

Custom Threat Hunt

Key Benefits

- Detailed analysis of your environment—focused on finding evidence of ongoing or past compromises
- Targeted analysis—tailored to the particulars of your technology stack and the threats targeting you
- Identification of opportunities to further your organization’s ability to effectively detect and respond to future threats
- Documented threat hunt hypotheses, context, and analysis to jumpstart your own threat hunting program

Uncover ongoing or past threat actor activity in your environment while improving your ability to effectively detect future threats.

Enterprise networks are a complex mix of on-premises, cloud-based workloads, and SaaS applications. This challenging complexity requires security teams to become experts at monitoring diverse data sources for a continually evolving set of threats. Threat actors, in turn, have become increasingly adept at targeting areas where traditional security tools can fall flat, such as living off the land tools and legacy devices.

Mandiant provides threat hunting customized to your threat profile and the complexities of your environment to search for specific threats and assess if you have the capabilities to detect those threats.

How It Works

Mandiant performs context-driven threat hunting. Prior to forming any hypotheses to hunt for, we gather an understanding of your organization’s IT architecture, current security controls, toolset, and availability telemetry. By combining this context with Google leading threat intelligence capabilities and Mandiant experience responding to incidents, we can identify high impact attacker techniques that are actively used in the wild to hunt for.

Mandiant consultants will use your organization’s security tools, as well as standalone datasets you provide, to look for evidence of threat actor activity. Our threat hunting activities go beyond atomic indicators such as IP addresses, domains, and hashes. Instead, we gather available data, informed by our discovery of your controls and architecture, to identify patterns of activity that are anomalous or match threat actor tactics.

A threat hunt may discover suspicious activities that require further follow up or it may find that your organization does not have the required data to search for particular threat actor techniques. In these cases, Mandiant will provide guidance for the potential impact of the technique and the steps required to improve the ability to detect it.

Environment discovery workshop	Hunt development	Threat hunt	Read out
<ul style="list-style-type: none"> Meet with technology stakeholders to understand core environment technologies such as security tooling, IAM, Logging, and Cloud. Meet with stakeholders to understand threat profiles and management cyber risk concerns 	<ul style="list-style-type: none"> Identify data sources and systems to focus hunts, based on workshop outcomes Gather relevant TTPs from Google Threat Intelligence Create high impact hunts based on the identified TTPs and the workshop outcomes 	<ul style="list-style-type: none"> Perform threat hunts using existing tooling such as EDR and SIEM Perform hunts over data extracted from other platforms such as SaaS applications Report on any findings of active compromise as it is discovered 	<ul style="list-style-type: none"> Summarize any findings of past or ongoing compromise Include the data queries and methodology used to perform hunts Recommendations to address any visibility gaps and improve detection capabilities






Common Use Cases

Mandiant Custom Threat Hunts are often performed in conjunction with managed detection and response services or to supplement an in-house threat hunting program. Some common use cases for a threat hunt include:

- Increased targeting by specific threat actors in your industry or vertical
- Implementation of new technologies, cloud platforms, or SaaS solutions
- Business partners or supply chain impacted by an incident or breach
- To assess and hunt across newly acquired security tools, log sources, and controls
- Planned or recent mergers and acquisitions (M&A)

Threat Hunt Continuum

Google Cloud Security and Mandiant provide training, custom engagements, and managed services to help address your threat hunting goals.

					
Phase	Train	Design/Build	Assess Program	Execute	Monitor and Execute
	Mandiant Academy: Practical Threat Hunting	Threat Hunt Program Development	Threat Hunt Program Assessment	Mandiant Custom Threat Hunt	Managed Defense Mandiant Hunt
Objective	Understand how to plan and execute a threat hunt.	Develop a threat hunt program with the help of Mandiant experts.	Assess your existing threat hunt program and provide recommendations for improvement.	Uncover ongoing or past threat actor activity in your environment while improving your ability to effectively detect future threats.	24/7 managed detection and response service including IOC and TTP-based hunting on your EDR and NDR telemetry. Continual threat hunting, seamlessly using your Chronicle Security Operations and Security Command Center Enterprise data.