Enhancing Cybersecurity and Compliance for a Fintech Processing Leader

About the Customer

The customer is a Bahrain-based fintech and business process outsourcing provider, licensed by the country's central financial regulator as an Ancillary Services Provider. Established in the mid-2000s and later acquired by a large regional retail group, this company offers a wide range of services including payment processing, application handling, call center operations, and infrastructure management. Its solutions are tailored to help financial institutions and retailers improve operational efficiency while reducing costs.

Industry	Fintech / Business Process Outsourcing (BPO)
Challenge	Securing sensitive financial data and ensuring regulatory compliance across diverse services
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

As this fintech processor expanded its service offerings and clientele, it encountered several cybersecurity and compliance roadblocks:

Protecting sensitive financial and personal data across multiple platforms	Ensuring compliance with ISO 27001 and Central Bank of Bahrain (CBB) regulations	Managing cybersecurity risks with limited internal resources
Detecting and responding to threats across a hybrid IT environment	Maintaining business continuity while fending off increasing cyber threats	

The Invinsense Solution

To address these challenges, the organization deployed Invinsense's integrated platform, creating a proactive and resilient security posture across its critical operations.

Invinsense XDR: Unified Threat Detection Across Services

Invinsense XDR enabled centralized monitoring across the client's fintech processing platforms, call center infrastructure, and support systems, allowing the team to detect and respond to threats in real-time.

Key Results:

- 72% faster detection of security incidents
- Reduced false positives, increasing analyst efficiency
- Significant reduction in dwell time for threat actors

Invinsense OXDR + CTEM: Proactive Exposure Management

By integrating OXDR with a Continuous Threat Exposure Management (CTEM) framework, the client gained full visibility into their digital estate and proactively closed risk gaps.

Scoping	• Mapped over 2,500 digital assets, including payment systems, databases, and backend services
Discovery	• Uncovered more than 180 misconfigurations and exposed assets
Prioritization	• Assessed risks based on financial transaction volumes and data sensitivity
Validation	• Simulated attacker techniques to validate exploitability
Mobilization	• 90% of identified risks remediated within 15 days

Key Result

- 72% faster detection of security incidents
- 4.5x improvement in vulnerability remediation timelines
- 96% alignment with ISO 27001 and CBB compliance requirements
- 5.8x increase in early threat identification through deception technology

Executive Insight

"Invinsense transformed our security posture. We now detect threats faster, resolve risks more efficiently, and maintain confidence in meeting our regulatory obligations."
— Chief Information Security Officer, Fintech Processing Leader

CTEM Outcomes

- 4.5x faster closure of critical vulnerabilities
- 70% reduction in exploitable misconfigurations
- Strengthened internal collaboration between operations and security teams

Invinsense XDR+: Advanced Threat Detection with Deception

XDR+ introduced deception capabilities into the environment, enabling the client to detect lateral movement and insider threats early in the attack lifecycle.

Outcomes:

5.8x increase in early-stage threat identification	Improved detection of credential misuse and unauthorized access	Valuable intelligence generated from attacker interactions with decoys

Invinsense GSOS: Streamlined Regulatory Compliance

Invinsense GSOS was configured to track and manage cybersecurity control requirements tied to both ISO 27001 and local financial regulations.

Compliance Outcomes:

96% alignment with mandated compliance frameworks	Automated control assessments and evidence collection	Reduced audit preparation time by 65%

Quantifiable Impact

Category	Improvement
Detection of Security Incidents	↑ 72% faster
Vulnerability Remediation Timelines	↑ 4.5x improvement
Regulatory Compliance Alignment	↑ 96%
Early Threat Identification	↑ 5.8x increase
Efficiency in Incident Response	↑ Enhanced through reduced false positives

Conclusion

With Invinsense's layered security approach, the client fortified its infrastructure, proactively managed threat exposure, and streamlined its compliance operations—ensuring security and trust in the services it delivers to its financial partners.

Infopercept | INVINSENSE

Imprint

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