Securing Shariah-Compliant Lending with Continuous Threat Management

About the Customer

The customer is a leading Shariah-compliant finance provider in Saudi Arabia, offering personal finance, auto finance, and digital credit solutions to individuals and businesses. Operating under the regulation of the Saudi Central Bank (SAMA), the firm has embraced digital transformation to enhance customer experience through mobile and web-based platforms, enabling fast approvals and real-time financing services.

The Challenge

With increasing digital adoption and regulatory scrutiny, the organization faced critical cybersecurity challenges:

- Protecting sensitive customer data across loan origination, credit checks, and disbursement systems.
- Ensuring compliance with the SAMA Cybersecurity Framework, especially in identity management, access control, and incident handling.
- Securing API-driven integrations with credit bureaus and internal decision engines.
- Mitigating fraud attempts via mobile app spoofing and fake loan applications.
- Strengthening visibility across hybrid infrastructure, including legacy banking tools and modern digital apps.

The customer sought a comprehensive cybersecurity approach tailored to financial services and compliant with national standards.

Governance & Compliance with GSOS (SAMA Framework)

GSOS helped structure the organization's cyber program around SAMA's key control domains:

- Risk Management: Automated risk assessments tied to asset inventory and exposure scoring.
- Access Control: Enforced SAMA-mandated privilege restrictions with audit-ready reporting.
- Incident Response: Simulated breach scenarios with playbooks mapped to SAMA's response guidelines.

This framework integration ensured both audit readiness and continuous improvement across their cybersecurity posture.

Deception-Led Detection with Invinsense XDR+

To stay ahead of attackers:

- Deployed fake mobile loan workflows and decoy user accounts to attract malicious activity.
- Flagged multiple reconnaissance attempts mimicking legitimate users.
- Helped reduce mean time to detect (MTTD) by 42%, particularly for app-level threats.

Solutions Used

The customer adopted the full Invinsense suite for integrated cybersecurity and compliance enablement:

- Invinsense XDR for real-time detection across user accounts, devices, and loan platforms.
- Invinsense XDR+ for deception-based controls across the mobile and web finance ecosystems.
- Invinsense OXDR for exposure management, red teaming, and threat validation.
- Invinsense GSOS for risk and compliance management aligned with the SAMA Cybersecurity Framework.

CTEM in Action CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Identified 1,150+ digital assets, including mobile apps, loan portals, and internal APIs.
Discovery	Detected 34 critical vulnerabilities, including misconfigured identity providers and outdated encryption libraries.
Prioritization	Mapped 17 exploitable threat paths targeting credit scoring APIs and admin access.
Validation	Simulated fraud attempts, data exfiltration, and privilege escalation across digital channels.
Mobilization	Resolved 90% of critical gaps within 45 days via a mix of tech and manual patching.

Key Results

- 90% of high-risk vulnerabilities remediated in 45 days.
- 42% faster threat detection, especially in the mobile finance environment.
- 24% increase in SAMA control coverage through automated policy enforcement.
- Increased customer trust via hardened digital loan processes and real-time visibility.

Executive Quote

"Invinsense brought structure, speed, and compliance to our cybersecurity journey. Their deep understanding of both financial operations and SAMA regulations helped us reduce risk, build trust, and stay ahead of emerging threats."

— Head of Information Security, Leading Shariah-Compliant Finance Institution

Infopercept | INVINSENSE

About Infopercept - Infopercept is one of the fastest growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Contact
sos@infopercept.com
www.infopercept.com/knowledge/casestudy