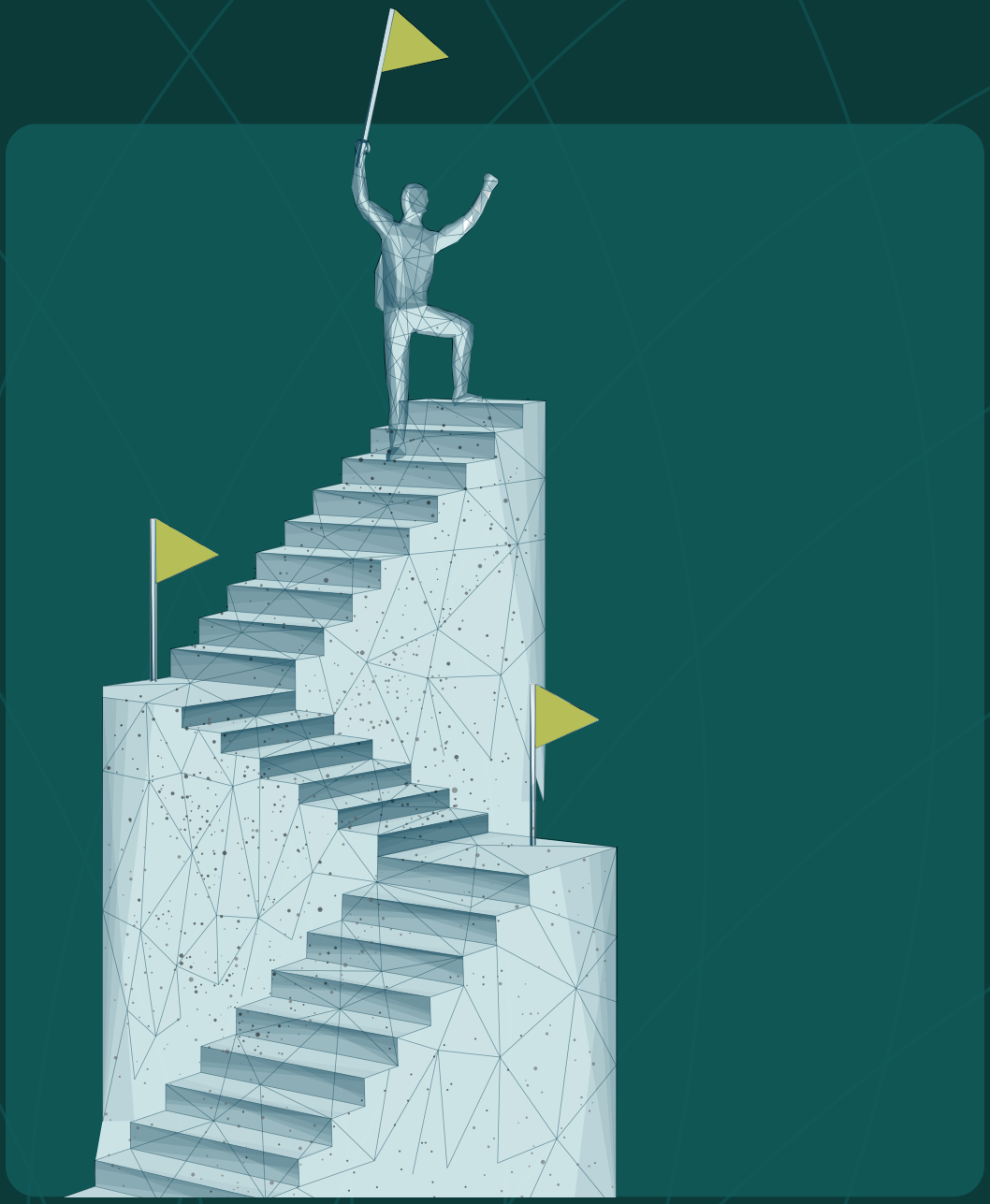
SISA



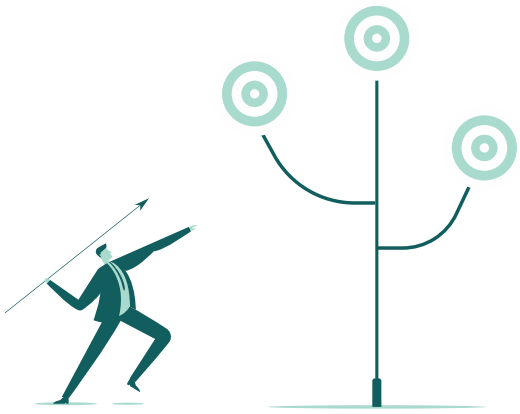
Customer Success Story

SISA Agentic SOC's Geo-Redundant Disaster Recovery Setup Helps Al Ansari Secure Business Uptime and Build Cyber Resilience.

About The Customer

Al Ansari Exchange is one of the UAE's most established financial services providers, with a legacy spanning nearly six decades. As the leading provider of outward remittance and foreign exchange services, they enable seamless and secure global movement of money. Their wide range of financial services also includes prepaid cards, corporate payment solutions, bill payments and value-added services such as insurance, investments and saving schemes. Given the scale and sensitivity of transactions, ensuring security, uptime, and resilience is critical for the team to consistently sustain customer trust across the payment ecosystem.

Business Challenge



Large payment-focused organizations like Al Ansari Exchange operate in an environment where uptime, data integrity, and transaction continuity are non-negotiable. Against this backdrop, the organization faced a dual challenge. First, the need to establish a robust and fail-safe Disaster Recovery (DR) architecture that could ensure seamless business continuity, minimize downtime, and enable controlled, predictable cutover during both planned and unplanned events.

Second, there was a growing need for centralized visibility across their IT and security landscape. Disparate systems and fragmented logging limited their ability to monitor events holistically, respond to incidents in real time, and meet increasingly stringent regulatory and audit expectations. The organization required a unified logging and monitoring framework capable of ingesting, correlating, and retaining up to 12 months of log data, while enabling efficient search, analysis, and reporting.

SISA's Solution

Team SISA implemented an integrated security operations and resilience framework that combined **centralized monitoring** with a high-availability **Disaster Recovery (DR) architecture**, enabling the organization to strengthen both cyber defense and business continuity.

At the core of the deployment was a centralized logging and monitoring solution that **unified visibility** across the organization's IT and security landscape. Logs from critical infrastructure, applications, network devices, and security controls were consolidated to support **real-time monitoring**, faster threat detection, and efficient incident investigation. The solution was engineered to retain and efficiently search up to **12 months of log data**, helping the organization meet regulatory, compliance, and audit obligations while improving forensic readiness. The monitoring environment was further enhanced with selective Agentic AI and Generative AI capabilities within SISA's ProACT Agentic SOC platform.

Key Tenets of SISA's Solution

- Centralized logging with up to **12 months of data retention**
- **Real-time monitoring**
- **DR hot site** with RPO of <15 minutes
- **Data redundancy** mechanisms for log back-up
- **Agentic AI** for threat detection and forensic analysis

A key focus of the engagement, however, was the design and implementation of a robust DR architecture to ensure uninterrupted operations under adverse conditions. SISA established a geographically separated DR site from the primary environment, significantly reducing the risk of simultaneous impact from natural disasters, regional outages, or site-level disruptions.

The DR environment was configured as a **hot site**, enabling **seamless switchover** of operations whenever required. With continuous synchronization and replication of critical data, the architecture was designed to support a Recovery Point Objective (RPO) of **less than 15 minutes**, ensuring minimal data exposure in the event of failover.

To further strengthen resilience, **data redundancy** mechanisms were built into the setup. Logs ingested at the primary site were simultaneously backed up to the DR environment, ensuring continuity of historical records, preserving visibility during failover, and eliminating the risk of log loss during incidents.

This architecture enabled a controlled and **disruption-free cutover** process for both planned maintenance and unexpected outages. Security monitoring and operational functions could continue without interruption from the DR site, with secure restoration to the primary environment once stabilized.

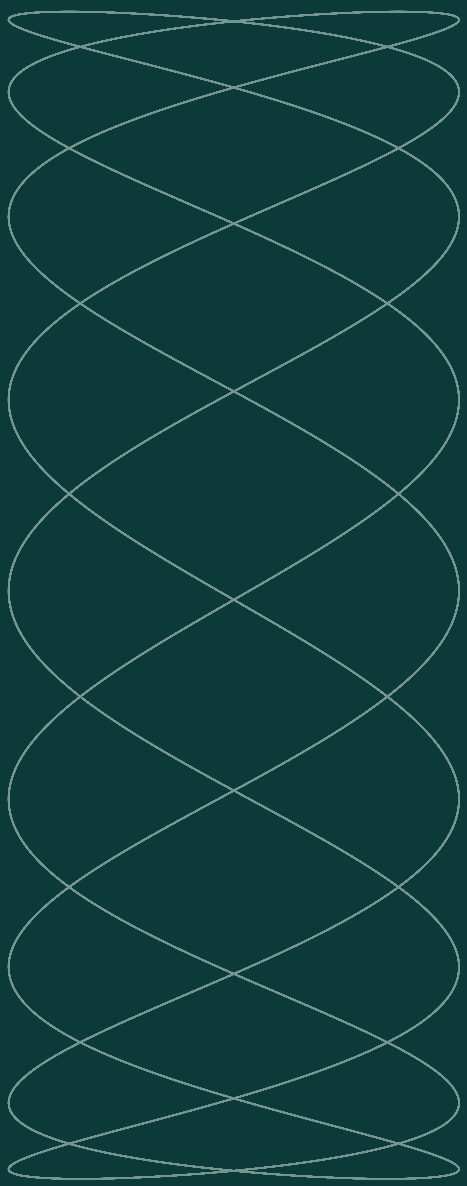
Customer Speak

Al Ansari Financial Services leveraged SISA's ProACT Agentic SOC to enhance its security operations with greater speed, intelligence, and consistency. The platform's agentic AI–driven threat investigation capabilities strengthened our cyber defenses, enabling proactive identification and response to risks across our environment. The inclusion of an isolated DR setup also greatly improves operational resilience during times of global uncertainty. Based on the value delivered, we have also extended this service to our subsidiary company BFC - Bahrain. SISA ProACT's combination of advanced threat intelligence, expert-led oversight, and exceptional support has significantly strengthened our security posture and increased our confidence in maintaining 24×7 cyber resilience.

Shiva Shankar G,
Information Security Manager,
Al Ansari Financial Service L.L.C

Business Impact

SISA's implementation of a robust Disaster Recovery architecture, combined with a well-defined cutover strategy and centralized monitoring, enabled the organization to realize tangible improvements across resilience, risk management, and operational assurance by transitioning from reactive recovery to a state of continuous operational readiness.



Uninterrupted Operations and Monitoring

Ensured continuous security monitoring and IT operations during outages or incidents, eliminating visibility gaps and maintaining control at all times.

Reduced Downtime and Business Risk

Minimized service disruptions through seamless failover, protecting critical payment systems from operational and financial impact.

Data Integrity and Loss Prevention

Enabled continuous data synchronization and secure backups, ensuring zero data loss during failover or recovery scenarios.

Stronger Cyber Resilience

Established a resilient architecture with reliable failover capabilities, enhancing the organization's ability to withstand and recover from disruptions.

Improved Compliance and Audit Readiness

Strengthened regulatory alignment with centralized logging, assured data availability, and long-term retention for audit and reporting needs.

Sustained Customer Trust and Brand Stability

Maintained consistent service delivery, reinforcing customer confidence and protecting brand reputation in a high-stakes payments environment.

Enhanced Leadership Assurance

Provided management with confidence through 24×7 security visibility and operational readiness, ensuring business continuity is always under control.

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

Compliance

Payment Security

- PCI DSS Compliance
- PCI PIN
- PCI 3D Secure (3DS)
- PCI P2PE Compliance
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- PCI SAQ Compliance
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance

Strategy & Risk

- SWIFT
- HIPAA
- ISO Management System Services
- NIST
- SOC Compliance
- HITRUST Certification
- Information Security Risk Assessment
- CSA STAR Assessment & Certification
- Crisis Management Exercise / Crisis Management & Incident Response Simulation Exercises
- Indian Regulatory Cybersecurity Audit & Assurance Services

Unified Audits

Managed Compliance

Security

Security Testing

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

ProACT Agentic SOC

Digital Forensics & IR (DFIR)

- Payment Forensics Investigation
- Internal Forensic Investigation
- Acquirer Led Investigation
- Ransomware Incident Response
- Breach and Attack Simulation
- Compromise Assessment
- Cloud Forensics
- Retainer Services
- Digital Threat Report Briefing Session

PRISM

- Prism Discovery (AIBOM)
- Prism Strike (Gen AI app PT)
- Prism Secure (Model Security)
- Prism Observe (Live AI App monitoring)

Quantum Security

Privacy

Data Protection and Governance

- SISA Radar (Discovery & Classification)

Data Privacy Consulting Services

- DPDPA (India) Compliance Consulting
- GDPR
- CCPA

SISA is a global cybersecurity leader for the payments ecosystem

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

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