Executive Security Report

Client: Altera Fund Advisors

Reporting Period: 2025-11

EXECUTIVE SUMMARY

The organization has maintained a stable security posture during the reporting period, with no critical incidents or data breaches reported. The user base experienced minimal changes, as two new users joined and seven existing users departed. Similarly, no new devices were added to the network while none were retired. This stability underscores our effective control coverage across users and assets.

IDENTITY & ACCESS MANAGEMENT

Two new users (ddenieunkerk@alteradevco.co and office.manager@alteradevco.co) joined the organization during this period, while seven existing users departed. The departing users included ddenieunkerk@alteradevco.com, demery@alteradevco.com, kdevinney@alteradevco.com, kwinant@alteradevco.com, office.manager@alteradevco.com, rmartinez@alteradevco.com, and rstark@alteradevco.com. The absence of notable identity-related observations indicates a maturing access governance process.

ENDPOINT & ASSET SECURITY

Four devices (SN:5CG302492B, SN:MXL11947NM, SN:NAN, and SN:PF5ZJ0EP) were added to the network during the reporting period. None of the existing devices were retired. The consistent backup posture across all endpoints demonstrates our commitment to data resilience and operational continuity.

THREAT & INCIDENT ANALYSIS

No critical EDR incidents or phishing failures were reported during this period. The absence of such events underscores the effectiveness of our proactive threat detection measures, as well as the vigilance of our users in confronting cyber threats.

USER RISK & AWARENESS

No users failed the phishing simulations this period, indicating a higher level of user awareness and adherence to security best practices.

POSITIVE SECURITY OBSERVATIONS

The successful avoidance of phishing attacks and the healthy backup status of all monitored devices signify our robust cybersecurity measures and their critical role in maintaining business resilience.

RECOMMENDATIONS & NEXT STEPS

To build upon this stable security posture, we recommend:

Continuing regular phishing simulations and security awareness training to maintain user vigilance.

Ensuring backup coverage remains enabled for all endpoints, as data resilience is essential to operational continuity.

Maintaining strict identity lifecycle management processes to minimize access-related risks.

Continuing proactive endpoint monitoring and threat detection to maintain our strong security posture.