

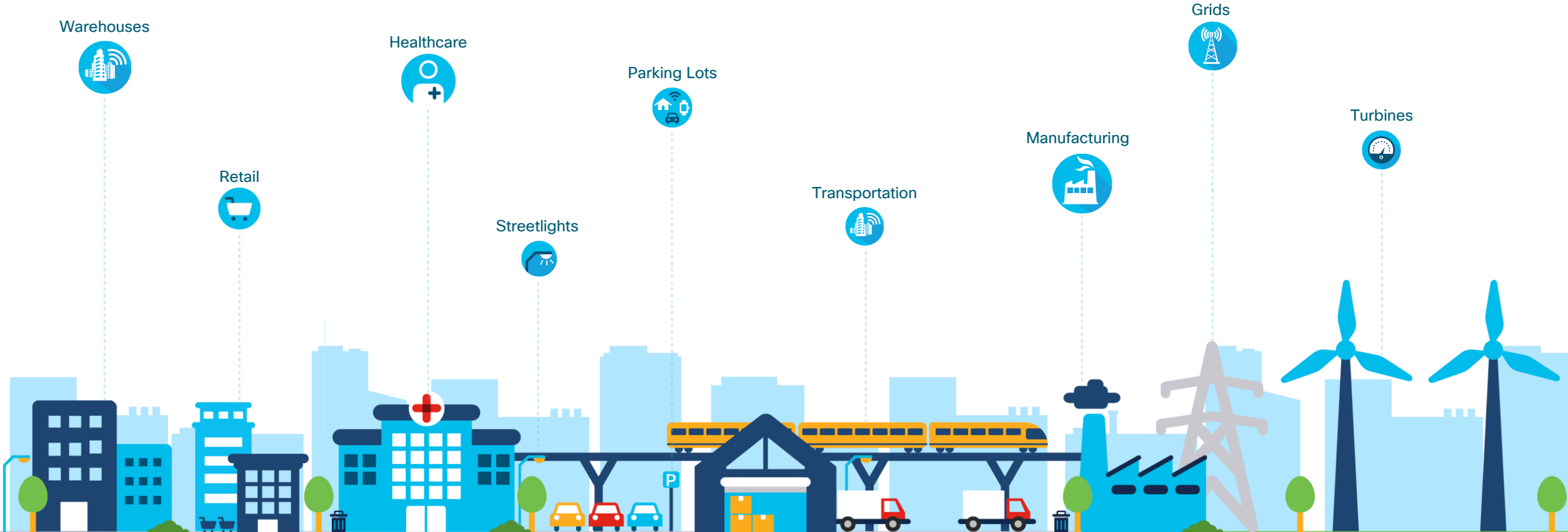
Quint@sQuinze

Sistema de Segurança Industrial e Novidades do Cisco Cyber Vision 4.0

Julio Cesar Gouy – TSA IoT LATAM & Field Advisor – CCIE#8863
August 2021



Every industry is going through **digital transformation** ...every “thing” is getting connected



Digitization is accelerating **seamless movement of data across Enterprise**



68%

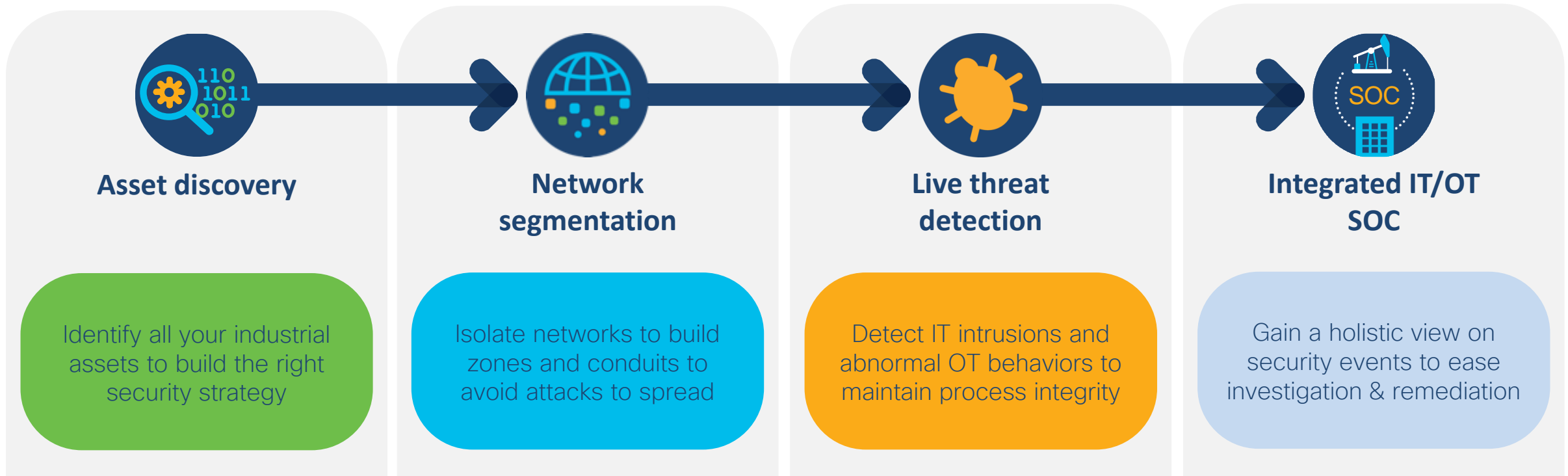
Security is the biggest challenge for IoT deployments

Digitization *Increases* **The Attack Surface**

The IIoT Security Journey



The **4-step journey** to secure your industrial network



Cisco's integrated security portfolio helps customers through this journey

You cannot secure what you don't know

55% have no or low confidence that they know all devices in their network



List all the assets you are defending



Identify asset communication issues



Detect bypass or leaks in the IDMZ



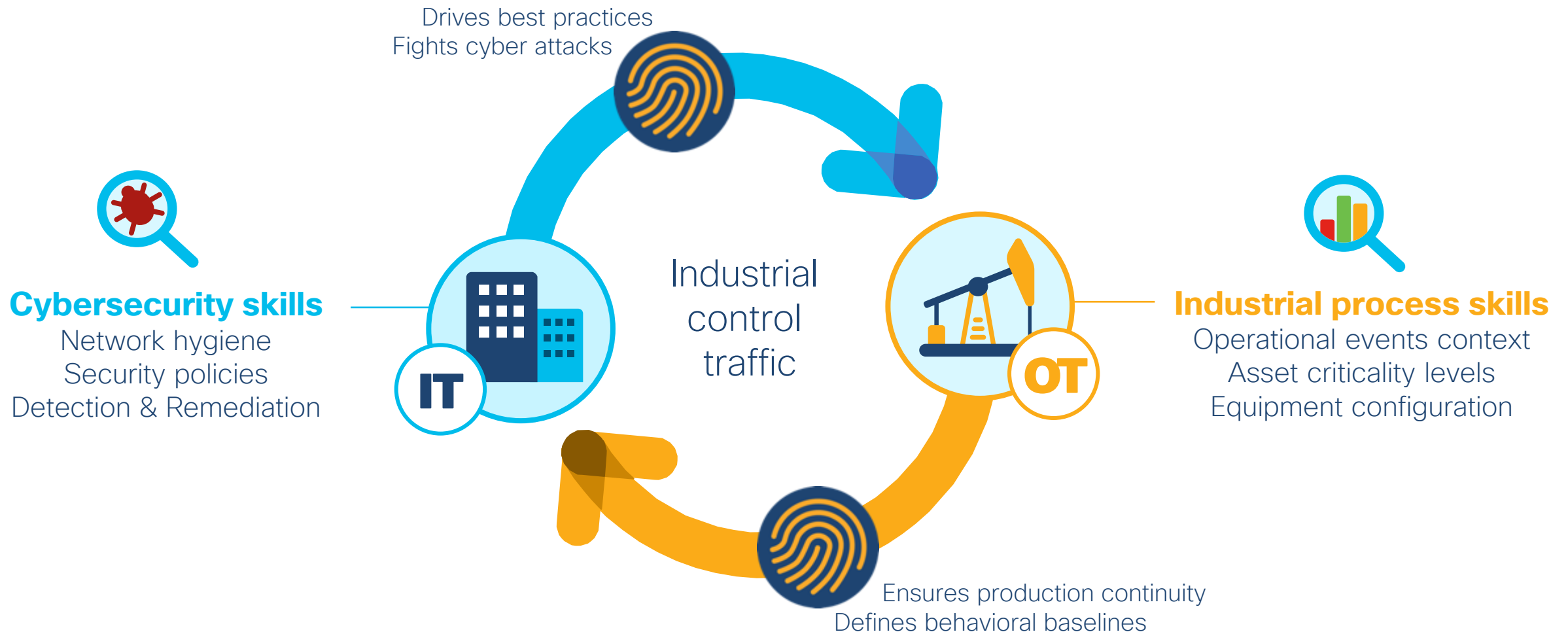
Spot vulnerable assets



Build compliance reports

Gain visibility to take corrective actions, segment networks, build security policies and drive best practices

Need visibility to enable **IT-OT collaboration**



Kick-start your Industrial IoT security project

Cisco & Partners assessment service gives you a comprehensive picture of your industrial security posture so you can build your project plan



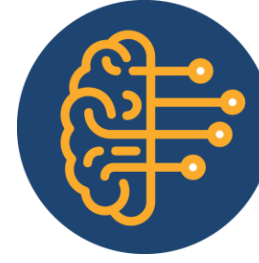
Industrial Asset
Inventory



Vulnerability
Detection



Communication
Maps



Actionable
Insights



Detailed
Reports

Asset discovery and assessment service led by Cisco OT & Partners Security experts

Cisco Cyber Vision

Visibility & Threat Detection for the Industrial IoT

Protect your industrial control systems against cyber risks



Visibility

Asset inventory
Device vulnerabilities
Risk scoring



Operational Insights

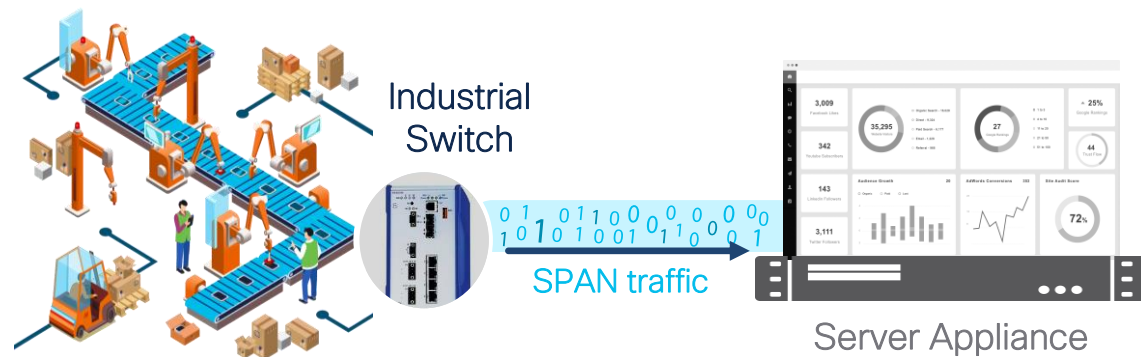
Track process/device modifications
Record control system events
Map communication patterns



Threat Detection

Behavioral anomaly detection
Snort IDS with Talos signatures
SecureX threat investigation

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

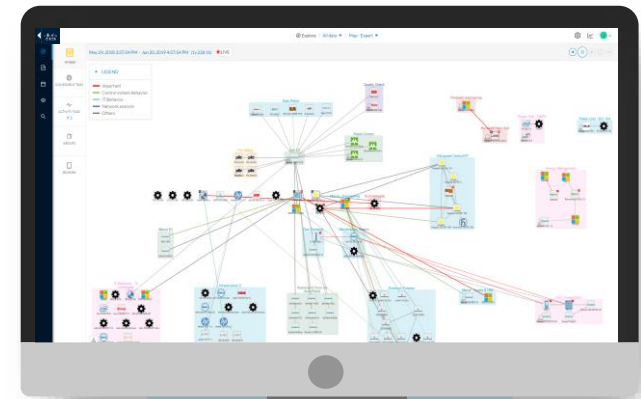
TCO of SPAN based solutions is **not** sustainable over long-term growth

Enlist your OT network for security



Cisco Industrial Ethernet switches and gateways give you visibility into assets and processes to **protect against cyber risk** and **reduce downtime**

Cyber Vision Center



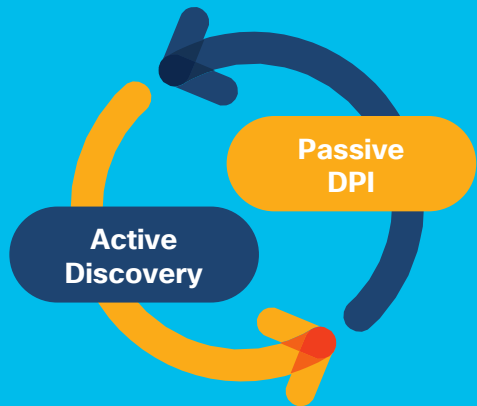
1 0 0 1
0 0 1
Application Flow

Cyber Vision Sensor

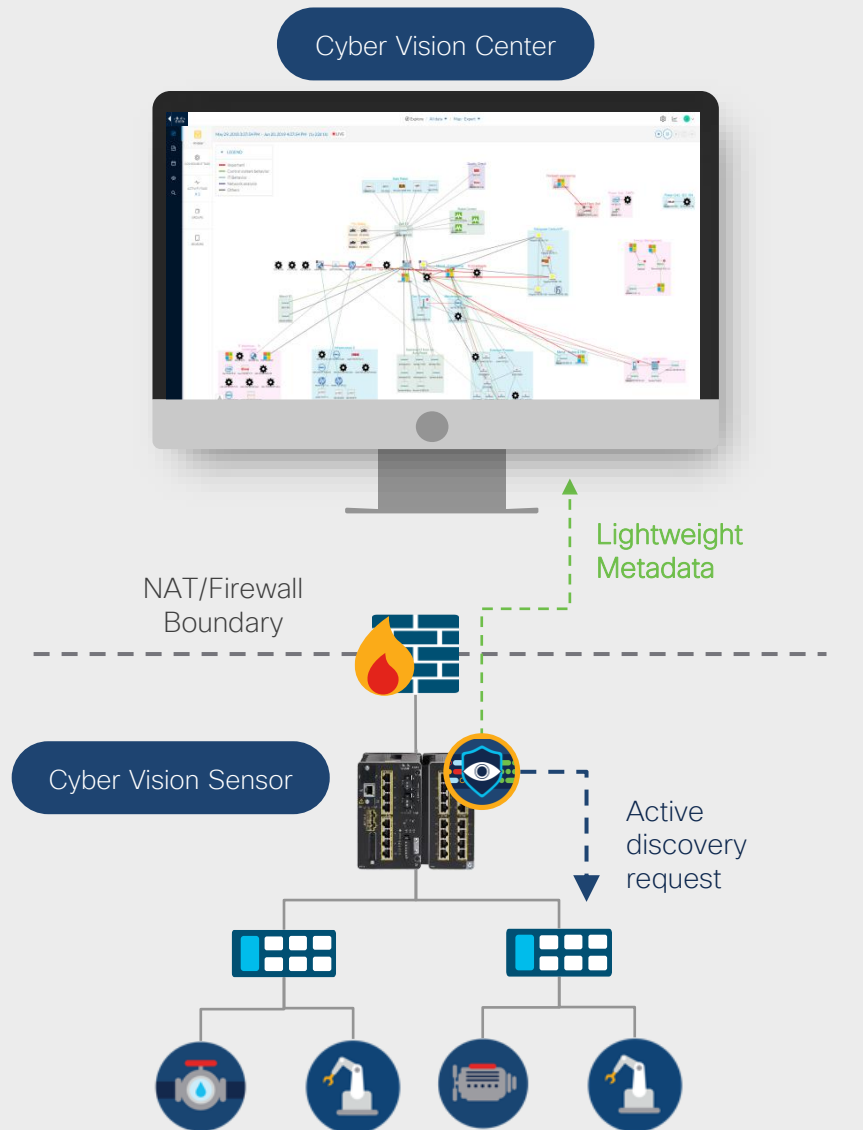


Industrial protocol Deep Packet Inspection built into your network infrastructure

Distributed Edge Active Discovery



Closed-loop control between Passive DPI and **Active Discovery by Distributed Sensor** provides **100% Visibility**



Targeted communication without scanning
See below NAT and Firewall boundaries



Asset Inventory

Comprehensive up to date inventory of all assets in your environment



Vulnerability Detection

Identify known asset vulnerabilities so you can patch them before they are exploited



Risk Scoring

Asset risk scoring based on impact and likelihood to help you improve compliance

The screenshot displays the Cisco Cyber Vision dashboard with three main sections highlighted by blue callouts:

- Asset Inventory:** Shows details for a component named '1769-L16ER/B LOGIX5 316ER' with IP 192.168.249.50. It lists first and last activity, tags like 'Controller', 'Rockwell Automation', and 'Stop CPU', and activity tags like 'Read Var' and 'Write Var'.
- Vulnerability Detection:** Shows 73 vulnerabilities for the 192.168.1 subnet. A donut chart indicates 10 most matched vulnerabilities. A table lists CVEs such as CVE-2018-5627, CVE-2017-2680, and CVE-2017-12741, along with their CVSS scores and affected components.
- Risk Scores:** Shows a risk score of 69 for device SCS0102. A bar chart compares the current risk score (69) to the achievable risk score (44). A table details the criteria for the score, including device type, group impact, and vulnerabilities.

Cisco Cyber Vision



Communication Patterns

Dynamic communication map with detailed application flow level information



Control System Activities

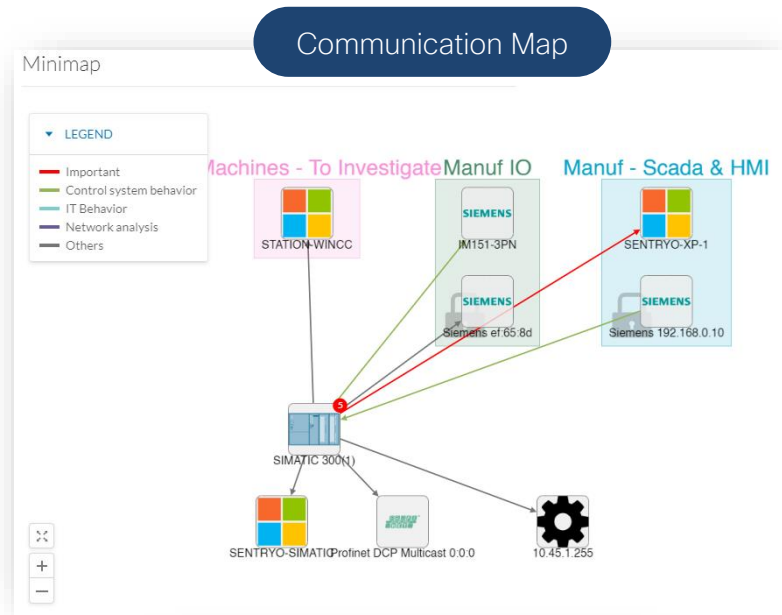
Track process modifications
Identify configuration changes
Record control system events



Variable Access

See which variables, objects, setpoints are being accessed or modified

Gain Operational Insights



Application Flows

Device	Device	First activity
Vmware 192.168.198.203	DESKTOP-GBJUF2N	Apr 20, 2021 9:32:14 AM
DESKTOP-GBJUF2N	1769-L16ER/B LOGIX5316ER	Apr 20, 2021 9:20:06 AM
DESKTOP-GBJUF2N	192.168.249.255	Apr 20, 2021 9:20:08 AM
DESKTOP-GBJUF2N	1734-AENTR/B Ethernet Adapter	Apr 20, 2021 9:20:06 AM
DESKTOP-GBJUF2N	255.255.255.255	Apr 20, 2021 9:20:06 AM

Control System Activities

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 CPU, Read Var, Write Var, ARP, S7Plus (hide)

Variable / Setpoint Access

Variables accesses

Variable	Types	Accessed by	First access
> M 2.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM
▼ M 2.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM
	READ	Siemens 192.168.0.10	Apr 6, 2017 11:29:22 PM
	READ	SENTRYO-XP-1	Apr 6, 2017 11:29:22 PM
> M 8.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM
> M 8.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM
> M 8.2	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM

Cisco Cyber Vision



Anomaly Detection

Detect attempts to modify OT assets with behavioral analytics, create baselines to detect deviations



Intrusion Detection

Detect malicious intrusions with snort IDS and Talos threat intelligence



Threat Investigation

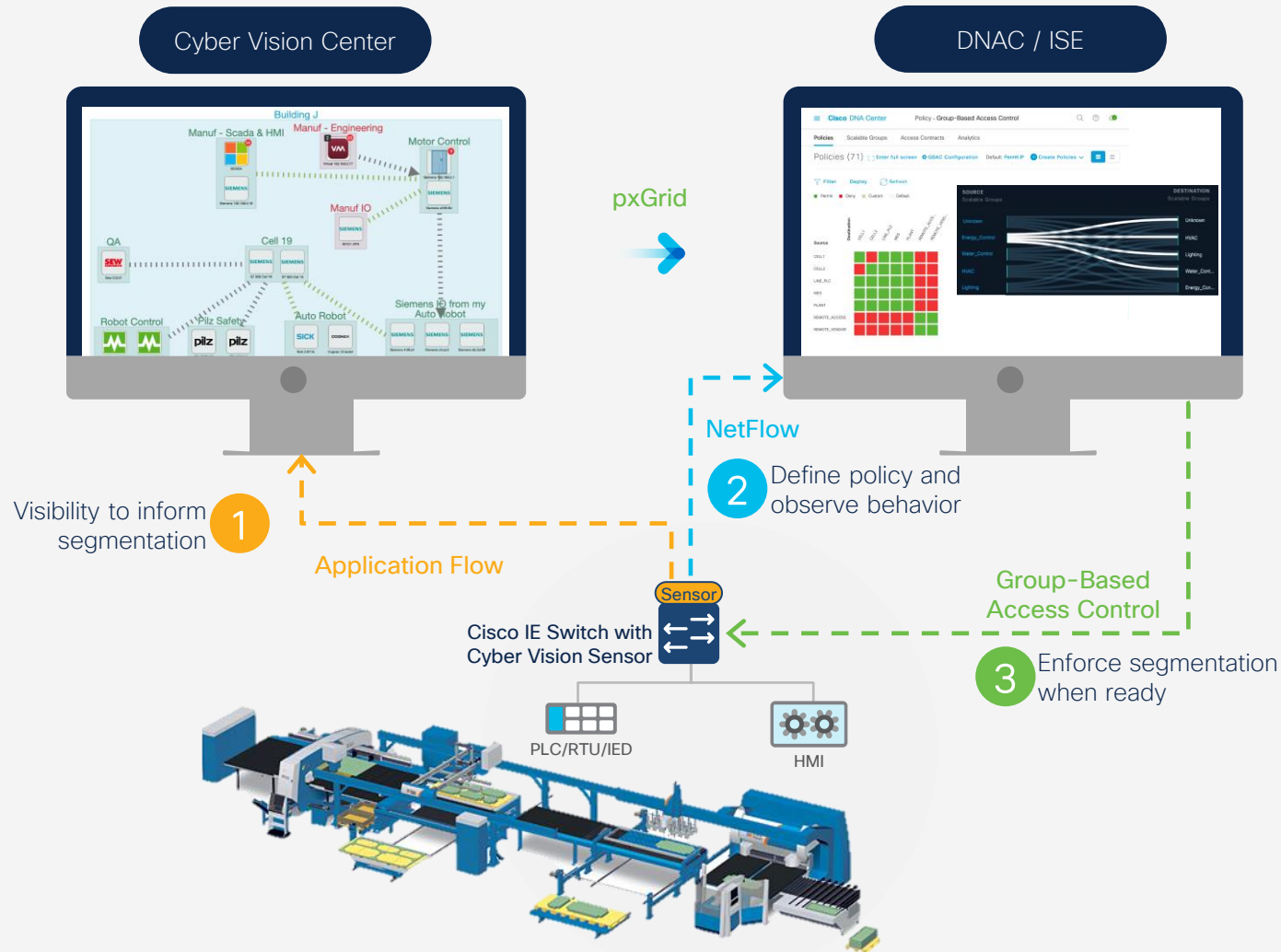
Investigate events in SecureX incident manager with enrichment from Cisco and 3rd party security products

Detect & Investigate Threats

The screenshot displays the Cisco Cyber Vision interface, which is divided into three main sections:

- Anomaly Detection:** This panel shows a list of detected anomalies. Two entries are visible, both labeled "Rockwell Automation" and "Paint Line 2" with a high severity. The first entry has IP: 192.168.249.50 and MAC: f4:54:33:91:cb:ee. The second entry has IP: 192.168.249.40 and MAC: f4:54:33:9b:77:76. A "Variables" section is highlighted with a red box, showing: SYNC_NEW1 read Rockwell 192.168.249.50, SYNC write Rockwell 192.168.249.50, and SYNC read Rockwell 192.168.249.50. Below this, there are buttons for "Acknowledge differences", "Report difference", and "Remove and keep warning".
- Intrusion Detection:** This panel shows a list of intrusion events. Two events are visible, both labeled "Signature based Detection". The first event is "Snort allow on TCP of 27679 with signature A Network Trojan was detected" and the second is "Snort allow on TCP of 42339 with signature Attempted Information Leak". Each event includes details such as "Occurred at", "Sensor", "Action", "Gid", "Signature ID", "Priority", "Rule", and "Classification".
- Threat Investigation:** This panel shows a detailed view of a threat event. The event is titled "Control system event: Stop CPU command has been detected from...". It includes a "Summary" tab, "Observables", "Timeline", and "Sightings" tabs. The "Sightings" tab is active, showing the event details: Source: Cisco Cyber Vision, Sensor: Network Sensor, IP Address: 192.168.249.114, and device: 192.168.249.50. The event is categorized as "High" severity and "Amber" TLP. A "Targets" section shows the IP address 192.168.249.50, which is linked to the "IP Address" field in the "Observables" section. A "Relations" section shows the IP address 192.168.249.114 connected to the IP address 192.168.249.50.

Segment your network with Visibility & Analytics



Visualize Zones & Conduits

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



Dynamic SGT Mapping

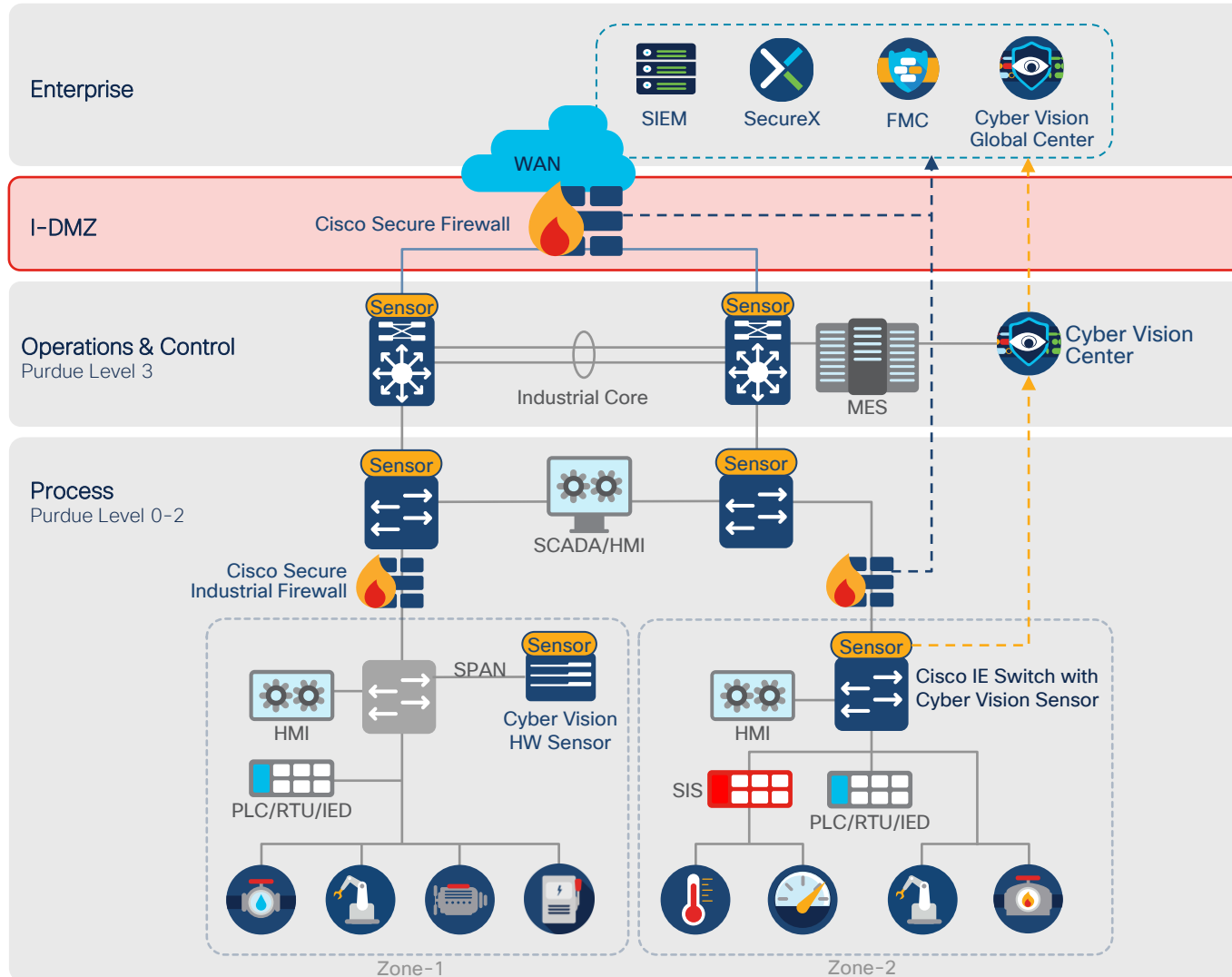
Cyber Vision grouping results in dynamic Group-based policy assignment to endpoints through ISE



Monitor Before Enforcement

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

Extend security operations to OT



Protect your industrial processes with macro & micro segmentation built into the industrial network



Share context from the industrial network with the enterprise SOC



Detect, investigate, and remediate across IT-OT integrated security technologies



Reduce time spent on investigations with common aggregated threat intelligence

Cyber Vision has the OT information the SOC needs

Visibility

Provides **OT context**, asset inventory and communications map to your SOC

Risks

Identify asset vulnerabilities and **assess risks** to prioritize actions

Intrusions

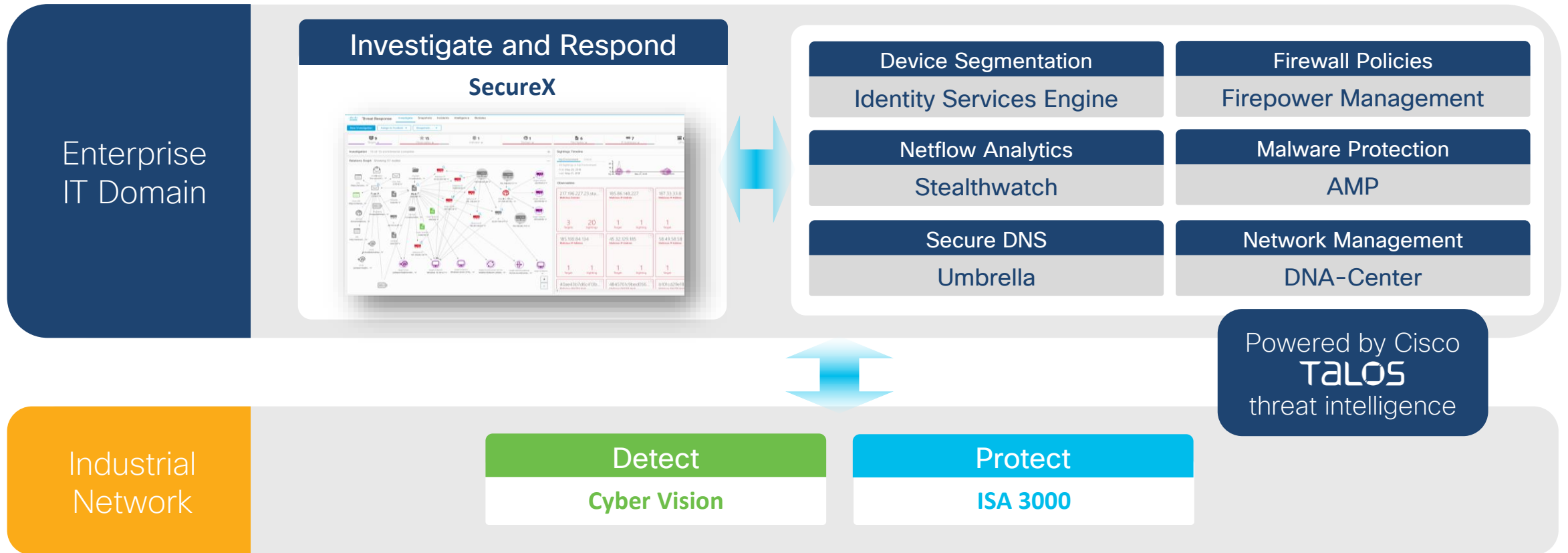
Leverages Talos signatures to detect known and emerging **IT attacks**

Anomalies

Monitor mode detects **malicious behaviors** and unknown attacks

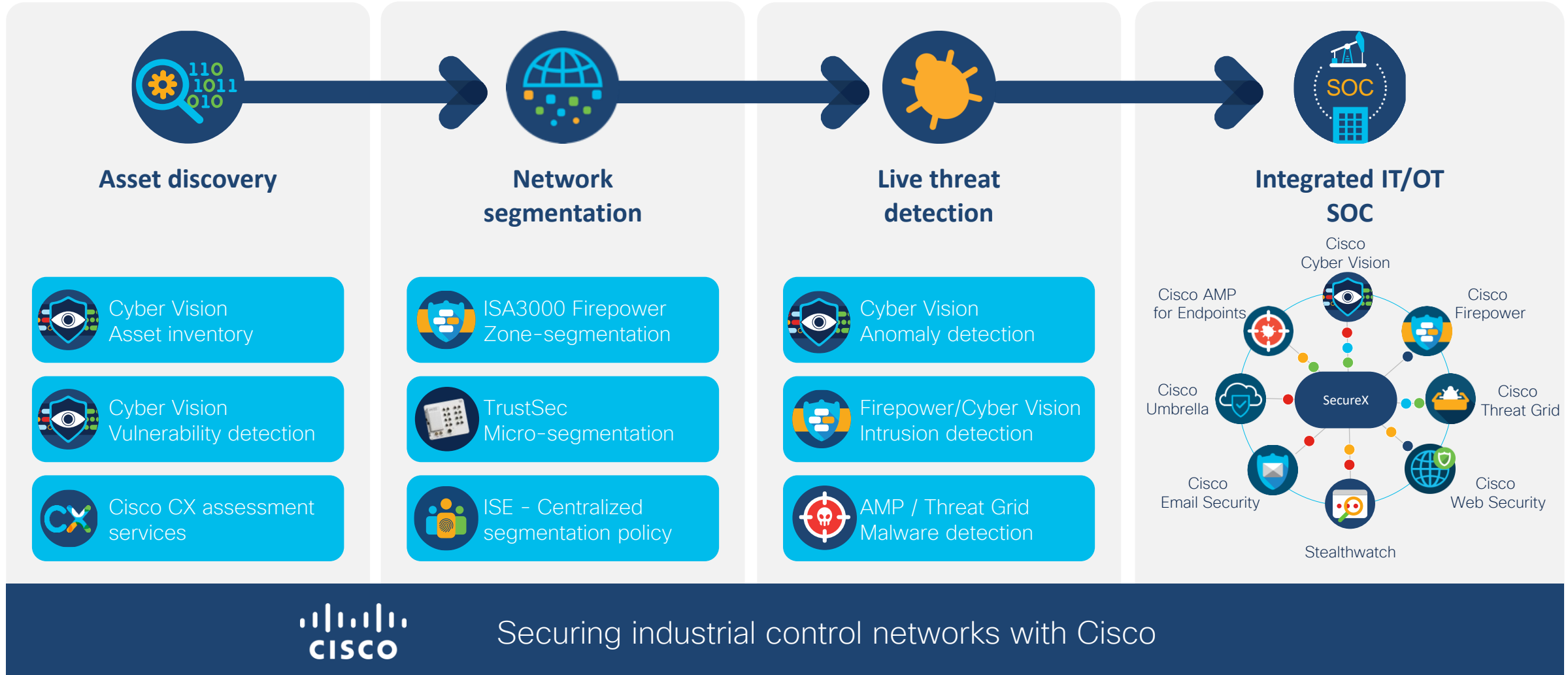
OT events and context shared with your SIEM and IT security platforms

Cisco's fully integrated IT-OT security solution



Cisco Security for Industrial IoT

The **4-step journey** to secure your industrial network



Securing industrial control networks with Cisco

Bring Cisco Scale and Simplicity to IIoT Security



Cisco Industrial Networks

Connect anything anywhere



Cisco Security

Comprehensive IT/OT cybersecurity



Cisco Validated Designs

State-of-the-art architecture guides



Cisco Customer Services

Human skills to enable deployments

All working together for successful Industrial IoT security deployments



What's new in Cyber Vision 4.0

Enhanced Insights and Security Posture Identification



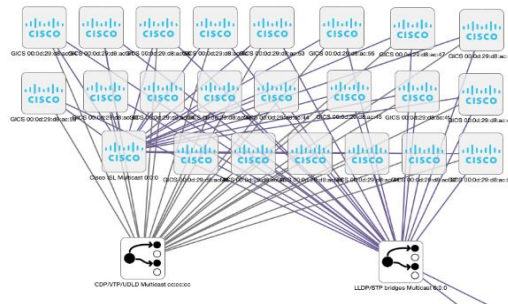
Enhanced Visibility



Understanding Components vs. Devices

Cyber Vision 3.x was listing **Components**

- Hardware identified by a MAC or IP addresses or Slot IDs
- Can be directly related to the network logic of the OT process



Catalyst switch in 3.0



Cyber Vision 4.0 now lists **Devices**

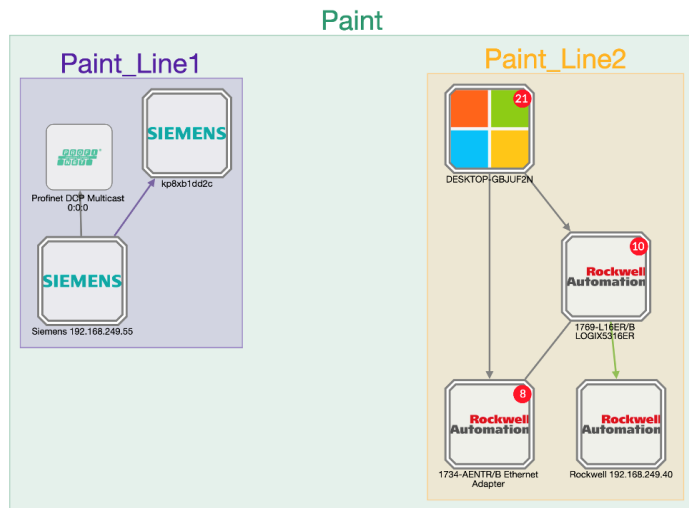
- Physical devices made of several components
- Can be directly related to the device performing a certain task in the industrial process



Catalyst switch in 4.0

Enhanced device aggregation

Map view



New double-border icons indicate a device

ID Cards

Controller Rack

1769-L16ER/B LOGIX53...
Paint_Line2 ▲ high
IP: 192.168.249.50
MAC: f4:54:33:91:cb:ee

First activity: Apr 28, 2021 11:48:40 AM
Last activity: Apr 28, 2021 11:48:46 AM

Sensor: -

Tags: ● Controller, ● Rockwell Automation

Activity tags: ● Read Var, ● Write Var, ● Low Volume, ● CIP-IO, ● EthernetIP

Risk score: 80% [See details](#)

Modules:

- Rockwell 192.168.249.50
- Rockwell 192.168.249.50
- Rockwell 192.168.249.50
- Rockwell 192.168.249.50
- 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)
- Rockwell 192.168.249.50
- 1769-L16ER/B LOGIX5316ER
- SecDemo_LinePLC | 1769-L16ER/B LOGIX5316ER
- Rockwell 192.168.249.50

Properties:

fw-version: 31.011
ip: 192.168.249.50
mac: f4:54:33:91:cb:ee
model-ref: 24VDC 16PT INPUT & 16PT OUTPUT, 1769-L16ER/B LOGIX5316ER
name: Rockwell 192.168.249.50, 24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01), 1769-L16ER/B LOGIX5316ER...
[... show more](#)

Technical Sheets

8 Components

Component	First activity	Last activity	IP	MAC	Tags	Vulnerabilities	Flows	VLAN ID	Sensor
1756-L55/A 1756-M12/A LOGIX5555 (Port1-Link00)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	Controller	2	-10	-	
1756-OB16I/A DCOUT ISOL (Port1-Link04)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	
1756-IB16I/A DCIN ISOL (Port1-Link03)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	
1756-IB16I/A DCIN ISOL (Port1-Link02)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	
1756-OB16I/A DCOUT ISOL (Port1-Link05)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	
SUBSTATION-119-PLC01	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	9	-10	-	
1756-ENB/A (Port1-Link01)	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	9	-10	-	
Rockwell 192.168.0.200	Oct 11, 2019 11:12:58 AM	May 24, 2021 12:32:15 PM	192.168.0.200	00:00:bc:5f:bc:ce	No tags	0	-10	-	

Easily list the components of a device. Click on a component to view more details

Consolidating components into devices

- Devices match the customer's industrial processes
 - More natural for non-technical users
 - Reduced complexity when looking at large inventories/maps
- Optimized database storage

Enhanced Performance



Many changes under the hood to boost performance



8x faster data ingestion



Speedy UI even with large datasets



Smarter data retention to avoid disk saturation

Cyber Vision 4.0 lays the foundation for large scale deployments

Enhanced Security Insights

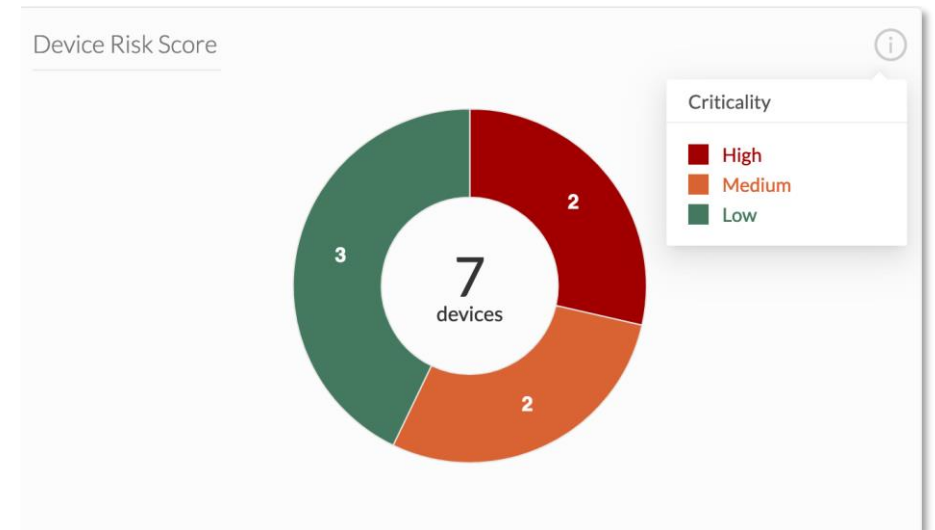


Tracking Security Events in 4.0

- Risk scoring
- Network boundaries
- New dashboards
- New vulnerability detection
- New protocol support
- New activity tags
- Splunk integration

Risk scoring helps focus on what's important

- Guides non-expert users to devices they should deal with first
- A first step in security management to help make urgent decisions
- Provides simple information on the security posture



Defining the Cyber Vision Risk Scores

- Risk = Likelihood x Impact
- Likelihood
 - Activity tags (some communications create more risks)
 - Exposure to external IP addresses
 - Discovered vulnerabilities
- Impact
 - Device tags (some devices can create more damages)
 - User-defined industrial impact for groups

Impact	Critical	High	High	High	High
	high	negligible	Significant	High	High
	limited	negligible	negligible	Significant	Significant
	No impact	negligible	negligible	negligible	negligible
		Minimal	Significant	High	Maximal
		Likelihood			

Source: EBIOS

Understanding a Device Risk Score

The screenshot displays the Cisco Cyber Vision interface for a device named SCS0102. The device is identified as 'Building K' with a 'very high' risk level. Key details include IP: 192.168.1.4 (+ 1 other) and MAC: 00:00:64:8c:86:08 (+ 1 other). The interface shows a current risk score of 69 and an achievable risk score of 44. A bar chart compares these scores, with a note that the achievable score can be reached by patching vulnerabilities and removing insecure traffic. The 'Details' section provides a breakdown of the score based on criteria: Device type (13%), Group impact (51%), Activities (0%), and Vulnerabilities (36%). The most impacting vulnerability is 'Path Traversal Vulnerability in Yokogawa CENTUM' with a CVSS score of 9.8. A gear icon in the top right corner is highlighted, indicating a focus on understanding what impacts the risk score.

Criteria	Matching	Distribution	Description
Device type	SCS0102 type: Controller	13%	CC key element. Compromise 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 see... show more See details

Understanding how to lower risk

Understanding what impacts the risk score

DPI Enhancements: Protocol Decoding

Cyber Vision 4.0 decodes the NTCIP protocol (North America Roadways)

Improvements to existing protocol support:

- Emerson ROC+ (Utilities)
- Yokogawa DCS (Chemicals and Oil&Gas)
- Ethernet/IP (Manufacturing)

Active Discovery can now send queries using ICMPv6

Now also detecting vulnerabilities on network equipment

Cyber Vision 4.0 detects vulnerabilities on switches, routers and firewalls from:

- Hirschmann
- Moxa
- Siemens
- Cisco

Splunk's OT Security Add On

The screenshot displays the Splunk Enterprise Security interface for the OT Asset Investigator. The top navigation bar includes 'splunk-enterprise', 'App: Enterprise Security', and various user and system menus. The main content area is titled 'OT Asset Investigator' and shows search filters for 'Investigating Asset' (172.100.104.98) and 'Time Window' (Last 24 hours). Below this, there's a section for 'OT Asset Information' with a table of asset details.

Asset	Hostname	Priority	ID	Type	Vendor Model	Status	System	Version	Site ID	Location
dcc_js81.ples.local 172.100.104.98 8d:1e:15:10:04:5c dcc_js81	dcc_js81	high		remote access	hewlett packard : proliant d1300	operational	ppit		pleasanton plant	pleasanton plant

Below the table, there are four key metrics:

- Asset Risk Score Changes: 220 (up arrow)
- Total number of Hosts in Communication: 425 (up arrow, 25 change)
- Total number of network ports accessed: 550 (up arrow, 309 change)
- Total number of sessions: 7,306 (up arrow, 5,569 change)

The bottom section shows 'Subnets in Communication' with a table of destination subnets and their counts/percentages, and a 'Session Traffic Analysis' diagram.

dest	count	percent
173.16.2	1850	29.110797
173.16.1	1493	26.340861
10.11.36	778	13.585039
172.104.1	574	10.127829
173.16.0	563	9.932957
172.100.1	317	5.92802
172.104.104	77	1.358504
172.105.1	69	1.217361
172.110.1	54	0.952717
172.100.15	18	0.317572

- Expands Splunk's capabilities across IT and OT environments
- OT centric view of assets
- NERC CIP compliance reporting
- MITRE ICS correlation rules
- Integration with enterprise security

SecureX Incidents



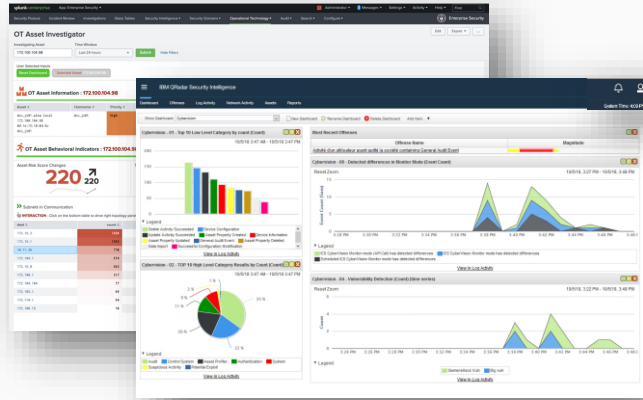
Simplify IT/OT threat hunting with Cisco SecureX



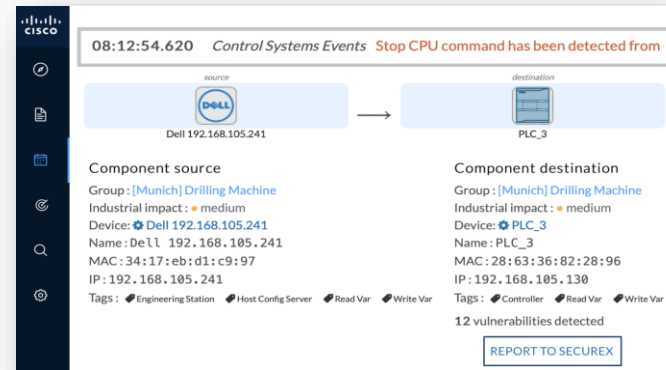
- Cyber Vision with SecureX enables a converged IT/OT threat management strategy
- Makes it easy for OT to share relevant threat intel with IT/Security analysts
- ‘One-click’ promotion of Cyber Vision security events for further investigation on SecureX
 - Signature-based detection events
 - Control systems events
 - Anomaly detection events

Investigate Industrial Events in your IT SOC

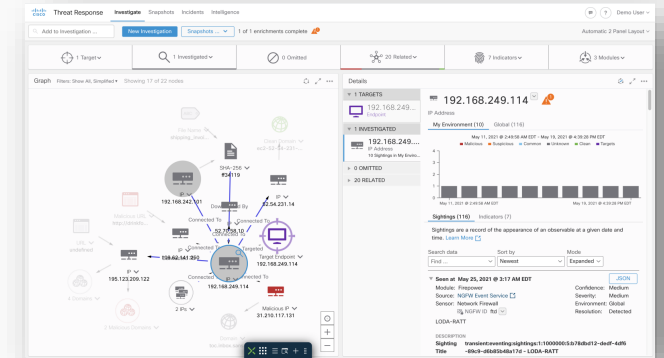
Cyber Vision Apps for Splunk & QRadar



Cyber Vision



SecureX



1

Get alerted to incidents in the industrial network in your SIEM through syslog and API integration with Cyber Vision

2

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

3









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

Investigate industrial events in your IT SOC

View events in Cyber Vision

Launch investigation in SecureX

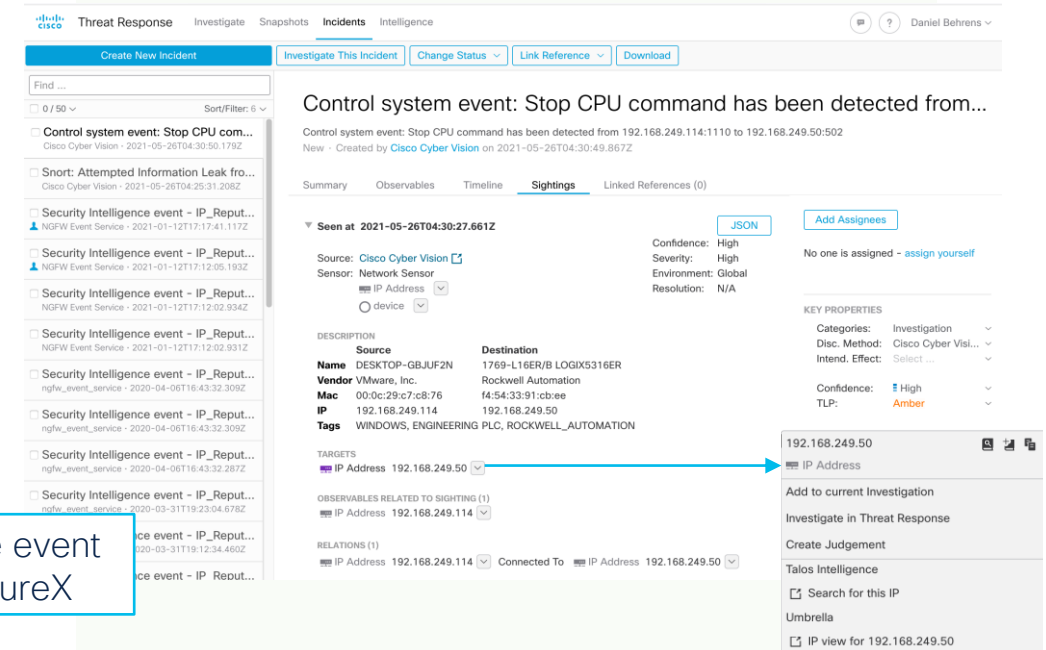
00:30:27.661 Control Systems Events Stop CPU command has been detected from DESKTOP-GBJUF2N (DESKTOP-GBJUF2N) | IP: 192.168.249.114 | MAC: 00:0c:29:c7:c8:76 to 1769-L16ER/B LOGIX5316ER (1769-L16ER/B LOGIX5316ER) | IP: 192.168.249.50 | MAC: f4:54:33:91:cb:ee

source	destination	Flow	Component source	Component destination
 DESKTOP-GBJUF2N	 1769-L16ER/B LOGIX5316ER	Source port: 1110 Destination port: 502	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	Device:  1769-L16ER/B LOGIX5316ER Name: 1769-L16ER/B LOGIX5316ER MAC: f4:54:33:91:cb:ee IP: 192.168.249.50 Tags:  Controller  Rockwell Automation 10 vulnerabilities detected

[See Technical sheet](#)

REPORT TO SECUREX

Promote event to SecureX

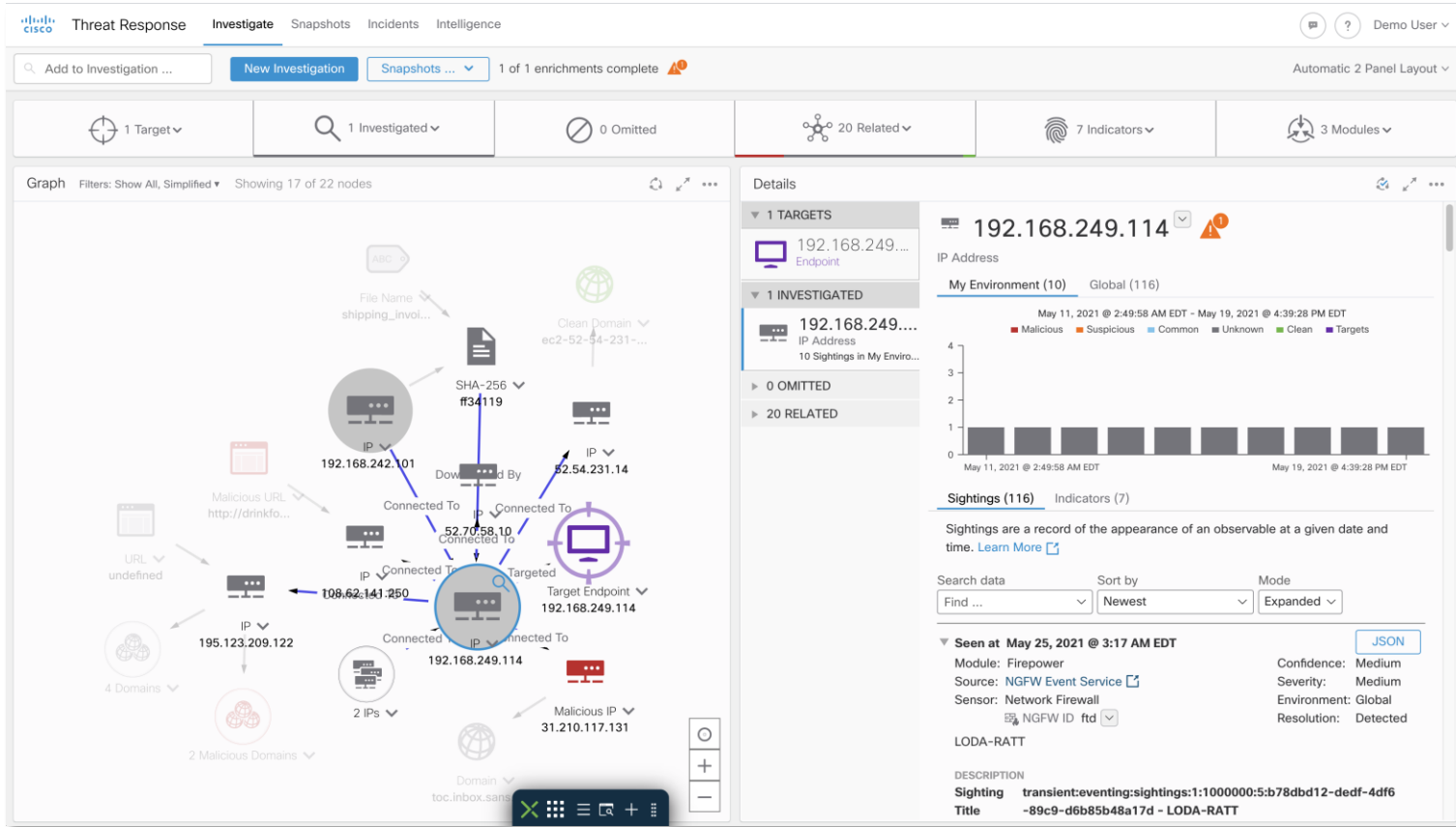


The screenshot shows the Cisco SecureX interface. The main panel displays an investigation for the event "Control system event: Stop CPU command has been detected from...". The event details include the source (DESKTOP-GBJUF2N) and destination (1769-L16ER/B LOGIX5316ER). The interface also shows a list of related events and a "Sightings" section with a "JSON" button and "Add Assignees" option. A "KEY PROPERTIES" section on the right shows the event's confidence (High) and TLP (Amber). A "TALOS INTELLIGENCE" section at the bottom provides search and IP view options for the destination IP address.

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

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

Expand investigation across the enterprise



Leverage information across enterprise security deployment

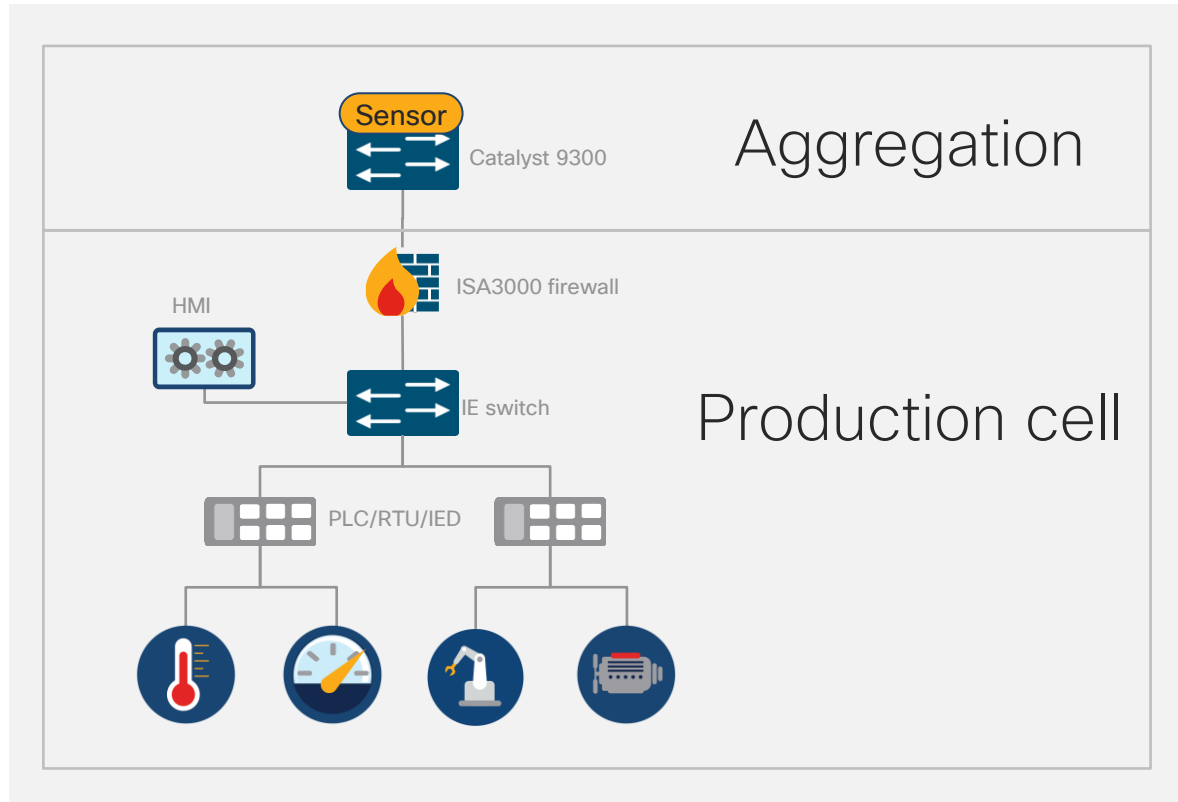
- FMC
- ISE
- Stealthwatch
- Umbrella
- AMP
- Many, many more

Tie into orchestration workflows

Simplifying Deployments

- Catalyst 9000 Sensor now with IDS
- MSLA licenses
- Mass scale deployments via Ansible scripts
- PCAP import
- New UI languages

Catalyst 9000 as a Cyber Vision sensor



Cyber Vision DPI
Now with the
Snort IDS

- Sensor is an application running in IOx
- Runs on Catalyst 9300 and 9400
- Can be deployed as access, aggregation, core or as an out of band span aggregation sensor

Cyber Vision offers highly flexible IDS deployment options

Choice of hardware/architecture

- At the edge with the Cisco IC3000 hardware-sensor
- At the aggregation layer with the sensor in the Catalyst 9300/9400
- In the datacenter with the sensor in the Cyber Vision Center

Choice of detection signatures

- Snort Community Signatures (free)
- Custom Signatures (your own)
- Talos Subscriber Rules (optional license)

Ease of Deployment

Bulk sensor deployment options

- Enabling simplified workflow for mass deployment via the Cyber Vision API
- New Ansible scripts to automate tasks

Support for Center in AWS

- Cyber Vision now in the AWS marketplace for customers to deploy their own instance in the Cloud

Simplified POC

Import PCAP files in the Cyber Vision Center

- 1 Get packet captures from customers
- 2 Import via the Cyber Vision UI
- 3 Demo Cyber Vision with your customer's data

Cyber Vision 4.0: Scalable OT Security Insights



Enhanced device aggregation



Enhanced optimizations and performances



Enhanced security insights and new risk scores



Enhanced SOC integrations



Simplified mass deployments



Quint@sQuinze



The bridge to possible

Muito Obrigado

