**Google Cloud**

# Security

# Mandiant Managed Defense for Google Security Operations

**Strengthen your security operations with 24/7 managed detection and response from Mandiant.**

Mandiant Managed Defense delivers expert-led managed detection and response (MDR) capabilities on top of the AI-infused Google SecOps platform, enriched with unmatched threat intelligence, for 24x7x365 peace of mind and confidence that your organization is ready to defend against adversaries.

Mandiant's team of seasoned defenders, analysts, and threat hunters work seamlessly with your security team and the capabilities of Google SecOps to quickly and effectively monitor, detect, triage, investigate, and respond to incidents, reducing risk to your organization.

## Service Highlights

- Human-led hunting performed by Mandiant frontline experts

- Unparalleled visibility of threat actor activity and tactics through Google Threat Intelligence

- Seamless monitoring for Corelight Open NDR, Crowdstrike Falcon Insight XDR, SentinelOne Singularity XDR, Microsoft Defender for Endpoint, and Palo Alto Next-Generation Firewall (Public Preview)

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

Mandiant Managed Defense supports threat hunting, alert triage, investigation, and rapid response capabilities for Google Security Operations customers.

**+ Enhance your critical security technologies with Mandiant expertise**

Get 24x7x365 monitoring across your alert and event data in Google SecOps. Managed Defense experts use curated response playbooks to contain impacted hosts and files, investigate security incidents quickly, and provide actionable remediation guidance.

**+ Take a decisive, intelligence-led approach**

Quickly identify multifaceted threat actors with the help of Mandiant experts to help protect your business from extortion, ransom, downtime, and data theft using in-depth knowledge about attacker behavior and the results of Google SecOps' applied threat intelligence.

**+ Expose hidden adversaries with proactive threat hunting**

Quickly find anomalies to help reduce attacker dwell time in your environment with threat hunting at the speed and scale of Google. Mandiant hunters proactively refine and adapt hunt scenarios based on insights from Google Threat Intelligence, and map the results to the MITRE ATT&CK Framework.

## Let Mandiant be your trusted security advisor

Since 2011, Mandiant Managed Defense has been helping customers detect, respond, and mitigate threats. Together, with our customers we learn and adapt from previous incidents and augment security operations with intelligence and AI to enhance Google Cloud Security tools and empower defenders to anticipate and prevent future attacks. Managed Defense provides dedicated experts to complement and supplement internal security teams to provide 24x7x365 security threat monitoring to uncover malicious activity with support for their preferred endpoint, network, OT, and cloud providers.

### Customer Benefits

- Augment your security team's skills with Mandiant expertise

- Find actionable incidents in real time

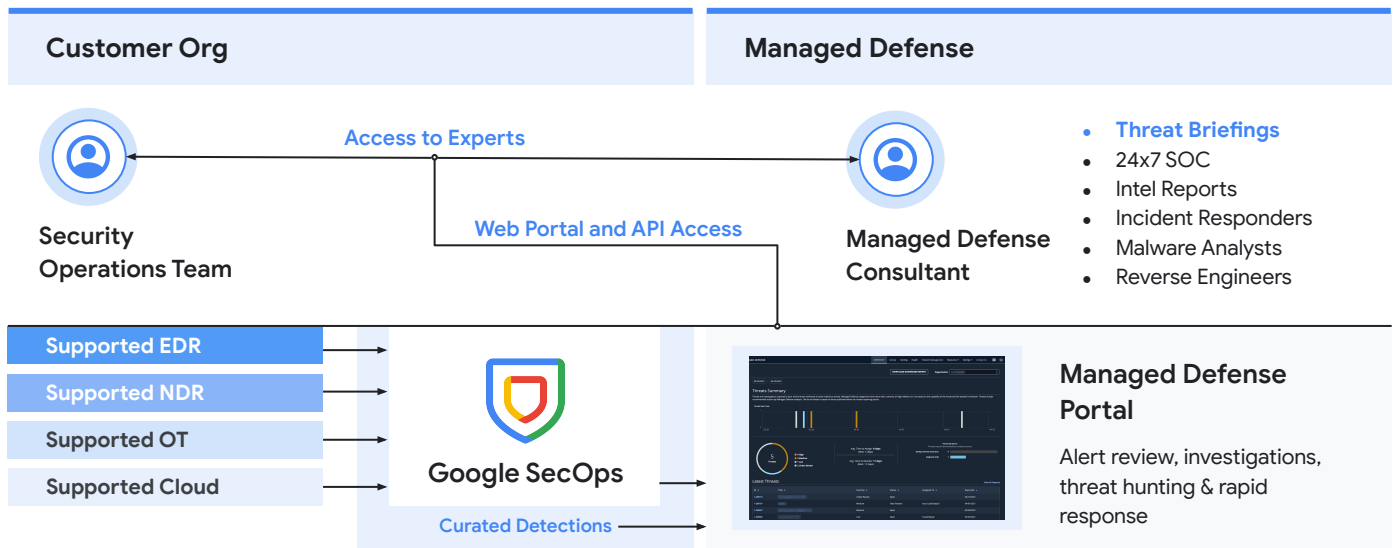- Accelerate containment and remediation of threats

### Customer Org

### Managed Defense

**Security Operations Team**

**Access to Experts**

**Web Portal and API Access**

**Managed Defense Consultant**

- **Threat Briefings**
- 24x7 SOC
- Intel Reports
- Incident Responders
- Malware Analysts
- Reverse Engineers

Supported EDR
Supported NDR
Supported OT
Supported Cloud

**Google SecOps**

**Curated Detections**

**Managed Defense Portal**

Alert review, investigations, threat hunting & rapid response

Figure 1: Sample architecture of Managed Defense for Google Security Operations

## Make Google part of your security team.

Learn more about **Mandiant Managed Defense**.