CISCO Live!

#CiscoLive

cisco The bridge to possible

Leveraging Visibility to drive Zero Trust for Industrial Security

Dan Behrens – TME – IoT Security
@danielrbehrens
BRKIOT-2353

Cisco Webex App

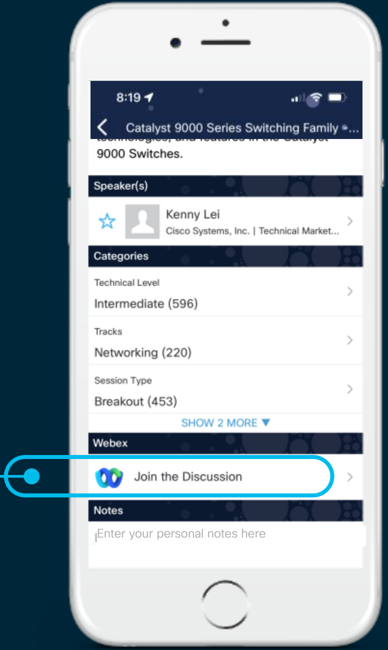
Questions?

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/#BRKIOT-2353

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

Digitization brings new requirements & challenges

- More automation devices
- IoT devices connecting to cloud
- Remote access/Hybrid work
- Malware intrusions
- New regulatory requirements

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

Agenda

- What is Zero Trust
- How Does Zero Trust translate to Industrial Environments
- What is Cisco Cyber Vision
- Integrations with Cisco Enterprise Security products
- Examples of it in action

What is Zero Trust

What is Zero Trust?

- Replaces trust then verify, with least privilege
- Built around creating trusted zones of access – continual enforcement, closest to the protected resource
- Secures all users and application connections
- Identifying and classifying not just users, but endpoints/devices and applications critical

Cisco Secure Zero Trust

A comprehensive approach to securing all access across your networks, applications, and environment.

Workforce

Ensure only the right users and secure devices can access applications.

Workloads

Secure all connections within your apps, across multi-cloud.

Workplace

Secure all user and device connections across your network, including IoT.

The foundations of Zero Trust for workplaces

Grant the right level of network access to users and devices across domains

with

Visibility

Shrink zones of trust and grant access based on least privilege

with

Segmentation

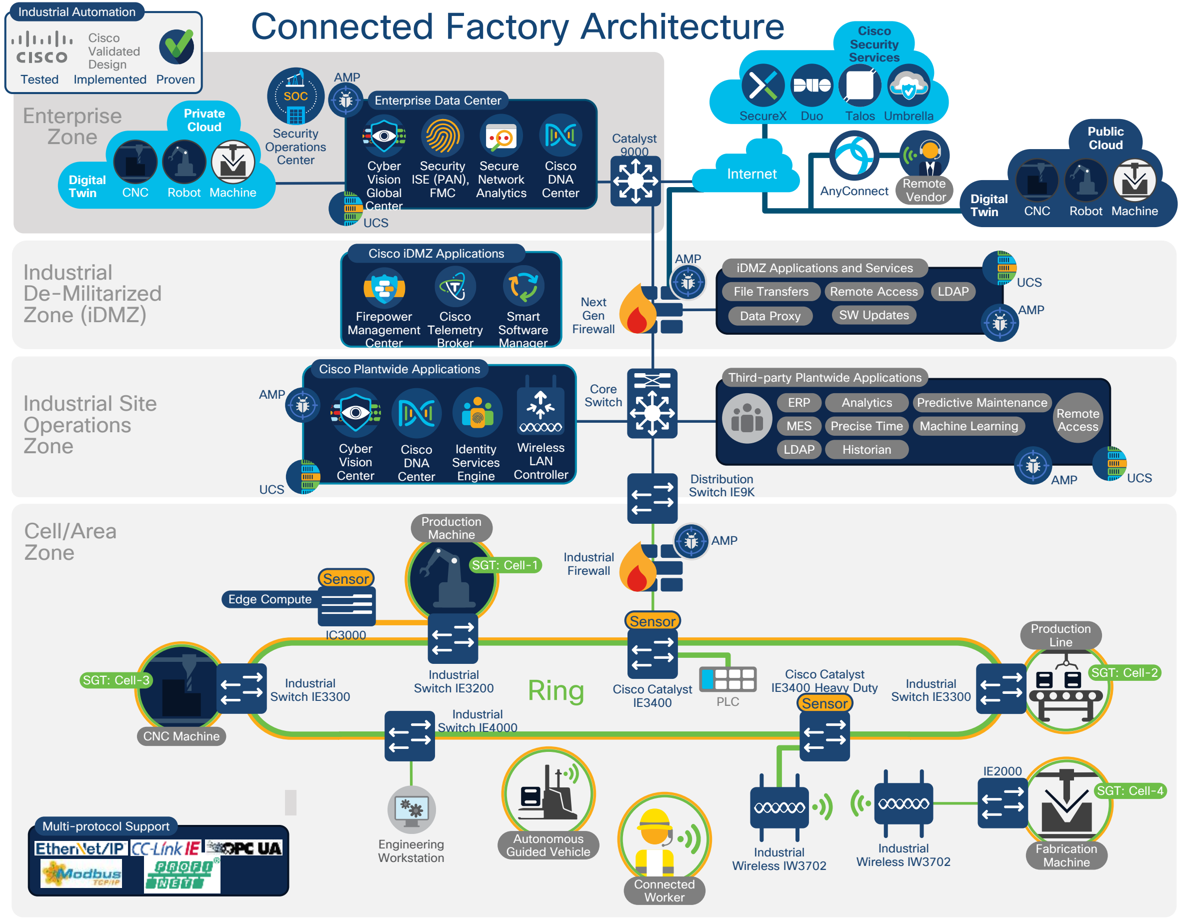
Automate containment of infected endpoints and revoke network access

with

Containment

Zero Trust in Industrial Environments

Connected Factory Architecture



Industrial Security Framework

Visibility & Posture

Cyber Vision
(Industrial Assets)

Secure Endpoint
(Workstations, Compute, Tablets)

Secure X
(SOC Integration)

Secure Network Analytics
(Netflow)

Segment & Protect

Secure Firewall
(IDMZ, App Segmentation)

Identity Services Engine
(User/Device Segmentation)

Secure Access by Duo
(Multi-Factor Authentication)

Threat Detection & Response

Secure Firewall
(Intrusion Prevention)

Secure Endpoint
(Malware Protection)

Secure X
(Incident Investigation & Response)

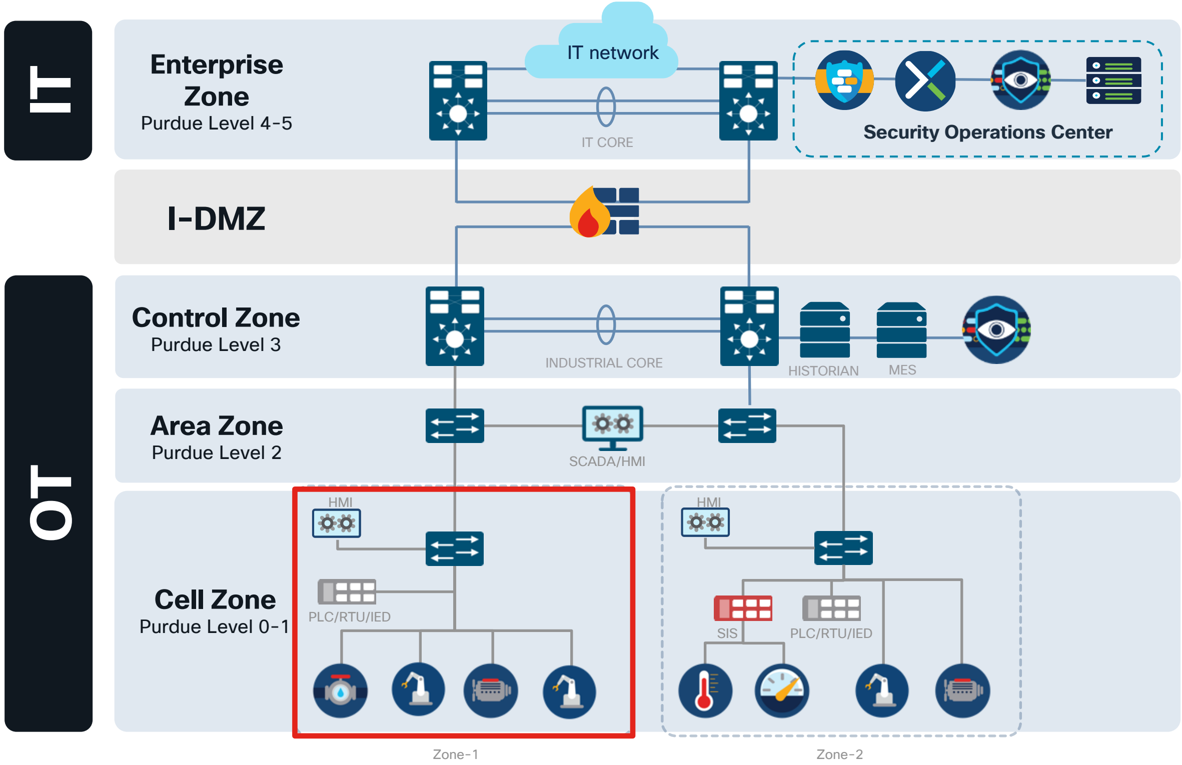
Secure Network Analytics
(Behavioral Modeling & Encrypted Traffic Analytics)

Managed Secure Network Infrastructure
(Built-In Visibility & Enforcement)

- IEC 62443-4-1 certified
- Secure Supply Chain
- Secure Trustworthy Technologies
- Network Access Control
- CSDL
- Validated Designs

Powered by Talos Threat Intelligence

Zero Trust for Industrial



Extending Workplace Zero Trust to Industrial Settings

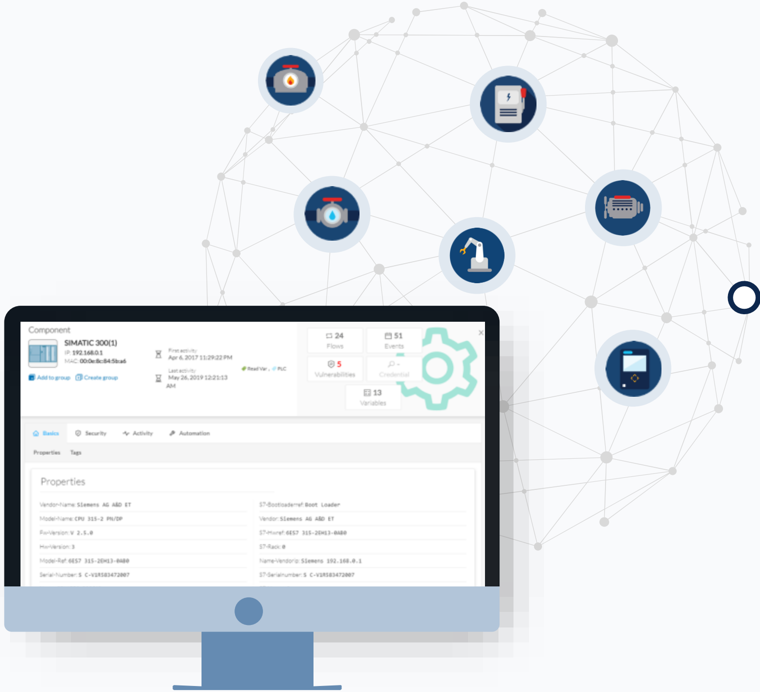
Endpoint Visibility

Endpoint Compliance

Network Segmentation

Threat Detection & Response

Industrial Endpoint Visibility



SIMATIC 300(1)
IP: 192.168.0.1
MAC: 00:0e:8c:84:5b:a6

First activity
Apr 6, 2017 11:29:22 PM

Last activity
May 26, 2019 12:21:13 AM

Read Var , PLC

24 Flows
51 Events
5 Vulnerabilities
- Credential
13 Variables

Properties

Vendor-Name: Siemens AG A&D ET
Model-Name: CPU 315-2 PN/DP
Fw-Version: V 2.5.0
Hw-Version: 3
Model-Ref: 6ES7 315-2EH13-0AB0
Serial-Number: S C-V1R583472007

S7-Bootloaderref: Boot Loader
Vendor: Siemens AG A&D ET
S7-Hwref: 6ES7 315-2EH13-0AB0
S7-Rack: 0
Name-Vendorip: Siemens 192.168.0.1
S7-Serialnumber: S C-V1R583472007

Industrial Control System device visibility based on application-level decoding of industrial protocol traffic and behavior modeling of industrial endpoints

What is Cisco Cyber Vision

Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT

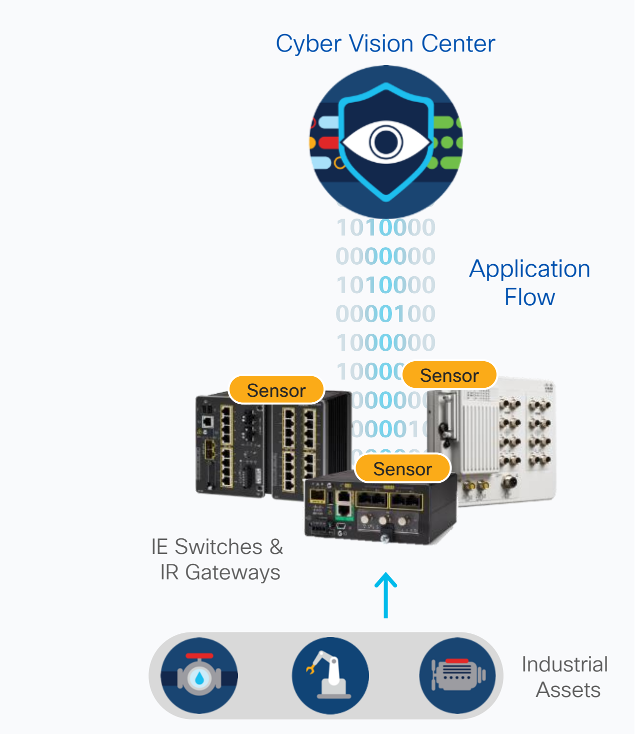
Visibility
Asset inventory
Communication patterns

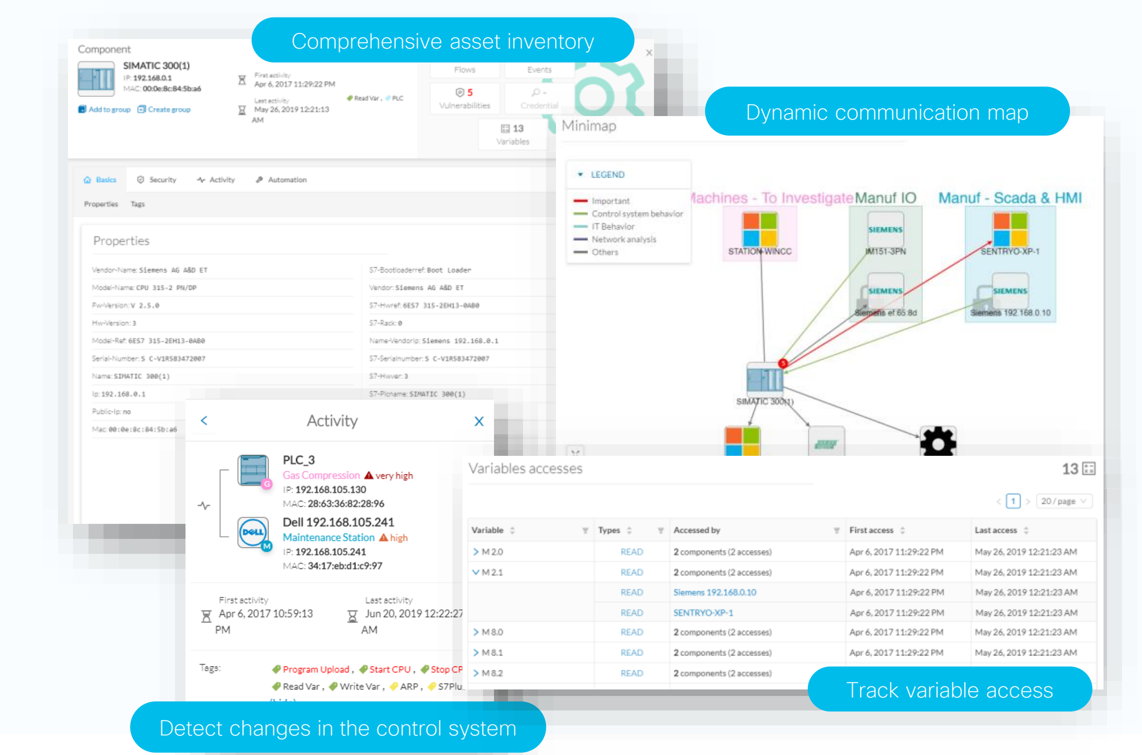
Security Posture
Device vulnerabilities
Risk scoring

Operational Insights
Track process/device modifications
Record control system events

Context and insights that are foundational to building reliable and secure OT networks

Industrial Endpoint Visibility with Cyber Vision





Comprehensive asset inventory

Component

SIMATIC 300(1)
IP: 192.168.0.1
MAC: 00:0e:8c:84:5b:a6

Add to group   Create group

First activity
Apr 6, 2017 11:29:22 PM

Last activity
May 26, 2019 12:21:13 AM

Read Var , PLC

Flows   Events

5 Vulnerabilities   - Credential

13 Variables

Basics   Security   Activity   Automation

Properties   Tags

Properties

Vendor-Name: Siemens AG A&D ET
Model-Name: CPU 315-2 PN/DP
Fw-Version: V 2.5.0
Hw-Version: 3
Model-Ref: 6ES7 315-2EH13-0AB0
Serial-Number: S C-V1R583472007
Name: SIMATIC 300(1)
Ip: 192.168.0.1
Public-Ip: no
Mac: 00:0e:8c:84:5b:a6

S7-Bootloaderref: Boot Loader
Vendor: Siemens AG A&D ET
S7-Hwref: 6ES7 315-2EH13-0AB0
S7-Rack: 0
Name-Vendorip: Siemens 192.168.0.1
S7-Serialnumber: S C-V1R583472007
S7-Hwver: 3
S7-Plcname: SIMATIC 300(1)

Dynamic communication map

Minimap

Activity

PLC_3
Gas Compression ▲ very high
IP: 192.168.105.130
MAC: 28:63:36:82:28:96

Dell 192.168.105.241
Maintenance Station ▲ high
IP: 192.168.105.241
MAC: 34:17:eb:d1:c9:97

First activity
Apr 6, 2017 10:59:13 PM

Last activity
Jun 20, 2019 12:22:27 AM

Tags: Program Upload , Start CPU , Stop CP
Read Var , Write Var , ARP , S7Plu

Variables accesses   13

1   20 / page

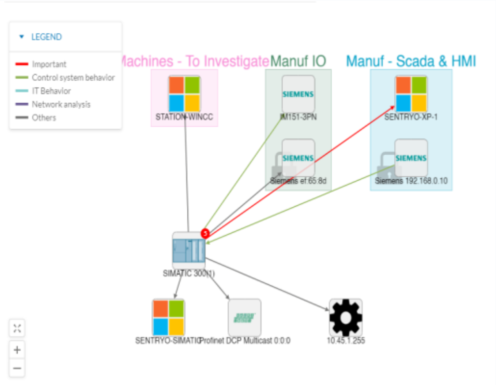
Variable	Types	Accessed by	First access	Last access
> M 2.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
∨ M 2.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	Siemens 192.168.0.10	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	SENTRYO-XP-1	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M 8.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M 8.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M 8.2	READ	2 components (2 accesses)		

Track variable access

Detect changes in the control system

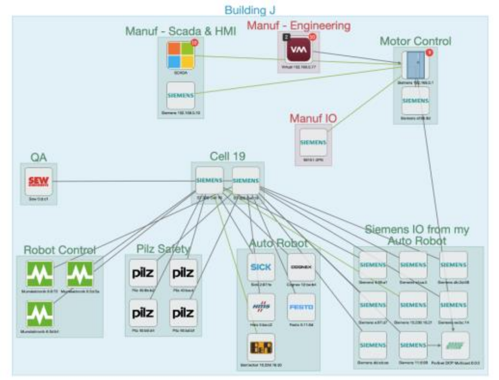
Identify Zones and Conduits

Identify Application Relationships



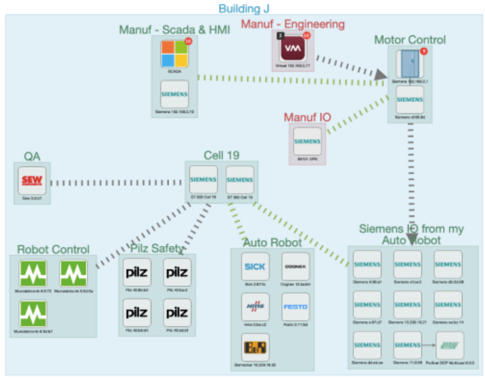
Cyber Vision maps traffic flows between endpoints and provides application-level details within the flows

Group endpoints into Zones



Users can leverage these application relations to group endpoints to match the industrial processes they represent

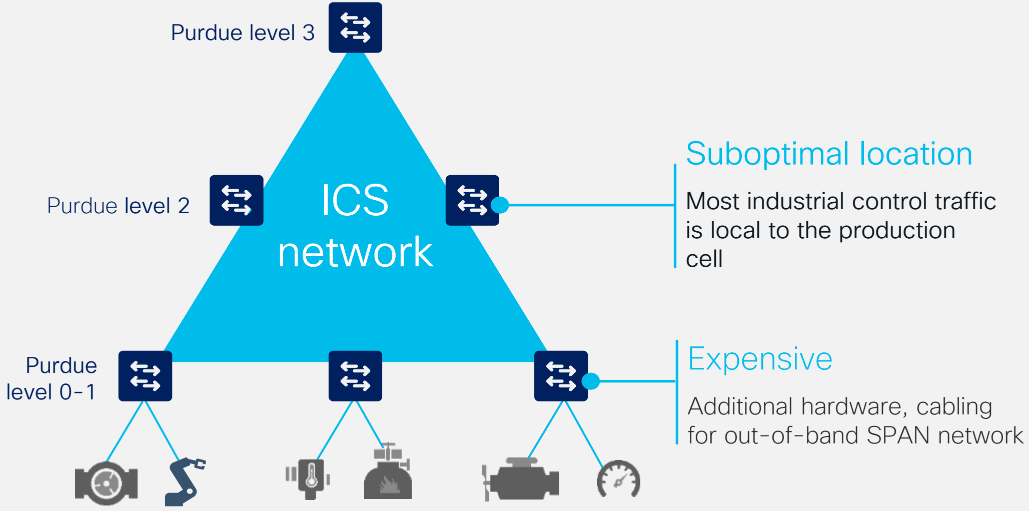
Visualize Conduits between Zones



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

Industrial Traffic Collection

Most industrial network traffic is East-West, not North-South



Suboptimal location

Most industrial control traffic is local to the production cell

Expensive

Additional hardware, cabling for out-of-band SPAN network

DPI location matters!

- Mirroring traffic at the aggregation layer results in visibility to only North-South traffic
- Mirroring traffic at the cell layer requires an expensive out-of-band SPAN network

Cisco Cyber Vision **portfolio**

Cyber Vision **Center**

Hardware Appliance

UCS based servers with Hardware RAID

CV-CNTR-M5S5
- 16 core CPU
- 64 GB RAM
- 800GB drives

CV-CNTR-M5S3
- 10 core CPU
- 32 GB RAM
- 480GB drives

Software Appliance

Virtual Machines

VMWare ESXi OVA

HyperV VHD

Minimum requirements
Intel Xeon, 4 cores
16GB RAM and 200GB SSD
1 or 2 network interfaces

Amazon Web Services

Microsoft Azure

Minimum requirements
Intel Xeon, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Cyber Vision **Sensors**

Sensor

Catalyst IE3300 10G and IE3400 Switches

Sensor

Catalyst IE3400HD IP67 Switch

Sensor

Catalyst IR1101 LTE Gateway

Sensor IDS

Catalyst IR8300 Multiservice Router

Sensor IDS

Catalyst 9300/9400 Aggregation Switch

Network-Sensors

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

Sensor IDS

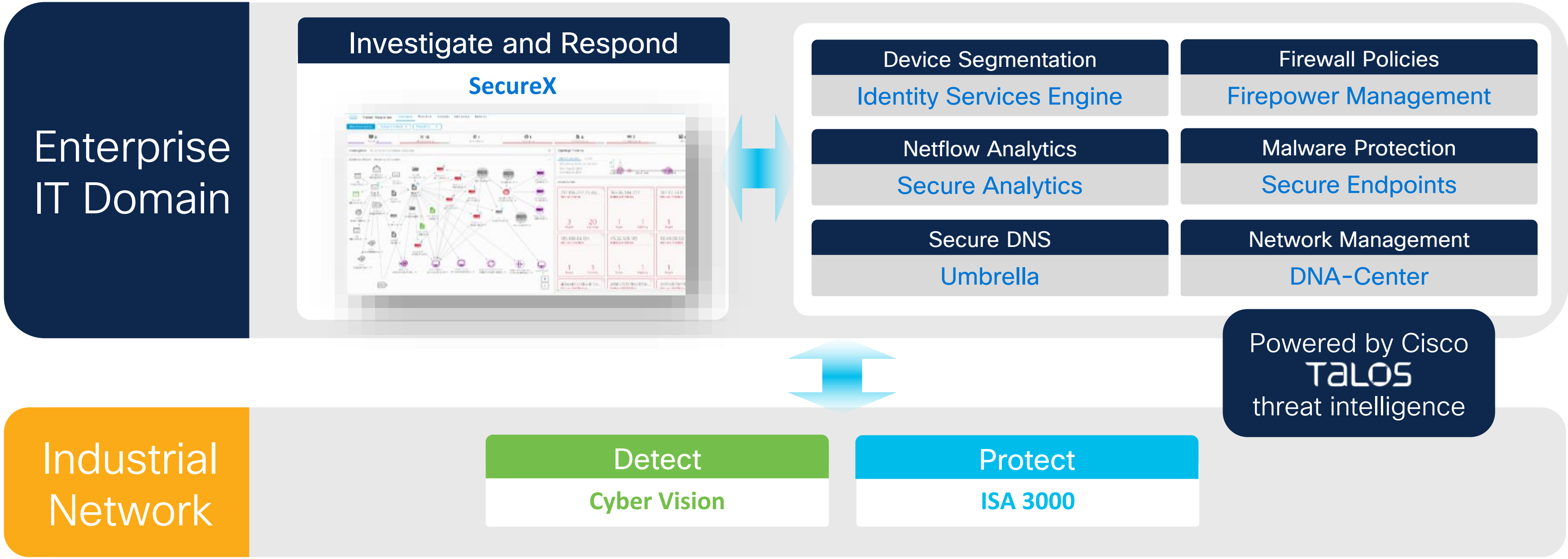
IC3000 Industrial Compute

Hardware-Sensor

DPI via SPAN to support brownfield

Integrations with Cisco Enterprise Security products

Cisco’s fully integrated IT-OT security solution



Enterprise IT Domain

Investigate and Respond
SecureX

Device Segmentation
Identity Services Engine

Firewall Policies
Firepower Management

Netflow Analytics
Secure Analytics

Malware Protection
Secure Endpoints

Secure DNS
Umbrella

Network Management
DNA-Center

Powered by Cisco TALOS threat intelligence

Industrial Network

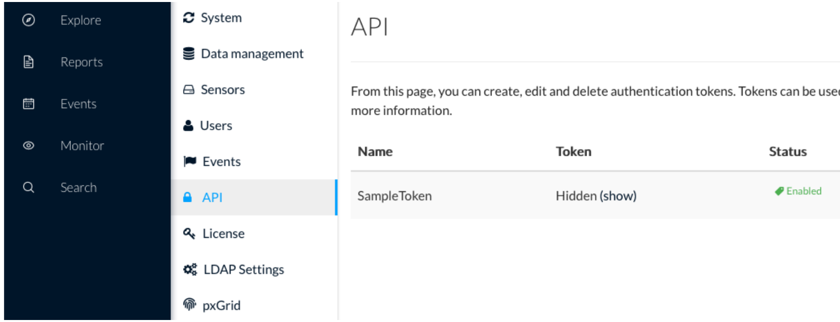
Detect
Cyber Vision

Protect
ISA 3000

Cisco Security for Industrial IoT

Cyber Vision RESTful API

- Access data about components and communication flows available in Cyber Vision
- Leverage sandboxed application hosting to automate functions and integrations



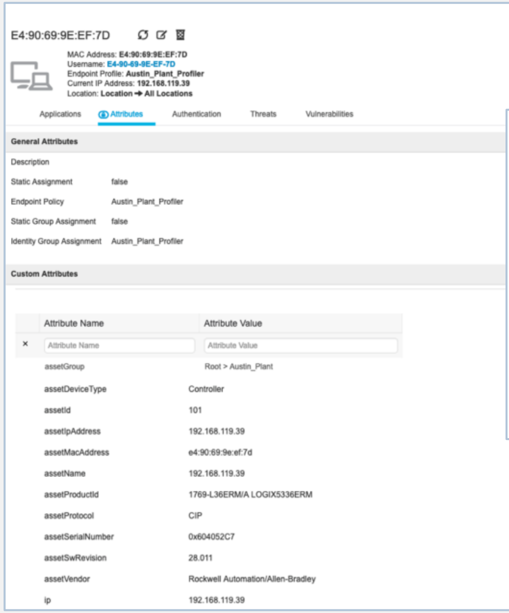
API

From this page, you can create, edit and delete authentication tokens. Tokens can be use
more information.

Name	Token	Status
SampleToken	Hidden (show)	Enabled

Integrate data from Cyber Vision into additional tools

Segment your Network with Cisco ISE



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**

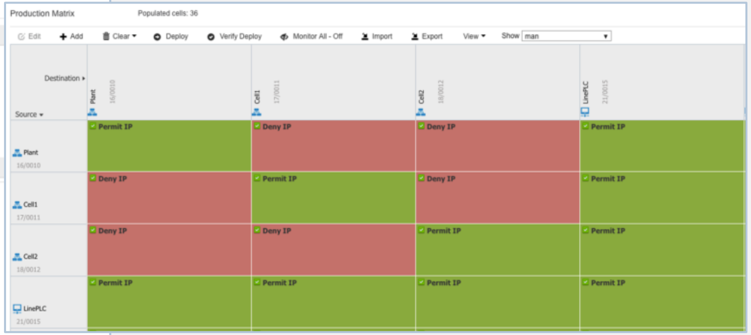
General Attributes

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
assetProtocol	CIP
assetSerialNumber	0x604052C7
assetSwRevision	28.011
assetVendor	Rockwell Automation/Allen-Bradley
ip	192.168.119.39

Device in ISE get attributes from Cyber Vision



Production Matrix   Populated cells: 36

Source ▾ / Destination ▸	Plant 16/0010	Cell1 17/0011	Cell2 18/0012	LinePLC 21/0015
Plant 16/0010	Permit IP	Deny IP	Deny IP	Permit IP
Cell1 17/0011	Deny IP	Permit IP	Deny IP	Permit IP
Cell2 18/0012	Deny IP	Deny IP	Permit IP	Permit IP
LinePLC 21/0015	Permit IP	Permit IP	Permit IP	Permit IP

TrustSec Policy to enforce zone segmentation

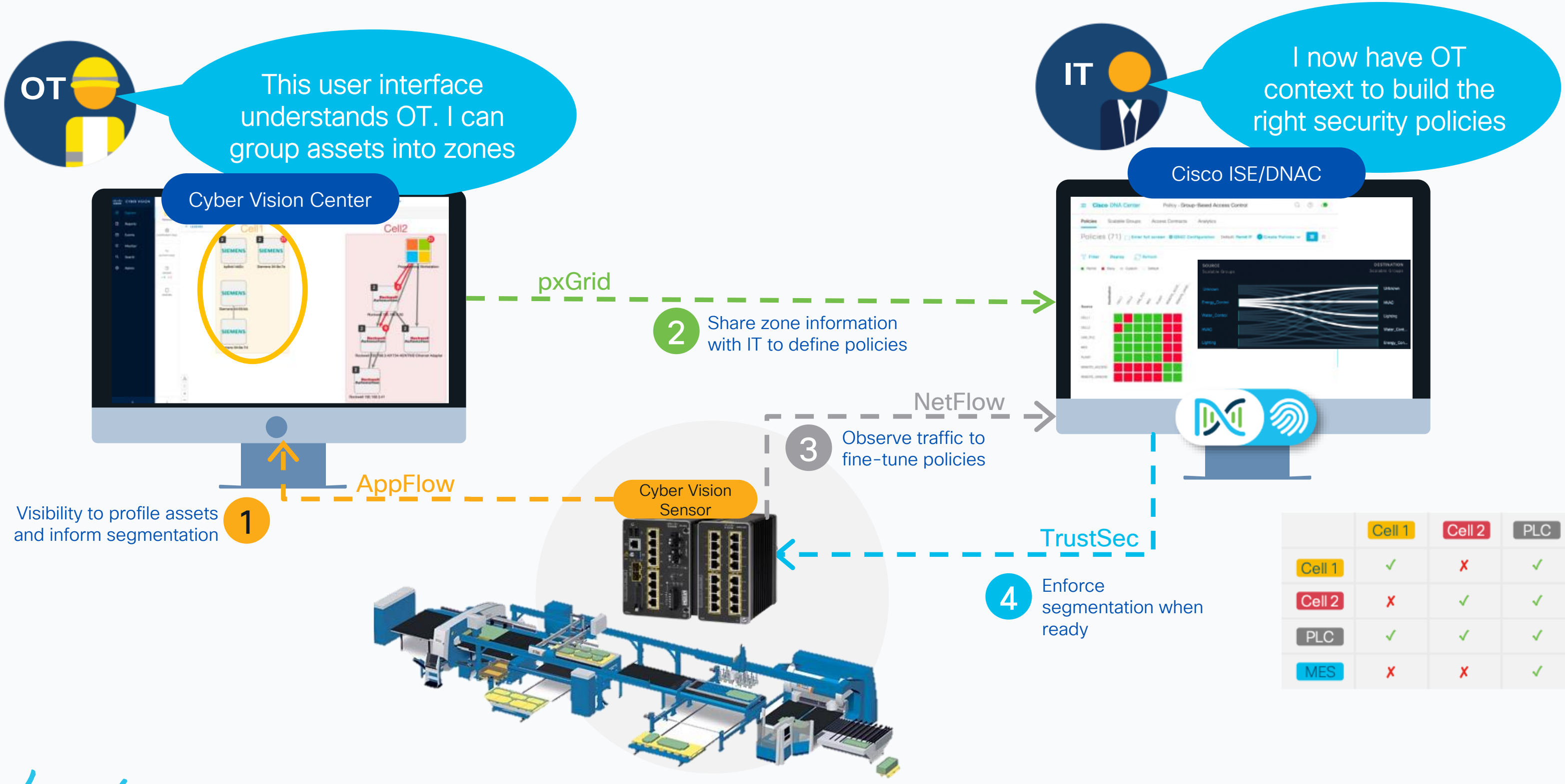
Enrich endpoint attributes in ISE with rich context from Cyber Vision

Assign SGTs based on Cyber Vision grouping for dynamic policy assignment to endpoints

Enforce segmentation through dynamic assignment of VLAN, dACLs or TrustSec

Cyber Vision and ISE enable dynamic segmentation of industrial networks

Segment your Network with Cisco ISE



OT: This user interface understands OT. I can group assets into zones

IT: I now have OT context to build the right security policies

1 Visibility to profile assets and inform segmentation

2 Share zone information with IT to define policies

3 Observe traffic to fine-tune policies

4 Enforce segmentation when ready

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

Visualize activity between scalable groups

Endpoint Visibility

Compliance

Segmentation

TDR

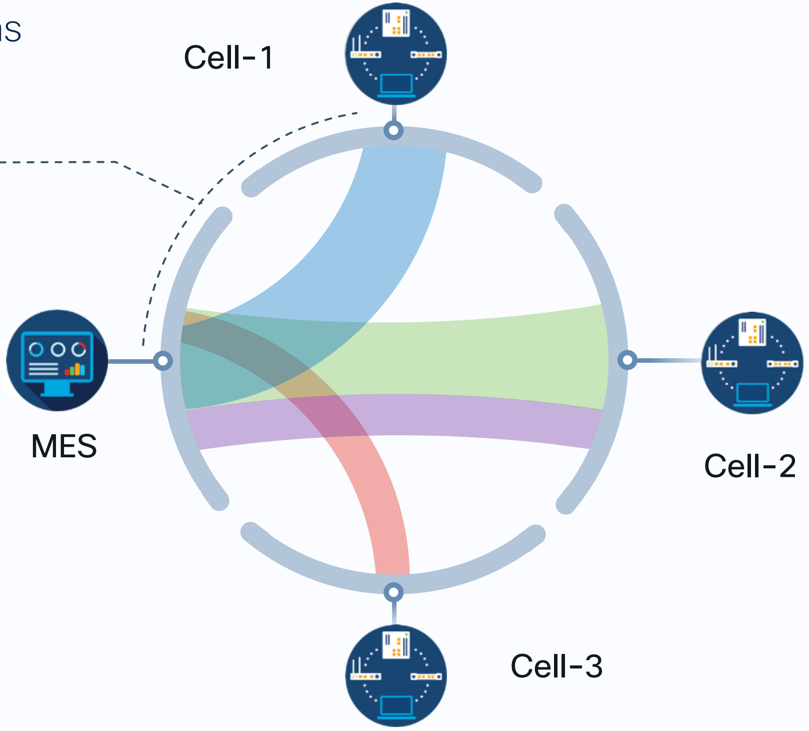
DNAC Policy Modeling – With traffic patterns

	MES	Cell-1	Cell-2
Cell-1	✓	✓	⛔

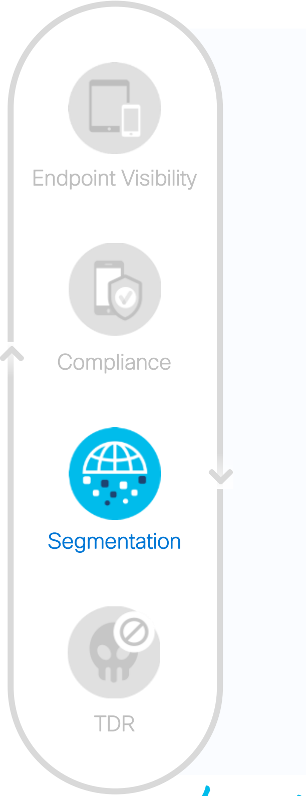
Unearth critical access that must be allowed / denied

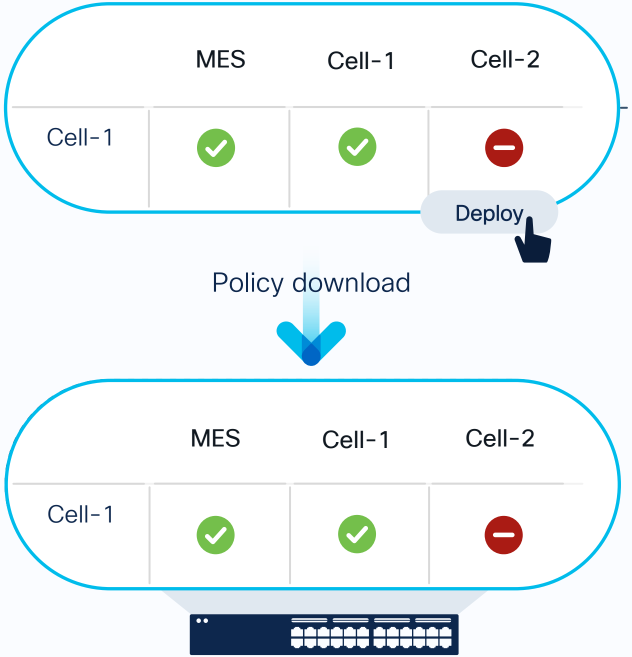
Observe and fine-tune for days/weeks

No policy on the network, yet



Deploy segmentation policies with confidence



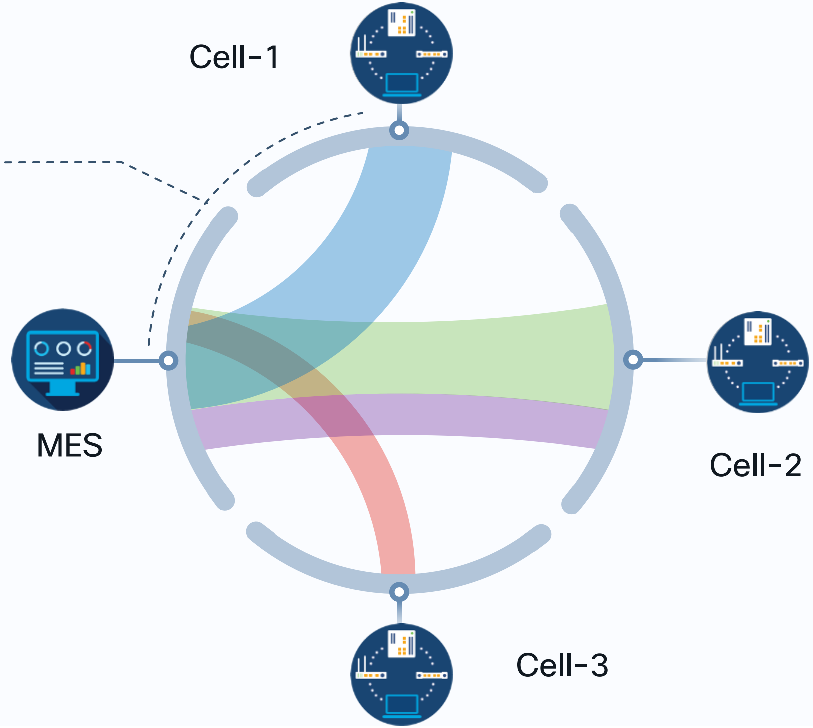


Group-based **Policies** – for segmentation

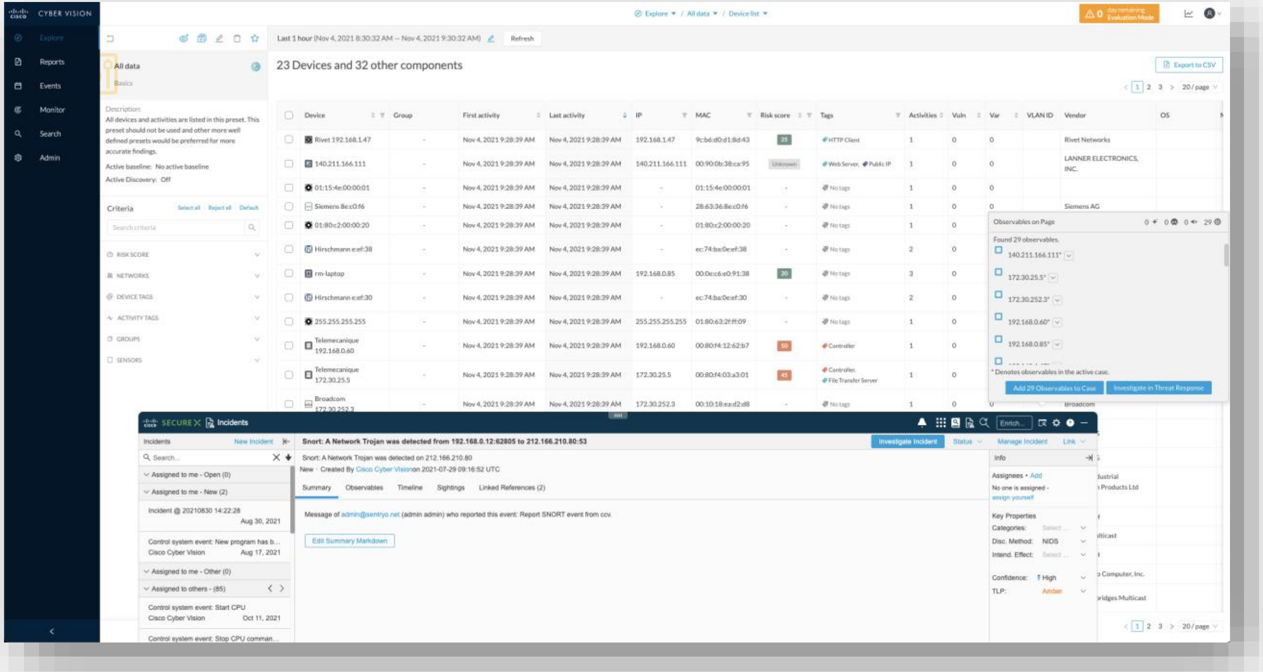
	MES	Cell-1	Cell-2
Cell-1	✓	✓	⛔

Policy download

	MES	Cell-1	Cell-2
Cell-1	✓	✓	⛔



Investigation & Orchestration with SecureX



Last 1 hour (Nov 4, 2021 8:30:32 AM – Nov 4, 2021 9:30:32 AM)

All data

Basics

Description:
All devices and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline

Active Discovery: Off

Criteria — Select all · Reject all · Default

Search criteria

RISK SCORE
NETWORKS
DEVICE TAGS
ACTIVITY TAGS
GROUPS
SENSORS

23 Devices and 32 other components

Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags	Activities	Vuln	Var	VLAN ID	Vendor	OS
Rivet 192.168.1.47	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	192.168.1.47	9c:b6:d0:d1:8d:43	25	HTTP Client	1	0	0		Rivet Networks	
140.211.166.111	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	140.211.166.111	00:90:0b:38:ca:95	Unknown	Web Server, Public IP	1	0	0		LANNER ELECTRONICS, INC.	
01:15:4e:00:00:01	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	-	01:15:4e:00:00:01	-	No tags	1	0	0			
Siemens 8e:c0:f6	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	-	28:63:36:8e:c0:f6	-	No tags	1	0	0		Siemens AG	
01:80:c2:00:00:20	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	-	01:80:c2:00:00:20	-	No tags	1	0				
Hirschmann e:ef:38	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	-	ec:74:ba:0e:ef:38	-	No tags	2	0				
rm-laptop	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	192.168.0.85	00:0e:c6:e0:91:38	20	No tags	3	0				
Hirschmann e:ef:30	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	-	ec:74:ba:0e:ef:30	-	No tags	2	0				
255.255.255.255	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	255.255.255.255	01:80:63:2f:ff:09	-	No tags	1	0				
Telemecanique 192.168.0.60	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	192.168.0.60	00:80:f4:12:62:b7	50	Controller	1	0				
Telemecanique 172.30.25.5	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	172.30.25.5	00:80:f4:03:a3:01	45	Controller, File Transfer Server	1	0				
Broadcom 172.30.252.3	-	Nov 4, 2021 9:28:39 AM	Nov 4, 2021 9:28:39 AM	172.30.252.3	00:10:18:ea:d2:d8	-	No tags	1	0	0		Broadcom	

Observables on Page — 0 0 0 29

Found 29 observables.

□ 140.211.166.111*
□ 172.30.25.5*
□ 172.30.252.3*
□ 192.168.0.60*
□ 192.168.0.85*

* Denotes observables in the active case.

Add 29 Observables to Case · Investigate in Threat Response

Incidents — New Incident

Search...

Assigned to me - Open (0)

Assigned to me - New (2)

Incident @ 20210830 14:22:28 — Aug 30, 2021

Control system event: New program has b... — Cisco Cyber Vision — Aug 17, 2021

Assigned to me - Other (0)

Assigned to others - (85)

Control system event: Start CPU — Cisco Cyber Vision — Oct 11, 2021

Control system event: Stop CPU comman...

Snort: A Network Trojan was detected from 192.168.0.12:62805 to 212.166.210.80:53

Snort: A Network Trojan was detected on 212.166.210.80

New · Created By Cisco Cyber Visionon 2021-07-29 09:16:52 UTC

Summary · Observables · Timeline · Sightings · Linked References (2)

Message of admin@sentryo.net (admin admin) who reported this event: Report SNORT event from ccv.

Edit Summary Markdown

Info

Assignees • Add

No one is assigned - assign yourself

Key Properties

Categories: Select ...

Disc. Method: NIDS

Intend. Effect: Select ...

Confidence: High

TLP: Amber

Leverage Cyber Vision Observables to:

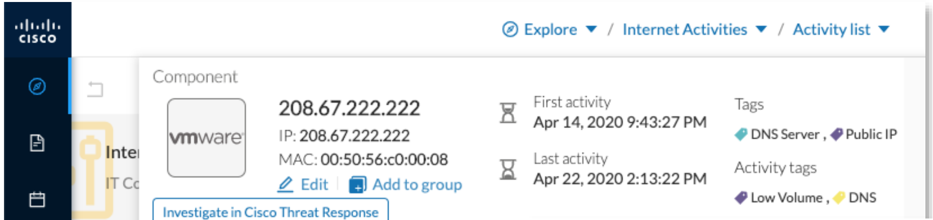
Create and **manage incidents** in SecureX

Create and **orchestrate playbooks**

Launch investigations in Talos, Umbrella, Secure Endpoint, Threat Grid etc.

SecureX Ribbon in Cyber Vision for investigations and remediation orchestration

Investigate threats with SecureX Threat Response


Explore / Internet Activities / Activity list
Inter
IT Co
Active h
vmware
Edit
Add to group
Investigate in Cisco Threat Response

Component

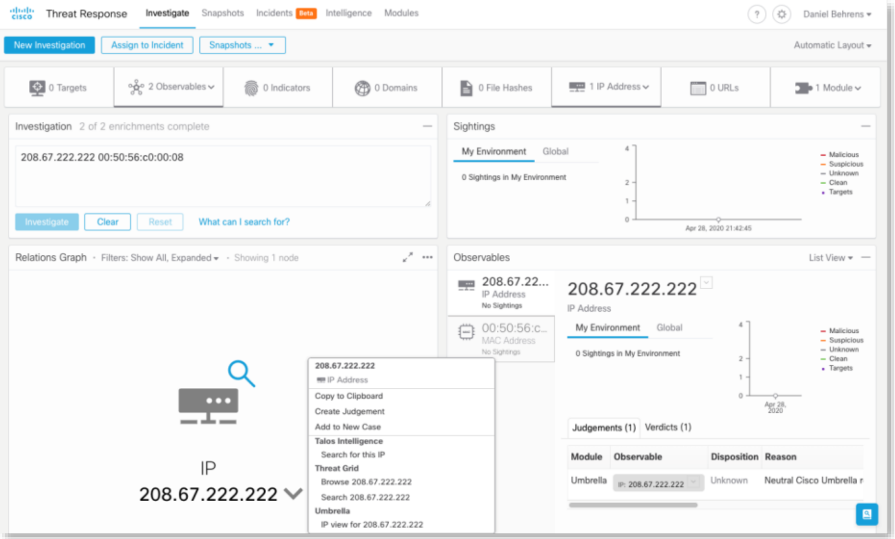
208.67.222.222
IP: 208.67.222.222
MAC: 00:50:56:c0:00:08

First activity
Apr 14, 2020 9:43:27 PM

Last activity
Apr 22, 2020 2:13:22 PM

Tags
DNS Server , Public IP

Activity tags
Low Volume , DNS



Investigation 2 of 2 enrichments complete

208.67.222.222 00:50:56:c0:00:08

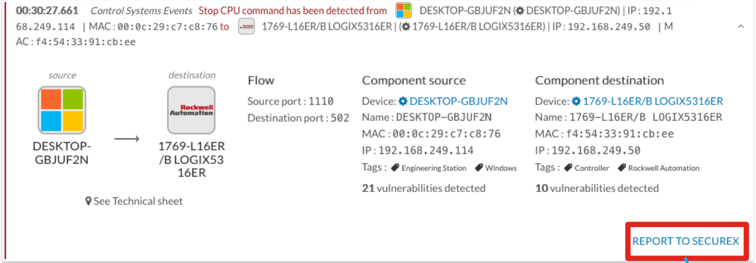
Module	Observable	Disposition	Reason
Umbrella	IP: 208.67.222.222	Unknown	Neutral Cisco Umbrella r

Pivot from Cyber Vision to SecureX to investigate observables

Pull details from Umbrella, FTD, Talos, AMP, Stealthwatch, etc.

Promote Cyber Vision Events to SecureX Incidents

View events in Cyber Vision



00:30:27.661 *Control Systems Events* Stop CPU command has been detected from DESKTOP-GBJUF2N (DESKTOP-GBJUF2N) | IP : 192.168.249.114 | MAC : 00:0c:29:c7:c8:76 to 1769-L16ER/B LOGIX5316ER | (1769-L16ER/B LOGIX5316ER) | IP : 192.168.249.50 | MAC : f4:54:33:91:cb:ee

See Technical sheet

Flow

Source port : 1110
Destination port : 502

Component source

Device: DESKTOP-GBJUF2N
Name : DESKTOP-GBJUF2N
MAC : 00:0c:29:c7:c8:76
IP : 192.168.249.114
Tags : Engineering Station Windows
21 vulnerabilities detected

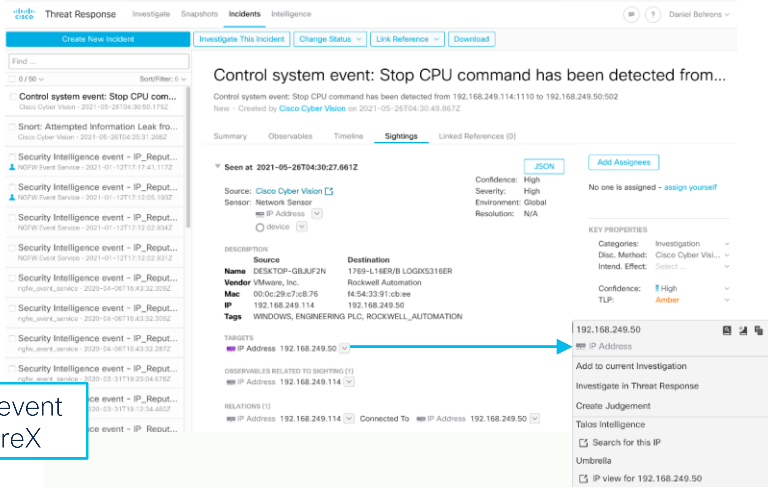
Component destination

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

REPORT TO SECUREX

Promote event to SecureX

Launch investigation is SecureX



Control system event: Stop CPU com...
Cisco Cyber Vision - 2021-05-26T04:30:50.179Z

Snort: Attempted Information Leak fro...
Cisco Cyber Vision - 2021-05-26T04:25:31.208Z

Security Intelligence event - IP_Reput...
NGFW Event Service - 2021-01-12T17:17:41.117Z

Security Intelligence event - IP_Reput...
NGFW Event Service - 2021-01-12T17:12:05.193Z

Security Intelligence event - IP_Reput...
NGFW Event Service - 2021-01-12T17:12:02.934Z

Security Intelligence event - IP_Reput...
NGFW Event Service - 2021-01-12T17:12:02.931Z

Security Intelligence event - IP_Reput...
rgfw_event_service - 2020-04-06T16:43:32.309Z

Security Intelligence event - IP_Reput...
rgfw_event_service - 2020-04-06T16:43:32.309Z

Security Intelligence event - IP_Reput...
rgfw_event_service - 2020-04-06T16:43:32.287Z

Security Intelligence event - IP_Reput...
rgfw_event_service - 2020-03-31T19:23:04.678Z

...ce event - IP_Reput...
...20-03-31T19:12:34.460Z

...ce event - IP_Reput...

Control system event: Stop CPU command has been detected from...

Control system event: Stop CPU command has been detected from 192.168.249.114:1110 to 192.168.249.50:502
New · Created by Cisco Cyber Vision on 2021-05-26T04:30:49.867Z

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

No one is assigned - assign yourself

DESCRIPTION

	Source	Destination
Name	DESKTOP-GBJUF2N	1769-L16ER/B LOGIX5316ER
Vendor	VMware, Inc.	Rockwell Automation
Mac	00:0c:29:c7:c8:76	f4:54:33:91:cb:ee
IP	192.168.249.114	192.168.249.50
Tags	WINDOWS, ENGINEERING PLC, ROCKWELL_AUTOMATION	

KEY PROPERTIES

Categories: Investigation
Disc. Method: Cisco Cyber Visi...
Intend. Effect: Select ...

Confidence: High
TLP: Amber

TARGETS
IP Address 192.168.249.50

OBSERVABLES RELATED TO SIGHTING (1)
IP Address 192.168.249.114

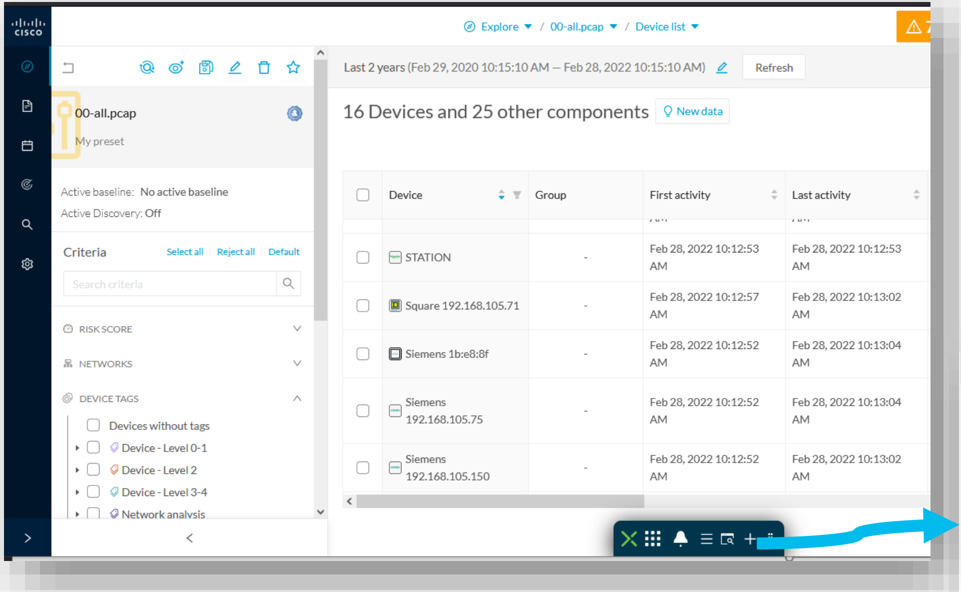
RELATIONS (1)
IP Address 192.168.249.114 Connected To IP Address 192.168.249.50

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

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

SecureX Ribbon on Cyber Vision



Explore / 00-all.pcap / Device list

00-all.pcap

My preset

Active baseline: No active baseline

Active Discovery: Off

Criteria Select all | Reject all | Default

Search criteria

RISK SCORE

NETWORKS

DEVICE TAGS

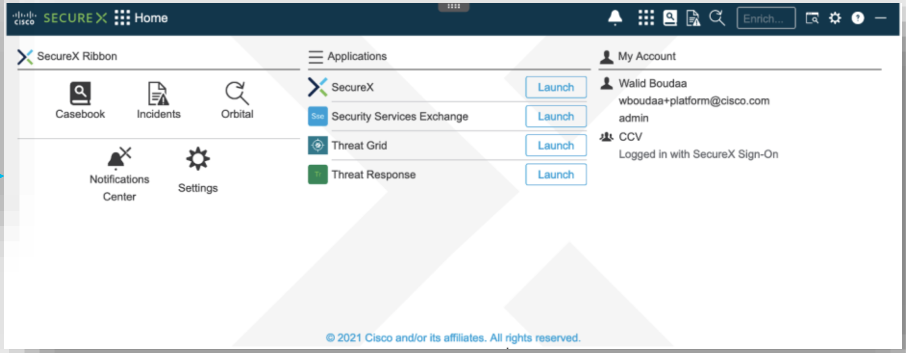
- □ Devices without tags
- □ Device - Level 0-1
- □ Device - Level 2
- □ Device - Level 3-4
- □ Network analysis

Last 2 years (Feb 29, 2020 10:15:10 AM — Feb 28, 2022 10:15:10 AM) Refresh

16 Devices and 25 other components New data

□	Device	Group	First activity	Last activity
□	STATION	-	Feb 28, 2022 10:12:53 AM	Feb 28, 2022 10:12:53 AM
□	Square 192.168.105.71	-	Feb 28, 2022 10:12:57 AM	Feb 28, 2022 10:13:02 AM
□	Siemens 1b:e8:8f	-	Feb 28, 2022 10:12:52 AM	Feb 28, 2022 10:13:04 AM
□	Siemens 192.168.105.75	-	Feb 28, 2022 10:12:52 AM	Feb 28, 2022 10:13:04 AM
□	Siemens 192.168.105.150	-	Feb 28, 2022 10:12:52 AM	Feb 28, 2022 10:13:02 AM

Unify visibility and **accelerate** incident response using Cyber Vision observables



SECUREX Home

Enrich...

SecureX Ribbon

Casebook | Incidents | Orbital | Notifications Center | Settings

Applications

Application	
SecureX	Launch
Security Services Exchange	Launch
Threat Grid	Launch
Threat Response	Launch

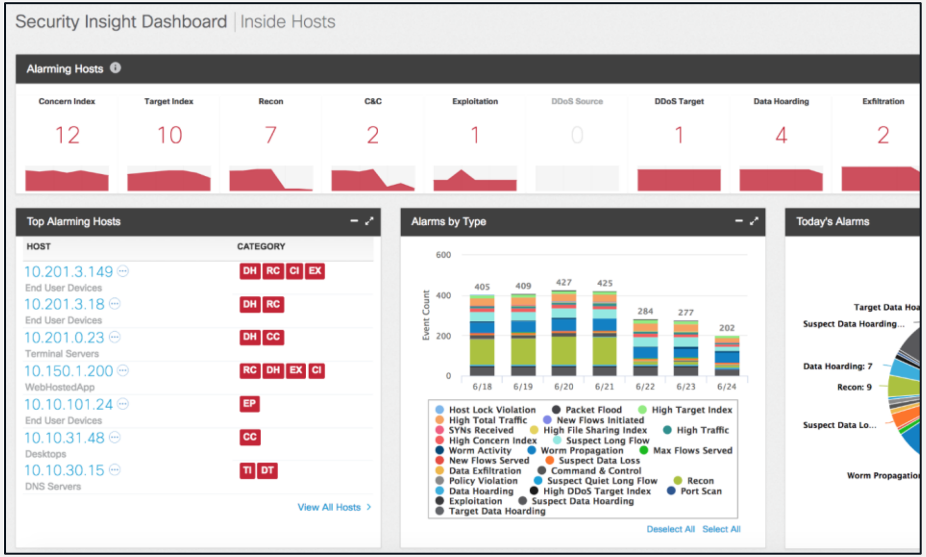
My Account

Walid Boudaa
wboudaa+platform@cisco.com
admin

CCV
Logged in with SecureX Sign-On

© 2021 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Analytics + Cyber Vision



Security Insight Dashboard | Inside Hosts

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration
12	10	7	2	1	0	1	4	2

Top Alarming Hosts

HOST	CATEGORY
10.201.3.149 End User Devices	DH RC CI EX
10.201.3.18 End User Devices	DH RC
10.201.0.23 Terminal Servers	DH CC
10.150.1.200 WebHostedApp	RC DH EX CI
10.10.101.24 End User Devices	EP
10.10.31.48 Desktops	CC
10.10.30.15 DNS Servers	TI DT

View All Hosts ›

Alarms by Type

Today's Alarms

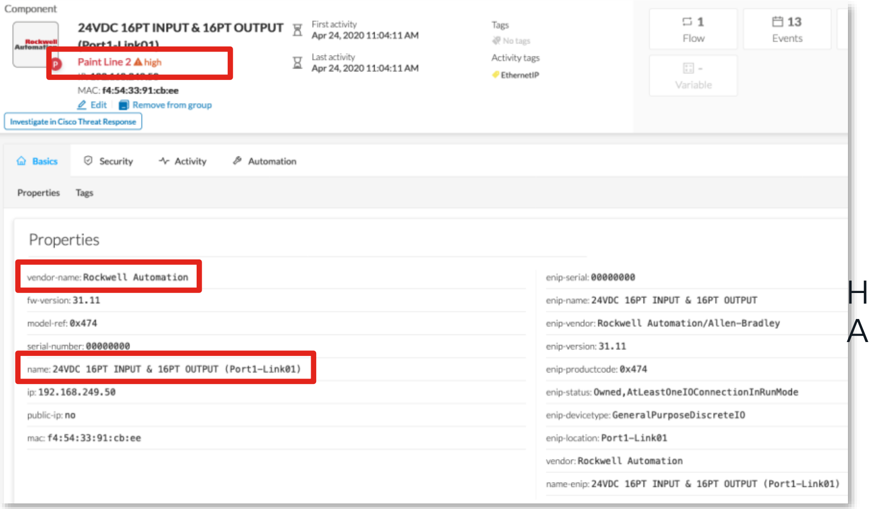
Enrich hosts information in Cisco Secure Analytics with rich context from Cyber Vision

Easily identify flows mapped to industrial endpoints with Cyber Vision informed host-group attributes

Create alert policies to identify and alert on inter-zone communications

Cyber Vision helps Secure Analytics investigate and detect threats in industrial networks

Secure Analytics Dynamic Host Groups



Component

24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)

Paint Line 2 ⚠ high

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

Edit | Remove from group

Investigate in Cisco Threat Response

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

Last activity: Apr 24, 2020 11:04:11 AM

Tags: No tags

Activity tags: EthernetIP

1 Flow | 13 Events | - Variable

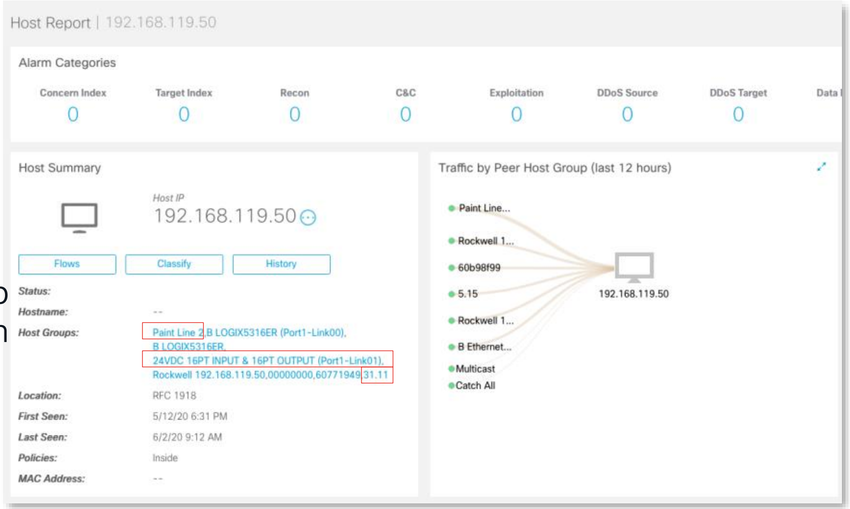
Basics | Security | Activity | Automation

Properties | Tags

Properties

vendor-name: Rockwell Automation	enip-serial: 00000000
fw-version: 31.11	enip-name: 24VDC 16PT INPUT & 16PT OUTPUT
model-ref: 0x474	enip-vendor: Rockwell Automation/Allen-Bradley
serial-number: 00000000	enip-version: 31.11
name: 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)	enip-productcode: 0x474
ip: 192.168.249.50	enip-status: Owned,AtLeastOneIOConnectionInRunMode
public-ip: no	enip-devicetype: GeneralPurposeDiscreteIO
mac: f4:54:33:91:cb:ee	enip-location: Port1-Link01
	vendor: Rockwell Automation
	name-enip: 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)

Host Group Automation



Host Report | 192.168.119.50

Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target
0	0	0	0	0	0	0

Host Summary

Host IP: 192.168.119.50

Flows | Classify | History

Status:

Hostname: --

Host Groups: Paint Line 2,B LOGIX5316ER (Port1-Link00), B LOGIX5316ER, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01), Rockwell 192.168.119.50,00000000,60771949,31.11

Location: RFC 1918

First Seen: 5/12/20 6:31 PM

Last Seen: 6/2/20 9:12 AM

Policies: Inside

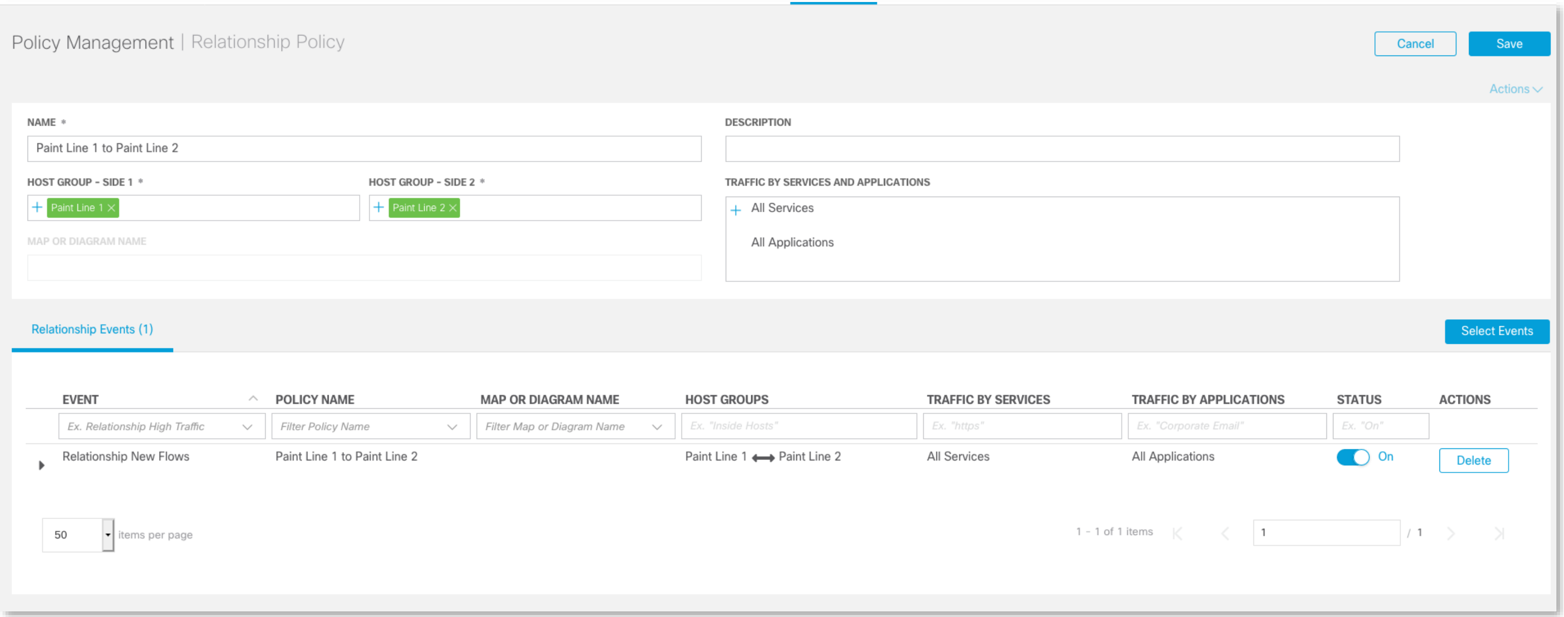
MAC Address: --

Traffic by Peer Host Group (last 12 hours)

Cyber Vision identifies attributes of assets via industrial Deep Packet Inspection

Dynamic Host Groups are created and devices as assigned via Host Group Automation API

Secure Analytics Relationship Policies

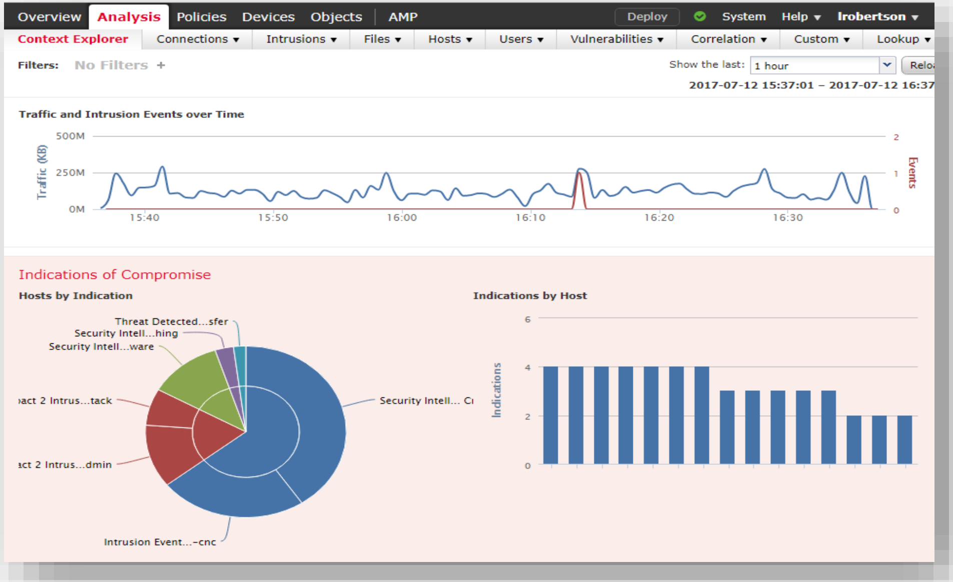


NAME *	Paint Line 1 to Paint Line 2
DESCRIPTION	
HOST GROUP - SIDE 1 *	Paint Line 1
HOST GROUP - SIDE 2 *	Paint Line 2
MAP OR DIAGRAM NAME	
TRAFFIC BY SERVICES AND APPLICATIONS	All Services All Applications

EVENT	POLICY NAME	MAP OR DIAGRAM NAME	HOST GROUPS	TRAFFIC BY SERVICES	TRAFFIC BY APPLICATIONS	STATUS	ACTIONS
Relationship New Flows	Paint Line 1 to Paint Line 2		Paint Line 1 ⟷ Paint Line 2	All Services	All Applications	On	Delete

Create custom alerts based on attributes from Cyber Vision including Groups – ie. Paint Line 1 should never talk to Paint Line 2

Secure Firewall Management Center Integration

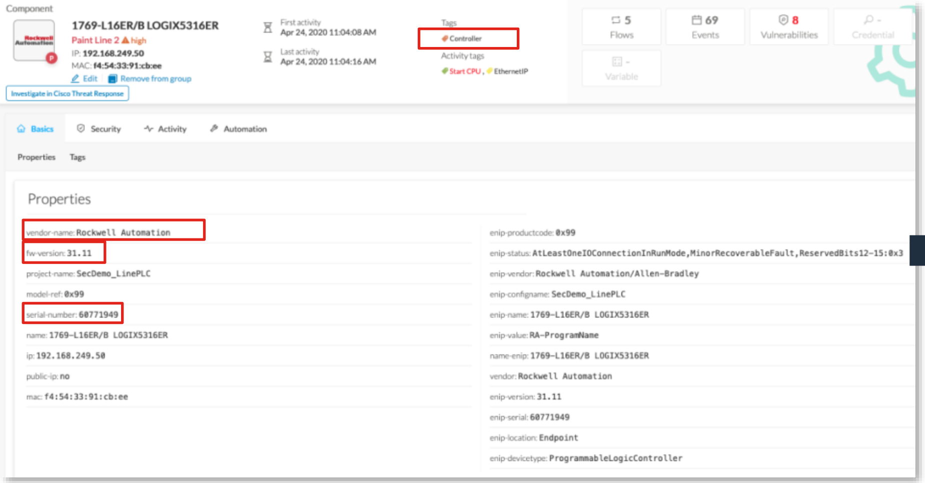


Map **ICS device identity** to Hosts in Firepower for use in Secure Firewall correlation policy

Identify anomalous flows in Cyber Vision and **kill FTD Firewall sessions**

Leverage Host Attributes from Cyber Vision to alert on unexpected behavior

Firewall Management Center Host Attributes



1769-L16ER/B LOGIX5316ER
Paint Line 2 high
IP: 192.168.249.50
MAC: f4:54:33:91:cb:ee

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

Last activity
Apr 24, 2020 11:04:16 AM

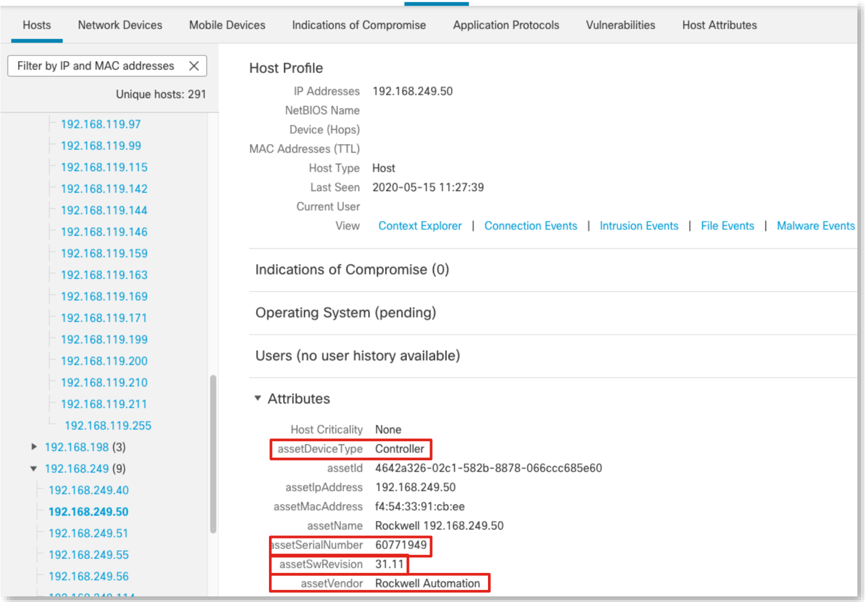
Tags
Controller

Activity tags
Start CPU , EthernetIP

Properties

```
vendor-name: Rockwell Automation
fw-version: 31.11
project-name: SecDemo_LinePLC
model-ref: 0x99
serial-number: 60771949
name: 1769-L16ER/B LOGIX5316ER
ip: 192.168.249.50
public-ip: no
mac: f4:54:33:91:cb:ee

enip-productcode: 0x99
enip-status: AtLeastOneIOConnectionInRunMode,MinorRecoverableFault,ReservedBits12-15:0x3
enip-vendor: Rockwell Automation/Allen-Bradley
enip-configname: SecDemo_LinePLC
enip-name: 1769-L16ER/B LOGIX5316ER
enip-value: RA-ProgramName
name-enip: 1769-L16ER/B LOGIX5316ER
vendor: Rockwell Automation
enip-version: 31.11
enip-serial: 60771949
enip-location: Endpoint
enip-devicetype: ProgrammableLogicController
```



Unique hosts: 291

192.168.119.97
192.168.119.99
192.168.119.115
192.168.119.142
192.168.119.144
192.168.119.146
192.168.119.159
192.168.119.163
192.168.119.169
192.168.119.171
192.168.119.199
192.168.119.200
192.168.119.210
192.168.119.211
192.168.119.255
▸ 192.168.198 (3)
▾ 192.168.249 (9)
192.168.249.40
192.168.249.50
192.168.249.51
192.168.249.55
192.168.249.56

Host Profile

IP Addresses	192.168.249.50
NetBIOS Name	
Device (Hops)	
MAC Addresses (TTL)	
Host Type	Host
Last Seen	2020-05-15 11:27:39
Current User	
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (0)

Operating System (pending)

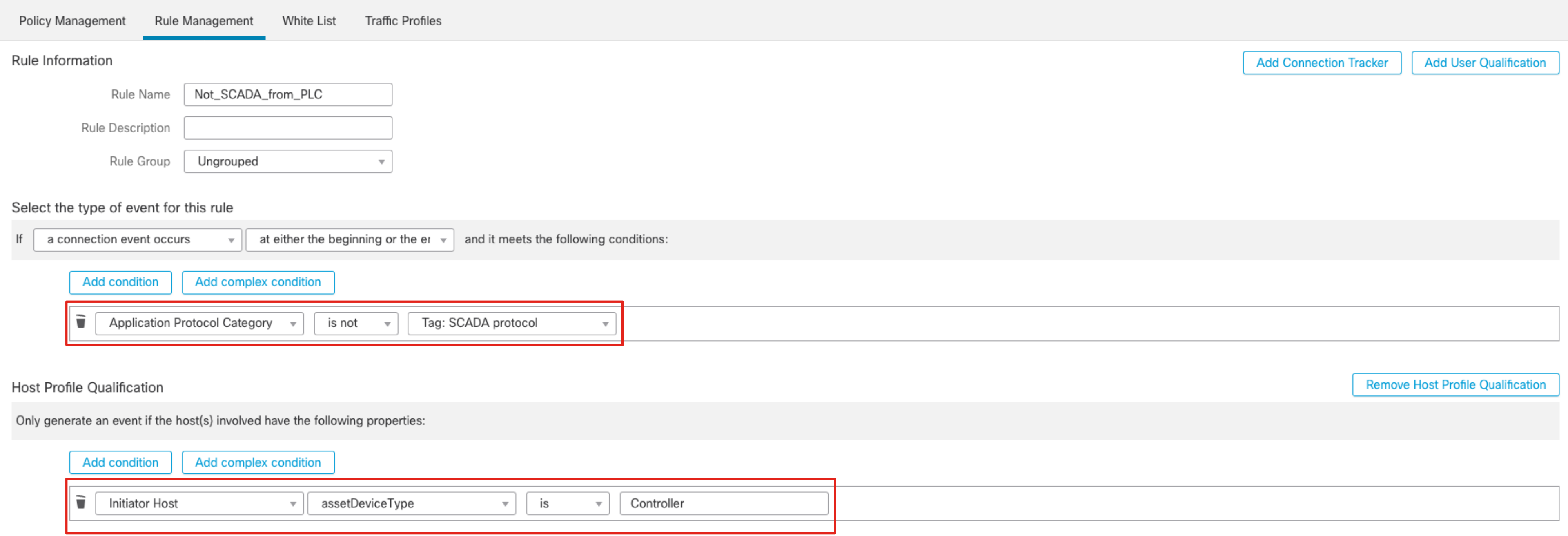
Users (no user history available)

▾ Attributes

Host Criticality	None
assetDeviceType	Controller
assetId	4642a326-02c1-582b-8878-066ccc685e60
assetIpAddress	192.168.249.50
assetMacAddress	f4:54:33:91:cb:ee
assetName	Rockwell 192.168.249.50
assetSerialNumber	60771949
assetSwRevision	31.11
assetVendor	Rockwell Automation

- Cyber Vision populates Host Attributes in Firewall Management Center
- FMC can leverage attributes for policies to alert and enforce

Firewall Management Center Correlation Policy



Rule Information

Rule Name: Not_SCADA_from_PLC

Rule Description:

Rule Group: Ungrouped

Select the type of event for this rule

If a connection event occurs at either the beginning or the er and it meets the following conditions:

Application Protocol Category is not Tag: SCADA protocol

Host Profile Qualification

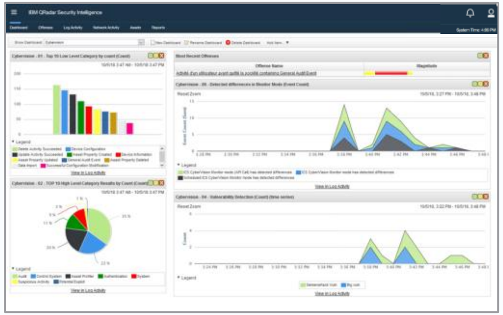
Only generate an event if the host(s) involved have the following properties:

Initiator Host assetDeviceType is Controller

Leverage Host Attributes from Cyber Vision to alert on unexpected behavior
ie – Controller communicating using unexpected protocols

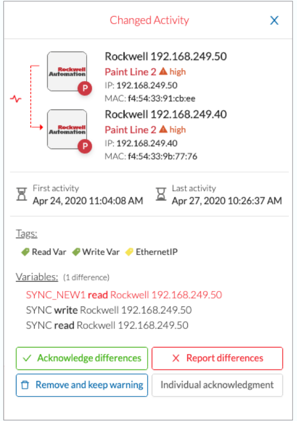
Investigate industrial events in the IT SOC

Get alerts on SIEM in the SOC



Get alerted to incidents in the industrial network at the IT SOC by streaming syslog events from Cyber Vision to your SIEM

View Details in Cyber Vision



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

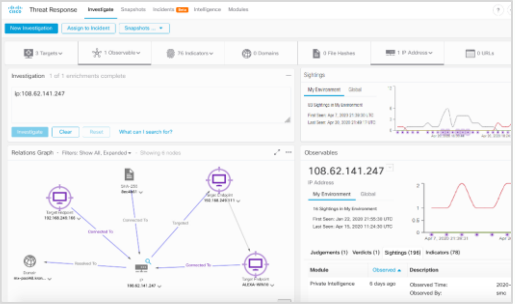
Last activity
Apr 27, 2020 10:26:37 AM

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

Pivot to the corresponding instance of Cyber Vision to get more details on the event that generated the alert

Launch investigation is SecureX



Promote the event to SecureX incident manager and investigate the threat with enrichment from Cisco and 3rd party security products

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.

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)

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

Connect, Automate, and Operate Anywhere

Introducing new wireless and remote operational capabilities from Cisco IoT

Learn how Cisco’s newest industrial wireless and operation tools enable organizations to securely connect, automate and operate at scale.

Join us on June 21st for this 35-minute webinar where we will discuss:

- How to meet new requirements in wireless networking and security
- How operational networks can benefit from enterprise-grade capabilities
- The latest Cisco innovations in industrial wireless technology from Wi-Fi 6 to fiber-like wireless connectivity
- Improving IT and OT more efficiently through better visibility and enhanced tools to enable operations from anywhere

Thank you

cisco Live!

#CiscoLive