SISA

CUSTOMER SUCCESS STORY

SISA's Pentest Reveals Active Directory Exposure and Ransomware Risk for a Banking Solution Provider

ABOUT THE CUSTOMER

The customer is a leading banking and payments solutions provider specializing in omni-channel payment processing and unified merchant acquiring. With deep expertise in digital payments, transaction processing, and security, the company enables banks, financial institutions, PayFacs, ISOs, fintechs, and neo-banks to deploy scalable, industry-ready payment solutions through SaaS and PaaS delivery models. Their unified acquiring platform streamlines multi-channel payment acceptance, including UPI, payment gateway, POS, and QR-based payments, while offering seamless API integrations, connected banking capabilities, and advanced analytics for real-time business insights. Focused on secure, frictionless, and innovative payment technologies, the platform empowers organizations to accelerate growth and modernize their digital payment infrastructure.

BUSINESS CHALLENGE

During an in-depth internal penetration test covering - Domain Controllers, Active Directory forests and domains, LDAP/LDAPS interfaces, service accounts, SPNs, ACLs, file servers, and endpoints- several high-risk security gaps were uncovered that exposed the environment to potential ransomware, privilege escalation, and lateral movement.

The internal assessment revealed significant weaknesses across the customer's identity, access, and configuration landscape. Evidence of undetected ransomware activity within the Active Directory environment highlighted gaps in endpoint detection and resilience, while misconfigurations in certificate services, service accounts, and Kerberos handling exposed multiple high-privilege impersonation and credential-theft paths. Weak access controls on critical file shares further increased the risk of sensitive key leakage and lateral movement.

Together with several privilege-escalation routes mapped through AD trust relationships, the environment presented a layered set of vulnerabilities that an attacker could leverage to gain elevated access, disrupt authentication, and compromise core services.

These weaknesses carry substantial business consequences, including:

- Potential disruption of authentication and critical business services such as ERP, email, and VPN, resulting in revenue loss and operational interruption.
- Exposure of confidential data and cryptographic keys, increasing the risk of stealthy persistence or unauthorized decryption of backups.
- Heightened regulatory, legal, and reputational risk if sensitive data or essential services were impacted.
- Significant long-term remediation costs due to complex KRBTGT resets, PKI clean-up, key rotations, forensic investigations, and recovery activities needed to fully restore a secure state.

Key Security Gaps Uncovered

Ransomware Artifacts on AD-Adjacent Server

Encrypted files and a ransom note were discovered on an AD-adjacent file server, none of which were detected by the existing EDR. This strongly indicates prior or ongoing ransomware activity close to the organization's core identity infrastructure, giving attackers the opportunity to disrupt authentication flows, compromise backups, and potentially interfere with domain-wide recovery processes.

Certificate Template and CA ACL Misconfigurations

Several certificate templates and CA ACLs were configured to allow principals with unintended permissions to enroll, auto-enroll, or request certificate issuance. Such misconfigurations could enable an attacker to obtain certificates mapped to other users or services and leverage certificate-based authentication to impersonate them, bypassing password controls entirely and making malicious access far harder to detect.

MSSQL SPNs Mapped to Privileged Accounts

Multiple MSSQL service accounts were incorrectly linked to highly privileged users, allowing attackers to extract Kerberos ticket hashes and attempt Kerberoasting. If successful, this gives them powerful credentials that can unlock domain-level access. With these credentials, attackers could also enter critical databases and business systems, putting sensitive data, business operations, and revenue-generating services at risk.

World-Readable Kerberos Ticket Cache in /tmp

A valid Kerberos ticket stored in /tmp with excessively permissive access rights which allows anyone on the system to reuse it and log in as that user without a password. This enables lateral movement, increasing the scale of compromise. It also allows attackers to impersonate employees and access internal applications, file shares, and confidential data.

Weak ACLs on SMB Shares Exposing Private Keys

SMB shares contained sensitive materials, including private keys and encrypted archives that were accessible to users with insufficient privileges within the environment. Exposure of such keys can allow attackers to decrypt backups, impersonate services, and expand their lateral movement using cryptographic assets.

Cracked MSSQL SPN Service Ticket Hash Yielding Valid Credentials

A captured MSSQL service ticket hash was cracked offline, giving valid service account credentials. This foothold can quickly extend into broader access across SMB shares and internal services including business-critical systems such as databases and file servers - which could result in risks of data loss, corruption, or application outages.

Privilege Escalation Paths Identified via BloodHound

BloodHound analysis revealed multiple trust and ACL paths that could be abused to escalate privileges across the domain. These routes clearly articulate how an attacker with an initial foothold could climb to higher levels of access. Such paths significantly increase the risk of a full domain compromise in a future attack, potentially causing major business disruption and substantial remediation costs.

SISA's SOLUTION

To address the identified risks, SISA developed a structured and prioritized remediation plan across three phases - Immediate, Short Term, and Long Term - ensuring the environment was stabilized quickly, critical attack paths were removed, and a resilient identity and governance model was established for the future. Each phase focused on progressively strengthening controls, closing privilege-escalation routes, and building sustainable security governance that would protect the organization from both current and emerging threats.

01 Immediate

At this stage, the priority was to rapidly reduce operational and legal exposure by stabilizing the environment within a few hours.

To contain risk, preserve evidence, and prevent any further escalation across the environment the immediate phase focused on isolating impacted systems, neutralizing potential points of compromise, and safeguarding identity infrastructure from misuse. This included quickly cutting off escalation pathways, securing exposed credentials and revoking exposed keys/certificates, while strengthening EDR detection coverage so that any lingering threats could be identified and contained. These rapid stabilization measures created a safe operating baseline from which structured short-term and long-term remediation could be executed.

02 Short term

In the short-term phase, the focus was on eliminating identified attack paths and restoring the environment to a secure and trusted state. This involved restructuring service accounts and SPNs to remove unnecessary privileges, hardening CA/template permissions and auditing and remediating risky AD ACL configurations highlighted during assessment.

SMB share permissions were hardened, and sensitive secrets were systematically discovered, removed from open shares, and centralized in a secure vault, while endpoint configurations were strengthened to reduce the risk of credential leakage. In parallel, AD, domain controller, and certificate authority logs were forwarded to the SIEM, with targeted detection rules implemented for TGS/SPN anomalies, suspicious certificate enrolments', and ransomware patterns. Finally, multi-factor authentication was enforced for administrative and sensitive accounts, helping to ensure that identity, access, and core services operated from a much more hardened baseline.

03 Long term

Over the long term, the focus is on strengthening governance, reducing structural identity risks, and building long-term resilience across the environment. This involved enhancing the organization's identity architecture through measures such as controlled KRBTGT rotation, adoption of a tiered administrative model, and reducing standing administrative privileges. Certificate governance and lifecycle management were formalized, supported by periodic PKI audits and strict rotation of keys and certificates. Enterprise secrets management was reinforced to ensure cryptographic assets remain protected at all times. To sustain ongoing security posture, regular ACL reviews, red-team simulations, and incident response tabletop drills are recommended to be integrated into the operating model.

BUSINESS IMPACT

SISA's comprehensive, pentesting exercise transformed the client's security posture from one with hidden, high-risk identity and access weaknesses to a resilient, well-governed environment. By uncovering deep-rooted misconfigurations, undetected ransomware traces, and privilege-escalation paths, SISA enabled the client to not only remediate immediate threats but also strengthen long-term governance, visibility, and operational resilience.

Strengthened Identity & Access Security

Closed high-risk privilege-escalation paths, corrected misconfigured certificates and service accounts, and reduced standing administrative privileges.

Secured Critical Assets & Secrets

Protected cryptographic keys, sensitive data, and service credentials, reducing the risk of data theft, impersonation, or backup compromise.

Reduced Regulatory, Legal & Remediation Risk

Minimized exposure to compliance violations, reputational damage, and high-cost remediation by addressing systemic vulnerabilities early.

Improved Threat Detection & Visibility

Enhanced monitoring across AD, SPNs, certificates, and endpoints, enabling faster identification of suspicious or malicious activity.

Increased Operational Resilience

Reduced the likelihood of authentication outages, business system disruption, and ransomware impact through proactive hardening and recovery readiness.

About SISA

SISA is a global cybersecurity company focused on the digital payment ecosystem for nearly two decades. Trusted by leading payment brands and financial institutions across 40+ countries, SISA secures over 1,000 organizations through forensics-driven cybersecurity powered by real-world breach intelligence.

SISA integrates forensic investigation insights directly into prevention, leveraging deep expertise as payment security assessors, forensic investigators, and contributors to global payment security standards to convert breach learnings into predictive defense.

SISA unifies security, compliance, privacy, and intelligence into a continuous, AI-driven lifecycle spanning AI-powered compliance automation, advanced offensive security testing, agentic SOC capabilities, and outcome-focused cybersecurity training.

Through focused R&D initiatives such as Cyber Nalanda, SISA continues to advance innovation in Quantum Security, Hardware Security, AI Security, and post-quantum readiness for the global payments ecosystem. Recognized by Financial Express, DSCI-NASSCOM, and The Economic Times, SISA is shaping the future of payment security where breach intelligence powers proactive resilience.

For more information on how SISA enables the digital payment ecosystem to become cyber-resilient and future-ready, visit **www.sisainfosec.com** or contact **mediaconnect@sisainfosec.com.**

Follow us:

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

Cyber Resilience

SISA ProACT Agentic SOC

- 24x7 Monitoring
- UEBA
- Threat Intel
- Advanced Threat Hunting
- SOAR
- Use-case Factory

Digital Forensics and Incident Response

- Compromise Assessment Services
- Breach and Attack Simulation
- Advanced Threat Hunting
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensic Investigation
- Internal Forensic Investigation
- Ransomware Incident Response
- ATM Malware Analysis

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

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

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 ANAB 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

Forensic Briefing Sessions for Senior Management