Mandiant

HOW MANDIANT THREAT DEFENSE USES CURATED DETECTIONS

Curated detections (https://cloud.google.com/chronicle/docs/detection/curated-detections) are YARA-L rules that are maintained by Google. They are used to identify, prioritize, and hunt for threats and other events across data in your Google Security Operations (SecOps) instance. Mandiant Threat Defense uses curated detections in both broad and precise mode. It does not require any rules to be in alerting mode.

Access curated detection rule sets

1. In Google SecOps, go to **Detection > Rules and Detections**.
2. To view and manage the underlying Curated Detection Rule Sets, select **Rule Sets**. The vendor alerts appear.

Detection strategy

Mandiant Threat Defense uses a tiered approach to monitor for evidence of security events or attacks in the data integrated into your Google SecOps instance. Data is labeled for security relevant context and then classified, clustered, and prioritized for analyst triage and investigation.

See the following visualization for how Mandiant Threat Defense uses the data within Google SecOps:

The detection strategy consists of two stages of attack identification and classification, followed by two stages of investigation and response:

- **Identification:** The identification stage uses curated detections to apply security context to all data from supported technology integrations such as Endpoint detection and response, network detection and response, cloud, and OT sources. An event that receives one or more identifications during this stage may not be reviewed by the security operations or threat hunting teams.
- **Classification:** The classification stage correlates the events from the identification stage and assigns a priority. Composite detections or multi-event rules are typically used in this stage to correlate the identified events. This stage determines which detections require analyst review.
- **Triage and Investigate:** Mandiant Threat Defense analysts receive the prioritized output from the correlation stage and perform an initial triage and investigation. If the activity is not assessed as malicious, the analyst closes the detection. If the activity is a true positive indicating an attack or requiring further investigation, an analyst creates an investigation report.
- **Report and Remediate:** The reporting and remediation stage is for detections that represent malicious activity or require additional follow-up by your team. A Mandiant Threat Defense analyst will publish an investigation report with their assessment and findings and provide remediation recommendations or take remediation actions on the affected systems, as permitted.

Curated Detection requirements

To enable the detection strategy, the following rule sets should be enabled on a customer's Google SecOps instance for Mandiant Threat Defense service:

Rule Set	Rules	Precise	Broad	Alerting
Mandiant doesn't monitor vendor alerts. Instead, a Mandiant Threat Defense rule pack is used for specific technologies.				

Rule Set	Rules	Precise	Broad	Alerting
Applied Threat Intelligence	• Active Breach Priority Host Indicators • Active Breach Priority Network Indicators	Enabled	Off	Optional
Cloud Threats	All Applicable	Enabled	Enabled	Optional
Composite Rules	All Applicable	Enabled	Enabled	Optional
Linux Threats	All Applicable	Enabled	Enabled	Optional
macOS threats	All Applicable	Enabled	Enabled	Optional
Mandiant Hunting Rules	All Applicable	Enabled	Enabled	Off
Windows Threats	All Applicable	Enabled	Enabled	Off
Vendor Alerts	All Applicable	Enabled	Off	Optional, but recommended to remain off[1]

[1] Mandiant doesn't monitor vendor alerts. Instead, a Mandiant Threat Defense rule pack is used for specific technologies.

Rules are applicable based on the data source integrated into your Google SecOps instance. For example, if you do not have logs from your cloud environment integrated into Google SecOps, then you do not need to enable the rules related to cloud threats.

Mandiant Threat Defense provides support for all curated detections in Google SecOps. The table above represents the minimum rule sets that must be enabled for service delivery. The effectiveness of the service in detecting threats in your organization depends on enabling the appropriate curated detections in your Google SecOps instance.

Log sources that are monitored, triaged, and investigated

Depending on the telemetry you have in your Google SecOps instance, you should enable the curated detection rule sets for Cloud Threats, Windows Threats, and Linux Threats in both broad and precise mode. Mandiant Threat Defense also gives you access to the **Mandiant Frontline Threats** rule set, which includes Mandiant Threat Hunting rules.This rule set must be enabled in broad mode for the Mandiant Threat Defense Threat Hunting service.

You can also choose to enable some of the precise rules in alerting mode.

> Precise mode detections not set to alerting don't generate alerts in the Google SecOps console, but are still monitored for Mandiant Threat Defense service delivery. Broad rules generate signals for threat hunting and should not be set to alerting mode.

Example log sources

As customers integrate new telemetry sources into Google SecOps, the log data becomes available to Mandiant Threat Defense, if matched to an alert generated by a curated detections rule pack.

The following list is non-exhaustive and shows examples of expanded log sources matched through curated detections:

- AWS CloudTrail
- AWS GuardDuty
- Azure Activity
- Azure Active Directory Audit
- Chrome Management
- Elastic Winlogbeat
- Google Cloud Security Command Center Threat
- Google Cloud Cloud Audit
- Google Cloud Firewall
- Google Cloud DNS
- Google Cloud Load Balancing
- Google Cloud Run
- Google Cloud Security Command Center Observation
- Google Cloud Cloud SQL
- Kubernetes Node
- Linux Audit Daemon (Auditd)
- Microsoft Internet Information Services (IIS)
- Nix System
- Workspace Activity
- Windows System Monitor (Sysmon)
- Windows Event Log (winevtlog)

Customers are responsible for monitoring, triaging, and investigating alerts that are not covered by curated detections for Mandiant Threat Defense. Mandiant Threat Defense supports native detection content.

Composite rules

Mandiant Threat Defense monitors **composite rule (https://cloud.google.com/chronicle/docs/detection/composite-rules-category)** detections from your Google SecOps instance. These rules correlate findings from multiple detection rules that relate to the same endpoint over a defined time period. Confidence and risk levels are determined by specific characteristics of those detections.

You must enable composite rules in your Google SecOps instance. These rules provide improved correlation and enable enhanced accuracy in the prioritization of events.

Vendor alerts

Google SecOps has introduced a curated detection rule set for vendor alerts. These rules identify alerts from specific security technologies integrated into Google SecOps and create detections from these events. Once an event has been prioritized for triage by the detection strategy, it can be monitored by Mandiant Threat Defense or added to a case within SOAR. Further details about this rule set are available in the **curated detection rules documentation (https://cloud.google.com/chronicle/docs/detection/third-party-vendor-alerts-category)**.

Mandiant Threat Defense uses the Vendor Alerts to identify alerts from supported vendor security detection technologies integrated with Google SecOps. Detections from these rules are prioritized for review by Mandiant Threat Defense security analysts.

Custom detections

Mandiant Threat Defense does not yet support monitoring of custom detections (live rules).

- The Vendor Alerts rule pack uses slightly modified versions of the rules in the Third Party Vendor Passthrough Rules rule pack with aggregation criteria specific to Mandiant Threat Defense.
- If you disable curated detections on an instance with Mandiant Threat Defense, you will not receive service.