seceon
SECURITY FOR EONS

Seceon aiSecOT360

AI-Powered OT, ICS & IoT Security for Critical Infrastructure.

A purpose-built OT security platform for passive asset discovery, deep protocol inspection, AI/ML threat detection, OT intelligence, and automated response across PLCs, RTUs, HMIs, SCADA, and IIoT, without disrupting operations.

aiSecOT360™ Platform for Critical Infrastructure

Seceon aiSecOT360 secures industrial control systems and physical processes that traditional IT tools cannot reach. Aligned to the Purdue Model, it monitors Levels 0–5 from sensors and actuators to enterprise IT through a single pane of glass.

Deep packet inspection covers 60+ industrial protocols, including Modbus, DNP3, BACnet, OPC UA, IEC 61850, Profinet, EtherNet/IP, and more. Patented AI/ML models baseline every PLC, RTU, HMI, and SCADA server to identify zero-day threats, ICS malware (Stuxnet, Triton, PIPEDREAM/INCONTROLLER), unauthorized programming, and IT-to-OT lateral movement.

Deployment is non-intrusive: Seceon CCE sensors monitor via SPAN/TAP at the cell area zone with one-way data flow to the APE, preserving process safety and availability while SOC and OT teams gain unified visibility, MITRE ATT&CK for ICS mapping, and 10 dedicated OT alert categories.

Highlights

PASSIVE OT VISIBILITY & ASSET DISCOVERY

Non-intrusive discovery of PLCs, RTUs, HMIs, SCADA, and IIoT devices with deep inspection across 70+ protocols for real-time asset visibility, including role, Purdue level, and criticality.

AI-POWERED THREAT DETECTION

Patented AI/ML detects zero-days, ICS malware, unauthorized PLC programming, and lateral movement with OT threat intelligence and vulnerability context.

SAFE FOR PRODUCTION

One-way SPAN/TAP-based passive monitoring at the cell area zone. Zero impact on PLCs, RTUs, or process safety. Purdue Model-aligned architecture.

CONTINUOUS COMPLIANCE

Built-in mapping to IEC 62443, NIST 800-82, NERC CIP, NIS 2, NCIIPC, and CMMC 2.0 with automated audit reporting and continuous posture monitoring.

Platform Overview

- Passive asset discovery and profiling of PLCs, RTUs, HMIs, SCADA servers, historians, engineering workstations, and IIoT devices without active scans or agents. Asset records include available device pedigree and operational context.
- Industrial protocol deep packet inspection across 70+ OT protocols, including Modbus, DNP3, BACnet, OPC UA, IEC 61850, IEC 60870-5-104, Profinet, EtherNet/IP, S7 Communication, HSR/PRP, DLMS/COSEM, and other industrial protocols.
- Dynamic threat modeling with patented AI/ML that learns and adapts to each environment, eliminating manual rule tuning while baselining normal behavior for every device, protocol, and conversation pair.
- Zero-day and ICS malware detection using behavioral analytics surfacing Stuxnet-class, Triton, Industroyer, PIPEDREAM/INCONTROLLER, and unknown threats targeting safety instrumented systems.
- Multi-source IT/OT correlation automatically links events across enterprise IT, OT, identity, cloud, and threat intelligence, enriching asset risk with vulnerability context and MITRE ATT&CK for ICS mapping.
- Ten-category alerting framework covering unauthorized access, protocol anomalies, lateral movement, malicious activity, policy violations, time-based and communication anomalies, threat intel, configuration, and system health.
- OT-aware response and remediation via integrated AI SOAR, playbook-driven recommendations, IT/OT segmentation, traffic allow-listing, account quarantine, and configured enforcement actions while preserving OT availability.
- Continuous compliance and reporting with built-in audit packs for IEC 62443, NIST 800-82, NERC CIP, NIS 2, NCIIPC, and CMMC 2.0 generated automatically from live telemetry.
- ~92 OT/ICS playbooks provide detection-specific recommendations and controlled response actions for protocol abuse, unauthorized control activity, PLC manipulation, lateral movement, ransomware preparation, and vulnerability exposure.

"With Seceon aiSecOT360 we finally have one view of IT and OT. We see every PLC and SCADA conversation, catch unauthorized configuration changes the moment they happen, and respond all without ever putting a packet on the control network."
— Seceon Industrial Sector Customer

Protect critical infrastructure with passive OT monitoring

Continuous deep packet inspection of every OT protocol, Modbus, DNP3, IEC 61850, OPC UA, and more, with zero footprint on PLCs, RTUs, or process safety. AI/ML baselining surfaces only what matters.

Detect ICS malware and operator-impact threats

Behavioral analytics catch Stuxnet-class, Triton, Industroyer, PIPEDREAM, unauthorized PLC uploads, IEC 61850 protection-relay changes, and DNP3 control operations from unknown sources.

Unify IT and OT operations on one platform

Seceon OTM correlates OT alerts with identity, endpoint, network, and cloud telemetry — eliminating tool sprawl and giving SOC and OT teams a shared view of risk across all Purdue levels.

Seceon aiSecOT360 continuously monitors OT, ICS, and IIoT environments to detect anomalous behavior, validate security posture, and prioritize operational risks using patented AI/ML-driven analytics.

Why Choose Seceon aiSecOT360?

- Unified IT and OT visibility on a single platform, replacing 6+ disparate OT and IT security tools, with correlated asset, threat, and risk context across Purdue Levels 0–5.
- Real-time AI/ML detection and OT-aware response with sub-90-second automated containment for incidents that meet defined response criteria.
- Comprehensive industrial protocol coverage: 70+ OT protocols supported out of the box, with custom parsers available on a 96-hour SLA for proprietary protocols.
- Purdue Model-aligned deployment: Seceon CCE sensors operate between Level 1 and Level 2 with one-way data flow to APE, fully compatible with air-gapped environments.
- MITRE ATT&CK for ICS coverage with multi-source correlation, threat intelligence, contextual risk scoring, and 10 dedicated OT alert categories.
- Continuous compliance for IEC 62443, NIST 800-82, NERC CIP, NIS 2, NCIIPC, and CMMC 2.0 with automated audit reporting.
- Flexible deployment on-premises, private cloud, hybrid, or fully air-gapped to match the operational and regulatory needs of utilities, manufacturing, oil and gas, transportation, water, and government sectors.
- Native integration with the full Seceon OTM platform: aiSIEM, aiXDR, aiSOAR, NDR, UEBA, aiITDR, TI360, and CMX360 for unified detection, response, threat intelligence, and compliance.

OT • ICS • IoT • IIoT Unified Industrial Cybersecurity

ACCURACY, CONTEXT, SPEED

Real-time processing of large telemetry volumes combines industrial protocol behavioral baselining, threat intelligence, asset context, and AI/ML analytics to produce validated, prioritized OT alerts.

FLEXIBLE DEPLOYMENT FOR INDUSTRIAL ORGANIZATIONS

On-premises, private cloud, hybrid, or fully air-gapped deployment options span multiple plants, substations, and branch sites. Multi-tenancy and segregation are built in for asset owners, system integrators, and MSSPs delivering managed OT security.

About Seceon

Seceon simplifies cybersecurity for MSPs, MSSPs, and IT teams by reducing risk and complexity. Our AI and ML-powered aiSIEM and aiXDR platform provides comprehensive threat detection and response. By integrating data from logs, identity management, networks, endpoints, clouds, and applications, we deliver real-time, accurate alerts and automated remediation. Trusted by over 850 partners, Seceon supports more than 9,800 clients with efficient, high-margin security services and continuous compliance.

Learn more about Seceon

Schedule a Demo www.seceon.com/contact-us/