MANAGED DEFENSE THREAT HUNTING

As part of the Managed Defense service offering, Managed Defense analysts perform hunting missions throughout your environments. Hunting missions may be regularly performed (such as checks for commonly used threat vectors by attackers) or ad hoc (for instance, a specific response to a new emerging threat). Hunting mission entails collecting a subset of data from available endpoint agents in the field and then using techniques a hypothesis to analyze the data for locating malicious activities and also evolve detection capabilities as attacker TTPs change.

> Hunting on specific host sets in your environment is possible, but not done by default. Contact your assigned Managed Defense Consultant (MDC) if you would like to implement hunting in this way.

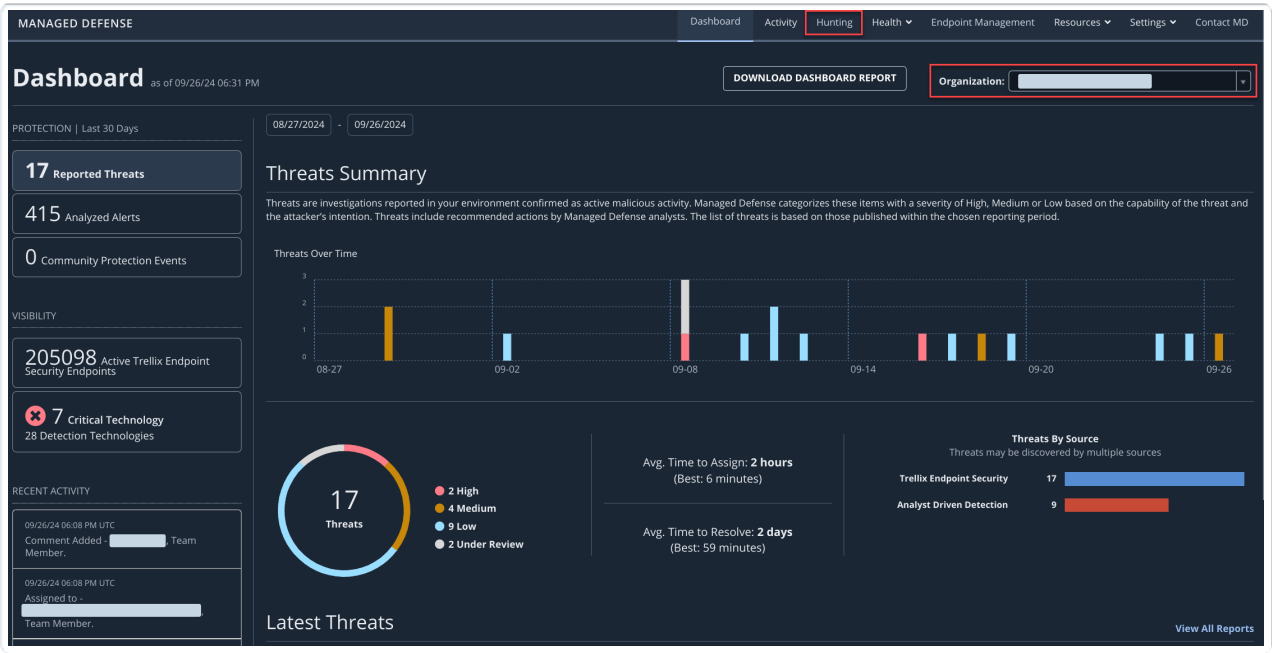
Hunt Overview

Mission Based Hunting results can be viewed on the **Hunting** page. To go to **Hunting** from the main **Dashboard** page:

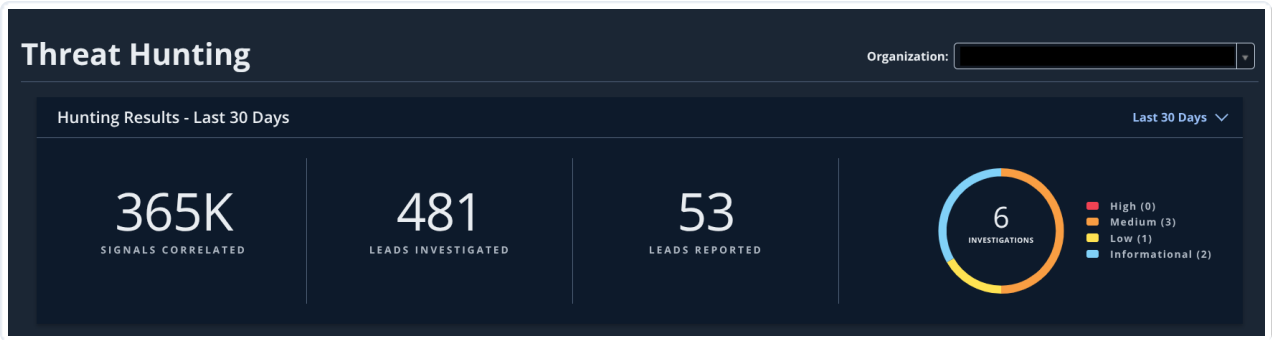
1. Select an **Organization** from the list.

   > Selecting an organization is only required if your Managed Defense account has multiple organizations.

2. Click **Hunting** in the navigation header.



The **Threat Hunting** dashboard shows an overview of hunting results along with two tabs: **Investigations** and **Missions**.



Hunting Results

The **Hunting Results** overview includes:

- **Signals Correlated**: Shows the number of composite detections generated by correlating logs including the **Mandiant Hunting Rules** (https://docs.cloud.google.com/chronicle/docs/detection/mandiant-hunt-category). This represents the number of unique threat hunting detections or leads that required analyst review. A threat hunting lead consists of one or more related events indicative of suspicious or malicious activity.
- **Leads Investigated**: The number of leads that required a follow-up investigation by Mandiant Threat Hunting analysts. This number does not include leads that Mandiant determined were not a threat without a full investigation.
- **Leads Reported**: The investigation reports published by Mandiant Threat Hunting analysts based on their review of the threat hunting leads. Mandiant does not publish investigation reports for **Leads Investigated** that analysts determined were not a threat.
- **Investigations by severity**: A graph of the investigations published categorized by the severity assigned by Mandiant Threat Hunting analysts

You can filter **Hunting Results** by selecting a date range. By default, this is set to the **Last 30 Days**.

MITRE ATT&CK® Tactics Filter

The **MITRE ATT&CK® Tactics** matrix is a visualization tool to filter forensic data gathered during adversary's different tactical objectives for performing an attack. This matrix is available on both the **Investigations** and **Missions** tabs. As per the **MITRE ATT&CK® Matrix** (https://attack.mitre.org/), this matrix is divided into a number of categories:

- **Initial Access**
- **Execution**
- **Persistence**
- **Privilege Escalation**
- **Defense Evasion**
- **Credential Access**
- **Discovery**
- **Lateral Movement**
- **Collection**
- **Command & Control**
- **Exfiltration**
- **Impact**

Each tile in this matrix represents a corresponding **MITRE ATT&CK® tactic (https://attack.mitre.org/tactics/enterprise/)** and contains information about the number of forensic evidences identified in that adversary's attacking phase during hunting.

Investigations

The table of **Investigations** includes the following fields:

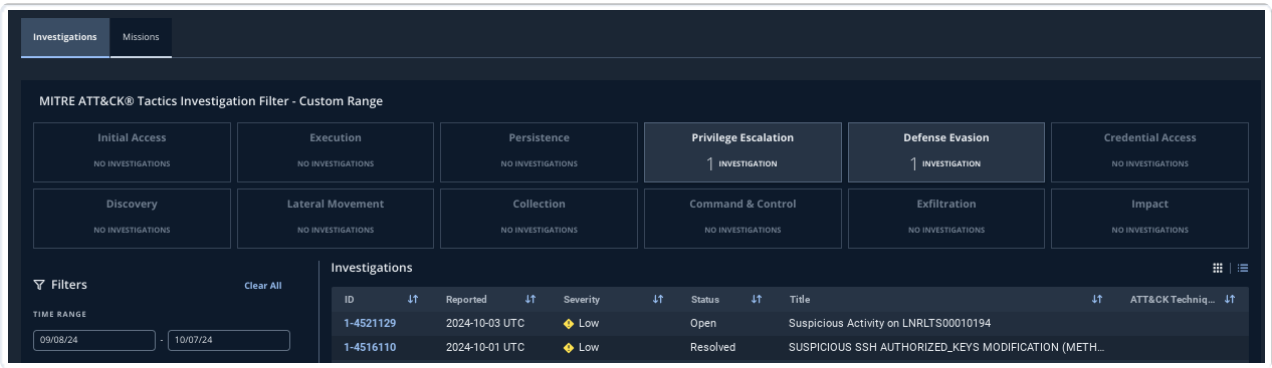
- **ID**: A link to the published Investigation report
- **Reported**: The time when the malicious activity was found
- **Severity**: The severity level of the IOCs detected
- **Status**: The current status of the Investigation
- **Title**: The title of the Investigation report
- **ATT&CK Technique**: The ATT&CK technique used in the Investigation

To sort Investigations listed in the table, click the navigation arrows associated with a column header.

You can filter Investigations using the following filters:

- **MITRE ATT&CK® Tactics Investigation Filter - Custom Range matrix**
- **Time Range**
- **Severity**
- **Status**

Click **Clear All** to remove filters.



Missions

Navigate to the **Missions** tab to see all the current hunting missions. The table of **Missions** includes the following fields:

- **Mission Name**
- **Platform**
- **Description**
- **ATT&CK Technique**

To sort Missions listed in the table, click the navigation arrows associated with a column header. To search for missions, use the **Search missions** option. keywords can be associated with any of the column headers. To filter missions, click a tile on the **MITRE ATT&CK® Tactics Mission Filter matrix**.

Click a **Mission Name** to see detailed information about that mission. Click an **ATT&CK Technique** to open MITRE

ATT&CK® information specific to that technique.