



CUSTOMER SUCCESS STORY

SISA's Red Team Engagement with a
Leading Payment Gateway

| About the Customer

The client is a leading payment gateway provider specializing in online payment solutions across South-East Asia. With operations spanning across Malaysia and Southeast Asia, the company offers comprehensive payment solutions for e-commerce, retail, and e-wallets. Their customer base includes merchants ranging from startups to multinational businesses, helping them scale their online operations. With an approach that combines proprietary gateway technology and state-of-the-art solutions, the client delivers secure payment processing. With a leading presence in the South-East Asian region and close to 8,000 customers, they are the region's trusted choice for online payments.

| The Challenge

The customer faced a rapidly expanding risk surface that outpaced its existing defenses. As a leading digital payments provider operating across multiple domains, their environment had become a patchwork of interconnected systems, cloud services, third-party integrations, and customer-facing applications. While this complexity powered their growth, it also multiplied the opportunities for attackers. The challenges were in 3 key categories:

01 Technology Surface - Too Broad, Too Fragile

The customer's technology environment had grown into a sprawling, interconnected mesh of on-premises systems, multi-cloud deployments, and customer-facing applications. While this architecture enabled agility and scale, it also introduced blind spots. Misconfigurations could easily slip through unnoticed, leaving weak controls scattered across domains. The proliferation of web applications and payment APIs further expanded the attack surface, offering adversaries multiple entry points to exploit. Inside the network, inadequate segmentation and unchecked user privileges created pathways for attackers to move laterally once inside, turning a single foothold into a potential full-scale compromise.

02 Human & Physical Layer - The Unseen Weak Points

With over 190 publicly accessible employee email addresses made the organization an inviting target for phishing and social engineering campaigns. Employees, never truly tested against real-world adversarial tactics, lacked the readiness to identify and counter such threats. Compounding this, critical physical spaces were inadequately secured against tailgating and unauthorized entry. These human and physical gaps, often underestimated, could serve as the easiest entry points for an attacker to gain access and escalate further.

03

**Ecosystem & Compliance -
Risks Beyond the Perimeter**

Beyond its own walls, the organization operated within a vast network of third-party relationships from banks and payment processors to e-wallet partners that expanded the threat surface to include supply chain risks outside its direct control. This interconnectedness meant a single weak link could trigger cascading security failures. Simultaneously, as a financial services provider, the company faced intense regulatory scrutiny and the constant need to demonstrate compliance with stringent industry standards. Yet, fragmented detection and response across hybrid environments made meeting these expectations increasingly difficult. These combined external pressures demanded a holistic and proactive approach to security validation.



SOLUTION OFFERED BY SISA

To address these multifaceted risks, SISA conducted a **Full-Spectrum Red Team Assessment** - a controlled, adversary-simulated engagement that mirrored how real attackers would attempt to breach the organization. SISA's three-pronged assessment ensured that vulnerabilities across people, technology, and physical environments were uncovered, providing the organization with a **realistic, attacker's-eye view of its security posture**, all while ensuring business continuity remained intact.

Simulate real-world cyberattacks using the same tactics, techniques, and procedures (TTPs) employed by today's threat actors.

Test defense-in-depth, including employee awareness, network resilience, and detection/response capabilities against stealthy multi-vector intrusions.



Reveal the true state of security posture, beyond certifications like PCI DSS or ISO 27001, by exposing vulnerabilities that could be exploited in real attacks.

Strategic Goals Behind the Assessment

01**People Layer – Passive Reconnaissance and Social Engineering**

The first phase targeted the human element, often the weakest link in security. SISA conducted open-source intelligence (OSINT) investigations to identify exposed employee email addresses and leaked credentials that attackers could exploit. This was followed by simulated phishing campaigns, designed to mimic real-world credential harvesting attempts, revealing how employees responded under pressure. Throughout this phase, SISA evaluated internal security awareness and adherence to security protocols, uncovering behavioral gaps that could be exploited in an actual attack.

02**Technology Layer – Active Cloud, Network, and Application Exploitation**

The second phase saw SISA actively probe the customer's technology stack and find critical cloud misconfigurations that could expose sensitive data. Wireless testing uncovered weak WPA2-PSK setups and no Network Access Control, which allowed SISA to access the Wi-Fi and compromise Active Directory without entering the office. Simulated black-box and grey-box attacks against ATM and payment systems revealed transaction flow vulnerabilities. Employees lacked awareness of physical threats, password policies were weak, and the Active Directory configuration was generic, all factors that make the environment highly prone to modern attacks.

02**Physical Security – Facility and Process-Oriented Exploitation**

In the final phase, SISA turned its attention to the physical security controls safeguarding critical infrastructure. Simulated adversarial attempts were made to tailgate into restricted areas, including the IT department, to test whether unauthorized access could be achieved. The team evaluated visitor authentication processes and access control measures, exposing process-oriented weaknesses that attackers could exploit to bypass physical defenses. These findings highlighted how physical and cyber risks often intersect, creating opportunities for blended attack scenarios.

The Attack Lifecycle: SISA's Multi-Phase Simulation

Initial Access

Launched a **phishing campaign** using fake domains

Tailgated into the office, bypassing physical security checks

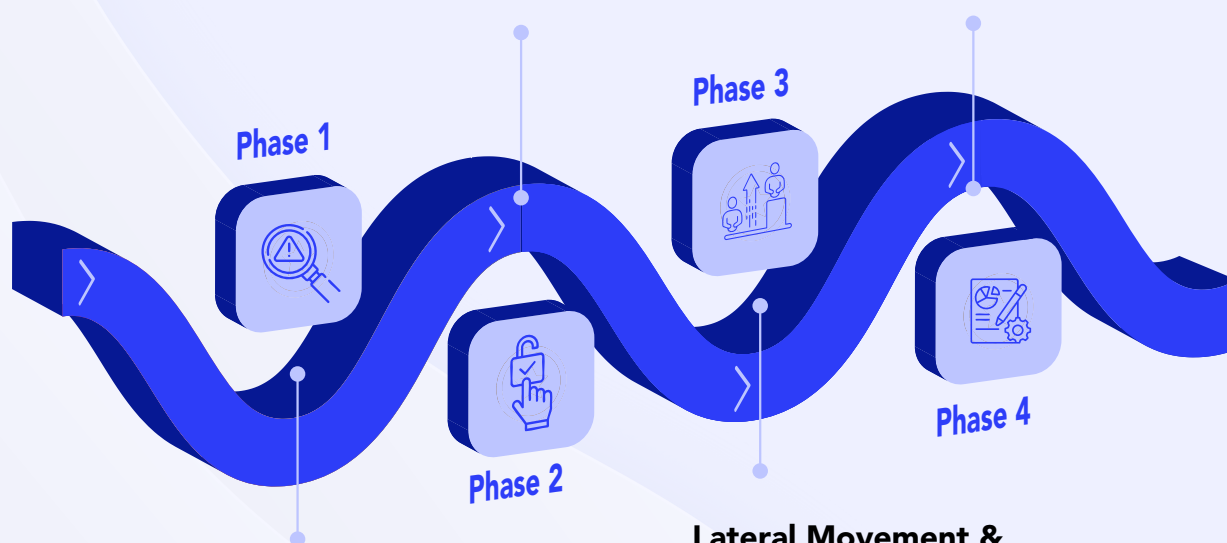
Captured a **WPA2 handshake** and cracked it in under 3 hours

Post-Exploitation & Reporting

Accessed **VOP Tech IP phones** using default credentials

Dumped **2,000+ Active Directory hashes**, confirming widespread credential reuse

Uncovered **18 key vulnerabilities** spanning misconfigurations, credential reuse, and physical security gaps.



Reconnaissance

Identified **40+ subdomains** and **64+ internal IPs**

Discovered **190+ employee email addresses** susceptible to phishing

Found **breached credentials** on the Dark Web

Lateral Movement & Privilege Escalation

Used **Responder** to capture **40+ NTLM hashes**, cracking **10+**

Found **admin password reuse** across four critical systems, including the domain controller

Escalated privileges with **Pass-the-Hash** and **WmiPrivSE abuse**

Leveraged **Velociraptor (a legitimate tool)** to exfiltrate data through a blacklisted domain

Recommendations

SISA's remediation roadmap was designed in two tiers:



Immediate Priorities

Actions aimed at quickly closing critical gaps, reducing exposure across networks, credentials, and human factors to prevent potential breaches.



Future Focus

Long-term measures to build a resilient security posture, emphasizing advanced detection, stronger governance, and a culture of continuous cyber vigilance.

| Business Impact

The Red Team engagement with SISA delivered to the customer a clear picture of its security reality. On the people and physical front, the simulation elevated employee awareness, exposing how phishing and tailgating could bypass existing defenses. These insights, rarely uncovered in routine audits sparked behavioral changes and reinforced the importance of security vigilance across the workforce.

From a technology perspective, the assessment revealed misconfigurations, weak credentials, and other hidden flaws that could have led to real breaches. At the same time, it validated existing strengths such as effective patch management and biometric access, giving the organization confidence in areas where its defenses were already working well.

At the ecosystem and compliance level, the exercise shifted the organization's stance from reactive to proactive. The findings, backed by a quantified risk score of 1.187 (Vulnerable) and a prioritized remediation plan, empowered internal teams to strengthen detection and response capabilities, even against stealthy attacks leveraging legitimate tools.

Ultimately, the collaboration with SISA helped the customer transition toward a culture of proactive security ownership and laid the foundation for a stronger, more resilient cybersecurity posture.

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

