Enterprise-Wide Security Assessment for Global Financial Institution

A multinational financial institution engaged CyberOps for its annual security assessment, validating over 100 customer-facing platforms, APIs, mobile applications, and AI-driven services against real-world cyber threats targeting financial infrastructure.

The Engagement

Our team conducted full-spectrum security testing across the client's entire digital ecosystem, employing multiple testing methodologies to ensure thorough coverage of all potential attack vectors.

- ### Application Security Testing
  Comprehensive assessment of 100+ web and mobile applications using black box, grey box, and manual exploitation techniques. Testing aligned with OWASP Top 10, PCI DSS, and ISO frameworks to ensure regulatory compliance.
- ### AI and LLM Security
  Specialised testing of AI-driven chatbot services to identify model abuse scenarios, prompt injection vulnerabilities, and data leakage risks unique to large language model implementations.
- ### Infrastructure Assessment
  Internal vulnerability assessment covering network segmentation, firewall configurations, and access control mechanisms to identify lateral movement opportunities and privilege escalation risks.

Critical Findings and Business Impact

Our assessment uncovered significant security gaps across the application portfolio and infrastructure, with findings categorised by severity and potential business impact. The discovery of over 250 vulnerabilities demonstrated the value of comprehensive, expert-led security testing.

Critical Severity Issues

50+

Vulnerabilities Identified

Representative Issues:

- Backend validation weaknesses enabling transaction manipulation
- Insecure API trust boundaries allowing unauthorised access
- Authentication bypass opportunities

Business Impact: Unauthorised financial activity, privilege escalation, and regulatory non-compliance exposing the institution to significant financial and reputational risk.

High Severity Issues

200+

Vulnerabilities Identified

Representative Issues:

- Access control inconsistencies across platforms
- Network segmentation gaps enabling lateral movement
- AI model abuse scenarios and prompt injection vectors

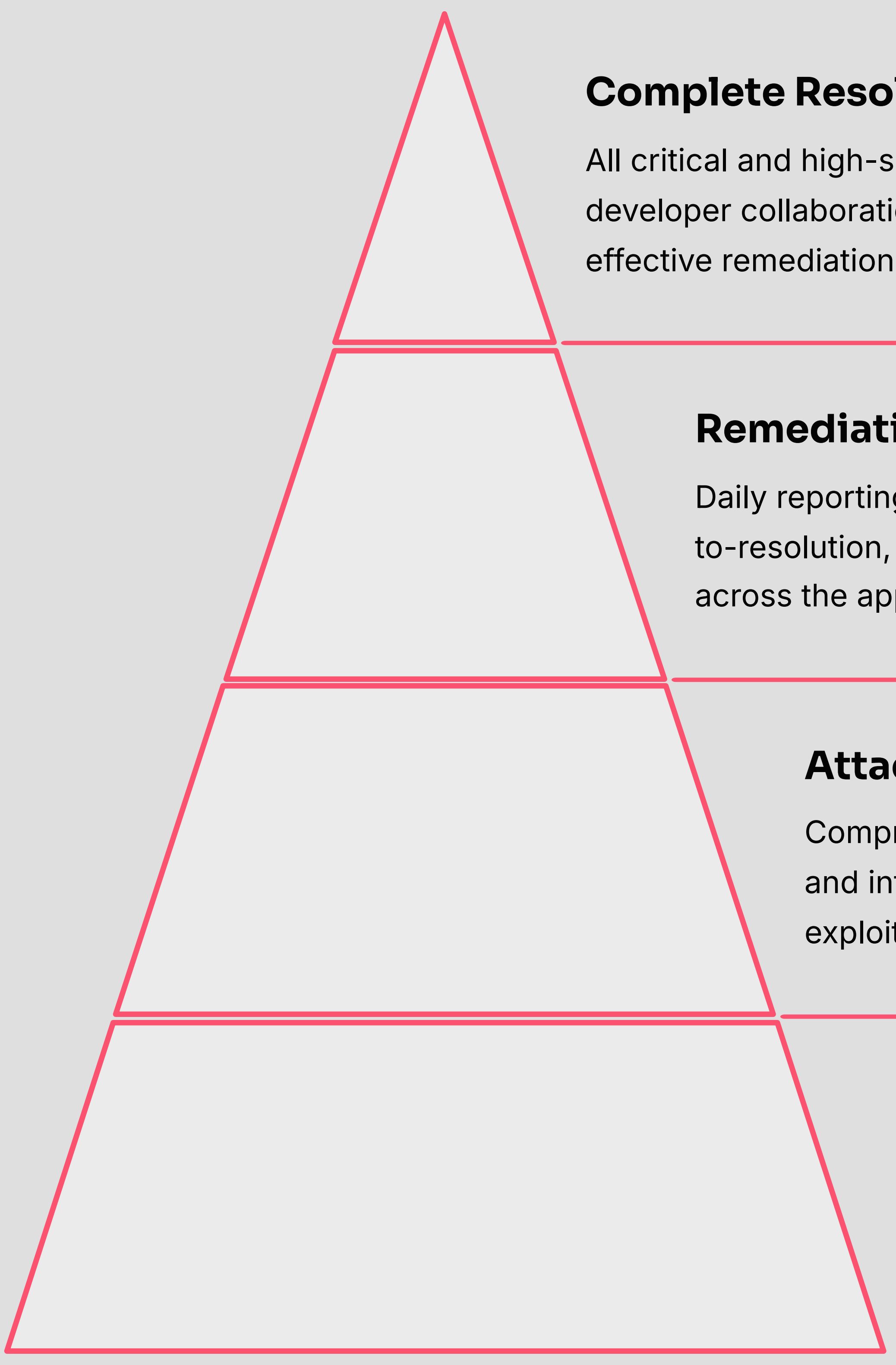
Business Impact: Sensitive data exposure, increased attack surface for lateral movement, and potential service disruption affecting customer trust and operational continuity.

Notable Discovery: CVE Assignment

CyberOps researchers identified a previously unknown vulnerability in the client's Jira environment, resulting in official CVE assignment. This discovery demonstrates our advanced testing methodology that extends beyond standard assessment frameworks, delivering genuine security research value.

Remediation and Outcomes

Through close collaboration between our testing team and the client's development organisation, we achieved comprehensive remediation of all critical and high-severity findings.



Complete Resolution of Critical Findings

All critical and high-severity vulnerabilities resolved through direct tester-developer collaboration, ensuring thorough understanding of root causes and effective remediation strategies.

Remediation Velocity Increased

Daily reporting and real-time fix validation significantly reduced time-to-resolution, enabling rapid deployment of security improvements across the application portfolio.

Attack Surface Measurably Reduced

Comprehensive security improvements across both application and infrastructure layers resulted in quantifiable reduction of exploitable vulnerabilities and enhanced security posture.

Third-Party Validation

Sanitised public reports delivered for stakeholder validation, demonstrating transparency and commitment to security excellence for regulators, partners, and customers.

Client Impact and Ongoing Partnership

The Chief Information Security Officer confirmed strong satisfaction with the technical quality of our assessment, the accuracy of risk identification, and the collaborative approach taken throughout the engagement. Our ability to work seamlessly with internal teams whilst maintaining rigorous testing standards differentiated the CyberOps engagement from previous assessments.

Based on the demonstrated value and measurable security improvements achieved, the institution committed to an ongoing annual partnership with CyberOps. This long-term engagement enables continuous security validation, proactive threat identification, and sustained improvement of the organisation's security posture in an evolving threat landscape.

Key Success Factors

- Advanced testing methodology delivering genuine research value
- Real-time collaboration enabling rapid remediation
- Comprehensive coverage across all digital assets
- Clear communication of business impact
- Regulatory alignment and stakeholder transparency

Schedule a call