Enhancing Splunk with OT context using Cisco Cyber Vision

Andrew McPhee
IIoT Security Solution Manager

Kartik Kamra
IIoT Security Product Manager

BRKIOT-2846

Webex App

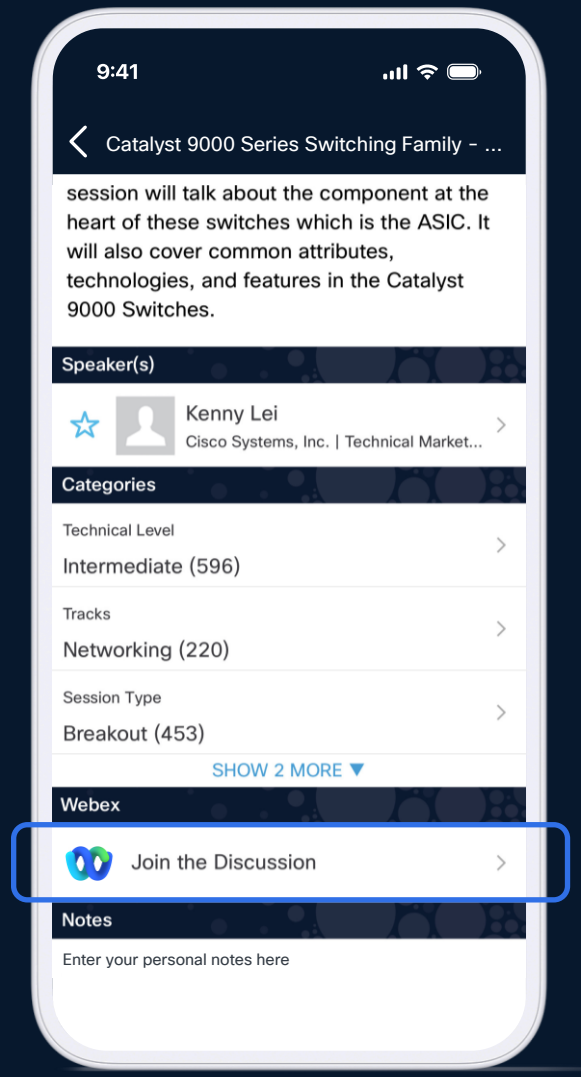
Questions?

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.



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

Cisco Confidential

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

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

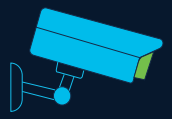
Cisco Confidential

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

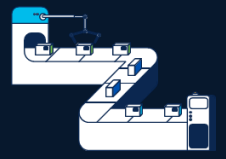
2024 State of Industrial Networking Report

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

Cisco Confidential



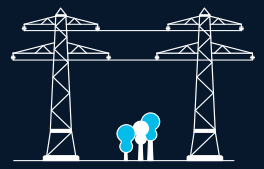
Security and facilities



Warehouse automation

Industrial automation

Energy management



Utilities

Patient monitoring

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

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

Cisco Confidential

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

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

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

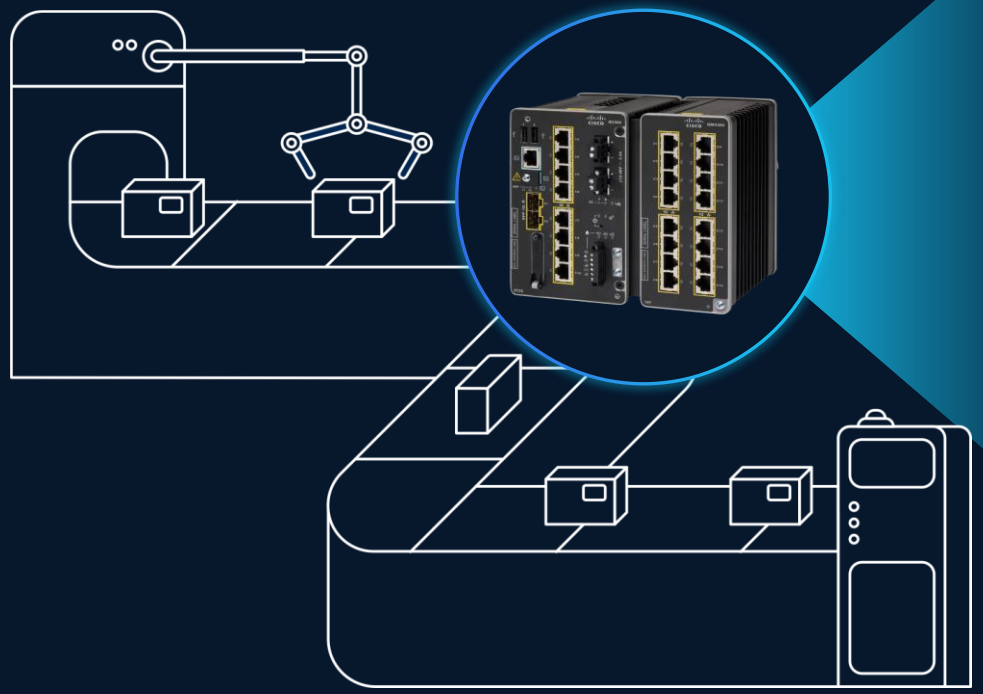
AI-Assisted Malware Evolves into a Daily Threat

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

Cisco Confidential

Cisco Industrial Security

Security fused into the network to protect OT at scale



OT Visibility
embedded in
network equipment

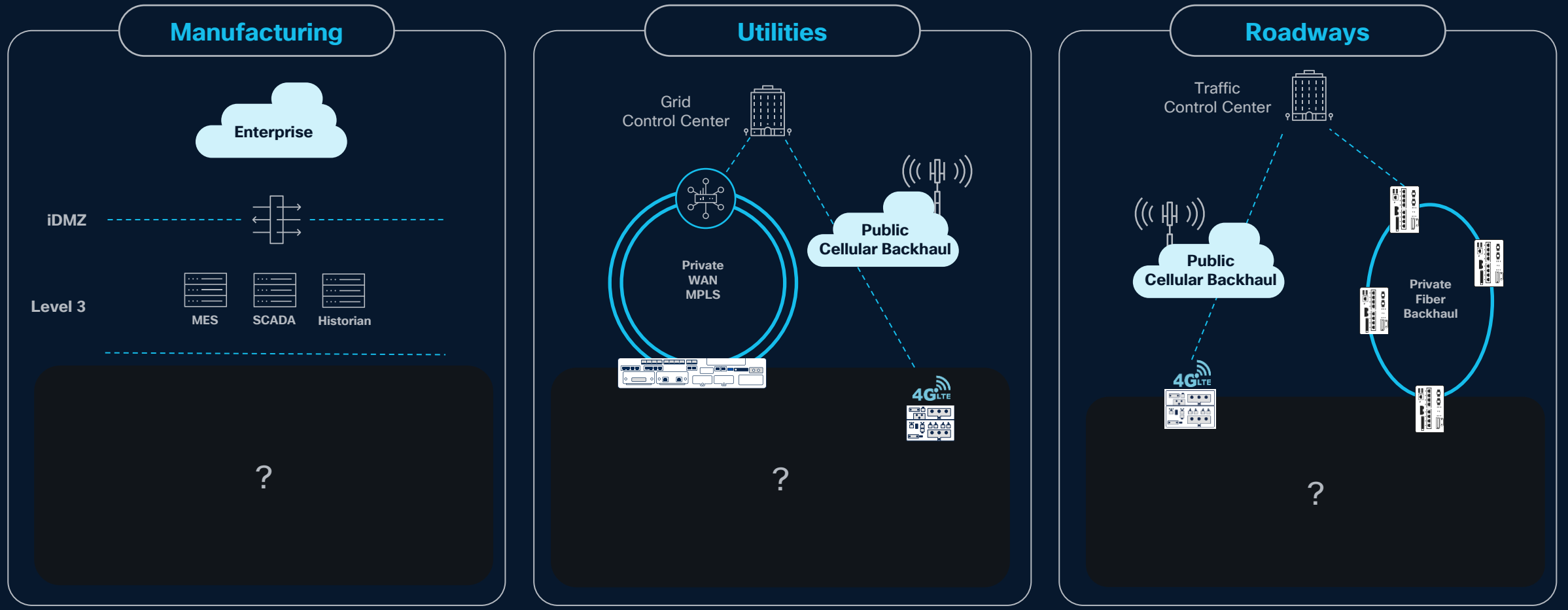
Segmentation
enforced by
network equipment

Secure Remote Access
embedded in
network equipment

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

Cisco Confidential

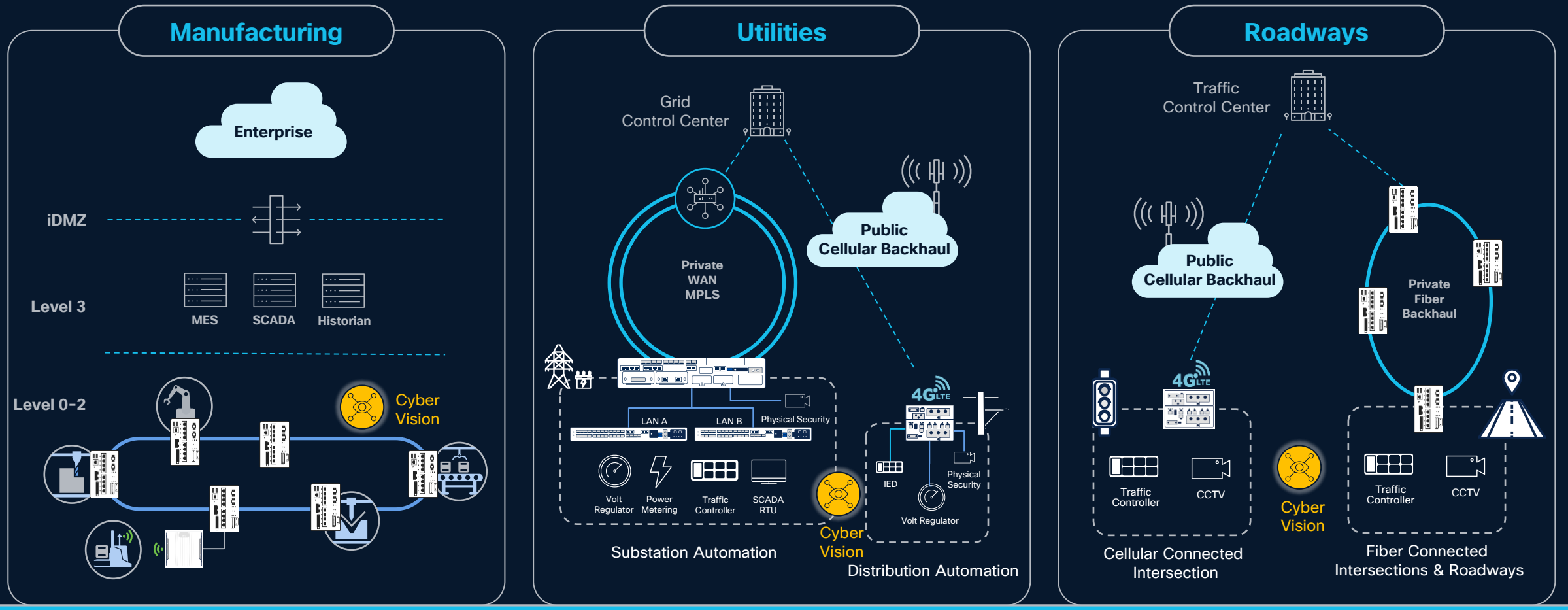
We do not have enough visibility into our most critical assets



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

Cisco Confidential

Cisco Cyber Vision “turns on the lights” for industries



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

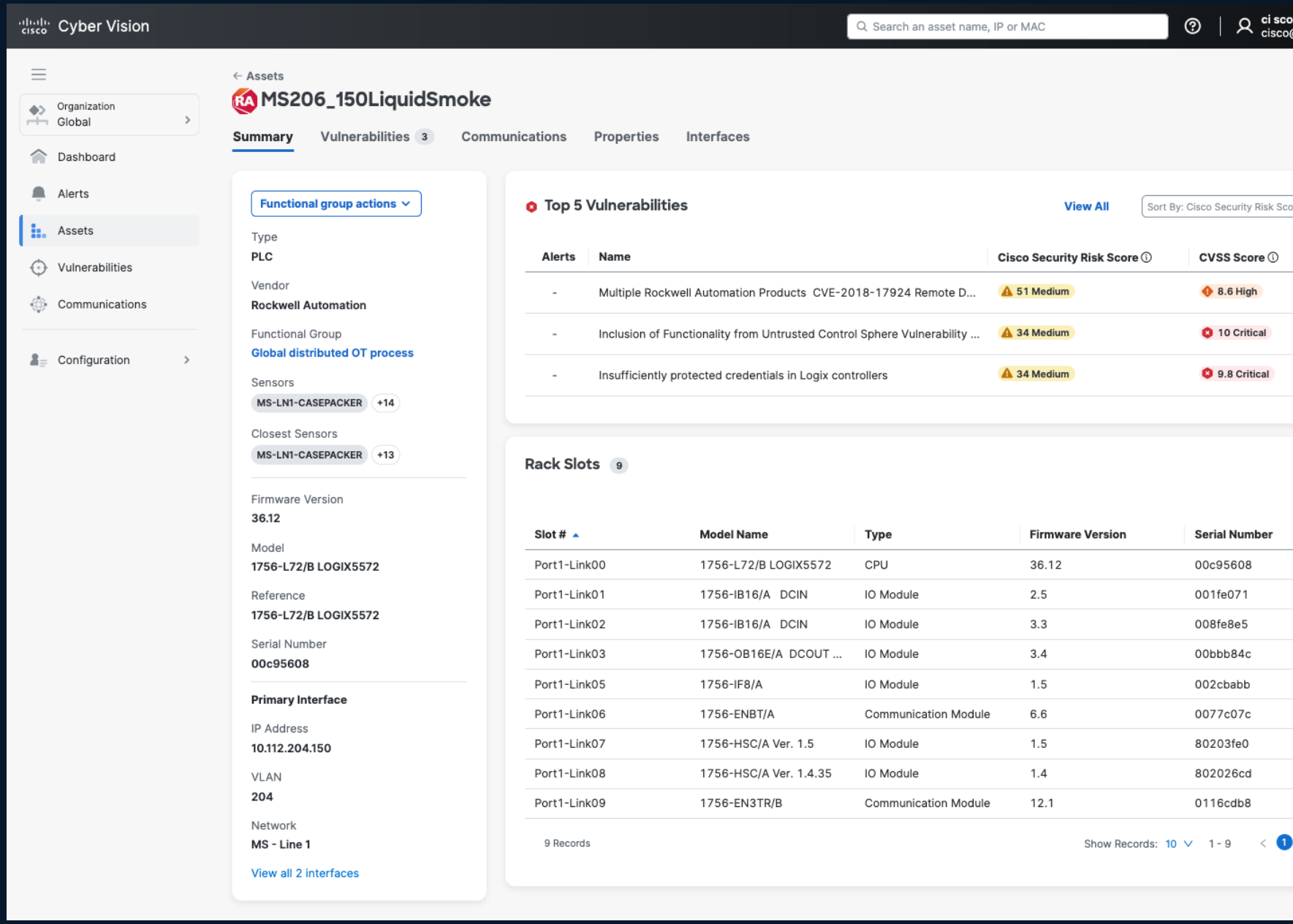
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cyber Vision

Visibility into connected industrial assets

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



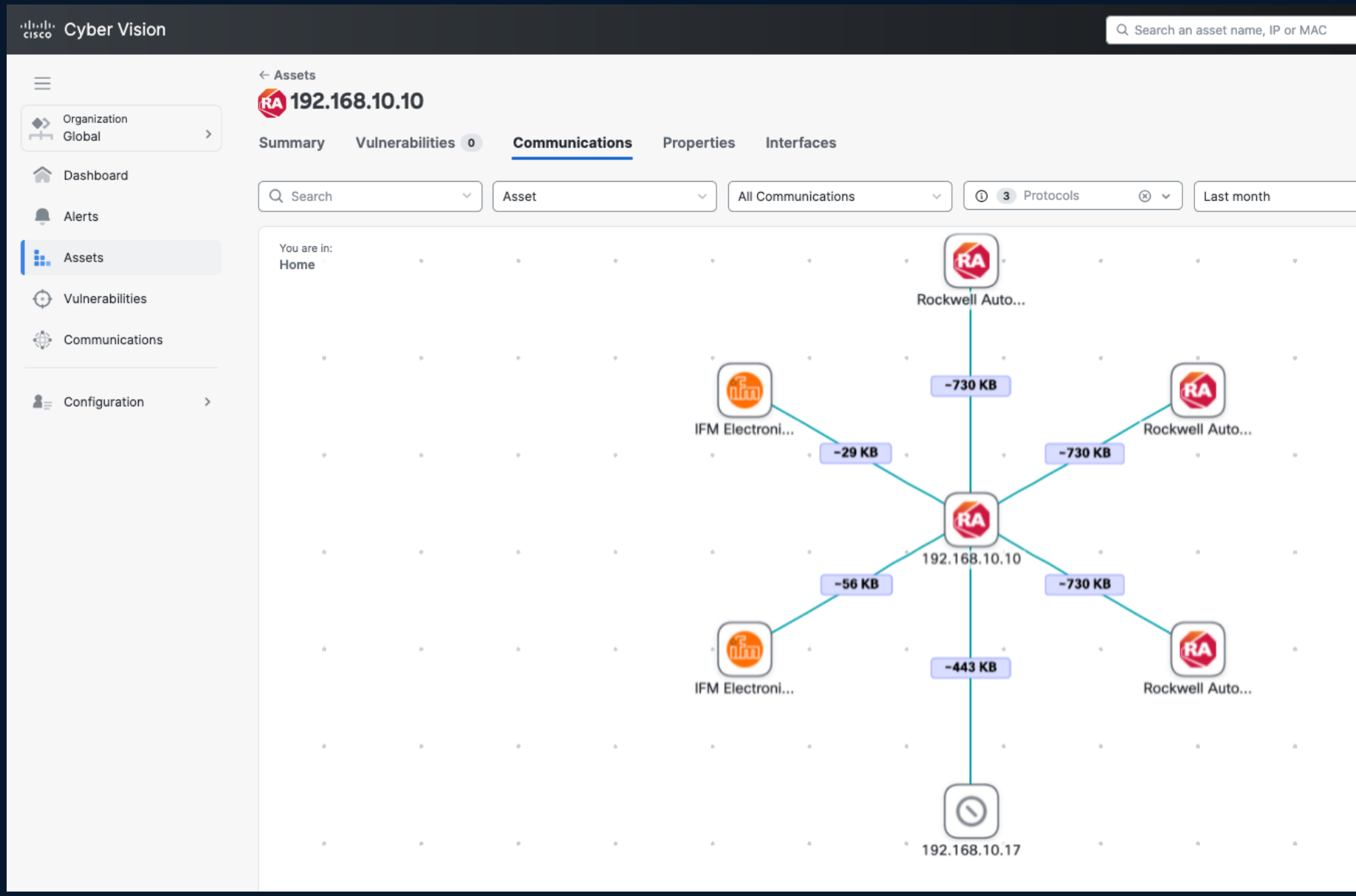
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cyber Vision

Communication Map

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



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

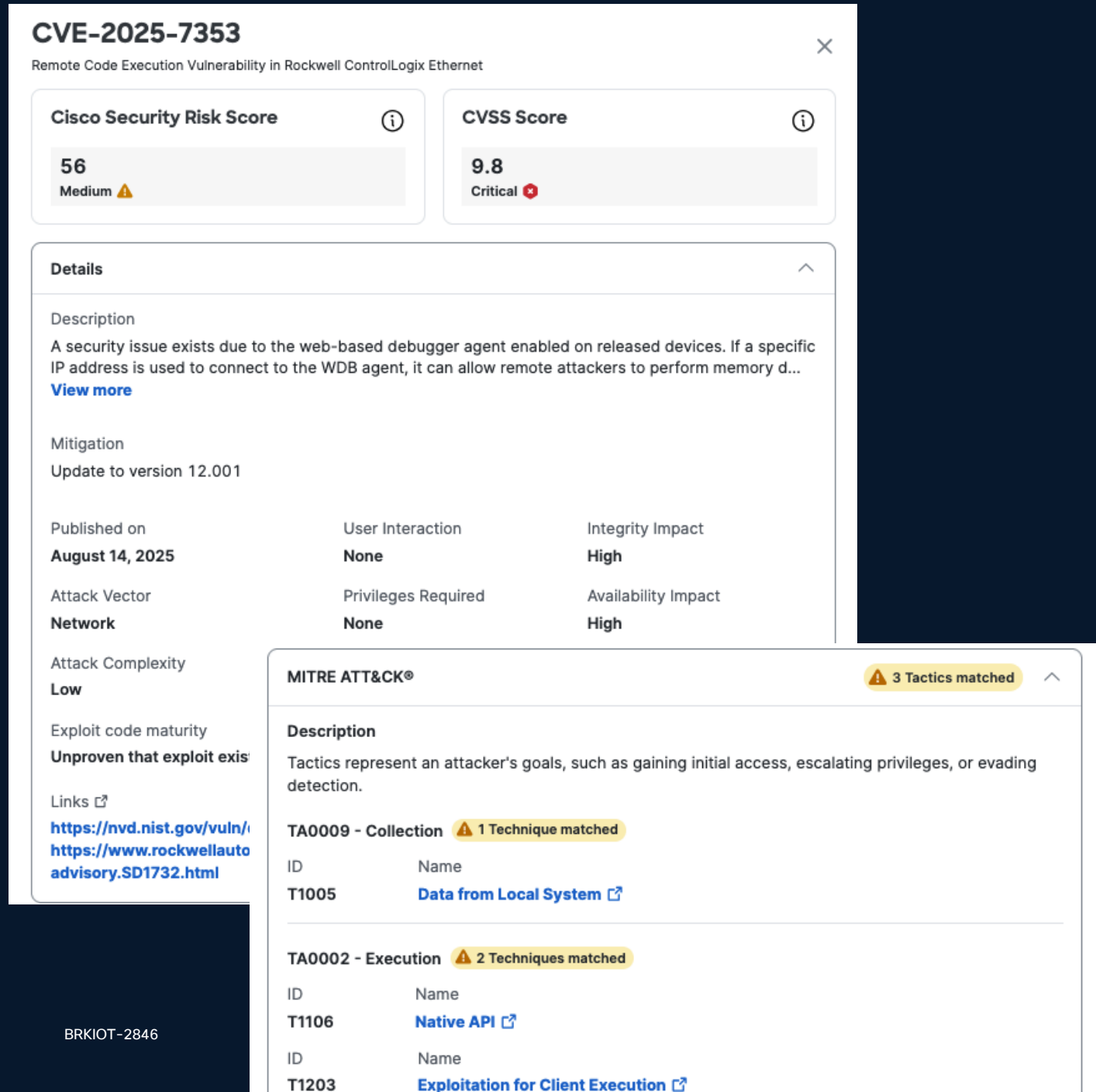
Cisco Confidential

Cyber Vision

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

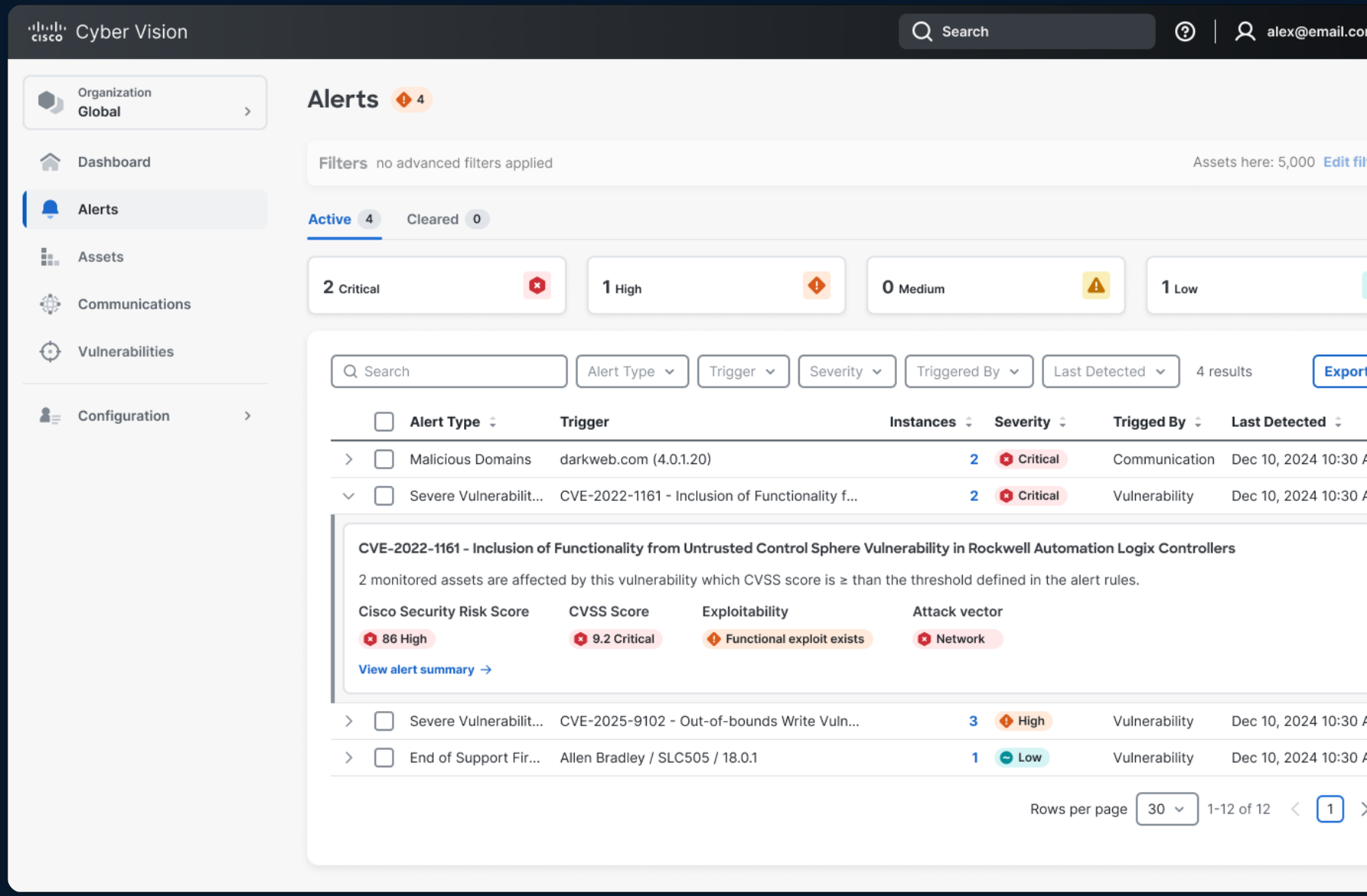


© 2026 Cisco and/or its affiliates. All rights reserved.

Cyber Vision

Alerts

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



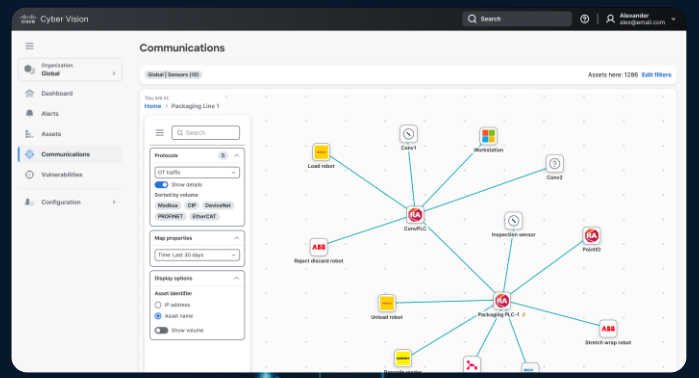
© 2026 Cisco and/or its affiliates. All rights reserved.

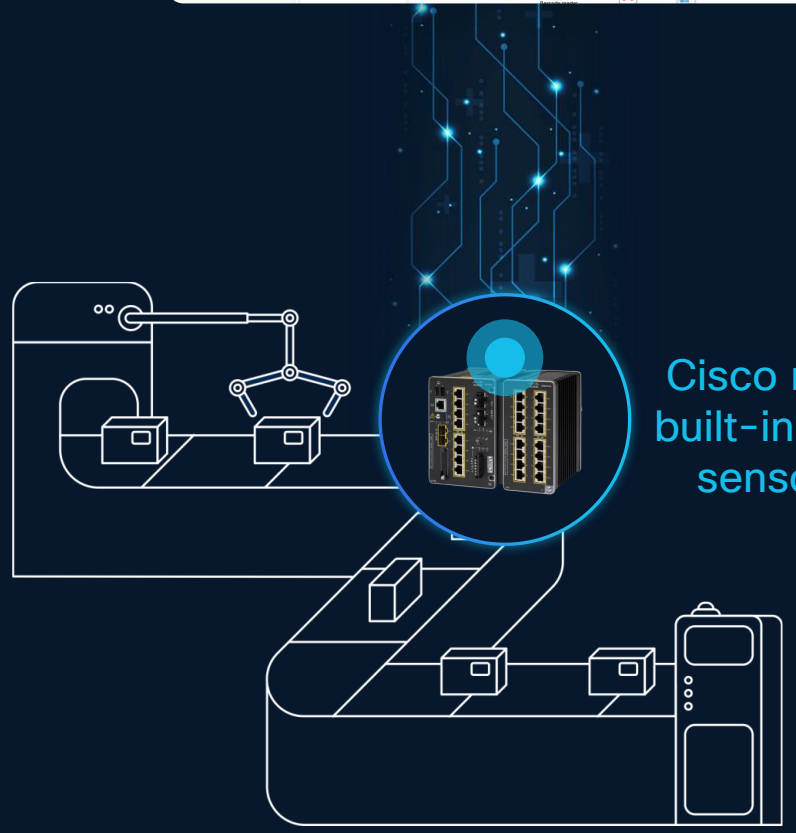
Cisco Confidential

Visibility built-in, not bolted on

- ✓ 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

Cyber Vision Center



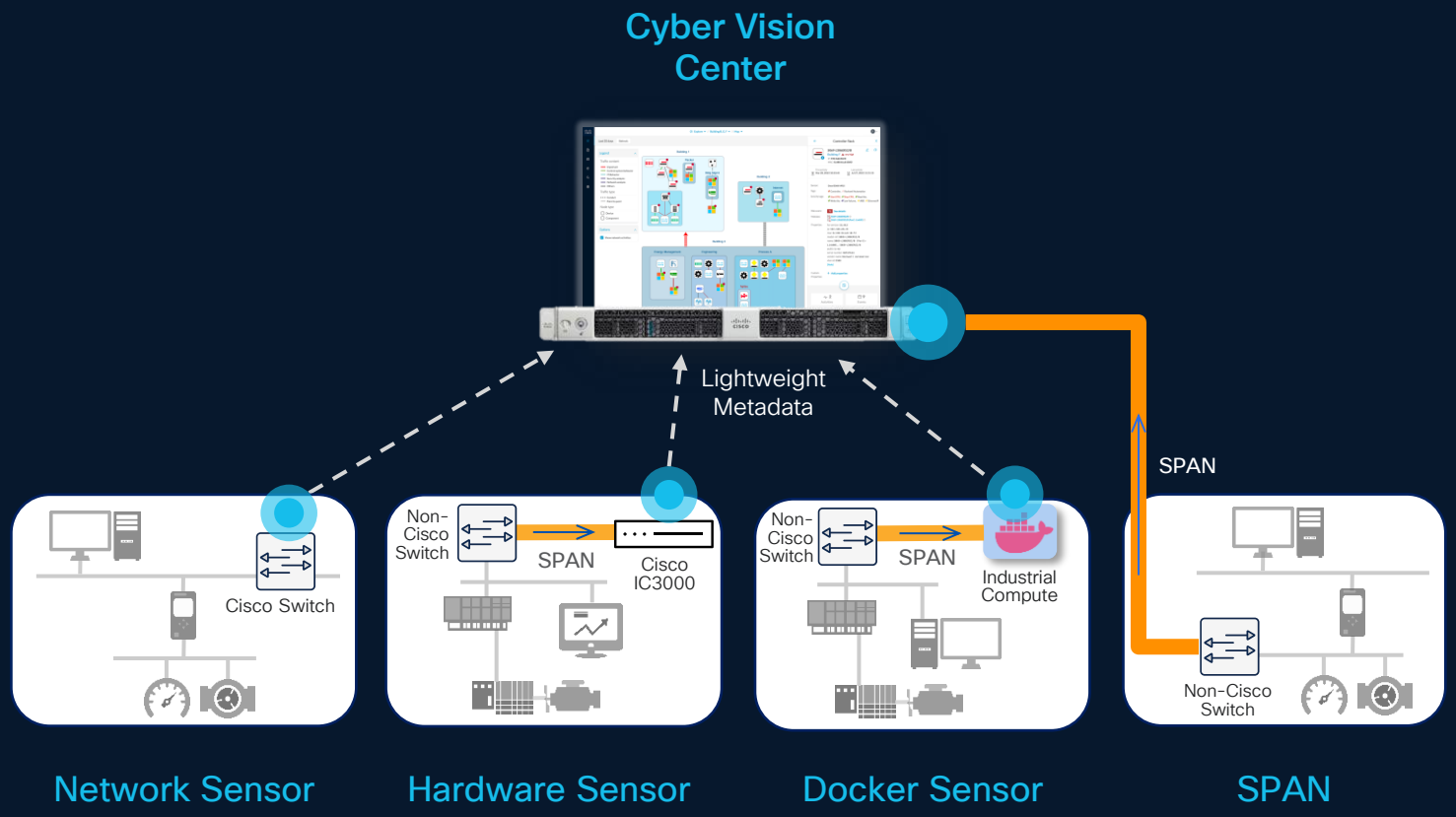


Cisco network with built-in Cyber Vision sensor software

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

Cisco Confidential

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

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

Cisco Confidential

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

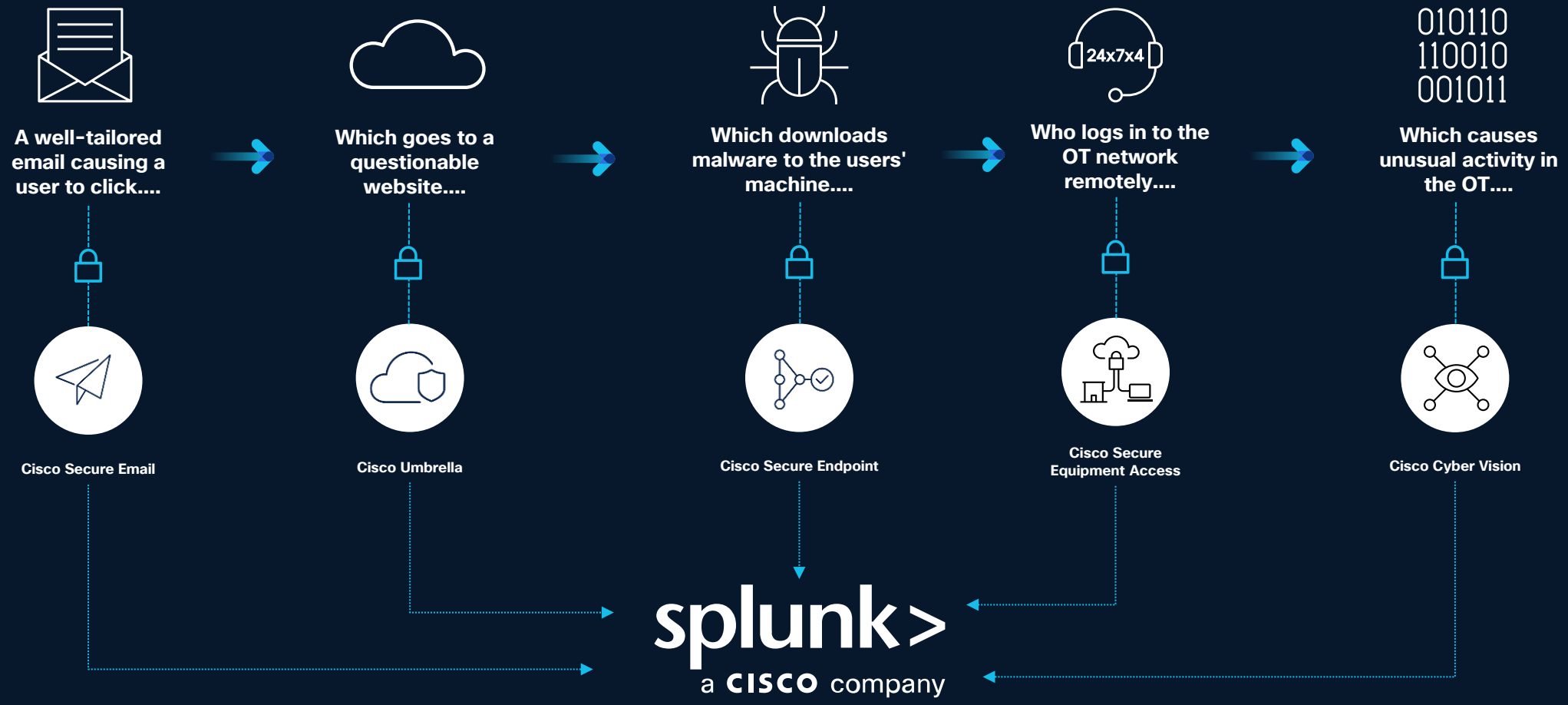
Ravie Lakshmanan Jan 16, 2023 Industrial Control Systems

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

Cisco Confidential

A siloed approach is not enough to secure OT

Detecting threats requires cross-domain visibility



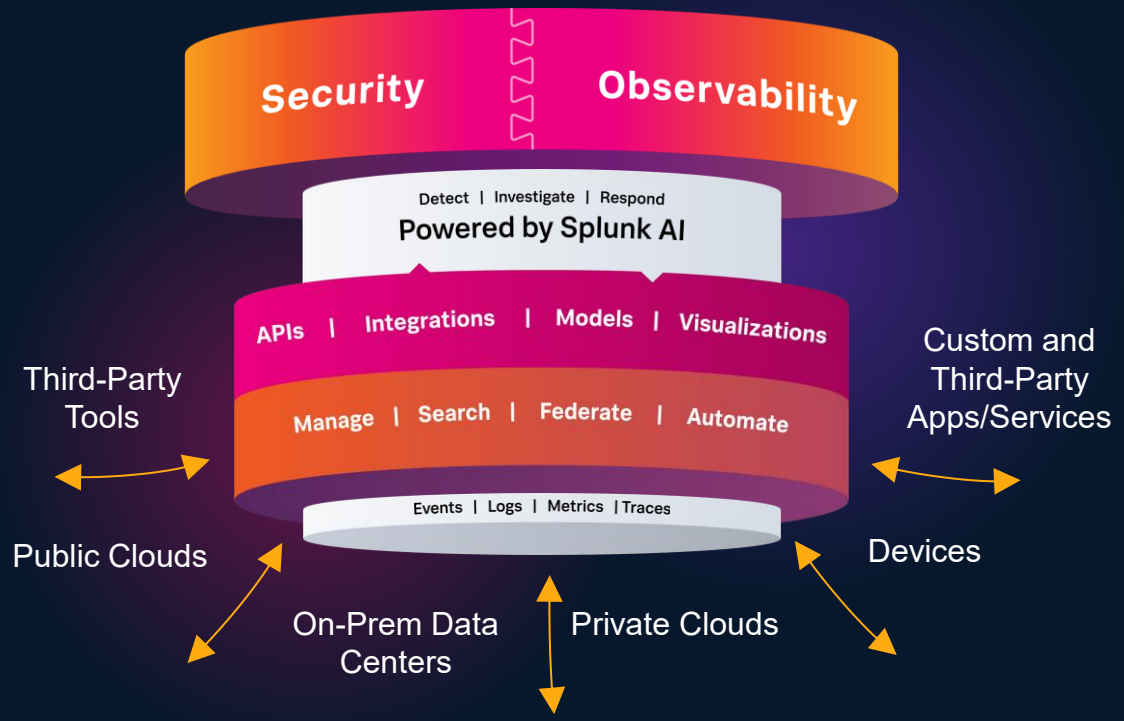
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

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.

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

Cisco Confidential

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

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

Cisco Confidential

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

+ much more

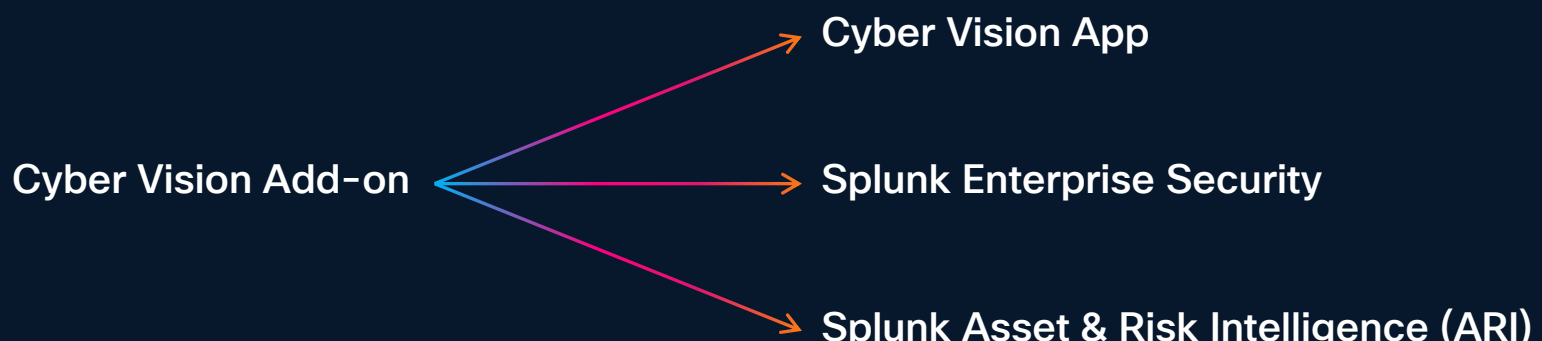
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

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

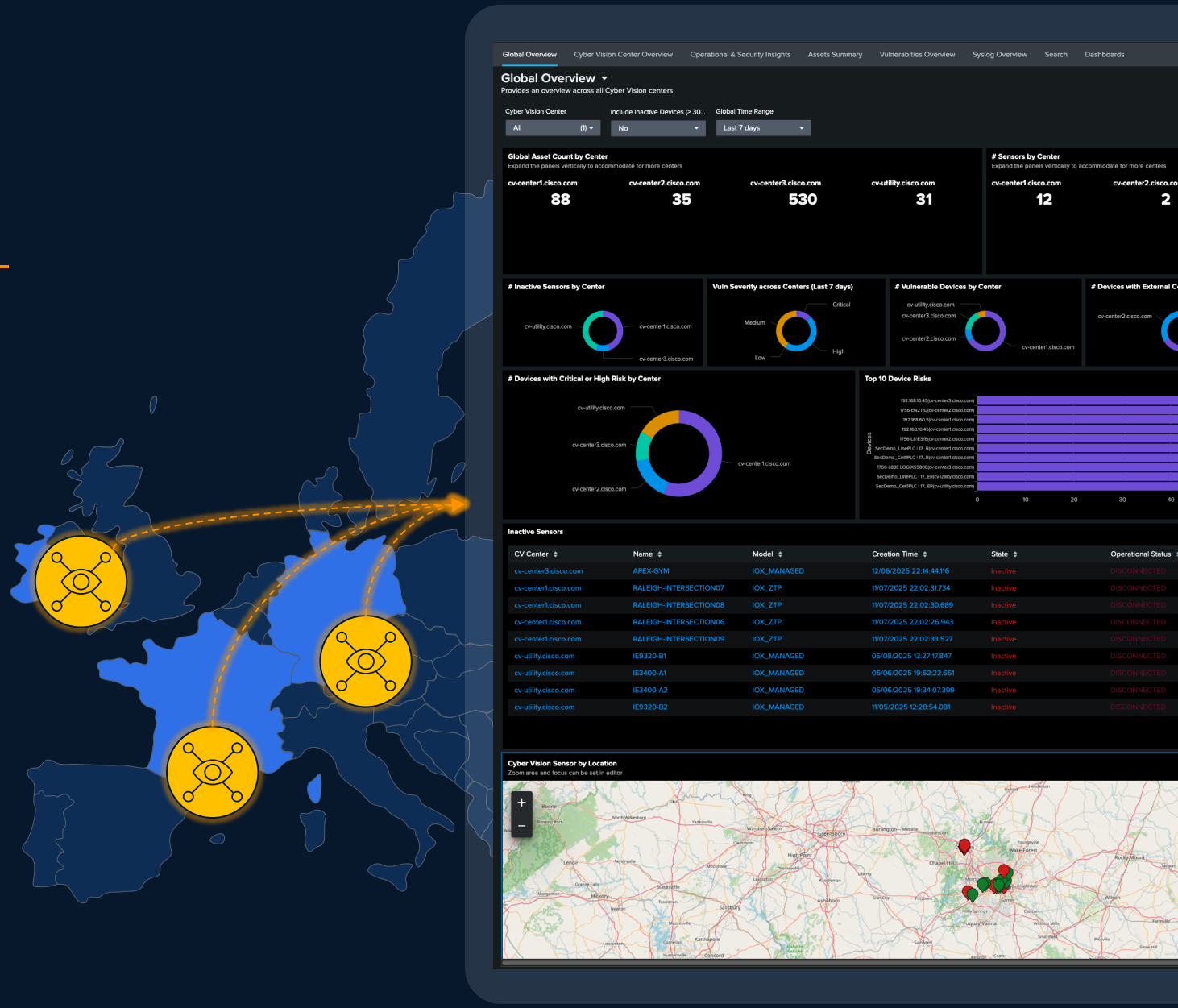


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

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



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

Cisco Confidential

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)

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

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

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

Thank you

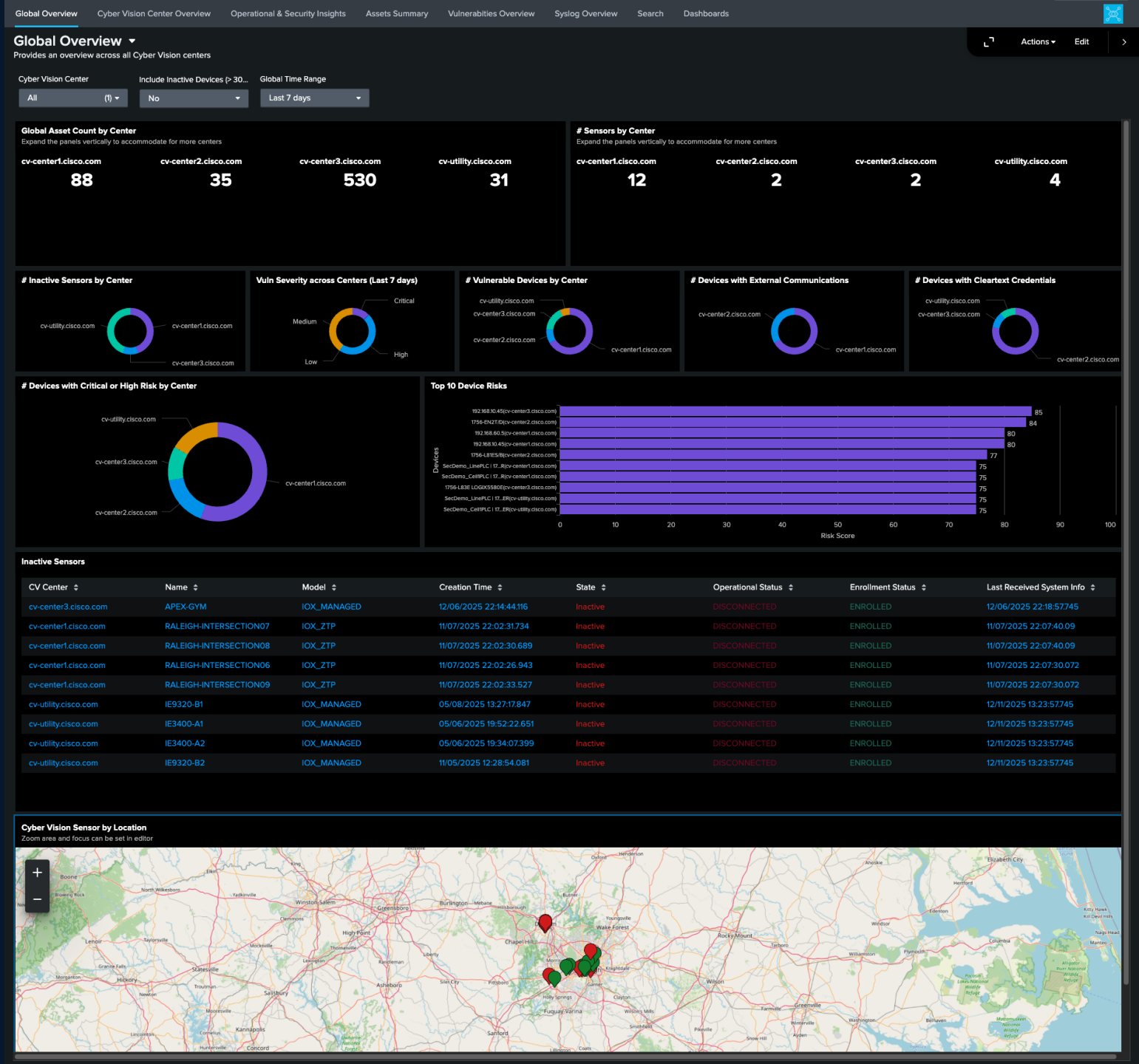

CISCO

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

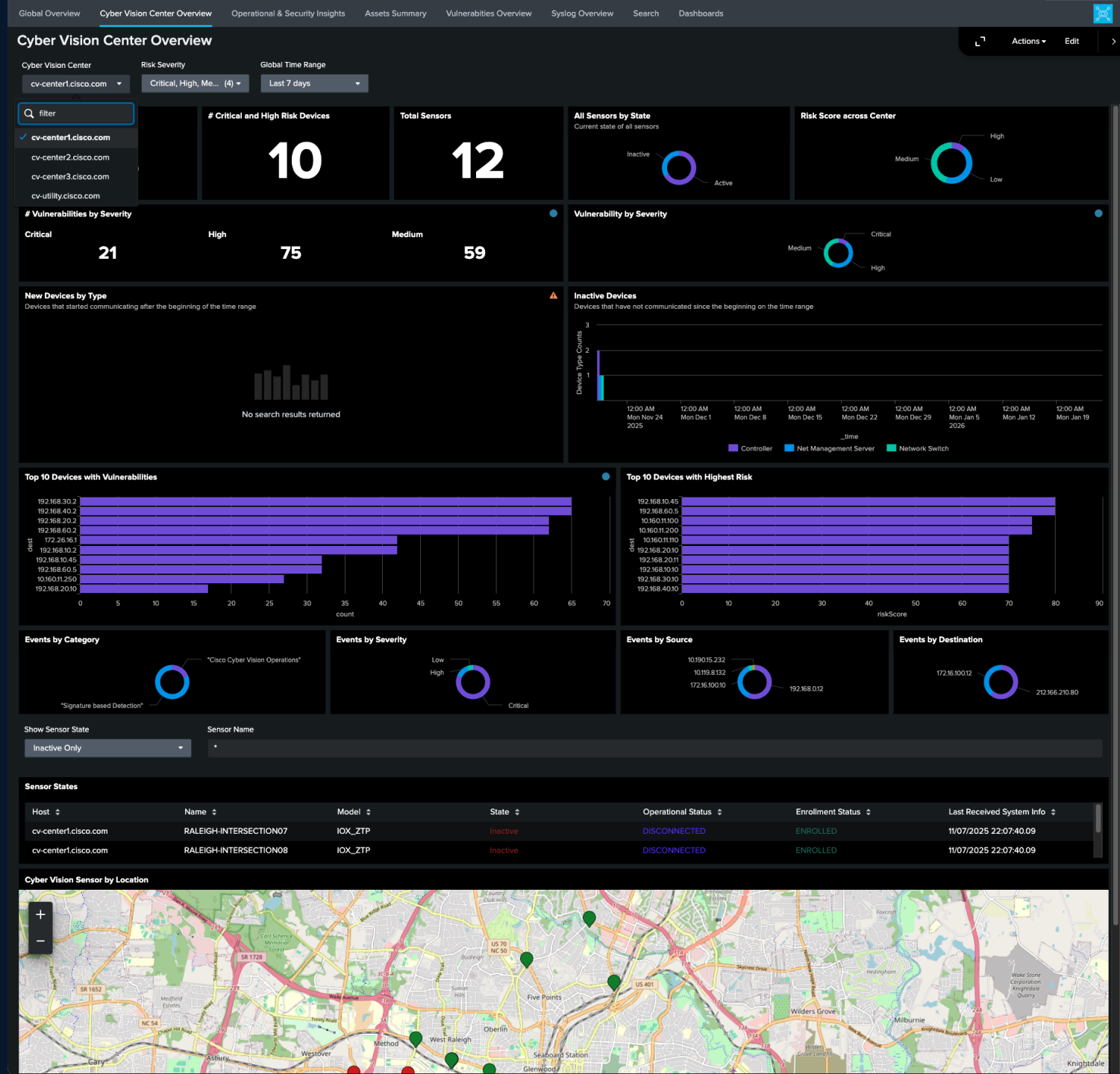


© 2026 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Splunk App

Focused views per Local Center

Dedicated screens for each local instance when further analysis is required

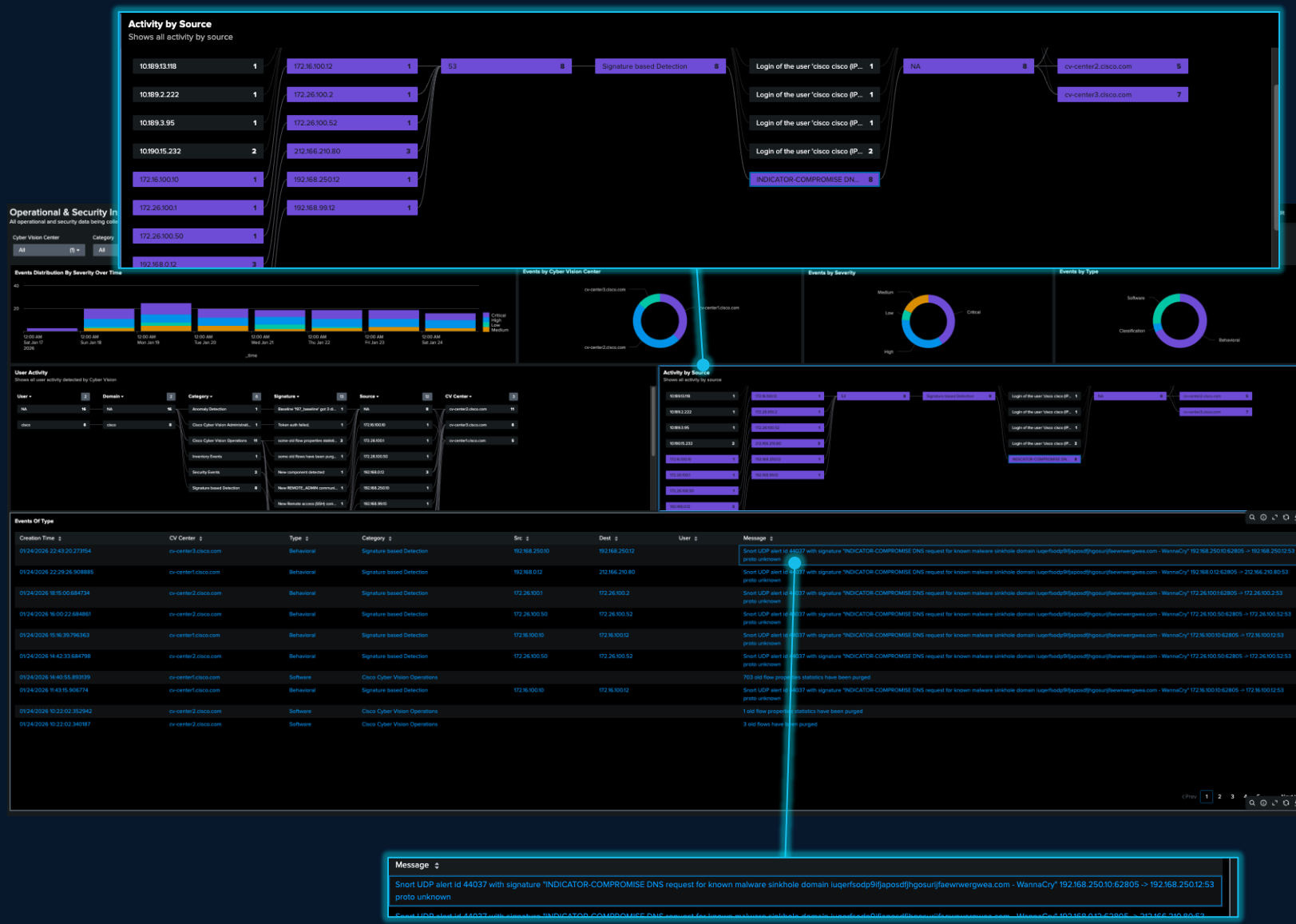


© 2026 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Splunk App

Operational & Security Overview

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



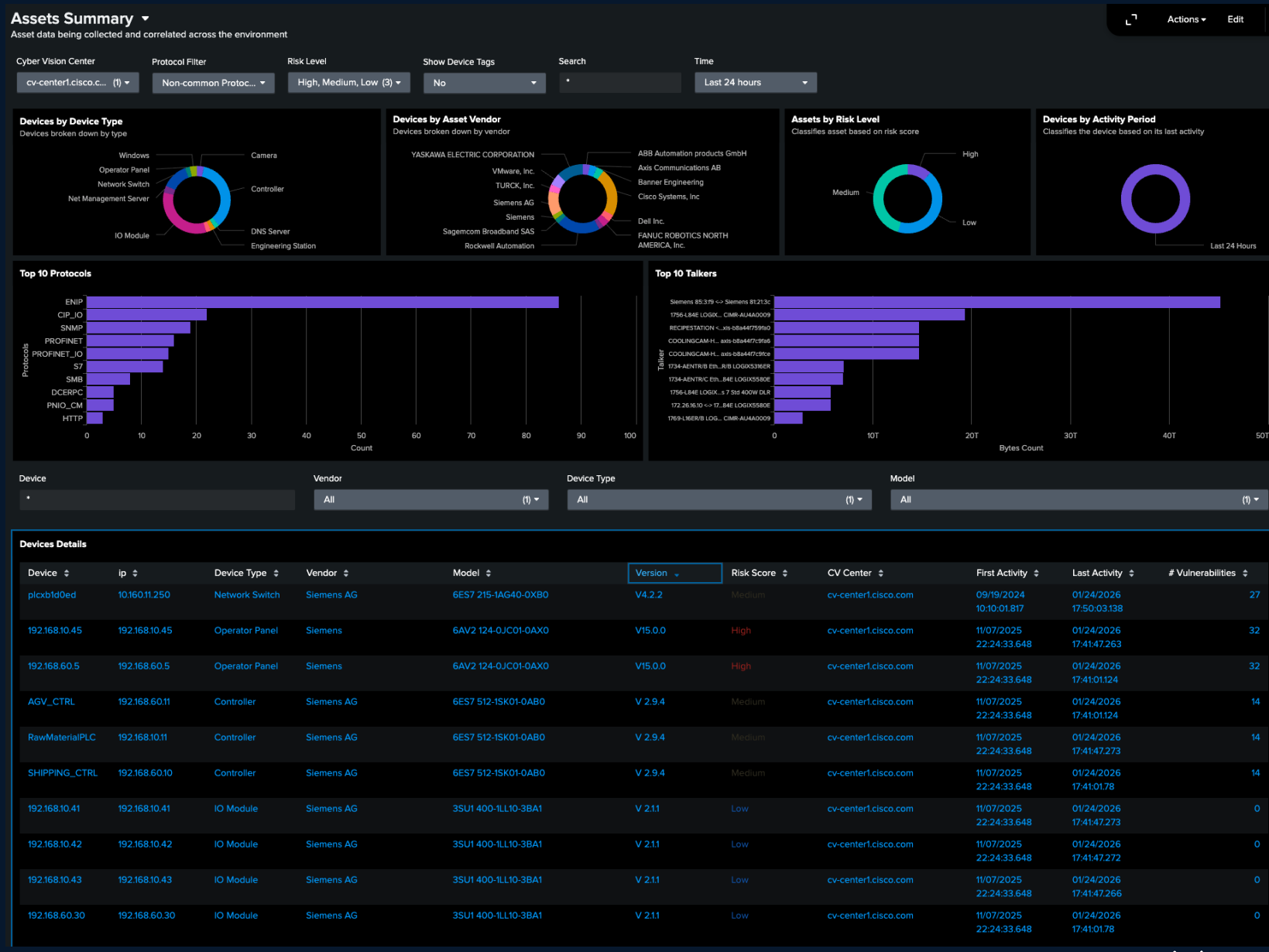
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cyber Vision Splunk App

Asset Summary

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



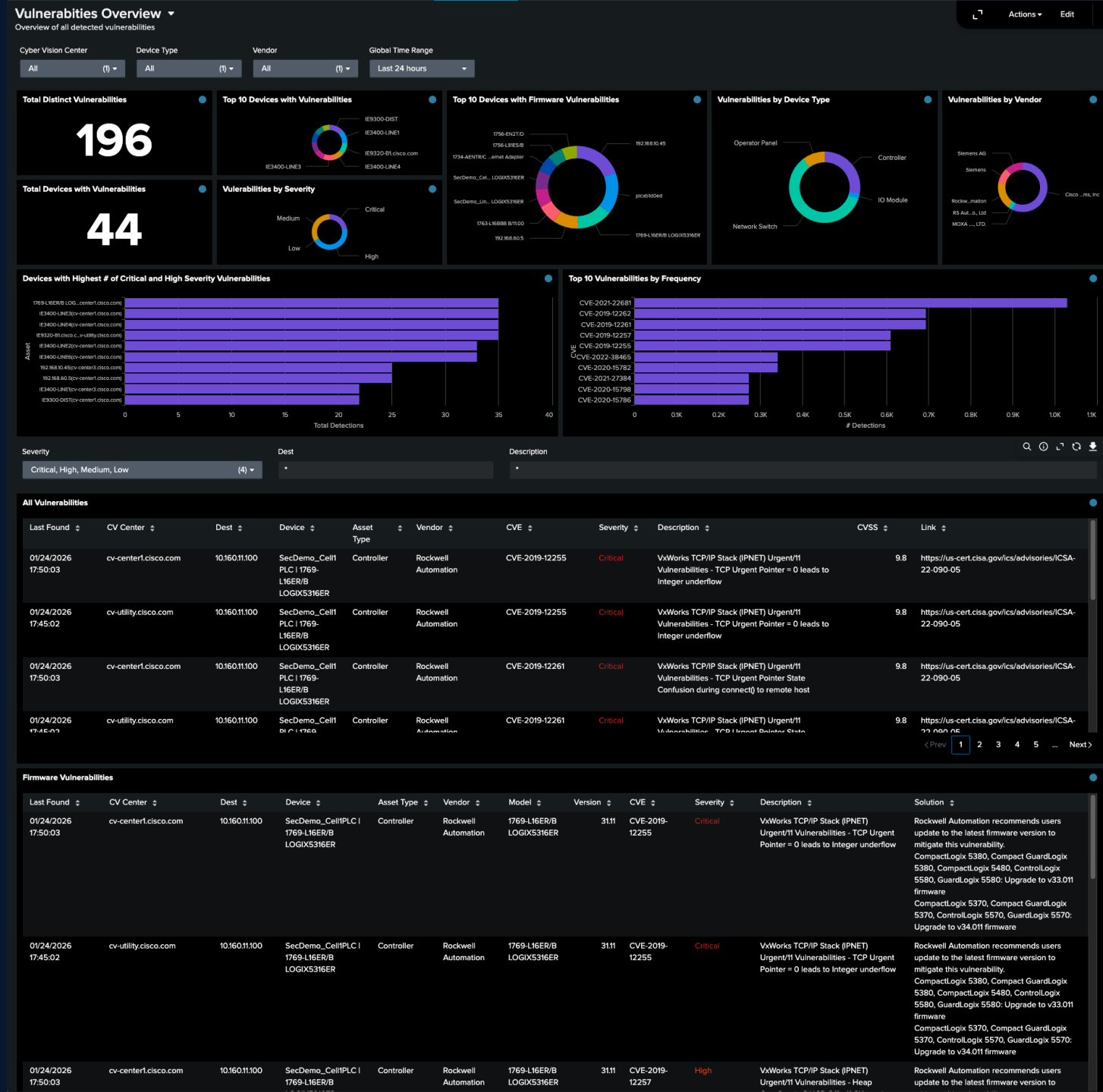
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cyber Vision Splunk App

Vulnerabilities Overview

Identify the riskiest vulnerabilities in my environment & which ones can be eliminated in the next maintenance window

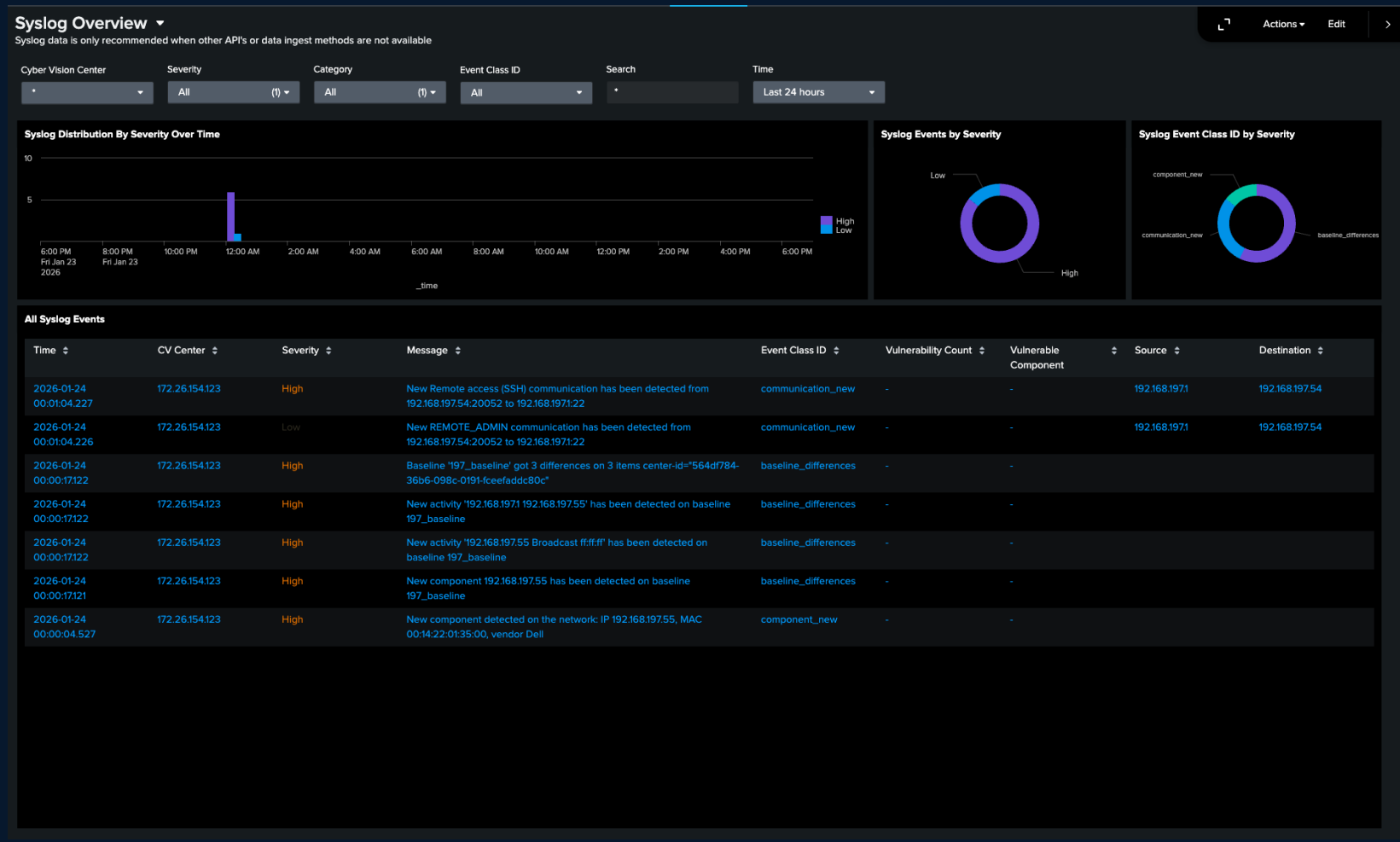


© 2026 Cisco and/or its affiliates. All rights reserved.

Cyber Vision Splunk App

Real Time Syslog Collection

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



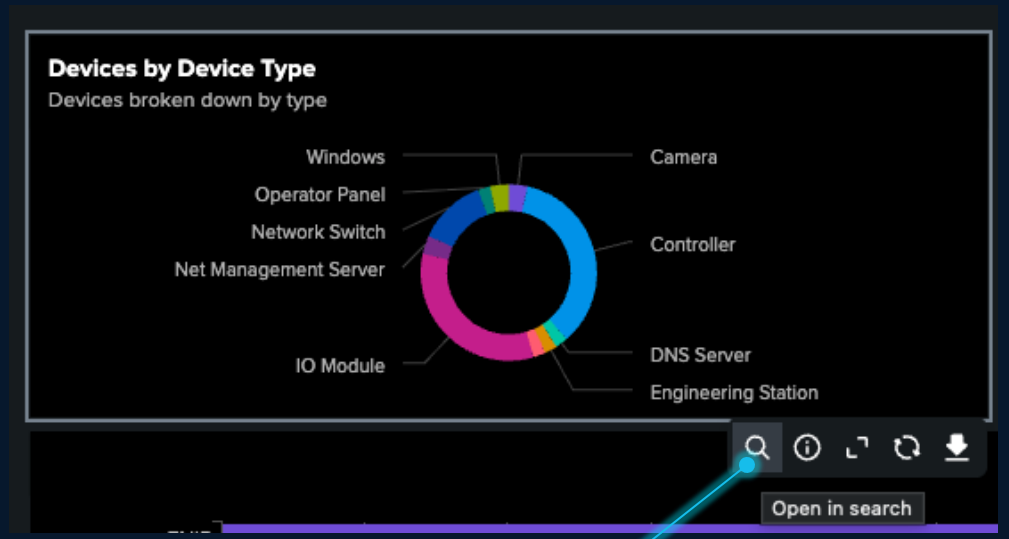
© 2026 Cisco and/or its affiliates. All rights reserved.

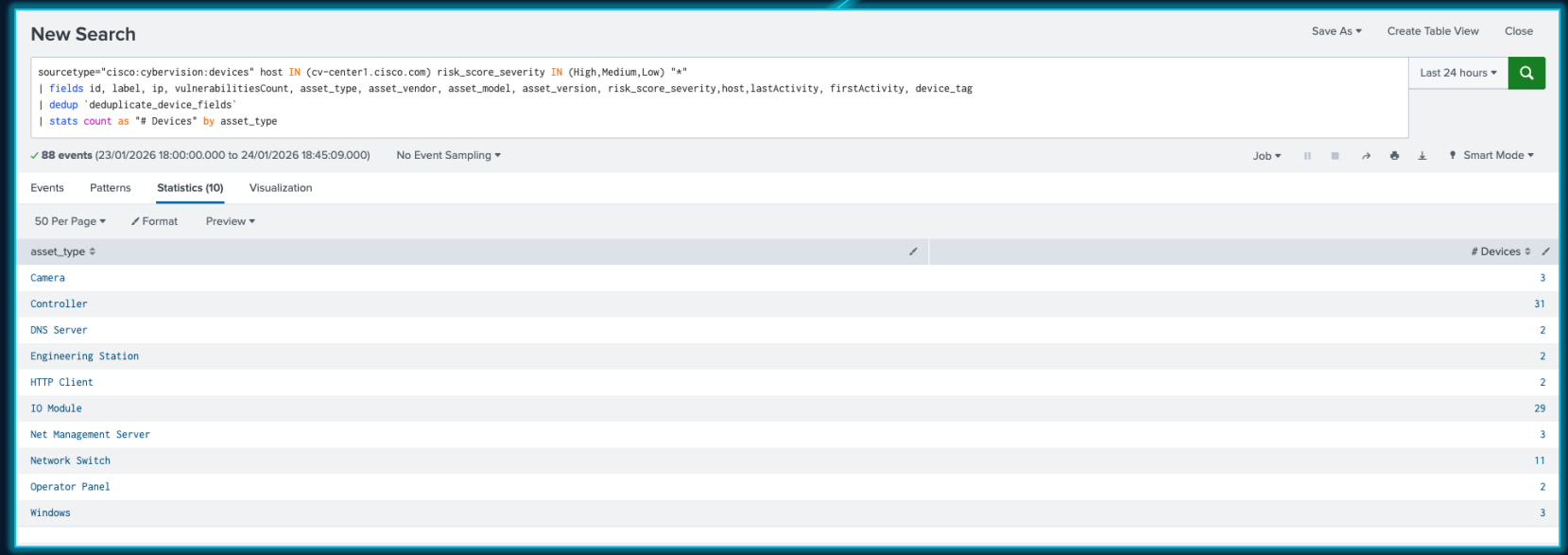
Cisco Confidential

Cyber Vision Splunk App

Build your own dashboard

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





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

Cisco Confidential

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)

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

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

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

Thank you


CISCO