CUSTOMER SUCCESS STORY

SISA Helps a Global Enterprise Strengthen Wireless Security and SOC Resilience Across Complex Network Environments

About the Customer

The client is a global consulting and technology services firm specializing in providing solutions that support businesses in their digital transformation journey. With a strong presence in over 40 countries, the company offers a wide range of services, including IT consulting, cloud services, and business analytics. They work with clients across various industries to drive innovation, enhance customer experiences, and improve operational efficiency. Their approach combines deep industry knowledge with cutting-edge technology to deliver scalable and sustainable results.

The Challenge

As a global provider of business and service solutions serving a diverse, multi-industry clientele, the client faced mounting complexity in securing its wireless infrastructure. With numerous SSIDs deployed across geographically dispersed locations, ensuring consistent and robust protection across all wireless access points was a critical challenge.

The scope of the security assessment included eight distinct wireless networks (SSIDs), covering internal and external user groups such as employees, guests, mobile devices, IoT systems, and BYOD setups. The network environment featured a mix of WPA2-Enterprise networks, a WPA2-PSK network, and an open-access guest network, each presenting unique security considerations. The primary objective was to identify exploitable weaknesses and ensure adherence to best practices in wireless network security.

Adding to the complexity, the client emphasized the need for a comprehensive evaluation of their Wi-Fi architecture, specifically focusing on potential misconfigurations, weak encryption standards, and risks of unauthorized access. They also sought to validate the operational readiness of their Security Operations Center (SOC). This included assessing the SOC team's ability to detect, investigate, and respond to wireless-based threats in a timely and coordinated manner. The goal was to benchmark the effectiveness of existing security protocols, monitoring tools, and incident response strategies against the organization's stringent standards for cyber resilience.

SOLUTION OFFERED BY SISA

SISA, a forensics-driven cybersecurity solutions provider, CERT-In Empaneled and CREST-accredited, was uniquely positioned to meet the client's stringent security and regulatory requirements. To carry out the wireless security assessment, SISA followed globally recognized best practices, including the 802.11x security testing standards.

The engagement followed a structured 4-phased methodology

Scoping and Site Pinning
The process began with a detailed scoping exercise, which included identifying the target SSIDs and physically mapping the client's wireless network infrastructure across locations.

Wireless Fidelity Security Assessment
A thorough Wi-Fi penetration test was conducted based on the documented TTPs, evaluating architecture, configurations, and security controls.

TTP Documentation and Downtime Communication
Once the scope was finalized, SISA shared a comprehensive document outlining the Tactics, Techniques, and Procedures (TTPs) to be used during testing, along with anticipated system and infrastructure downtime to ensure full transparency and alignment.

Vulnerability Analysis and Remediation Guidance
Drawing from its extensive experience, SISA identified 10 critical vulnerabilities within the client's wireless infrastructure. Each finding was communicated with detailed context, highlighting severity, potential impact, and proof of concept. SISA also provided actionable best practices and strategic recommendations to mitigate the risks.

4 PHASED METHODOLOGY

SISA Recommendations

A detailed report outlining all findings, severity levels, and remediation strategies was shared to support the client's internal security enhancement and compliance goals. Key recommendations included:

01 Strengthening Network Architecture & Access Controls

Isolation of Vulnerable Networks

Restrict access to vulnerable internal networks (e.g., guest/external networks) to prevent lateral movement.

Reconfiguration of Wireless Security Settings

Harden WPA2-PSK and Enterprise setups with stronger encryption and access control.

Patch Management

Update firmware and devices to eliminate known vulnerabilities.

02 Enhancing Identity & Credential Security

Credential Management

Rotate credentials and access keys for all compromised accounts, with priority on exposed NTLMv2 hashes and sensitive user data.

Multi-Factor Authentication (MFA)

Enforce MFA for all critical wireless network administrative accounts and those with access to sensitive network segments and configurations

03 Improving Detection & User Awareness

Real-Time Monitoring & Intrusion Detection

Deploy WIPS and monitoring tools to detect rogue access points and anomalous activity in real-time across all sites.

User Training & Awareness

Conduct training to strengthen defences against social engineering and improper access.

Summary of findings: wireless security assessment by SISA

SISA uncovered critical vulnerabilities across the client's wireless network environment that could have been exploited by threat actors. Key findings included:

Unauthorized Access Risks
Multiple instances of wireless leakage, rogue access points, and network misconfigurations-posing a serious threat to data integrity and network availability.

Improper Network Segregation
Guest and employee networks were inadequately secured, increasing exposure to data exfiltration, lateral movement, and unauthorized access.

Protocol & Configuration Weaknesses
Vulnerabilities like WPA/WPA2 handshake captures, misconfigured VLANs, and insecure captive portals were prevalent across sites.

Credential Exposure
During the assessment, NTLMv2 hashes and login credentials belonging to a senior management member were captured. These hashes were then subjected to offline cracking attempts, revealing gaps in internal authentication security.

Gaps in Detection & Monitoring
Absence or misconfiguration of IDS, WIPS, and rogue access point detection limited the client's ability to monitor and respond to wireless threats in real-time.

Business Impact

SISA's forensics-driven approach enabled the client to identify and mitigate critical vulnerabilities before the application's release. Through a comprehensive security assessment and actionable recommendations, the client implemented robust controls—ensuring the application was production-ready with no major security concerns. This not only protected sensitive data and met regulatory requirements but also reinforced customer trust. SISA's consultative engagement, including multiple rounds of discussion, helped address security gaps without disrupting application functionality.

SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and correctivecybersecurity 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
- HITRUST

Unified Audits

Managed Compliance

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
- Firewall Rule Review
- PCI ASV Scan

Phishing Simulation

Red Teaming Exercise
- Layer Security Testing

Cyber Defense

Managed Extended Detection and Response Solution - SISA ProACT
- 24x7 Monitoring
- UEBA
- Threat Intel
- Advanced Threat Hunting
- Breach & Attack Simulation
- SOAR
- Use-case Factory

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 Protection & Governance

Data Discovery and Classification
- PCI/PII/PHI Data Discovery
- Data Classification in Endpoint (Windows, Linux)
- Data Classification in O365, Metadata
- Dynamic Masking, Redact, Truncation
- Integration to DRM, DLP, SIEM

Data Privacy Professional Services
- Assessments (Unified Privacy Maturity, DPIA, 3rd Party Risk)
- Data Inventory, Mapping and Process flow, RoPA
- Data Privacy Framework - Policy, Notice, SoPs
- Consent and Notice Management framework
- Data Breach and Management
- Principal management
- Privacy by Design implementation guide
- Define Data Retention Guidelines and processes
- Technical/Organization measures
- Privacy Training/Awareness

Trainings & Certifications

Payment Data Security Training and ANSI Accredited Certification
- CPISI (2 Day Program
- CPISI (3 Day Program)
- CPISI- Advanced (3 Day Program)
- CPISI-D (Developers)
- CPISI Hybrid (4 Weeks)

Certification Program in Cybersecurity for AI – CSPAI
- CSPAI
- CSPAI - Developers

Forensic Briefing Sessions for Senior Management

Leading Tech Security

AI PRISM
- AI PRISM LLM Vulnerability Scanner Solution
- AI Risk Management and Governance Solution Framework
- AI Compliance and Governance Consulting Service

Hardware and IoT Security Testing
- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing
- MPOC/ PCI PTS

Quantum Security
- Quantum Cryptographic Consulting
- Quantum Security Risk Assessment
- Quantum Security Standards Compliance

For more Information visit us at www.sisainfosec.com
or
write to us at contact@sisainfosec.com

Follow us