Mandiant

MANDIANT THREAT DEFENSE HUNTING DASHBOARD

Mandiant Threat Defense dashboard is designed to provide you with the information you require to track your Mandiant Threat Defense subscription service metrics and act on Investigations.

Mandiant Threat Defense uses the customer Google Security Operations (SecOps) instance as the telemetry source and the hunt outcomes (reports, dashboards) are available on the **Threat Hunting page in the Mandiant Managed Defense portal (https://md.mandiant.com/threat_hunting)**. Threat hunting in Mandiant Threat Defense uses ingested data from Google SecOps in the form of a **Unified Data Model (UDM) (https://cloud.google.com/chronicle/docs/event-processing/udm-overview)**.

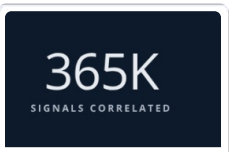
Threat Hunting Overview

The Mandiant Threat Defense dashboard lets you quickly access summary information, information about any threat-related activity, including threat hunting missions and Investigations. You can view the status updates for your Mandiant Threat Defense service components in real-time. The dashboard shows aggregated **Hunting Results** for the selected date range which can be selected from:

- `Last 30 Days`
- `Last 60 Days`
- `Last 90 Days`
- `Last 120 Days`
- `Last Year`

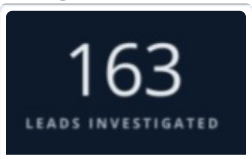
The aggregated hunting results include:

- **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.



Signals Correlated

- **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 Investigated

- **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.

Leads Reported

- **Investigations** Pie Chart: Shows **Investigations** based on the severity assigned by Mandiant Threat Hunting analysts.

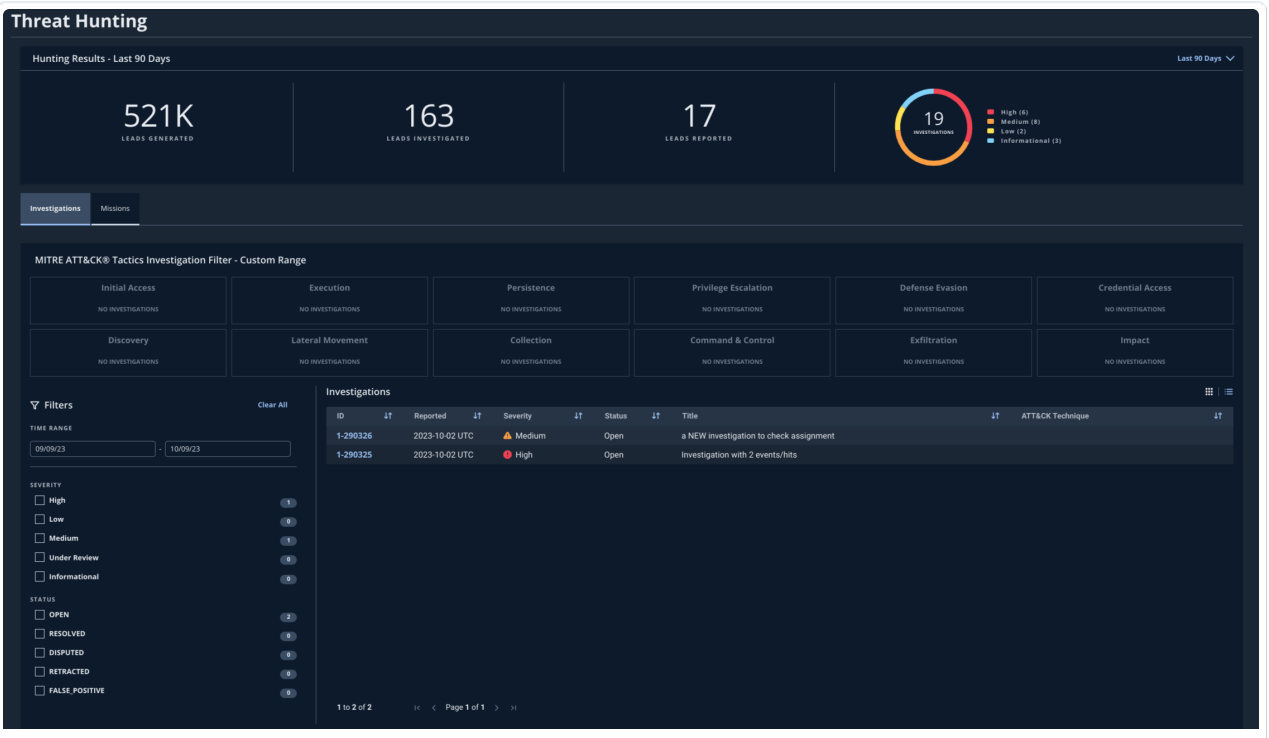
Investigations by Severity Pie Chart

In addition, there are two tabs:

- **Investigations**
- **Missions**

Investigations

In this tab, you can view the progress of threat hunts and related Investigations in your environment.



Hunting Investigations

There are two views for the Investigations:

- **Card View**: Card View lets you view Investigations as discrete objects, the contextual information always being displayed with the header information in every cell. An example:

Card View

- **Table View**: Table View lets you see information about Investigations in rows, referencing the header when needed. An example:

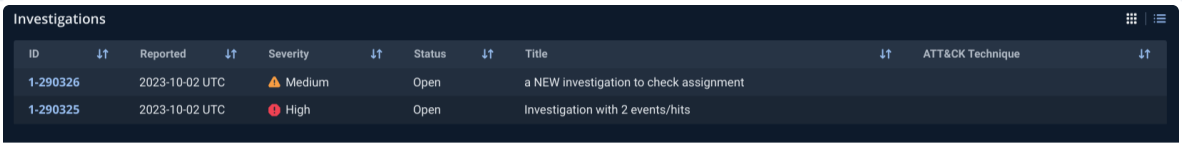


Table View

The default view for Investigations is the card view, but based on your preference, you can toggle the views ( ) as needed. The table view shows fields including:

- **ID**: Investigation identifier, by selecting the ID, you can view the published Investigation report
- **Severity**: Severity level of IOCs detected:
  - **High**
  - **Low**
  - **Medium**
  - **Below the average Review**
  - **Informational**
- **Reported**: Time when the malicious activity is found
- **Title**: Title of the Investigation report
- **ATT&CK Technique**: **MITRE ATT&CK® Technique (https://attack.mitre.org/techniques/enterprise/)** used in the Investigation
- **Status**: Status of Investigation:
  - **Open**: The Investigation is awaiting analyst assignment.
  - **Resolved**: The Investigation is resolved.
  - **Disputed**: There is a disagreement about the Investigation.
  - **Retracted**: The Investigation is withdrawn.
  - **False Positive**: The Investigation is a false positive.

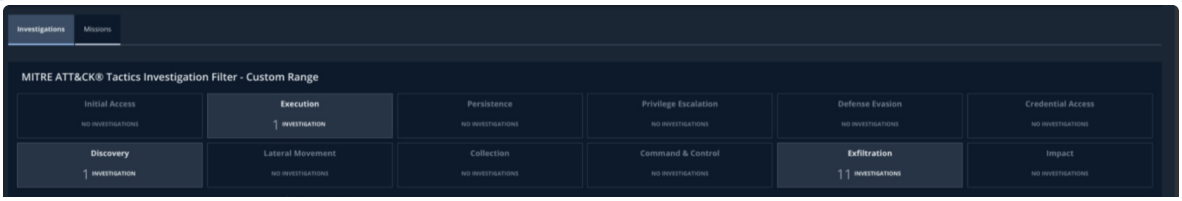
You can sort individual fields in either ascending or in descending order. Selecting a technique in the table view leads you to the respective MITRE ATT&CK® Technique.

Investigation Filters

You can filter Investigations by:

- **MITRE ATT&CK® Tactics (https://attack.mitre.org/tactics) Investigation Filter**: The MITRE ATT&CK® Tactics Investigation Filter highlights the tactics used in the current set of Investigations. The total number of Investigations using the tactic is also displayed. For example, in the sample **MITRE ATT&CK® Tactics Investigation Filter** image, there is one Investigation with the **Execution** tactic, one Investigation with the **Discovery** tactic, and 11

Investigations with the **Exfiltration** tactic. These highlighted tactics can be selected for further filtering of Investigations.

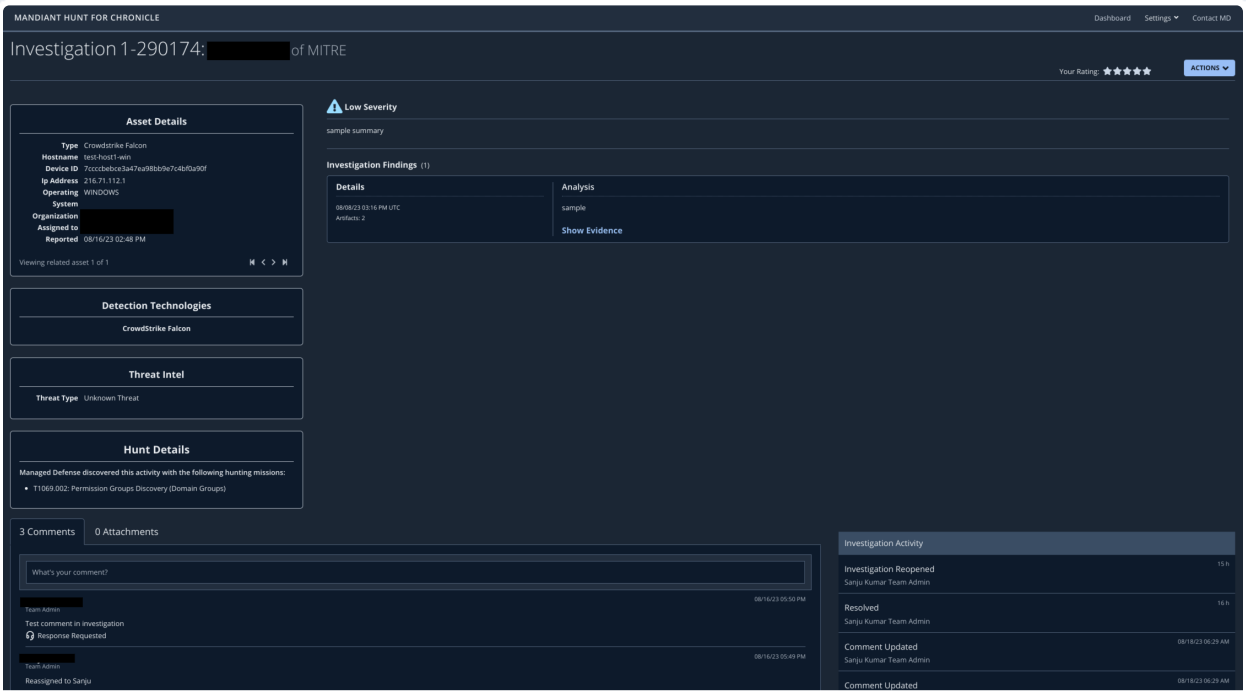


MITRE ATT&CK® Tactics Investigation Filter

- **Date**, **Severity**, and **Status**: These filters let you narrow down the Investigations based on:
  - A customized date range (the default setting is for a one-month range)
  - Selected severity values
  - Selected status values

Investigation Reports

To access the Investigation report page, select either a single Investigation from the **card view** or an **ID** from the **table view**. On this page, you have multiple panes displaying *Asset Details*, *Detection Technologies*, *Threat Intel* (associated, if any), *Hunt Details (associated, if any)*, and *Investigation Findings* with Evidence.



Investigation Report

Furthermore, on the **Investigation report** page, you have access to Investigation *Comments*, *Attachments*, and the current state of the *Investigation Activity* record. By selecting the **Actions** menu option in the Investigation report page, you can assign the Investigation to your team member, export it to a PDF file, or close the Investigation.

In the investigation details section, you find the **View In Google SecOps** button. You can navigate to your Google SecOps Investigations view filtered down to the events associated with the report by clicking this button.

Mandiant

Only evidence with a Google SecOps `metadata.id` field is available to view in Google SecOps.

Investigation Evidence

Selecting **Show Evidence** on the **Investigation Findings** pane displays the evidence fields, which include *Artifact Type*, *Artifact Source*, *Timestamp*, and metadata attributes.

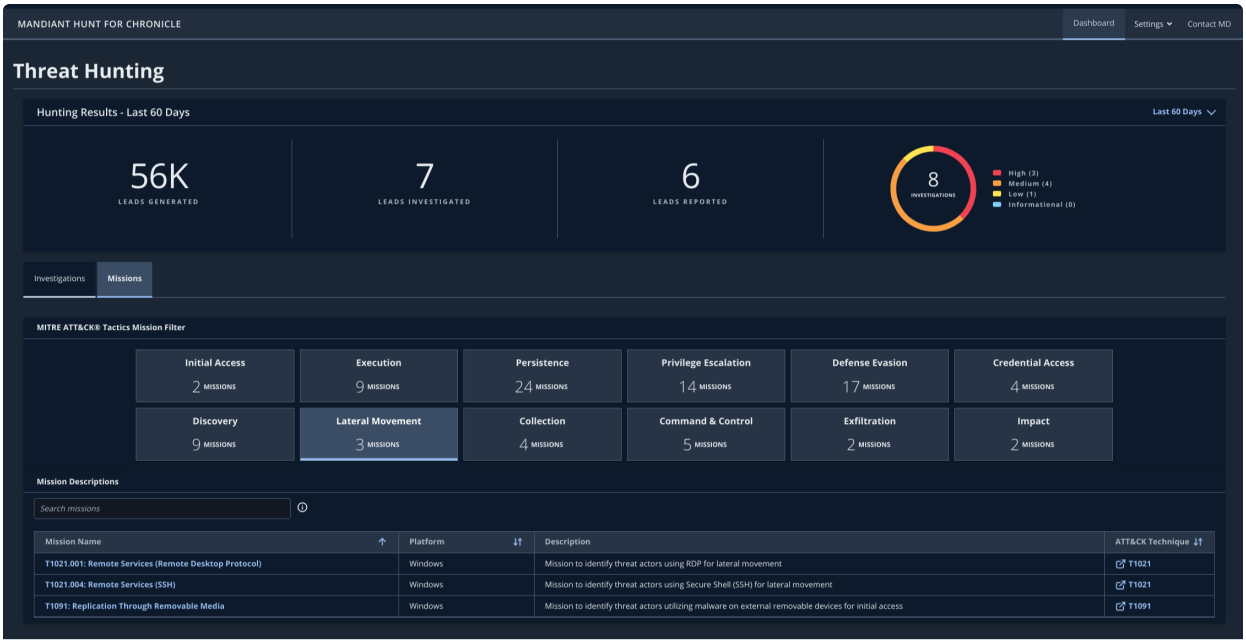
Investigation Evidence Details

Examples of artifacts collected as evidence during a hunting mission include:

- Evidence of process execution on the endpoint (for example, Application Compatibility Cache, Windows Prefetch metadata, Linux Shell History).
- Network metadata (for example, Packet capture, Net flow, HTTP/TLS/DNS data).

Missions

Hunting Missions are curated collection techniques based on Mandiant front-line intelligence which are not instrumented in standard detection technology. Hunting Missions are designed to label security relevant data. The labeled data is analyzed separately and correlated with other labeled data to generate leads that are reviewed by analysts for further Investigation. Labeled hunting telemetry is not expected to be suspicious at the event level, but when correlated together, many weak signals may indicate activity that warrants further Investigation.



Hunting Missions

The **Missions** tab displays the hunting missions within your environment and they are associated with MITRE ATT&CK® Techniques. You can filter the missions using the **MITRE ATT&CK® Tactics Mission Filter**. For example, after selecting the **Lateral Movement**, the **Hunting Missions** screenshot displays three missions with the following fields:

- **Mission Name**
- **Platform**
- **Description**
- A link to the **ATT&CK® Technique**

You can view the mission details by selecting the **Mission Name**. An example:

Mission Details

The **MITRE ATT&CK® Tactics Mission Filter** highlights all available MITRE ATT&CK® tactics and with the aggregated number of missions available. Selecting each tactic category displays the available missions and their descriptions.

You may search missions by mission name, attack technique number, or description.