

2026

seceon

Telecom Cybersecurity: Protecting Every Layer of the Telecom Stack

How Seceon OTM Defends 14 Telecom Technology Layers with AI-Powered, Unified Security

Executive Summary

Telecommunications networks carry voice, data, signaling, and control information for billions of users and critical national systems. Their complexity - multi-vendor hardware, legacy protocols coexisting with cloud-native 5G Network Functions, OT systems at thousands of tower sites, and millions of IoT endpoints - creates an attack surface that no combination of point security tools can adequately cover.

This whitepaper maps each of the 14 major telecom technology layers against their most significant threat vectors, and demonstrates how the **Seceon Open Threat Management (OTM) Platform** - with its 15 integrated AI/ML-powered modules - defends all of them from a single unified platform at carrier-grade scale.

2.4T	9,800+	95%	<90 Sec
Security Events / Day	Organizations Protected	False Positive Reduction	Automated Response

> *Telecom is the #2 most targeted sector for nation-state cyberattacks globally. A single SS7 exploit can expose subscriber location and intercept communications for millions of users simultaneously, often with zero detection by conventional tools.*

Why Telecom Security Is Different

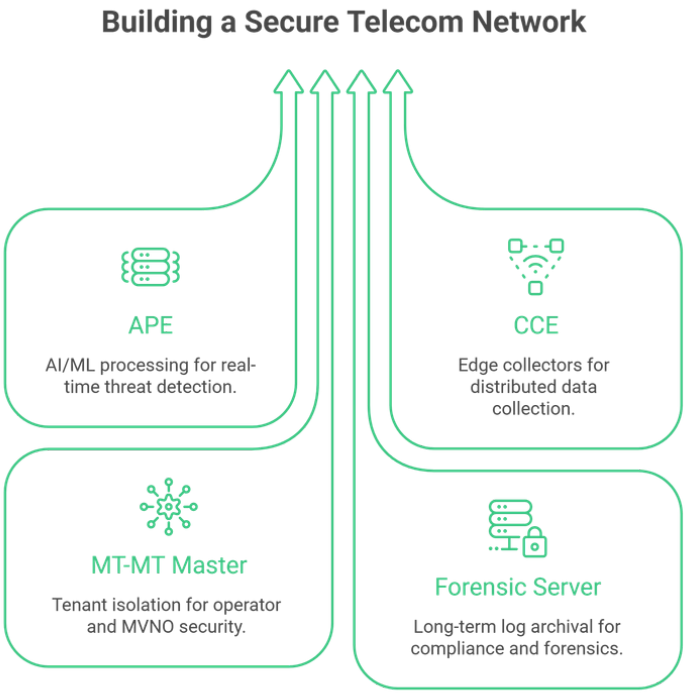
Telecom environments present security challenges that generic enterprise tools cannot address:

- **Massive scale and heterogeneity -** millions of endpoints, hundreds of protocols, multi-vendor hardware from Ericsson, Nokia, Huawei, Cisco, and Juniper
- **Protocol diversity -** BGP, SS7, Diameter, GTP, SIP, IEC 61850, Modbus, SNMP, NETCONF/YANG, and dozens of proprietary OT protocols
- **Legacy and modern coexistence -** 2G/3G/4G equipment running alongside 5G cloud-native Network Functions in the same NOC
- **Critical infrastructure status -** telecom outages have national security, economic, and public safety consequences
- **Regulatory obligations -** lawful intercept, TRAI, EU NIS2, FCC, NERC CIP, GDPR, and national cybersecurity frameworks - simultaneously
- **Insider threat exposure -** administrators with access to subscriber data, billing, and network configuration represent high-value targets
- **Supply chain and interconnect risk -** roaming partners and MVNO interconnect points introduce untrusted traffic and potentially compromised equipment

The Seceon OTM Platform - Architecture for Telecom

Seceon OTM is a unified platform built on a distributed analytics and collection architecture engineered for high-throughput, multi-site environments. Its three-tier architecture maps directly to how telecom operators build their networks:

Component	Role & Telecom Application
APE (Analytics & Processing Engine)	Core AI/ML processing cluster for national NOC/SOC integration, capable of processing up to 150M events per second using Spark Streaming.
CCE	Distributed edge collectors deployed across Points of Presence (PoPs), core network sites, and regional data centers for localized data collection and processing.
MT-MT Master	Federated multi-tier, multi-tenant controller providing secure separation and management of operator and MVNO environments.
Forensic Server (LTS)	Long-term raw log archival for up to 7 years to support lawful intercept requirements, forensic investigations, and regulatory compliance.



The 15 Seceon OTM Modules:

Module	Primary Function
aiSIEM	AI-driven SIEM platform capable of processing 50B+ events per day and 150M events per second, while reducing false positives by up to 95%.
aiXDR	Extended Detection and Response across network, endpoint, cloud, and identity environments with comprehensive MITRE ATT&CK framework coverage.
SOAR 4.0	GenAI-powered orchestration and automated response platform delivering remediation in under 90 seconds with support for 950+ integrations.
NDR	Network Detection and Response with Deep Packet Inspection (DPI), encrypted traffic analysis, and support for OT/ICS protocols.
UEBA	User and Entity Behavior Analytics leveraging 4,000+ machine learning behavioral models to detect insider threats, privilege abuse, and credential compromise.
aiIDGuard*	Agentless identity discovery and correlation across 60+ platforms with 98% fuzzy match accuracy. (Coming Soon)
aiITDR	Identity Threat Detection and Response platform designed to identify impossible travel scenarios, Active Directory attacks, and identity-based threats with 99%+ detection accuracy.
TI360	Threat intelligence platform integrating 100+ intelligence feeds, 2B+ Indicators of Compromise (IOCs), and advanced DGA detection capabilities.
CMX360	Automated compliance management supporting 45+ regulatory frameworks, including NIST, GDPR, NERC CIP, PCI-DSS, and ISO 27001.
aiITSM	AI-driven IT Service Management with MITRE-mapped workflows, 40% faster MTTR, and integration with platforms such as ServiceNow and JIRA.
aiBAS360	Continuous Breach and Attack Simulation platform for kill-chain validation aligned with the MITRE ATT&CK framework.
aiSecOT360	OT and IoT security solution offering passive asset discovery, ICS/SCADA visibility, Purdue Model alignment, and IEC 62443 support.

Module	Primary Function
aiSecurityScore360	Provides a real-time 0–100 cybersecurity risk posture score with predictive risk probability and trend analysis.
Email AI*	AI-powered email security using machine learning and DistilBERT transformers to detect BEC and phishing attacks with 97% accuracy and sub-50ms response times. (Coming Soon)
aiSAT360*	Security awareness training platform featuring 500+ phishing templates, support for 30+ languages, and AI-powered coaching capabilities. (Coming Soon)

Telecom Technology Landscape

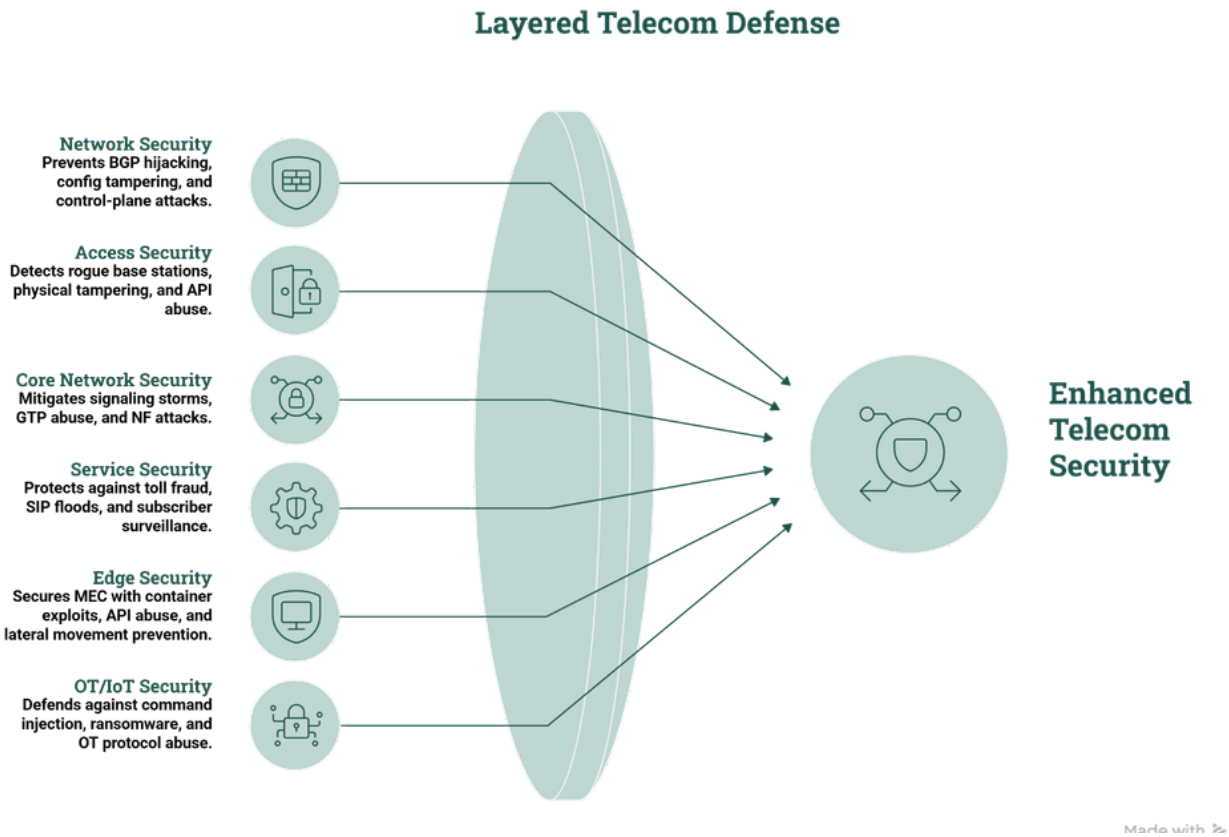
Threats, Breach Vectors & Seceon OTM Defenses Across All 14 Technology Layers

The sections below examine each of the 14 major technology layers that make up a modern telecom operator's stack. For every layer this whitepaper covers: what the technology does, how attackers exploit it, and exactly how Seceon OTM detects, responds to, and prevents those attacks in real time.

Technology Domain	Primary Breach / Risk	Focus Category
Carrier-Grade Routers & Switches	BGP hijacking, configuration tampering, and control-plane attacks targeting critical network infrastructure.	Network
Firewalls & NGFW	Security rule misconfigurations, management plane compromise, and traffic evasion techniques.	Network
Radio Access Network (RAN / Open RAN)	Rogue base stations, physical tampering, and API abuse affecting radio infrastructure.	Access
EPC & 5G Core Network Functions	Signaling storms, GTP abuse, and attacks targeting cloud-native network functions.	Core

Technology Domain	Primary Breach / Risk	Focus Category
IMS, VoIP & Session Border Controllers	Toll fraud, SIP flooding attacks, and media stream interception.	Core
SS7, Diameter & Interconnect Gateways	Subscriber surveillance, SMS interception, and telecom protocol abuse.	Core
DNS, DHCP & NTP Services	Cache poisoning, DGA/C2 resolution, and amplification-based DDoS attacks.	Services
AAA, HSS & Subscriber Identity Stores	Credential theft, SIM cloning, and billing manipulation attempts.	Services
OSS/BSS & Provisioning Systems	Insider threats, data exfiltration, and supply chain compromise risks.	Services
Multi-Access Edge Compute (MEC)	Container exploitation, API abuse, and cross-tenant lateral movement attacks.	Edge
OT & Site Control Systems (SCADA/BMS)	Command injection, ransomware propagation, and OT protocol abuse.	OT/IoT
IoT Devices & Gateways (NB-IoT / LPWAN)	Botnet recruitment, unauthorized onboarding, and data poisoning attacks.	OT/IoT
IDS/IPS & DDoS Mitigation	Signature evasion techniques, signaling floods, and improperly tuned detection rules.	Security
Security Infrastructure (SIEM/XDR/KMS)	Telemetry manipulation, cryptographic key theft, and supply chain attacks targeting security platforms.	Security

Each section is structured identically: a technology overview, a threat-to-defense mapping table showing the attack vector and the specific Seceon OTM capability that counters it, followed by the exact platform modules engaged.



Carrier-Grade Routers & Switches

Routers and switches form the data-plane backbone of every telecom operator. Carrier-grade platforms (Cisco CRS/NCS, Juniper PTX, Nokia SR, Huawei NE) run BGP, OSPF, IS-IS, MPLS, and segment routing at terabit scale. Any compromise can redirect or black-hole national traffic flows.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
BGP Route Hijacking / Route Leaks	aiSIEM and NDR detect abnormal BGP update patterns and route anomalies, while SOAR 4.0 can automatically block sessions originating from unauthorized ASNs in under 90 seconds.

Attack Vector / Threat	Seceon OTM Defense Capability
Management Plane Credential Theft (SSH, SNMP)	aiITDR and UEBA identify anomalous administrator logins and privileged access behavior, while aiIDGuard provides a unified inventory of administrative identities across environments.
Firmware Supply Chain / Backdoor Compromise	aiXDR detects unexpected processes, communications, and behavioral changes following firmware updates, while TI360 correlates indicators against known firmware-related threat actors and campaigns.
Control Plane CPU Floods	NDR leverages Deep Packet Inspection (DPI) to identify control-plane flooding attacks, while SOAR 4.0 can automatically enforce upstream ACLs and rate-limiting actions.
Unauthorized Configuration Changes	aiSIEM establishes configuration baselines and generates alerts on unauthorized modifications, while CMX360 continuously validates compliance against frameworks such as NERC CIP and NIST 800-53.

Firewalls & Next-Generation Firewalls (NGFW)

NGFWs enforce perimeter and internal segmentation policy across telecom environments - protecting core, edge, peering, and data center boundaries. In telecom, firewall rulesets can contain tens of thousands of rules managing inter-AS, roaming partner, and service provider traffic.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Misconfigured / Overly-Permissive Rules	CMX360 and aiSIEM provide continuous rulebase auditing against defined policy baselines, while aiSecurityScore360 identifies and flags configuration drift that increases risk exposure.

Attack Vector / Threat	Seceon OTM Defense Capability
Admin Credential Theft / Management Compromise	aiIDGuard and aiITDR deliver administrator identity discovery, privileged access monitoring, and impossible travel detection, while SOAR 4.0 can automatically initiate credential revocation and containment actions.
Encrypted Payload Hiding / Application Evasion	NDR performs encrypted traffic analysis without requiring decryption, while TI360 correlates activity against known command-and-control (C2) infrastructure and DGA-generated domains.
Firewall Bypass via Protocol Tunneling	NDR and aiXDR provide multi-layer correlation across network and endpoint telemetry to detect protocol tunneling and evasion techniques that single-layer security controls may miss.

Radio Access Network (RAN) - BBU, RRH, Open RAN

The RAN encompasses Baseband Units (BBUs), Remote Radio Heads (RRHs), and in 5G Open RAN, Distributed/Central Units (DU/CU). Their distributed physical presence at thousands of tower sites - often with limited physical security - creates a broad and heterogeneous attack surface.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Physical Tampering at Tower Sites / Equipment Theft	aiSecOT360 and aiSIEM correlate physical security alarms with network events and operational anomalies to rapidly identify tampering or unauthorized access attempts.
Rogue Base Stations / IMSI Catchers	NDR and aiSIEM detect indicators such as mass user equipment re-registrations, abnormal handover activity, and rogue eNodeB signatures associated with IMSI catcher attacks.

Attack Vector / Threat	Seceon OTM Defense Capability
Insecure Management Interfaces (Default Credentials)	aiIDGuard discovers and inventories management accounts, UEBA establishes administrator access baselines, and aiITDR detects credential misuse and privilege abuse.
Open RAN API Abuse (O1/O2/E2 Interfaces)	aiXDR and NDR identify API anomalies, unauthorized requests, and suspicious xApp behavior across Open RAN controller interfaces including O1, O2, and E2.

EPC & 5G Core Network Functions

5G decomposes core functions into cloud-native Network Functions (AMF, SMF, UPF, AUSF, UDM, PCF) exposing HTTP/2-based APIs on a Service-Based Architecture (SBA). This cloud-native transformation dramatically increases API attack surface while enabling greater agility.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Signaling Storms / Control-Plane Resource Exhaustion	NDR and aiSIEM detect sudden spikes in attach and authentication requests, session churn, and bearer setup anomalies indicative of signaling storms and resource exhaustion attacks.
GTP / Diameter Protocol Abuse (Traffic Tunneling, Billing Fraud)	NDR provides DPI-based analysis of GTP and Diameter traffic, while aiSIEM correlates billing records with session events to identify fraud and protocol abuse.
5G SBA API Compromise (Weak mTLS, Unauthenticated NF Access)	aiXDR and NDR detect unauthorized API communications between Network Functions (NFs), while aiIDGuard discovers and inventories NF service accounts.

Attack Vector / Threat	Seceon OTM Defense Capability
Cloud-Native NF Container Compromise / Lateral Movement	aiXDR correlates container telemetry and runtime activity, while NDR identifies anomalous east-west traffic patterns and lateral movement between NF pods.

IMS, VoIP & Session Border Controllers (SBCs)

VoIP fraud (toll fraud) remains one of the highest-impact threats in telecom losses, exceeding $38 billion annually (CFCA). SBCs sit at network borders protecting SIP/RTP traffic between operators and enterprise customers.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Toll Fraud (SIP Registration Spoofing, Unauthorized Call Routing)	UEBA establishes per-subscriber calling behavior baselines, while aiSIEM detects anomalies such as excessive call durations, unusual calling patterns, and premium-rate number abuse.
SIP INVITE Flood / VoIP DDoS	NDR identifies abnormal SIP request rates and signaling patterns, while SOAR 4.0 can automatically enforce rate-limiting actions through SBC APIs. TI360 correlates activity against known VoIP attacker infrastructure and malicious IP addresses.
RTP Eavesdropping / Media Stream Interception	NDR detects unencrypted RTP streams, unexpected media routing paths, and suspicious traffic flows, while TI360 correlates against indicators associated with known interception infrastructure.
Vishing / Social Engineering via Telecom Infrastructure	Email AI helps identify inbound phishing and social engineering attempts, while aiSAT360 strengthens employee awareness through AI-driven security awareness training focused on vishing recognition and response.

SS7, Diameter & Interconnect Protocol Gateways

Protocol gateways bridge legacy SS7 with IP-based Diameter and SIP. SS7 and Diameter vulnerabilities are actively exploited by state actors and criminal organizations for location tracking, SMS interception, and subscriber data extraction - often from roaming interconnect abuse.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
SS7 Location Tracking / Subscriber Surveillance (MAP Abuse)	NDR detects anomalous MAP SendRoutingInfoForSM requests and signaling behavior, while aiSIEM correlates events with potential subscriber impact. TI360 enriches detections using intelligence on known SS7 attacker ASNs and threat infrastructure.
SMS Interception via SS7 MAP Exploitation	NDR performs deep analysis of SS7 MAP messages to identify interception attempts, while SOAR 4.0 can automatically block or isolate malicious MAP signaling sources.
Malicious Signaling from Fraudulent Roaming Partners	aiSIEM establishes behavioral baselines for interconnect and roaming partners, UEBA identifies abnormal signaling volumes and usage patterns, and SOAR 4.0 can automatically terminate suspicious partner sessions.
Diameter Protocol Abuse (Session Hijacking, DoS)	NDR provides deep packet inspection of Diameter traffic, while aiXDR correlates signaling anomalies with subscriber session behavior and potential billing impacts to identify hijacking and denial-of-service attempts.

DNS, DHCP, NTP & Core Infrastructure Services

DNS, DHCP, and NTP are foundational services every other telecom system depends on. Compromise cascades across authentication, routing, billing, and operational systems. In telecom, DNS resolves billions of queries daily - including C2 lookups from malware using Domain Generation Algorithms (DGA).

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
DNS Cache Poisoning / Subdomain Takeover	aiSIEM and NDR detect anomalous DNS query behavior, spikes in NXDOMAIN responses, and unusual TTL patterns, while TI360 correlates activity with known poisoned domains and malicious infrastructure.
DNS Amplification DDoS	NDR identifies amplification traffic patterns and volumetric anomalies, while SOAR 4.0 can automatically initiate upstream BGP RTBH (Remotely Triggered Black Hole) routing and ACL enforcement to block malicious sources.
DGA / C2 Domain Resolution by Malware-Infected Assets	TI360 leverages a database of over 2B Indicators of Compromise (IOCs) and a DGA prediction engine to identify malicious domains, while aiSIEM correlates suspicious DNS lookups with endpoint and user context.
Rogue DHCP Servers (MITM for Gateway / DNS)	aiSIEM detects unauthorized DHCP offers through network telemetry and DHCP snooping data, while UEBA correlates abnormal lease events and suspicious client behavior indicative of man-in-the-middle activity.

AAA, HSS & Subscriber Identity Stores

RADIUS authenticates broadband and enterprise customers; HSS/HLR stores 4G/5G subscriber profiles; AUSF/UDM manages authentication in 5G SA core. Compromise of these systems enables mass identity theft, fraudulent billing, and service disruption at scale.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Credential Theft / Replay Attacks on RADIUS/AAA	aiITDR and UEBA detect anomalous authentication patterns and credential misuse, while aiIDGuard maintains a unified credential inventory across environments. SOAR 4.0 can automatically trigger credential resets and containment actions in under 90 seconds.
IMSI/MSISDN Cloning / SIM Swapping Fraud	UEBA and aiSIEM identify duplicate identity usage and suspicious subscriber activity, while aiIDGuard correlates identities across systems to detect fraud indicators. SOAR 4.0 can automatically initiate subscriber freezes and response workflows.
Unauthorized Access to Subscriber Databases	UEBA detects abnormal database access patterns and data retrieval behavior, while aiITDR identifies privilege escalation chains and identity-based attacks. SOAR 4.0 can suspend compromised accounts to contain threats rapidly.
Forged Accounting Records (Billing Manipulation)	aiSIEM establishes integrity baselines for accounting and billing records to identify tampering attempts, while CMX360 supports compliance validation and audit controls aligned with frameworks such as SOX and PCI-DSS.

OSS/BSS, Management Consoles & Provisioning Systems

OSS and BSS are the operational brain of a telecom operator - managing provisioning, billing, CRM, inventory, and orchestration. They are prime insider threat targets due to rich data access, and attractive external targets due to their integration with virtually every other network system.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Insider Abuse by Privileged Administrators (Billing, CRM, SIM)	UEBA: admin behavior baseline; aiITDR: privilege chain detection; SOAR 4.0: JIT access revocation
Mass Provisioning Changes (SIM Swaps, Number Porting Fraud)	UEBA: bulk provisioning anomaly; aiSIEM: high-volume change events; SOAR 4.0: automated quarantine
BSS Data Exfiltration (Subscriber PII, Payment Data)	aiITDR + UEBA: data exfiltration detection; SOAR 4.0: credential blocking; CMX360: GDPR/PCI-DSS controls
Supply Chain / Third-Party API Compromise	aiIDGuard: API key and service account inventory; NDR: unexpected API call patterns from partner integrations

Multi-Access Edge Compute (MEC) & Edge Servers

MEC brings compute to the network edge for ultra-low latency applications. MEC nodes run containerized workloads from multiple tenants - including third-party developers - creating significant tenant isolation and supply chain risk alongside standard cloud-native security challenges.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Vulnerable Container Images / Insecure CI/CD Pipeline	aiXDR: container runtime anomaly detection; TI360: known malicious registry IOCs; aiBAS360: CI/CD pipeline simulation
API Abuse by Malicious Edge Applications	NDR + aiXDR: API call pattern anomaly; aiIDGuard: edge API key inventory; SOAR 4.0: application isolation
Cross-Tenant Lateral Movement at Edge	NDR: east-west traffic baseline between tenant segments; aiXDR: container escape detection; SOAR 4.0: tenant isolation

OT & Site Control Systems (SCADA, PLCs, BMS)

MEC brings compute to the network edge for ultra-low latency applications. MEC nodes run containerized workloads from multiple tenants - including third-party developers - creating significant tenant isolation and supply chain risk alongside standard cloud-native security challenges.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Unauthorized Command Injection (Shutdown / Physical Disruption)	aiSecOT360: passive OT traffic analysis; NDR: protocol-aware command validation; SOAR 4.0: OT network isolation
Ransomware Propagation into OT via IT/OT Convergence	aiXDR: kill-chain detection at IT/OT boundary; SOAR 4.0: automated firewall isolation; aiBAS360: ransomware simulation
Firmware Tampering via Compromised Maintenance Tools	aiXDR + aiSecOT360: detect unexpected firmware change events; UEBA: maintenance engineer access anomaly

Attack Vector / Threat	Seceon OTM Defense Capability
Exposed OT Protocols (Modbus, DNP3, BACnet) on Network	aiSecOT360: protocol-specific detection; NDR: unexpected OT protocol traffic; CMX360: IEC 62443 / NERC CIP compliance

IoT Devices & Gateways (NB-IoT, LPWAN, 5G IoT)

Telecom operators connect billions of IoT devices - smart meters, connected vehicles, industrial sensors - through their networks. Resource-constrained devices, infrequent patching, and massive deployment scale create a persistent security challenge that traditional endpoint tools cannot address.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Default Credential Takeover and Botnet Enlistment (Mirai variants)	aiSecOT360: IoT device discovery; UEBA: device behavioral baseline; TI360: botnet C2 IOCs; NDR: scanning/beaconing detection
Mass Rogue Device Onboarding / Resource Exhaustion	aiSecOT360: new device fingerprinting; aiSIEM: mass onboarding anomaly; aiIDGuard: device identity correlation
Unauthenticated Telemetry Injection (Data Poisoning)	NDR: detect protocol anomalies and unexpected telemetry sources; UEBA: device traffic baseline deviation

IDS/IPS & DDoS Mitigation Systems

IDS/IPS inspect traffic for malicious patterns while DDoS mitigation platforms detect and divert volumetric and application-layer floods. In telecom, threats include signaling floods, GTP flood attacks, and amplification abuse using the carrier infrastructure itself.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
Signature Evasion (Fragmentation, Obfuscation, Encryption)	NDR: behavioral detection without signature dependency; aiXDR: multi-stage correlation catching evasion patterns
High-Volume Floods Saturating Mitigation Capacity	SOAR 4.0: automated BGP FlowSpec / RTBH announcement; NDR: volumetric anomaly with geo-correlation
Signaling Flood Attacks (SIP, GTP, Diameter)	NDR + aiSIEM: protocol-specific rate anomaly detection for GTP, SIP, Diameter signaling traffic
Mis-tuned Rules Creating False Positives / Missed Attacks	aiBAS360: continuous IDS/IPS validation and tuning guidance; aiSIEM: low-and-slow pattern correlation

Security Infrastructure (SIEM, XDR, KMS, HSM)

Security tools themselves are high-value targets - compromising a SIEM blinds the defender; corrupting KMS/HSM stores enables impersonation across the entire network. Seceon OTM addresses this through tamper-evident telemetry collection, signed data channels, and continuous self-validation.

Threat Landscape & Seceon OTM Defense

Attack Vector / Threat	Seceon OTM Defense Capability
SIEM/XDR Telemetry Tampering / Log Deletion	aiSIEM: multi-source correlation - loss of any feed triggers alert; signed telemetry verification checks
HSM / KMS Compromise / Cryptographic Key Theft	UEBA + aiITDR: HSM admin access anomaly; aiIDGuard: HSM operator identity governance; SOAR 4.0: access suspension
Security Tool Supply Chain Compromise	aiXDR: behavioral deviation detection post-update; TI360: known security tool supply chain IOCs
Misconfigured Automation Creating Disruptive False Blocks	aiBAS360: continuous playbook validation; SOAR 4.0: human-in-the-loop gates for high-impact actions

Compliance - Frameworks Covered by CMX360

CMX360 supports 45+ compliance frameworks simultaneously - covering every major telecom cybersecurity regulatory obligation from a single automation engine:

Framework	Applicability	CMX360 Outcome
NIST 800-53 / CSF	US Federal and Critical Infrastructure environments	Full control mapping with automated evidence collection and reporting.
NERC CIP	Power, Utility OT, and Telecom Facilities	OT and ICS control validation through aiSecOT360 and CMX360 integration.
IEC 62443	Industrial Control Systems (ICS) environments	Purdue Model segmentation validation and industrial protocol monitoring.
ISO 27001:2022	Global Information Security Management programs	Up to 95% automated evidence collection for audits and compliance activities.

Framework	Applicability	CMX360 Outcome
PCI-DSS	Payment card environments and billing systems	Monitoring and control validation for BSS platforms, billing systems, and cardholder data environments.
GDPR / PDPB	Subscriber and personal data protection requirements	PII discovery, monitoring, and exfiltration detection capabilities.
EU NIS2 Directive	European Critical Infrastructure organizations	Automated incident detection, reporting, and compliance workflows.
EU DORA	Digital Operational Resilience requirements for financial services	Continuous control validation and resilience testing through aiBAS360.
HIPAA / HITECH	Healthcare and healthcare convergence environments	PHI breach detection and insider threat monitoring capabilities.
CMMC 2.0 / FISMA	Defense contractors and government organizations	Support for air-gapped deployments and classified security controls.
3GPP Security Standards	4G and 5G Network Function security requirements	Continuous monitoring of 5GC APIs and Network Function security controls.
TRAI / DoT Guidelines	Indian telecom regulatory requirements	Regulatory control mapping and reporting support available on request.

CMX360 generates full cross-framework compliance reports in under 1 hour - a process that previously required 6 weeks of manual effort across 3 separate teams.

Technology-to-Module Master Reference

The table below shows which Seceon OTM modules provide primary defense coverage for each of the 14 telecom technology layers:

Technology Layer	Primary Seceon OTM Modules
Routers & Switches	aiSIEM, aiXDR, NDR, UEBA, SOAR 4.0, TI360, CMX360, aiSecurityScore360
Firewalls & NGFW	aiSIEM, aiXDR, NDR, UEBA, aiIDGuard, aiITDR, SOAR 4.0, CMX360, aiBAS360
IDS/IPS & DDoS	aiSIEM, aiXDR, NDR, UEBA, SOAR 4.0, TI360, aiBAS360
RAN (BBU/RRH/Open RAN)	aiSIEM, aiXDR, NDR, UEBA, aiIDGuard, aiSecOT360, SOAR 4.0, TI360
EPC & 5G Core (NFs)	aiSIEM, aiXDR, NDR, UEBA, aiIDGuard, aiITDR, SOAR 4.0, TI360, CMX360
IMS, VoIP & SBCs	aiSIEM, NDR, UEBA, SOAR 4.0, TI360, CMX360, aiBAS360, aiSAT360, Email AI
SS7/Diameter Gateways	aiSIEM, aiXDR, NDR, SOAR 4.0, TI360, CMX360, aiBAS360, aiSecurityScore360
DNS, DHCP, NTP	aiSIEM, NDR, UEBA, SOAR 4.0, TI360, CMX360
AAA / HSS / RADIUS / AUSF	aiSIEM, aiXDR, UEBA, aiIDGuard, aiITDR, SOAR 4.0, TI360, CMX360
OSS/BSS & Provisioning	aiSIEM, UEBA, aiIDGuard, aiITDR, SOAR 4.0, aiITSM, TI360, CMX360, aiBAS360
Multi-Access Edge Compute	aiSIEM, aiXDR, NDR, UEBA, aiIDGuard, aiITDR, SOAR 4.0, TI360, aiBAS360

TELECOM CYBERSECURITY

Protecting Every Layer of the Telecom Stack

100%
SS7 networks vulnerable to subscriber surveillance & DoS

#2
Most targeted sector for nation-state cyberattacks globally

20-30%
More privileged accounts than operators know exist

8+
Disparate point tools still failing to cover telecom protocols

Critical Threat Vectors

SS7 & Signaling Attacks
- Subscriber location tracking and SMS interception at scale
- Lateral movement invisible to conventional SIEM tools
- Single exploit can expose millions of users simultaneously

5G Core & GTP Abuse
- 100% vulnerable to info disclosure
- 38% success rate for location tracking
- 33% vulnerable to fraud exploitation
- Only 33% implement traffic filtering

OT, IoT & RAN
- Tower-site SCADA and BMS - no agent, no visibility
- Millions of NB-IoT endpoints vulnerable to botnet enlistment
- Open RAN API abuse and physical tampering at remote sites

Identity & Insider Risk
- OSS/BSS insider abuse, data exfiltration, billing fraud
- SIM cloning, AAA credential theft, RADIUS compromise
- Supply chain and MVNO interconnect as untrusted entry points

Seceon OTM Platform Defense

AI-Native Detection at Telecom Scale
- 150M events/sec - native SS7, Diameter, GTP, SIP, 5G DPI
- 4,000+ ML behavioral models for insider and protocol threats
- 100+ threat intel feeds, 2B+ IOCs via TI360

Unified 15-Module Platform
- aiSIEM, aiXDR, SOAR 4.0, NDR, UEBA, and more
- Replaces 8+ point tools, 2 - 4 week deployment
- 950+ integrations, ServiceNow and JIRA sync via aiITSM

OT, IoT & Identity Coverage
- aiSecOT360: passive ICS/SCADA discovery, IEC 62443
- aiUIDGuard: agentless identity across 60+ platforms
- aiITDR: impossible travel detection, AD attack protection

Compliance Automation
- 45+ frameworks: NERC CIP, GDPR, NIS2, 3GPP, ISO 27001
- Full audit reports in <1 hour vs. 6 weeks manually
- CMX360 continuous cross-framework evidence collection

Proven Results

95-99%
Threat detection accuracy

70%
Reduction in SOC costs

40%
Faster MTTR

45+
Compliance frameworks covered

Technology Layer	Primary Seceon OTM Modules
OT/SCADA (Tower & DC Sites)	aiSecOT360, aiSIEM, aiXDR, NDR, SOAR 4.0, CMX360, aiBAS360, aiSecurityScore360
IoT / LPWAN / NB-IoT	aiSecOT360, aiSIEM, NDR, UEBA, aiIDGuard, SOAR 4.0, TI360, aiBAS360
Security Infrastructure	aiSIEM, aiXDR, UEBA, aiIDGuard, aiITDR, SOAR 4.0, aiBAS360, CMX360

Conclusion - The Unified Telecom Security Platform

Telecom cybersecurity cannot be solved with point tools. Protocol diversity, deployment scale, regulatory complexity, and operational criticality demand a unified platform that spans detection, response, identity, network, OT/IoT, compliance, and human risk - simultaneously and at carrier-grade throughput. Seceon OTM delivers exactly that.

Key Takeaways for Telecom Security Leaders

- **Protocol-aware detection is non-negotiable.** SS7, GTP, Diameter, 5G SBA, and OT protocols require native deep packet inspection - generic SIEM/XDR tools produce blind spots across the most critical telecom attack surfaces.
- **OT and IoT require passive, agentless coverage.** aiSecOT360 handles thousands of tower sites and millions of IoT devices without operational disruption or agent deployment.
- **Identity sprawl is a critical telecom risk.** aiIDGuard routinely discovers 20-30% more privileged accounts than operators believe exist across their multi-vendor OSS/BSS systems.
- **Automated response in < 90 seconds is a necessity**. Signaling storms, toll fraud, and SS7 attacks cascade at machine speed - human-speed response creates unacceptable exposure windows.

- **One platform, all 15 modules, replaces 8+ disparate tools** - reducing tooling costs while dramatically improving detection coverage and analyst efficiency.
- **45+ compliance frameworks from a single automation engine** - CMX360 eliminates the manual multi-team effort of separate GRC tools for NERC CIP, GDPR, PCI-DSS, and NIS2.

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 and aiXDR 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 850 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,800 clients.

References and Citations:

This whitepaper is based on research and data from:

- IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation. Available at: *https://www.ibm.com/reports/data-breach*
- National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. Available at: https://www.nist.gov/cyberframework
- European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
- 3rd Generation Partnership Project (3GPP). 3GPP TS 33 Series – Security Architecture and Procedures for 5G Systems. Available at: https://www.3gpp.org/specifications
- Communications Fraud Control Association (CFCA). (2023). Global Telecom Fraud Loss Survey. Available at: https://cfca.org

About the Author

Niraj Mishra

Sr. Customer Success Engineer, Seceon Inc.



Niraj is a cybersecurity professional with over 5.5 years of experience in Security Operations, Customer Success, and Technical Support. He has strong expertise in SIEM, SOAR, EDR, and NDR solutions, along with hands-on experience in log analysis, threat detection, incident investigation, and Linux administration. Niraj also brings solid knowledge of backend troubleshooting, parser and API integrations, and cloud log onboarding. His experience with enterprise security platforms helps organizations improve security operations, enhance detection capabilities, and resolve complex technical challenges across modern environments.

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.

© 2026 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.