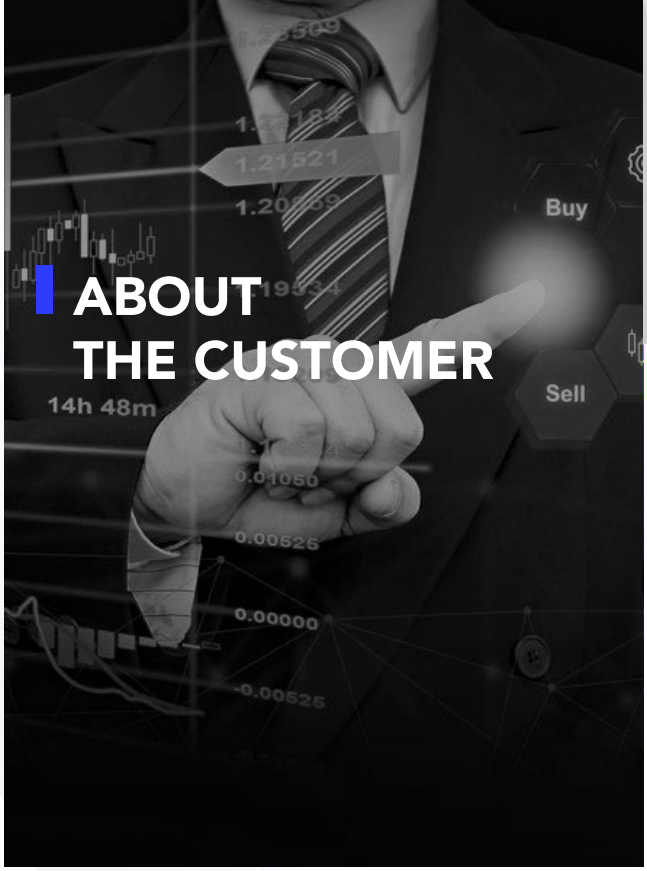
SISA

CUSTOMER SUCCESS STORY

SISA's forensics-driven MXDR Solution helps a bank in Africa defend from Ransomware Attacks

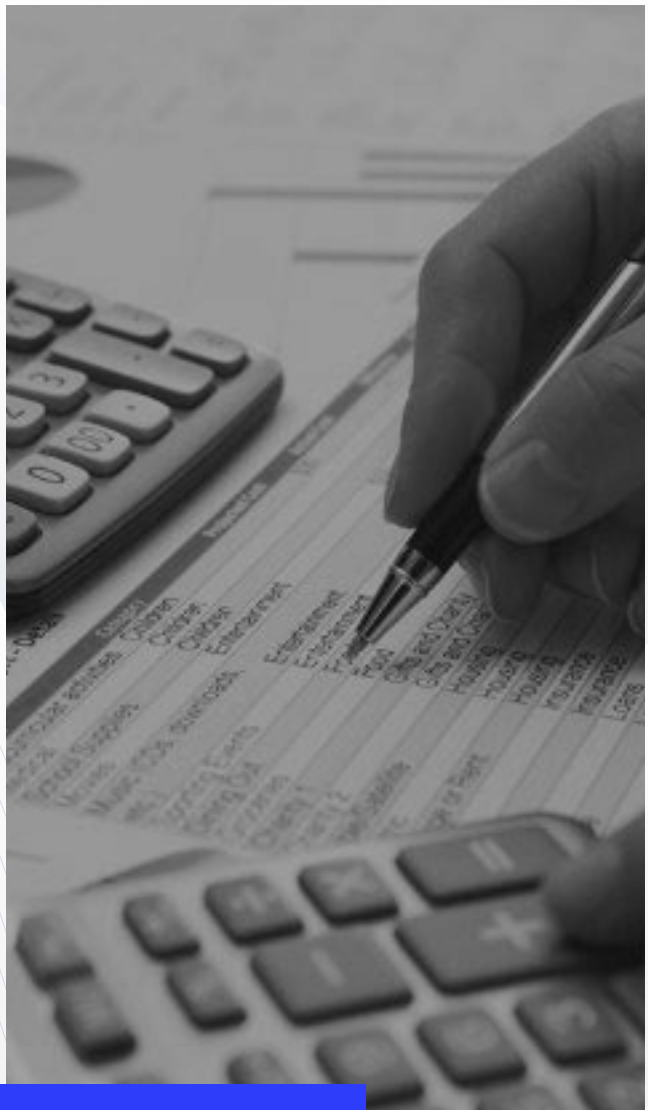


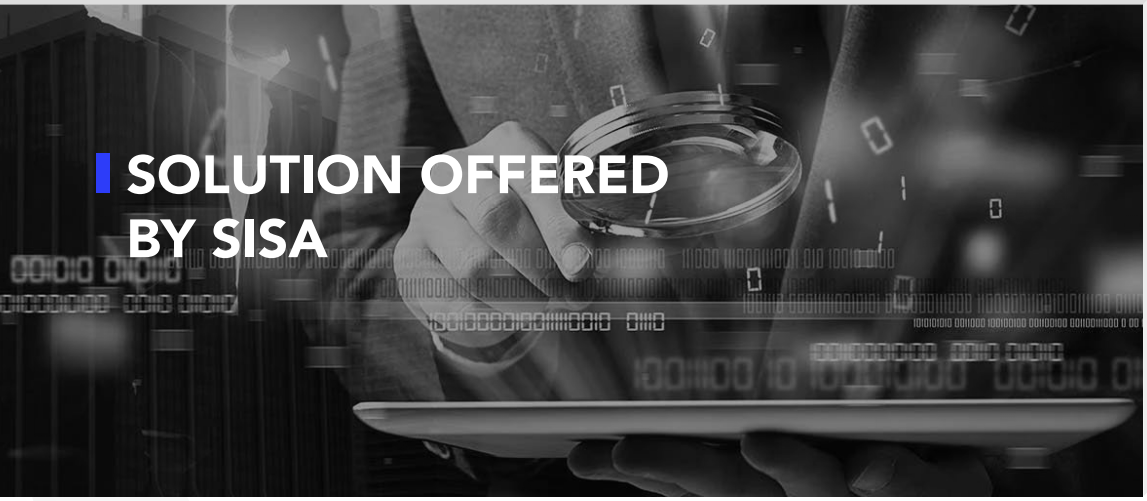
ABOUT THE CUSTOMER

The client is a full-service commercial bank based out of Africa. Through its three main business divisions: Retail, Wholesale, and Treasury, it provides a suite of financial services and products to retail customers, farmers, SMEs, Corporates, Institutions and the Government. Serving over 4 million customers, it has been a recipient of several awards and accolades for excellence in banking, treasury and finance.

THE CHALLENGE

The bank noticed some malicious activity in dormant accounts and found high cash withdrawals associated with these accounts in multiple locations in a short span of time. It then reached out to SISA. SISA's internal forensics investigation confirmed that the bank was hit by a security breach following which its business operations were impacted significantly. The bank, at the time of breach, did not have an threat monitoring solution to detect internal and external threats. Additionally, it was facing challenges in scoping cardholder data to meet the regulatory requirements. With critical systems being affected, the immediate need was to streamline sensitive data discovery, create awareness about forensic investigation and deploy a threat monitoring solution.





SOLUTION OFFERED BY SISA

The customer chose SISA for 24/7 SOC Monitoring through implementation of SISA ProACT MXDR platform. The implementation included of 250+ use cases through SISA's USECASE Factory derived from SISA's unique forensics-driven approach for improved threat detection. The various services provided by the SISA MXDR team are as follows:

- Advanced Threat Hunting
- Breach and Attack Simulation (BAS)
- AI/ML-based UEBA
- Customized Threat Advisories
- Use Case Factory
- Quarterly CXO Reports
- Support for Audits

BUSINESS BENEFITS

SISA's MXDR platform enabled the client to monitor over 500 critical assets 24/7 and significantly improve threat detection. Since implementing our MXDR solution, the **Mean Time To Detect (MTTD)** has been reduced to less than **30 minutes**. SISA's threat hunting team frequently conducts hypothesis-based and IOC-based manual threat hunting, as well as breach and attack simulation exercises, to identify detection gaps and proactively create use cases to continuously enhance threat detection. Our flagship Use Case Factory team has been instrumental in creating custom use cases for the bank, ensuring we stay ahead of emerging threats.

In addition to improving threat detection, the MXDR team collaborates closely with the client to enhance their overall security posture through SISA's MXDR flagship Security Posture Assessment and Defense in Depth Assessment programs. These value-added services have significantly benefited the client, resulting in **no significant security threats** or **cyber-attacks** impacting their business over the **past four years**.

SISA's governance model ensures regular connection with clients at strategic, tactical, and operational levels on a weekly, monthly, and quarterly basis. Our proprietary CXO reports provide senior business leaders with insights into the performance of security operations, a comprehensive view of their organizational security posture, and support in making informed business decisions.

SISA's PORTFOLIO OF CYBERSECURITY SOLUTIONS

A forensics-driven cybersecurity company, trusted by organizations across the globe for securing their businesses with robust preventive, detective, and corrective security services, and solutions.

Compliance

PCI Compliance

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ

Risk & Compliance

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Swift
- HITRUST
- Cloud Security
- Risk Assessment
- Quarterly Security Audits

Security Testing

Application Security

- Application
- Penetration Testing
- CREST/CERT-in Approved
- Security Testing
- API Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- ASV Scan

IoT Security Testing

Managed Security Services

Phishing Simulation

Cyber Resilience

Managed Extended Detection & Response Solution

SISA ProACT

Incident Response and Forensics

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation

Advanced Threat Hunting

Dark Web and Brand Monitoring

Data Protection

Data Discovery and Classification

SISA Radar

- Card Data Discovery
- PII (Privacy) Data Discovery
- Data Classification

Data Discovery as a Service

Training

Payment Data Security Implementation Programs

- CPISI
- CPISI Advanced
- CPISI-D

Security Incident Detection and Response Programs

- CIDR

Forensic Learning and Ransomware Awareness Sessions for Senior Management

For more Information visit us at www.sisainfosec.com OR write to us at *contact@sisainfosec.com*

Follow us