

2025

Defending the MSP Supply Chain:

Unified Security & Compliance Against Lazarus Group APT

A strategic guide for MSPs and MSSPs to stop Lazarus-led supply-chain intrusions with unified visibility, machine-speed response, and automated compliance.

seceon

Executive Summary: The Nexus of Nation-State Threats and the Managed Services Ecosystem

The global cyber threat landscape is accelerating in complexity as **state-sponsored actors and financially driven cybercrime converge**, with the **Lazarus Group (DPRK APT38)** leading this evolution. In 2024 and 2025, Lazarus intensified **record-breaking crypto thefts** and **high-precision espionage campaigns** using **custom malware**, **LOTL techniques**, and **RMM tool abuse** to bypass traditional defenses.

Their most dangerous vector is now the **MSP and MSSP supply chain**, where a single compromise provides **scalable access to thousands of downstream clients**. Legacy and **siloed security tools** such as separate SIEM, EDR, SOAR, and compliance systems **cannot detect or correlate threats at the speed required** to stop **sub-second lateral movement** or **identity-based attacks**.

The **Seceon Open Threat Management (OTM)** platform delivers the required architectural shift. By unifying **SIEM, XDR, NDR, UEBA, SOAR 4.0, and ITDR** in one platform, OTM enables **95 percent false-positive reduction**, **3 to 5 times analyst efficiency**, and **sub 5 minute MTTD and MTTR**. With **aiCompliance CMX360**, MSPs achieve **90 percent automated reporting** and **real-time readiness** for SOC 2, ISO 27001, NIST CSF, and other frameworks.

In an era of **advanced persistent threats** and increasing regulatory pressure, **Seceon OTM empowers MSPs and MSSPs to secure clients at scale**, eliminate tool fragmentation, and maintain **continuous compliance** through a single unified platform.

Lazarus Group's Strategic Evolution: Financial and Espionage Operations (2024-2025)

The DPRK's Cyber Mandate and the Fusion of APT and Cybercrime Operations

The Lazarus Group's operations are driven by a national imperative: generating revenue to circumvent international sanctions. Analysis confirms that Pyongyang has successfully secured over $5 billion worth of cryptocurrency since 2017 through these operations. This strategic mandate positions Lazarus activities not merely as cybercrime, but as state-backed financial warfare.

The group's operational approach has evolved significantly in the 2024-2025 timeframe, shifting emphasis toward high-value centralized financial exchanges (CeFi) and decentralized finance (DeFi) platforms. This concentration on lucrative targets demands unparalleled technical sophistication. In 2024 alone, North Korea was reportedly responsible for approximately 35% of all stolen funds globally, underscoring their dedication to high-impact operations that were nearly five times larger than those perpetrated by other actors.

Financial Warfare: Post-2023 Crypto Heists and the Targeting of CeFi/DeFi Infrastructure

The scale of Lazarus's financial ambition was underscored by the two largest reported incidents in the last two years:

- **The $1.5 Billion Bybit Exploit (February 2025):** This event is now recognized as the largest crypto exploit on record. The attack infiltrated Bybit's multi-signature wallet solution, Safe{Wallet}, resulting in the theft of approximately $1.5 billion in Ethereum tokens. This incident highlights a sophisticated strategy focused on compromising supply chain security or utilizing zero-day weaknesses within critical financial infrastructure to target high-value assets.

- The WazirX Attack (July 2024): This exploit disrupted over $200 million, resulting in $235 million in losses from the Indian cryptocurrency exchange's multi-signature wallet. The techniques employed included sophisticated phishing and API exploitation, emphasizing the group's continued reliance on social engineering to achieve initial access.

Following successful attacks, the Lazarus Group employs complex laundering techniques to rapidly obscure the illicit funds. For example, after the June 2023 Atomic Wallet hack, where over $100 million was stolen, the group utilized crypto mixers such as Sinbad.io. Further analysis shows the use of cross-chain transfers, bridging funds from one blockchain to Ethereum using previously associated Lazarus bridges (e.g., following the September 2023 CoinEx hack) and employing multiple mixing rounds to combine funds from separate operations, such as the $41 million taken from Stake.com.

This extreme velocity in post-exploitation activity, where hundreds of millions of dollars are mixed or bridged within hours, creates a critical challenge for security providers. Incident containment must happen immediately, requiring the security platform to correlate the initial access (T1566: spearphishing) with internal reconnaissance (T1021: lateral movement) and asset exfiltration (T1048) *before* the multi-stage laundering can commence. The window for human-speed detection is nonexistent. This operational environment confirms that MTTD and MTTR benchmarks must be measured in minutes, mandating the deep integration of AI-powered security orchestration (SOAR) and automated response capabilities.

Attack Name / Target	Date	Approximate Loss (USD)	Techniques Used	Significance
Bybit Safe{Wallet}	February 2025	$1.5 Billion	Multi-signature wallet breach, supply chain compromise	Largest crypto exploit on record; confirms focus on high-value CeFi operations.
WazirX Exchange	July 2024	$235 Million	Phishing, API exploitation, multi-signature wallet breach	Shows combined social engineering and technical precision in high-impact attacks.
Atomic Wallet	June 2023	$100+ Million	Sophisticated laundering (Sinbad.io, cross-chain transfers)	Demonstrated complex, rapid multi-stage laundering across blockchain ecosystems.

Intelligence Gathering Campaigns: IP Theft and Critical Infrastructure Espionage

Lazarus continues to run strong espionage operations alongside financial attacks, focusing on industrial automation, defense, and advanced technology sectors across regions such as Poland, the UK, and India. Their objective is stealing proprietary intelligence to support strategic state programs, including drone development.

Initial access often begins with sophisticated social engineering, particularly the ongoing Contagious Interview campaigns that trick cryptocurrency professionals into executing malicious payloads. The group's primary espionage malware, ScoringMathTea, is a highly advanced RAT with 40 commands, anti-analysis protections, and custom encryption that enables it to evade traditional detection.

Lazarus also exploits critical vulnerabilities for rapid privilege escalation, including CVE-2024-38193 in Windows AFD.sys and the CVE-2024-21338 kernel flaw. These capabilities allow them to gain SYSTEM-level access and bypass defensive controls.

Because tools like ScoringMathTea are engineered to avoid perimeter and signature-based detection, traditional EDR and SIEM cannot reliably identify these campaigns. Effective defense requires behavioral analytics (UEBA) and Network Detection and Response (NDR) to spot anomalous C2 traffic, identity misuse, and lateral movement after the initial breach.

The Service Provider Supply Chain: A Critical Vulnerability for Lazarus Exploitation

Why MSPs and MSSPs Are Strategic Force Multipliers for APTs

MSPs and MSSPs operate under a high-trust model, managing the IT infrastructure, cybersecurity, and sensitive data of numerous clients across diverse, often regulated, sectors. For state-sponsored threat actors like Lazarus, compromising a service provider offers an irresistible strategic advantage: it grants scalable, pre-authenticated access to an entire portfolio of high-value targets via a single breach point, making the service provider a force multiplier for exploitation.

Lazarus specifically targets this trust relationship. Their initial access often involves Tactics, Techniques, and Procedures (TTPs) such as **Spearphishing via Service (T1566)**, where they compromise vendor or partner email chains to deliver weaponized documents or installers to the ultimate client target. Furthermore, the group has been observed exploiting zero-day software vulnerabilities in network-linked and security authentication systems as part of a supply chain attack strategy to gain unauthorized access to targets' intranets.

Operationalizing the Attack: Abuse and Exploitation of Remote Monitoring and Management (RMM) Tools

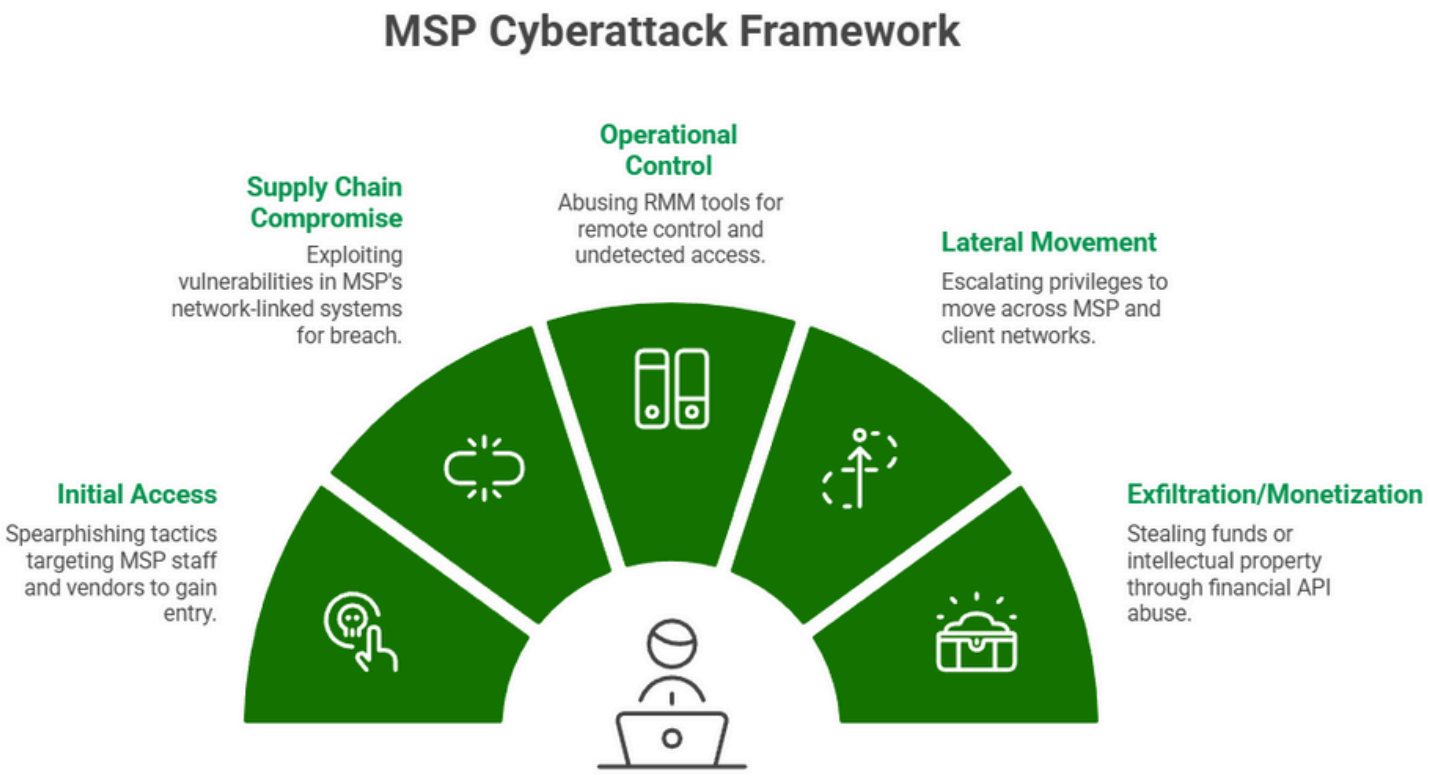
Once Lazarus gains initial access, they rely heavily on **RMM tools** for lateral movement (T1021). Although RMM platforms are legitimate for IT management, their built-in capabilities for **remote control, file transfer, and software installation** make them easy targets for abuse.

A key example is the exploitation of **CVE-2022-47966** in ManageEngine, a widely used RMM solution. This allowed Lazarus to compromise **internet backbone infrastructure and healthcare organizations** across the US and Europe and deploy **QuietRAT** and **CollectionRAT** as follow-on malware.
Their success comes from **Living Off the Land (LOTL)** tactics, using trusted IT tools to blend into normal operations. Because RMM traffic is often **whitelisted or ignored**, attackers can use weak credentials, default configurations, or even install their own RMM agents after phishing or social engineering.

The core vulnerability is not the RMM software itself but the **identity and behavior** behind it. When a high-privilege RMM agent performs **anomalous commands, privilege escalation, or bulk data transfers**, it signals compromise. Effective defense must shift toward **Identity Threat Detection and Response (ITDR)** and **UEBA**, which detect abnormal behavior from legitimate accounts and tools before the breach escalates.

To visualize the strategic targeting of the MSP supply chain by the Lazarus Group, the following table maps the key stages:

Stage	TTP (Technique)	Target / Vector	Objective
1. Initial Access	Spearphishing via Service (T1566)	MSP staff / vendor email or API channels	Gain trusted credentials or deploy initial loaders (e.g., Contagious Interview).
2. Supply Chain Compromise	Zero-day / vulnerability exploitation	MSP's network-linked systems (e.g., ManageEngine)	Breach MSP infrastructure to access client management tools.
3. Operational Control	RMM tool abuse (LOTL)	Remote Monitoring & Management (RMM) agents	Use legitimate, whitelisted RMM tools for remote control while avoiding detection.
4. Lateral Movement	Privilege escalation (T1068)	MSP's downstream client networks	Move from compromised MSP access into high-value client environments.
5. Exfiltration / Monetization	Custom C2 / financial API abuse	Crypto exchanges or espionage targets	Steal funds (e.g., Bybit) or exfiltrate sensitive IP (e.g., ScoringMathTea).



Quantifying Risk: Financial and Reputational Impact of a Service Provider Breach

A breach that uses the MSP/MSSP as a supply chain vector creates catastrophic financial and regulatory risks. When a service provider is compromised, it becomes the conduit for compliance failure across its entire client base. Clients subject to frameworks like GDPR, HIPAA, or the NIS 2 Directive will face immediate non-compliance challenges, leading to potential fines and severe reputational damage for the service provider.

The ability of an MSSP to demonstrate **effective control and rapid incident containment**, validated by objective performance metrics like sub-5-minute MTTR, is no longer a competitive advantage, but a regulatory requirement for maintaining customer trust, particularly in financial services (DORA) and government contracting (NIST SP 800-53).

Unified Defense Against Advanced Persistent Threats: The Seceon OTM Platform

Eliminating Silos: The Strategic Advantage of Unified SIEM, XDR, SOAR, and UEBA Architecture

Defending against the advanced, multi-vector campaigns of the Lazarus Group requires a fundamental shift away from the legacy, siloed security stack. The Seceon Open Threat Management (OTM) platform is designed specifically to eliminate tool sprawl by consolidating core security functions, aiSIEM, aiXDR-PMax, SOAR 4.0, UEBA, NDR, and ITDR, into a unified, AI-powered system.

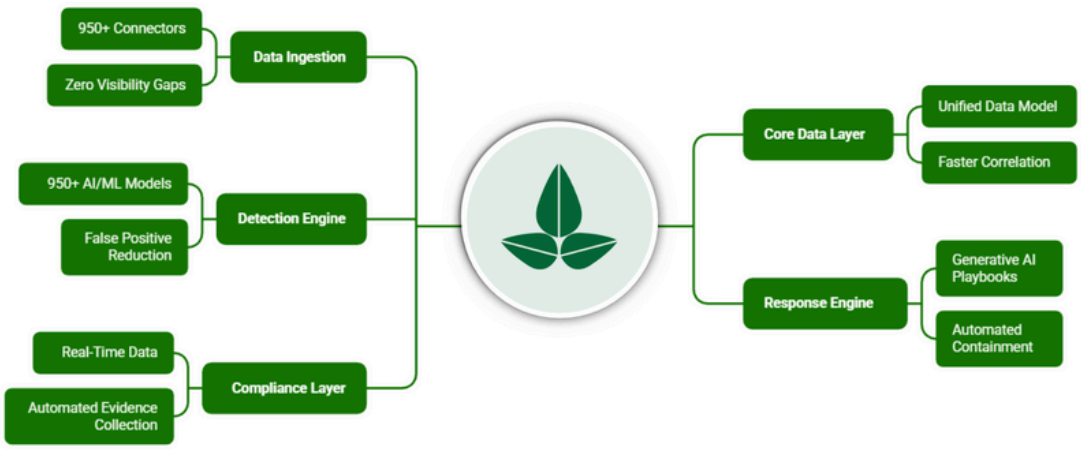
The strategic advantage of this architecture lies in its foundation: the **Seceon Event Format (SEF)**. SEF is a unified, lossless data model built into the platform from the ground up, ensuring seamless data flow, consistent analytics, and perfect fidelity across all security domains (IT, OT, Cloud). Unlike systems that are "kludged together" from disparate acquired tools, OTM’s unified data model ensures 95% faster correlation and eliminates the fragmented dashboards and integration difficulties that plague traditional security operations.

This architectural integrity enables massive scale and performance. The platform is engineered to handle enterprise-scale capacity, processing 1.6 Trillion events per day and utilizing Apache Spark for real-time analytics processing over 250PB per day. By leveraging over 950 pre-built integrations with essential security (CrowdStrike, Palo Alto), cloud (AWS, Azure), and identity platforms (Active Directory, Okta, ServiceNow), OTM guarantees unified visibility and zero correlation gaps, which is mandatory for tracking Lazarus's multi-platform and multi-stage TTPs.

The core differentiator is this unified approach, as illustrated by the platform's consolidation of capabilities:

Component	Function / Role	Driven By	Operational Advantage
Data Ingestion	Collects all logs, flows, and events	950+ connectors	Zero visibility gaps across IT, OT, Cloud, and Identity.
Core Data Layer	Seceon Event Format (SEF)	Unified, lossless data model	Enables 95% faster correlation and 70% lower storage requirements.
Detection Engine	aiSIEM + aiXDR + NDR + UEBA + ITDR	Over 950 AI/ML models	95% false-positive reduction; sub-5-minute MTTD.
Response Engine	SOAR 4.0 (Security Orchestration)	Generative AI playbooks (SERAai)	Automated containment in under 5 seconds; 70% incident automation.
Compliance Layer	aiCompliance CMX360™	Real-time security posture data	Automated evidence collection for SOC 2, ISO 27001, NIST, and more.

Seceon's AI-Powered Defense Architecture



Real-Time Detection and Behavioral Analytics (aiSIEM + UEBA + NDR)

Against sophisticated threats that rely on anti-analysis and LOTL tactics, Seceon's core detection technologies prioritize behavioral anomalies over signatures.

Combating LOTL and RMM Abuse (UEBA/ITDR)

Seceon’s Machine Learning-powered UEBA component is crucial for threat protection. It uses dynamic threat modeling to learn baseline behavior for every user, asset, and process, correlating minute anomalies via graph neural networks to uncover lateral movement and insider risks. The dedicated ITDR capability focuses specifically on the identity misuse—credential abuse and privilege escalation that is characteristic of RMM exploitation and post-compromise reconnaissance. The OTM platform can instantly detect and flag the deployment of malware like QuietRAT, or the use of compromised RMM credentials, by identifying anomalous command execution or unusual file access patterns by a typically quiet service account.

Neutralizing Custom C2 Communications (aiXDR-PMax + NDR)

The highly complex, memory-resistant nature of espionage malware like ScoringMathTea, which relies on custom encryption and anti-analysis checks, renders traditional endpoint protection insufficient. To counter this, Seceon OTM integrates aiXDR-PMax for unified detection across endpoints and cloud workloads with Advanced Network Detection and Response (NDR). The NDR capability provides Deep Packet Inspection (DPI) and NetFlow telemetry visibility, crucial for detecting lateral movement and network anomalies.

By combining these functions, the platform detects the effect of the malware: highly encrypted, non-standard Command and Control (C2) traffic (T1573) generated by ScoringMathTea over protocols like TCP. The cross-domain correlation within aiXDR links the subtle network anomaly identified by NDR with the suspicious entity behavior flagged by UEBA, ensuring comprehensive threat identification even when the payload itself is cloaked.

Autonomous Response at Machine Speed (SOAR 4.0)

As established, the shrinking window between initial access and major asset exfiltration necessitates automated, machine-speed response. Seceon OTM achieves superior security effectiveness by delivering sub-5-minute Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), automating the containment for 70% of incidents.

SOAR 4.0 is the orchestration engine, leveraging Generative AI (SERAai) to accelerate investigations and execute self-learning playbooks. This functionality ensures that threat intelligence gathered across the entire platform is immediately translated into decisive action, executed in under 5 seconds.

Against Lazarus TTPs, SOAR playbooks automatically mitigate the attack chain:

1. **RMM Abuse Containment:** Upon detection of lateral movement or anomalous RMM activity, SOAR instantly executes endpoint isolation and file quarantine.
2. **Identity Control:** Integration with identity platforms allows for immediate credential revocation and policy enforcement upon detecting privilege escalation or misuse.
3. **Financial Theft Prevention:** Detection of unauthorized, large-scale API calls or asset transfers (as seen in the Bybit or WazirX exploits) triggers automated blocking or suspension of the compromised service/account.

The unified visibility achieved through OTM's single architecture is fundamental to this success. A fragmented system cannot seamlessly correlate a weak phishing signal (log data) with a RMM process anomaly (UEBA) and the final unauthorized network connection (NDR), but Seceon's single data pipeline ensures the complete attack chain is identified and acted upon instantly.

Lazarus TTP / Malware	Seceon Capability	Detection / Mitigation Mechanism	Operational Impact	Significance
RMM Tool Abuse (LOTL, QuietRAT)	UEBA, aiXDR, ITDR	Dynamic behavioral modeling detects abnormal RMM activity, lateral movement, and credential misuse.	Sub-5-minute detection of supply-chain compromise and immediate endpoint isolation.	Largest crypto exploit on record; confirms focus on high-value CeFi operations.

Lazarus TTP / Malware	Seceon Capability	Detection / Mitigation Mechanism	Operational Impact
Custom RAT C2 (ScoringMathTea)	NDR, aiSIEM	Deep Packet Inspection and NetFlow analytics identify anomalous, encrypted C2 traffic (T1573) against baselines.	Alerts analysts to stealthy communications even with anti-analysis protections.
Zero-Day Privilege Escalation (CVE-2024-38193)	aiXDR-PMax, SOAR 4.0	Cross-domain correlation links vulnerability data to kernel-level anomalies; automated process termination/quarantine.	Enables rapid pre- and post-exploit remediation through automated response.
Financial Exfiltration (API / Wallet)	aiSIEM, UEBA, SOAR 4.0	Behavioral analytics catch anomalous API calls or unauthorized large transfers; automated blocking.	Immediate disruption of large-scale crypto theft attempts such as Bybit.

Operationalizing MSSP Success: Scalability, Efficiency, and Profitability

True Multi-Tier Multi-Tenancy (MTMT) for Global Scale and Data Isolation

For MSSPs seeking to defend thousands of clients against nation-state actors while managing complex regulatory obligations, the platform architecture must be optimized for multi-tenancy. Seceon OTM is purpose-built with a true Multi-Tier, Multi-Tenant (MTMT) design, empowering Master MSSPs to manage regional or sub-MSSPs efficiently under a single unified platform.

This MTMT architecture guarantees complete data isolation through unique tenant IDs, which is non-negotiable for adhering to data residency requirements and ensuring compliance (e.g., GDPR mandates). Furthermore, the platform utilizes per-tenant AI/ML threat models, ensuring that behavioral analytics are customized to the specific environment of each client. This eliminates the "noise" typical in shared threat intelligence models and maximizes detection accuracy, which is critical when dealing with diverse client footprints ranging from critical infrastructure to financial services.

The MTMT design allows for horizontal scalability, effortlessly onboarding new tenants without duplication or downtime, ensuring the MSSP can maximize profitability and grow its client base.

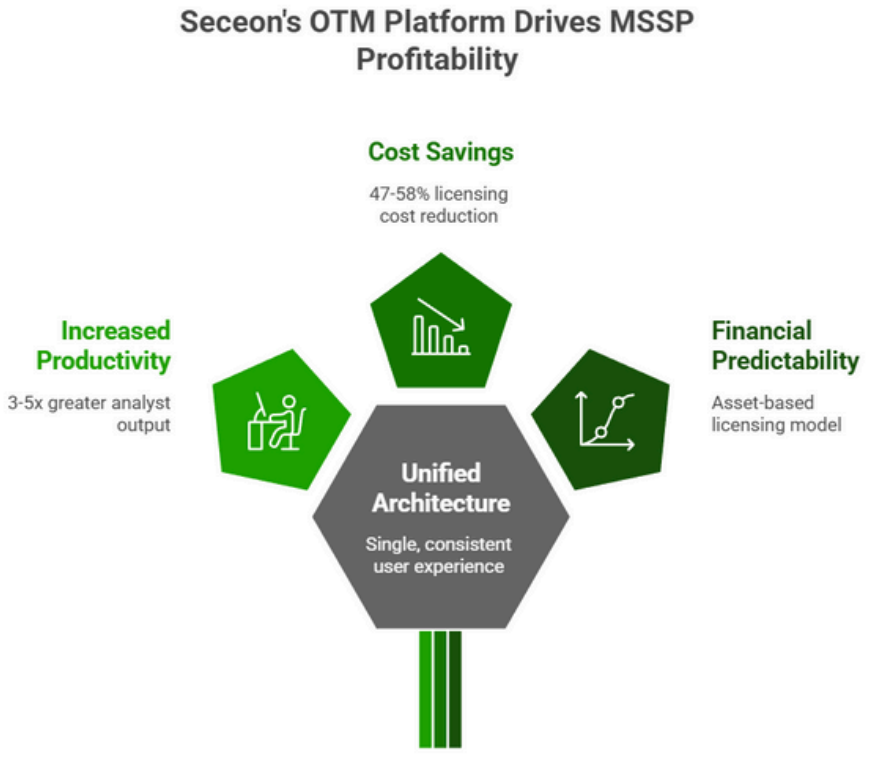
Driving Operational Efficiency and Cost Reduction

The unified architecture of OTM directly translates security effectiveness into operational profitability for MSSPs.

Productivity and Efficiency: By consolidating disparate tools and providing a single, consistent user experience, the platform drives 3-5x greater analyst productivity. This efficiency is further bolstered by a 95% reduction in false positives achieved through advanced AI-driven correlation, allowing analysts to focus only on genuine threats.

Quantified Cost Savings: The shift to a single, integrated system results in measurable business value through cost optimization. MSSPs report realizing 47-58% savings in licensing costs by replacing multiple tools, an 84% reduction in integration costs (due to no custom connectors), and a 70% reduction in overall SOC expenses due to automated workflows.

Financial Predictability: The adoption of an asset-based licensing model ensures predictable pricing, providing financial stability for MSSPs by insulating them from the volatile, high costs associated with data ingestion or volume limits common in traditional SIEM pricing models. Organizations leveraging the OTM platform realize a full Return on Investment (ROI) within 6-9 months, with annual savings ranging from $2.5 million to $4.2 million compared to multi-vendor approaches.



Continuous Compliance in the Face of Advanced Threats: aiCompliance CMX360™

Regulatory Imperatives for Service Providers

The sophistication and cross-sector targeting employed by the Lazarus Group underscore the necessity for MSSPs to maintain continuous, verifiable compliance. Service providers are subject to a complex landscape of global and sector-specific mandates, including SOC 2 Type II, ISO 27001, NIST CSF, HIPAA, PCI-DSS, GDPR, EU DORA, and NERC CIP.

For service organizations, demonstrating control over customer data and processes via SOC 2 Type II is fundamental for securing and maintaining client trust. The NIST Cybersecurity Framework (CSF) is a crucial benchmark, particularly for MSSPs serving critical infrastructure or federal contractors, as its goal is to establish shared best practices around cybersecurity risk management. ISO 27001 provides the framework for establishing a formal Information Security Management System (ISMS) required by many global enterprises. Achieving and maintaining these standards while actively defending against APTs like Lazarus is a critical differentiator.

Posture-Driven Compliance: Automating Evidence Collection from Live Security Telemetry

Seceon's aiCompliance CMX360™ component fundamentally transforms compliance from a documentation-heavy, periodic manual task into a continuous, posture-driven outcome. CMX360 builds compliance evidence directly from live security posture and the platform's accumulated SIEM data, enabling organizations to achieve 60-80% compliance readiness instantly upon deployment.

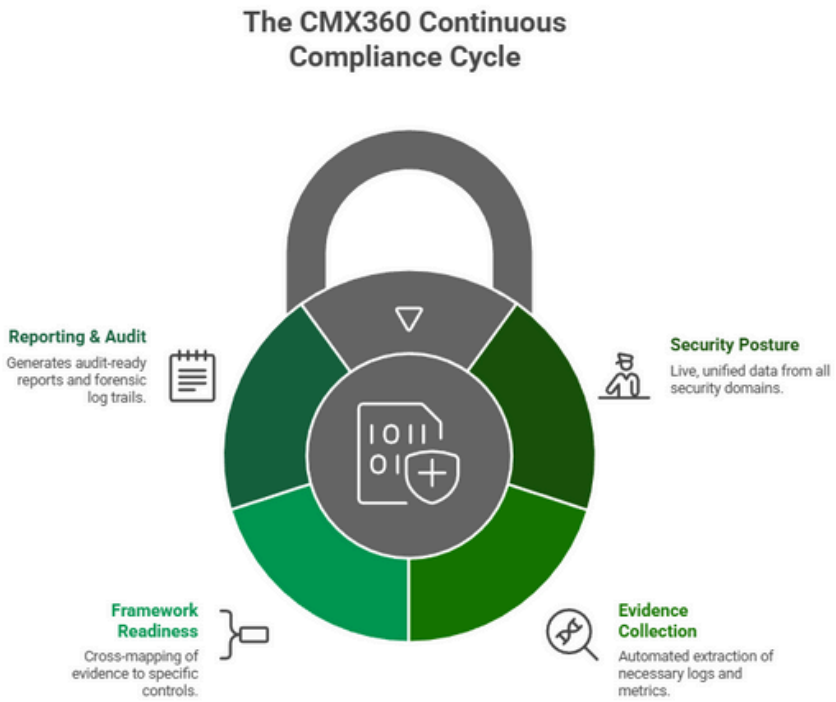
This process streamlines governance and audit readiness:

- **Automated Evidence and Reporting:** CMX360 delivers up to 90% automated reporting, reducing preparation time for audits from typical multi-week efforts down to just two hours. The platform achieves a 95% audit prediction accuracy, cutting audit timelines by up to 75%.
- **Forensic Assurance:** To satisfy stringent regulatory requirements, the platform ensures complete audit trails and chain of custody. It features a Long-Term Storage (LTS) architecture providing 7-year log retention with forensic search capabilities.

- **Multi-Framework Support:** CMX360™ provides multi-framework visibility, tracking progress and collecting evidence across all applicable standards including SOC 2, ISO 27001, NIST, DORA, and GDPR simultaneously.

The following flow chart summarizes the continuous, automated compliance process enabled by the Seceon platform:

Phase	Description / Source	Automation Feature	Output Metric
1. Security Posture	Live, unified data from SIEM, XDR, NDR, and UEBA security domains	Real-time monitoring of control execution	95% audit prediction accuracy
2. Evidence Collection	Automated extraction of required logs and telemetry from live posture data	Automated evidence mapping and validation	90% faster evidence collection
3. Framework Readiness	Cross-mapping evidence to controls across multiple frameworks	Multi-framework simultaneous support (SOC 2, NIST, ISO)	60–80% compliance readiness at deployment
4. Reporting & Audit	Generates audit-ready reports and complete forensic log trails	Automated reporting generation	Audit preparation reduced from 2 weeks to 2 hours



Mapping CMX360™ to Critical Controls for Advanced Threats

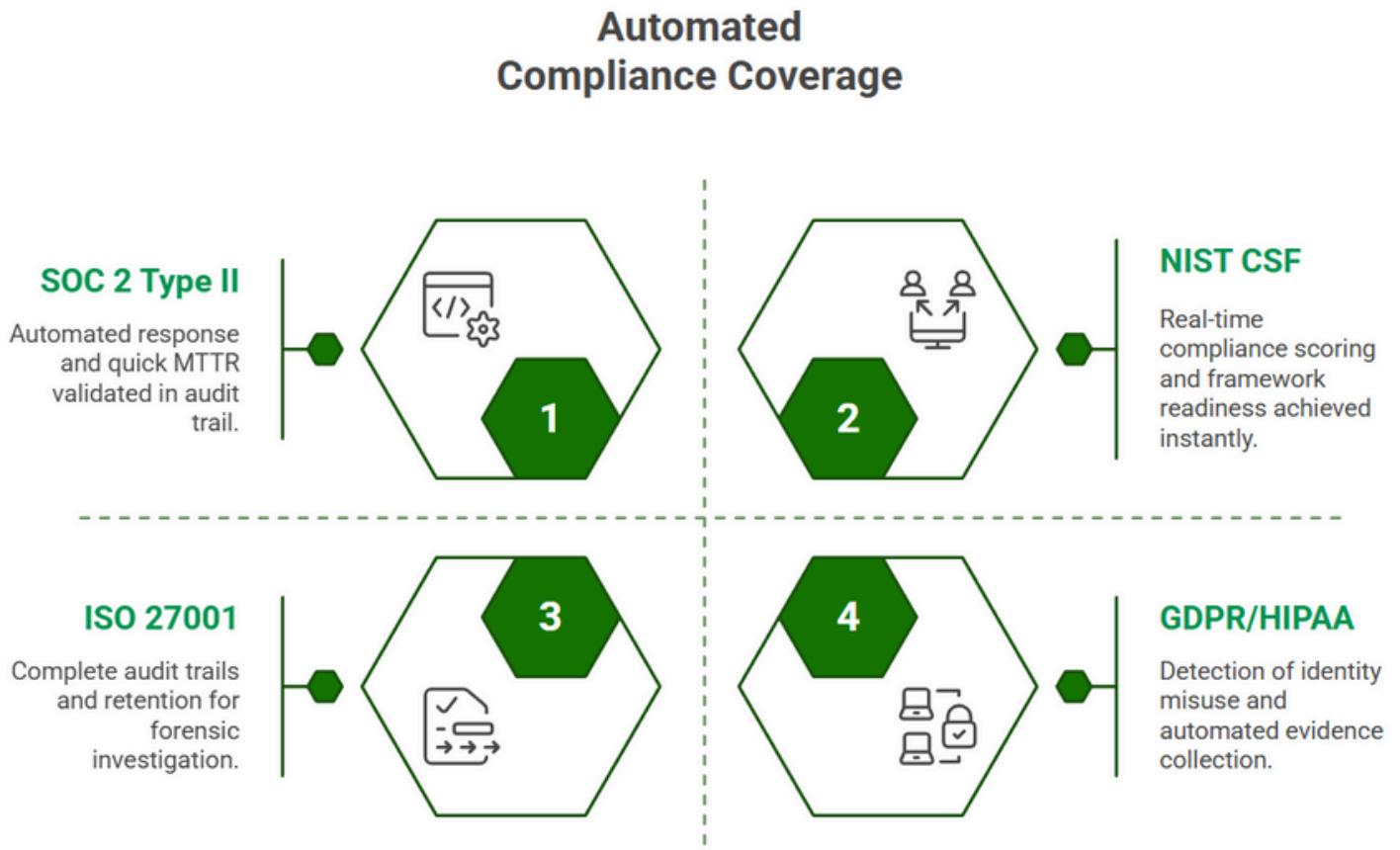
The ability to link security performance directly to regulatory assurance is essential for MSSPs defending against actors like Lazarus.

- **NIST CSF Alignment (Detect and Respond):** The platform's core security effectiveness directly fulfills high-priority controls within the NIST CSF. The unified detection capabilities (aiSIEM/aiXDR), which provide real-time correlation and 95% false-positive reduction, directly address the requirements for continuous monitoring and advanced threat analysis within the Detect category. Furthermore, the automated response delivered by SOAR 4.0, which executes mitigation and documents every action taken, provides verifiable evidence for controls within the Respond category, demonstrating automated containment against RMM abuse and lateral movement.
- **SOC 2 Trust Services Criteria Coverage:** OTM's comprehensive defense provides critical evidence for the Security and Availability criteria of SOC 2. The robust defense against credential theft and privilege escalation, provided by UEBA and ITDR, documents the effectiveness of logical access controls and risk mitigation strategies. The sub-5 minute MTTR ensures high availability by rapidly restoring compromised services, satisfying the critical availability criteria for service organizations.

By leveraging continuous, automated evidence collection based on machine-speed threat response, CMX360 transforms compliance from a cost center into a demonstrably superior resilience posture. This performance-based compliance validation is a strategic necessity for MSSPs serving the financial, critical infrastructure, and government sectors targeted by Lazarus.

Compliance Framework / Domain	MSSP Imperative / Lazarus Defense Need	Seceon CMX360 Feature	Impact / Automation Metric	Significance
SOC 2 Type II (Security, Availability)	Incident detection and rapid response time	aiXDR, SOAR 4.0	70% automated response; sub-5-minute MTTR validated in audit trail.	Largest crypto exploit on record; confirms focus on high-value CeFi operations.

Compliance Framework / Domain	MSSP Imperative / Lazarus Defense Need	Seceon CMX360 Feature	Impact / Automation Metric
NIST CSF (Detect, Respond, Recover)	Continuous monitoring of RMM abuse and LOTL tactics	aiSIEM, UEBA, NDR	Real-time compliance scoring; 60–80% framework readiness instantly.
ISO 27001 (A.16 Information Security Management)	Logging and monitoring with long-term evidence retention	LTS, aiSIEM forensic search	Complete audit trails and 7-year retention for forensic investigation.
GDPR / HIPAA (Confidentiality)	Identity and access control to prevent credential abuse	ITDR, UEBA	Detects identity misuse; automated evidence collection for data-processing controls.



Lazarus Group APT Defense Reality Check

Why Traditional Approaches Fail and How Seceon OTM Succeeds

Four Pillars of Challenges

$5B+
Cryptocurrency stolen by DPRK since 2017

35%
Of all global stolen funds in 2024 attributed to North Korea

$1.5B
Largest crypto exploit - By bit February 2025

MSP/MSSP
Supply chain force multiplier providing scalable access

Current Threat Level

40+
Commands in ScoringMathTea RAT with anti-analysis protection

Zero-Day
CVE-2024-38193 & CVE-2024-21338 exploited for privilege escalation

LOTL
Living Off the Land tactics using RMM tools

Hours
Mixing & laundering hundreds of millions within hours

Current Problems

- **Siloed tools:** Separate SIEM, EDR, SOAR, and compliance systems cannot correlate threats fast enough
- **Supply chain targeting:** Single MSP/MSSP breach provides access to thousands of clients
- **RMM abuse:** Legitimate tools (ManageEngine CVE-2022-47966) exploited for lateral movement
- **Custom malware:** ScoringMathTea RAT evades signature-based detection with encryption
- **Speed gap:** Sub-second lateral movement requires machine-speed response
- **Manual compliance:** Multi-week audit preparation across SOC 2, ISO 27001, NIST frameworks

Seceon Solution

- **Unified platform:** SIEM, XDR, NDR, UEBA, SOAR 4.0, ITDR in one architecture
- **MTMT design:** Multi-Tier Multi-Tenancy with complete data isolation
- **UEBA/ITDR:** Behavioral detection of anomalous RMM activity and credential abuse
- **NDR + DPI:** Deep packet inspection spots encrypted C2 traffic patterns
- **Sub-5 min MTTD/MTTR:** 70% automated incident response via SOAR 4.0
- **aiCompliance CMX360:** 90% automated reporting, 2-hour audit prep vs 2 weeks

Results

95%
False Positive Reduction

3-5x
Analyst Productivity Increase

47-58%
Licensing Cost Savings

6-9mon
Full ROI Achievement

Why Seceon OTM for MSPs/MSSPs Now?

Lazarus APT campaigns demand unified AI defense. Stop nation-state threats with sub-5 minute response. Eliminate tool sprawl - achieve 60-80% compliance readiness instantly across SOC 2, ISO 27001, NIST CSF, and DORA.

Conclusion: Securing the Future of Managed Services

The Lazarus Group's intensified campaigns marked by unprecedented financial thefts and sophisticated espionage malware that targets the MSP/MSSP supply chain have redefined the necessary standard for managed security services. Traditional security architectures, characterized by siloed tools and manual correlation, are fundamentally incapable of matching the speed and complexity of nation-state adversaries. The technical and regulatory pressures facing MSPs demand a transition to a unified, automated defense strategy.

The Seceon Open Threat Management (OTM) platform offers the architectural resilience and operational efficiency required to meet this threat head-on. Its unified design, underpinned by the Seceon Event Format (SEF), ensures comprehensive visibility and correlation across IT, OT, Cloud, and Identity domains, eliminating the correlation gaps exploited by Lazarus's multi-vector attacks. The fusion of AI-driven capabilities specifically UEBA and ITDR for identity and behavioral threat detection, NDR for custom C2 tracking, and SOAR 4.0 for autonomous response—delivers the crucial sub-5 minute MTTD and MTTR necessary to contain breaches before catastrophic financial or intelligence loss occurs.

For MSSPs, OTM delivers strategic success by providing:

1. **Superior Threat Neutralization:** Effective counter-measures against advanced TTPs like RMM abuse and ScoringMathTea C2, resulting in a 95% reduction in false positives.
2. **Scalable Operations:** True Multi-Tier Multi-Tenancy (MTMT) allows for efficient, profitable scaling with guaranteed data isolation across thousands of clients.
3. **Continuous Compliance:** aiCompliance CMX360™ transforms compliance into an automated, demonstrable outcome of security posture, reducing audit preparation time by up to 75% and ensuring immediate readiness for critical global frameworks.

By leveraging the Seceon OTM platform, Managed Service Providers can solidify their role as resilient defenders, providing enterprise-grade protection, superior operational efficiency, and verifiable continuous compliance, thereby securing the future of their managed services ecosystem against the most advanced persistent threats.

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 700 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

References and Citations:

This whitepaper is based on research and data from:

- CISA. (2024). Threat Actor Activity Reports and Supply Chain Security Guidance. Cybersecurity and Infrastructure Security Agency.
- CrowdStrike Intelligence. (2024). Global Threat Report: DPRK Intrusion Activity and Emerging APT Trends.
- ENISA. (2023). Cybersecurity Supply Chain Risk Guidelines for Managed Service Providers.
- ESET Research. (2024). Analysis of Lazarus Group Campaigns and Custom Malware Tooling.
- FBI & DOJ. (2024). North Korean State-Sponsored Cybercrime and Cryptocurrency Theft Investigations.
- Google Mandiant. (2024). APT38 and DPRK Cyber Operations Report.
- Kaspersky Global Research & Analysis Team. (2023–2024). Lazarus Group Malware Analysis Including QuiteRAT and CollectionRAT.
- Microsoft Threat Intelligence. (2024). Behavioral TTP Analysis of DPRK Identity-Based Intrusions.
- MITRE ATT&CK. (2024). Techniques and Procedures for APT38 and Associated DPRK Units.
- NIST. (2023). NIST Cybersecurity Framework (CSF) and Zero Trust Architecture Guidance.
- PwC Threat Intelligence. (2023). Living Off the Land Attacks and RMM Exploitation Trends.
- Secureworks Counter Threat Unit. (2024). Analysis of ScoringMathTea RAT and DPRK Espionage Campaigns.
- SentinelOne Labs. (2024). Lazarus Malware Evolution and Windows Kernel Exploitation Techniques.
- Symantec Threat Hunter Team. (2024). DPRK Credential Theft and Supply Chain Targeting Patterns.
- U.S. Treasury Department OFAC. (2023–2024). Sanctions Reports on DPRK Cyber-Enabled Financial Theft.
- Unit 42 (Palo Alto Networks). (2024). Threat Vectors in MSP and MSSP Environments and RMM Abuse.
- US-CERT. (2024). Alerts on CVE-2022-47966 and Ongoing ManageEngine Exploitation.

About the Author

Smit Kadakia

Co-founder, Seceon Inc.



Smit leads Seceon's data science and machine learning team, focused on developing a state-of-the-art behavior anomaly detection solution. Smit holds a B.S. from VJTI, Mumbai, an MS in Computer Science from Indian Statistical Institute, Kolkata, and an MBA from Southern New Hampshire University, Manchester. Smit and the team at Seceon have built the industry's first and only fully automated threat detection and remediation system using a combination of machine learning and artificial intelligence techniques. Seceon's approach includes analysis of all traffic, flows, and processes in and out of the network and correlates them near-simultaneously with behavioral analytics, recognized and zero-day exploits, and policies to surface threats and proposed responses in near-record real-time.

About the Author

Aditya Kumar

AI/ML Cybersecurity Engineer, Seceon Inc.



Aditya brings deep expertise in applying artificial intelligence and machine learning to safeguard IT, OT, IoT, and cloud ecosystems against advanced and evolving cyber threats. At Seceon, he plays a key role in strengthening enterprise security resilience, ensuring alignment with global compliance frameworks, and delivering measurable ROI through the company's next generation aiSIEM and OTM platforms.

© 2025 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.