

Enhancing Splunk with OT context using Cisco Cyber Vision

CISCO Live !

Andrew McPhee
IIoT Security Solution Manager

Kartik Kamra
IIoT Security Product Manager

Webex App

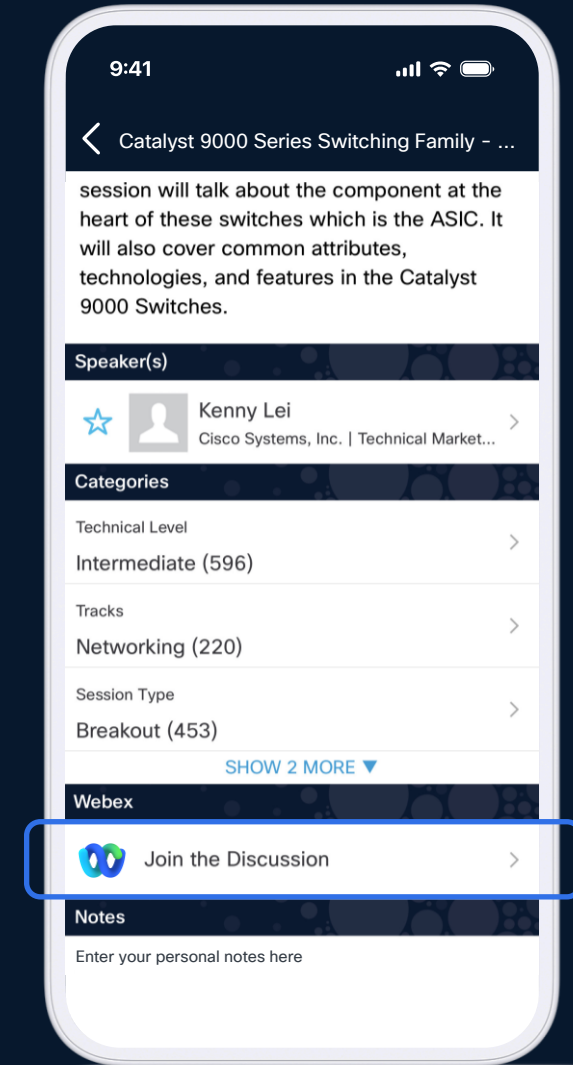
Questions?

Use Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events 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 February 27, 2026.



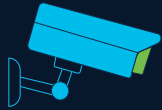
Agenda

- 01 What is Cisco Cyber Vision?
- 02 How Cyber Vision complements Splunk
- 03 What exactly is Splunk?
- 04 [Demo] Splunk's Cyber Vision App
- 05 [Demo] Building your own dashboards

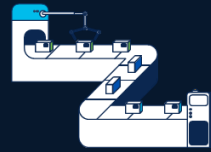
48% of respondents believe **AI** is the emerging technology likely to have the **biggest impact** within the **next five years**.



2024 State of Industrial Networking Report



Security and facilities



Warehouse automation



Industrial automation



Energy management



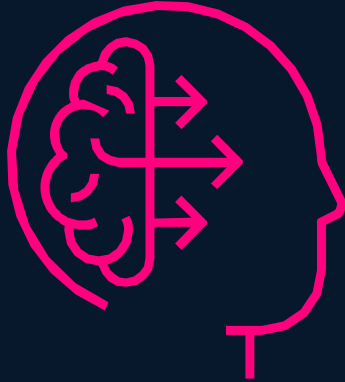
Utilities



Patient monitoring

75% of enterprise-generated AI data will be **created in industrial environments**

AI-Driven Vulnerability Exploitation
Fuels Up to 45% of Initial Access



How I Used AI to Create a Working Exploit for CVE-2025-32433 Before Public PoCs Existed

By Matthew Keeley | April 17, 2025

Red Teaming

Research

Threat Intelligence

Cyber Security News Vulnerability News

AI Systems Can Generate Working Exploits for Published CVEs in 10-15 Minutes

By Florence Nightingale - August 22, 2025

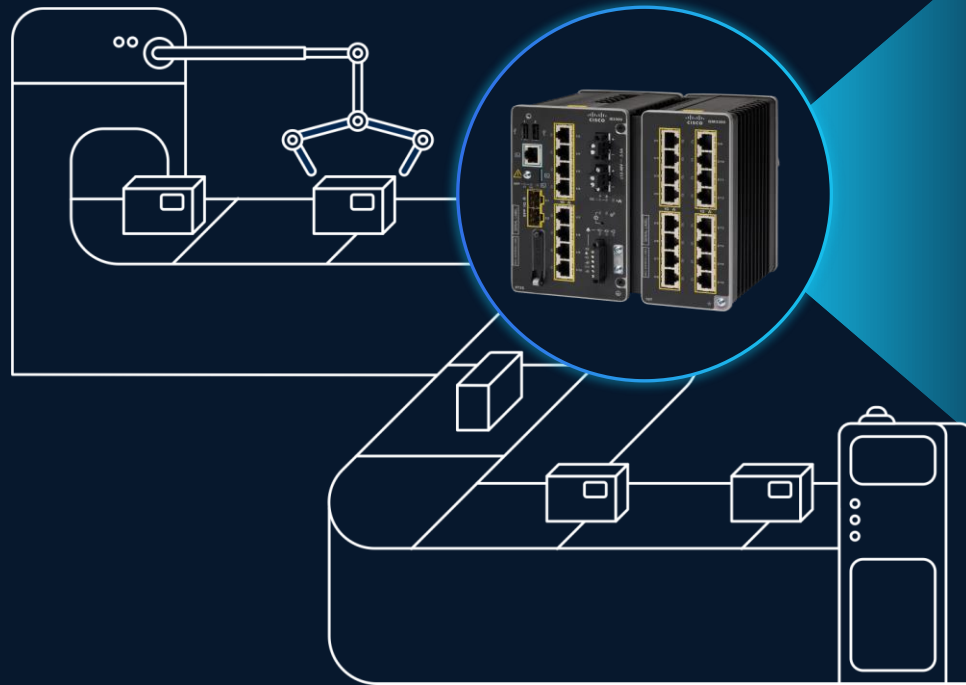
ChaosGPT | The AI That Went Rogue? Exploring Autonomous AI, Its Risks, and the Future of AI Safety

AI-Assisted Malware Evolves into a
Daily Threat

But AI also makes
**hacking the network
easier than ever...**

Cisco Industrial Security

Security fused into the network to protect OT at scale



OT Visibility
embedded in
network equipment

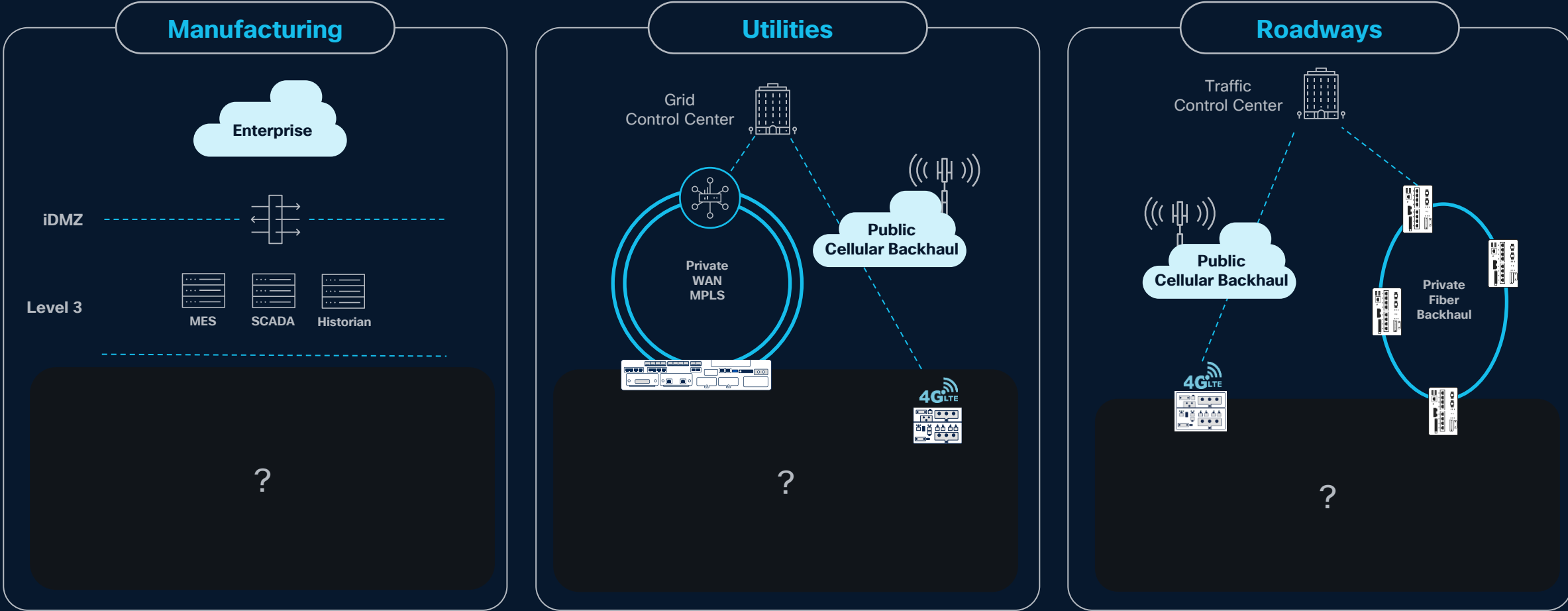


Segmentation
enforced by
network equipment

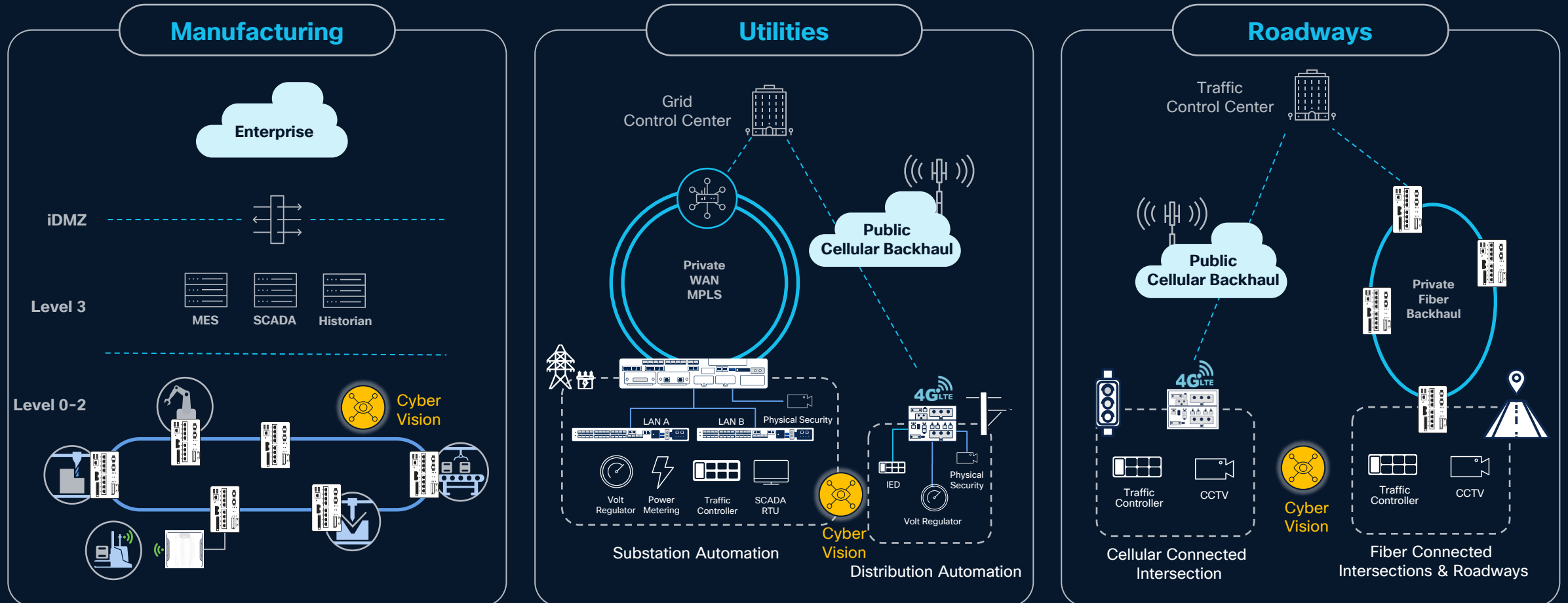


Secure Remote Access
embedded in
network equipment

We do not have enough visibility into our most critical assets



Cisco Cyber Vision “turns on the lights” for industries



Automated discovery of assets, vulnerabilities, and communication across the industrial network

Visibility into connected industrial assets

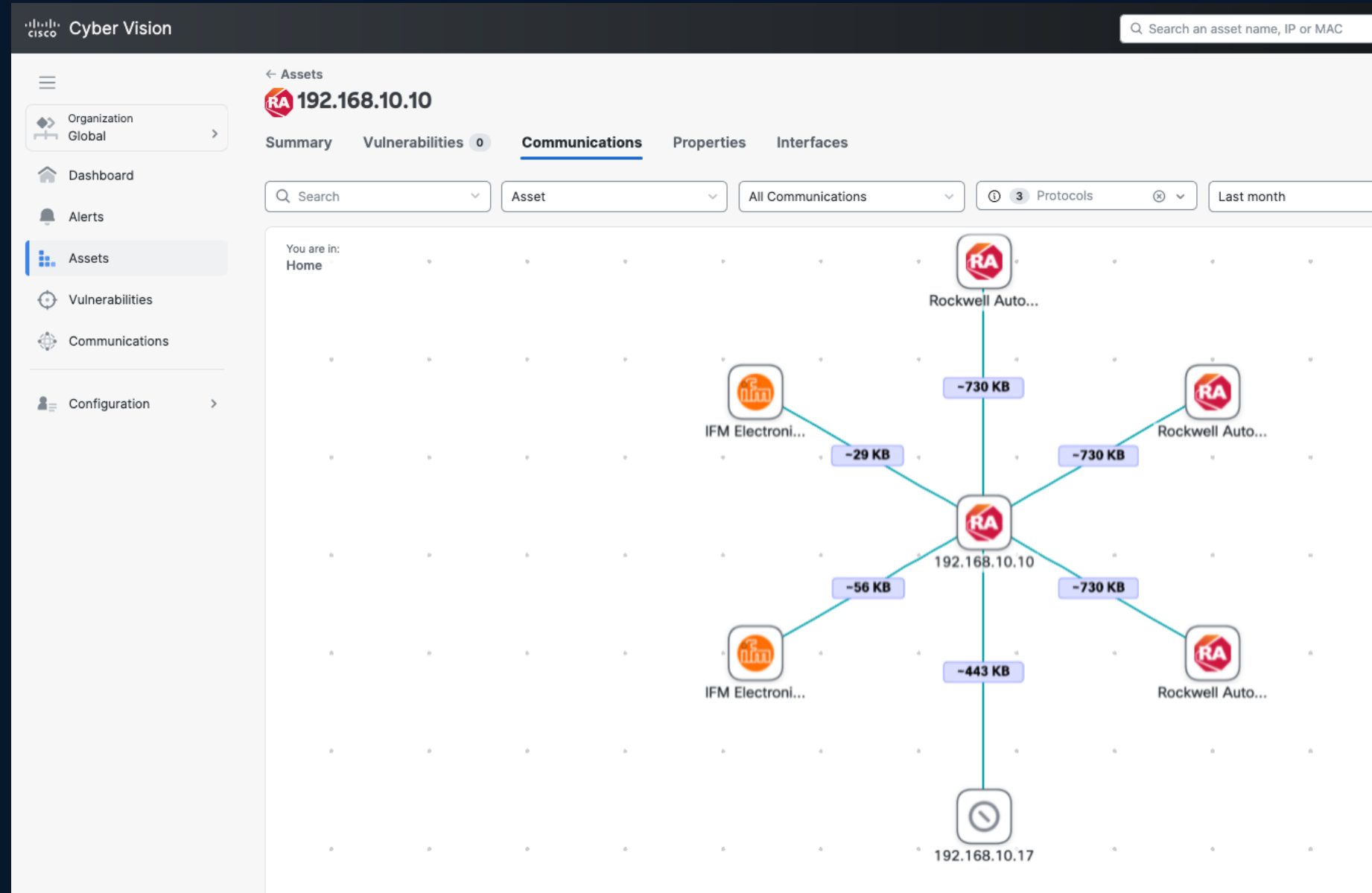
Understand the identity of all assets in the environment. View rack slot details for modular assets.



Cyber Vision

Communication Map

- Highly performant rendering for thousands of nodes
- Rich overlay capability to turn on visuals as needed to reduce distractions



Identify & Track Vulnerabilities

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

Cisco Security Risk Score provides dynamic vulnerability scoring using indicators such as being actively exploited in the wild

CVE-2025-7353

Remote Code Execution Vulnerability in Rockwell ControlLogix Ethernet

Cisco Security Risk Score

56

Medium

CVSS Score

9.8

Critical

Details

Description

A security issue exists due to the web-based debugger agent enabled on released devices. If a specific IP address is used to connect to the WDB agent, it can allow remote attackers to perform memory d...
[View more](#)

Mitigation

Update to version 12.001

Published on

August 14, 2025

User Interaction

None

Integrity Impact

High

Attack Vector

Network

Privileges Required

None

Availability Impact

High

Attack Complexity

Low

Exploit code maturity

Unproven that exploit exists

Links

<https://nvd.nist.gov/vuln/>
<https://www.rockwellautoadvisory.SD1732.html>

MITRE ATT&CK

3 Tactics matched

Description

Tactics represent an attacker's goals, such as gaining initial access, escalating privileges, or evading detection.

TA0009 - Collection

1 Technique matched

ID

Name

T1005

Data from Local System

TA0002 - Execution

2 Techniques matched

ID

Name

T1106

Native API

ID

Name

T1203

Exploitation for Client Execution

© 2026 Cisco and/or its affiliates. All rights reserved.

BRKIOT-2846

- New rule engine to configure Alert thresholds
- Alerts grouped based on trigger to reduce number of alerts generated

Cyber Vision

Search

alex@email.com

Organization Global

Dashboard

Alerts

Assets

Communications

Vulnerabilities

Configuration

Alerts 4

Filters no advanced filters applied

Assets here: 5,000

Active 4Cleared 0

2 Critical1 High0 Medium1 Low

SearchAlert TypeTriggerSeverityTriggered ByLast Detected4 resultsExport

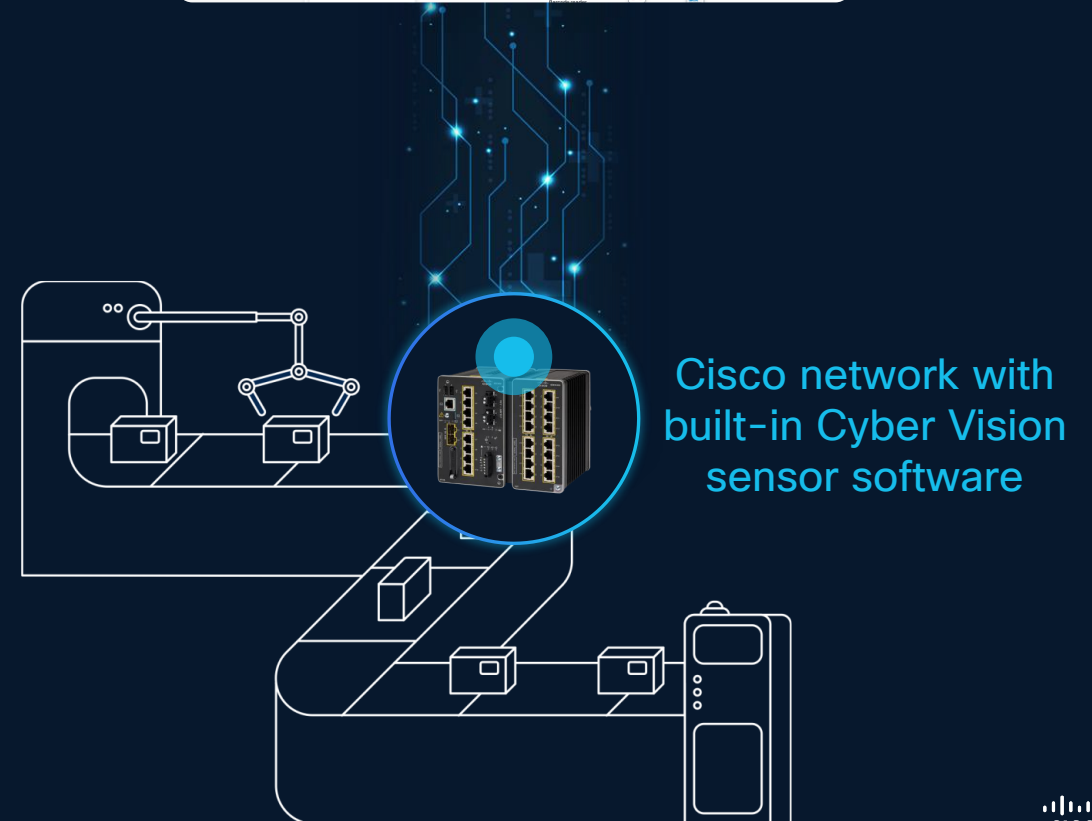
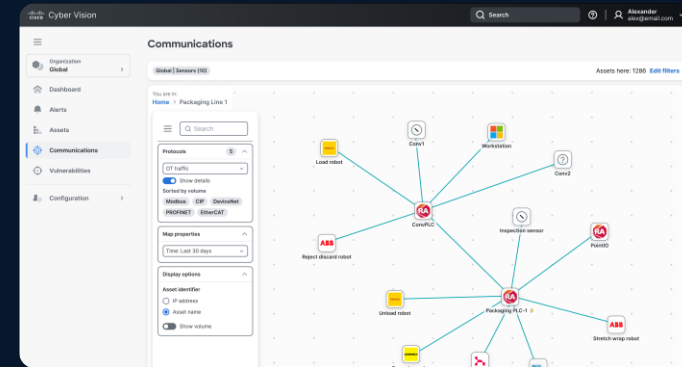
Alert Type	Trigger	Instances	Severity	Triggered By	Last Detected								
Malicious Domains	darkweb.com (4.0.1.20)	2	Critical	Communication	Dec 10, 2024 10:30 A								
Severe Vulnerabilit...	CVE-2022-1161 - Inclusion of Functionality f...	2	Critical	Vulnerability	Dec 10, 2024 10:30 A								
CVE-2022-1161 - Inclusion of Functionality from Untrusted Control Sphere Vulnerability in Rockwell Automation Logix Controllers 2 monitored assets are affected by this vulnerability which CVSS score is ≥ than the threshold defined in the alert rules. <table><thead><tr><th>Cisco Security Risk Score</th><th>CVSS Score</th><th>Exploitability</th><th>Attack vector</th></tr></thead><tbody><tr><td>86 High</td><td>9.2 Critical</td><td>Functional exploit exists</td><td>Network</td></tr></tbody></table> View alert summary →						Cisco Security Risk Score	CVSS Score	Exploitability	Attack vector	86 High	9.2 Critical	Functional exploit exists	Network
Cisco Security Risk Score	CVSS Score	Exploitability	Attack vector										
86 High	9.2 Critical	Functional exploit exists	Network										
Severe Vulnerabilit...	CVE-2025-9102 - Out-of-bounds Write Vuln...	3	High	Vulnerability	Dec 10, 2024 10:30 A								
End of Support Fir...	Allen Bradley / SLC505 / 18.0.1	1	Low	Vulnerability	Dec 10, 2024 10:30 A								

Rows per page 301-12 of 121

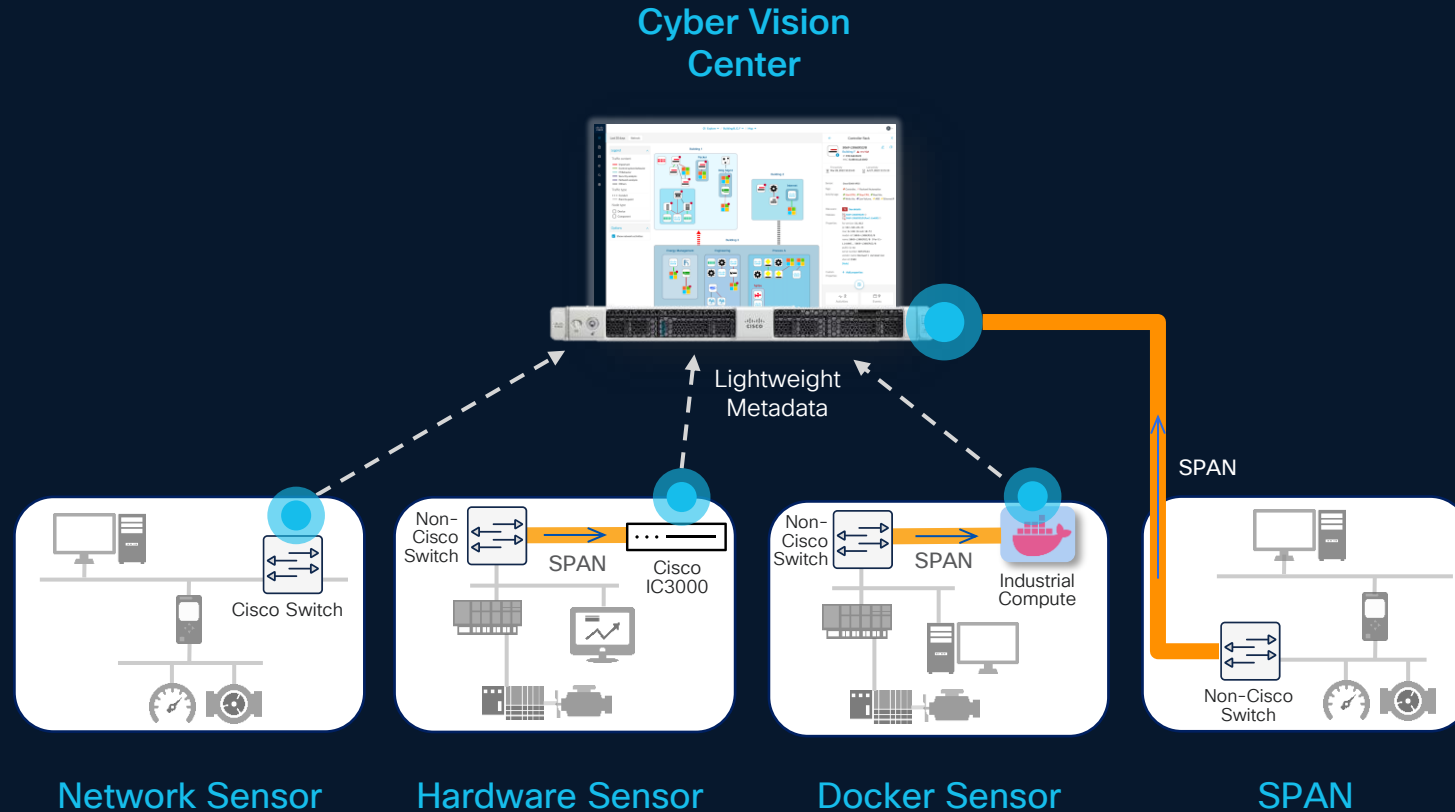
Visibility built-in, not bolted on

- ✓ Network embedded sensor
No need for additional hardware
- ✓ No need for SPAN collection
networks
- ✓ Active discovery passes NAT
boundaries
- ✓ Comprehensive visibility, even at
lowest Purdue levels

Cyber Vision Center



Flexibility to mix and match sensor types



- Network embedded sensor - No need for addition hardware
- No need for SPAN collection networks
- Active discovery passes NAT boundaries
- Comprehensive visibility, even at lowest Purdue levels

Scales across brownfield and greenfield environments

Attacks can come from anywhere

Chinese APT41 Exploits Google Calendar for Malware Command-and-Control Operations

👤 Ravie Lakshmanan 📅 May 29, 2025

Malware / Cloud Security

Chinese Hackers Target Taiwan's Semiconductor Sector with Cobalt Strike, Custom Backdoors

👤 Ravie Lakshmanan 📅 Jul 17, 2025

Malware / Cyber Espionage

EdgeStepper Implant Reroutes DNS Queries to Deploy Malware via Hijacked Software Updates

👤 Ravie Lakshmanan 📅 Nov 19, 2025

Cyber Espionage / Malware

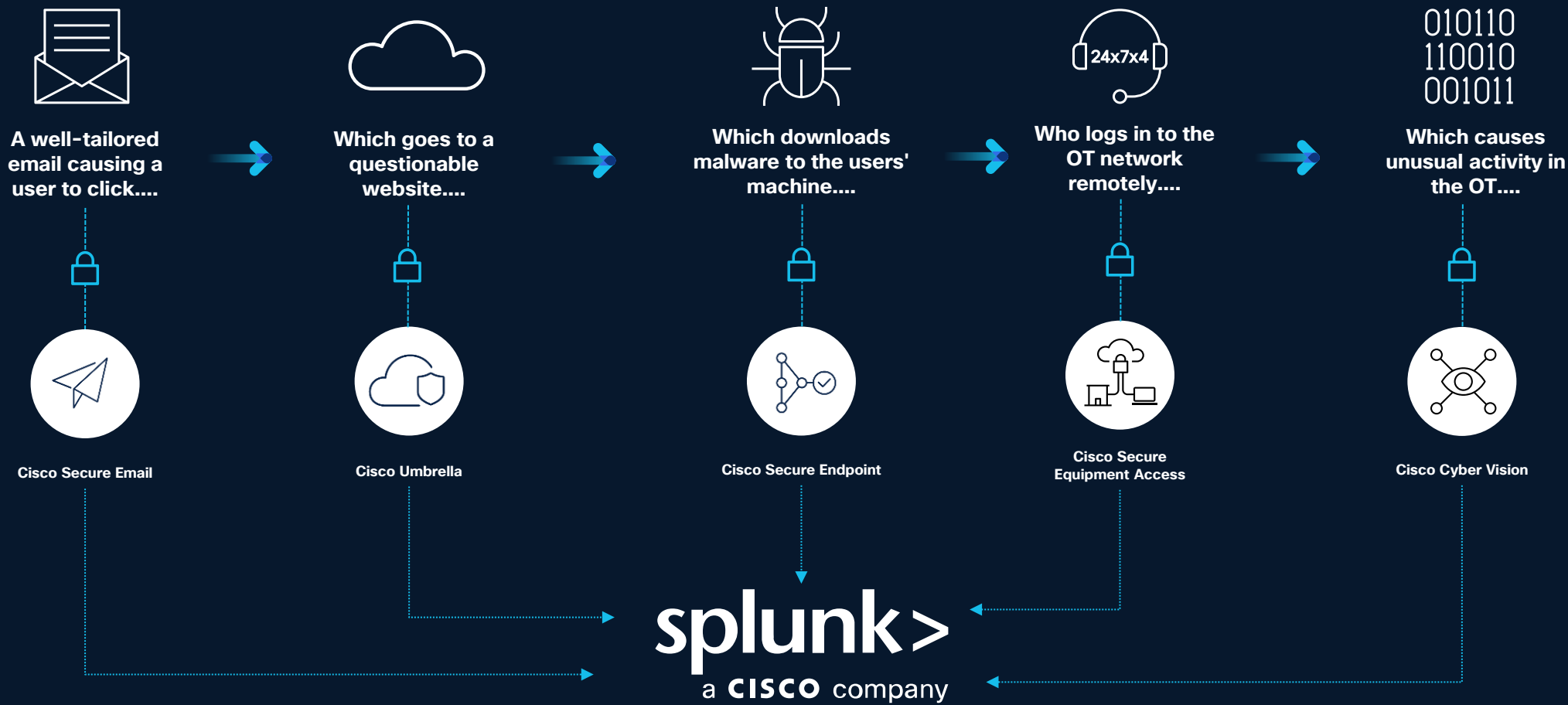
CISA Warns of Flaws Affecting Industrial Control Systems from Major Manufacturers

👤 Ravie Lakshmanan 📅 Jan 16, 2023

Industrial Control Systems

A siloed approach is not enough to secure OT

Detecting threats requires cross-domain visibility

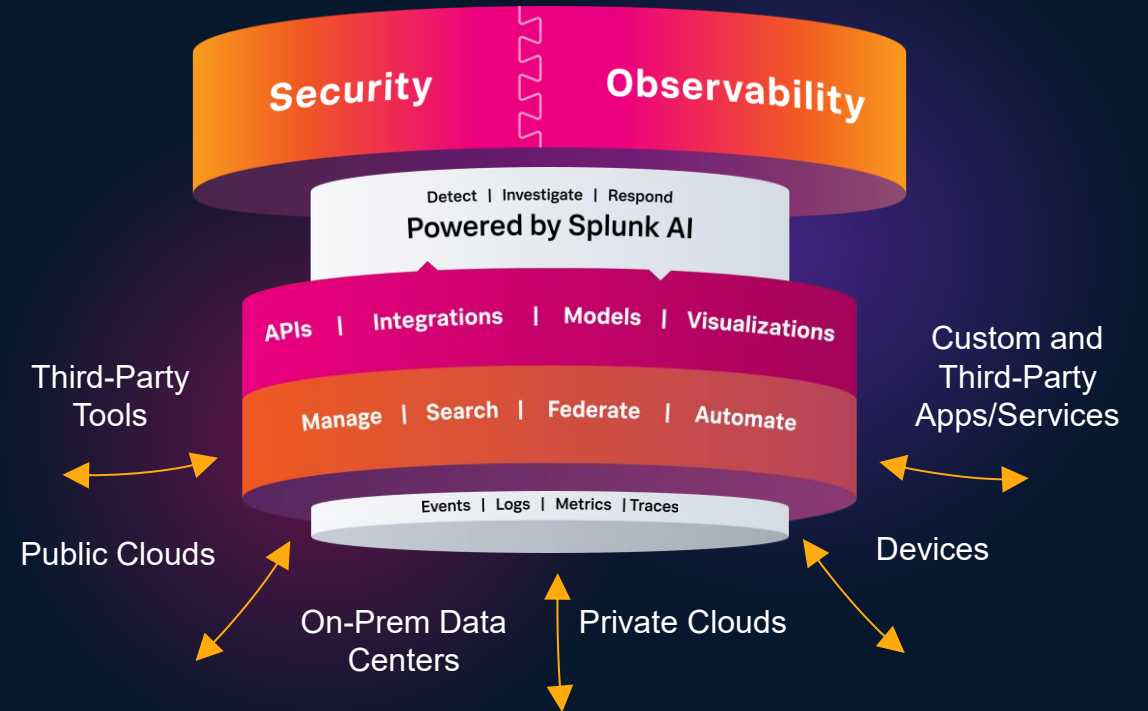


What is Splunk?

Splunk Security focuses on finding, investigating and stopping threats

Splunk Observability helps understand the health and performance of systems and applications, to eliminate downtime and find the root cause of failures

Digital resilience is important in a modern industrial environment. **Security** and **Observability** are two sides of the same coin – you can't have a "safe" factory if it's offline, and you can't have a "high-performing" factory if it's compromised.



Splunk Enterprise has two core components – SIEM & SOAR

Security Information & Event Management (SIEM) is a central hub that collects and analyses log data from across your entire network to detect suspicious activity and provide real-time security alerts.

Security Orchestration, Automation & Response (SOAR) takes SIEM alerts a step further by using automated "playbooks" to coordinate and execute rapid responses to threats without needing manual intervention for every task

The focus of this presentation will be Splunk's SIEM capabilities

Splunk Enterprise is not the same as Splunk Enterprise Security

Splunk Enterprise

The full name of the product. This is the foundational software.

- ✓ Collect and Index Data
- ✓ Search, Analyze and Visualize
- ✓ Monitor, Alert and Report
- ✓ Powerful App Library

Cyber Vision App runs on Splunk Enterprise

Splunk Enterprise Security 8.0

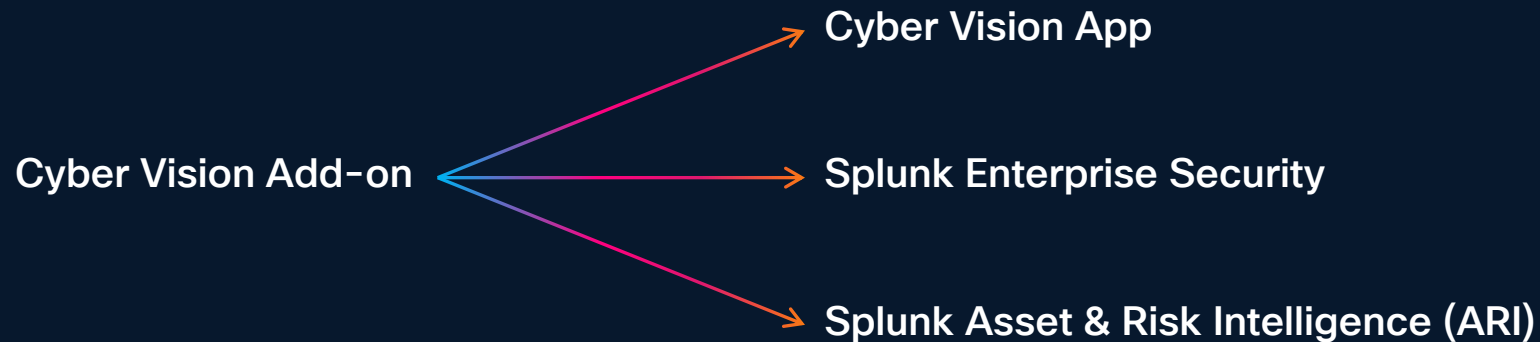
A premium app that sits on top of Splunk Enterprise

- ✓ Complete TDIR platforms
- ✓ Native Splunk SOAR integrations
- ✓ Detection Engineering
- ✓ Risk Based Alerting
- ✓ MITRE ATT&CK visualizations
- ✓ Splunk OT Security

Add-ons are for the system, Apps are for Humans

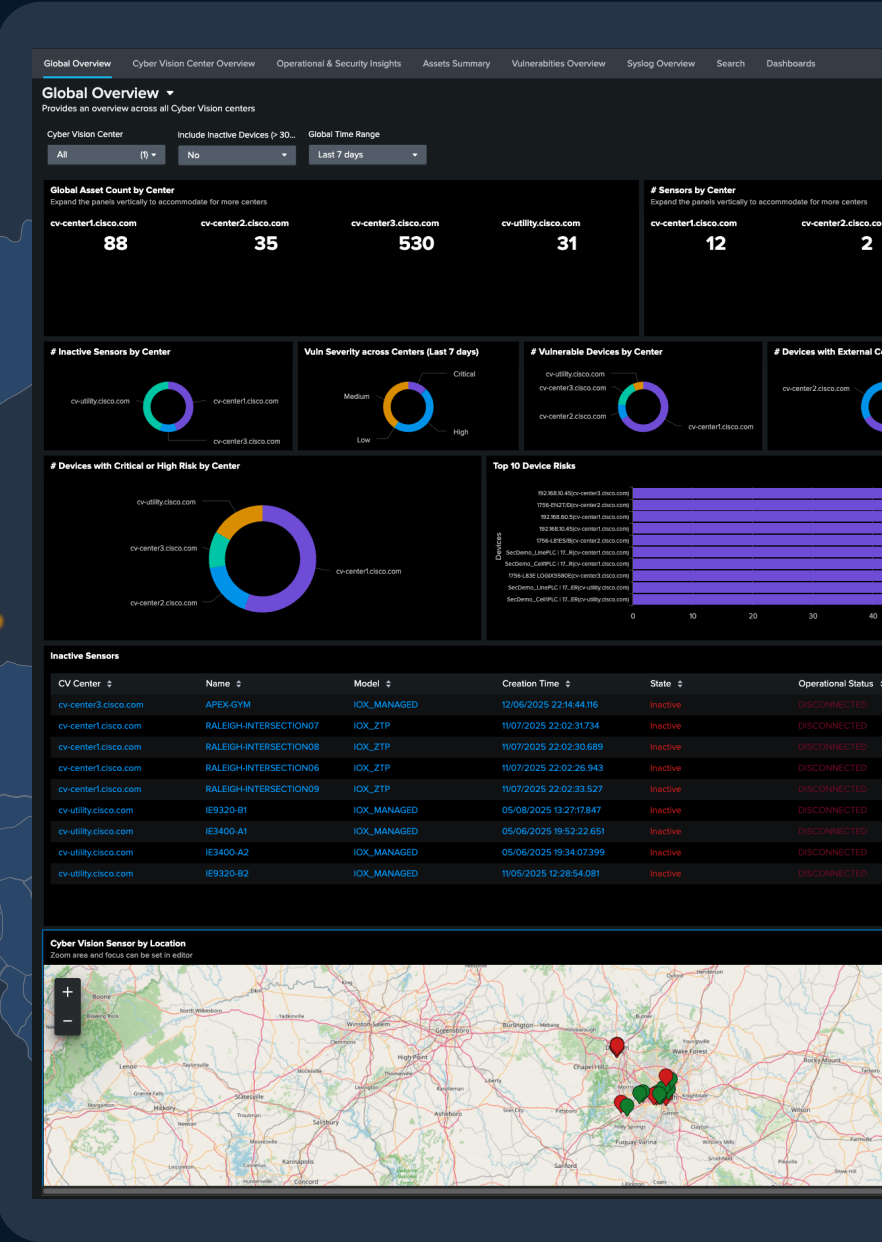
Cyber Vision Add-on is a background process that contains data parsing rules, field extractions, and configurations to ingest data from Cyber Vision correctly

Cyber Vision App contains dashboards, reports, saved searches and custom navigation menus so humans can make use of the data ingested by the add-on



Introducing the New Cyber Vision App

- ✓ Aggregate all Cyber Vision deployments
- ✓ Focused view per local center
- ✓ Operational & Security Overview
- ✓ Vulnerabilities Overview
- ✓ Real Time Syslog Collection
- ✓ Schedule reports over email



The background of the slide is a dark blue field filled with dynamic, flowing light streaks. These streaks are primarily in shades of bright blue and cyan, with some warmer orange and pinkish tones visible in the upper right quadrant. The lines are curved and layered, creating a sense of depth and movement, reminiscent of light trails or data flow.

Demo

Complete your session surveys



Complete your surveys in the Cisco Events App.



Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Contact us at: kakamra@cisco.com , anmcphee@cisco.com

Thank you

CISCO Live !

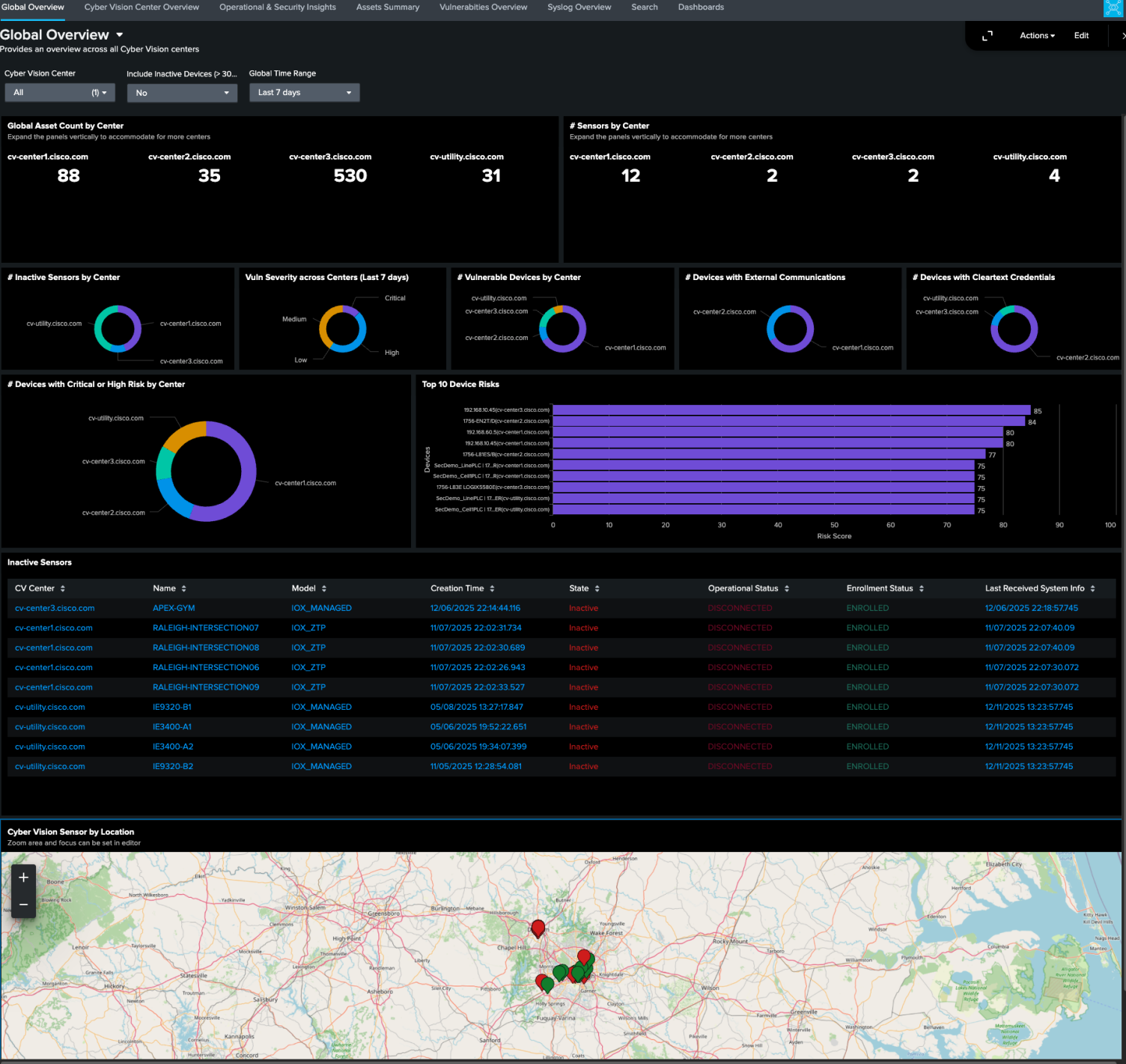


**Backup slides if demo has
connection issues**

Cyber Vision Splunk App

A Global Overview across your entire installation

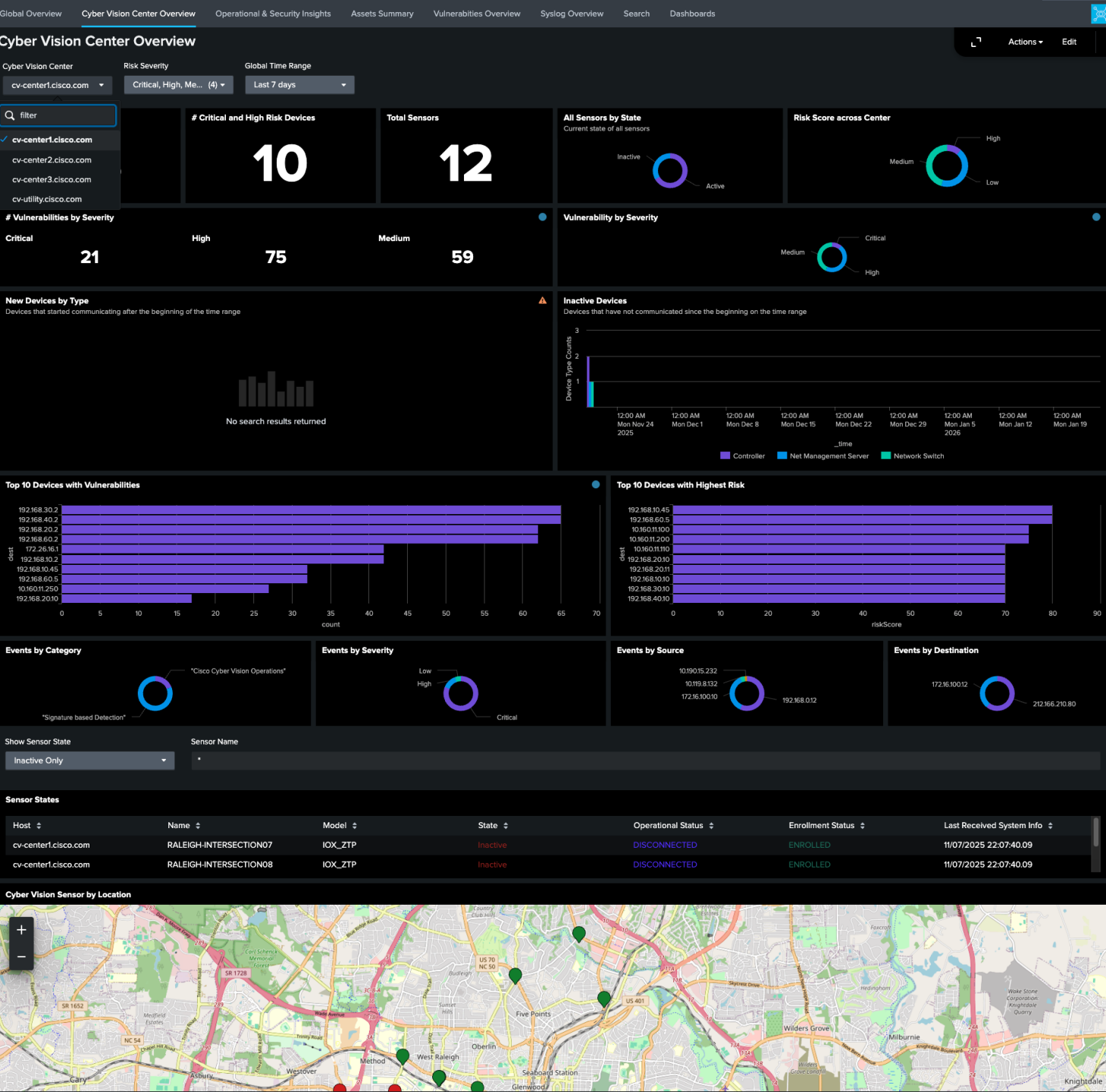
Aggregate data from all local Cyber Vision Centers in a single platform



Cyber Vision Splunk App

Focused views per Local Center

Dedicated screens for each local
instance when further analysis is
required



Cyber Vision Splunk App

Operational & Security Overview

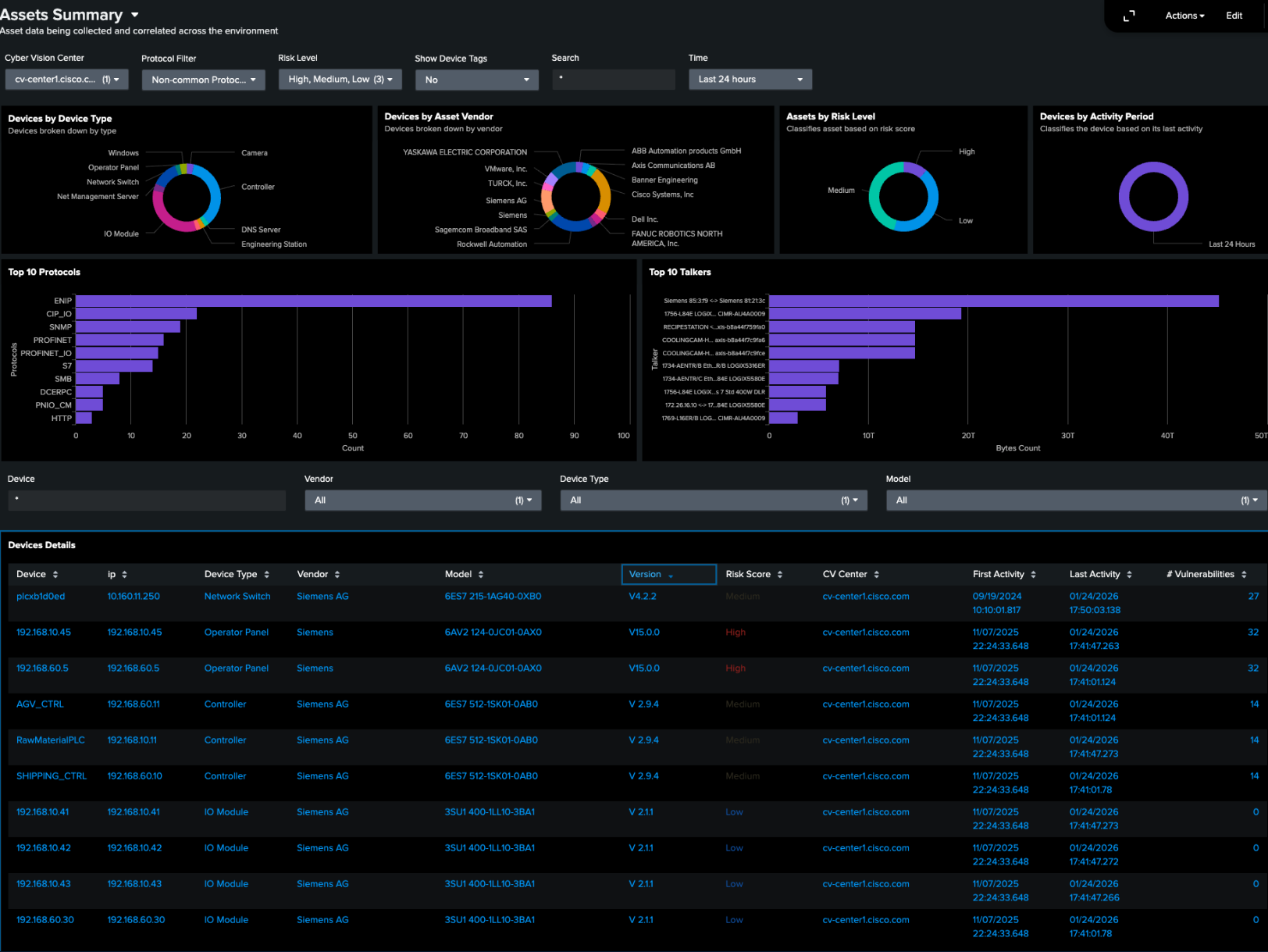
Aggregated view of security events with a timeline view to understand origin and impact



Cyber Vision Splunk App

Asset Summary

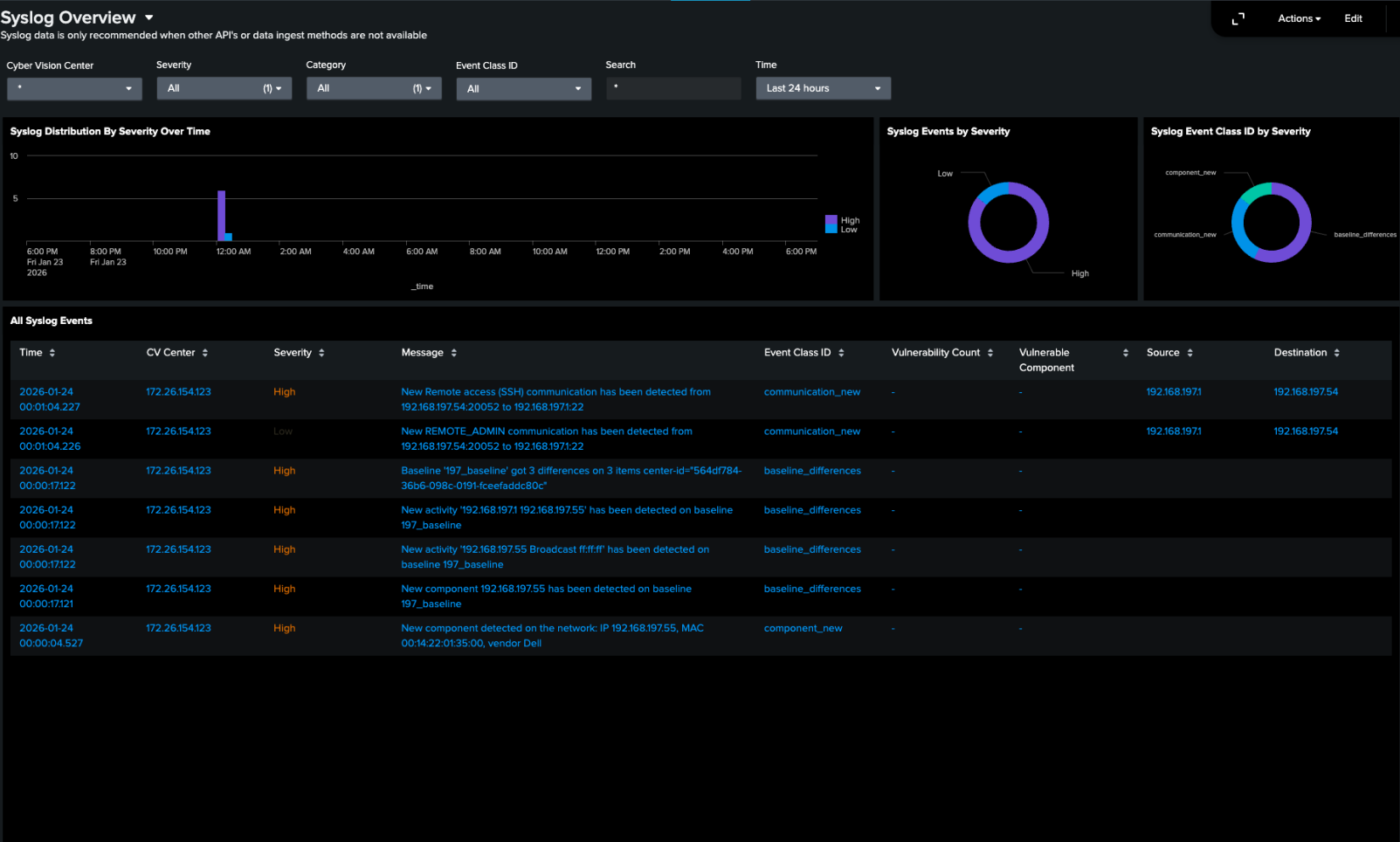
Help understand which assets need refreshed & identify risky vendors in your deployment



Cyber Vision Splunk App

Real Time Syslog Collection

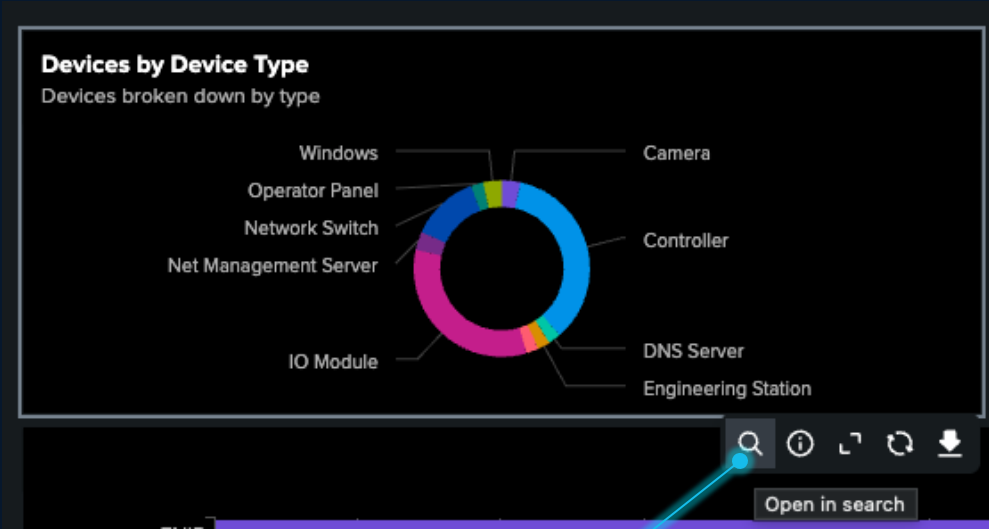
Customize your alerts to be notified immediately of events that matter the most to you



Cyber Vision Splunk App

Build your own dashboard

All graphs are powered by Splunk Processing Language (SPL).
Customize the search and save your own



New Search

source="cybervision:devices" host IN (cv-center1.cisco.com) risk_score_severity IN (High,Medium,Low) "*" | fields id, label, ip, vulnerabilitiesCount, asset_type, asset_vendor, asset_model, asset_version, risk_score_severity, host, lastActivity, firstActivity, device_tag | dedup 'deduplicate_device_fields' | stats count as "# Devices" by asset_type

88 events (23/01/2026 18:00:00.000 to 24/01/2026 18:45:09.000) No Event Sampling

asset_type	# Devices
Camera	3
Controller	31
DNS Server	2
Engineering Station	2
HTTP Client	2
IO Module	29
Net Management Server	3
Network Switch	11
Operator Panel	2
Windows	3

Complete your session surveys



Complete your surveys in the Cisco Events App.



Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Thank you

CISCO Live !

