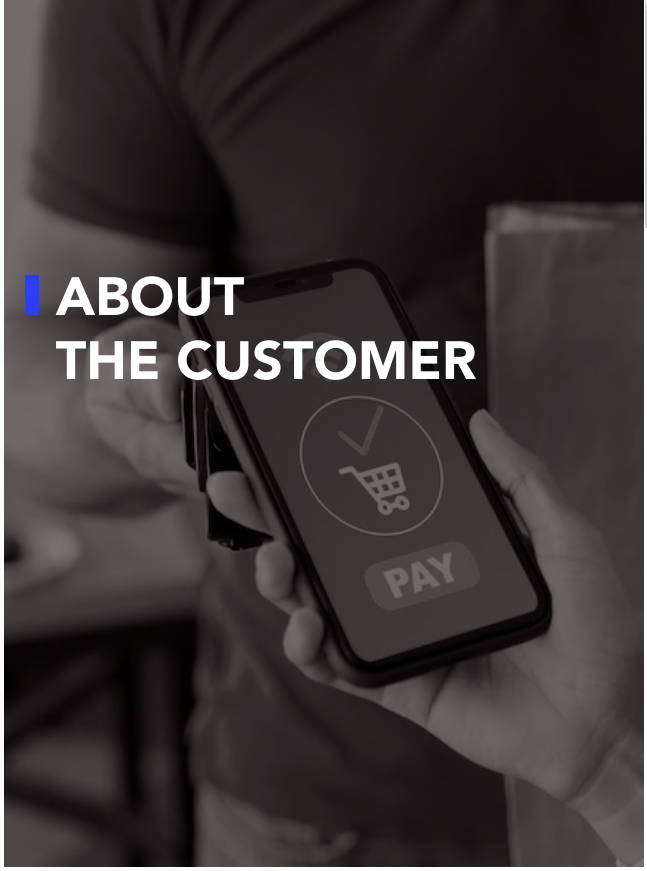
SISA

CUSTOMER SUCCESS STORY

SISA ProACT's cloud-based MDR solution helps neobank improve real-time threat detection and response



ABOUT THE CUSTOMER

The client is one of the earliest digital-only (NEO) banks to operate in the Asia Pacific region. The bank offers retail banking products including deposits, savings accounts, payments, loans, and cards. Being one of the leading digital-only banks, it gained a lot of popularity among digitally savvy customers and witnessed accelerated adoption amidst the COVID-19 pandemic. Its USPs (Unique Selling Propositions) are extremely user-friendly and secure banking applications.

Currently, the bank serves over 100K customers and manages more than $60 million worth of deposits in its country of operation.

THE CHALLENGE

Being a digital-only bank, it was of paramount importance for the customer to secure sensitive data and adhere to compliance standards. It needed to take a proactive approach to secure against increasing sophistication and frequency of cyberattacks, advanced attacks on endpoints, third-party risk, and inherent threats from its cloud infrastructure. Maintaining a secure environment while enabling uninterrupted operations for rapid business growth was the top most priority.

To achieve these objectives the bank was evaluating solutions that could help them with proactive threat detection, enhance the visibility of their digital assets, and secure their dispersed infrastructure along with setting up 24-hour alert monitoring.

SOLUTION OFFERED BY SISA

SISA leveraged forensics learnings along with practitioner-guided insights to provide the bank's security team with the necessary direction they needed to move forward. The bank had previously partnered with SISA for performing application penetration testing, vulnerability assessment and PCI DSS compliance audit. The positive outcomes from the engagement along with SISA team's consultative approach gave them the confidence to enlist SISA as their MDR services provider. The bank then chose the SISA ProACT MDR solution for its comprehensive, next-gen, scalable, and user-friendly solution that helped them address their business challenges. Using SISA ProACT, the bank was able to detect anomalies in its network traffic and improve its security posture with real-time visibility into potential threats.

A unified dashboard with in-built drag-and-drop features, ProACT's user interface allowed the bank to create bespoke reports on the state of their infrastructure.

SISA's SOC team also provided the bank with 24x7 monitoring of all its assets, including on weekends. Staffed with a highly trained group of threat analysts and researchers, the SOC team helped the bank by accelerating the detection, prioritization, and response to advanced cyber threats.

More importantly, SISA ProACT being a 100% cloud-native application, it gave the bank the flexibility to expand based on the growing needs of its business and realize considerable cost savings in infrastructure.

BUSINESS IMPACT

With SISA's 24x7x365 monitoring, the bank was able to identify and respond to potential threats, swiftly. It also allowed them to have proactive threat-hunting capabilities with an automated incident response system. SISA's Forensics-driven approach with a rigorous focus on learning from every forensic investigation together with the proven process of layering on practitioner insights, helped the bank advance their cyber security program in parallel with their aggressive growth strategy.

The bank has seen many advantages with this service such as improved detection accuracy, faster incident resolution time, reduced false positives, and improved compliance levels.

SISA ProACT's MDR solution also enabled the bank to get PCI-DSS certified, by helping them meet all the compliance metrics and providing them with all the required reports for audits.

Post-the implementation, the bank's threat detection and response capability improved significantly with:

- Mean Time to Detect (MTTD) being reduced to <60 minutes and
- Mean Time to Respond (MTTR) cut down to <24 hours.

In addition, through actionable IOCs (Indicators of Compromise) and forensics-based intelligence, shared with the client, every day, the client's overall security posture improved significantly. As part of the continuous awareness program, SISA also conducted a Forensic Learning Session (FLS) and SISA Ransomware Prevention Learning Session to help improve employee awareness and preparedness for any future breach incidences. The bank has continuously given SISA a promoter score for the past four quarters.

SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance

Payment Data Security

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance
- SWIFT

Strategy and Risk

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security

Security Testing

Application Security

- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Security Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- PCI ASV Scan
- Phishing Simulation

Hardware and IoT Security Testing

- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing

Cyber Resilience

Managed Detection and Response Solution – SISA ProACT

- Monitoring
- Attack Simulation
- Use-case Factory
- Advanced Threat Hunting

Digital Forensics and Incident Response

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation
- Ransomware Simulation

Data Governance

Data Discovery and Classification - SISA Radar

- Card Data Discovery
- PII (Privacy) Discovery
- Data Classification
- Data Masking/Encryption

Data Security as a Service

Cyber Academy

Payment Data Security Implementation

- CPISI
- CPISI Advanced
- CPISI-D (Developers)

Security Incident Detection and Response Programs

- CIDR

Cybersecurity Awareness

Forensic Learning Sessions for Senior Management

For more Information visit us at www.sisainfosec.com
OR
write to us at *contact@sisainfosec.com*

Follow us