Enhancing Cyber Resilience & SEBI Compliance for a Leading Wealth Management Firm

About the Customer

The client is one of India's leading wealth management and financial services providers. With a strong presence in investment advisory, broking, insurance, and portfolio management, the organization serves thousands of high-net-worth individuals (HNIs) and institutions. Their operations span multiple digital platforms—trading portals, mobile apps, APIs, and CRM systems—all governed by SEBI's Cyber Security and Cyber Resilience Framework (CSCRF).

The Challenge

The organization was scaling rapidly but faced growing challenges in:

Meeting all control mandates under SEBI CSCRF	Gaining unified threat visibility across cloud, mobile, and on-prem systems	Streamlining GRC, audits, and employee security awareness
Managing exposures from third-party tools and APIs	Detecting insider threats and lateral movements proactively	

They needed a partner who could help them shift from compliance checklists to real cyber resilience.

Solution: Invinsense Platform by Infopercept

To build a 360-degree security foundation, the client deployed the full Invinsense suite — covering XDR, XDR+, OXDR, and GSOS — integrated into a Continuous Threat Exposure Management (CTEM) lifecycle.

Invinsense XDR — Smarter Detection & Faster Response

- Integrated 120+ data sources including trading platforms, CRMs, endpoint tools, and cloud logs
- Built 500+ use cases mapped to MITRE ATT&CK
- Deployed real-time alerts and automated escalation workflows
- Integrated threat intelligence for proactive hunting

Impact:

- Detection time reduced from 7 hours to 23 minutes
- 3x improvement in visibility across asset types
- 98% logging control coverage as per SEBI mandate

OXDR — Continuous Threat Exposure Management

- External and internal attack surface mapping
- Continuous vulnerability management with real-world exploitability insights
- Breach & Attack Simulations on trading APIs, mobile apps, and backend infrastructure
- CTEM lifecycle aligned to asset criticality and SEBI risk thresholds

Impact:

- 74 critical issues discovered and patched
- 92% reduction in risk exposure window (from 21 days to 36 hours)
- Detected 3 unauthorized external integrations during CTEM scans

XDR+ — Deception & Patch Management

- Planted 35 deception assets across internal networks (decoy CRMs, logins, endpoints)
- Triggered early alerts on attacker lateral movement and credential misuse
- Linked deception insights with patching and alert workflows

Impact:

- Identified 5 high-risk internal threat behaviors missed by SIEM
- Enabled patching of 93% of SEBI-relevant vulnerabilities within SLA
- Prevented access escalation via decoy-based redirection

GSOS — GRC and SEBI Compliance Enablement

- Mapped 96 SEBI CSCRF controls to Invinsense capabilities
- Automated policy documentation, risk registers, and audit tracking
- Linked controls to real-time asset visibility and playbooks
- Conducted phishing, smishing, and vishing simulations organization-wide

Impact:

- Achieved full SEBI CSCRF compliance in 5.5 months
- 75% reduction in manual effort for SEBI and internal audits
- Phishing click rate dropped from 26% to 4.5%
- Smishing/vishing susceptibility reduced by 80%+ across 1,400 users

At a Glance

Area	Outcomes Delivered
SEBI Compliance	Achieved full CSCRF control coverage in 5.5 months
Detection & Response	Reduced detection time from 7 hours to 23 minutes
Exposure Management (CTEM)	92% reduction in critical risk exposure window
Deception Technology	Detected 5 insider threat indicators missed by legacy tools
GRC Automation (GSOS)	Cut manual audit workload by 75%
Phishing Simulation	Click rates reduced from 26% to 4.5% in 3 simulations
Smishing/Vishing Readiness	User response to social engineering dropped by 80%+

Executive Quote

"Cybersecurity used to feel like a compliance headache. With Invinsense, we've moved to a living, breathing defense strategy—where threats are hunted, gaps are closed, and compliance is a natural by-product. Invinsense is not just a product; it's a transformation partner."

— Chief Information Security Officer, Leading Wealth Management Company

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