



CUSTOMER SUCCESS STORY

SISA's comprehensive red teaming assessment helps a leading cooperative bank uncover critical security flaws and improve defences



ABOUT THE CUSTOMER

The client, a leading scheduled bank in India with a history of over 125 years is one of the oldest and most recognized names in the co-operative banking space. The bank, originally registered as a Co-operative Credit Society has expanded its business line over the years and now offers a full suite of personal and corporate banking services. It accepts deposits, issues loans, and provides currency exchange services, as well as offers insurance products and mutual funds. Headquartered in Maharashtra, the bank has a vast spread of 198 branches across 11 states with employee strength of over 2,500.

THE CHALLENGE

As a banking entity operating in a regulated sector and dealing with sensitive customer data, the bank's foremost priority was to secure its digital systems to process transactions, store sensitive information, and maintain the trust of customers. The bank also wanted to have a better understanding of its security posture, detect any weaknesses and gaps in the infrastructure, and identify areas for improvement. They had partnered with a few other cybersecurity service providers for red teaming exercise, however none of them were able to gain access to the servers containing critical data and/or recommend actions for enhancing their security posture. They were looking for a specialist vendor to help them update their security policies, identify weak points in their network, servers and endpoints, educate their Blue Teams on the counter measures to be adopted in the event of a breach, and create awareness about social engineering attacks among the employees.



SOLUTION OFFERED BY SISA

The bank engaged SISA to conduct a multi-layered attack simulation and red team assessment to measure how well the bank's personnel, networks, applications, and physical security controls can withstand an attack from a real-life adversary. SISA adopted a four-step framework that consisted of Reconnaissance, Planning & Preparation, Attack Execution and Reporting & Remediation, and worked closely with the bank's team to tailor the red team activities to their specific requirements and goals.

The scope of this assessment covered physical security assets, wireless access points, and social engineering defences.

PHYSICAL SECURITY ASSESSMENT

SISA kicked off the assessment by conducting a physical security evaluation of the bank's premises. SISA's red team inspected all the assets in the bank and identified that one VLAN port was open, which allowed the team to connect their exploitation framework (Parrot OS) to the bank's network. During this stage, SISA's team also noticed that one of the bank employees had left their computer unlocked, giving them access to the IP address, DNS server IP, and MAC address of the computer. They were able to inject pen drive into the target and access all critical/generic data available in the machine without authorization. The red team then performed Wardriving to locate and exploit connections to Wi-Fi networks. By following the USB drop approach and using a Linux OS to crack the Windows password, SISA's team was successful in locating the credentials and decrypting them.

NETWORK ENUMERATION AND VULNERABILITY SCANNING

SISA began performing all testing activities from the perspective of an unauthenticated user on the internal network. It first started enumerating all the connected devices in the network and discovered that the IP addresses were assigned via static allocation. SISA's red team spoofed the MAC address of the employee's computer and assigned the same IP address to the red team's machine, which enabled SISA to scan the network for vulnerabilities. When performing network scanning, SISA tried to poison the entire VLAN to get the Hashes. The team was also able to identify that one of the bank's SQL servers was vulnerable to MS17-010 (vulnerability which allows for remote code execution and can spread through networks). This allowed them to execute the arbitrary payload and compromise the server thereby letting them access sensitive data. However, as the agreement restricted dumping of data, there was no data exfiltration.

DOMAIN ENUMERATION AND EXPLOITATION

The next attack vector used in the red teaming exercise was Domain Enumeration. As SISA continued to explore the bank's network, the team discovered that there was another VLAN, which was separated from the employees' assets, and all the payment servers were restricted from being accessed through the VLAN. These servers were only reachable from the compromised SQL server. Based on the scan results, the red team found a vulnerability in the Active Directory (AD) domain through DNS query injection. They exploited this to successfully update the DNS records which gave them access to the domain and allowed them to perform lateral movement.

B BUSINESS IMPACT

The full red teaming exercise executed by SISA was highly successful and yielded a significant set of results, highlighting critical gaps and vulnerabilities in the bank's security architecture. SISA's team identified seven vulnerabilities (with three of them rated as high risk) and demonstrated the potential impact of threat vectors on the confidentiality, integrity, and availability of the bank's information systems. At the end of the assessment, SISA provided the bank with a detailed report outlining findings and recommendations for improving their security posture.

SISA also shared best practices from forensic learnings derived from previous investigations to help the bank address the security gaps. The forensic learnings which encompass a set of 'Preventive, Detective and Recovery' controls above and beyond the PCI DSS controls, helped the bank implement stronger protocols. Overall, the red teaming exercise helped the bank strengthen its security defences and improve preparedness for real-world cyberattacks.



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

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