cisco Live!

#CiscoLive

The bridge to possible

Securing Industrial Networks: Where do I start?

Content by Francesca Martucci, Technical Solutions Architect – GSSO EMEA
Delivered by Dan Behrens – IoT Technical Marketing Engineer – Industrial Security
BRKSEC-2077

Cisco Webex App

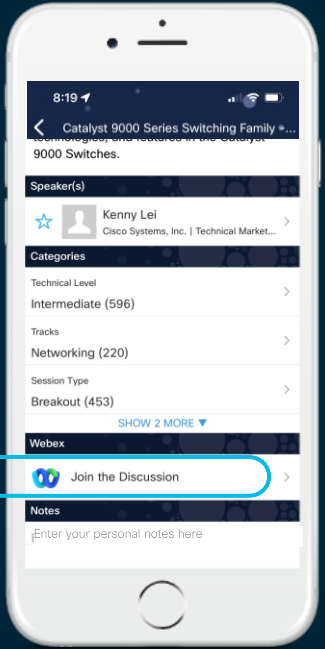
Questions?

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

How

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

Webex spaces will be moderated
by the speaker until June 17, 2022.



8:19

Catalyst 9000 Series Switching Family • ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2077

~~Who am I?~~ Who is Francesca

- Technical Solutions Architect

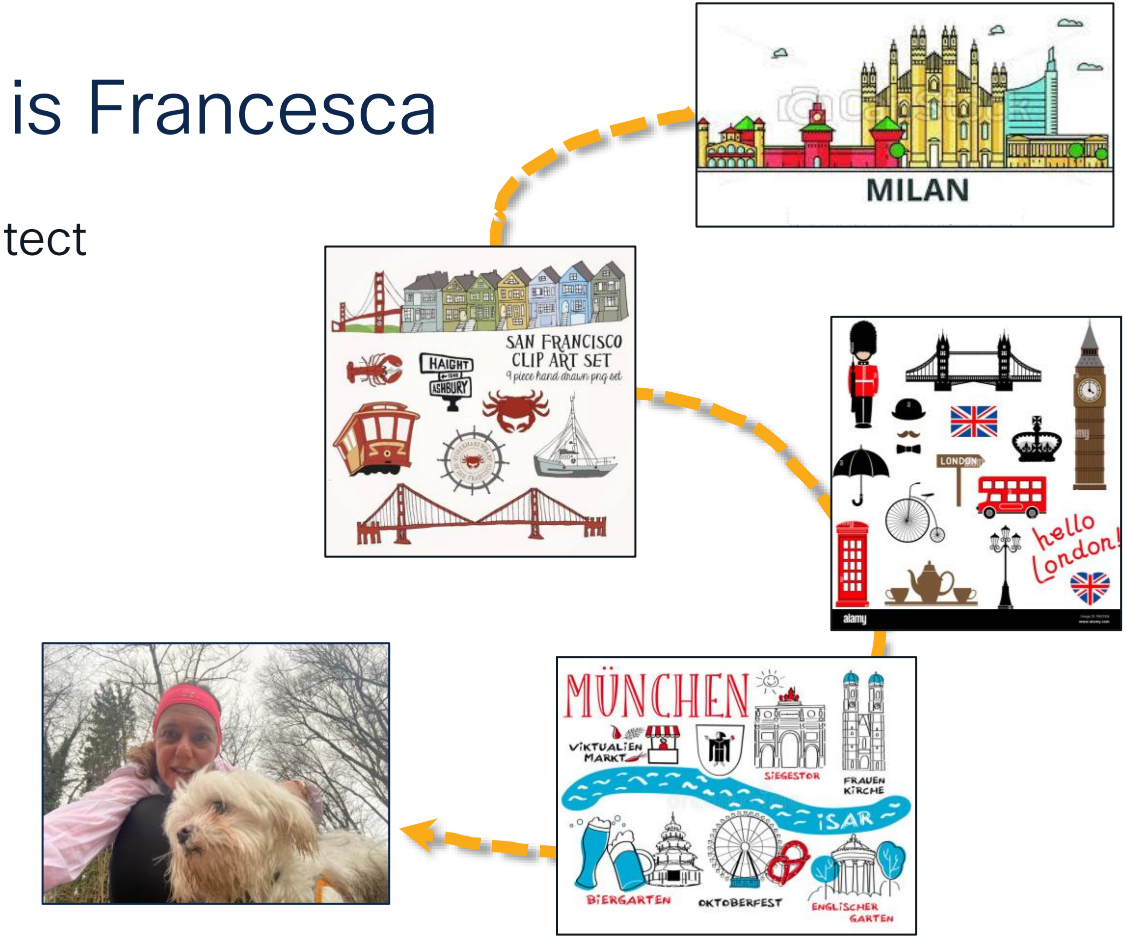
  Cyber Security EMEA

- In Cisco since 22 years...

  ... And 3 countries

Main interest on

- Policy and Access
- Segmentation
- Industrial Security



Who am I?

- Technical Marketing Engineer

  IoT Industrial Security

- At Cisco for 9 years
  - Spent over 8 years at Rockwell Automation

- Currently in MSISE Program at SANS
  - Focus on ICS Security

Security in Industrial is a big challenge

Systems are often very old

Most OT assets cannot be patched

Low visibility over endpoints

Network uptime and reliability

Lack of Segmentation

Standard IT security solutions and methodologies are not sufficient to fulfil OT cybersecurity requirements

What about Zero Trust ?

The Traditional Approach

Trust is based on the network location

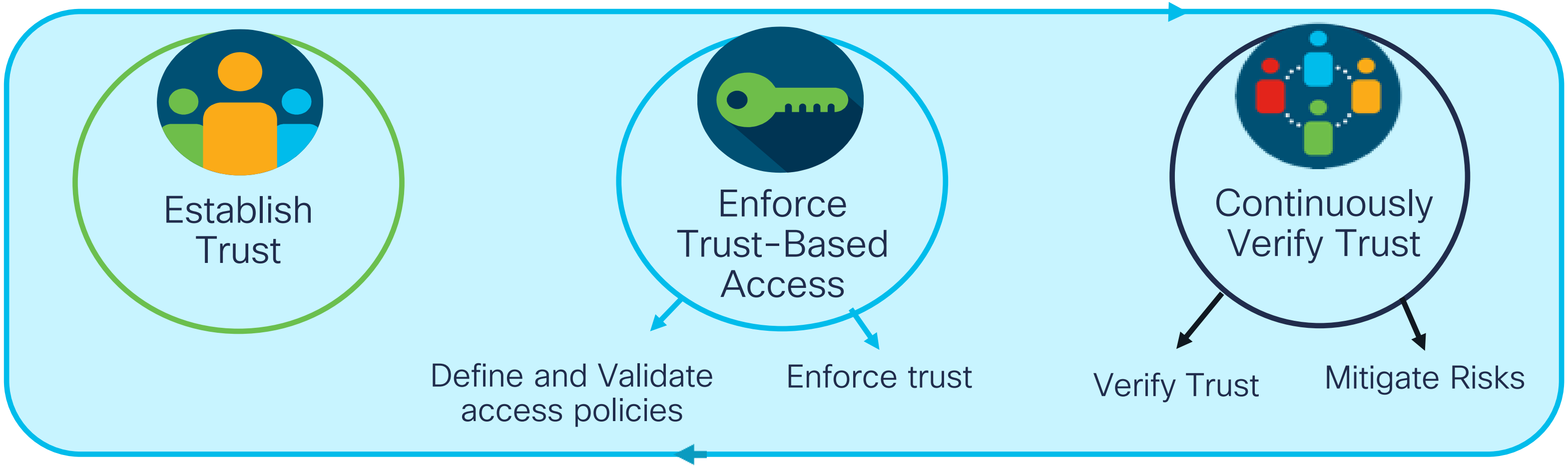
The Zero Trust Approach

Trust is established for every access request, regardless of where the request is coming from

Once attackers are in, they can move laterally within a network/cells/areas

Ensures only right users and devices have access, and only the right level of access

What are the steps for a Zero Trust network?



Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Define and Validate access policies

Enforce trust

Verify Trust

Mitigate Risks

Discover & classify devices.

When possible, check device posture and compliance

Network access control policies for users & devices.

Network segmentation.

Continuous monitoring & identifying indicators of compromise.

Capability to quarantine.

Agenda

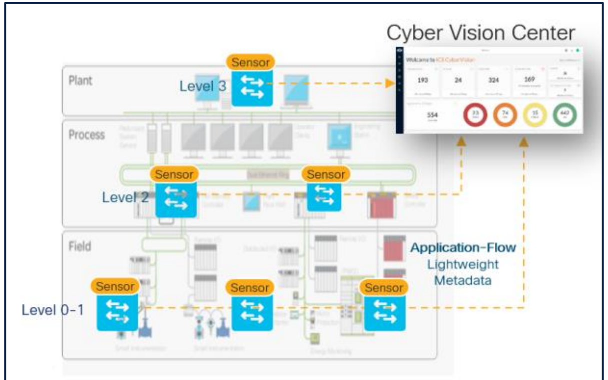
- Industrial Networks and Zero Trust Security ✓
- How to apply Zero Trust to protect your asset
  - Establishing Trust
  - Enforcing Trust Based Access
  - Continuous Trust Verification

Establish Trust

Dynamic visibility of all devices on the network

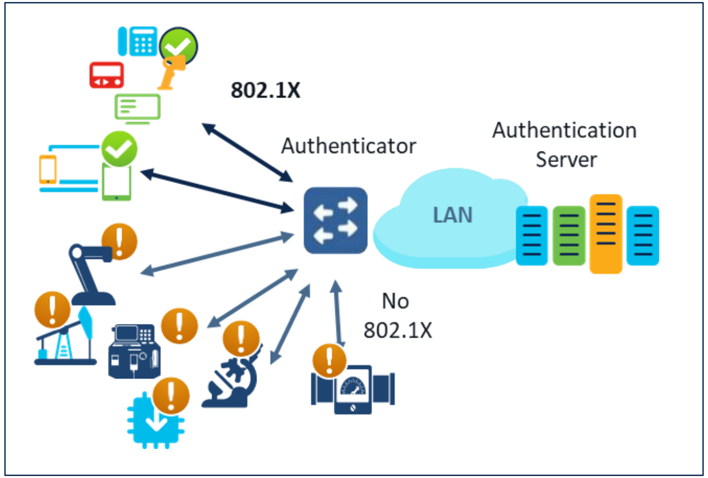
- Identification and trust of Industrial and non-industrial devices is needed
- **55%** customers have no or low confidence that they have proper visibility

Cisco Cyber Vision



Cyber Vision Sensors embedded
in your industrial network equipment

ISE



Cisco Cyber Vision

Security for the Industrial Control Systems

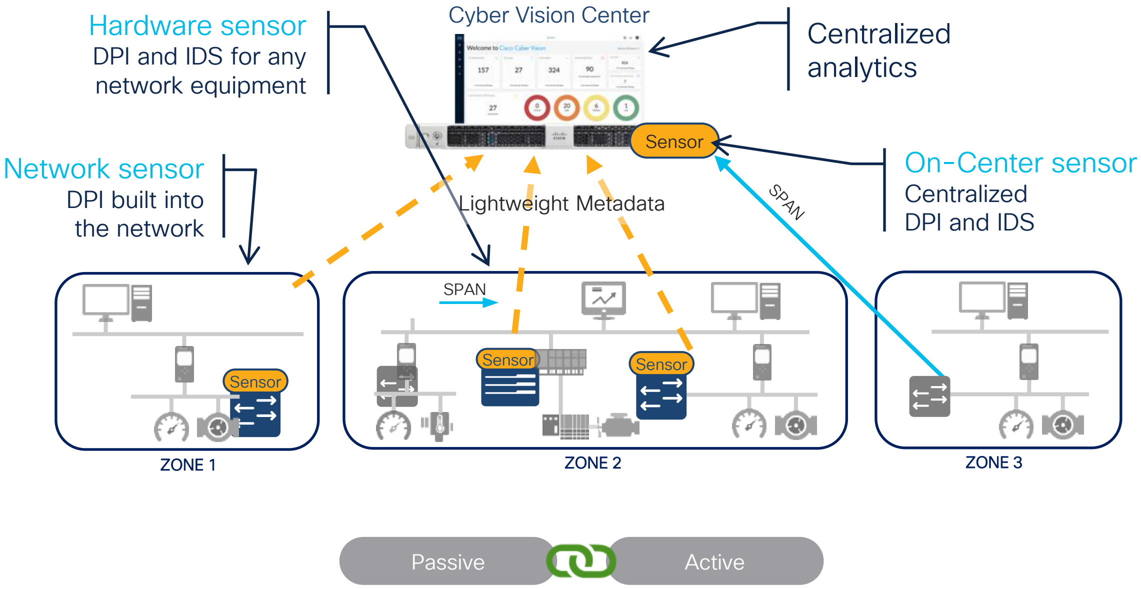
CyberVision:

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.

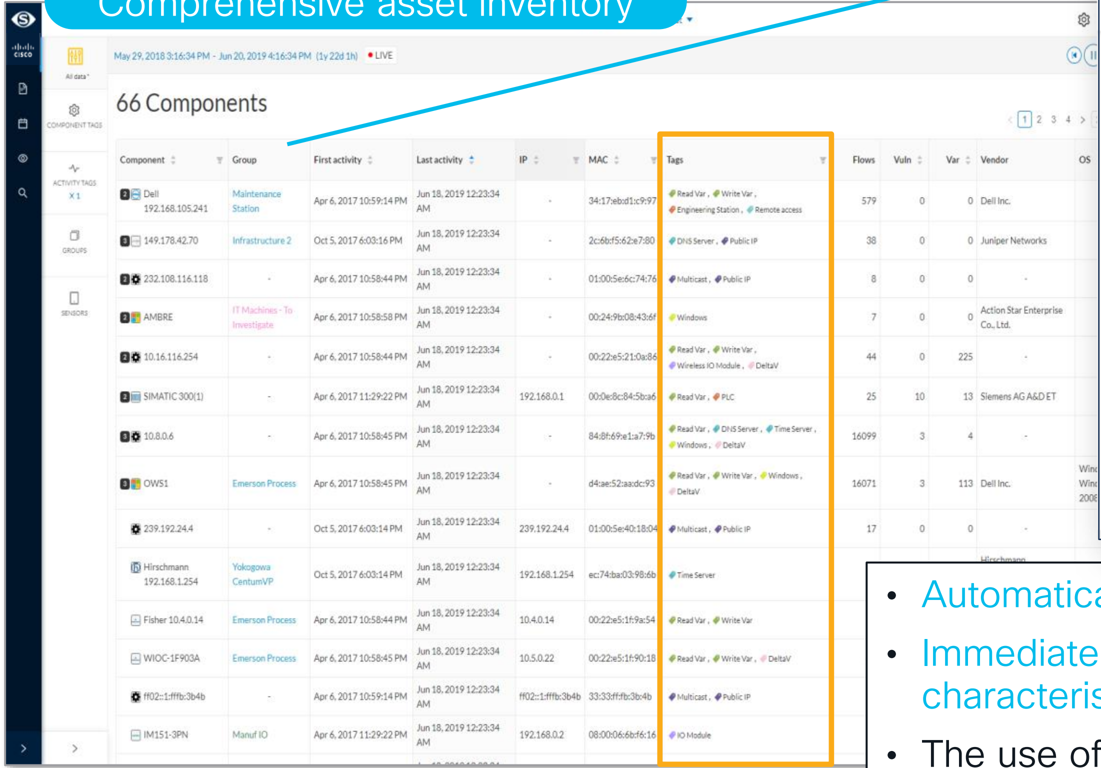
3. Operational insight: extracts process information from network flows to give OT staff visibility on industrial events.

4. Provides advanced anomaly detection, and real-time alerts for any threat to operational continuity and system integrity.



Industrial Endpoint Visibility

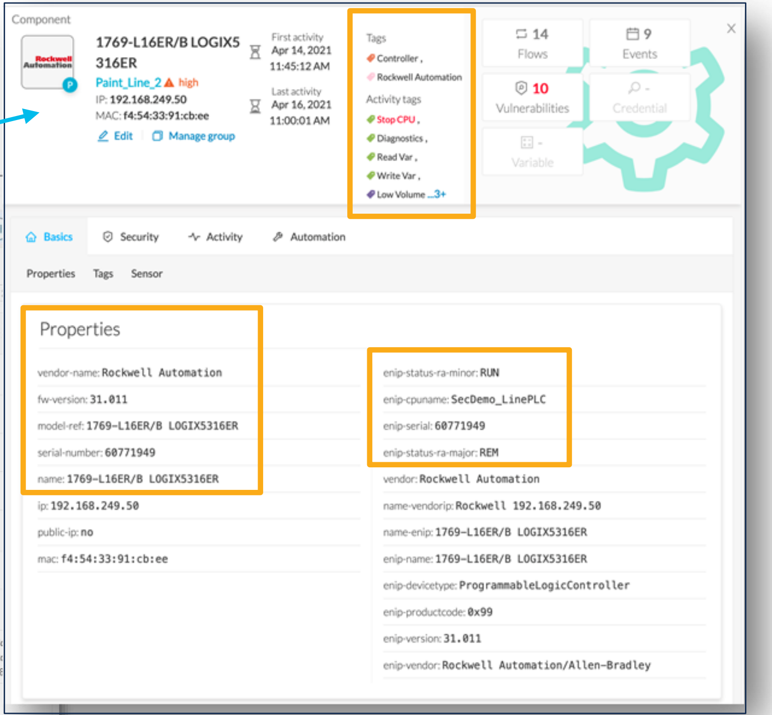
Comprehensive asset inventory



May 29, 2018 3:16:34 PM - Jun 20, 2019 4:16:34 PM (1y 22d 1h) ● LIVE

66 Components

Component	Group	First activity	Last activity	IP	MAC	Tags	Flows	Vuln	Var	Vendor	OS
2 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.	
3 149.178.42.70	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	
2 232.108.116.118	-	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	-	
2 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.	
2 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	-	
2 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	
3 10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	84:8f:69:e1:a7:9b	Read Var , DNS Server , Time Server , Windows , DeltaV	16099	3	4	-	
3 OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4:ae:52:aa:dc:93	Read Var , Write Var , Windows , DeltaV	16071	3	113	Dell Inc.	Winc Winc 2008
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	239.192.24.4	01:00:5e:40:18:04	Multicast , Public IP	17	0	0	-	
Hirschmann 192.168.1.254	Yokogowa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	192.168.1.254	ec:74:ba:03:98:6b	Time Server				Hirschmann	
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	10.4.0.14	00:22:e5:1f:9a:54	Read Var , Write Var					
WIOC-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	10.5.0.22	00:22:e5:1f:90:18	Read Var , Write Var , DeltaV					
ff02::1:fffb:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	ff02::1:fffb:3b4b	33:33:ff:fb:3b:4b	Multicast , Public IP					
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.2	08:00:06:6b:f6:16	IO Module					



Component

1769-L16ER/B LOGIX5 316ER

Paint_Line_2 ⚠ high

IP: 192.168.249.50

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

Edit | Manage group

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

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

Tags: Controller , Rockwell Automation

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

14 Flows

9 Events

10 Vulnerabilities

- Credential

- Variable

Properties

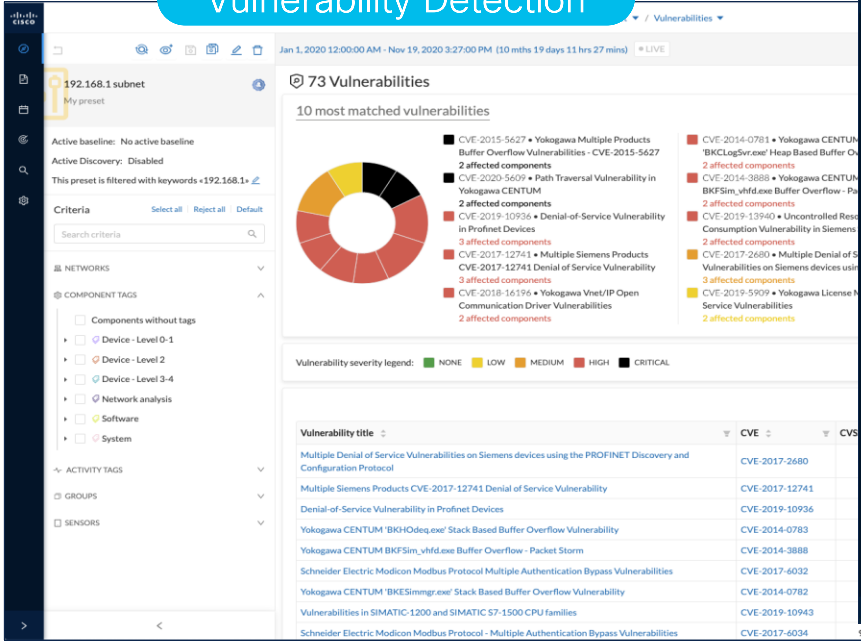
vendor-name: Rockwell Automation
fw-version: 31.011
model-ref: 1769-L16ER/B LOGIX5316ER
serial-number: 60771949
name: 1769-L16ER/B LOGIX5316ER
ip: 192.168.249.50
public-ip: no
mac: f4:54:33:91:cb:ee

enip-status-ra-minor: RUN
enip-cpuname: SecDemo_LinePLC
enip-serial: 60771949
enip-status-ra-major: REM
vendor: Rockwell Automation
name-vendorip: Rockwell 192.168.249.50
name-enip: 1769-L16ER/B LOGIX5316ER
enip-name: 1769-L16ER/B LOGIX5316ER
enip-devicetype: ProgrammableLogicController
enip-productcode: 0x99
enip-version: 31.011
enip-vendor: Rockwell Automation/Allen-Bradley

- Automatically crate a detailed list of all equipment
- Immediate access to software and hardware characteristics
- The use of tags make it easy to understand asset functions and properties

Industrial Endpoint compliance

Vulnerability Detection



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

192.168.1 subnet
My preset

Active baseline: No active baseline

Active Discovery: Disabled

This preset is filtered with keywords «192.168.1»

Criteria

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

73 Vulnerabilities

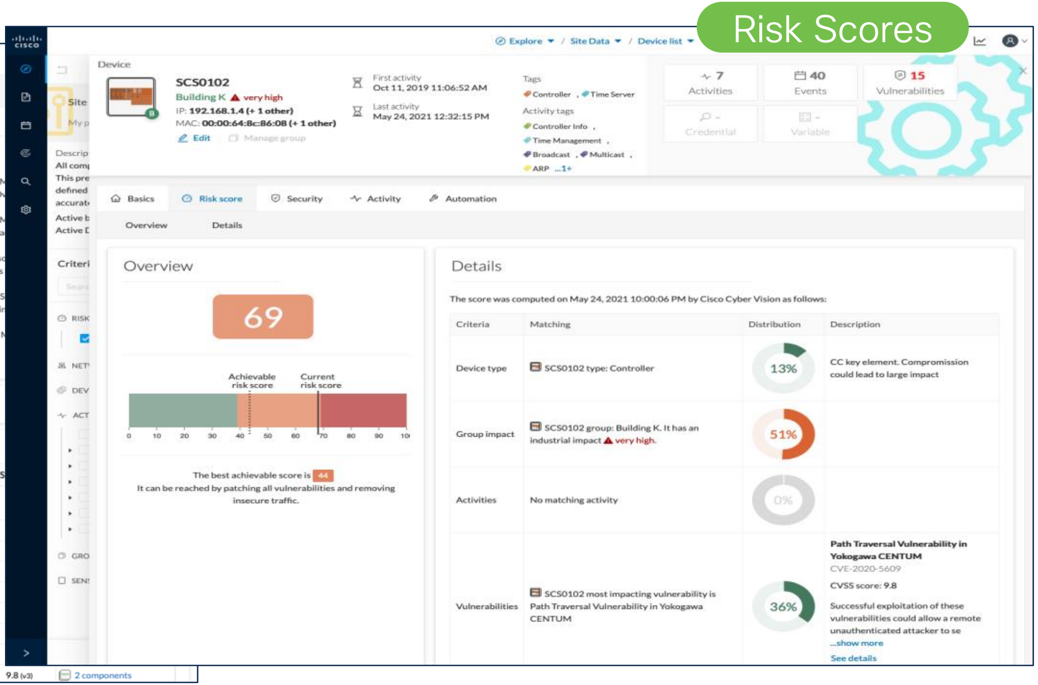
10 most matched vulnerabilities

- CVE-2015-5627 • Yokogawa Multiple Products Buffer Overflow Vulnerabilities - CVE-2015-5627 — 2 affected components
- CVE-2020-5609 • Path Traversal Vulnerability in Yokogawa CENTUM — 2 affected components
- CVE-2019-10936 • Denial-of-Service Vulnerability in Profinet Devices — 3 affected components
- CVE-2017-12741 • Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability — 3 affected components
- CVE-2018-16196 • Yokogawa Vnet/IP Open Communication Driver Vulnerabilities — 2 affected components
- CVE-2014-0781 • Yokogawa CENTUM 'BKCLogSvr.exe' Heap Based Buffer O — 2 affected components
- CVE-2014-3888 • Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Pa — 2 affected components
- CVE-2019-13940 • Uncontrolled Reso Consumption Vulnerability in Siemens — 2 affected components
- CVE-2017-2680 • Multiple Denial of S Vulnerabilities on Siemens devices usin — 3 affected components
- CVE-2019-5909 • Yokogawa License M Service Vulnerabilities — 2 affected components

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

Vulnerability title	CVE	CVS
Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and Configuration Protocol	CVE-2017-2680	
Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability	CVE-2017-12741	
Denial-of-Service Vulnerability in Profinet Devices	CVE-2019-10936	
Yokogawa CENTUM 'BKHOdeq.exe' Stack Based Buffer Overflow Vulnerability	CVE-2014-0783	
Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Packet Storm	CVE-2014-3888	
Schneider Electric Modicon Modbus Protocol Multiple Authentication Bypass Vulnerabilities	CVE-2017-6032	
Yokogawa CENTUM 'BKESimmgr.exe' Stack Based Buffer Overflow Vulnerability	CVE-2014-0782	
Vulnerabilities in SIMATIC-1200 and SIMATIC S7-1500 CPU families	CVE-2019-10943	
Schneider Electric Modicon Modbus Protocol - Multiple Authentication Bypass Vulnerabilities	CVE-2017-6034	9.8 (v3) 2 components

Risk Scores



Device

SCS0102
Building K ▲ very high
IP: 192.168.1.4 (+ 1 other)
MAC: 00:00:64:8c:86:08 (+ 1 other)

First activity Oct 11, 2019 11:06:52 AM

Last activity May 24, 2021 12:32:15 PM

Tags: Controller, Time Server

Activity tags: Controller Info, Time Management, Broadcast, Multicast, ARP ...1+

7 Activities · 40 Events · 15 Vulnerabilities · - Credential · - Variable

Overview

69

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

Details

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

Criteria	Matching	Distribution	Description
Device type	SCS0102 type: Controller	13%	CC key element. Compromission could lead to large impact
Group impact	SCS0102 group: Building K. It has an industrial impact ▲ very high.	51%	
Activities	No matching activity	0%	
Vulnerabilities	SCS0102 most impacting vulnerability is Path Traversal Vulnerability in Yokogawa CENTUM	36%	**Path Traversal Vulnerability in Yokogawa CENTUM** CVE-2020-5609 CVSS score: 9.8 Successful exploitation of these vulnerabilities could allow a remote unauthenticated attacker to se ...show more See details

Cyber Vision matches device attributes against the Talos CVE vulnerability database to easily identify vulnerable components

Risk Scores based on likelihood of impact:

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

ISE

How Identity Services Engine enforces Zero Trust

Connecting trusted users and endpoints with trusted resources

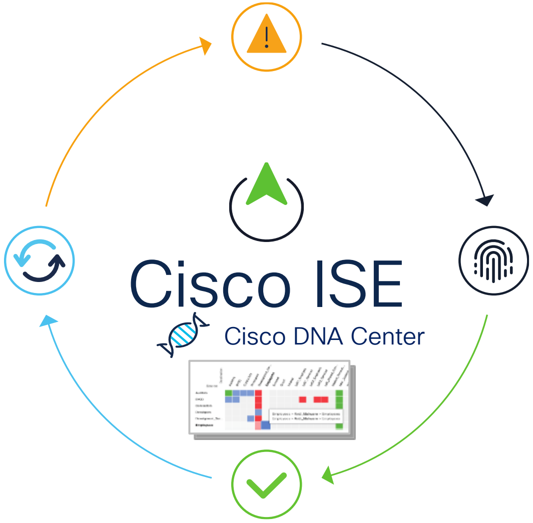
- Who
- What
- When
- How
- Where
- Posture
- Threat
- Vulnerability

Endpoint Request Access

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

Trust continually verified

- Continually monitors and verifies endpoint trust level
- Vulnerability assessments to identify indicators of compromise
- Automatically Updates access policy



Endpoint classified, and profiled into groups

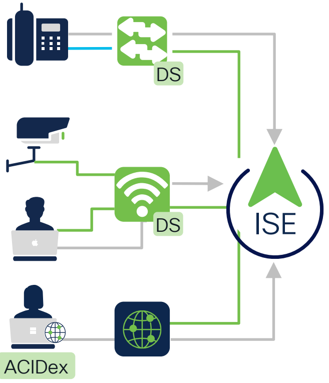
- Endpoints are tagged x/SGTs
- Policy applied to profiled groups based on least privilege

Endpoint authorized access based on least privilege

- Access granted
- Network segmentation achieved

Profiling devices dynamically

Endpoints send interesting data, that reveal their device type



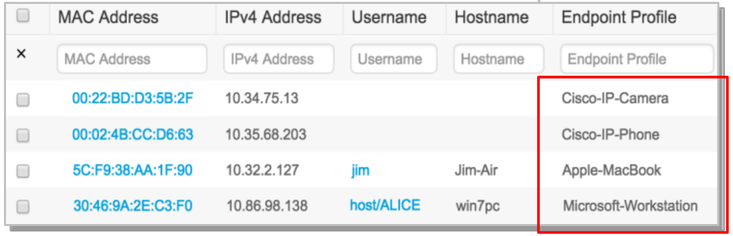
ISE Data Collection Methods for Device Profiling

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

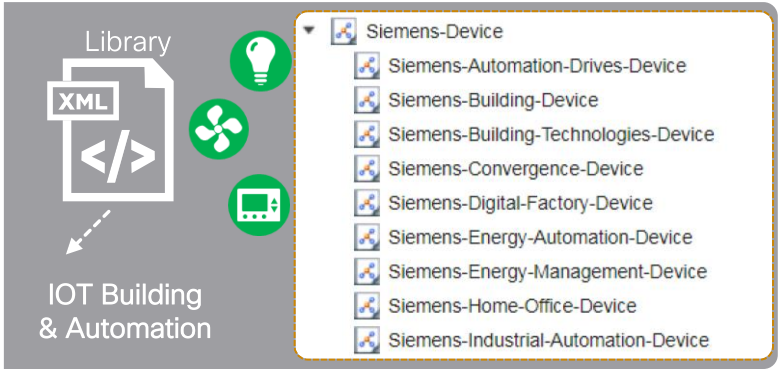
Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

AnyConnect: ACIDex

Feed Service (Online/Offline)



□	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



- Siemens-Device
  - Siemens-Automation-Drives-Device
  - Siemens-Building-Device
  - Siemens-Building-Technologies-Device
  - Siemens-Convergence-Device
  - Siemens-Digital-Factory-Device
  - Siemens-Energy-Automation-Device
  - Siemens-Energy-Management-Device
  - Siemens-Home-Office-Device
  - Siemens-Industrial-Automation-Device

AnyConnect Identity Extensions (ACIDex)
Device Sensor (DS)

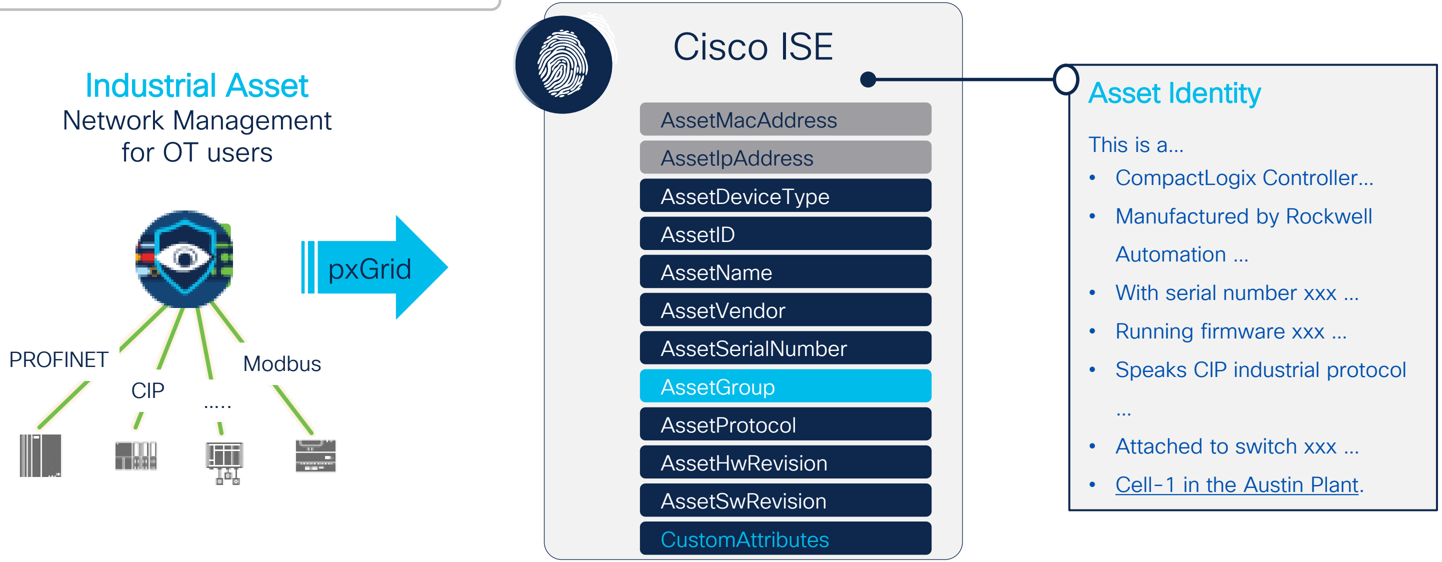
Enhancing profiling with CyberVision data

ISE Data Collection Methods for Device Profiling

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

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

AnyConnect: ACIDex



Industrial Asset

Network Management for OT users

Cisco ISE

- AssetMacAddress
- AssetIpAddress
- AssetDeviceType
- AssetID
- AssetName
- AssetVendor
- AssetSerialNumber
- AssetGroup
- AssetProtocol
- AssetHwRevision
- AssetSwRevision
- CustomAttributes

Asset Identity

This is a...

- CompactLogix Controller...
- Manufactured by Rockwell Automation ...
- With serial number xxx ...
- Running firmware xxx ...
- Speaks CIP industrial protocol ...
- Attached to switch xxx ...
- Cell-1 in the Austin Plant.

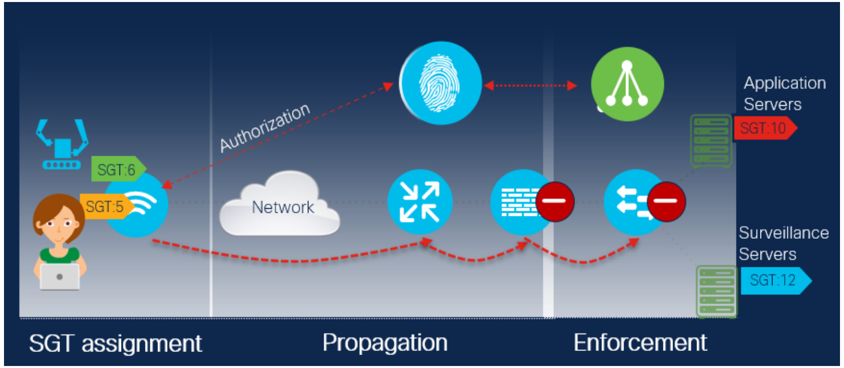
Enforce Trust via segmentation

Network Segmentation

ASA/FTD

- Segmentation
- Identity
- Application detection
- Application control
- IDS/IPS
- VPN access

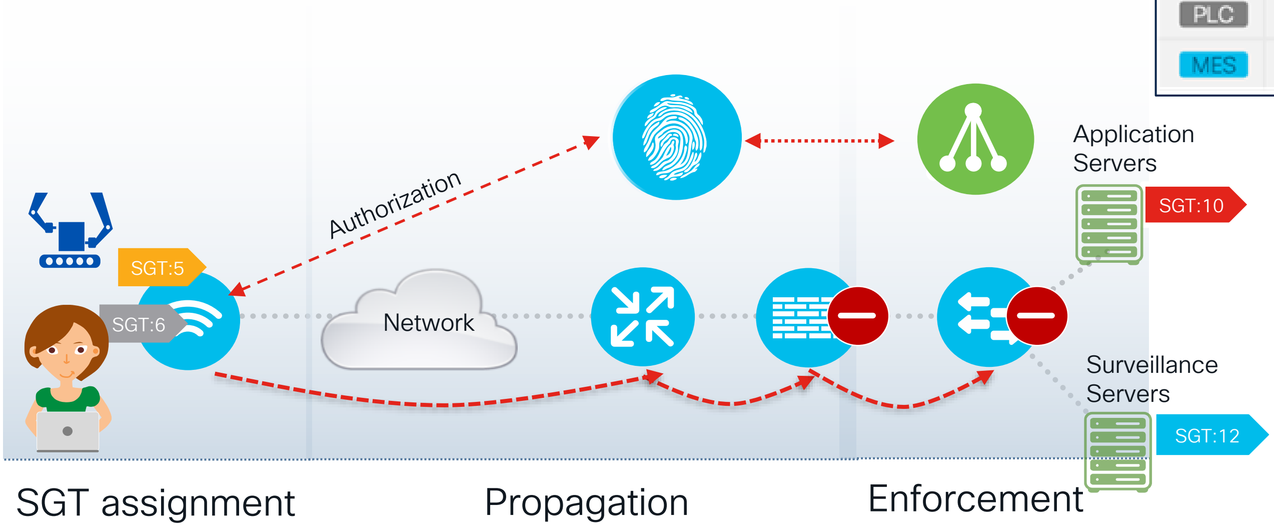
Segmentation with Firewall



Segmentation with Trustsec allows also for micro-segmentation

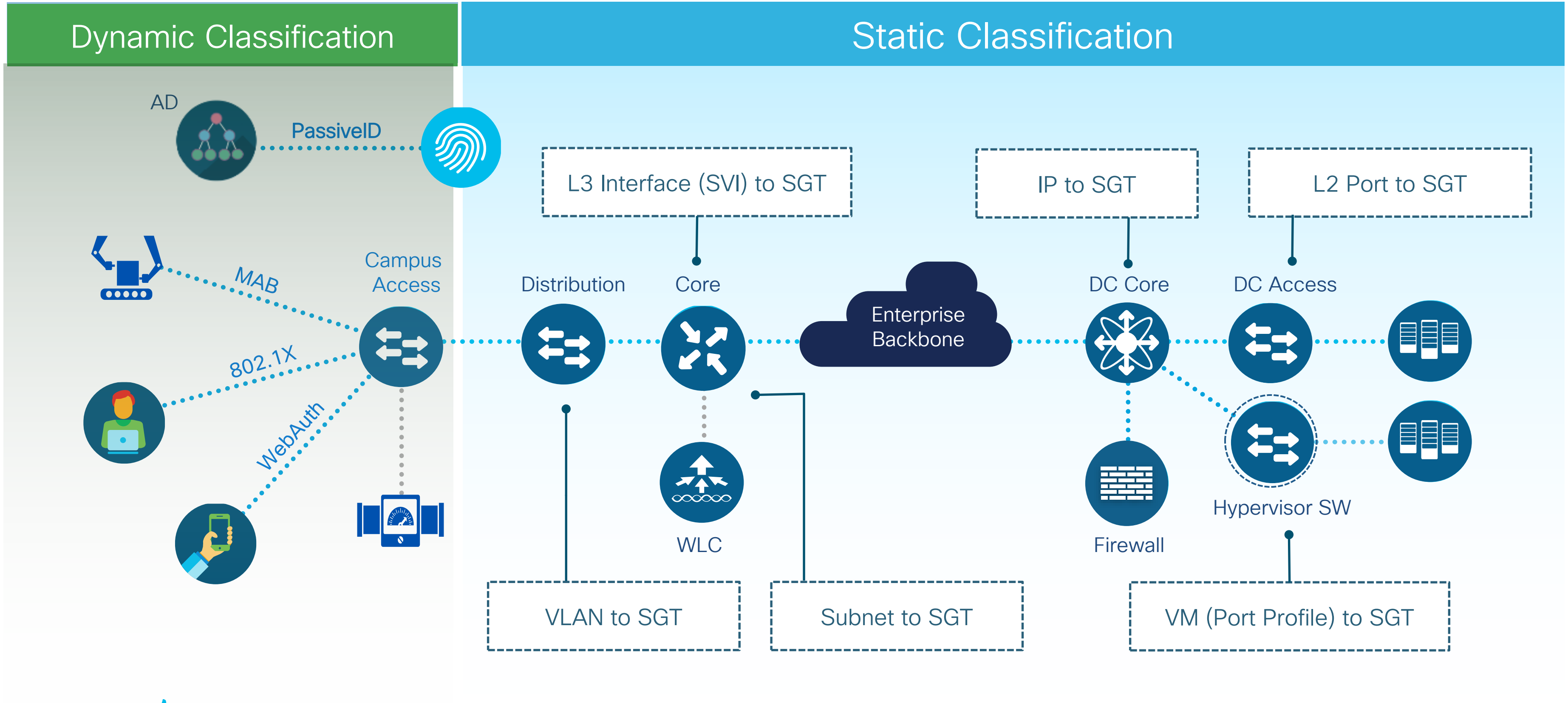
TrustSec concepts

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



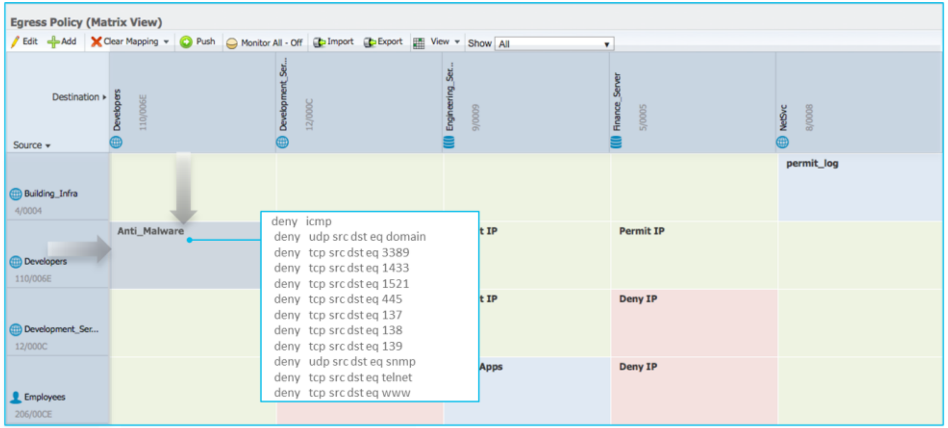
- Assignment of Security Group Tag (SGT) based on context (identity, device group, etc.).
- SGT are carried propagated through the network
- Firewalls, routers and switches use SGT to make filtering decisions via SGACL.

Classification Mechanisms



Enforcement options

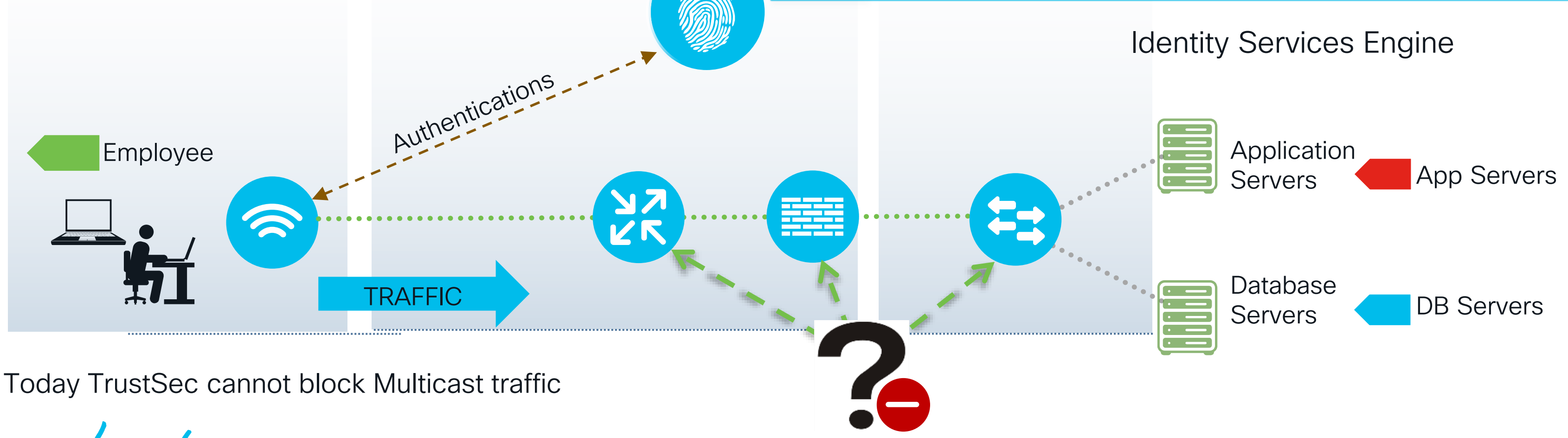
- Policies based on SGT and not on network dependent element like IP address
- SGACL include only protocol and port, while the source and destination are dynamically inserted



Egress Policy (Matrix View)

Source ▾ / Destination ▸	Developers 110/006E	Development_Ser... 12/000C	Engineering_Ser... 9/0009	Finance_Server 5/0005	NetSvc 8/0008
Building_Infra 4/0004					permit_log
Developers 110/006E	Anti_Malware		t IP	Permit IP	
Development_Ser... 12/000C			t IP	Deny IP	
Employees 206/00CE			Apps	Deny IP	

```
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
```



Today TrustSec cannot block Multicast traffic

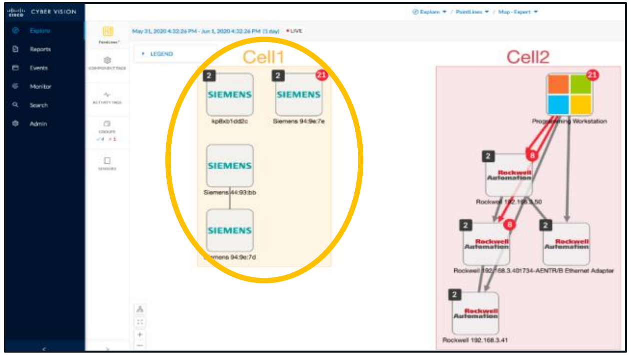
Dynamic segmentation via CyberVision fosters IT/OT collaboration

Step 2: Both teams create a policy matrix with all the needed use cases for segmentation

	Cell 1	Cell 2	PLC	MES	Remote Asset
Cell 1	✓	✗	✓	✗	✗
Cell 2	✗	✓	✓	✗	✗
PLC	✓	✓	✓	✓	✗
MES	✗	✗	✓	✓	✗
Remote User	✗	✗	✗	✗	✓

TrustSec policy Matrix

Step 3: The OT team can now independently assign devices to the right policies directly from Cybervision



Cybervision

Step 1: IT and OT team define the needed roles and create the SGT and associated CyberVision groups.

Cell 1 Cell 2 PLC MES Remote User

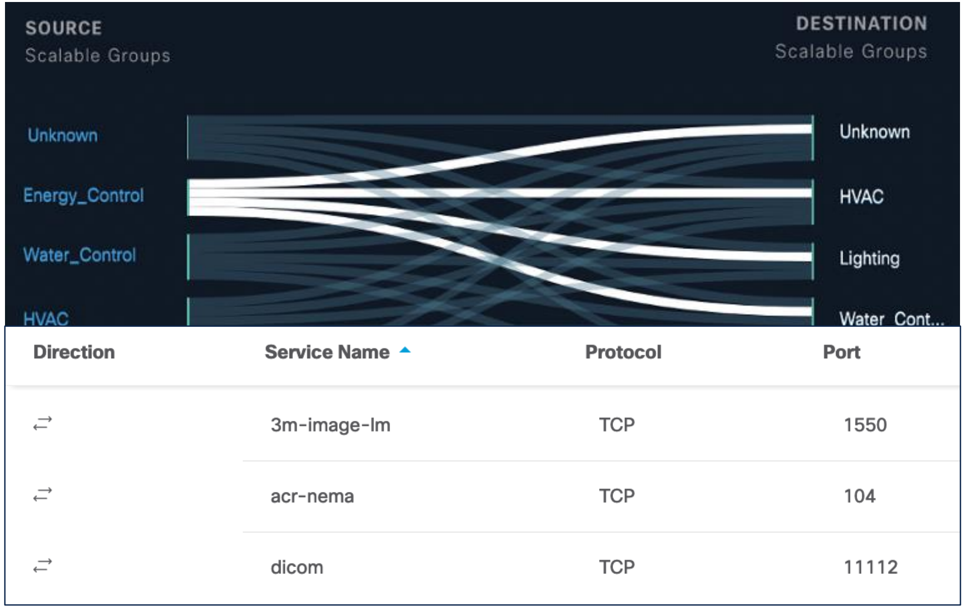
Step 4: The group name is sent to ISE via PxGrid and mapped to the associated SGT

Define and validate access policies

Communication visibility with Policy Analytics

Policy Analytics (An application on DNA Center)

- Policy Analytics ingests Netflow data from network devices and analyzes the flows seen inside the network
- When DNAC is used in the Enterprise network, it can be expanded into the Industrial area
- For each communication shows protocol and port seen



Direction	Service Name ▲	Protocol	Port
⇄	3m-image-lm	TCP	1550
⇄	acr-nema	TCP	104
⇄	dicom	TCP	11112

Visualize activity flows

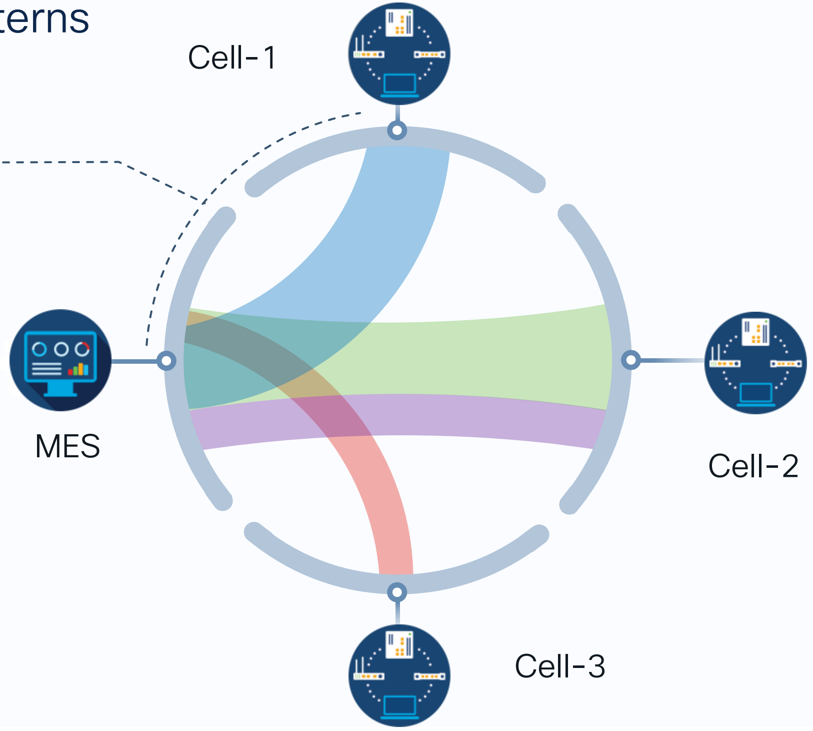
DNAC Policy Modeling – With traffic patterns

	MES	Cell-1	Cell-2
Cell-1	✓	✓	⛔

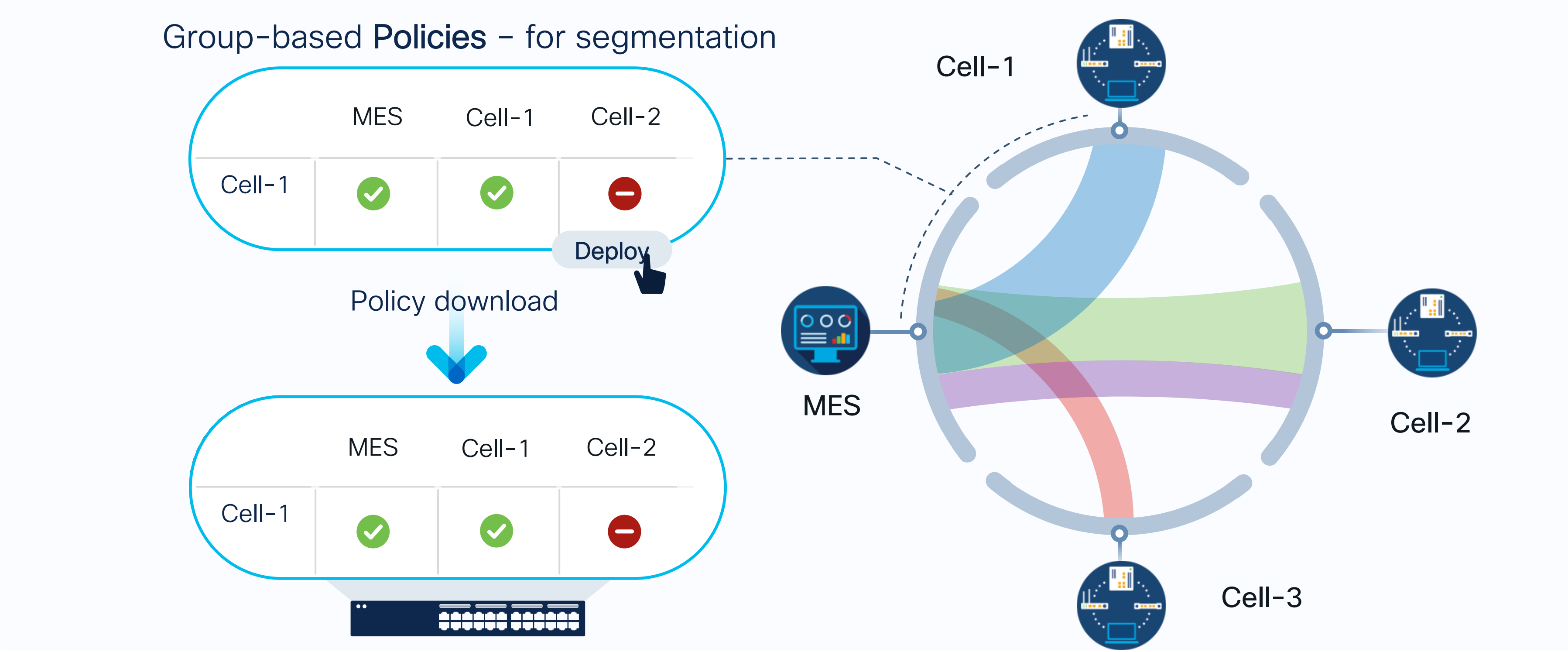
Unearth critical access that must be allowed / denied

Observe and fine-tune for days/weeks

No policy on the network, yet



Deploy segmentation policies with confidence



Group-based **Policies** – for segmentation

	MES	Cell-1	Cell-2
Cell-1	✓	✓	⛔

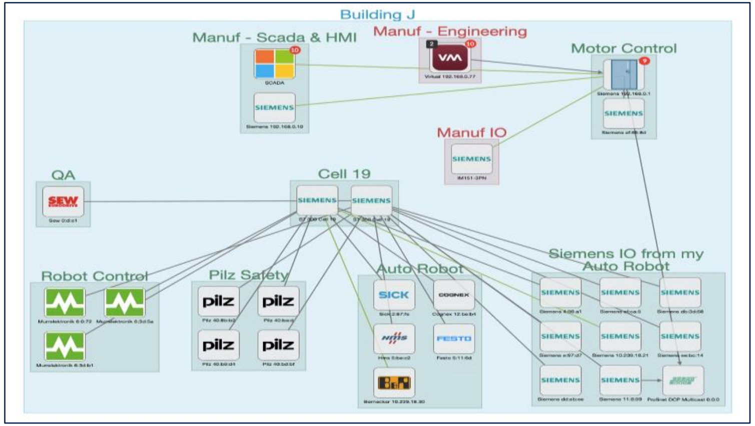
Deploy

Policy download

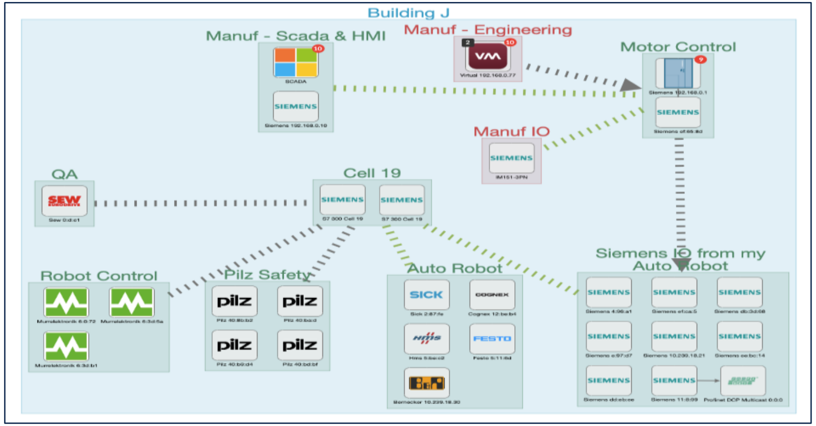
	MES	Cell-1	Cell-2
Cell-1	✓	✓	⛔

Communication visibility with CyberVision

Knowing the actual communication flows allows for better policy definition



Communication flows



Conduits

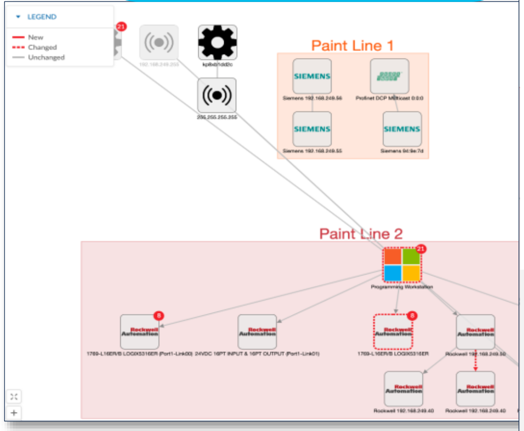
- Maps communication flows including application-level details
- OT team can group endpoints based on the industrial process they represent

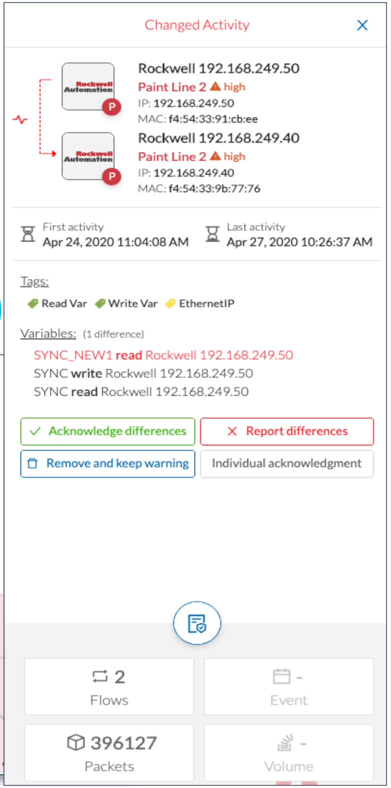
Contunuously verify Trust

Industrial Endpoint Anomaly & Intrusion Detection

Triggers automatic alerts on deviation from the baseline

Behavior Modeling based Anomaly Detection





Changed Activity ✕

Rockwell 192.168.249.50
Paint Line 2 ▲ high
IP: 192.168.249.50
MAC: f4:54:33:91:cb:ee

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

First activity
Apr 24, 2020 11:04:08 AM

Last activity
Apr 27, 2020 10:26:37 AM

Tags:
Read Var · Write Var · EthernetIP

Variables: (1 difference)

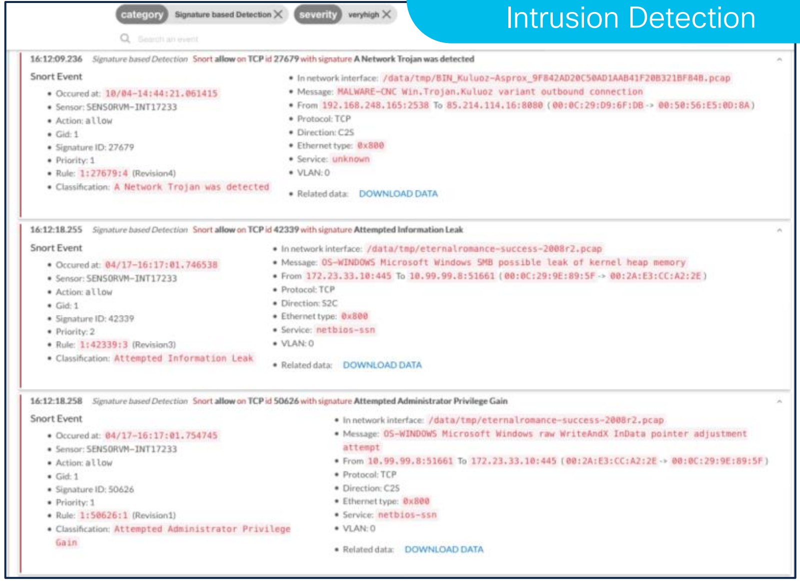
SYNC_NEW1 **read** Rockwell 192.168.249.50
SYNC **write** Rockwell 192.168.249.50
SYNC **read** Rockwell 192.168.249.50

✓ Acknowledge differences | ✕ Report differences
Remove and keep warning | Individual acknowledgment

2 Flows | - Event
396127 Packets | - Volume

Some sensor models have a built-in Snort engine which includes several industrial protocols processors
(Modbus, DNP3, CIP, IEC-60870-5-104, IEC 61850 – MMS, S7COM)

Snort Signature based Intrusion Detection



category Signature based Detection ✕ severity veryhigh ✕

Search an event

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

Snort Event

- Occured at: 10/04-14:44:21.061415
- Sensor: SENSORVM-INT17233
- Action: allow
- Gid: 1
- Signature ID: 27679
- Priority: 1
- Rule: 1:27679:4 (Revision4)
- Classification: A Network Trojan was detected
- In network interface: /data/tmp/BIN_Kuluoz-Asprox_9F842AD20C50AD1AAB41F20B321BF84B.pcap
- Message: MALWARE-CNC Win.Trojan.Kuluoz variant outbound connection
- From 192.168.248.165:2538 To 85.214.114.16:8080 (00:0C:29:D9:6F:DB -> 00:50:56:E5:0D:8A)
- Protocol: TCP
- Direction: C2S
- Ethernet type: 0x800
- Service: unknown
- VLAN: 0
- Related data: DOWNLOAD DATA

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

Snort Event

- Occured at: 04/17-16:17:01.746538
- Sensor: SENSORVM-INT17233
- Action: allow
- Gid: 1
- Signature ID: 42339
- Priority: 2
- Rule: 1:42339:3 (Revision3)
- Classification: Attempted Information Leak
- In network interface: /data/tmp/eternalromance-success-2008r2.pcap
- Message: OS-WINDOWS Microsoft Windows SMB possible leak of kernel heap memory
- From 172.23.33.10:445 To 10.99.99.8:51661 (00:0C:29:9E:89:5F -> 00:2A:E3:CC:A2:2E)
- Protocol: TCP
- Direction: S2C
- Ethernet type: 0x800
- Service: netbios-ssn
- VLAN: 0
- Related data: DOWNLOAD DATA

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

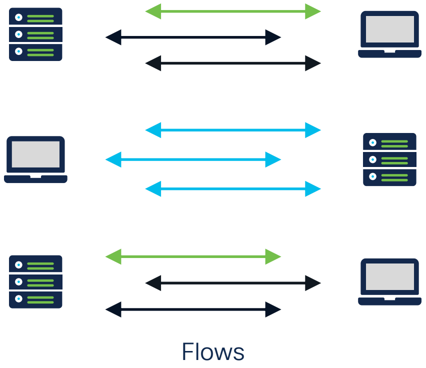
Snort Event

- Occured at: 04/17-16:17:01.754745
- Sensor: SENSORVM-INT17233
- Action: allow
- Gid: 1
- Signature ID: 50626
- Priority: 1
- Rule: 1:50626:1 (Revision1)
- Classification: Attempted Administrator Privilege Gain
- In network interface: /data/tmp/eternalromance-success-2008r2.pcap
- Message: OS-WINDOWS Microsoft Windows raw WriteAndX InData pointer adjustment attempt
- From 10.99.99.8:51661 To 172.23.33.10:445 (00:2A:E3:CC:A2:2E -> 00:0C:29:9E:89:5F)
- Protocol: TCP
- Direction: C2S
- Ethernet type: 0x800
- Service: netbios-ssn
- VLAN: 0
- Related data: DOWNLOAD DATA

Anomaly detection with Secure Network Analytics

Collect and analyze telemetry

Comprehensive data set optimized to remove redundancies



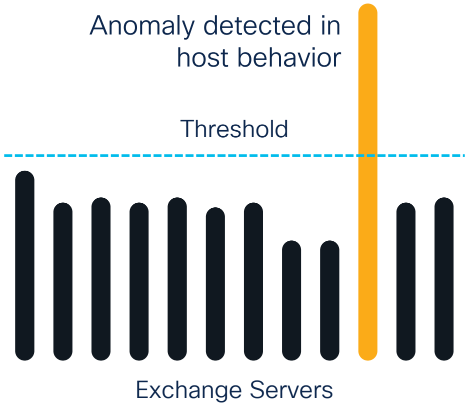
Create a baseline of normal behavior

Security events to detect anomalies and known bad behavior

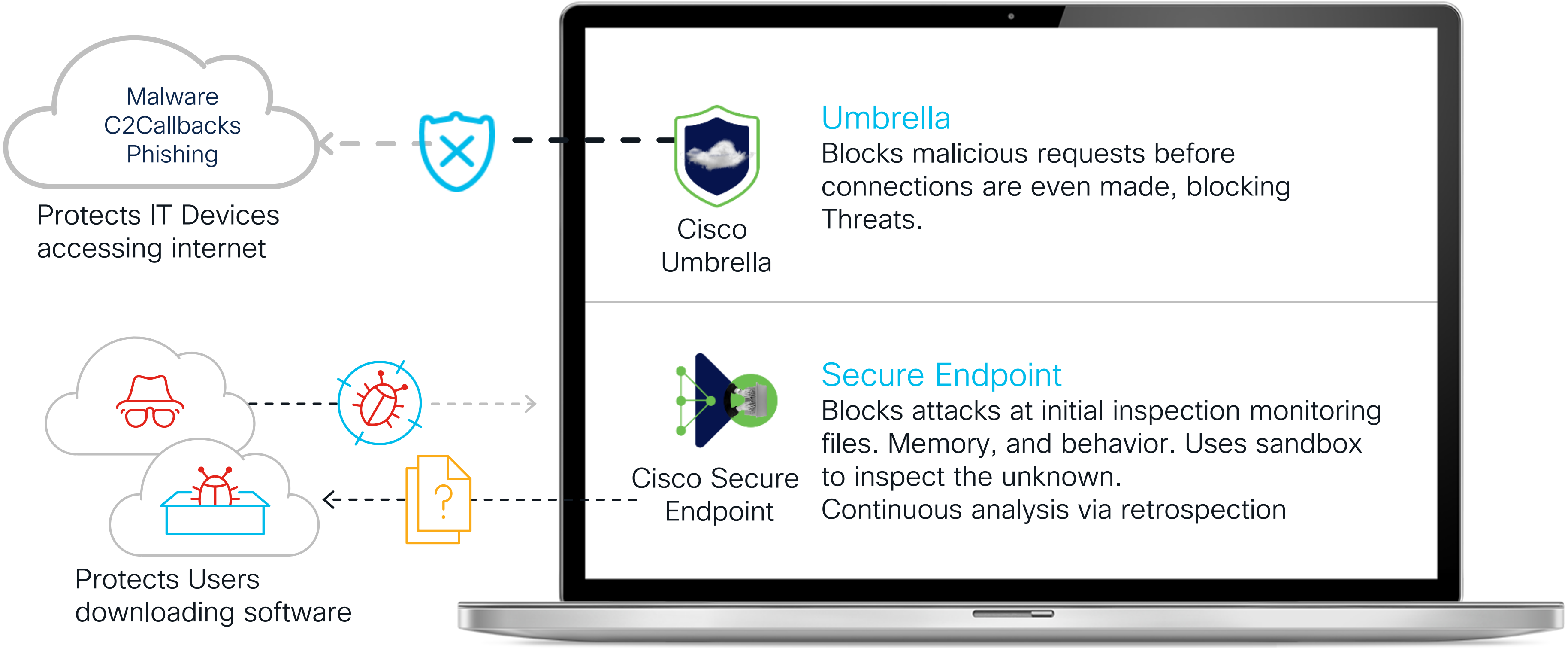
Security Observations		
Number of concurrent flows	New flows created	Number of SYNs received
Packet per second	Number of SYNs sent	Rate of connection resets
Bits per second	Time of day	Duration of the flow

Alarm on anomalies and behavioral changes

Alarm categories for high-risk, low-noise alerts for faster response



Threat Prevention and Control for Human devices



Malware
C2Callbacks
Phishing

Protects IT Devices accessing internet

Cisco Umbrella

Umbrella

Blocks malicious requests before connections are even made, blocking Threats.

Protects Users downloading software

Cisco Secure Endpoint

Secure Endpoint

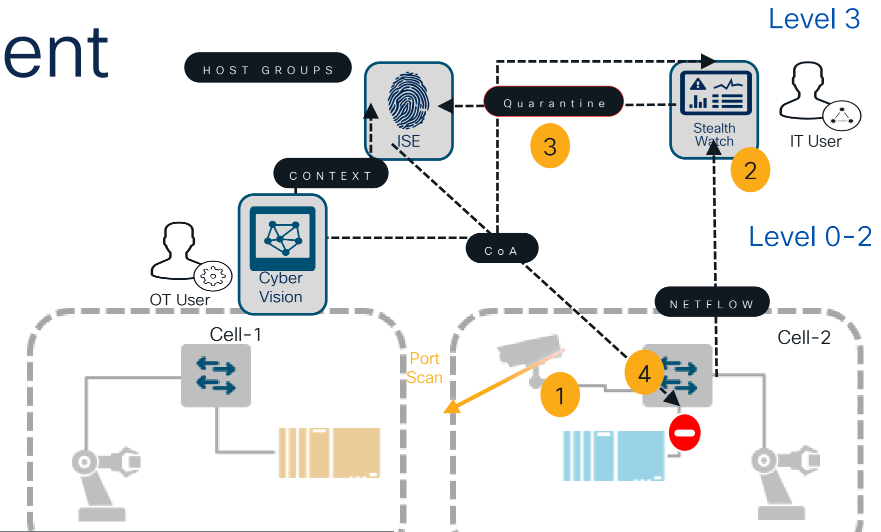
Blocks attacks at initial inspection monitoring files. Memory, and behavior. Uses sandbox to inspect the unknown.
Continuous analysis via retrospection

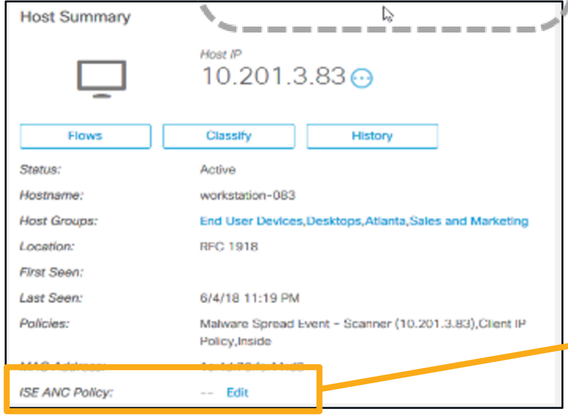
User endpoint

Mitigate risk

Rapid Threat Containment

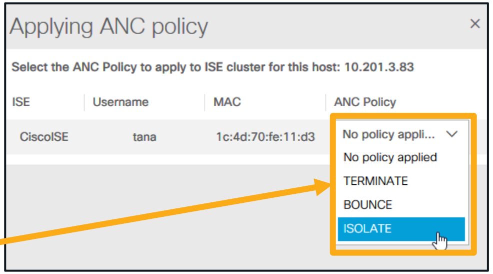
- Anomalous traffic behavior detected in communication between assets in trust zones
- Easily detect the source of anomaly & quarantine if necessary
- Quarantine can be non invasive (Change SGT or pass through an IDS)





Host IP
10.201.3.83

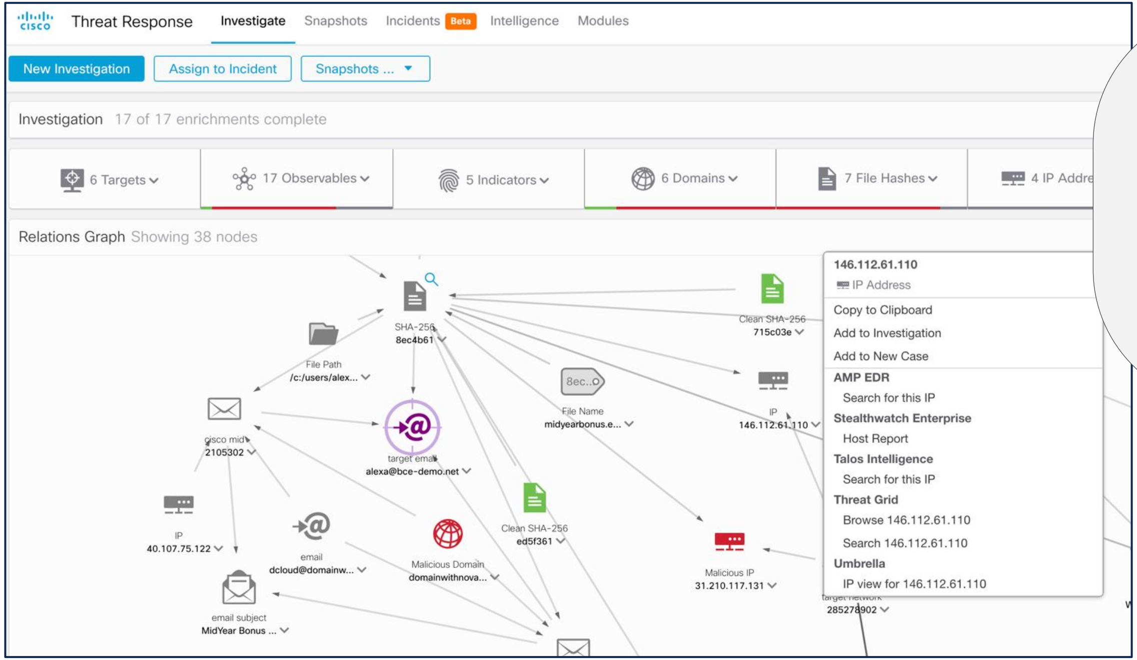
Status: Active
Hostname: workstation-083
Host Groups: End User Devices,Desktops,Atlanta,Sales and Marketing
Location: RFC 1918
First Seen:
Last Seen: 6/4/18 11:19 PM
Policies: Malware Spread Event - Scanner (10.201.3.83),Client IP Policy,Inside
MAC Address: 1c:4d:70:fe:11:d3
ISE ANC Policy: -- Edit



Select the ANC Policy to apply to ISE cluster for this host: 10.201.3.83

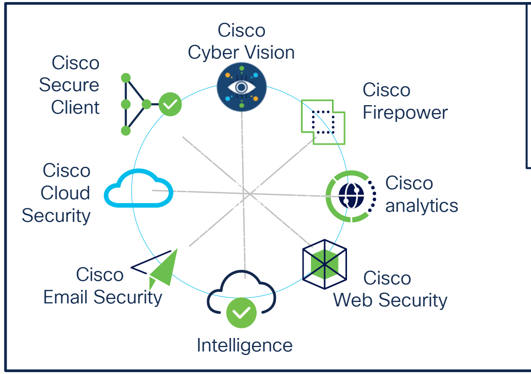
ISE	Username	MAC	ANC Policy
CiscoISE	tana	1c:4d:70:fe:11:d3	No policy appli...

SecureX accelerates investigations



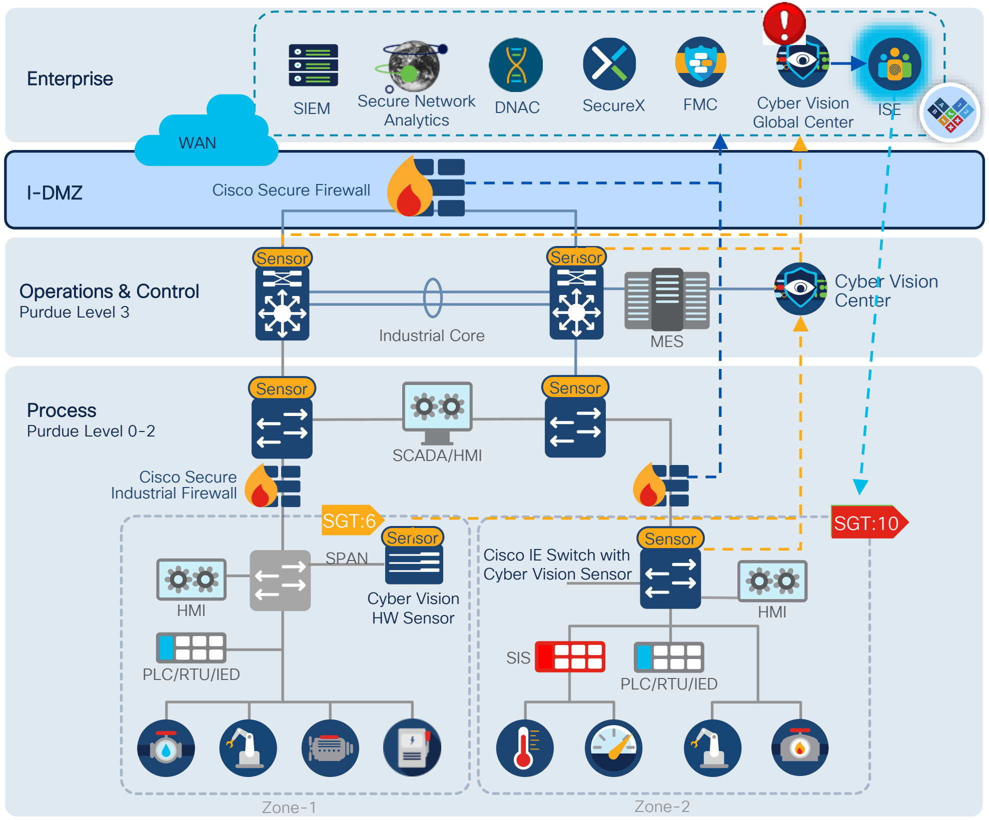
- Aggregate and query global intel and local context in one view
- Visualize the impact of treats across your environment
- Take immediate action to isolate hosts, block destinations or files
- Automate workflows

Observables: 1) File hash, 2) IP address, 3) Domains, 4) URLs, etc



Any 3rd party tool capable of interacting via API

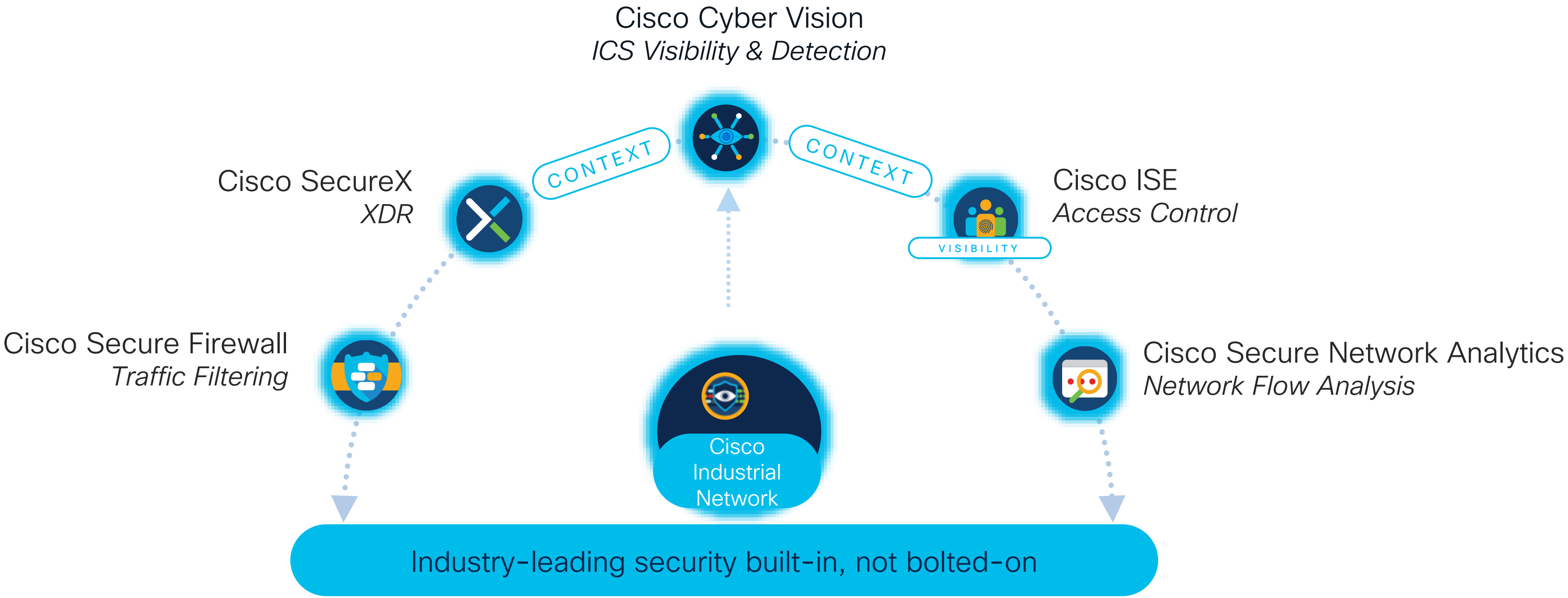
Let’s put everything together



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. Visualize traffic activity between SGT in DNAC policy analytics
5. Deploy segmentation with confidence once you are comfortable with the observed network behavior
6. CyberVision, Secure Network Analytics or other analytics tools raise alarms endpoint behavior anomalies and threat detection.
7. Investigate in SecureX and SOC tools
8. Users can trigger quarantine of offending asset.

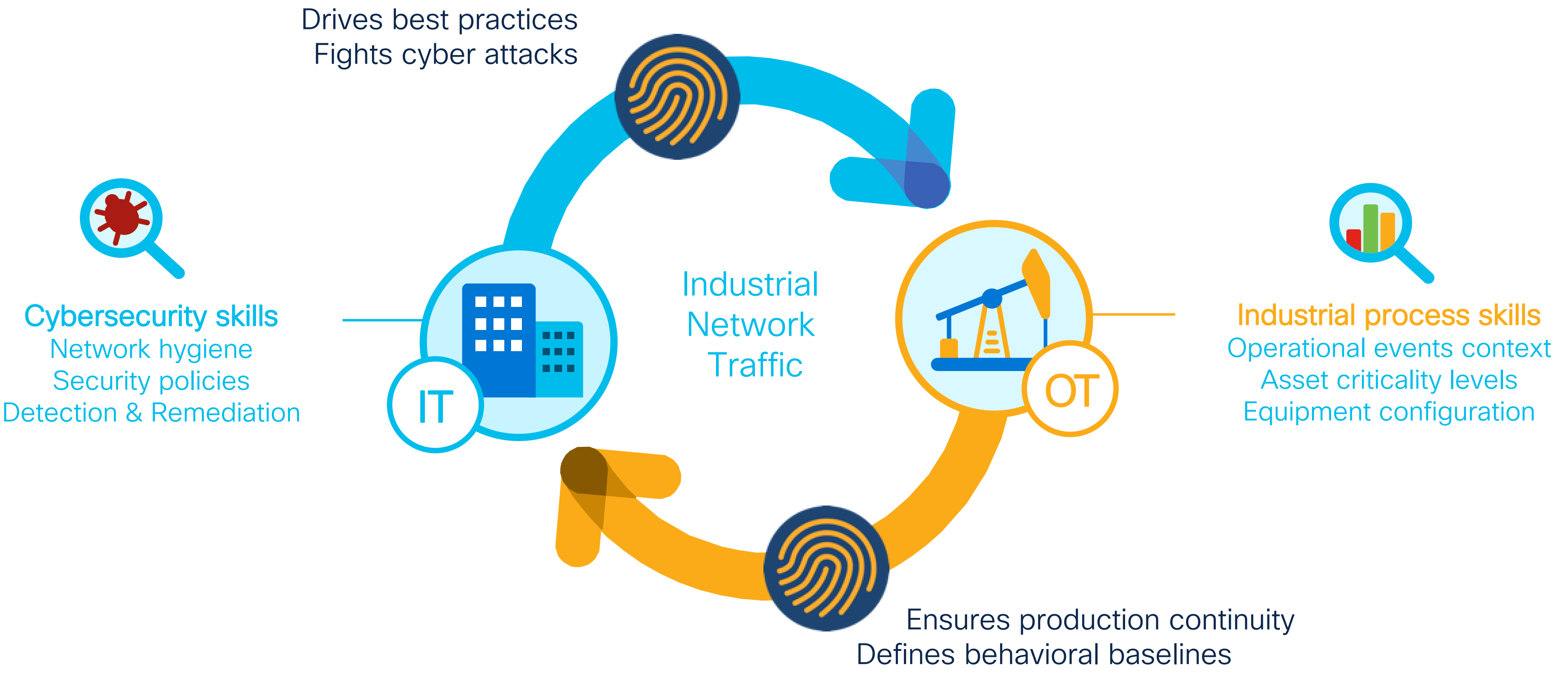
Conclusion

A Fully Integrated OT Security Solution



Working together to define & apply IoT security policies

IT-OT collaboration is vital for securing ICS



Drives best practices
Fights cyber attacks

Cybersecurity skills
Network hygiene
Security policies
Detection & Remediation

Industrial process skills
Operational events context
Asset criticality levels
Equipment configuration

Ensures production continuity
Defines behavioral baselines

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Live 2022 FOR REFERENCE BRKSEC-2077

Reference Sessions

- BRKIOT-2012 Industrial Zero Trust: Opportunities and Realities -
- BRKIOT-2353 Leveraging Visibility to drive Zero Trust for Industrial Security
- LABIOT-2357 Securing Industrial Networks

- BRKSEC-2480: Threat Centric Network Security
- BRKSEC-2053: Zero Trust: Securing the Evolving Workplace
- BRKSEC-2347: ISE Deployment Staging and Planning
- BRKSEC-1483: SecureX All The Things (With Hosted and Remote Relays)
- BRKSEC-2053: Zero Trust: Securing the Evolving Workplace
- BRKSEC-1014: Cisco Security Air-Gapped deployments best practices
- LTRSEC-2045: Zero Trust Workshop

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

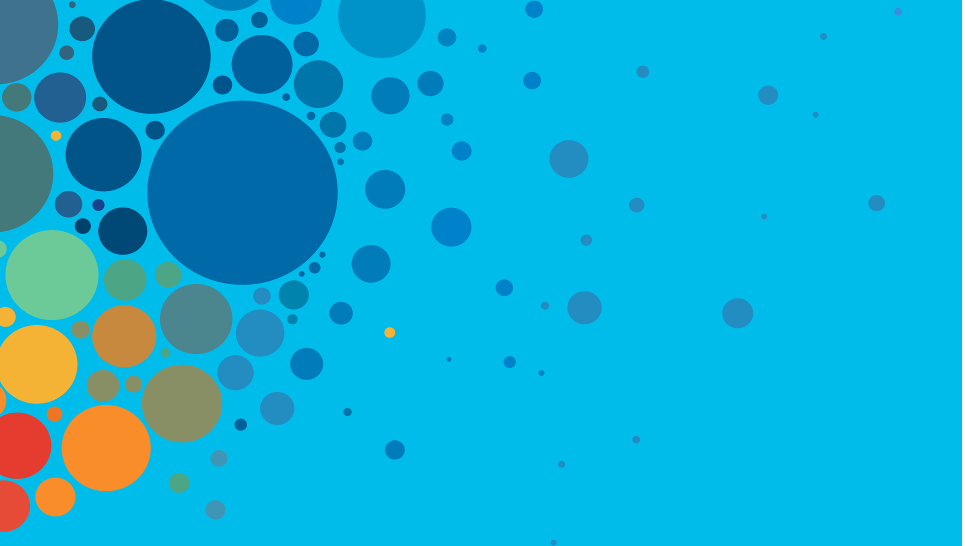
Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



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 www.CiscoLive.com/on-demand

The bridge to possible

Thank you

cisco Live!

#CiscoLive