



CYBERSECURITY MONITORING REPORT

ANONYMIZED EXAMPLE

Prepared for: confidential client



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

116



Firewalls

4



M365 Accounts

0

Event Sources

- ✔ Endpoint Event Log Monitor
- ✔ BitDefender Monitor

Security Analyst Findings

The SOC triaged and analyzed **42369** logs and events for suspicious or malicious behavior during the reporting period. After reviewing the data, the SOC Analyst Team created **10** security incidents, indicating that the activity warranted deeper investigation. Of those security incidents, **2** have been resolved and **1** are still open.



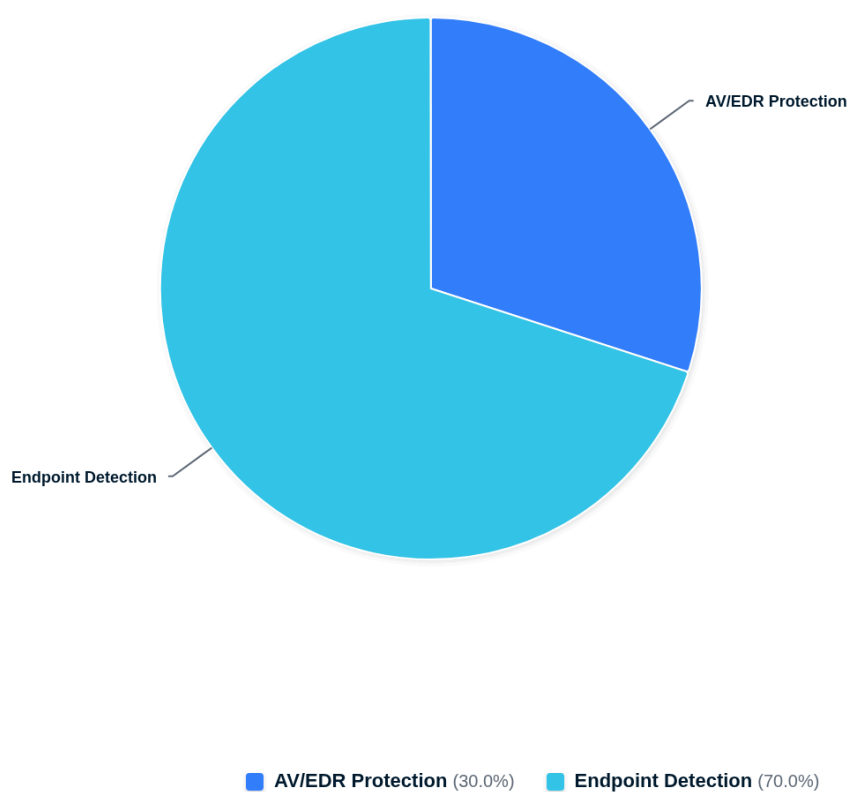
Events: 42.3k
Total number of logs, events, and other data points collected, triaged and analyzed by the SOC.

Incidents: 10
Total number of events that were potentially suspicious or malicious that warranted further investigation.

Open: 1
Total number of incidents that have not been resolved and are still open.

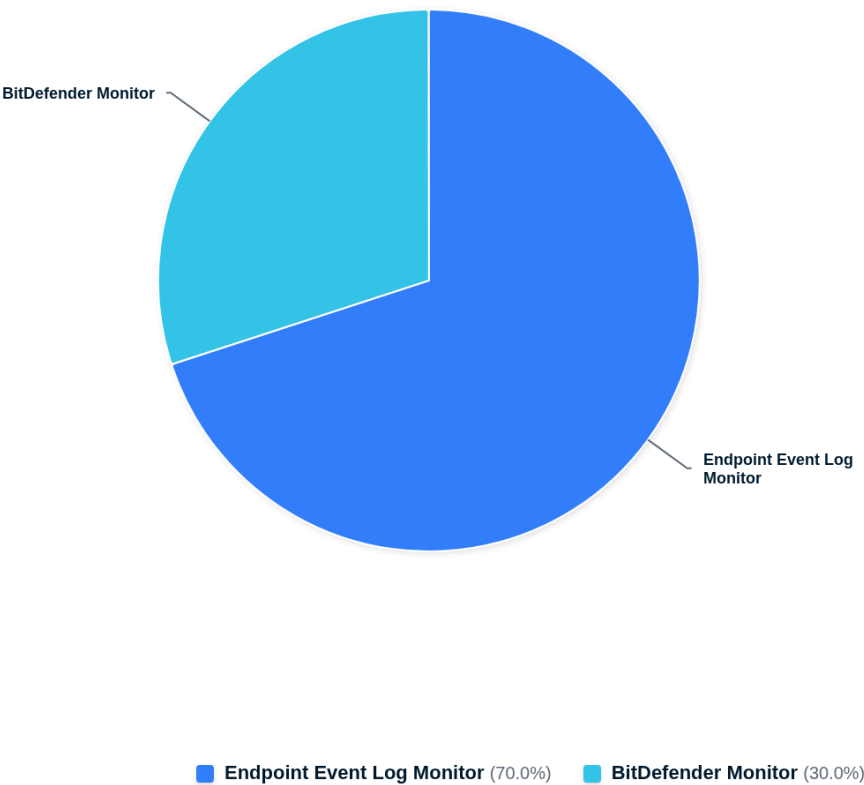
Incident Origin Analysis

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.



Incident register (anonymized)

Monthly example. Identifiers, systems and dates have been anonymized.

Reference	Incident category	Events	Status
INC-01	Endpoint alert: potentially unwanted application	1	Suppressed
INC-02	Failed logon (event 4625)	1	Suppressed
INC-03	Failed logon (event 4625)	16	Suppressed
INC-04	Failed logon (event 4625)	1	Suppressed
INC-05	Failed logon (event 4625)	1	Suppressed
INC-06	Failed logon (event 4625)	1	Suppressed
INC-07	Endpoint alert: potentially unwanted application	1	Suppressed
INC-08	User created (event 4720) on HOST-A	4	Resolved
INC-09	User created (event 4720) on HOST-B	4	Resolved
INC-10	Endpoint protection: application detection	1	Open