SISA

Customer Success Story

How SISA Helped a Global Hospitality Platform Provider Safeguard Source Code Integrity Through Repository Exposure Hardening

About The Customer

The customer is a provider of cloud-based hospitality technology platform that automates the distribution of hotel inventory across online travel agencies (OTAs), Global Distribution Systems (GDS), hotel websites, and other booking channels. Headquartered in New Zealand with operations spanning multiple regions including Asia-Pacific, Middle East, Europe and Africa, the company serves hotels in 90+ countries and supports more than 20,000 hospitality properties worldwide.

Business Challenge

As the platform scaled across financial services and e-commerce use cases, its web application became central to customer engagement and transaction processing. The organization followed a fast-moving DevOps model, with frequent feature releases and continuous updates to support business growth.

However, this rapid delivery cycle also increased the risk of security gaps being introduced into production. With a growing user base, sensitive transaction flows, and expanding third-party payment integrations, the customer needed independent assurance that its application and deployment practices were secure, resilient, and not exposing the business to avoidable vulnerabilities.

The key challenge was to maintain speed of innovation without compromising application security, payment integration security, or customer trust.

SISA's Solution

SISA conducted a focused web application security assessment to evaluate whether the customer's rapid deployment practices were exposing sensitive application assets, source code, or production credentials. The assessment followed a phased approach to identify, validate, and help remediate critical security risks across the application and DevOps environment.

Phase 1

Application Discovery and Scoping

SISA began by mapping the customer's publicly accessible web application environment to understand its exposed paths, deployment structure, and potential entry points. This helped establish the assessment scope and identify areas where misconfigured directories, hidden files, or development artifacts may have been unintentionally exposed in production.

Phase 2

Threat Modeling and Attack Surface Mapping

The team then assessed the application from an attacker's perspective, focusing on risks that could arise from DevOps misconfigurations, exposed repositories, hard-coded credentials, and third-party integration dependencies. Given the customer's reliance on frequent releases and payment integrations, SISA prioritized risks that could lead to source code exposure, credential compromise, and unauthorized access to backend systems.

Phase 3

Security Testing and Exploitation

As part of the assessment, SISA performed directory fuzzing on the customer's web application using fuzzing ffuf tool with the SecLists combined_words.txt wordlist. The scan revealed that hidden Git paths, including /.git/index and /.git/config were publicly accessible. These files should never be exposed on a production server.

Using a Git dumping tool, SISA was able to download the full repository locally, confirming that the application's complete source code was publicly exposed and readable. The team then scanned the codebase using TruffleHog tool and identified multiple hard-coded secrets, including database credentials and API tokens.

Phase 4

Validation and Impact Analysis

SISA further inspected encoded Git objects using “git cat-file –p" and confirmed that sensitive credentials were permanently present in the repository’s commit history. This validated a critical attack path: an anonymous internet user could access the exposed Git directory, retrieve the full source code, extract embedded secrets, and potentially compromise production systems or connected services.

The assessment demonstrated that the issue was not just limited to source code exposure, but extended to credential leakage and long-term secret persistence within Git history.

Phase 5

Reporting and Remediation Guidance

SISA provided detailed findings, evidence and prioritized remediation steps to help the customer close the exposure and strengthen its DevOps security practices.

Key recommendations included:

01
Blocking all requests to hidden directories, especially /.git/, through strict server-side access controls at the web server level.

02
Rotating all exposed credentials and invalidating any secrets found in the repository.

03
Sanitizing the exposed repository using history-rewriting tools to remove hard-coded secrets from the Git object tree.

04
Deploying a secrets management vault to replace static credentials with dynamic, short-lived secrets.

05
Integrating automated secret scanning tools such as TruffleHog or Gitleaks into the CI/CD pipeline as blocking gates.

06
Implementing pre-commit hooks to prevent developers from committing secrets into repositories.

07
Running scheduled directory fuzzing and exposure checks to detect misconfigurations before they reach production.

Business Impact

The assessment gave the customer clear visibility into a critical exposure that could have allowed an anonymous internet user to download proprietary source code, extract live credentials, and compromise production databases and APIs, potentially leading to financial theft, data breaches, regulatory fines under PCI DSS and GDPR. By validating the full attack path, SISA helped the customer understand the real business risk beyond a standard vulnerability finding.

Key benefits included:

Reduced application-layer breach risk

By identifying the exposed Git repository and embedded credentials, SISA helped eliminate a high-risk path to source code leakage, credential compromise, and unauthorized access.

Stronger security without slowing DevOps

The recommendations were aligned to the customer's DevOps model, that allowed embedding controls such as CI/CD secret scanning, pre-commit hooks, and scheduled fuzzing into existing workflows, without disrupting rapid feature delivery.

Clear visibility into exploitable risk

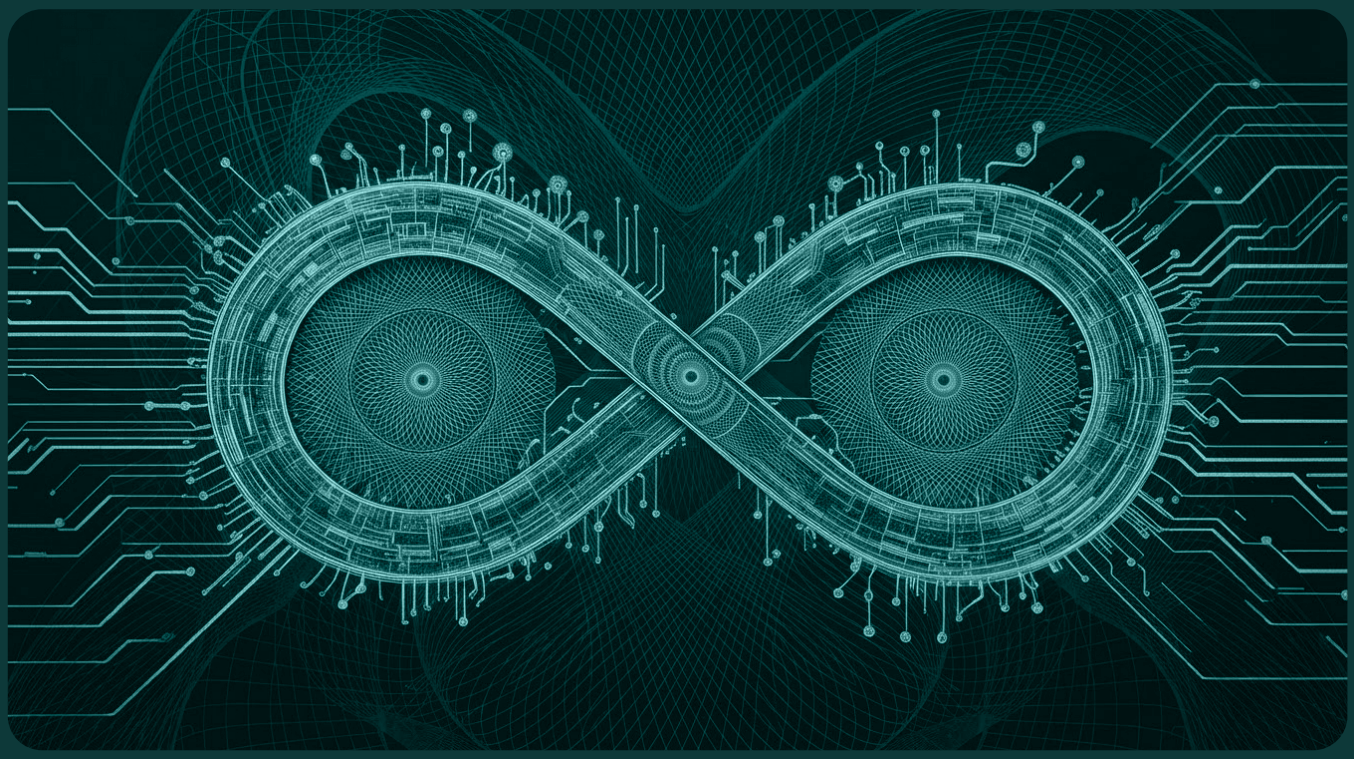
SISA validated the full attack path, showing how a misconfigured production server could lead to repository download, secret exposure, and wider system compromise.

Faster remediation cycles

Evidence-backed findings and prioritized guidance enabled quick action across credential rotation, repository sanitization, access control hardening, and secrets management.

Conclusion

Through this phased security assessment, SISA helped the customer move beyond vulnerability identification to root-cause validation and practical remediation. As a result, the customer strengthened its application security posture, improved DevOps governance, and gained greater confidence that future releases could be delivered securely at speed.



About SISA

SISA is a global leader in cybersecurity for the payment ecosystem, operating at the intersection of AI, cybersecurity, and payments. Trusted by leading brands and financial institutions across 40+ countries, SISA secures over 1,000 organizations by helping them anticipate threats, strengthen resilience, and protect critical payment infrastructure. Powered by real-world breach intelligence, SISA enables organizations to stay ahead of evolving cyber risks. Follow SISA on LinkedIn for the latest insights on cybersecurity, payment security innovation, and emerging technologies.

SISA's Portfolio of Forensics-driven Cybersecurity Solutions

SISA ONE

Unified Platform for Compliance, Security and Privacy

Radar
Data Protection & Governance
- Radar Discovery
- Radar Classification

Pulse
Continuous Compliance
- Pulse Continuous Monitoring
- Pulse Evidence Automation

ProACT
- ProACT Agentic SOC

PRISM
AI Security and Governance
- PRISM AI Runtime Security & Observability
- PRISM AI Attack Surface Visibility
- PRISM In-Model LLM Hardening
- PRISM AI Adversarial Testing
- PRISM ML Artifact & Supply-Chain Integrity
- PRISM Govern AI GRC Automation

SISA SERVICES

Expert-led Services

Compliance
- PCI DSS Compliance
- PCI PIN
- PCI 3D Secure (3DS)
- PCI P2PE Compliance
- PCI S3
- PCI S-SLC
- PCI CP
- PCI SAQ
- SWIFT
- Quantum
- MPoC

DFIR/Sappers
- Payment Forensics Investigation
- Internal Forensic Investigation
- Acquirer-led Investigation
- Breach and Attack Simulation
- Compromise Assessment
- Cloud Forensics
- DFIR Retainer Services
- Forensic Resilience Assurance

Offensive Security/Warlabs
- Application Security Testing
- Infrastructure & Network Security
- Cloud & Container Security
- IoT Security Testing
- Adversary-Led Ransomware Simulation
- Red Teaming
- Hardware Security

Data Protection
- HIPAA
- ISO Management System
- NIST
- SOC Compliance
- HITRUST Certification
- Information Security Risk Assessment
- CSA STAR
- Crisis Management Exercise
- Indian Regulatory Cybersecurity Audit
- DPDPA Consulting

SISA INSTITUTE

Education, Certification & Capability Building

Payment Data Security Programs
- CPISI
- CPISI - Hybrid
- CPISI - Advanced
- CPISI - D

Quantum Security
- CQSP

AI Security
- CSPAI

Certified Payment Privacy Professional (CP3)

SISA is a global cybersecurity leader for the payments ecosystem

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

www.sisa.ai | contact@sisa.ai