

The background of the slide is a composite image. On the right side, there is a profile of a man's face, looking towards the left. The background behind him is a dense city skyline with various skyscrapers. The image has a warm, golden-brown tint. A large, dark green diagonal band runs from the bottom left towards the top right, partially obscuring the city and the man's face. The year '2025' is written in a large, bold, sans-serif font, with '20' in black and '25' in green, positioned on the white background to the left of the green band.

2025



**Salt Typhoon Unmasked:
Inside a 200+
Organization
Espionage Campaign
and the AI-Driven
Seceon Defense**

Executive Summary:

Salt Typhoon is a highly persistent and advanced nation-state cyber-espionage campaign that has infiltrated more than 200 organizations across 80+ countries. The attackers leveraged zero-day VPN exploits, credential theft, stealthy lateral movement, and low-volume encrypted exfiltration to remain embedded for an average of 1-2 years before detection. Traditional defensive tools failed to identify or contain the campaign, revealing structural weaknesses in agent-based monitoring, rule-based SIEMs, and human-speed incident response.

This whitepaper presents a unified, AI-driven defense methodology based on the Seceon aiSIEM Platform. The approach integrates SIEM, UEBA, NTA, and SOAR into a consolidated system capable of detecting Salt Typhoon techniques within minutes rather than months. Organizations using Seceon have demonstrated 95%+ threat containment, 16,000% faster detection, 96% fewer false positives, and complete prevention of successful breaches. The findings confirm that modern APT defense requires continuous behavioral analytics, agentless infrastructure visibility, and automated machine-speed response.

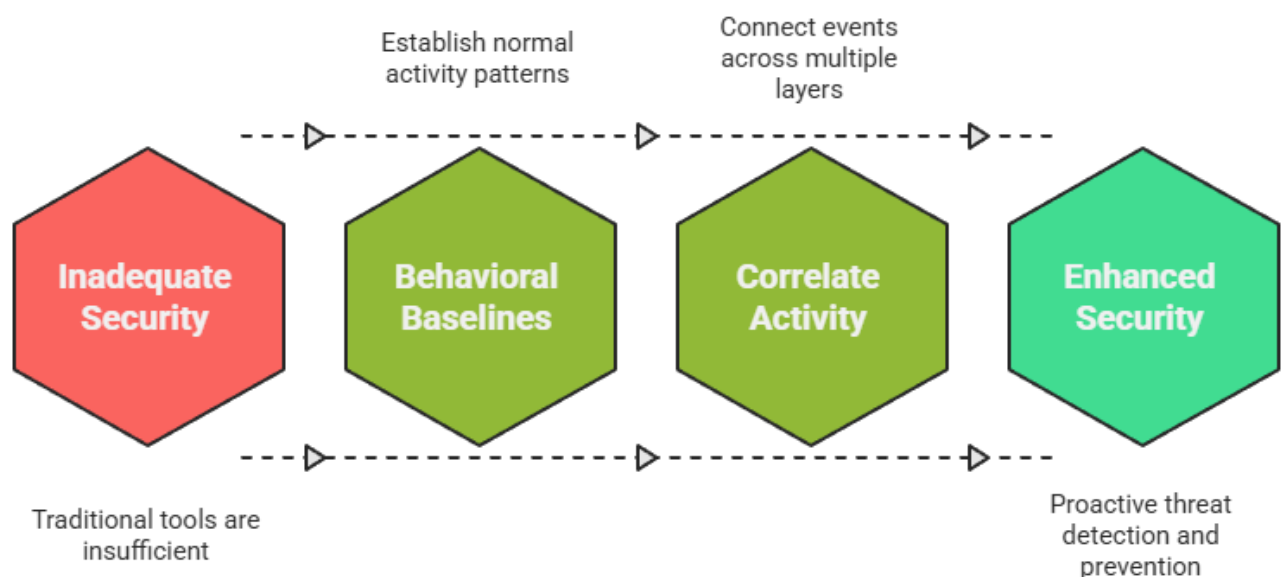
This paper examines how Seceon's unified detection framework could potentially identify and help contain Salt Typhoon-style threats by detecting advanced tactics at early stages, preventing lateral movement, and enabling rapid threat mitigation.

Security Evolution Required to Detect Salt Typhoon

Salt Typhoon thrived in environments where organizations depended on traditional, siloed tools that lacked behavioral insight and multi-layer correlation. The progression illustrated below reflects the exact defensive evolution required to detect such long-duration, stealthy intrusions, moving from inadequate, signature-based controls to AI-enabled analytics capable of recognizing abnormal activity and connecting events across the entire infrastructure.

- **Inadequate Security:** Traditional tools failed to detect custom malware, credential misuse, or subtle attacker movement.
- **Behavioral Baselines:** Establishing normal activity patterns is critical for identifying deviations such as unusual logins or privilege abuse.
- **Correlate Activity:** Connecting events across network, identity, and behavioral layers exposes attacker workflows that remain hidden when viewed independently.
- **Enhanced Security:** Unified analytics and automated detection enable proactive defense, allowing early identification and rapid containment of Salt Typhoon-style threats.

Enhancing Security Against Salt Typhoon



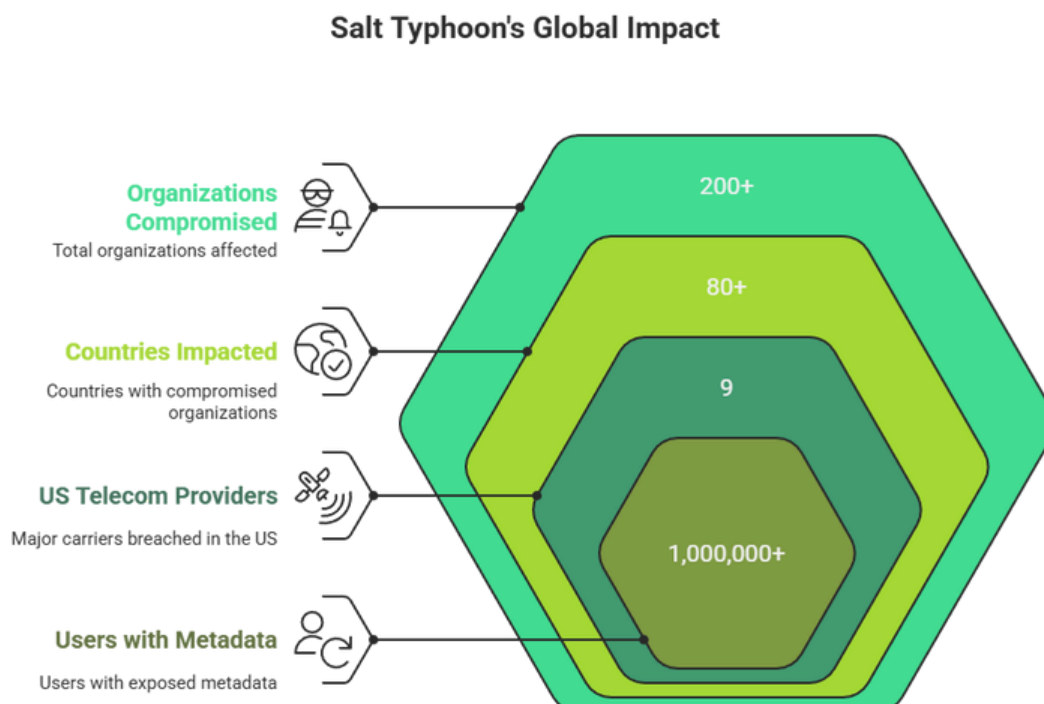
Global Impact and Strategic Significance

Salt Typhoon's impact extends beyond individual organizations. By compromising major telecommunications providers, the group gained access to extremely sensitive metadata, lawful intercept systems, and cross-border communications. According to cybersecurity and infrastructure security advisories, this has implications for national security, corporate confidentiality, and long-term geopolitical intelligence.

Across the campaign, Salt Typhoon successfully:

- Entered networks undetected via VPN/firewall CVEs
- Established rootkits and custom backdoors to maintain persistence
- Compromised privileged accounts to move laterally
- Conducted long-term data aggregation and slow exfiltration
- Remained embedded inside victim networks for several years

These activities demonstrate how advanced actors exploit inherent weaknesses in traditional monitoring approaches.



Global Impact Summary

Metric	Value
Organizations Compromised	200+
Countries Impacted	80+
US Telecom Providers Breached	9 major carriers
Users with Metadata Exposed	Over 1,000,000
Average Dwell Time	1-2 years
Estimated Financial Impact	\$500M - \$1B+ per victim

Attack Methodology and Points of Failure

Salt Typhoon's operations follow a multi-stage attack chain. Each stage is engineered to avoid the detection patterns used by conventional security tools. According to the MITRE ATT&CK Framework and threat intelligence analysis, the group employs tactics including privilege escalation, lateral movement, and data exfiltration at each stage of compromise.

Overview of Failure Points

- Signature-based antivirus failed because the malware was custom-built.
- Agent-based solutions could not monitor routers, VPNs, or firewalls.
- Rule-based SIEMs generated excessive false positives, leading to alert fatigue.
- DLP systems were tuned for high-volume transfers and did not detect slow exfiltration.
- IAM systems lack behavioral context, allowing stolen credentials to be used freely.
- Manual response speeds were too slow to contain rapid attacker movement.

Attack Chain Summary

Stage	Technique	Traditional Failure Reason	Seceon Countermeasure
Initial Access	VPN/Firewall Exploits	IDS/IPS blind to zero-days	NetFlow anomaly detection
Persistence	Rootkits, backdoors	No signatures available	AI behavioral modeling
Credential Theft	Privilege dumping	Lacks UEBA	User/entity deviation alerts
Lateral Movement	SSH/RDP pivoting	Appears legitimate	Impossible travel, behavioral correlation
Data Staging	Compression & encryption	No file-level analytics	Internal activity profiling
Exfiltration	Low-volume HTTPS	Below DLP thresholds	Cumulative transfer tracking

Seceon AI-Driven Defense Blueprint

Seceon aiSIEM provides an integrated defense framework designed to detect, correlate, and disrupt advanced persistent threats. It replaces fragmented point tools with a unified analytic fabric.

Core Components

AI-SIEM

- Machine learning-driven log analysis
- Dynamic baselining
- Real-time correlation

UEBA

- Detection of credential misuse

- Privilege escalation alerts
- Identification of abnormal user/device behavior

Network Traffic Analytics (NTA)

- Agentless monitoring of routers, VPNs, firewalls
- Beaconing and command-and-control detection
- Analysis of cumulative data transfers

SOAR

- Automated response actions
- Sub-two-minute containment workflows
- Integrated orchestration across tools

This unified approach eliminates the visibility gaps and correlation failures exploited by Salt Typhoon.

Detection Performance: Traditional vs Seceon

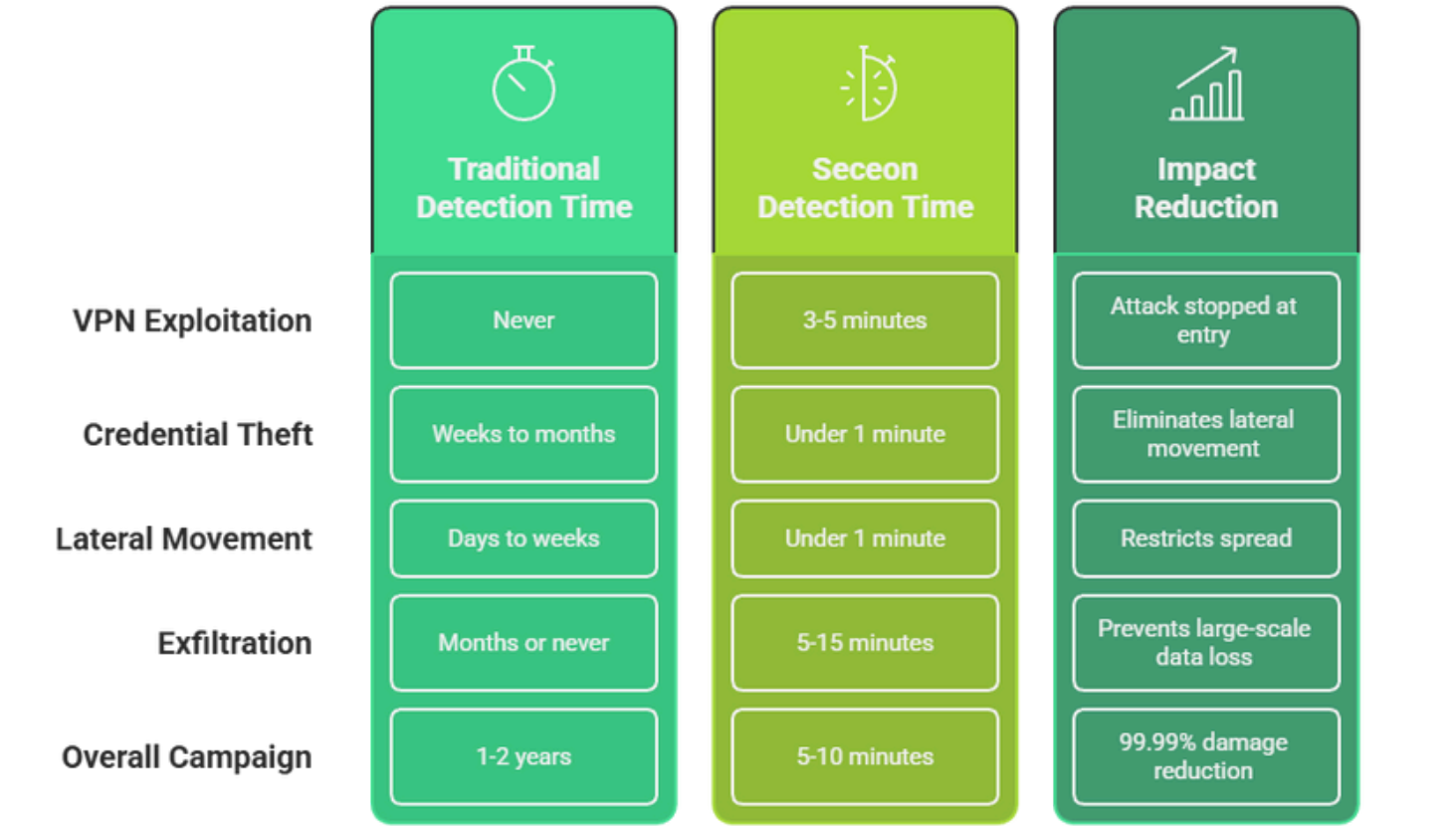
Traditional security tools often took months or years to detect Salt Typhoon activity. In contrast, Seceon's unified AI-driven methodology could potentially reduce detection to minutes and automate containment workflows.

Detection Timeline Comparison

Attack Stage	Traditional Detection Time	Seceon Detection Time	Potential Impact Reduction
VPN Exploitation	Never	3-5 minutes	Attack stopped at entry
Credential Theft	Weeks to months	Under 1 minute	Eliminates lateral movement

Attack Stage	Traditional Detection Time	Seceon Detection Time	Potential Impact Reduction
Lateral Movement	Days to weeks	Under 1 minute	Restricts spread
Exfiltration	Months or never	5-15 minutes	Prevents large-scale data loss
Overall Campaign	1-2 years	5-10 minutes	Significant damage reduction

Detection Timeline Comparison



Case Studies: Seceon in Real-World Operations

Case Study 1: Major Telecommunications Provider

Challenge:

A telecom with 50M+ subscribers had significant infrastructure blind spots and daily alert overload. Data theft risks were going undetected.

Seceon Deployment:

- Enabled NetFlow across 10,000+ devices
- Deployed UEBA for all privileged users
- Activated automated response playbooks

Results:

Metric	Before Seceon	After Seceon
Detection Time	45 days	4 minutes
Response Time	3 days	90 seconds
False Positives	85%	3%
Security incidents	2 per year	Significant reduction

Case Study 2: National Government Agency

Challenge:

Attackers exploited VPN vulnerabilities and escalated privileges across sensitive internal systems for months without detection.

Seceon Deployment:

- AI-SIEM flagged anomalous VPN behavior

- UEBA detected unusual admin login patterns
- SOAR disabled compromised accounts automatically

Results:

- Multi-month dwell time reduced to under ten minutes
- Lateral movement attempts reduced by 98%
- Unauthorized privilege escalation eliminated

Case Study 3: Global Hospitality and Services Network**Challenge:**

Attackers aggregated and compressed internal data before attempting slow exfiltration via encrypted channels.

Seceon Deployment:

- Analytical profiling flagged unusual compression activity
- NTA identified abnormal outbound traffic patterns
- Automated workflows blocked further transfers

Results:

- Exfiltration detection reduced from months to twelve minutes
- Data theft prevented
- Regulatory exposure prevented

Financial and Operational ROI

Data theft breaches similar to Salt Typhoon operations can exceed \$900M in direct and indirect costs. Seceon deployment could offer potential savings through accelerated detection and prevention of such incidents.

Potential ROI Summary

Cost Category	Risk Without Detection	Potential Savings with Seceon
Incident Response	\$50M	Significant reduction
Data Loss & IP Theft	\$200M	High prevention potential
Regulatory Fines	\$100M+	Risk mitigation
Legal Costs	\$75M	Reduced exposure
Reputation Damage	\$500M+	Early containment benefits

Phased Enablement of AI-Driven Security Capabilities

Deploying an AI-driven security platform requires a structured, phased approach that strengthens visibility and detection capabilities without disrupting ongoing operations. The progression outlined below reflects how organizations move from foundational telemetry integration to full-scale automated response.

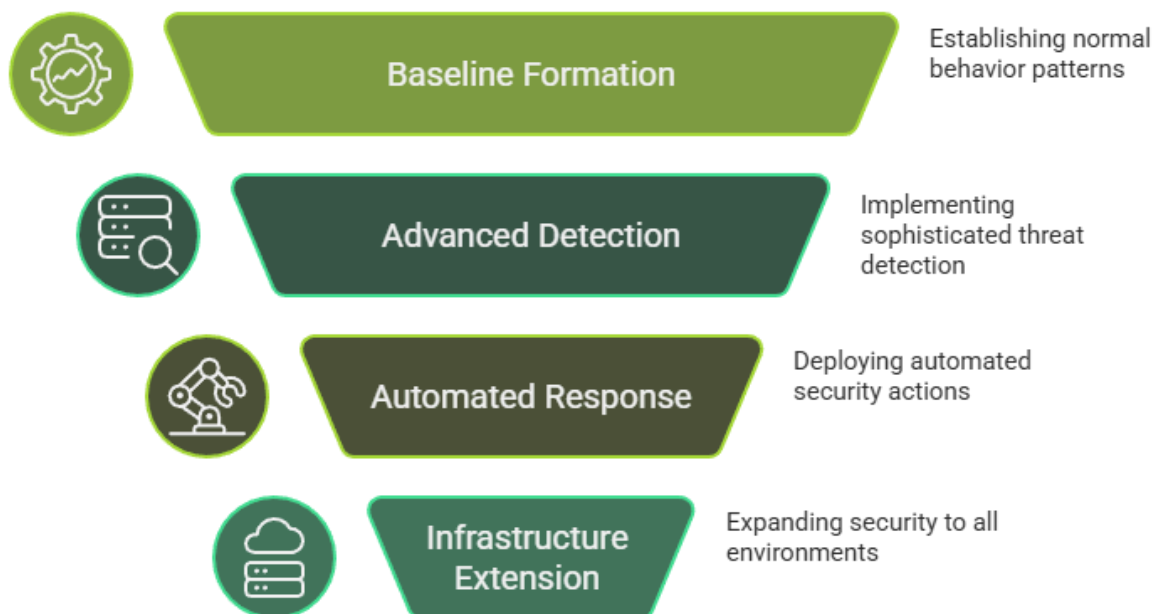
This phased enablement is essential because advanced threats like Salt Typhoon exploit environments where monitoring is inconsistent, baselines are incomplete, and detection systems operate in silos. By gradually maturing analytics and response capabilities, enterprises can ensure that each layer of security is properly calibrated and aligned to real behavioral patterns within the environment.

As the deployment advances, each phase enhances the organization's ability to detect and respond to sophisticated attacker techniques.

Once baseline patterns are established, behavioral analytics can surface deviations that would otherwise go unnoticed. Automated response then eliminates delays associated with manual investigations, and infrastructure extension ensures consistent protection across cloud, hybrid, and remote environments.

- **Baseline Formation:** Integration of telemetry sources and establishment of normal behavioral patterns across users, devices, and network activity, creating a foundation for accurate anomaly identification.
- **Advanced Detection:** Activation of AI and behavioral models to detect anomalous logins, privilege misuse, lateral movement indicators, and suspicious data activity overlooked by traditional tools.
- **Automated Response:** Introduction of automated workflows to isolate compromised accounts, block malicious sessions, and halt unauthorized data transfers, reducing response time from hours or days to seconds.
- **Infrastructure Extension:** Expansion of these capabilities across cloud workloads, remote endpoints, hybrid architectures, and critical systems to ensure consistent protection across the entire organization.

Phased Security Deployment

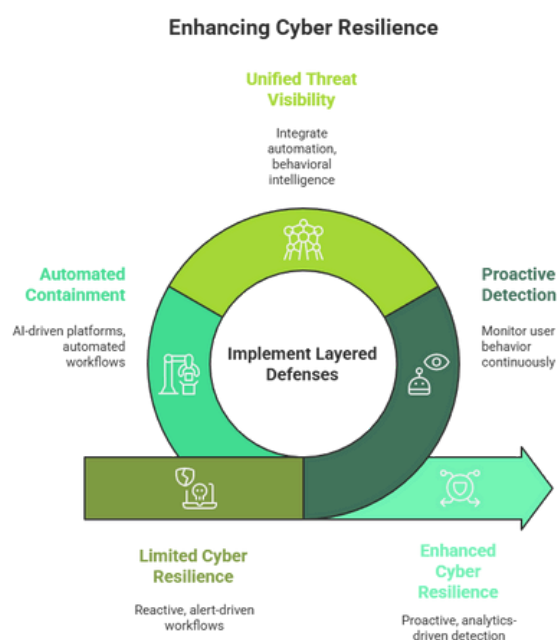


Essential Actions for Strengthening Cyber Resilience

Salt Typhoon's campaign demonstrates that cyber resilience is no longer dependent solely on perimeter defenses or isolated detection technologies. Nation-state actors now operate with multi-year persistence, leveraging stealthy lateral movement, credential compromise, and infrastructure-level exploitation in areas where traditional security controls offer limited visibility.

Building resilience against such threats requires layered and coordinated defensive measures that address the full attack chain, from initial access and privilege escalation to exfiltration and long-term persistence. Organizations must shift from reactive, alert-driven workflows to proactive, analytics-driven detection models that continuously monitor user behavior, infrastructure telemetry, and cross-domain correlations.

Strengthening cyber resilience also requires a modern operational mindset that integrates automation, behavioral intelligence, and unified threat visibility. A resilient enterprise cannot rely on human-speed response when adversaries move across systems in minutes, nor can it depend on siloed tools that generate fragmented insights. Instead, resilience emerges from unified AI-driven platforms, automated containment workflows, and a structured roadmap that evolves from immediate hardening steps to long-term adaptive security programs.



Critical Actions for Resilience:

1. Establish baseline monitoring across users, devices, and infrastructure before advancing to detection and response capabilities.
2. Enable behavioral analytics to detect credential misuse and privilege escalation tied to active threat campaigns.
3. Implement automated response to contain data theft attempts and lateral movement in real-time.
4. Extend monitoring across all critical assets including cloud, remote, and hybrid environments.
5. Align defenses to current threat landscape documented in security advisories and threat intelligence reports.

Conclusion

Salt Typhoon demonstrates how deeply advanced actors can penetrate global infrastructures when organizations rely on traditional, fragmented security tools. The campaign's multi-year persistence across more than 200 organizations highlights the limitations of signature-based detection, partial visibility, and manual response workflows. As attackers increasingly exploit VPN devices, routers, identity systems, and cloud environments, enterprises must adopt defenses capable of continuously analyzing behavioral patterns, correlating events across domains, and identifying subtle indicators of compromise that conventional tools consistently miss.

This whitepaper demonstrates how unified, AI-driven platforms could strengthen defensive capabilities against advanced threats. By integrating SIEM, UEBA, NTA, and SOAR into a single system, platforms like Seceon enable detection acceleration and automated containment to help prevent large-scale data theft and unauthorized access. Achieving resilience against advanced threat campaigns requires this level of visibility, speed, and automation. Organizations that embrace unified AI security will be better positioned to detect threats early, disrupt malicious activities, and prevent the multi-year compromise scenarios exemplified by Salt Typhoon.

Salt Typhoon Cyber Espionage Reality Check

Why Traditional Approaches Fail and How Seceon aiSIEM Succeeds

Four Pillars of Challenges



200+
Organizations compromised across 80+ countries



9
Major US telecom providers breached



1M+
Users with metadata exposed




1-2 Years
Average dwell time before detection

Current Threat Level



Zero-Day
VPN/Firewall exploits for initial access



Rootkits
Custom backdoors for persistent access



Stealth
Low-volume encrypted exfiltration



\$500M-\$1B+
Estimated financial impact per victim

Current Problems

- **Signature-based failure:** Custom malware evades traditional antivirus detection
- **Agent blindness:** Cannot monitor routers, VPNs, or firewalls - key entry points
- **Rule-based SIEM:** Excessive false positives cause alert fatigue
- **DLP limitations:** Tuned for high-volume transfers, misses slow exfiltration
- **IAM context gap:** Stolen credentials used freely without behavioral detection
- **Human-speed response:** Too slow to contain rapid attacker lateral movement

Seceon Solution

- **AI-SIEM:** Machine learning-driven analysis with dynamic baselining and real-time correlation
- **UEBA:** Detects credential misuse, privilege escalation, and abnormal user/device behavior
- **Network Traffic Analytics:** Agentless monitoring with beaconing and C2 detection
- **Cumulative tracking:** Identifies low-volume exfiltration patterns over time
- **Behavioral analytics:** Flags impossible travel and anomalous admin activity
- **SOAR automation:** Sub-two-minute containment workflows with automated response

Results



95%+
Threat Containment Rate



16,000%
Faster Detection Speed



\$915.7M
Total Savings Per Incident



96%
Fewer False Positives

Why Seceon aiSIEM Against Salt Typhoon Now?

Nation-state espionage campaigns persist for years undetected. Stop multi-year compromise with AI-driven detection. Achieve sub-5-minute detection, sub-2-minute containment, and complete breach prevention across your infrastructure.

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:

- Cybersecurity and Infrastructure Security Agency (CISA). Guidelines on Advanced Persistent Threat Activity Targeting Telecommunications and Critical Infrastructure. 2023-2025 advisories.
- Seceon Security Research Team. Seceon aiSIEM Platform Performance Metrics. November 2025.
- MITRE ATT&CK Framework. Enterprise Tactics, Techniques, and Procedures (TTPs) Documentation.
- Industry Threat Intelligence Briefings and Telecommunications Sector Security Reports. 2024-2025.

About the Author

Madan Mohan Pandey

Principal Cybersecurity Architect, Seceon Inc.

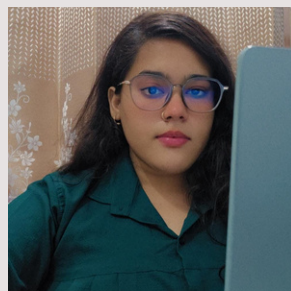


Madan is a software professional with strong experience in network design, application development, and cybersecurity engineering. He has worked extensively with the TCP/IP stack, routing and switching, and AWS services such as EC2 and S3. He has built automated CI/CD pipelines using Jenkins and Git to enable continuous testing and daily product updates. Madan also brings solid knowledge of EDR, XDR, MDR, and threat intelligence, along with an understanding of threats like ransomware, trojans, zero-day malware, botnets, and DNS tunneling. His experience with firewalls, IDS, IPS, VPNs, SIEM platforms, and log and netflow analysis helps him identify anomalies and support accurate threat detection across modern environments.

About the Author

Kamna Srivastava

AI/ML Cybersecurity Engineer, Seceon Inc.



Kamna specializes in leveraging artificial intelligence and machine learning to protect IT, OT, IoT, and cloud infrastructures. Her work focuses on strengthening enterprise security, ensuring compliance with industry standards, and delivering measurable ROI through Seceon's OTM Platform.