

The section header "CUSTOMER SUCCESS STORY" is positioned in the lower left area of the page. It is written in a large, bold, black, sans-serif font. Below the text is a short, solid blue horizontal line. The background of this section features a dark blue world map with a network of white lines and various icons (like a house, a server, and a location pin) overlaid on it, suggesting a global technology theme.

CUSTOMER SUCCESS STORY

SISA Mitigates Active Directory Intrusion Risks for a
Global Technology Services Firm



About the Customer

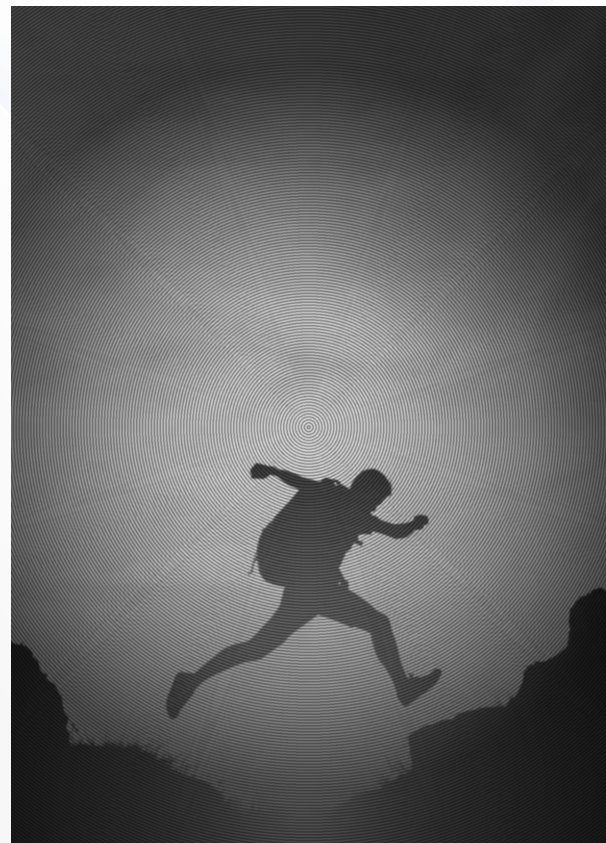
Founded in 2014 and headquartered in Dallas-Fort Worth, the client is a global digital technology services firm with over 5,000 employees. Specializing in BFSI, the company drives digital transformation through cloud, AI, cybersecurity, and customer experience solutions. Working with legacy financial institutions, the client helps modernise financial operations. Key focus areas include green banking, open banking, payments modernization, digital lending, and sustainable finance. The client is a leader in technology and analytics, collaborating with major players across banking, payments, wealth management, and insurance.

The Challenge

Understanding that their Active Directory (AD) environment represented a critical attack vector, the client required a comprehensive Active Directory security assessment to proactively identify and address vulnerabilities in their domain infrastructure before they could be exploited. Their key concerns included privilege escalation risks, credential theft, unauthorized access, lateral movement threats, and weak password policies that could compromise both their domain security and expose sensitive client data.

The primary objective was to comprehensively evaluate their Active Directory security posture against industry best practices and receive actionable recommendations to proactively mitigate identified threats and risks.

The goal was to ensure the elimination of vulnerabilities to their AD infrastructure security while maintaining adherence to industry standards and causing minimal disruptions to business operations.



Solution Offered By SISA

To address the client's concerns around privilege escalation, unauthorized access, and domain-wide exposure risks, SISA designed a methodical and minimally invasive assessment approach. The goal was to uncover hidden vulnerabilities, benchmark the Active Directory setup against industry standards, and provide a clear path from immediate remediation to long-term resilience.

SISA executed the engagement in the following phases:



Environment Scoping and Asset Identification

SISA conducted a comprehensive evaluation of the client's on-premises Active Directory environment, covering Domain Controllers (DCs), user accounts and groups, shared network resources, GPO configurations, and authentication mechanisms.



Immediate Breach Containment

To address immediate risks, SISA recommended revoking excessive permissions on high-risk accounts, rotating exposed credentials, disabling legacy authentication protocols to prevent NTLM relay attacks, enabling audit logging for all privileged actions, and enforcing stricter password reset controls.



Benchmarking Against Best Practices

The assessment benchmarked the client's AD environment against industry-recognized security standards, focusing on key areas such as authentication, access control, privilege management, and monitoring.



Strategic Enhancement Framework

SISA also recommended a strategic six-point framework for security enhancements encompassing - least privilege enforcement, robust authentication policies including MFA, hardened Active Directory configurations, advanced monitoring and real-time threat detection, comprehensive PAM, and stringent controls over password reset operations to significantly reduce risk and strengthen overall domain security.



Detection of Configuration and Policy Gaps

Several critical weaknesses were uncovered due to misconfigurations, weak credential policies, and insufficient monitoring controls, exposing the environment to significant security risks.

SISA recommendations: Improving Active Directory security

A detailed report outlining all findings, severity levels, and remediation strategies was shared to support the security of the client's Active Directory environment. The recommendations included:

01

Establish Privilege Management Framework

A comprehensive privilege management approach that combines least privilege principles with regular auditing, effectively addressing privilege issues while maintaining operational efficiency.

02

Implement Stronger Access Controls

Recognizing the need to protect critical accounts, a strategic access control approach was designed to secure password reset from unauthorized use.

03

Secure Credential Storage and Encryption

An integrated approach combining strong encryption with secure storage practices was recommended, protecting sensitive information and eliminating plaintext credential risks in shared folders.

04

Deploy Multi-Factor Authentication

Understanding current threat patterns, a comprehensive authentication strategy integrating multi-factor authentication (MFA) with stronger password policies was recommended, effectively blocking Pass-the-Hash attacks and establishing layered security controls.

05

Enhance Detection and Monitoring

To enable proactive threat detection, an advanced monitoring framework with real-time capabilities was recommended, allowing faster identification of suspicious activity and providing comprehensive visibility across the Active Directory environment.

Key security weaknesses identified

The Active Directory Security Assessment revealed multiple misconfigurations and security weaknesses, that included:

Weak Active Directory permissions

with excessive user privileges and non-expiring passwords, increasing the risk of unauthorized access and credential compromise.

Credential exposure

through SMB shares, with unauthorized access to shared folders containing sensitive information, including plaintext passwords and a SQL SuperAdmin credential.

Weak password policies

and successful Pass-the-Hash attacks enabled lateral movement and unauthorized access to critical servers.

Misconfigured access controls

allowed unauthorized users to reset privileged account passwords and escalate privileges.

Absence of Privileged Access Management,

including lack of MFA and active stale admin accounts, increased the environment's attack surface.

| Business Impact

By enhancing their Active Directory (AD) security posture, the client significantly reduced the risk of unauthorized access thereby safeguarding critical business data, client information, and core infrastructure consequently reducing the business to exposure from financial, reputational, and regulatory consequences. Strengthening security controls not only minimized the likelihood of security breaches but also ensured operational continuity by preventing potential disruptions caused by unauthorized access.

Additionally, by proactively mitigating identified risks and vulnerabilities, the client fortified their resilience against cyber threats, reinforcing trust among stakeholders, customers, and regulatory bodies. This exercise also positioned the organization to meet compliance requirements more effectively.



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

