

2026

seceon

Agentic AI-Driven SOC:

The Autonomous SOC That Thinks, Investigates, and Responds

How the AI/ML-based Seceon OTM Platform with SeraAI agentic intelligence continuously detects, correlates, investigates, and responds to threats in real time, reducing analyst workload and accelerating threat response.

Executive Summary

Introduction

Security operations have reached an inflection point. Threat actors now weaponize AI to compress intrusion timelines from days to minutes, while defenders remain constrained by alert overload, fragmented tooling, and a global shortage of skilled analysts. Traditional SIEM, SOAR, and XDR deployments, even when stacked together, leave the critical bottleneck untouched: human-speed triage and investigation. The next evolution of the SOC is agentic — an AI-driven operation that thinks, investigates, and responds autonomously, with analysts governing outcomes rather than chasing alerts. The **Seceon Open Threat Management** (OTM) Platform delivers this today: a unified AI/ML-based platform in which 4,000+ machine learning models detect and correlate threats in real time, the SeraAI agentic intelligence layer autonomously investigates and resolves the majority of Level-1 alerts, and native SOAR contains confirmed threats in under 90 seconds.

Key Benefits of an Agentic AI-Driven SOC

- **Autonomous Investigation:** agentic AI independently triages, validates, and closes routine alerts — Seceon's SeraAI autonomously resolves ≥70% of Level-1 alerts, escalating confirmed threats with full context, and flagging any case it cannot resolve with evidence as degraded, naming the missing data with full investigation context.
- **Machine-Speed Response:** policy-governed automation executes containment in seconds rather than hours, shrinking attacker dwell time below the breakout window.
- **Radical Noise Reduction:** AI/ML correlation across network, endpoint, identity, cloud, and OT telemetry eliminates up to 95% of false positives before an analyst ever sees an alert.
- **Always-On Scalability:** 24×7 investigation capacity that scales with data volumes and tenants without proportional headcount growth, a decisive advantage for enterprises and MSSPs alike.
- **Proactive Resilience:** continuous attack simulation, posture scoring, and control validation shift the SOC from reactive firefighting to preventive assurance.

Implementation Strategies

The value of agentic AI depends on how it is grounded and governed. Organizations should consolidate telemetry onto a unified data fabric so the AI reasons over complete context, define autonomy tiers that keep humans in command of mission-critical decisions, and measure outcomes against hard KPIs — detection time, containment time, autonomous resolution rate, and false-positive elimination. Equally important, the AI layer itself must be secured and sovereign: models should run within the customer's environment, never train on customer data, and be protected against prompt injection and shadow-AI misuse**.**

How Seceon Delivers the Autonomous SOC

- **Think**: aiSIEM, aiXDR, EDR, NDR, and UEBA apply 4,000+ ML models and Dynamic Threat Models (DTM) to every event in stream — no manual rule tuning, MTTD under 5 minutes.
- **Investigate**: SERA AutoSOC conducts natural-language and fully autonomous investigations across all platform data, explains root cause in plain language, and closes ≥70% of L1 alerts without analyst intervention.

- **Respond:** SOAR 4.0 executes 100+ production playbooks, including host isolation, credential suspension, firewall rule injection, and DNS sinkholing in under 90 seconds, with new playbooks generated from natural language in ~30 seconds.
- **Unify:** one platform consolidates 8–10 point products on a single data fabric with 3,000+ pre-built connectors, while integrating openly with the customer's existing security stack.
- **Sovereign AI:** SeraAI deploys on-premises or air-gapped with local inference and no required outbound traffic; raw telemetry never leaves the customer’s environment, and aiTRiSM360 redacts sensitive data before any model call and secures the organization’s own AI estate against shadow AI and prompt injection.

Conclusion

The shift from manual to agentic security operations is inevitable. Attackers already use AI to scale and accelerate their campaigns; defenders who answer with an autonomous, human-governed SOC will detect faster, respond in machine time, and free scarce analysts for the work that genuinely requires human judgment. Seceon operationalizes that shift today on one platform, with measurable outcomes.

The Time for Agentic AI in the SOC Is Now

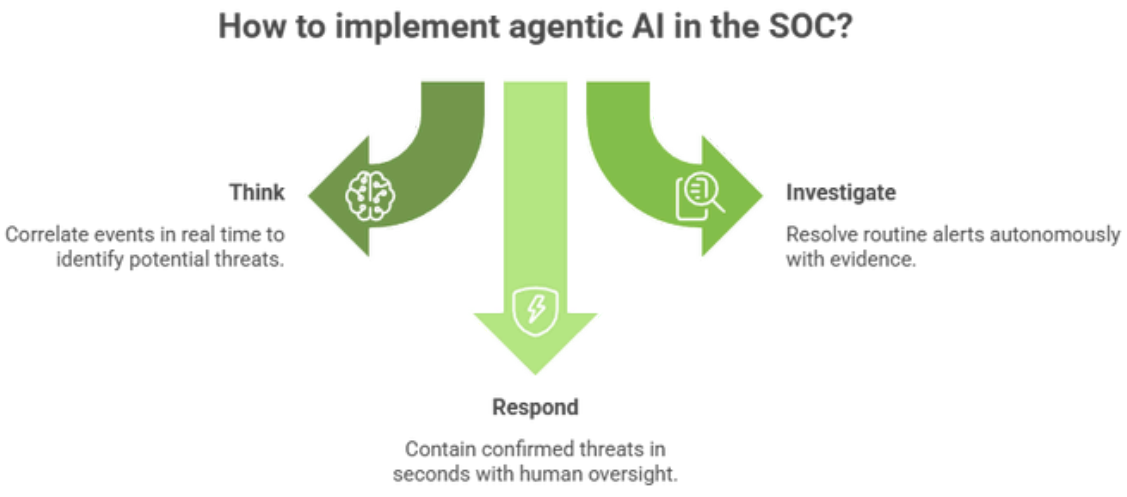
In 2026, SOC teams face an adversary that has already industrialized AI. Phishing lures are machine-written and flawless, voice and video deepfakes defeat identity verification, and polymorphic malware mutates faster than signatures can be published. Industry threat reporting shows that average eCrime breakout time the interval between initial access and lateral movement **has fallen to 48 minutes, with the fastest observed intrusion breaking out in 51 seconds.** No human-paced triage queue can keep up with that clock.

The SOC remains the nerve center of organizational cyber resilience: the team charged with identifying, investigating, and containing threats before they become business-disrupting incidents, while simultaneously evidencing compliance to regulators. Yet the people carrying that mandate are stretched to the limit. The global cybersecurity workforce gap is estimated at close to five million unfilled roles, and a large majority of security professionals report that the work is taking a measurable toll on their wellbeing and retention.

Agentic AI changes the equation. Where earlier machine learning classified and correlated, and generative AI assisted and summarized, agentic AI perceives, reasons, plans, and acts toward defined goals under explicit human governance. Applied to security operations, this means AI that does not merely rank alerts for a human queue, but independently investigates them, validates or dismisses them with evidence, and executes approved response actions at machine speed.

Organizations best prepared for the coming threat landscape will be those that integrate agentic AI deliberately grounded in complete telemetry, bounded by policy, and transparent in its reasoning without adding yet another silo to the stack. For enterprises and MSSPs alike, AI in the SOC is no longer a question of “if” or “when.” The only questions left are “how fast” and “how safely.”

> ***THE AUTONOMOUS SOC MANDATE***
>
> *Think: correlate every event in real time. Investigate and resolve routine alerts autonomously with evidence. Respond to and contain confirmed threats in seconds, governed by policy and human oversight.*



Why Modern SOCs Are at a Breaking Point

Whether you run security for a single enterprise or operate as an MSSP responsible for dozens of client environments, SOC teams confront the same structural challenges, and those challenges carry a steep operational and human price.

Drowning in Alerts

Alert fatigue is not new, but it has never been this severe. The proliferation of devices, cloud services, identities, and monitoring tools generates more signals than any human team can process. Industry surveys consistently find that a typical SOC contends with several thousand alerts per day; roughly two-thirds of analysts admit they cannot keep pace with the volume, and an overwhelming majority worry they are missing genuinely critical events buried in the noise. In practice, a large share of alerts dominated by false positives and duplicates are never investigated at all. The result is predictable: real attacks hide in plain sight while analysts burn hours dismissing noise.

Burned Out and Short-Staffed

Sustained alert pressure has a human cost. Surveys of SOC professionals report burnout rates above 70%, with roughly two-thirds of analysts actively considering a role change within a year. Attrition compounds the problem: filling a vacant SOC seat routinely takes many months against a global talent gap of several million unfilled cybersecurity positions. Every departure drains institutional knowledge, and every vacancy pushes more volume onto the analysts, who remain in a self-reinforcing cycle of overload and turnover. Meanwhile, the pace of attacker innovation demands continuous skill development that overloaded teams have no time to pursue.

Tool Sprawl, Data Silos, and Diminishing Returns

Most SOCs still operate through “swivel-chair integration”: analysts pivot across eight to ten consoles SIEM, EDR, NDR, threat intel, ticketing, cloud security manually stitching context together under time pressure. Each tool sees a fragment of the attack; none sees the whole.

Legacy SIEMs convert logs into yet more alerts, first-generation SOAR automates only narrow, brittle slices of response, and XDR centralizes visibility without removing the Tier-1 triage bottleneck. Volume-based licensing punishes organizations for the very visibility they need, encouraging dangerous blind spots. Most critically, sophisticated multi-vector attacks deliberately scatter low-severity signals across silos and without cross-domain correlation, no single tool recognizes the pattern until the attacker has already achieved their objective.

SOC Challenge	Operational Impact	Why Point Tools Fail
Alert Overload & False Positives	Critical events missed; analyst hours consumed dismissing noise	Rule-based correlation generates alerts, not verdicts; no autonomous validation
Analyst Burnout & Attrition	Knowledge loss, extended vacancies, degraded 24×7 coverage	Tooling adds work (tuning, pivoting, copy-paste) instead of removing it
Tool Sprawl & Data Silos	Fragmented context; multi-vector attacks evade recognition	Each product analyzes its own slice; cross-domain correlation is manual
Attacker Speed (Breakout in Minutes)	Human-paced triage cannot beat machine-paced intrusion	Response depends on queue position and staffing, not on threat severity



The Agentic AI-Driven SOC: From Assisted to Autonomous

SIEM, EDR, XDR, NDR, and SOAR each promised relief, yet all five stop short of what analysts actually need: decisions. These tools aggregate and sometimes contextualize information, but they still hand the analyst a queue of questions rather than a set of validated answers. Agentic AI closes that gap. It does not simply surface an alert it investigates the alert, assembles the evidence, reaches a verdict, and either closes it or escalates it with a complete narrative and a recommended course of action.

The Evolution of AI in the SOC

Era	Key Milestones	Impact on the SOC
Perception & ML2010s →	Machine learning matures from research to production; streaming analytics enable behavioral baselining at scale. Seceon is founded on this principle with real-time AI/ML correlation instead of static rules.	Anomaly detection and event correlation reduce false positives and shorten time to detect. Behavioral baselines expose insider threats and credential misuse.
Generative AI2022 →	Large language models popularize natural-language interfaces. Security copilots emerge for summarization, rule authoring, and playbook drafting. Seceon embeds SeraAI as a copilot across every OTM module.	Analysts query security data in natural language. Detection content and SOAR playbooks are generated in seconds, while investigation narratives become easier for stakeholders to understand.
Agentic AI2024 →	Autonomous agents perceive, reason, plan, and act with defined roles and autonomy levels. Seceon operationalizes agentic investigation with a an adversarial committee of agents prosecutor, defender, adjudicator and chief analyst whose verdicts are scored deterministically in code, never by the model.	AI independently investigates and closes routine alerts, proactively hunts threats, and triggers policy-validated responses. Human analysts supervise outcomes and retain control over critical decisions.

Think: Continuous Detection and Correlation

The agentic SOC begins with perception at machine scale: every log, flow, identity event, cloud API call, and OT signal analyzed in stream, not in batches. Machine learning models establish dynamic behavioral baselines for users, entities, and applications, while cross-domain correlation reconstructs multi-stage kill chains from signals that would look benign in isolation. Context asset criticality, identity risk, and threat intelligence are attached at detection time, so severity reflects business impact rather than raw signature confidence.

Investigate: Autonomous Triage and Validation

For each high-fidelity alert, the agentic layer runs the same loop a senior analyst would, only in seconds. It enriches the alert with threat intelligence, entity timelines, asset relationships, and prior incident history; reasons through the evidence step by step; and reaches a verdict. Benign and duplicate alerts are closed with a documented rationale. Confirmed threats are escalated with a plain-language root-cause explanation, a complete evidence chain, and a recommended action plan transforming Tier-1 work from a human bottleneck into a governed, machine-speed process.

Respond: Machine-Speed, Policy-Governed Containment

Investigation without action leaves dwell time on the table. In the agentic SOC, validated verdicts trigger orchestrated response, isolating hosts, suspending credentials, injecting firewall rules, sinkholing malicious domains, quarantining email executed in seconds and always validated against organizational policy, change control, and blast-radius assessment before any action fires. Every action is logged, auditable, and reversible.

Human-in-the-Loop Governance

Autonomy is a dial, not a switch. Mature agentic SOCs define autonomy tiers: routine, low-blast-radius actions execute automatically; actions touching mission-critical systems require explicit analyst approval. Analyst feedback overrides, reclassifications, and false-positive labels feed into platform memory and rules, so the system's judgment improves with every decision. The outcome is not fewer humans in security operations; it is humans doing higher-value work: threat hunting, adversary emulation, engineering, and strategy.

The Path to the Autonomous SOC: The Building Blocks

Set Your Goals and KPIs

Begin with the bottleneck, not the technology. If analysts drown in false positives, target noise elimination first; if dwell time is the risk, target detection and containment speed. Whatever the entry point, define measurable KPIs before evaluating vendors and hold the platform to them in production.

KPI	What It Measures	Seceon OTM Benchmark
Mean Time to Detect (MTTD)	Time from first malicious activity to a correlated, contextualized alert	Under 5 minutes
Automated Containment Time	Time from confirmed verdict to executed response action	Under 90 seconds
Autonomous L1 Resolution Rate	Share of Level-1 alerts investigated and closed without analyst input	≥70% (SeraAI)
False-Positive Elimination	Noise removed by AI/ML correlation before analyst review	Up to 95% reduction
Playbook Creation Time	Time to author a production-ready automated response workflow	~30 seconds (LLM-generated)

Think Human-First

An AI-driven strategy is not an AI-only strategy. The objective is to remove toil from analysts, not judgment from the organization. Calibrate the balance deliberately: let AI own repetitive validation and routine containment, and reserve human approval for high-severity incidents and mission-critical systems. No matter how urgent isolation appears, actions with significant business blast radius warrant human oversight.

Demand a Unified Data Foundation

Agentic AI is only as good as the context it reasons over. If the AI sees only one tool's data or if analysts must copy and paste context into a chat window, the investigation is incomplete by design. The platform should ingest telemetry in any format from every relevant source, normalize it into a single fabric, and give the AI full-platform context spanning logs, network, endpoint, identity, cloud, and OT while protecting sensitive information end to end.

Require Transparency, Explainability, and Sovereignty

AI can err, and unexplained verdicts cannot be trusted or audited. Insist on evidence-linked conclusions: every verdict traceable to the underlying events, every action logged with rationale. For regulated and government environments, insist equally on sovereignty models that run inside your boundary, never train on your data, never transmit it unencrypted, and carry no dependency on overseas AI services.

Secure the AI Itself

The autonomous SOC introduces and must defend a new attack surface: the organization's own AI estate. Shadow use of external LLMs leaks sensitive data; prompt injection can manipulate locally deployed models; hijacked agents and RPA bots can be weaponized from inside. An agentic SOC platform should therefore discover every AI agent on the network, detect prompt-injection and jailbreak attempts in real time, block sensitive data from reaching unapproved AI endpoints, and isolate compromised agents automatically. Seceon addresses this natively with aiTRiSM360, aligned to the emerging AI trust, risk, and security management (AI TRiSM) category.

Benchmark and Optimize

“Is the AI doing its job?” should be answerable with data. Establish a performance baseline at go-live, review autonomous-resolution accuracy and analyst-override rates on a fixed cadence, and treat vendor commitment to continuous model improvement as a selection criterion in its own right. The feedback loop where analyst decisions update platform memory and rules is where an agentic SOC compounds in value over time.

Agentic AI-Driven SOC

Seceon OTM Platform with SeraAI — Detects, Investigates, and Responds Autonomously in Real Time

Convergence Architecture Overview

Traditional Multi-Tool SOC

Alert overload
Thousands of alerts/day, most never investigated

Tool sprawl
8–10 point products, siloed data, manual pivoting

Human-paced triage
Hours-to-days detection, staffing-dependent response

Analyst burnout
70%+ burnout, chronic understaffing

SeraAI Agentic Layer

Seceon Agentic AI SOC

4,000+ ML models
Real-time correlation, MTTD under 5 minutes

SeraAI investigation
Autonomously resolves ≥70% of Level-1 alerts

SOAR 4.0 response
Policy-governed containment in under 90 seconds

One data fabric
3,000+ connectors, single unified platform

The Autonomous Alert Lifecycle

1. Detect
APE correlates telemetry, generates a high-fidelity alert

2. Enrich
SeraAI adds threat intel, entity timeline, asset context

3. Investigate
SeraAI reasons through evidence, reaches a verdict

4. Validate
APE checks policy, change control, blast radius

5. Respond
SOAR 4.0 executes containment in under 90 sec

6. Audit & Learn
Case logged; analyst feedback updates memory and rules

The Autonomous SOC, Delivered Today

<5 min	<90 Sec	≥70%	95%
Mean Time to Detect	Automated Containment	L1 Alerts Resolved Autonomously	False-Positive Reduction

Seceon's Agentic AI-Driven SOC: The OTM Platform

The market is crowded with point solutions and bolt-on copilots that add capability in one corner of the SOC while deepening sprawl everywhere else. Seceon took the opposite path. The Open Threat Management (OTM) Platform was architected from inception as a unified, AI/ML-native security operations platform: one data fabric, one analytics brain, one response layer, now extended with SeraAI, the agentic intelligence embedded across every module. Trusted by 9,800+ customer organizations and 850+ MSSP/MSP partners, the platform analyses on the order of 2.4 trillion security events every day.

One Platform, One Data Fabric, One AI Brain

OTM's three-tier architecture separates collection, analytics, and retention so each scales independently. Collection & Control Engine (CCE) at sites and tenants normalize, deduplicate, and compress telemetry from 3000+ connectors. The central Analytics & Policy Engine (APE) applies 4,000+ AI/ML models and Dynamic Threat Models to the full event stream in real time. Long-Term Storage (LTS) preserves forensic data for up to seven years. SeraAI operates across this entire fabric its context window is the whole platform, not a single tool or log source.

Ingest (CCE) → Think: Correlate with 4,000+ ML Models (APE) → Investigate: Autonomous Triage (SeraAI) → Respond: Policy-Governed Containment (SOAR 4.0) → Report & Retain (GUI / APE / LTS)

Think: Detect and Correlate in Real Time

aiSIEM, aiXDR, NDR, and UEBA analyse every event in stream. Dynamic Threat Models self-adjust to the environment from first data receipt no manual rule authoring or months of tuning- while behavioral analytics baseline every user and entity to expose insider threats, credential compromise, and privilege abuse. Cross-domain correlation reconstructs multi-stage attack chains mapped to MITRE ATT&CK, attaches asset criticality and identity risk at detection time, and suppresses up to 95% of false positives.

The result: mean time to detect under 5 minutes, with alert quality high enough for autonomous downstream investigation.

Investigate: SeraAI Autonomous Investigation

SeraAI is the AI intelligence layer embedded across every OTM module, not a standalone chatbot. It autonomously investigates, validates, and resolves ≥70% of Level-1 alerts, escalating confirmed threats and flagging any case it cannot resolve with evidence accompanied by a plain-language root-cause explanation, a supporting evidence summary, and recommended next steps. Analysts interrogate the platform in natural language: “show me all lateral movement in the last 24 hours,” with cross-module answers spanning SIEM, NDR, XDR, and identity data, and contextual follow-up questions resolved automatically. Because SeraAI can be deployed entirely on-premises or in sovereign cloud, classified and regulated environments gain agentic capability without data ever leaving their boundary.

Respond: SOAR 4.0 Machine-Speed Containment

OTM's native SOAR 4.0 converts verdicts into action in under 90 seconds: host isolation, credential blocking, firewall rule injection, DNS sinkholing, and endpoint or email quarantine, orchestrated across 950+ integrated security tools. More than 100 production playbooks ship out of the box, and SeraAI generates new, context-aware playbooks from a natural-language description in roughly 30 seconds, adapted to threat type, asset criticality, and regulatory requirements. Every proposed action passes the APE policy engine organizational security policy, change control, and blast-radius checks before execution, and every action lands in an immutable audit trail.

Step	Component	Action
1	APE – Detection	AI/ML correlation generates a high-fidelity alert with UEBA score, kill-chain stage, and asset criticality attached.

Step	Component	Action
2	SeraAI – Context Assembly	Alert enriched in real time with threat intelligence, entity timelines, asset relationships, and prior incident history.
3	SeraAI – Reasoning	Multi-step investigation produces a verdict, risk score, evidence chain, and recommended action plan.
4	APE – Policy Validation	Proposed actions checked against security policy, change control, and blast-radius rules before anything executes.
5	SOAR 4.0 – Response	Approved actions execute in under 90 seconds: block, isolate, suspend, sinkhole, and quarantine.
6	Case & Audit	Full investigation report, evidence, and action trail written to case management; analyst feedback updates platform memory and rules

Every Module, One Autonomous Operation

OTM Module	Role in the Agentic AI-Driven SOC
aiSIEM™	Real-time ingestion and AI/ML correlation at nation-scale throughput; no manual rule tuning; up to 95% false-positive reduction.
aiXDR™	Cross-domain detection spanning network, endpoint, cloud, and identity; multi-stage attack-chain reconstruction with every rule mapped to MITRE ATT&CK v20.0.
NDR & UEBA	Passive network analysis for lateral movement and C2; behavioral baselines for every user and entity, including OT/ICS environments.
aiITDR™ / aiIDGuard™	Human, non-human and AI identities across AD, Entra ID, Okta, AWS IAM and 20 PAM vaults; unified identity threat detection with sub-90-second automated containment.

OTM Module	Role in the Agentic AI-Driven SOC
TI360™	100+ threat intelligence sources and 2B+ IOCs with AI-generated behavioral indicators grounding every investigation.
aiSOAR 4.0™	100+ production playbooks, LLM-powered playbook generation in ~30 seconds, and containment in under 90 seconds.
SeraAI™	The agentic layer providing natural-language investigation, ≥70% autonomous L1 resolution, root-cause explanation, and sovereign deployment.
aiTRiSM360™	AI agent discovery across hosts, containers and APIs
CMX360™	Continuous compliance across 50+ frameworks with about 90% reporting automation, delivering audit-ready evidence from the same data fabric.
aiSecOT360™ / aiBAS360™	Passive OT/ICS visibility with Purdue Model segmentation, plus continuous breach-and-attack simulation to proactively validate security controls.

Built for MSSPs: Multi-Tier Multi-Tenancy

For MSSPs, agentic AI is a margin engine: autonomous investigation absorbs client growth without linear headcount growth. OTM is the industry's first platform with true Multi-Tier Multi-Tenancy (MT-MT) a purpose-built Master MSSP → Regional MSSP → Client hierarchy with full tenant isolation, per-tenant AI baselines, per-tenant billing and reporting, and white-label delivery. SeraAI's autonomy applies per tenant, so every client benefits from machine-speed triage under the MSSP's governance.

Sovereign and Air-Gapped AI

Unlike cloud-dependent AI products, the entire OTM platform, including SeraAI's language models, deploys on-premises, in a private or sovereign cloud, or fully air-gapped.

Customer data is never used to train shared models and never leaves the environment, with no dependency on overseas AI services. For defense, government, banking, and critical-infrastructure operators, this makes agentic security operations compatible with the strictest data-residency and classification mandates.

Open Integration Ecosystem

OTM strengthens the stack you already own rather than demanding rip-and-replace. 3000+ pre-built connectors span firewalls, endpoints, identity providers, cloud platforms, email, and OT systems; STIX/TAXII APIs exchange threat intelligence with any third-party source; bidirectional integrations with ServiceNow, JIRA, Slack, and Teams keep existing workflows intact; and new parsers and connectors are typically delivered in 48–72 hours. Deployment is measured in hours, not quarters: a 5-hour installation with a fully operational platform and active detections within two weeks.

Seceon: The Autonomous SOC, Delivered Today

Within a few years, running SOC triage without an agentic AI layer will feel like navigating an unfamiliar city without GPS technically possible, competitively indefensible. Attackers have already made their choice: AI now writes their lures, mutates their malware, and compresses their breakout times to minutes. The defender's answer cannot be another dashboard or another queue. It must be an operation that thinks, investigates, and responds at the same speed with humans firmly in command of what matters.

That is precisely what the Seceon OTM Platform delivers: a single AI/ML-native platform where detection, investigation, and response are one continuous, governed motion measurable from day one.

Outcome	Traditional Multi-Tool SOC	Seceon Agentic AI-Driven SOC
Mean Time to Detect	Hours to days	Under 5 minutes
Containment of Confirmed Threats	Hours, dependent on staffing	Under 90 seconds, policy-governed
Level-1 Alert Workload	Fully manual triage	≥70% resolved autonomously by SeraAI
False-Positive Noise	Dominates analyst hours	Reduced by up to 95% through AI/ML correlation
Security Stack	8–10 point products with siloed data	One unified platform with up to 58% lower TCO
Time to Value	6–18 months of integration	5-hour installation; operational in 2 weeks

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 850 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,800 clients.

References and Citations:

This whitepaper is based on research and data from:

- ISC2: Cybersecurity Workforce Study (2024)
- SANS Institute: SOC Survey (2024)
- CrowdStrike: Global Threat Report (2025)
- IBM: Cost of a Data Breach Report (2025)
- Gartner: Innovation Insight for Autonomous Security Operations (2025)
- MITRE: ATT&CK Framework
- NIST: Cybersecurity Framework (CSF) 2.0 (2024)

About the Author

Nilesh Mojidra

Presales Head, EMEA, Seceon Inc.



As Presales Head, EMEA at Seceon, Nilesh Mojidra leads cybersecurity solution strategy for enterprises and MSSPs across the region. Leveraging extensive expertise in AI-driven security operations, he helps organizations simplify security, accelerate threat detection, automate response, and strengthen cyber resilience through Seceon's Open Threat Management Platform.

© 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.