



CUSTOMER SUCCESS STORY

SISA Helps a Financial Services
Major Achieve Detection Readiness
with Breach and Attack Simulation

About Client

The client is a financial services provider and is considered one of the leaders in digital payments and Card processing in the Middle East region. Since 2009, it has specialized in delivering end-to-end card processing and electronic banking solutions for both financial and non-financial institutions. Its services span the full spectrum of card processing, supported by a robust back-end infrastructure.

As the processing arm of a national electronic payments network, the organization helps partner banks scale securely and efficiently by offering outsourced services that lower operational costs and boost profitability. Leveraging advanced technology and deep domain expertise, the client delivers reliable, user-friendly systems for card issuance, ATM management, and merchant acquiring.

The Challenge

The client was at a critical juncture facing rising cyber threats, increasing audit scrutiny, and the need to justify existing security investments. They needed to shift from a reactive security posture to a more resilient, threat-informed strategy. This meant not only validating the effectiveness of their existing controls but also testing how well their teams and technologies could respond under pressure. At the same time, they aimed to elevate security awareness across the organization and demonstrate stronger compliance to satisfy both regulators and internal stakeholders.

To meet their strategic goals, the client faced challenges on two fronts.

Internal Security Constraints



Limited Internal Visibility

across endpoints, cloud workloads, and devices made it hard to understand actual exposure.



Current SIEM and Monitoring Stack

with incomplete use cases and gaps in detection logic reduced the overall monitoring accuracy.



Existing Policy Configurations

on network and security devices, where silent misconfigurations often remained undetected.



Time and Resource Constraints

that made it challenging for teams to run manual or large-scale testing regularly.

External Pressures and Compliance Triggers

Beyond internal limitations, the client faced growing external drivers that demanded measurable improvements in security maturity:



Regulatory and Audit Findings

A recent audit highlighted gaps in incident readiness, policy enforcement, and threat detection coverage.



Pressure To Demonstrate Detection Capabilities

As part of compliance mandates, the organization needed the ability to detect and respond to adversarial activity in a timely manner.



Need For Proactive Control Validation

Rather than wait for a breach to test their defenses, the client wanted a proactive and repeatable mechanism to validate security controls.

Client's Key Strategic Imperatives

- Proactively Manage Cyber Risk
- Validate the Effectiveness of Security Controls and enhance security posture
- Assess Incident Response Readiness
- Strengthen Security Awareness Across Teams
- Meet Compliance and Regulatory Expectations

Technologies and Systems in Scope

- Windows
- Linux
- Firewall
- IPS
- WAF
- Web Servers
- Cloud (AWS, Azure, GCP)
- HSM
- Database
- Mail Filter (O365)
- Proxy
- Antivirus / EDR

*Not limited to the above...



SOLUTION OFFERED BY SISA

A Forensic-Driven Simulation Framework: SISA deployed a customized Breach and Attack Simulation (BAS) framework aligned with real-world adversary behavior.

01 Attack Simulation Design

SISA's approach was anchored in real world threat intelligence, industry attack patterns, and forensic insights from recent global breach investigations:



Custom Attack Scenarios

We built simulation playbooks tailored to the client's business context, infrastructure, and risk profile. These reflected tactics used by threat actors targeting similar industries.



MITRE ATT&CK-Aligned Methodology

All simulations were mapped to the MITRE ATT&CK framework, enabling structured coverage of TTPs (Tactics, Techniques, and Procedures) and alignment with global threat models.



Forensic Intelligence Integration

Drawing from SISA's breach response experience, the scenarios included real attack artifacts and behavior patterns, making them as close to live threats as possible.

02 Comprehensive Simulation Execution

The simulations were conducted using both internal and external vantage points, spanning the client's hybrid environment:



Types of Simulations

Internal Attack Simulation

Lateral movement, privilege escalation, and data exfiltration from within the network.

External Attack Simulation

Perimeter breach attempts, web application compromise, ransomware injection.

Cloud Attack Simulation

Misconfiguration exploitation and access control testing in AWS, Azure, and GCP environments.

Ransomware Attack Simulation

End-to-end simulation of ransomware infection to help validate EDR performance, containment protocols, and recovery processes.

Regulatory Cyber Drill

Simulate targeted cyberattacks to assess an organization's detection and response readiness, validate existing controls and ensure alignment with regulatory expectations.

03

Tailored Enhancements
for the Client**Custom Script Development**

SISA's team created scripts to simulate business-critical data access and bypass detection mechanisms..

**Use Case Validation**

Each simulation was mapped to the client's SIEM detection rules to test real-time alerting and response efficiency.

**Incident Response Drill**

Simulations were designed to assess how quickly and effectively internal teams responded to attacks, including ransomware events.

Key SISA Deliverables

- Tactics-wise success and failure ratio
- Technique-wise success and failure ratio
- Evaluation of security controls (EDR, Firewall, DLP, etc.)
- Identification of improvement areas through detailed reporting
- Use case effectiveness assessment
- SOC threat monitoring capability analysis
- Recommended mandatory use cases by device type based on activity

Business Impact

SISA's Breach and Attack Simulation engagement transformed the client's security posture to one with evidence-backed readiness. The impact was visible across four key dimensions:

**Improved Visibility into Actual Control Performance**

Simulations revealed exactly how each layer of defense - EDR, SIEM, firewall, cloud controls, and more - responded to real-world attack techniques. As security controls were evaluated in live attack conditions, removed guesswork and gave the client a clear view of how each control performed under stress.

**Clear Action Plan for Detection and Response Maturity**

Each simulation was mapped to detection logic and incident response workflows, providing a step-by-step roadmap to elevate operational security. Further device-level use case mandates were created thus ensuring minimum viable detection capability across all critical assets.

**Evidence for Audit and Compliance Requirements**

The simulation report served as structured, audit-ready proof of cybersecurity testing, directly supporting compliance obligations. Reports included detailed findings, logs, timelines, and control performance metrics ready for submission to auditors, regulators, and internal stakeholders.

**Strengthened Readiness for Real-World Attacks**

By simulating ransomware and targeted breach scenarios across internal, external, and cloud environments, the client strengthened its breach response capabilities.

To learn more

about our Breach and Attack Simulation, kindly visit our Webpage



<https://www.sisainfosec.com/cyber-resilience/incident-response-forensics/breach-and-attack-simulation/>

Key SISA Deliverables



Tactics-wise success and failure ratio



Technique-wise success and failure ratio



Evaluation of security controls (EDR, Firewall, DLP, etc.)



Identification of improvement areas through detailed reporting



Use case effectiveness assessment



SOC threat monitoring capability analysis



Recommended mandatory use cases by device type based on activity

Business Impact

SISA's Breach and Attack Simulation engagement transformed the client's security posture to one with evidence-backed readiness. The impact was visible across four key dimensions:



Improved Visibility into Actual Control Performance

Simulations revealed exactly how each layer of defense - EDR, SIEM, firewall, cloud controls, and more - responded to real-world attack techniques. As security controls were evaluated in live attack conditions, removed guesswork and gave the client a clear view of how each control performed under stress.



Evidence for Audit and Compliance Requirements

The simulation report served as structured, audit-ready proof of cybersecurity testing, directly supporting compliance obligations. Reports included detailed findings, logs, timelines, and control performance metrics ready for submission to auditors, regulators, and internal stakeholders.



Clear Action Plan for Detection and Response Maturity

Each simulation was mapped to detection logic and incident response workflows, providing a step-by-step roadmap to elevate operational security. Further device-level use case mandates were created thus ensuring minimum viable detection capability across all critical assets.



Strengthened Readiness for Real-World Attacks

By simulating ransomware and targeted breach scenarios across internal, external, and cloud environments, the client strengthened its breach response capabilities.

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	Security Testing	Cyber Defense	Data Protection & Governance	Trainings & Certifications	Leading Tech Security
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	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	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 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	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	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

