MARKETSANDMARKETS™

seceon
SECURITY FOR EONS

MAKING THREAT INTELLIGENCE ACTIONABLE ACROSS IT AND OT ENVIRONMENTS



Threat Intelligence

EXECUTIVE SUMMARY

The cybersecurity threat environment worldwide is undergoing a structural transformation. Rapid advances in attacker automation, AI-augmented intrusion techniques, and the convergence of information technology (IT) and operational technology (OT) attack surfaces have fundamentally altered what security operation teams must detect and respond to.

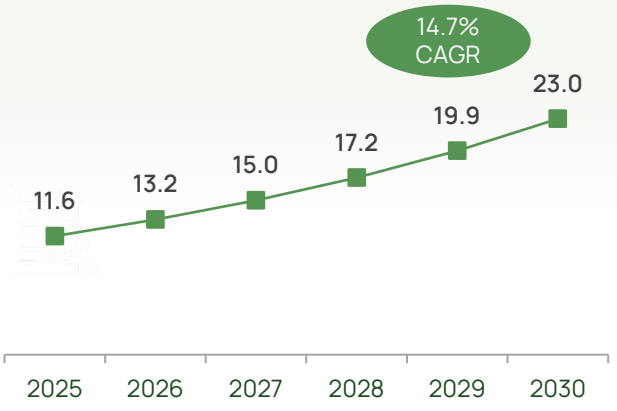
The core challenge is no longer data collection. Most enterprises are drowning in telemetry. The critical gap is the ability to correlate, prioritize, and operationalize that data within the narrow detection windows that determine breach outcomes. Fragmented tool stacks, siloed analyst workflows, and reactive security architectures have created measurable exposure that attackers routinely exploit.

Insights from SANS Institute indicate that 55% of security operations teams experience excessive alert volumes, while IBM X-Force data shows that organizations relying on traditional SIEM-only architectures take an average of 194 days to identify and 64 days to contain an active breach. This dwell time creates substantial exposure windows that directly translate to financial and reputational damage.

68%	Of data breaches involve human element
44%	Of the incidents involve Ransomware
55%	Of orgs report alert fatigue as top challenge
194	Mean days to detect an active breach

Source: Verizon DBIR 2025; SANS SOC Survey 2025; CrowdStrike Global Threat Report 2025; IBM X-Force Threat Intelligence Index 2025, MnM Analysis

GLOBAL THREAT INTELLIGENCE MARKET ($ BN)



Source: MarketsandMarkets

MarketsandMarkets research stated that the global threat intelligence (TI) market is projected to grow from USD 11.6 billion in 2025 to USD 22.9 billion by 2030, at a 14.6% CAGR, driven by demand for real-time, AI-enriched intelligence across increasingly complex, multi-environment deployments. The research reinforces that the organizations that integrate AI-driven threat detection with cross-domain visibility reduce their mean time to respond (MTTR) by up to 70%. This is expected to help organizations achieve measurably lower total cost of breach remediation compared to organizations operating disconnected tool stacks.

In this evolving landscape, **Seceon** delivers an intelligence-driven approach to security operations through its Open Threat Management (OTM) platform. By unifying threat detection, intelligence, and automated response within a single operational framework, Seceon enables organizations to transform fragmented security data into real-time, actionable threat intelligence.

TABLE OF CONTENTS

01 Evolution And Challenges In Modern Threat Intelligence

02 The Shift Toward Ai-driven, Unified Threat Intelligence Platforms

03 Seceon's Approach To Threat Intelligence

04 Strategic Partnership And Ecosystem

05 Seceon-enabled Industry Use Cases

06 Conclusion

This whitepaper explores how Seceon's unified approach enables enterprises to move from reactive security postures to proactive, scalable, and intelligence-driven operations. Supported by real-world deployment outcomes across critical sectors, including power and energy, transportation, and healthcare.

EVOLUTION AND CHALLENGES IN MODERN THREAT INTELLIGENCE

- **Increasing Sophistication Of Cyber Threats And Expanding Attack Surfaces**

The global cybersecurity landscape is undergoing a structural shift, in which rapid digital transformation intersects with increasingly sophisticated and scalable cyber threats. As organizations expand across cloud, remote, and OT environments, traditional security boundaries are dissolving, exposing enterprises to a broader and more complex attack surface. What was once a perimeter-driven security model has now evolved into a distributed ecosystem of interconnected systems, identities, and data flows.

Key trends defining the current threat environment include:

MODERN THREATS ARE ACCELERATING ACROSS MULTIPLE FRONTS

62%	47%	70%	500%	42%
Increase in AI-driven attacks	Growth in identity-based attacks	Identities linked to malicious activity	Growth in underground market access	Identity abuse involved in attacks

GLOBAL SCANS

56,000

scans per second globally



INSIGHT
Attackers are leveraging AI, identity, and underground ecosystems at scale—expanding speed, reach, and impact across the digital world.

The convergence of AI-driven attacks, identity risks, and underground economies is reshaping the threat landscape and demanding unified, intelligence-driven defenses.

Source: CrowdStrike Global Threat Report 2025; Fortinet Global Threat Landscape Report 2025; World Economic Forum Global Cybersecurity Outlook 2025

The convergence of faster attack execution, identity-centric intrusion methods, and expanding digital ecosystems is redefining the threat intelligence imperative. Intelligence is no longer a supplemental input to security operations; it is the primary mechanism for achieving detection accuracy, response efficiency, and analyst prioritization. Security Boulevard's 2025 SOC Effectiveness Survey confirms that organizations whose threat intelligence is operationally disconnected from detection workflows report a mean time to respond that is 40% longer than that of those with integrated frameworks.

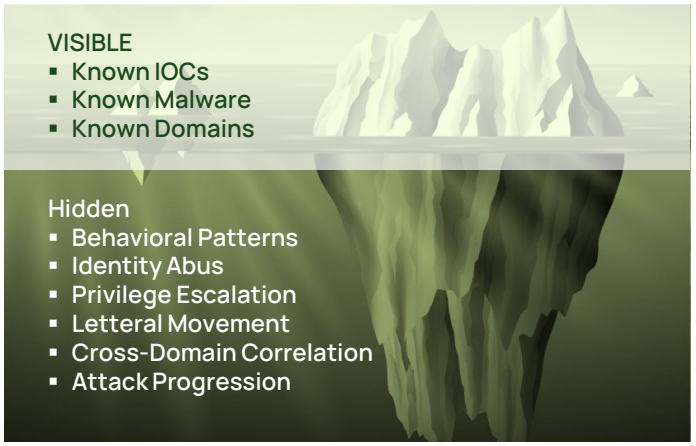
MARKETSANDMARKETS KEY OBSERVATION

- ✓ AI, automation, and identity-centric attack techniques are reshaping how threats are executed, forcing security teams to move beyond indicator-based intelligence models
- ✓ Modern attack paths span multiple domains and generate fragmented signals, increasing the importance of contextual analytics and cross-domain correlation
- ✓ Future-ready intelligence programs are likely to prioritize context, correlation, and operational relevance, enabling security teams to understand attack progression rather than simply identify malicious activity

> The next phase of threat intelligence maturity will be defined by how effectively organizations transform intelligence into operational action. As attack execution becomes faster, security teams will require more automated, and increasingly identity-centric intelligence platforms.

LIMITATIONS OF TRADITIONAL THREAT INTELLIGENCE APPROACHES

WHAT TRADITIONAL INTELLIGENCE MISSES



What Security Teams Are Missing?

- **Identity has become the primary attack vector.** Microsoft reported a **32% increase in identity-based attacks in 2025.**
- Attack execution is becoming increasingly commoditized, as reflected by the 500% growth in underground access markets, enabling adversaries to acquire credentials, sessions, and initial access.
- **Modern attacks span multiple domains.** With **75% of organizations experiencing cloud-related incidents and 68% of attacks involving endpoint compromise.**
- **AI is accelerating attack scale and execution.** The **62% increase in AI-assisted attacks** highlights how automation is enabling adversaries to conduct reconnaissance, phishing, and credential abuse activities more efficiently than traditional attack methods.
- Agentic AI and attack automation are compressing attacker timelines, increasing the importance of real-time correlation and decision support.

EVOLUTION OF THREAT INTELLIGENCE

PAST	Present	FUTRUE
Traditional TI	**Context-Aware TI**	**Operational TI**
▪ IOC-Centric ▪ Periodic Updates ▪ Analyst Driven	▪ Behavior Analytics ▪ Threat Correlation ▪ Cross-Domain Visibility	▪ Continuous Intelligence ▪ Automated Decisions ▪ Real-Time Response

Key Message

The evolution from IOC-centric intelligence to operational threat intelligence enables proactive, contextual, and outcome-driven security operations.

Modern attacks increasingly rely on identities, legitimate access, and behavioral techniques that generate limited indicator-based visibility. As a result, organizations require intelligence capabilities that can uncover attack progression and establish context across distributed environments.

Growing reliance on cloud environments, interconnected applications, and legitimate credentials is driving demand for intelligence capabilities that can continuously correlate behaviors, entities, and events across environments, enabling security teams to uncover attack progression, establish context, and prioritize response based on operational risk rather than isolated indicators.

MODERN ATTACK CHAIN

IDENTITY
80% of breaches involve compromised identities

CLOUD
75% of organizations experienced cloud-related incidents

ENDPOINT
68% of attacks involve endpoint compromise

APPLICATION
70% of branches involve application exploitation

DATA
60% of organizations faces data exfiltration attempts

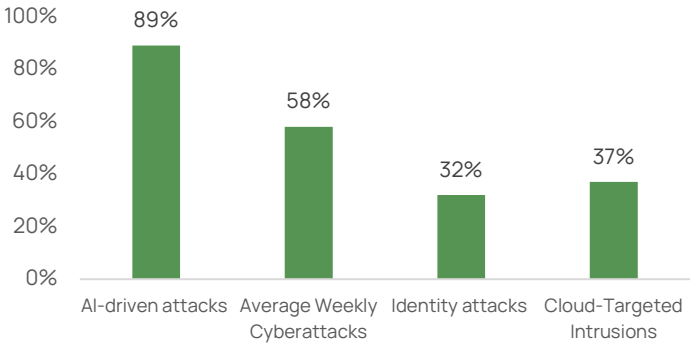
Traditional TI

Sees individual indicators and isolated events

Operational TI

Correlated the entire attack chain across domain in real-time

GROWTH OF MODERN ATTACK VECTORS, 2025-26



Source: CrowdStrike Global Threat Report 2026, Microsoft Digital Defense Report 2025, Zscaler ThreatLabZ 2025 Ransomware Report, MarketsandMarkets Analysis

While traditional approaches focused on collecting indicators and supporting analyst investigations, modern security environments require intelligence that continuously adapts to changing threats, correlates activities across domains, and drives real-time operational decisions. **From a MarketsandMarkets perspective**, the convergence of identity-centric attacks, AI-enabled adversaries, and interconnected attack paths is shifting threat intelligence from indicator analysis to operational decision support. Organizations that can continuously correlate activities across environments will be better positioned to reduce investigative effort and accelerate response times.

▪ FRAGMENTED SECURITY ARCHITECTURES AND SOC INEFFICIENCIES

The modern SOC is not failing for lack of tools; it is failing because of too many of them and fragmented architectures

Modern SOCs no longer face the challenge of a lack of security telemetry or tools; rather, they face the inability to operationalize intelligence efficiently across fragmented environments. As organizations continue to deploy specialized security technologies, many SOCs are experiencing diminishing operational returns despite increasing security investments.

KEY SOC PAIN POINTS

CHALLENGE	IMPACT
Fragmented Tools and Data Silos	Limited Cross-Domain Visibility
Increased Operational Overhead	Manual and Inefficient Workflows
Reactive, Tool-Centric SOC Operations	Reduced Threat Prioritization
Lack of Unified Workflows	Slowed Detection and Response
Underutilized Threat Intelligence	Poor Intelligence Integration
Delayed Detection and Response Cycles	Increased Risk Exposure

THE NOISE PROBLEM: WHY VISIBILITY IS LOST?

40%
More Operational Labor Costs

46%
Of Alerts Are False Positives

10.9
Security Consoles Managed Daily on Average

2,992
Alerts Per Day On Average

(63% go entirely unaddressed)

Source: IBM Cost of Data Breach 2025, Microsoft Digital Defense Report 2025, MnM Research and Analysis

According to MnM research and supported facts by IBM and Microsoft's State of SOC Report 2026, from a threat intelligence perspective, the issue is not intelligence availability but intelligence accessibility and actionability. Threat data often remains distributed across multiple tools, workflows, and security domains, limiting analysts' ability to establish context and accelerate investigations. This creates a cascading operational effect: analysts spend more time triaging alerts, detection and response cycles slow down, and threat intelligence becomes underutilized despite significant investments in security technologies.

IMPACT ON THE MODERN SOC

SIGNAL-TO-NOISE RATIO IS BROKEN
Too much noise, meaningful threats get lost.

ANALYST OVERLOAD & BURNOUT
Analysts spend time triaging noise instead of real threats.

TRIAGE TAKES HOURS, NOT MINUTES
Every hour of undetected threat increases risk.

FRAGMENTED ENVIRONMENT SLOWS EVERYTHING
Moving laterally, escalating privileges, staging impact.

DETECTION OUTCOMES DETERIORATE
Noise and tool sprawl continue to degrade SOC effectiveness.

The future of threat intelligence is not defined by collecting more intelligence but by operationalizing intelligence within security operations. Organizations are increasingly shifting toward AI-driven, unified threat intelligence and security operations platforms that can consolidate visibility, correlate activity across environments, reduce analyst workload, and transform intelligence into faster detection, investigation, and response outcomes.

✓ THE SHIFT TOWARD AI-DRIVEN, UNIFIED THREAT INTELLIGENCE PLATFORMS

The shift toward AI-driven threat intelligence is being driven by a simple reality: security teams are processing more data than traditional analysis methods can handle.

THE EVOLUTION OF THREAT INTELLIGENCE

01	02	03
REACTIVE INTELLIGENCE	**CONTEXTUAL INTELLIGENCE**	**AI-DRIVEN OPERATIONAL INTELLIGENCE**
Intelligence as Data Collection	Intelligence as Threat Context	Intelligence as Operational Action
▪ Static IOC feeds ▪ Manual investigations ▪ Siloed threat analysis ▪ Delayed response	▪ Behavioral analytics ▪ Machine learning correlation ▪ Threat prioritization ▪ Cross-domain visibility	▪ Continuous monitoring across environments ▪ Real-time correlation & threat detection ▪ AI-assisted investigations ▪ Automated response and remediation
Outcome: Limited Visibility	Outcome: Improved Context	Outcome: Operational Resilience

FROM INFORMATION → TO INSIGHT → TO ACTION

THE REALITY DRIVING THE SHIFT

EXPANDING ATTACK SURFACE	Cloud, identity, endpoint, network, and OT environments increase complexity.
AI & ML ADOPTION	Enhances prioritization and reduces investigation time.
FASTER & ACCURATE RESPONSE	AI-driven intelligence enables earlier detection and automated actions.
CONTINUOUS CORRELATION	Events correlated across domains for stronger detection accuracy.

WHY ARE ORGANIZATIONS SHIFTING?

600M+
CYBERATTACKS OBSERVED DAILY

32%
INCREASE IN IDENTITY-BASED ATTACKS IN 2025

80 DAYS FASTER
BREACH IDENTIFICATION & CONTAINMENT WITH AI & AUTOMATION

$1.9M LOWER
AVERAGE BREACH COST WITH EXTENSIVE AI & AUTOMATION

4.5 MILLION
NEW MALWARE FILES BLOCKED DAILY

Source: IBM Cost of Data Breach 2025, Microsoft Digital Defense Report 2025, MnM Research and Analysis

Organizations are no longer securing isolated endpoints and networks but increasingly interconnected ecosystems spanning cloud infrastructure, identities, applications, OT environments, and third-party systems. This expanded attack surface is driving unprecedented threat volumes, with Microsoft's 2025 Digital Defense Report indicating that more than 600 million cyberattacks are observed daily.

In response, organizations are adopting AI- and machine learning-driven security operations to analyze vast telemetry streams, correlate events across environments, and prioritize threats based on contextual risk. According to IBM's 2025 Cost of a Data Breach Report, organizations that extensively leverage AI and automation identify and contain breaches up to 80 days faster while reducing average breach costs by approximately USD 1.9 million, highlighting the growing business value of intelligence-driven security operations.

KEY TAKEAWAYS

- Threat intelligence is becoming an operational capability.
- AI and machine learning are improving contextual awareness
- Unified intelligence architectures are reducing investigative complexity
- Automation is increasingly embedded across the security lifecycle
- Security leaders are prioritizing platforms that deliver measurable operational outcomes

MARKETSANDMARKETS PERSPECTIVE

"The strategic value of threat intelligence is shifting from insight generation to operational execution. As security teams face growing pressure to reduce response times and improve efficiency, investments are increasingly focused on platforms that can translate threat intelligence into prioritized actions, automated workflows, and measurable security outcomes. The next phase of market growth will be driven less by data aggregation capabilities and more by the ability to operationalize intelligence across the security lifecycle."

✓ AI AND AUTOMATION AS THE FOUNDATION FOR SCALABLE INTELLIGENCE OPERATIONS

Threat intelligence is evolving from an analytical function into an operational capability. As organizations adopt AI/ML, LLMs, agentic AI, and intelligent automation, the focus is shifting from collecting intelligence to operationalizing intelligence across detection, investigation, response, compliance, and resilience workflows. The growing emphasis on Data Foundations, Autonomous AI Agents, AIOps, and Business as Code reflects the need for operating models that can continuously transform telemetry into context, context into decisions, and decisions into coordinated action.

CORE PILLARS OF AI-DRIVEN INTELLIGENCE OPERATIONS

1. DATA FOUNDATIONS

THE BEDROCK OF OPERATIONS

- ✓ Unified telemetry ingestion
- ✓ Data normalization & enrichment
- ✓ Data governance & quality controls
- ✓ LLM-ready, trusted datasets
- ✓ Privacy, security & compliance

OUTCOME

High-quality data powers accurate models and reliable decisions.

2. AUTONOMOUS AI AGENTS

FROM AUTOMATION TO AUTONOMY

- ✓ Context-aware understanding
- ✓ Workflow Automation
- ✓ Executes actions across multiple applications
- ✓ Adapts to real-time context

OUTCOME

Dramatically reduces manual effort and accelerates mean time to resolution.

3. AIOPS (AI FOR IT OPS)

INTELLIGENCE EMBEDDED IN OPERATIONS

- ✓ Continuous monitoring
- ✓ Anomaly detection & root cause analysis
- ✓ Predictive insights & risk scoring
- ✓ Automated remediation & self-healing actions
- ✓ Closed-loop learning

OUTCOME

Prevents issues, minimizes downtime, and improves operational resilience.

4. BUSINESS AS CODE

OPERATIONALIZING PROCESSES AT SCALE

- ✓ Version-controlled workflows and policies
- ✓ Continuous integration & delivery
- ✓ Consistent governance, audit, compliance
- ✓ Rapid iteration and scalability

OUTCOME

Enables agility, consistency, continuous improvement across operations.

KEY BUSINESS IMPACTS OF AI-POWERED OPERATIONS

30–40%

Reduction in operational costs with intelligent automation

78%

Of organizations plan to increase investment in AI and automation for operations by 2026

90%+

Of IT leaders expect AI to be critical to scaling operations over the next 2 years

By unifying strong data foundations, autonomous agents, AIOps, and business-as-code, organizations can transform threat intelligence into a **self-improving**, **scalable**, and **outcome-driven** operational capability.

Source: IBM, 2025; Accenture, 2025; MnM Research and Analysis

The business impact of this transition is becoming increasingly measurable, with organizations reporting lower operational costs, increased investment in AI-driven operations, and growing recognition of AI as a critical enabler of future security operations.

STRATEGIC IMPLICATIONS

- ✓ **Intelligence is becoming operational.** Threat intelligence increasingly influences real-time security decisions rather than serving as a standalone analytical function.
- ✓ **AI requires an operating model.** Data, automation, analytics, and governance must work together to deliver reliable outcomes.
- ✓ **Agentic AI extends security capacity.** Agentic AI is expanding investigative capacity and accelerating decision support.
- ✓ **AIOps enables continuous intelligence.** AIOps enables intelligence to be embedded directly into monitoring, response, and remediation workflows.
- ✓ **Governance becomes a competitive advantage.** Policy-driven execution and repeatability are becoming essential as AI adoption scales.

▪ REQUIREMENT FOR INTEGRATED SECURITY OPERATIONS AND CROSS-DOMAIN VISIBILITY

According to Flexera's 2025 State of the Cloud Report, organizations increasingly operate hybrid and multi-cloud environments, utilizing an average of more than two public cloud providers and nearly three private cloud environments. At the same time, enterprises continue to expand their security technology portfolios, with large organizations often deploying 40–80 security tools across different operational functions.

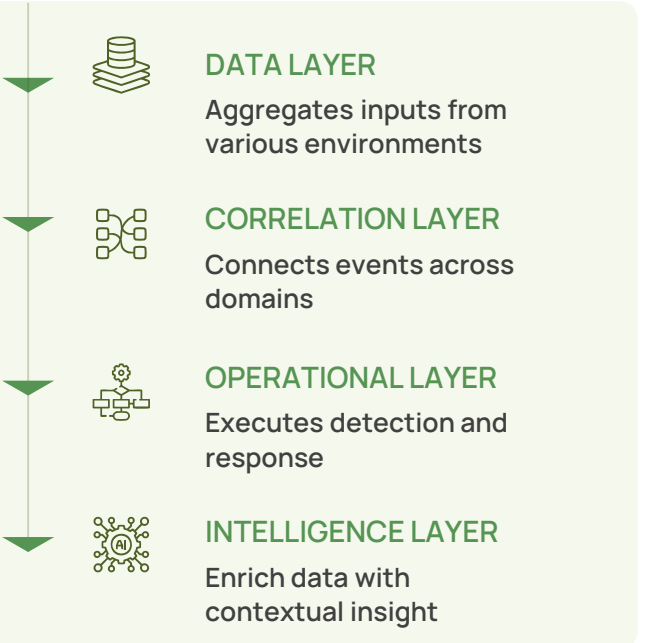
This fragmentation creates disconnected data streams, inconsistent context, and isolated workflows, making it difficult to correlate threats across environments. As a result, organizations are increasingly adopting integrated security operating models that unify telemetry, intelligence, and response processes within a common operational framework.

To address this, organizations must adopt an architecture that connects data ingestion, correlation, and response into a continuous workflow. This ensures that intelligence is not siloed but is consistently shared and operationalized across environments. It enables:

Operational Benefits of Integrated Intelligence Operations:

- Eliminates visibility gaps by consolidating telemetry across cloud, identity, endpoint, network, and OT environments.
- Improves threat prioritization through cross-domain correlation and contextual intelligence.
- Accelerates security decisions by embedding intelligence directly into detection, investigation, and response workflows.
- Reduces response latency through coordinated execution across security functions and domains.

The framework below illustrates how intelligence moves from raw telemetry to operational action through a continuously connected decision pipeline.



Leading organizations are embedding intelligence directly into detection, investigation, response, and governance workflows. The progression from data aggregation and event correlation to contextual intelligence and operational action illustrates how modern security teams are transforming fragmented telemetry into coordinated decision-making.

The ability to continuously convert data into context, context into decisions, and decisions into action is becoming a key differentiator for improving operational efficiency, reducing analyst workload, and strengthening cyber resilience.

BEYOND ARCHITECTURAL INTEGRATION, AI-INTEGRATED THREAT INTELLIGENCE MODEL ENABLES SEVERAL KEY OPERATIONAL CAPABILITIES:

End-to-End Threat Lifecycle Visibility

Enable continuous tracking of threats across entry, movement, and impact-stages, ensuring complete coverage across the attack lifecycle.

- Entry point detection
- Lateral movement tracking
- Impact stage visibility
- Continuous threat monitoring

Continuous threat monitoring

Provide synchronized visibility across endpoint, network, cloud, and identity environments for unified situational awareness.

- Endpoint and network correlation
- Cloud and identity visibility
- Unified monitoring across domains

Seamless Intelligence-to-Action Execution

Ensure insights generated through correlation and analysis are directly operationalized into detection and response actions.

- Automated threat prioritization
- Direct response execution
- Reduced response latency
- Integrated workflows

Reduced Operational Fragmentation

Eliminate reliance on disconnected tools by enabling a unified workflow across detection, investigation, and remediation processes.

- Tool consolidation
- Unified security workflows
- Reduced operational complexity
- Streamlined investigation

Consistent Context-Driven Decision-Making

Enable faster and more accurate prioritization through a centralized and enriched view of threats across environments.

- Centralized threat context
- Improved prioritization accuracy
- Faster decision-making
- Contextual intelligence insights

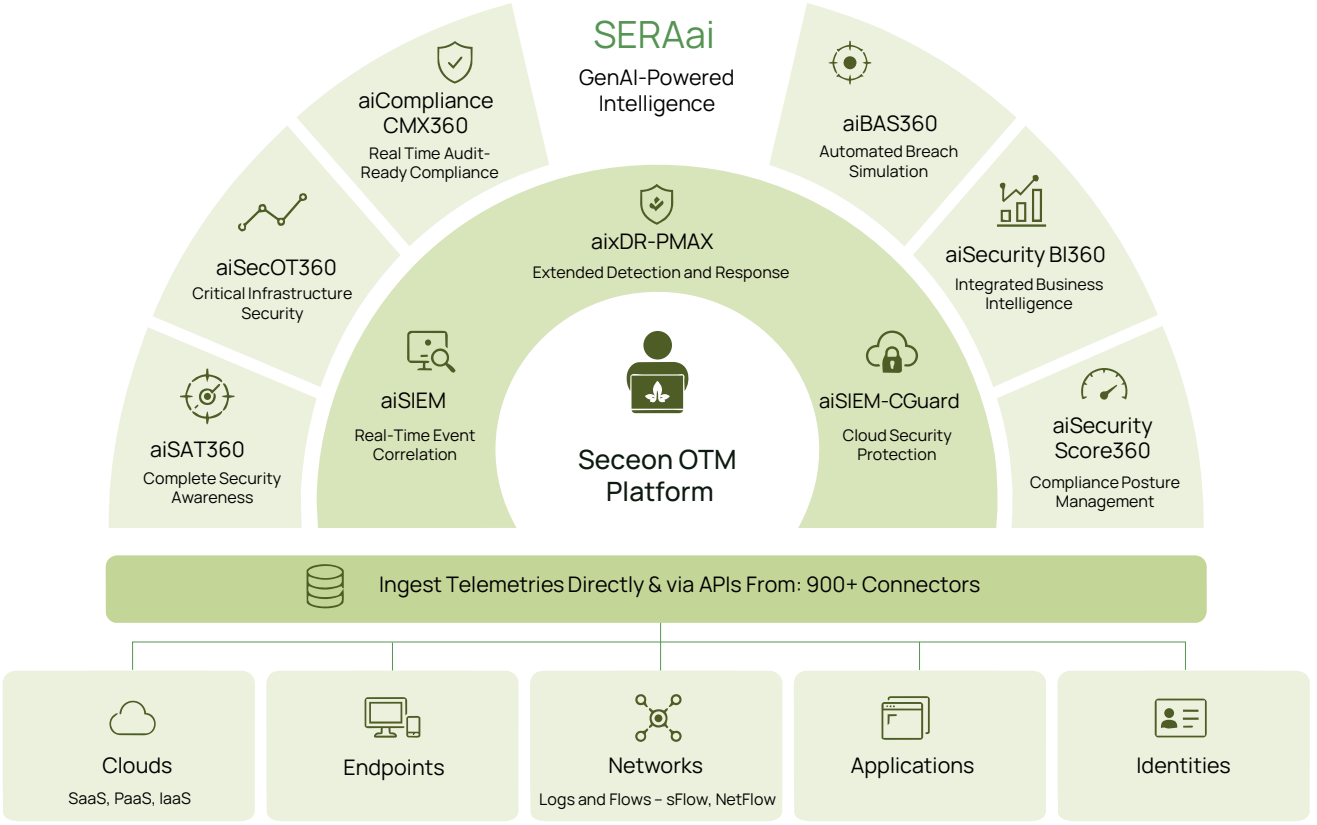
> MarketsandMarkets observes that the next generation of threat intelligence platforms is being evaluated not by the volume of indicators collected, but by their ability to operationalize intelligence across the security lifecycle. Organizations increasingly seek solutions that combine broad visibility, continuous monitoring, contextual risk analysis, workflow automation, and coordinated response capabilities within a unified operating model.
>
> This shift is enabling security teams to reduce operational complexity, improve analyst productivity, accelerate threat detection and remediation, and make more informed risk-based decisions. As threat volumes continue to rise and cybersecurity talent shortages persist, integrated and AI-enabled threat intelligence architectures are expected to become foundational components of modern security operations.



SECEON'S APPROACH TO AI-DRIVEN OPERATIONAL THREAT INTELLIGENCE

Seceon's Open Threat Management (OTM) Platform is a comprehensive, AI-powered security ecosystem that consolidates ten specialized capabilities, including SIEM, XDR, SOAR, NDR, UEBA, and OT security, into a single cohesive operational framework.

The platform is purpose-built to eliminate tool sprawl, unify fragmented security telemetry, and enable organizations to detect, analyze, and respond to threats across their entire digital infrastructure in real time, within a continuous, self-reinforcing intelligence cycle.



Source: Seceon Open Threat Management (OTM) Platform

A UNIFIED, INTEGRATED CAPABILITY ARCHITECTURE

The Seceon OTM platform is designed to address one of the most persistent challenges in modern security operations: the fragmentation of threat intelligence, detection, investigation, response, and compliance workflows across multiple tools.

By consolidating these capabilities within a shared intelligence architecture, OTM enables security teams to correlate events across environments, enrich alerts with contextual intelligence, and automate response actions from a single operational framework. The platform's AI-powered analytics continuously process security telemetry to identify anomalous behavior, prioritize high-risk threats, and reduce investigation effort.

Combined with integrated XDR, SOAR, UEBA, and compliance capabilities, this unified approach helps organizations improve threat visibility, reduce false positives, accelerate incident response, and strengthen overall cyber resilience while simplifying day-to-day security operations.



OTM CAPABILITIES	FUNCTION	OPERATIONAL ROLE
aiSIEM	ML Event Correlation	Core detection engine; processes 1.6T events/day, 95% false-positive reduction, 7-year forensic retention.
aiSIEM-CGuard	Cloud Security Platform	Extends aiSIEM into cloud environments; manages cloud posture and automates cloud threat containment.
aiXDR-PMax	Extended Detection & Response	Unified detection across endpoints, networks, cloud, and identity; correlates multi-domain attack chains.
SOAR 4.0	Automated Orchestration	GenAI-powered playbooks across 950+ integrations; resolves 70% of incidents automatically in <5 seconds.
UEBA	Behavioral Analytics	Models' user/entity baselines; surfaces insider threats, identity misuse, and compromised credentials.
aiSecOT360	OT/ICS Security	Agentless visibility across 70+ industrial protocols; NERC CIP and IEC 62443 compliant.
aiSecurity BI360	Security Business Intelligence	Executive dashboards, breach analytics, and board-level security reporting.
aiCompliance CMX360	Compliance Automation	Automates 90% of compliance reporting across SOC 2, ISO 27001, NIST, HIPAA, PCI-DSS, NIS2, DORA.
aiSecurity Score360	Posture & Risk Scoring	Real-time compliance scoring and vendor posture monitoring for continuous risk quantification.
aiBAS360	Breach Attack Simulation	Continuously validates defensive controls against real-world attack techniques.
SERAai	GenAI Intelligence	Synthesizes cross-domain signals into threat narratives; 95% audit prediction accuracy.

Source: Seceon

Security leaders are increasingly consolidating security operations capabilities to reduce tool sprawl, improve operational visibility, and accelerate incident response. By integrating threat intelligence, detection, analytics, automation, and compliance into a unified architecture, Seceon OTM enables organizations to operationalize security intelligence more efficiently while reducing the complexity of managing multiple standalone platforms.

THE FOUR OPERATIONAL PILLARS OF THE OTM PLATFORM

The OTM platform follows a closed-loop operational model organized across four interconnected pillars — Protect, Detect, Remediate, and Evolve. Each pillar is purpose-built to address a distinct phase of the security lifecycle while feeding intelligence continuously into the others, ensuring that the platform's defensive posture evolves in real time alongside the threat landscape.

PROTECT

Forms the security foundation by ensuring continuous visibility into assets, configurations, and organizational risk posture.

- Security Posture & Asset Management — continuous monitoring of assets, vulnerabilities, misconfigurations, and exposure risks across the enterprise.
- Security Analytics & Compliance Reporting — real-time analytics that support threat visibility while automating compliance and audit readiness.
- Container & Database Security — monitoring of modern application environments for suspicious activity within containers and databases.
- Comprehensive Visibility — unified view across networks, endpoints, and cloud environments for full situational awareness.

REMEDIATE

Automates and orchestrates response actions to neutralize threats in real time — reducing mean time to respond to under five minutes.

- SOAR 4.0 — automated incident response orchestration with GenAI-powered playbooks executed across 950+ tool integrations in under five seconds.
- Endpoint Detection & Response (EDR) — real-time detection and automated containment of threats targeting endpoint devices and hosts.
- Real-Time Threat Containment - instant neutralization of active threats through automated policy enforcement and network segmentation.
- Dynamic Threat Containment - adaptive response to evolving threats through continuously updated containment policies informed by live intelligence.

EVOLVE

Continuously strengthens the organization's security posture through advanced analytics, threat hunting, and next-generation capabilities.

- Comprehensive Network Security — foundational network protections encompassing perimeter defense, segmentation, and traffic analysis at scale.
- Cloud & SaaS Security - protection of cloud environments and SaaS applications through continuous monitoring of configurations and access behavior.
- Forensic Analysis & Threat Hunting — retrospective investigation of security events combined with proactive threat hunting across the full historical dataset.
- Next-Gen SIEM (NG-SIEM) - AI-enhanced event management delivering intelligent correlation, anomaly detection, and adaptive security operations.

DETECT

Applies AI-driven analytics across all data sources to identify threats in real time — from known attack signatures to novel behavioral anomalies.

- Threat Intelligence & Threat Hunting - integration of 70+ threat intelligence sources to proactively identify and correlate emerging attack patterns.
- Network Detection & Response (NDR) - real-time analysis of network flows to identify C2 communications, lateral movement, and data exfiltration.
- Intrusion Detection System (IDS) - detection and prevention of unauthorized access attempts across network and endpoint perimeters.
- UEBA - ML-powered behavioral analytics to identify abnormal user and entity activity indicative of insider threats or compromised accounts.

Source: Seceon

CLOSED-LOOP INTELLIGENCE MODEL

Effective threat intelligence programs create value only when intelligence continuously informs detection, investigation, and response activities. The closed-loop operating model enables security teams to apply lessons learned from active incidents to future threat detection strategies, thereby improving detection accuracy, reducing response delays, and strengthening organizational resilience over time.

COMPLIANCE & GRC EXCELLENCE

Recent regulations such as NIS2, DORA, SEC cyber disclosure requirements, and evolving critical infrastructure mandates are increasing pressure on organizations to maintain continuous visibility into security controls and compliance posture. Seceon's OTM Platform addresses this shift through aiCompliance CMX360, an integrated compliance automation engine that delivers real-time, audit-ready compliance coverage across 40+ global and industry-specific regulatory frameworks. By building compliance evidence directly from live security posture data, the platform eliminates the historical trade-off between operational security and regulatory adherence.

GOVERNMENT & CRITICAL INFRASTRUCTURE FRAMEWORKS

For government agencies and critical infrastructure operators, the OTM platform provides native, automated compliance coverage across the most demanding regulatory standards. The platform maps security telemetry and control evidence directly to NIST CSF 2.0, NIST 800-53, and NIST 800-66 for federal security requirements, as well as ISO 27001 for information security management and NIST 800-171 for controlled unclassified information protection. Compliance with GDPR, CMMC 2.0, FedRAMP, CJIS, and FISMA is maintained through continuous, automated evidence collection, reducing audit preparation time from 2 weeks to under 2 hours.

INDUSTRY-SPECIFIC & PRIVACY COMPLIANCE

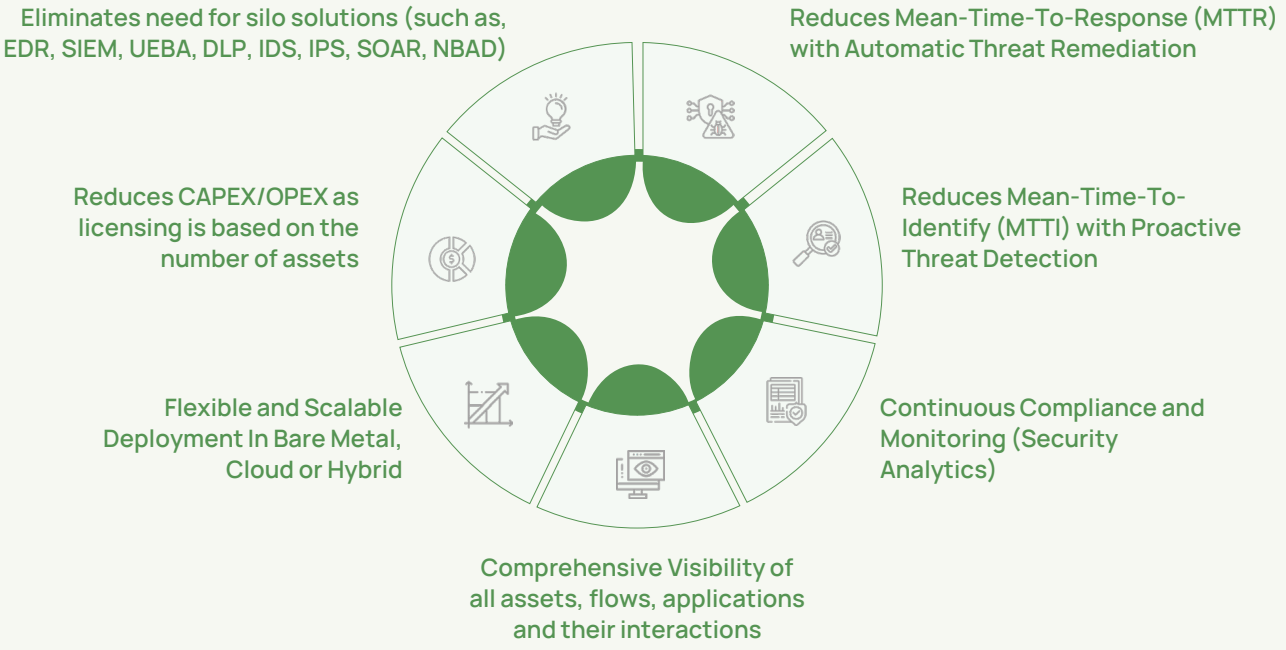
FINANCIAL SERVICES	HEALTHCARE & CRITICAL INFRA.	EUROPEAN & GLOBAL
▪ PCI-DSS v4.0 ▪ SOC 2 Type II ▪ GLBA ▪ FFIEC ▪ NYDFS ▪ SWIFT	▪ HIPAA ▪ NERC-CIP ▪ IEC 62443 ▪ CIS Controls ▪ SDX Controls	▪ NIS2 ▪ DORA ▪ GDPR ▪ ISO 27001 ▪ FISMA ▪ FedRAMP

PRIVACY STANDARDS | PRIVACY SHIELD | VCDPA | LGPD | CPA | PIPEDA | CCPA/ CPRA | GDPR

Powered by SERAai, the compliance engine achieves 95% audit prediction accuracy, enabling organizations to anticipate audit findings and address control gaps proactively — cutting audit timelines by up to 75% and reducing findings by 65%. The platform leverages accumulated SIEM telemetry to auto-complete up to 80% of compliance framework requirements from day one, dramatically accelerating time-to-compliance for newly regulated organizations.

The compliance automation layer operates without additional hardware deployment — activated directly on top of the existing aiSIEM infrastructure — delivering unified compliance visibility through pre-built dashboards, automated control validation, and continuous multi-framework monitoring. Organizations maintain simultaneous compliance across all applicable frameworks with zero manual overhead and complete audit trail preservation.

✓ OTM PLATFORM OUTCOMES AND VALUE REALIZATION



Source: Seceon

Organizations are increasingly evaluating security platforms based on measurable operational outcomes rather than feature breadth alone. Capabilities such as automated threat detection, integrated compliance monitoring, and AI-driven investigation workflows help reduce manual effort while improving response consistency. By consolidating security operations, compliance, and threat intelligence within a unified platform, organizations can strengthen cyber resilience while simplifying operational management.

POWERING SCALABLE THREAT INTELLIGENCE THROUGH PARTNERSHIPS AND ECOSYSTEM

✓ STRATEGIC PARTNERSHIPS

As threat environments become increasingly interconnected, organizations are seeking security platforms that can integrate intelligence, detection, response, and managed services within broader cybersecurity ecosystems. Strategic partnerships enable organizations to accelerate deployment, extend operational coverage, and access specialized expertise without increasing internal complexity.

Seceon collaborates with system integrators, distributors, and managed security service providers (MSSPs) to extend its platform capabilities into diverse operational environments and geographies. These partnerships are not limited to technology integration; they also focus on operationalizing cybersecurity services, enabling organizations to adopt advanced threat intelligence capabilities without the complexity of building in-house infrastructure.

GLOBAL MSSP ENABLEMENT THROUGH CALCULUS NETWORKS

Through its partnership with Calculus Networks, Seceon enables the delivery of next-generation cybersecurity services on a global scale. This collaboration focuses on integrating the OTM platform into managed service offerings, allowing enterprises to access continuous monitoring, threat detection, and response capabilities without significant internal resource investments.

EUROPEAN MARKET EXPANSION VIA HAMMER DISTRIBUTION

In collaboration with Hammer Distribution, Seceon launched "SENSA," an always-on managed security service across the UK and Europe. This initiative highlights the platform's adaptability within distributor-led ecosystems, enabling regional partners to deliver 24/7 threat monitoring and response services powered by Seceon's OTM capabilities.

INTEGRATED CYBERSECURITY SERVICES WITH EXPRIVIA

Seceon's partnership with Exprivia combines its OTM platform with Exprivia's cybersecurity service expertise to deliver fully integrated security solutions. This collaboration emphasizes the convergence of platform technology with managed services, enabling organizations to benefit from both advanced analytics and operational execution.

✓ PARTNER ECOSYSTEM

hgs · TRIGENT · Tech Mahindra · GMR · network techlab (Adding Values to Work) · smsam · NETSYNC · SAMAY INFOSOLUTIONS (SAFEGUARDING YOUR FUTURE) · kyndryl · MindCypher · exprivia · VisioNet · airtel · IP Clarity · GAVS · ZyBiSys (keep innovating...!) · ACCEL IT SERVICES (a division of Accel Limited)

Source: Seceon

SECEON'S ENABLED USE CASES AND CUSTOMER SUCCESS STORIES

Critical infrastructure operators continue to face increasing pressure from ransomware groups, supply chain threats, and nation-state adversaries. As OT and IT environments become more interconnected, organizations are prioritizing intelligence-driven security operations that improve visibility and reduce response times.

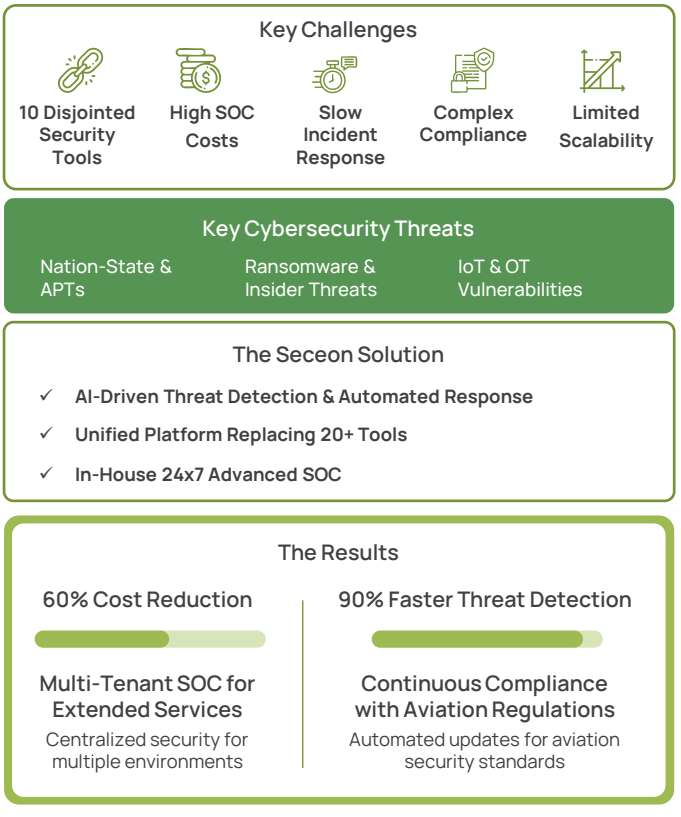
This section provides insights into the value of Seceon's OTM platform, which is best demonstrated through real-world use cases in complex, high-risk environments.

POWER AND ENERGY

Multiple real-world cyber incidents in the energy sector highlight how disruptions in IT environments can directly impact operational systems and critical infrastructure. The Colonial Pipeline ransomware attack forced a shutdown of fuel supply operations, while large-scale grid disruptions such as the Iberian blackout demonstrated how failures across interconnected digital systems can cascade into regional outages. Water utilities and petrochemical facilities have also been exposed to credential-based attacks and OT-targeted malware such as TRITON.

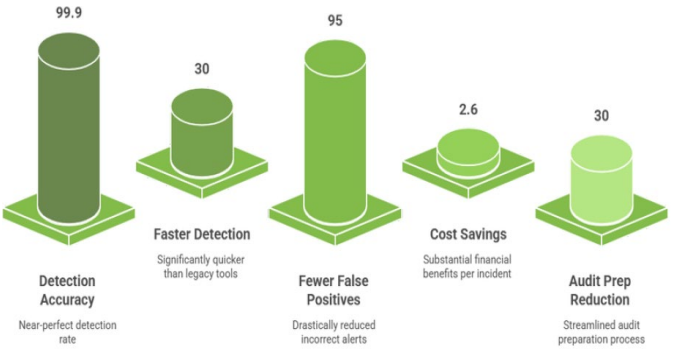
Seceon's Open Threat Management (OTM) platform addresses these risks by enabling unified visibility across IT, OT, and IoT environments. Through AI-driven behavioral analytics, correlated threat detection, and automated response, the platform identifies anomalies within seconds and enables immediate containment before operational disruption occurs.

TRANSPORTATION AND RAIL SYSTEM



Source: Seceon

The measurable outcomes demonstrate strong operational and financial impact. Organizations achieved 99.9% detection accuracy, 95% reduction in false positives, and significantly faster detection timelines compared to legacy systems. Additionally, automated responses and shorter breach lifecycles contribute to USD 2.6M+ in cost savings per incident, along with improved compliance readiness and shorter audit timelines.



Source: Seceon

One of the world's largest airports faced significant cybersecurity challenges due to its reliance on a fragmented architecture comprising more than 10 standalone security tools and an outsourced 24/7 Security Operations Center. This setup resulted in high operational costs, delayed incident response, limited scalability, and lack of unified visibility across critical airport systems such as passenger data platforms, IoT-enabled baggage systems, and operational infrastructure.

By deploying Seceon's AI-driven Open Threat Management (OTM) platform, the airport consolidated its entire security ecosystem into a single unified platform. This enabled real-time threat detection, automated incident response, and centralized monitoring across all systems. A key transformation was the establishment of an in-house 24/7 Security Operations Center, eliminating dependency on third-party providers and improving response efficiency.

Outcomes:

The transformation delivered measurable outcomes, including a 60% reduction in cybersecurity costs, 90% faster threat detection, and significantly improved compliance management through automation. Additionally, the airport leveraged the platform's multi-tenant capabilities to extend cybersecurity services to other critical infrastructure entities, creating new revenue opportunities.

HEALTHCARE AND PHARMACEUTICAL

Englewood Health faced critical cybersecurity limitations due to reliance on a traditional SIEM system that functioned primarily as a log aggregator, lacked real-time analytics, and required extensive manual effort. The complexity of healthcare environments—including IoMT devices, legacy systems, and strict regulatory requirements—further increased exposure to ransomware, insider threats, and advanced persistent threats.

By implementing Seceon's AI-driven aiSIEM platform, the organization transformed its cybersecurity operations through real-time event processing, behavioral analytics, and integration with multiple threat intelligence sources. The platform enabled automated response workflows, continuous compliance monitoring, and improved visibility across healthcare infrastructure, including medical devices and hybrid IT environments.

The results were substantial across operational, technical, and financial dimensions. The platform analyzed 1.16 billion events and identified 80 million threat indicators, achieving a 95% reduction in false positives and 90% faster detection and response. Additionally, manual investigation time was reduced by 70%, compliance preparation efforts decreased by 85%, and overall cybersecurity costs were reduced by 40–60%, significantly improving operational efficiency and resilience.

Key Challenges

Traditional SIEM Limitations
Basic log aggregation without advanced analytics

Complex Healthcare Environment
IoMT devices, legacy systems, hybrid architecture

Regulatory Compliance
HIPAA, HITECH compliance requirements

Resource Constraints
Limited staff, alert fatigue, manual processes

Healthcare Threat Landscape

- Ransomware campaigns (WannaCry, Ryuk) targeting healthcare infrastructure
- Insider threats and supply chain attacks via medical device vendors
- State-sponsored APT groups increasingly focusing on healthcare data

Seceon Solution

IoMT Device Discovery
Medical device vulnerability assessment and monitoring

AI/ML Analytics
Behavioral baselines without manual rule writing

MITRE ATT&CK
Healthcare-relevant attack technique mapping

HIPAA Automation
Automated compliance reports and audit trails

Proven Results

95%	70%	82%	40-60%
Faster threat detection and response	Less manual investigation time	Reduced compliance prep time	Lower total ownership costs

Source: Seceon



CONCLUSION

Threat intelligence is entering a new phase—one where success is measured not by the amount of intelligence collected, but by how effectively that intelligence influences security decisions and operational outcomes.

As attack techniques become more automated, identity-centric, and difficult to detect using traditional methods, organizations are rethinking how intelligence is integrated into security operations. The focus is shifting toward continuous intelligence workflows that improve threat prioritization, accelerate investigations, and support faster response actions. In this environment, organizations that can connect intelligence, analytics, automation, and response within a unified operating model will be better positioned to manage cyber risk, reduce operational complexity, and strengthen resilience against emerging threats. Platforms such as Seceon's Open Threat Management (OTM) framework are helping organizations operationalize this approach by transforming intelligence into measurable security outcomes.

Looking ahead, several key trends will continue to shape the future of Threat Intelligence:

Identity-Centric Threat Detection

- Identity is becoming the primary attack surface
- Increased focus on behavioral and access-based analytics

Agentic AI in Security Operations

- AI-assisted investigation and triage
- Autonomous response recommendations

Cyber-Physical Threat Visibility

- Convergence of IT, OT, IoT, and cyber-physical systems
- Unified monitoring across critical infrastructure

Threat Intelligence Operationalization

- Intelligence directly informing detection and response
- Reduced dependence on standalone threat feeds

Continuous Compliance & Risk Monitoring

- Real-time compliance validation
- Compliance integrated into security operations workflows

Looking ahead, the organizations that derive the greatest value from threat intelligence will be those that successfully integrate intelligence into everyday security operations rather than treating it as a standalone function. As AI, automation, and cross-domain visibility continue to mature, threat intelligence will increasingly serve as a real-time decision support capability that enables faster, more adaptive, and more resilient cybersecurity operations.



Contact

Sayali Saste
Manager

sayali.saste@marketsandmarkets.com

Vidhu Rawat
Assistant Manager

vidhu.rawat@marketsandmarkets.com

Akshita
Research Analyst

akshita01@marketsandmarkets.com



MARKETSANDMARKETS™

About MarketsandMarkets

Founded in 2009, MarketsandMarkets (MnM) was built on a forward-looking vision: to identify and monetize the next wave of business opportunities embedded within global disruption. While others discussed megatrends like AI, 3D printing, IoT, and robotics, MnM saw a deeper insight—the unrealized revenue potential these shifts could unlock across industries.

MnM anticipates a USD 25 trillion revenue transformation in the B2B economy by 2030—driven not just by technology, but by macroeconomic shocks, policy shifts, climate pressures, and geopolitical flashpoints. Today, MnM tracks both emerging innovations and global dislocations—including landmark disruptions such as the 2025 US reciprocal tariffs—to help clients decode complexity, quantify exposure, and seize asymmetric growth opportunities ahead of competitors.

Over the past 13+ years, MnM has worked with 10,000+ clients across 30+ sectors, delivering over USD 140 billion in revenue impact. We've evolved from a market research publisher to a growth-enablement partner, powered by a 'GIVE Growth' philosophy and a 1,500+ strong team driven by outcome, not output.

Our commitment to strategic foresight and execution has earned us recognition from Forbes as one of America's Best Management Consulting Firms, and we remain the only India-origin firm on that prestigious list. What makes us a blue-ocean partner is our proprietary platform: Knowledge Store™—an AI-enabled, primary-research-driven market intelligence engine built to empower CXOs, strategy teams, and growth leaders to identify hidden inflection points and future profit pools in real-time.

