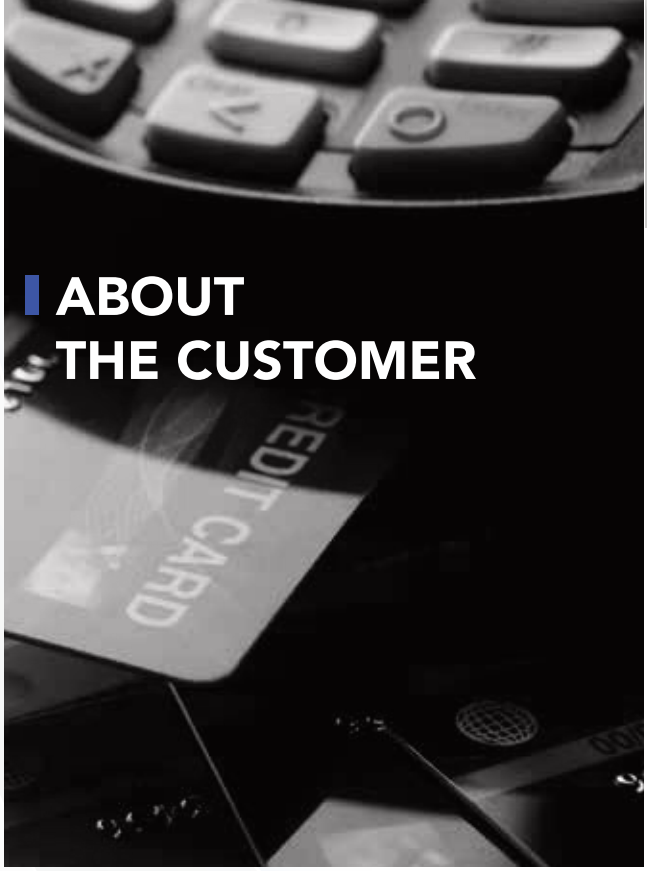
SISA

CUSTOMER SUCCESS STORY

SISA Radar helps global payments processor optimize sensitive data discovery and storage.



ABOUT THE CUSTOMER

The client is one of the leading enablers of digital commerce in the Middle East and Africa (MEA) region. It provides a robust suite of payment products and services to merchants and financial institutions including payment devices, online payment solutions, and debit & credit card services. With over 20 years of industry experience in financial services, payments, and technology sectors, the client also offers processing, fraud protection, loyalty, and bill payment solutions to its customers.

THE CHALLENGE

As one of the largest acquirers in the region, it was a challenging task for the client to scan its huge data environment to identify and remediate sensitive data spread across networks, servers, and endpoints. At first, the agents deployed for scanning continued to disconnect frequently due to recurring network drops and connectivity issues. In addition to that, the client found it challenging to add multiple IP addresses by range or hostname to the scans. With its business expanding across multiple regions, scanning a high volume of subnets every quarter increased the complexity. Further, the client was unable to discover data stored in USB storage devices and hard disks. Taking remediation actions for the discovered data was also an uphill battle as the existing data discovery solution couldn't recognize the last modified files for scanning. Moreover, the client was using two separate tools to quarantine the data sets as part of remediation actions which prevented them from obtaining a unified view.

SOLUTION OFFERED BY SISA

As a first step to streamline the scanning process for the client, SISA identified the root cause of frequent connectivity interruptions. It was found that the LAN repeatedly disconnected from the network as a consequence of the latest patch updates, resulting in the systems getting turned off. SISA Radar provided an option to initiate the scans automatically once the connection was restored. The client was also able to easily add all the IP addresses for scanning by leveraging the template provided by SISA Radar with an additional option to import them. As scanning the entire system in a single batch was a complex exercise and extremely time-consuming, SISA Radar provided the option of modular scanning that enabled the client to scan only the specific folders in the system at a given time. With SISA Radar's assistance, the client was also able to accurately scan all the external storage devices as well as the databases with a reduced impact on the database server end. Optimizing the possibility of incremental scans, SISA Radar was able to recognize and scan only the last modified files for the client to take necessary remediation actions. Additionally, SISA Radar provided options to scan the network and servers with low, medium, and high CPU usage to regulate the impact on their performance. The client also sought SISA Radar's assistance to scan Emirates IDs and National IDs of its customers. Moreover, SISA Radar simplified the assessment process by generating customized reports with user-defined columns to analyze and classify the department-wise sensitive data and send them automatically to a secure location. SISA also shared best practices and recommendations based on forensics learnings from previous investigations to assist the client in closing security gaps. The forensics learnings, which include a set of 'Preventive and Detective' controls in addition to the PCI controls, assisted the client in implementing stronger controls without hampering the PCI certification program.

BUSINESS IMPACT

Learnings from SISA's forensics-driven cybersecurity approach aided in the development of the necessary features in SISA Radar for use in this specific case. By leveraging the solutions provided by SISA Radar, the client was able to successfully scan all the external devices to identify and remediate any stored card data. After taking the necessary remediation actions, the client was also able to achieve compliance with Payment Card Industry Data Security Standards (PCI DSS). As the agent services were running in the background, the frequent network drops didn't affect them, and the client was able to complete the scans on time. Minimal human intervention and one-time activity to add all the targets (operating systems & databases) reduced the scan time and enabled the client to efficiently monitor them for its large data environment.

SISA

A forensics driven cybersecurity company, trusted by organizations across the globe for securing their businesses with robust preventive, detective, and corrective security services and solutions.

Compliance

PCI Compliance

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ

PCI Compliance

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Swift
- Cloud Security
- Risk Assessment
- Quarterly Security Audits

Security Testing

Application Security

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

Network Security

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

IoT Security Testing

Managed Security Services

Phishing Simulation

Cyber Resilience

Managed Detection and Response Solution

SISA ProACT

Incident Response and Forensics

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

Advanced Threat Hunting

Data Protection

Data Discovery and Classification Tool - SISA Radar

- Card Data Discovery
- PII (Privacy) Data Discovery
- Data Classification

Data Discovery as a Service

Training

Payment Data Security Implementation Programs

- CPISI
- CPISI Advanced
- CPISI-D

Security Incident Detection and Response Programs

- CIDR

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