AI4IT SERVICES

BUILDING A 24X7 SECURITY OPERATIONS CENTER FOR A FINTECH PLATFORM

Client Overview

Company: NovaLedger Financial

Industry: FinTech / Digital Banking

Location: New York, NY

Size: 80+ employees | 500K+ active users

Challenge: Growing cyber threats, regulatory pressure, and lack of in-house 24x7 security coverage.

The Problem

NovaLedger processed high volumes of sensitive financial data but lacked visibility across their infrastructure. Their internal IT team monitored logs during business hours but:

- Missed alerts from overnight attack attempts
- Couldn't correlate threats across endpoints, cloud, and network
- Had no formal incident response SOP or containment capabilities
- Faced pressure from partners to improve their SOC 2 Type II readiness

With rising fraud attempts and phishing campaigns, they needed a robust, round-the-clock security operations setup — fast.

BUILDING A 24X7 SECURITY OPERATIONS CENTER FOR A FINTECH PLATFORM

The Solution by AI4IT Services

We deployed a fully managed 24x7 Security Operations Center (SOC) with real-time monitoring, MDR, and compliance alignment.

🔧 Key Deliverables:

- Threat Detection Tools: Integrated SentinelOne, AWS GuardDuty, and custom SIEM dashboards for full-stack visibility.
- SOC-as-a-Service: Delivered centralized monitoring, triage, and remediation response via our 24x7 team.
- Incident Playbooks: Created tailored runbooks for ransomware, phishing, insider threats, and zero-day detection.
- MDR: Enabled active threat hunting and AI-powered behavioral analytics across endpoints and cloud.
- Compliance Readiness: Mapped alerting, logging, and documentation to SOC 2 & PCI DSS requirements.

BUILDING A 24X7 SECURITY OPERATIONS CENTER FOR A FINTECH PLATFORM

Metric	Before	After
Security Event Response Time	8–12 hours	< 15 minutes (24x7)
Threat Dwell Time	Unknown	Avg. < 2 hours
Audit Gaps (SOC 2)	6+ issues	0 flagged in latest audit
False Positive Rate	High	Reduced by 60%
Team Load	5+ hrs/week in alerting	Near-zero, offloaded to AI4IT

Client Testimonial

“We went from flying blind to having a real-time command center. AI4IT’s SOC and MDR team not only protected us — they made our auditors happy too.”

— VP of Infrastructure, NovaLedger

AI4IT SERVICES

BUILDING A 24X7 SECURITY OPERATIONS CENTER FOR A FINTECH PLATFORM

Technologies Used

Monitoring: SentinelOne, AWS GuardDuty, Elastic SIEM
Cloud: AWS (EC2, S3, CloudTrail)
EDR/MDR: SentinelOne ActiveEDR
Compliance Frameworks: SOC 2 Type II, PCI DSS
Tooling: Slack integrations, JIRA, Syslog pipelines

Services Provided

✓ 24x7 SOC-as-a-Service
✓ Managed Detection & Response (MDR)
✓ Cloud Security Monitoring
✓ Audit-Ready Reporting
✓ Threat Intelligence & Triage

📩 hello@ai4itservices.com 📞 +1 (281) 730-2359
🌐 https://ai4itservices.com