

# Mandiant Threat Defense

## Service Highlights

- AI-assisted hunting performed by Mandiant frontline experts
- Unparalleled visibility of threat actor activity and tactics through Google Threat Intelligence
- Expert alert triage, investigation, and prioritized escalation with curated recommendations.
- Seamless monitoring for telemetry integrated into Google SecOps and technology partner products

## *Comprehensive active threat detection, hunting, and rapid response backed by Mandiant experts*

Mandiant Threat Defense supercharges your security with active threat detection across Google SecOps. Combining the power of AI with the expertise of Mandiant, our team rapidly converts intelligence from incident response engagements into an advanced detection pipeline of curated detection content, Mandiant experts efficiently identify and prioritize critical security cases, enabling rapid response and faster threat mitigation. Working alongside your team or MSSP partner, Mandiant experts maximize the power of Google SecOps and Gemini to operate at scale and speed, and operationalize frontline intelligence in real time.

## Save time and augment your security operations with Mandiant experts

Mandiant experts actively monitor your environment, crafts targeted threat hunts, and responds with expert-led investigations and remediation recommendations. Gain executive-level insights via native reporting and extend your team with personalized guidance.

### **Comprehensive Active Threat Detection**

All security data sources supported by Google SecOps, including 3rd party alerts, can be evaluated through applied threat intelligence, threat hunts, and curated detection rule packs.

### **AI-Assisted, Continual Threat Hunting**

Mandiant experts leverage security models trained on Google Threat Intelligence and attacker behavior observed in Mandiant incident response engagements to automatically create and execute threat hunting missions.

### **Effective Prioritization**

We respond to threats with expert-led investigations and scaled SOAR playbooks, leveraging Gemini for enhanced remediation recommendations.

### **Native Reporting**

Executive-level SOC reporting available directly within Google SecOps.

### **Expert-led and Automated Response**

Our team will respond to threats on your behalf, with a combination of expert-led investigations and scaled response through SOAR playbooks.

### **Expert Mandiant Support**

Mandiant experts help maximize your Google SecOps investments with personalized threat briefings, tuning suggestions, and remediation guidance, acting as an extension of your security team.

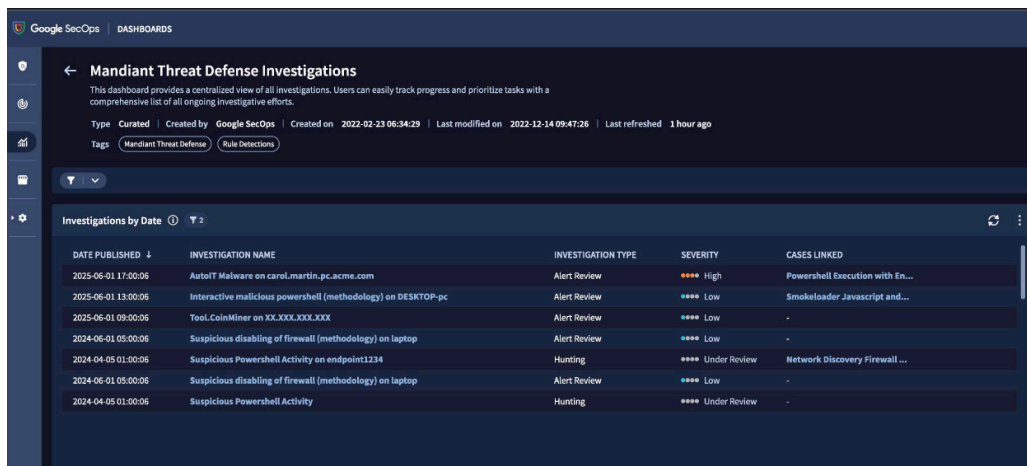
## Support for curated detections

Through the curated detections available within Google Security Operations, Mandiant Threat Defense can review an expanded set of log sources while performing triage and initiating investigations. As customers integrate new telemetry sources into Google Security Operations, the log data will be parsed into the Security Operations Unified Data Model and curated detection rules will be applied. Alerts that are generated by these rules become available to Managed Defense for triage investigation.

Curated detections coverage is dependent on a customer's [Google SecOps license](#).

## About curated detections

The Google Threat Intelligence (GCTI) team provides and manages a set of YARA-L rules to help customers identify threats to their enterprise. These predefined rules are called [curated detections](#). Curated detections can be enabled within a customer-owned Google Security Operations instance.



DATE PUBLISHED	INVESTIGATION NAME	INVESTIGATION TYPE	SEVERITY	CASES LINKED
2025-06-01 17:00:06	AutoIT Malware on carol.martin.pc.acme.com	Alert Review	High	Powershell Execution with En...
2025-06-01 13:00:06	Interactive malicious powershell (methodology) on DESKTOP-pc	Alert Review	Low	Smokeloader Javascript and...
2025-06-01 09:00:06	Tool.CoinMiner on XX.XXX.XXX.XXX	Alert Review	Low	-
2024-06-01 05:00:06	Suspicious disabling of firewall (methodology) on laptop	Alert Review	Low	-
2024-04-05 01:00:06	Suspicious Powershell Activity on endpoint1234	Hunting	Under Review	Network Discovery Firewall ...
2024-06-01 05:00:06	Suspicious disabling of firewall (methodology) on laptop	Alert Review	Low	-
2024-04-05 01:00:06	Suspicious Powershell Activity	Hunting	Under Review	-

Figure 1: Mandiant Threat Defense investigations will be available through Native Dashboards in Google SecOps.

## Technology partnerships

The Mandiant Threat Defense service is most effective when a broad set of security telemetry sources are integrated into Google SecOps. Customers are empowered to use the available default [Google SecOps parsers](#) to streamline alert and event ingestion.

Customers can also benefit from using Mandiant Threat Defense Technology Partner products. The partnership agreements facilitate deep collaboration between the Managed Defense team and the vendor that can allow for deeper response and orchestration actions to be taken on behalf of customers. For example, host containment and file acquisition.

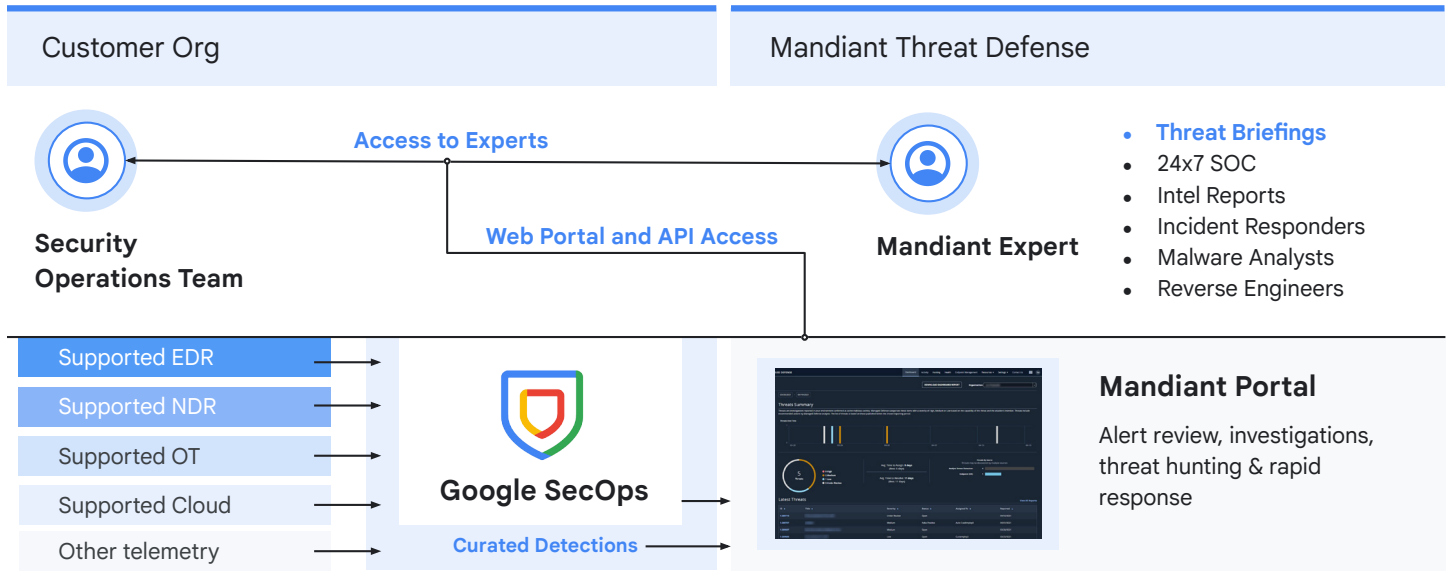


Figure 2: Sample architecture of Mandiant Threat Defense.

## Explore Mandiant Threat Defense supported technology partners

Category	Vendor	Products Supported	Product License Requirements	Required SecOps Parsers
Endpoint detection and response (EDR)	CrowdStrike	Falcon Insight XDR	Falcon Data Replicator	Alerts: CS_DETECTS Telemetry: CS_EDR
	SentinelOne	Singularity XDR	Cloud Funnel	Alerts: SENTINELONE_ALERT Telemetry: SENTINELONE_CF
	Microsoft	Defender for Endpoint	Microsoft Defender for Endpoint Plan 2 Azure Blob Storage	Alerts: MICROSOFT_GRAPH_ALERT Telemetry: MICROSOFT_DEFENDER_ENDPOINT
Identity	Microsoft	Defender for Identity	One of the following: Endpoint Plan 2 Defender for Business Defender for Identity license	Alerts: MICROSOFT_GRAPH_ALERT
Network detection and response (NDR) and Firewall	Corelight	Open NDR	N/A	Alerts and Telemetry: CORELIGHT
	Palo Alto Networks	Next-Generation Firewall	N/A	Alerts and Telemetry: CORELIGHT