# AI-Powered Cybersecurity for Financial Organizations

| $6.08M | 1,318% | <90 sec | 1,000+ |
|---|---|---|---|
| Avg breach cost in financial services (2024) | Ransomware surge targeting BFSI sector | Detection & automated remediation time | BFSI customers on Seceon OTM platform |

## Executive Summary

### The Financial Sector is Under Siege And Conventional Security is Failing

Financial organizations globally are the most targeted industry sector facing sophisticated nation-state APTs, ransomware syndicates, insider threats, business email compromise (BEC), account takeover fraud, and an ever-expanding multi-jurisdictional regulatory compliance burden. Traditional point-product security stacks introduce integration fragility, visibility gaps, analyst alert fatigue, and unmanageable operational overhead that attackers actively exploit.

With average breach costs of $6.08M (IBM, 2024), 94% of attacks arriving via four primary vectors phishing, malware, DDoS, and insider threats and regulatory penalties reaching millions across every major jurisdiction, financial institutions require a fundamentally different approach: unified AI intelligence that detects, correlates, and responds at machine speed.

> Seceon's Open Threat Management (OTM) Platform consolidates 25 natively integrated security modules into a single AI-driven platform scaling to process multi-millions of security events per second in real time across 9,800+ customers worldwide, including 1,000+ banking and financial services institutions delivering threat detection and automated remediation within 90 seconds, 95% false-positive reduction, and fully automated regulatory compliance reporting across all major global frameworks.

## Quantified Business Outcomes

| 80% | 90% | <5 min | 40-60% |
|---|---|---|---|
| Reduction in compliance reporting overhead | Reduction in false positive alerts | Mean time to respond to critical threats | Reduction in total cybersecurity ownership cost |

# Financial Sector Threat Landscape

## Six Threat Categories Every Financial CISO Must Address

Financial organizations face a convergence of criminal, nation-state, and insider threats operating across an expanding digital perimeter cloud infrastructure, mobile banking, open APIs, third-party integrations, and branch networks. The sophistication and persistence of these threats demands behavioral AI that understands financial workflows, not generic signature-based pattern-matching.

**1. Ransomware & Double Extortion**
Modern ransomware groups encrypt AND exfiltrate data, threatening both operational continuity and regulatory disclosure obligations. The financial sector experienced a 1,318% surge in ransomware attacks in 2024. Groups such as LockBit, BlackCat/ALPHV, and RansomHub specifically target banking institutions due to their operational dependency on continuous availability. Seceon detects pre-ransomware behavioral precursors lateral movement, shadow copy deletion, credential harvesting, and mass file staging before encryption can begin.

**2. Nation-State APT Campaigns**
State-sponsored groups actively target SWIFT infrastructure, central bank systems, trading platforms, and cryptocurrency exchanges. Key threat actors include Lazarus Group (North Korea - SWIFT heists, crypto theft), APT38 (North Korea), Salt Typhoon (China - telecom and financial infrastructure), and Scattered Spider (ransomware/extortion targeting financial services). These actors use living-off-the-land techniques, fileless malware, and dwell times measured in months - all designed to evade signature-based detection.

**3. Insider Threats & Privileged Account Abuse**
Malicious or negligent insiders with legitimate access to core banking systems, SWIFT operators, trading terminals, and customer PII represent one of the highest-risk vectors. Research indicates 81% of breaches involve compromised credentials. Seceon's UEBA establishes behavioral baselines for every user, account, and device, flagging anomalous access patterns, off-hours privileged activity, and data exfiltration attempts in real time with full audit trails.

**4. Business Email Compromise (BEC)**
BEC attacks targeting wire transfer fraud, payroll diversion, and vendor payment manipulation cost the global financial sector billions annually. Attackers impersonate executives, regulators, and trusted vendors with sophisticated, context-aware email campaigns that defeat traditional gateway controls. Seceon's aiEmail module and UEBA analytics detect impersonation patterns, unusual authorization workflows, and communication anomalies before financial damage occurs.

**5. Account Takeover (ATO) & Fraud**
Credential stuffing, SIM-swap attacks, Aadhaar-linked authentication abuse (India), and synthetic identity fraud target digital banking customers at scale. Seceon's aiIDGuard monitors identity lifecycle across all channels, detecting impossible travel, concurrent sessions, device fingerprint anomalies, and behavioral shifts, stopping ATO before unauthorized transactions can be executed.

**6. Third-Party & Supply Chain Risk**
Financial institutions rely on hundreds of third-party integrations payment processors, core banking vendors, cloud services, and fintech APIs each representing a potential breach vector. Third-party compromises are among the most difficult to detect with traditional tools. Seceon provides continuous vendor risk monitoring, API anomaly detection, and supply chain threat intelligence correlation to identify third-party intrusions at the earliest stage.

## Seceon OTM Platform - Overview

### One Platform. 25 Modules. Zero Integration Gaps.

The Seceon Open Threat Management (OTM) Platform is a purpose-built, natively unified cybersecurity platform where every module shares a single data model, a single analytics engine, and a single management console. Unlike multi-vendor stacks assembled from acquired point products, Seceon eliminates the correlation gaps, integration fragility, and data loss between tools that sophisticated attackers actively exploit.

The platform scales to process multi-millions of security events in real time continuously, without sampling or delay enabling consistent protection across the largest and most complex financial environments globally. This scale is achieved without sacrificing detection fidelity: Seceon delivers threat detection and automated remediation within 90 seconds of an incident occurring, a capability that fundamentally changes the economics of a cyber breach.

### Platform Scale Facts (March 2026)

| | |
|---|---|
| 9,800+ customers worldwide | 100+ Threat Intelligence sources |
| 67+ Global Fortune 500 customers | 7-year forensic log retention |
| 1,000+ BFSI customers | <90 seconds detection and automated remediation |
| 750+ global MSSP/MSP partners | ≥70% autonomous L1 alert resolution |
| Multi-million events per second real-time processing | 95%+ false positive reduction vs. legacy SIEM |
| 1,100+ integrations and connectors | 98% annual customer retention rate |

## 25 OTM Modules - Financial Services Module Stack

| Module | Category | Key Capabilities |
|---|---|---|
| aiSIEM | Detection & Analytics | AI-powered event correlation across all data sources, real-time multi-dimensional threat analytics, 95% false-positive reduction, and long-term forensic log retention for investigations and regulatory audits |
| aiXDR-PMax (EDR) | Endpoint Detection & Response | Deep behavioral analytics across endpoints, memory forensics, process chain analysis, and automated endpoint containment protecting servers, workstations, ATMs, and banking terminals |
| NDR | Network Detection & Response | Full network visibility including east-west traffic, C2 beacon detection, lateral movement identification, and encrypted traffic analysis across branch and data center environments |
| UEBA | Behavior Analytics | AI-driven behavioral baseline per user and entity, insider threat detection, peer group analysis, and dynamic risk scoring across all financial system interactions |
| aiITDR | Identity Threat Detection | Real-time identity lifecycle monitoring, impossible travel and concurrent session detection, credential abuse identification, and lateral movement via identity vectors |
| aiIDGuard | Identity & Access | Privileged account monitoring, AI-driven access anomaly detection, and continuous identity graph analysis to protect SWIFT operators, admins, and privileged users |
| aiSOAR | Orchestration & Response | Automated response playbooks for financial-specific scenarios with autonomous L1 alert resolution and pre-built workflows for CERT-In, SEBI, RBI, GDPR, and DORA reporting |

| | | |
|---|---|---|
| SeraAI | AI Security Co-Pilot | Natural language threat investigation and automated playbook generation enabling analysts to query threats in plain English deployable fully on-premises with no external AI dependency |
| Threat Intelligence | Threat Intelligence | 100+ global and regional threat intelligence feeds, financial crime intelligence, nation-state TTP tracking, real-time IOC enrichment, and dark web monitoring |
| CSPM / CDR | Cloud Security | Continuous cloud security posture management across AWS, Azure, GCP and regional cloud providers, real-time misconfiguration detection, and cloud-native threat detection with automated response |
| aiCompliance CMX360 | Compliance Automation | Continuous posture-driven compliance automation, automated evidence collection, and regulatory report generation for all major global frameworks always audit-ready, never scrambled at examination time |
| aiSecOT360 | OT/ICS Security | Passive, zero-disruption monitoring of operational technology and industrial control systems across financial data centers and critical infrastructure supporting 70+ industrial protocols |

## Financial Service-Specific Capabilities

### Purpose-Built Detection for Financial Workflows

Unlike generic cybersecurity platforms, Seceon's OTM includes financial services-specific AI detection models, pre-built banking use cases, and compliance automation tuned for the regulatory demands of the BFSI sector. The platform's AI understands normal banking operations, transaction flows, and user behavioral patterns eliminating the false positive storms that plague generic SIEM deployments in financial environments and enabling actionable alerts that security teams can act on with confidence.

## Key Financial Use Cases

| Use Case | How Seceon Addresses It |
|---|---|
| SWIFT / Wire Fraud Detection | Correlates authentication anomalies, SWIFT operator behavioral baselines, and transaction patterns to detect unauthorized wire initiation before funds leave the institution. Integrates with SWIFT Alliance platforms. |
| Ransomware Pre-Encryption Detection | Identifies lateral movement, shadow copy deletion, credential harvesting, and mass file staging before encryption begins enabling containment during the dwell-time window. |
| Privileged Account Abuse | Detects domain admin credential misuse, service account anomalies, and privilege escalation against core banking systems, databases, mainframes, and payment platforms. |
| Account Takeover (ATO) | Correlates credential stuffing attempts, impossible travel, device fingerprint changes, and behavioral shifts to detect compromised customer and employee accounts across digital channels. |
| Data Exfiltration Prevention | Monitors egress traffic, cloud uploads, email attachments, and USB activity for unusual data movement particularly customer PII, card data, and proprietary trading positions. |
| Third-Party Breach Detection | Identifies anomalous activity originating from vendor API sessions, contractor accounts, and supply chain integrations detecting third-party compromises in real time with automated containment. |
| Payment Fraud Analytics | Analyzes transaction patterns for anomalies consistent with ACH fraud, card-not-present fraud, and mule account behavior. Supports BSA/AML suspicious activity reporting workflows. |
| Insider Trading Detection | Monitors privileged access to market-sensitive information alongside communication and trading activity anomalies to identify potential insider trading risks for capital markets firms. |

# Global Regulatory Compliance Coverage

## Native Compliance Automation Across All Major Jurisdictions

Financial institutions operating globally face a complex, overlapping web of regulatory requirements across multiple jurisdictions. Seceon's aiCompliance CMX360 module transforms compliance from a periodic, manual documentation exercise into a continuous, posture-driven automated outcome with pre-built frameworks, automated evidence collection, and audit-ready report generation for every major global regulatory framework.

> All compliance frameworks below are supported natively within the Seceon OTM platform no third-party compliance tools, manual report assembly, or custom integrations required. Evidence packages are generated automatically, continuously, and are always audit-ready.

## United States - Regulatory Compliance

| Framework | Applies To | Seceon Coverage | Status |
|---|---|---|---|
| FFIEC | Banks, credit unions, thrifts - IT examination readiness | Risk assessment automation, ISE program documentation, incident response records aligned to FFIEC booklets. Replaces FFIEC CAT (sunsetted August 2025) with continuous maturity assessment. | Automated |
| PCI-DSS v4.0 | All card-processing institutions | Req 10 log monitoring, Req 11 security testing, CDE segmentation validation, QSA evidence package auto-generation. Automated network security testing integration. | Automated |
| GLBA Safeguards Rule | All financial institutions handling consumer data | Written information security program monitoring, qualified individual oversight dashboards, incident response documentation, breach notification workflows. | Automated |

| | | | |
|---|---|---|---|
| SOX IT Controls | Publicly traded financial institutions | Continuous monitoring of IT general controls, change management audit trails, privileged access logs, financial system integrity monitoring, external auditor evidence packages. | Automated |
| BSA / AML | Banks, broker-dealers, MSBs, FinTechs | Transaction anomaly detection, Suspicious Activity Report (SAR) workflow support, high-risk account monitoring, cross-border payment surveillance, FinCEN reporting. | Automated |
| NIST CSF 2.0 | All financial institutions (best practice, examiner-referenced) | Full six-function coverage (Govern, Identify, Protect, Detect, Respond, Recover) with continuous maturity scoring and gap remediation tracking. | Automated |
| NCUA Examination | Credit unions (supplemental to FFIEC) | NCUA Information Security Examination (ISE) program alignment, ATM/ITM skimming incident documentation, third-party vendor oversight reports. | Automated |

## India - Regulatory Compliance

India represents one of the fastest-growing and most regulated financial markets globally, with the BFSI sector reporting 1,30,000+ cyberattacks in 2023 alone. Seceon's platform provides comprehensive native coverage for all Indian financial regulatory frameworks, including mandatory CERT-In 6-hour incident reporting, SEBI CSCRF continuous monitoring, RBI Cybersecurity Framework controls, and DPDPA 72-hour breach notification all delivered through automated workflows without manual report assembly.

| Framework | Applies To | Seceon Coverage | Status |
|---|---|---|---|
| CERT-In Directions 2022 | All regulated entities - MANDATORY | Automated 6-hour incident reporting playbook for all reportable categories. NTP-synchronized log timestamps. 180-day log retention within India. Point-of-contact designation support. CERT-In reporting gateway API integration. | Automated |
| RBI Cybersecurity Framework | All RBI-regulated banks | Full coverage of RBI CSF Governance, Identification, Protection, Detection, Response, and Recovery domains. Pre-built RBI CSF control monitoring dashboards. RBI examination-ready evidence generation. | Automated |
| SEBI CSCRF 2024 | All SEBI Regulated Entities (effective April 2025) | Cyber Capability Index (CCI) score continuous monitoring. All control domains: Governance, Identify, Protect, Detect (24x7 SOC), Respond, Recover. Automated quarterly SEBI submission evidence packages. | Automated |
| RBI IT Directions 2023 | NBFCs and Payment System Operators | IT governance, information security, cyber resilience, vendor risk management, audit trail, and incident reporting requirements for NBFCs and payment operators. | Automated |

| | | | |
|---|---|---|---|
| DPDPA 2023 | All entities processing personal data | Personal data breach detection, affected data subject scope estimation, automated 72-hour breach notification workflow to Data Protection Board of India. Supports penalties framework up to INR 250 crore. | Automated |
| IT Act 2000/2008 | All regulated financial entities | Reasonable security practices compliance (SPDI Rules 2011), sensitive personal data protection monitoring, Section 43A / 72A evidence collection. | Automated |
| NPCI / Payment System Compliance | UPI, IMPS, AePS, FASTag, RuPay participants | Fraud detection aligned to NPCI guidelines, transaction anomaly monitoring, UPI fraud response playbooks, SIM-swap containment, NPCI fraud reporting API integration. | Automated |
| IRDAI Cybersecurity Guidelines | Insurance companies in India | Information and Cyber Security Guidelines for insurance sector, incident reporting, cyber resilience framework alignment, IRDAI examination documentation. | Automated |
| NCIIPC Guidelines | Designated Critical Information Infrastructure operators | CII operator compliance monitoring, mandatory incident reporting to NCIIPC/CERT-In, critical infrastructure protection controls. | Automated |
| ISO 27001:2022 | All entities (aligned to SEBI CSCRF) | Annex A controls monitoring, continuous gap assessment, remediation tracking, and certification evidence generation aligned to SEBI CSCRF ISO 27001 references. | Automated |

| | | | |
|---|---|---|---|
| Data Localisation (RBI) | All entities processing payment data | Verification that all payment data is stored exclusively within India. Cross-border transfer monitoring. Immutable audit trail demonstrating India data residency compliance. | Automated |

## Europe & United Kingdom - Regulatory Compliance

| Framework | Applies To | Seceon Coverage | Status |
|---|---|---|---|
| GDPR / UK GDPR | All entities processing EU/UK personal data | Automated breach detection and 72-hour notification workflow to Data Protection Authorities. Data subject rights monitoring, consent framework controls, and transfer mechanism compliance. | Automated |
| DORA (EU) | All EU financial sector entities (effective January 2025) | ICT risk management continuous monitoring, digital operational resilience testing, third-party ICT provider oversight, major incident reporting to EBA/ESMA/EIOPA within required timelines. | Automated |
| NIS 2 Directive | Essential and important entities in EU member states | Security incident notification workflows, supply chain security monitoring, cyber hygiene controls, and competent authority reporting within 24/72-hour timelines. | Automated |
| EBA Guidelines | EU banks and payment institutions | EBA ICT Risk Management Guidelines alignment, outsourcing risk monitoring, operational resilience requirements, and supervisory reporting documentation. | Automated |

| | | | |
|---|---|---|---|
| PSD2 / Open Banking | Payment service providers across EU/EEA | Open banking API security monitoring, strong customer authentication (SCA) compliance controls, TPP access anomaly detection, and incident reporting to national competent authorities. | Automated |
| FCA Cyber Guidelines (UK) | FCA-regulated financial firms | Operational resilience requirements, important business services monitoring, cyber incident reporting, and CBEST threat intelligence-led assessment support. | Automated |

## Asia-Pacific - Regulatory Compliance

| Framework | Applies To | Seceon Coverage | Status |
|---|---|---|---|
| MAS TRM (Singapore) | All MAS-regulated financial institutions | MAS Technology Risk Management Guidelines alignment, third-party oversight monitoring, cyber incident reporting, and Technology and Cyber Risk Returns (TCRR) documentation. | Automated |
| MAS Notice on Cyber Hygiene | Banks, insurers, capital markets in Singapore | Continuous monitoring against MAS cyber hygiene requirements, privilege access management controls, and security patch management tracking. | Automated |
| APRA CPS 234 (Australia) | All APRA-regulated entities | Information security capability monitoring, material information security incident notification to APRA, third-party dependency management, and control testing documentation. | Automated |

| | | | |
|---|---|---|---|
| HKMA Cyber Resilience (HK) | All HKMA-regulated authorized institutions | Cyber resilience assessment framework alignment, incident management, threat intelligence sharing with HKMA, and examination-ready compliance evidence. | Automated |
| PDPA (Thailand/Malaysia/Singapore) | Entities processing personal data in SEA | Personal data breach detection, breach notification workflow automation to relevant Data Protection Authorities, consent framework monitoring. | Automated |

## Global & Universal Frameworks

| Framework | Applies To | Seceon Coverage | Status |
|---|---|---|---|
| ISO 27001:2022 | All financial institutions globally | Full Annex A controls monitoring with continuous evidence collection, automated gap assessment, remediation tracking, and certification-ready documentation packages. | Automated |
| NIST CSF 2.0 | Global financial institutions (US-origin, globally adopted) | All six functions: Govern, Identify, Protect, Detect, Respond, Recover with continuous maturity scoring, gap identification, and remediation prioritization. | Automated |
| PCI-DSS v4.0 | Any entity processing card payment data globally | Complete Requirement coverage with automated evidence collection, network segmentation validation, and QSA audit package generation. | Automated |

| | | | |
|---|---|---|---|
| SWIFT Customer Security Programme (CSP) | All SWIFT network participants | SWIFT CSP mandatory security controls monitoring, behavioral baseline for SWIFT operators, anomalous transaction pattern detection, and CSP self-attestation documentation support. | Automated |
| COBIT 2019 | IT governance framework (globally adopted) | IT governance controls mapping, continuous control monitoring, and audit evidence aligned to COBIT 2019 governance objectives for financial services. | Supported |
| MITRE ATT&CK | Universal threat framework | All 14 MITRE ATT&CK tactics and 200+ techniques mapped across all 25 OTM modules. Real-time ATT&CK heatmap, threat hunting by technique, and ATT&CK-aligned incident reports. | Automated |

# Deployment Options

## Flexible Deployment for Every Financial Infrastructure

Seceon supports the full spectrum of financial institution deployment requirements from air-gapped core banking environments to fully cloud-native digital banks with the same platform, the same data model, and the same management console.

| Deployment Model | Description | Compliance Consideration |
|---|---|---|
| On-Premises / Air-Gapped | Full data sovereignty for regulated institutions. Supports core banking, mainframe integration, and air-gapped trading infrastructure. Ideal for jurisdictions with strict data localisation mandates (India RBI, EU DORA, China MLPS). | Full compliance with RBI, CERT-In, and other data localisation mandates. All data processing and storage within the institution's own infrastructure. |
| Cloud-Native / SaaS | Multi-tenant SaaS delivery through 750+ global MSSP partners. Ideal for digital banks, credit unions, and FinTechs seeking operational simplicity with enterprise-grade security at global scale. | Sovereign cloud options available for EU (DORA), India (RBI), and APAC jurisdictions. No data crosses regulatory boundaries without explicit configuration. |
| Hybrid (On-Prem + Cloud) | Single management console spanning on-premises data centers, private cloud, and public cloud environments. Supports AWS GovCloud, Azure Government, and regional sovereign cloud for regulated institutions. | Consistent compliance posture and evidence collection across hybrid environments. Single audit trail spanning all deployment models. |
| MSSP-Managed | Fully managed service through 750+ certified global MSSP partners with 24x7x365 SOC operations. Enables small and mid-size financial institutions to access enterprise-grade capabilities without building internal SOC teams. | MSSP partners certified on all regional regulatory frameworks. Jurisdiction-appropriate data handling with contractual SLA guarantees. |

# Business Value & ROI

## Measurable Return on Investment Within 12 Months

Financial institutions implementing Seceon's OTM Platform achieve significant, quantifiable operational and financial benefits transforming cybersecurity from a cost center into a competitive advantage while reducing total cost of ownership compared to multi-vendor security stacks.

### Cost Reduction

- 40-60% reduction in total cybersecurity ownership cost through platform consolidation (eliminating 8-10 separate point tools)
- 80% reduction in compliance reporting overhead through automated evidence collection and report generation
- 58% average reduction in licensing costs compared to best-of-breed alternatives
- 84% reduction in integration and maintenance overhead (no inter-tool integration fragility)
- 91% reduction in compliance reporting preparation time per regulatory cycle

### Operational Efficiency

- 90% reduction in false positive alerts (from average 95% FP rate with legacy SIEM to <1%)
- Sub-5-minute mean time to respond (MTTR) to critical incidents vs. industry average of 257 days to detect and contain
- ≥70% of L1 alerts autonomously resolved without analyst intervention via SeraAI co-pilot
- Single-analyst operations achievable for mid-size institutions through intelligent automation
- Single management console for all 25 modules, eliminating context-switching and tool fatigue

### Risk Reduction

- Threat detection and automated remediation within 90 seconds vs. an industry average of 194 days to detect and contain without an AI-driven platform
- 7-year forensic log retention satisfying all major regulatory investigation and audit requirements globally
- Continuous compliance posture always audit-ready, eliminating point-in-time compliance failures
- Automated breach notification workflows ensuring compliance with CERT-In (6hr), DPDPA (72hr), GDPR (72hr), and DORA deadlines

# Why Seceon - Competitive differentiation

## What Sets Seceon Apart in Financial Services

| Differentiator | Description |
|---|---|
| Native Unification | 25 modules built on a single data model, one analytics engine, one console vs. multi-vendor stacks requiring complex integration maintenance that fails under adversarial pressure. No correlation gaps. No data loss between tools. |
| Financial-Grade AI Detection | Purpose-built AI detection models tuned to financial workflows, transaction patterns, and banking-specific threat TTPs delivering actionable, high-fidelity alerts from day one, not generic models requiring months of tuning before delivering value. |
| <90 Second Detection & Remediation | From the moment a threat occurs to automated remediation in under 90 seconds across multi-million events per second real-time processing. Industry-leading speed that contains breaches before they become reportable incidents. |
| Multi-Jurisdictional Compliance | The only platform with native automated compliance coverage spanning USA (FFIEC, PCI-DSS, GLBA, SOX), India (CERT-In, RBI, SEBI CSCRF, DPDPA, NPCI), EU (GDPR, DORA, NIS2), APAC (MAS, APRA), and global frameworks (ISO 27001, SWIFT CSP) all in a single platform. |
| Data Sovereignty by Design | On-premises, hybrid, and sovereign cloud deployment options with full data localisation support compliant with RBI mandates, EU DORA, and all jurisdiction-specific data residency requirements globally. |
| SeraAI Natural Language Co-Pilot | AI co-pilot enabling natural language threat investigation, automated playbook generation, and autonomous L1 resolution deployable fully on-premises with no external AI service dependency, satisfying sovereign AI requirements. |
| Proven BFSI Scale | 9,800+ customers worldwide with 1,000+ BFSI institutions. Real-time processing of multi-million events per second. 67+ Fortune 500 customers. 98% annual retention rate. 100% recommendation rate from reference customers. |
| Asset-Based Licensing | Transparent asset-based licensing model with no per-volume data ingestion charges, no alert volume caps, and no per-module licensing surprises providing full cost predictability for financial institution budget cycles. |

## Getting started

### Recommended Engagement Path

| # | Phase | Description |
|---|---|---|
| Step 1 | Discovery Workshop | 1-2 day workshop with your security and compliance teams to assess current environment, identify capability gaps, map regulatory requirements, and define deployment architecture. |
| Step 2 | Proof of Concept (PoC) | 30-day PoC in your environment with pre-configured financial services detection models, automated compliance framework mapping, and measurable KPI benchmarking against your current toolset. |
| Step 3 | Platform Deployment | Phased deployment through Seceon's global MSSP partner network or direct professional services. 750+ global MSSP partners available with jurisdiction-specific regulatory expertise. |
| Step 4 | Optimization & Value Realization | Continuous refinement of AI detection models to your specific environment, playbook customization for your regulatory workflows, and quarterly business value reviews measuring ROI against baseline. |

## About Seceon

Seceon enables MSPs and MSSPs 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 augments and automates MSP and MSSP security services with an AI and ML-powered aiSIEM, aiXDR, and aiMSSP platform. It delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It’s all enriched and analyzed in real-time with threat intelligence, AI, and ML models built on behavioral analysis and correlation engines to create reliable, transparent detections and alerts. Over 750 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 9,800 clients.

## Learn more about Seceon OTM Platform

Schedule a Demo www.seceon.com/contact-us/