TD SYNNEX

Sicurezza OT/IoT con Cisco

Visibilità e protezione capillare con Cisco Cyber Vision

4 Luglio 2025

Webinar

Federico Frosini – BDM – TD SYNNEX
Giacomo Casati – Cisco Presales Specialist – TD SYNNEX
Marco Stangalino - Cisco
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

Ambiente OT e IoT

Entro il 2030, ci saranno circa 29 miliardi di connessioni IoT in tutto il mondo.

Un ambito da governare nell’immediato

- Protocolli proprietari
- Scarsa visibilità
- Zone grigie
- Mancata segmentazione e microsegmentazione
- Appalti
- Manutenzioni esterne
- Gestione del ciclo di vita
- Software e sistemi operativi non manutenuti
- Patch Management inesistente

Cyberattack in Norvegia: apertura forzata della diga evidenzia la vulnerabilità dei sistemi OT/SCADA

Cisco Industrial Threat Defense

Marco Stangalino
mstangal@cisco.com

Cisco Industrial IoT investment priorities

CISCO Live!

San Diego, CA
June 8–12, 2025

+

+

+

Security

OT asset visibility to drive segmentation and Zero Trust Remote Network Access

Automation

To simplify, automate, and manage networks at scale

Mobility

Connect the most critical applications wirelessly, reliably, anywhere

AI Infrastructure

Connect assets to allow data extraction to build AI model to drive outcome

Best in class industrial networking to arm our customers to enable IT/OT partnership

NIS2: EU mandate for critical organizations to strengthen their cybersecurity practices

NIS1 Sectors

- Energy
- Transport
- Drinking water
- Healthcare
- …

NIS2: 350,000+ organizations in scope*

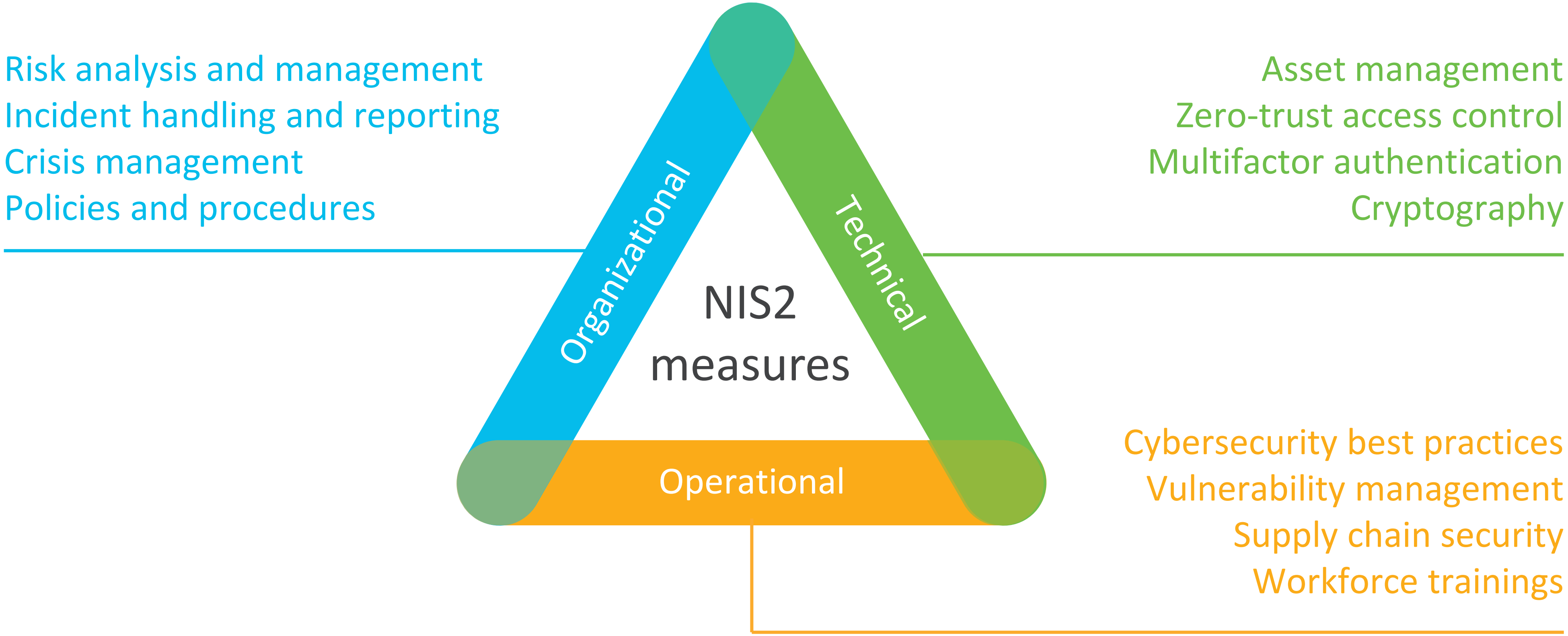
- Wastewater
- Waste
- Manufacturing
- Food & Beverage
- Pharmaceutical
- Postal & Courier
- Chemicals
- …

- NIS2 will be enforced starting Oct 18, 2024
- Mandate to report cyber incidents
  - 24hr incident notification
  - 72hr follow-up report
  - Final report within 1 month
- Personal liabilities for individuals at board level
- Organizations must ensure their suppliers are not putting them at risks

* Source: radargrp.com

EU NIS2 Regulation

Mandatory measures to manage risks



Risk analysis and management
Incident handling and reporting
Crisis management
Policies and procedures

Asset management
Zero-trust access control
Multifactor authentication
Cryptography

Cybersecurity best practices
Vulnerability management
Supply chain security
Workforce trainings

Cisco Validated Designs

Cisco Validated Design

Reference architectures validated for the specific needs of your industry

- Faster deployments
- Less risk
- Predictability
- End to end designs

Design, deploy, and extend networking and cybersecurity technologies successfully

Cisco Secure — Industrial Security — Protecting industrial operations against cyberthreats — Overview

Cisco Secure — Secure Remote Access for OT — Enabling Zero-Trust Network Access (ZTNA) in Operational Spaces — Overview

Cisco Secure — Robust Cybersecurity to Safeguard Roadways Infrastructure — Benefits

Hybrid Cloud Industrial DMZ — Driving industry digitization at scale

Cisco Secure — Securing Distributed Energy Infrastructures with SD-WAN

Cisco Secure — NIS2 Compliance for Industrial Operations with Cisco

NERC CIP Compliance — A Solutions-Based Approach to Network and Cybersecurity for Power Utilities — Overview

ISA/IEC-62443-3-3 — A Cybersecurity Framework to Protect Industrial Automation and Control Systems — Overview

Helping industries with generic and specific designs, as well as addressing regulatory requirements

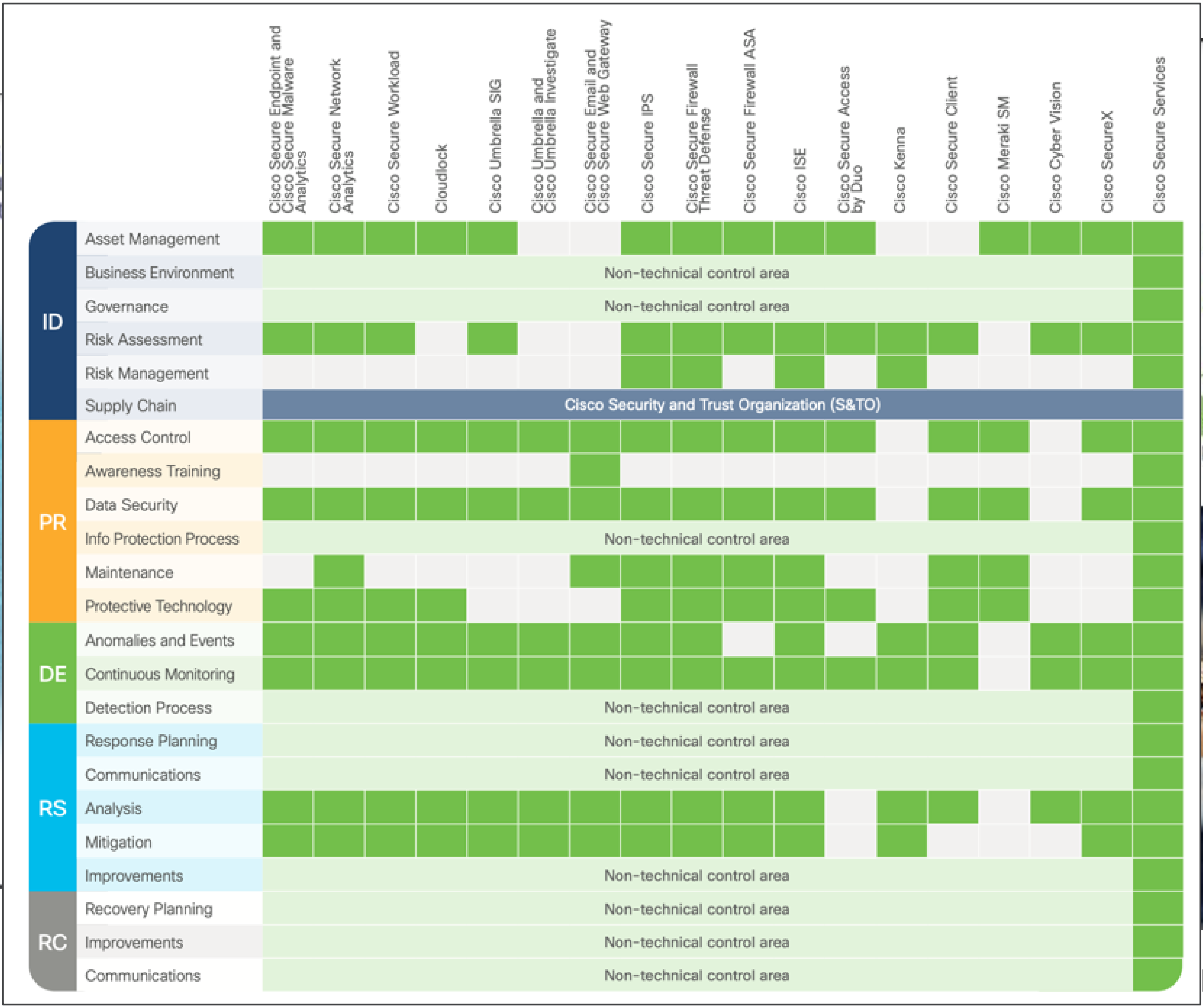
Cybersecurity Framework

Framework Nazi
per la Cybersecu
e la Data Protect

Febbraio 2019

Cyber Intelligence
and Information
Security Center

SAPIENZA
Università di Roma



		Cisco Secure Endpoint and Cisco Secure Malware Analytics	Cisco Secure Network Analytics	Cisco Secure Workload	Cloudlock	Cisco Umbrella SIG	Cisco Umbrella and Cisco Umbrella Investigate	Cisco Secure Email and Cisco Secure Web Gateway	Cisco Secure IPS	Cisco Secure Firewall Threat Defense	Cisco Secure Firewall ASA	Cisco ISE	Cisco Secure Access by Duo	Cisco Kenna	Cisco Secure Client	Cisco Meraki SM	Cisco Cyber Vision	Cisco SecureX	Cisco Secure Services
ID	Asset Management	🟩	🟩	🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩			🟩	🟩	🟩	🟩
	Business Environment	Non-technical control area																	🟩
	Governance	Non-technical control area																	🟩
	Risk Assessment	🟩	🟩	🟩		🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩
	Risk Management								🟩	🟩		🟩		🟩					🟩
	Supply Chain	Cisco Security and Trust Organization (S&TO)																	
PR	Access Control	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩		🟩	🟩
	Awareness Training							🟩											🟩
	Data Security	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩		🟩	🟩
	Info Protection Process	Non-technical control area																	🟩
	Maintenance		🟩					🟩	🟩	🟩	🟩	🟩			🟩	🟩			🟩
	Protective Technology	🟩	🟩	🟩	🟩				🟩	🟩	🟩	🟩	🟩		🟩	🟩			🟩
DE	Anomalies and Events	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩		🟩	🟩		🟩	🟩	🟩
	Continuous Monitoring	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩
	Detection Process	Non-technical control area																	🟩
RS	Response Planning	Non-technical control area																	🟩
	Communications	Non-technical control area																	🟩
	Analysis	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩		🟩	🟩	🟩
	Mitigation	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩				🟩	🟩
	Improvements	Non-technical control area																	🟩
RC	Recovery Planning	Non-technical control area																	🟩
	Improvements	Non-technical control area																	🟩
	Communications	Non-technical control area																	🟩

White Paper
Cisco Public

ure
ST
urity
k
Management

l/security/nist-cybersecurity.pdf

Industrial security themes from our customers

Scalable Visibility

- An order of magnitude more assets in OT than in IT
- Deploying visibility is expensive, leading to stalled projects
- CISOs must depend on IT manpower to deploy and maintain site systems

Dynamic Segmentation

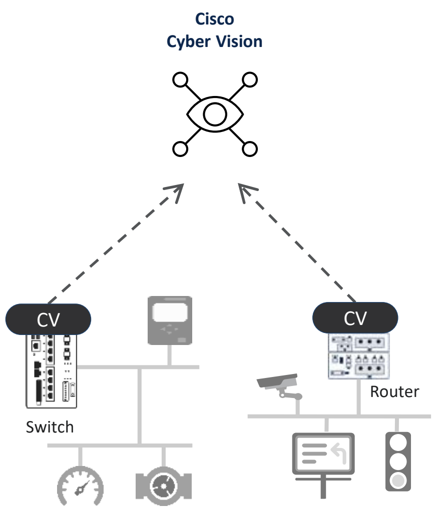
- Downtime due to legitimate process flows getting blocked
- Defining security policy using network constructs is challenging as no one is tracking IP addresses
- Policy needs to evolve dynamically as assets are not always static

Cross-Domain SOC

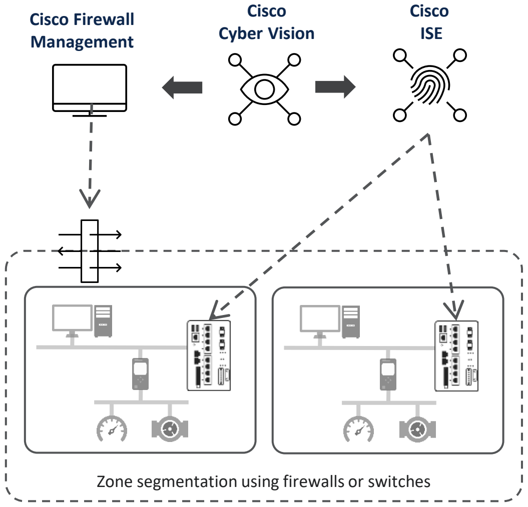
- Poor OT visibility in the SOC
- Lack of IT/OT cross-domain threat context to detect lateral movement
- Risk based alerts to reduce SOC analyst fatigue

Comprehensive industrial security capabilities

1 Asset Visibility and Security Posture

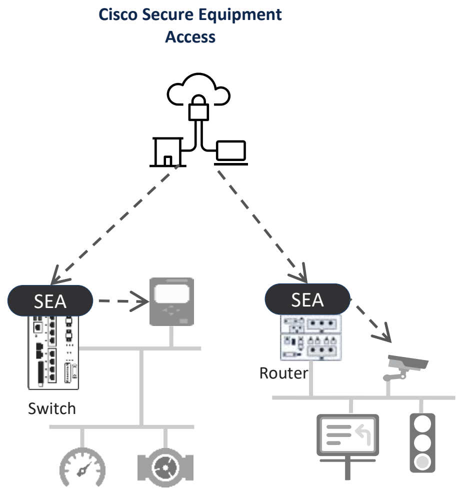


2 Zero Trust Segmentation

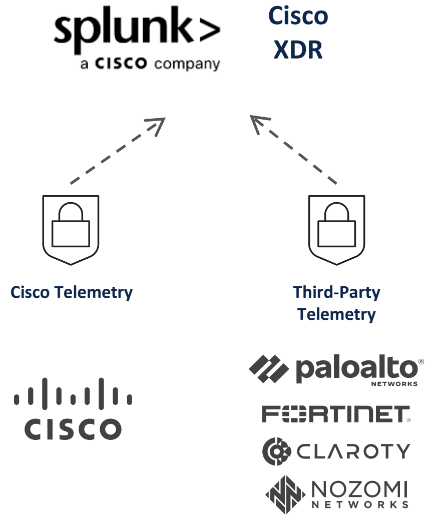


Zone segmentation using firewalls or switches

3 Zero Trust Network Access (ZTNA)



4 Cross-Domain Detection, Investigation & Response

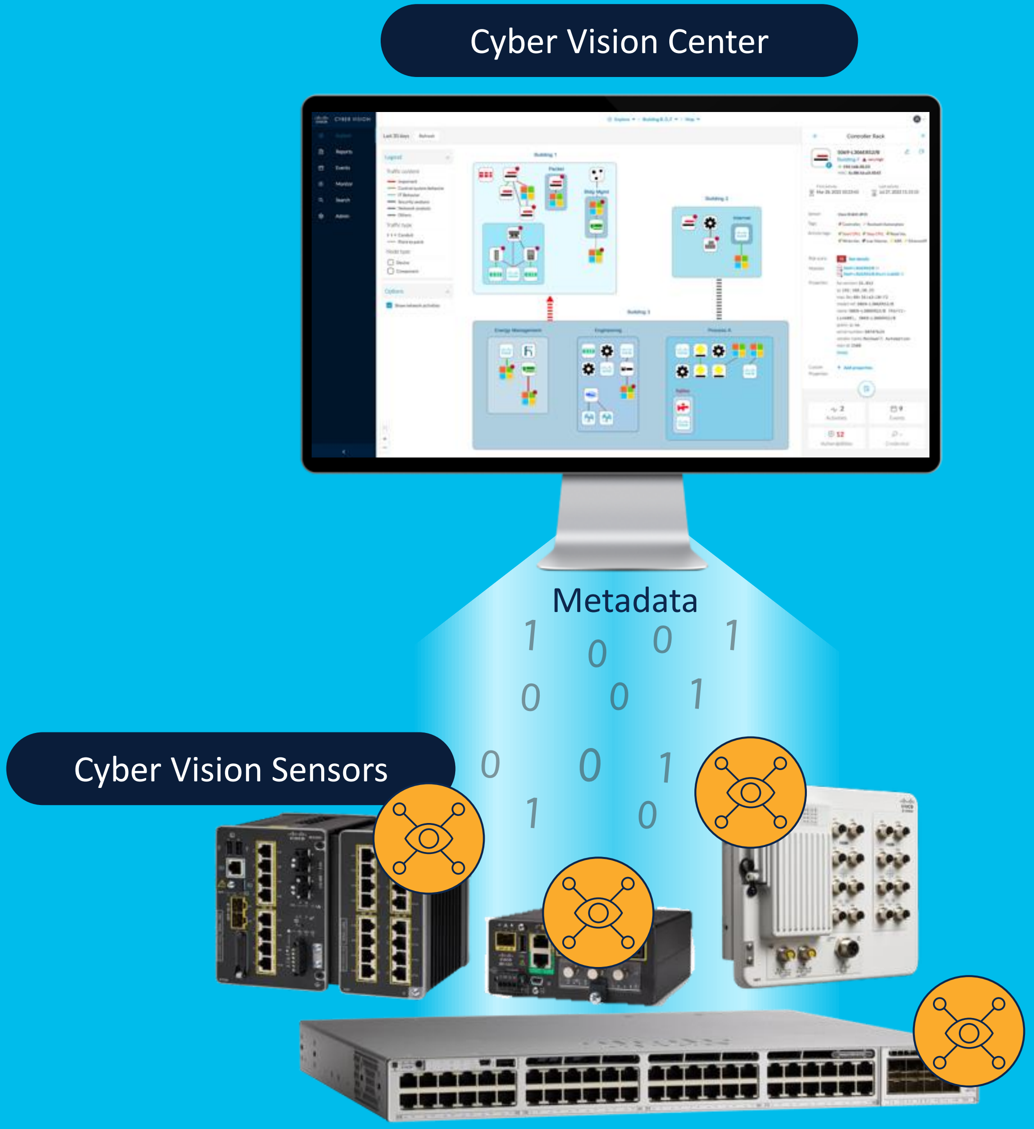


Talos Threat Intelligence + Talos Incident Response

Cyber Vision

Manage risks from OT assets with full visibility
on your industrial security posture

- ✓ Asset Inventory & Profiling
- ✓ Asset Communications
- ✓ Asset Vulnerabilities
- ✓ Asset Risk Scores
- ✓ Behavior Baselining
- ✓ Snort Threat Detection
- ✓ Talos Threat Intelligence



Cyber Vision Center

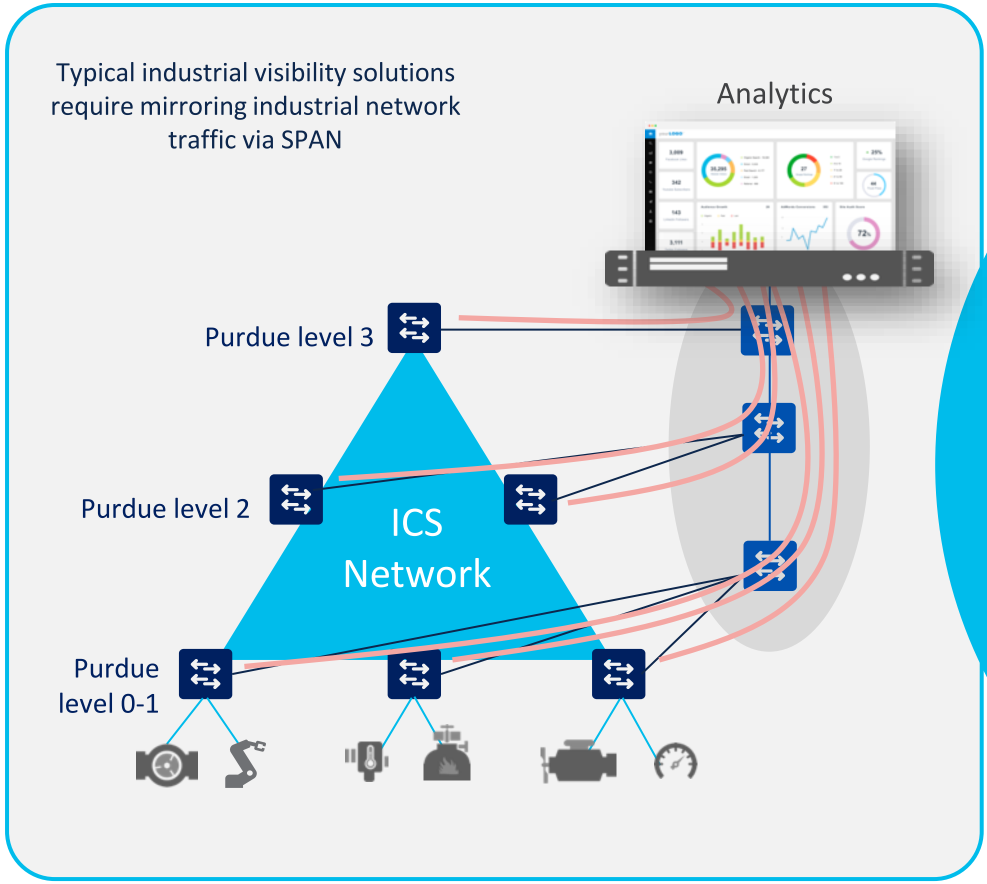
Metadata

Cyber Vision Sensors

Deep Packet Inspection & Active Discovery
built into your network infrastructure

Industrial security starts with OT visibility

But beware of hidden costs!



Typical industrial visibility solutions require mirroring industrial network traffic via SPAN

Additional switches
for SPAN collection

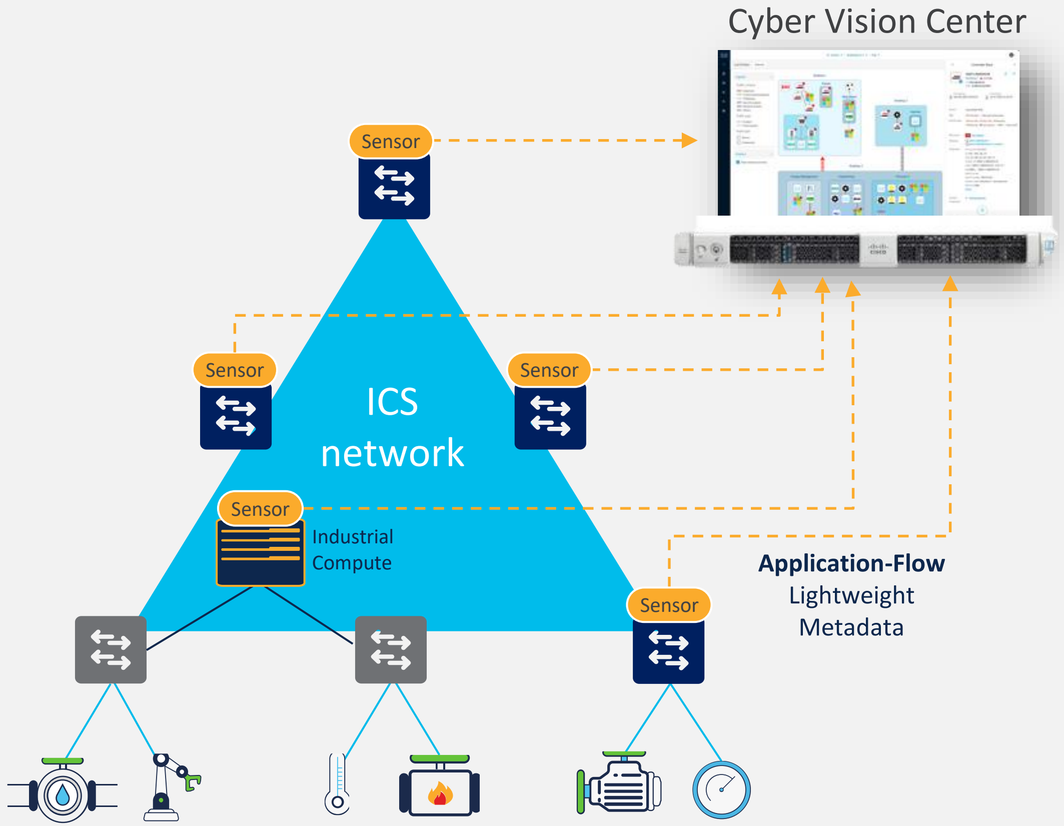
Expensive cabling
for collection network

Exponential traffic increase
due to SPAN

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

Cisco Cyber Vision

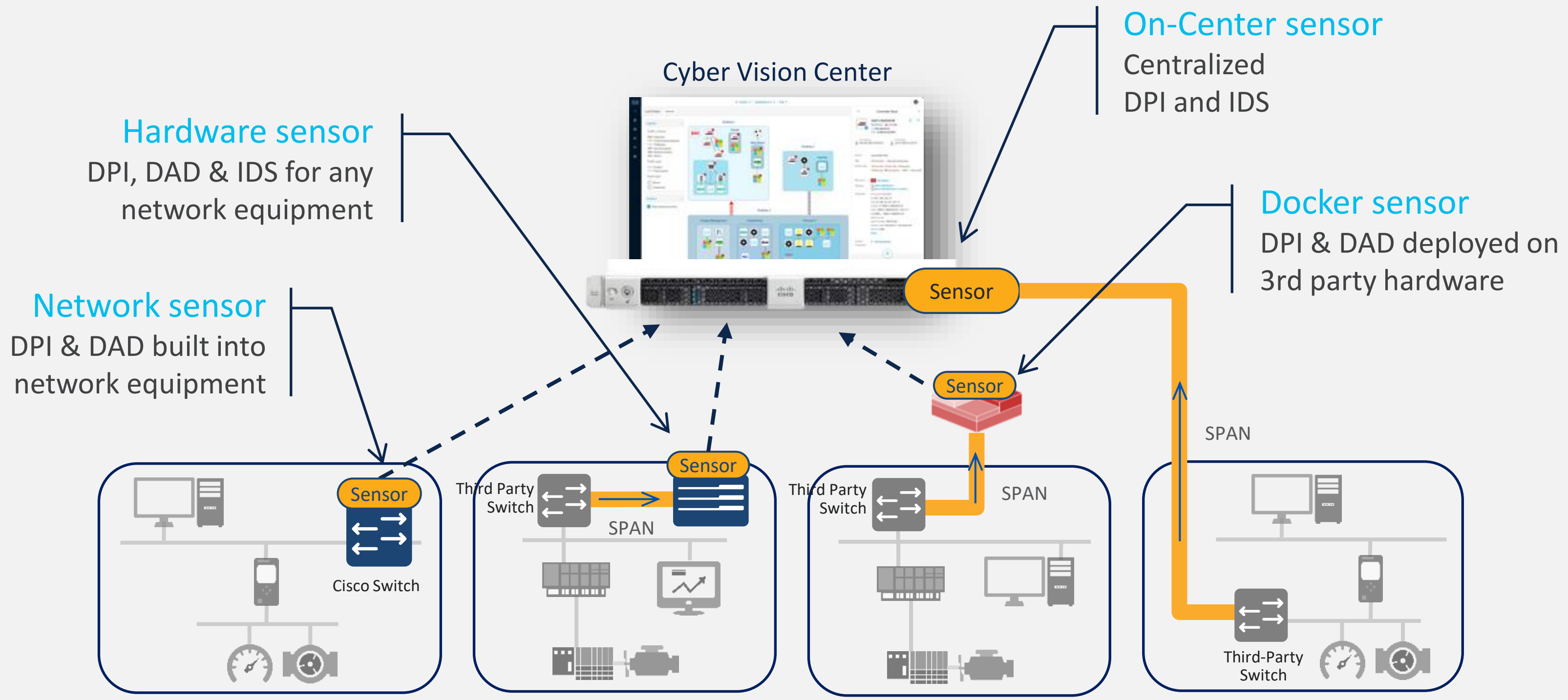
Visibility built into your network infrastructure



- No additional hardware needed
- No need for an out-of-band collection network
- Sends metadata to monitoring console (only ~5% extra traffic)
- Active discovery requests see pass NAT & firewall boundaries
- No complexity (everything is managed from the Center)
- No impact on network performance
- Easy deployment and low TCO

Visibility that can scale to see everything, even at the lower levels of the industrial network

Easy to deploy in Brownfield and Greenfield environments



Hardware sensor
DPI, DAD & IDS for any network equipment

Network sensor
DPI & DAD built into network equipment

On-Center sensor
Centralized
DPI and IDS

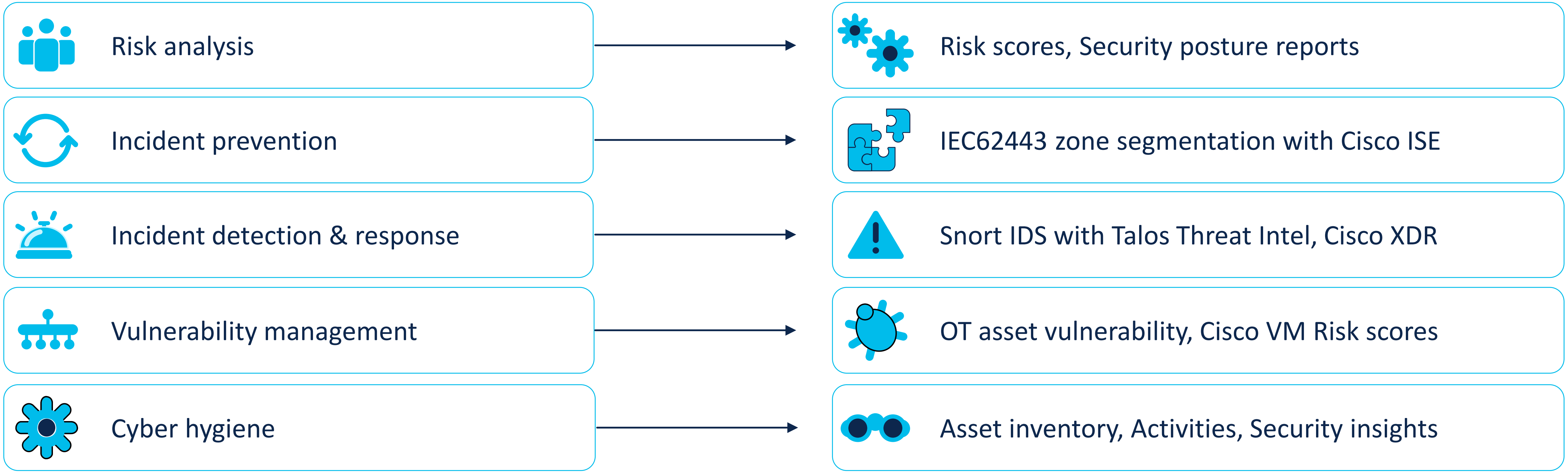
Docker sensor
DPI & DAD deployed on 3rd party hardware

- **Network-sensors** embedded in Cisco networking for simple and highly scalable deployments
- **Hardware or Virtual sensors** capturing traffic on any switch with a single hop SPAN to support brownfield deployments
- **On-Center sensor** to leverage existing SPAN infrastructures, or collect traffic within the datacenter

Cyber Vision offers flexible deployment options

DPI = Deep Packet inspection
DAD = Distributed Active Discovery
IDS = Intrusion Detection System

Understand and minimize risk with Cyber Vision



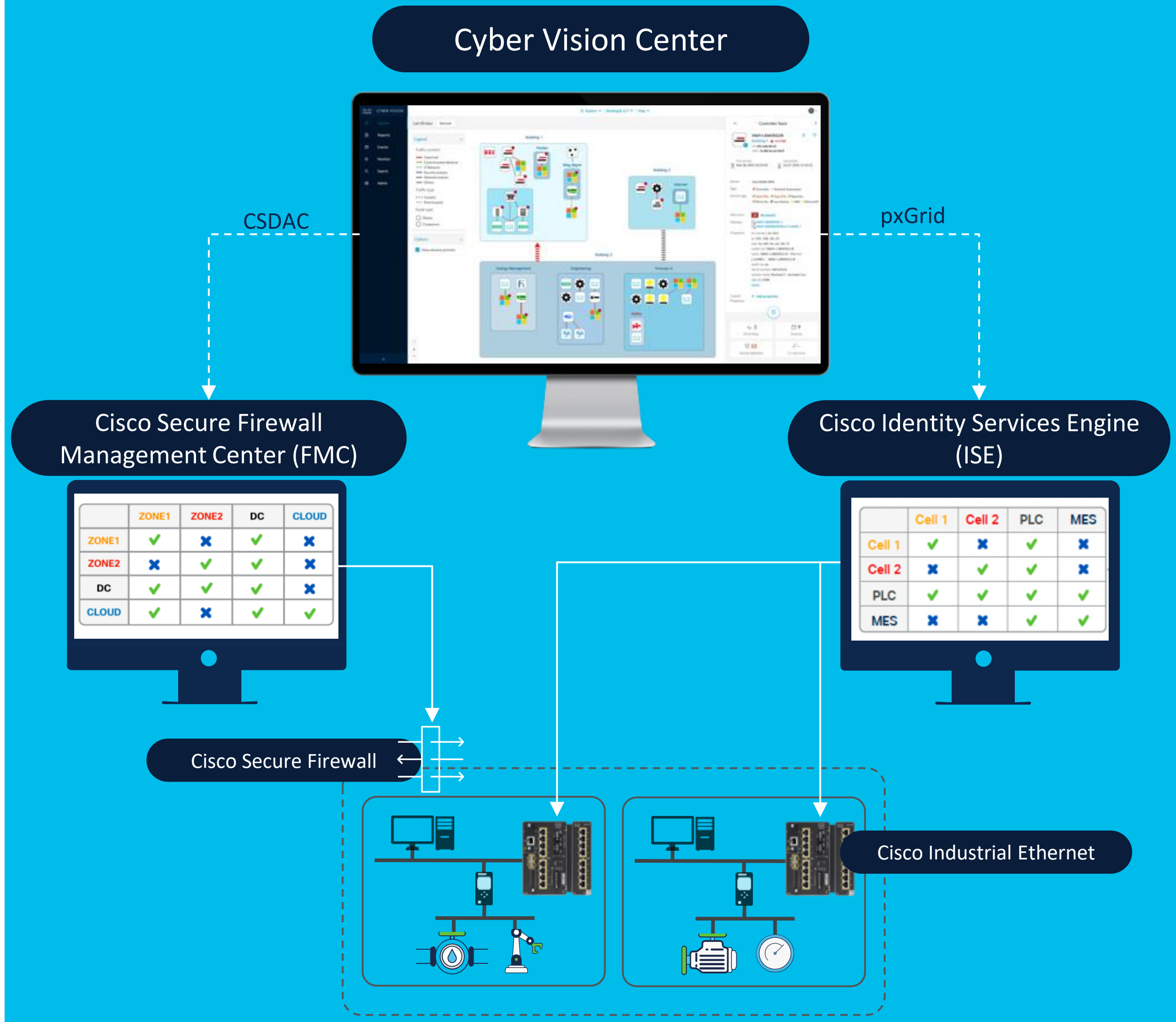
Required NIS2 Measures	Cyber Vision Capabilities
Risk analysis	Risk scores, Security posture reports
Incident prevention	IEC62443 zone segmentation with Cisco ISE
Incident detection & response	Snort IDS with Talos Threat Intel, Cisco XDR
Vulnerability management	OT asset vulnerability, Cisco VM Risk scores
Cyber hygiene	Asset inventory, Activities, Security insights

Assess OT cyber risks with Cyber Vision to implement best practices

Zero Trust Segmentation

OT visibility drives segmentation to mirror industrial processes

- ✓ Enable OT teams to group assets into zones by using Cyber Vision
- ✓ Visualize conduits
- ✓ Identify traffic violations
- ✓ Share context with other platforms to enforce segmentation
- ✓ Automatically update security policy as assets move across the network


Cyber Vision Center
CSDAC
pxGrid
Cisco Secure Firewall Management Center (FMC)
Cisco Identity Services Engine (ISE)
Cisco Secure Firewall
Cisco Industrial Ethernet

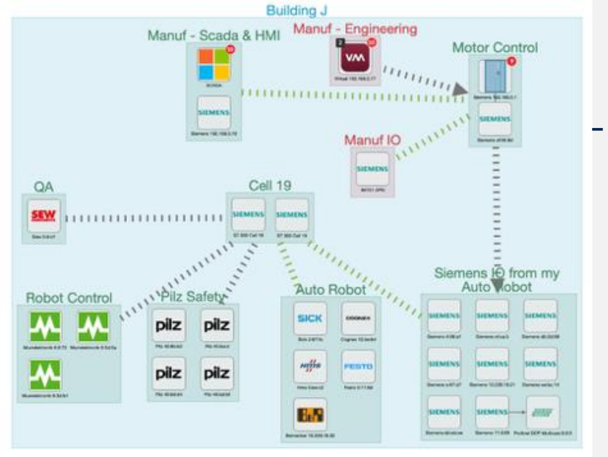
	ZONE1	ZONE2	DC	CLOUD
ZONE1	✓	✗	✓	✗
ZONE2	✗	✓	✓	✗
DC	✓	✓	✓	✗
CLOUD	✓	✗	✓	✓

	Cell 1	Cell 2	PLC	MES
Cell 1	✓	✗	✓	✗
Cell 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

Automated **ISA/IEC-62443** zone segmentation using firewalls or switches

Visibility drives segmentation with Cisco Secure Firewalls

Grouping assets in Cyber Vision…



CSDAC

…populates dynamic objects in FMC

Cisco Secure Firewall Management Center

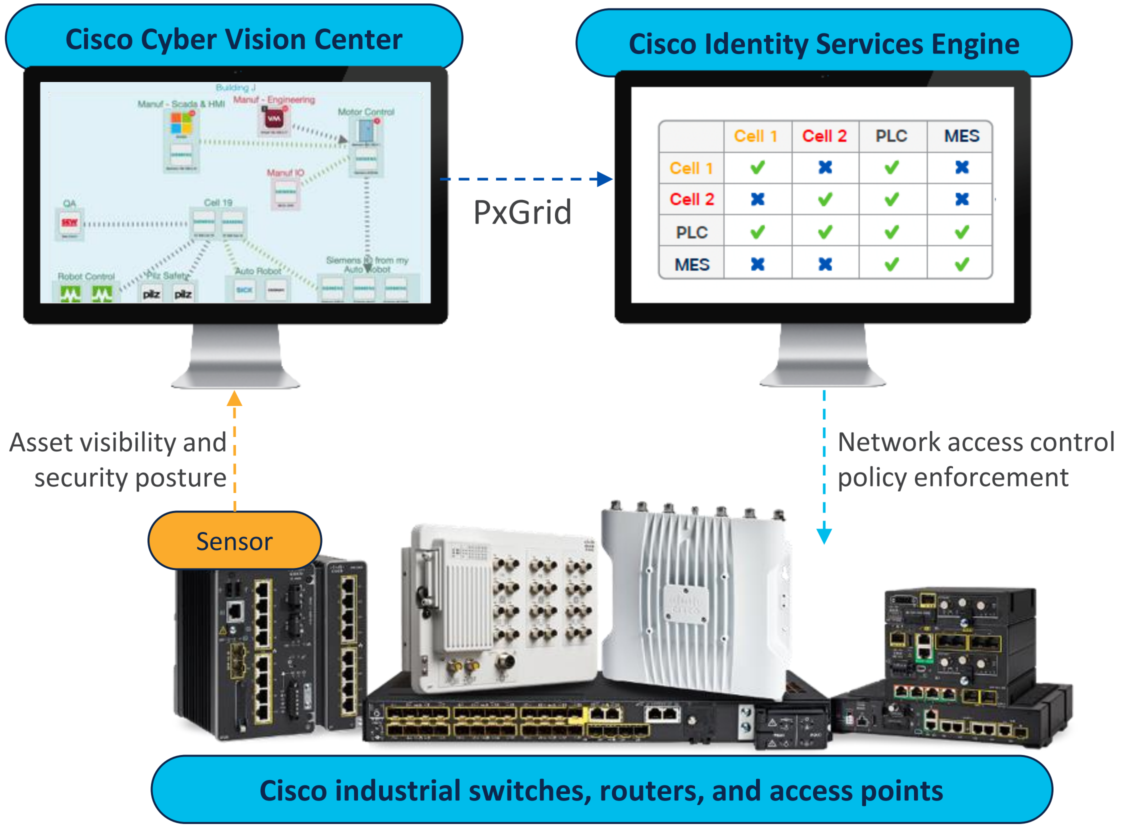
Cisco Secure Firewall

Cisco Cyber Vision
Gain full visibility into assets, and group them according to their role in the industrial process

Cisco Secure Firewall
Automatically restrict zone to zone communication based on Cyber Vision groups

Simplifying network segmentation with dynamic firewall rules informed by OT visibility

Visibility drives segmentation with Cisco ISE


Cisco Cyber Vision Center
Building J
Manuf - Scada & HMI
Manuf - Engineering
Motor Control
Manuf IO
QA
Cell 19
Robot Control
Pilz Safety
Auto Robot
Siemens from my Auto Robot
PxGrid
Cisco Identity Services Engine
Asset visibility and security posture
Sensor
Network access control policy enforcement
Cisco industrial switches, routers, and access points

	Cell 1	Cell 2	PLC	MES
Cell 1	✓	✗	✓	✗
Cell 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

Cisco Cyber Vision
Gain full visibility into assets, and group them according to their role in the industrial process

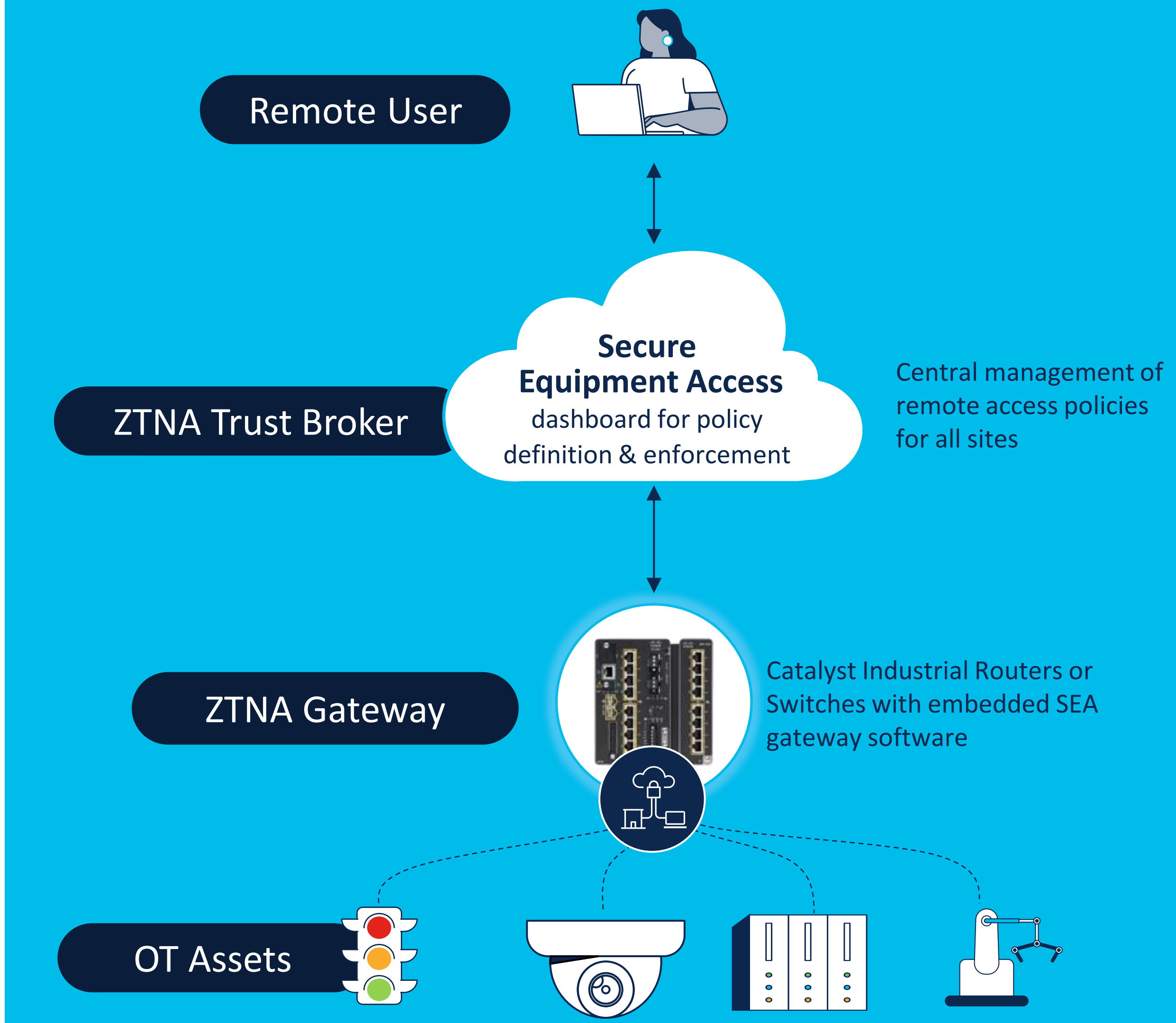
Cisco Identity Services Engine
Automatically update access control policies for the network to enforce zero-trust segmentation based on Cyber Vision groups

Enforcing TrustSec network segmentation with profiling policy driven by Cyber Vision

Secure Equipment Access (SEA)

Manage risks from suppliers with ZTNA remote access to OT assets

- ✓ Zero Trust MFA & SSO
- ✓ OT Asset Resource Isolation
- ✓ Clientless & Agent-based Access
- ✓ Remote User Host Posture Check
- ✓ Session Scheduling
- ✓ Session Recording, Monitoring & Kill
- ✓ Session Approval on Request



Remote User

ZTNA Trust Broker

Secure Equipment Access dashboard for policy definition & enforcement

Central management of remote access policies for all sites

ZTNA Gateway

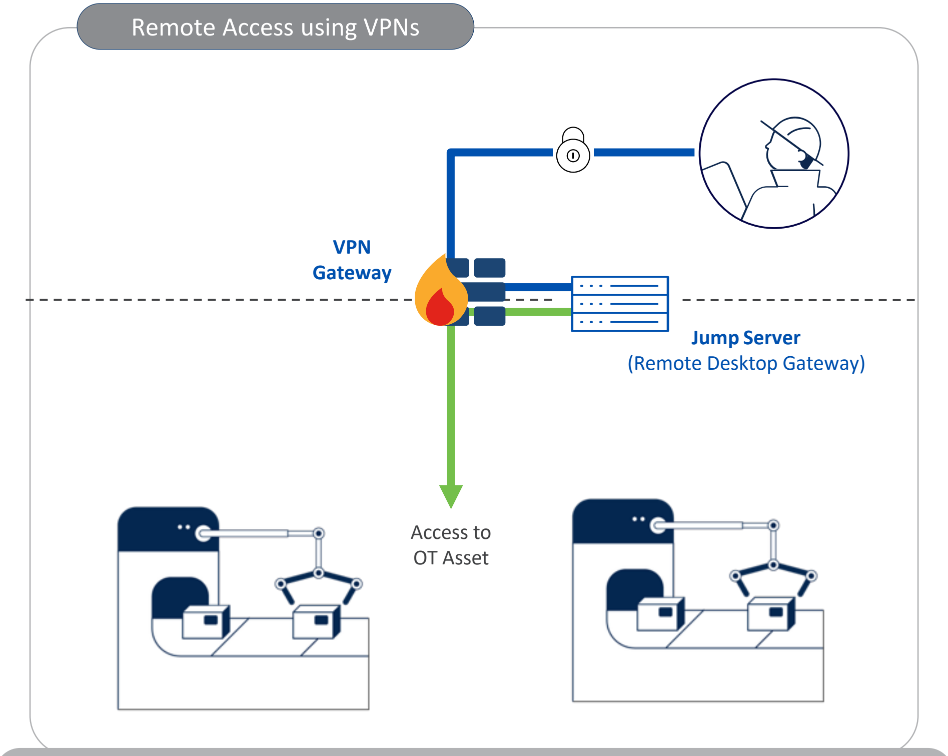
Catalyst Industrial Routers or Switches with embedded SEA gateway software

OT Assets

One-click **zero trust remote access to any OT asset** connected to Cisco industrial network

Secure Remote Access for OT

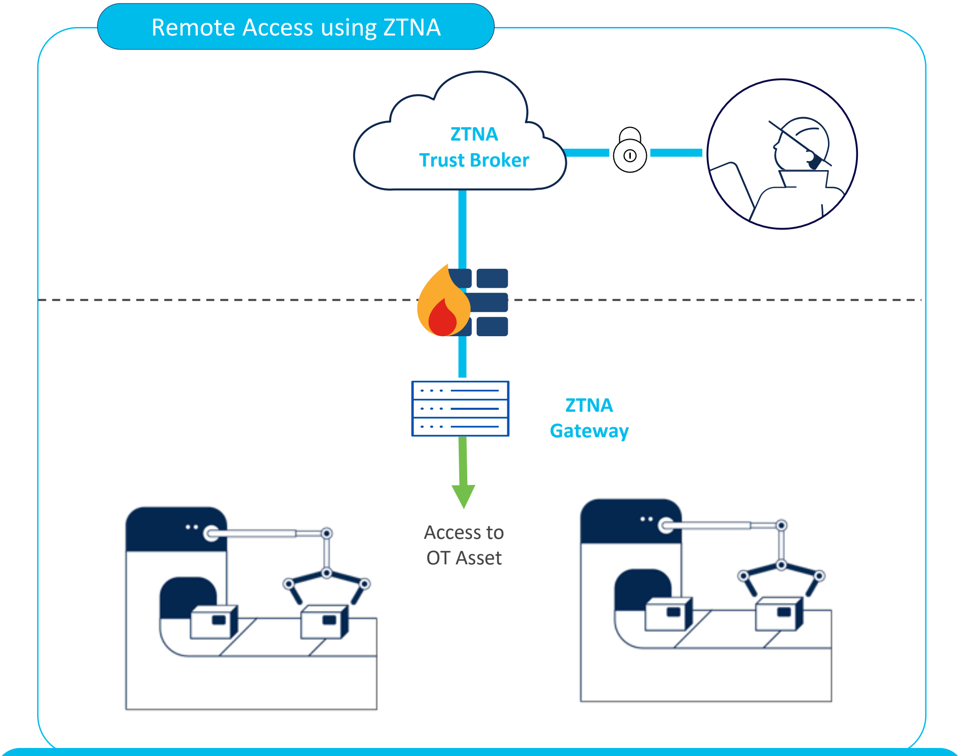
Evolving from VPNs to ZTNA



Remote Access using VPNs

Always-on solutions with all-or-nothing access

Granular access policies hard to enforce and maintain



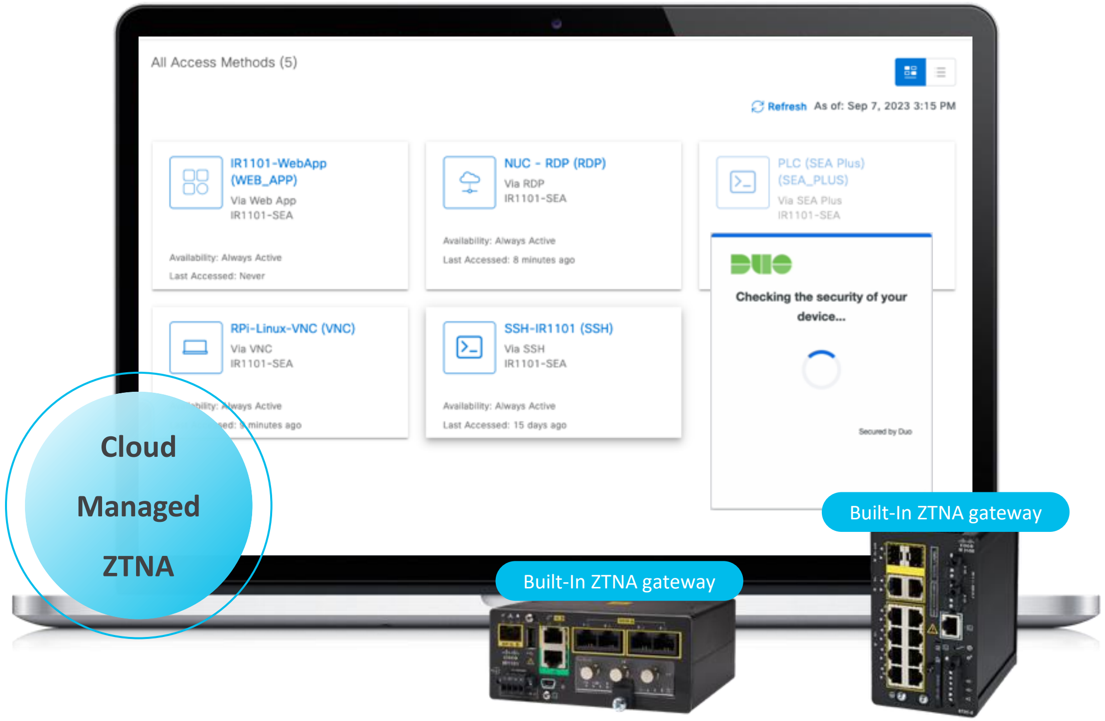
Remote Access using ZTNA

Granular access policies defined and enforced centrally

Seamless connectivity to OT assets

Cisco Secure Equipment Access

Move beyond conventional remote access to ZTNA for OT assets



All Access Methods (5)

Refresh As of: Sep 7, 2023 3:15 PM

IR1101-WebApp (WEB_APP)
Via Web App
IR1101-SEA
Availability: Always Active
Last Accessed: Never

NUC - RDP (RDP)
Via RDP
IR1101-SEA
Availability: Always Active
Last Accessed: 8 minutes ago

PLC (SEA Plus) (SEA_PLUS)
Via SEA Plus
IR1101-SEA

RPi-Linux-VNC (VNC)
Via VNC
IR1101-SEA
bility: Always Active
sed: 9 minutes ago

SSH-IR1101 (SSH)
Via SSH
IR1101-SEA
Availability: Always Active
Last Accessed: 15 days ago

DUO

Checking the security of your device...

Secured by Duo

Catalyst Industrial Routers

Catalyst Industrial Switches

Stop security backdoors from cellular gateways

Take control back and eliminate complexity of maintaining point hardware for remote access.

Eliminate the IDMZ/Firewall complexity

Get remote access to assets using the same switch that provides secure connectivity.

Enforce zero trust controls in OT

Configure least-privilege access and enforce schedules, device posture check, MFA, and more.

Empower operations teams while enforcing least-privilege remote access policies

Minimize risk from suppliers and contractors with SEA

Required NIS2 Measures

- Access Control Policies
- Supply Chain Security
- Multifactor Authentication

Strong authentication

SSO, MFA, and remote workstation posture check

Least privilege access policies

OT asset and resource isolation

Context-aware access policies

Agent-based and clientless controls

Fine grained Access Control

Time-based access policies

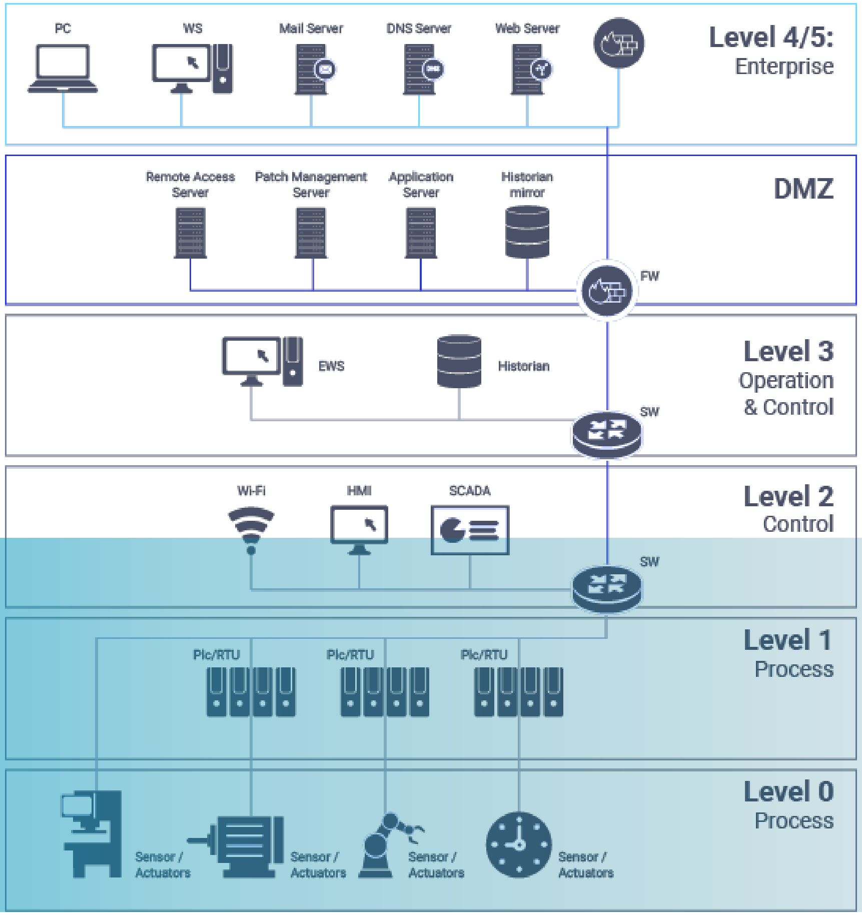
Comprehensive audit trial

Exporting logs, session monitoring and termination

Minimize cyber risk from remote users with Secure Equipment Access

A siloed approach is not enough to secure OT

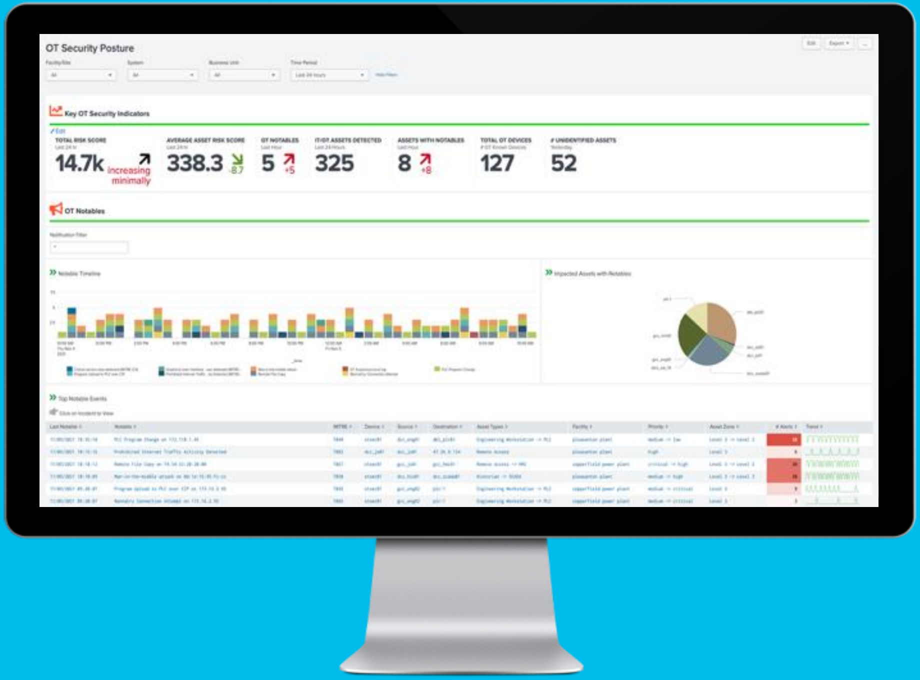
With digitization, OT, IT, and Cloud domains are getting increasingly interconnected



Splunk OT Security

Break silos between OT & IT domains with cross-domain detection and remediation

- ✓ OT Asset Investigator
- ✓ NERC-CIP compliance reports and MITRE ATT&CK ICS correlation rules
- ✓ Perimeter Monitoring
- ✓ Risk Based Alerting
- ✓ OT Baselining
- ✓ OT Use Case Library
- ✓ Unified IT/OT security events management in Splunk SIEM

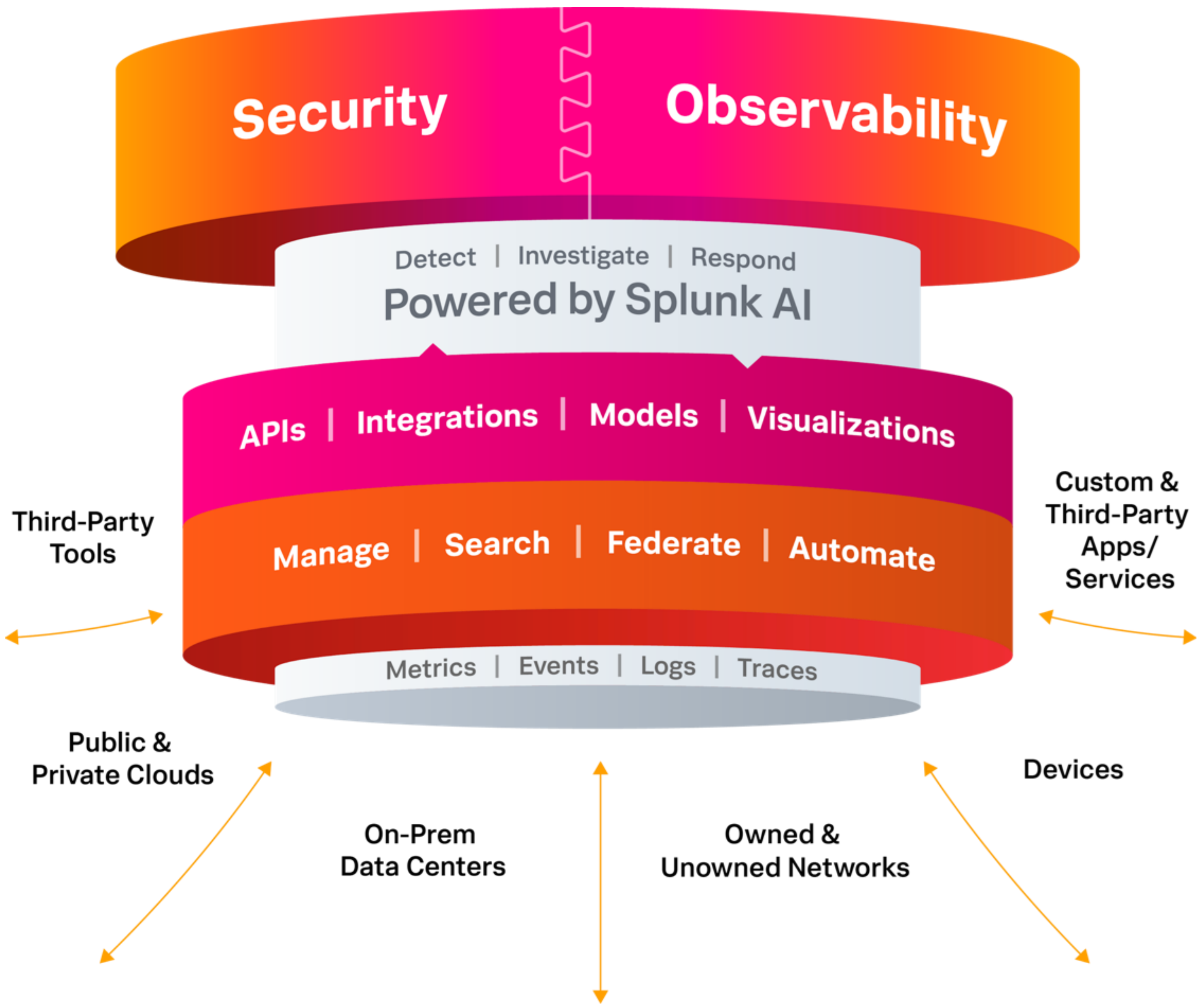


Improve threat detection, incident investigation, and response **across OT & IT domains** with telemetry from Cisco and 3rd party security products

The Unified Security and Observability Platform

Monitor, investigate and respond rapidly at scale with comprehensive visibility and shared tooling.

8B
monthly searches
2.8K+
apps & add-ons on Splunkbase
~1K
purpose built data source integrations
splunk>


Security
Observability
Detect | Investigate | Respond
Powered by Splunk AI
APIs | Integrations | Models | Visualizations
Manage | Search | Federate | Automate
Metrics | Events | Logs | Traces
Third-Party Tools
Custom & Third-Party Apps/ Services
Public & Private Clouds
On-Prem Data Centers
Owned & Unowned Networks
Devices

From raw data to business value

Prevent unplanned outages

Visibility is key to a modernized grid. Poor insight and increasing complexity can lead to catastrophic downtimes.

Improve uptime, performance and response times of business-critical applications and the infrastructure they run on.

Enhance operational efficiency

Operational efficiency is crucial, but systems have become more complex and difficult to oversee.

Predict failures and make informed decisions faster across complex, cloud-native, on-premises and hybrid environments.

Reimagine the service delivery experience

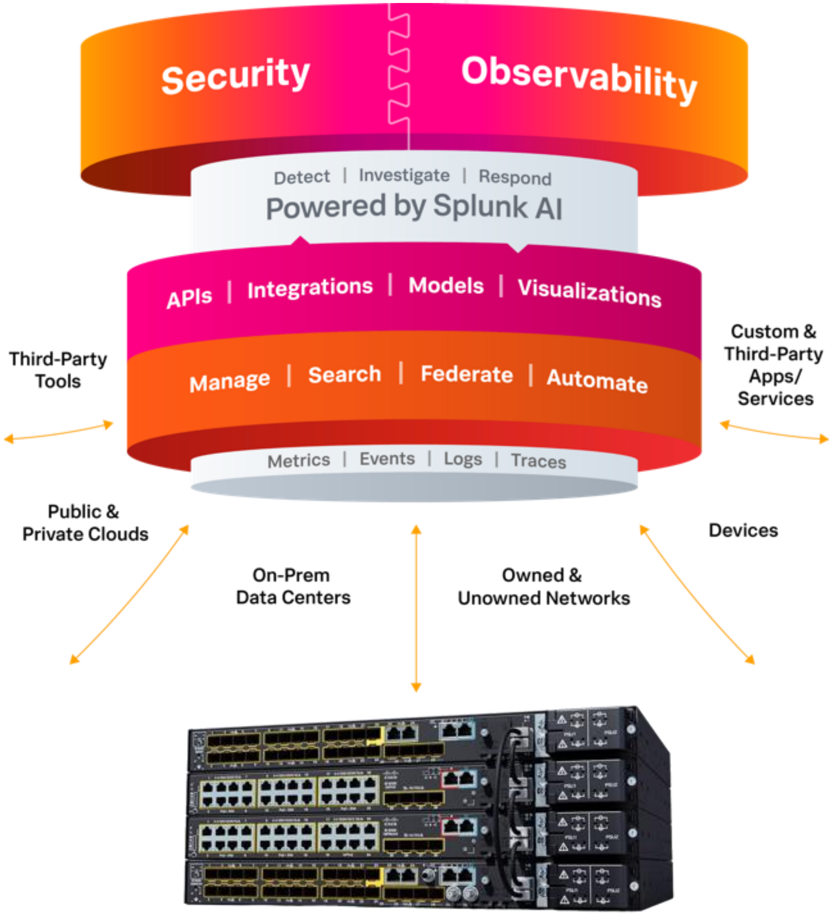
Consumers are changing — it's time to change with them.

Deliver exceptional user experiences that match the pace of innovation.

Maintain security and compliance

Critical infrastructure is at risk — and the attack surface is widening.

Protect essential data, assets and infrastructure from internal and external threats.



Security | Observability

Detect | Investigate | Respond

Powered by Splunk AI

APIs | Integrations | Models | Visualizations

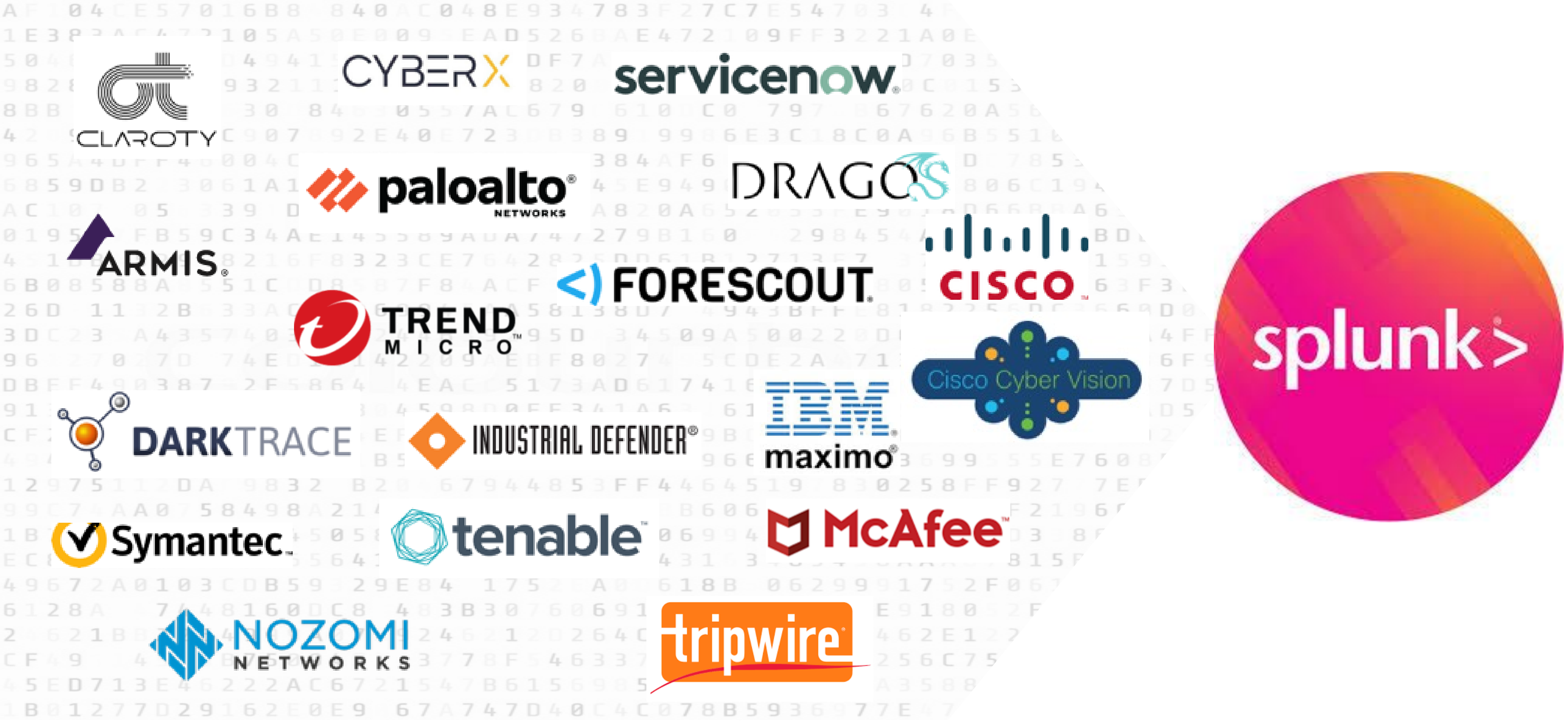
Manage | Search | Federate | Automate

Metrics | Events | Logs | Traces

Devices

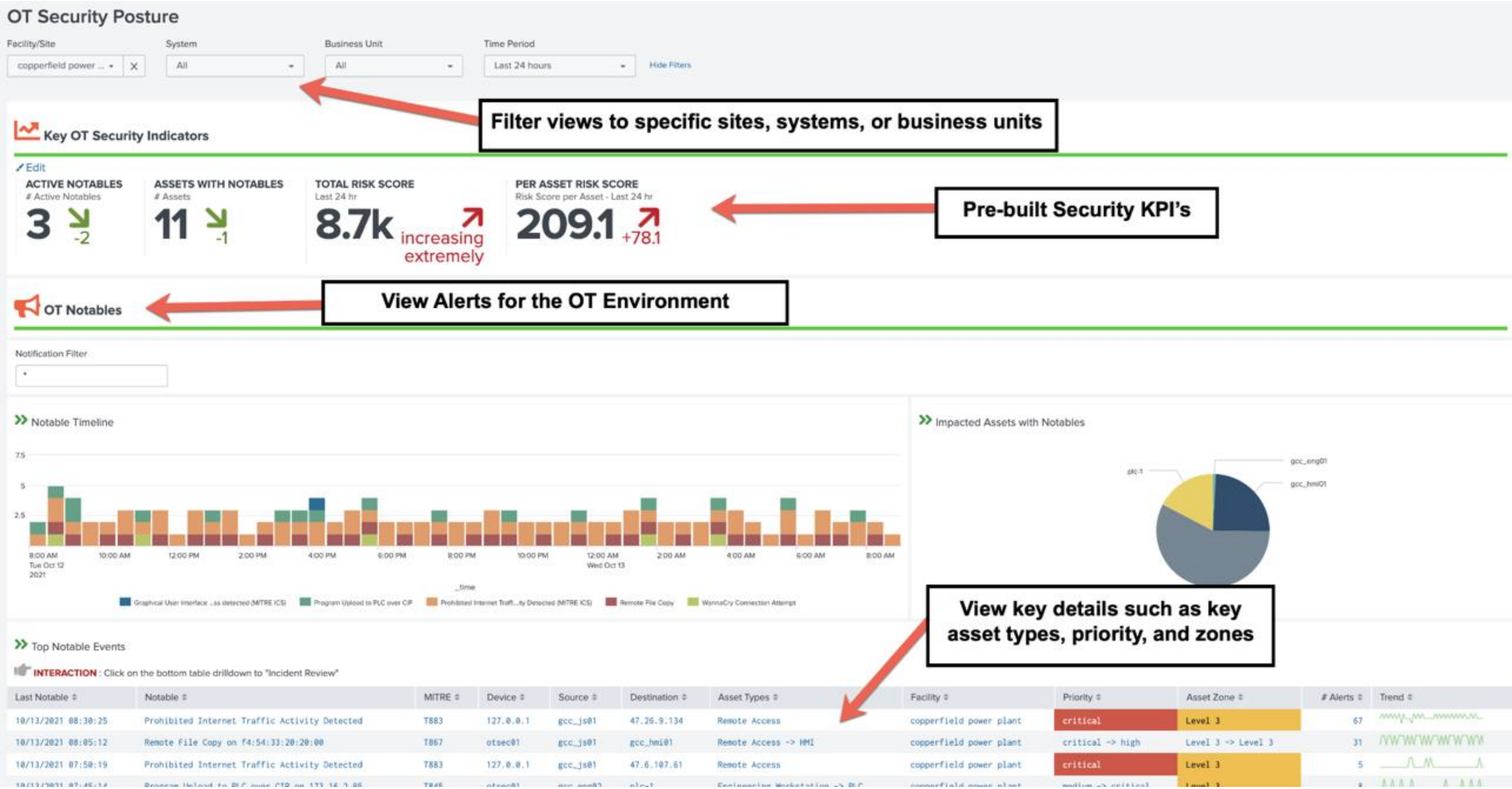
OT Data Source Integrations

A wide variety of sources integrate to Splunk's Common Information Model



- Logs (OS, App, etc.)
- CVEs
- Network Traffic
- Asset Inventory
- Notables
- Patch Management
- Endpoint activity

OT Security Posture



OT Security Posture

Facility/Site: copperfield power ... ✕

System: All

Business Unit: All

Time Period: Last 24 hours

Filter views to specific sites, systems, or business units

Key OT Security Indicators

ACTIVE NOTABLES	ASSETS WITH NOTABLES	TOTAL RISK SCORE	PER ASSET RISK SCORE
# Active Notables	# Assets	Last 24 hr	Risk Score per Asset - Last 24 hr
3 ↘ -2	11 ↘ -1	8.7k ↗ increasing extremely	209.1 ↗ +78.1

Pre-built Security KPI's

OT Notables

View Alerts for the OT Environment

Notification Filter: *

Notable Timeline

7.5
5
2.5
8:00 AM
Tue Oct 12
2021
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
12:00 AM
Wed Oct 13
2:00 AM
4:00 AM
6:00 AM
8:00 AM
_time
Graphical User Interface ...ss detected (MITRE ICS)
Program Upload to PLC over CIP
Prohibited Internet Traff...ty Detected (MITRE ICS)
Remote File Copy
WannaCry Connection Attempt

Impacted Assets with Notables

View key details such as key asset types, priority, and zones

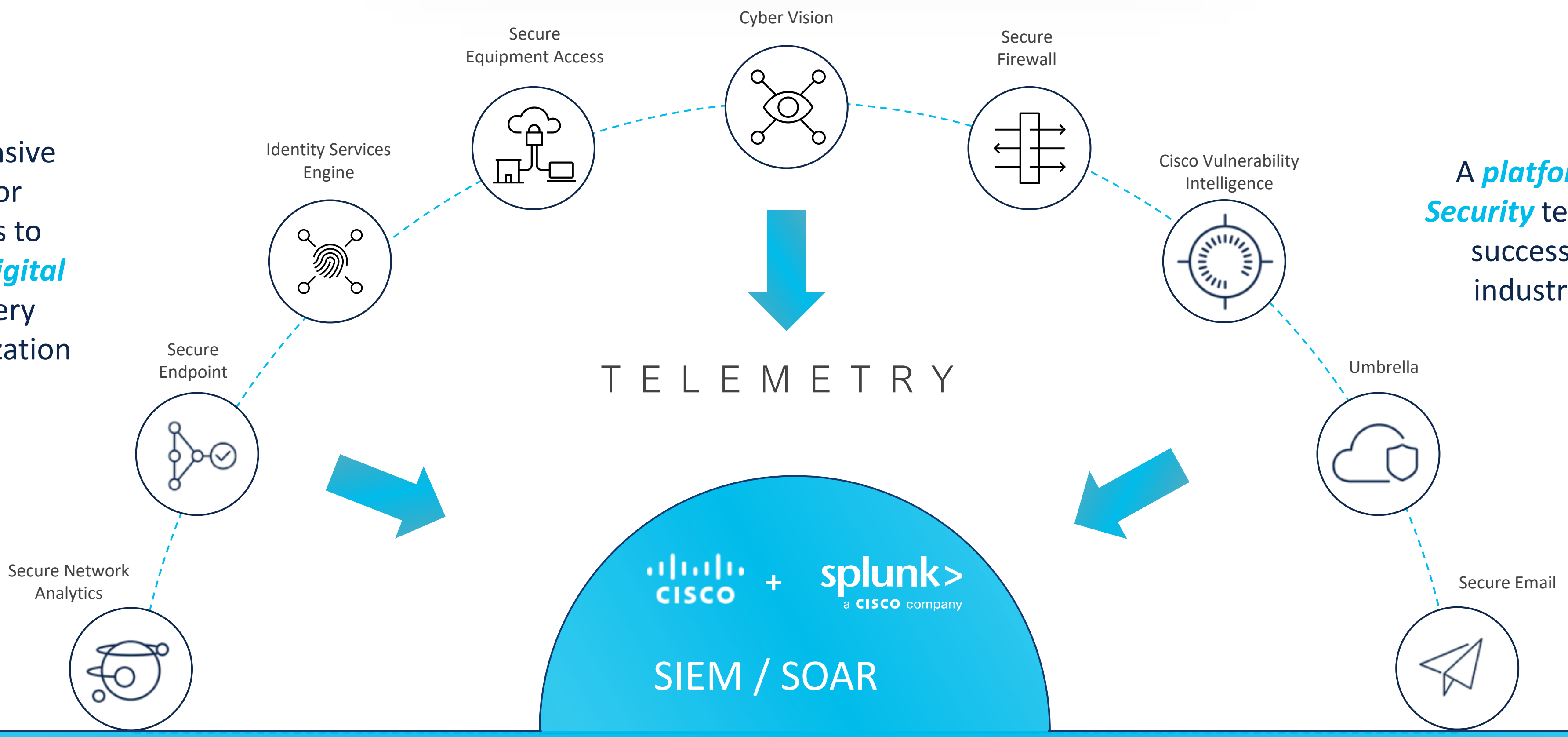
Top Notable Events

INTERACTION : Click on the bottom table drilldown to "Incident Review"

Last Notable ⇕	Notable ⇕	MITRE ⇕	Device ⇕	Source ⇕	Destination ⇕	Asset Types ⇕	Facility ⇕	Priority ⇕	Asset Zone ⇕	# Alerts ⇕	Trend ⇕
10/13/2021 08:30:25	Prohibited Internet Traffic Activity Detected	T883	127.0.0.1	gcc_js01	47.26.9.134	Remote Access	copperfield power plant	critical	Level 3	67	
10/13/2021 08:05:12	Remote File Copy on f4:54:33:20:20:00	T867	otsec01	gcc_js01	gcc_hmi01	Remote Access -> HMI	copperfield power plant	critical -> high	Level 3 -> Level 3	31	
10/13/2021 07:50:19	Prohibited Internet Traffic Activity Detected	T883	127.0.0.1	gcc_js01	47.6.107.61	Remote Access	copperfield power plant	critical	Level 3	5	
10/13/2021 07:45:14	Program Upload to PLC over CIP on 172.16.2.06	T845	otsec01	gcc_eng02	plc-1	Engineering Workstation -> PLC	copperfield power plant	medium -> critical	Level 3	8	

Threat Intelligence — AI — Identity Intelligence

The most comprehensive security solution for industrial customers to ***protect their entire digital footprint*** across every aspect of their organization



A ***platform for OT, IT, and Security*** teams ***to partner*** and successfully defend the industrial environment

AI powered cross-domain security across IT, OT, and Cloud

Putting it all together

Helping Industries Connect and Secure Operations

Best of Cybersecurity

Comprehensive capabilities

+

Best of OT Networking

Deep understanding of industrial requirements

OT Visibility

Zero Trust Network Access

Network Segmentation

Cisco + Splunk SOC of the future

Threat Intelligence & Incident Response

From OT visibility to Cross-Domain Detection, Investigation, and Remediation

The bridge to possible

“You couldn't bomb a plant you didn't know about, but you could possibly cyberbomb it”

Kim Zetter

Q&A

11 LUGLIO: Accesso Sicuro, Futuro Protetto: Il Viaggio con Cisco Duo

18 LUGLIO: TBD

https://events.tdsynnex.it/cyber-unit-missione-protezione/

TEAM CISCO: it.cisco@tdsynnex.com
SPEAKER: federico.frosini@tdsynnex.com mstangal@cisco.com
giacomoalberto.casati@tdsynnex.com andrea.pezzoni@tdsynnex.com