Securing Lending with Precision: How a Leading Consumer Finance Institution Gained Resilience and SAMA Compliance with Invinsense

About the Customer

This customer is a well-established non-bank financial institution (NBFI), offering Shariah-compliant personal, auto, and SME finance. Operating in a digitally evolving regulatory environment, they rely heavily on secure, cloud-based systems to deliver fast and transparent financial services. As a publicly listed entity under the governance of the Saudi Central Bank (SAMA), their cybersecurity posture is critical to maintaining operational integrity, customer trust, and regulatory compliance.

Industry	Consumer & SME Finance
Challenge	Safeguarding lending applications while meeting SAMA and Shariah regulatory mandates
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

As the organization scaled its digital lending operations, it faced mounting pressure to enhance its cybersecurity and compliance posture:

Exposed APIs in credit verification, document uploads, and loan processing pipelines	**Credential abuse** across customer mobile portals and agent dashboards	**Cloud workload vulnerabilities** with varying patch levels
Stringent SAMA Cybersecurity Framework and Shariah compliance mandates	**Inconsistent remediation cycles** across product and IT security teams	**Insider misuse and data tampering risks** in loan origination processes

The Invinsense Solution

The customer partnered with Invinsense to deploy a platform-led security program, enabling full visibility, exposure reduction, and compliance with SAMA and Islamic finance governance.

Invinsense XDR: Detecting Threats Across Lending Applications

By ingesting and correlating telemetry from digital lending apps, credit scoring engines, and customer onboarding flows, Invinsense XDR offered complete visibility into real-time threats.

Key Results:

- 67% faster detection of credential misuse across user roles
- Blocked unauthorized credit score manipulation via early-stage signals
- Contained API scraping attempts on pre-qualification calculators
- Integrated seamlessly with native SIEM and cloud logging tools

Invinsense OXDR + CTEM: Continuous Threat Exposure Management

With OXDR and CTEM, the customer adopted a proactive and cyclical approach to risk management across its fintech stack.

Scoping	• Catalogued 5,000+ digital assets, including mobile finance apps, KYC services, and internal decision engines
Discovery	• Exposed 190+ misconfigured endpoints with access to customer and transaction data • Identified container vulnerabilities affecting core underwriting modules
Prioritization	• Prioritized exposures based on their proximity to sensitive financial workflows and regulatory obligations
Validation	• Emulated attacks on the loan calculator logic and backend APIs • Validated exploitation paths using phishing simulations and credential testing
Mobilization	• Enabled DevSecOps squads to patch 89% of verified exposures within 30 days • Aligned remediation timelines with control implementation plans under SAMA guidelines

Invinsense XDR+: Deception-Based Threat Detection

To detect sophisticated fraud and insider misuse, the organization deployed deception strategies around its high-value systems.

Deception Outcomes:

Lured unauthorized access attempts to decoy customer data repositories	Flagged identity misuse in simulated agent environments	Detected bot-driven application tampering in under 5 minutes	Reduced false positives from endpoint detection pipelines by 63%

Key Result

- 67% faster response to fraud-based access attempts
- 84% reduction in web app misconfigurations
- 3.9x faster resolution of validated exposures
- 97% alignment with SAMA Cybersecurity Framework controls
- Full risk reporting integrated into quarterly security governance reviews

Executive Insight

“With Invinsense, we’ve transformed from being audit-driven to being truly security-driven. The platform helped us comply with SAMA requirements and secure every step of our customer journey.”

CTEM Outcomes

- 84% reduction in misconfigurations across cloud-native fintech apps
- 3.9x faster remediation of validated vulnerabilities
- 70% improvement in exposure awareness among Dev and Infra teams
- Full risk reporting integrated into quarterly security governance reviews

Invinsense GSOS: SAMA and Shariah Compliance Implementation

The customer operates under the close scrutiny of the Saudi Central Bank (SAMA), which mandates implementation of the SAMA Cybersecurity Framework.

GSOS was deployed to guide, monitor, and report compliance across critical domains including:

Cybersecurity Governance and Risk Management	Asset Management, Access Control, and Application Security	Third-Party Risk, Incident Management, and Business Continuity	Data Security aligned with Shariah-compliant financial operations

Compliance Outcomes:

Lured unauthorized access attempts to decoy customer data repositories	Flagged identity misuse in simulated agent environments	Detected bot-driven application tampering in under 5 minutes	Reduced false positives from endpoint detection pipelines by 63%

Quantifiable Impact

Category	Improvement
Exposure Remediation Speed	↑ 3.9x
Web App Misconfigurations	↓ 84%
Detection of Insider Threats	↑ 61% faster
Compliance with SAMA Controls	↑ 97% alignment
API Abuse Response Time	↓ 67% faster

Conclusion

For this Shariah-compliant financial innovator, Invinsense became the cornerstone of a modern, compliant, and continuously improving cybersecurity practice. With SAMA-aligned governance, threat-led defense, and exposure-informed action, the organization now moves forward with greater speed, trust, and resilience.

Infopercept | INVINSENSE

Imprint

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