Mandiant Managed Defense support for Corelight Open NDR

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

Mandiant Managed Defense provides continuous, 24/7 threat detection and response for Corelight Open NDR customers. This integration empowers your organization to proactively identify and mitigate threats on the network before they cause harm.

Managed Defense enables organizations with Mandiant's advanced security expertise, including attacker behavior analysis, proactive threat hunting, and rapid incident response. By leveraging EDR alerts, Corelight logs, and world-class threat intelligence within Google Security Operations, we uncover hidden threats and keep your business secure.

Service Highlights

- Human-led hunting performed by Mandiant experts

- Unparalleled visibility of threat actor activity and tactics through Mandiant frontline intelligence and VirusTotal

- Comprehensive, expert monitoring across the network and endpoint

Save time and augment your security operations with Mandiant experts

Mandiant Managed Defense supports threat hunting, alert triage, investigation, and rapid response capabilities for Corelight Open NDR customers.

➕ Enhance your critical security technologies with Mandiant expertise

Corelight enhances network visibility across hybrid, multi-cloud, and distributed environments and OT devices, while Managed Defense offers threat transparency and expert detection, investigation and response, empowering your team to effectively mitigate threats.

➕ Take a decisive, intelligence-led approach

Reduce the business impact of extortion, ransomware, downtime, and data theft by leveraging Mandiant's expertise combined with Google SecOps' applied threat intelligence and Corelight's comprehensive, high-fidelity network telemetry for rapid identification of multifaceted attacks.

➕ Expose hidden adversaries with proactive threat hunting

Reduce attacker dwell time and expose both known and novel threats with Mandiant's expert threat hunters, leveraging Google's speed and scale to proactively identify anomalies and hidden threats in your network. Mandiant hunters proactively refine and adapt hunt scenarios based on insights from frontline 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

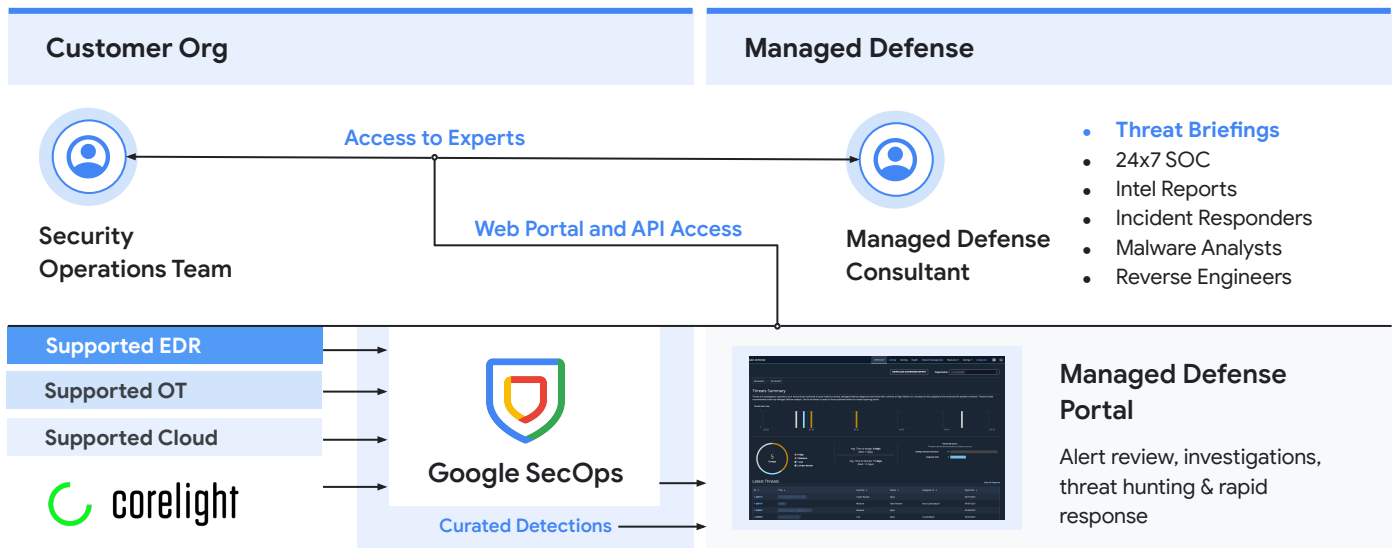- Accelerate containment and remediation of threats

Figure 1: Sample architecture of how Corelight is supported by Managed Defense for Google Security Operations

Make Google part of your security team with Mandiant frontline experts, intel-driven security operations, and cloud security—supercharged by AI. Contact us.

https://cloud.google.com/contact/security

To learn more about Corelight for Google Cloud Security, request a demo.

info@corelight.com | 888-547-9497

https://corelight.com/contact