Cisco Cyber Vision OT Security Transformation

Industrial OT Visibility, Threat Detection, Asset Discovery, Risk Scoring and SOC Integration for Critical Infrastructure

EXECUTIVE CONTEXT

Cisco Cyber Vision provides real-time OT asset visibility, industrial protocol inspection, threat detection and risk management for critical infrastructure environments. COMnet positions the solution as a non-disruptive OT cybersecurity program for ICS, SCADA, PLC and industrial control networks, helping leadership reduce operational risk while enabling security teams to connect OT telemetry with enterprise SOC workflows.

OT
Asset visibility

DPI
Industrial protocols

SOC
Integration

IMPACT

- Created complete OT asset visibility across ICS, SCADA, PLC, HMI and industrial communication environments without deploying agents on production assets.
- Improved early detection of abnormal industrial behavior, lateral movement and ransomware indicators through passive traffic analysis and behavioral monitoring.
- Reduced operational and regulatory risk by enabling risk scoring, vulnerability visibility, segmentation recommendations and audit-ready evidence.
- Strengthened IT-OT collaboration by integrating OT security telemetry with existing SIEM, SOC and incident response processes.
- Supported secure critical infrastructure operations without impacting production performance, availability or deterministic industrial communication flows.

MAJOR ISSUES

- Limited visibility of OT assets and network communications made it difficult to maintain an accurate industrial asset inventory and communication baseline.
- Legacy industrial systems lacked built-in security controls, increasing exposure to vulnerabilities and compensating-control requirements.
- Ransomware, targeted attacks and lateral movement threats increased risk to critical infrastructure uptime, safety and operational continuity.
- Flat OT network architectures and weak segmentation expanded blast radius and complicated policy enforcement across industrial zones.
- Compliance obligations such as IEC 62443, NIST and NCIIPC required better evidence, governance and repeatable risk-management workflows.
- IT SOC teams lacked context-rich OT telemetry, limiting cross-domain detection, escalation and incident response alignment.

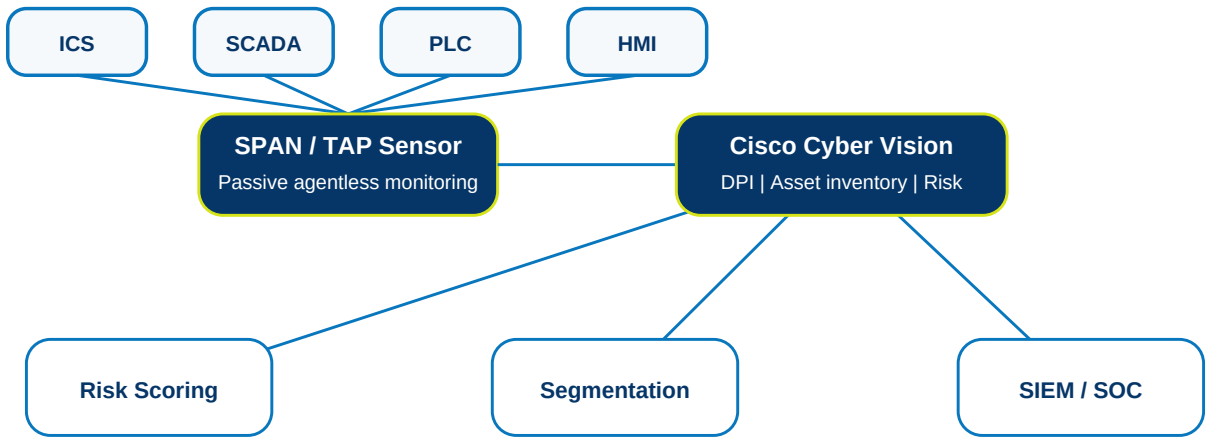
Cisco Cyber Vision OT Security Transformation

Industrial OT Visibility, Threat Detection, Asset Discovery, Risk Scoring and SOC Integration for Critical Infrastructure

HIGHLIGHTS

ARCHITECTURE AND DEPLOYMENT SCOPE

REFERENCE ARCHITECTURE - CISCO CYBER VISION FOR OT



Zero-disruption OT monitoring | Modbus, DNP3, IEC 104 | SOC integration | Multi-site scalability

- Passive, agentless OT monitoring through SPAN/TAP deployment to avoid disruption to production environments.
- Deep Packet Inspection of industrial protocols including Modbus, DNP3 and IEC 104 to identify assets, flows and anomalous behavior.
- Automated asset discovery and classification for ICS, SCADA, PLCs, HMIs and connected industrial devices.
- Vulnerability and risk scoring to prioritize remediation based on exposure, criticality and operational dependency.
- Segmentation recommendations and enforcement integration to reduce lateral movement and strengthen OT zoning.
- Integration with existing SIEM/SOC platforms to provide unified monitoring across IT and OT domains.

- OT Asset Layer: Industrial assets such as PLCs, HMIs, SCADA servers, engineering workstations and ICS devices remain untouched and continue operating normally.
- Passive Collection Layer: SPAN/TAP connectivity mirrors OT network traffic to Cyber Vision sensors without inline dependency or production-path impact.
- Protocol Inspection Layer: DPI analyzes industrial protocols, device conversations, commands, anomalies and communication patterns to build an OT baseline.
- Cyber Vision Center: Central platform provides asset inventory, risk scoring, communication mapping, anomaly detection, vulnerability context and reporting.
- Segmentation and Enforcement Layer: Findings support zone/conduit design, firewall policy recommendations and reduced lateral movement risk.
- SOC Integration Layer: Events and enriched telemetry can be forwarded to SIEM/SOC platforms for consolidated IT-OT detection, triage and governance.

Cisco Cyber Vision OT Security Transformation

Industrial OT Visibility, Threat Detection, Asset Discovery, Risk Scoring and SOC Integration for Critical Infrastructure

KEY STRATEGIES

- Visibility-First OT Security: Establish an accurate asset inventory and network communication map before enforcing policy changes in sensitive industrial environments.
- Zero-Disruption Deployment: Use passive SPAN/TAP-based monitoring so production systems are not interrupted and industrial performance remains stable.
- Risk-Based Prioritization: Combine vulnerability context, asset criticality and communication exposure to prioritize remediation and compensating controls.
- Segmentation Roadmap: Use observed traffic flows to define OT zones, conduits, policy boundaries and enforcement plans aligned to industrial standards.
- IT-OT SOC Convergence: Feed OT context into existing SIEM/SOC workflows to improve incident response, escalation and leadership-level risk reporting.
- Compliance Alignment: Map visibility, risk scoring, and segmentation recommendations to IEC 62443, NIST, NCIIPC and internal audit requirements.
- Scalable Multi-Site Model: Design the architecture for repeatable rollout across plants, utilities and distributed industrial environments.

EXECUTIVE TAKEAWAY

Cisco Cyber Vision enables critical infrastructure organizations to move from limited OT visibility to measurable industrial cyber resilience. By combining passive monitoring, protocol-aware detection, risk scoring, segmentation guidance and SOC integration, COMnet can help decision makers reduce operational risk, improve compliance readiness and build a scalable OT cybersecurity foundation.

EXPECTED OUTCOMES

- Comprehensive OT asset inventory and communication-flow mapping across industrial networks.
- Risk and vulnerability assessment report with prioritized remediation and segmentation recommendations.
- Enhanced SOC visibility across IT and OT domains with stronger early-warning capability for critical infrastructure threats.

TRANSFORMATION SUMMARY

Cisco Cyber Vision | OT asset inventory | DPI | anomaly detection | risk scoring | segmentation | SOC integration