Mandiant

MANDIANT THREAT DEFENSE

Mandiant Threat Defense is a threat detection, investigation and response service that combines the expertise of Mandiant's frontline security analysts and Google Security Operations (SecOps) to help organizations protect against cyber threats.

The Mandiant Threat Defense service includes:

- **Active threat detection**: continuous monitoring of an organization's security data through Google SecOps. Mandiant Threat Defense evaluates all data sources (including third-party alerts) integrated into Google SecOps to identify malicious activity.
- **AI-assisted threat hunting**: Mandiant experts use AI models trained on Google Threat Intelligence and real-world incident response data to proactively hunt for threats that may have evaded other security controls. Hunt leads are validated and investigated by the Mandiant team.
- **Expert-led response**: Mandiant provides expert-led investigations and remediation response of detected security threats.
- **Efficient prioritization**: A proprietary case prioritization model helps security teams focus on the most critical incidents, reducing alert fatigue.

Mandiant Threat Defense is designed to augment an organization's existing security team. This is done by providing expert support and a deeper level of threat intelligence, helping to reduce the time it takes to detect and respond to attacks.

For more details, see:

- The **Mandiant Threat Defense overview** **(https://cloud.google.com/security/products/mandiant-managed-threat-hunting)**
- The **Mandiant Threat Defense datasheet** **(https://services.google.com/fh/files/misc/mandiant_threat_defense-ds_en.pdf)**