ThreatDown™
Powered by Malwarebytes

Data Sheet

# ThreatDown Managed Threat Hunting

Empower your threat response with 24x7x365 service for alert prioritization and guided remediation

## Overview

Organizations that monitor their own endpoints often suffer from overwhelming volumes of endpoint security alerts, known as alert fatigue. And when combined with a lack of expertise to recognize advanced and emerging Indicators of Compromise (IoC), the result is many alerts that go ignored leading to missed threats and potentially dire security and financial consequences. And the longer intruders are on your network and endpoints, the more time they have to gather reconnaissance and execute their plan to hurt your customers and your business.

ThreatDown Managed Threat Hunting (MTH) is a 24x7x365 service that proactively identifies and prioritizes critical alerts. Using internal and external threat intelligence, MTH discovers events, behaviors, and threats that may be unknown, hidden, or overlooked. When a threat is found, MTH notifies the customer with the details and sends an easy-to-follow, step-by-step set of remediation steps. This information enables IT staff to prioritize and remediate incidents before an active attack can begin. MTH is essential to stop intrusions that can cause the greatest damage.

## ThreatDown MTH Advantages

- **24x7x365 Threat Hunters :** Identify indicators of compromise using internal and external threat intelligence, bolstered by our many years of experience. Our accomplished Threat Hunters are always working even when you're not.
- **Risk Mitigation:** Finds hidden intruders faster as well as reducing dwell time and potential for damage to significantly reduce the risk of a crippling breach.
- **Alert Prioritization:** Cuts through the noise to identify critical alerts that require immediate attention, giving you more control, stronger security, and greater confidence.

## Challenges

- **Limited expertise and resources** - 73% lack skilled staff for threat hunting[1]
- **Lack accurate alert prioritization** - 80% of endpoint security alerts are being ignored[2]
- **Hidden intruders in the network** - 277 days average number of days to identify and contain a breach[3]

## Benefits

- **Empower your respone** - Use our security analysts' experiece and expertise to effectively remediate alerts
- **Prioritize your alerts** - Know which alerts are critical to address first
- **Reduce dwell time** - Remediate quickly with easy-to-follow, step-by-step guidance

[1]2023 SANS Threat Hunting Survey, SANSt [2]ThreatDown Research. [3]Cost of a Data Breach Report 2022, Ponemon Institute.

- **Guided Response :** Notifies customers with step-by-step guidance for easier and faster remediation resulting in time and cost savings.

- **EDR Integration:** MTH is built to optimize the usage of internal and external intelligence in combination with the alerts gathered by ThreatDown Endpoint Detection & Response Integration.

## How Does it Work?

On a recurring basis (both weekly and adhoc), MTH creates a unique dataset within the SOAR system that includes endpoint security alerts enriched with external threat intelligence. MTH creates and deploys a hunt strategy (e.g., search, analytics) for each threat hunt. Hunting strategies may include searching for evidence in the early or late stages of an intrusion that follows MITRE's seven stage ATT&CK lifecycle. For example, a search may focus on IOC in the internal reconnaissance or lateral movement stages. Recent threat intelligence may form new hypotheses which will be used to influence the hunt strategy for a particular session. Once the search is executed and discovers IOC that match the hunt criteria; a notification, including a link to the EDR alert, is sent to the customer along with guided remediation content specific to the detected IOC detected. The customers follows the step-by-step instructions to address the IoC.

## ThreatDown's Industry Accolades

Consistent top ranking of Level 1 certification in MRG Effitas 360 degree testing and #1 Endpoint Security Suite by G2 validates ThreatDown's effective and easy-to-use solution.


## Learn More

To learn more about how ThreatDown MTH can help enhance security and reduce costs, please visit www.threatdown.com/mth



Copyright © 2024, Malwarebytes. All rights reserved. Malwarebytes, the Malwarebytes logo, ThreatDown, and the ThreatDown logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind. 04/24