SISA

CUSTOMER SUCCESS STORY

How SISA's Multi-Layered Penetration Test Strengthened Active Directory Security for a Major Enterprise Software Company

About the Customer

The Client is a software company focused on digital adoption, process automation and enterprise learning solutions. Their products help organizations document business processes, train users on enterprise applications and improve end-user productivity during digital transformation. Headquartered in Bangalore, India with operations across USA, Middle East, Europe and APAC, the company works with large and mid-size enterprises and has a strong customer base in sectors like IT, BFSI, manufacturing, telecom, healthcare and government.

With an established presence in the Digital Adoption Platforms and Process Knowledge Management space, it is focused on enhancing user onboarding through use of automation and AI, increasing workforce productivity through guided learning and process compliance, and improving system adoption during large-scale IT rollouts (ERP, CRM, Core Banking etc.)

BUSINESS CHALLENGE

During the Internal Penetration Testing activity that SISA performed on the Client's Active Directory environment, several misconfigurations and excessive permission settings were identified that allowed the tester to escalate privileges and gain full control over the domain environment. Using valid domain credentials, the tester enumerated Active Directory through Lightweight Directory Access Protocol (LDAP) and leveraged weak access controls to execute replication and privilege escalation attacks.

These weaknesses could enable a malicious actor to gain unrestricted control over the organization's Active Directory, allowing the attacker to access confidential data, impersonate any user (including administrators), and maintain persistent, covert access even after password resets. Such a compromise could lead to complete business service disruption, data theft, regulatory non-compliance, and reputational damage if exploited by an adversary.

SISA's SOLUTION

To assess the resilience of the Client's internal environment, SISA executed a structured, **multi-layered penetration testing** methodology grounded in real-world adversarial behaviour, leading to the discovery of systemic weaknesses that enabled full domain compromise.

SISA's Structured Penetration Testing Methodology Contextualized to the Case Environment

Credential Validation

SISA verified that the supplied username and password belonged to a valid domain account, establishing an initial foothold consistent with what an insider or low-privileged attacker might possess.

Directory Enumeration

Using LDAP enumeration tools, SISA collected detailed information on usernames, Service Principal Names (SPNs), AD objects, and configuration attributes.

Kerberos Pre-Auth & Roastability Checks

The team examined whether any accounts had Kerberos pre-authentication disabled - conditions that would make them vulnerable to **AS-REP roasting**. No such accounts were present, ruling out this path.

SPN Enumeration & Kerberoast Target Discovery

An enumeration of SPNs revealed a MySQL-related service mapped to a user-administered account with elevated privileges, indicative of a potential **Kerberoasting target** and a sign of improper service account hygiene.

Privilege and Relationship Analysis Using BloodHound

All collected data was imported into BloodHound to visually map AD relationships, group memberships, Access Control Lists (ACLs), and hidden escalation paths.

Abuse of Rights & DCSync Replication Attack

Using the over-permissive ACL rights, SISA executed a **DCSync-style replication** attack. This allowed unauthorized extraction of password hashes for domain accounts, including administrative ones.

Post-Exploitation Persistence

With Domain Admin–level hashes in hand, SISA forged a Golden Ticket, granting persistent, stealthy access across the environment. This established a long-term foothold that could survive password resets and normal security controls.

Key Security Gaps Uncovered

SISA's penetration testing approach uncovered several critical weaknesses that, when chained together, created a clear and exploitable path to full domain compromise. The most impactful findings were:

Excessive AD permissions enabling replication abuse, increasing the risk of DCSync attack, by exposing all user hashes and opening the door to complete domain compromise.

Domain Credential obtained but offline crack attempts unsuccessful, presenting risks of pass-the-hash and ticket forgery attacks.

Service Principal Name mapped to a user-administered MySQL account, creating unnecessary exposure to Kerberoasting attacks.

Successful Golden Ticket creation & Domain Admin persistence, offering the attacker long-term access that persists beyond password changes.

The penetration test allowed SISA to achieve full domain compromise, perform lateral movement across all interconnected systems and maintain continuous persistence even after password resets, thereby resulting in critical impact.

Remediation Measures

To restore security and prevent recurrence of the attack paths identified, SISA executed a focused, prioritized remediation plan combining immediate containment steps, structural AD hardening, and long-term governance improvements.

01 Immediate Containment & Access Reset

SISA directed the Client to disable compromised accounts, end active sessions, and isolate affected Domain Controllers to contain misuse of elevated privileges. Passwords for all privileged, service, and high-value accounts were rotated, followed by a two-step KRBTGT key reset to invalidate forged Kerberos tickets, effectively eliminating any Golden Ticket persistence that may have been created during the compromise.

02 Hardening Service Accounts & Privilege Structures

As part of structural hardening, SISA advised the Client to replace user-managed service accounts with Group Managed Service Accounts (gMSAs), removing static credentials from the environment. The team also eliminated GenericAll-level permissions and other excessive ACL configurations and revoked unauthorized replication rights that had previously enabled a DCSync attack. In parallel, SISA helped the Client transition to a tiered administrative model supported by Privileged Access Management (PAM), ensuring that privileged pathways were segmented and governed more tightly.

03 Strengthening Active Directory Monitoring & Detection

SISA recommended to implement enhanced monitoring across Active Directory to improve visibility of high-risk activities. Directory Replication Services (including DRS calls and DS-Replication RPCs) were placed under active surveillance, while Kerberos operations were monitored for anomalies such as unexpected ticket issuance or unusually long-lived tickets. AD ACL changes, privileged group membership modifications, SPN updates, and new service account creations were all brought under continuous audit to ensure early detection of suspicious behaviour.

04 Enhancing Authentication Security

To mitigate credential misuse and pass-the-hash style attacks, SISA recommended to enable Multi-Factor Authentication for all administrative and privileged accounts. This added a critical layer of identity security, significantly reducing the likelihood of unauthorized access even in the event of credential compromise.

05 Post-Remediation Validation

After completing all remediation steps, SISA conducted comprehensive validation testing to ensure the misconfigurations were fully resolved and that no persistence mechanisms remained active within the environment. This confirmed that the Client's environment had returned to a secure baseline and that the organization's AD posture was resilient against similar attack vectors moving forward.

BUSINESS IMPACT

SISA's internal penetration testing and remediation support uncovered and eliminated security gaps that could have enabled a real attacker to gain and maintain complete domain control. By addressing these issues proactively, the Client strengthened both immediate defence mechanisms and long-term identity security.

Significantly Reduced Business Risk

The assessment gave the Client clear visibility into AD weaknesses. By remediating these gaps early, the Client substantially lowered the likelihood of credential theft, domain compromise, and widespread system impact.

Strengthened Security of Critical Services

Hardening Active Directory directly improved the security of essential business functions including user authentication, applications, email systems, finance operations, and internal workflows.

Prevention of Financial and Reputational Damage

By closing the misconfigurations that could have led to fraud, data breaches, regulatory findings, or customer-impacting incidents, the Client reduced the risk of exposure to penalties, financial loss, and reputational damage.

Improved Operational Continuity

With Golden Ticket persistence removed, unauthorized replication rights revoked, and excessive privileges eliminated, the risk of attackers disabling systems, corrupting configurations, or taking servers offline was drastically reduced.

Enhanced Governance, Audit Readiness & Trust in Controls

Eliminating privilege escalation paths, securing authentication mechanisms, and enforcing PAM and MFA strengthened identity governance, helping reinforce trust in internal controls.

About SISA

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry. As a Global Payment Forensic Investigator of the PCI Security Standards Council, we leverage forensics insights into preventive, detective, and corrective security solutions, protecting 1,000+ organizations across 40+ countries from evolving cyberthreats. Our suite of solutions from AI-driven compliance, advanced security testing, agentic detection/ response and learner focused-training has been honored with prestigious awards, including from Financial Express, DSCI-NASSCOM and The Economic Times. With commitment to innovation, and pioneering advancements in Quantum Security, Hardware Security, and Cybersecurity for AI, SISA is shaping the future of cybersecurity through cutting-edge forensics research.

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
- PCI Forensic Investigation (PCI)
- Internal Forensic Investigation (IFI)
- 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 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

Leading Tech Security

PRISM
- 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

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia

To learn more about SISA's offerings visit us at **www.sisainfosec.com** or
Contact your SISA sales representative at **contact@sisainfosec.com**