



The bridge to possible

Gaining visibility into OT with Cyber Vision to secure your industrial networks

Ruben Lobo
Director, Product Management
PSOIOT-1007



#CiscoLive

Cisco Webex App

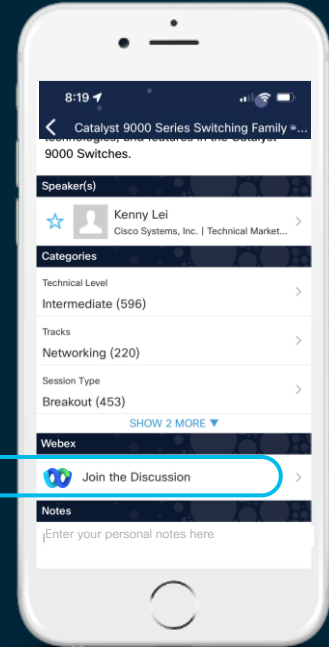
Questions?

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.



<https://ciscolive.ciscoevents.com/ciscolivebot/#PSOIoT-1007>

Agenda

- The need for visibility
- Introduction to Cyber Vision
- Getting started with visibility
- Improving your Security Posture
- Leveraging visibility to drive segmentation
- Conclusion



It's no secret that most industrial networks have poor network hygiene and inadequate security controls

Industry digitization brings new requirements and challenges



- More automation devices
- New IoT devices
- Secure cloud connectivity
- Remote access/hybrid work
- New regulatory

The role of IT is critical to help OT secure industrial operations



Securing OT is a multi-step process that **starts with OT Visibility**



Identify every OT
assets and their
communications



Detect bypass
or leaks in the
IDMZ



Spot asset
vulnerabilities to
patch or protect



Build action
plan and set
priorities



Segment
networks with
access policies

Cisco Named a Leader in ICS Security



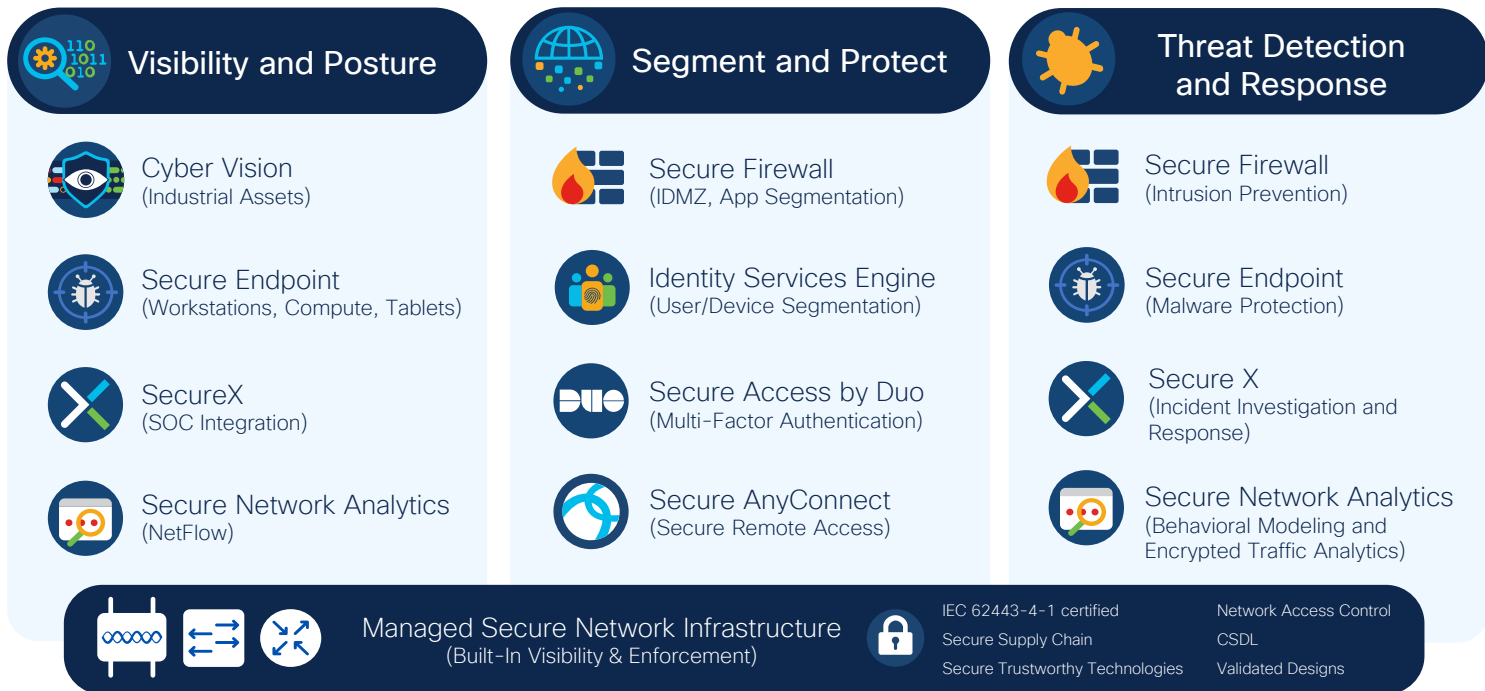
“While ICS/OT security requires unique strategies, buyers need a holistic security picture across the enterprise.”



“Its comprehensive range of products enables Cisco to provide ‘Full Spectrum Security’, including asset visibility, threat detection and micro segmentation.”

Cisco Industrial Security Framework

Powered by Talos Threat Intelligence



Introduction to Cyber Vision



Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT

Context & insights foundational to building reliable and secure OT networks



Visibility

Asset inventory
Communication patterns



Security Posture

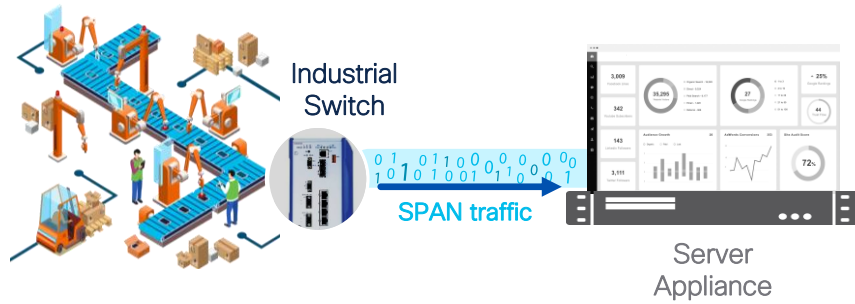
Device vulnerabilities
Risk scoring



Operational Insights

Track process/device modifications
Record control system events

Security Starts with Visibility But Beware of Hidden Costs!



Typical industrial Visibility and Detection solutions require SPAN (traffic mirroring)



Additional switches
for SPAN collection



Expensive cabling
for collection network



**Exponential
increase in traffic**
due to SPAN

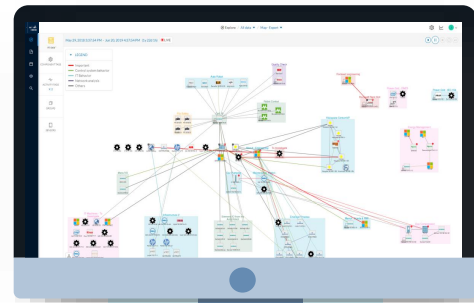
TCO of SPAN based solutions is **not** sustainable over long-term growth

Enlist your OT network for security



Cisco Industrial switches and gateways
see everything that attaches to them so
you can gain **visibility at scale**

Cyber Vision Center



1 0 0 1
0 0 1
Application Flow
Metadata

Cyber Vision Sensor



Deep Packet Inspection & Active Discovery
built into your network infrastructure

Cyber Vision Network Sensors

Deep Packet Inspection built into
network-elements eliminating the
need for SPAN

** IR8300 & C9300 support the optional add-on Snort IDS*

CISCO *Live!*

Industrial Din-Rail / IR67 Switches



IE3400



IE3300-10G



IE3400H

Industrial Gateways & Routers



IR1101



IR8300

Industrial & Enterprise Rackmount Switches

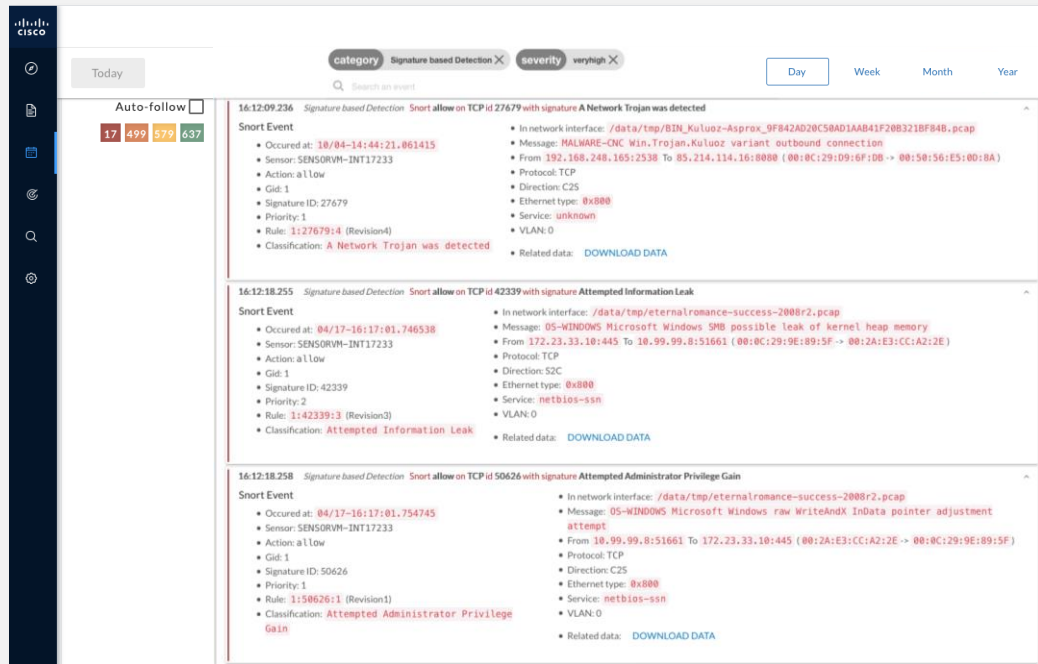


IE9300 (Q3FY23)



C9300

Snort Intrusion Detection Add-On



The screenshot displays the Cisco Security Center interface with the 'Snort' category selected. It shows three intrusion detection events:

- Event 1 (16:12:09.236):** Signature-based Detection. Snort allow on TCP id 27679 with signature A Network Trojan was detected. Details include: Occurred at: 18/04-14:44:21.061415, Sensor: SENSORVM-INT17233, Action: allow, Gid: 1, Signature ID: 27679, Priority: 1, Rule: 1:27679:4 (Revision4), Classification: A Network Trojan was detected. Related data: DOWNLOAD DATA.
- Event 2 (16:12:18.255):** Signature-based Detection. Snort allow on TCP id 42339 with signature Attempted Information Leak. Details include: Occurred 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. Related data: DOWNLOAD DATA.
- Event 3 (16:12:18.258):** Signature-based Detection. Snort allow on TCP id 50626 with signature Attempted Administrator Privilege Gain. Details include: Occurred 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. Related data: DOWNLOAD DATA.



Cyber Vision Center



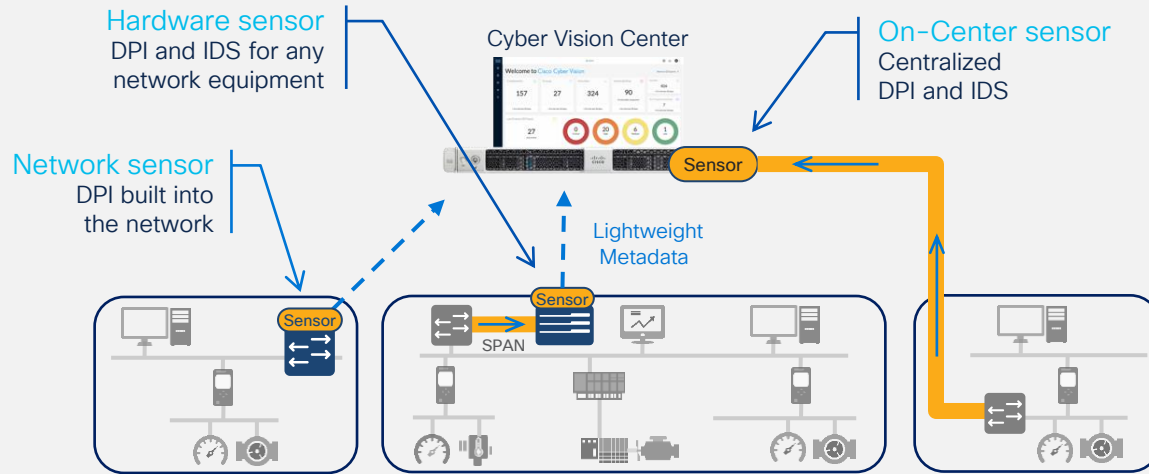
Catalyst 9300
Enterprise Switch



Catalyst IR8300 Series
Rugged Router

Detect malicious intrusions with Snort IDS and Talos threat intelligence

Cyber Vision offers flexible deployment options



Network-sensors embedded in Cisco networking for simple and highly scalable deployments

Hardware-sensors capturing traffic on any switch with a single hop SPAN

On-Center sensor to leverage existing SPAN infrastructures, or collect traffic within the datacenter

SPAN option and Hardware sensors to support brownfield

Network embedded sensors as you evolve and grow your operations

Getting started with visibility

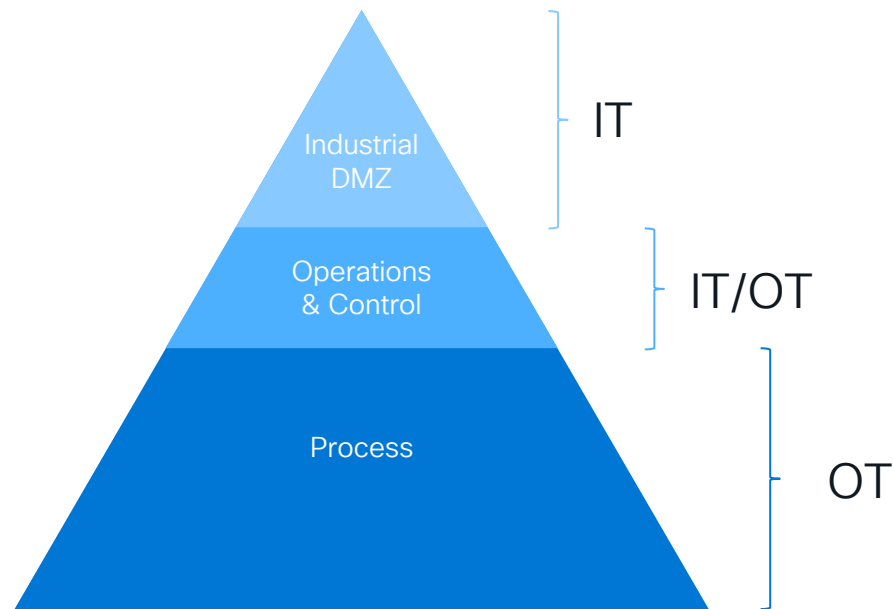


A photograph of an industrial manufacturing environment. In the foreground, two large orange robotic arms are visible, one on the left and one on the right, both equipped with various sensors and cables. They are positioned around a large, white, curved metal component, likely a car part, which is being assembled or inspected. The background shows a complex network of metal structures, pipes, and other industrial equipment, all under bright overhead lighting. A dark blue circular overlay is present in the top left corner, containing white text.

The role of IT is
expanding to help
manage & secure
the industrial
network

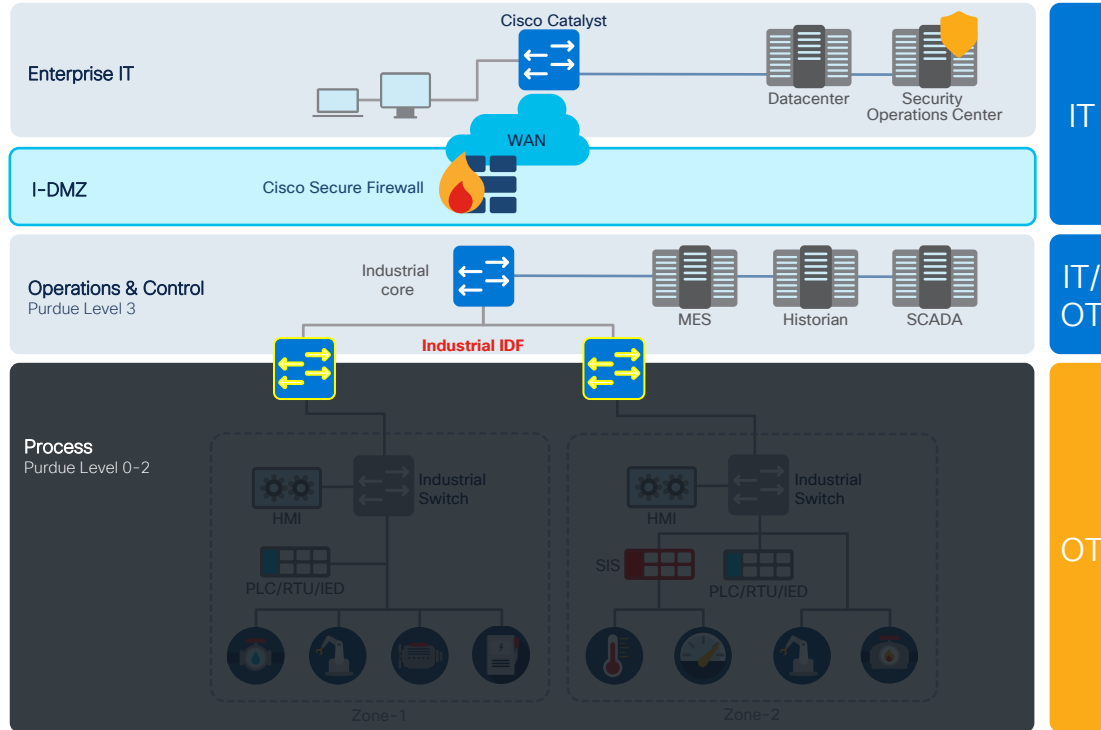
IT's pain point: Starting trouble due to lack of visibility into industrial control networks and devices

Typical domains of control



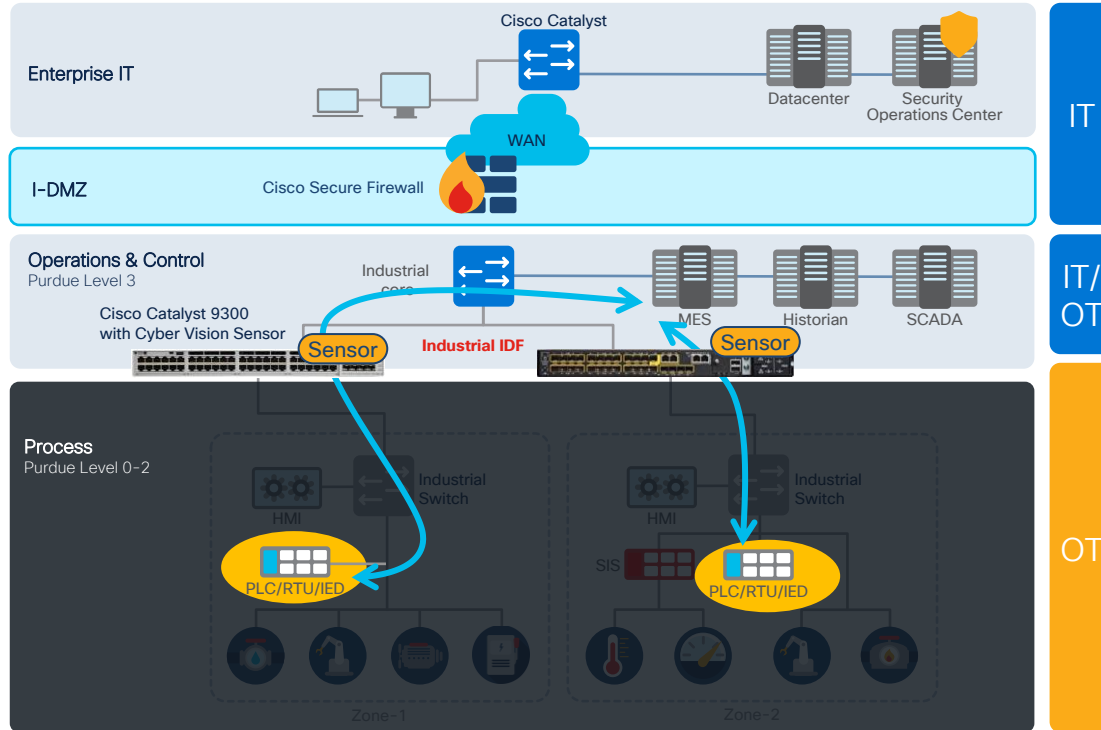
Varying degrees of influence based on industrial vertical and customer operations

IT usually has no visibility below the Industrial IDF



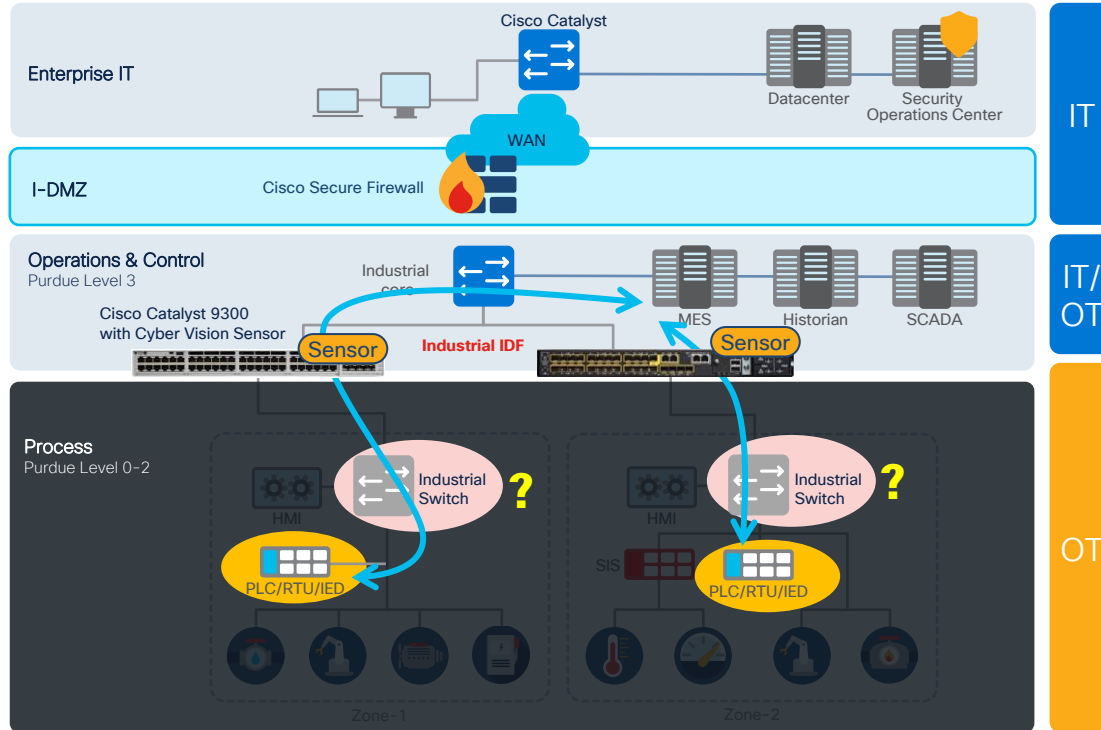
How can IT leverage network equipment it owns to gain visibility into OT?

Your Catalyst switches let you turn on the lights



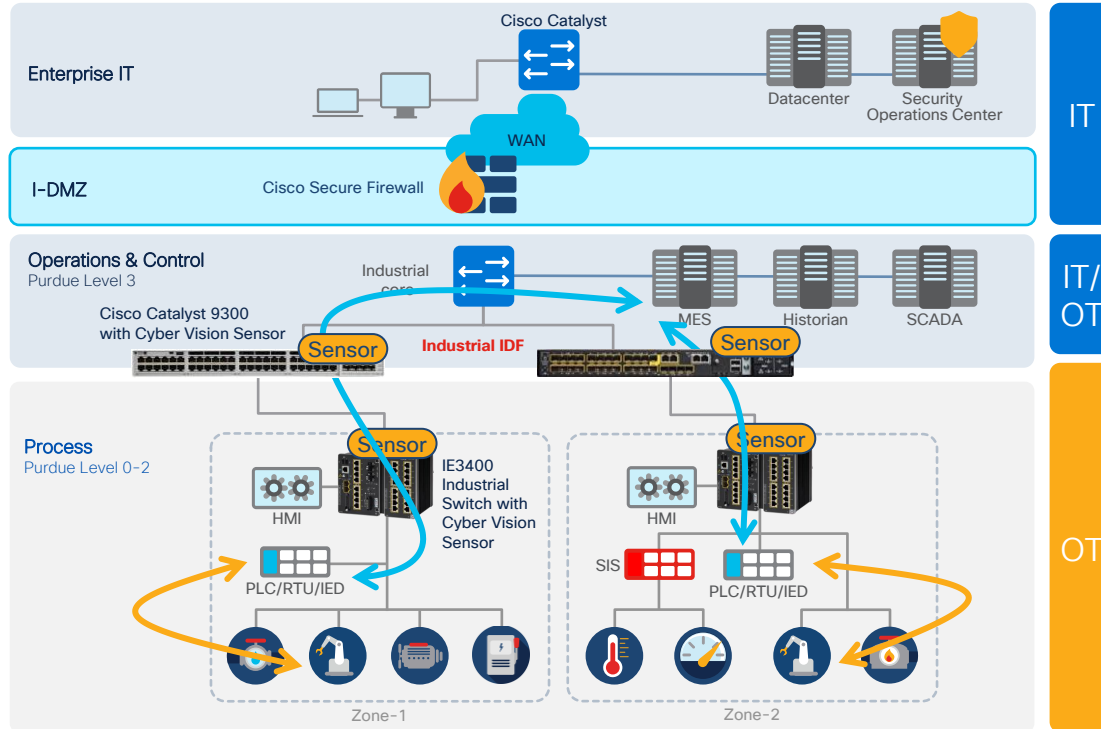
Step-1: Cyber Vision Sensor on C9300 & IE9300 in your IDF gives you visibility to North-South communications to identify key assets

Helps you start a dialogue with OT



Step-2: Work with OT to Identify the critical industrial switches that connect these key assets

Helps you get a footprint into OT



Step-3: Replace critical switches with Cisco IE3400 running Cyber Vision sensor to see the entire OT network

Note: You don't need to replace all industrial switches, just the ones connecting to PLC's

Improving your Security Posture





With visibility into OT, you can start to **assess your security posture**, **build an action plan**, and **set priorities**

Organize assets with Presets to reflect operations

NETWORKS

IP address/Subnet mask - *Optional*
Set an IP address. Ex: 192.168.1.0/24

VLAN ID - *Optional*
Set a number. Ex: 12

Criteria Select all Reject all Default

3 criteria found

RISK SCORE ▼

NETWORKS ✓1 ▼

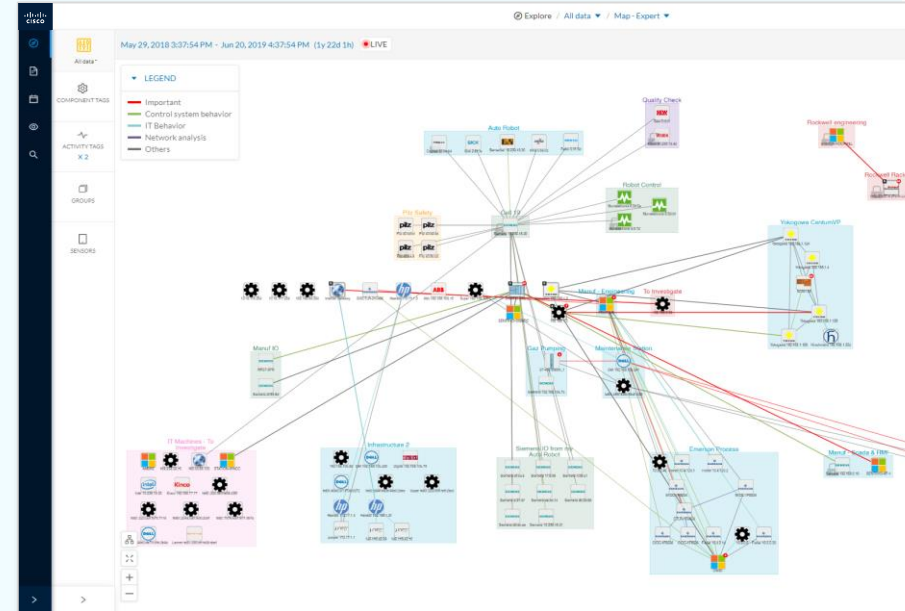
DEVICE TAGS ▲

☐ Controller

ACTIVITY TAGS ✕3 ▲

☐ Controller Name

☐ Controller Info



Filter inventory using subnets, VLANs, device and activity tags to build **presets** that map assets to industrial operations

Use Risk Scoring to assess your security posture

Identify Riskiest Operations

| Preset | Risk score | Last precomputation | Devices | Vulnerabilities |
|------------------------|------------|-------------------------|---------|-----------------|
| All Controllers | 36.5 | Jun 17, 2021 9:46:41 AM | 14 | 94 |
| Broadcast traffic only | 12 | Jun 17, 2021 9:46:47 AM | 30 | 158 |
| IT Activities | 16 | Jun 17, 2021 9:46:47 AM | 36 | 169 |
| IT Devices | 25 | Jun 17, 2021 9:46:49 AM | 23 | 94 |
| Internet Activities | 12 | Jun 17, 2021 9:46:45 AM | 0 | 0 |
| OT Devices | 28 | Jun 17, 2021 9:46:46 AM | 21 | 128 |

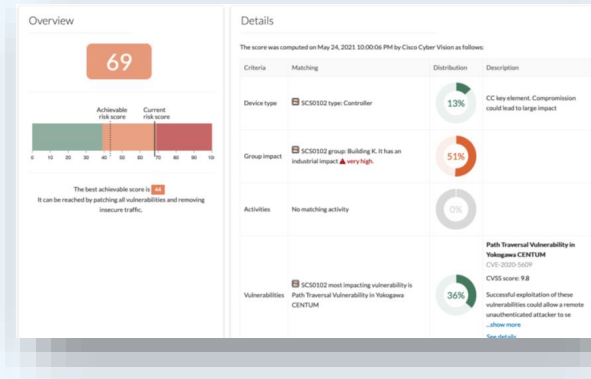
Preset widgets help identify operations at highest risk

Identify Riskiest Endpoints within operations

| Device | Group | First activity | Last activity | IP | NAC | Risk score | Tags |
|--------------------------|-----------------|--------------------------|--------------------------|---------------|--------------------------------|------------|-------------------------|
| SC50102 | Building K | Oct 11, 2019 11:06:52 AM | May 24, 2021 12:30:15 PM | 192.168.1.1 | 0000:64:8b:8c:9f:10 (+1 other) | 69 | @ Controller |
| Falser 10.5.0.22 | Emerson Process | Oct 11, 2019 11:03:46 AM | May 24, 2021 12:30:15 PM | 10.5.0.22 | 00:22:45:3f:90:10 | 69 | @ Controller |
| Falser 10.4.0.14 | Emerson Process | Oct 11, 2019 11:03:46 AM | May 24, 2021 12:30:15 PM | 10.4.0.14 | 00:22:45:3f:90:10 | 69 | @ Controller |
| 10.4.0.30 | Emerson Process | Oct 11, 2019 11:03:46 AM | May 24, 2021 12:30:15 PM | 10.4.0.30 | 00:22:45:3f:90:10 | 69 | @ Controller |
| Yokogawa 192.168.1.124 | Yokogawa | Oct 11, 2019 11:06:52 AM | May 24, 2021 12:30:15 PM | 192.168.1.124 | 0000:64:8b:8c:9f:10 (+1 other) | 69 | @ Controller |
| Falser 10.5.0.18 | Emerson Process | Oct 11, 2019 11:03:46 AM | May 24, 2021 12:30:15 PM | 10.5.0.18 | 00:22:45:3f:90:10 | 69 | @ Controller |
| Falser 10.4.129.2 | Emerson Process | Oct 11, 2019 11:03:46 AM | May 24, 2021 12:30:15 PM | 10.4.129.2 | 00:22:45:04:45:44 | 69 | @ Non Management Server |
| Falser 10.4.129.1 | Emerson Process | Oct 11, 2019 11:03:46 AM | May 24, 2021 12:30:15 PM | 10.4.129.1 | 00:22:45:32:4c:9c | 69 | @ Non Management Server |
| 192.168.1.123 | Yokogawa | May 11, 2020 6:21:58 PM | May 24, 2021 12:30:15 PM | 192.168.1.123 | 4c:52:62:33:95:9f (+1 other) | 69 | @ Email Server |
| Hirschmann 192.168.1.254 | Building K | Oct 11, 2019 11:06:52 AM | May 24, 2021 12:30:15 PM | 192.168.1.254 | ec:74:ba:03:99:4d | 69 | @ Time Server |
| Yokogawa 192.168.1.128 | Yokogawa | Oct 11, 2019 11:06:52 AM | May 24, 2021 12:30:15 PM | 192.168.1.128 | 0000:64:8b:8c:9f:10 (+1 other) | 69 | @ Time Server |

Sort and Filter Risk scores of endpoints to identify riskiest devices

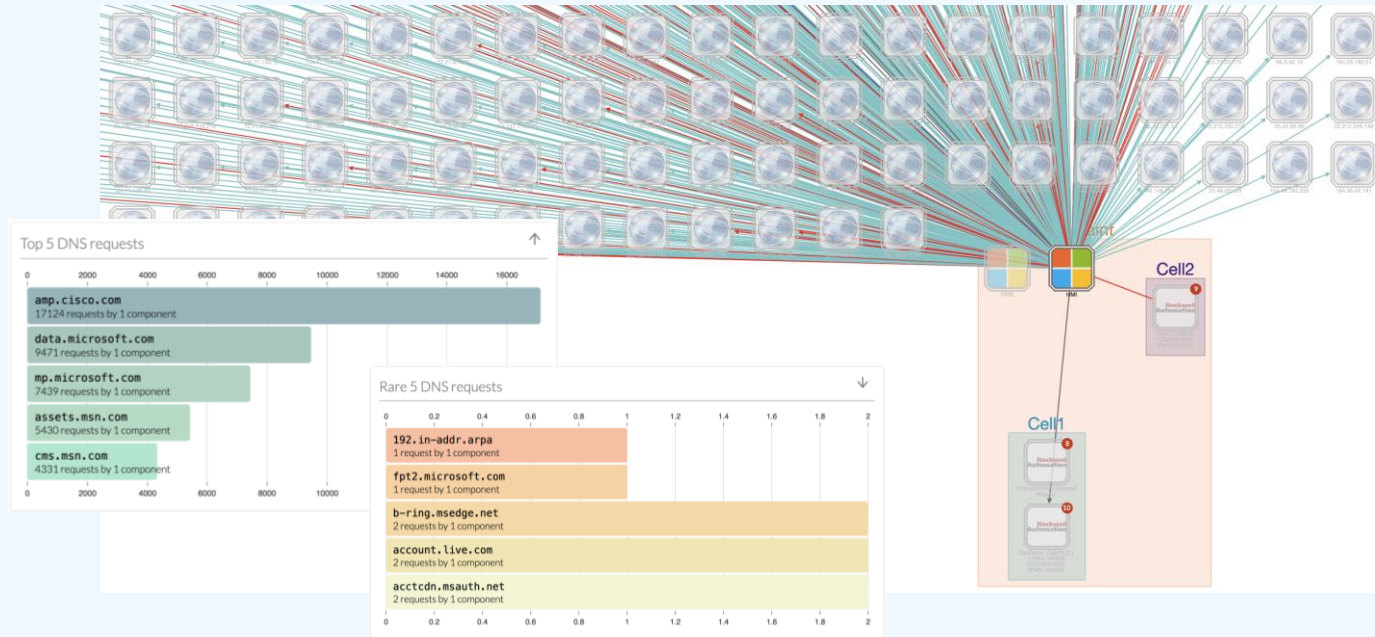
Understand Scoring to Reduce Risk



See what impacts endpoint risk score
See where you are, and where you could be

Build an action plan to to reduce risk

Identify and stop DMZ leaks



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

Identify and stop malicious traffic

Explore / 192.168.0 subnet / Activity list

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

30 Activities [New data](#) [Export to CSV](#)

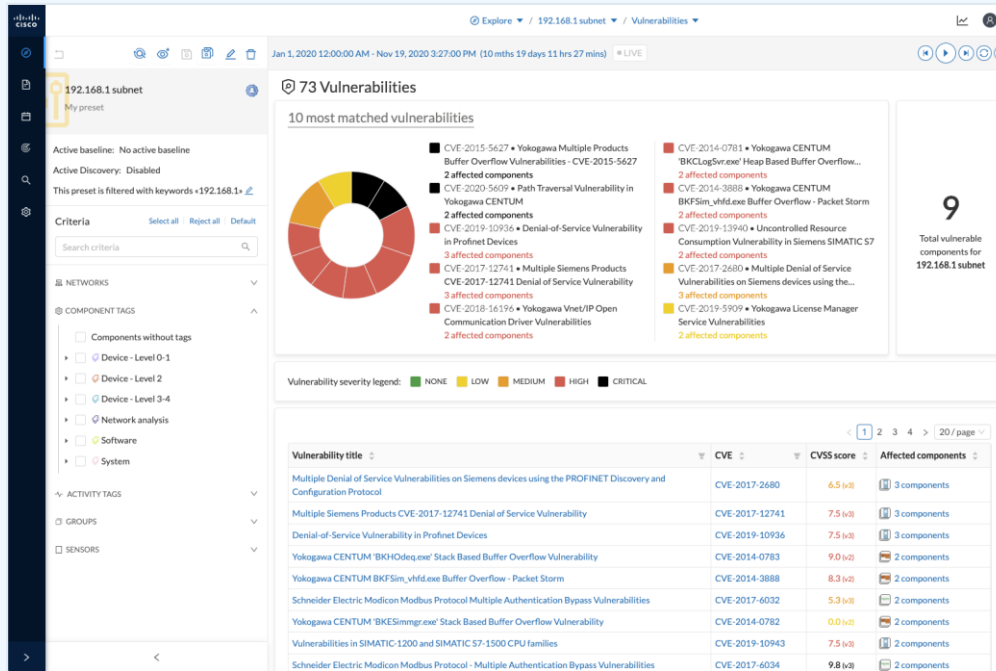
1 2 > 20 / page

| Device | Device | First activity | Last activity | Tags | Flows | Packets | Volume |
|---------------------------------------------------|---------------------|--------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------|---------|---------|
| STATION | VM-XP-PRO | Oct 11, 2019 11:39:57 AM | May 24, 2021 12:32:16 PM | Program Download, Start CPU, Stop CPU, Unite | -10 | 91036 | 6.59 MB |
| Virtual 192.168.0.77 | Siemens 192.168.0.1 | Oct 11, 2019 10:59:49 AM | May 24, 2021 12:32:16 PM | ARP, 57 | -10 | 1255 | 109 kB |
| IE11WIN7 | DESKTOP-GBJUF2N | May 26, 2021 12:14:06 AM | May 26, 2021 12:19:04 AM | Insecure, Authentication, Procedure Call, Exception, Low Volume, Netbios, Netbios Name Service, SMB, SMCRT Policy Violation | -20 | 234 | 35.6 kB |
| 1756-L55/A 1756-M12 (A LOGIX5555 (Port1-L ink00)) | STATION-WINCC | Oct 11, 2019 11:23:14 AM | May 24, 2021 12:32:16 PM | Read Var, Write Var, ARP, EthernetIP | -10 | 29239 | 1.46 MB |
| 192.168.0.255 | VM-XP-PRO | Oct 11, 2019 11:39:57 AM | May 24, 2021 12:32:16 PM | Insecure, Broadcast, Low Volume, Netbios, SMB | -10 | 4 | 972 B |

- ☐ Security analysis
 - ☐ DDOS
 - ☐ Insecure
 - ☐ Port Scan Activity
 - ☐ Snort Alert
 - ☐ Snort Browser
 - ☐ Snort Deleted
 - ☐ Snort Experimental-DoS
 - ☐ Snort Experimental-Scada
 - ☐ Snort Exploit-Kit
 - ☐ Snort File
 - ☐ Snort Malware-Backdoor
 - ☐ Snort Malware-CNC
 - ☐ Snort Malware-Other
 - ☐ Snort Misc
 - ☐ Snort OS-Other
 - ☐ Snort OS-Windows
 - ☐ Snort Server-Other
 - ☐ Snort Server-Webapp

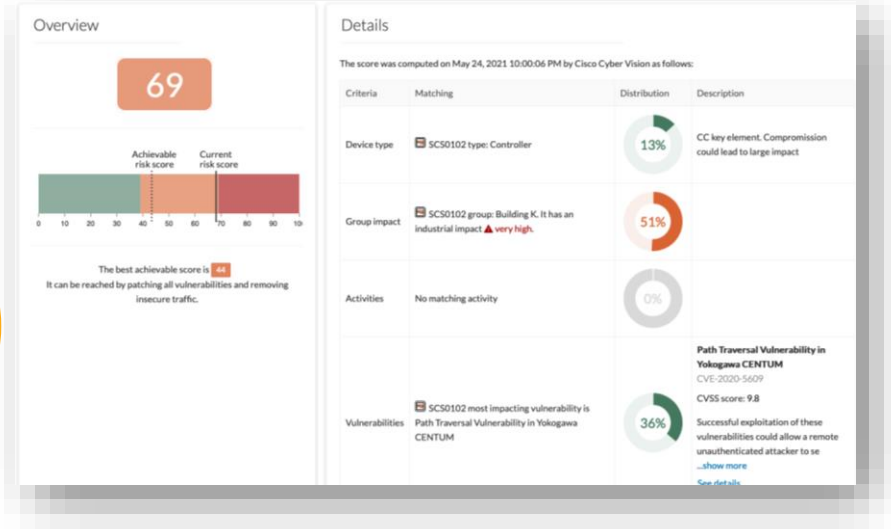
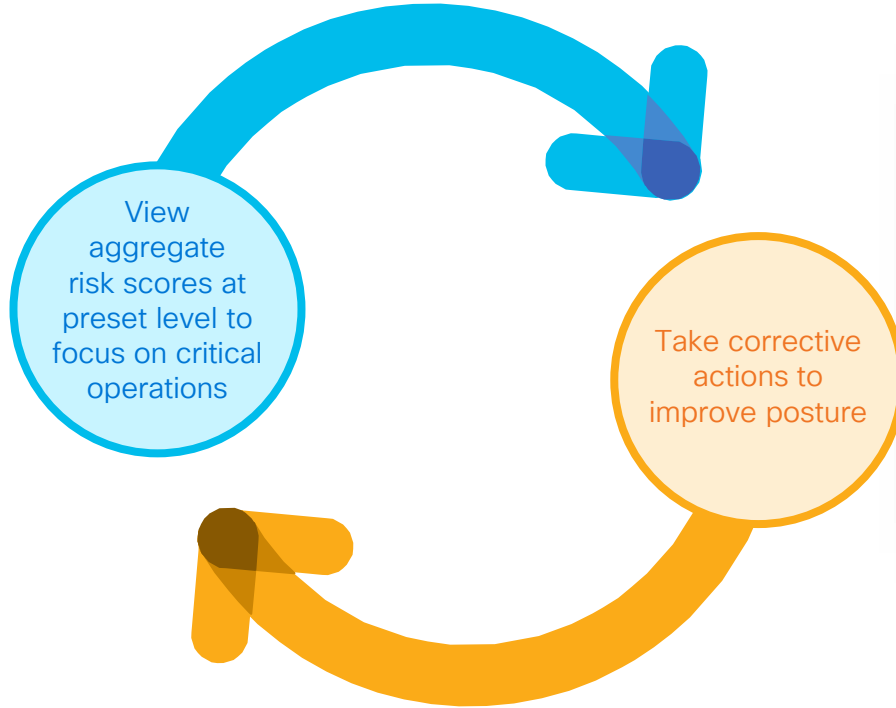
Activity tags associated with events detected by the Snort IDS provide context to understand malicious activities

Track vulnerabilities and build a remediation plan



- Identify most matched vulnerabilities based on severity
- Easily identify affected endpoints
- Build a remediation plan to patch or implement security controls

Iterate until your posture is where it needs to be



Endpoint risk score indicates what is impacting the current scoring, and shows the best achievable score

Leveraging visibility to drive segmentation



Crawl → Walk → Run

Lessons learnt from customer deployments



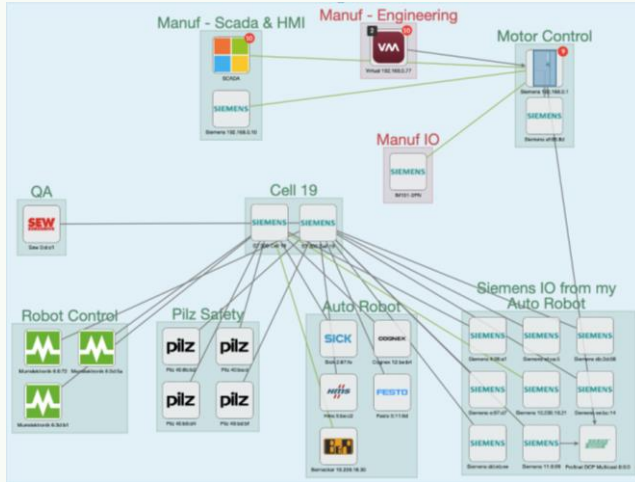
Most customers are not staffed to operationalize micro-segmentation in industrial networks right from the get-go

1. Start with Visibility & Security Posture
2. Advance to macro-segmentation
3. Evolve towards shrinking the zones of trust with micro-segmentation as teams local to the plant get comfortable with the technology

As you shrink zones of trust, OT's ability to see/understand why certain flows are blocked becomes important for seamless operations

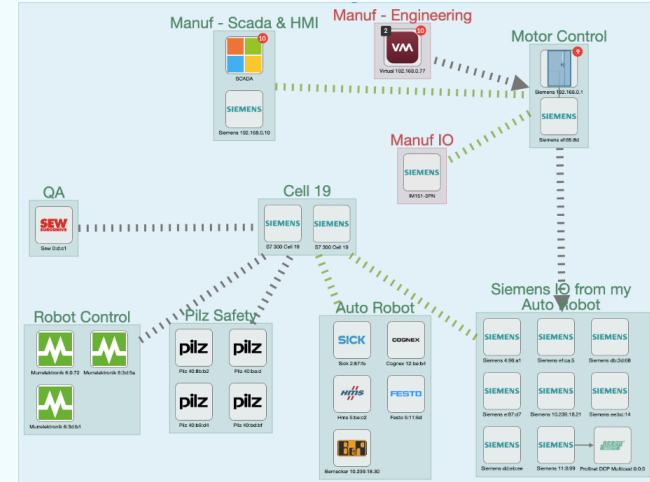
Group endpoints to visualize Zones and Conduits

Group endpoints into **Zones** within Presets



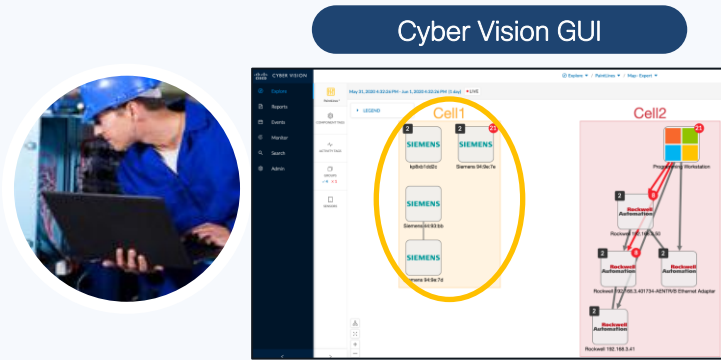
Leverage traffic flows within presets to group endpoints to match the industrial processes they represent

Visualize **Conduits** between Zones



Traffic flows can be aggregated into conduits which can be used to inform segmentation policies

Dynamically map zones to scalable group tags



pxGrid

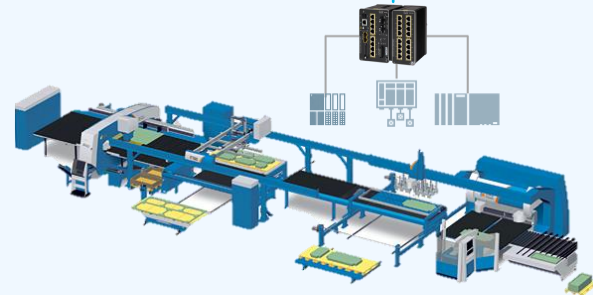
ISE profiles endpoints based on "Cell1" custom attribute and assigns SGT in AuthZ policy

| | Cell 1 | Cell 2 | PLC | MES |
|--------|--------|--------|-----|-----|
| Cell 1 | ✓ | ✗ | ✓ | ✗ |
| Cell 2 | ✗ | ✓ | ✓ | ✗ |
| PLC | ✓ | ✓ | ✓ | ✓ |
| MES | ✗ | ✗ | ✓ | ✓ |



Cisco DNA Center & ISE

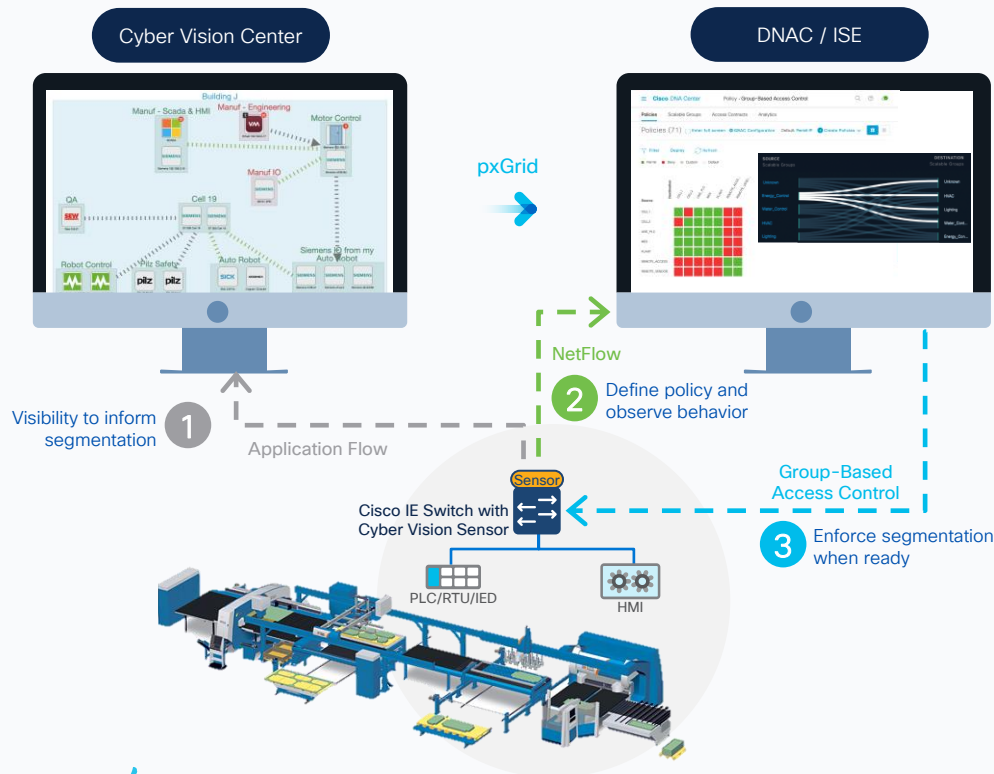
RADIUS



1. OT users understands industrial processes
2. They have the context to group industrial endpoint belonging to a specific process / machine into zones
3. Cyber Vision send pxGrid update with endpoint identities and group "Cell1" to ISE

Segmenting with Visibility & Policy Analytics

Monitor segmentation policy before enforcement



Visualize Zones & Conduits



Group endpoints into zones to visualize aggregated flows as conduits to inform segmentation policy

Dynamic SGT Mapping



Cyber Vision grouping results in dynamic Group-based policy assignment to endpoints through ISE

Monitor Before Enforcement



Visualize Group-based network behavior in DNAC and enable enforcement when confident after monitoring



Cisco industrial network helps you secure OT



Leverage your
network to **gain**
visibility



Leverage your
network to **gain**
insights



Leverage your
network to **enforce**
security controls

Continue your education

- 1 Industrial Zero Trust: Opportunities and Realities ([BRKIOT-2012](#))
- 2 Leveraging Visibility to drive Zero Trust for Industrial Security ([BRKIOT-2353](#))
- 3 Securing Industrial Networks: Where do I start? ([BRKSEC-2077](#))
- 4 Extending Cisco Cyber Vision capabilities by using REST API ([DEVNET-1818](#))

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 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**

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