Cisco IoT

Quint@sQuinze

Sistema de Segurança Industrial e Novidades do Cisco Cyber Vision 4.0

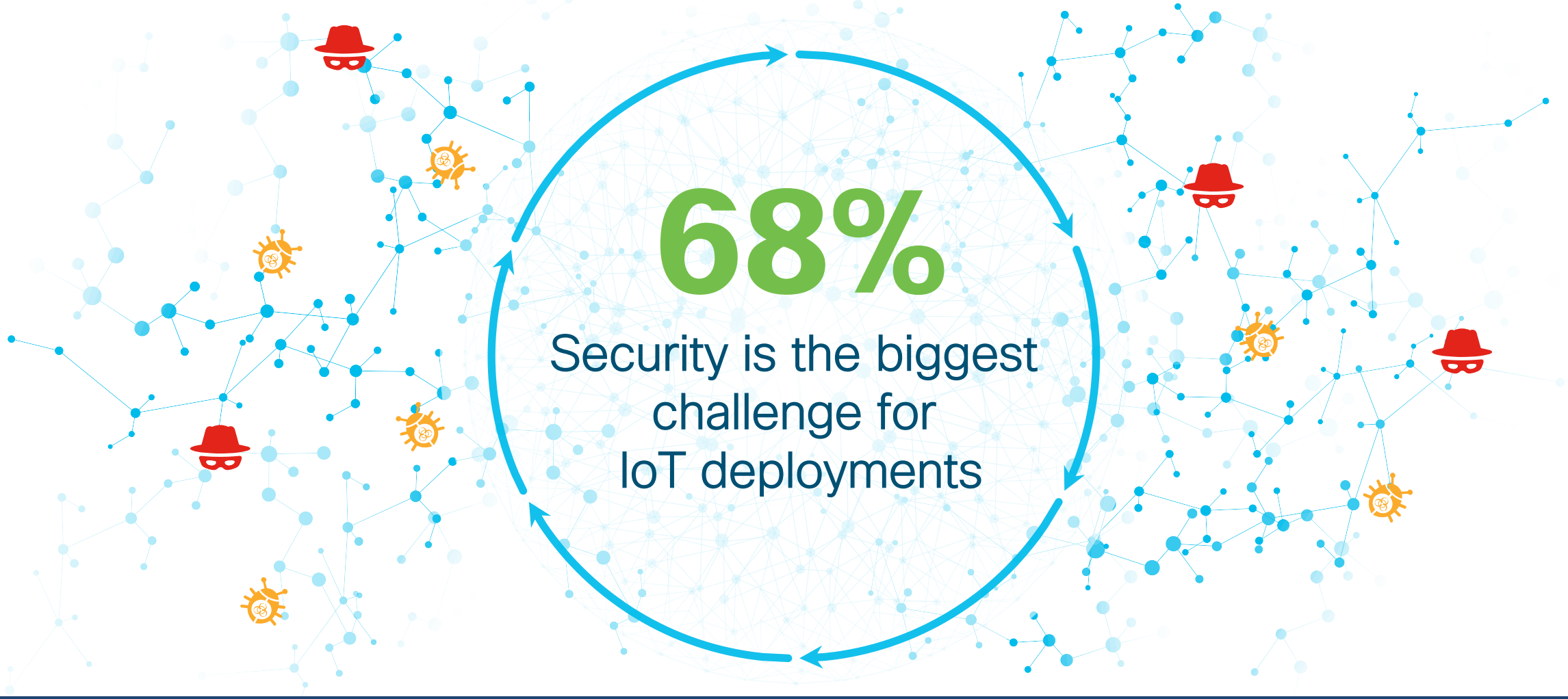
Julio Cesar Gouy - TSA IoT LATAM & Field Advisor - CCIE#8863

August 2021

Every industry is going through **digital transformation**

...every "thing" is getting connected

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



Digitization Increases **The Attack Surface**

The IIoT Security Journey

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

Asset discovery

Identify all your industrial assets to build the right security strategy

Network segmentation

Isolate networks to build zones and conduits to avoid attacks to spread

Live threat detection

Detect IT intrusions and abnormal OT behaviors to maintain process integrity

Integrated IT/OT SOC

Gain a holistic view on security events to ease investigation & remediation

Cisco's integrated security portfolio helps customers through this journey

Cisco IoT

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

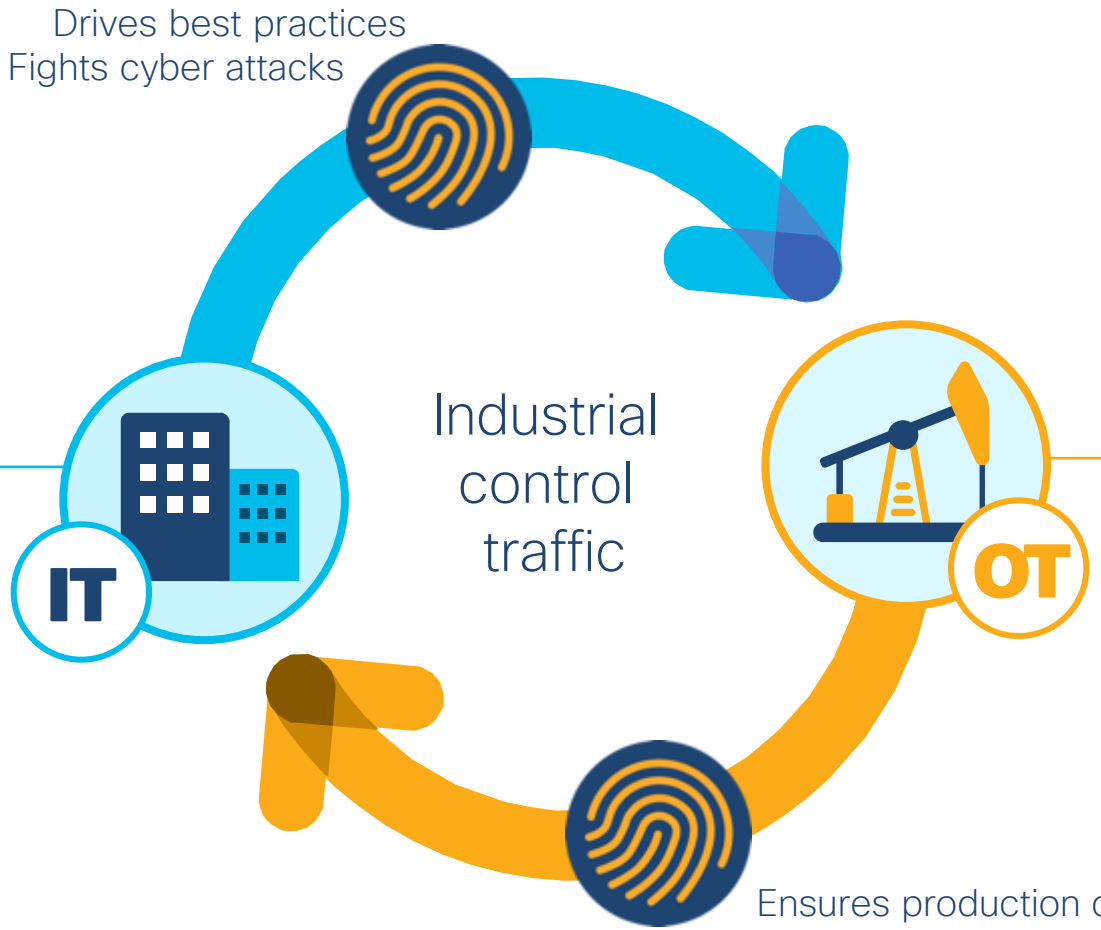
Detect bypass or leaks in the IDMZ

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**



Cybersecurity skills
Network hygiene
Security policies
Detection & Remediation

Industrial process skills
Operational events context
Asset criticality levels
Equipment configuration

Cisco IoT

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

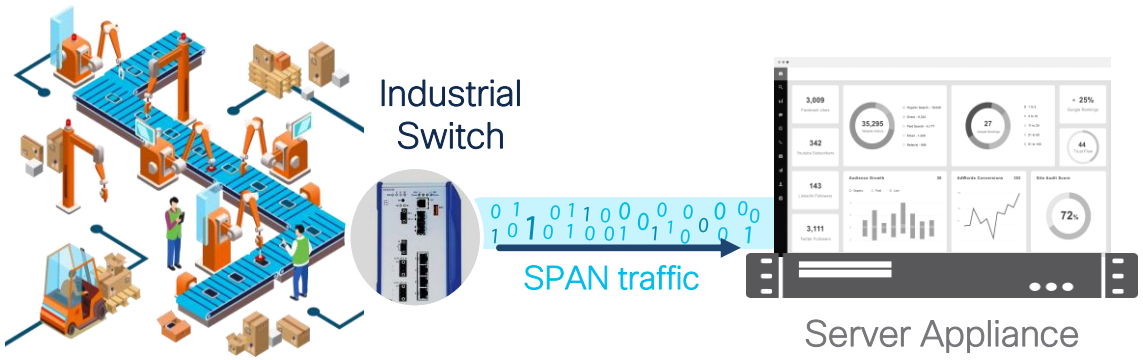
Track process/device modifications
Record control system events
Map communication patterns

Threat Detection

Behavioral anomaly detection
Snort IDS with Talos signatures
SecureX threat investigation

Cisco IoT

Security Starts with Visibility
But Beware of Hidden Costs!



Typical industrial visibility and detection solutions require SPAN (traffic mirroring)

Additional switches for SPAN collection

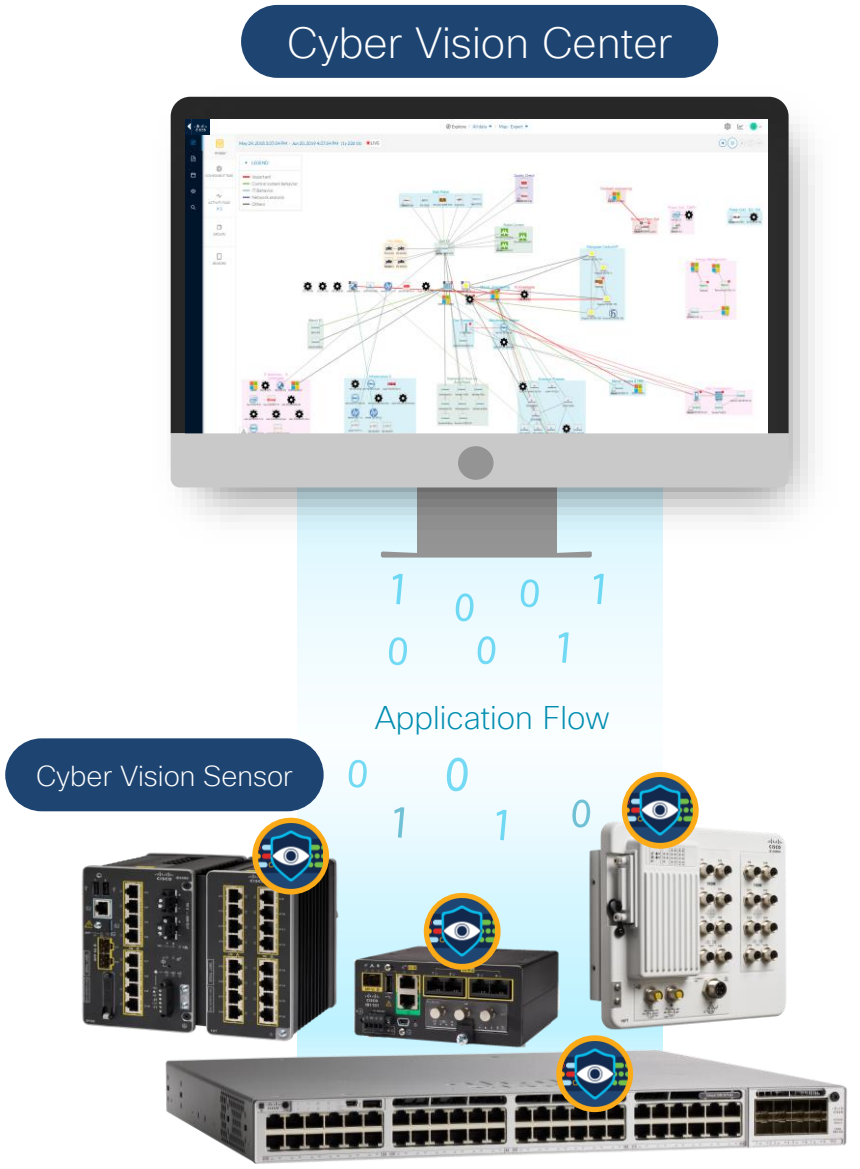
Expensive cabling for collection network

Exponential increase in traffic due to SPAN

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

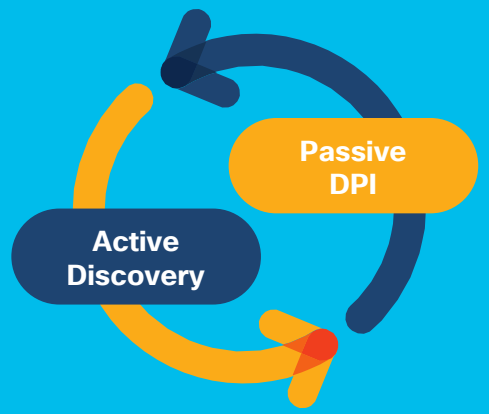
Enlist your OT network for security

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



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

Cisco Cyber Vision

Asset Inventory

Comprehensive up to date inventory of all assets in your environment

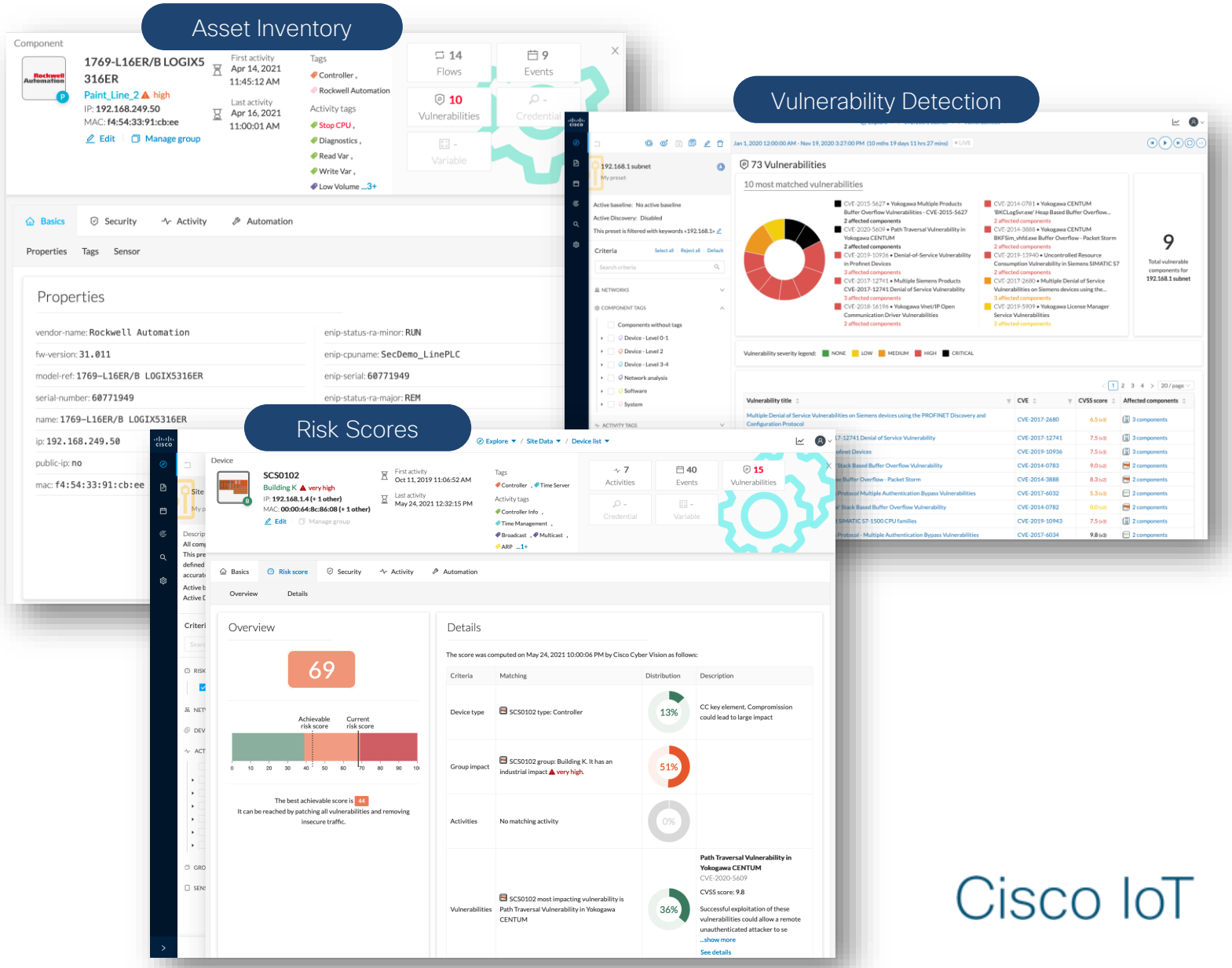
Vulnerability Detection

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

Get Asset Visibility



Cisco IoT

Cisco Cyber Vision

Communication Patterns

Dynamic communication map with detailed application flow level information

Control System Activities

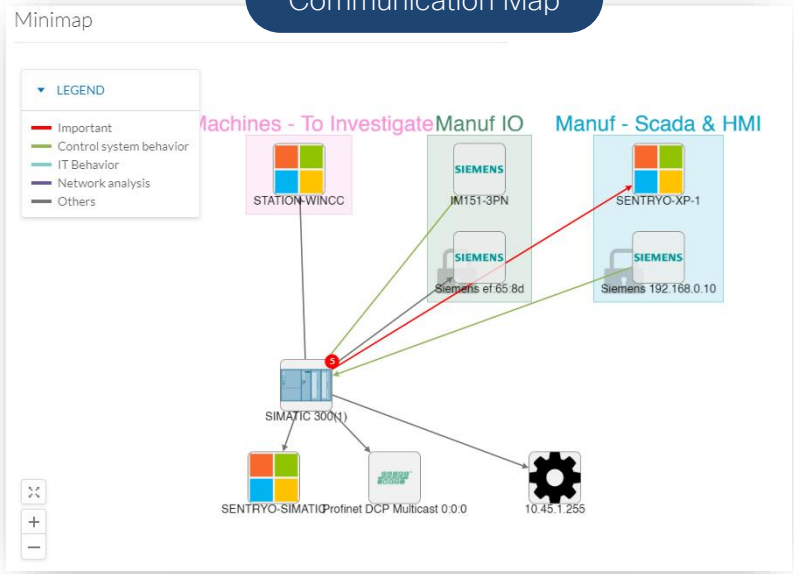
Track process modifications
Identify configuration changes
Record control system events

Variable Access

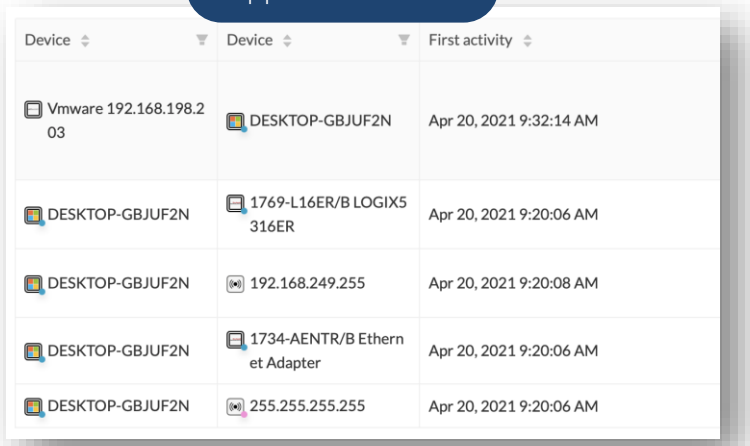
See which variables, objects, setpoints are being accessed or modified

Gain Operational Insights

Communication Map

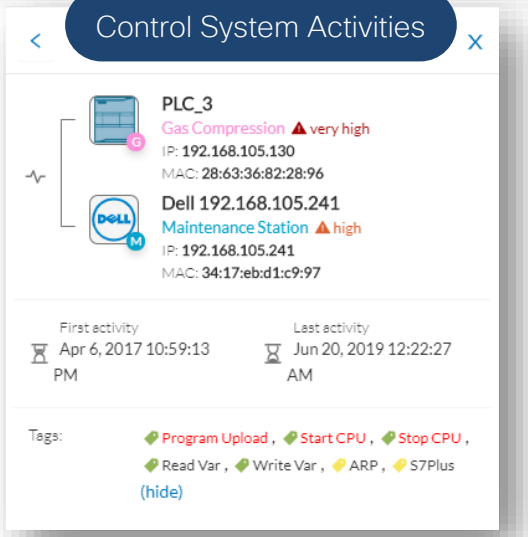


Application Flows

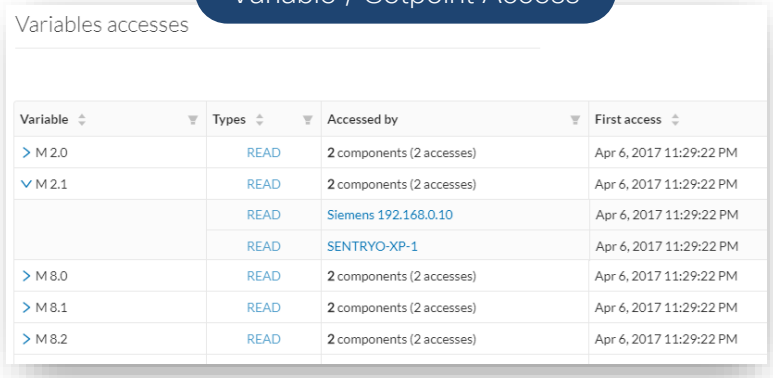


Device	Device	First activity
Vmware 192.168.198.203	DESKTOP-GBJUF2N	Apr 20, 2021 9:32:14 AM
DESKTOP-GBJUF2N	1769-L16ER/B LOGIX5316ER	Apr 20, 2021 9:20:06 AM
DESKTOP-GBJUF2N	192.168.249.255	Apr 20, 2021 9:20:08 AM
DESKTOP-GBJUF2N	1734-AENTR/B Ethernet Adapter	Apr 20, 2021 9:20:06 AM
DESKTOP-GBJUF2N	255.255.255.255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

Control System Activities



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
v 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 IoT

Cisco Cyber Vision

Anomaly Detection

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

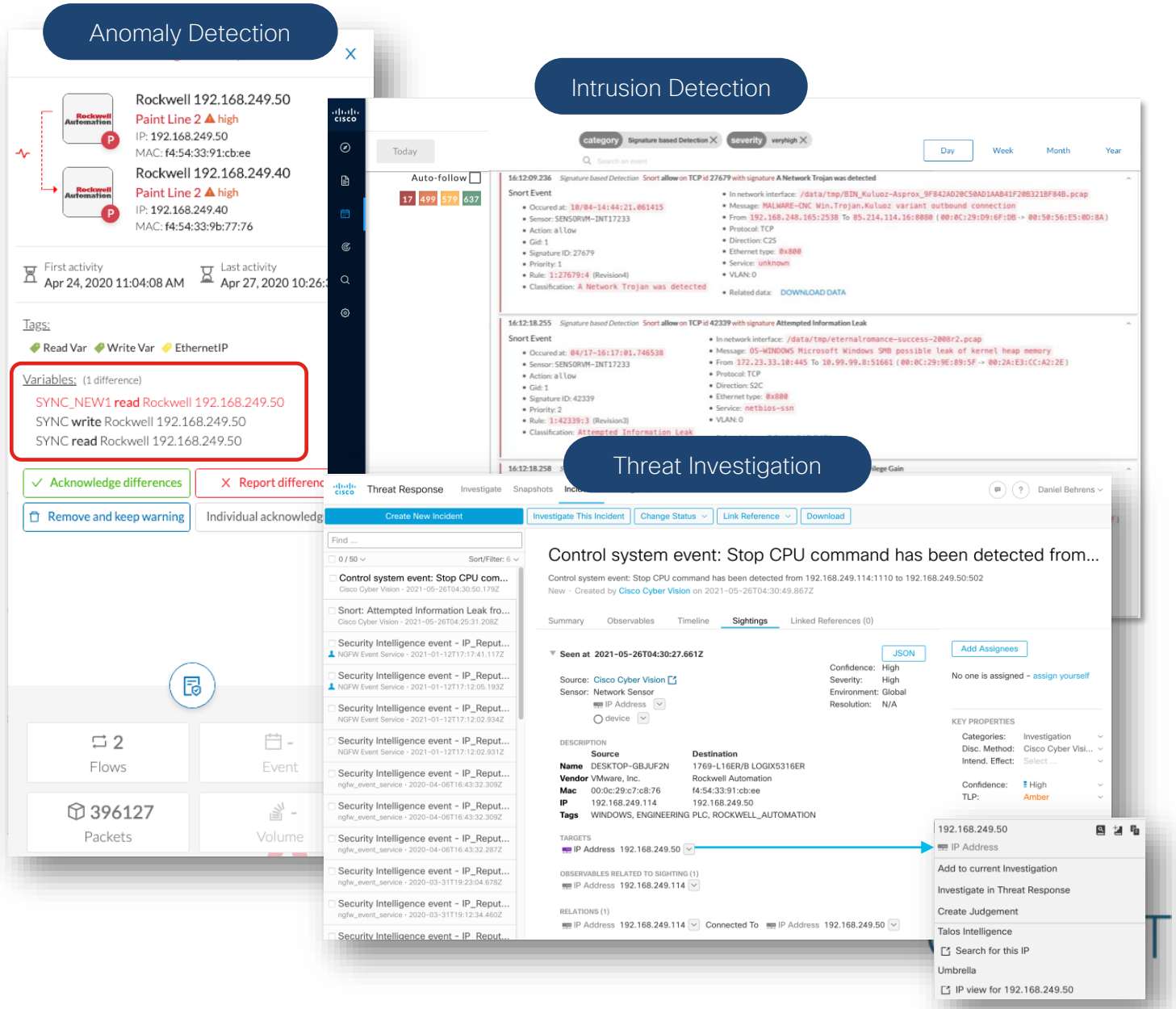
Intrusion Detection

Detect malicious intrusions with snort IDS and Talos threat intelligence

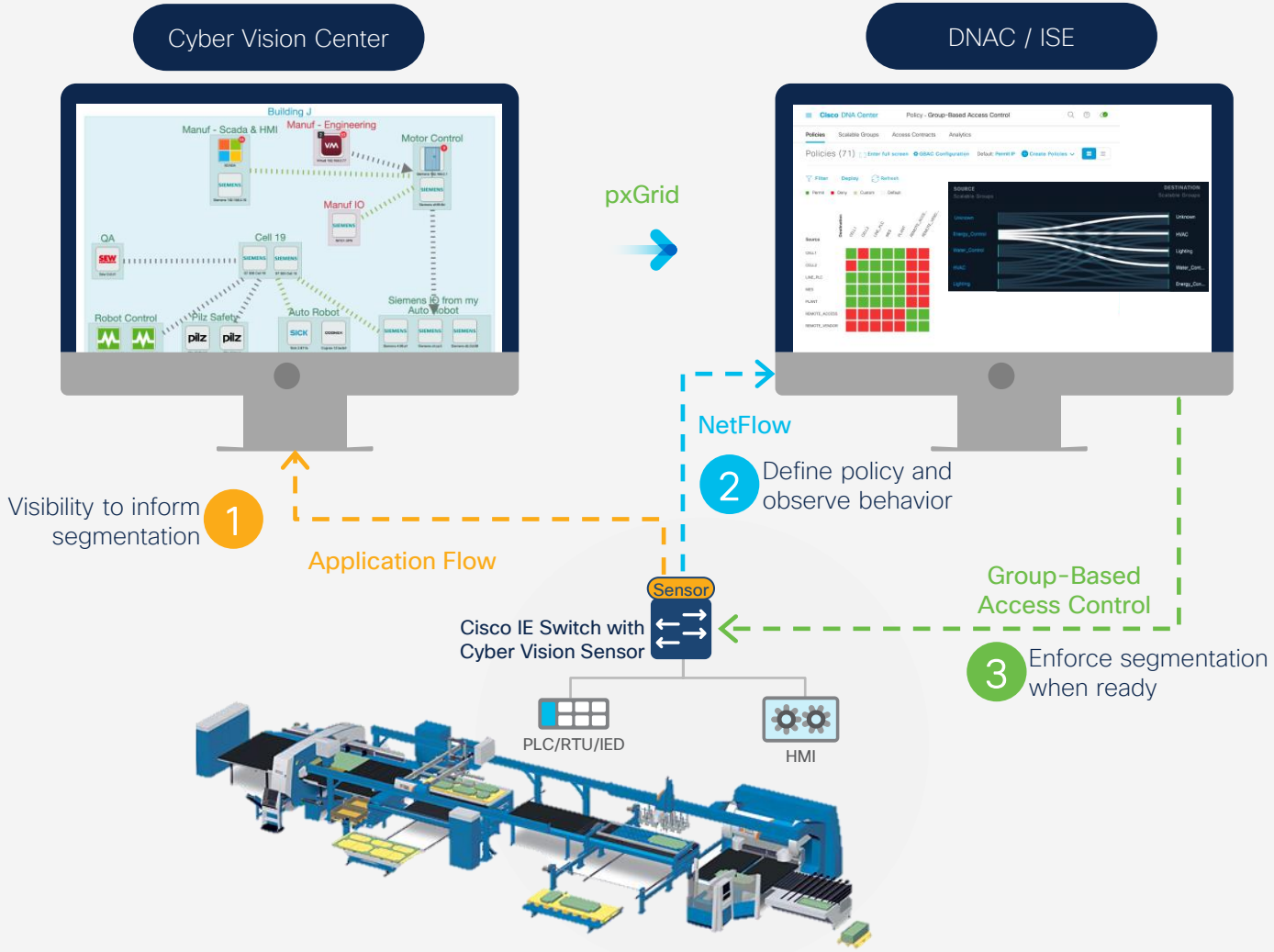
Threat Investigation

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

Detect & Investigate Threats



Segment your network with Visibility & Analytics



Visualize Zones & Conduits

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

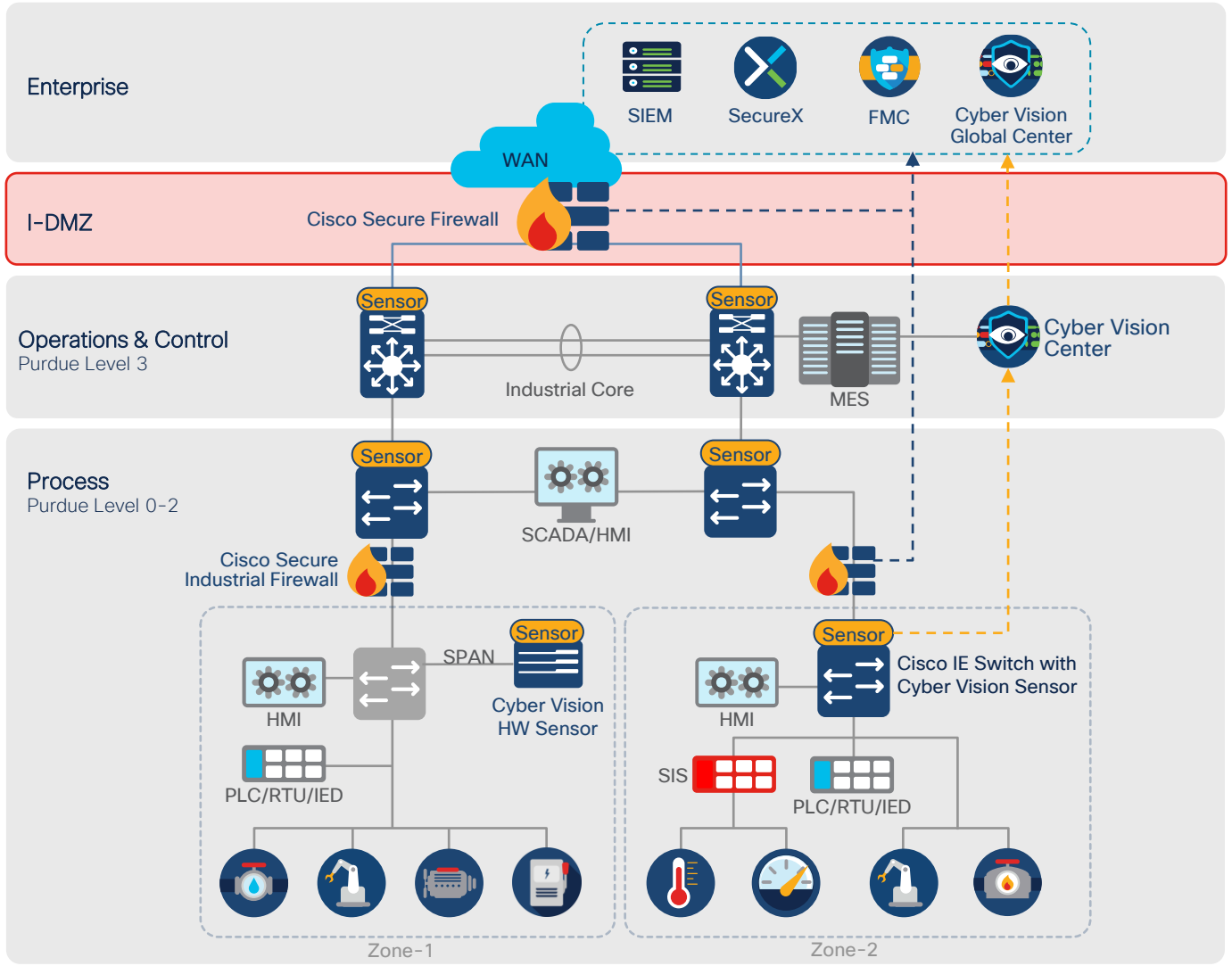
Dynamic SGT Mapping

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

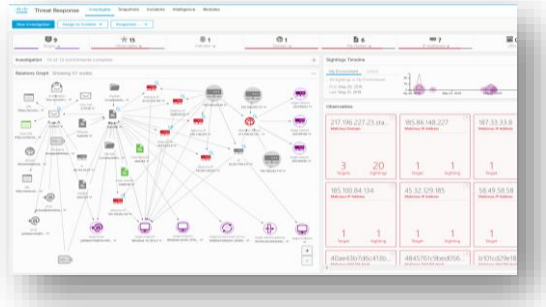
OT events and context shared with your SIEM and IT security platforms

Cisco's fully integrated IT-OT security solution

Enterprise IT Domain

Investigate and Respond

SecureX



Device Segmentation	Firewall Policies
Identity Services Engine	Firepower Management
Netflow Analytics	Malware Protection
Stealthwatch	AMP
Secure DNS	Network Management
Umbrella	DNA-Center

Powered by Cisco Talos threat intelligence

Industrial Network

Detect	Protect
Cyber Vision	ISA 3000

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

Asset discovery

- Cyber Vision Asset inventory
- Cyber Vision Vulnerability detection
- Cisco CX assessment services

Network segmentation

- ISA3000 Firepower Zone-segmentation
- TrustSec Micro-segmentation
- ISE - Centralized segmentation policy

Live threat detection

- Cyber Vision Anomaly detection
- Firepower/Cyber Vision Intrusion detection
- AMP / Threat Grid Malware detection

Integrated IT/OT SOC

Securing industrial control networks with Cisco

Cisco IoT

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

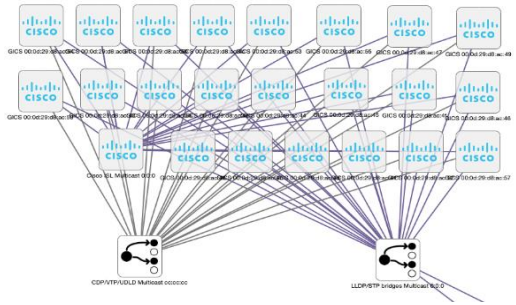
Enhanced Insights and Security Posture Identification

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

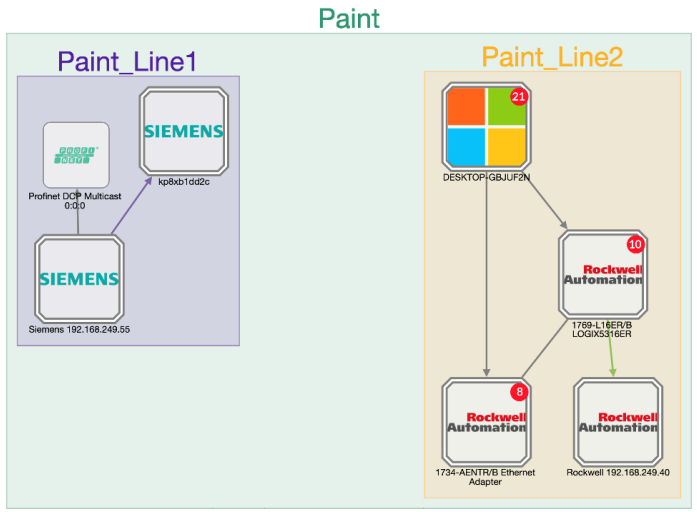
Cyber Vision 4.0 now lists **Devices**

- 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

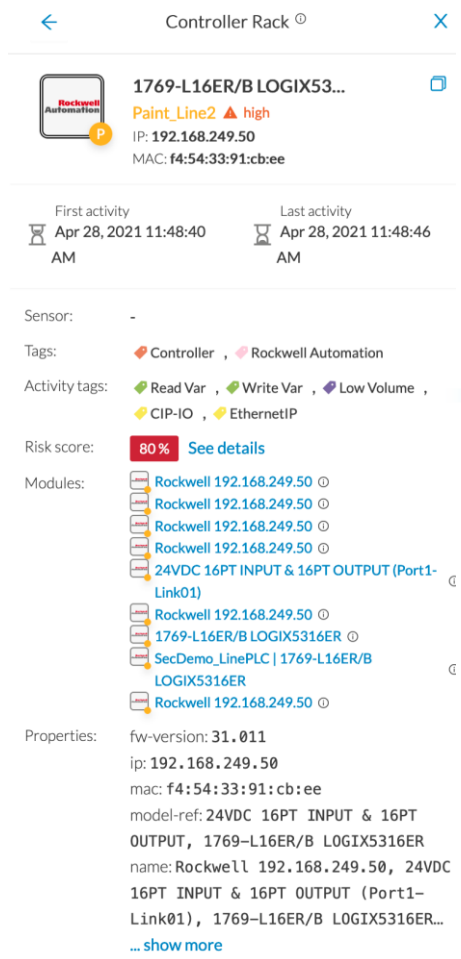
Enhanced device aggregation

Map view

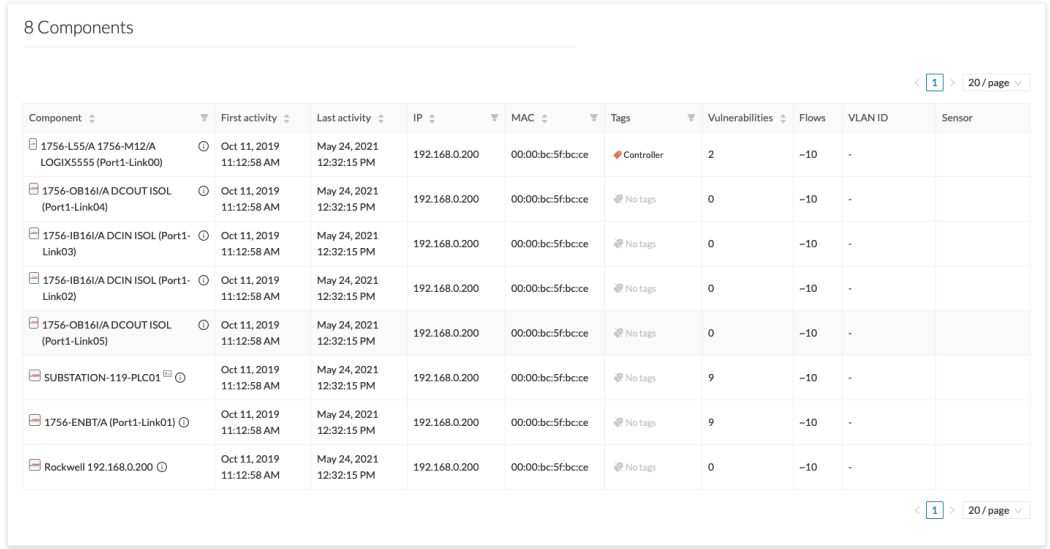


New double-border icons indicate a device

ID Cards



Technical Sheets



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

Cisco IoT

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

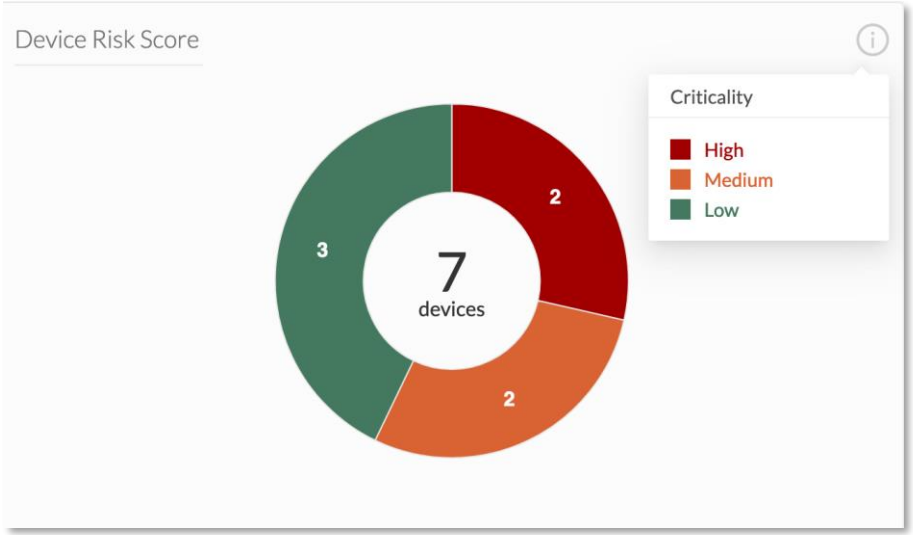
Enhanced Security Insights

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

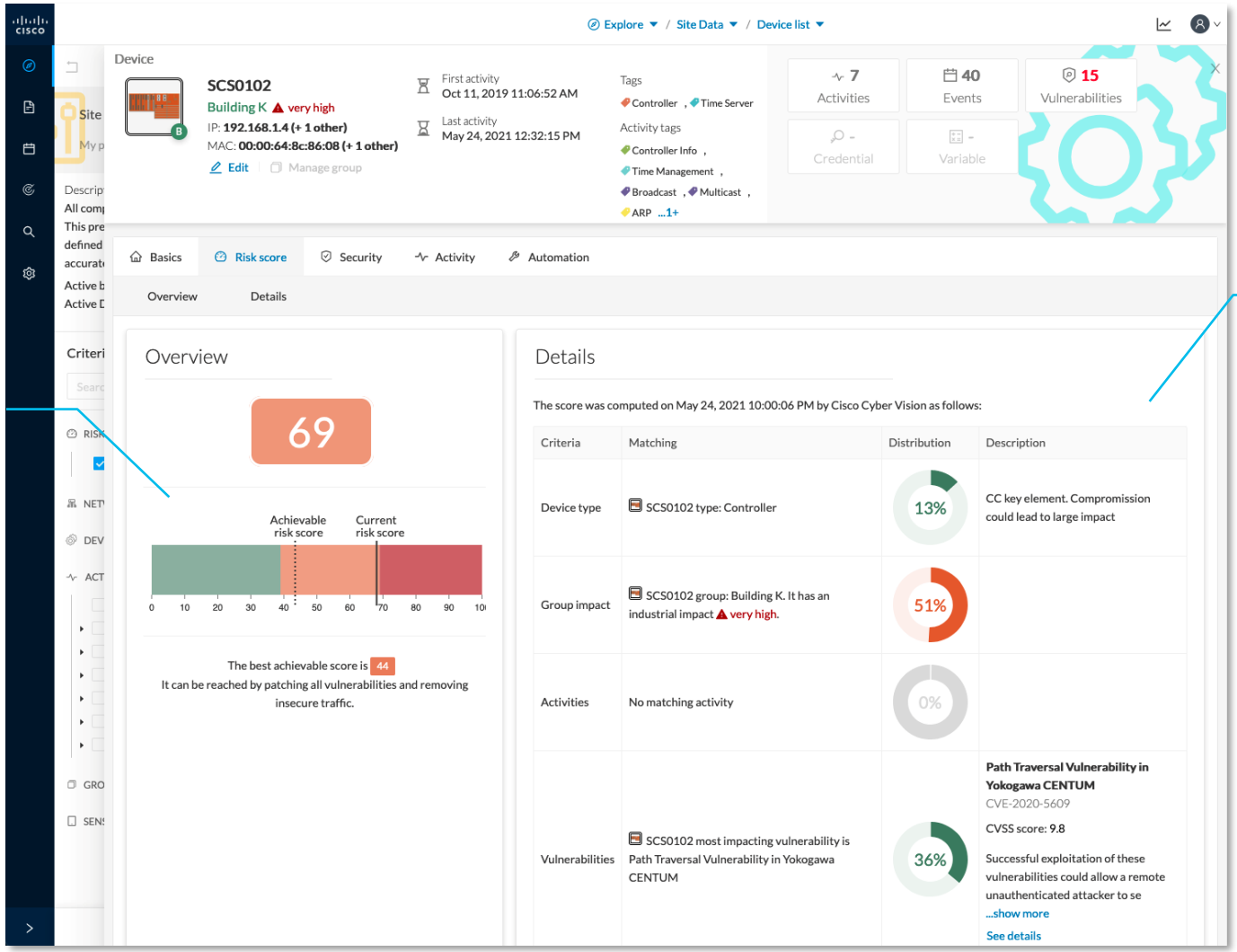
- Risk = Likelihood x Impact
- Likelihood
  - Activity tags (some communications create more risks)
  - Exposure to external IP addresses
  - Discovered vulnerabilities
- Impact
  - Device tags (some devices can create more damages)
  - User-defined industrial impact for groups

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

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)

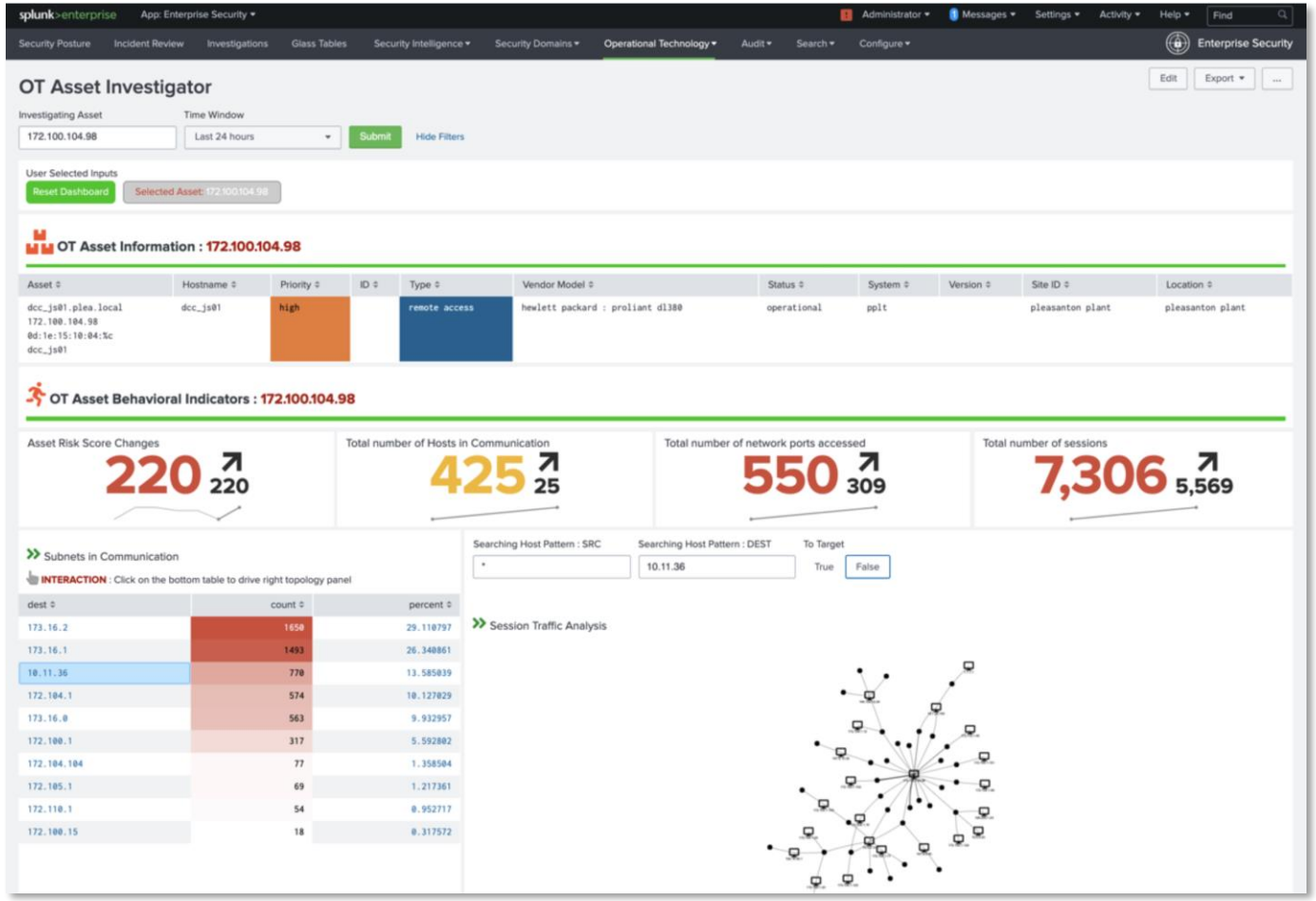
Active Discovery can now send queries using ICMPv6

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



- 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

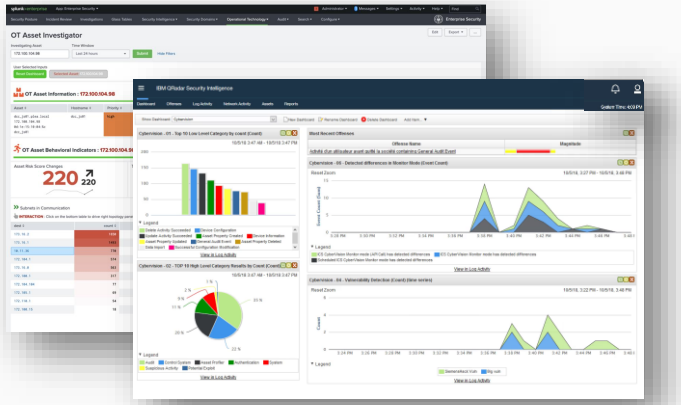
SecureX Incidents

Simplify IT/OT threat hunting with Cisco SecureX

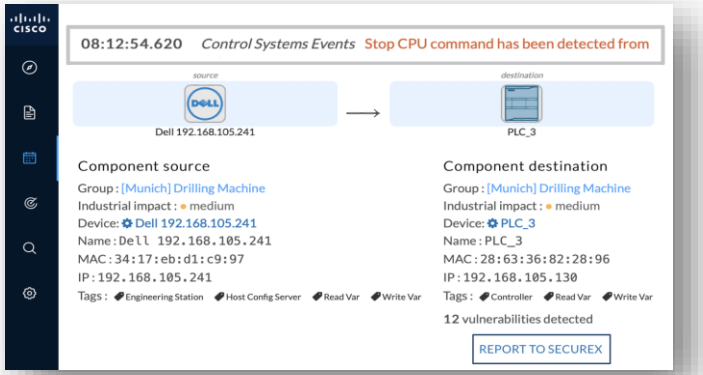
- Cyber Vision with SecureX enables a converged IT/OT threat management strategy
- Makes it easy for OT to share relevant threat intel with IT/Security analysts
- ‘One-click’ promotion of Cyber Vision security events for further investigation on SecureX
  - Signature-based detection events
  - Control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

Investigate Industrial Events in your IT SOC

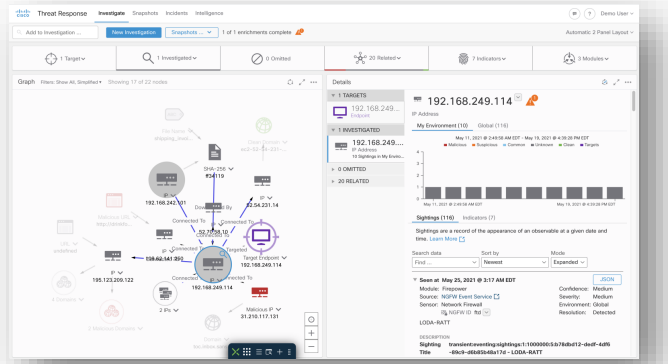
Cyber Vision Apps for Splunk & QRadar



Cyber Vision



SecureX



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

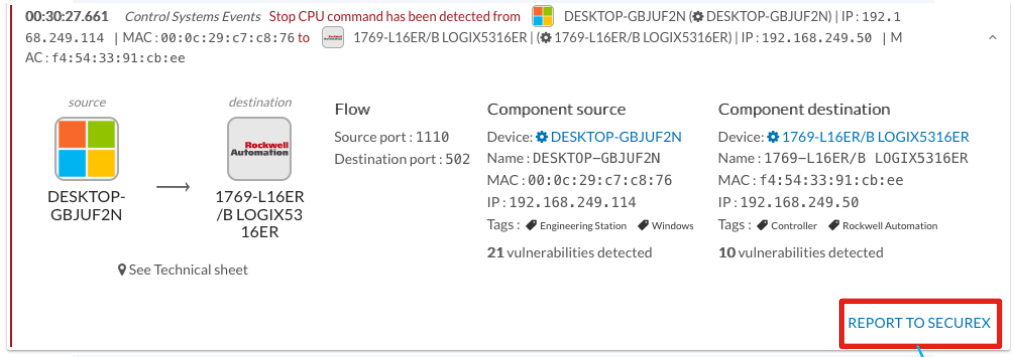
2. Pivot to the corresponding instance of Cyber Vision to get more details on the event that generated the alert

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

Cisco IoT

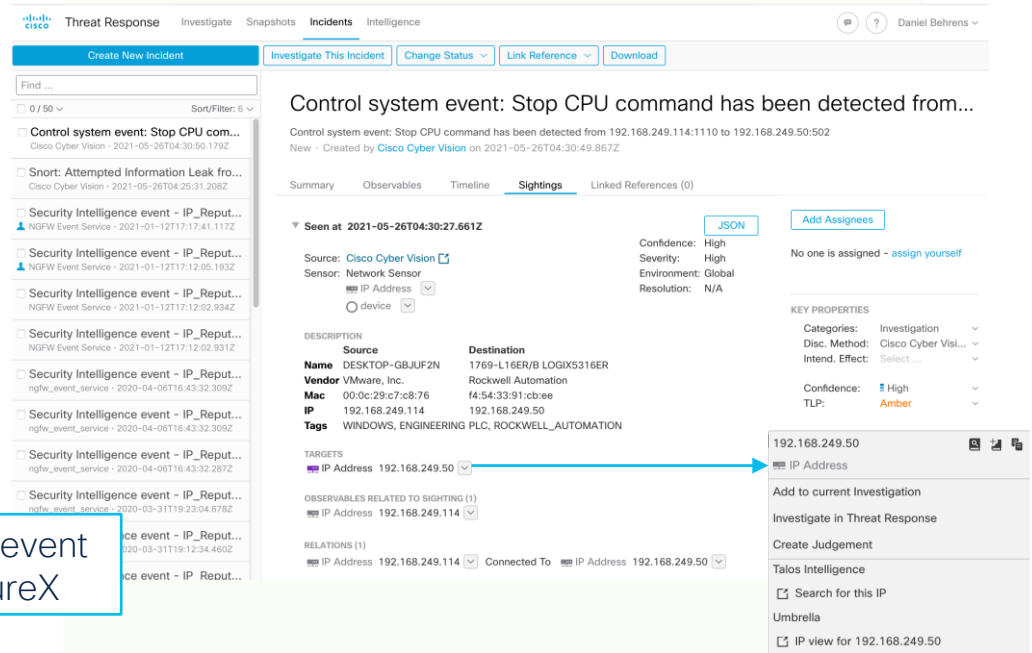
Investigate industrial events in your IT SOC

View events in Cyber Vision



Promote event to SecureX

Launch investigation is SecureX

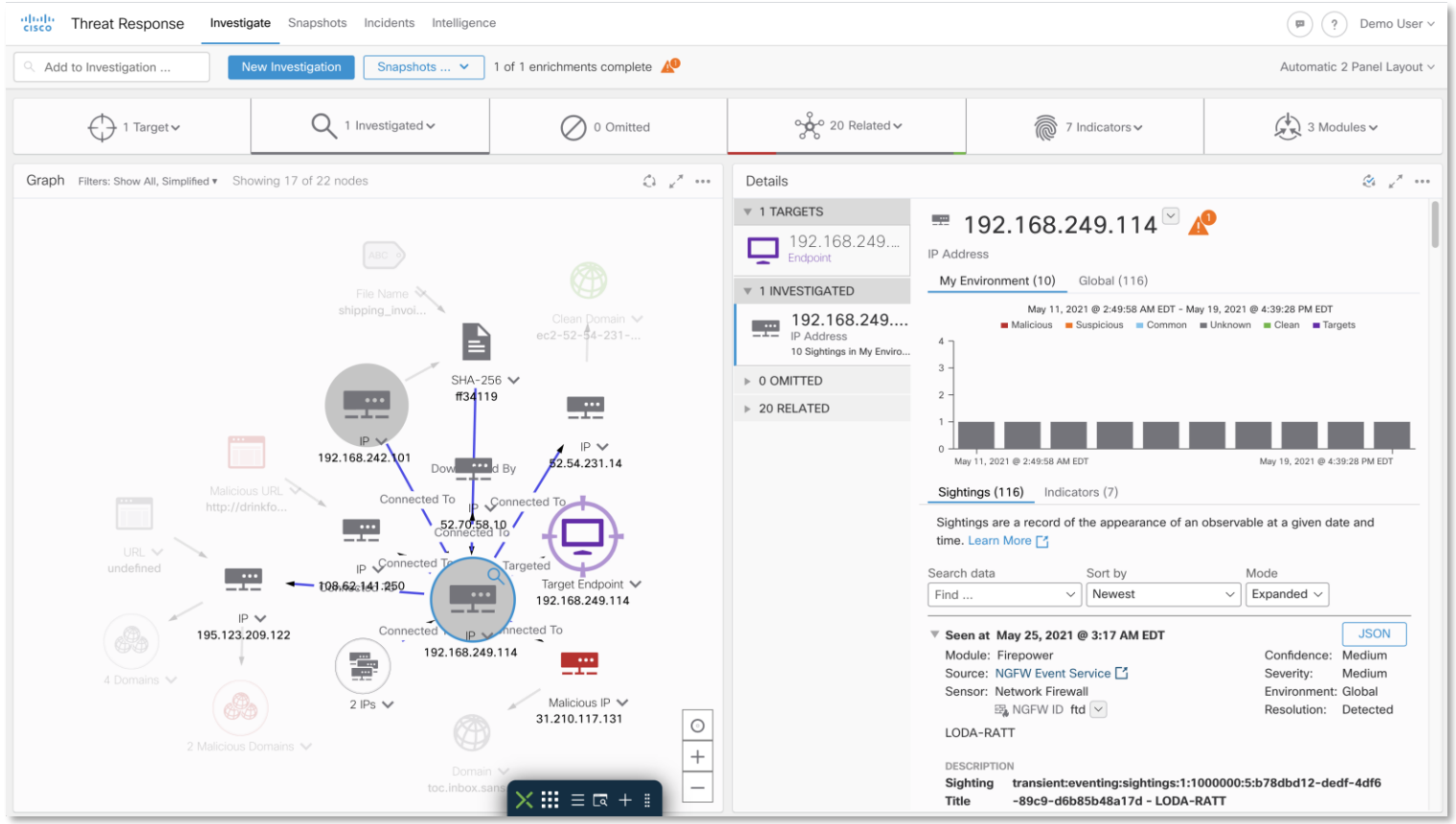


Events generated in Cyber Vision for process anomalies, signatures and control system

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

Cisco IoT

Expand investigation across the enterprise



Leverage information across enterprise security deployment

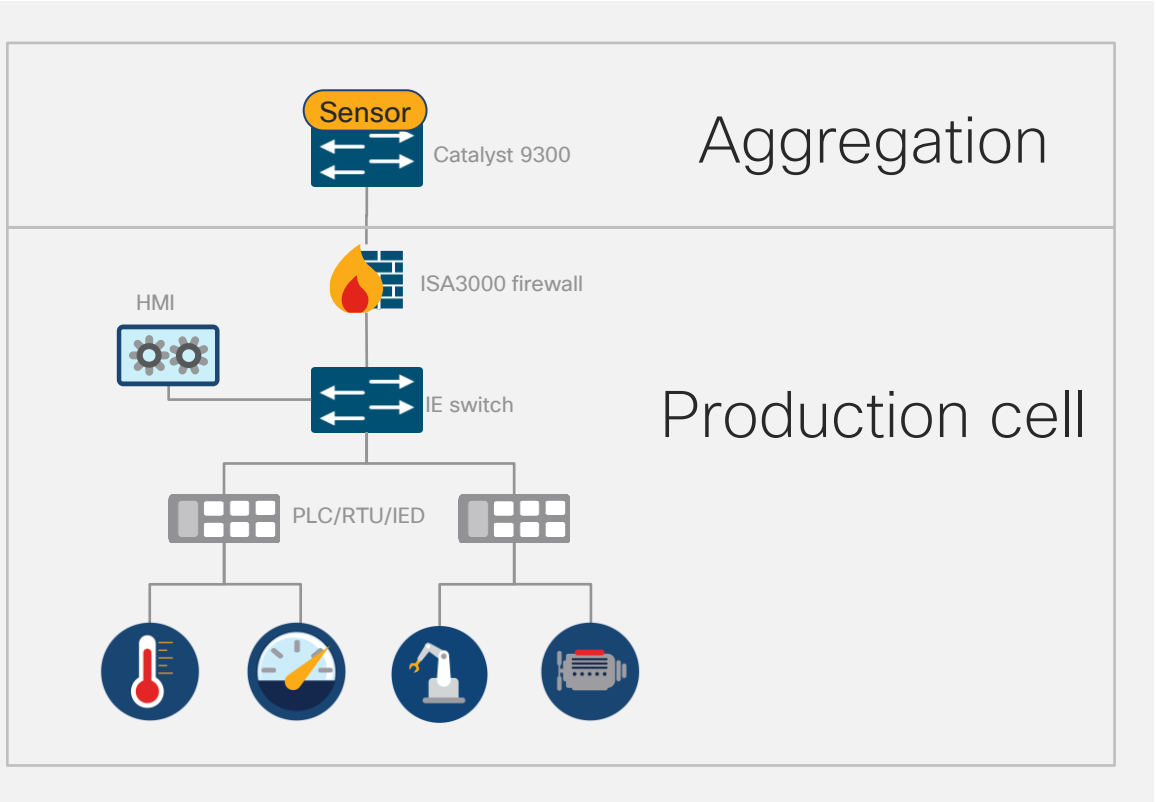
- FMC
- ISE
- Stealthwatch
- Umbrella
- AMP
- Many, many more

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



- 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

Cisco IoT

Quint@sQuinze

cisco

The bridge to possible

Muito Obrigado