SISA

CUSTOMER SUCCESS STORY

SISA's forensics-driven consultative approach to application security helps a global service provider mitigate critical security vulnerabilities

ABOUT THE CUSTOMER

The client is a global service provider headquartered in India with domain expertise in digital customer experience, back-office processing, and contact centers. It operates with 30+ delivery centers in 8 countries and has over four decades of experience working with some of the world's top brands. The client offers services that integrate automation, analytics, and artificial intelligence to assist its customers across key industry verticals in overcoming challenges posed by labor, productivity, and technology.

THE CHALLENGE

As a global leader in customer experience and business process management, with customers across industries, the client faced substantial challenges in achieving compliance and meeting audit requirements associated with application security. To meet some of these requirements, it was mandatory for them to conduct a security assessment by an organization that was CERT-In Empaneled (Indian Computer Emergency Response Team) and CREST-Accredited (Council for Registered Ethical Security Testers). Failure to comply with these regulations could result in significant fines and legal penalties for the client. Furthermore, any new and ongoing developments in the application led to new challenges, and the internal security team was unable to discover the hidden critical vulnerabilities. Insecure coding practices and a lack of effective security controls in the application exposed sensitive data to security risks of confidentiality, integrity, and availability. This posed a serious threat to the client's ability to safeguard its customers' data and maintain their trust. To address these challenges, the client required a comprehensive security solution that would enable them to identify and mitigate critical vulnerabilities, implement appropriate security controls, and meet regulatory requirements.

SOLUTION OFFERED BY SISA

SISA, being a forensics-driven cybersecurity solutions company that is both CERT-In Empaneled and CREST-Accredited, was well-suited to fulfill the client's requirements and provide an in-depth security assessment that met all regulatory standards. To conduct the application security testing, SISA adhered to the best practices from global industry standards such as OWASP, SANS, and NIST, and followed a 4-phased methodology that included application walkthrough, penetration testing, vulnerabilities clarification and revalidation, to address the client's application security concerns. The engagement began with scoping exercise and a detailed walkthrough of the application to understand the process flow and identify the vulnerabilities in business logic. SISA performed a comprehensive application security assessment using a combination of automated and manual application penetration testing adhering to the OWASP Application Security Verification Standard (ASVS). Leveraging the learnings from the past forensic investigations, SISA identified a total of 16 vulnerabilities, with 2 critical and 1 high vulnerability in the application including SQL injection, server-side template injection, input validation issues, and inadequate access control. To help close these security gaps, SISA educated the client on the severity of vulnerabilities and their potential impact on the application and shared best practices and recommendations to mitigate them. Finally, SISA revalidated the application to ensure that the remediation efforts were successful and that the detected vulnerabilities were fixed. A complete report containing the identified vulnerabilities, their potential impact, severity, proof of concept, and recommendations was also shared with the client.

BUSINESS IMPACT

The vulnerabilities uncovered by SISA's comprehensive application penetration testing posed the risks of data loss, theft, denial of service, data integrity loss, and system compromise by an attacker. SISA's forensics-driven approach to cybersecurity helped the client identify and mitigate these critical flaws prior to application release. A thorough security assessment and detailed recommendations by SISA enabled the client to implement the necessary security controls, assuring that the application was secure and ready to go into production without any major security concerns. This provided true security for the client, ensuring that sensitive data was protected, regulatory requirements were met, and customer trust was reinforced. SISA's consultative approach, which involved multiple rounds of discussion, assisted the customer in addressing the security gaps without impacting the application's functioning. SISA's deep domain expertise and responsiveness also enabled the client to promptly fulfil its customer requirements for security assessments.

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