



# Cisco CyberVision

Zabezpečte své průmyslové řídicí systémy

Jiří Rott

6.10.2021

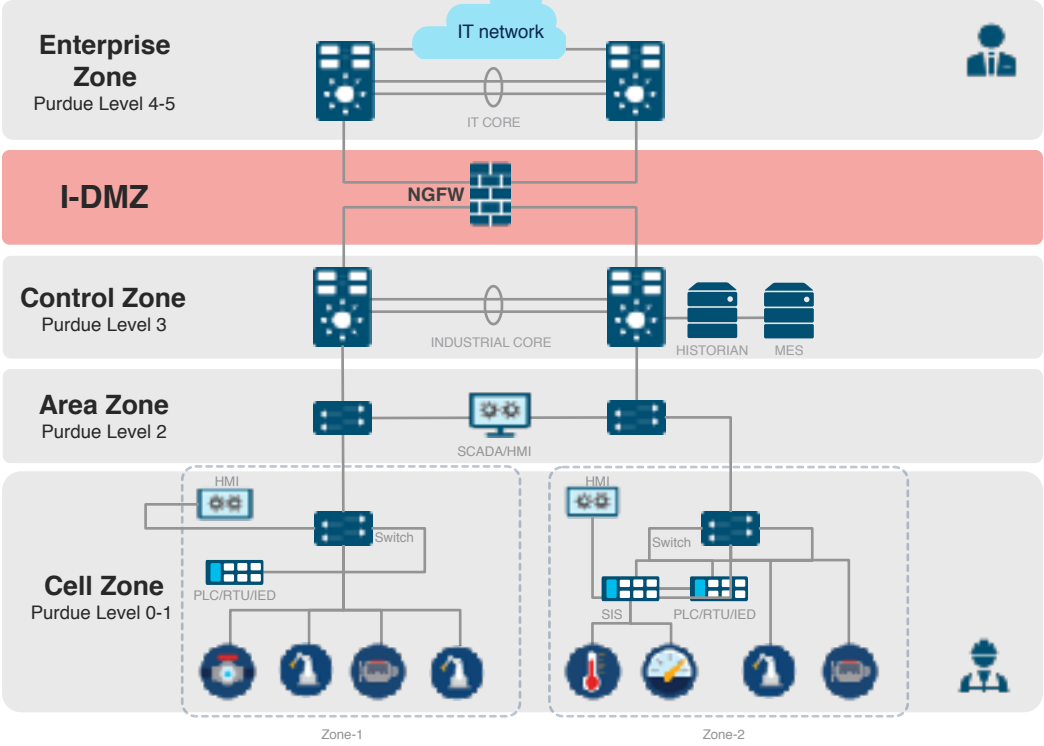
# Security is a journey



Foundation Security is next level

# Step 1: Minimal Security

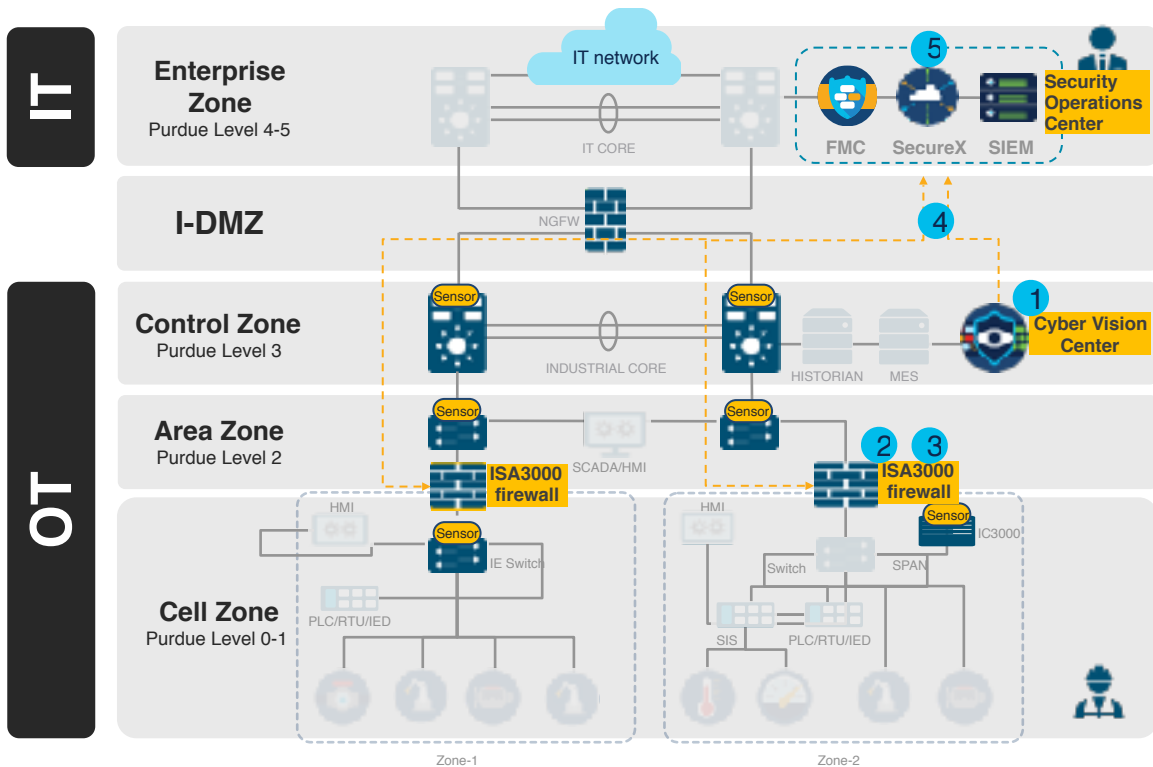
IT



How do we enhance security posture to go from minimal security (IDMZ) to foundation security ?

# Step 2: Foundation Security

A simple architecture, easy to operate with few products



1. Know your assets with Cisco Cyber Vision
2. Segment networks and secure production cells with Cisco ISA3000
3. Protect against malware and intrusion with Firepower
4. Feed SOC with OT context
5. Investigate and remediate threats with Cisco SecureX

# Foundation Security

*New capabilities to secure industrial networks*



## 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



## Investigate and Respond

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

**Gain visibility on your OT to build and enforce the right security policies**



# Cisco CyberVision

# Cisco Cyber Vision

Asset Inventory & Security Platform for the Industrial IoT



## ICS Visibility

Asset Inventory  
Communication Patterns  
Device Vulnerability



## Operational Insights

Identify configuration changes  
Record control system events  
relevant to the integrity of the system



## Threat Detection

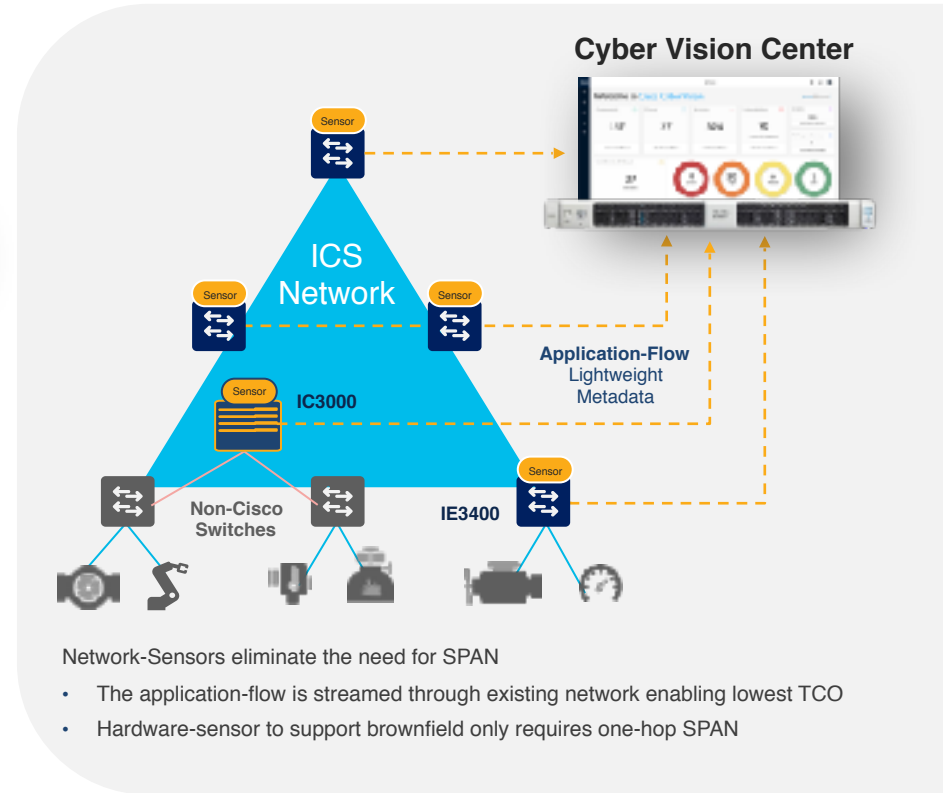
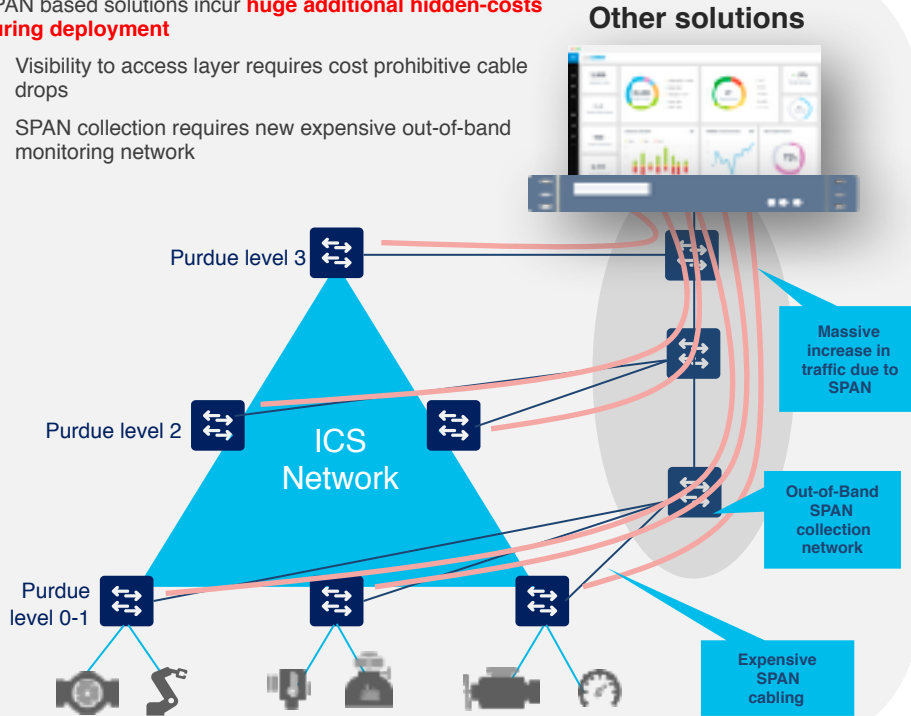
Behavioral Anomaly Detection  
Signature based IDS  
Real-time alerting

Cisco Cyber Vision helps companies protect  
their industrial control systems against cyber risks

# Unique Cyber Vision **scalable** architecture

SPAN based solutions incur **huge additional hidden-costs during deployment**

- Visibility to access layer requires cost prohibitive cable drops
- SPAN collection requires new expensive out-of-band monitoring network

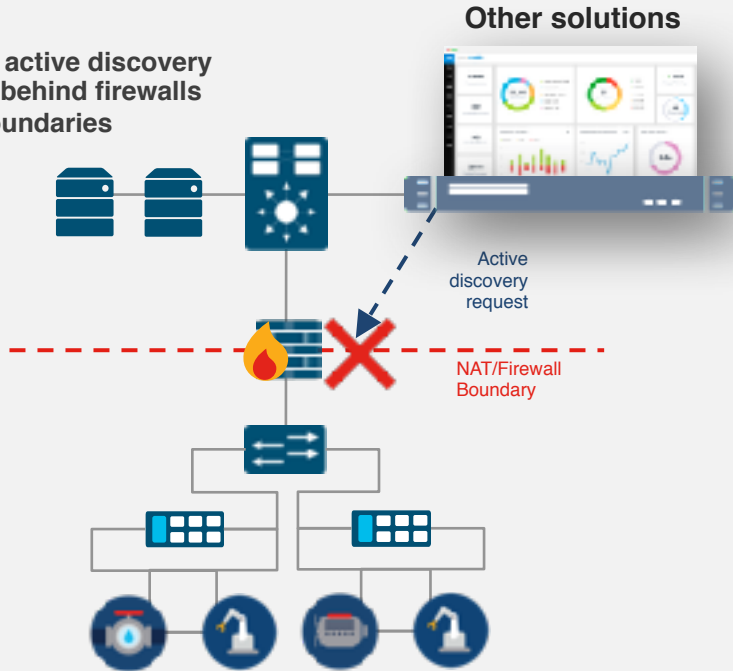




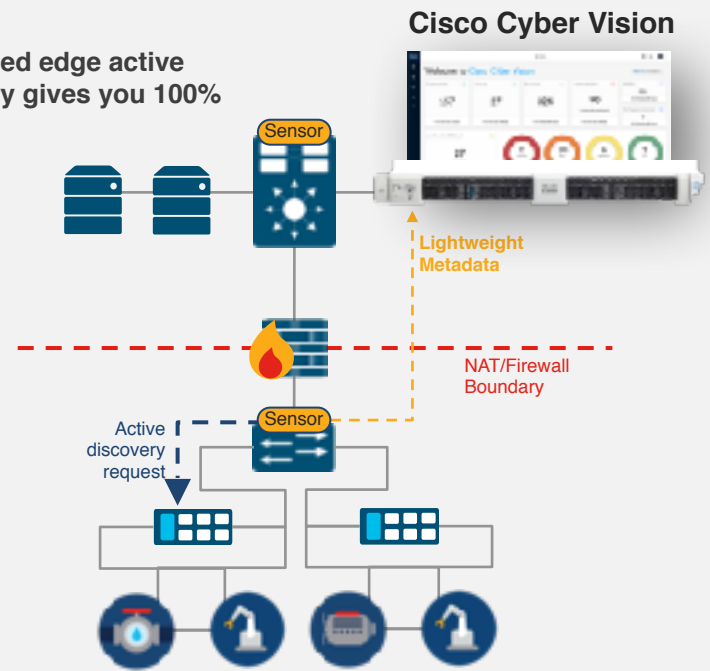
# Distributed edge discovery sees more

## Silent devices, FWs

Centralized active discovery cannot see behind firewalls and NAT boundaries

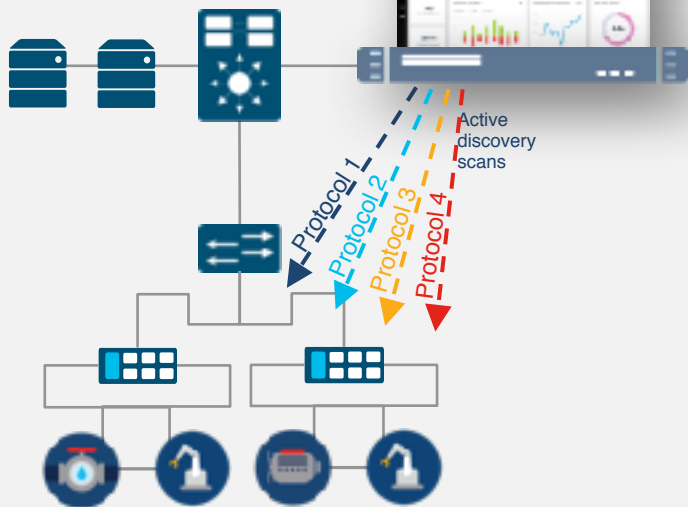


Distributed edge active discovery gives you 100% visibility

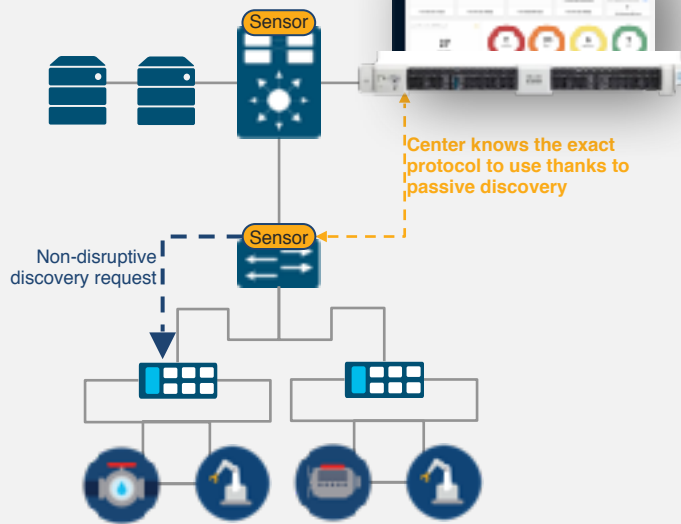


# Closed-loop control makes active discovery safe

Basic active discovery solutions scan networks overloading devices with ARP requests



Closed-loop between passive and active discovery enables precise and non-disruptive requests



# Cyber Vision Global Center - hierarchy

## Global visibility

Asset inventory

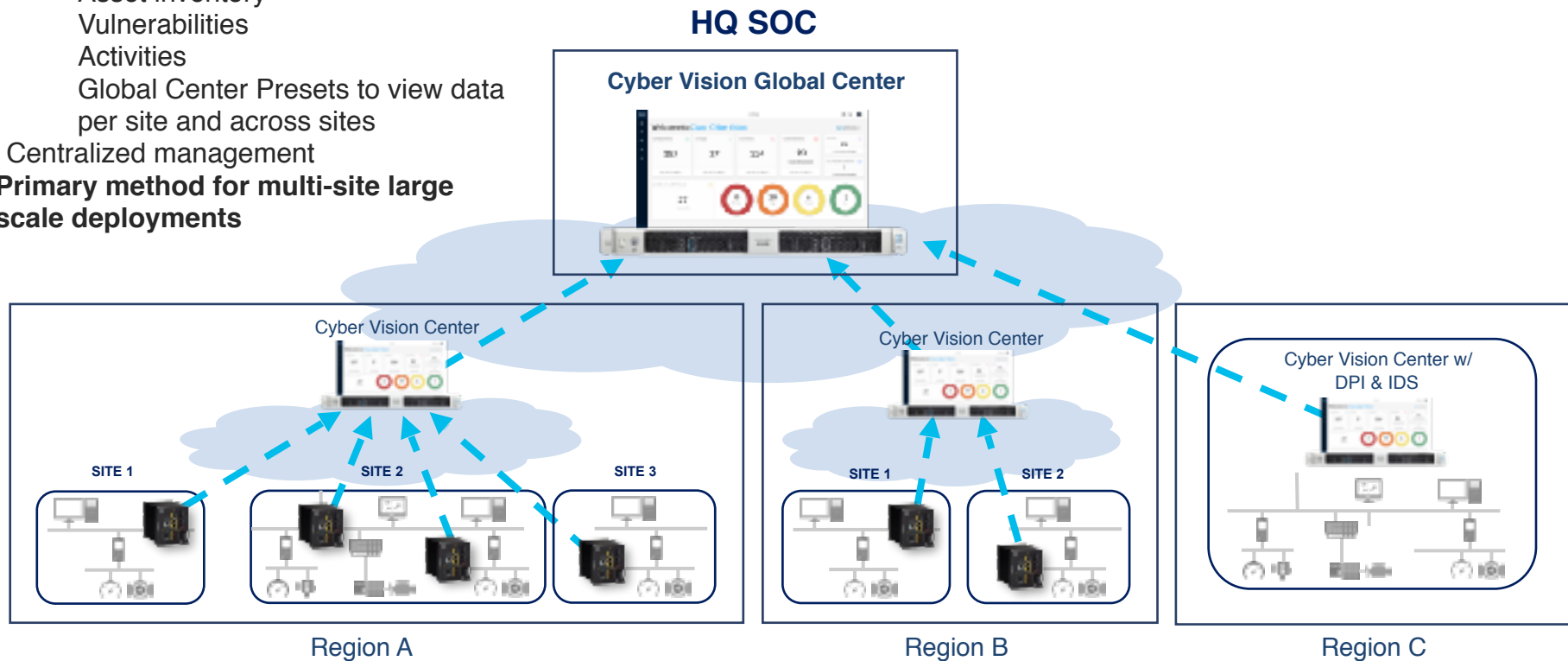
Vulnerabilities

Activities

Global Center Presets to view data per site and across sites

Centralized management

**Primary method for multi-site large scale deployments**



Giving global visibility on all industrial assets and security events across all sites from a central console

# Získání kontextu průmyslových protokolů



# Comprehensive visibility on all assets

- Automatically maintain a detailed list of all OT and IT equipment
- Immediate access to software and hardware characteristics
- Track rack-slot components
- Tags make it easy to understand asset functions and properties

**Track the industrial assets  
to protect throughout their  
life cycles**

The screenshot displays a web-based interface for managing industrial assets. At the top, it shows the date range 'Nov 21, 2018 21:24:00 - Jul 26, 2019 14:16:00' and a '66 Components' header. Below this is a table with the following columns: Component ID, Group, First available, Last updated, IP, MAC, and Tags. The table lists various components such as 'Dell P2130-001', 'ABB 100-001', 'ABB 100-002', 'ABB 100-003', 'ABB 100-004', 'ABB 100-005', 'ABB 100-006', 'ABB 100-007', 'ABB 100-008', 'ABB 100-009', 'ABB 100-010', 'ABB 100-011', 'ABB 100-012', 'ABB 100-013', 'ABB 100-014', 'ABB 100-015', 'ABB 100-016', 'ABB 100-017', 'ABB 100-018', 'ABB 100-019', 'ABB 100-020', 'ABB 100-021', 'ABB 100-022', 'ABB 100-023', 'ABB 100-024', 'ABB 100-025', 'ABB 100-026', 'ABB 100-027', 'ABB 100-028', 'ABB 100-029', 'ABB 100-030', 'ABB 100-031', 'ABB 100-032', 'ABB 100-033', 'ABB 100-034', 'ABB 100-035', 'ABB 100-036', 'ABB 100-037', 'ABB 100-038', 'ABB 100-039', 'ABB 100-040', 'ABB 100-041', 'ABB 100-042', 'ABB 100-043', 'ABB 100-044', 'ABB 100-045', 'ABB 100-046', 'ABB 100-047', 'ABB 100-048', 'ABB 100-049', 'ABB 100-050', 'ABB 100-051', 'ABB 100-052', 'ABB 100-053', 'ABB 100-054', 'ABB 100-055', 'ABB 100-056', 'ABB 100-057', 'ABB 100-058', 'ABB 100-059', 'ABB 100-060', 'ABB 100-061', 'ABB 100-062', 'ABB 100-063', 'ABB 100-064', 'ABB 100-065', 'ABB 100-066', 'ABB 100-067', 'ABB 100-068', 'ABB 100-069', 'ABB 100-070', 'ABB 100-071', 'ABB 100-072', 'ABB 100-073', 'ABB 100-074', 'ABB 100-075', 'ABB 100-076', 'ABB 100-077', 'ABB 100-078', 'ABB 100-079', 'ABB 100-080', 'ABB 100-081', 'ABB 100-082', 'ABB 100-083', 'ABB 100-084', 'ABB 100-085', 'ABB 100-086', 'ABB 100-087', 'ABB 100-088', 'ABB 100-089', 'ABB 100-090', 'ABB 100-091', 'ABB 100-092', 'ABB 100-093', 'ABB 100-094', 'ABB 100-095', 'ABB 100-096', 'ABB 100-097', 'ABB 100-098', 'ABB 100-099', 'ABB 100-100'. Each row includes a small icon, a component ID, a group name, a 'First available' date, a 'Last updated' date, an IP address, a MAC address, and a list of tags.

# Understand asset roles and communications

- Asset characteristics and communications are automatically translated to Tags
- A common language whatever the vendor reference
- Users do not need to be protocol experts to understand what is going on
- New tags can be added via RESTful API

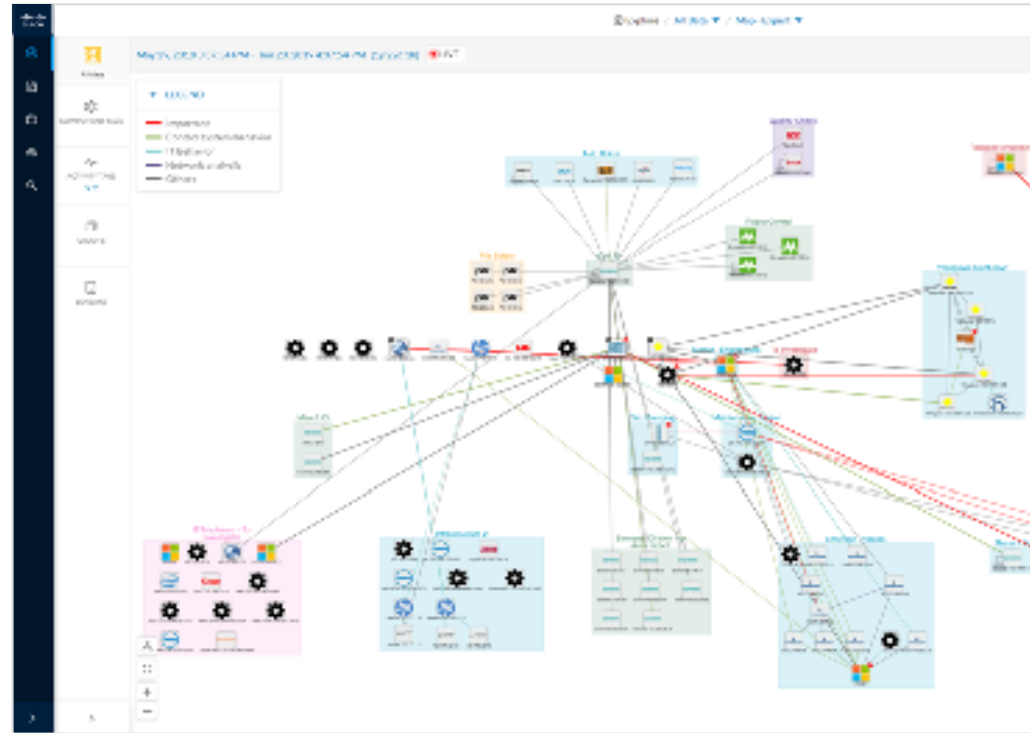
**Cyber Vision tags help  
you drive data analysis**



# Track all communications and their content

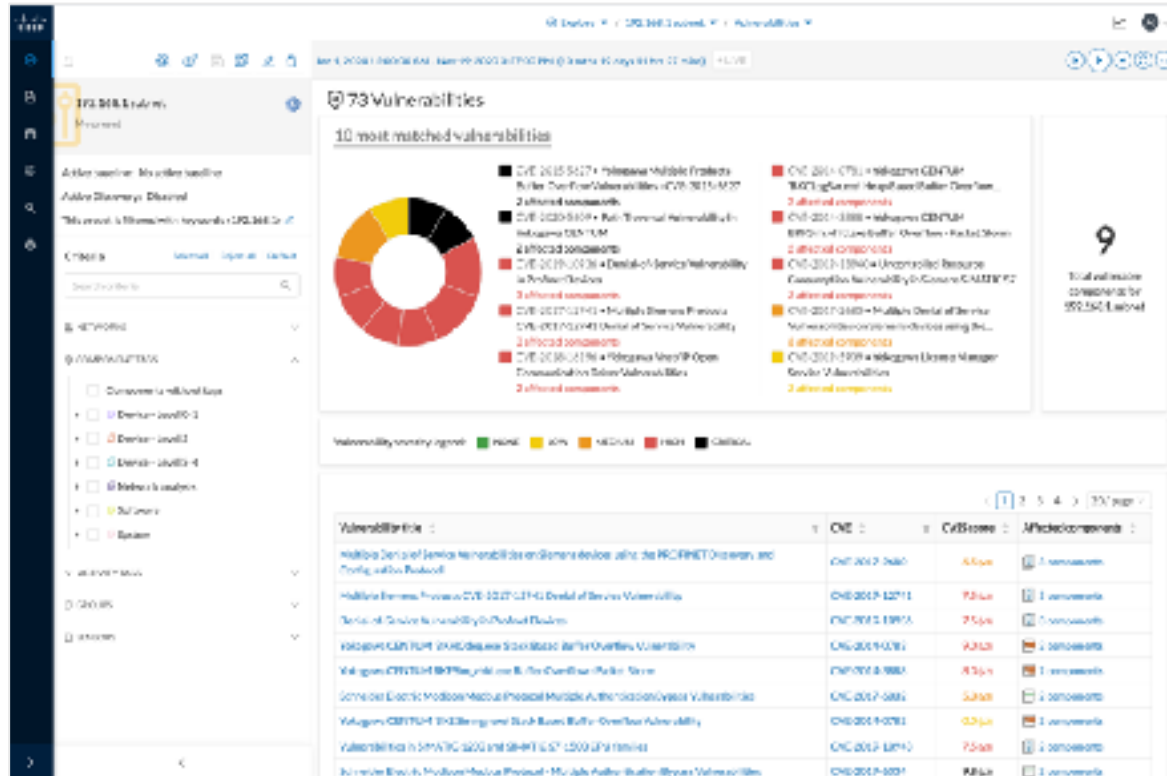
- Identify all relations between assets including application flows
- Spot unwanted communications & noisy assets
- Tags make it easy to understand the content of each communication flow
- View live information or go back in time

**Drive network  
segmentation and  
fine-tune configurations**



# Vulnerability dashboard

- Quickly spot vulnerabilities
  - Dashboard based on Presets
  - Drill down by site, zone, tag, vendor, sensor...
- Easily identify affected components
- Links to quickly pivot to component view
- Additional context for impact and remediation





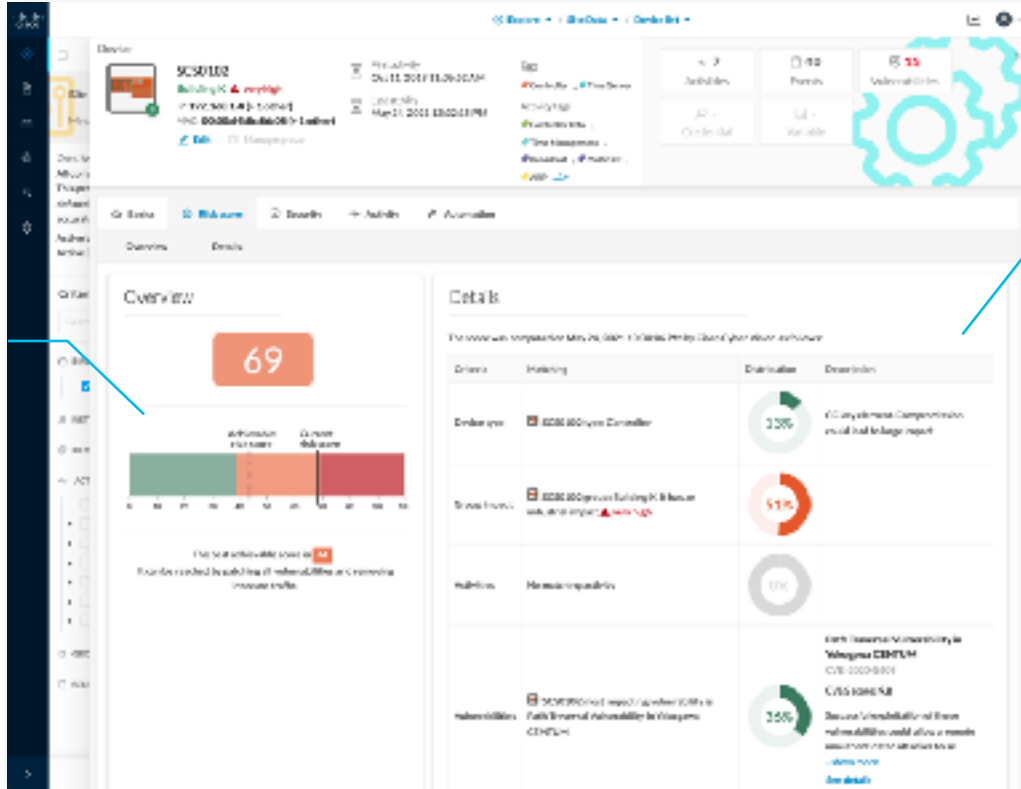
# Identify vulnerabilities to assess risks

- Automatically spot software & hardware vulnerabilities
- Access comprehensive information on vulnerability severities and solutions
- Track vulnerability acknowledgements
- Built-in vulnerability database curated by Cisco Research Teams always up to date

**Enforce cybersecurity best practices**

The screenshot displays a vulnerability management interface. At the top, a component is identified as 'SMBATIC.000(1)' with a CVSS score of 7.8. The interface includes a navigation bar with 'Vulnerabilities' and 'Details' tabs. The main content area shows a list of vulnerabilities, with the first one being 'Multiple CVEs (CVE-2023-0741) Detail of service vulnerability'. This entry has a CVSS score of 7.8 and a severity of 'High'. The description states: 'New studies of products in the library vulnerability. This indicates vulnerabilities in a set of service-...'. The interface also shows a 'Vulnerability' section with a '7.8' score and a 'CVSS' label. The 'Acknowledged' status is set to 'Unacknowledged'.

# Understanding a device risk score



Understanding how to lower risk

Understanding what impacts the risk score

# Operational insights for OT teams

- Detailed asset properties
- Communication maps
- PLC program changes
- Variable accesses

Monitor the integrity of your industrial process

The screenshot displays a comprehensive network management interface for industrial environments. It includes several key components:

- Component Details:** A panel for 'SIMATIC 300-31' showing its IP address (192.168.0.2), location (Area 1), and last update time (May 26, 2017 12:21:13 AM).
- Properties Panel:** A detailed view of the component's configuration, including its name, IP address, and various system parameters.
- Communication Map:** A network diagram titled 'Machines - To Investigate Manuf IC' and 'Manuf - Scada & HMI'. It shows connections between various industrial devices like SIMATIC 300-31, SIMATIC 300-32, and SIMATIC 300-33, along with a SCADA system and an HMI.
- Variables Accesses Table:** A table listing variable access events across different components.

Instance ID	Type	Accessed by	Accessed at	Last access at
> M1.0	RWE	[Component (Division)]	Apr 4 2017 11:29:23 PM	May 26, 2017 12:12:23 AM
> M1.1	RWE	[Component (Division)]	Apr 4 2017 11:29:23 PM	May 26, 2017 12:12:23 AM
	CCAT	Control System (SCADA)	Apr 4 2017 11:29:23 PM	May 26, 2017 12:12:23 AM
> M1.2	CCAT	[Component (Division)]	Apr 4 2017 11:29:23 PM	May 26, 2017 12:12:23 AM
	FCPE	[Component (Division)]	Apr 4 2017 11:29:23 PM	May 26, 2017 12:12:23 AM
	FCPE	[Component (Division)]	Apr 4 2017 11:29:23 PM	May 26, 2017 12:12:23 AM

# Rich context added to all events

The screenshot displays a security monitoring interface with a list of events. A search dropdown is open over the first event, showing search criteria like 'Search with wildcards enabled' and 'Search events with associated severity'. The event list includes:

- OS:IN:CD:21:0254** - FirewallDeny: New security vendor name Fujitsu Technology Solutions End P'edected to 195.195.1.124 [Host: 195.195.1.124 | MAC: 48:0D:21:82:11:1829]
- OS:IN:CD:21:1954** - AnomalyDetector: 304-9References have been detected in the console monitoring
- OS:IN:CD:21:1954** - SecurityAlert: The component PLC\_1 (Cm Compression) [IP: 192.168.1.112 | MAC: 18:0F:15:01:1:5:3D] has been added to the list of components to be monitored for IPsec and Tunnel-related threats. Vulnerability IDs: CVE-2017-12927, CVE-2017-12929, CVE-2017-12928

A detailed view for the PLC\_1 component is shown below the event list:

Properties	Vulnerabilities
<b>Group:</b> CM (Compression)	Segment Search interface IP-Stack based CVE information
<b>Individual Impact:</b> Every Line	Individual Devices
<b>Name:</b> PLC_1	CVE-2017-12927-594-592292
<b>MAC:</b> 18:0F:15:01:1:5:3D	Vulnerability ID: CVE-2017-12927-594-592292
<b>IP:</b> 192.168.1.112	CVE Information Link
<b>Tag:</b> #Critical	CVE ID: CVE-2017-12927-594-592292
<b>16 vulnerabilities detected</b>	

# Baselines highlight abnormal behaviors

- Cyber Vision behavior modeling automatically triggers alerts on deviations to the baselines
  - New and modified assets
  - New activities between assets
  - Variable changes
  - Program modifications
- Continuously improve detection with classification of new events
- Accept changes to continuous monitoring or trigger alerts to investigate changes
- Provide feedback on anomalies to give context to security analysts

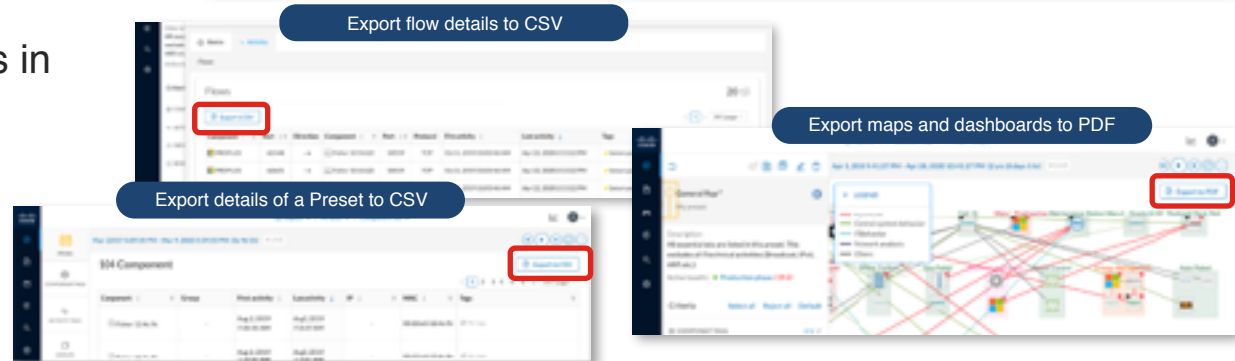
The screenshot displays the Cisco Cyber Vision interface. On the left, a network diagram shows a central 'LUCERO' node connected to various devices, including two 'Paint Line' nodes (Paint Line 1 and Paint Line 2). The 'Paint Line 2' node is highlighted in red, indicating an abnormal behavior. On the right, a 'Changed Activity' panel provides details for a specific activity. The activity is titled 'Changed Activity' and shows a list of variables that have changed. A red box highlights the following variables:

- SYNC read ReadLevel: 192.168.249.50
- ENVC write ReadLevel: 192.168.249.50
- SYNC read ReadLevel: 192.168.249.50

Below the variables, there are buttons for 'Acknowledge Differences' (checked), 'Report Differences', 'Remove and Re-monitoring', and 'Include in administration'. At the bottom of the panel, there are statistics for 'Files' (2) and 'Packets' (396127).

# Drive compliance with detailed reports

- Built-in reports to export all details to Excel or PDF
- Export custom views to build your own reports and compliance statements
- Share with your teams the list of vulnerabilities to be fixed
- Export data for risk analysis in third party tools



# Cisco's fully integrated IT-OT security solution

