Cisco CyberVision

Zabezpečte své průmyslové řídicí systémy

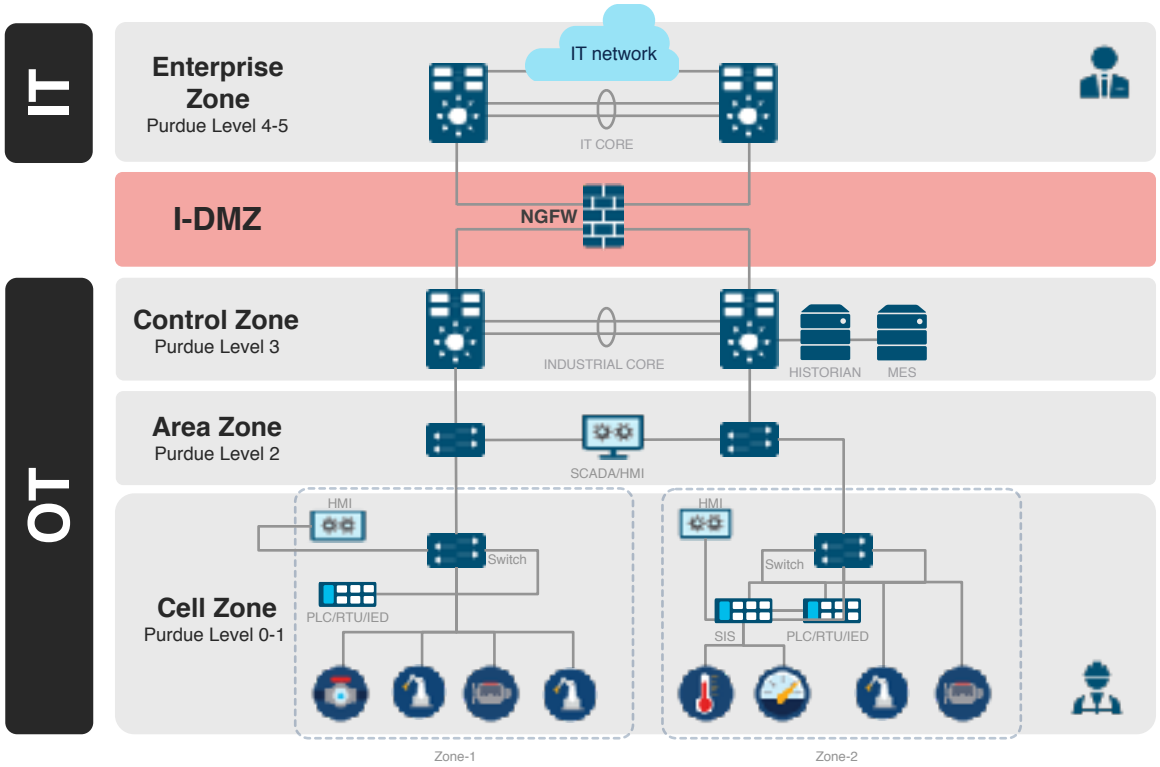
Jiří Rott

6.10.2021

Security is a journey

Foundation Security is next level

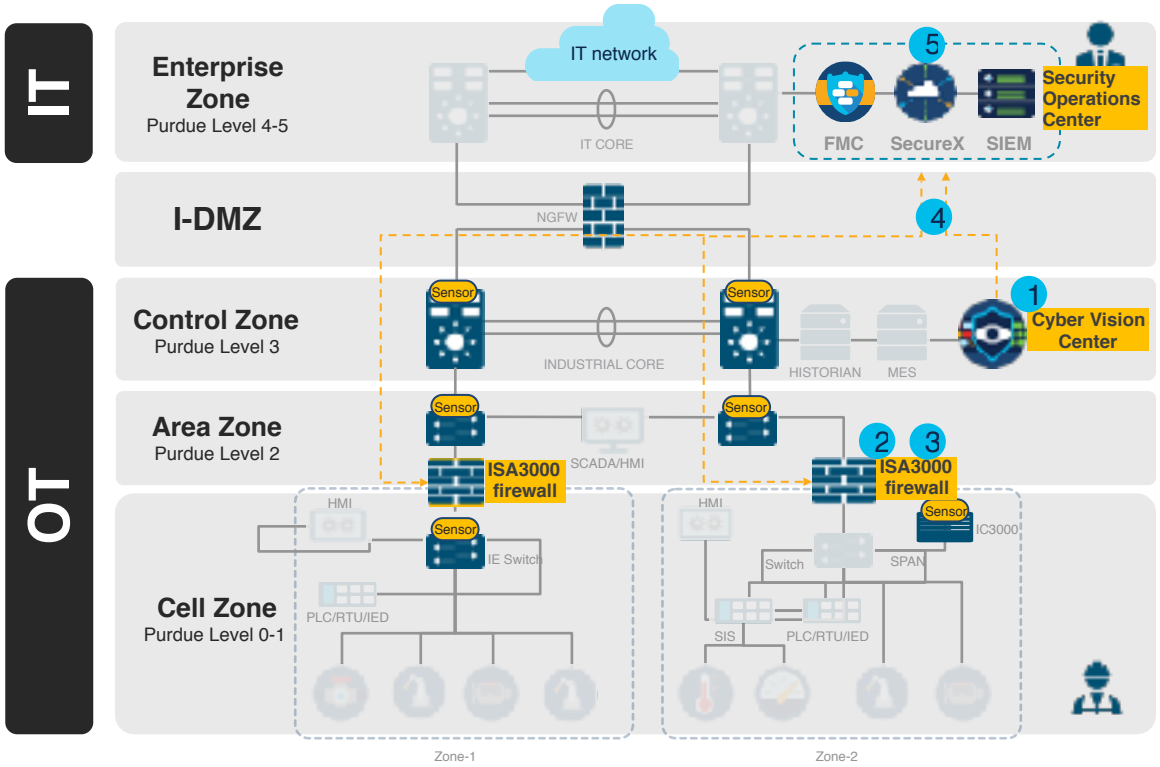
Step 1: Minimal Security



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

Step 2: Foundation Security

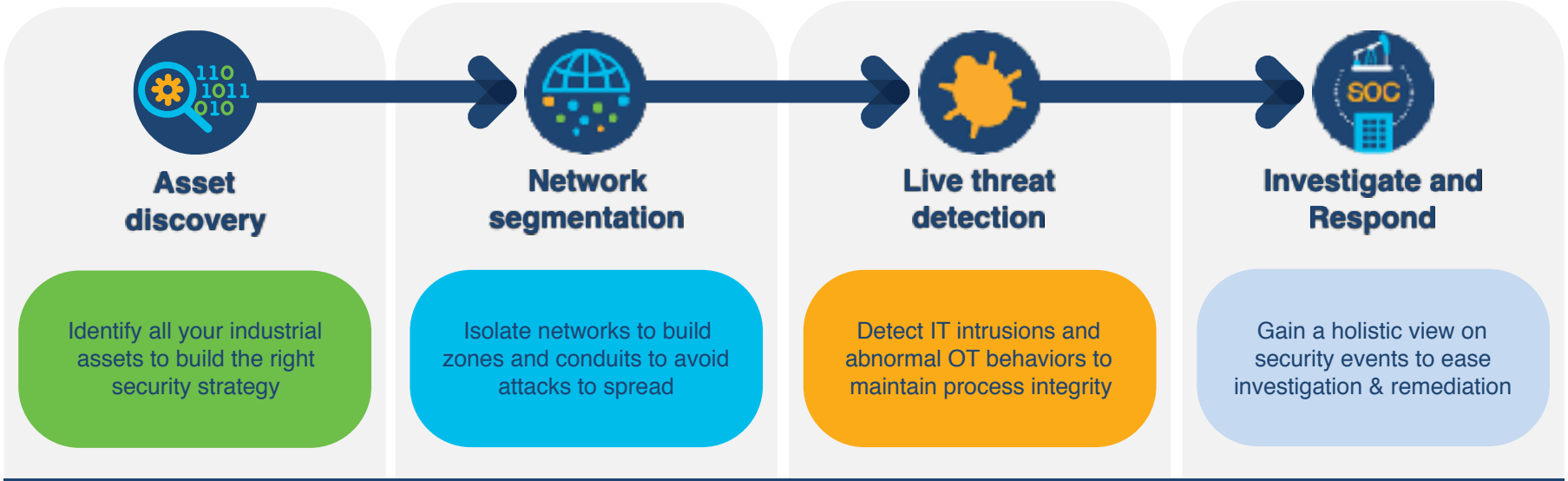
A simple architecture, easy to operate with few products



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



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

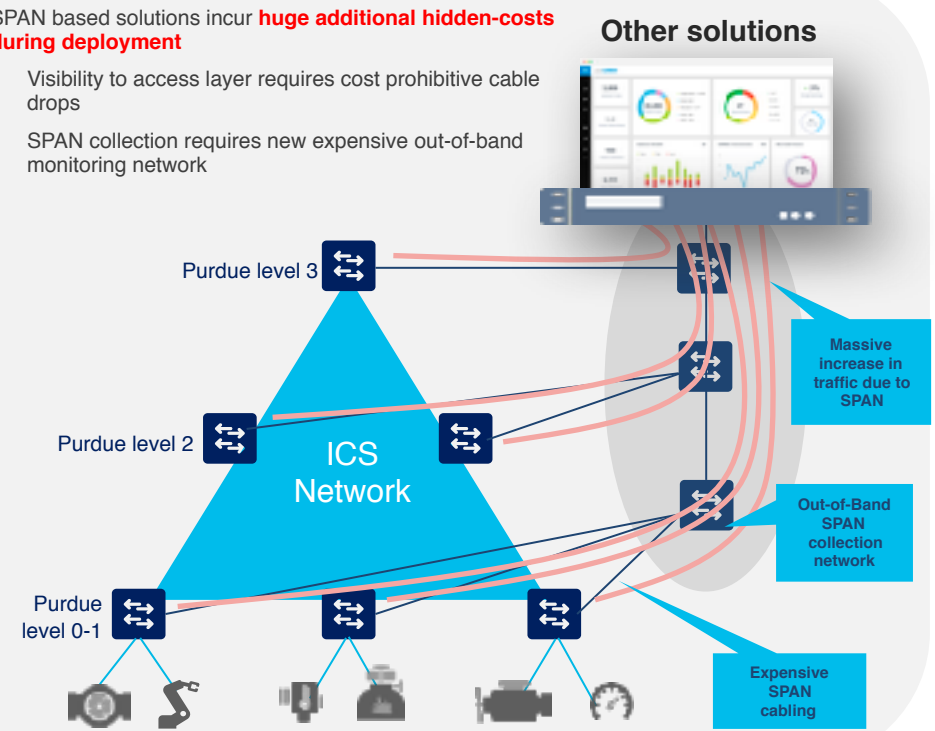
Behavioral Anomaly Detection
Signature based IDS
Real-time alerting

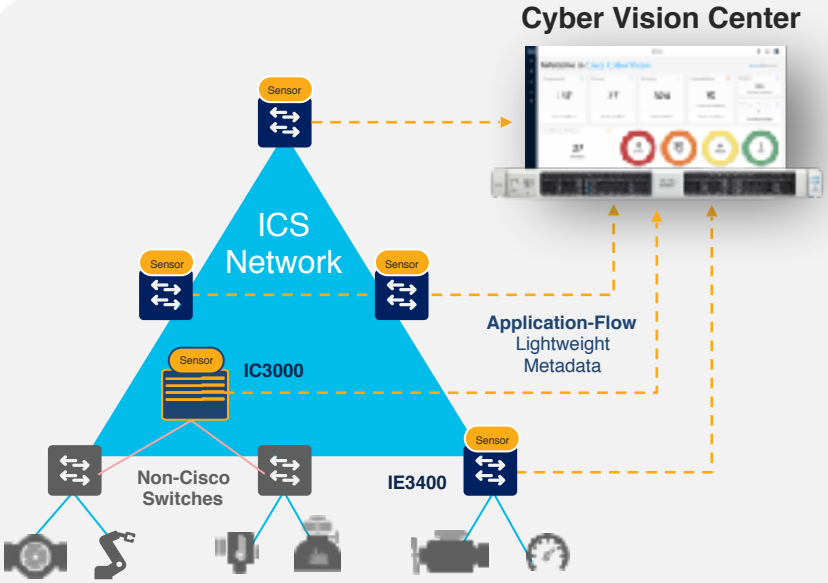
Cisco Cyber Vision helps companies protect their industrial control systems against cyber risks

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





Network-Sensors eliminate the need for SPAN

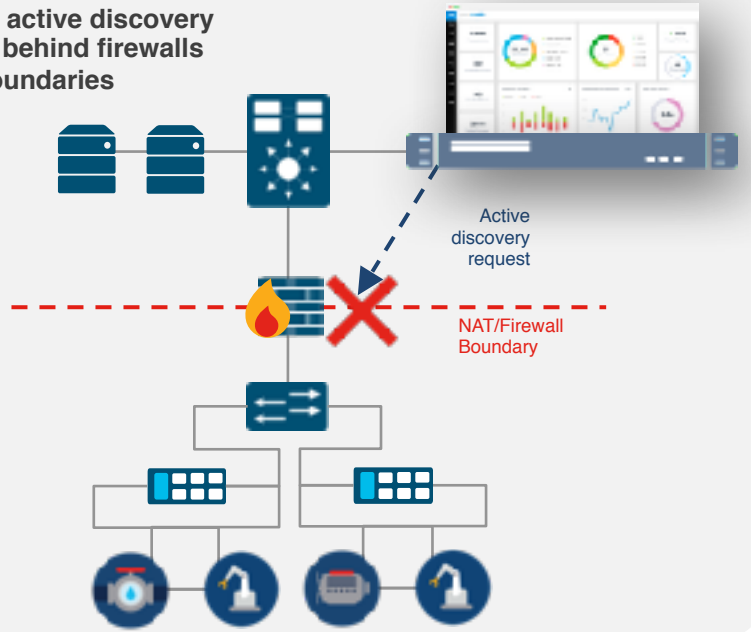
- The application-flow is streamed through existing network enabling lowest TCO
- Hardware-sensor to support brownfield only requires one-hop SPAN

Distributed edge discovery sees more

Silent devices, FWs

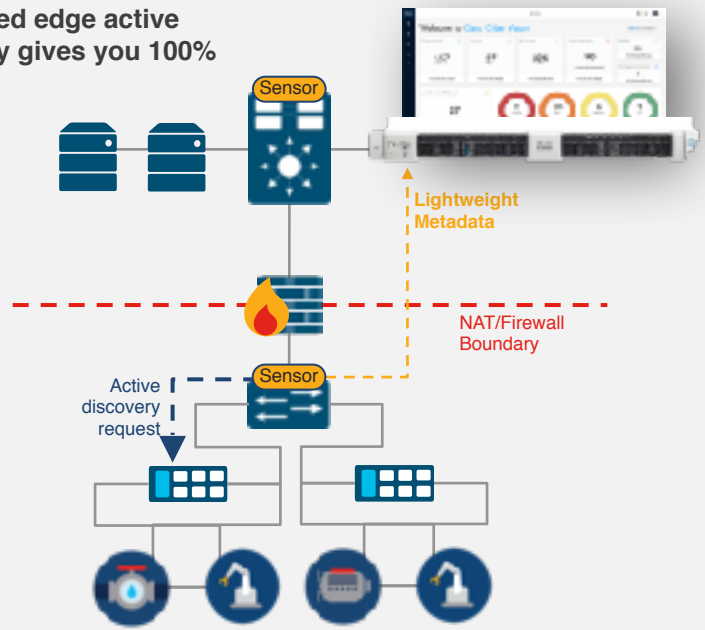
Other solutions

Centralized active discovery cannot see behind firewalls and NAT boundaries



Cisco Cyber Vision

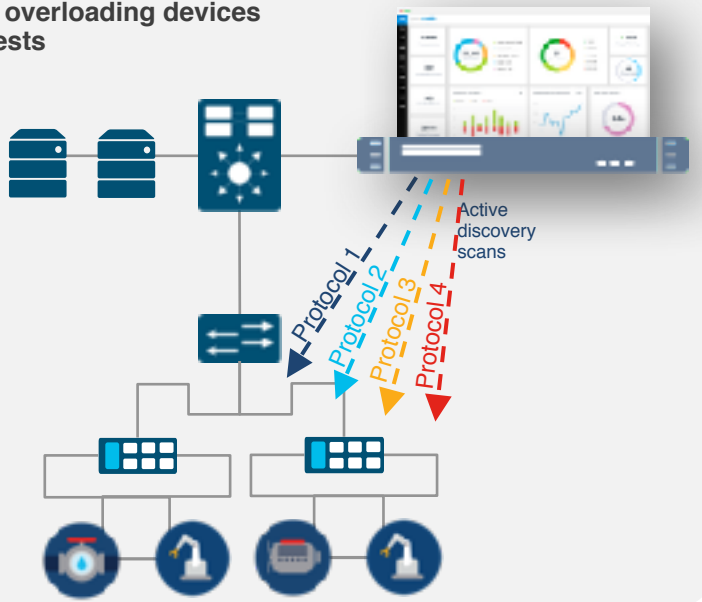
Distributed edge active discovery gives you 100% visibility



Closed-loop control makes active discovery safe

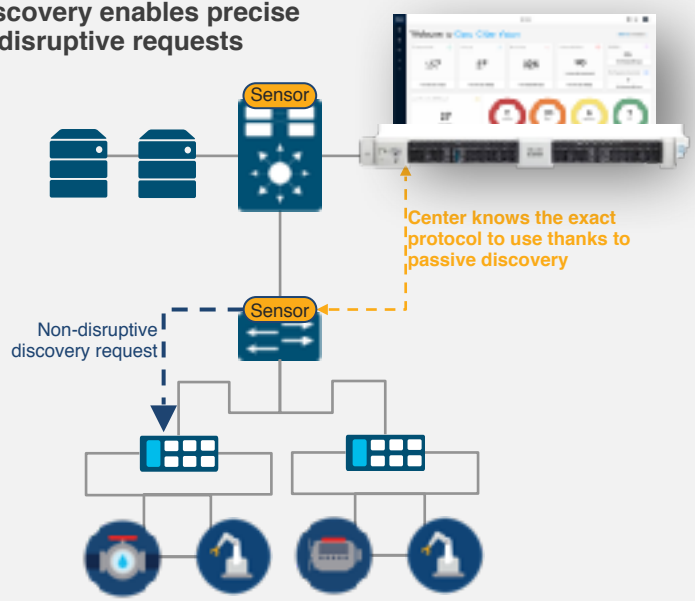
Basic active discovery solutions scan networks overloading devices with ARP requests

Other solutions



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

Cisco Cyber Vision



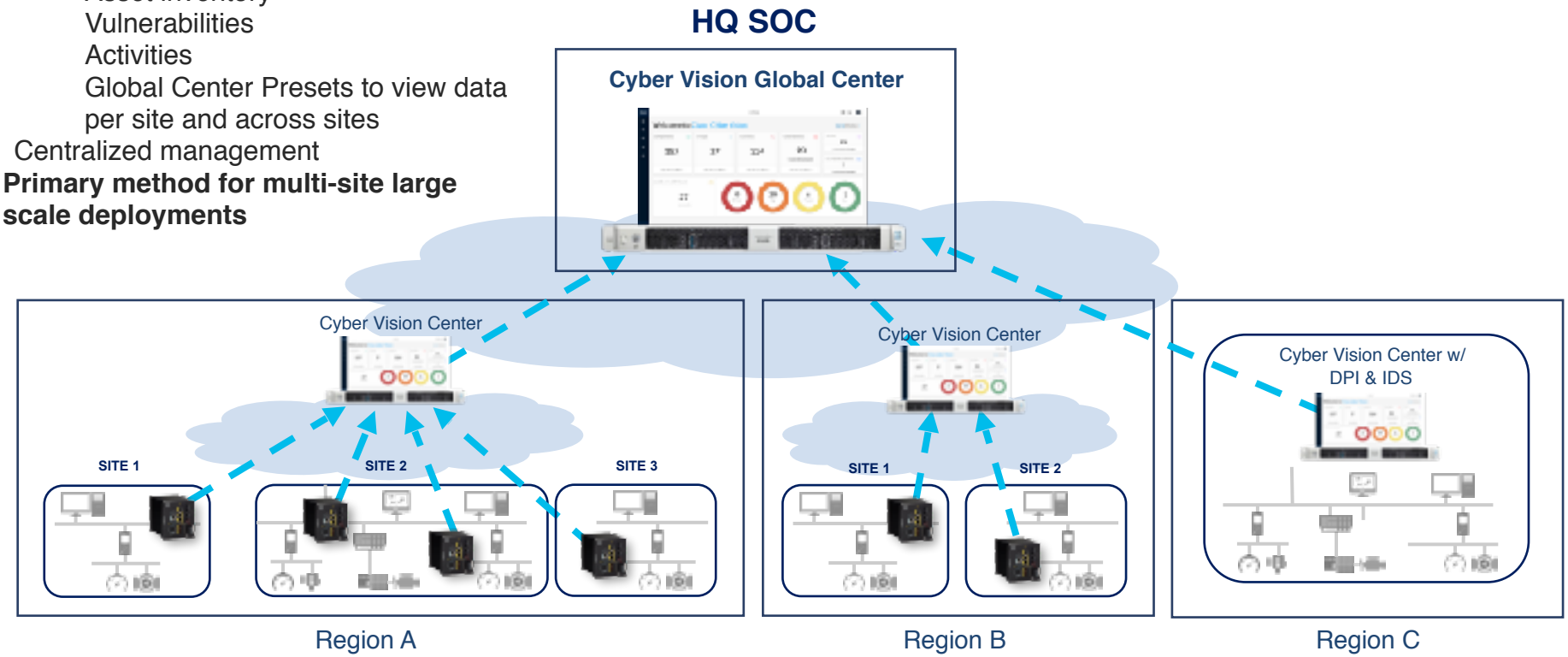
Cyber Vision Global Center - hierarchy

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



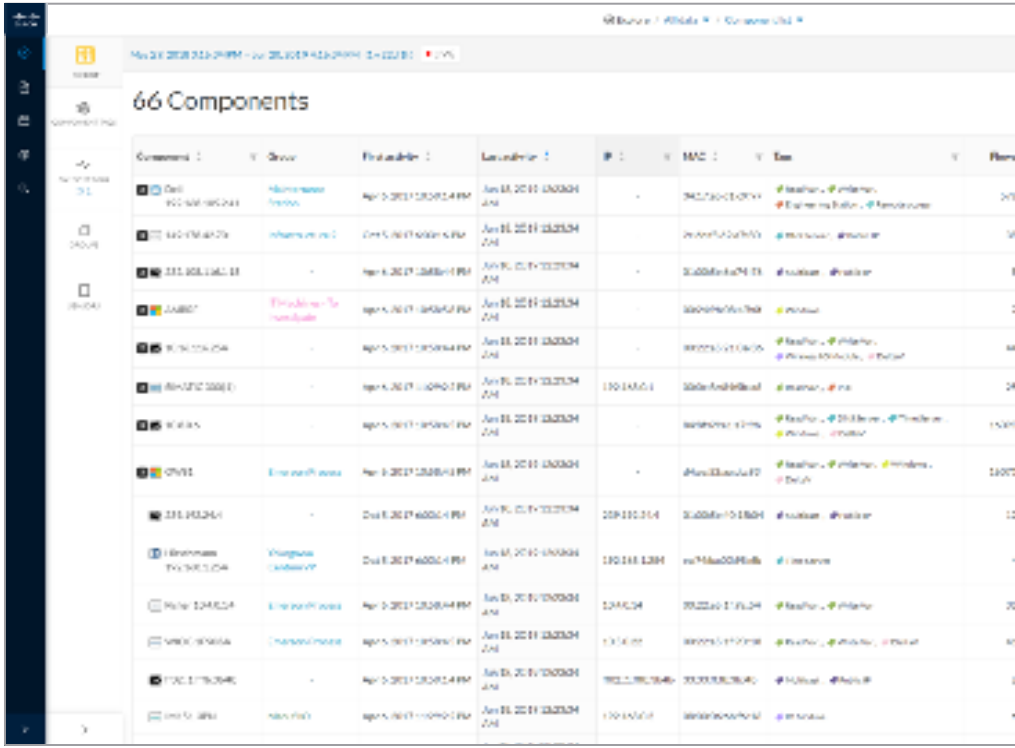
Giving global visibility on all industrial assets and security events across all sites from a central console

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

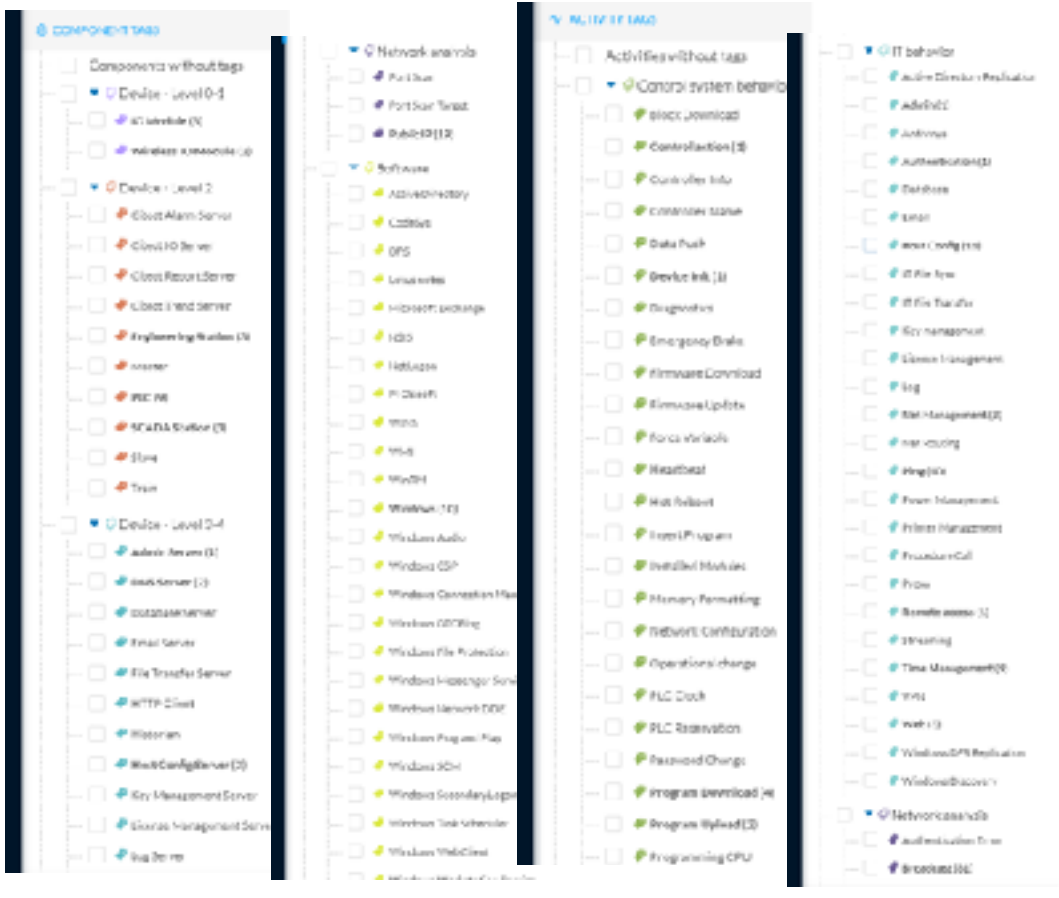
Track the industrial assets to protect throughout their life cycles



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

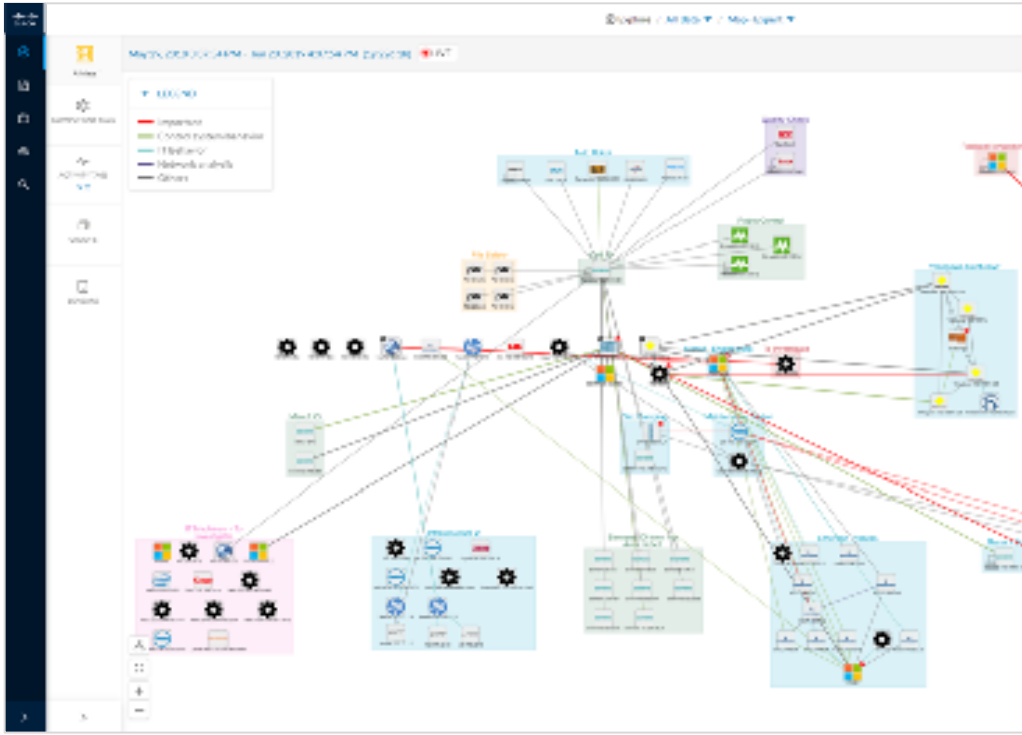
Cyber Vision tags help you drive data analysis



Track all communications and their content

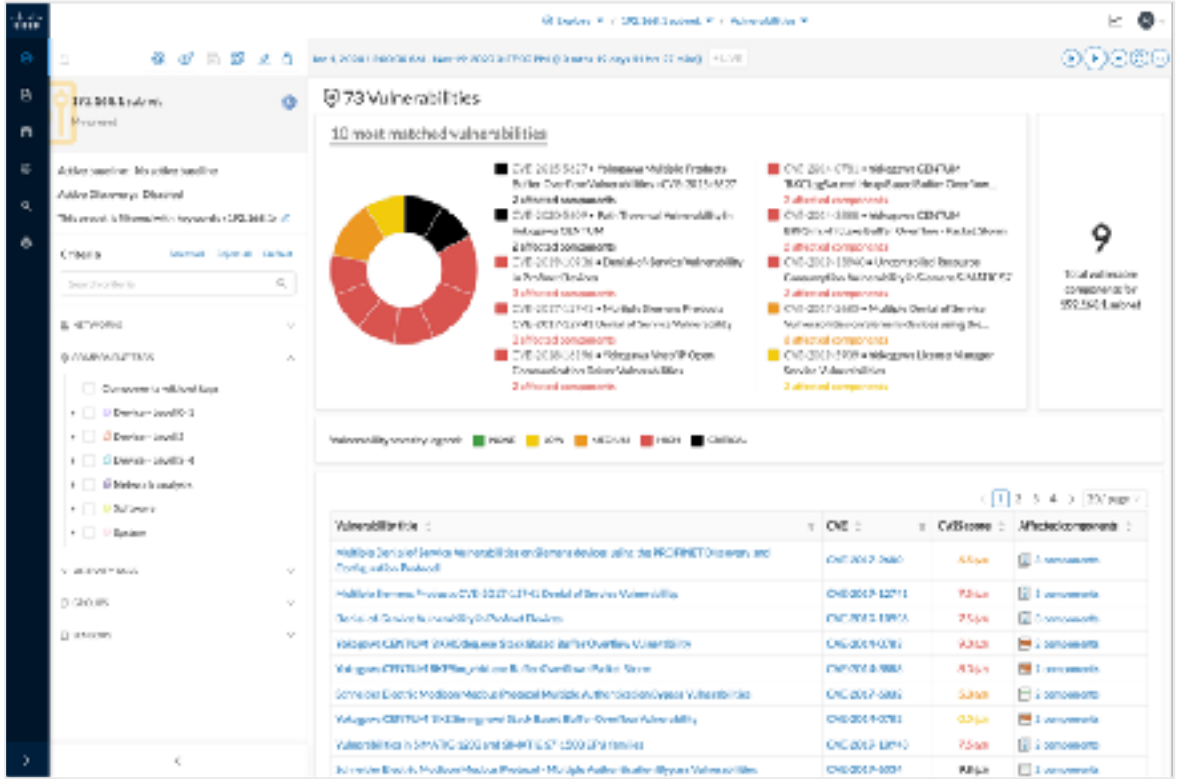
- Identify all relations between assets including application flows
- Spot unwanted communications & noisy assets
- Tags make it easily to understand the content of each communication flow
- View live information or go back in time

Drive network segmentation and fine-tune configurations



Vulnerability dashboard

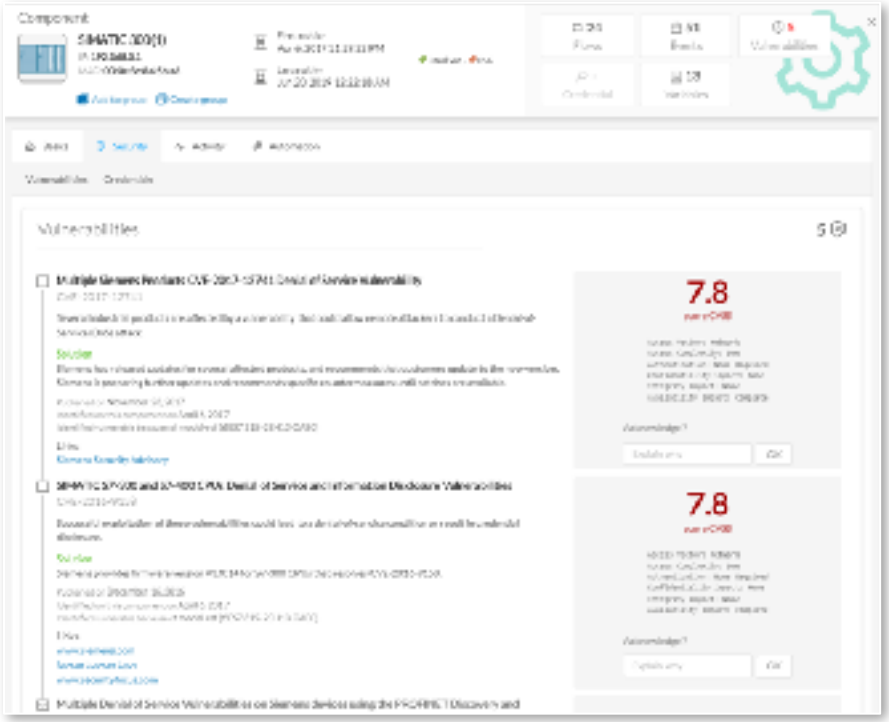
- Quickly spot vulnerabilities
  - Dashboard based on Presets
  - Drill down by site, zone, tag, vendor, sensor…
- Easily identify affected components
- Links to quickly pivot to component view
- Additional context for impact and remediation



Identify vulnerabilities to assess risks

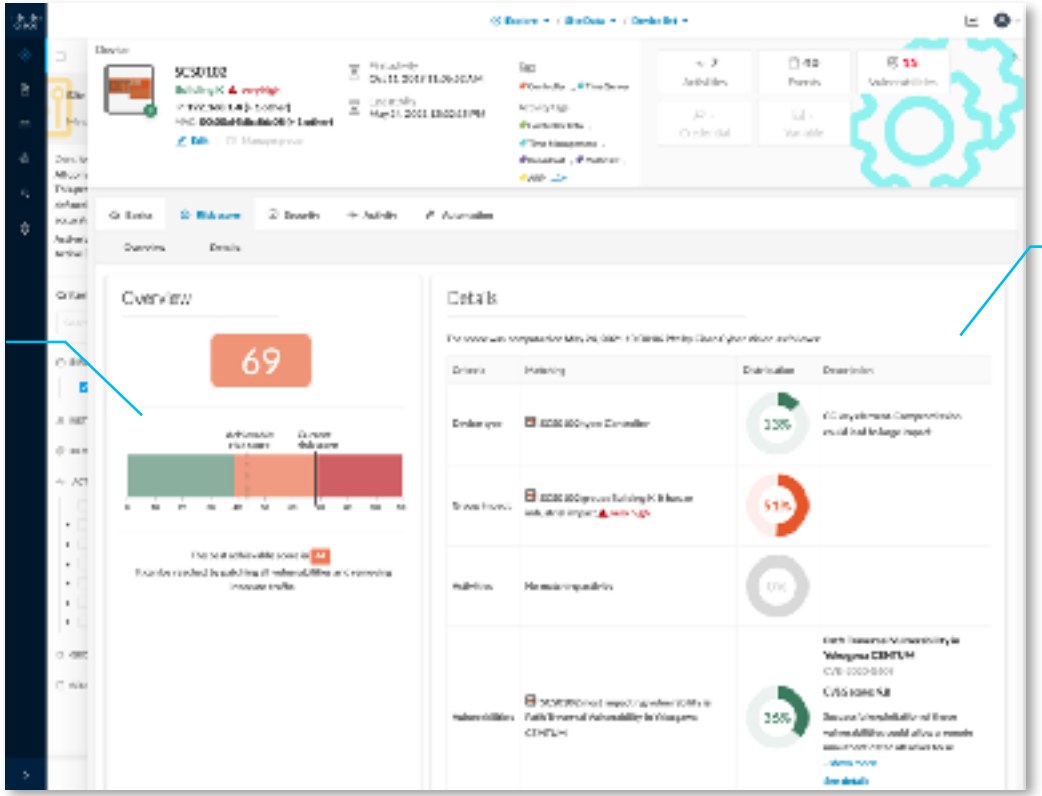
- Automatically spot software & hardware vulnerabilities
- Access comprehensive information on vulnerability severities and solutions
- Track vulnerability acknowledgements
- Built-in vulnerability database curated by Cisco Research Teams always up to date

Enforce cybersecurity best practices



Understanding a device risk score

Understanding how to lower risk

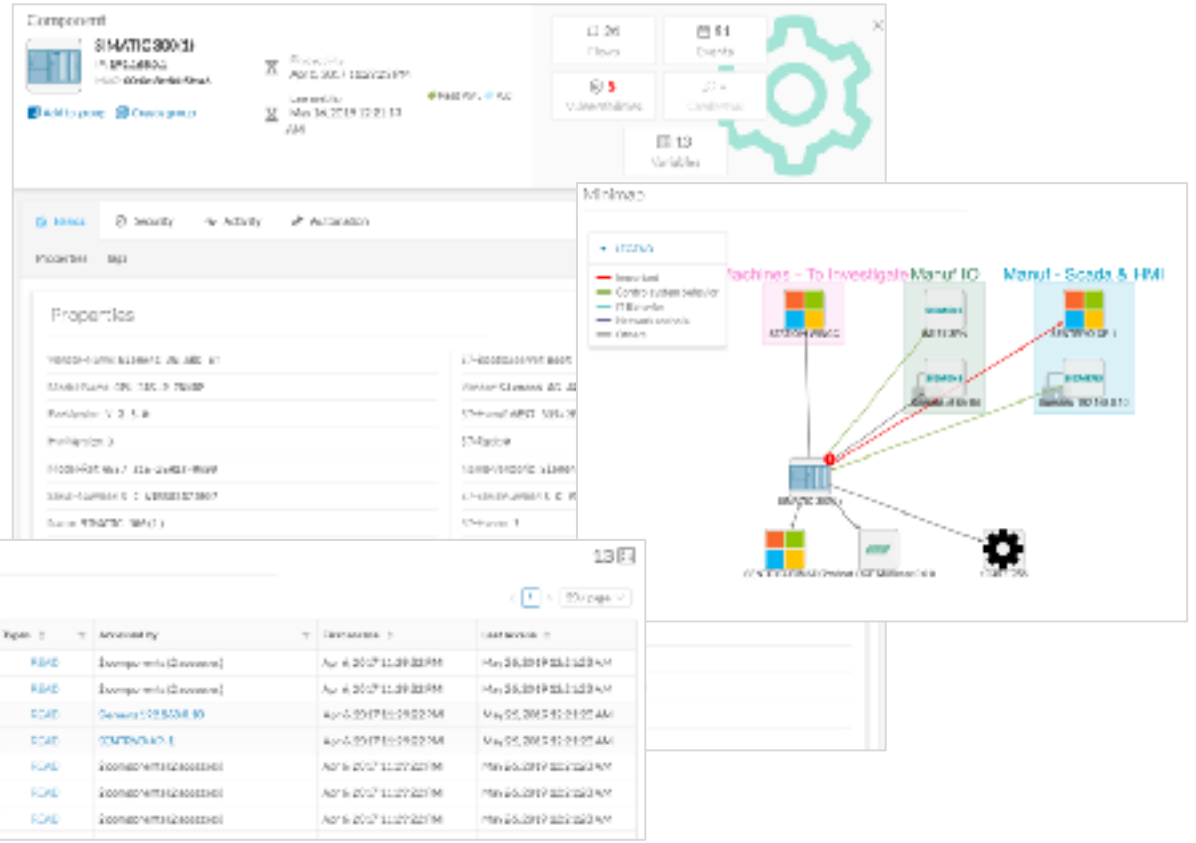


Understanding what impacts the risk score

Operational insights for OT teams

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

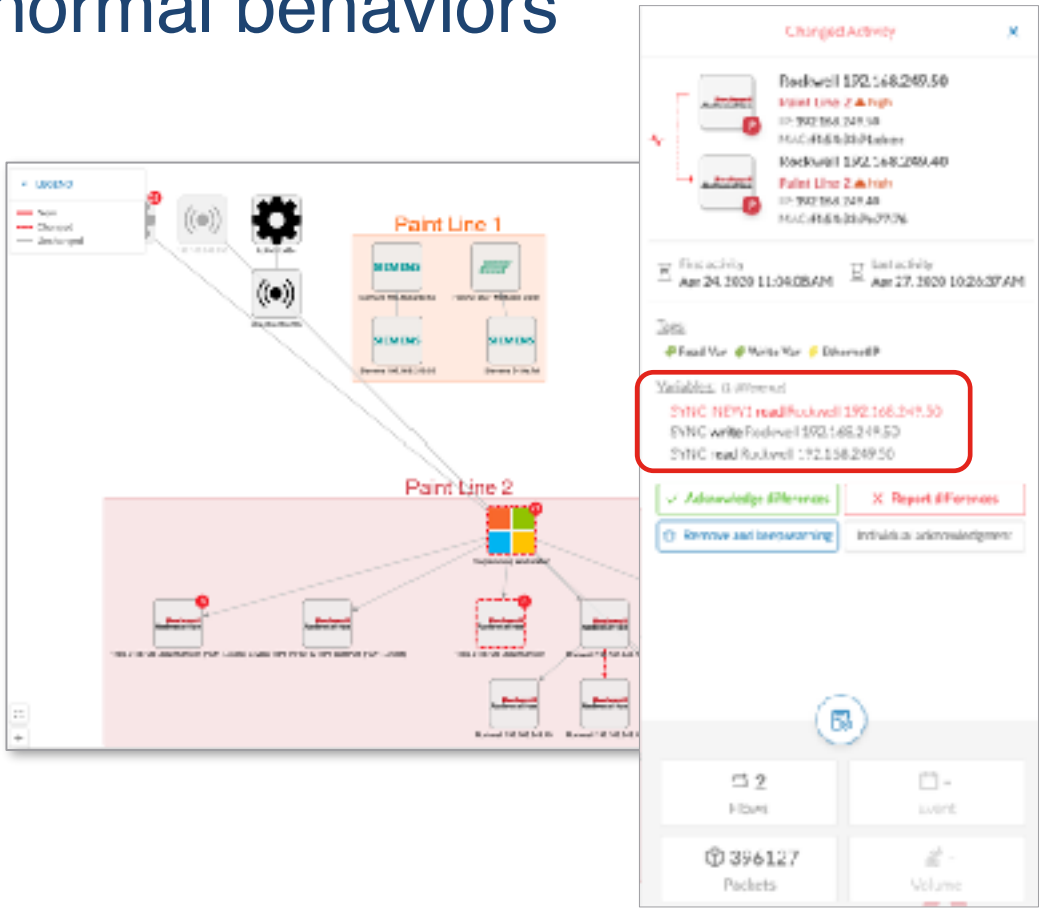
Monitor the integrity of your industrial process



Rich context added to all events

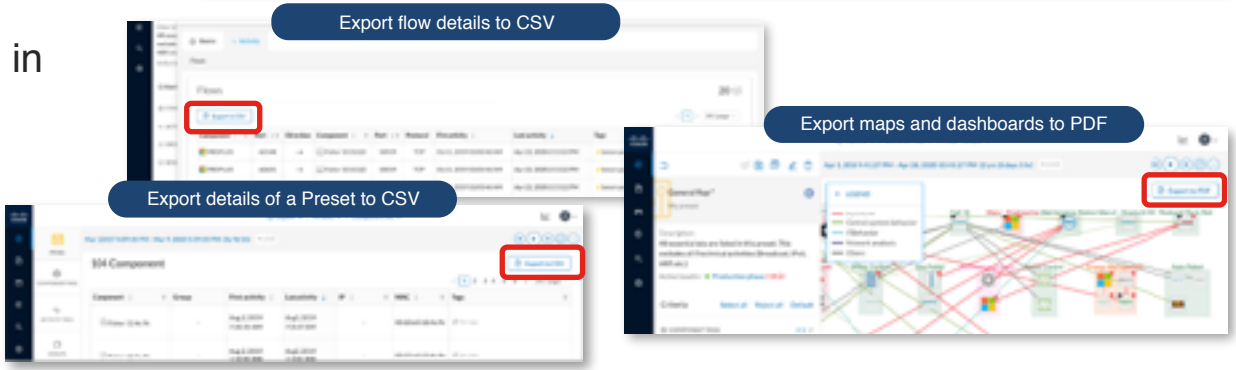
Baselines highlight abnormal behaviors

- 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

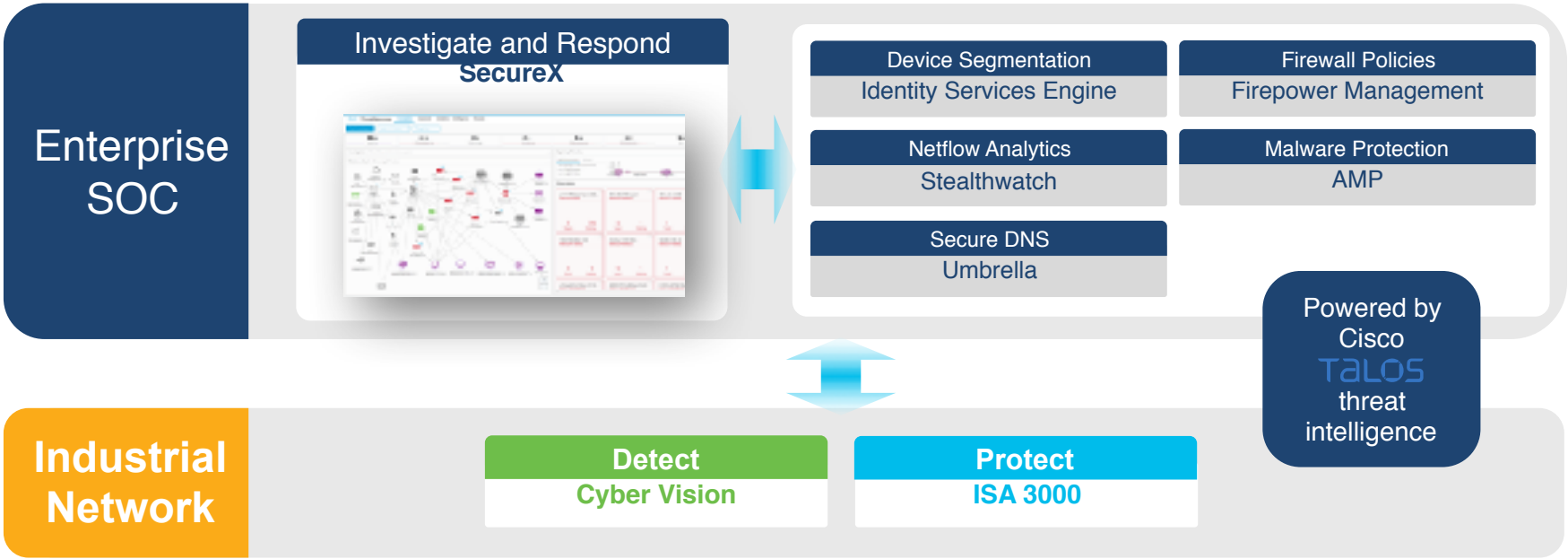


Drive compliance with detailed reports

- 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




CISCO