Securing a Sovereign Financial Cloud at National Scale



How an apex banking authority's technology arm achieved real-time threat visibility across a national payment infrastructure, fully air-gapped, zero data egress, automated response in under 5 minutes.

aiSIEM | aiXDR | UEBA | SOAR | Sovereign Cloud | Air-Gapped

Client Snapshot

Attribute	Detail
Sector	Sovereign Financial Technology Infrastructure
Organization Type	Wholly-owned subsidiary of an apex monetary authority
Infrastructure Scope	500+ Connected Banks and Financial Institutions
Payment Systems	National RTGS · NEFT · SWIFT-equivalent Messaging
Data Sovereignty	ABSOLUTE — Zero external data transfer permitted
Deployment Model	Fully air-gapped, on-premises sovereign cloud
Regulatory Frameworks	Central Bank IT Directives · ISO 27001 · SWIFT CSP · National Data Protection Law · Mandatory Incident Reporting
Incident Reporting SLA	6-Hour Mandatory Obligation
Prior Security Posture	Siloed legacy SIEM · Fragmented tooling · Heavy manual operations

500+	6H	100%	5+	7 YR
Payment Institutions Connected	Mandatory Incident Reporting SLA	Data Sovereignty — On-Premises	Compliance Frameworks	Forensic Archive Requirement

The Challenge

Nation-State Targeting
As operator of national payment rails and interbank messaging infrastructure, the organization represents a prime target for sophisticated nation-state threat actors and financially motivated APT groups targeting central banking systems globally.

Absolute Sovereign Cloud Constraints
All security operations had to function in a fully air-gapped, on-premises sovereign cloud with no internet dependency, no external analytics pipeline, no cross-boundary data transfer, disqualifying most SaaS-based vendors outright.

Massive Scale & Complexity
Hundreds of financial institution connections, thousands of internal endpoints, and high-frequency transaction systems generate millions of security events daily, overwhelming legacy SIEM approaches.

Multi-Framework Regulatory Complexity
Simultaneous compliance with apex bank IT directives, mandatory 6-hour incident reporting, SWIFT CSP, ISO 27001, and national data protection legislation, each with distinct monitoring, logging, and reporting obligations.

Legacy Tool Fragmentation
Disparate, siloed tools with no unified correlation create visibility gaps across network, endpoint, identity, and application layers, requiring heavy manual analyst effort for basic threat triage.

Unacceptable Detection Latency
The mean time to detect threats exceeded 18 hours with manual processes. Response to containment averaged 4–8 hours an existential risk window against APT-class adversaries targeting national payment operations.

> *"Managing cybersecurity for national payment infrastructure requires a platform that operates at the intersection of scale, sovereignty, and speed. Seceon's OTM platform delivered all three — within our sovereign cloud boundary, with automated detection and response that no legacy SIEM could match."*
>
> — **Chief Information Security Officer · National Payment Infrastructure Entity · Identity Anonymized**

Why Seceon OTM Was Selected

Requirement	How Seceon Delivered
Air-Gapped Sovereign Deployment	Zero dependency on internet or external cloud resources. All AI/ML processing, correlation, and storage run entirely within the sovereign boundary.
Unified Platform Architecture	Single platform replacing siloed SIEM, SOAR, NDR, UEBA, and compliance tools. One data model, one analytics engine, one console — eliminating integration complexity.
Proven Scale	Stream-processing engine handles 150M events per second with sub-second detection latency and up to 1.6 trillion events per day — supporting national-scale telemetry.
Regulatory Automation	Pre-built compliance frameworks for apex bank directives, ISO 27001, and SWIFT CSP with automated evidence generation and on-demand reporting.
Threat Intelligence Depth	70+ threat intelligence feeds, including government CERTs, SWIFT threat networks, and financial sector sources — all processed locally.
Flexible Sovereign Deployment	Supports bare metal, private cloud VMs, and containerized environments with full feature parity within existing sovereign infrastructure.

Platform Deployment

Seceon OTM was deployed across the sovereign cloud environment encompassing the following modules:

- **aiSIEM™**

AI-Powered SIEM
Real-time ingestion and correlation of logs from network infrastructure, endpoints, application servers, identity systems, and payment transaction platforms. Dynamic threat models eliminate manual rule tuning from day one.

- **aiXDR™**

Extended Detection and Response
Cross-domain detection spanning network behavior, endpoint telemetry, application layer, and identity analytics with automated MITRE ATT&CK mapped investigation and kill chain visualization.

- **UEBA**

Behavioral Analytics
Behavioral baselines for all users, privileged accounts, service accounts, and inter-institution API connections, detecting compromised credentials and insider threats without signature dependency.

- **SOAR**

Automated Response

Automated playbooks for incident containment, account isolation, IP blocking, and forensic evidence preservation, delivering sub-5-minute automated response across 70% of incident types.

- **Compliance**

Regulatory Automation

Continuous automated monitoring aligned to central bank directives, mandatory 6-hour incident reporting, ISO 27001, and SWIFT CSP, with automated evidence packaging for regulatory submissions.

- **LTS**

Long-Term Storage

7-year forensic data retention with full chain of custody and cryptographic integrity verification, stored entirely within the sovereign cloud boundary and meeting all audit and regulatory requirements.



Results Achieve

Verified Operational Metrics — Post-Deployment

95%	70%	60%	100%
Reduction in False Positives	Incidents Auto-Contained	Reduction in Analyst Manual Effort	Data Sovereignty — Zero Egress

Metric	Before Seceon	After Seceon
Mean Time to Detect (MTTD)	18+ hours	< 5 minutes
Mean Time to Respond (MTTR)	4–8 hours (manual)	< 5 minutes (automated)
False Positive Rate	Analyst-fatiguing volume	95% reduction
Incidents Auto-Contained	0%	70% fully automated
Compliance Reporting	Manual — weeks of prep	Continuous, automated
Mandatory 6-hour Incident SLA	At risk	Consistently met
Asset Visibility Coverage	Siloed, fragmented	Unified — 100% coverage
Regulatory Audit Readiness	Weeks of preparation	On-demand, real-time
Data Sovereignty Compliance	Partial	100% — zero data egress

Securing a Sovereign Financial Cloud With seceon

The Cybersecurity Challenge

Nation-State Targeting
Prime target for sophisticated nation-state threat actors and financially motivated APT groups

Absolute Sovereign Cloud Constraints
Fully air-gapped environment with no internet dependency or external data transfer

Massive Scale And Complexity
Millions of daily security events across interconnected financial systems

Multi-Framework Regulatory Complexity
Central bank directives, ISO 27001, SWIFT CSP, and data protection laws

Legacy Tool Fragmentation
Siloed tools with no unified correlation across network, endpoint, identity, and applications

Unacceptable Detection Latency
18+ hours detection and 4–8 hours response time

Why Seceon OTM Was Selected

Air-Gapped Sovereign Deployment	All AI/ML processing, correlation, and storage run entirely within the sovereign boundary
Unified Platform Architecture	Single platform replacing SIEM + SOAR + NDR + UEBA + Compliance tools
Proven Scale	150M events per second and 1.6 trillion events per day capacity with sub-second detection latency
Regulatory Automation	Pre-built compliance frameworks with automated evidence generation and reporting
Threat Intelligence Depth	70+ threat intelligence feeds processed locally within the environment
Flexible Sovereign Deployment	Supports bare metal, private cloud VM, and container architectures

95%
Reduction in False Positives

70%
Incidents Auto-Contained

<5
Minutes Detection and Response

100%
Data Sovereignty Zero Egress

18+ hours to < 5 Minutes
Detection

4 to 8 hours to <5 Minutes
Response

Manual to Continuous
Automated Compliance

Key Outcomes

National Payment Rail Protection
Real-time behavioral monitoring of interbank settlement and messaging transaction flows, protecting hundreds of institutions from manipulation, fraud injection, and APT interference.

Absolute Sovereign Cloud Integrity
Complete security operations within the sovereign cloud boundary. No data ever leaves the on-premises environment, satisfying the absolute data localization mandate.

Regulatory Leadership
Automated evidence generation for every major regulatory framework with on-demand audit readiness, replacing weeks of manual compliance preparation.

Threat Detection at National Scale
Processing millions of daily events across hundreds of connected institutions with sub-second latency, previously unachievable with legacy SIEM infrastructure.

Insider Threat and Privileged Access Control
UEBA continuously monitors all privileged users and service accounts, providing behavioral intelligence to detect insider threats and compromised credentials.

Autonomous SOC Operations
70% of incidents are auto-contained without analyst intervention. The SOC team is refocused from reactive triage to proactive threat hunting and strategic security improvement.

Key Platform Numbers

Platform metrics	
Events/Second	150 Million
Events/Day Capacity	1.6 Trillion
Pre-Built Connectors	800+
TI Feeds Integrated	70+
Detection Latency	Sub-second
Auto Response Time	< 5 minutes

Platform metrics	
Data Retention	7 years on-prem
Platform Uptime SLA	99.9%
MITRE ATT&CK Coverage	92% techniques

> *"Managing cybersecurity for national payment infrastructure requires a platform that operates at the intersection of scale, sovereignty, and speed. Seceon's OTM platform delivered all three, within our sovereign cloud boundary, with automated detection and response that no legacy SIEM could match."*
>
> — **Chief Information Security Officer · National Payment Infrastructure Entity · Identity Anonymized**

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.

Learn more about Seceon

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



© 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.