

2026

seceon

Seceon aiSecOT360:

Securing the Future of OT, IoT, ICS & CPS Environments

By Chandra Shekhar Pandey, Founder & CEO, Seceon Inc.

Executive Summary

The convergence of Information Technology (IT) and Operational Technology (OT) has fundamentally transformed the industrial landscape, creating unprecedented opportunities for efficiency and innovation. However, this digital transformation has also exposed critical infrastructure to sophisticated cyber threats that can disrupt operations, compromise safety systems, and cause significant economic damage.

Seceon aiSecOT360 represents a breakthrough in OT/ICS security, delivering AI-driven, real-time threat monitoring and comprehensive asset discovery specifically designed for industrial environments. As an integral component of the broader aiXDR360 platform, aiSecOT360 provides unified visibility and protection across IT, OT, IoT, and IoMT ecosystems while maintaining the operational continuity essential to industrial processes.

This white paper examines the critical security challenges facing modern industrial environments and demonstrates how Seceon aiSecOT360 addresses these challenges through advanced AI-powered capabilities, comprehensive protocol support, and seamless integration with existing security infrastructure.

The Critical State of OT/ICS Security

Current Threat Landscape

Industrial organizations face an evolving and increasingly sophisticated threat landscape that specifically targets operational technology environments. Recent high-profile attacks demonstrate the real-world impact of OT security failures:

CHERNOVITE (2023): The Industroyer2 malware specifically targeted Ukraine's electrical grid, highlighting the devastating potential of custom ICS malware designed to disrupt critical infrastructure operations. WannaCry Variant in Medical IoMT (2024): Ransomware attacks successfully compromised diagnostic devices across hospital networks in Asia, demonstrating the vulnerability of medical IoT environments and their potential to disrupt life-critical services.

TRITON Reemergence (2023): Renewed attempts to disable industrial safety controllers in Middle Eastern facilities underscore the persistent threat to safety instrumented systems (SIS) that protect both personnel and equipment.

Mirai IoT Botnet Resurgence (2024): The compromise of thousands of smart building HVAC systems and IP cameras illustrates how IoT devices serve as entry points for broader network infiltration.

Volt Typhoon (2024): Chinese threat actors have been pre-positioning within U.S. critical infrastructure networks, particularly targeting OT environments, demonstrating the strategic value of industrial systems to nation-state actors.

Fundamental OT Security Challenges

Industrial environments present unique security challenges that distinguish them from traditional IT networks:

The OT Security Challenge Matrix

CHALLENGE	IMPACT LEVEL	SOLUTION GAP
Legacy Systems	95%	No built-in security
Flat Networks	87%	Minimal segmentation
Visibility Gaps	83%	Poor asset inventory
Patching Issues	78%	Can't update without production downtime
Availability Requirements	99%	Security can't disrupt operations

78% of OT environments have known vulnerabilities that cannot be patched due to operational constraints

Legacy Infrastructure: OT networks are predominantly legacy-heavy systems that were designed for reliability and performance rather than security. These systems often lack basic security features such as encryption, authentication, and access controls.

Flat Network Architecture: Many industrial networks employ flat architectures with minimal segmentation, creating significant lateral movement risks once an attacker gains initial access.

Visibility Gaps: Organizations typically have poor asset inventory and limited real-time monitoring capabilities across their OT environments, making it difficult to detect unauthorized changes or malicious activities.

Patching Challenges: Critical industrial systems often cannot be patched or updated without significant operational disruption, leaving known vulnerabilities exposed for extended periods.

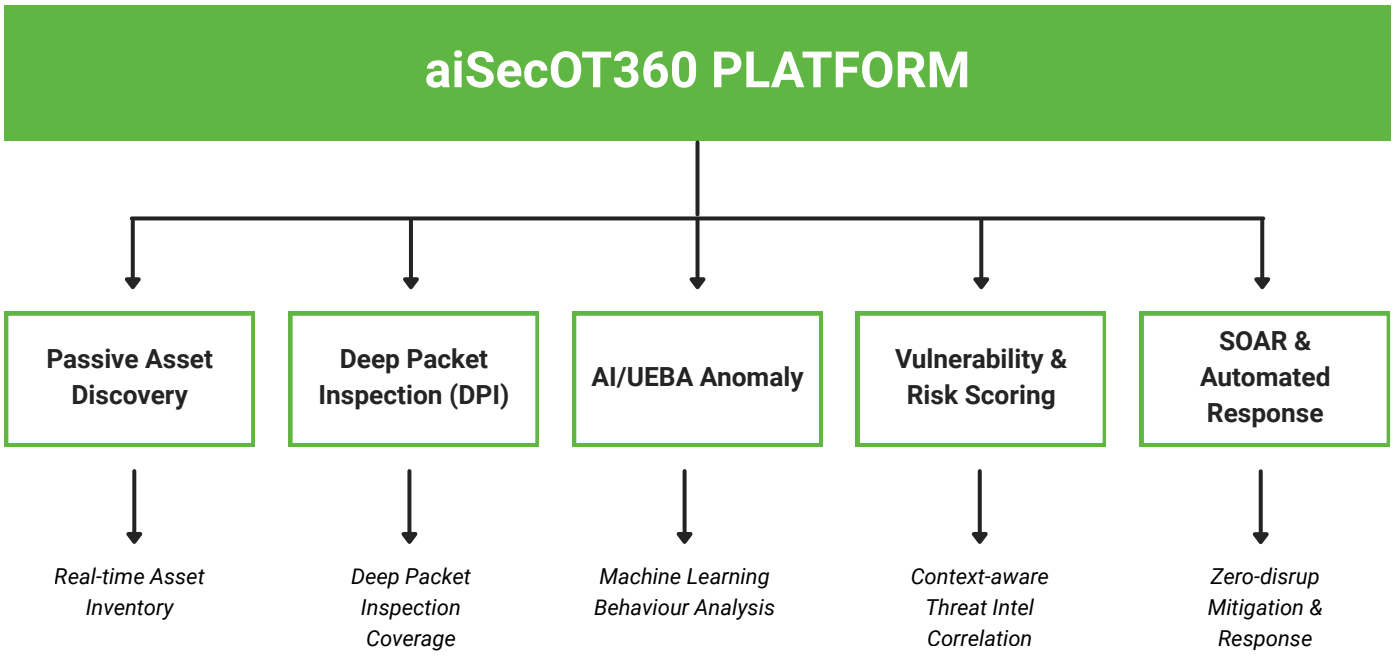
Operational Continuity Requirements: Security solutions must operate without interfering with production processes, as even minor disruptions can result in significant financial losses and safety risks

Seceon aiSecOT360: A Comprehensive Solution

Platform Overview

Seceon aiSecOT360 represents a paradigm shift in OT security, delivering AI-driven, real-time threat monitoring and deep asset discovery capabilities specifically engineered for industrial environments. The platform integrates seamlessly with the broader aiXDR360 ecosystem, providing unified visibility and protection across IT, OT, IoT, and IoMT environments.

Core Capabilities



Proven Results:

- *10,000+ assets automatically discovered*
- *95% reduction in false positives*
- *Real-time threat detection across OT/ICS networks*
- *70+ protocol support for full packet-level visibility*

1. Passive Asset Discovery

aiSecOT360 provides comprehensive visibility into ICS/SCADA devices through passive monitoring techniques that do not disrupt operational processes. The platform automatically discovers and catalogs all connected devices, providing real-time asset inventory management that addresses one of the most fundamental challenges in OT security.

Recent deployments have demonstrated the platform's effectiveness, with over 10,000 OT/ICS assets discovered in a single implementation, providing organizations with unprecedented visibility into their industrial infrastructure.

2. Deep OT Protocol Inspection

The platform supports deep packet inspection (DPI) across more than 70 industrial and ICS/OT protocols, including:

- **Distributed Network Protocol (DNP3):** Commonly used in utility and power generation environments
- **Modbus**: Widely deployed serial communication protocol for industrial automation
- **BACnet**: Building automation and control network protocol
- **IEC 61850**: International standard for power utility automation
- **OPC UA:** Industrial communication protocol for interoperability
- **Ethernet/IP**: Industrial Ethernet protocol
- **Siemens S7**: Proprietary protocol for Siemens PLCs
- **Rockwell RNA**: Rockwell Automation network architecture protocols

This comprehensive protocol coverage ensures that aiSecOT360 can monitor and analyze communications across diverse industrial environments spanning energy, manufacturing, pharmaceuticals, and utilities sectors.

3. AI-Powered Anomaly Detection

The platform employs User and Entity Behavior Analytics (UEBA) specifically calibrated for machine and network behavior in industrial environments. Unlike traditional signature-based detection methods, aiSecOT360's AI engine learns normal operational patterns and identifies deviations that may indicate security incidents.

This approach has proven highly effective, achieving a 95% reduction in false positives compared to traditional OT security tools, enabling security teams to focus on genuine threats rather than managing alert fatigue.

4. OT Threat Intelligence & Vulnerability Risk Scoring

aiSecOT360 enriches OT assets and events with real-time, context-aware threat and vulnerability intelligence. Asset identity, firmware, vulnerability severity, asset criticality, and current threat intelligence are correlated to identify exposed assets, assess risk, and prioritize remediation based on operational criticality.

5. Policy Enforcement and Compliance

The platform delivers continuous posture scoring through AI-driven rules engine that monitors compliance with security policies and regulatory requirements. This capability supports organizations in meeting various compliance frameworks, including NIST CSF, IEC 62443, and NERC CIP requirements.

6. OT-Aware Playbooks & Security Orchestration

aiSecOT360 uses OT/ICS-specific playbooks to translate detection signals into contextual recommendations and controlled response actions. The playbook framework includes approximately 92 OT/ICS scenarios covering protocol abuse, unauthorized control activity, PLC manipulation, lateral movement, ransomware preparation, vulnerability exposure and other industrial security conditions. Recommended actions may include engineering-workstation quarantine, network segmentation, ACL enforcement, malicious-source blocking, investigation and evidence preservation, remote-access revocation and endpoint/EDR remediation where integrated.

Advanced Threat Detection Capabilities

Comprehensive Threat Coverage

aiSecOT360 addresses a wide range of threats specific to industrial environments:

aiSecOT360 THREAT DETECTION MATRIX

THREAT TYPE	DETECTION METHOD	RESPONSE TIME
Unauthorized PLC Cmd	DPI + Protocol Anomaly	< 30 seconds
HMI/SCADA Changes	UEBA + Flow Analytics	< 1 minute
Rogue Device	Passive Discovery	Real-time
Lateral Movement	AI Traffic Analysis	< 2 minutes
Vulnerability Exploit	TI Correlation + CVE	< 1 minute
Ransomware	Behavioral Detection	< 30 seconds
IoMT Hijacking	Device Identity UEBA	Real-time
Supply Chain Attack	Deep Inspection + TI	< 5 minutes
Malware Infection	IOC Matching + Behavior	< 1 minute
Zero-Day Exploit	AI/ML Heuristics	< 3 minutes
Policy Violation	Continuous Monitoring	Real-time

SUCCESS METRICS

- 95% False Positive Reduction
- 99.9% Threat Detection Accuracy
- <30 Second Average Response Time
- Zero Production Disruption
- ~92 OT/ICS Playbooks

Threat Type	Detection Method
Unauthorized PLC Command	DPI + Protocol Behavior Anomaly Analysis
HMI/SCADA Traffic Changes	UEBA + Flow Analytics
New Device Introduction	Passive Discovery + Real-time Alerting
Lateral Movement	AI–Driven Traffic Baseline Analysis
Known Vulnerability Exploitation	Threat Intelligence Correlation + CVE Matching
Ransomware in IoT	Behavioral Deviation Detection
Devices	Isolation Policies
IoMT Sensor Hijacking	UEBA + Device Identity Monitoring
Supply Chain Tampering	Deep Inspection + External Threat Intelligence
Malware-Infected Hosts	Threat Behavior Correlation + IOC Matching
Zero-Day Exploits	AI/ML–based Detection + Heuristic Analysis
Policy Violations	Continuous Rule Compliance Monitoring

Real-World Attack Response

The platform has demonstrated its effectiveness against sophisticated real-world threats:

VOLT TYPHOON

- **Detect:** UEBA identifies abnormal user and device behavior; AI/ML detects protocol misuse
- **Contextualize:** OT asset identity + behavioral anomalies + credential activity
- **Recommend:** Investigate compromised credentials and restrict suspicious lateral movement
- **Respond:** Block lateral movement using configured SOAR controls

TRITON

- **Detect:** DPI identifies suspicious SIS protocol activity
- **Contextualize:** OT asset identity + protocol behavior + threat intelligence
- **Recommend:** Restrict unauthorized sources and investigate affected engineering systems
- **Respond:** Apply configured policy/enforcement controls

R4IoT

- **Detect:** Passive discovery identifies rogue IoT devices; behavioral AI detects malware indicators
- **Contextualize:** Asset identity + device behavior + threat intelligence
- **Recommend:** Isolate suspicious IoT devices and investigate potential OT pivot points
- **Respond:** Trigger configured quarantine policies

INDUSTROYER2 / CHERNOVITE

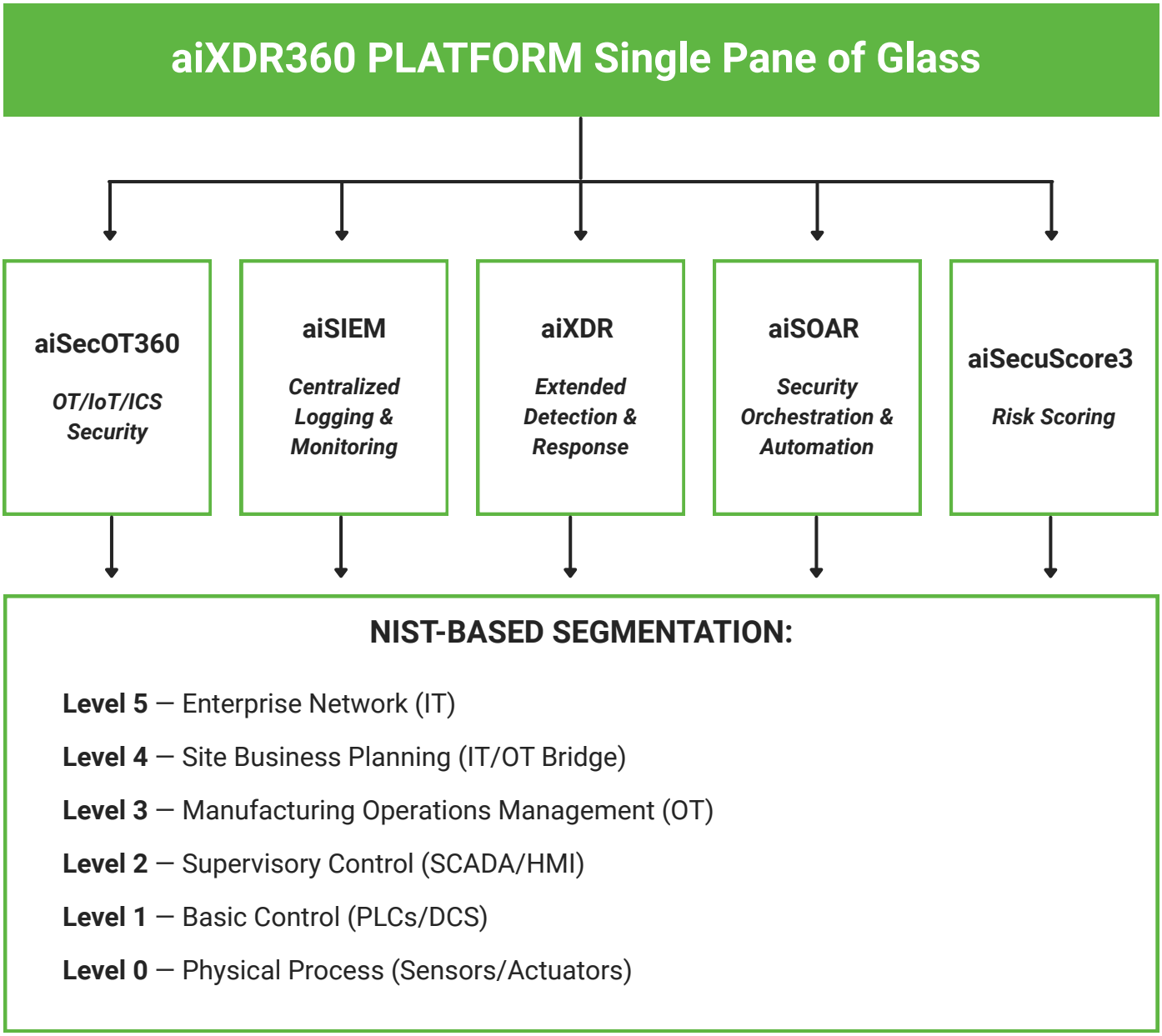
- **Detect:** DPI identifies suspicious IEC 61850 and DNP3 activity
- **Contextualize:** OT asset identity + protocol behavior + threat intelligence
- **Recommend:** Investigate indicators of compromise and restrict affected systems
- **Respond:** Deploy automated mitigation through integrated SOAR capabilities

Integration with aiXDR360 Platform

Integration with aiXDR360 Platform

Unified Security Architecture

aiSecOT360 operates as an integral component of Seceon's comprehensive aiXDR360 platform, providing single-pane-of-glass visibility across IT, OT, and cloud environments. This integration delivers several critical advantages:



Integration Benefits:

- *Multi-tenant MSSP Support*

- *Cross-domain Correlation*
- *Unified IT/OT Risk Views*
- *Centralized Incident Response*

Centralized Management: The platform integrates with Seceon aiSIEM, aiXDR, and aiSOAR to provide unified alert management and incident response coordination across all environments.

Native Risk Assessment: Integration with aiSecurityScore360 provides native vulnerability and asset risk scoring capabilities that consider both IT and OT contexts.

MSSP Scalability: The platform supports multi-tenant OT/ICS visibility and response capabilities, making it suitable for managed security service providers serving multiple industrial clients. NIST-Based Segmentation: The platform supports NIST-based Level 0-5 segmentation with Seceon C-SOC nodes distributed across IT/OT environments, enabling proper network segmentation while maintaining visibility.

MSSP Scalability: The platform supports multi-tenant OT/ICS visibility and response capabilities, making it suitable for managed security service providers serving multiple industrial clients. NIST-

Based Segmentation: The platform supports NIST-based Level 0-5 segmentation with Seceon C-SOC nodes distributed across IT/OT environments, enabling proper network segmentation while maintaining visibility.

CMDB & Asset Management Integration: aiSecOT360 integrates with CMDB and asset management platforms to synchronize OT asset information and maintain contextual asset records. The integration enables monitoring and auditing of CMDB transactions and asset changes, providing security teams with traceability of asset creation, modification, and related configuration activity.

Centralized Response Orchestration

Detection recommendations and response actions can be coordinated across OT, IT, endpoint and network security controls. Enforcement depends on configured integrations and organizational policy.

Convergence Enablement

The platform supports the convergence of IT, OT, IoT, and IoMT environments by providing unified risk views and coordinated security policies across all domains. This capability is essential for organizations implementing digital transformation initiatives that blur traditional network boundaries.

Business Value and Compliance Benefits

Regulatory Compliance

aiSecOT360 supports compliance with major regulatory frameworks:

- **NIST Cybersecurity Framework:** Comprehensive coverage of Identify, Protect, Detect, Respond, and Recover functions
- **IEC 62443:** Industrial communication networks cybersecurity standards
- **NERC CIP**: North American Electric Reliability Corporation Critical Infrastructure Protection standards

Asset pedigree, vulnerability context, security events, recommended actions and response activity provide additional evidence for security posture assessment and audit workflows.

Zero Trust Implementation

The platform enables Zero Trust architecture implementation for OT environments through:

- Continuous device verification and authentication
- Least-privilege access enforcement
- Real-time risk assessment and adaptive controls
- Comprehensive logging and audit capabilities

Operational Benefits

Organizations implementing aiSecOT360 experience significant operational improvements:

- **Reduced Downtime Risk**: Early threat detection and automated response capabilities minimize the risk of production disruptions

- **Enhanced SOC Effectiveness:** Contextual, OT-aware alerts enable security teams to respond more effectively to industrial environment threats
- **Simplified Management:** Unified platform reduces complexity and training requirements for security personnel
- **Cost Optimization:** Comprehensive platform eliminates the need for multiple point solutions

Deployment and Implementation

Agentless Architecture

aiSecOT360 employs an agentless architecture that simplifies deployment and minimizes impact on industrial systems. This approach enables organizations to implement comprehensive OT security without modifying critical operational systems or risking production disruptions.

Scalable Implementation

The platform is designed to scale across diverse industrial environments:

- **Manufacturing**: Production line monitoring and automation system protection
- **Pharmaceuticals**: Compliance-focused security for regulated manufacturing environments
- **Power and Utilities:** Critical infrastructure protection for generation and distribution systems
- **Oil and Gas:** Upstream, midstream, and downstream operational security
- **Healthcare**: Medical IoT and IoMT device security and compliance

Hybrid Environment Support

aiSecOT360 seamlessly integrates legacy OT systems with modern Industrial Internet of Things (IIoT) implementations, supporting organizations throughout their digital transformation journey.

Safety-Aware Response

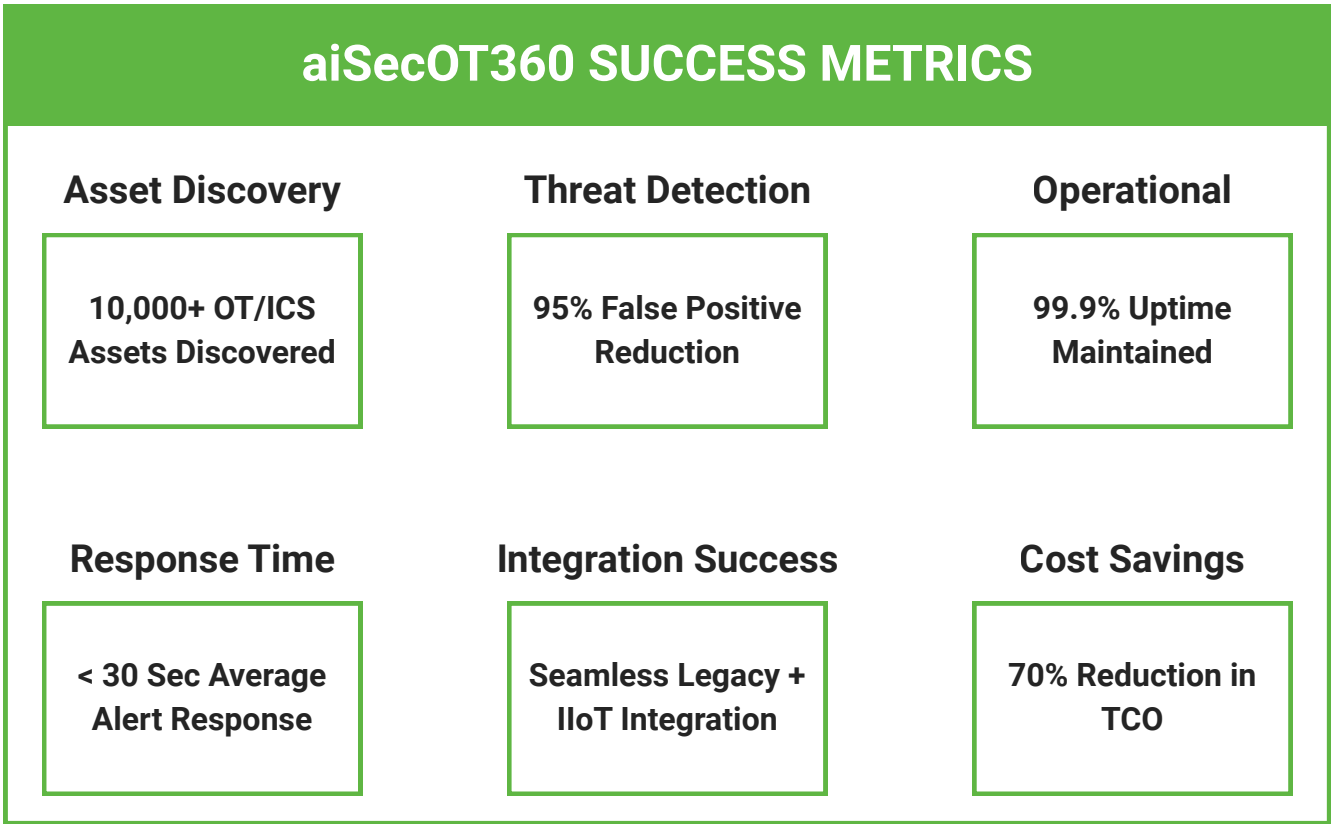
Detection and response are designed to minimize operational disruption. Enforcement can occur at network, endpoint or access-control layers, allowing security teams to contain threats without requiring direct modification of PLC logic.

Proven Results and Performance

Deployment Metrics

Real-world implementations of aiSecOT360 have demonstrated significant value:

- **Asset Discovery:** Over 10,000 OT/ICS assets discovered in recent deployments
- **False Positive Reduction:** 95% reduction in false positives compared to traditional OT security tools
- **Threat Detection:** Early breach detection achieved across manufacturing and energy sectors



SECTOR SUCCESS STORIES:

- ***Manufacturing****: Early breach detection prevented $2M+ in downtime*
- ***Energy****: 100% compliance achievement for NERC CIP requirements*
- ***Pharmaceuticals****: Zero FDA audit findings related to cybersecurity*
- ***Healthcare****: 95% reduction in medical device security incidents*

- **Integration Success:** Seamless integration demonstrated in hybrid environments, combining legacy systems with modern IIoT implementations

Competitive Advantages

aiSecOT360 delivers several key advantages over alternative solutions:

- **AI-Native Architecture:** Purpose-built AI capabilities reduce complexity while improving accuracy in threat detection and response.
- **Comprehensive Protocol Support**: Support for 70+ industrial protocols ensures compatibility across diverse industrial environments.
- **Unified Platform Integration:** Single platform approach eliminates the complexity and cost associated with managing multiple point solutions.
- **Operational Continuity:** Passive monitoring and non intrusive deployment ensure industrial processes remain uninterrupted.
- **Cost-Effective Scaling:** Affordable, scalable architecture makes comprehensive OT security accessible to organizations of all sizes
- **Deep OT Asset Intelligence:** Detailed asset pedigree and nested-device visibility provide security teams with the context required to prioritize vulnerabilities and operational risk.
- **OT-Aware Response:** Approximately 92 OT/ICS playbooks combine industrial detection logic with recommended response actions and configurable remediation.
- **Security Validation:** aiBAS360 provides Breach & Attack Simulation capabilities for validating defensive controls and detection coverage.
- **CMDB Integration & Auditability:** Integration with CMDB and asset management systems provides synchronized asset context and audit visibility into CMDB transactions and changes.

Future-Proofing Industrial Security

Emerging Threat Adaptation

The AI-driven architecture of aiSecOT360 enables continuous adaptation to emerging threats through:

- Machine learning model updates based on new threat intelligence
- Behavioral baseline adjustments for evolving operational patterns
- Protocol support expansion for new industrial technologies
- Integration capabilities for emerging security technologies

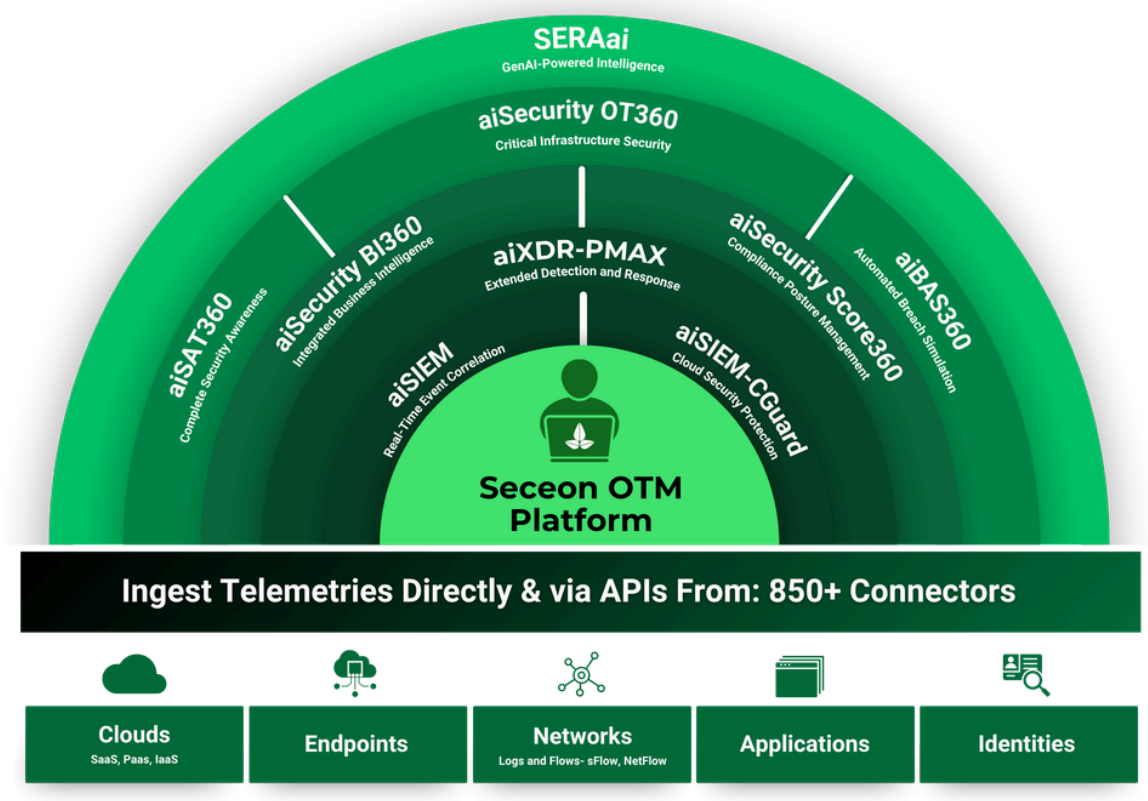
Digital Transformation Support

As industrial organizations continue their digital transformation initiatives, aiSecOT360 provides the security foundation necessary to safely implement:

- Industrial Internet of Things (IIoT) initiatives
- Edge computing deployments
- Cloud integration projects
- Advanced analytics and AI implementations

Conclusion

Seceon aiSecOT360 represents a significant advancement in OT/ICS security, delivering comprehensive protection engineered for industrial environments. Its AI-driven approach, extensive protocol support, and integration with the broader aiXDR360 platform provide unified visibility, threat detection, and response across complex OT, IoT, and ICS environments.



Beyond detection, aiSecOT360 delivers the context and response mechanisms needed to operationalize OT security. Detailed asset pedigree establishes what is operating in the environment, while threat intelligence and vulnerability correlation identify what requires attention. OT-specific playbooks provide recommended response actions, and configurable enforcement mechanisms support controlled remediation. For security validation, aiBAS360 extends the platform with Breach & Attack Simulation capabilities.

With proven asset discovery, reduced false positives, and effective threat detection across industrial environments, aiSecOT360 helps organizations address evolving threats while supporting digital transformation. Its unified IT/OT approach, scalable architecture, and automation help protect critical infrastructure, maintain operational continuity, and support regulatory compliance.

For organizations securing OT, IoT, and ICS environments, aiSecOT360 provides a strategic foundation for operational resilience and future-ready industrial cybersecurity, combining unified visibility, AI-powered detection, contextual risk analysis, and controlled response in a single platform.

For more information about Seceon aiSecOT360 and to schedule a demonstration, contact Seceon directly to explore how this comprehensive platform can secure your industrial environment while maintaining operational excellence.

About the Author

Chandra S. Pandey
Founder & CEO, Seceon Inc.



As a Founder and CEO of Seceon, Chandra Pandey brings over 20 years of cybersecurity and networking experience. He leads the development of integrated SIEM, SOAR, and XDR solutions, helping over 8,800 organizations simplify security, reduce costs, and achieve real-time threat protection.

© 2026 Seceon Inc. All rights reserved. aiSIEM, aiXDR, are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.