SISA


# CUSTOMER SUCCESS STORY

SISA Helps A Leading Conversational AI Company Achieve Centralized Logging and Scalable Security Operations with Seamless Integration

# ABOUT THE CUSTOMER

The client is a US-based company that offers AI deployment services for enterprises. Its enterprise-grade AI platform is built to help large organisations deploy AI agents, automate workflows, and integrate data across systems. Its AI and data platform helps automate customer support, HR processes, and supply chain workflows. Working with more than 2,000 businesses worldwide, including several Fortune 500 companies, the platform helps enterprises improve productivity and scalability, while reducing manual effort.

# BUSINESS CHALLENGE

The company needed to strengthen its security and compliance posture while ensuring operational resilience across its rapidly expanding technology ecosystem. The organization sought a centralized logging and monitoring solution capable of ingesting, parsing, and analyzing logs from a diverse mix of SaaS applications, cloud environments, and on-premises platforms. The leadership recognized that without a unified approach to log management, the organization risked blind spots in threat detection, inefficiencies in operations, and potential lapses in regulatory compliance.

**The mandate for a centralized logging and monitoring solution was anchored around four strategic goals:**

### Visibility

Ensuring continuous, real-time monitoring across heterogeneous platforms without blind spots.

### Compliance

Maintaining adherence to stringent audit and regulatory frameworks such as PCI DSS and ISO.

### Scalability

Designing an architecture resilient enough to handle surging data volumes and expanding integrations.

### Standardization

Establishing robust SOPs for consistent and efficient onboarding of future log sources.

The company's IT landscape however was far from simple. The solution had to operate across multiple cloud providers, SaaS platforms, and regional deployments, each with its own data formats, access controls, and rate limitations. Ensuring consistency and performance at scale demanded a design that could navigate both volumetric challenges and integration constraints.

### Integration in Practice: Two Critical Use Cases

**Microsoft Services** (Azure AD Entra, Microsoft Defender)

01

- **Integration Type**
  API integration via Microsoft Graph
- **Challenge**
  The reliance on token-based authentication added significant complexity in managing secure access. Moreover, Microsoft's API rate limiting constrained log retrieval, creating risks of incomplete ingestion and delayed visibility.

**AWS CloudTrail (High-Volume Processing)**

02

- **Scope**
  Logs from 28 AWS accounts across 17 regions, generating 476 unique S3 prefixes
- **Integration Type**
  CloudTrail integration using AWS S3 plugins
- **Challenge**
  API rate limits meant that each node could only process 15–20 prefixes simultaneously, leading to processing bottlenecks and slowing down analysis of critical events.


# SISA's SOLUTION

SISA approached the company's challenge as a strategic transformation of the logging and monitoring function. The engagement was structured into five consultative phases, each designed to balance technical rigor with long-term scalability and compliance readiness.

## 01 Discovery and Planning - Setting the Foundation

The engagement began with a comprehensive assessment of the company's log ecosystem. SISA analyzed log formats, data volumes, and growth trends, while prioritizing critical systems based on risk exposure and regulatory obligations. This diagnostic phase ensured that every downstream activity was aligned to business priorities rather than purely technical convenience.

## 02 Standardizing Onboarding SOPs - Bringing Order to Complexity

To overcome the challenge of heterogeneity, SISA created tailored Standard Operating Procedures (SOPs) for each log source, spanning Azure AD, Microsoft Defender, Signal Sciences, DLP, Nile Secure, Teleport, CrowdStrike, GitHub, and others. Pre-validation mechanisms (via Postman/API Explorer) were embedded into the process to test endpoints before ingestion, reducing downstream failures and enabling faster time-to-value.

## 03 Adaptive Infrastructure Planning - Designing for Scale

Recognizing the volumetric complexity of sources like AWS CloudTrail, RDS, and MongoDB, SISA assessed ingestion volumes per source and provisioned infrastructure accordingly. Parser logic with fallback rules was applied to high-volume streams, ensuring continuity of log ingestion without service disruption. Hardware provisioning was future-proofed to account for data growth patterns, rather than point-in-time estimates.

## 04 Collaborative Troubleshooting – Partnering Beyond Technology

SISA engaged directly with the company's engineers and third-party vendors (e.g., GitHub, Teleport) to resolve integration bottlenecks. By proposing viable workarounds in cases of plugin or version mismatches, and implementing secure transfer protocols such as client-signed certificates for Syslog, the approach emphasized collaboration and risk reduction over one-sided fixes.

## 05 Documentation & Handover – Institutionalizing Knowledge

Beyond solving today's problem, SISA ensured future readiness. Detailed documentation was created for each source integration, along with reusable SOPs for new sources such as Nile Secure and Signal Sciences. Exception lists and action plans were developed for "On-Hold" or "Not-Priority" sources, ensuring that the client had a clear roadmap for incremental adoption.

## Key Deliverables

### Custom API Agent
Built in-house to overcome integration hurdles, speed up onboarding, and improve interoperability.

### Standardized SOPs & Integration Maps
Streamlined onboarding with faster deployment and consistent processes.


### Scalable Forwarder Architecture
Designed for future log sources, reducing complexity and ensuring high efficiency.

### Collaborative Troubleshooting
Enabled swift issue resolution through close coordination with client teams and vendors.

# BUSINESS IMPACT

### Operational Transformation
SISA streamlined the company's fragmented logging and monitoring into a unified, future-ready operating model.

### Collaboration & Trust
Challenges like plugin mismatches and secure transfers were resolved swiftly, strengthening alignment across internal teams and vendors.

### Efficiency & Focus
Automated ingestion and optimized infrastructure cut down manual effort, enabling security teams to shift from firefighting to strategic initiatives.

### Compliance Strengthening
Standardized integrations ensured adherence to PCI DSS, ISO, and other frameworks, minimizing regulatory risk and reinforcing customer trust.

### Scalable & Resilient Architecture
With forwarder scaling, auto-scaling logic, and reusable SOPs, the company can now handle rapid log growth and onboard new sources consistently, ensuring resilience and faster time-to-value.

In sum, SISA enabled the company to move beyond tactical fixes and establish a resilient, compliant, and scalable log management capability. The result was not just improved visibility today, but a sustainable foundation that positions this leading conversational AI company for secure, compliant, and efficient growth in the future.

# 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**