CISCO
SECURE

Modernisierung der Netzwerksicherheit: Strategien für verbesserte Resilienz in kritischen Infrastrukturen

NIS-2 Compliance with Cisco Secure

Andreas Hack
Cybersecurity Architect Austria
Juni, 2024

Agenda

- NIS-2 Big Ten Measures – Cisco can help
- Secure Critical Infrastructure
- OT Secure Remote Access
- Network Segmentation and Integrations
- Threat Hunting with XDR
- Cisco Security Portfolio

NIS-2 Big Ten Measures

Security Regulatory & Standards

European

NIS Directive (EC2016/1148)

Cybersecurity Act (EC2019/881)

Cyber Resilience Act

ENISA (European Union Agency for Cybersecurity

EPCIP, European Programme for Critical Infrastructure

Digital Operational Resilience Act (DORA)

National

NISG (AT: NIS-2-RL)

IT-Sicherheitsgesetz (DE: IT-SiG2.0)

Kritische Infrastruktur (DE: BSI-KritisV; AT: APCIP)

DE: BSIG § 3 Qualifizierte APT-Response Dienstleister
(Cisco Talos Incident Response Retainer)

Standards

ISO/IEC 27001 (InfoSec)

ISO/IEC 27019 (Energy)

ISO/IEC 27799 (Gesundheit)

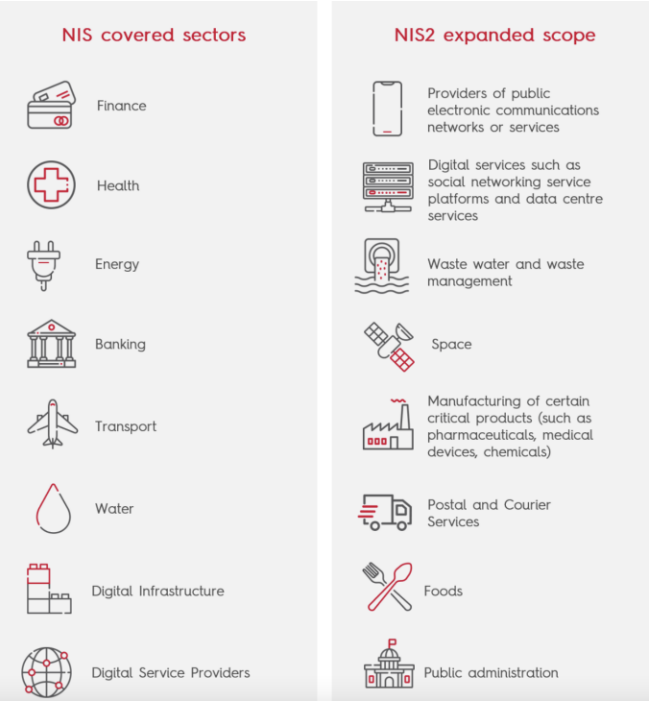
IEC 62443 (OT Security)

NIST Cybersecurity Framework

NISG – Netz und Informationssicherheitsgesetz
BSIG - Bundesamt für Sicherheit in der Informationstechnik Gesetz
APCIP - Österreichisches Programm zum Schutz kritischer Infrastrukturen
APT - Advanced Persistent Threat Response

Massive increase in scope in comparison to NIS 1

- 40 times more entities are involved/subject to comply with
- IT and OT are in the scope
- Companies with 50+ employees or €10m + turnover
- Terminology changes vs NIS1 (Operators of Essential Services (OESs), Digital Service Providers (DSPs):
  - ***Essential Entities (EE),*** detailed in Annex I of the NIS2 text
  - ***Important Entities (IE),*** detailed in Annex II of the NIS2 text



Mapping NIS-2 Article 21 and 23 to Cisco Solutions

Required NIS-2 Measures	Cisco Capabilities
Policy and Risk Analysis	CX Advisory services
Incident handling	CX Services, Talos Incident Response
24h reporting	Cisco XDR, Splunk
Vulnerability management	Cisco Vulnerability Management in the future: Cisco Hypershield
Cyber hygiene / training	Cisco helping building awareness, Cisco Networking Academy, Cisco Skills For All
Zero Trust	Duo, Segmentation, IoT

NIS-2 “Big 10” Measures – Cisco Security Reference	How Cisco can help – Mapping					
a) risk analysis and information system security policies;	ISMS, InfoSec Pentest (CX) ISO 27001	ASRM (Attack Surface Management) GAP-A (CX)	EDR (Secure Endpoint) XDR/MDR Awareness (CX)	NAC (ISE) MFA (DUO)	Secure FW VPN (Secure Client)	Web Sec (Umbrella) (Secure Email)
b) Incident handling (prevention, detection, and response to incidents);	IR (Talos)	SOC (XDR/MDR)	EDR (Secure Endpoint) XDR/MDR	NDR (SNA, SW)	BMS (Cyber Vision)	
c) business continuity and crisis management;	IR (Talos)	SOC (XDR/MDR)	Backup / Restore (Cohesity)	BMS (Cyber Vision)	Emergency Handbook (CX)	
d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;	Certificates ISO 27000	SBOM (Cloud Application Security)	Jumphost (Secure Firewall, Secure Equipment Access)	VPN (Secure Firewall, Secure Client)	MFA (DUO)	
e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	ISMS, InfoSec IR (Talos)	ASRM (Attack Surface Management) XDR/MDR	EDR (Secure Endpoint) XDR/MDR	NAC (ISE) MFA (DUO) NDR (SNA, SW)	Secure FW VPN (Secure Client)	Web Sec (Umbrella) (Secure Email)
f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;	ISMS, InfoSec Pentest (CX) ISO 27000	ASRM (Attack Surface Management) GAP-A (CX)	(Vulnerability Management)			
g) basic cyber hygiene practices and cybersecurity training;	Pentest (CX)	GAP-A (CX)	Awareness (CX)			
h) policies and procedures regarding the use of cryptography and, where appropriate, encryption:	FW (Secure Firewall) VPN (Secure Client)	ZTNA (Secure Access)	Web Sec (Umbrella)	Data Encryption (Webex)	Data Loss Prevention (CloudLock)	
i) human resources security, access control policies and asset management;	GAP-A (CX)	Awareness (CX)	MFA (DUO)	NAC (ISE)	Asset Visibility (Cyber Vision)	ZTNA (Secure Equipment Access)
j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	MFA (DUO)	NAC (ISE)	ZTNA (Secure Access)	Email (Secure Email)	Voice, Video (CUCM, SRST)	Messaging, Calling (Webex)

How Cisco Cyber Vision helps with NIS-2 compliance

Required NIS-2 Measures	Cyber Vision Capabilities
Risk analysis	Risk scores, Security posture reports
Incident prevention	IEC62443 segmentation with Cisco ISE & FMC
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

Reference

Network Segmentation, IAM, ZTNA and Remediation with Cisco

Network	Macro- Segmentation	Micro- Segmentation	Nano- Segmentation	Remediation
Cloud	Multicloud Defense cdFW	Multicloud Defense Secure Workload	Secure Workload	XDR cdFMC CDO
DMZ	Secure Firewall Meraki MX			XDR FMC CDO
Campus	Secure Firewall SD-Access	Identity Services Engine (Adv.) TrustSec Catalyst Center	Secure Network Analytics	XDR FMC ISE
Datacenter/Apps	Secure Firewall ACI	ACI Secure Workload cdFW	Secure Workload	XDR FMC
WAN	Secure Firewall Meraki MX	Catalyst SD-WAN Meraki SD-WAN	Secure Access	XDR FMC CDO
Industrial DMZ	Secure Firewall			XDR FMC
OT	Secure Firewall	Cyber Vision Identity Services Engine (Adv.) TrustSec	Cyber Vision Identity Services Engine Secure Network Analytics	XDR FMC ISE
Endpoint/Client	Secure Firewall Meraki MX	Secure Endpoint Secure Client Secure Email ISE Posture		Secure Endpoint XDR FMC CDO ISE

Secure Critical Infrastructure

OT Components – ICS Vendors & Protocols

Industrial Devices

- Valves
- Pumps
- Sensors
- Thermostats
- Machines
- Robots
- Motors
- Boilers

and more…

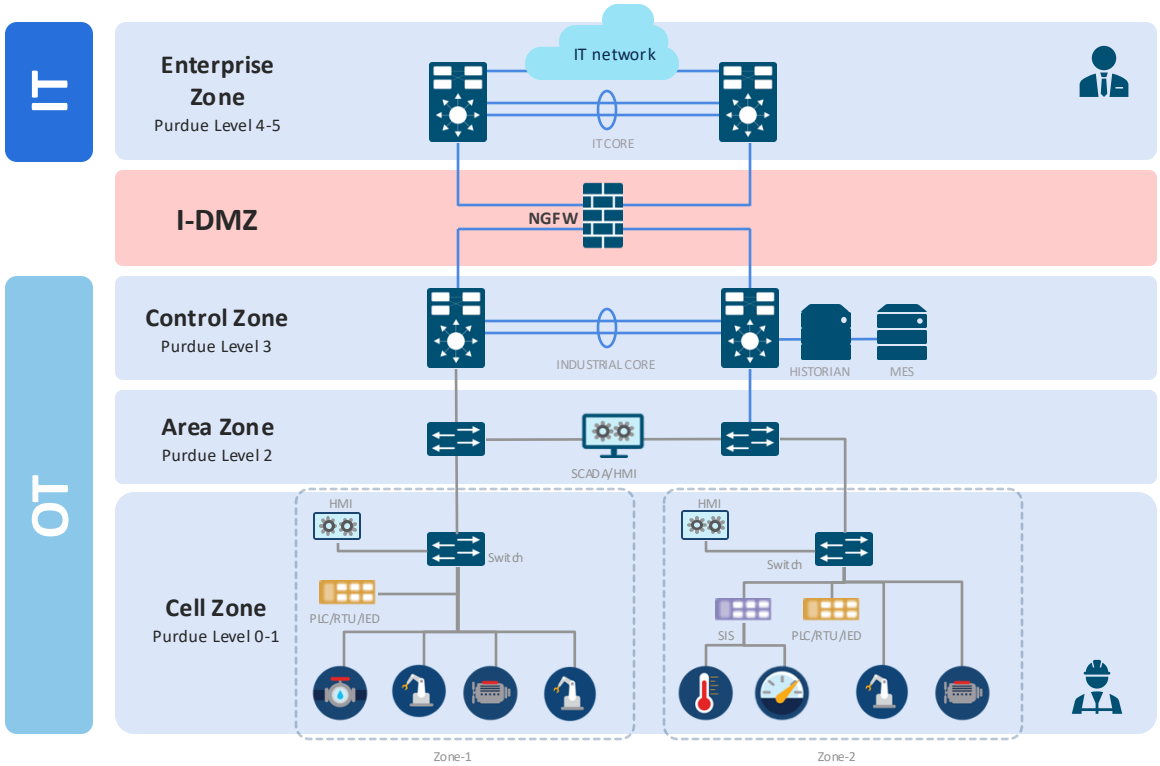
Industrial Control Systems

- Remote Terminal Units (RTU)
- Programmable Logic Controllers (PLC)
- Intelligent Electronic Devices (IED)
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control Systems (DCS)
- Human Machine Interfaces (HMI)

ABB, GE, Schneider Electric, SIEMENS, Rockwell Automation, PHOENIX CONTACT, TOYODA, EMERSON, OMRON, MITSUBISHI ELECTRIC, Honeywell, EATON, BECKHOFF, YOKOGAWA, CODESYS, BACnet, Modbus, OPC, IEC 101, IEC 104, IEC 61850, EtherNet/IP, dnp

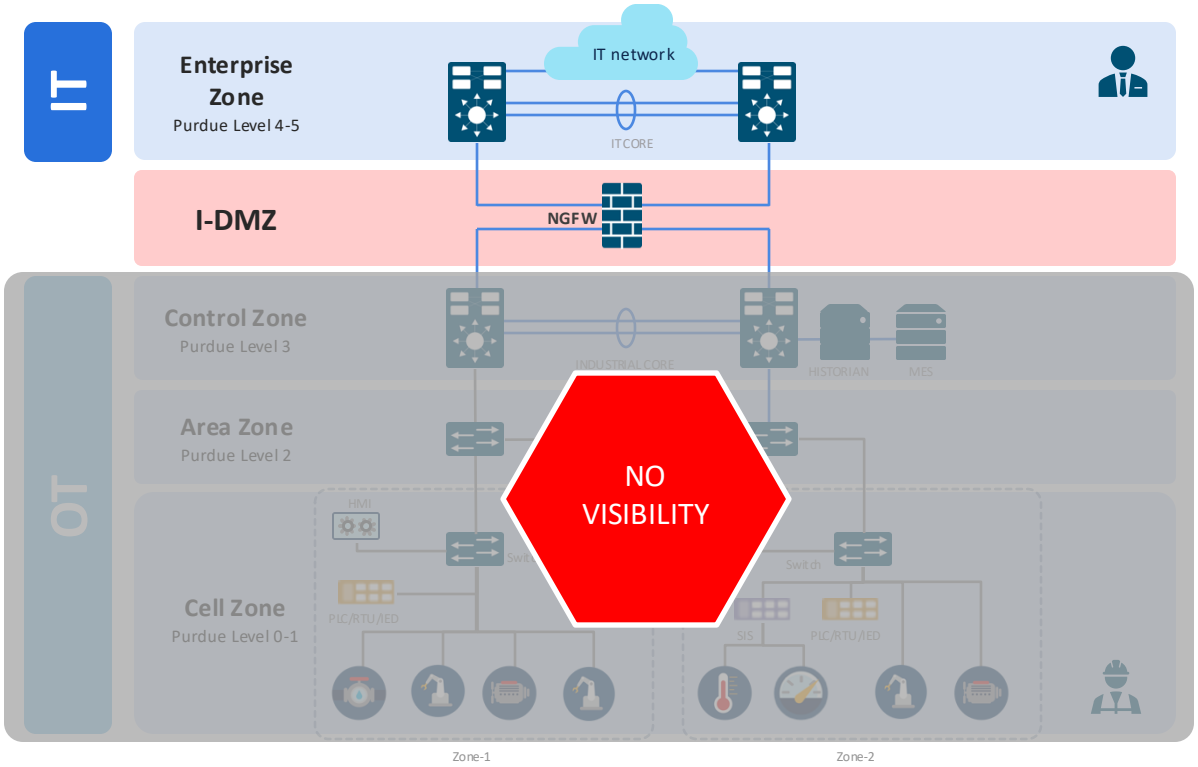
and more…

Typical Industrial Control System (ICS) network



How do we secure this environment that has minimal security with just an I-DMZ?

Typical Industrial Control System (ICS) network

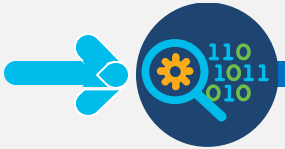


No visibility to OT devices and OT protocols.

No context in change of Assets, new Protocols and change in Communication Flows or lateral movements.

A firewall is not enough!

Cisco’s **4-step journey** to secure your industrial network



Asset discovery

- Discovery of Devices (Assets) with Cyber Vision
- (New) Communication between Devices

Network segmentation

- Segmentation with Firewalls
- SGT with ISE
- Access Control

Live threat detection

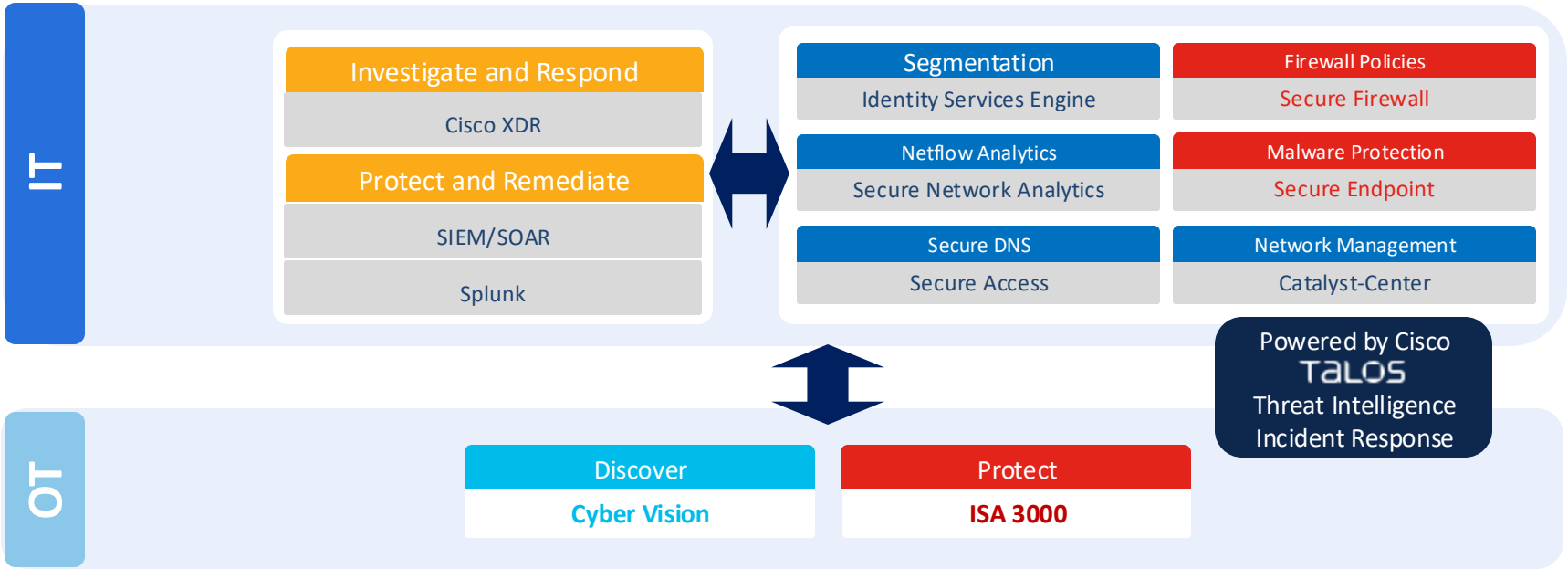
- Difference to Baseline, Change of Assets, new Protocols and change in communication flows
- Vulnerability and Anomaly Detection (IDS)

Integrated IT/OT SOC

- SIEM / SOC / XDR Integration
- Protection & Remediation
- Change of Authorization

Powered by Talos Threat Intelligence

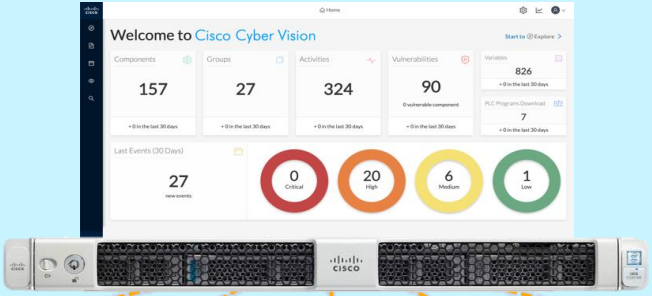
Cisco’s best of integrated IT-OT security solution



Asset Discovery and Network Segmentation with Cyber Vision

Cyber Vision - Architecture

Cisco Cyber Vision Center:
Centralized analytics & data visualization



Cisco integrations

XDR, FMC, ISE,
SNA, DNA-C

Partner integrations

SIEM, CMDB,
ICS vendor software

Application flow

Sensor
Industrial Switching

Sensor
IoT Gateways / Compute

Sensor
Industrial Routing

Sensor
Industrial Wi-Fi

Sensor
Sensor Networking (RF Mesh)

Cyber Vision Sensors: Deep Packet Inspection built into network elements

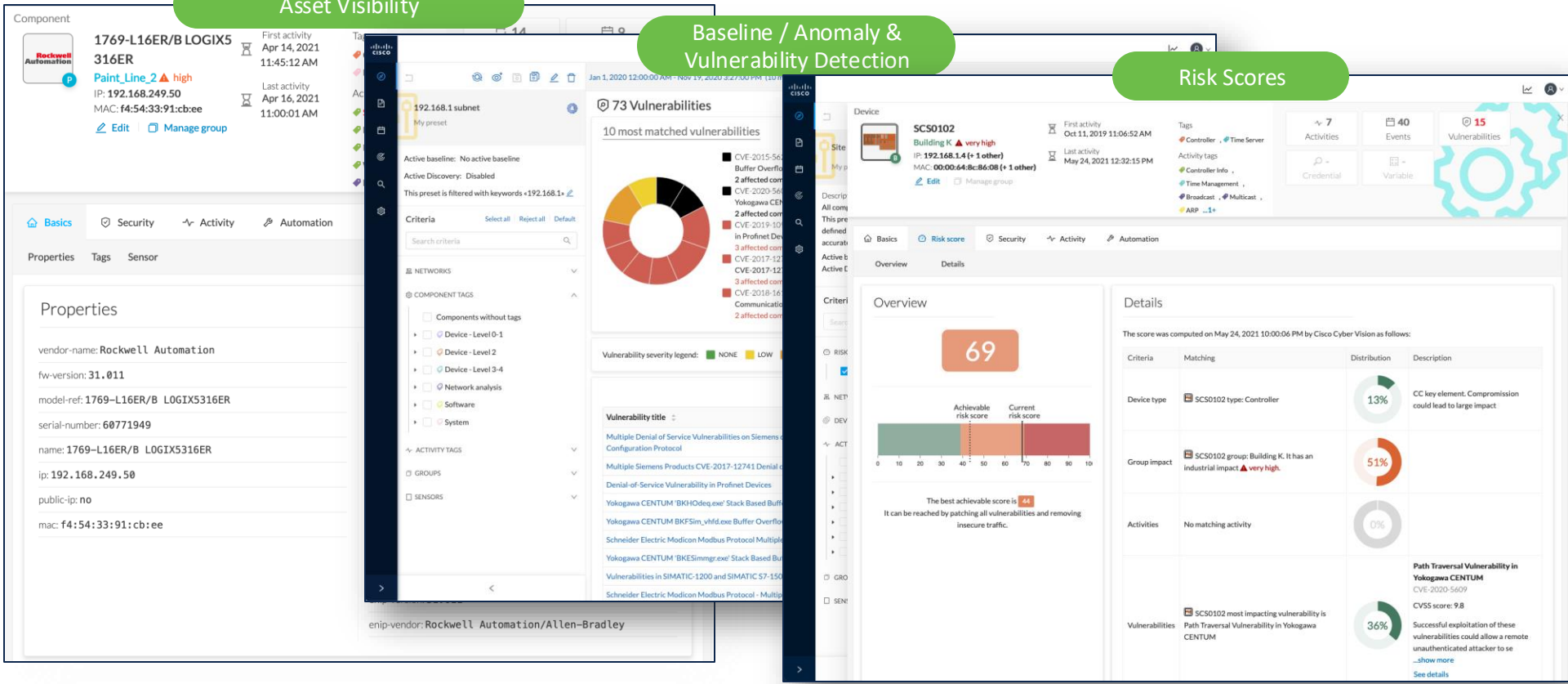
Cyber Vision

Cyber Vision Asset Visibility & Posture

Asset Visibility

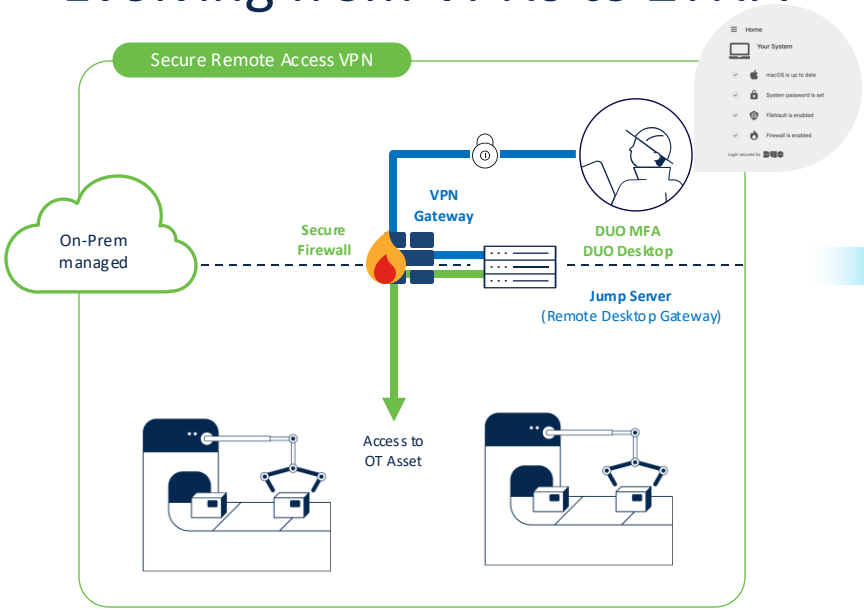
Baseline / Anomaly & Vulnerability Detection

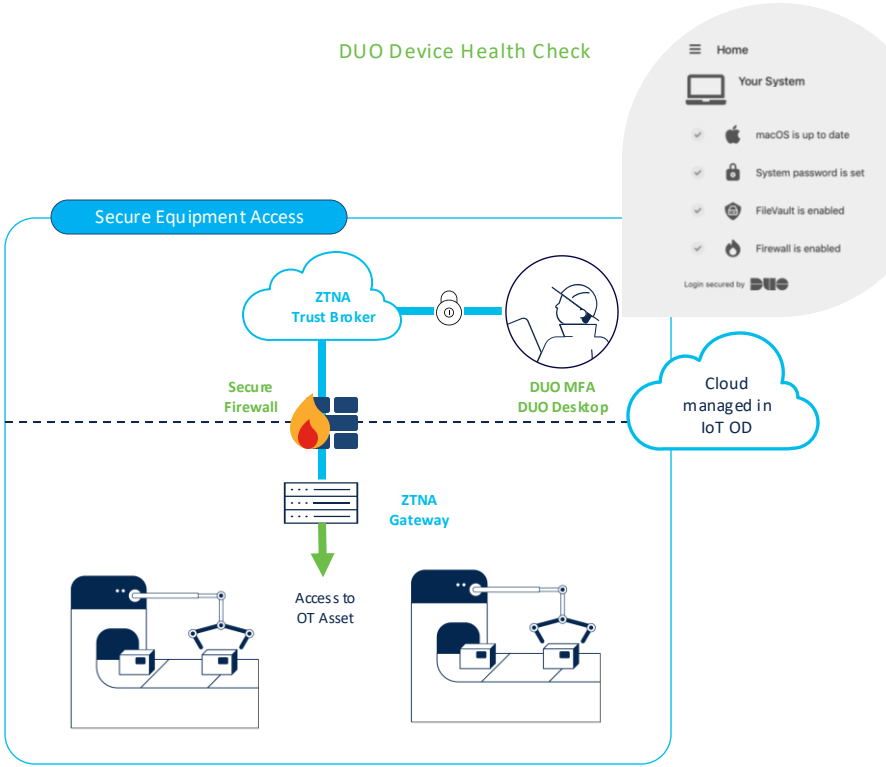
Risk Scores



Secure Remote Access & Multifactor Authentication

Evolving from VPNs to ZTNA



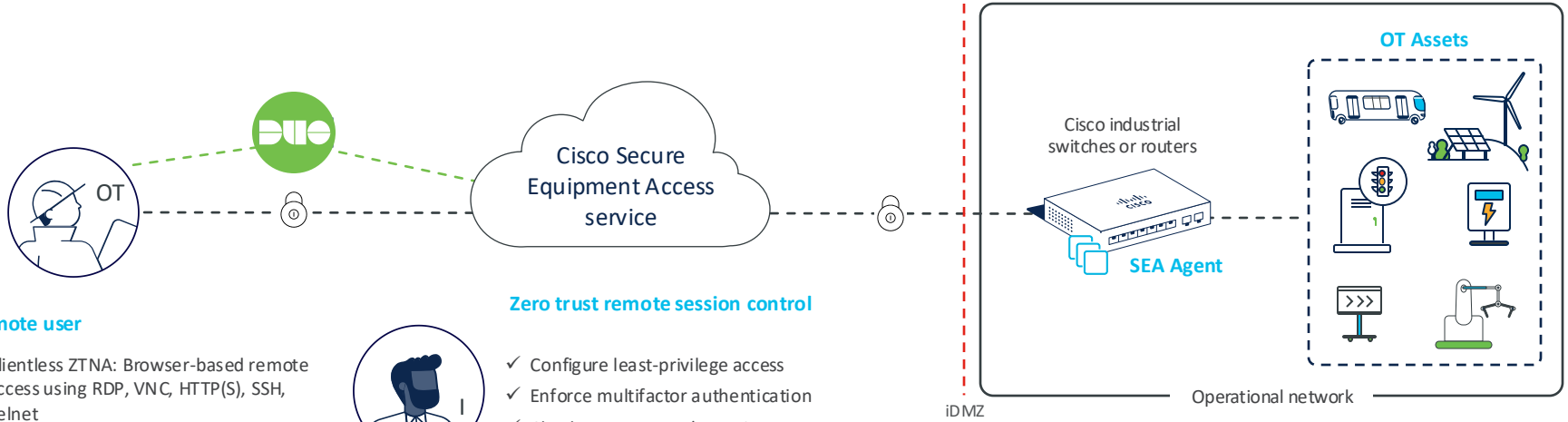


- Always-on solutions with all-or-nothing access
- Firewall rules need to be frequently updated
- Manual session management using jump servers
- DUO MFA and device health check

- Trust broker manages policy based on identity and context, and grants access to specific resources at specific times
- Gateway establishes an outbound connection to the trust broker eliminating complexity of firewall rules
- DUO MFA and device health check

Cisco Secure Equipment Access Architecture

Empower OT teams to easily perform remote operations while enforcing strong zero trust cybersecurity controls



Remote user

- ✓ Clientless ZTNA: Browser-based remote access using RDP, VNC, HTTP(S), SSH, Telnet
- ✓ Agent-based ZTNA: remote access that supports native desktop applications

Zero trust remote session control

- ✓ Configure least-privilege access
- ✓ Enforce multifactor authentication
- ✓ Check remote users' security posture
- ✓ Record, monitor, terminate sessions

Cloud simple
Accelerate time to value

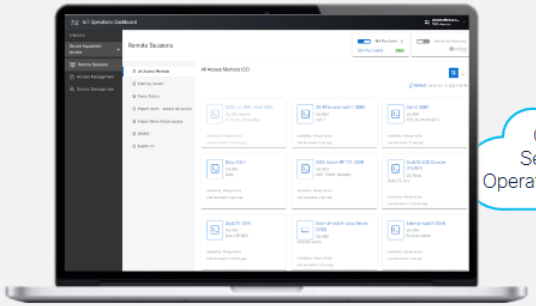
Cisco secure
Built to keep operations safe

Designed for OT
Drive business outcomes

Highly scalable
Cloud + network working together

Cisco Secure Equipment Access **portfolio**

Secure Equipment Access
(ZTNA Trust Broker)



Cisco SEA Service in IoT Operations Dashboard

SEA Agent
(ZTNA gateway)

Catalyst IR1101 Routers

Catalyst IR1800 Routers

Industrial Routers
EDM (IoT OD)-managed IRs

Catalyst IE3300 (4GB) and IE3400 Switches

Catalyst IE3100 Switches

Industrial Switches
Customer-managed IE3x00 (CLI, DNAC)

Network Segmentation with Identity Services Engine

ISE

How Identity Services Engine enforces Zero Trust

Connecting trusted users and endpoints with trusted resources

Endpoint Request Access

- Endpoint is identified and trust is established
- Posture of endpoint verified to meet compliance

Trust continually verified

- Continually monitors and verifies endpoint trust level
- Vulnerability assessments to identify indicators of compromise
- Automatically Updates access policy

Endpoint classified, and profiled into groups

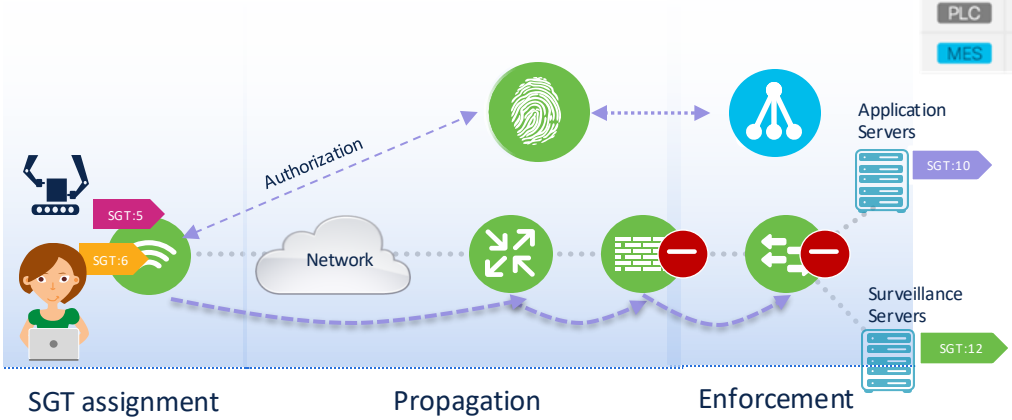
- Endpoints are tagged x/SGTs
- Policy applied to profiled groups based on least privilege

Endpoint authorized access based on least privilege

- Access granted
- Network segmentation achieved

ISE and TrustSec Segmentation

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



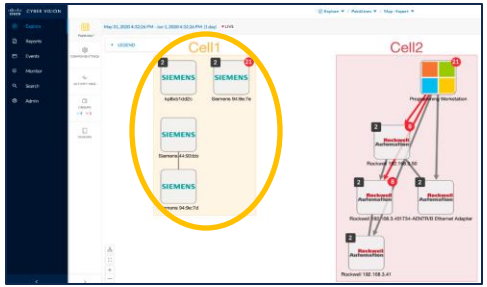
- Assignment of Security Group Tag (SGT) based on context (identity, device group, etc.).
- SGT are carried propagated through the network
- Firewalls, routers and switches use SGT to make filtering decisions via SGACL.

Dynamic Segmentation via Cyber Vision

TrustSec policy Matrix
(Cisco ISE or Catalyst Center)

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

Cyber Vision



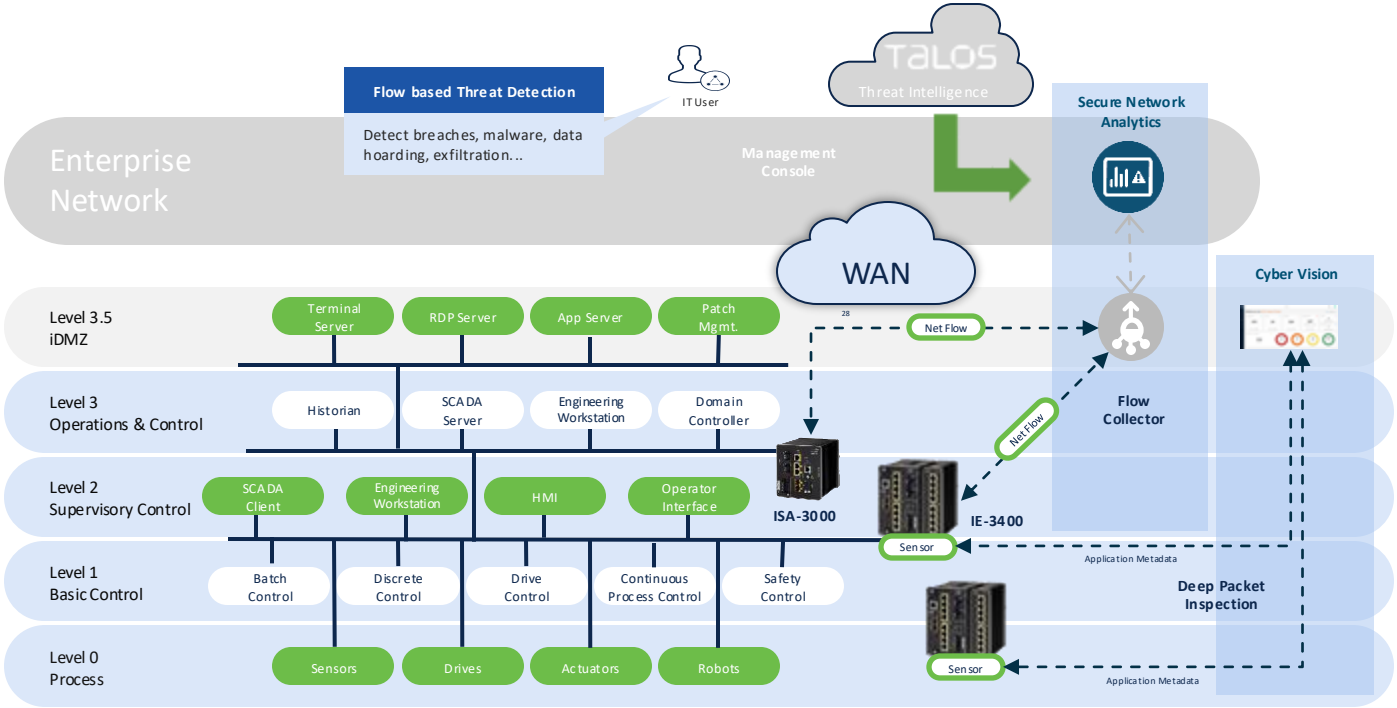
IT and OT teams create a policy matrix with all the needed use cases for segmentation

- The groups in Cyber Vision are mapped to SGTs used in the policies.
- The groups are sent to ISE together with the profiling information.
- The OT team can now assign the right policies directly from Cyber Vision

Netflow Analytics with Secure Network Analytics

Cyber Vision vs. Secure Network Analytics

Secure Network Analytics



Threat Hunting and Remediation with Cisco XDR

Threat Hunting and Remediation with Cisco XDR

XDR

Cisco

Network
Endpoint
Email
Cloud
Applications
Identity

Built on the Cisco security platform

Open and extensible
Clear prioritization
Automation and response guidance
Streamlined investigations

Your Infrastructure

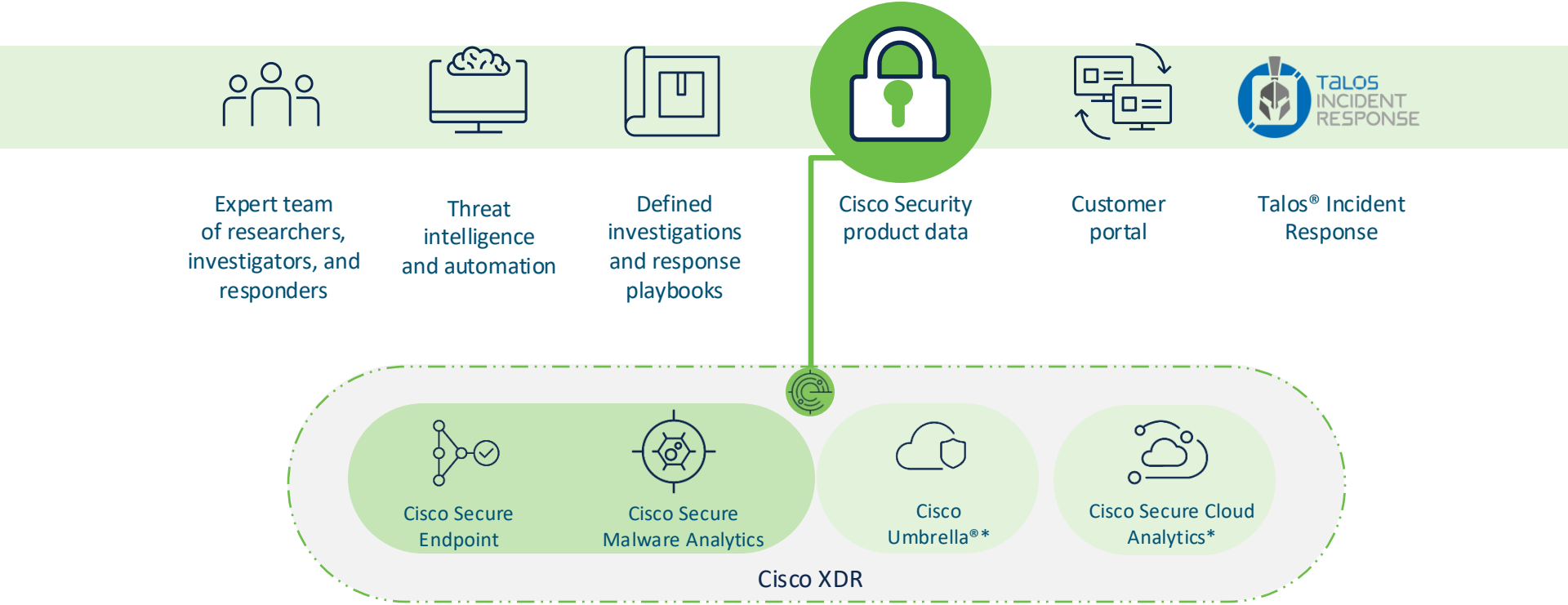
3rd party tools
Intelligence
Others
SIEM/SOAR

Your SOC

SecOps Analyst
CISO
Incident responder

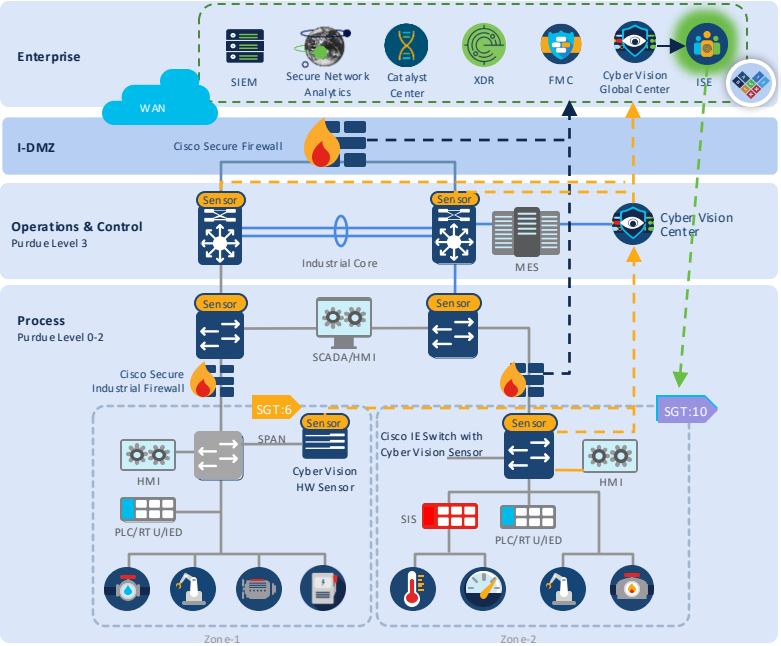
Cisco Managed Detection and Response (MDR)

XDR



*Optional

Let’s put everything together



Cyber Vision discovers industrial assets and communications and groups it into Zones.

ISE implemented for visibility and Cyber Vision context is shared with ISE.

Components are dynamically classified in SGTs via group assignment directly from Cyber Vision

Visualize traffic activity between SGT in Catalyst Center policy analytics

Deploy segmentation with confidence once you are comfortable with the observed network behavior

Cyber Vision, Secure Network Analytics or other analytics tools raise alarms endpoint behavior anomalies and threat detection.

Users can trigger quarantine of offending asset.

CISCO SECURE

Security Reference Architecture

cisco.com/go/sra

v3.0

TALOS THREAT INTELLIGENCE

- Actionable threat intelligence
- Collective responses
- Comprehensive visibility
- Signal identification
- Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Kenna | Secure Cloud Insights | XDR | Talos Incident Response

SERVICES

- Custom threat research on demand
- Implement and manage
- Incident response retainer
- Managed detection & response
- Strategy & assessment

CAPABILITIES

- Cloud security posture management
- Device discovery & insights
- Endpoint detection & response
- Open API platform & 3rd party native integrations
- Risk-based vulnerability management
- Security analytics
- Security orchestration, automation & response
- Threat visibility, incident response & threat hunting

ZERO TRUST

SASE

User/Device Security

SASE/REMOTE WORKER: Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes

- Cloud managed
- VPN
- Posture
- Telemetry/ Visibility
- Endpoint detection & response
- DNS-layer security
- Secure Web
- Anti-virus/ Anti-malware
- Query
- Host FW
- Mobile device management
- Risk-based MFA
- Passwordless
- Device trust
- Continuous trust
- Email, Phishing, SPAM, BEC, DLP, content filtering
- Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Connect | Umbrella

- Browser access control
- Cloud access security broker
- Cloud malware detection
- Data loss prevention
- DNS-layer security
- Identity/ posture
- FWaaS
- RAaaS
- Remote browser isolation
- Secure web gateway
- Tenant restrictions
- TLS decryption
- Zero Trust Network Access

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall
ThousandEyes | Catalyst SDWAN

- Analytics
- Application performance optimization
- Cloud based orchestration
- Cloud On Ramp
- Digital experience monitoring
- IPSec VPN
- Integrated security
- Middle mile optimization
- Segmentation
- Visibility
- Group tag propagation

In the Office/Managed Location

Catalyst | Catalyst Center | ISE | Meraki | Secure Firewall
Secure Network Analytics | Web Appliance

- Application network gateway
- Configuration orchestration
- Content filtering
- Encrypted visibility
- Group tag classification
- Identity/ pxGrid Cloud
- Network access control
- Network security analytics
- NGFW
- NGIPS
- Security analytics & logging
- Segmentation
- Threat mitigation
- Profiling

Industrial Threat Defense

Catalyst Center | CyberVision | Industrial Networking
ISE | Secure Firewall | Secure Network Analytics

- Anomaly detection
- Compliance
- Group tag classification
- Identity/ pxGrid
- Ruggedized
- Segmentation
- Threat mitigation
- Visibility

Workload, Application, and Data Security

HYBRID MULTI-CLOUD: ACI | Cloud Insights | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Secure Cloud Analytics | Secure Workload

- Anti-virus/ Anti-malware
- API security
- App discovery
- Cloud analytics
- Cloud Native Security
- Cloud Posture Management
- DDoS, WAF/Bot
- Identity/ pxGrid
- Micro/Macro Segmentation
- Run-time application
- Telemetry
- Threat mitigation
- Visibility

CISCO
SECURE

Secure your resilience.