



Securing Industrial Networks

Strategies and Best Practices

Tilman Taubert
Leader - EMEA IoT Industry Specialists
BRKSEC-2821

CISCO *Live!*



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?

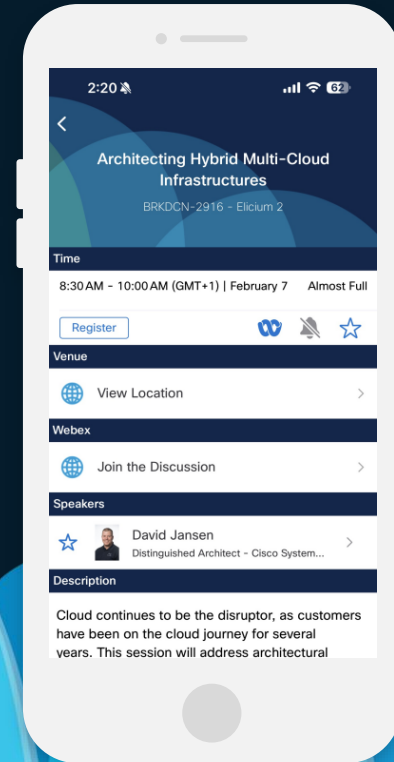
Use the Webex app to chat with the speaker after the session

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.

CISCO *Live!*



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%).



2024 State of Industrial Networking Report

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

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



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

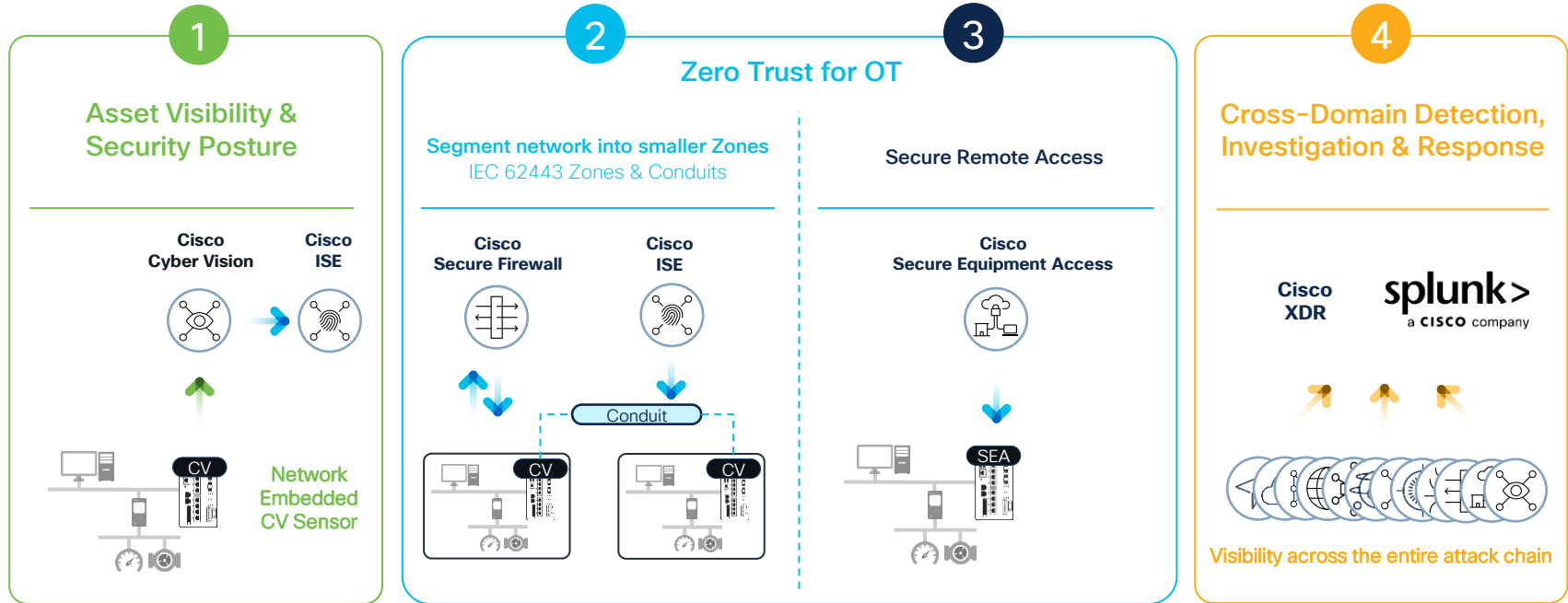
Protect Industrial Platform and Applications from Attack.

Protect from both Known and Unknown **Malware**.

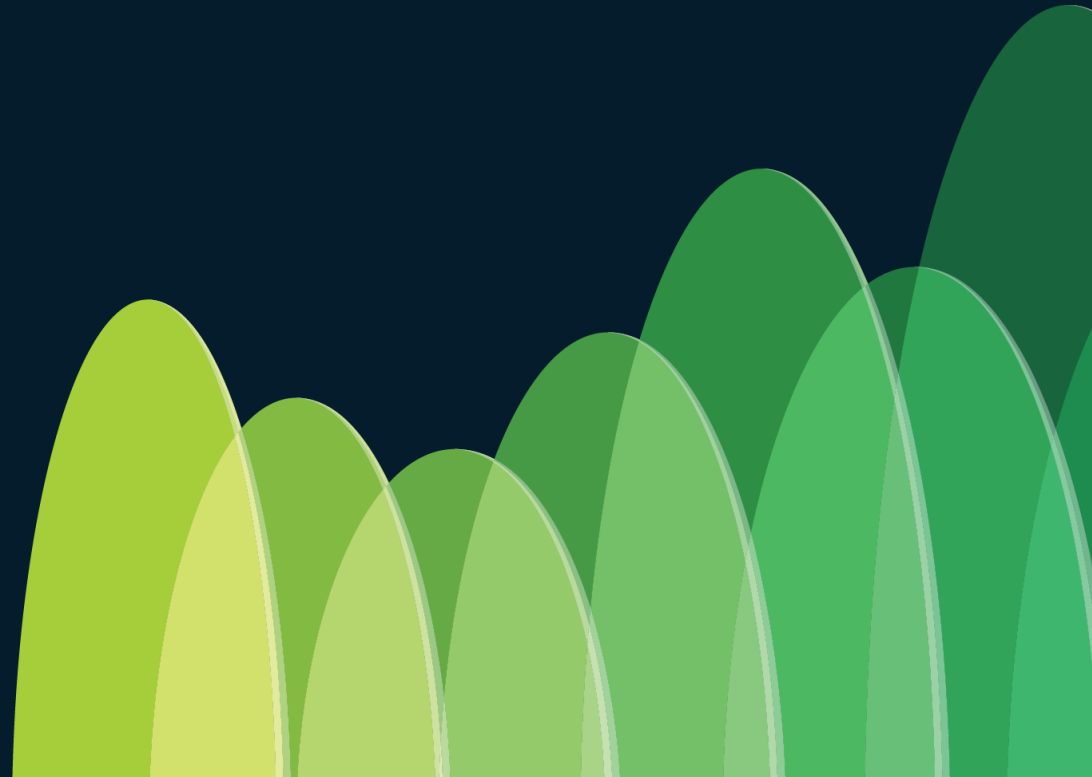
5

Limit Network Traffic and Network Path leveraged to get to Critical Industrial Systems.

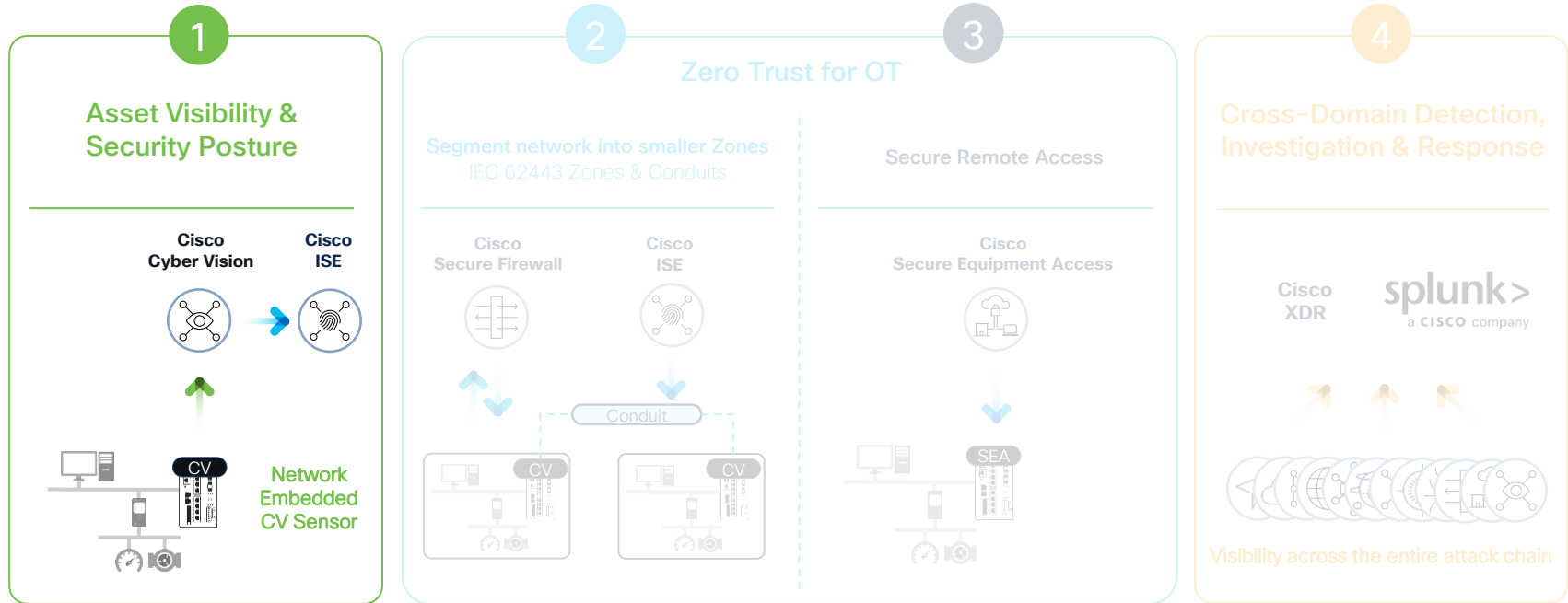
Cisco's Industrial Threat Defense Journey



Asset Visibility & Security Posture

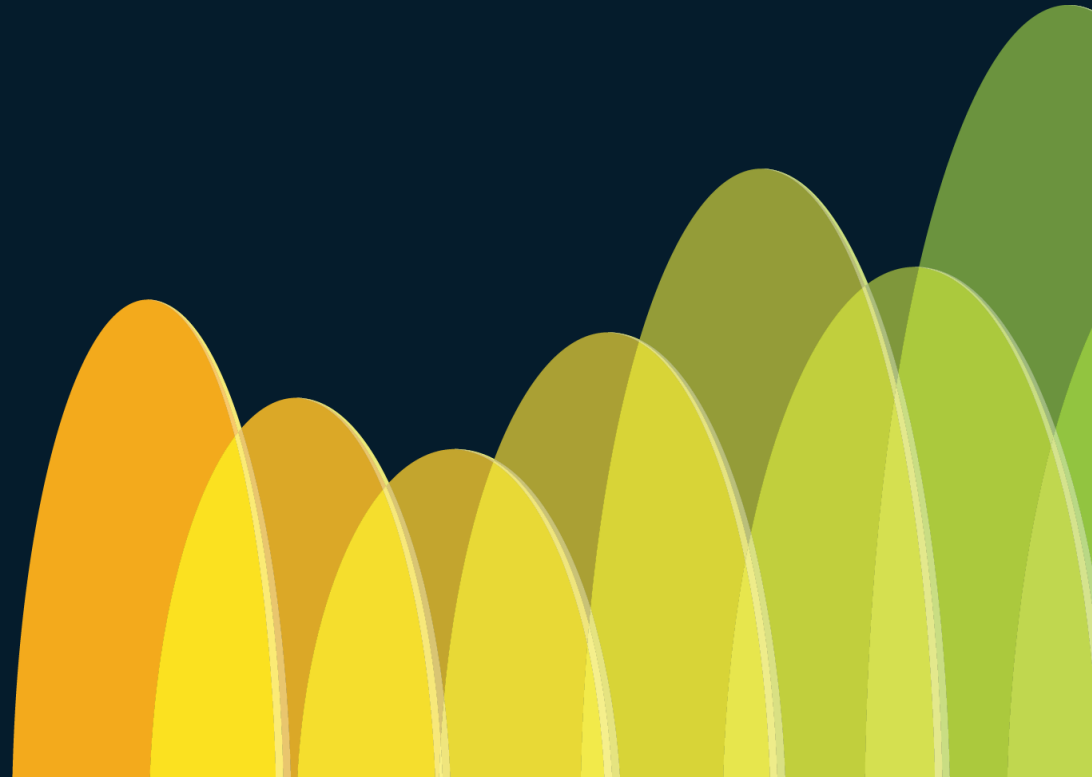


Cisco's Industrial Threat Defense Journey

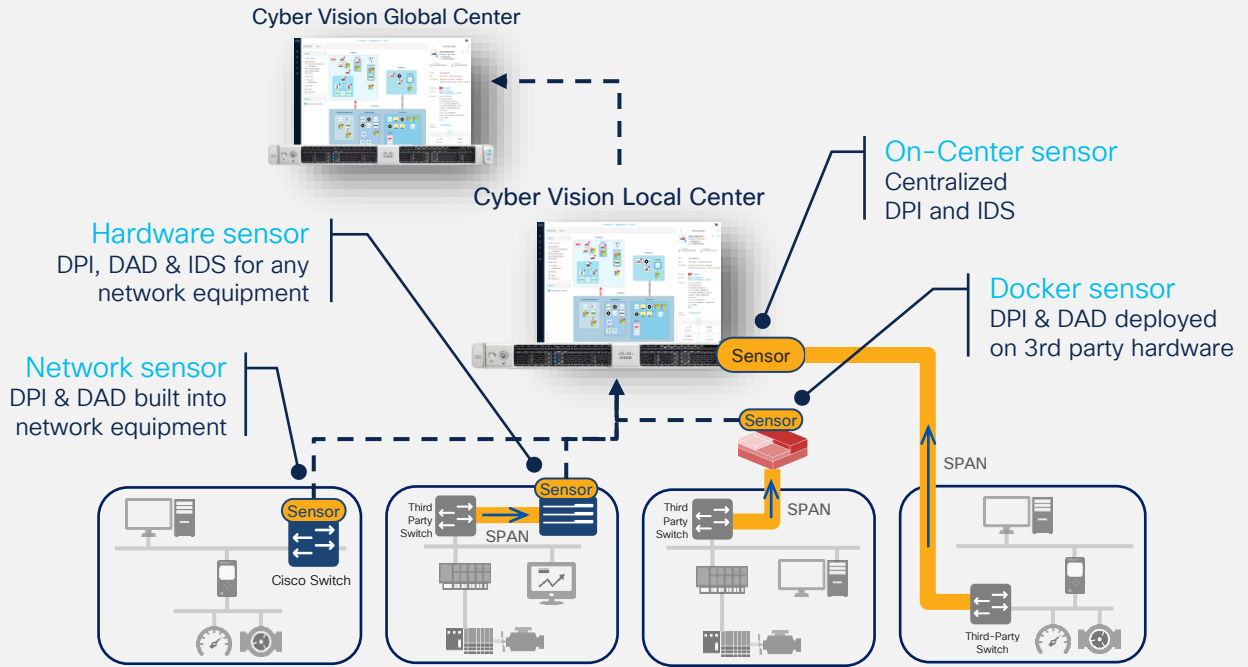


Cisco Cyber Vision

CISCO *Live!*



Cisco Cyber Vision Architecture



DPI = Deep Packet inspection

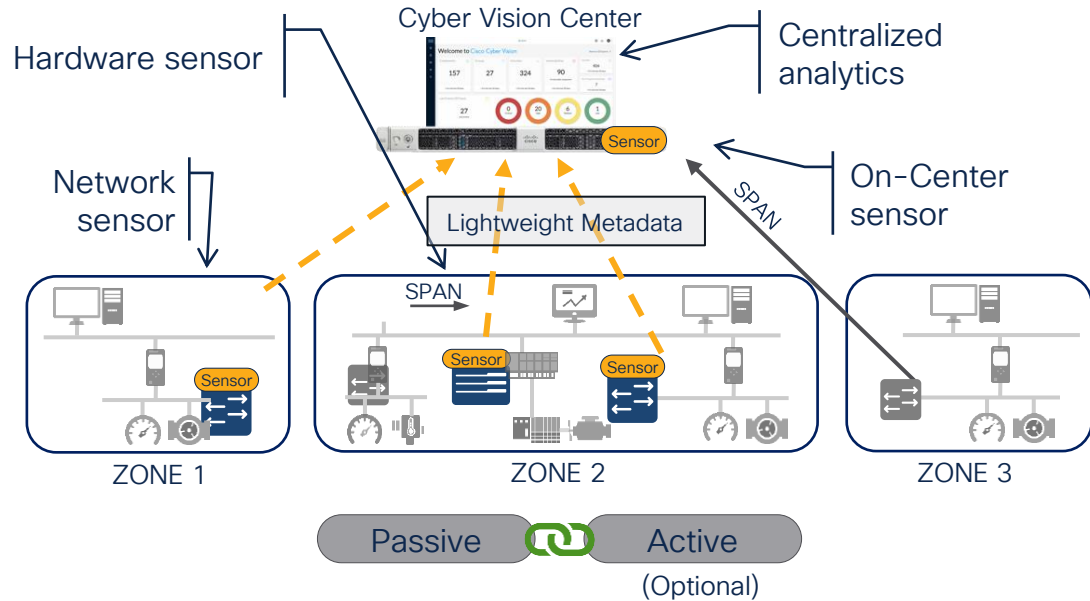
DAD = Distributed Active Discovery

IDS = Intrusion Detection System

- **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

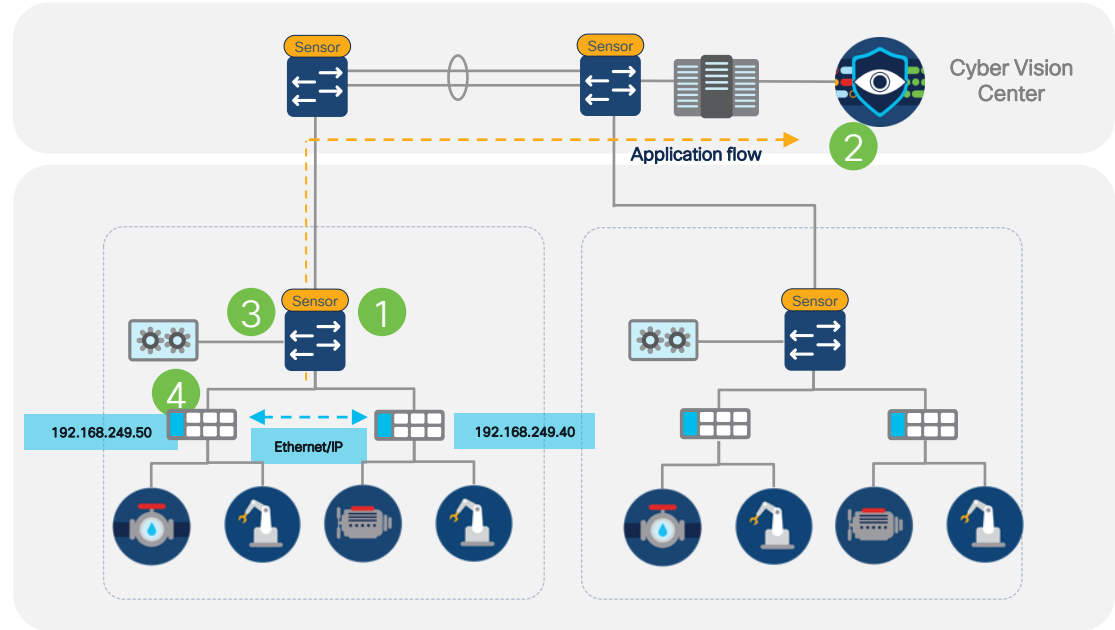
The Role of the Cyber Vision Sensor

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

Comprehensive asset inventory

All data*

66 Components

COMPONENT TAGS

ACTIVITY TAGS X 1

GROUPS

SENSORS

Component	Group	First activity	Last activity	IP	MAC	Tags	Flows	Vuln	Var	Vendor	OS
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	-	34:17:eb:d1:c9:97	Read Var, Write Var, Engineering Station, Remote access	579	0	0	Dell Inc.	
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6b:f5:62:e7:80	DNS Server, Public IP	38	0	0	Juniper Networks	
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	01:00:5e:6c:74:76	Multicast, Public IP	8	0	0	-	
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:34 AM	-	00:24:9b:08:43:6f	Windows	7	0	0	Action Star Enterprise Co., Ltd.	
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	00:22:e5:21:0a:86	Read Var, Write Var, Wireless IO Module, DeltaV	44	0	225	-	
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.1	00:0e:8c:84:5b:a6	Read Var, PLC	25	10	13	Siemens AG A&D ET	

- 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



COMPONENT TAGS

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

ACTIVITY TAGS

- Activities without tags
- Control system behavior
 - Block Download
 - Control action (1)
 - Controller Info
 - Controller Name
 - Data Push
 - Device Init (1)
 - Diagnostics
 - Emergency Brake
 - Firmware Download
 - Firmware Update
 - Force Variable
 - Heartbeat
 - Hot Reboot
 - Insert Program
 - Installed Modules
 - Memory Formatting
 - Network Configuration
 - Operational change
 - PLC Clock

Detailed information on assets

Device
PLC
 Rockwell Automation
 Munich
 IP: 192.168.249.50
 MAC: f4:54:33:91:cb:ee

First activity: Sep 10, 2020 3:36:37 PM
 Last activity: Jan 19, 2022 2:00:01 AM

Tags: Controller, Rockwell Automation
 Activity Tags: Start CPU, Stop CPU, Diagnostics, Read Var, Write Var, Low Volume, CIP-IO, EthernetIP, Umas (hide)

4 Activities, 42 Events, 10 Vulnerabilities

Basics, Risk score, Security, Activity, Automation

Properties

Normalized Properties

- fw-version: 31.11, 31.011
- ip: 192.168.249.50
- mac: f4:54:33:91:cb:ee
- model-ref: 0x99, 0x474, 1769-L16ER/B LOGIX5316ER
- name: 1769-L16ER/B LOGIX5316ER, SecDemo_LinePLC, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)
- public-ip: no
- serial-number: 60771949, 00000000
- vendor-name: Rockwell Automation

Other Properties

- enip-cpname: SecDemo_LinePLC
- enip-devicetype: ProgrammableLogicController, GeneralPurposeDiscreteIO
- enip-location: Endpoint, Port1-Link00, Port1-Link01
- enip-name: 1769-L16ER/B LOGIX5316ER, 24VDC 16PT INPUT & 16PT OUTPUT
- enip-productcode: 0x99, 0x474
- enip-serial: 00000000, 60771949
- enip-status: Owned, AtLeastOneIOConnectionInRunMode, NoIOConnectionsEstablished, AtLeastOneIOConnectionInRunMode, MinorRecoverableFault, ReserveBits12-15:0x3
- enip-value: RA-ProgramName
- enip-vendor: Rockwell Automation/Allen-Bradley
- enip-version: 31.11, 31.011
- name-enip: 1769-L16ER/B LOGIX5316ER, SecDemo_LinePLC, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)
- name-vendorip: Rockwell 192.168.249.50
- vendor: Rockwell Automation

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

Variables accesses

Variable	Types	Accessed by	First access	Last access
M2.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
M2.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
M8.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
M8.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
M8.2	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM

Rack slot component details

Device properties

Variable accesses

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

The screenshot displays the Cisco Cyber Vision interface for a device named 'SIMATIC 300(1)'. The device details include its IP address (192.168.0.1), MAC address (00:0e:8c:84:5b:a6), and activity history. A summary of 16 vulnerabilities is shown, with two specific entries highlighted in an orange box:

- Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability**
CVE:-2017-12741
Several industrial products are affected by a vulnerability that could allow remote attackers to conduct a Denial-of-Service (DoS) attack.
Solution
Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.
Published on November 23, 2017
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0)
Links
Siemens Security Advisory
- SIMATIC S7-300 and S7-400 CPUs Denial of Service and Information Disclosure Vulnerabilities**
CVE:-2016-9158
Successful exploitation of these vulnerabilities could lead to a denial-of-service condition or result in credential disclosure.
Solution
Siemens provides firmware version V3X.14 for S7-300 CPUs that resolves CVE:-2016-9158.
Published on December 16, 2016
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0)
Links
www.siemens.com
ics-cert.us-cert.gov
www.securityfocus.com

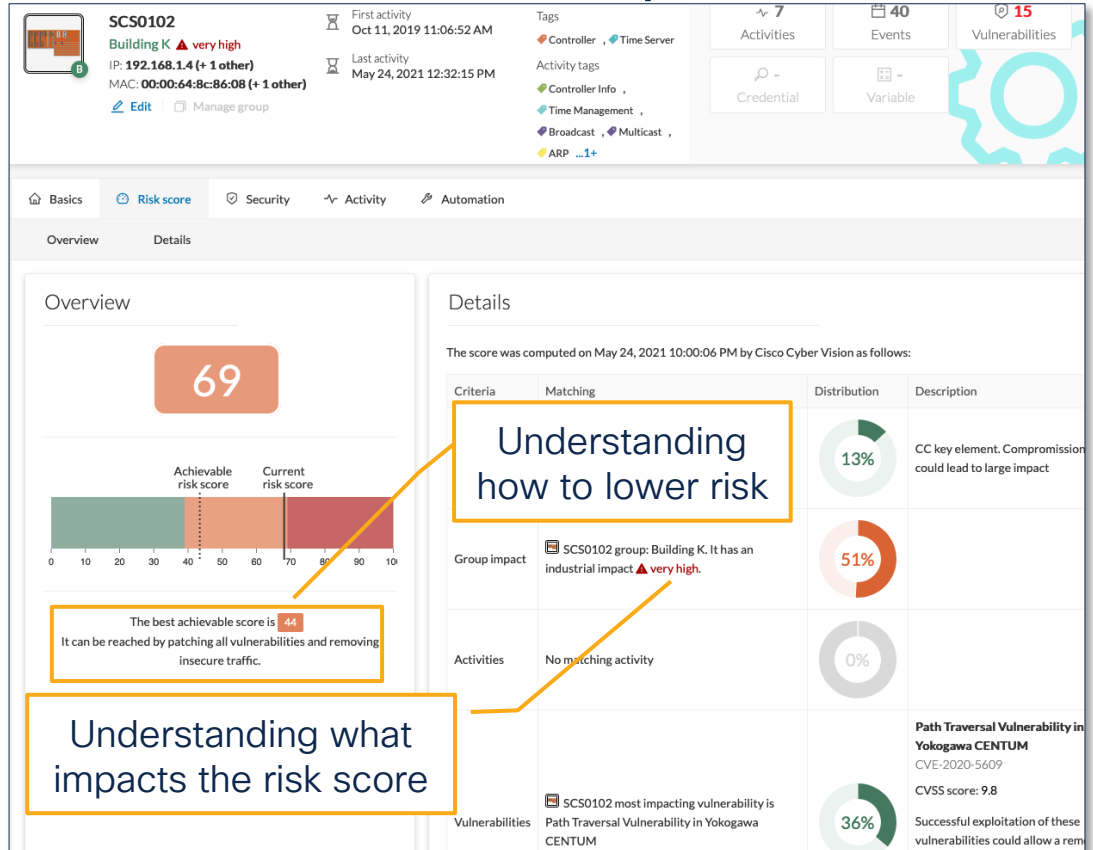
Each vulnerability entry shows a CVSS score of 7.8 and includes an 'Acknowledge?' section with 'Explain why' and 'OK' buttons.

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”**?

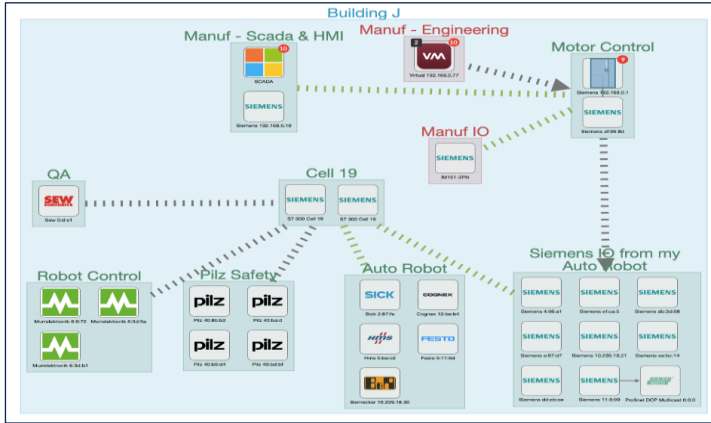


Understanding how to lower risk

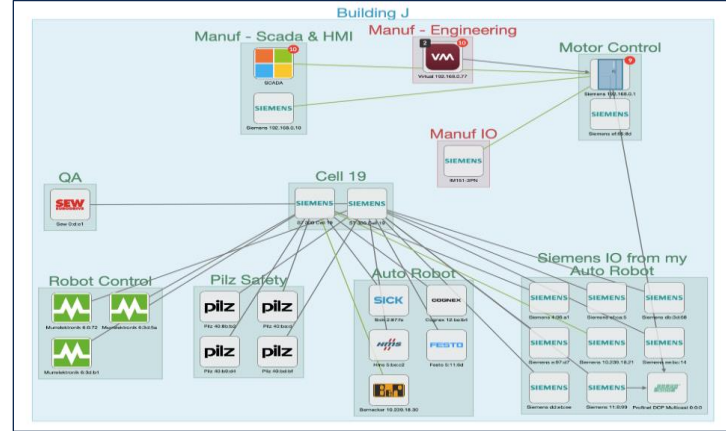
Understanding what impacts the risk score

Communication visibility with CyberVision

Conduits



Communication flows



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

- 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!*



Explore - 1. Manufacturing - Cisco Cyber Vision

cybercenter

Home

Welcome to Cisco Cyber Vision

Last 30 days overview

Operational overview Security overview

All Protocol distribution Most critical events Presets highlight

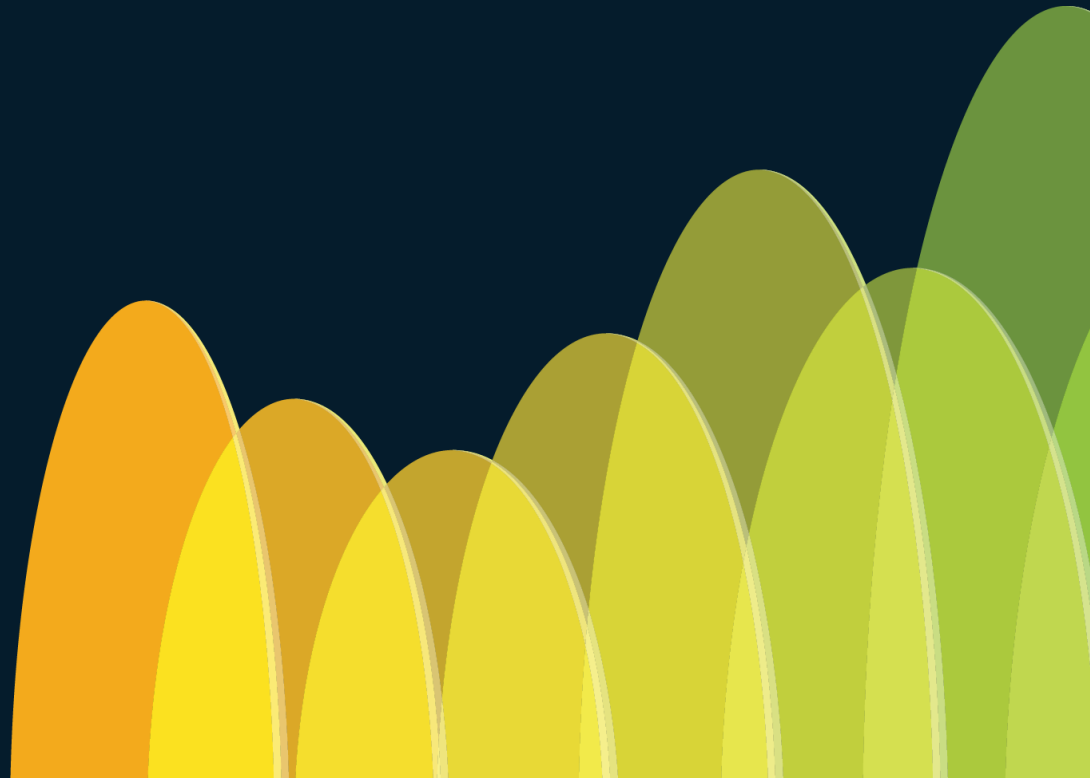
Protocol distribution

Protocol	Count
OTHERS	249
APP	137
NETBIOS	-
SMB	-
DELTAV	-
VNETIP	-

Most critical events

Apr 25, 2024 3:00:28 AM	Critical	System has not been updated	Cisco C...
Apr 25, 2024 3:00:28 AM	Critical	Sensor 8e2fb2fe-c4dd-46a6-8e01-279...	
Apr 25, 2024 3:00:28 AM	Critical	System has been updated	Cisco Cybe...
Apr 25, 2024 3:00:28 AM	Critical	System has been updated	Cisco Cybe...
Apr 25, 2024 3:00:28 AM	Critical	Center has been rebooted	Cisco Cybe...

Cisco Identity Service Engine (ISE)



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

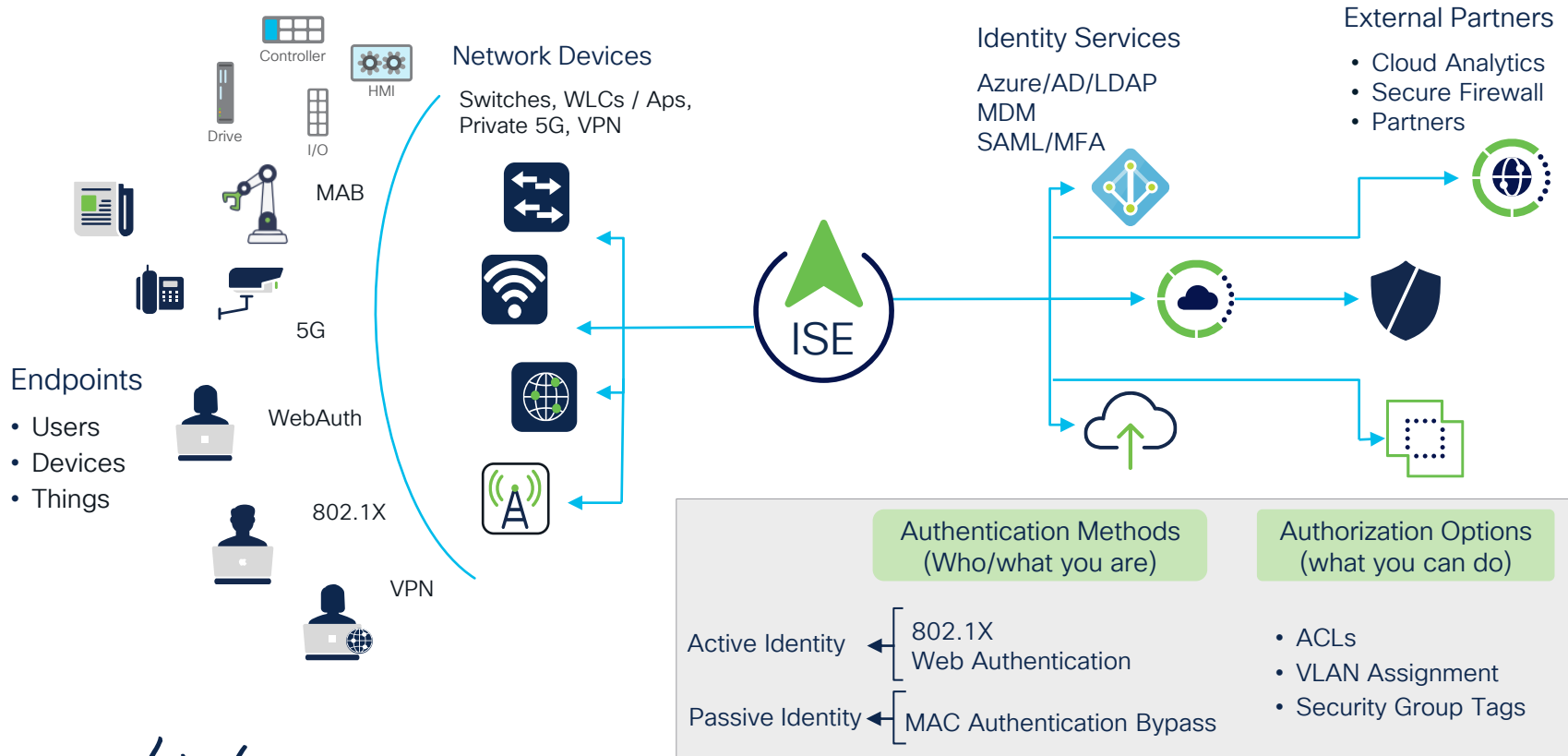
- Continually monitors and verifies endpoint trust level
- Automatically Updates access policy

Authorized access based on least privilege

- Access granted
- Network segmentation achieved



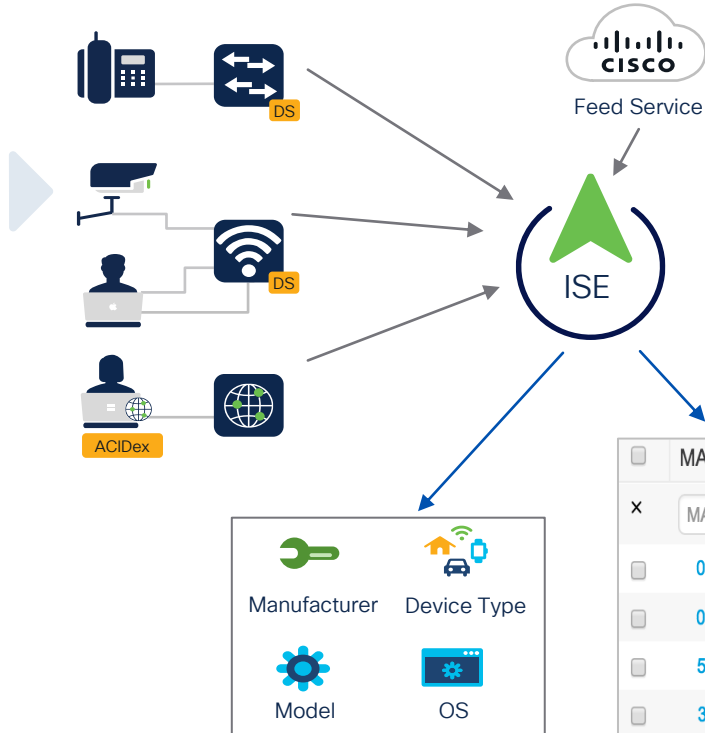
ISE Provides Zero Trust for the Workplace



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)

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

Enhancing ISE profiling with CyberVision data

ISE Data Collection Methods for Device Profiling

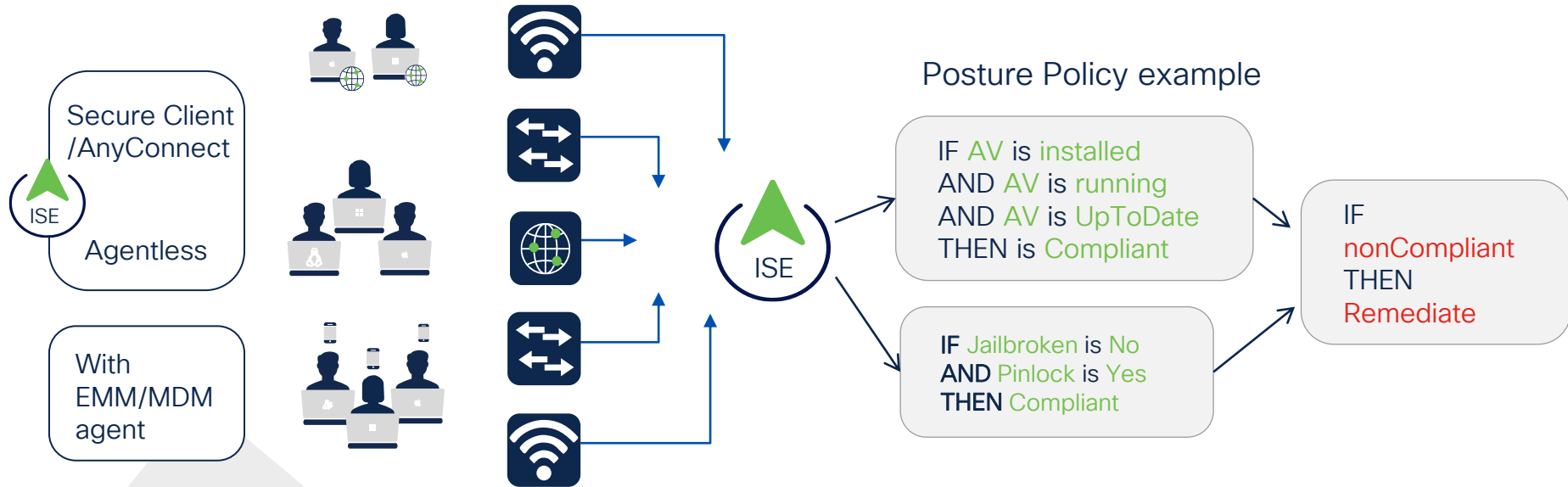
Active Probes: AD | DHCP | DNS | HTTP | RADIUS | NMAP | SNMP



MACAddress	00:1D:9C:CA:85:8B
MatchedPolicy	Rockwell-Automation-Device
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	5
assetConnectedLinks.assetDeviceType	Switch
assetConnectedLinks.assetId	40109
assetConnectedLinks.assetIpAddress	10.195.119.22
assetConnectedLinks.assetName	IE4000-119-22
assetConnectedLinks.assetPortName	GigabitEthernet1/2
assetDeviceType	Controller
assetId	60100
assetIpAddress	10.195.119.38
assetMacAddress	00:1d:9c:ca:85:8b
assetName	10.195.119.38
assetProductId	1756-EN2TR/C 217021900
assetProtocol	CIP
assetSerialNumber	12174476
assetVendor	Rockwell Automation/Allen-Bradley

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



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

CISCO *Live!*



Explore · Plant - Cisco Cyber Vi... Identity Services Engine

ise.dcloud.cisco.com/admin/#administration/administration_messageservice/pxgrid_clientmanagement/pxgrid_clientmanagement_clients

Cisco Cyber Vision ISE FMC SMC

Cisco ISE Administration · pxGrid Services

Summary **Client Management** Diagnostics Settings

Click here to do visibility setup [Do not show this again.](#)

Clients

Clients must register and receive account approval to use pxGrid services in Cisco ISE. Clients use the pxGrid Client Library through the pxGrid SDK to register as clients. Cisco ISE supports both auto and manual registrations.

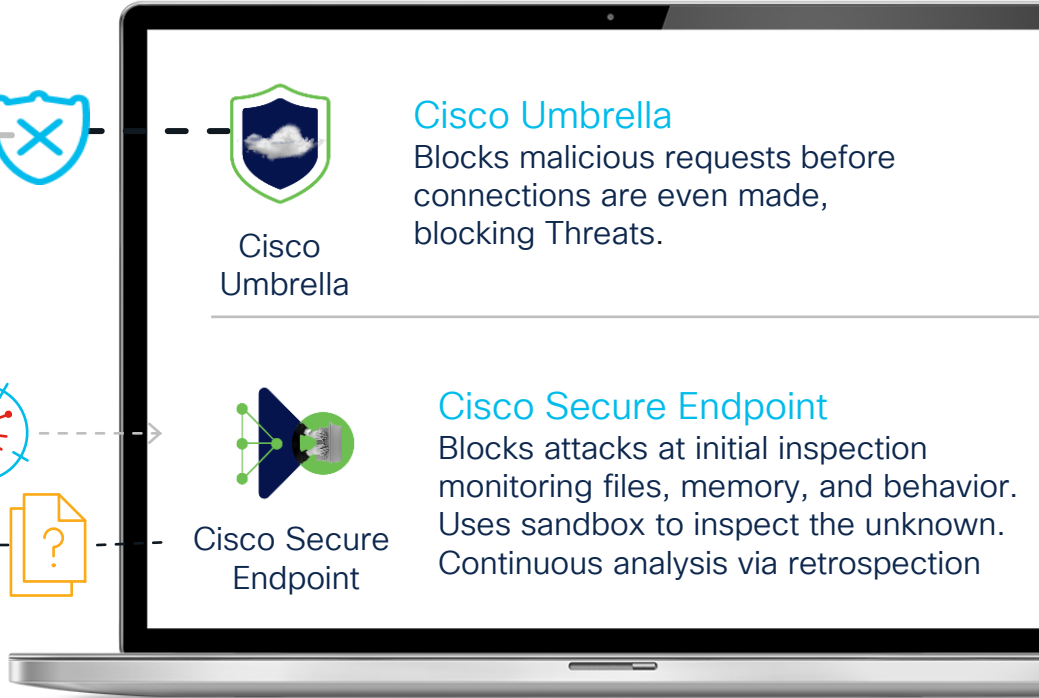
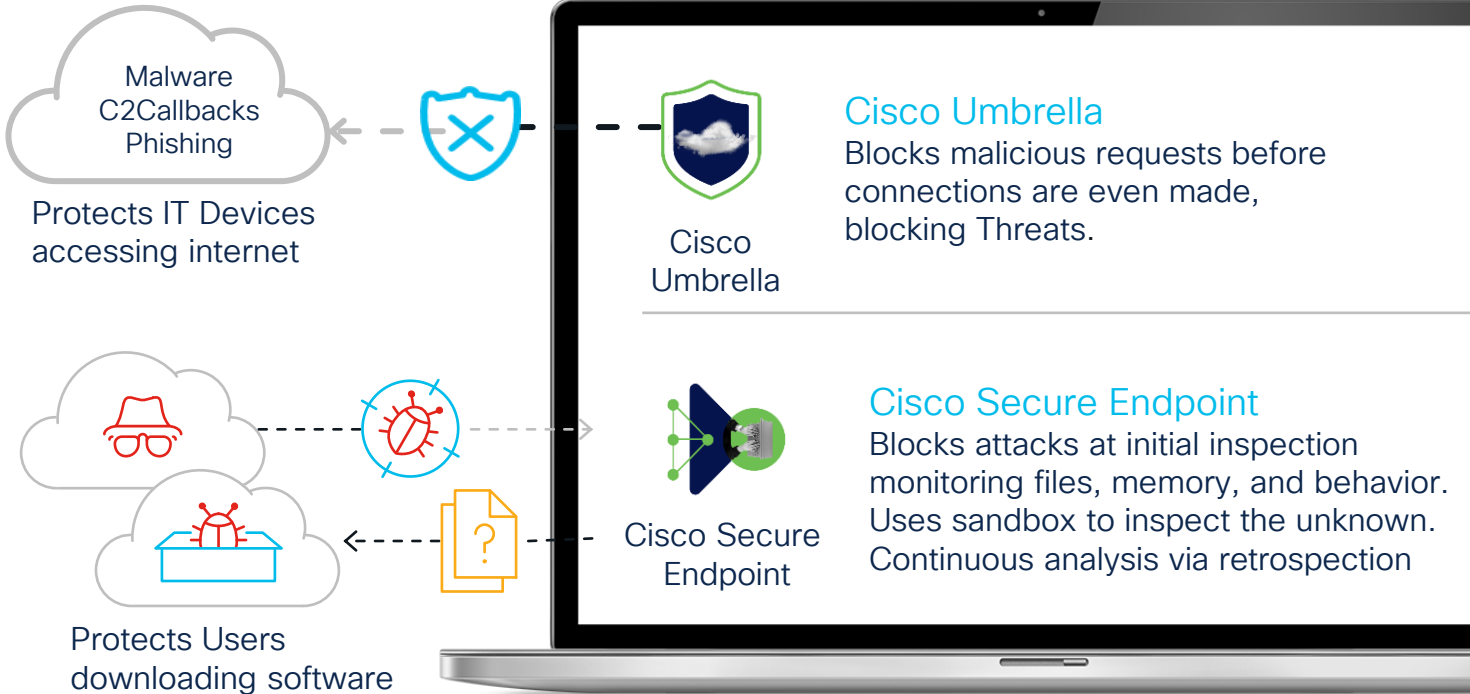
pxGrid Clients

Rows/Page 4 << 1 / 1 >> 4 Total Rows

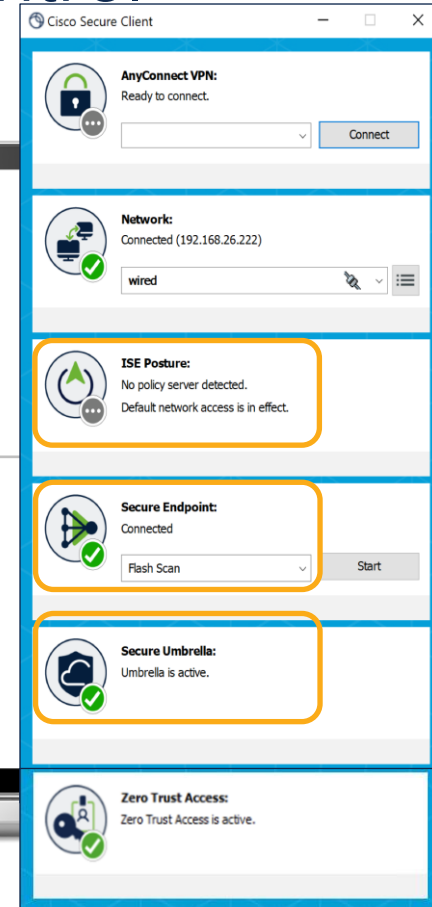
<input type="checkbox"/>	Name	Description	Client Groups	Status
<input type="checkbox"/>	smc-ise-client	Account for SW		● Enabled
<input type="checkbox"/>	fmc-10de14d6c2fd11eb91b2f946f...			● Enabled

Do not forget Threat Prevention and Control

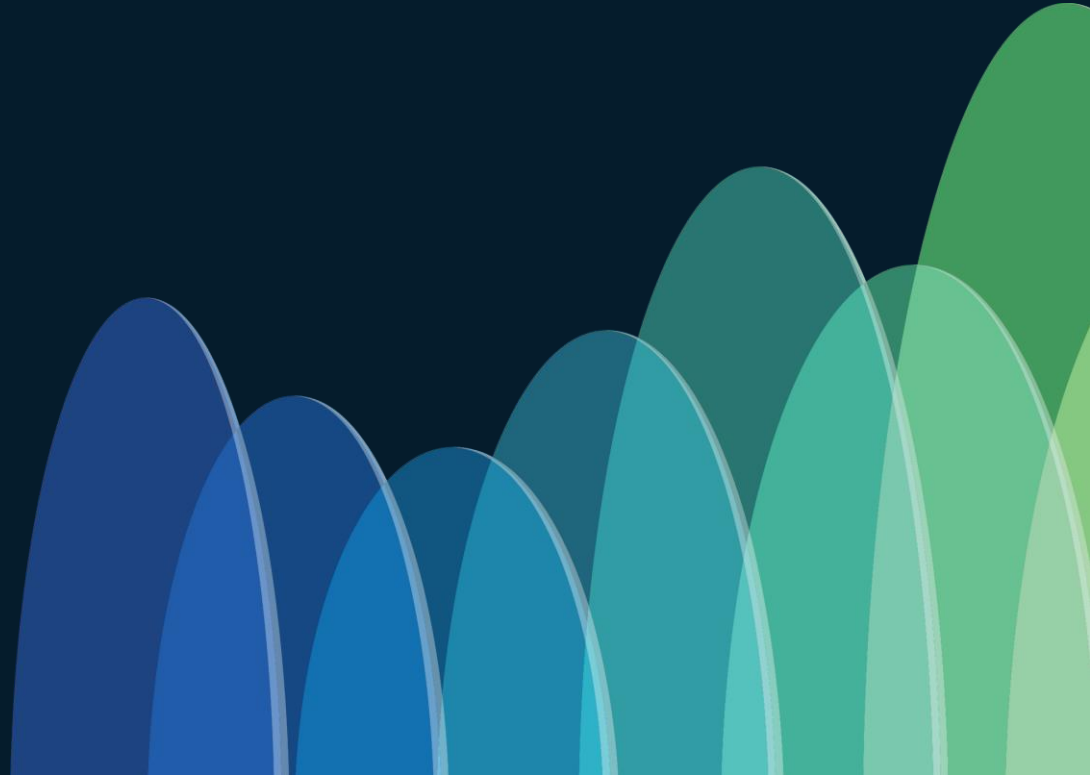
for user devices



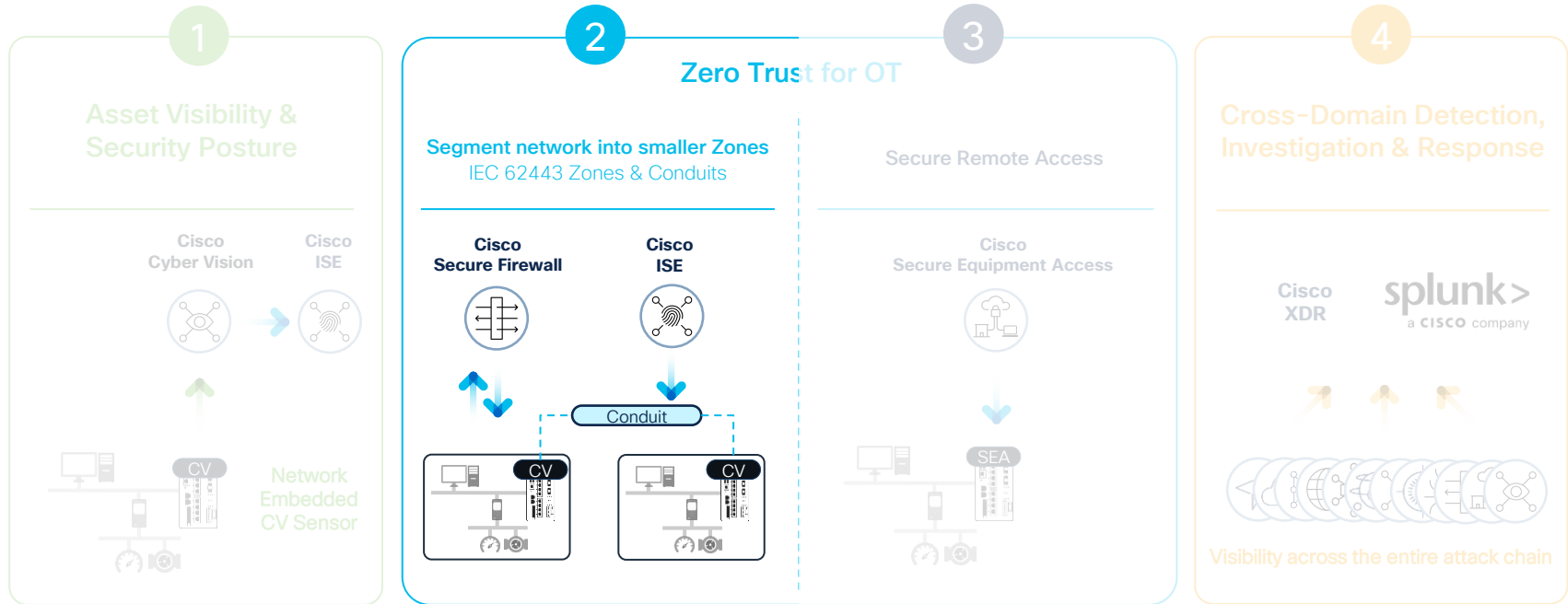
User endpoint



Segment
network into
smaller zones



Cisco's Industrial Threat Defense Journey

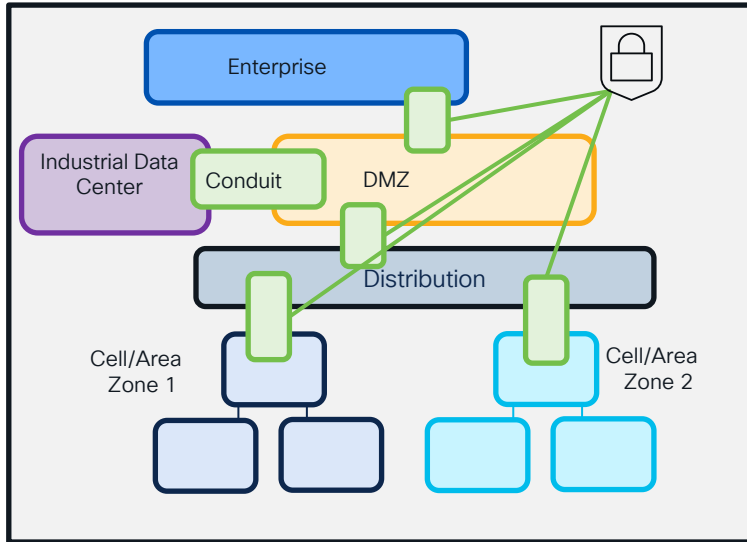


Macro and Micro segmentation

Macro Segmentation

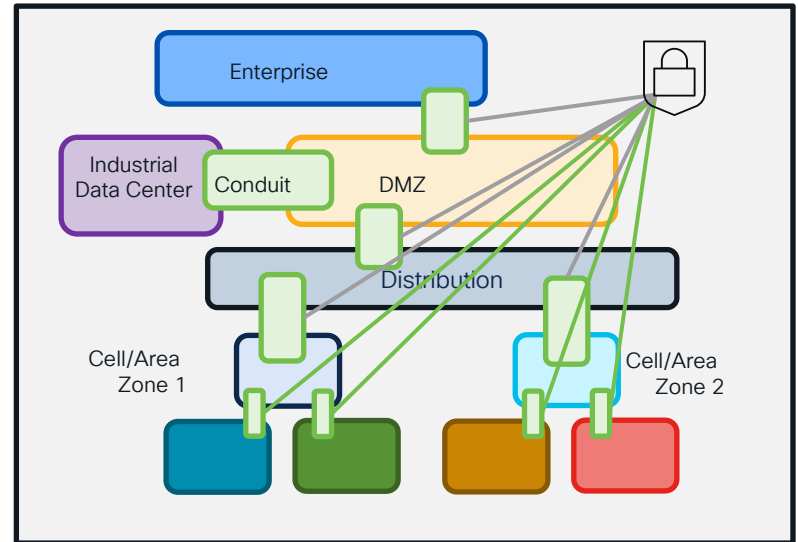
- Policy across “large” zones (between Cell/Area Zones / Production Lines)
- Distribution is typically point of VLAN termination
- Generally done at Firewall level

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

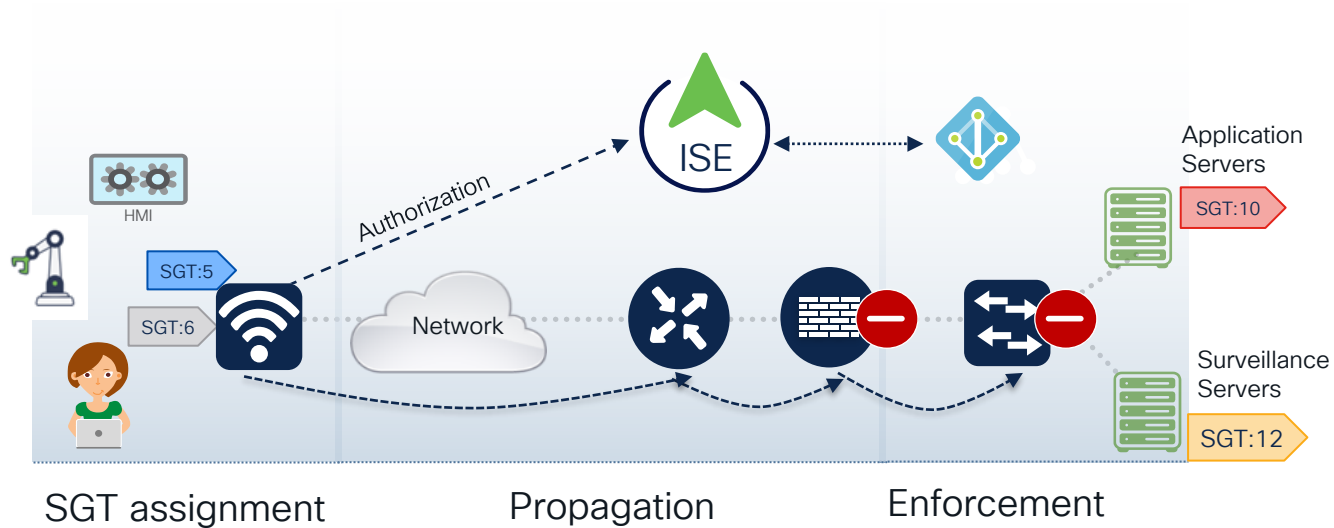
```
Switch-1# show cts role-based permissions
```

```
IPv4 Role-based permissions default:
```

```
Deny IP-00
```

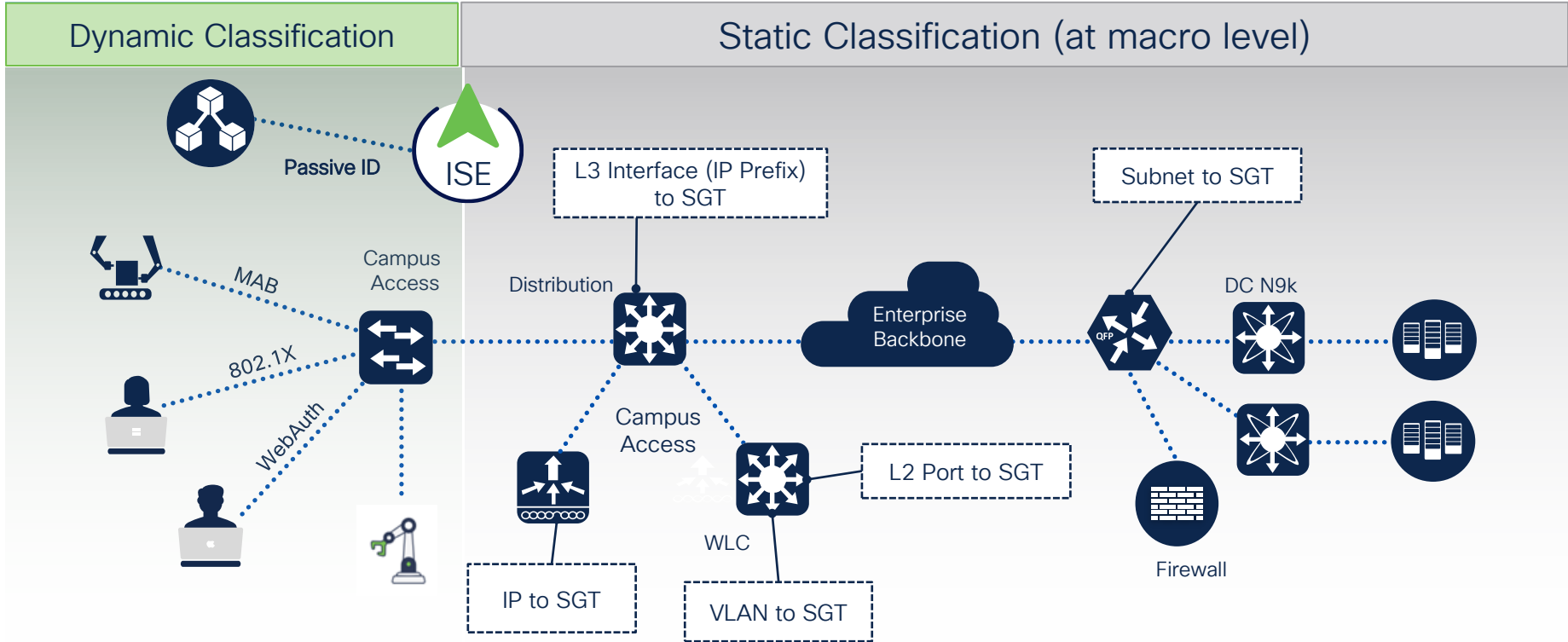
```
IPv4 Role-based permissions from group 10:Area_1 to group 100:Area_2:
```

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**.

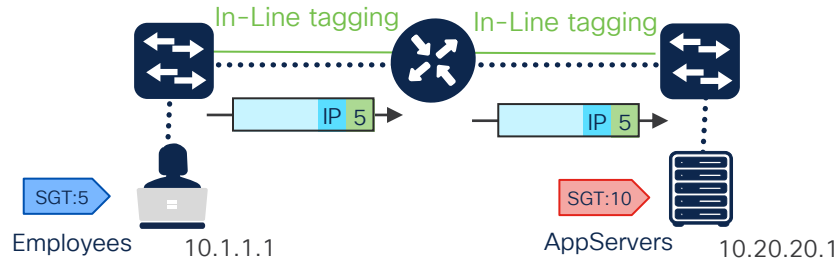
Classification Mechanisms



SGT Propagation

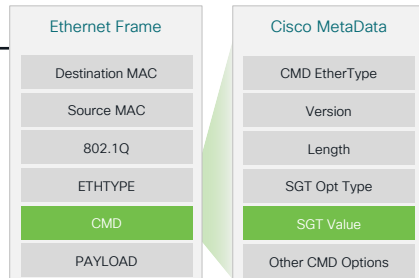
DATA PLANE PROPOGATION (INLINE TAGGING)

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



Propagation options

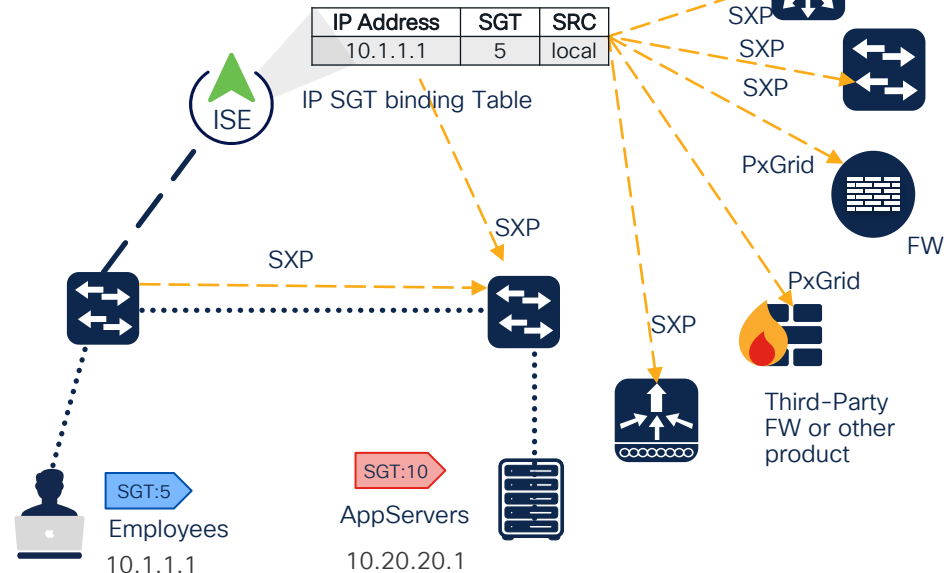
Cisco Meta Data (CMD)	Ethernet	MACsec	VXLAN
IPsec	DMVPN	GETVPN	



CISCO Live!

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

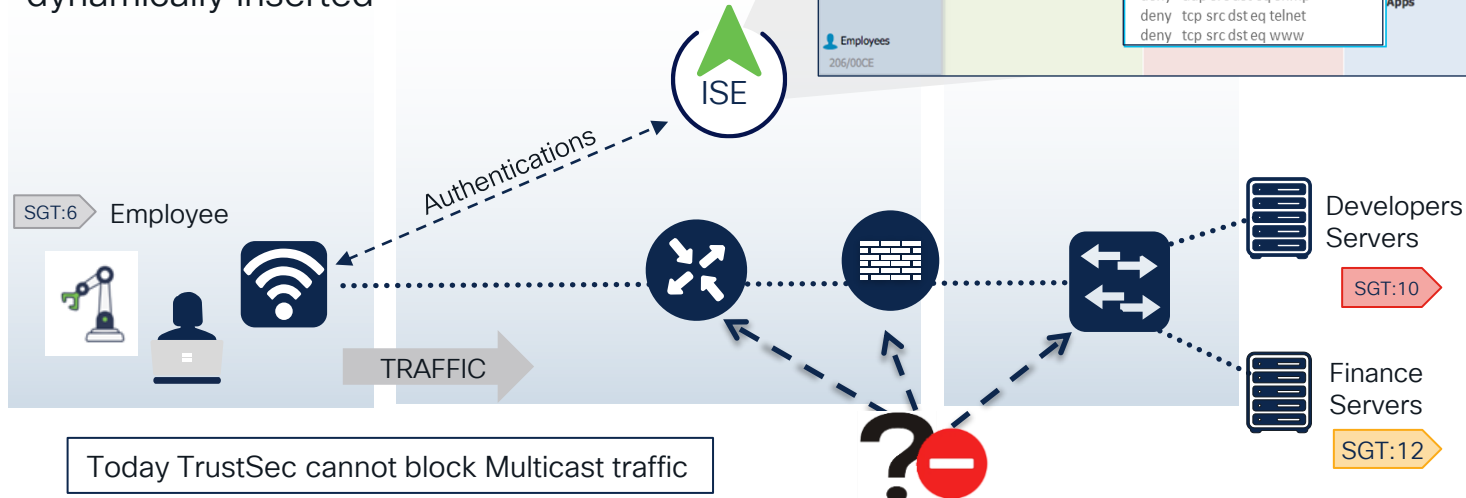
Egress Policy (Matrix View)

[Edit](#) [Add](#) [Clear Mapping](#) [Push](#) [Monitor All - Off](#) [Import](#) [Export](#) [View](#) Show All

Destination	Source	Policy	App	Action
Developers 110/006E	Building_Infra 4/0004	Anti_Malware	t IP	Permit IP
Development_Ser... 12/000C	Developers 110/006E		t IP	Deny IP
Engineering_Ser... 9/0009	Development_Ser... 12/000C		Apps	Deny IP
Finance_Server 5/0005	Employees 206/00CE			

```

deny icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
deny tcp src dst eq www
    
```

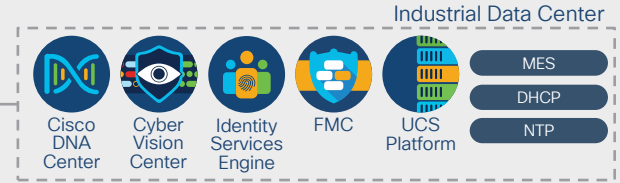


Network based zoning model

Site Operations Zone

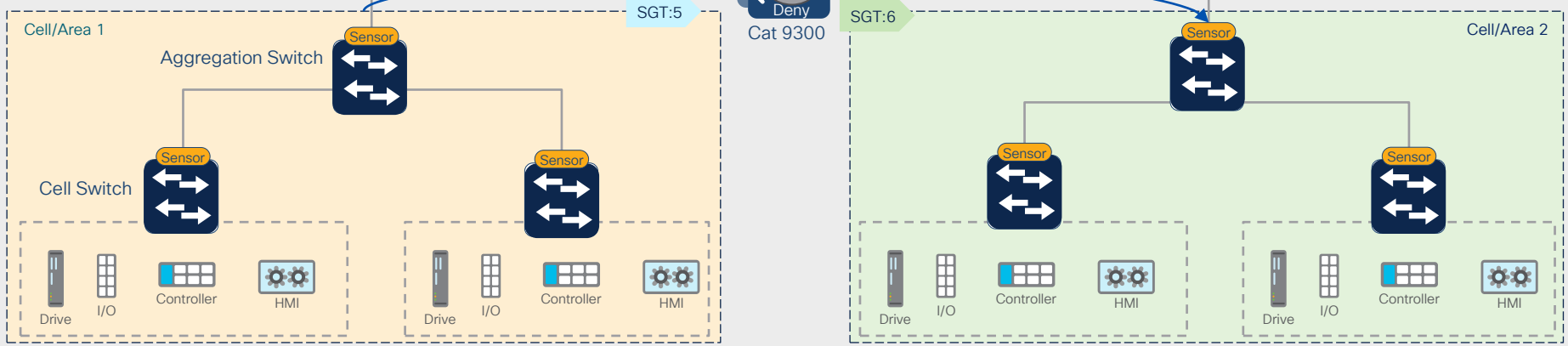
	Zone 1	Zone 2
Zone 1	✓	✗
Zone 2	✗	✓

Policy enforcement point



Static classification for Cell/Area

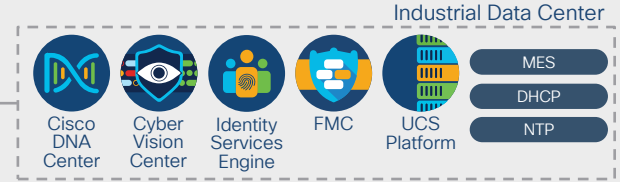
Cell/Area Zone



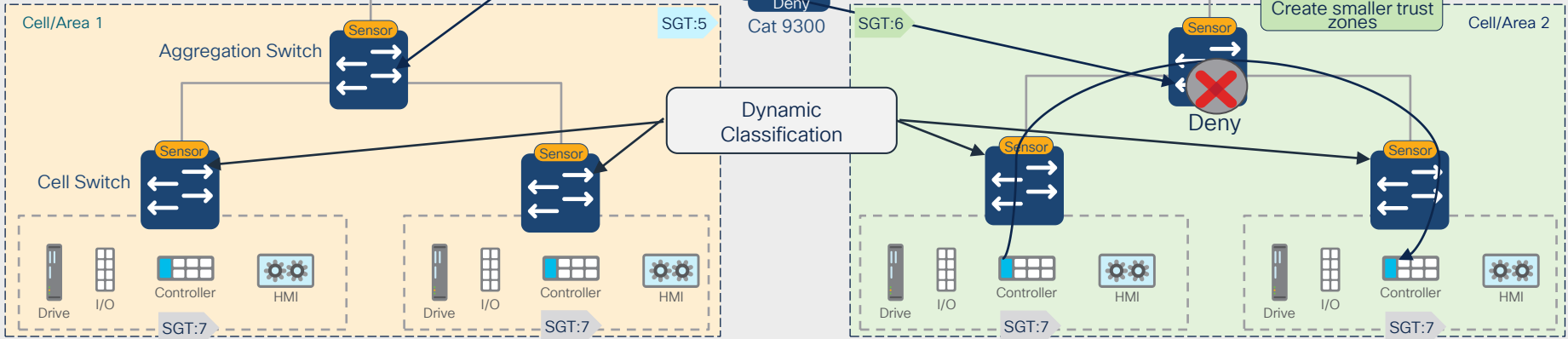
Extending segmentation to the Cell/Area zone

Site Operations Zone

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



Cell/Area Zone



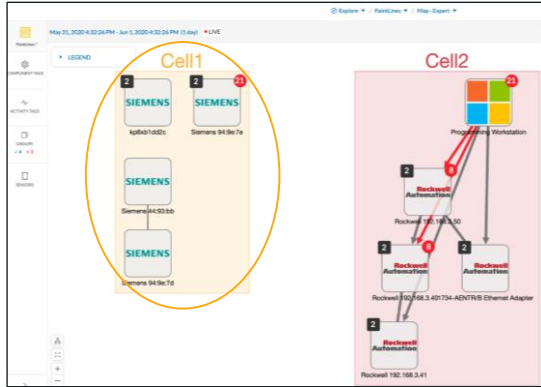
Policy control directly from CyberVision



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



I now have OT context to build the right security policies

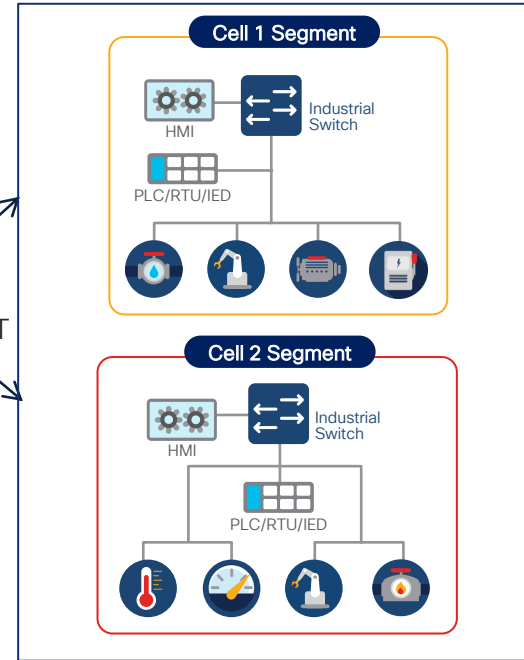


Cyber Vision Map View

	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

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

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

Applications | **Attributes** | Authentication | Threats | Vul

General Attributes

Description

Static Assignment false

Endpoint Policy Austin_Plant_Profiler

Static Group Assignment false

Identity Group Assignment Austin_Plant_Profiler

Custom Attributes

Attribute Name	Attribute Value
assetGroup	Root > Austin_Plant
assetDeviceType	Controller
assetId	101
assetIpAddress	192.168.119.39
assetMacAddress	e4:90:69:9e:ef:7d
assetName	192.168.119.39
assetProductId	1769-L36ERM/A LOGIX5336ERM

Results

Profiles Security Groups

Search

Status	Rule Name	Conditions	Profiles	Security Groups
✔	Plant	EndPoints:EndPointPolicy EQUALS Plant	× PermitAccess +	Plant × +
✔	Cell1	EndPoints:EndPointPolicy EQUALS Cell1	× PermitAccess +	Cell1 × +
✔	Cell2	EndPoints:EndPointPolicy EQUALS Cell2	× PermitAccess +	Cell2 × +
✔	LinePLC	EndPoints:EndPointPolicy EQUALS LinePLC	× PermitAccess +	LinePLC × +

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



StartHMI - FactoryTalk View SE Client - [MainDisplay - /SecDem] HMI1

HMI1 TrustSec Segmentation

Data IN Cell Controller FROM Line

13 Days 5 Hours 38 Minutes 33 Seconds

Cell 1 Controller
13 Days 5 Hours 40 Minutes 7 Seconds

Line Controller - Cell 2
13 Days 5 Hours 38 Minutes 33 Seconds

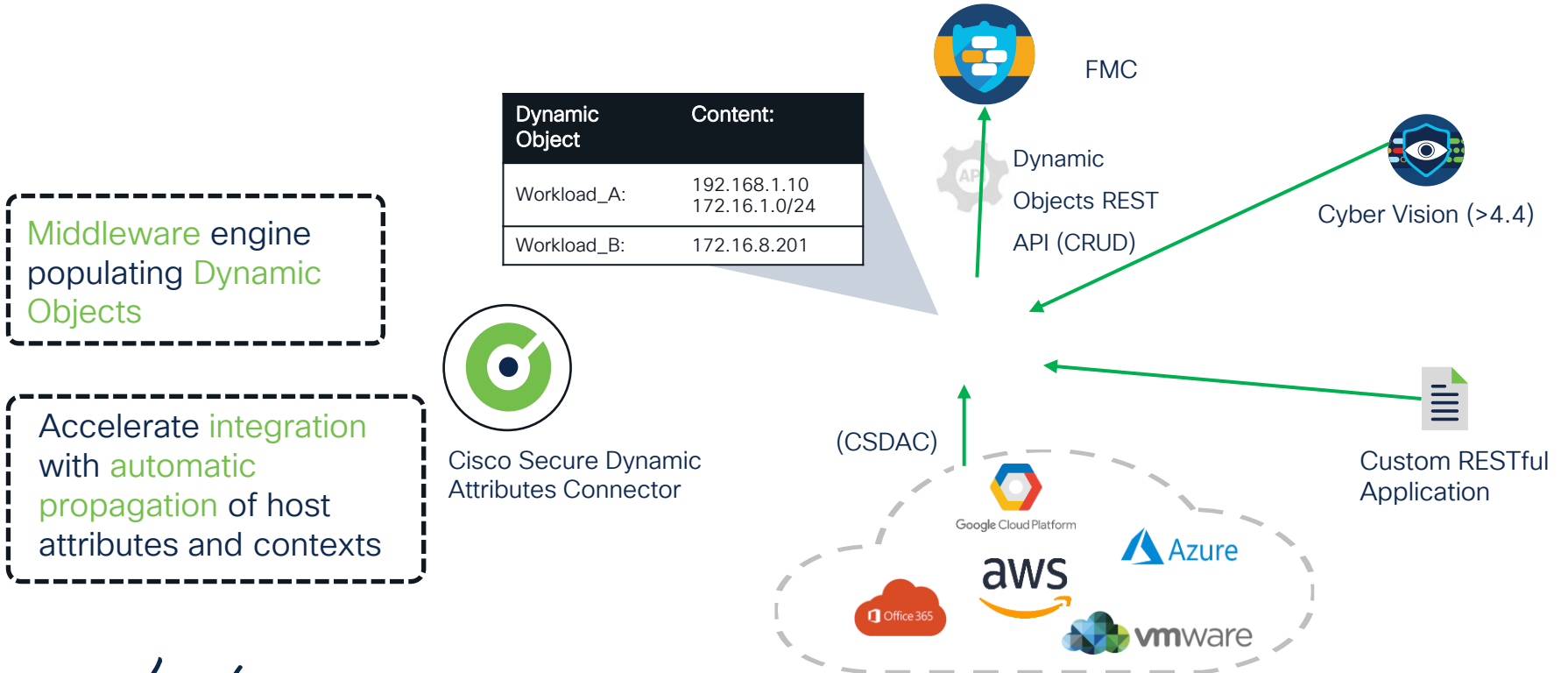
Buttons: Disable Timer, Reset Timer, Load Timer from Line, Enable Remote Access, Configuration

Arrow: CIP Write

Status Bar: Symbol upload ends successfully for 1789-L60/A in slot 1 of the chassis at 198.18.10.1. [Clear] [Clear All]

Dynamic objects in Cisco Secure Firewall

Cisco Secure Dynamic Attributes Connector



Dynamic Objects in Action

Cisco Secure Dynamic Attributes Connector

Cyber Vision



Dynamic Objects (REST)

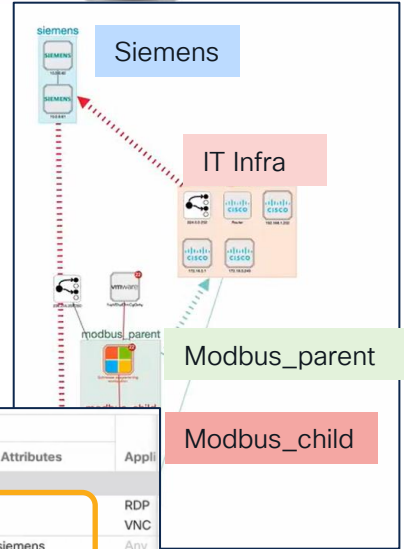


API calls for groups and associated IPs

Dynamic Objects	
Name	
center1_it_infra	
center1_modbus_child	
center1_modbus_parent	
center1_ot_infra	
er1_siemens	
er1_suspicious_block	
er1_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	Zones	Networks	Ports	Dynamic Attributes	Zones	Networks	Ports	Dynamic Attributes	Appli
Mandatory (1 - 3)										
1	siemens cell block RDP an...	Block	Any	Any	Any	center1_siemens	Any	Any	Any	RDP VNC
2	cyber vision block inter cell	Block	Any	Any	Any	center1_modbus_child	Any	Any	center1_siemens	Any
3	suspicious cyber vision 1 -...	Block	Any	Any	Any	center1_very_suspicious...	Any	Any	Any	Any
default (-)										

Demo: Cisco Secure Dynamic Attributes Connector


CISCO *Live!*




Explore - Plant - Cisco Cyber Vi... Identity Services Engine... Policy Editor | Secure Firewall... Cisco Secure Dynamic Attributi... +



csdac.dcloud.cisco.com/adapters

Cisco Cyber Vision SE FMC SMC CSDAC

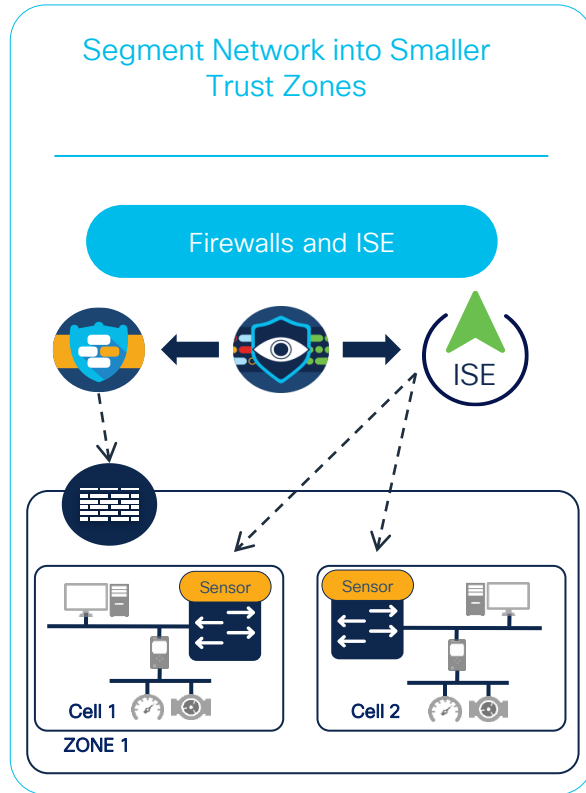
Dynamic Attributes Connector Connectors Dynamic Attributes Filters **Adapters** admin Administrator 

Adapters

1 adapter 

#	Name	Description	Type	Status 	Actions
1	FMC		FMC	Ok	

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.

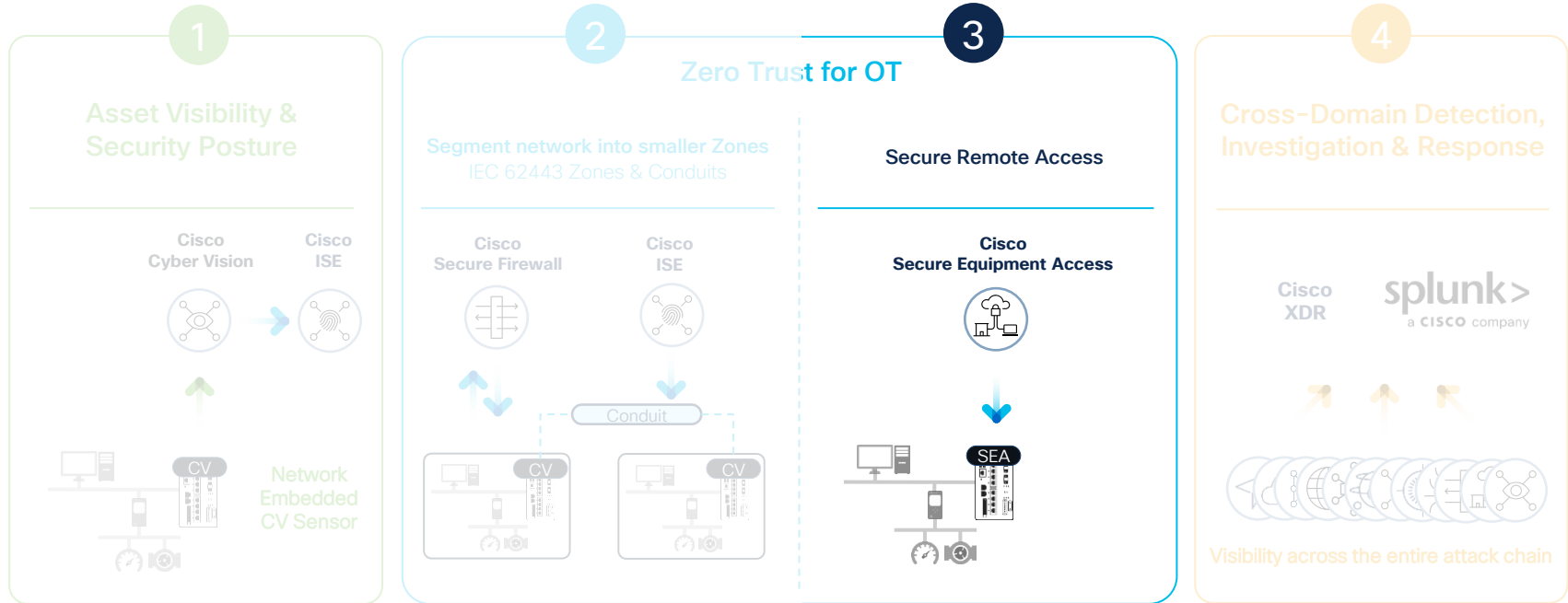
TrustSec with SGTs on switches or firewalls.

Secure Remote Access

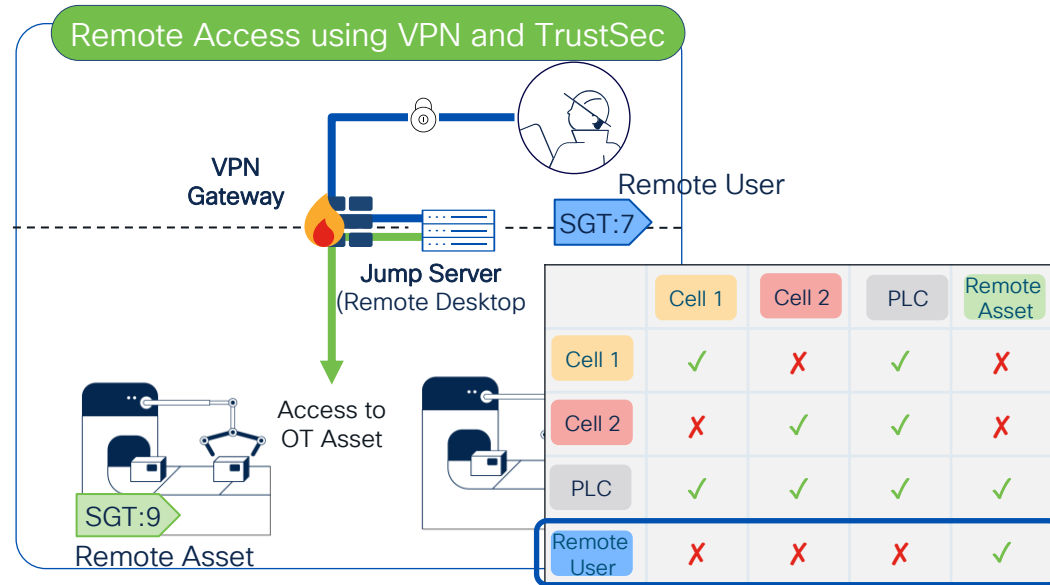
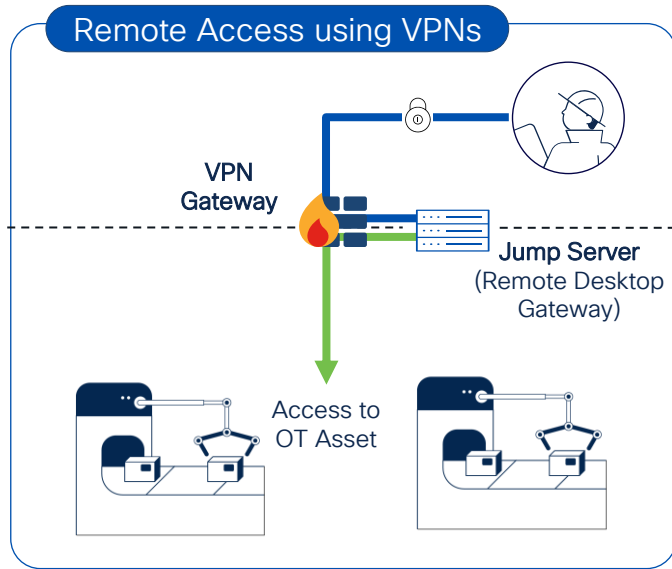
CISCO *Live!*



Cisco's Industrial Security Journey



Enhancing VPNs with TrustSec

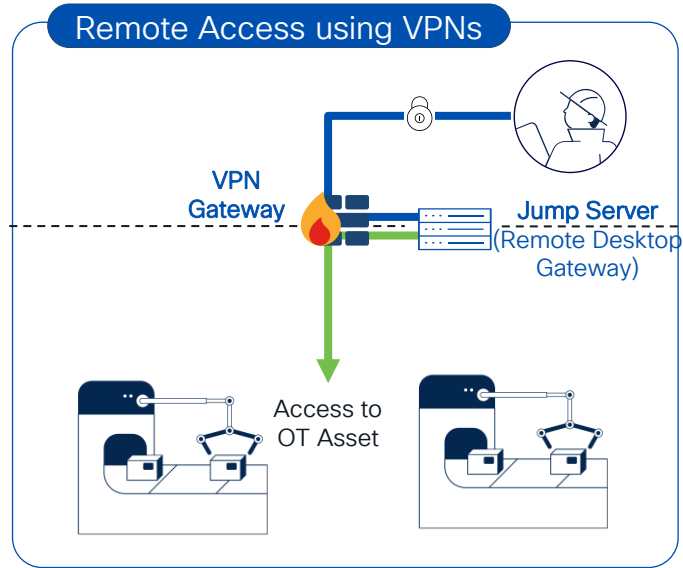


- Always-on solutions with all-or-nothing access
- Firewall rules need to be frequently updated
- Manual session management using jump servers

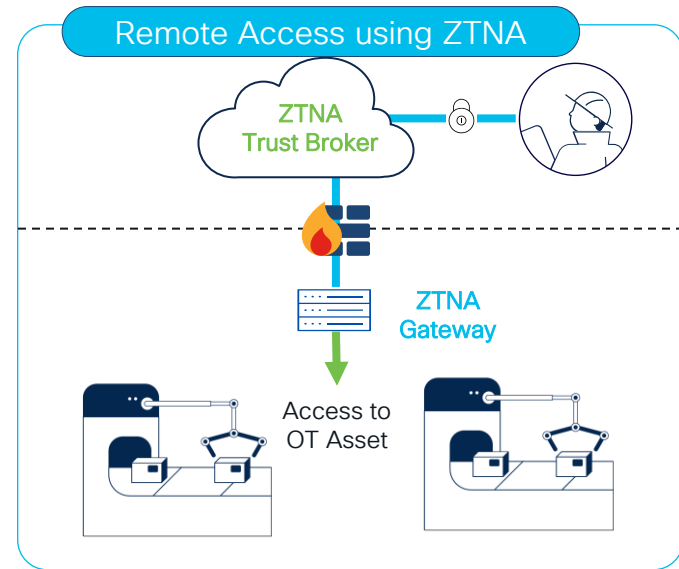
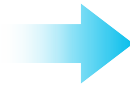
- Via CyberVision OT arraigns the device to a “Remote Asset” Group when access needed
- ISE dynamically reclassifies the device to the appropriate SGT
- The remote user has access only to the remote Asset device when it is needed

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

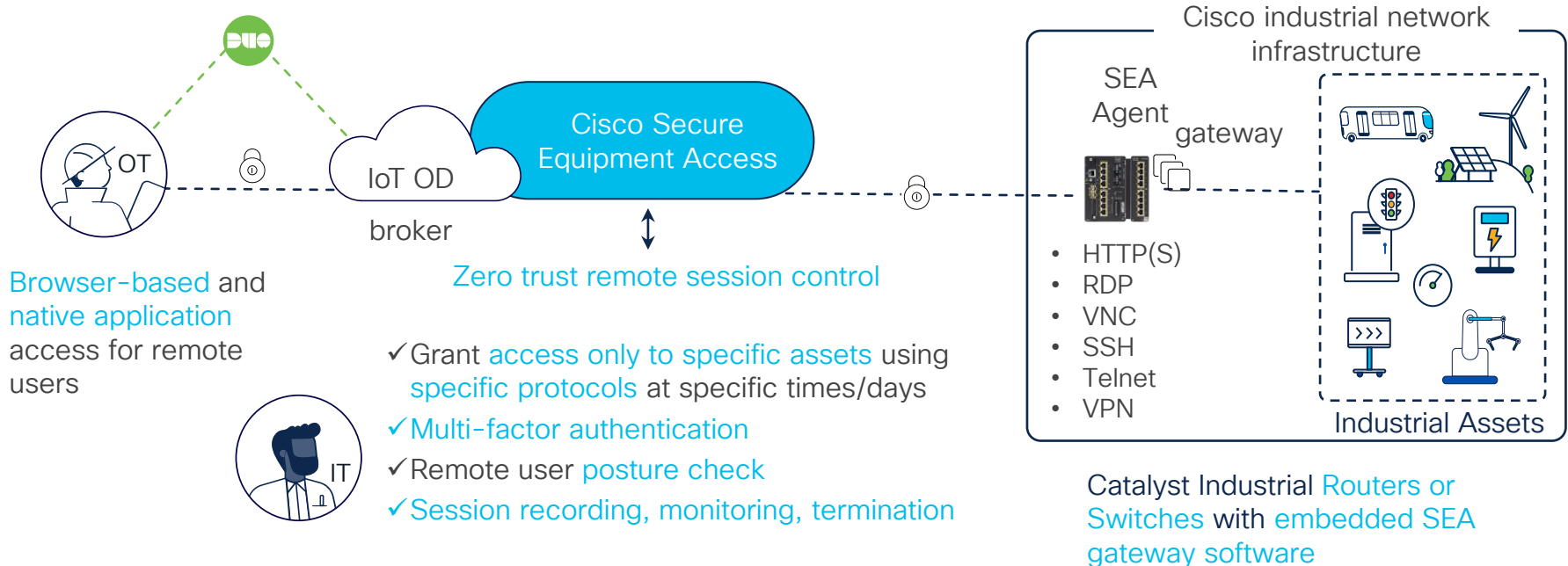


- Trust broker manages policy based on identity and context, and grants access to specific resources at specific times
- Gateway establishes an outbound connection to the trust broker eliminating complexity of firewall rules

Secure Remote Access

with Secure Equipment Access

Perform remote operations while enforcing strong zero trust controls



Demo: Cisco Secure Equipment Access

CISCO *Live!*



Cisco IoT

us.ciscoiot.com/coreshell/srapugin#/applicationlist

IoT Operations Dashboard

mai yub+seaad...
SEA Sandbox

Service Secure Equipment Access

Dashboard

Remote Sessions

Access Management

System Management

Quick Wizard

Remote Sessions

Download SEA Plus App

SEA Plus Offline

All Access Methods

- All Access Methods
- ABB Clientless access Always On
- PLC SEA Plus access Always On

ABB-1 (SSH)
Via SSH
Cell-1-IE3400

Availability: Always Active

ABB-2 Win Server 2022 (RDP)
Via RDP
Ethernet-IR1101

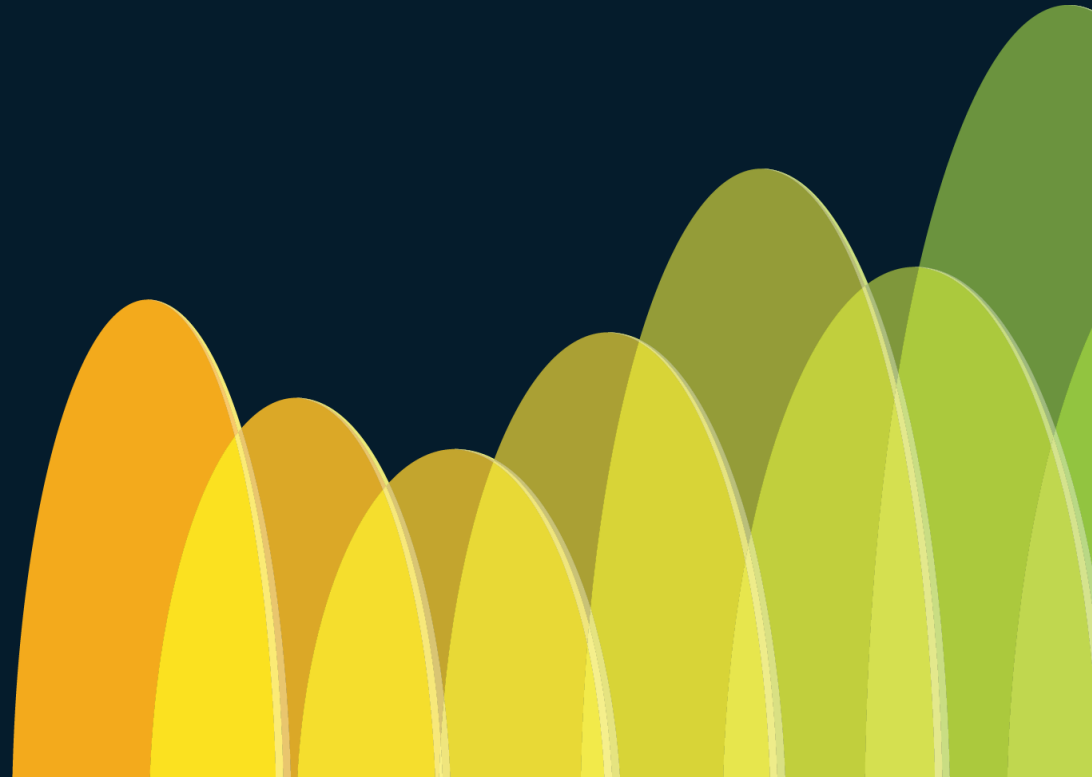
Availability: Always Active

ABB-4 (WEB_APP)
Via Web App
Cell-1-IE3400

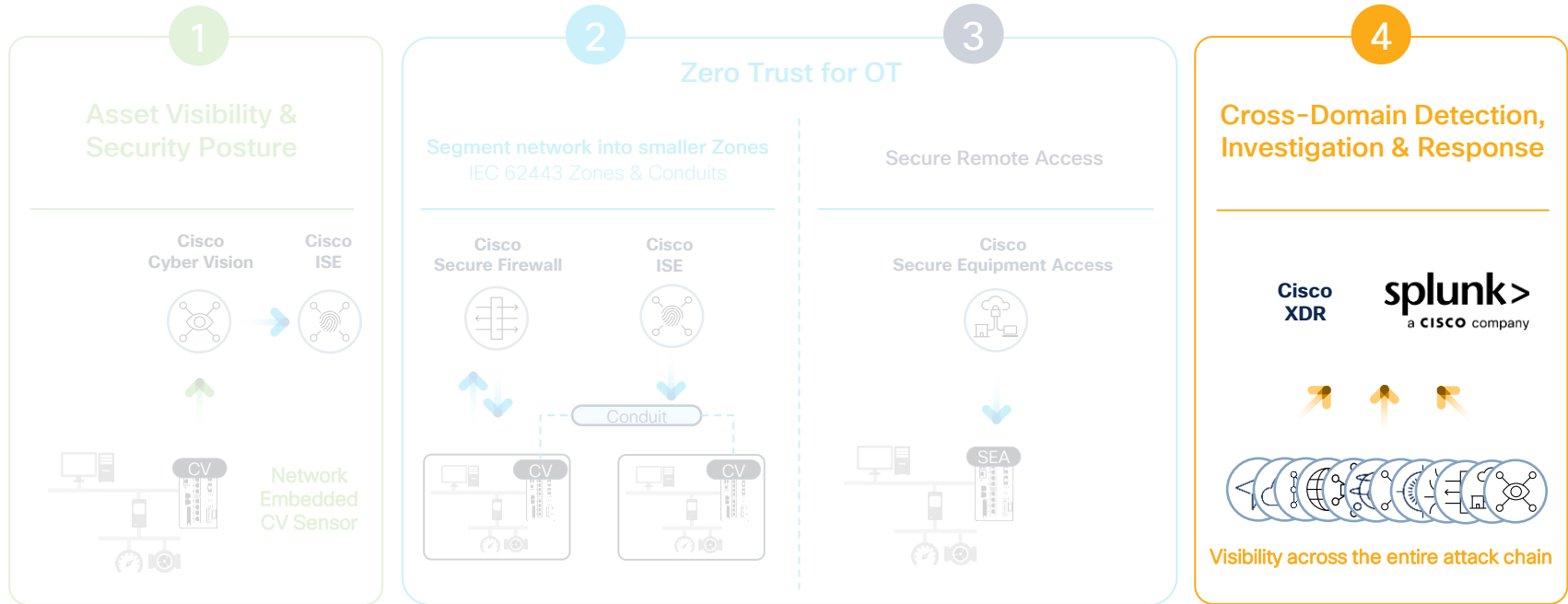
ABB-5 Cell-1-backup (TELNET)
Via Telnet
Distribution-Switch-IE3400

Guide me!

Detection, Investigation & Response



Cisco's Industrial Threat Defense Journey



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

Utilities see on Explore

Utilities Baseline

7 new components 6 new activities
2 changed components 1 changed activity

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

Last check: Jan 19, 2022 11:24:48 PM
Description: Utilities Baseline

Active criteria

GROUPS ✓7 X2 ^

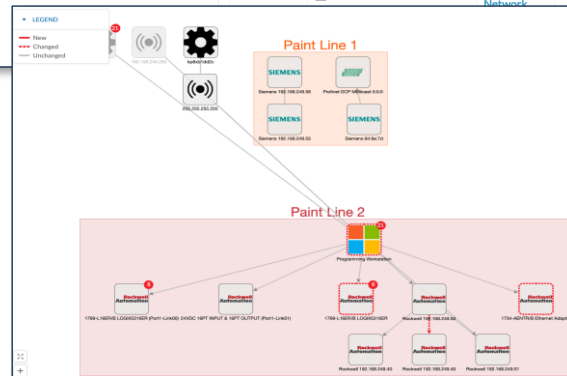
- Broadcast-Components Racket-replay
- Utilities Demo City Substation
- Process Bus Network Station Bus Network
- Control Center Enterprise Network
- Devices without groups

SENSORS ✓1 ^

- SENSORVM-INT17283

37 Components 7 new 2 changed

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



Changed Activity X

Rockwell Automation **Paint Line 2** ▲ high
IP: 192.168.249.50
MAC: f4:54:33:91:cbee

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

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

Tags:
Read Var Write Var EthernetIP

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

Acknowledge differences Report differences
Remove and keep warning Individual acknowledgment

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

source	destination	Component source	Component destination
intel 192.168.0.12	212.166.210.80	Name: Intel 192.168.0.12 MAC: 64:80:99:d8:5d:4c IP: 192.168.0.12 Tag: HTTP Client	Name: 212.166.210.80 MAC: a4:08:fs:e1:03:ec IP: 212.166.210.80 Tags: DNS Server, Public IP

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
9300/9300X/9400
Enterprise Switch



Cyber Vision Center



Catalyst IR8300 Series
Rugged Router



IC3000 Industrial Compute

Review what happened: "Events / Calendar"

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

Live! 11:00 AM

- 11:07:18.253 Cisco Cyber Vision Configuration "Admin User" has created the baseline My OT Baseline.
- 11:16:17.965 Control Systems Events Stop CPU command has been detected from Vmware 192.168.249.114 | IP: 192.168.249.114 | MAC: 00:0c:29:c7:c8:76 to 1769-L16ER/B LOGIX5316ER | IP: 192.168.249.50 | MAC: f4:54:33:91:cb:ee
- 11:16:20.324 Anomaly Detection 2 differences have been detected in the baseline My OT Baseline
- 11:17:45.302 Cisco Cyber Vision Configuration "Admin User" has created the baseline My IT Baseline.
- 11:25:13.204 Cisco Cyber Vision Configuration A new component Vmware 192.168.249.114 | IP: 192.168.249.114 | MAC: 00:0c:29:c7:c8:76 to 1769-L16ER/B LOGIX5316ER | IP: 192.168.249.50 | MAC: f4:54:33:91:cb:ee included to the baseline My OT Baseline by "Admin User" with the message "I installed this device, it's the new engineering station."
- 11:30:54.292 Cisco Cyber Vision Configuration A new activity Vmware 192.168.249.114 → 1769-L16ER/B LOGIX5316ER has been added to the baseline by "Admin User" This activity has not been included to the baseline and you will be informed if it is detected again.

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

... including how admin reacted

Communications and Device details

category Control Systems Events severity high

Search an event

◀ 1 2 3 ... 8 9 10 11 12 ▶

01/19/2022 02:00:01 Control Systems Events New program has been uploaded, flow from Dell 10.4.0.6 (Lyon| Windows Stations) | Dell 10.4.0.6 | IP: 10.4.0.6 | MAC: 84:8f:69:e1:a7:9b to

01/19/2022 02:00:01 Control Systems Events New program has been uploaded, flow from Dell 10.4.0.6 (Lyon| Windows Stations) | Dell 10.4.0.6 | IP: 10.4.0.6 | MAC: 84:8f:69:e1:a7:9b to

01/19/2022 02:00:01 Control Systems Events New program has been uploaded, flow from Dell 10.4.0.6 (Lyon| Windows Stations) | Dell 10.4.0.6 | IP: 10.4.0.6 | MAC: 84:8f:69:e1:a7:9b to

01/19/2022 02:00:01 Control Systems Events Stop CPU command has been detected from STATION-ROCKWEL (Munich| Packing Machine) | STATION-ROCKWEL | IP: 192.168.105.241 | MAC: 52:54:00:31:fd:ef to

01/19/2022 02:00:01 Control Systems Events New program has been uploaded, flow from Dell 192.168.105.241 (Munich| Drilling Machine) | Dell 192.168.105.241 | IP: 192.168.105.241 | MAC: 34:17:eb:d1:c9:97 to

01/19/2022 02:00:01 Control Systems Events New program has been uploaded, flow from Dell 10.4.0.6 (Lyon| Windows Stations) | Dell 10.4.0.6 | IP: 10.4.0.6 | MAC: 84:8f:69:e1:a7:9b to

01/19/2022 02:00:01 Control Systems Events New program has been uploaded, flow from Dell 10.4.0.6 (Lyon| Windows Stations) | Dell 10.4.0.6 | IP: 10.4.0.6 | MAC: 84:8f:69:e1:a7:9b to

01/19/2022 02:00:01 Control Systems Events New program has been uploaded, flow from OW51 (Station Bus Network) | FCS0101 | IP: 10.4.0.46 | MAC: d4:ae:52:aa:dc:93

01/19/2022 02:00:01 Control Systems Events Stop CPU command has been detected from Vmware 192.168.249.114 (Munich) | Vmware 192.168.249.114 | IP: 192.168.249.114 | MAC: 00:0c:29:c7:c8:76 to 1769-L16ER/B LOGIX5316ER (Munich) | 1769-L16ER/B LOGIX5316ER | IP: 192.168.249.50 | MAC: f4:54:33:91:cb:ee

source destination Flow Component source Component destination

vmware 1769-L16ER/B L OGIX5316ER

Vmware 192.168.249.114 1769-L16ER/B L OGIX5316ER

Flow Source port: 1110 Destination port: 502

Component source Group: Munich Industrial impact: none Group description: Munich Parent Group Device: Vmware 192.168.249.114 Name: Vmware 192.168.249.114 MAC: 00:0c:29:c7:c8:76 IP: 192.168.249.114 Tags: Engineering Station

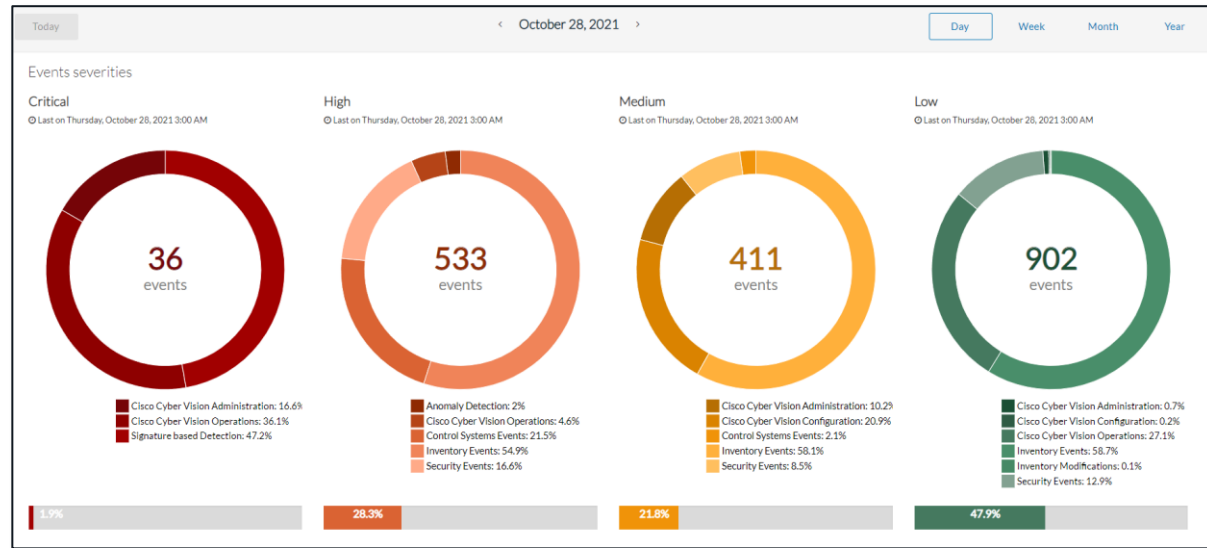
Component destination Group: Munich Industrial impact: none Group description: Munich Parent Group Device: 1769-L16ER/B LOGIX5316ER Name: 1769-L16ER/B LOGIX5316ER MAC: f4:54:33:91:cb:ee IP: 192.168.249.50 Tags: Controller Rockwell Automation 10 vulnerabilities detected

See technical sheet

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

CISCO *Live!*





Explore ▾ / All Presets ▾
📈 👤 ▾

Presets + New Preset




All My preset Basics Asset management Control Systems Management IT Communication Management Security Network Management

My preset


1. Manufacturing 

My preset

Manufacturing Demo Preset


 VNET/IP
  Profinet DCP
  Unite




Devices without groups
and 24 more criteria

2. Utilities 


My preset

Utilities Demo Preset.


 Utilities Baseline (17 🚩)


 Modbus
  HTTP
  IEC-104


and 11 more criteria

Emerson DCS 


My preset

 Program Download




 Programming Mode

 Memory Formatting


and 37 more criteria

Plant 


My preset

 RARP
  Broadcast
  ARP

and 7 more criteria

Yokogawa VNET/IP 

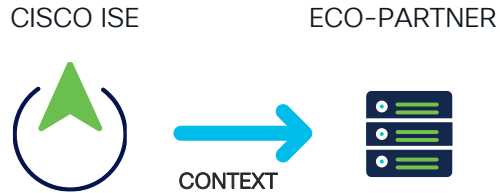
My preset

 VNET/IP

Mitigation

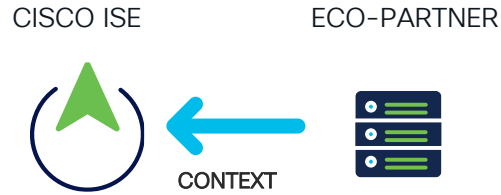
Power of integration pxGrid:

ISE CONTEXT OUT



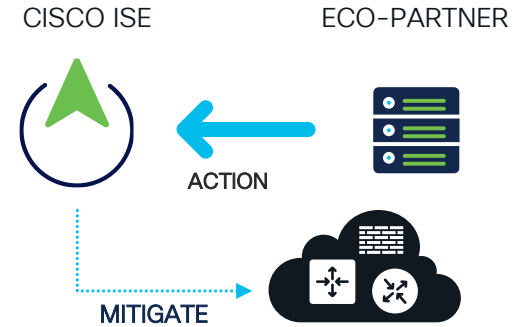
ISE makes Customer IT
Platforms User/Identity,
Device and Network Aware

ISE CONTEXT IN



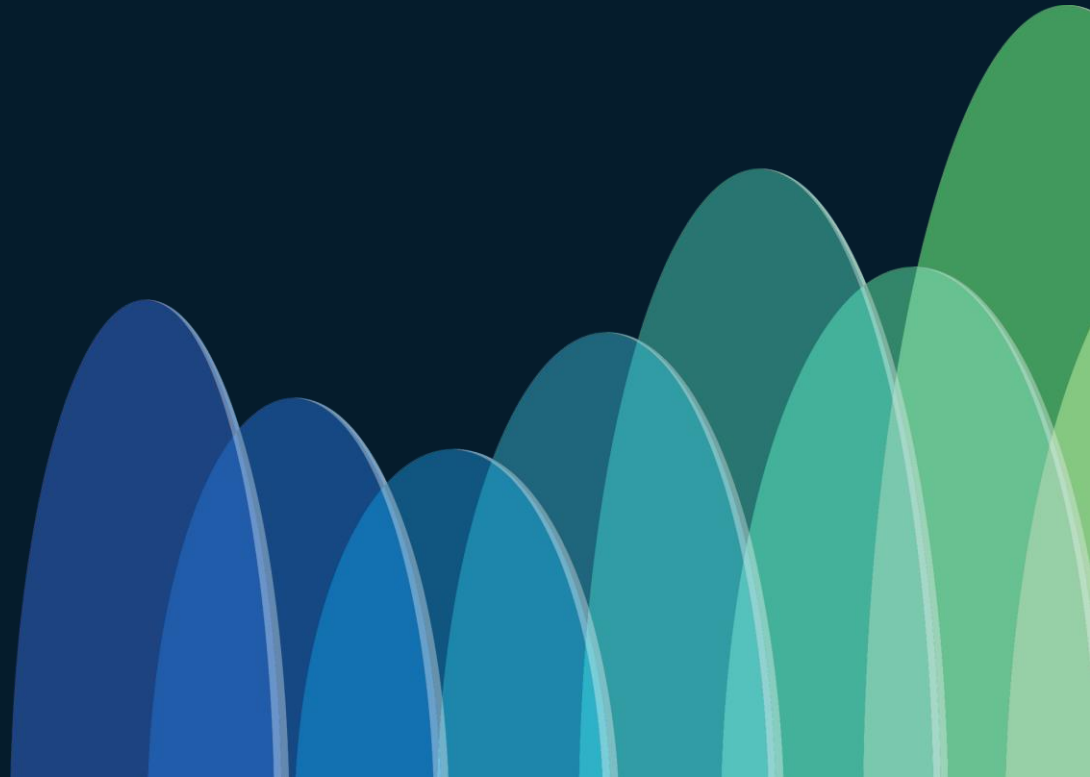
Enrich ISE context. Make ISE a
better Policy Enforcement
Platform

Rapid Threat Containment



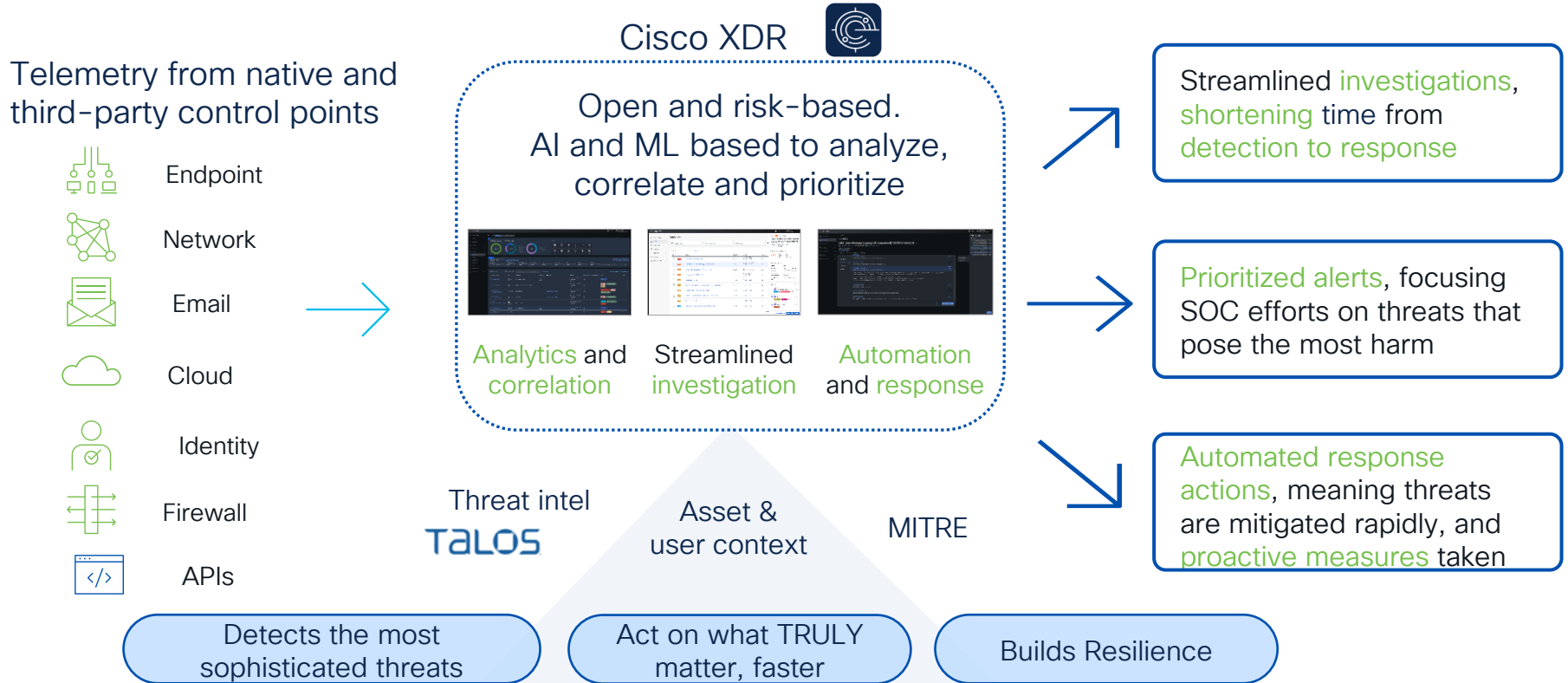
Enforce dynamic policies into
the network based on
Partner's request

Investigation



Cisco XDR

correlating and prioritizing security threats



Promote Cyber Vision events to Cisco XDR

View events in Cyber Vision

Launch investigation in XDR

April 2, 2024 11:40:55 AM critical Control Systems Events Stop CPU command has been detected from 192.168.105.241 (@ 192.168.105.241) | IP: 192.168.105.241 | MAC: 34:17:eb:d1:c9:97 to 192.168.105.112 (@ 192.168.105.112) | IP: 192.168.105.112 | MAC: 28:63:36:85:b3:32

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

[Report to XDR](#)

Control system event: Stop CPU command has been detected from...
New - Created by Cisco Cyber Vision on 2021-05-26T04:30:49.857Z

Summary Observables Timeline Signings Linked References (0)

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

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

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

KEY PROPERTIES

DESCRIPTION	Source	Destination
Name	DESKTOP-GBLJF2N	1759-118E1B16-LOCKSS316ER
Vendor	VMEI, Inc.	Rockwell Automation
Mac	00:0c:29:c7:c8:76	44:54:33:91:cb:ee
IP	192.168.249.114	192.168.249.50
Tags	WINDOWS, ENGINEERING PLC, ROCKWELL_AUTOMATION	

TABSETS

IP Address 192.168.249.50

192.168.249.50 IP Address

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

Promote event to Cisco XDR

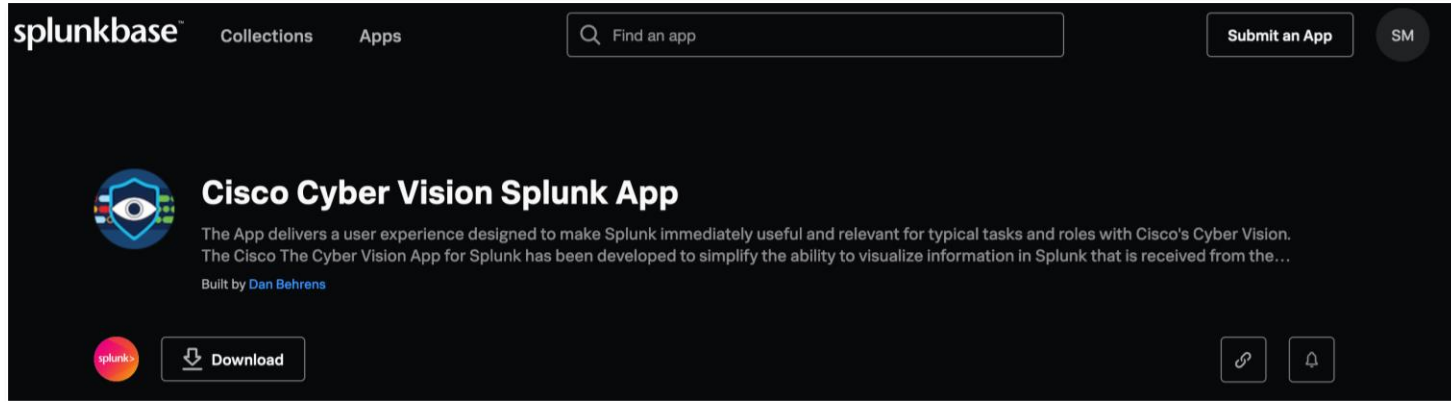
Events generated in Cyber Vision for process anomalies, signatures and control system can be promoted

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

cisco Live!

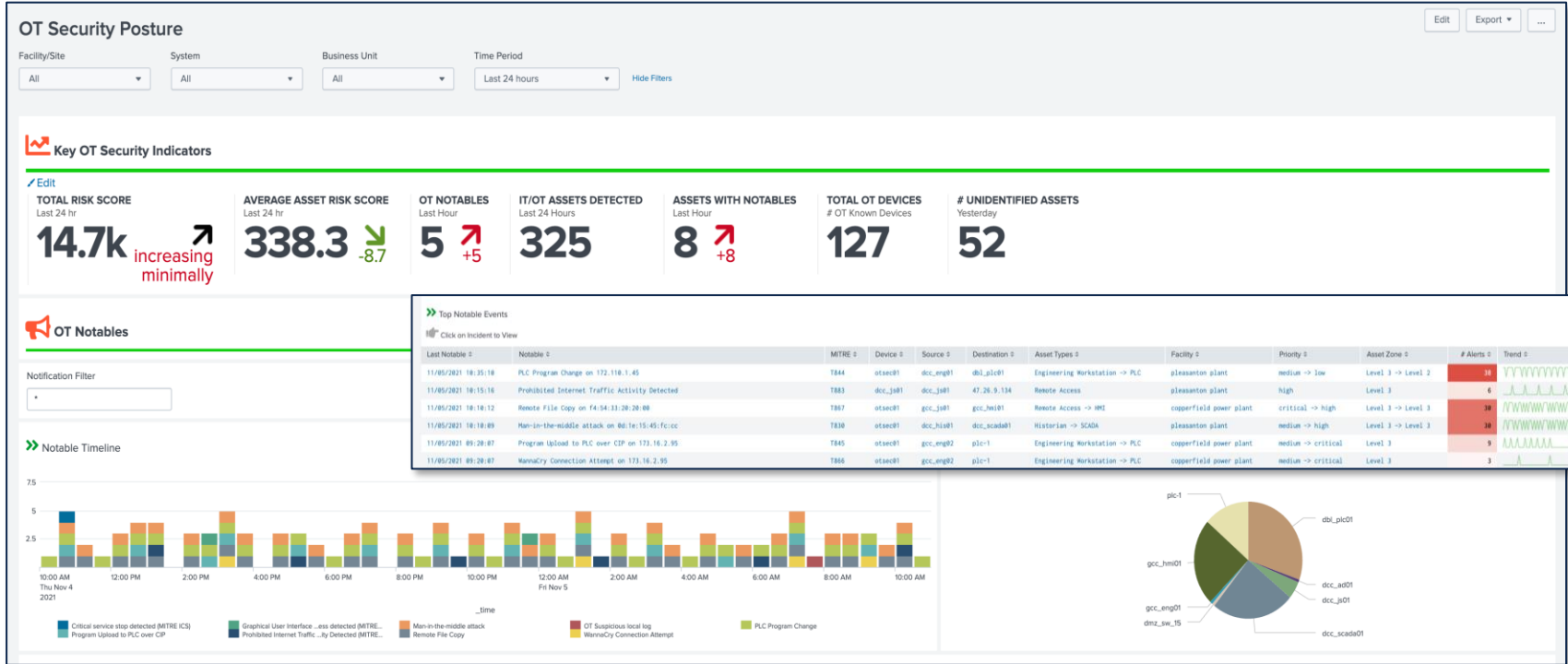


Integration of Splunk and Cyber Vision



- 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

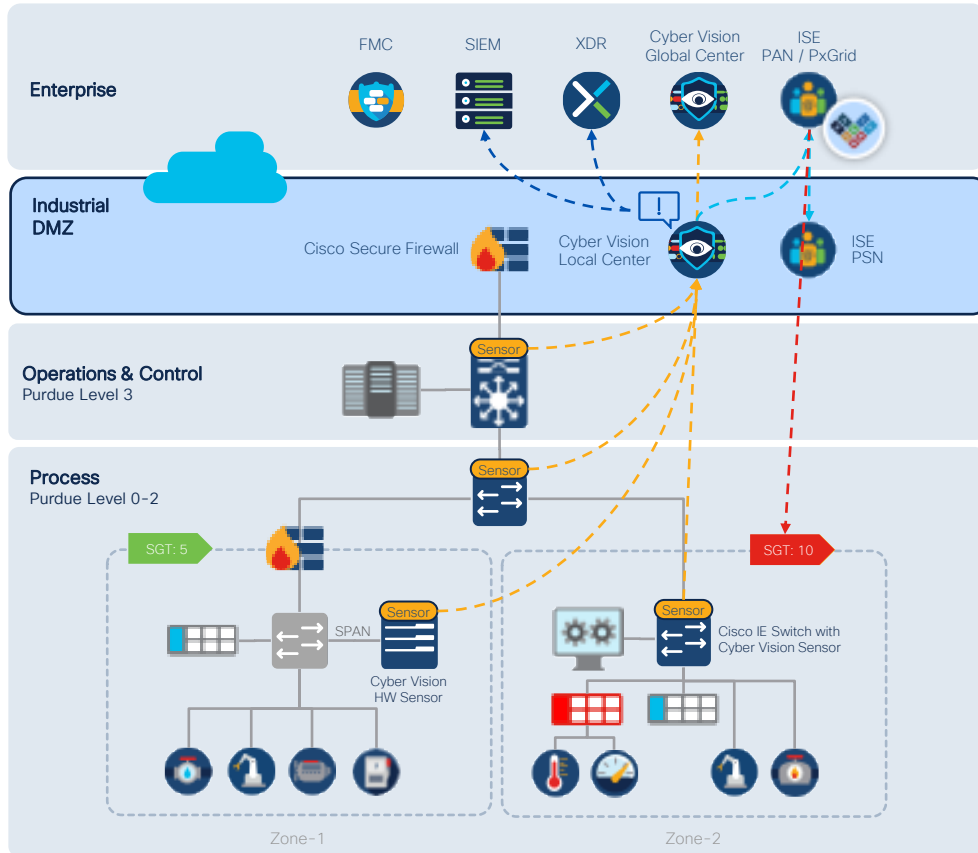
Splunk Dashboard



Wrapping up

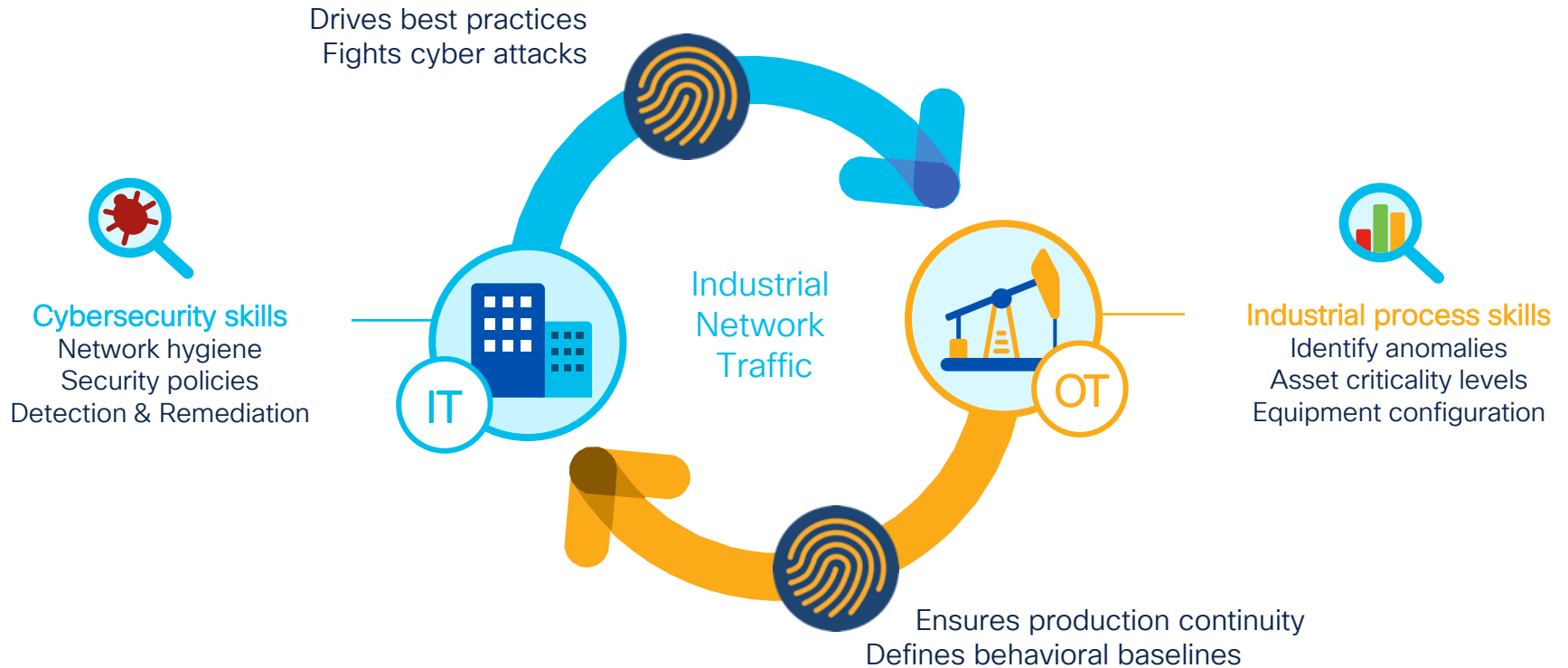


Let's put everything together



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

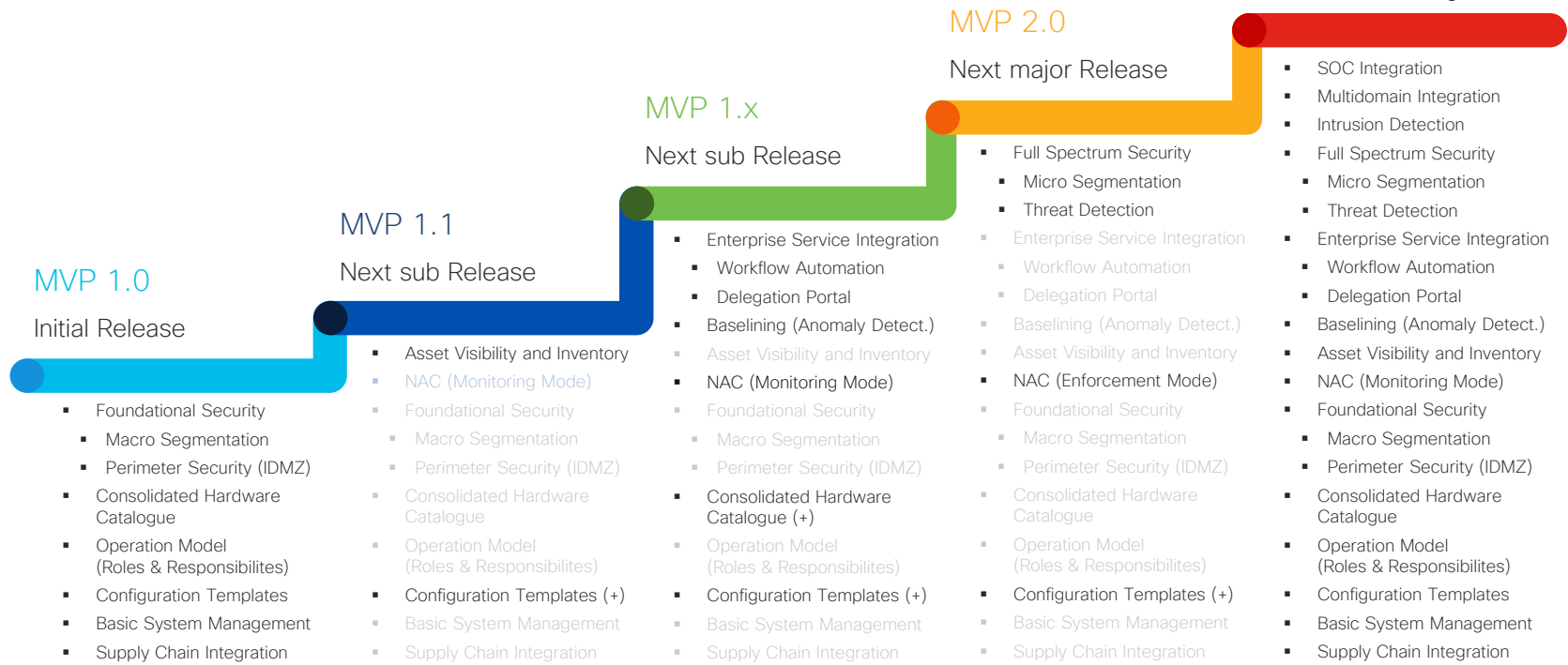


- Readiness of the current Infrastructure (Retrofit for brownfield needed to some degree)
- Fragmented knowledge about the systems in place
- What to do with all the Information ? (Iceberg effect)
- OT Procedures and Routines (Example: Troubleshooting Approach)
- Integration of the Supply-chain (EPC's,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



[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

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



Comprehensive

Provide tested system designs and configuration instructions



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



Thank you

CISCO *Live!*

CISCO *Live!*

GO BEYOND

A series of overlapping, vertically-oriented ovals in various shades of blue, ranging from light to dark, positioned on the right side of the image. The ovals are layered, with some appearing in front of others, creating a sense of depth and movement.