SISA

CUSTOMER SUCCESS STORY

An American healthcare MNC strengthened its data security policy by integrating SISA Radar with DLP solutions.

ABOUT THE CUSTOMER

The client is an American multinational healthcare company with a presence in over 160 countries. The MNC, is committed to building life-changing technologies to help its customers better manage their health, provides medical devices, diagnostics, nutritional products, and branded generic pharmaceuticals. The client is also one of the pioneers in glucose monitoring, point of care testing, chronic pain devices, and adult and pediatric nutrition.

THE CHALLENGE

Being a global healthcare leader with a dynamic data environment, scanning multiple servers, databases, endpoints, and cloud platforms for critical data was not an easy task. Firstly, as the sensitive data was scattered across the vast network, the client confronted challenges to meet compliance requirements of Payment Card Industry Data Security Standards (PCI DSS). Scanning trillions of records present in the database consumed a lot of time and impacted the performance of servers. In addition to that, with thousands of tables in the database and millions of new records being created every day, the client was unable to clearly determine the number of rows that were left for scanning or were found with errors. Once the scans were completed, the client also found it challenging to encrypt the card numbers in databases to prevent the data from being misused. Further, classifying the scanned files for the agentless scans based on their criticality level was a complex task and the client was confronted with the risk of these files being shared over untrusted networks.

Moreover, with its business presence in various geographies, scanning S3 buckets of multiple regions from one single location was an uphill battle. The healthcare company also encountered a high percentage of false positives as the existing tool identified health card numbers as real credit card numbers.

SOLUTION OFFERED BY SISA

As a first step to increase the speed of scans, SISA Radar automated the scanning of all the records in the database during non-working hours and provided an option to increase the thread counts and table offset value in GUI during the weekends. SISA Radar also helped to optimize the scans with an option to auto-pause or resume the scans for production servers at specific time intervals. Further, to keep track of databases being scanned every day and improve the visibility over row counts, SISA Radar provided an option to generate logs for each table to help determine if the scans for the particular rows were completed, incomplete, or resulted in an error. Once the scans were completed, SISA Radar also provided three types of encryption and decryption methods namely, AES 256, Triple DES, and Rijndael to secure sensitive data. To save the scanned files from being lost or misused, the client leveraged SISA Radar's ability to integrate with Data Loss Prevention (DLP) solutions.

SISA Radar was able to create classified watermarks (confidential/sensitive) for the identified files and apply the DLP rules such as edit access, file copy, and transfer to block these files from being shared over untrusted networks. SISA Radar also assisted the client with an option to create a customized regex to scan the network for health-related sensitive data and take the necessary remediation actions. With an option to select all the bucket-created regions for scanning in SISA Radar, the client was able to perform scans for all the S3 buckets through one single platform. Lastly, AI & ML integration enabled the data discovery and classification tool to improve data accuracy by eliminating false positives.

SISA also shared best practices and recommendations from forensics learnings derived from previous investigations to help the client address the security gaps. The forensics learnings which encompass a set of 'Preventive and Detective' controls above and beyond the PCI controls, helped the healthcare client implement stronger controls, without hampering the PCI certification program.

BUSINESS IMPACT

By choosing SISA Radar to automate the scans for a huge data environment, the client was able to achieve compliance with Payment Card Industry Data Security Standards (PCI DSS). The learnings from SISA's forensics-driven cybersecurity approach helped build in the requisite features in SISA Radar to be used in this specific case. SISA Radar's integration with DLP solutions helped the client prevent unauthorized access to sensitive data and avoid data leakage. SISA Radar tool also helped the client determine the estimated time to complete the scans along with the percentage of completed scans. By automating the discovery, classification, and remediation processes in one single tool, the client was able to efficiently regulate the scans with minimal impact on the servers' performance.

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