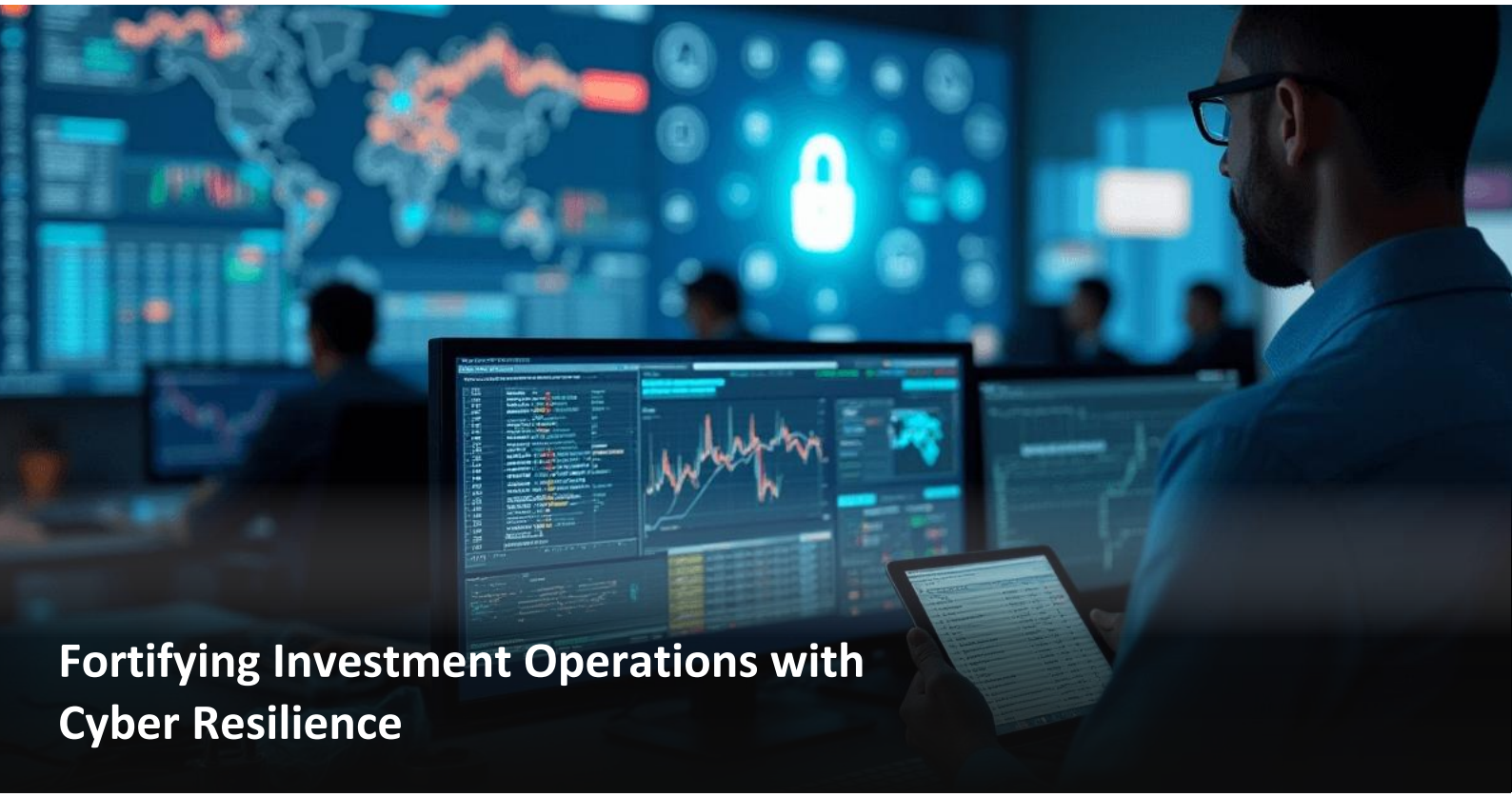

Fortifying Investment Operations with Cyber Resilience

About the Customer

The customer is a leading investment management firm headquartered in Saudi Arabia, specializing in Shariah-compliant asset management, private equity, and advisory solutions. Serving a wide range of investors and institutions across the region, the firm leverages digital platforms for managing portfolios, investor onboarding, performance reporting, and cross-border communication.

The Challenge

Operating in one of the most regulated financial markets in the region, the firm faced multiple cybersecurity challenges:

- Safeguarding sensitive investor data and financial records from insider threats and external breaches.
- Securing investment portals and portfolio management platforms accessed by wealth managers and institutional clients.
- Complying with the Saudi Arabian Monetary Authority (SAMA) cybersecurity framework for financial entities.
- Maintaining operational continuity amidst increasing cyber threats targeting the financial sector.
- Mitigating risks tied to third-party platforms and advisory partner integrations.

As the threat landscape evolved, the firm needed a robust, regulatory-aligned, and proactive cybersecurity approach.

Threat Deception with XDR+

To enhance visibility and proactive detection:

- Embedded fake investor portfolios and decoy admin panels within internal environments.
- Launched deceptive alerts to detect privilege escalation and lateral movement attempts.
- Resulted in a 39% faster response time to suspicious behavior across the network.

Security Compliance Enablement with GSOS

GSOS was critical in aligning the organization with SAMA's cybersecurity framework:

- Mapped internal security policies to SAMA domains, including Risk Management, Asset Management, and Access Control.
- Automated periodic compliance assessments and gap analyses.
- Enabled clear reporting for regulators and internal audit teams, ensuring continuous compliance and visibility.

CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Cataloged 1,300+ digital assets, including investment tools and reporting platforms.
Discovery	Uncovered 29 vulnerabilities, including insecure APIs and outdated access controls.
Prioritization	Mapped 14 high-risk threat paths, including exposure through third-party wealth apps.
Validation	Simulated adversary tactics targeting investor data access and internal workflows.
Mobilization	Resolved 88% of critical risks within the first month, with engineering-led patching.

Executive Quote

"Working with Invinsense helped us align our cybersecurity program with SAMA's rigorous framework while keeping our investment operations agile and secure. Their continuous threat validation and deception-based detection capabilities have elevated our resilience significantly."

– CISO, Leading Shariah-Compliant Investment Management Firm

Solutions Used

To meet these challenges, the customer deployed the full Invinsense cybersecurity stack:

- Invinsense XDR for centralized monitoring across endpoints, applications, and user behavior.
- Invinsense XDR+ for deploying deception-based defense within investor dashboards and admin consoles.
- Invinsense OXDR for attack surface management, vulnerability assessment, and validation of threat scenarios.
- Invinsense GSOS for managing governance, risk, and compliance aligned to the SAMA cybersecurity framework.

Key Results

- 88% of high-risk vulnerabilities eliminated within the first month.
- 39% faster detection and response to simulated attacks.
- 21% improvement in overall compliance posture through SAMA-aligned controls.
- Full attack surface visibility achieved across investment apps and advisory platforms.
- Boosted digital trust among stakeholders through resilient security and governance.

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.

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