SYGNIA

Insider Threat Simulation Penetration Test with Firi

Final Report

Firi

31 Dec 2025

TABLE OF CONTENTS

1.

EXECUTIVE SUMMARY

CONTEXT

Threat Landscape

Industry Trends

Digital asset platforms remain prime targets due to their direct access to monetary assets, sensitive customer data, and critical trading infrastructure. Increasing digitalization further elevates exposure to fraud and operational disruption.

Zoom In

As Norway's largest cryptocurrency exchange, Firi operates in a high-risk threat environment that attracts sustained adversarial interest and requires strong security controls to protect customer assets and trust.

Possible Outcomes

Compromise of Sensitive Data or Digital Assets

Financial Loss and Operational Disruption

Reputational Damage and Possible Legal Liability

Business Motivation

- Recognizing the evolving threat landscape facing digital asset platforms, Firi is strengthening its cybersecurity posture to ensure the resilience of its critical services.
- To support this effort, Firi engaged Sygnia to conduct an independent security assessment.
- The engagement focuses on evaluating the effectiveness of controls protecting Firi's platform and identifying opportunities to reduce business and security risk.

Scope

- The scope of this engagement was designed to support Firi in improving the cybersecurity posture of its platform.
- The assessment followed a grey-box approach, simulating an insider-threat scenario and focusing on access controls, privilege boundaries, and the potential impact of misuse or compromise.

Objectives

- Evaluate the effectiveness of Firi's security controls and their alignment with industry best practices.
- Identify vulnerabilities and misconfigurations, pinpoint areas of improvement, and highlight opportunities for impactful enhancements.
- Recommend actionable measures, provide concrete mitigation steps to address identified gaps, and improve application security.

ENGAGEMENT PHASES

Preparations

- Understand the organization's objectives, scope, and desired outcomes.
- Plan engagement.

Product Assessment

- Conduct comprehensive evaluation of Firi's platform through rigorous stress testing.

Analysis

- Identify and map the vulnerabilities and gaps.
- Document the results of the web application assessment.
- Collect relevant information for further analysis.

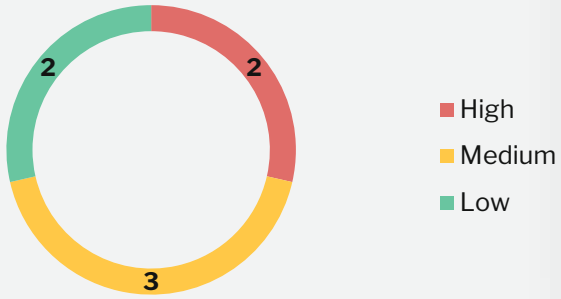
Delivery

- Develop detailed mitigation steps and executive summary based on the assessment findings.
- Prepare and validate draft report.
- Deliver the final report, including a comprehensive analysis of vulnerabilities, risks, and recommended actions.

KEY INSIGHTS

Findings Overview

FINDINGS BY RISK LEVEL



Main Opportunities

VDI Hardening Gaps

The Virtual Desktop Infrastructure environment lacks essential security hardening controls, significantly increasing the risk of compromise and malicious activity within the network.

Privilege Escalation Exposure

VDI systems are joined to the Active Directory domain, increasing the risk of privilege escalation in the event of a compromise. Third-party access to the VDI environment further increases the potential impact.

Lateral Movement Risk

Limited network segmentation enables lateral movement between VDI systems and into the broader Active Directory environment, increasing the likelihood of widespread compromise across multiple active application sessions.

Key Strengths

- The application demonstrates **strong resilience against client-side attacks;** all injection attempts across the application were unsuccessful.
- The application benefits from **Cloudflare's perimeter security controls,** which provide an additional layer of protection against common web-based threats.
- **User-supplied parameters are properly validated** across the core functionality, preventing server-side injections and command/SQL execution.
- Robust authorization controls are in place; **token-based enforcement** prevents cross-user access and ensures proper user segregation.
- **Authentication is integrated with Google Workspace,** leveraging a mature identity platform with enforced multi-factor authentication.