HUNTRESS

Huntress Managed Detection and Response for M365

How does it work?

MDR for M365 starts by collating Azure user, tenant and application data which is enriched with additional organic and external threat feeds. Over time a behavioral fingerprint is constructed from the enriched data, improving the fidelity of detections. Together this data is utilized by the Huntress ThreatOps Team to detect, analyze, and report on suspicious behaviors or dangerous threats and to provide remediation options.

Why do you need it?

With modern cloud-based infrastructure, a single stolen credential or compromised account can be used to launch a cyber attack. Simple and ever-present threats like Business Email Compromise and related fraud now cost more than ransomware. Locating suspicious logins or activity like new mail forward configurations can identify a nascent intrusion before damage can be done.

However, locating and responding to compromised accounts is not always so easy. Automated or AI tools produce too many false positives and require too much management. Fully managed detection and response can prove to be too costly for most, and alerts can still be missed. Those industrious enough to create their own detection rules and scripts will quickly find themselves straining under the volume of alerts.

> **“The client was extremely thankful that we had their back, and for us, we’re grateful that Huntress has ours.... The goal I give to every other vendor is ‘you guys should do it like Huntress.’”**

Matt Horning
Owner | Blue Tree Technology

Key Features

SUSPICIOUS LOGIN IDENTIFICATION

Suspicious Login Identification looks for "Impossible and Improbable travel." "Impossible and Improbable travel" is one of the most basic anomaly detections used to indicate that a user is compromised. The logic behind impossible travel is simple. If the same user connects from two different countries and the time between those connections can't be made through conventional air travel, it's impossible travel.

SUSPICIOUS MAIL FORWARDING CONFIGURATION

Threat actors can use compromised user accounts for several malicious purposes, including reading emails in a user's inbox, forwarding emails to external recipients, and sending phishing emails, among others. The targeted user might be unaware that their emails are being forwarded. This is a very common tactic that attackers use when user accounts are compromised.

ACCESS ACTIVITY

Threat actors will often need access to systems not available or unused by the accounts they have compromised. Novel or unauthorized access to applications, files, or data can be a key indicator of a compromised account.

PERMISSION CHANGES

Threat actors will often need to change, add or alter the permissions for the compromised account or others. Permission changes can include being granted high-level privileges, additional mailbox access, creating new accounts, MFA disengagement, and others.

ACCOUNT ISOLATION

When an account is compromised and accessed by a threat actor, its access must be shut down immediately. Account Isolation allows ThreatOps to disable an account and log them out from all applications or devices.

THREATOPS 24/7 SOC

Threats can happen at all hours but attackers target off hours and holidays to catch their targets unaware. Huntress 24/7 ThreatOps team of security experts are always reviewing incidents, removing false positives, investigating incidents and providing remediation directions. No more vague alerts.

WESTON
TECHNOLOGY SOLUTIONS