SISA

CUSTOMER SUCCESS STORY

A global payments solutions provider uses SISA's ProACT MDR solution to improve threat detection and response and enhance security posture.

ABOUT THE CUSTOMER

The client is a leading global payment solutions provider having a presence across 45+ countries. Through its wide array of technology-led cash and digital payment solutions, it empowers banks and merchant aggregators to provide top-of-the-line payment services to their customers. As a pioneer in the payments space, it uses its extensive industry know-how and a robust payment infrastructure to offer customizable and cost-effective solutions that range from ATM services and cash recycling machines to POS and internet payment gateway solutions.

THE CHALLENGE

Beyond developing innovative solutions, offering superior customer experience and staying ahead of the competition, the client also faced another key challenge – safeguarding sensitive customer data and business operations from cyberattacks. Their top focus was to minimize security risks, proactively detect threats and securely migrate from a legacy solution. Hence, they were looking for a robust Managed Detection and Response (MDR) solution with 24/7 threat monitoring and response and dedicated support for security operations. Secondly, they were migrating to a hybrid cloud environment and required an integrated solution that could secure on-premises and cloud workloads. Thirdly, they also needed quick and timely support for responding and reporting to CERT-In alerts. Besides, since they operated in a highly regulated environment, they had to ensure adequate security controls to meet PCI DSS compliance requirements.

SOLUTION OFFERED BY SISA

After evaluating a few third-party security operations solutions, the client enlisted SISA as their long-term partner for securing their end-to-end IT infrastructure. They had previously worked with SISA on a number of compliance and security testing projects that included Vulnerability Assessment and Penetration Testing (VAPT) activities, PCI PIN audit, PCI DSS assessment and certification, and implementation of SISA Radar solution for sensitive data scanning and discovery. Based on the positive results and the trusted relationship, they were convinced to go ahead with SISA as their MDR services provider.

SISA adopted a two-phase approach to implement SISA ProACT MDR solution. The first phase involved integrating the platform on the on-premises locations spread across two cities. The second phase included implementing the solution on AWS cloud. As the license of their existing MDR tool was nearing expiry, SISA began offering threat monitoring services using agile method, even before the completion of the first phase, to ensure no new threats were lurking in their network during transition. The solution included implementation of 990 use cases (including 59 custom use cases built using agile methodology) for improved threat detection through SISA's USECASE Factory. Through its alignment with MITRE ATT&CK framework along with integration of learnings from forensic investigations, SISA's USECASE Factory offers improved investigation quality and enhanced security monitoring. Secondly, the platform provided the client's team with the benefit of 60+ threat intel feeds for enhanced threat hunting along with daily actionable Threat Advisories to detect and remediate top vulnerabilities.

BUSINESS IMPACT

SISA's 24/7 monitoring helped the client to proactively identify and respond to potential threats. SISA also recommended remediation measures, which helped them contain threats with speed and accuracy, and work on other priorities without the fear of being compromised.
Following the implementation of ProACT MDR solution, SISA also performed Attack Simulation to test the use cases across Windows, Linux, and Firewall, which helped ensure that the use cases would function properly and be successfully activated in scenarios where actual attacks might occur in the future. The partnership has also helped the client improve their overall security posture and governance through SISA's quarterly review meetings, monthly reports and real-time dashboard offering 360-degree visibility into malicious activities. The in-depth reporting with detailed indicators and performance metrics made the handling of escalation issues easy and compelling.

Importantly, the client was able to see a 72% reduction in the Mean Time to Detect (MTTD) and a 64% reduction in the Mean Time to Respond (MTTR) over the course of six months with the help of SISA's efficient governance model consisting of weekly, monthly and quarterly connects with various stakeholders at different levels. Besides, the regular finetuning of the alert engine helped reduce the false positive count and improve the overall SOC monitoring. As part of its mission to disseminate forensic learnings among industry participants at large, SISA's MDR team also conducted a focused Forensic Learning Session (FLS) and Ransomware Prevention Learning Session which helped improve client's employee awareness and preparedness for any future cyber attacks.

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 Security & Governance

Data Discovery and Classification - SISA Radar

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

Data Security as a Service

SISA Training

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