detection, Investigation & Response

Cisco XDR

splunk> a CISCO company

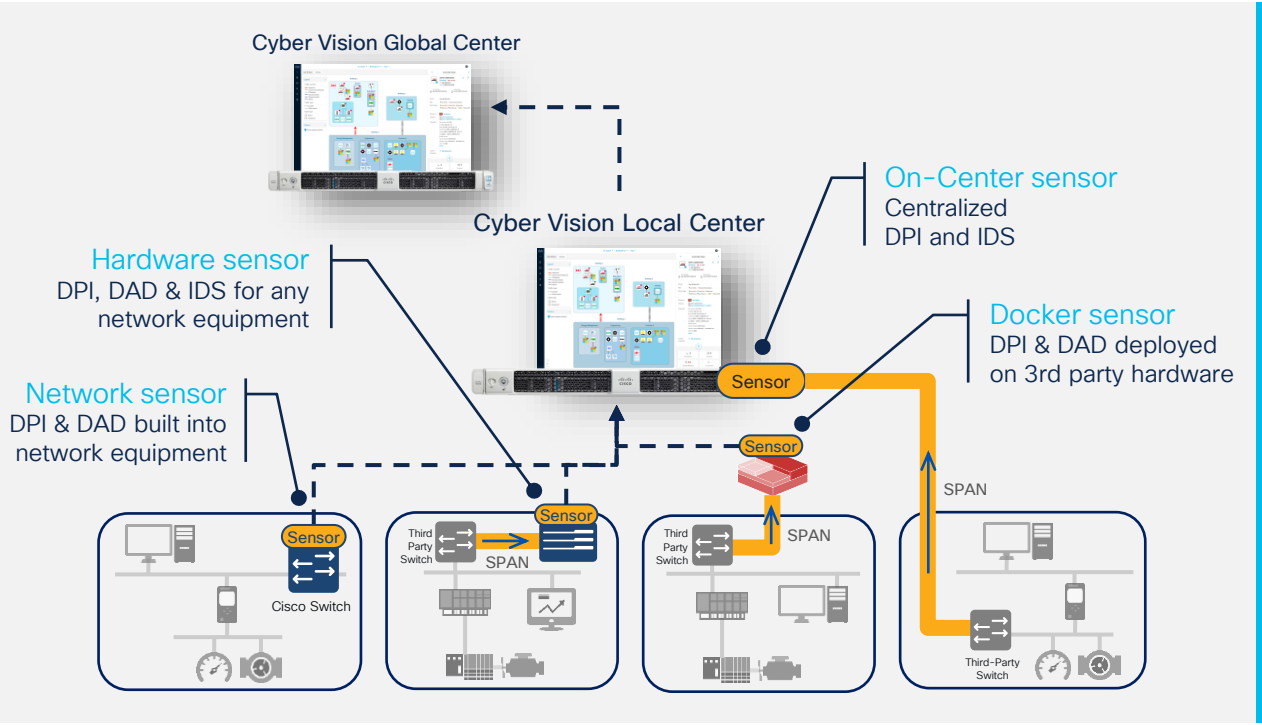
Visibility across the entire attack chain

Cisco Cyber Vision



cisco Live!

Cisco Cyber Vision Architecture

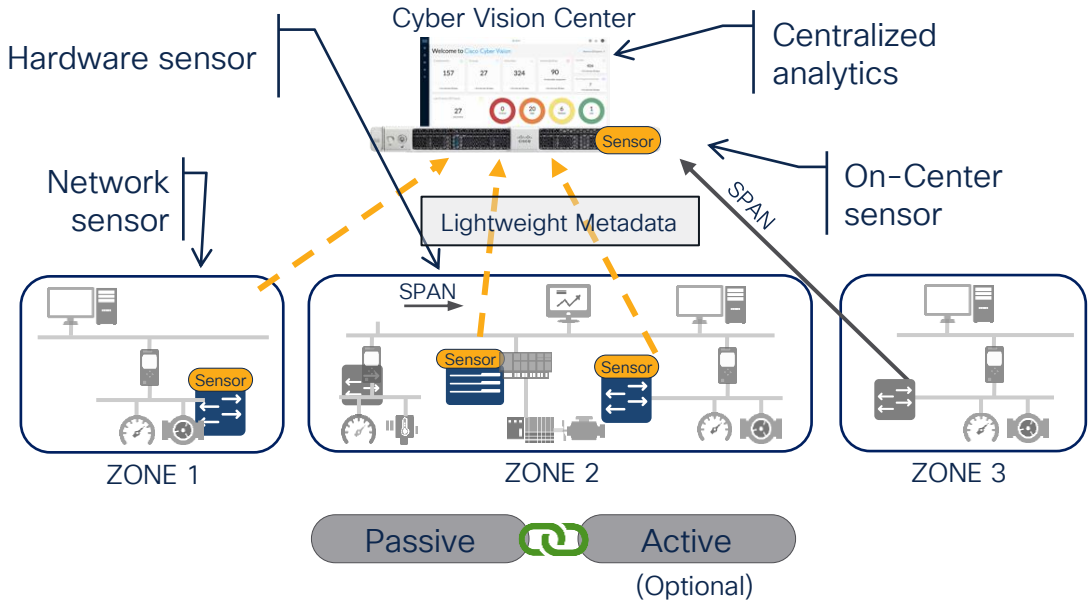


- **Network-sensors** embedded in Cisco networking for simple and highly scalable deployments
- **Hardware or Virtual sensors** capturing traffic on any switch with a single hop SPAN to support brownfield deployments
- **On-Center sensor** to leverage existing SPAN infrastructures, or collect traffic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

DPI = Deep Packet inspection *DAD = Distributed Active Discovery* *IDS = Intrusion Detection System*

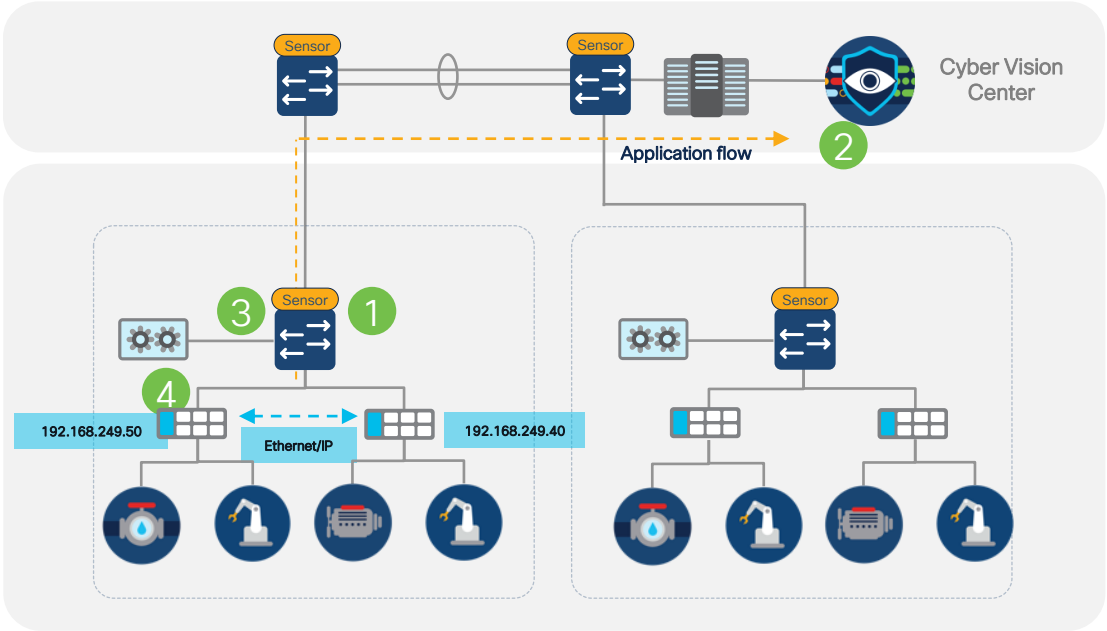
The Role of the Cyber Vision Sensor

1. Analyses industrial protocols and communications at application level, decoding industrial protocol traffic.
2. Dynamically builds an inventory of all components and a map of all connections.
3. Operational insight: extracts process information from network flows to give OT staff visibility on industrial events.
4. Provides advanced anomaly detection, and real-time alerts for any threat to operational continuity and system integrity.



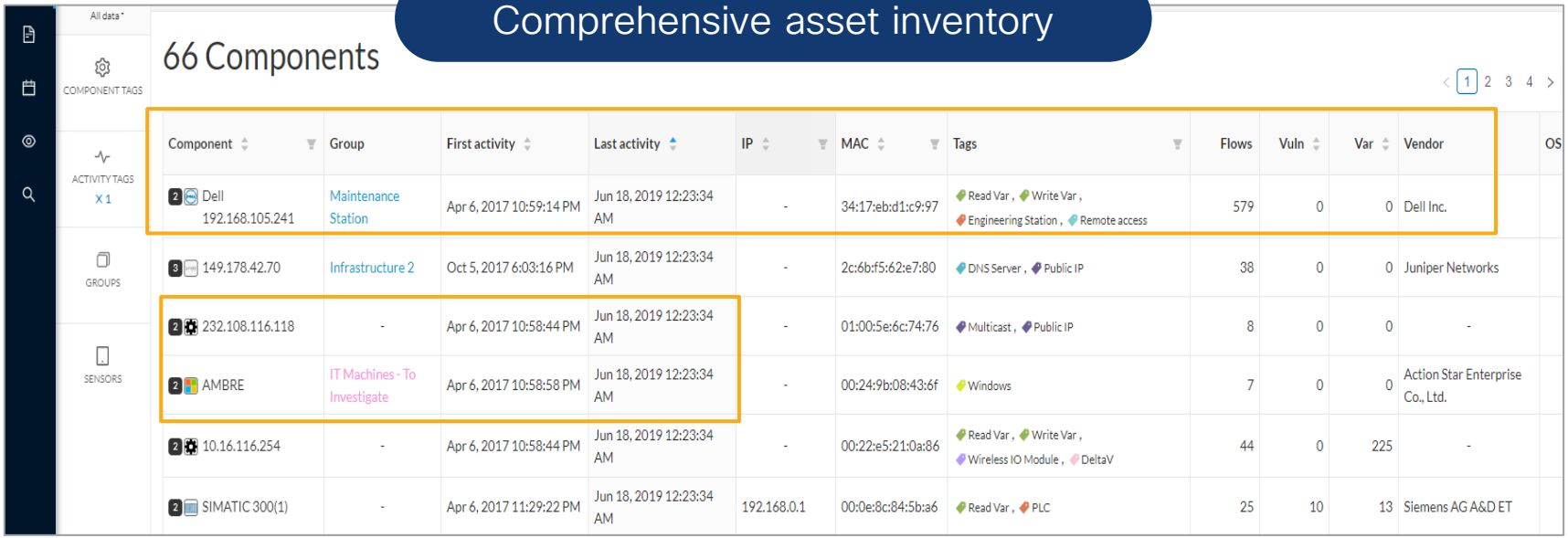
Active Discovery Closed Loop Control

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



Active Discovery from Sensor bypasses NAT/Firewall boundaries

Industrial Endpoint Visibility

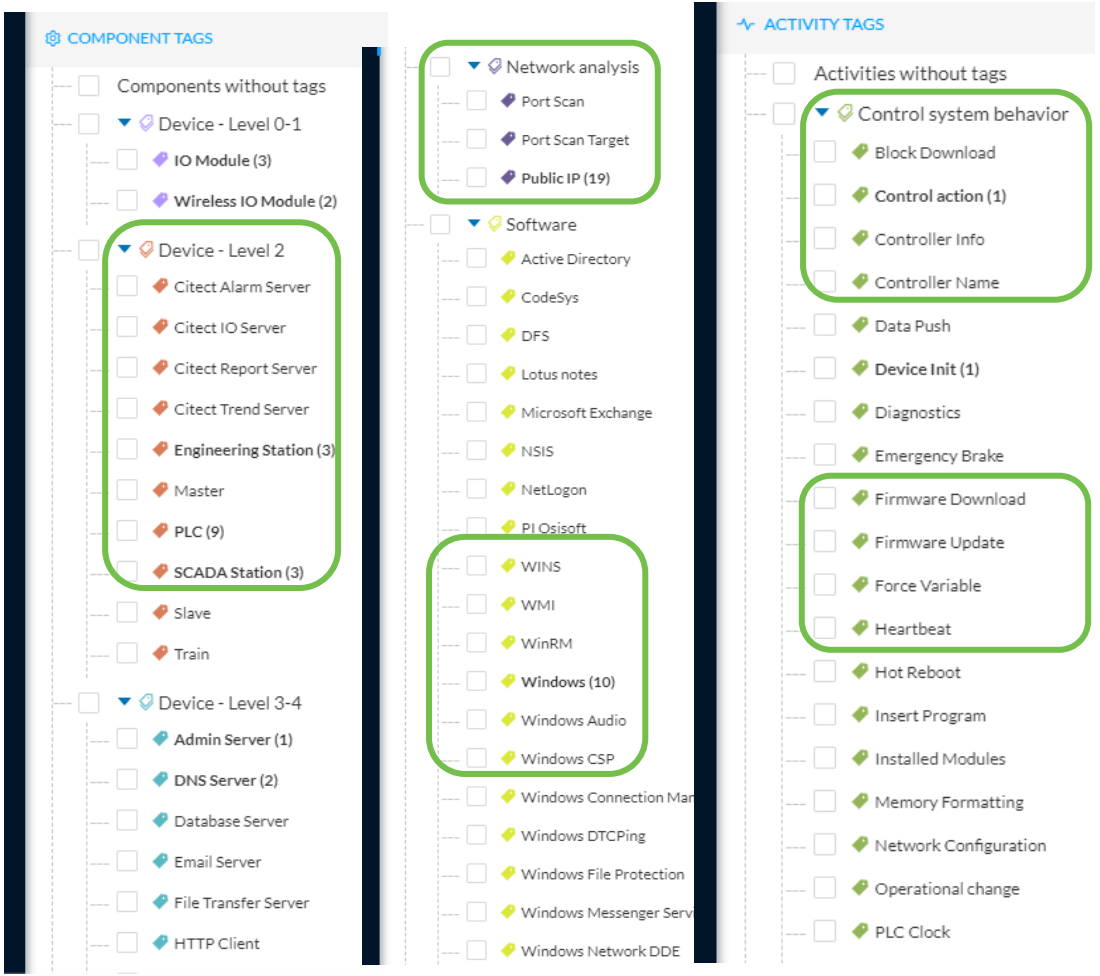


- Automatically maintains a detailed list of all OT and IT equipment
- Immediate access to software and hardware characteristics

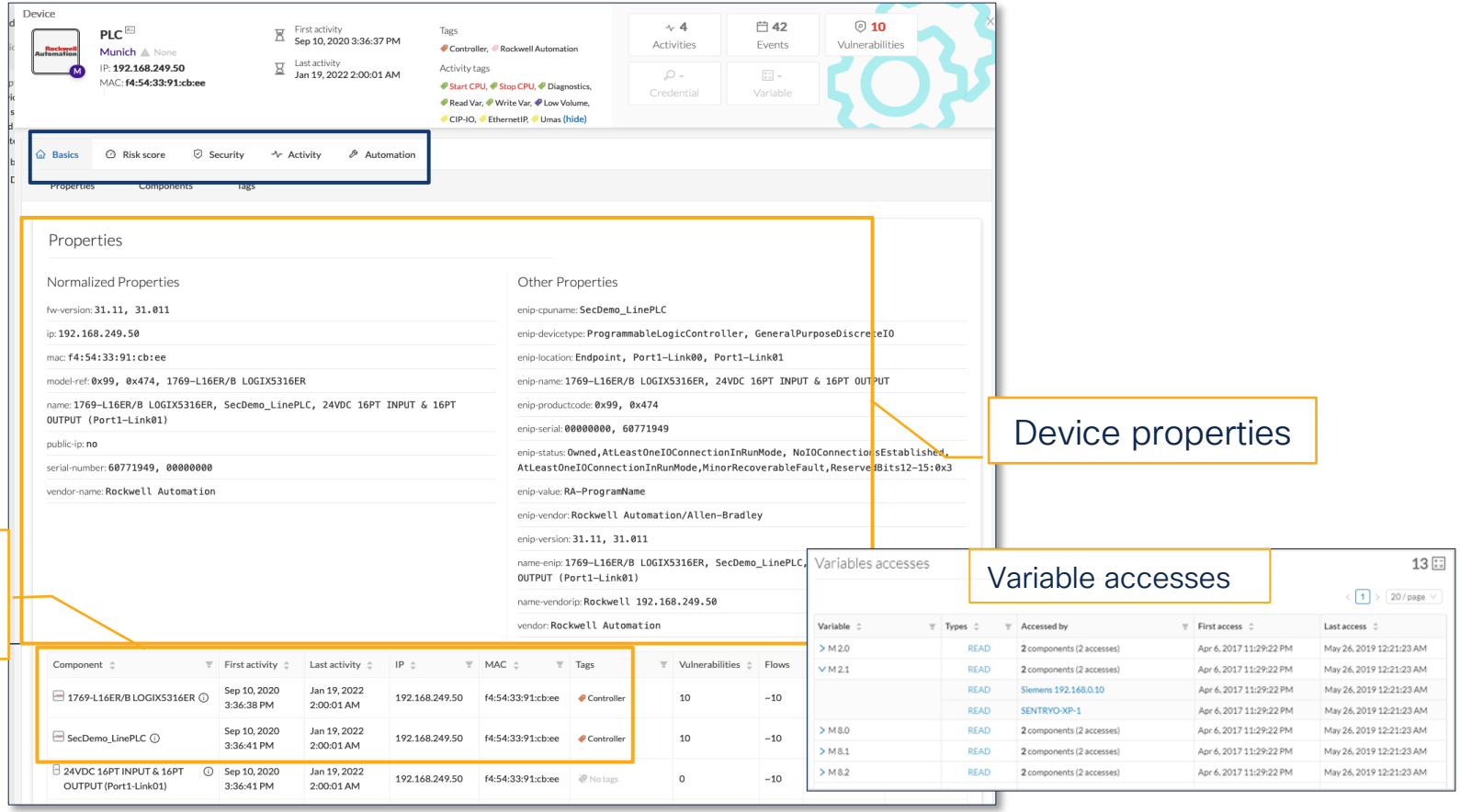
Automatic tagging

- Asset and communication characteristics are automatically translated to Tags
- A common language whatever the vendor reference
- Users do not need to be protocol experts to understand what is happening

Cyber Vision tags helps identify devices and activities to investigate



Detailed information on assets



Device properties

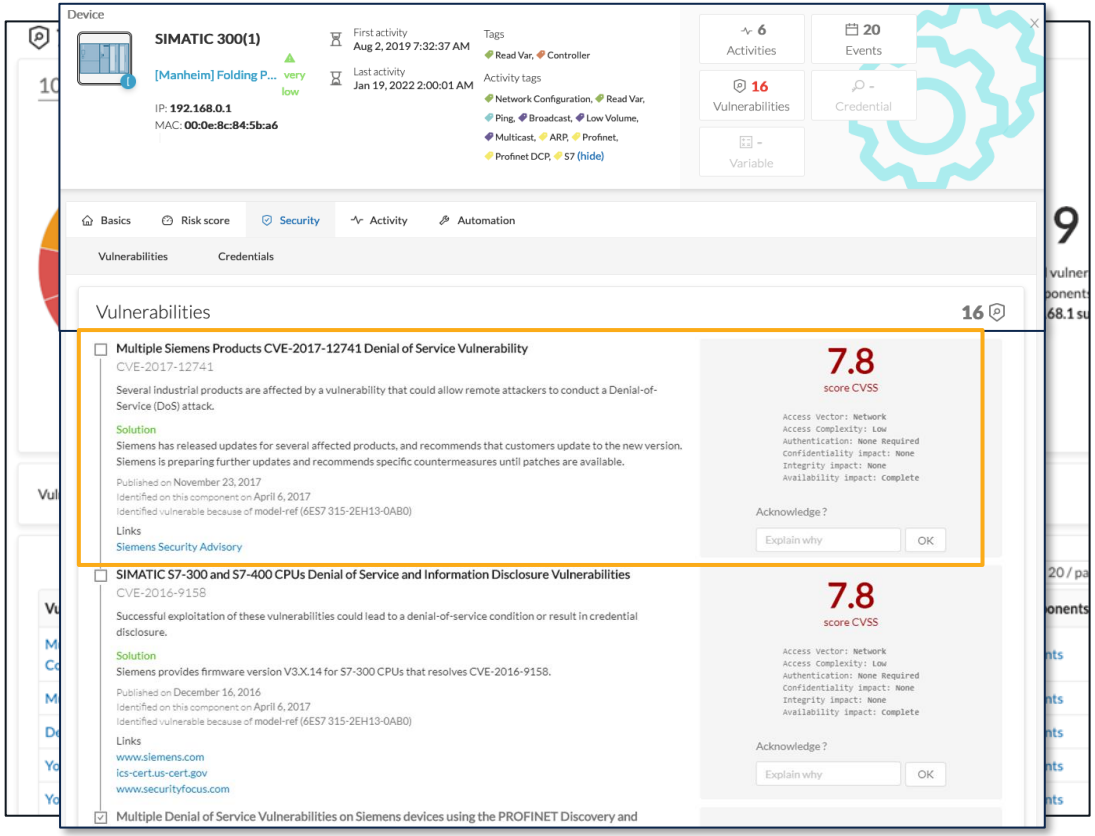
Variable accesses

Rack slot component details

Posture: Identify vulnerabilities to assess risks

Drive vulnerability remediation

- Cyber Vision matches device attributes against the Talos CVE vulnerability database to easily identify vulnerable components
- Automatically spot software & hardware vulnerabilities
- Access comprehensive information on vulnerability severities and solutions

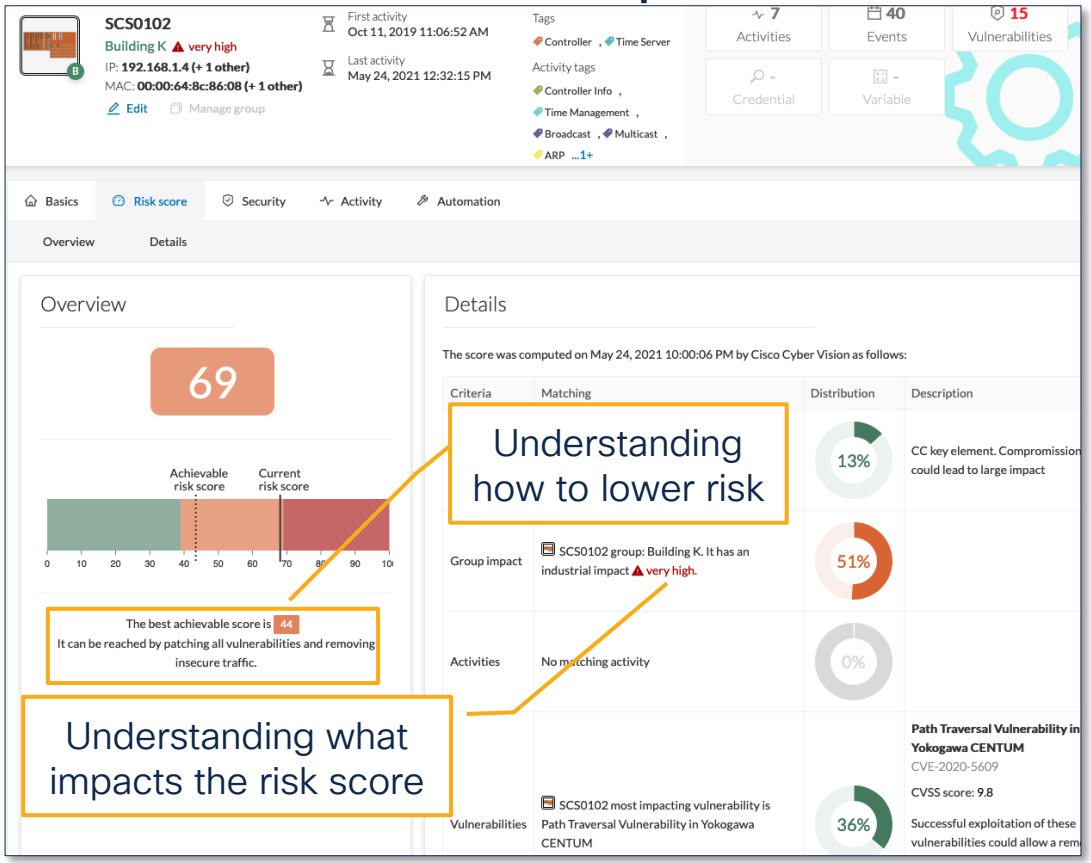


Risk scoring helps focus on what's important

- Provides simple information on the security posture
- Guides users to devices they should deal with first

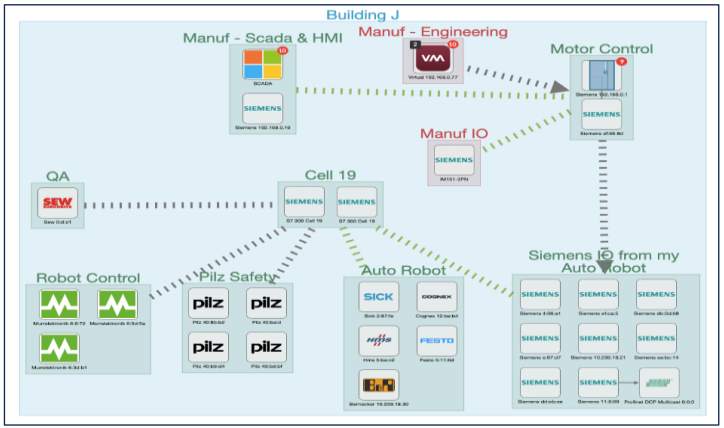
Risk Scores based on likelihood of impact:

- Likelihood → Is it more likely to be compromised?
- Impact → What is the component "criticality"?



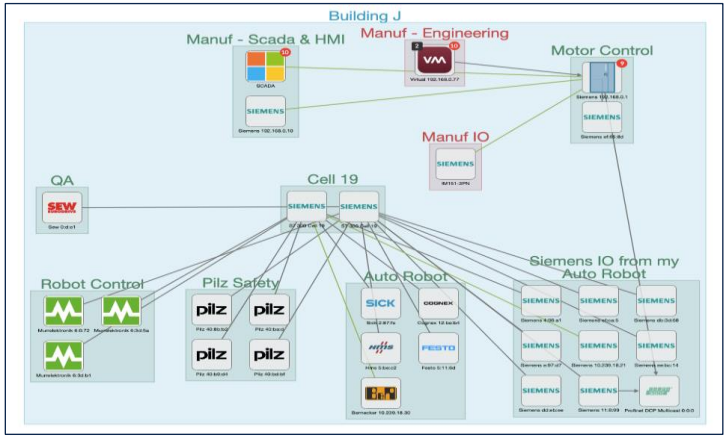
Communication visibility with CyberVision

Conduits



- Organize your map to match the business processes
- Helps with ISA/IEC 62443 compliance
- Enables IT/OT to define security policies

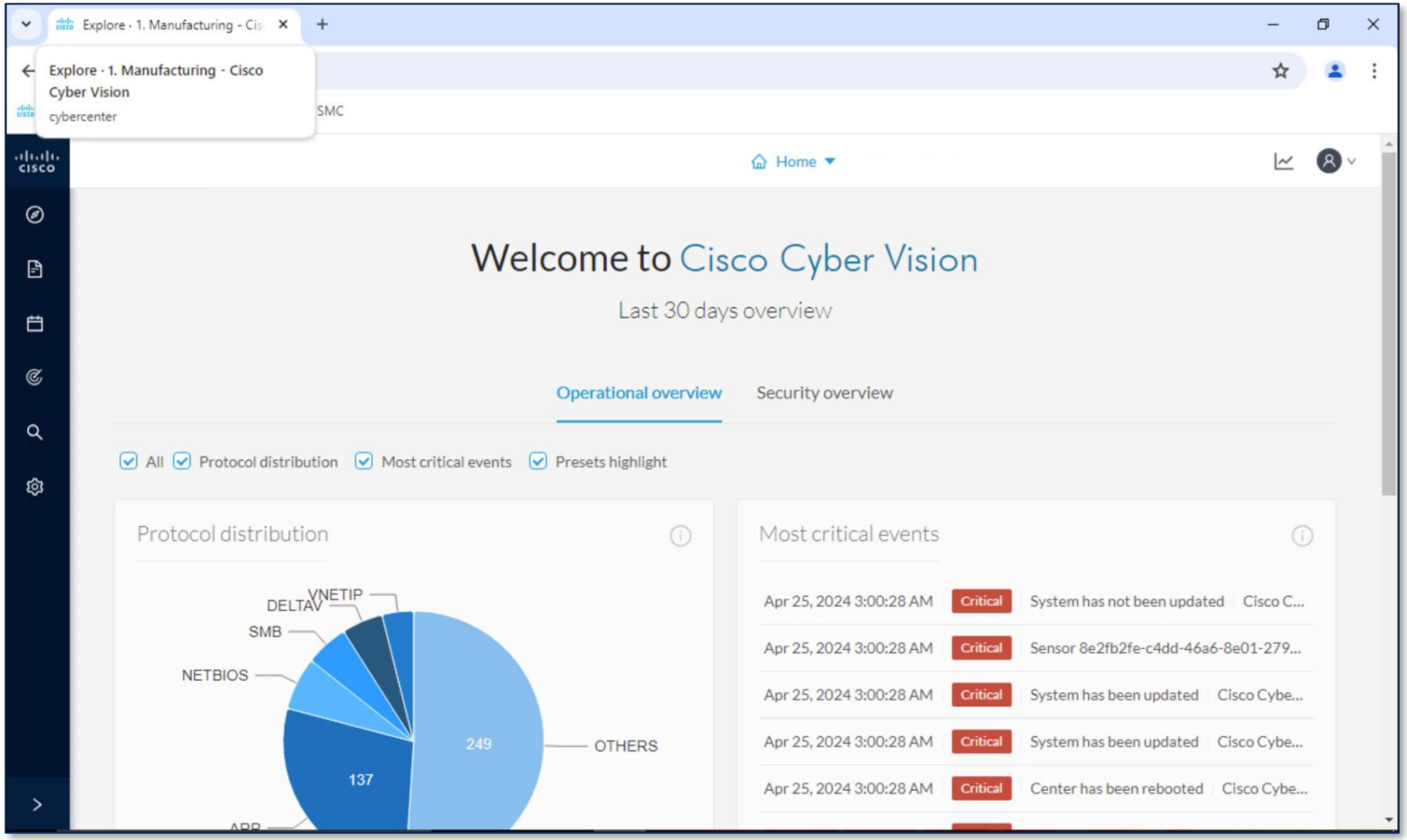
Communication flows



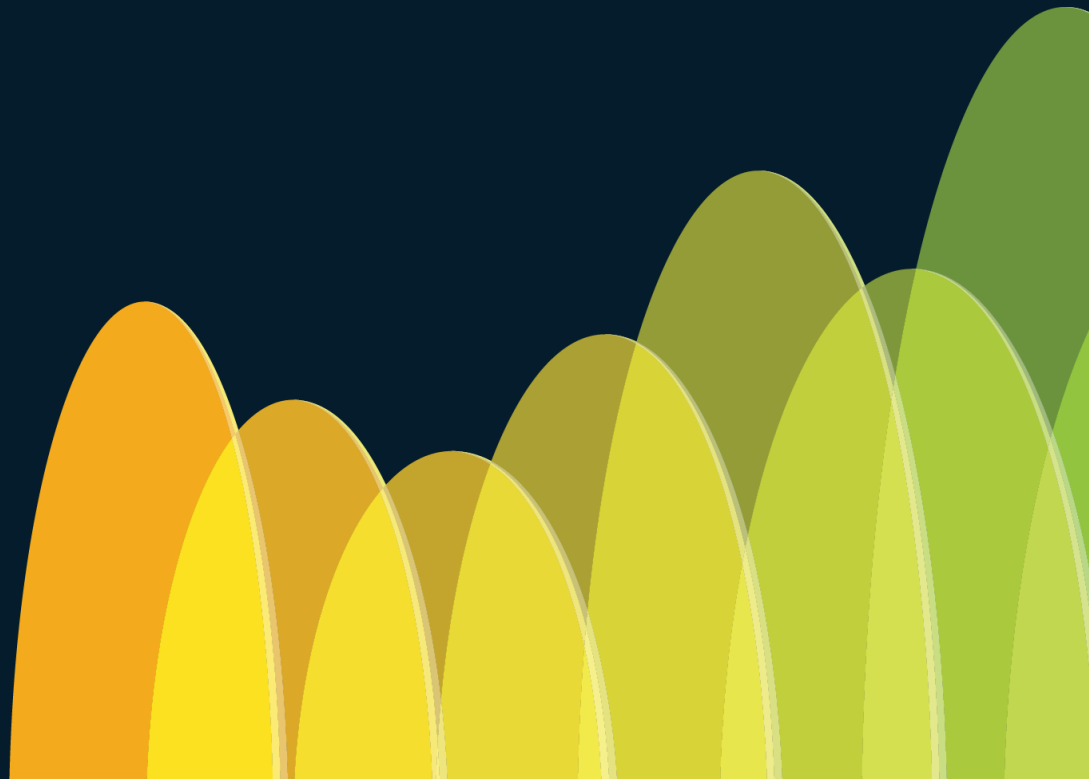
- Identify all relations between assets including application flows
- Spot unwanted communications
- View live information or go back in time

Demo:
Cisco Cyber Vision Overview

cisco Live!



Cisco Identity Service Engine (ISE)



cisco Live!

How ISE enforces Zero Trust

Connecting trusted users and endpoints with trusted resources

- Who
- What
- When
- How
- Where
- Posture
- Threat
- Vulnerability

Authentication

- Endpoint is identified and trust is established
- Posture of endpoint verified to meet compliance

Endpoint classified, and profiled into groups

- Endpoints are tagged x/SGTs
- Policy applied to profiled groups based on least privilege

Trust continually verified

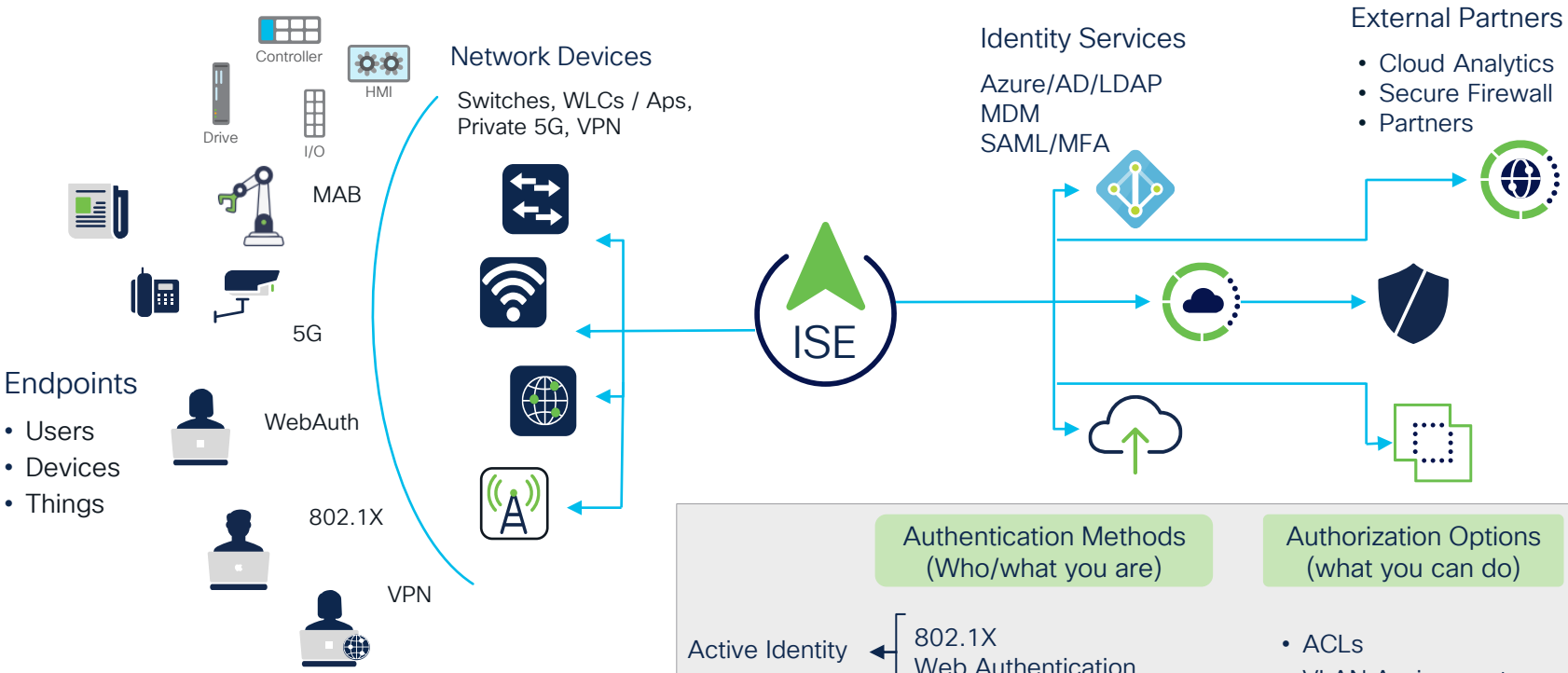
- Continually monitors and verifies endpoint trust level
- Automatically Updates access policy

Cisco DNA Center

Authorized access based on least privilege

- Access granted
- Network segmentation achieved

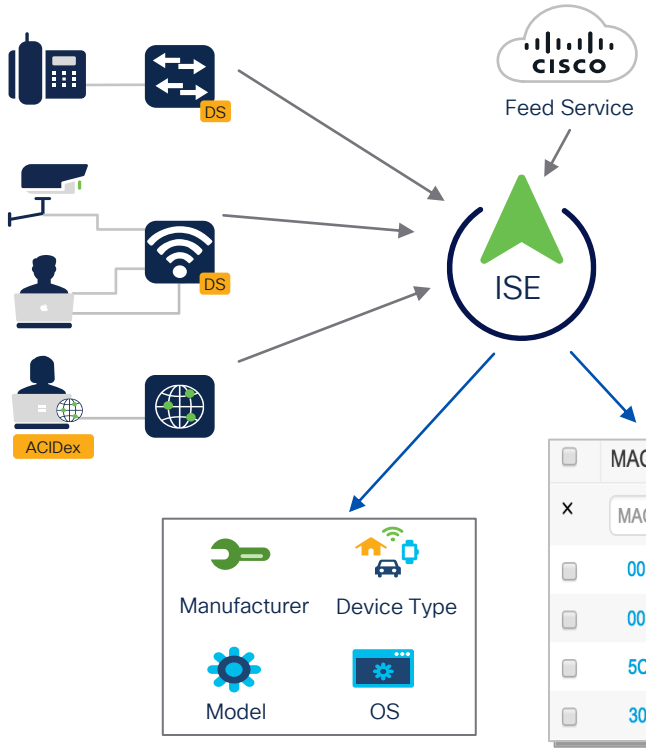
ISE Provides Zero Trust for the Workplace



Endpoint Profiling

The profiling service dynamically classifies devices connected to your network

Endpoints send interesting data, that reveal their device type



ISE Data Collection Methods for Device Profiling

Active Probes: DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

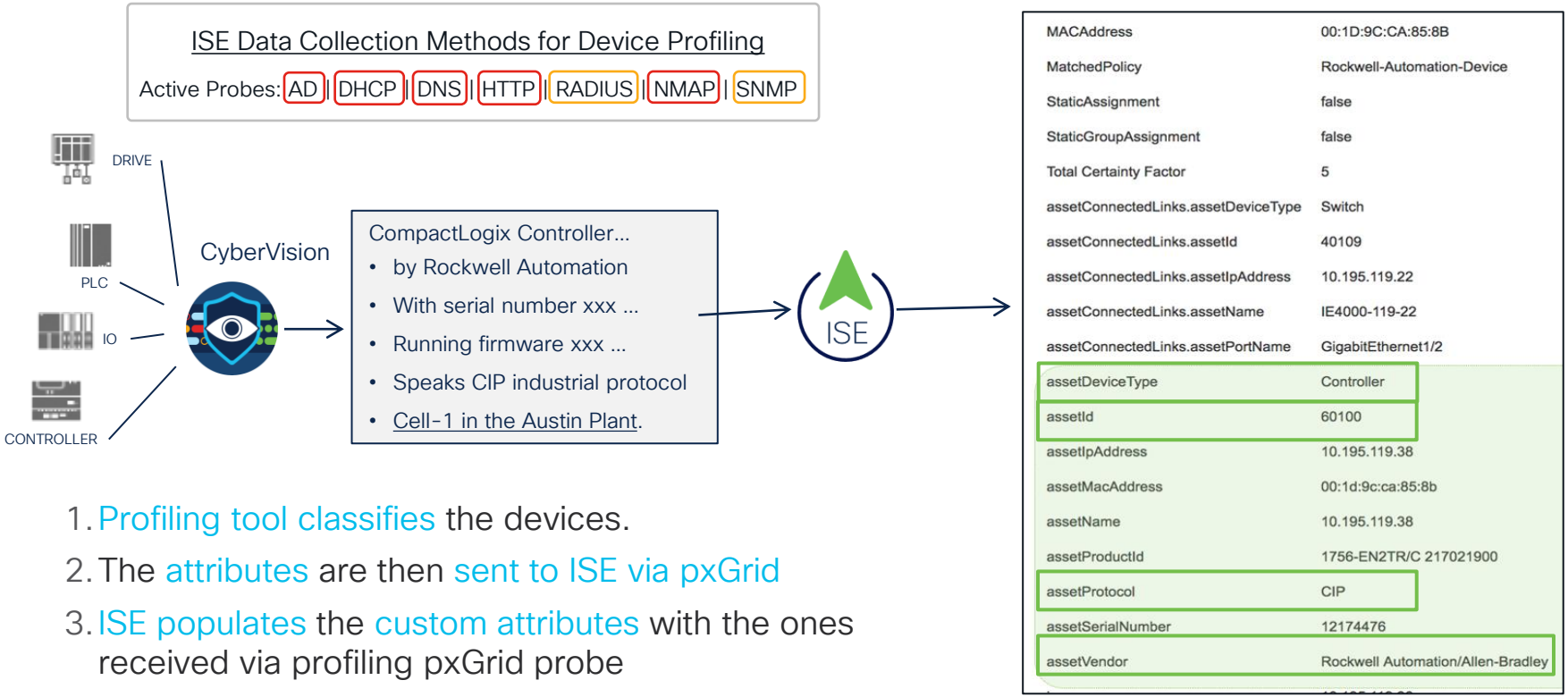
AnyConnect: ACIDex

pxGrid context-in: (DNAC Endpoint Analytics, CyberVision for industrial)

WIFI Edge Analytics: Firmware_version, HW_Model, Manufacturer, Model, OS_Version, Vendor (Samsung, Apple and Intel devices)

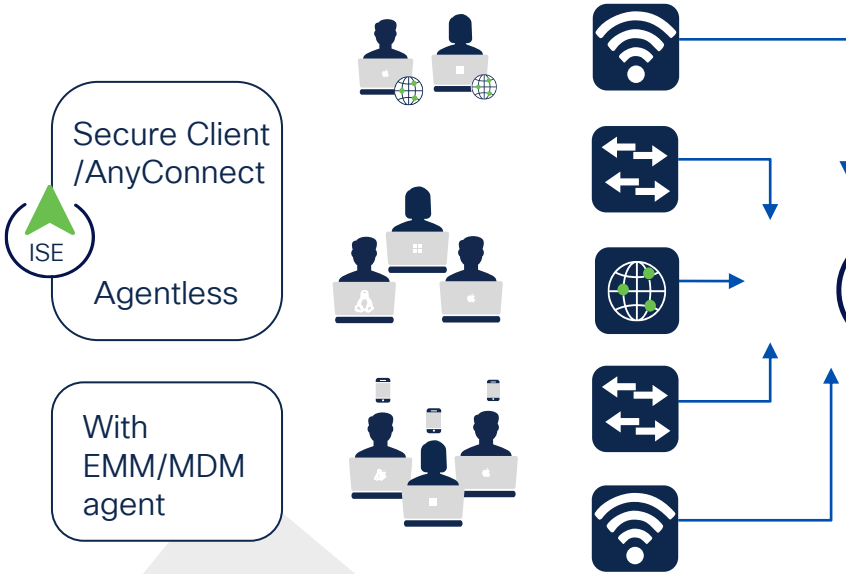
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

Enhancing ISE profiling with CyberVision data



1. Profiling tool classifies the devices.
2. The attributes are then sent to ISE via pxGrid
3. ISE populates the custom attributes with the ones received via profiling pxGrid probe

Posture for endpoint compliance



Posture Policy example

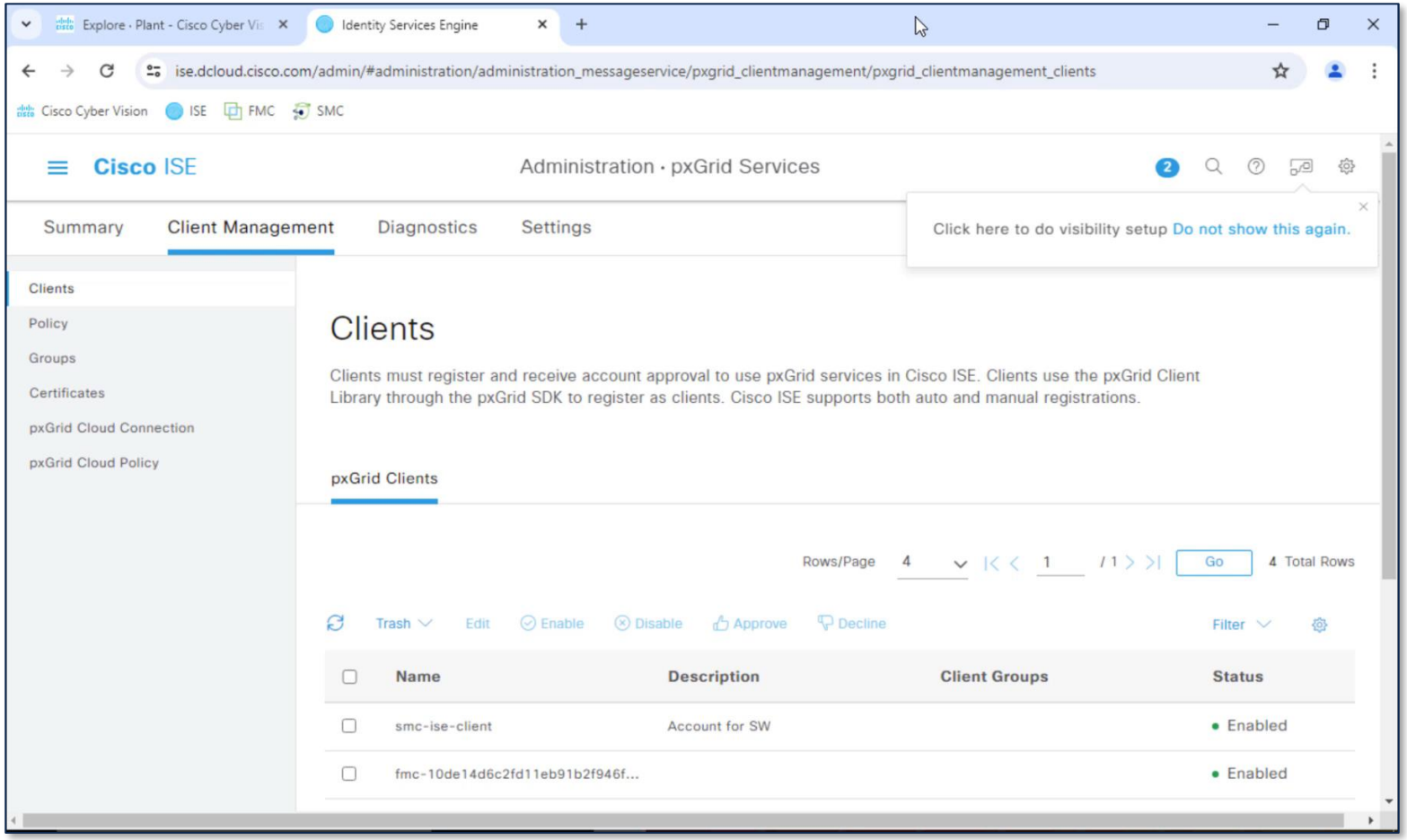
IF AV is installed
AND AV is running
AND AV is UpToDate
THEN is Compliant

IF Jailbroken is No
AND Pinlock is Yes
THEN Compliant

IF
nonCompliant
THEN
Remediate

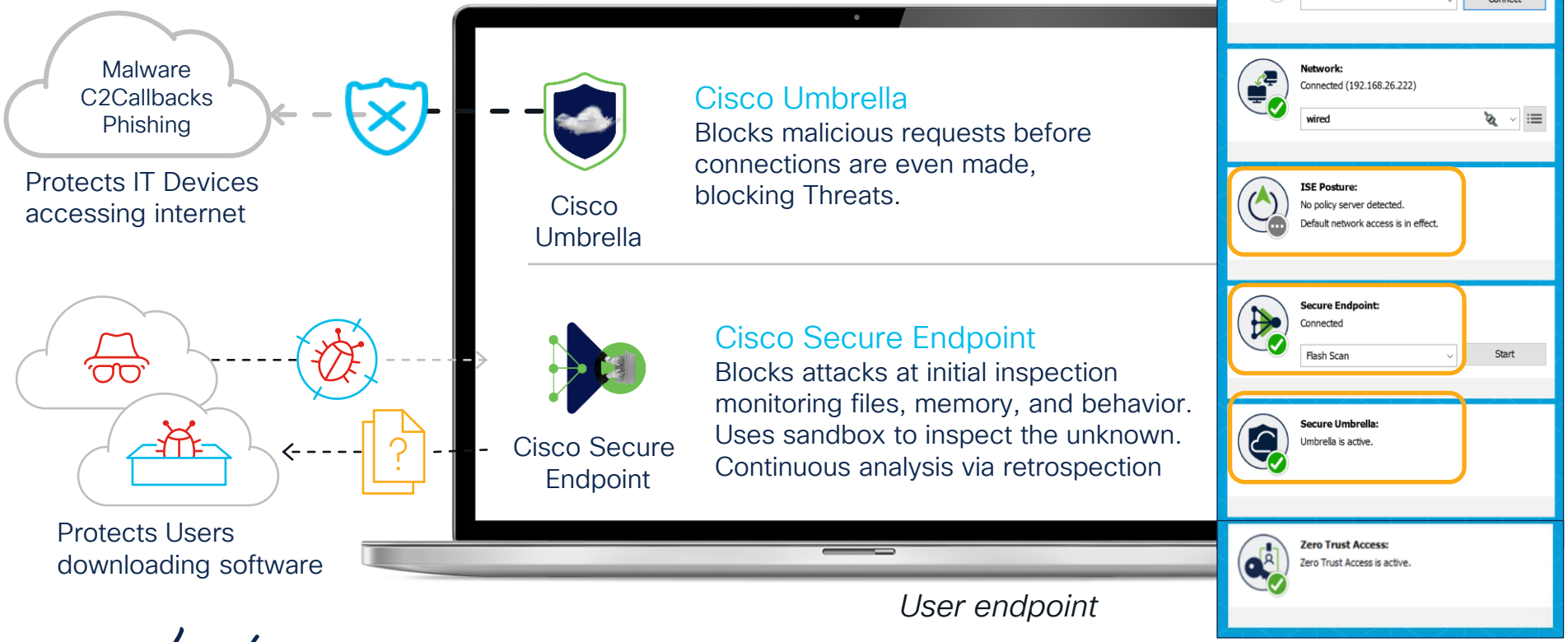
If integrating with EMM/MDM, the logic can be either in ISE or in the partner product, but ISE will enforce it.

Demo:
ISE profiling with Cyber Vision integration

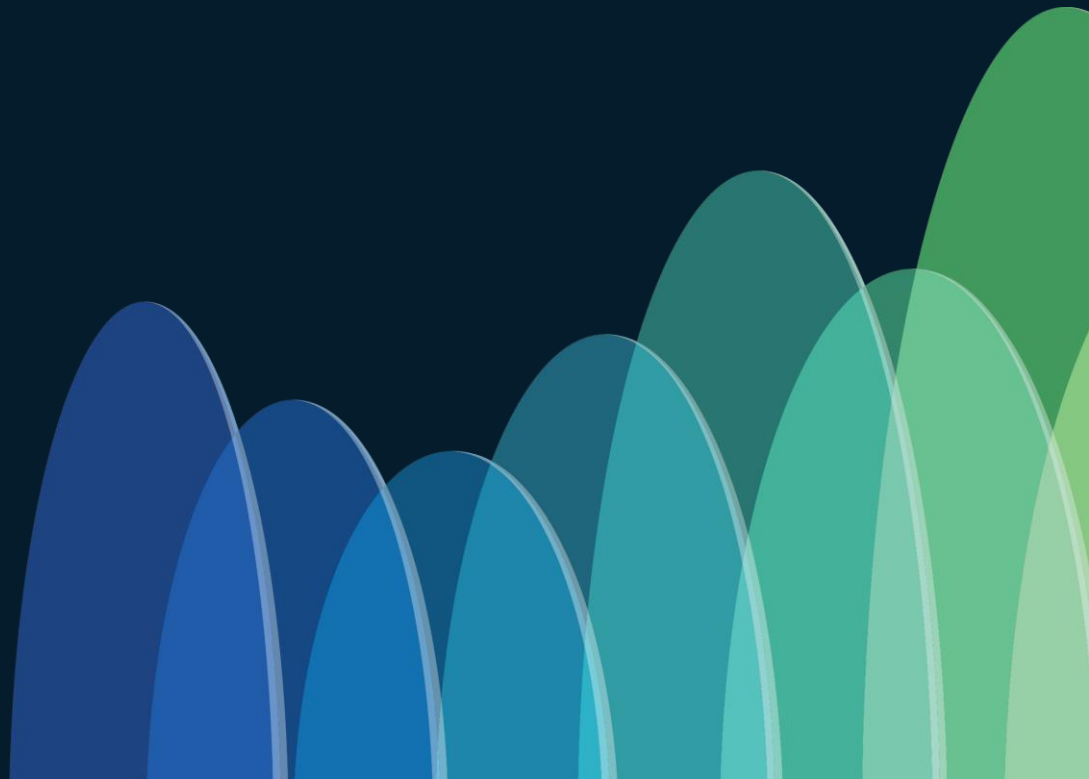


Do not forget Threat Prevention and Control

for user devices



Segment network into smaller zones



Cisco’s Industrial Threat Defense Journey

1

Asset Visibility & Security Posture

Cisco Cyber Vision

Cisco ISE

CV

Network Embedded CV Sensor

2

Zero Trust for OT

Segment network into smaller Zones

IEC 62443 Zones & Conduits

Cisco Secure Firewall

Cisco ISE

Conduit

CV

CV

3

Secure Remote Access

Cisco Secure Equipment Access

SEA

4

Cross-Domain Detection, Investigation & Response

Cisco XDR

splunk> a CISCO company

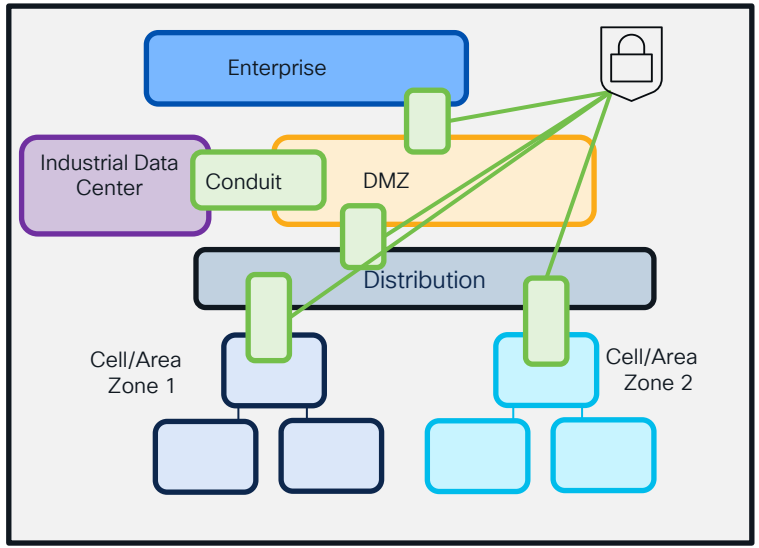
Visibility across the entire attack chain

Macro and Micro segmentation

Macro Segmentation

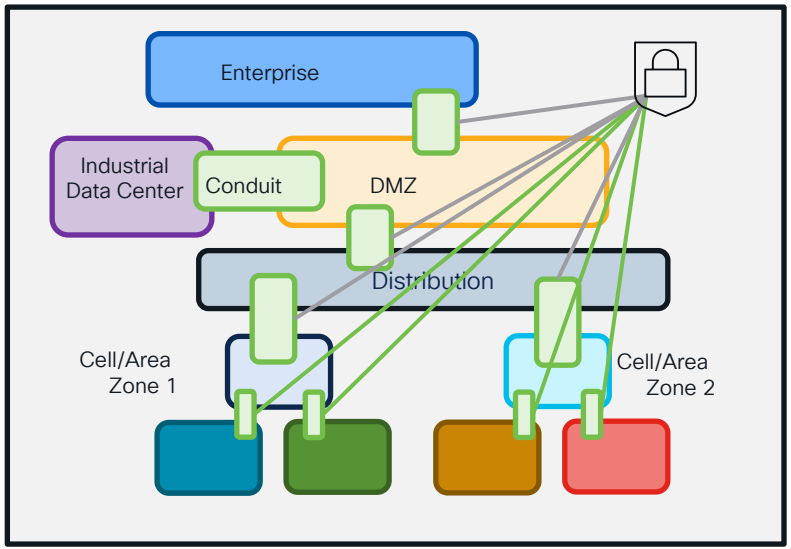
- Policy across “large” zones (between Cell/Area Zones / Production Lines)
- Distribution is typically point of VLAN termination
- Generally done at Firewall level

ISA/IEC 62443



Micro Segmentation

- Pushing policy across “small” zones
- Segmentation within Cell/Area Zones
- It can be done on firewall, switches or routers



The value of TrustSec

Intent Based segmentation

	Enterprise	DMZ	IDC	Cell 1	SIS
Enterprise	✓	✗	✓	✗	✗
DMZ	✗	✓	✓	✗	✗
IDC	✓	✓	✓	✓	✗
Cell 1	✗	✗	✓	✓	✗
SIS	✗	✗	✗	✗	✓

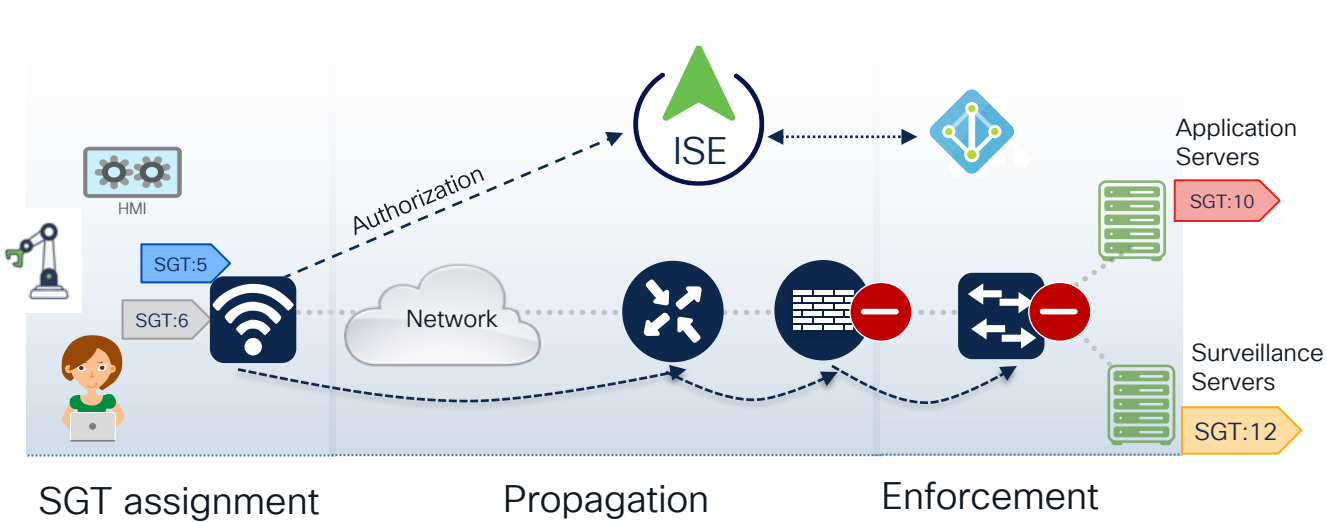
1. Traditional Segmentation Policy

```
Switch-1#show ip access-list
Extended IP access list CorpPolicy
    10 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 80
    20 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 443
```

2. TrustSec Segmentation Policy

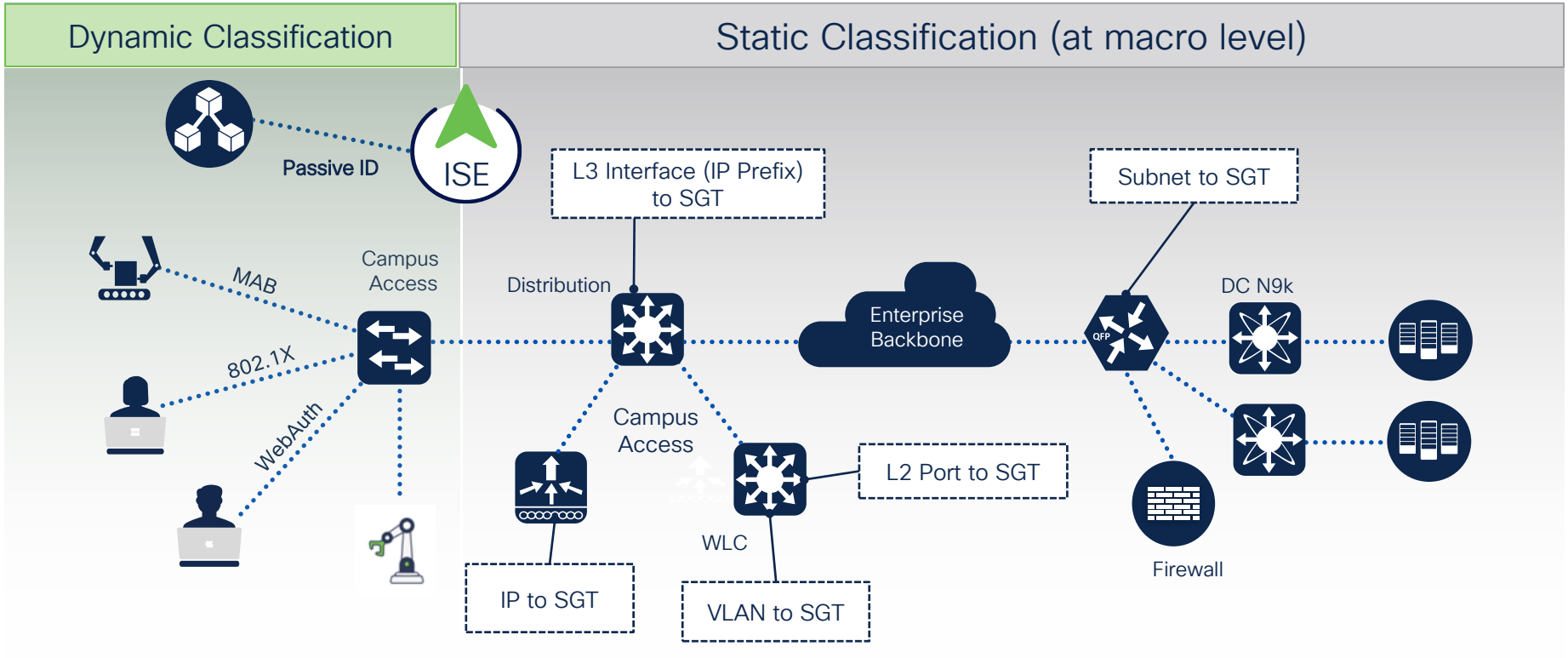
```
Switch-1# show cts role-based permissions
IPv4 Role-based permissions default:
        Deny IP-00
IPv4 Role-based permissions from group 10:Area_1 to group 100:Area_2:
```

TrustSec concepts



- Assignment of Security Group Tag (SGT) based on context (identity, device group, etc.).
- SGT are carried propagated through the network
- Firewalls, routers and switches use SGT to make filtering decisions via SGACL.

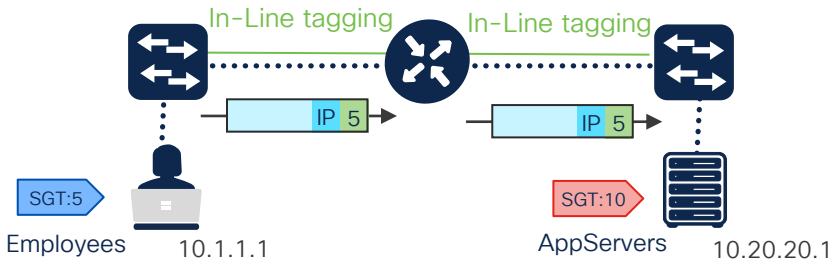
Classification Mechanisms



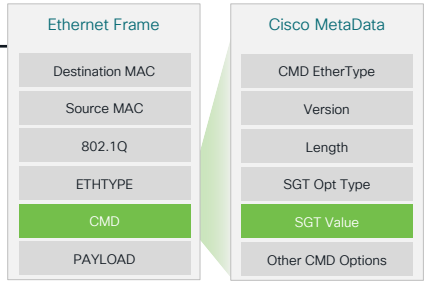
SGT Propagation

DATA PLANE PROPOGATION (INLINE TAGGING)

- 16 bit TAG in the CMD of the Ethernet Frame
- SGT Carried inline within the data traffic

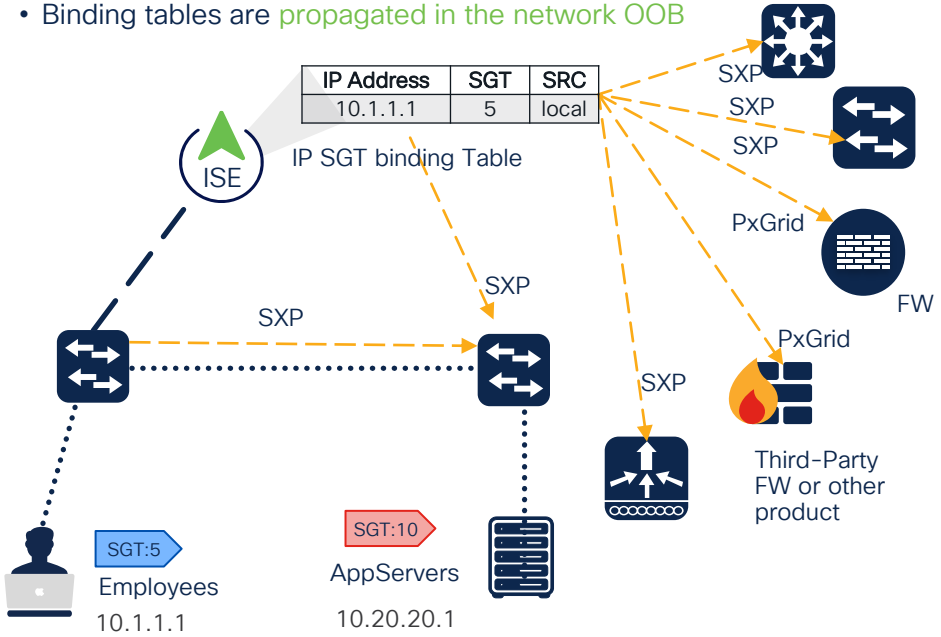


Propagation options			
Cisco Meta Data (CMD)	Ethernet	MACsec	VXLAN
IPsec	DMVPN	GETVPN	



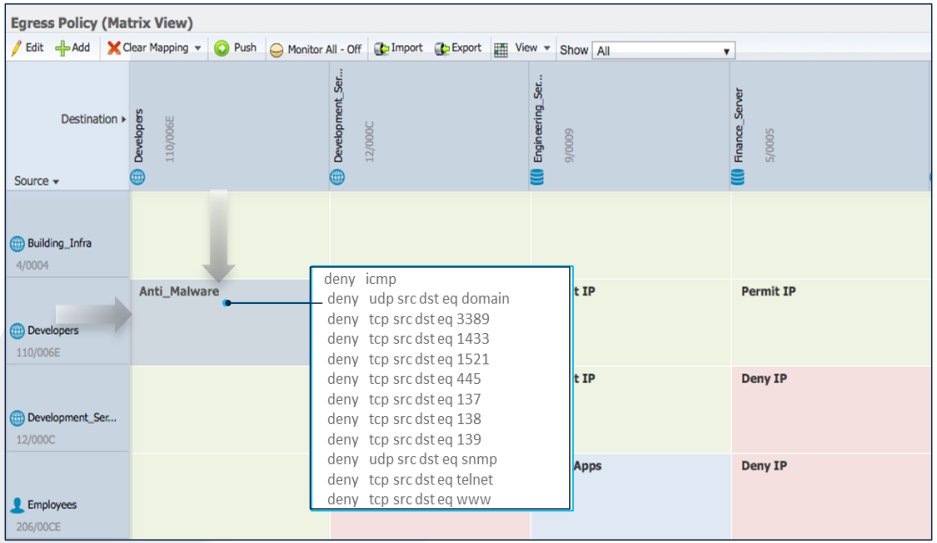
CONTROL PLANE PROPOGATION (SXP/PxGrid)

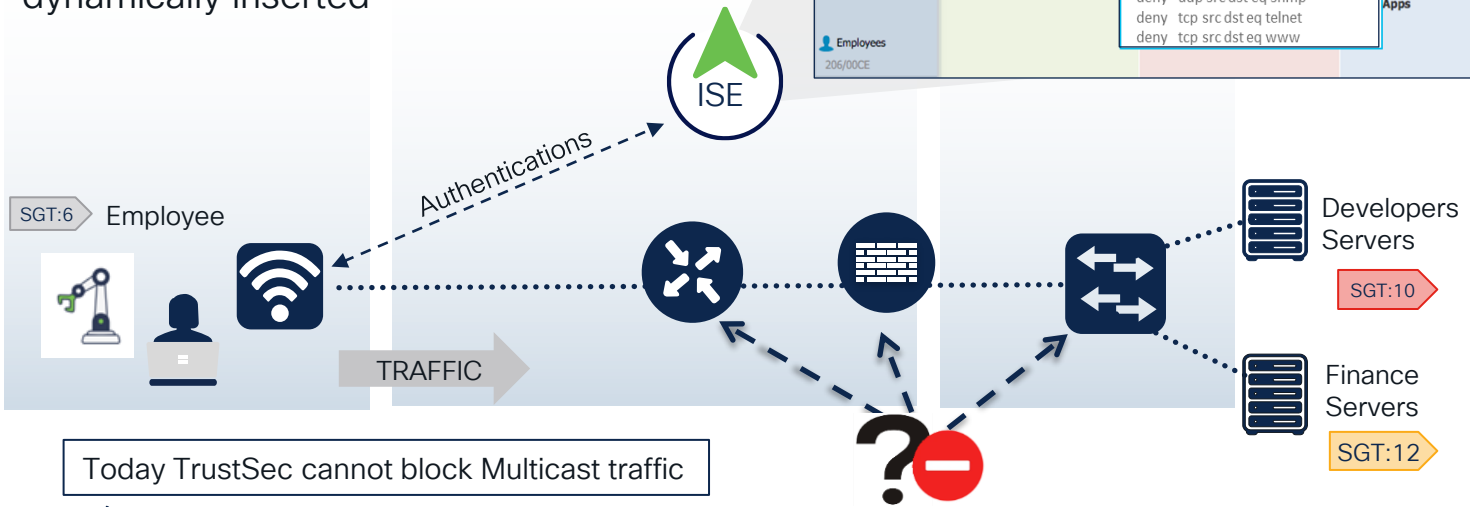
- IP-to-SGT data shared over control protocol.
- No SGT in the data plane and no hardware dependencies.
- Devices (and ISE) have their binding table with the mappings they know.
- Binding tables are propagated in the network OOB



Enforcement options

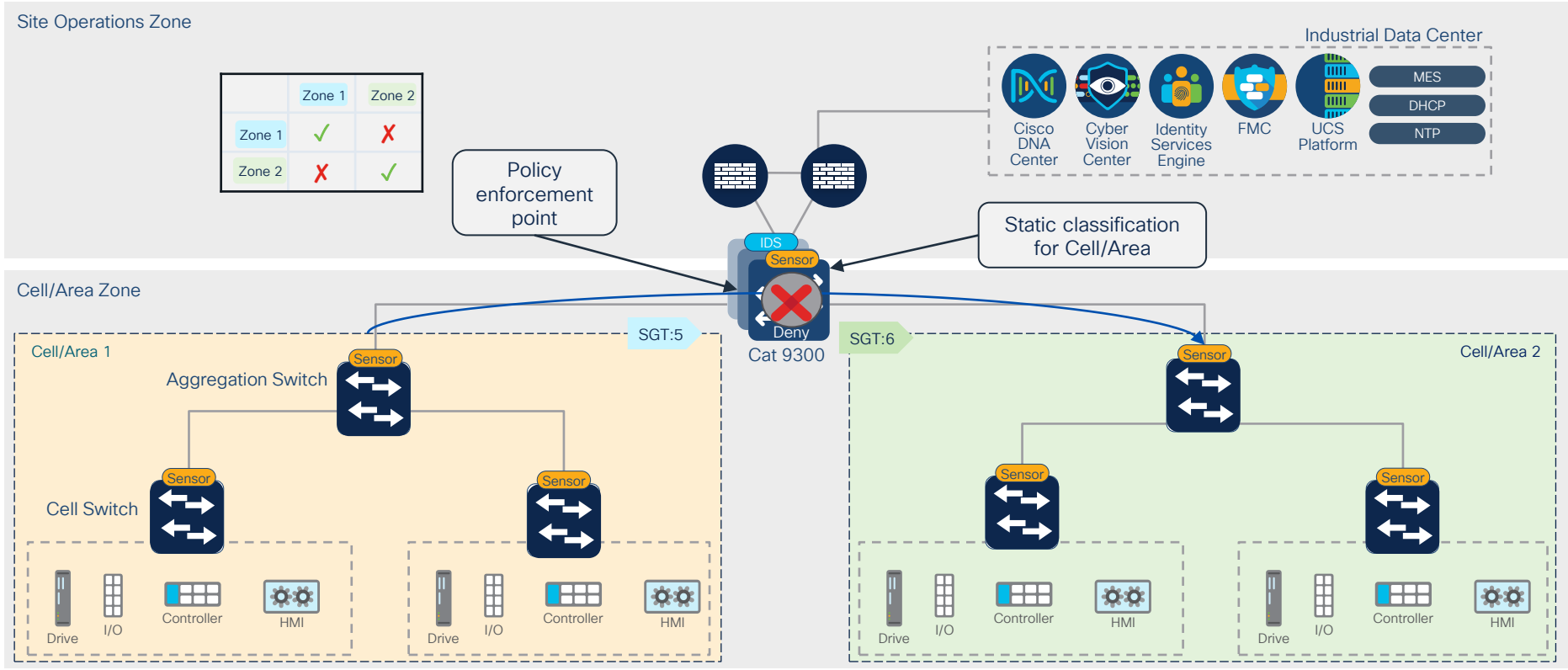
- Policies based on SGT and not on network dependent element like IP address
- SGACL include only protocol and port, while the source and destination are dynamically inserted



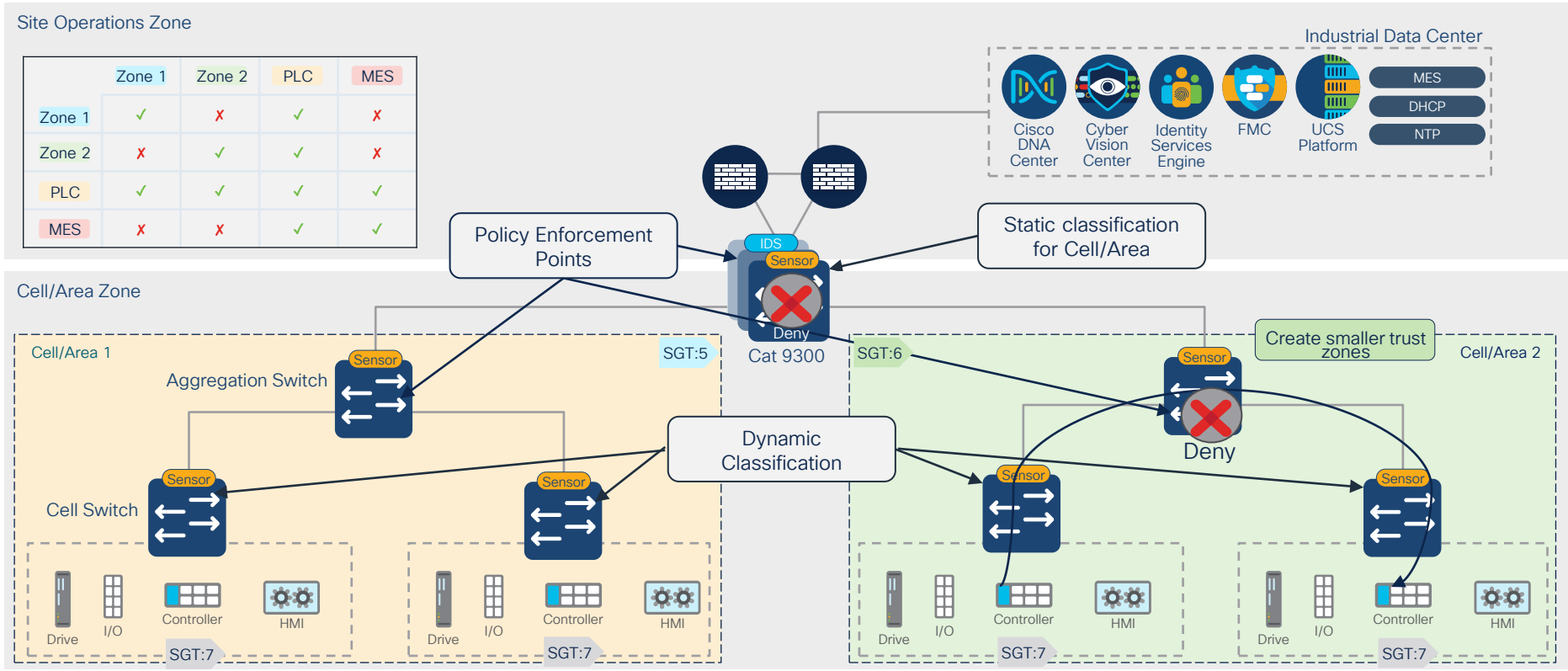


Today TrustSec cannot block Multicast traffic

Network based zoning model



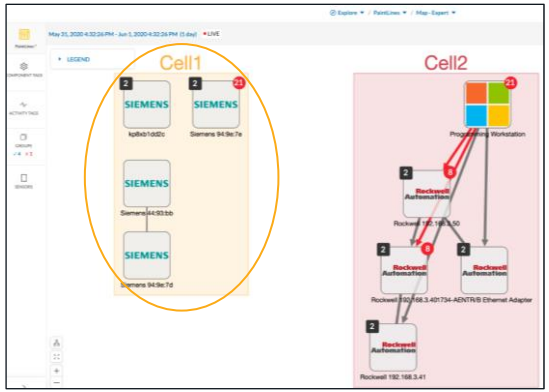
Extending segmentation to the Cell/Area zone



Policy control directly from CyberVision

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

I now have OT context to build the right security policies

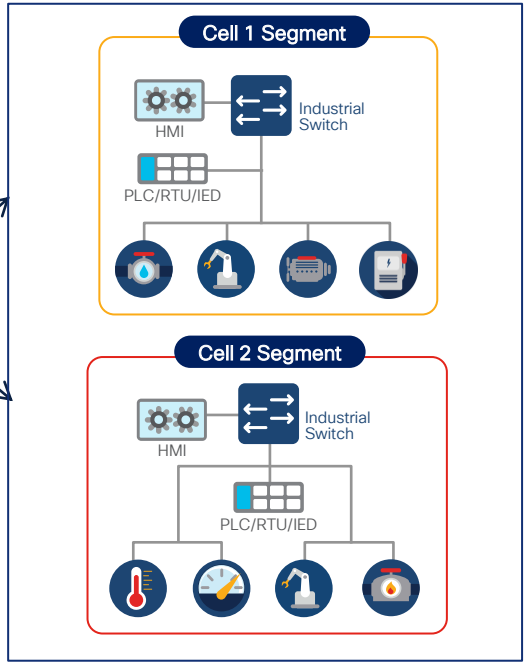


Cyber Vision Map View

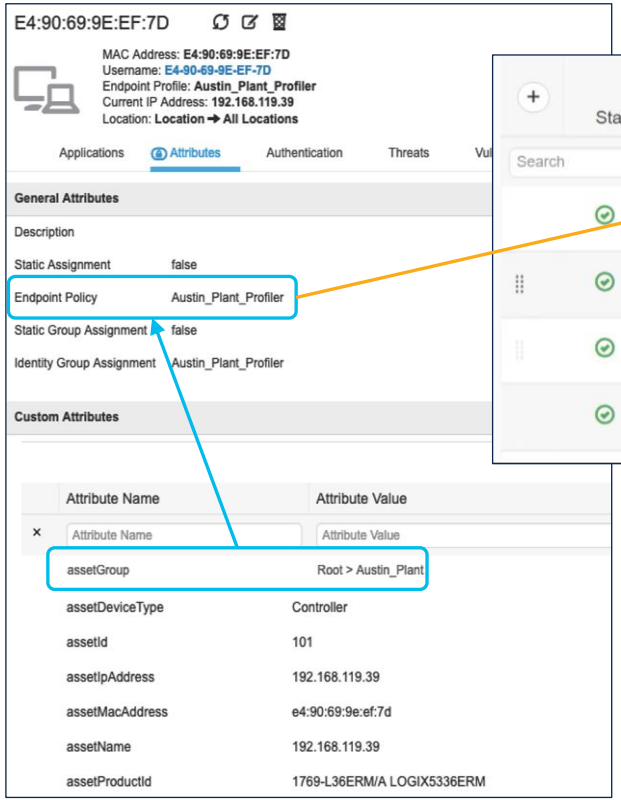
	Cell 1	Cell 2	PLC	MES
Cell 1	✓	✗	✓	✗
Cell 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

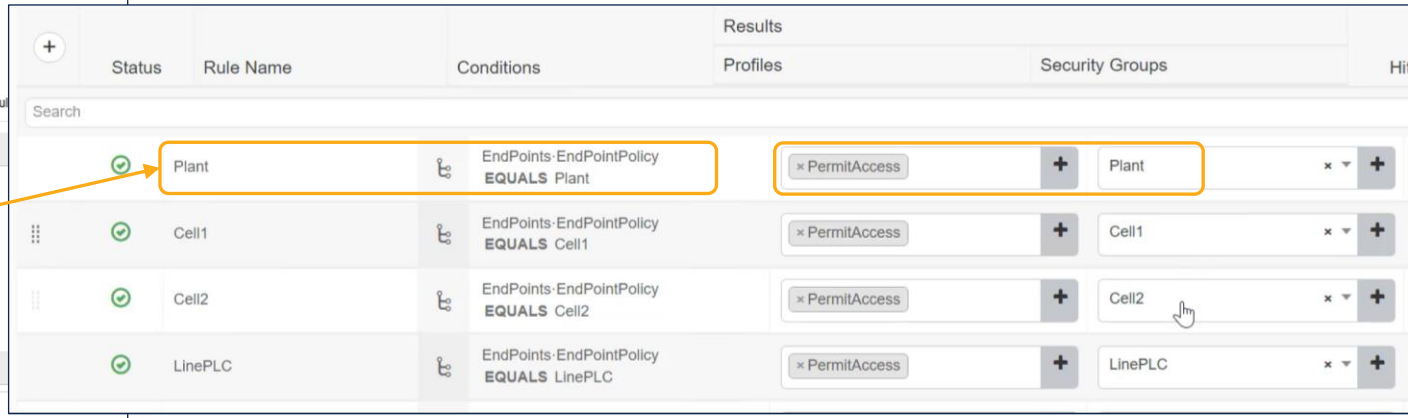
Cisco ISE Policy Matrix

Segmentation of industrial network



Dynamic Classification in the Network





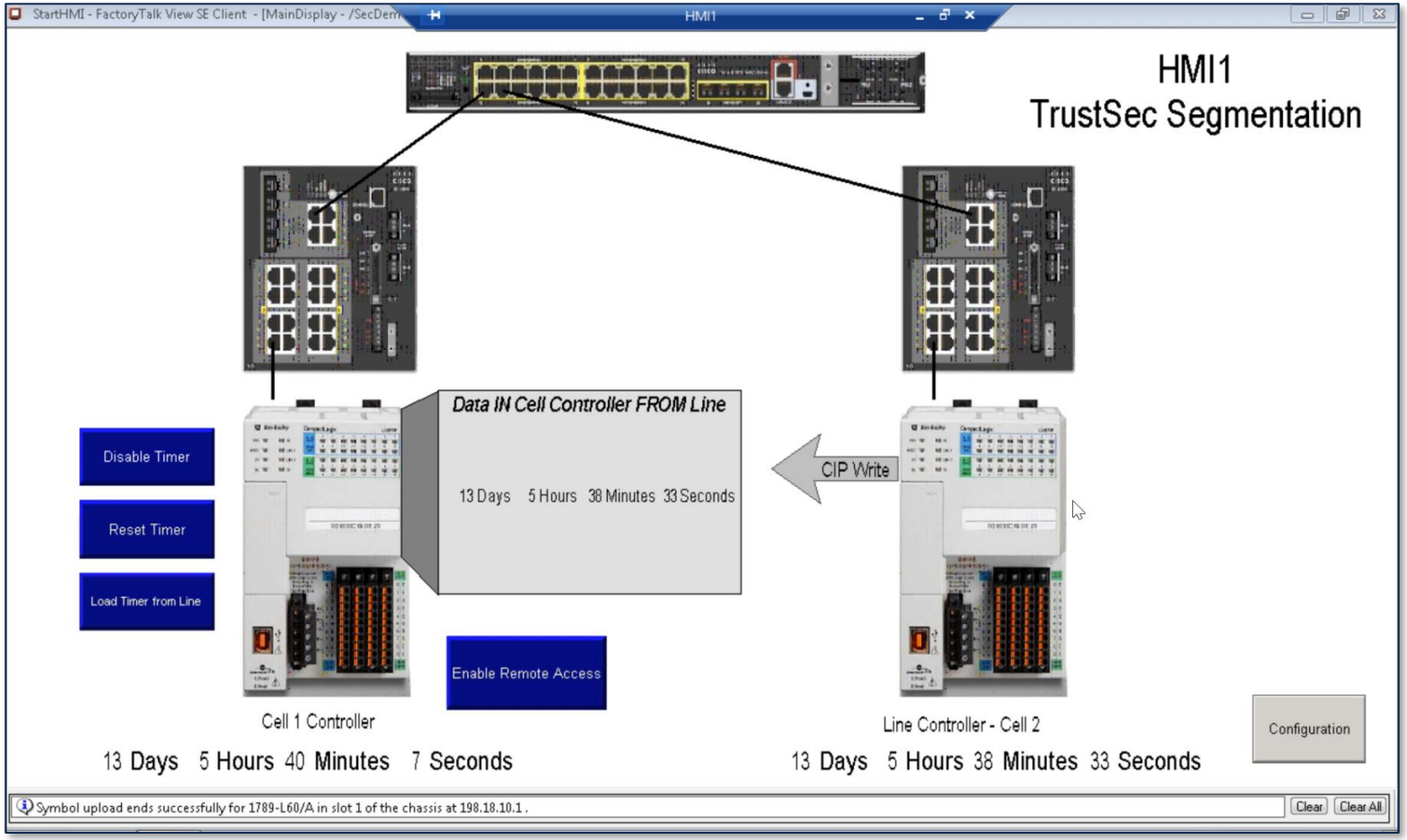
1. ISE receives devices' attributes from Cyber Vision

2. ISE classifies the device according to assetGroup received

3. ISE assigns dynamic policies (VLAN, DACL or TrustSec) based on the profile assigned

Demo: Dynamic Classification with Cyber Vision and ISE

cisco Live!

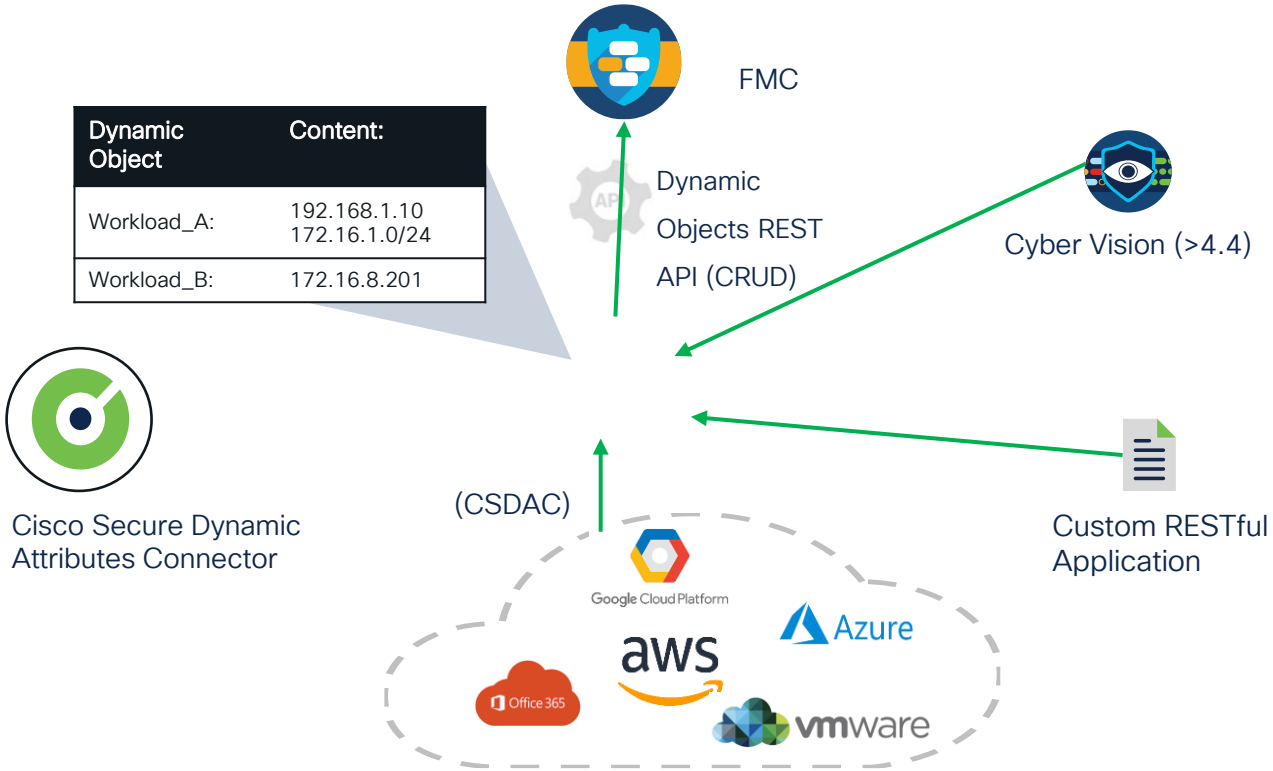


Dynamic objects in Cisco Secure Firewall

Cisco Secure Dynamic Attributes Connector

Middleware engine populating Dynamic Objects

Accelerate integration with automatic propagation of host attributes and contexts



Dynamic Objects in Action

Cisco Secure Dynamic Attributes Connector

API calls for groups and associated IPs

Cyber Vision

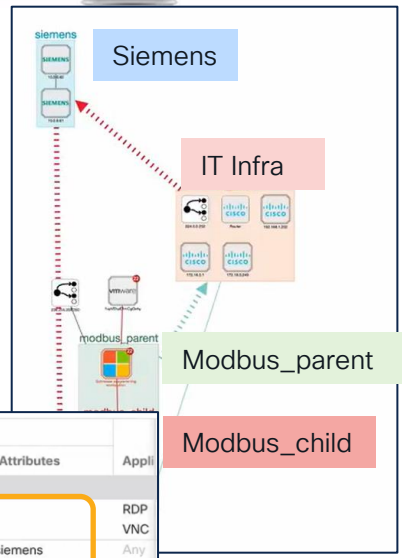
Dynamic Objects (REST)

FMC

Dynamic Objects

Name
center1_it_infra
center1_modbus_child
center1_modbus_parent
center1_ot_infra
center1_siemens
center1_suspicious_block
center1_very_suspicious_quarantine

Dynamic Object	Content:
IT Infra:	172.23.33.10 172.23.33.11
Siemens	10.99.99.8 10.99.99.9

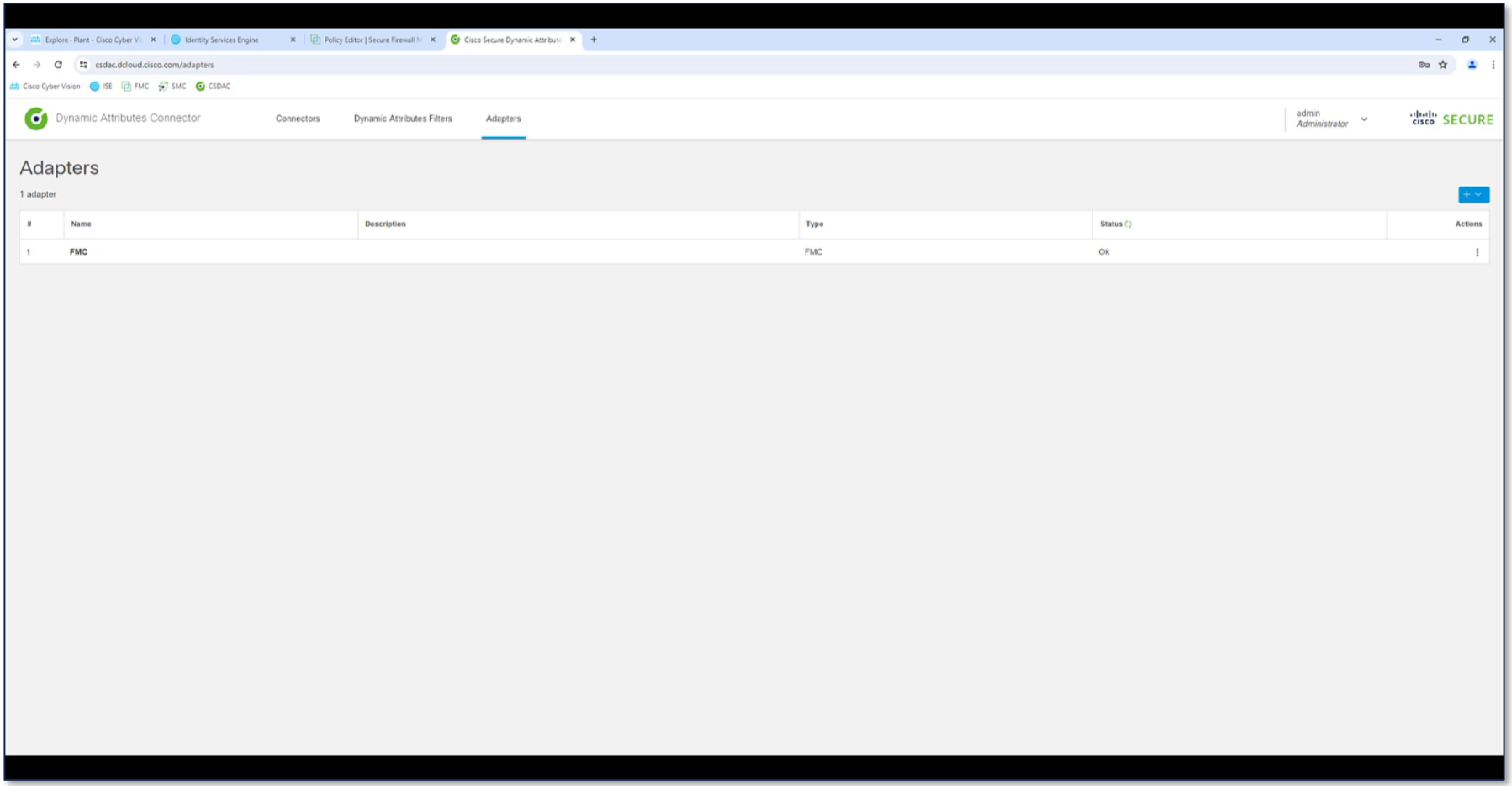


Show IP Mappings

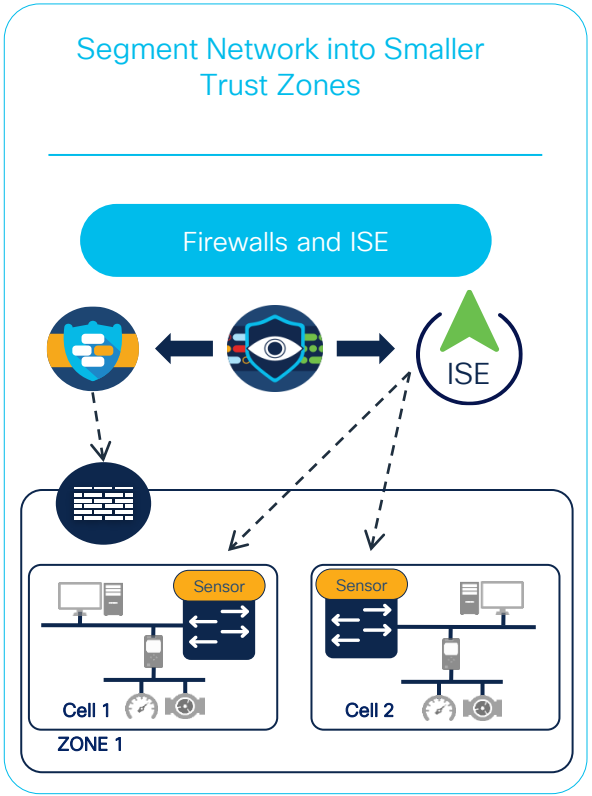
	Name	Action	Source				Destination				Appli
			Zones	Networks	Ports	Dynamic Attributes	Zones	Networks	Ports	Dynamic Attributes	
Mandatory (1 - 3)											
1	siemens cell block RDP an...	Block	Any	Any	Any	center1_siemens	Any	Any	Any	Any	RDP VNC
2	cyber vision block inter cell	Block	Any	Any	Any	center1_modbus_child	Any	Any	Any	center1_siemens	Any
3	suspicious cyber vision 1 -...	Block	Any	Any	Any	center1_very_suspicious...	Any	Any	Any	Any	Any
efault (-)											

Demo: Cisco Secure Dynamic Attributes Connector

cisco Live!



Dynamic Segmentation options



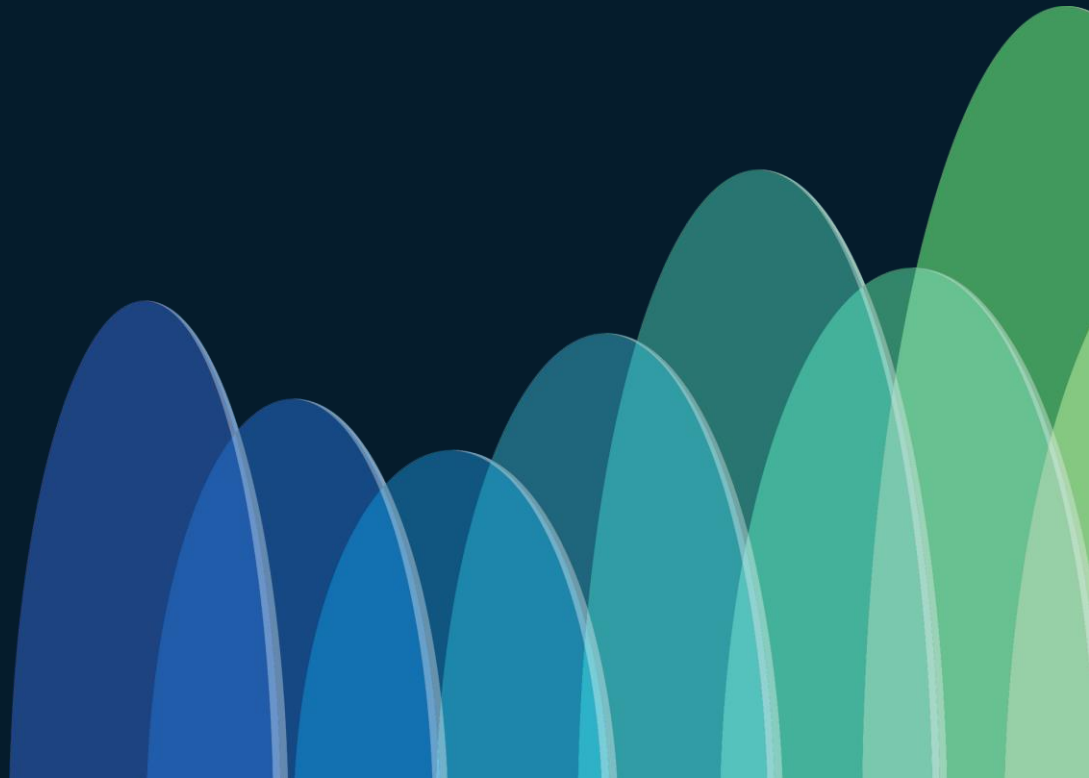
Segmentation policies based on business logic driven by Cyber Vision

No need to know IP and MAC addresses.

Dynamic Objects in the Firewall.

TrustSec with SGTs on switches or firewalls.

Secure Remote Access



cisco Live!

Cisco's Industrial Security Journey

1

Asset Visibility & Security Posture

Cisco Cyber Vision

Cisco ISE

Network Embedded CV Sensor

2

3

Zero Trust for OT

Segment network into smaller Zones

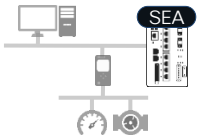
IEC 62443 Zones & Conduits

Cisco Secure Firewall

Cisco ISE

Secure Remote Access

Cisco Secure Equipment Access



4

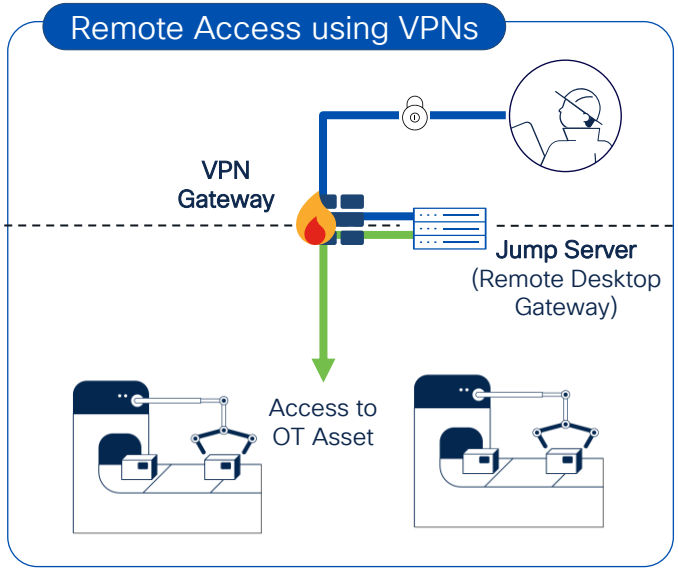
Cross-Domain Detection, Investigation & Response

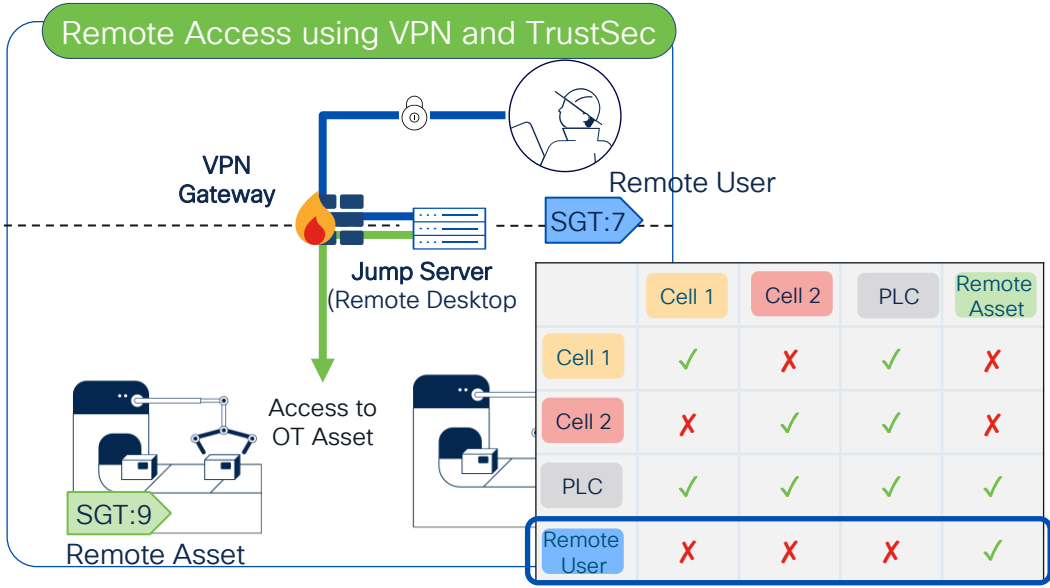
Cisco XDR

splunk> a CISCO company

Visibility across the entire attack chain

Enhancing VPNs with TrustSec



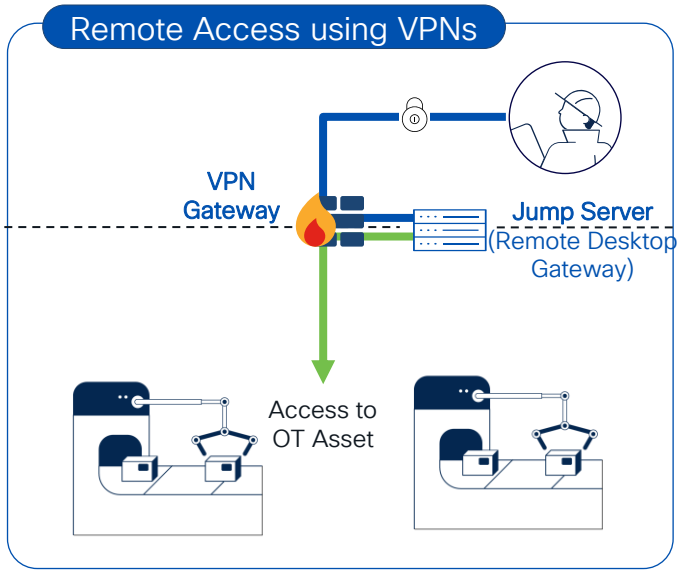


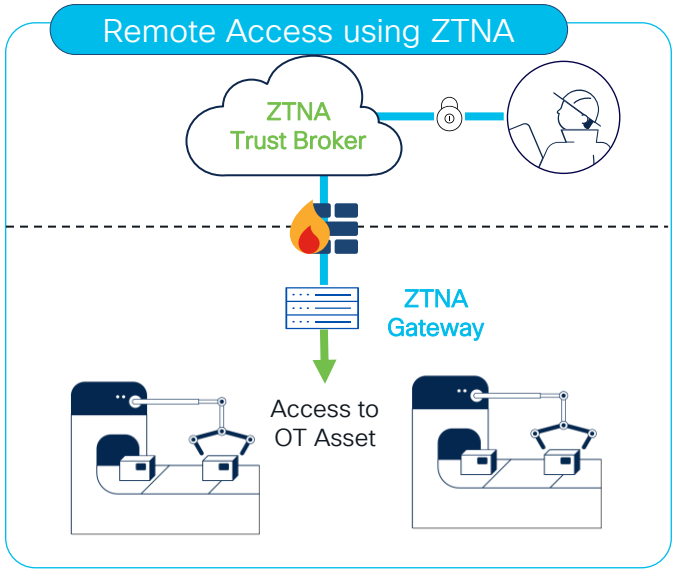
- Always-on solutions with all-or-nothing access
- Firewall rules need to be frequently updated
- Manual session management using jump servers

- Via CyberVision OT arraigns the device to a “Remote Asset“ Group when access needed
- ISE dynamically reclassifies the device to the appropriate SGT
- The remote user has access only to the remote Asset device when it is needed

Evolving to ZTNA

From Implicit to explicit Trust





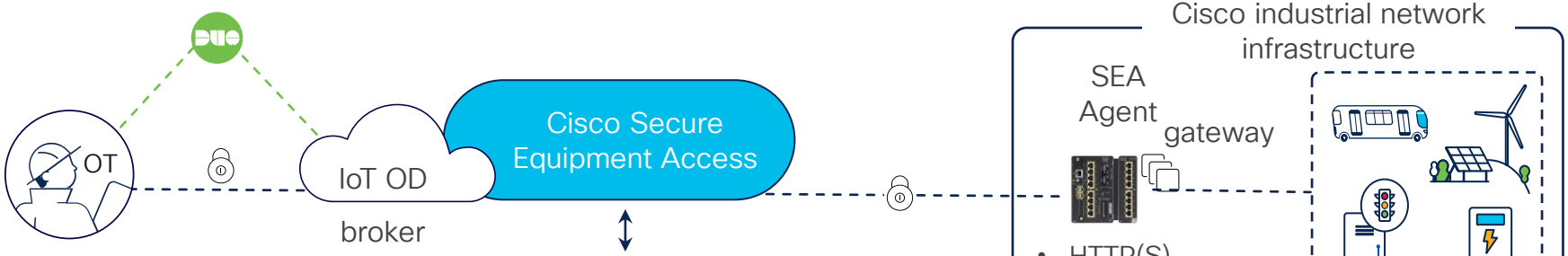
- Always-on solutions with all-or-nothing access
- Firewall rules need to be frequently updated
- Manual session management using jump servers

- Trust broker manages policy based on identity and context, and grants access to specific resources at specific times
- Gateway establishes an outbound connection to the trust broker eliminating complexity of firewall rules

Secure Remote Access

with Secure Equipment Access

Perform remote operations while enforcing strong zero trust controls



Browser-based and native application access for remote users

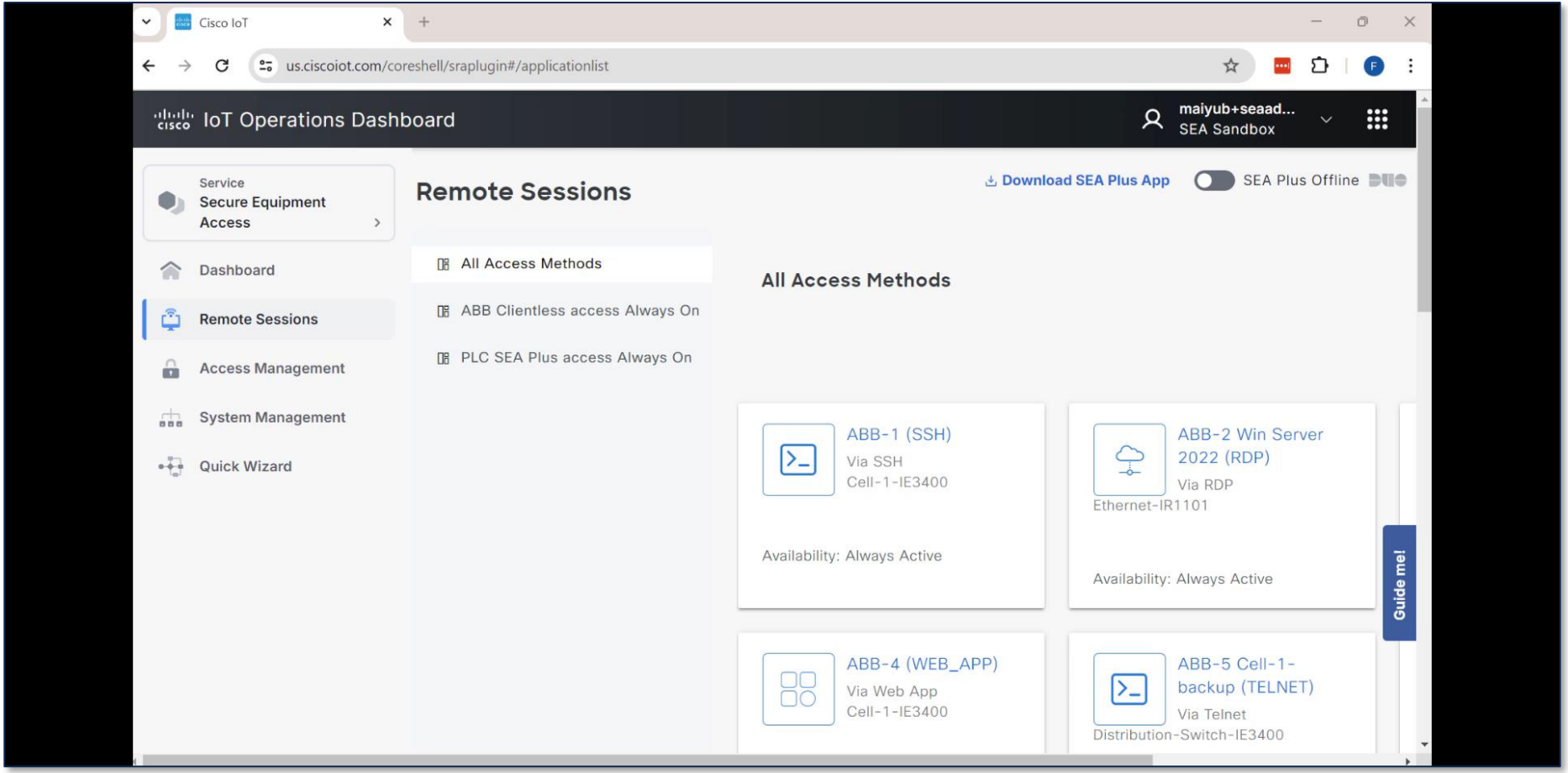
Zero trust remote session control

- ✓Grant access only to specific assets using specific protocols at specific times/days
- ✓Multi-factor authentication
- ✓Remote user posture check
- ✓Session recording, monitoring, termination

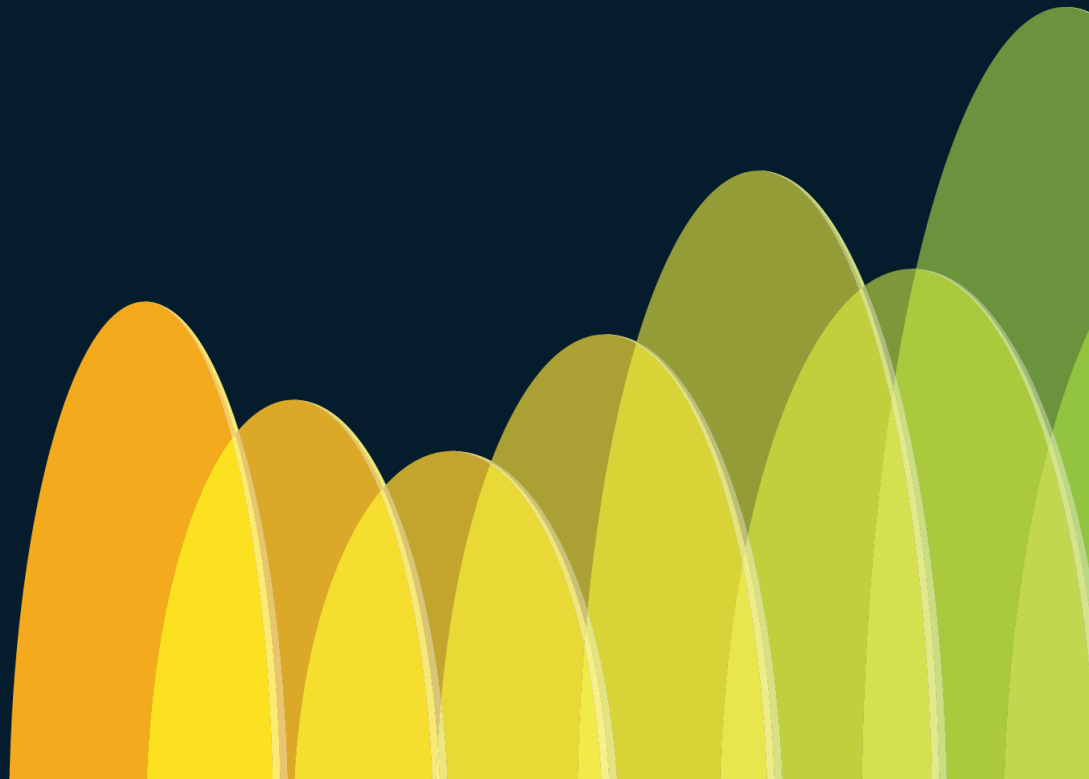
Catalyst Industrial Routers or Switches with embedded SEA gateway software

Demo: Cisco Secure Equipment Access

cisco Live!



Detection, Investigation & Response



cisco Live!

Cisco’s Industrial Threat Defense Journey

1

Asset Visibility & Security Posture

Cisco Cyber Vision

Cisco ISE

Network Embedded CV Sensor

2

3

Zero Trust for OT

Segment network into smaller Zones

IEC 62443 Zones & Conduits

Cisco Secure Firewall

Cisco ISE

Secure Remote Access

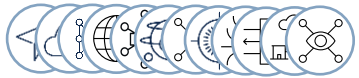
Cisco Secure Equipment Access

4

Cross-Domain Detection, Investigation & Response

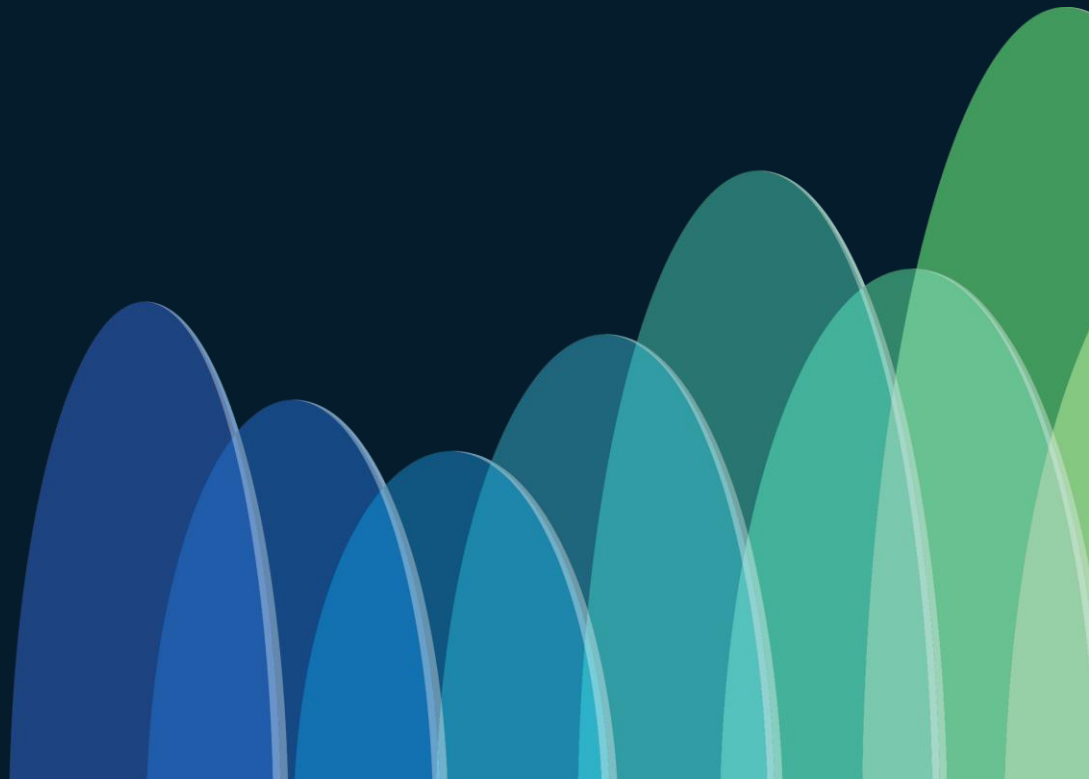
Cisco XDR

splunk> a cisco company



Visibility across the entire attack chain

Anomaly Detection



CyberVision Highlights abnormal behaviors

Cyber Vision behavior modeling automatically triggers alerts on deviations from the **baselines**

Cyber Vision Baselines let you define what “normal” should be and analyze every application flows to detect deviations

New asset

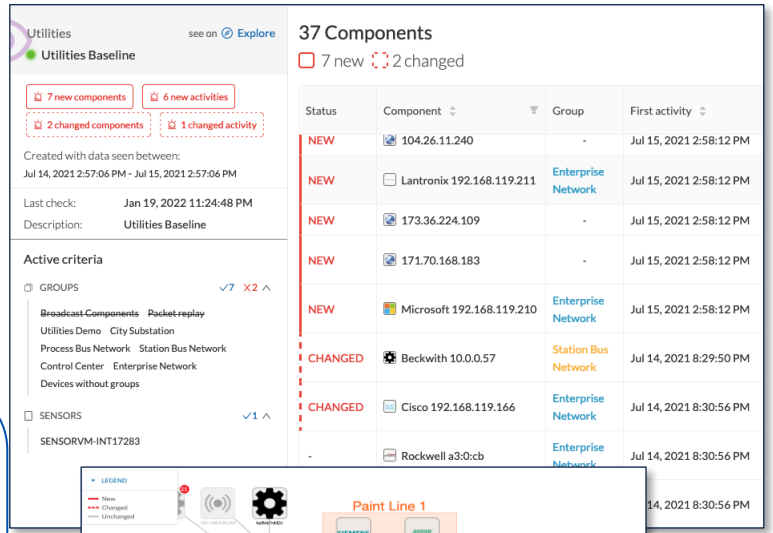
Variable changes

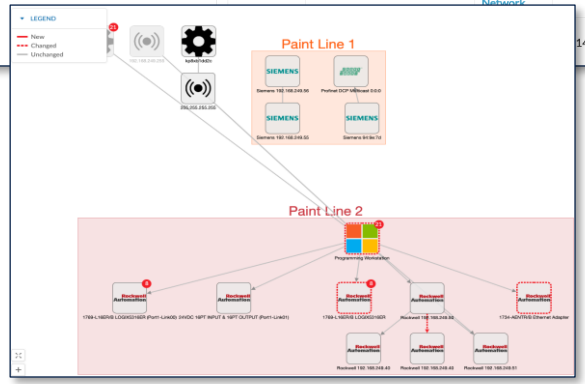
Remote accesses

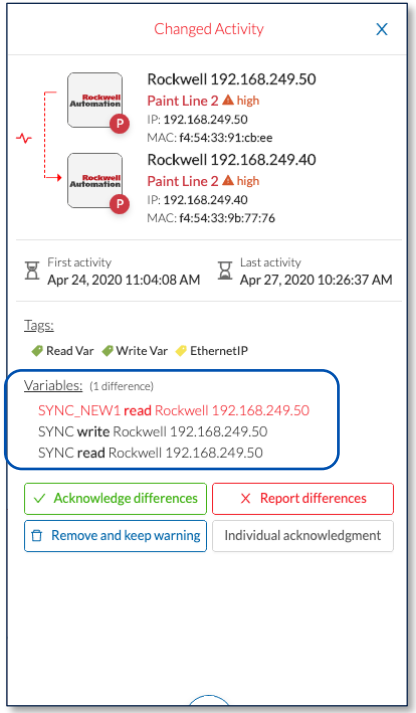
New activity

Process modifications

Asset configuration

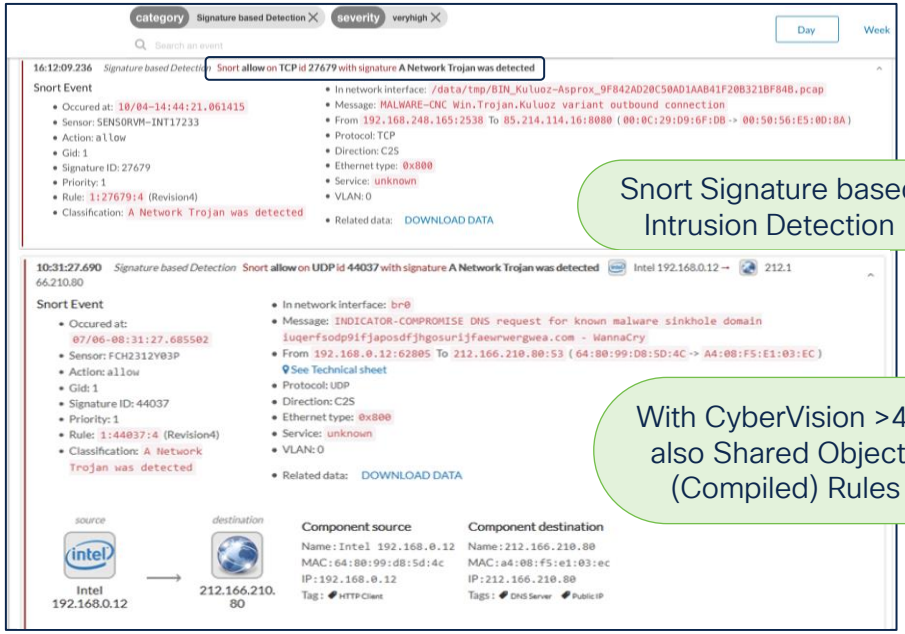






Industrial Intrusion Detection

Some CyberVision sensor models have a built-in Snort engine which includes several industrial protocols processors



Snort Signature based Intrusion Detection

With CyberVision >4.4 also Shared Objects (Compiled) Rules

Snort engine spots intrusions, malware and malicious traffic

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

Superior ICS vulnerability detection

- Modbus, DNP3, CIP, IEC-60870-5-104, IEC 61850 – MMS, S7COM
- Manually curated list of ICS vulnerabilities based on CERT and vendors information
- Talos research discovering over 200 vulnerabilities per year, 40% on ICS

Catalyst IR8300 Series Rugged Router

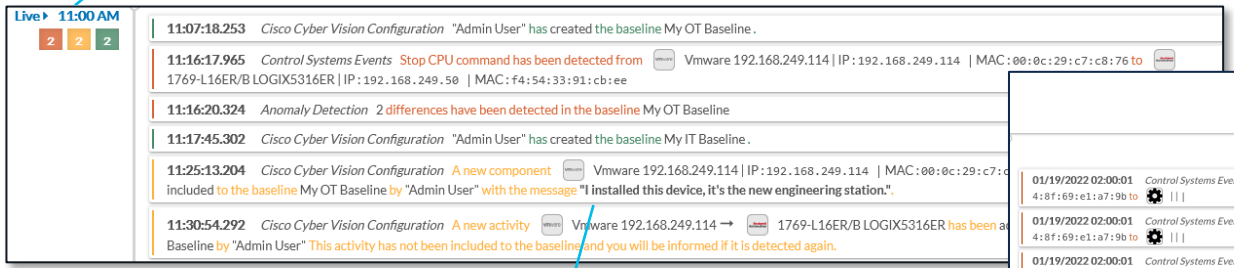
Catalyst 9300/9300X/9400 Enterprise Switch

Cyber Vision Center

IC3000 Industrial Compute

Review what happened: “Events / Calendar”

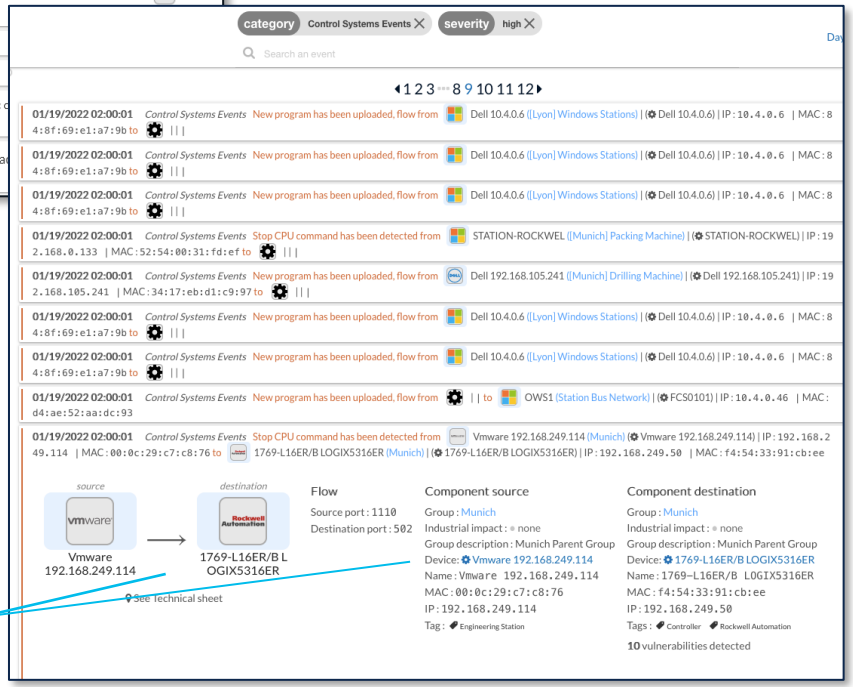
Summary, by severity.
Click on one to zoom in.



… including how admin reacted

Full list of all events for a given period of time…

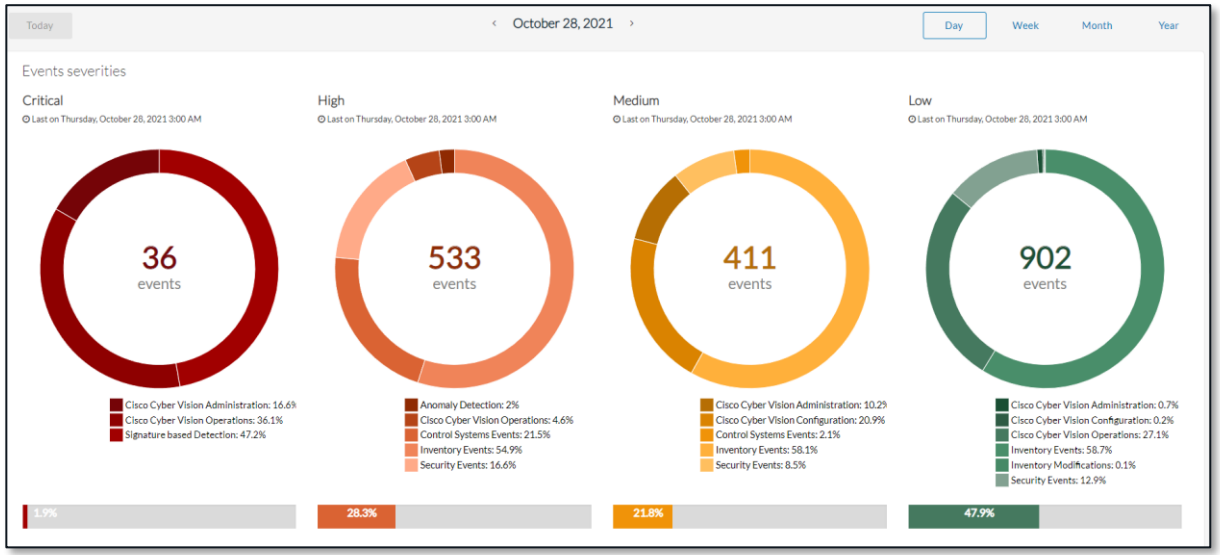
Communications and Device details



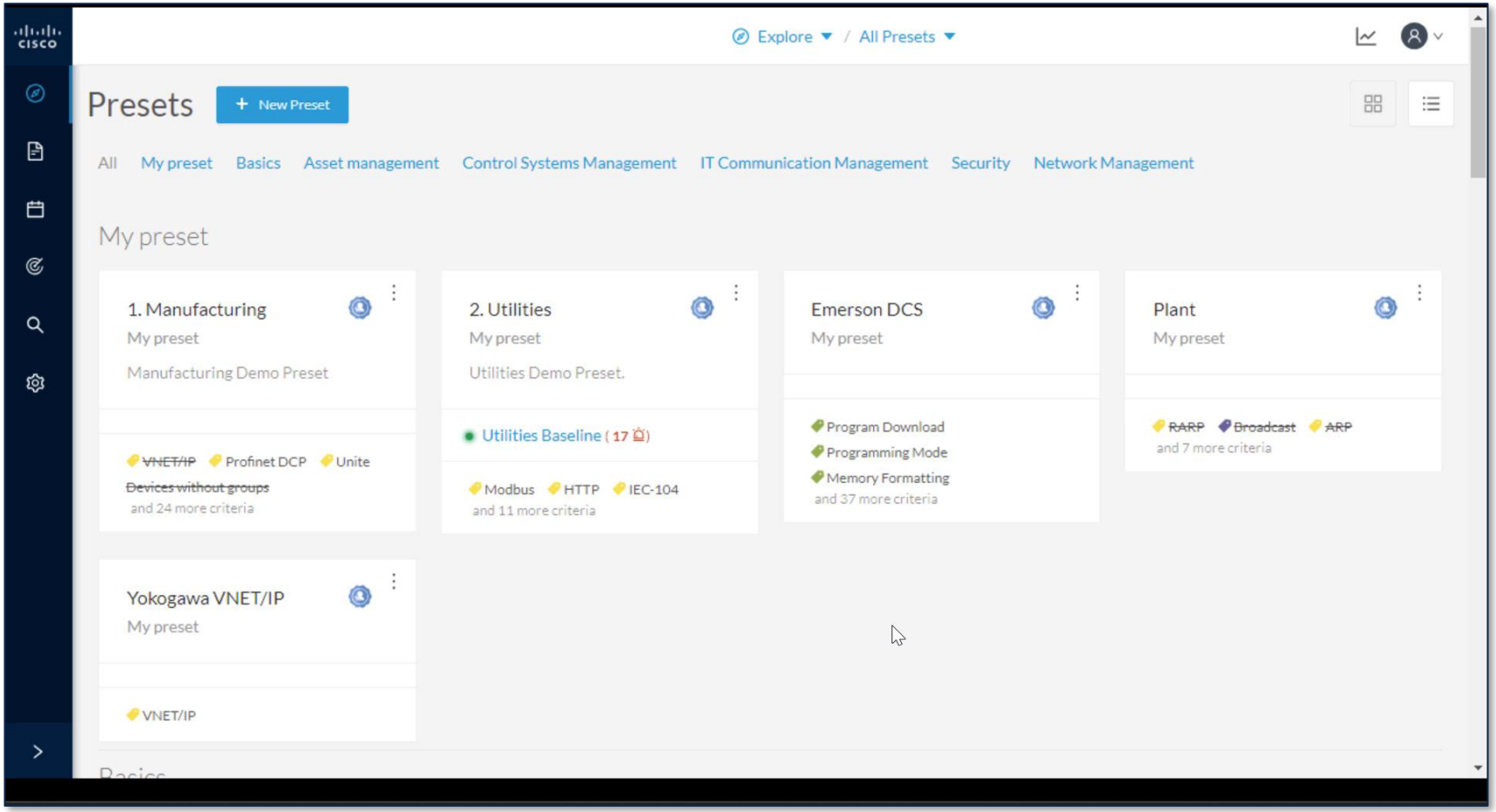
CyberVision Security Dashboard

Track everything happening within the industrial network

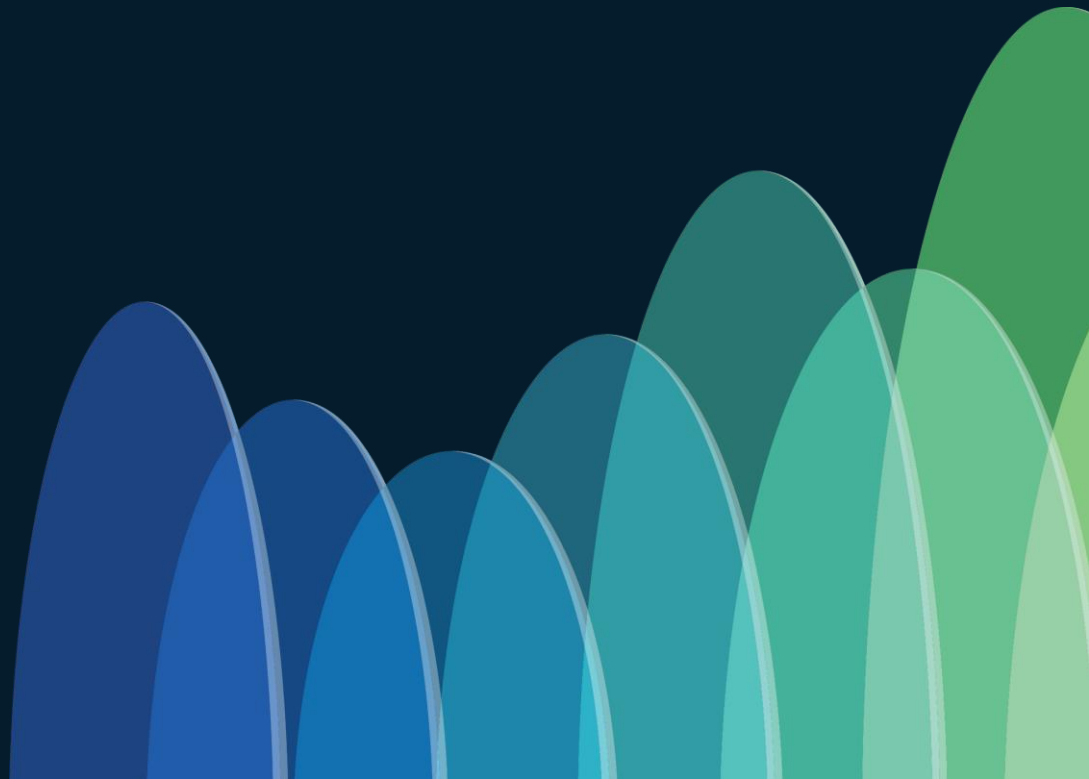
- Security events (vulnerabilities, port scan, protocol exception...)
- Signature-based detection (IDS)
- Control systems events (variable changes, program upload, stop/start CPU...)
- Changes to the Cyber Vision platform (user login, config changes...)



Demo:
Cisco Cyber Vision Baselines

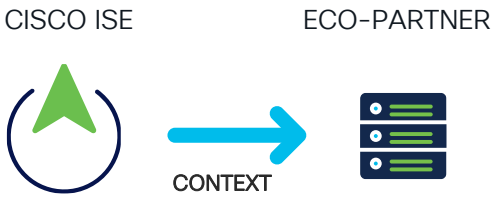


Mitigation



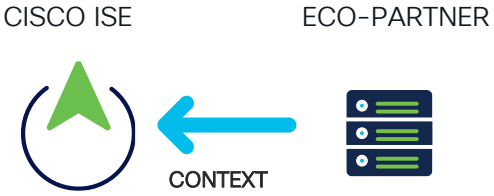
Power of integration pxGrid:

ISE CONTEXT OUT



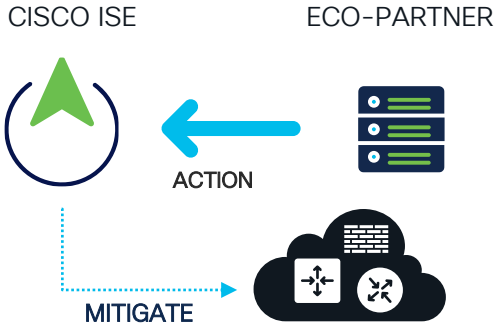
ISE makes Customer IT Platforms User/Identity, Device and Network Aware

ISE CONTEXT IN



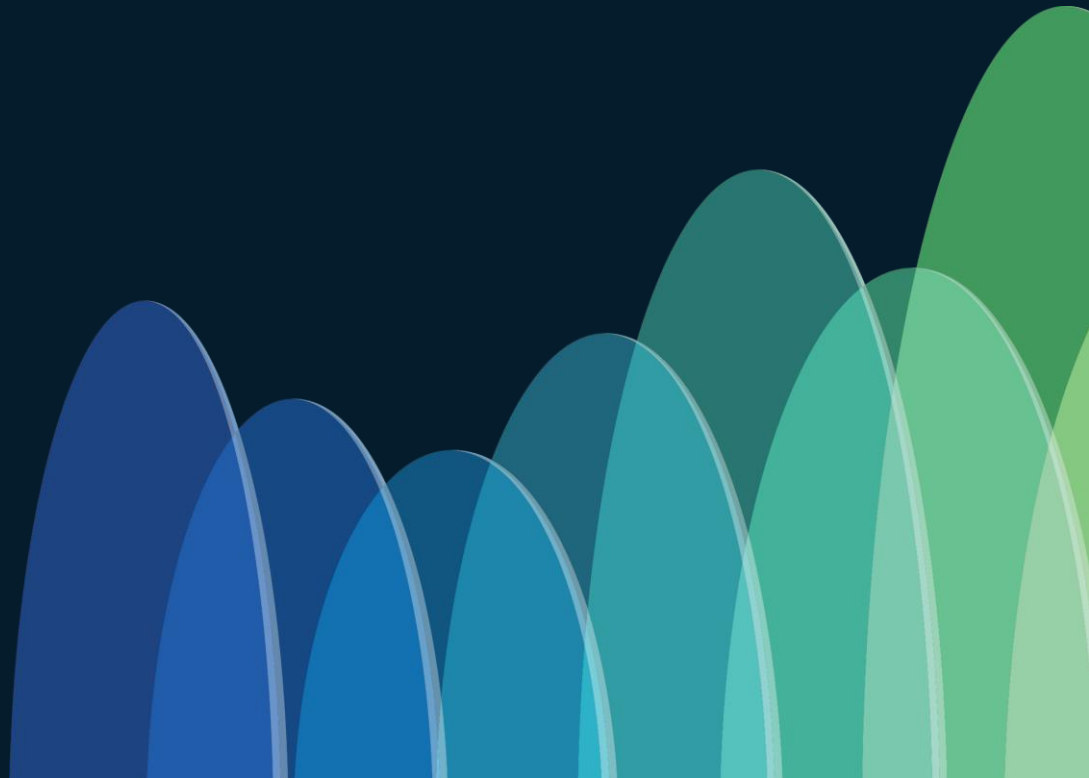
Enrich ISE context. Make ISE a better Policy Enforcement Platform

Rapid Threat Containment



Enforce dynamic policies into the network based on Partner's request

Investigation



Cisco XDR

correlating and prioritizing security threats

Telemetry from native and third-party control points

- Endpoint
- Network
- Email
- Cloud
- Identity
- Firewall
- APIs

Cisco XDR

Open and risk-based.
AI and ML based to analyze, correlate and prioritize


Analytics and correlation


Streamlined investigation


Automation and response

Threat intel
TALOS

Asset & user context

MITRE

Streamlined investigations, shortening time from detection to response

Prioritized alerts, focusing SOC efforts on threats that pose the most harm

Automated response actions, meaning threats are mitigated rapidly, and proactive measures taken

Detects the most sophisticated threats

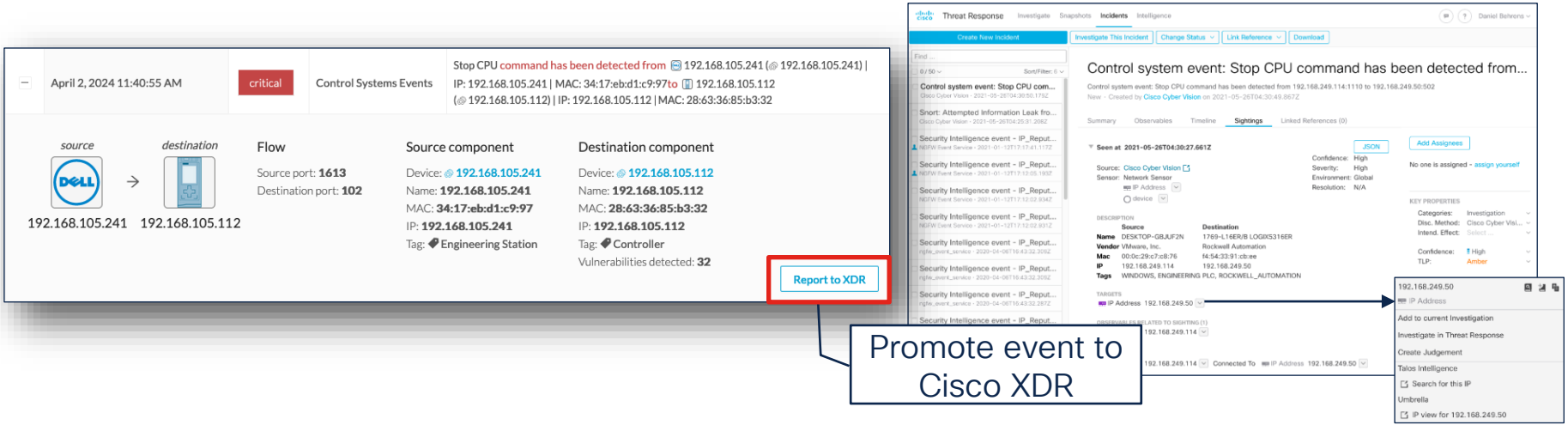
Act on what TRULY matter, faster

Builds Resilience

Promote Cyber Vision events to Cisco XDR

View events in Cyber Vision

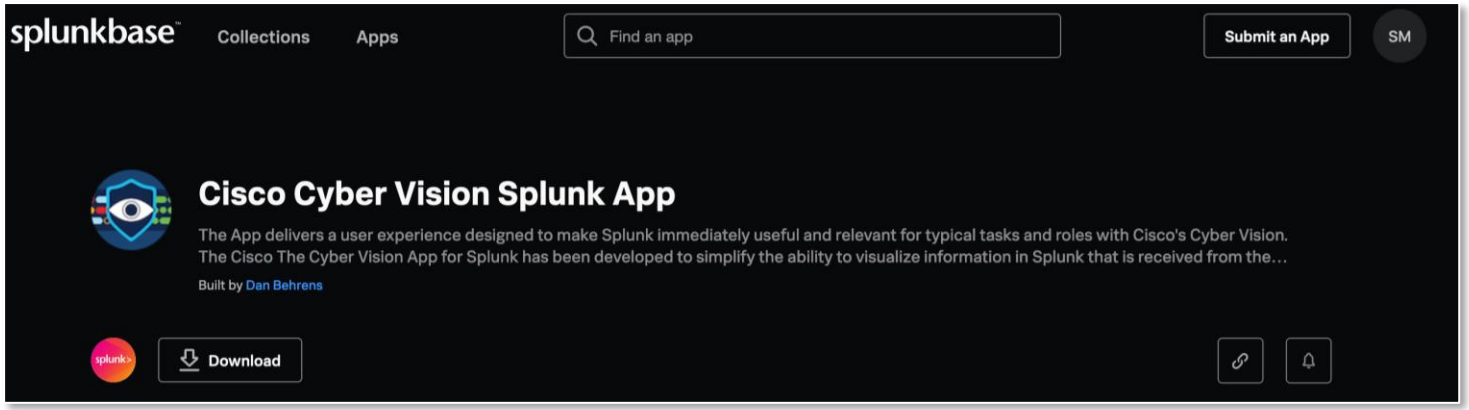
Launch investigation in XDR



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

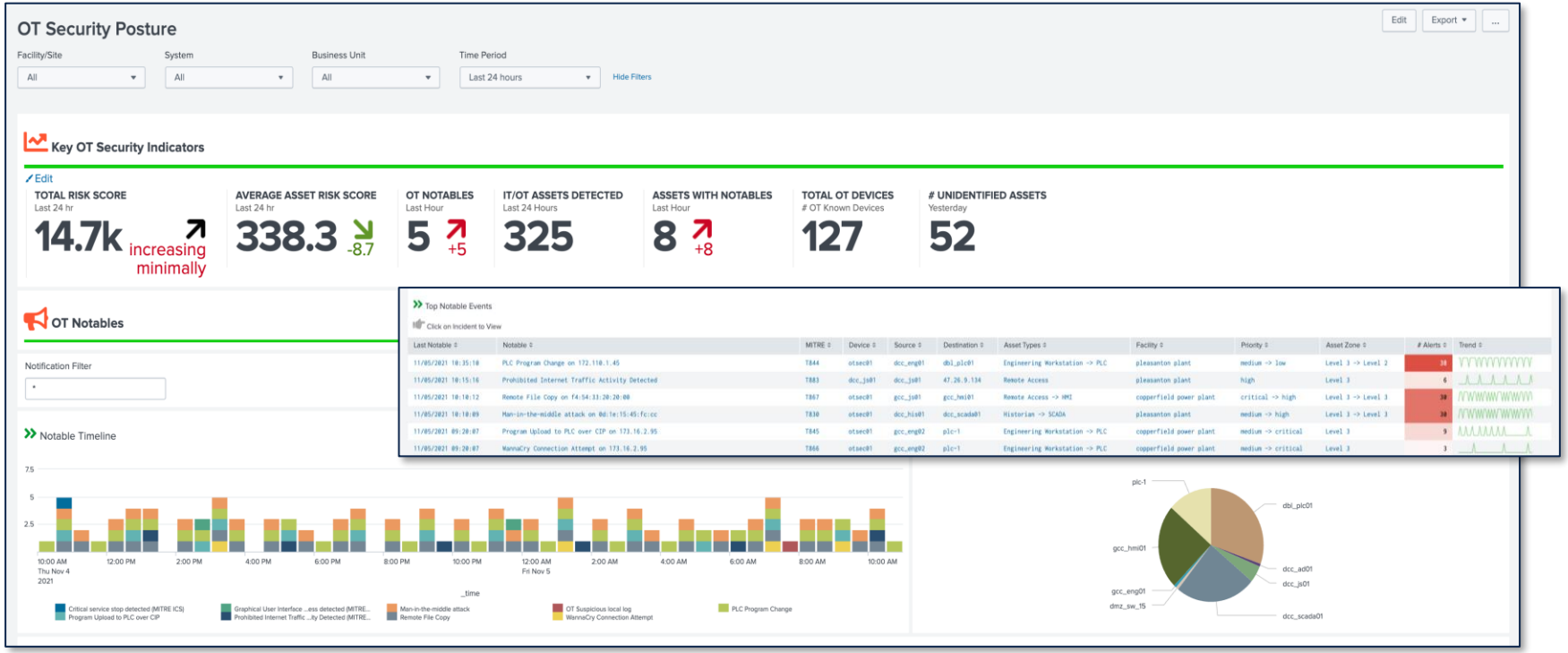
Investigate the threat with enrichment from Cisco and 3rd party security products

Integration of Splunk and Cyber Vision



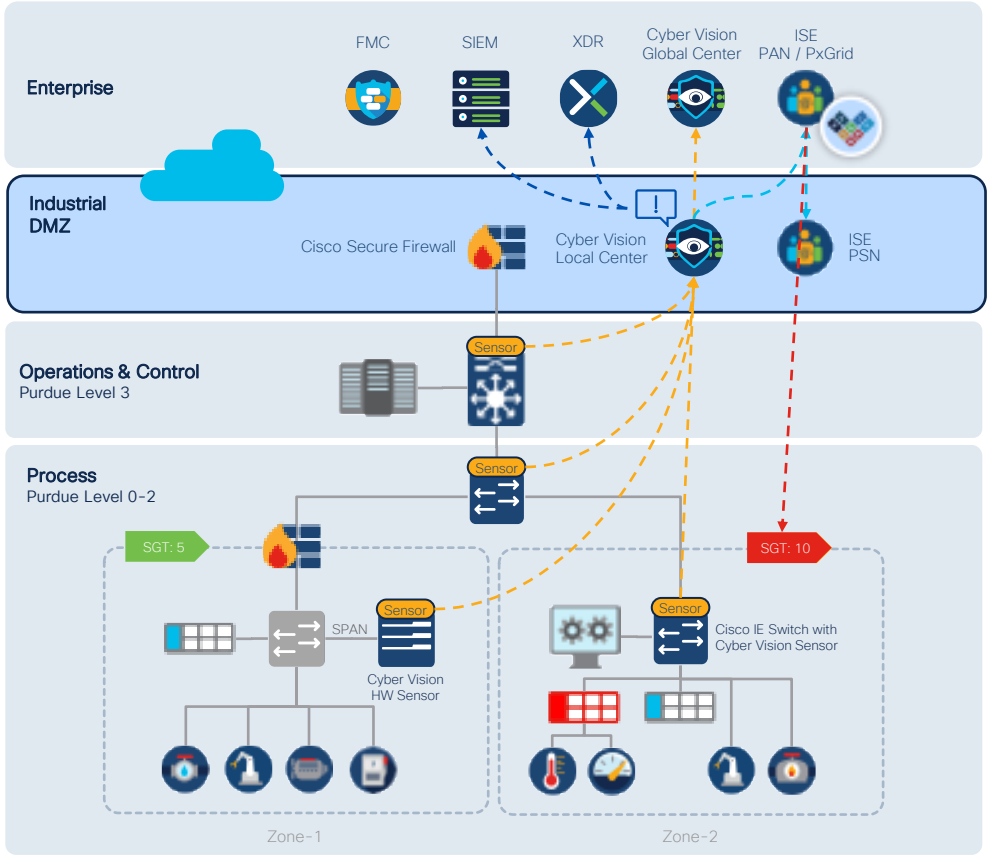
- Splunk has a native integration for Cyber Vision on Splunkbase
- If additional / advanced functionality is required
  - Splunk Enterprise Security & OT dashboards
  - Functionality provides a SOC view

Splunk Dashboard



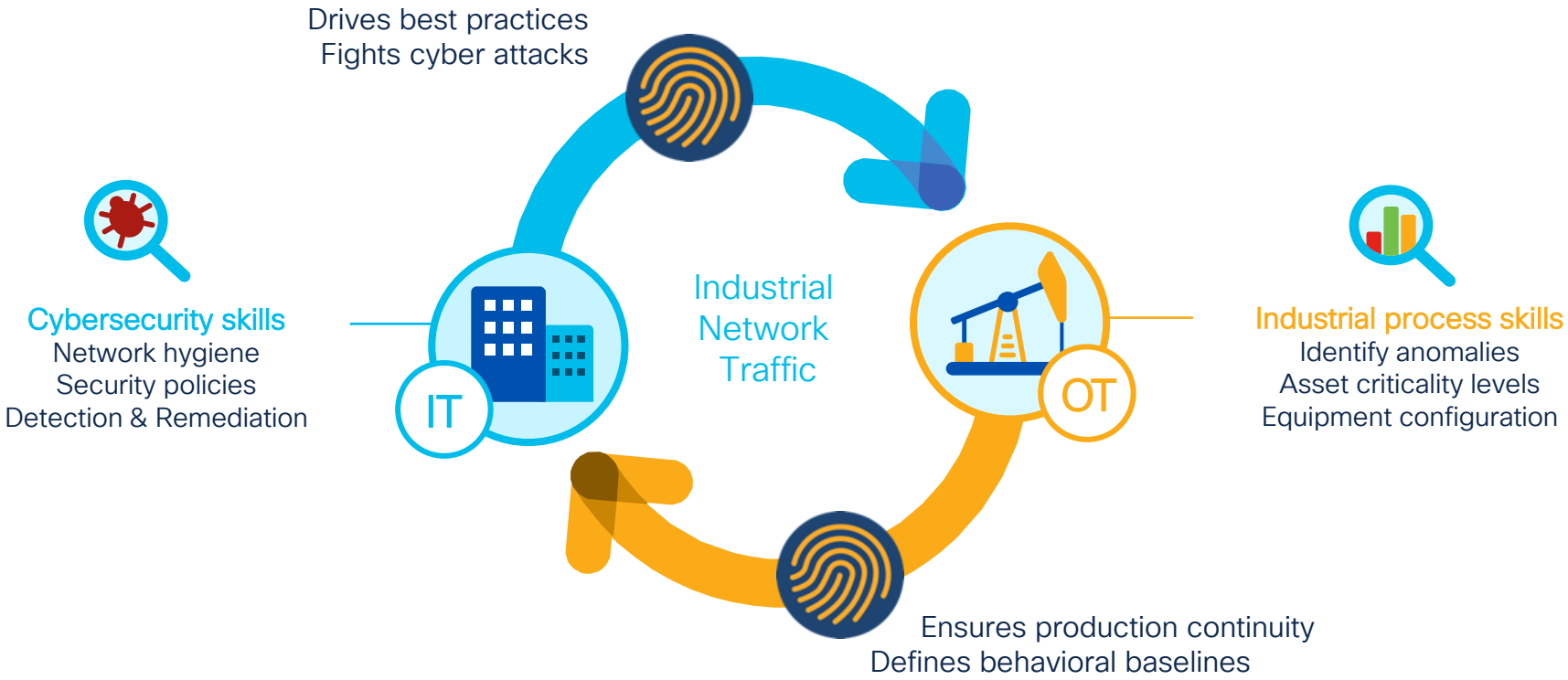
Wrapping up

Let’s put everything together



1. CyberVision discovers industrial assets and communications and groups it into Zones.
2. ISE implemented for visibility and CyberVision context is shared with ISE.
3. Components are dynamically classified in SGTs via group assignment directly from CyberVision
4. Deploy segmentation with confidence once you are comfortable with the observed network behavior
5. CyberVision or other analytics tools raise alarms on endpoint behavior anomalies and threat detection.
6. Investigate in XDR and SOC tools
7. Users can trigger quarantine of offending asset.

IT-OT collaboration is vital for securing ICS

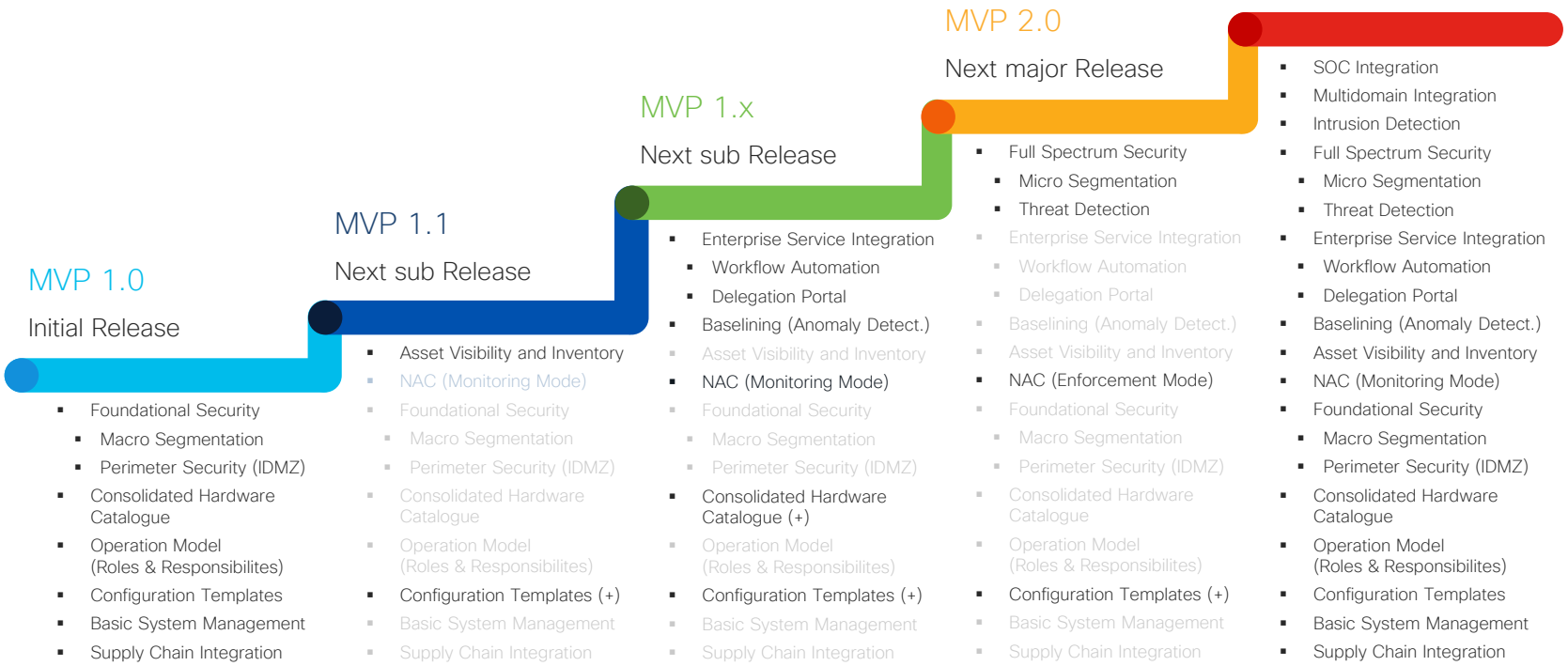


Typical Challenges

- Readyness of the current Infrastructure
  (Retrofit for brownfield needed to some degree)
- Fragmented knowledge about the systems in place
- What to do with all the Information ? (Iceberg effect)
- OT Procedures and Routines (Example: Troubleshooting Approach)
- Integration of the Supply-chain (EPC's, Machine builders, etc.)
- Over-engineering due to dependencies

Example of an agile Approach

Minimum viable product (MVP)



KEEP
CALM
AND
DON’T REINVENT
THE WHEEL

Resources for your consumption

Best practice & Design principles

Cisco Validated Design

Tested Implemented Proven

[Networking and Security in Industrial Automation Environments Design and Implementation Guide]

[Cisco DNA Center for Industrial Automation Design Guide]

[Industrial Security Design Guide]

End-End Architecture

CVDs start with the customer use cases and architecture from the edge device to the application, validating the key Cisco and 3rd party components

Best Practices

Document best practices so you can confidently set performance expectations

Reliability

Reliability

Reduce risk products won't work together or perform as promised

Comprehensive

Provide tested system designs and configuration instructions


cisco
Thank you
cisco Live!

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: WebEx

Cisco Live EMEA – Securing Industrial Learning Map

Monday – 10th

BRKSEC-2176 3:30 PM

Keeping up with Zero Trust

BRKIOT-1005 4:00 PM

Enable Zero Trust Network Access for Industrial Networks with Cisco Secure Equipment Access

Tuesday – 11th

BRKSEC-2113 12:00 PM

Cisco XDR – Making Sense of all the Parts and Pieces

BRKSEC-2236 1:30 PM

Keeping Up on Network Security with Cisco Secure Firewall

BRKSEC-2660 12:00 PM

Setting the Stage for ISE Deployment Success: A Guide to Effective Planning

BRKIOT-1968 3:00 PM

Secure your water Utility Operations with Cisco Industrial Threat Defense

BRKIOT-2910 4:30 PM

Securing Industrial Networks: Where to start – using Cyber Vision for OT Asset Visibility

Wednesday – 12th

BRKIOT-1126 8:00 AM

Connecting Remote and critical Asset with Cisco IoT Solutions

BRKSEC-2887 12:30 PM

Unify Threat Detection, Investigation, and Response with Splunk Enterprise security and SOAR

BRKSEC-2053 1:00 PM

Zero Trust: Security the Evolving Workplace

BRKSEC-1159 2:30 PM

Solving Cyber Insecurity

BRKSEC-1544 2:30 PM

Secure Endpoint : Unveiling Latest Key Features!

Thursday – 13th

BRKSEC-2821 1:00 PM

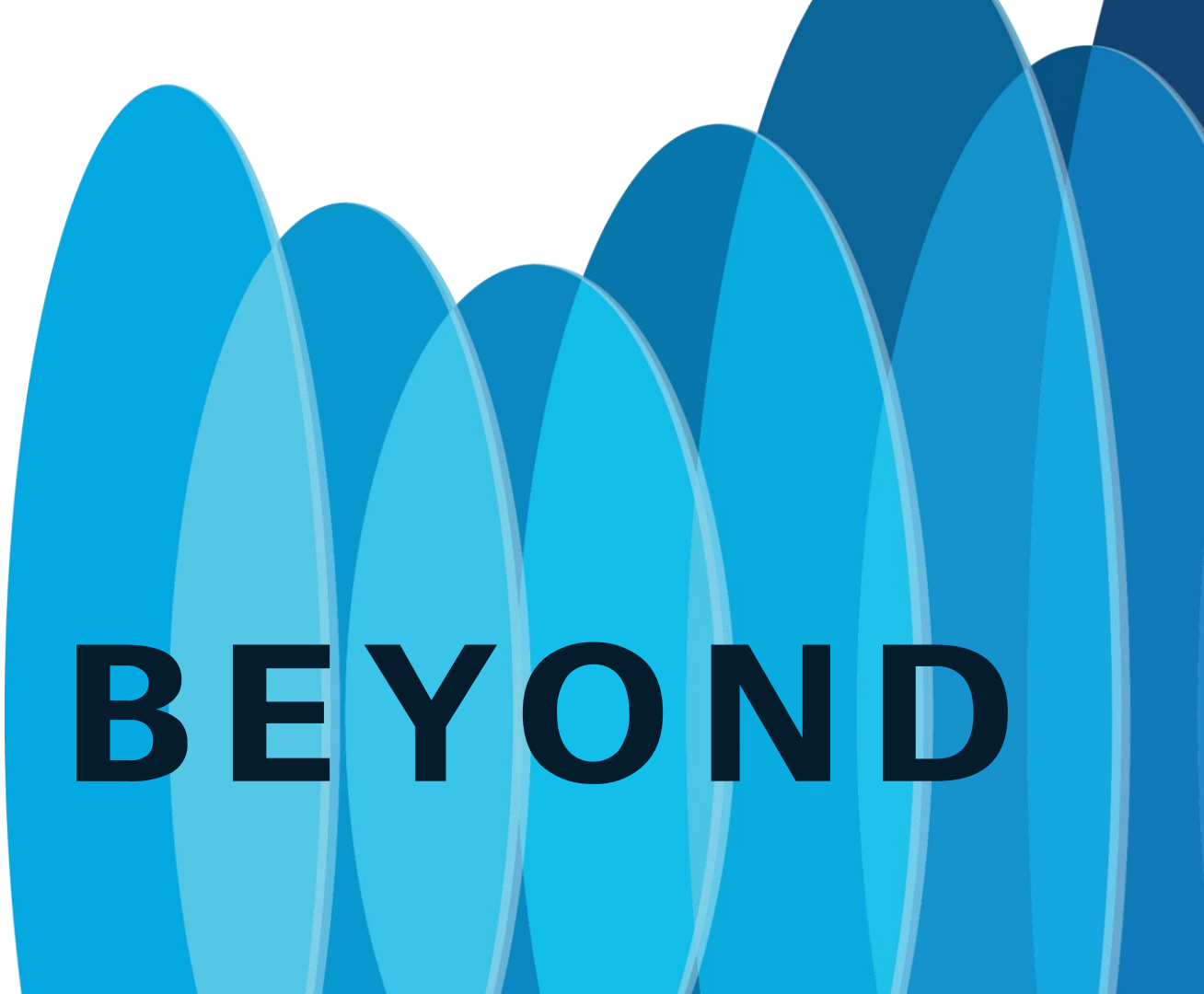
Security Industrial Networks: Strategies and Best Practices

BRKSEC-2623 5:15 PM

Accelerating Threat Analysis with Intelligent Automation


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND