Securing a Global Financial Leader through Offensive Security and Continuous Threat Exposure Management

About the Customer

The customer is one of the world's leading financial services organizations, operating across 70+ countries with a legacy that spans over a century. With offerings ranging from insurance and asset management to digital financial products, the organization serves over 100 million customers globally. As a systemically important institution, its digital infrastructure is vast, complex, and constantly evolving—comprising thousands of web applications, mobile platforms, APIs, and cloud-native services distributed across multiple geographies.

The Challenge

Operating in a high-risk, high-trust domain, the organization was faced with several cybersecurity challenges inherent to its scale and complexity:

A growing portfolio of digital assets and APIs across business units that needed continuous validation for security risks	Strict regulatory mandates across different countries requiring ongoing penetration testing and validation
A decentralized infrastructure that made it difficult to consistently identify and prioritize the most critical exposures	The need to move beyond point-in-time testing to a more continuous, adaptive security validation model

The organization sought a security partner capable of delivering comprehensive offensive security services across all environments while embedding a proactive and scalable exposure management strategy into their digital risk lifecycle.

Solutions Used

Infopercept's Offensive Security and CTEM (Continuous Threat Exposure Management) teams engaged with the organization to deliver an end-to-end, continuous security validation program. Key elements included:

Offensive Security Services

- Web Application Testing: Over 500+ critical internal and external web applications tested annually
- Mobile Application Testing: Regular testing of Android/iOS apps used by millions of global users
- API Security Testing: Continuous assessment of over 1,200 internal and public-facing APIs, with special focus on authorization, injection flaws, and business logic
- Cloud Penetration Testing: Testing across multi-cloud environments (AWS, Azure, GCP) aligned with CIS Benchmarks and real-world attacker tactics
- Dynamic and Static Application Security Testing (DAST + SAST): Integrated with CI/CD pipelines to ensure vulnerabilities are caught early in the SDLC

Continuous Threat Exposure Management (CTEM)

- Attack Surface Discovery: Mapping the organization's entire external attack surface using advanced reconnaissance and threat intel
- Prioritized Exposure Validation: Weekly adversary simulation cycles that replicate the latest TTPs (MITRE ATT&CK-aligned) to validate real-world exploitability of exposures
- Exposure Scoring and Reporting: Custom dashboards and monthly reports categorizing exposures by business impact, exploitability, and remediation feasibility
- Feedback into Patch and DevOps: Findings were integrated back into vulnerability management and DevSecOps pipelines for faster remediation

Executive Quote

"We operate in a landscape where both the complexity of our infrastructure and the sophistication of threats are constantly evolving. Infopercept's offensive security program has helped us move from reactive testing to a continuously validated security model. Their CTEM approach ensures that we're not just fixing issues—we're fixing the right issues first."

— Global Head of Information Security, Leading Financial Services Institution

Outcomes Achieved

Global Offensive Security at Scale

- Conducted 2,500+ security tests across 60+ global business units in one year
- Discovered and helped remediate 1,400+ critical and high-severity vulnerabilities
- Enabled shift-left testing by integrating SAST/DAST into 30+ agile development pipelines
- Maintained an average SLA of <72 hours for reporting critical issues
- Identified 75+ broken object-level authorization flaws across APIs, reducing data exposure risks

CTEM-Driven Exposure Reduction

- Mapped entire digital attack surface across multiple regions, brands, and subsidiaries
- Conducted bi-weekly exposure validation campaigns, focusing on high-risk assets
- Reduced overall mean time to remediate (MTTR) critical exposures by 47%
- Enabled board-level visibility into exposure trends and attack simulations through curated CTEM reporting

Conclusion

Through its robust offensive testing and CTEM program, Infopercept has helped this global financial leader evolve from periodic testing to continuous security validation—embedding offensive thinking into their digital DNA. The result is not just a stronger security posture, but a more agile, data-driven, and threat-resilient enterprise.

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