Executive Security Report

Client: Altera Fund Advisors

Reporting Period: 2025-10

Executive Summary

During the reporting period, the organization maintained a stable and secure posture with no critical incidents reported. This stability is evidenced by the absence of user additions (0 users joined) or departures (0 users departed), as well as the lack of new devices added or existing devices retired (0 devices in both cases). The consistent security controls in place have effectively mitigated potential threats and ensured business continuity.

Identity & Access Management

No user onboarding or offboarding activities were identified during this period. This lack of movement indicates a mature identity lifecycle management process, minimizing the risk associated with unauthorized access. However, it is essential to continue monitoring these processes to ensure they remain effective and up-to-date in response to evolving security threats.

Endpoint & Asset Security

No devices were added or retired during the reporting period, maintaining a consistent asset inventory. The endpoint observations also revealed no notable risks, demonstrating effective control coverage across all monitored devices. It is crucial to continue proactive monitoring and threat detection to maintain this level of security posture.

Threat & Incident Analysis

The lack of EDR incidents (0 reported) signifies a well-controlled environment with robust protective measures in place. The absence of significant threats indicates that the organization's proactive approach to cybersecurity is effective and mitigating potential risks successfully.

User Risk & Awareness

No users were found to have failed phishing simulations during this period, demonstrating a high level of user awareness and adherence to security best practices. Nevertheless, continuous security awareness training should be maintained to ensure that the workforce remains vigilant against emerging threats.

Positive Security Observations

The effective operation of various controls, such as phishing simulations and backup mechanisms, has significantly contributed to maintaining a secure environment. The absence of high-severity EDR incidents highlights the success of these controls in detecting and mitigating potential threats.

Recommendations & Next Steps

To maintain the current security posture, we recommend:

1. Continuing regular phishing simulations and security awareness training to ensure user vigilance against emerging threats;

2. Ensuring backup coverage remains enabled for all endpoints to minimize data loss risk in case of incidents;

3. Maintaining strict identity lifecycle management processes to control access and minimize unauthorized access risks;

4. Continuing proactive endpoint monitoring and threat detection to ensure prompt response to potential threats.