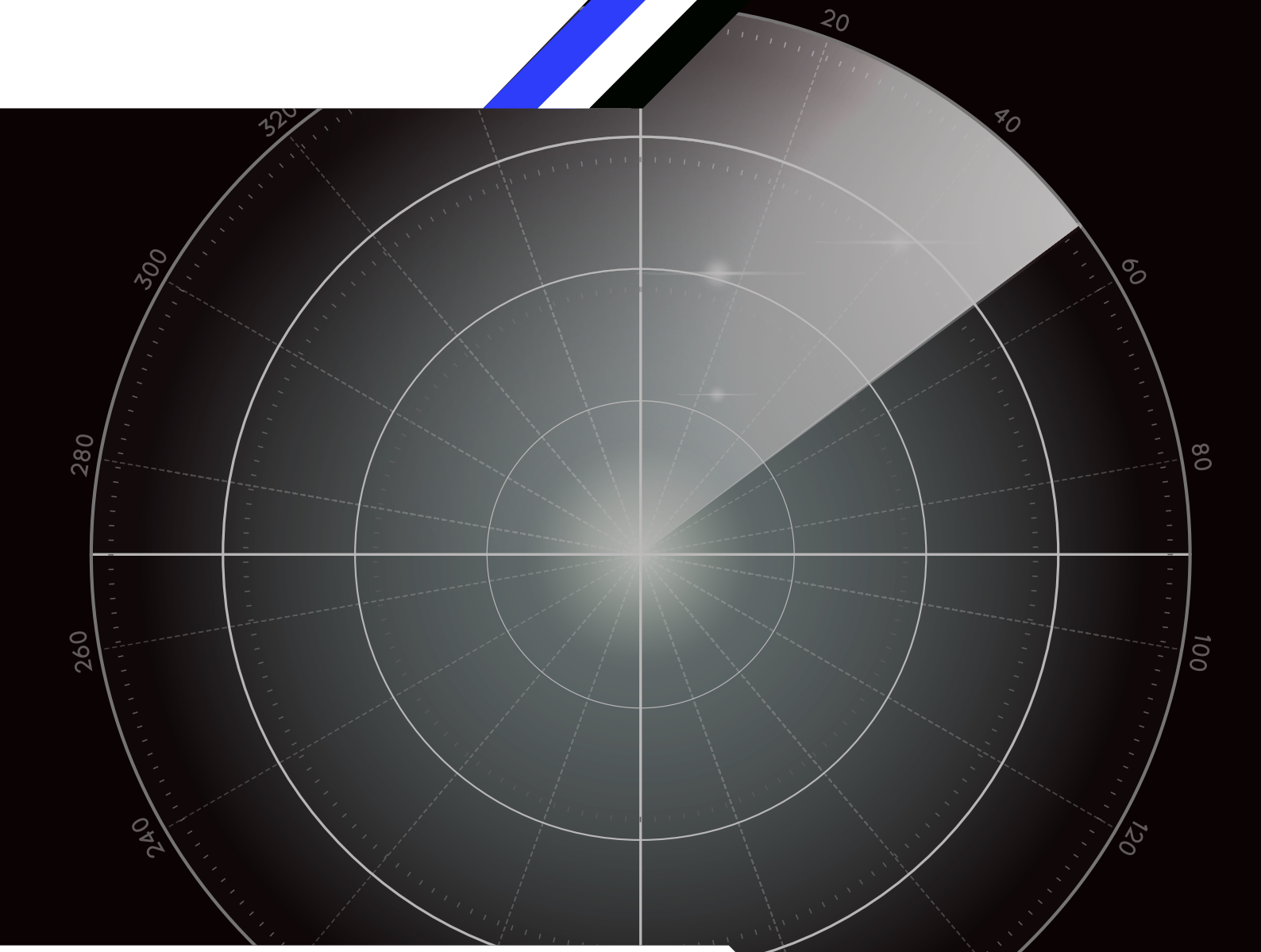
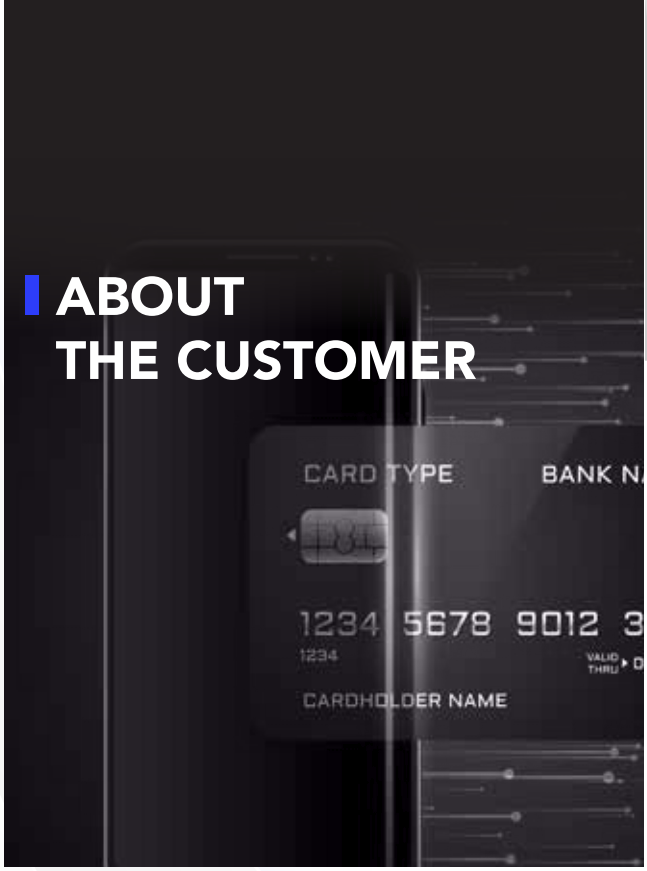
SISA



CUSTOMER SUCCESS STORY

A leading Indian private sector bank achieves compliance and secures sensitive data with SISA Radar



ABOUT THE CUSTOMER

The client is a banking and financial services company headquartered in India. It is one of the leading private sector banks in India by assets and one of the largest banks in the world by market capitalization. With 4,000+ branches, the bank has an extensive portfolio of products and services that covers transactional, commercial, and investment banking including wholesale banking, treasury, retail banking, auto loans, personal loans, lifestyle loans, and credit cards.

THE CHALLENGE

Being one of the largest employer banks in India, the client was confronted with multiple challenges while scanning its network environment for sensitive data. Data scattered across 10,000+ targets that included servers, endpoints and databases, made complying with Payment Card Industry Data Security Standards (PCI DSS) and Reserve Bank of India (RBI) norms, an uphill battle. The manual deployment of agents to scan 5,000 machines and terabytes of data and perform authentication without impacting transactions was complex and challenging. Further, the bank encountered multiple false positives, as most of the existing tools identified any 16-digit number as a card number. Thirdly, the bank was unable to complete the scans and identify the owner/creator of the files, as the IP addresses of the systems changed due to dynamic environment. Although the bank sought a solution by examining POCs of more than six data discovery vendors, they required high-configuration hardware equipment to deploy the scanning tool. Moreover, none of the previously tested data discovery tools was able to accurately scan multiple file formats to identify the sensitive card data.

SOLUTION OFFERED BY SISA

To simplify the scanning process and minimize manual efforts of deployment, SISA used System Center Configuration Manager (SCCM) tools for all 5,000 machines to deploy the agents with auto-registration to the server. With the agent running in the end machine, the bank's network bandwidth consumption was lowered, and SISA Radar was able to initiate the scans simultaneously for all 5,000 machines with minimum hardware requirements. Adhering to the RBI guidelines, SISA also deployed desktop applications in the centralized machine to increase reachability. With an optimized algorithm, SISA Radar was able to identify both structured and unstructured sensitive data in log files, text files, no extension files, images as well as PDF files with handwritten texts. Moreover, AI & ML integration enabled the tool to improve data accuracy by eliminating false positives. The bank was unable to run automated scans on 5,000 machines during non-business hours. To overcome this challenge, SISA Radar supported scheduled scans through auto pause and resume options and provided a customized display of estimated period to optimize and complete the scans on time. Additionally, SISA Radar provided options to scan the critical servers with low, medium, and high frequency to help control the impact on their performance. The bank also sought SISA's assistance to perform scans on isolated servers using SISA Radar manual agents with encrypted reports. SISA Radar also helped the bank take quick remediation actions on the discovered data by displaying detailed file fields and history in the customized reports generated by the tool.

BUSINESS IMPACT

By choosing SISA Radar to execute the scanning process, the bank was able to successfully meet the requirements of PCI DSS compliance as well as RBI guidelines. Any data identified as critical was either masked, deleted, or moved to secure locations; then the systems were re-scanned to get a clean report for compliance. SISA Radar also enabled the bank to identify sensitive data across the environment at scale and in a single-click and facilitate the quarterly scans with reduced time and cost. The bank was also able to avoid the risk of exposure to card data in multiple files and improve its data retention policy to stay compliant with the data protection and privacy regulations.

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