MARKETSANDMARKETS™

seceon
SECURITY FOR EONS

AI-NATIVE XDR FOR MODERN SOC OPERATIONS

Enabling Unified, Intelligence-driven Security Operations With

Seceon's AI-native XDR Platform.



EXECUTIVE SUMMARY

From Alert Overload to Intelligence Deficit: The Urgent Need for AI-Native SOC Transformation

The modern threat landscape is evolving faster than ever, driven by automation, AI-powered adversaries, and increasingly complex digital environments. At the same time, SOC teams are expected to defend sprawling infrastructures spanning network, endpoint, cloud, and hybrid environments, often with fragmented tools and limited resources.

IBM's Cost of a Data Breach Report 2025 found that the global average cost of a data breach reached $ 4.44 million, while organizations still require an average of 241 days to identify and contain a breach, highlighting the persistent challenges of detection and response at scale. Incidents involving compromised credentials cost organizations an average of $ 4.67 million and take even longer to contain. These figures underscore a systemic challenge: enterprise SOCs are overwhelmed not by insufficient investment, but by operational complexity, fragmented visibility, and the growing need for intelligent automation and correlation across security environments.

SOC UNDER PRESSURE — BY THE NUMBERS

241 Days Breach Lifecycle	Average Detection & Containment Time.
$4.44 Mn Average Breach Cost	Average global cost of a data breach in 2025.
4.8 Mn+ Roles Unfilled Cybersecurity Talent Shortage	Global workforce gap limits SOC capacity.
67% Ignored Alerts Analyst Burnout	Security alerts are deprioritized due to limited analyst capacity.

Source: IBM Cost of a Data Breach 2025 | ISC2 Cybersecurity Workforce Study| MnM Research and Analysis

MarketsandMarkets research indicates the SOC operational crisis is not primarily a technology problem; it is an architecture and intelligence problem. Despite record security spending, detection and response performance continue to deteriorate because organizations accumulate point tools without adding correlation intelligence. The transition to AI-native, unified security operations represents the single most impactful security investment decision for enterprise CISOs over the next three years.

This transition is expected to be a defining trend in the security industry over the next five years. MarketsandMarkets projects the global XDR market to grow from USD 7.9 billion in 2025 to USD 30.86 billion by 2030, at a CAGR of 31.2%. Organizations that invest in AI-Native XDR platforms today will be better positioned to overcome SOC inefficiencies, reduce operational complexity, and lead the next generation of intelligence-driven, outcome-focused security operations

The core issue is not just the volume of threats, but the inability to convert vast amounts of security data into actionable, prioritized intelligence. Traditional SIEM and EDR approaches, built on isolated telemetry and siloed data, are no longer sufficient to keep pace with modern attack techniques or operational scale. This is driving a shift toward AI-Native XDR, where security operations are built on unified data, intelligent correlation, and real-time response.

Seceon's aiXDR platform represents a practical and proven approach to modernizing SOC operations. Designed to unify detection and response across network, endpoint, and cloud environments, Seceon leverages AI-driven correlation, behavioral analytics, and large-scale data processing to deliver real-time, actionable intelligence.

As cyber threats continue to evolve and environments grow in complexity, adopting an AI-native, unified, and outcome-driven security operations model is no longer optional; it is essential for building resilient, future-ready SOC capabilities.

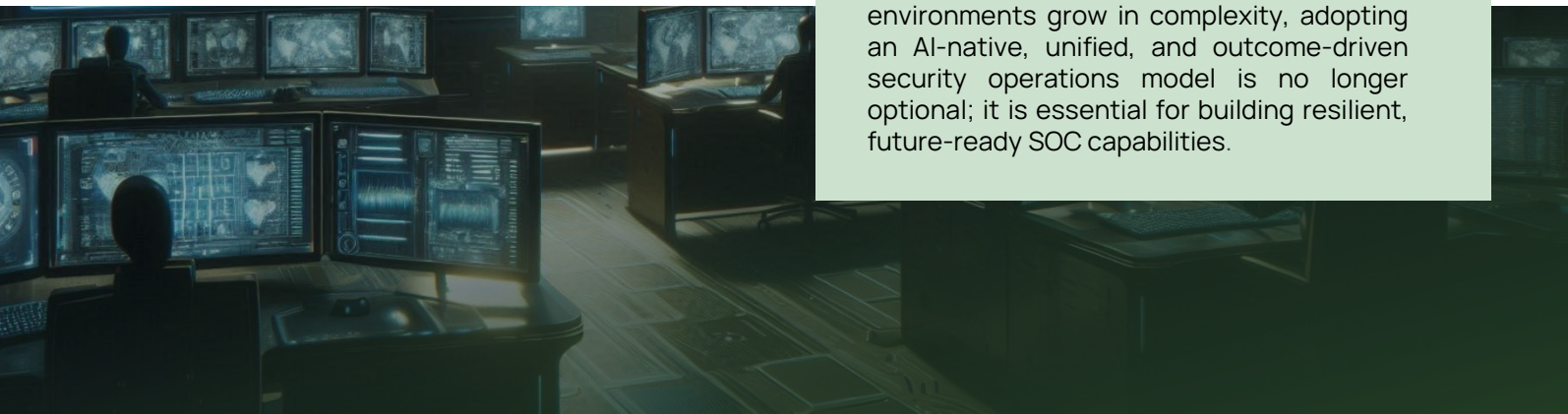


TABLE OF CONTENTS

Chapter 01 — The Core Problem — 04

Chapter 02 — Bridging the Gap: Why SOC Models Must Evolve to AI-Native XDR — 05-07

Chapter 03 — The Seceon Perspective: Enabling Modern SOC Operations with **aiXDR-PMax Platform** — 08-11

Chapter 04 — Conclusion — 12

This whitepaper examines the challenges of modern SOC operations driven by fragmented architectures, alert fatigue, and increasing complexity across network, endpoint, and cloud environments. It highlights the need for unified, intelligence-driven security operations and the role of AI-native XDR in improving detection and response.

It outlines how **Seceon's AI-XDR** helps reduce operational burden, enhance detection accuracy, and scale SOC performance, with a focus on CISOs, SOC leaders, and technology decision-makers..

THE CORE PROBLEM

Fragmented Visibility, Alert Overload, and Poor Scalability Are Structurally Breaking SOC Effectiveness

Modern SOCs are not constrained by a lack of tools or data; they are constrained by their inability to operate effectively at scale. Despite significant investments, SOC teams continue to struggle with fragmented visibility, overwhelming alert volumes, and operational models that are struggling to keep pace with modern threats.

At the foundation of this problem is fragmented detection and response. Enterprises today operate with 10–30+ security tools across endpoint, network, cloud, and identity, each generating isolated alerts with limited context. This results in incomplete visibility, preventing security teams from reconstructing the full attack chain. Instead, analysts are forced into manual, cross-tool investigations, significantly slowing detection and response operations and measurements.

At scale, these inefficiencies translate into measurable business risk. Attackers exploit gaps between tools, move laterally across environments, and remain undetected for extended periods. This is reflected in the broader industry reality, where breaches continue to take months to detect and contain.

ALERT VOLUME

~250 Mn+

Large enterprises generate hundreds of millions of security events annually across hybrid environments

IGNORED ALERTS

67%+

Alerts are ignored or deprioritized due to capacity constraints

THREATS MISSED

~65 / year

In ~450,000 alerts/year environments, nearly 65 real threats remain uninvestigated

HIDDEN IN NOISE

~2-3%

Low-severity alerts contain confirmed incidents — real threats hide in noise

Figures represent industry averages and aggregated findings from SOC operations research across large enterprise environments

AS TELEMETRY VOLUMES GROW, SOC WORKFLOWS REMAIN HEAVILY DEPENDENT ON MANUAL PROCESSES

Analysts spend **25–30% of their time on manual triage and correlation**

Detection timelines increase as environments scale, leading to **67% longer detection times in poorly optimized SOCs**

Inefficiencies drive **45% higher incident response costs** due to delays and rework

Source: IBM Cost of a Data Breach 2025 | ISC2 Cybersecurity Workforce Study | MnM Research and Analysis

Despite record cybersecurity investments, organizations still require an average of 241 days to identify and contain a breach, while the global cybersecurity workforce gap has grown to ~4.8 million professionals. At the same time, security analysts spend 30–35% of their time on manual triage, investigation, and correlation activities, limiting their ability to focus on high-priority threats. These challenges suggest that the primary obstacle to SOC effectiveness is not visibility, but the ability to convert growing volumes of telemetry into actionable intelligence.

As environments become increasingly distributed across cloud, endpoint, identity, and OT domains, organizations that continue to rely on fragmented security tools and manual workflows are likely to face longer response times, higher operational costs, and greater analyst burden.

The next phase of SOC modernization will be driven by platforms that unify telemetry, automate investigations, and apply AI-driven analytics to improve detection accuracy and operational efficiency.



BRIDGING THE GAP: WHY SOC MODELS MUST EVOLVE TO AI-NATIVE XDR

From Alert-Heavy Operations to AI-Driven, Outcome-Oriented Security

KEY GAPS IN TRADITIONAL SOC AND SECURITY MODELS:

Lack of Contextual, Cross-Domain Visibility:

Over 75% of organizations cite visibility gaps across hybrid, multi-cloud, and distributed environments.

Manual, Non-Scalable SOC Operations:

Security analysts still spend approximately 30–35% of their time on manual alert triage, investigation, and correlation activities.

Alert Overload with Minimal Actionability:

SOCs continue to process millions of security events daily, while only 15–20% of alerts are considered actionable, creating significant analyst burden and response inefficiencies.

Delayed Detection and Response (High MTTD & MTTR):

Organizations require an average of 241 days to identify and contain a breach.

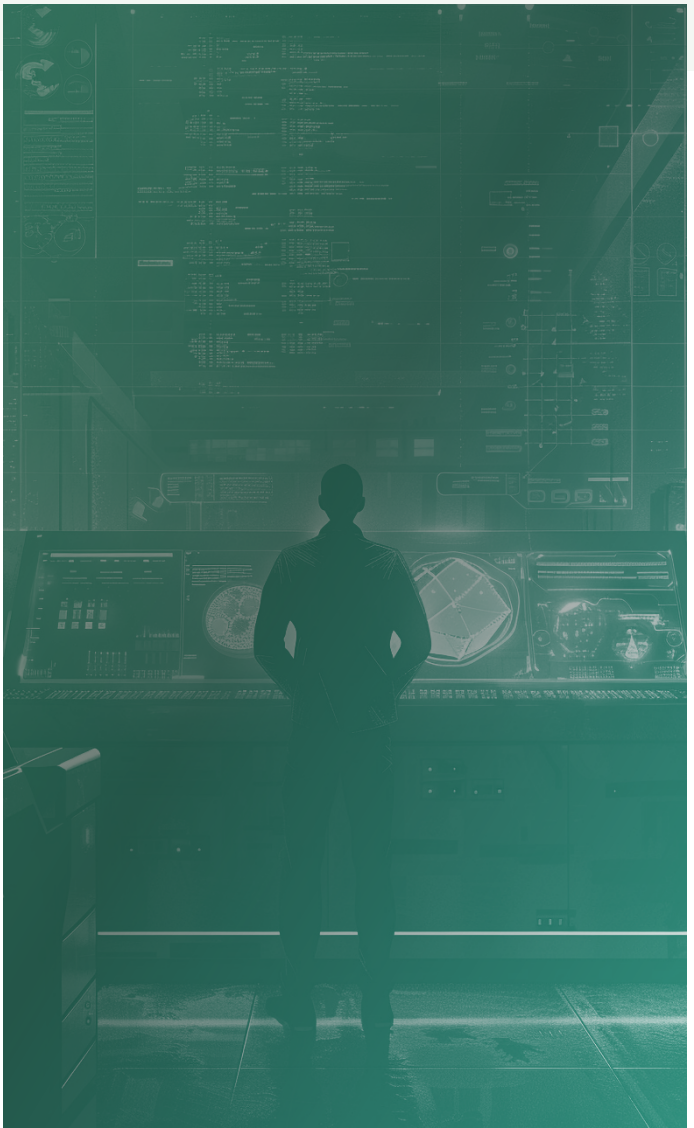
Detection Gaps Despite Tool Investments:

Despite growing security investments, only 2–3% of alerts typically warrant deeper investigation, making accurate prioritization and threat correlation critical.

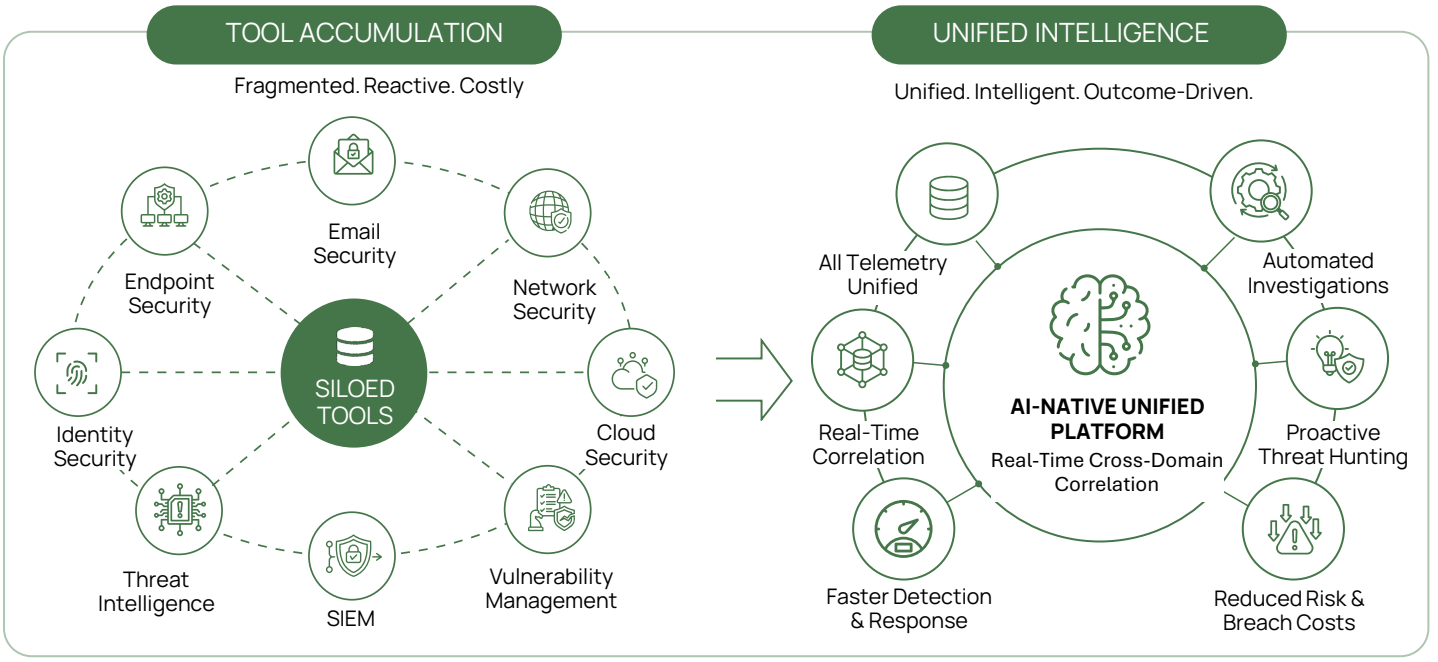
CrowdStrike's 2026 Global Threat Report revealed that the average eCrime breakout time dropped to 29 minutes in 2025, while the fastest observed breakout took just 27 seconds, leaving security teams with little time to respond before attackers establish deeper access. At the same time, AI-enabled attacks increased by 89% year-over-year, accelerating both the speed and scale of modern cyber threats. These developments are placing significant pressure on SOC teams to move beyond manual workflows toward AI-driven detection, investigation, and response capabilities.

The scale of the challenge is increasing rapidly as the attack surface expands. Enterprises now operate across hybrid cloud, SaaS, remote endpoints, identities, and APIs, which are significantly increasing the number of exposure points. At the same time, adversaries leverage AI-driven techniques to accelerate attacks, often compressing the time between initial access and lateral movement to under 30 minutes.

One of the key indicators of these gaps is detection efficiency. While alerts are generated continuously, only a fraction translates into meaningful outcomes. In many environments, only ~19% of alerts are considered actionable, while the rest contribute to operational noise. This inefficiency directly impacts Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), which remain unacceptably high in traditional SOC models. Delayed detection extends attacker dwell time, increasing the likelihood of data exfiltration, ransomware deployment, and business disruption.



MarketsandMarkets believes the root cause of SOC inefficiency is architectural, not budgetary. At the core of enterprise security, organizations are spending more on security tools than ever before, yet detection performance continues to deteriorate. This reflects an architectural mismatch. Security budgets are spent on point tools that add telemetry without adding correlation intelligence. Organizations that add more point solutions without unifying their data layer see 45% higher incident response costs due to delay and rework. Organizations must urgently shift from a 'tool accumulation' strategy to a 'unified intelligence' architecture.



Source: MnM Research and Analysis

The shift from **tool accumulation to unified intelligence** reflects one of the most significant changes occurring in modern security operations. Despite substantial investments in security technologies, many organizations continue to operate fragmented environments comprising separate tools for endpoint, email, network, cloud, identity, vulnerability management, and threat intelligence. This fragmentation creates operational silos, increases investigation complexity, and limits the ability of security teams to correlate threats across the attack surface

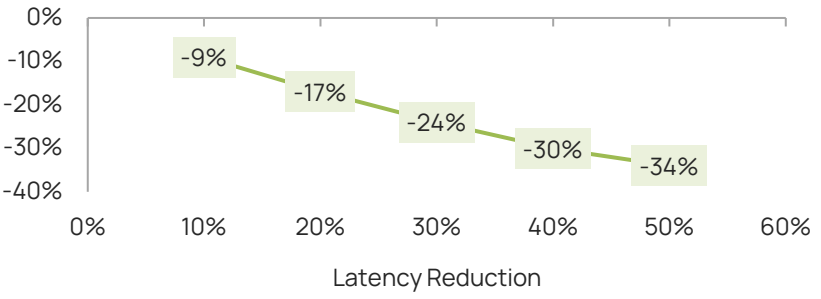
THE EVIDENCE IS CLEAR

Every 9% reduction in **DETECTION LATENCY**

correlates with a measurable reduction in **BREACH COSTS**

LOWER LATENCY. LOWER COSTS.

% Reduction in Breach Costs



Source: MnM Research and Analysis

Reducing detection latency directly lowers the impact of breaches by limiting the time attackers have to move laterally, exfiltrate data, and disrupt operations. The analysis shows that a 10% reduction in detection latency can reduce breach costs by approximately 9%, while a 50% reduction can lower costs by up to 34%. As attack timelines continue to shrink, organizations must move beyond manual investigations and fragmented tools toward AI-driven, automated security operations that enable faster detection and response.

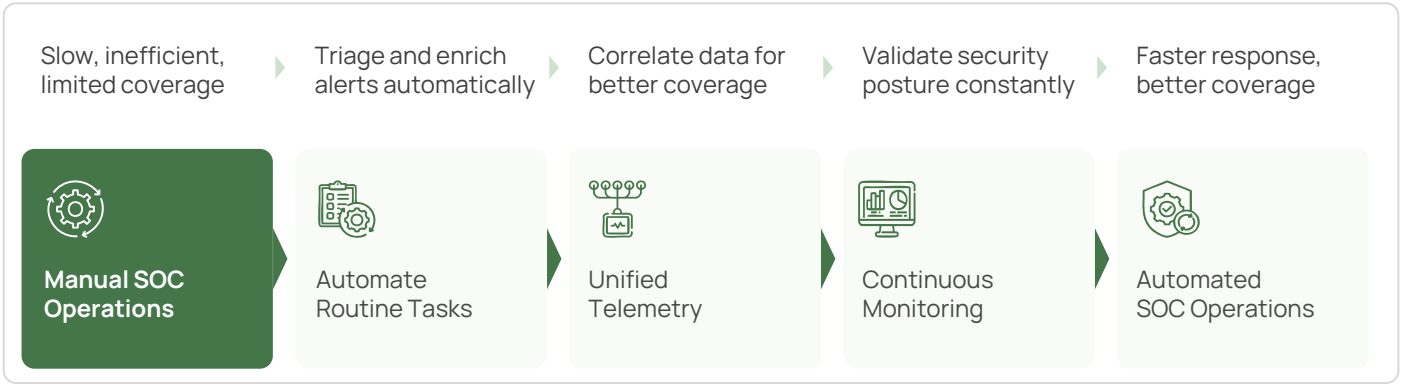
Organizations that reduce detection latency can significantly lower breach costs and improve operational resilience. As security environments become more distributed and attack timelines continue to compress, AI-native platforms such as **Seceon aiXDR-PMax** are increasingly enabling security teams to unify visibility, automate investigations, and respond to threats faster through intelligence-driven security operations.

SECURITY OPERATIONS EVOLUTION TIMELINE

GENERATION	WHY IT EMERGED	CAPABILITIES GAINED	REMAINING GAP
SIEM (2000S)	Need for centralized log management and compliance reporting	Centralized visibility, audit trails, regulatory compliance	High false positives, manual correlation, no behavioral context
EDR (2010S)	Rise of advanced endpoint threats requiring behavioral detection	Deep endpoint visibility, malware detection, device-level threat hunting	Endpoint-only; blind to network, cloud, and identity lateral movement
XDR (2019+)	Multi-domain attacks crossing endpoint, network, and cloud	Cross-domain correlation, unified incidents, reduced analyst pivoting	Vendor lock-in risks; limited automation; AI maturity varies significantly
AI-NATIVE XDR (2022+)	Machine-speed attacks exceeding analyst capacity	ML detection, automated investigation, UEBA, open telemetry, real-time response	Evolving; data governance and model transparency are emerging considerations

The evolution from SIEM to AI-Native XDR reflects a fundamental shift from visibility-focused security operations to intelligence-driven and increasingly autonomous security operations. While SIEM centralized data and EDR improved endpoint detection, modern attack surfaces spanning cloud, identity, network, SaaS, and OT environments have created a need for unified platforms capable of correlating telemetry and automating response at scale.

AUTOMATING SOC TASKS FOR FASTER RESPONSE



Source: MnM Research and Analysis

This is where the shift toward AI-native XDR is becoming critical. Unlike traditional models, AI-native XDR unifies telemetry across the entire attack surface, including endpoint, network, cloud, identity, and applications, and applies AI-driven correlation to convert fragmented signals into high-confidence incidents.

This transformation delivers measurable improvements:

- ✓ Automation of 80–90% of routine SOC tasks such as alert triage and enrichment
- ✓ Significant reduction in MTTD and MTTR, enabling faster containment
- ✓ Improved attack surface coverage through unified telemetry and correlation
- ✓ Enhanced validation of security posture through continuous monitoring and testing

MarketsandMarkets believes that by 2026, organizations at SOC Maturity Level 4–5 (AI-Assisted to Autonomous) will detect and contain breaches 60% faster than those operating at Level 1–2 (Reactive). The SOC modernization market will consolidate around platforms offering open telemetry ingestion, AI-native detection, and automated response, with AI-native XDR becoming the dominant architecture standard for enterprise security operations. CISOs who delay this transition face compounding operational risk as AI-enabled attack campaigns continue to shorten adversary breakout timelines.

✓ How Is Seceon Impacting This Shift?

For CISOs and security leaders, these challenges translate into critical operational pain points. Visibility remains fragmented across network, endpoint, and cloud environments, leading to gaps in detection. Teams must manage multiple tools, growing data volumes, and evolving threat vectors simultaneously. Remediation is delayed due to manual workflows and a lack of coordination across systems.

As a result, many organizations are rethinking how security operations should be structured. Rather than adding more tools that increase operational friction, there is a growing shift toward unified, AI-driven security models that reduce complexity, improve visibility, and enable faster, more consistent response. This shift is driving the adoption of AI-native XDR platforms, which simplify SOC operations while improving detection accuracy and operational resilience across increasingly distributed environments

Seceon's AI-XDR platform enables organizations to move toward outcome-driven SOC operations by combining AI-driven correlation with automated response and continuous monitoring. It helps improve attack surface coverage, reduce detection gaps identified through red team exercises, and lower MTTD and MTTR, all without increasing operational overhead. This allows SOC teams to convert high-volume telemetry into faster, more consistent, and actionable security outcomes.

How Seceon Adds Value?

- ✓ Up to **95% faster threat detection**
- ✓ Approximately **70% reduction in alert fatigue**
- ✓ Significant improvement in **MTTD and MTTR**, shifting detection timelines from hours to minutes

MarketsandMarkets believes the consolidation of detection, investigation, and response into a single AI-native platform, with open telemetry ingestion and behavioral analytics, is the defining architectural shift of the current SOC modernization cycle. Organizations evaluating XDR investments should prioritize platforms that demonstrate documented MTTD/MTTR improvements, MITRE ATT&CK coverage validation, and AI-driven automation rates above 60%.

How Seceon Supports Bridging the Gap with AI-Native XDR?

CHALLENGES	HOW AIXDR-PMAX SOLVES THEM
Limited visibility across hybrid environments	Unifies data from endpoints, networks, clouds, and OT
Slow detection and delayed response to advanced threats	Detects and neutralizes attacks in real time with AI-driven automation.
Overwhelmed security teams and alert fatigue	aiXDR-PMax correlates and prioritizes alerts using machine learning
Fragmented tools and disconnected data silos	Consolidates EDR, NDR, SIEM, and SOAR into one platform.
Ransomware and insider threats bypassing defenses	Detects hidden threats with continuous behavioral monitoring.

Source: Seceon

By consolidating telemetry across endpoints, networks, cloud, and OT environments, Seceon's aiXDR-PMAX provides comprehensive visibility across the attack surface. Its AI/ML, working through multimodal correlation and anomaly alerting, enables fast threat detection, automated responses, and effective alert prioritization, reducing manual effort and noise.

THE SECEON PERSPECTIVE: ENABLING MODERN SOC OPERATIONS

AI-Native XDR for Unified, Scalable, and Outcome-Driven Security

As organizations transition toward AI-Native security operations, the need for a platform that can deliver real-time visibility, intelligent correlation, and automated response across the entire attack surface becomes critical. According to Gartner's Market Guide for XDR, organizations seeking consolidated security operations should evaluate whether solutions offer native integration across endpoint, network, and cloud telemetry sources—a capability Seceon's aiXDR-PMAX delivers through 1,100+ pre-built data connectors.

✓ SECEON'S AIXDR-PMAX PLATFORM

Seceon's **aiXDR-PMax** delivers a defense-in-depth, AI-driven security platform. **aiXDR-PMax** unifies the capabilities such as EDR, EPP, DLP, and FIM into a single sub-50MB agent — natively integrated with the Seceon OTM platform's AI/ML engine, NDR, UEBA, ITDR, and SOAR 4.0. It ingests and processes large-scale telemetry from endpoints, networks, cloud, identities, applications, and IoT/OT environments to provide a holistic, context-rich view of threats.

There is no additional license, no separate console, and no integration tax. Organizations gain complete attack-chain visibility from endpoint to cloud, with automated response in under 90 seconds.

aiXDR PLATFORM PERFORMANCE

Measurable Outcomes, Day One

95% False positive reduction via Dynamic Threat Models	**<90s** Mean Time to Respond for known threat patterns
70% Automated incident response rate – no analyst touch	**1,100+** Pre-built data connectors normalizing to SEF format

Source: Seceon

The MITRE ATT&CK framework is the de facto industry standard for evaluating the breadth and depth of detection coverage. MarketsandMarkets recommends that enterprise XDR evaluations include explicit ATT&CK alignment testing across all 14 tactic categories. Seceon's aiXDR-PMAX demonstrates >96% coverage of the MITRE ATT&CK Enterprise framework, validated through structured red team exercises. By comparison, the industry-average SIEM/EDR stack covers 40–60% of the ATT&CK techniques. This gap represents the primary risk to detection coverage for organizations relying on legacy architectures.

✓ **aiXDR-PMax: Core Capabilities:**

- **Integration Capabilities:**

EDR & EPP INTEGRATION

Integrate aiXDR-PMax with your existing EDR and EPP solutions to centralize threat detection and automated response.

- ✓ Centralized Threat Data
- ✓ High-Fidelity Alerts
- ✓ Coordinated Remediation
- ✓ Unified Security Stack

CLOUD PLATFORM COMPATIBILITY

Protect workloads across AWS, Microsoft Azure, and Google Cloud with real-time monitoring and AI-driven threat detection.

- ✓ AWS Workload Protection
- ✓ Azure Monitoring
- ✓ Google Cloud Security
- ✓ Multi-Cloud Compliance

SIEM, SOAR & UEBA

Extend aiXDR-PMax with your SIEM, SOAR, and UEBA systems to correlate events, automate responses, and detect anomalies.

- ✓ Event Correlation
- ✓ Automated Responses
- ✓ Behavioral Anomaly Detection
- ✓ Actionable Intelligence

DEPLOYMENT

Broad OS Coverage. Minimal Resource Impact.

Windows	macOS	Linux
Win 10/11 & Server 2008+	macOS 12 Monterey and later	All major distributions

Cloud Workloads	AWS, Azure, GCP - CWPP + CSPM/CDR

Source: Seceon

- **Core Defense Capabilities:**

EDR + EPP | Endpoint Detection & Prevention

Ransomware protection | Zero-day prevention | Fileless detection | LOTL detection

Behavioral AI/ML detection (Dynamic Threat Models) layered over signature-based prevention. Catches zero-day exploits, fileless attacks, and LOTL techniques that evade traditional AV. Autonomous rollback via SOAR playbooks.

Memory Forensics & Process Chain Analysis

DLL injection detection | Rootkit discovery | Credential harvesting

Live memory acquisition across Windows, Linux, and macOS. Detects injected code, rootkits, DLL injection, credential harvesting, and process anomalies. Full parent-child process tree visualization with MITRE ATT&CK attribution.

DLP | Data Loss Prevention

USB device control | File exfiltration alerts | Policy enforcement

Monitors and controls data movement at the endpoint. USB and removable media device control, file exfiltration detection, and sensitive data policy enforcement. Integrated with network DLP for full-perimeter coverage without a separate console.

FIM | File Integrity Monitoring

Real-time file change tracking | Registry monitoring | Compliance-ready (PCI, HIPAA)

Natively built-in and GA today — not a third-party add-on. Tracks changes to critical system files, configurations, and registry keys in real time. Auto-correlates FIM events with user identity and process context for instant root-cause attribution.

Multi-Stage Attack Chain Reconstruction

Cross-domain correlation | Kill chain mapping | Transparent alert context

Correlates endpoint, network, identity, and cloud telemetry to reconstruct complete kill chains across all infrastructure domains. Transparent alert context shows every indicator - analysts understand full attack scope at a glance.

SOAR 4.0 | Automated Response via SOAR 4.0

950+ integrations | LLM playbook generation | No-code editor

Native integration with SOAR 4.0 delivers 70% automated incident response - endpoint isolation, process kill, account revocation, firewall policy push, and forensic evidence collection all triggered automatically within 90 seconds.

Source: Seceon

As organizations transition toward AI-native security operations, they increasingly require platforms that can deliver real-time visibility, intelligent correlation, and automated response across the entire attack surface simultaneously. MarketsandMarkets believes Seceon's aiXDR-PMAX represents a mature, production-ready implementation of this architecture for enterprise and MSSP environments, combining open telemetry ingestion, AI-native detection, behavioral analytics, and automated response in a single, consolidated platform.

THREAT COVERAGE -What aiXDR-PMax Detects and Stops

THREAT CATEGORY	DETECTION MECHANISM	MITRE ATT&CK TACTICS	RESPONSE
Ransomware	Anti-malware, DNS sinkholing, behavioral pattern matching, file entropy analysis	T1485, T1489, T1490	Automated
Fileless / In-Memory	Memory forensics + UEBA behavioral baselining, process chain anomaly detection	T1055, T1059, T1547	Automated
Living-off-the-Land	Detects abuse of PowerShell, WMI, PsExec, RMM tools (AnyDesk, TeamViewer)	T1218, T1570, T1021	Automated
Credential Theft	Memory scraping detection, LSASS access monitoring, Kerberoasting via aiTDR	T1003, T1558, T1555	Automated
Lateral Movement	NDR east-west detection + aiXDR host enumeration correlation	T1021, T1534, T1570	Automated
Zero-Day Exploits	Dynamic Threat Models with no prior signature required - behavioral anomaly scoring	T1190, T1203, T1068	Automated
Data Exfiltration	DLP module + network traffic volume anomalies + C2 beacon detection	T1041, T1048, T1071	Automated
Insider Threat	UEBA user risk scoring, pre-resignation behavior patterns, file staging detection	T1078, T1213, T1560	Analyst-assisted

✓ SECEON'S AIXDR-PMAX PLATFORM USE CASES

ENTERPRISE SOC

In-House Security Operations

Replace 3–5 point tools (EDR, SIEM, SOAR, DLP) with a unified platform. Reduce analyst workload by 70% through automation and near-zero false positives.

MSSP DELIVERY

Managed Security Services

Multi-Tier Multi-Tenancy (MtMt) enables MSSPs to manage hundreds of client tenants from a single console with per-client branding and isolated AI models.

REGULATED INDUSTRY

Healthcare, Finance, Government

7-year WORM log retention, FIM, automated compliance reporting for HIPAA, PCI-DSS, GDPR, NIST CSF, and ISO 27001 - all from the same platform.

OT/ICS

Industrial & Critical Infrastructure

Lightweight agent for IT endpoints correlates with aiSecOT360 passive OT monitoring — no agent on OT equipment. Unified IT/OT threat visibility.

CLOUD-FIRST

Hybrid & Multi-Cloud

Protects cloud workloads across AWS, Azure, and GCP with native CSPM/CDR integration. Single pane of glass across on-premises and cloud endpoints.

SMB VIA MSP

Smaller Organizations

Asset-based licensing with no per-GB ingestion fees or alert caps makes enterprise-grade XDR commercially viable for organizations of any size via MSP partners.

Source: Seceon

✓ INDUSTRY KPI BENCHMARK: SOC PERFORMANCE COMPARISON

KPI METRIC	TRADITIONAL SOC (Industry Average)	AI-NATIVE XDR (Platform Average)	SECEON aiXDR-PMAX (Reported Outcomes)
MEAN TIME TO DETECT (MTTD)	194 days (IBM 2024)	Hours to days	**35 minutes**
MEAN TIME TO RESPOND (MTTR)	64 days (IBM 2024)	Minutes to hours	**< 90 seconds (automated)**
FALSE POSITIVE RATE	80–90% (IBM Security)	30–50%	**< 5% (95% reduction)**
ALERT TRIAGE AUTOMATION	< 10%	50–70%	**~70%**
MITRE ATT&CK COVERAGE	40–60% (typical SIEM)	70–80%	**> 96%**
ANALYST CAPACITY FREED	Baseline	+ 20–30%	**+ 40–60%**
COMPLIANCE REPORTING EFFORT	30–50 hrs/month	15–25 hrs/month	**< 10 hrs/month**
SOC OPERATIONAL COST REDUCTION	Baseline	15–25%	**41% reported**

Source: Seceon

The demonstrated improvements in MTTD, MTTR, false-positive rates, automation, and analyst productivity indicate that integrated XDR platforms are helping enterprises, MSSPs, regulated industries, and critical infrastructure operators address increasing threat complexity without a proportional increase in SOC resources. MarketsandMarkets believes that as cybersecurity talent shortages persist and attack surfaces continue to expand across cloud, IT, and OT environments, organizations will increasingly invest in AI-native security platforms that can consolidate visibility, automate investigations, and deliver measurable business outcomes by improving resilience, enhancing scalability, and optimizing operational costs.

✓ Seceon - Applied Use Cases: Seceon aiXDR Platform

How Seceon aiXDR-PMAX Delivers Measurable Security and Business Outcomes

Seceon's role in modern SOC transformation becomes most evident in environments where organizations must manage **high-volume, distributed, and multi-tenant security operations with real-time threat visibility and response**. Seceon's aiXDR-PMAX platform addressed key requirements such as **unified telemetry across endpoints, networks, and cloud, real-time threat correlation, automated response, and multi-tenant scalability**.



GRAMAX Cybersec:
Deployment in a Next-Gen Security Operations Center

ABOUT GMR:

GMR Group is one of Asia's largest infrastructure developers, operating major airport assets including Delhi, Hyderabad, and Goa airports. The Group has an installed power generation capacity of over 3,000 MW and manages transportation infrastructure projects spanning 1,824+ lane kilometers across roads, highways, railways, and urban infrastructure sectors.

CHALLENGE:

GMR Group's legacy, outsourced SIEM-based SOC lacked visibility, advanced analytics, and real-time detection, covering **less than 40–60% of the attack surface** and excluding key areas like IoT. With **MTTD exceeding two weeks**, delayed response, and reliance on reactive, signature-based detection without AI/ML or threat hunting capabilities, the organization faced significant inefficiencies and increased risk exposure, highlighting the need for a unified, AI-driven SOC model.

SOLUTION:

GRAMAX Cybersec deployed **Seceon's aiXDR-PMax platform**, built on its Open Threat Management (OTM) architecture, to unify and automate its SOC operations. Key capabilities leveraged:

- ✓ **Multi-tenant AI-XDR platform** for MSSP scalability
- ✓ **Unified telemetry ingestion** across endpoints, networks, cloud, and applications
- ✓ AI/ML-driven behavioral analytics and Dynamic Threat Modeling (DTM)
- ✓ **Real-time threat detection and correlation** across environments
- ✓ Automated detection, investigation, and response (SOAR capabilities)
- ✓ Integrated SIEM, UEBA, NDR, and threat intelligence in one platform

This enabled GRAMAX to transition from **tool-driven operations to a unified, intelligence-driven SOC model**.

OUTCOME:

Following a structured RFP process, GMR selected Seceon's aiXDR and aiSIEM platform to modernize its SOC operations. Built on Open Threat Management (OTM) architecture, the platform enabled **unified telemetry collection, real-time AI/ML-driven analysis, and advanced threat correlation** across the entire attack surface. This allowed GMR to efficiently process large-scale data with a smaller team, improve operational transparency, and enhance analyst productivity. As a result, GMR and GRAMAX achieved **40% cost reduction, 60% improvement in visibility and threat detection coverage**, and faster detection and response compared to their previous legacy setup.

EFFICACY	WITH SECEON'S aiXDR AND aiSIEM PLATFORM & GMR SOC TEAM VS. GLOBAL SYSTEM INTEGRATOR
ATTACK SURFACE COVERAGE	95% (from <40%)
MTTD	99% real-time, others 2–3 hours (from 24+ hours)
MTTR	20 Minutes (vs. 1.5 Days)
RED TEAMING TEST	95% of threats were detected by Seceon vs. 69% with the former global system integrator

Efficiency	
Seceon Implementation Timeline	1,000 devices in 1st week, additional 110 devices within 20 days. Integrations with network, endpoint, and identity platforms in 1 day. 4 months to tune and refine alerts.
Cost (Overall Cybersecurity Program)	Decreased by 40% with Seceon vs. the cost of the global system integrator.)
Negative Business Impact	Downtime and other cybersecurity-related issues experienced by business users declined by 60%.

Source: Seceon Case Studies

CONCLUSION

Advancing Toward AI-Native, Outcome-Driven SOC Operations

The evolution of modern security operations is no longer defined by incremental improvements, but by a fundamental shift toward unified, AI-native, and intelligence-driven SOC models. As organizations expand across hybrid, multi-cloud, and distributed environments, the scale, speed, and sophistication of cyber threats continue to outpace traditional security approaches. Fragmented toolsets, reactive detection models, and manual workflows are increasingly insufficient to deliver the visibility, speed, and resilience required in today's threat landscape.

The organizations that will lead in cyber resilience through 2028 are those investing today in AI-native, unified security operations platforms. MarketsandMarkets research shows organizations adopting AI-native XDR platforms achieve 60–75% faster breach detection, 40–60% lower SOC operational costs, and measurably improved regulatory compliance posture compared to those maintaining legacy SIEM-centric architectures. Platforms like Seceon's aiXDR-PMAX deliver unified telemetry, AI-native correlation, and automated response at enterprise scale, which represent the architectural foundation for this transformation.

Looking ahead, Several Key Trends Will Continue To Shape The Future of SOC and XDR:

CONVERGENCE OF SECURITY FUNCTIONS

SIEM, SOAR, EDR, UEBA, and NDR are merging into unified XDR platforms

RISE OF AI AND GENAI IN SOC OPERATIONS

Enabling autonomous detection, investigation, and response

SHIFT TOWARD PROACTIVE AND PREVENTIVE SECURITY MODELS

Reducing the attack surface and preventing breaches earlier

GROWTH OF MSSP-DRIVEN SECURITY MODELS

Driving demand for scalable, multi-tenant XDR platforms

EMBEDDED COMPLIANCE AND CONTINUOUS MONITORING

Integrating governance into security operations

The Path Forward:

As cyber threats continue to evolve, organizations must move beyond reactive security models and embrace AI-native, unified, and intelligence-driven security operations. Platforms like Seceon's aiXDR-PMax are not just addressing current SOC challenges—they are defining the future of cybersecurity operations, enabling enterprises to achieve resilience, scalability, and operational excellence.

Ultimately, organizations that adopt AI-native XDR will be best positioned to bridge the gap between threat speed and response capability, transforming their SOCs into proactive, autonomous, and outcome-driven security engines.

Contact

Sayali Saste

Manager – MarketsandMarkets

sayali.saste@marketsandmarkets.com

Vidhu Rawat

Asst. Manager– MarketsandMarkets

vidhu.rawat@marketsandmarkets.com

Akshita

Research Analyst - MarketsandMarkets

akshita01@marketsandmarkets.com





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.