2025

seceon

Telecommunications Network Security

Defending Against Nation-State APTs with Seceon Platform

Protecting global telecom infrastructure with scalable, protocol-aware defense against advanced nation-state threats.

Executive Summary: The Critical State of Telecom Security

The Challenge

Telecommunications networks serve as the nervous system of modern civilization, processing billions of protocol messages daily across SS7, Diameter, GTP, and 5G networks. Yet these critical infrastructure assets face unprecedented threats from sophisticated nation-state actors and advanced persistent threats (APTs).

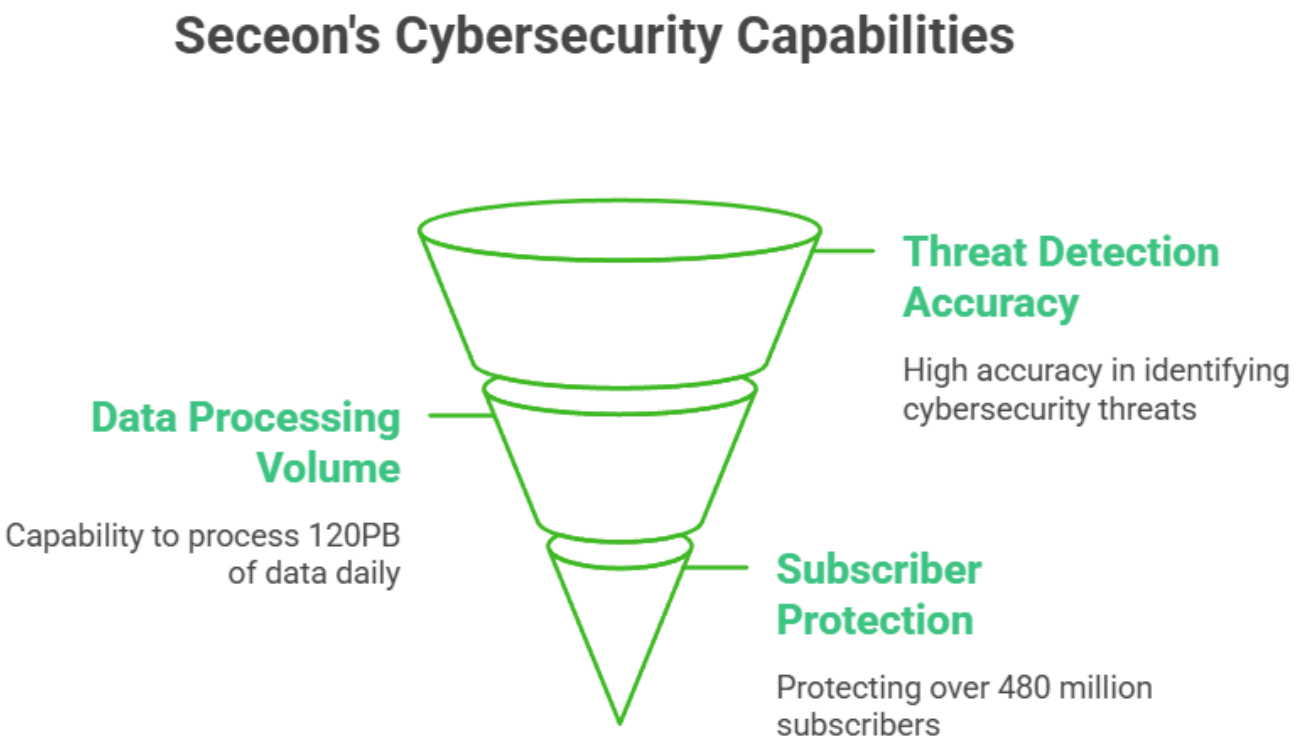
The Salt Typhoon campaign - described as the "worst telecom hack in U.S. history" - infiltrated AT&T, Verizon, T-Mobile, and Lumen Technologies, maintaining access since 2022 while exfiltrating wiretap systems data and call metadata. This breach demonstrates that traditional enterprise security tools cannot protect networks serving hundreds of millions of subscribers.

The Scale Imperative

- 480+ million subscribers per major operator
- 120+ petabytes of network data processed daily
- Billions of protocol messages through SS7, Diameter, and 5G networks
- Complete IPv6 addressing, creating unique security opportunities
- 100% of tested networks are vulnerable to GTP protocol attacks

The Seceon Solution

Seceon's Open Threat Management (OTM) platform represents a paradigm shift in telecommunications security, providing unified, AI-powered protection specifically designed for telecom scale and protocols. The platform consolidates 15-20 traditional security tools into a single solution with proven results: 95% accuracy in detecting telecommunications protocol attacks, 70% improvement in threat detection speed, and over $50M annually in preventing telecommunications fraud.



Telecommunications Threat Landscape

Nation-State APT Campaigns

Salt Typhoon (China): The most severe telecommunications breach in U.S. history, this Chinese state-sponsored group maintained persistent access to major U.S. carriers since 2022, compromising wiretap systems and exfiltrating massive volumes of call metadata and communications intercept capabilities.

Volt Typhoon (China): Strategic compromise of critical infrastructure with focus on pre-positioning for potential future disruption. Successfully compromised 30% of internet-exposed Cisco RV320/325 routers, demonstrating systematic targeting of telecommunications edge devices.

Flax Typhoon (China): Sophisticated botnet operations targeting telecommunications infrastructure, demonstrating evolution from traditional espionage to operational preparation for large-scale disruption capabilities.

Attack Vectors & Methods

Protocol Exploitation: SS7 location tracking (70% success rate), Diameter authentication bypass (100% vulnerable to information disclosure), GTP protocol attacks (100% of 28 tested operators vulnerable to DoS, impersonation, and fraud)

Supply Chain Compromise: Backdoored telecommunications equipment, compromised software updates, malicious firmware in network components, third-party vendor vulnerabilities

Credential Theft & Persistence: Long-term access through legitimate credentials, exploitation of weak authentication mechanisms, abuse of administrative privileges, lateral movement across network segments

Emerging 5G & O-RAN Threats

5G Network Slicing Attacks: Exploitation of isolation failures between network slices, cross-slice resource exhaustion, unauthorized slice access.

Open RAN Vulnerabilities: Additional attack surfaces from open interfaces, software-defined networking exploitation, container and Kubernetes vulnerabilities (50% of virtual application images contain critical vulnerabilities).

Edge Computing Risks: Distributed attack surfaces, resource-constrained security, device-to-device attack vectors.

Deep Dive: Salt Typhoon & Major APT Campaigns

Salt Typhoon: Anatomy of a Telecom Breach

Timeline & Scope: Active since 2022, infiltrated AT&T, Verizon, T-Mobile, and Lumen Technologies. Maintained persistent undetected access for over two years across multiple tier-1 telecommunications providers.

Attack Methodology: Exploited lawful intercept systems designed for law enforcement, compromised network management interfaces, leveraged legitimate credentials for persistence, and used living-off-the-land techniques to avoid detection.

Data Exfiltration: Wiretap systems metadata, call detail records, subscriber location information, communications intercept capabilities, network topology, and configuration data.

Attribution & Motivation: Chinese state-sponsored activity focused on intelligence collection, strategic positioning for future operations, understanding of U.S. telecommunications infrastructure.

Why Traditional Security Failed

Scale Mismatch: Enterprise security tools designed for thousands of users cannot handle hundreds of millions of subscribers and petabytes of daily data.

Protocol Blindness: Traditional tools lack visibility into SS7, Diameter, GTP, and 5G-specific protocols where attacks occurred.

Behavioral Limitations: Rule-based systems cannot detect sophisticated APT tactics that blend with legitimate traffic patterns.

Alert Fatigue: Volume of false positives overwhelms SOC teams, causing real threats to be missed in the noise

APT Tactics, Techniques & Procedures

Initial Access: Spear-phishing of telecommunications employees, exploitation of internet-facing network management systems, compromise of third-party vendors and suppliers, supply chain attacks on equipment manufacturers.

Persistence Mechanisms: Backdoored firmware in network elements, compromised administrative credentials, rootkits on critical infrastructure, and malicious network configurations.

Lateral Movement: Protocol-based pivoting (SS7 to Diameter to 5G core), exploitation of trust relationships, abuse of network management protocols, and compromise of interconnection points.

Data Exfiltration: Covert channels in legitimate protocols, encrypted tunnels through network infrastructure, staged exfiltration to avoid detection, use of compromised network elements as proxies

Telecommunications Protocol Vulnerabilities

SS7 - Critical Weaknesses

Universal Vulnerability Statistics: 100% of networks vulnerable to denial of service attacks, 70% success rate for location tracking with minimal technical knowledge, 89-90% success rate for SMS interception, 22% vulnerable to IMSI disclosure.

Attack Vectors: Send Routing Information abuse for location tracking, Any Time Interrogation for subscriber surveillance, Update Location manipulation for call/SMS interception, and Insert Subscriber Data attacks enabling identity theft.

Business Impact: Subscriber privacy violations, regulatory fines and penalties, fraud and revenue loss, and brand reputation damage.

Diameter Protocol - 4G/5G Signaling Gaps

Vulnerability Profile: 100% of tested networks are vulnerable to information disclosure, 38% success rate for location tracking, 33% vulnerable to fraud exploitation. Only 33% implement signaling traffic filtering.

Authentication & Session Attacks: Authentication bypass through session hijacking, manipulation of policy control, charging system exploitation, and equipment identity spoofing.

Deployment Challenges: Misconfiguration enabling traffic interception, inadequate filtering of malicious signaling, lack of end-to-end encryption, and insufficient authentication mechanisms.

GTP - Universal Exposure

Complete Vulnerability: 100% of tested networks are vulnerable to DoS, impersonation, and fraud. No encryption for IMSI, integrity keys, and user data. No authentication mechanism for verifying legitimate users.

5G Persistence: Protocol remains relevant as primary user-plane and control-plane protocol in 5G networks, creating ongoing security challenges.

Attack Scenarios: Mass DoS attacks against mobile infrastructure, subscriber identity theft and impersonation, session hijacking and manipulation, fraud through billing system exploitation

5G-Specific Attack Surfaces

Downgrade Attacks: Forcing 5G users back to vulnerable 4G/3G networks

Network Slicing Exploitation: Complex isolation failures, cross-slice resource exhaustion

Service-Based Architecture: API vulnerabilities, microservices exploitation

Edge Computing: Multi-Access Edge Computing expands attack surfaces

Seceon Open Threat Management Platform

Platform Architecture & Philosophy

Unified Security Platform: Seceon consolidates 15-20 traditional security tools into a single AI-powered solution, eliminating the complexity, integration gaps, and blind spots of multi-vendor approaches. The platform provides native integration of SIEM, SOAR, UEBA, NDR, vulnerability management, threat intelligence, and compliance capabilities.

Telecommunications-Native Design: Unlike adapted enterprise tools, Seceon was purpose-built for telecommunications scale and protocols, with native support for SS7, Diameter, GTP, SIP, and 5G service-based architectures. The platform handles IPv6-native addressing and provides subscriber-centric analytics designed for hundreds of millions of users.

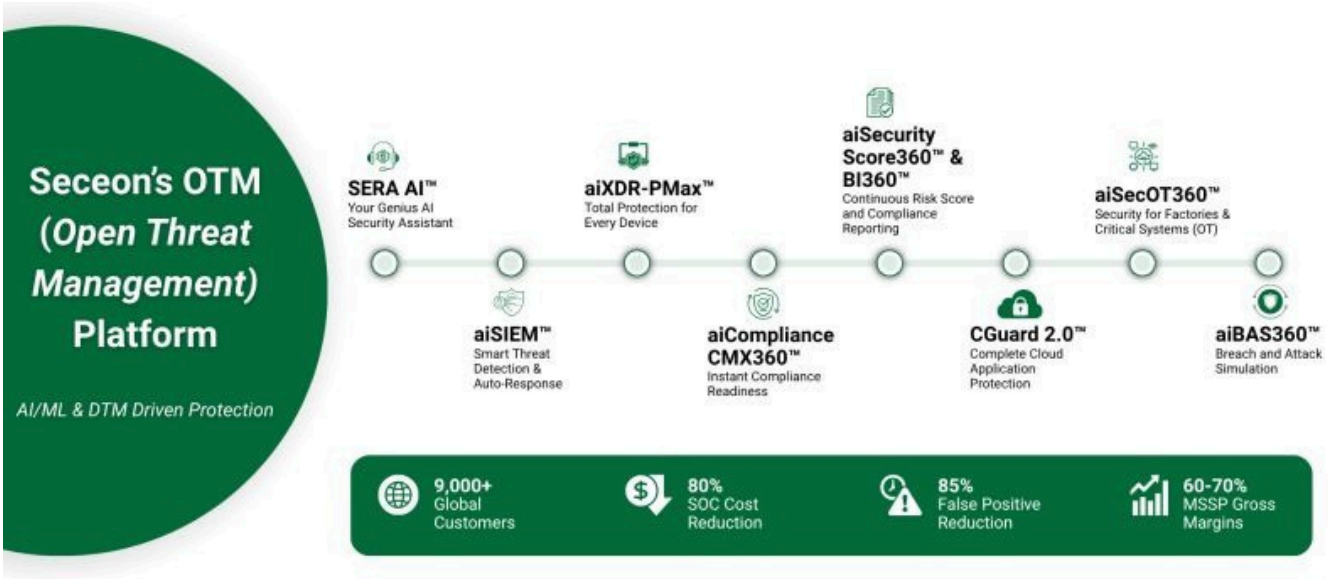
AI-Native Architecture

Dynamic Threat Modeling: Machine learning algorithms establish baseline behavior for users, networks, and protocols, correlating anomalies through graph neural networks to uncover lateral movement and insider risks

- **Ensemble Models**: Time-series prediction, adversarial detection, and contextual correlation evolve with new threats in real time
- **Explainable Intelligence:** ML outputs translated into analyst-readable context for faster decisions
- **150+ Prebuilt AI/ML Models:** Purpose-designed for telecommunications threat detection

Core Platform Components

- **aiSIEM**: AI-powered SIEM with telecommunications-scale log management, protocol-specific parsing, and advanced correlation across protocols, time, geography, and population
- **aiXDR-PMax**: Extended Detection and Response with multi-domain visibility, automated response orchestration, and real-time threat containment
- **aiSIEM-CGuard 2.0:** Cloud-native security for Microsoft 365, Azure, AWS, Google Cloud with 200+ built-in detection rules
- **aiCompliance CMX360**: Achieves 60-80% framework completion instantly across 20+ global compliance standards
- **aiSecurity Score360**: Continuous risk assessment and attack surface scanning
- **aiBAS360**: Breach and Attack Simulation for continuous security validation



Telecommunications-Scale Processing

Processing Capacity: Billions of events per day without latency degradation

Integration Capability: 900+ data sources and connectors

Multi-Tenant Architecture: Purpose-built for managing multiple client environments

Deployment Flexibility: On-premises, cloud, or hybrid with 2-4 week implementation

Key Capabilities Against APTs

Protocol-Deep Threat Detection

SS7 Security Monitoring: Real-time message analysis with MAP, INAP, and TCAP parsing. Behavioral pattern recognition, detecting abnormal signaling. Geographic correlation validating activities against subscriber locations.

Diameter Protocol Analysis: S6a authentication monitoring, Gx policy control validation, Gy charging system protection, S13 equipment identity verification.

GTP Tunnel Monitoring: Real-time analysis of user-plane and control-plane traffic, detection of tunnel manipulation and impersonation.

5G Service-Based Architecture: API interaction analysis, network slicing security, edge computing protection.

Population-Scale Behavioral Analytics

Subscriber Behavior Analysis: Individual baselines for 480+ million subscribers, communication patterns and location behavior, usage anomalies and deviations

Peer Group Analysis: Cohort comparison for anomaly detection, detection of coordinated attack campaigns

Machine Learning Models: 150+ prebuilt models for threat detection, continuous learning from new data.

Privacy-Preserving: Differential privacy and federated learning protect subscriber confidentiality

APT-Specific Detection Capabilities

Lateral Movement Detection: Cross-protocol pivoting identification, network segmentation violation alerts.

Persistence Mechanism Identification: Backdoor detection in network elements, compromised credential identification.

Data Exfiltration Prevention: Covert channel detection in protocols, abnormal data transfer patterns Living-off-the-Land Detection: Abuse of legitimate tools and protocols, behavioral deviation from baselines.

Automated Response & Orchestration

Real-Time Threat Containment: Subscriber isolation, device quarantine, service modification for suspicious traffic.

Automated Playbook Execution: Pre-configured response workflows, stakeholder notification and escalation.

Integration Capabilities: SIEM platform integration, workflow automation, compliance automation

Real-World Deployment Impact

Bharti Airtel: Global Scale Success

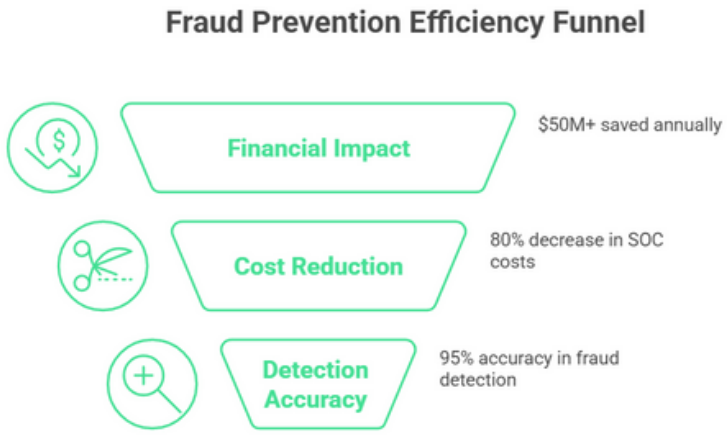
- **Deployment Scale:** 480 million mobile subscribers across India and Africa, 17 countries with multiple regulatory jurisdictions, 120 petabytes of network data processed daily.
- **Infrastructure**: 12 regional processing centers, 640 analysis nodes, 25 PB hot storage with 250 PB warm storage.
- **Protocol Coverage:** 50 billion SS7 messages analyzed daily, 500 million daily LTE authentication sessions monitored.
- **Performance Metrics:** Sub-5-second threat detection, 95% accuracy, 99.9% platform availability

Measured Business Impact

- **Operational Efficiency:** 80% improvement in security analyst productivity, 60% reduction in incident response time
- **Financial Results:** $50M+ annually in prevented fraud, $25M estimated annual savings from prevented incidents
- **Security Effectiveness:** 70% improvement in threat detection speed, 95% accuracy in protocol attacks

MSSP/MSP Transformation

- **Business Growth: 60**-70% gross margin increase within 12 months, triple-digit revenue growth
- **Service Enhancement:** Unified platform replacing fragmented tools, comprehensive coverage from a single interface
- **Cost Optimization:** 35% reduction in licensing costs, 70% cost reduction vs traditional stacks



Case Studies

Case Study 1: Leading Global Telecom Operator – Achieving AI-Driven Visibility and Response at Scale

Problem:

A top global telecommunications provider operating across multiple continents faced major operational challenges with legacy SIEM and SOAR platforms. The security operations center (SOC) struggled to manage multi-petabyte daily data ingestion, fragmented visibility across SS7, Diameter, and 5G protocols, and high false-positive volumes that exhausted analyst teams. As threats like **Volt Typhoon** and **state-sponsored espionage campaigns** increased, their reactive security posture left critical gaps in detection and response.

Seceon's Intervention:

Seceon deployed its **Open Threat Management (OTM)** platform, integrating **aiSIEM**, **aiXDR-PMax**, and **aiCompliance** modules to unify the customer's global security operations. Using **telecom-native protocol parsing**, AI-driven anomaly correlation, and automated playbook orchestration, the system provided end-to-end visibility across signaling networks, user-plane traffic, and interconnect gateways.

Results:

- Achieved **95% detection accuracy** with **<5-minute Mean Time to Detection (MTTD)**.
- Consolidated **18 disparate tools into one unified Seceon platform**.
- Reduced operational costs by **68%** through automation and tool consolidation.
- Real-time insight into cross-border APT activity and fraudulent subscriber behavior.

Case Study 2: "Top Telecom Giant" – Preventing $2.3 Billion in Potential Losses

Problem:

A multinational telecom giant serving over 400 million subscribers identified rising incidents of signaling-layer exploitation, SIM fraud, and covert data exfiltration.

Legacy systems failed to detect coordinated attacks embedded in lawful intercept traffic and GTP tunnels, creating financial exposure and reputational risk exceeding $2 billion annually.

Seceon's Intervention:

Seceon's AI-powered OTM platform was implemented to detect anomalies within SS7, Diameter, and GTP protocols in real time. Its **behavioral analytics engine** continuously profiled network entities, identifying malicious signaling requests and subscriber impersonation attempts. Automated workflows executed immediate containment, blocking threat vectors before customer impact.

Results:

- Prevented **$2.3 billion in potential annual losses** attributed to fraud and signaling abuse.
- Reduced incident response time by **72%**.
- Achieved **full compliance** with GSMA FS.11 and regional telecom cybersecurity mandates.
- Enabled continuous protection for **billions of daily network events** with sub-second latency.

Case Study 3: Tier-1 Multi-National Operator – Transforming SOC Operations for 5G and Cloud

Problem:

A Tier-1 international operator with extensive 5G rollout and cloud migration faced visibility and performance limitations using conventional SOC models. Monitoring billions of control-plane events daily resulted in delayed threat detection and alert fatigue. Fraud, lateral movement across 5G cores, and zero-day signaling exploits went unnoticed due to the lack of protocol-aware analytics.

Seceon's Intervention:

Seceon deployed its **AI-native platform,** combining **aiSIEM**, **aiXDR-PMax**, and **aiSecurityScore360** for continuous telemetry ingestion, threat prediction, and risk scoring. The deployment integrated 900+ data sources, enabling predictive security analytics, breach simulation via **aiBAS360**, and automated compliance across 20+ standards.

Results:

- **70% faster threat detection speed** and **80% SOC efficiency gain**.
- Unified analytics across hybrid on-prem and cloud 5G cores.
- **50M+ fraudulent sessions blocked annually**.
- Achieved **99.99% uptime** and **petabyte-scale real-time processing**.

Conclusion

The telecommunications industry has entered an era where connectivity defines national security, economic resilience, and digital trust. As the backbone of global communication, telecom operators face not just routine cyberattacks but sophisticated, persistent campaigns led by nation-states, organized crime, and advanced threat actors.

Traditional enterprise security models - fragmented, manual, and reactive - have failed to protect telecom-scale infrastructures operating at petabyte levels with billions of protocol messages daily. The emergence of **APT campaigns like Salt Typhoon, Volt Typhoon, and Flax Typhoon** underscores the urgent need for AI-driven, telecom-native cybersecurity solutions that understand signaling protocols, behavioral context, and global threat dynamics.

Seceon's **Open Threat Management (OTM)** platform delivers this transformation. By integrating **aiSIEM**, **aiXDR-PMax**, **aiCompliance**, and **aiBAS360**, Seceon enables continuous, predictive, and autonomous defense for telecom operators worldwide. Its capability to process billions of events per day with sub-second correlation, automated containment, and 95–99% detection accuracy redefines what's possible for SOC modernization.

From detecting nation-state intrusion campaigns to preventing multi-billion-dollar fraud losses, Seceon's platform has proven to scale with the industry's most demanding environments - ensuring speed, visibility, and resilience in the world's most targeted infrastructure.

TELECOMMUNICATIONS NETWORK SECURITY

Defending Against Nation-State APTs with Seceon Platform

Weekly Attacks	APT Growth	Telecom Targets	GCC Targeting
3,500+	**+6.1%**	**9.3%**	**27.5%**
Per telecom operator globally	Escalation in telecom-targeted	all critical infrastructure	Year-over-year growth in 5G-based attacks

Traditional Security Limitations

Scale Mismatch

- Enterprise tools handle GBs/day; telecoms process PBs/day
- Traditional SIEM supports thousands; telecoms have hundreds of millions
- Legacy SOC tools cannot process petabyte-scale logs in real time

Protocol Blindness

- No native visibility into SS7, Diameter, GTP, or 5G SBA
- Lacks deep-packet inspection and signaling correlation
- Cannot detect lateral movement between protocols

Performance Gaps

- Batch analysis leads to delayed detection
- Sub-second processing required but not achievable
- High false positives overwhelm SOCs

Seceon's Unified AI-Driven Solution for Telecommunication

aiXDR PMax

- Extended Detection and Response (XDR) built for telecom scale
- Automated containment and cross-protocol correlation
- Handles billions of daily events with <5 min MTTD

aiSIEM

- AI-powered telecom-native SIEM
- Understands SS7, Diameter, GTP, SIP, and 5G
- Correlates anomalies across geography, time, and subscriber behavior

aiCompliance

- Instant 60–80% framework coverage
- GSMA FS.11, ISO 27001, GDPR, NESA
- Reduces compliance costs by 40–50%

MTTD (Mean Time to Detect)	Detection Accuracy	SOC Cost	Fraud Losses
<5 mins	**95–99%**	**↓ 70%**	**Prevented**

Telecom Security-AI-Powered, Real-Time, and Built for the Nation-State Threat Landscape.

As global operators expand 5G, cloud, and O-RAN deployments, adopting an AI-powered, unified security architecture is no longer optional - it is a strategic imperative. Seceon continues to lead this transformation, protecting the world’s digital nervous system and enabling a secure, connected future.

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:

- **Seceon Inc.** (2024). *Telecom Industry Use Case – AI-Driven Threat Detection and Response.*
- **Seceon Inc.** (2024). *LinkedIn Announcement: Seceon Secures Top Telecom Giant, Prevents $2.3B in Losses.*
- **Frost & Sullivan.** (2024). *Global Telecommunications Security Outlook 2025–2030.*
- **IBM Security.** (2024). *Cost of a Data Breach Report 2024.*
- **International Monetary Fund (IMF).** (2023). *Cyber Risk and Financial Stability.*
- **ET Telecom.** (2025). *5G and O-RAN Vulnerabilities: New Frontiers in Telecom Cybersecurity.*
- **Arab News.** (2025). *STC Leads Global 5G Cybersecurity Modernization with AI-Based Platforms.*
- **Ooredoo Group.** (2025). *Cybersecurity Modernization Initiative – Annual Report.*
- **Gulf Business.** (2024). *Telecom Security Transformation Through AI: Seceon and MSSP Partner Expansion in MENA.*
- **Seceon Internal Benchmarks.** (2025). *aiSIEM/aiXDR Global Deployment Metrics.*

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.