RMM Site : Altera Fund Advisors

10/01/2025 - 10/31/2025

TECHNAGY IT
empowering you

EXECUTIVE
THREAT REPORT

Powered by

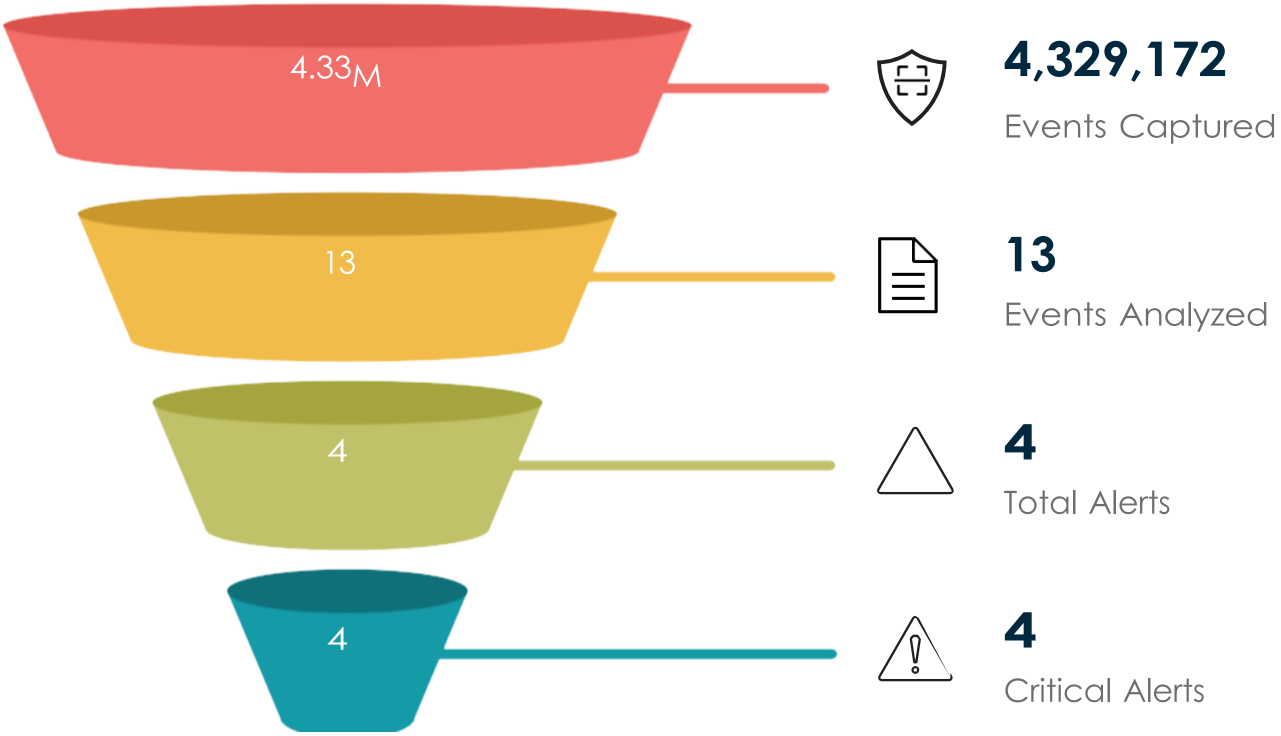
datto | EDR

Endpoint Security with Datto EDR

Datto EDR is an incredible addition to any customer's security stack. Our cloud-based software monitors for hundreds of common attack behaviors and is continually evolving to combat new techniques. Combining multi-source threat intel enrichment, advanced analytics and one of the most experienced security teams in the industry with rich memory analysis, known techniques, and scalable infrastructure EDR helps expand your business and secure your clients.

At A Glance

We have been vigilantly patrolling your network to ensure your safety and security. Between 10/01/2025 and 10/31/2025 we observed a total of 4,329,172 events. Of these events, 13 required additional analysis. From our analysis, 4 events were identified as possibly malicious with 4 deemed critical.



4,329,172
Events Captured

13
Events Analyzed

4
Total Alerts

4
Critical Alerts

Behaviors Analyzed

Protection	0	**Behavior**	9
File Reputation	4	**Extension**	0

Threat Analysis

Following is an overview of the total hosts monitored, broken down by operating systems, along with a detailed analysis of the top 5 alerts categorized by severity. A summary of alerts highlights key areas of concern, while the list of top 5 hosts by alert count pinpoints the endpoints requiring immediate attention. By leveraging this information, your security team can prioritize and implement measures to bolster your network's defenses against prevalent threats.

Hosts Monitored

29	29	0	0	0
Total Hosts Monitored	Windows	OSX	Linux	Other

Top 5 Alerts

Alert Name	Source Engine	Severity	Hosts	Alert Count
efx-le_editor_v141.exe	reputation	high	1	4
rundll32.exe	rule	medium	2	4
net.exe	rule	low	1	1
taskmgr.exe	rule	low	1	1
net1.exe	rule	low	1	1

Alert Summary

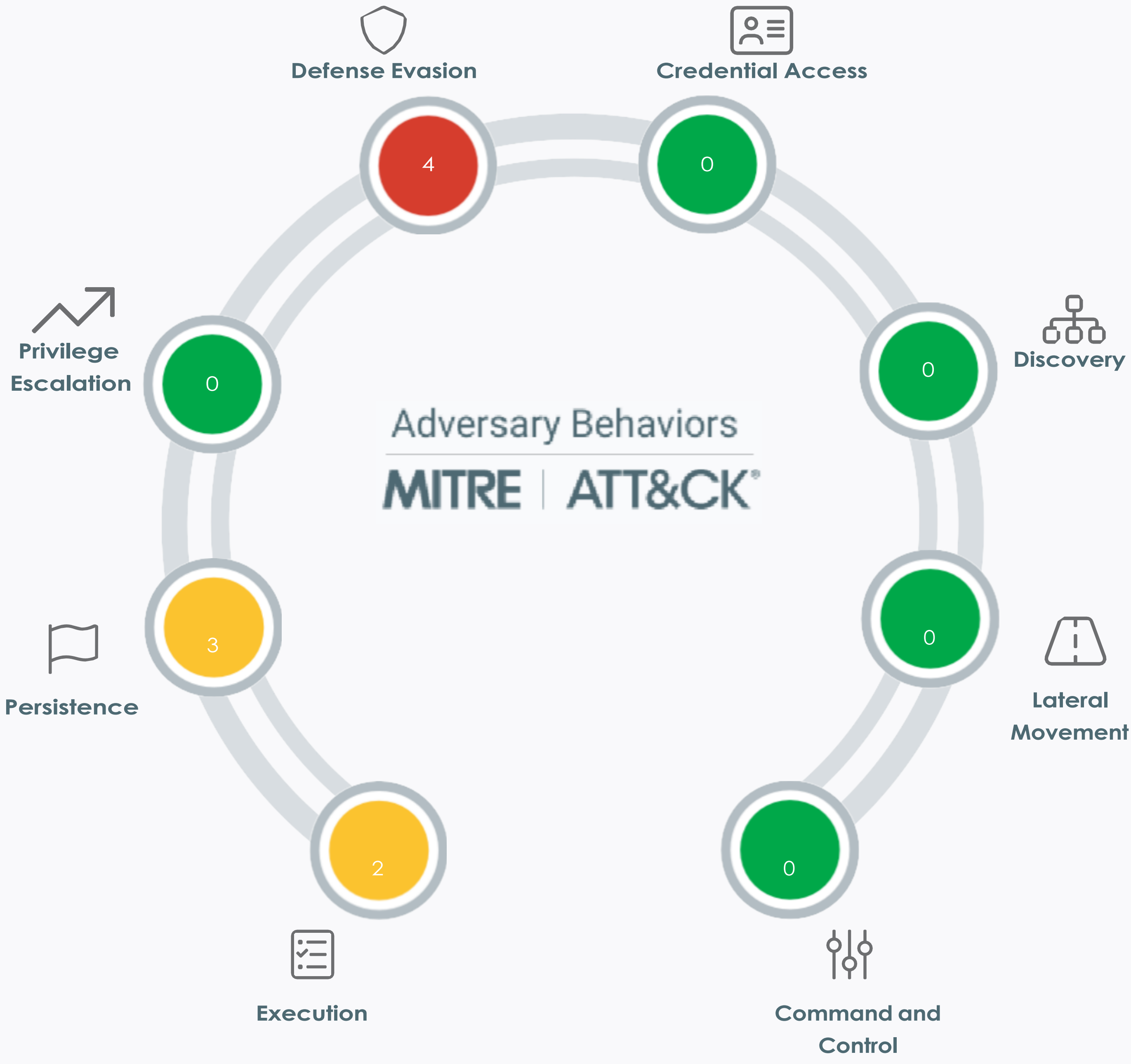
13	0	9	0	4	0	0
Top Alerts	Ransomware	Rules	Correlated	Reputation	Extension	AV

Top 5 Hosts By Alert Count

Host Name	Alert Count
lt-alt-mr	4
desktop-ponai23	3
afa-lt-0f36kg92	2
afa-lt-0f37dbm	1
alteraaltera	1

Detection

Datto EDR dynamically analyzes behaviors of your endpoint. These behaviors are collected and mapped using MITRE, which is a powerful framework designed to identify unique attack methods. Mapping behaviors with MITRE will drive implementing new security controls and techniques to defend your business.


Defense Evasion
4
Credential Access
0
Privilege Escalation
0
Discovery
0
Adversary Behaviors
MITRE | ATT&CK®
Persistence
3
Lateral Movement
0
Execution
2
Command and Control
0