TECHNAGY IT
empowering you

CYBERSECURITY MONITORING REPORT

2025-10-01 - 2025-10-31

Prepared for Altera Fund Advisors

Cybersecurity Monitoring Overview

Our Security Operations Center (SOC) monitors your environment for malicious and suspicious activity that evades conventional defenses. The SOC operates 24/7/365 and consists of skilled cybersecurity professionals who continuously analyze network, endpoint and cloud attack vectors to detect and respond to potential security incidents.
Below is a summary of the assets monitored by the SOC during the reporting period:

Monitored Assets

Agents	Firewalls	M365 Accounts
29	0	39

Event Sources

- Datto EDR / AV Monitor
- Endpoint Event Log Monitor
- Office 365 Login Analyzer

Security Analyst Findings

The SOC triaged and analyzed **1937** logs and events for suspicious or malicious behavior during the reporting period. After reviewing the data, the SOC Analyst Team created **8** security incidents, indicating that the activity warranted deeper investigation. Of those security incidents, **8** have been resolved and **0** are still open.

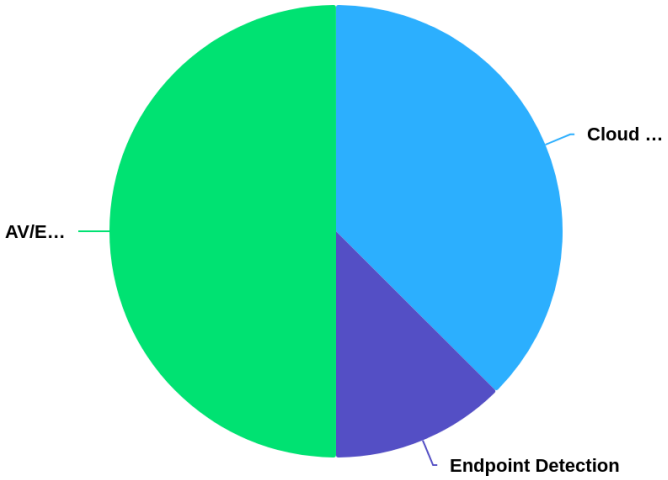
Events: **1.9k**
Total number of logs, events, and other data points collected, triaged and analyzed by the SOC.

Incidents: **8**
Total number of events that were potentially suspicious or malicious that warranted further investigation.

Open: **0**
Total number of incidents that have not been resolved and are still open.

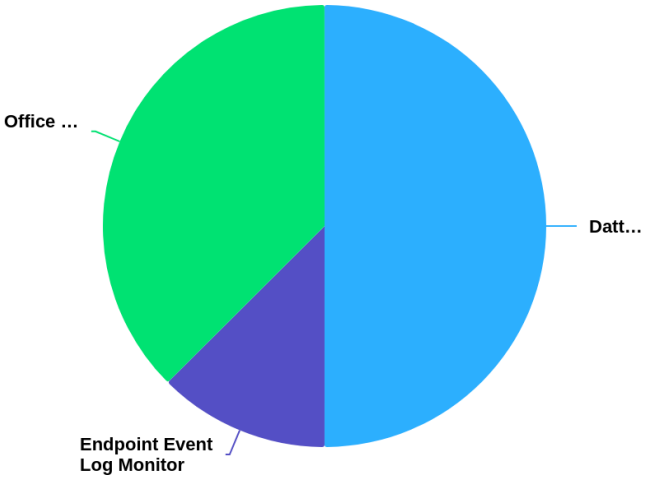
Incident Origin Analysis

Understanding the attack surface and identifying weaknesses in your security posture is critical to preventing attacks. The chart below outlines where incidents most commonly occur in your environment, providing insight into where you can make improvements to get ahead of the attackers.



Incident Category Breakdown

Many different detection methods are used to identify threats from both agent and cloud environments. These range from M365 login analysis to ransomware detection on local devices. The chart below shows a breakdown of the incident categories.



Incidents from 2025-10-01 to 2025-10-31

Incident ID	Incident Name	Date	Total Events	Status
9129769	O365 P1 Successful Login - MX tq@alteradevco.com for Altera Fund Advisors (Managed SOC)	2025-10-31	1	Resolved
9105825	O365 P1 Successful Login - MX tq@alteradevco.com for Altera Fund Advisors (Managed SOC)	2025-10-30	4	Resolved
9104158	SOC Called - O365 P1 Successful Login - MX tq@alteradevco.com for Altera Fund Advisors (Managed SOC)	2025-10-30	1	Resolved
8987524	Datto EDR Detected efx-le_editor_v141.exe on lt-alt-mr for Altera Fund Advisors (Managed SOC)	2025-10-25	1	Resolved
8987525	Datto EDR Detected efx-le_editor_v141.exe on lt-alt-mr for Altera Fund Advisors (Managed SOC)	2025-10-25	1	Resolved
8980689	Datto EDR Detected efx-le_editor_v141.exe on lt-alt-mr for Altera Fund Advisors (Managed SOC)	2025-10-24	1	Resolved
8980690	Datto EDR Detected efx-le_editor_v141.exe on lt-alt-mr for Altera Fund Advisors (Managed SOC)	2025-10-24	9	Resolved
8794119	4720 - Local User PquinnAltera Created on ALTERA for Altera Fund Advisors (Managed SOC)	2025-10-17	1	Resolved

Conclusion

This report summarizes the security monitoring activities for the 30-day reporting period. The Security Operations Center (SOC) maintained continuous visibility across all monitored assets, ensuring consistent oversight and timely response to any potential threats.

The SOC remains actively engaged in monitoring, detection, and response efforts to uphold a strong security posture across all environments. Continuous vigilance and proactive threat management help minimize risks and maintain a secure and stable operational environment.