MANDIANT
NOW PART OF Google Cloud

MANDIANT ADVANTAGE
DATASHEET

Threat Intelligence

Highlights

For security professionals who must manage threat intelligence

- Situational awareness on threat actors and malware on the rise
- Centralized repository for public known vulnerability descriptions with CVSS and EPSS severity scoring
- Ability to look up public known threat Indicators and embed unique Mandiant indicator confidence score directly into any web page with Browser Plugin

The persistence of modern threat actors requires attention and increased knowledge from all security professionals. With a combination of breach, machine, operational and adversarial intelligence, cultivated by more than 500 experts, across 30 countries and covering 30+ languages, Mandiant offers five use-case based subscriptions providing organizations with up-to-the-minute updated threat intelligence to perform their security tasks faster and with more accuracy.

These subscriptions, offered through Mandiant Advantage, give organizations of all sizes up-to-the-minute, relevant cyber threat intelligence so they can focus on the threats that matter to their business now and take action.

Mandiant Advantage Threat Intelligence Free

Public known threats and vulnerabilities centrally managed

Centralizing and managing threat intelligence is often rated as one of the most time-consuming tasks for security analysts. Mandiant Advantage Threat Intelligence Free offers organizations of all sizes free access to publicly known actors, malware, vulnerabilities. Mandiant Advantage Threat Intelligence Free also provides visibility into threats indicators enriched with the unique Mandiant indicator confidence score as well as public known vulnerability descriptions with Common Vulnerability Scoring System (CVSS) and the more dynamic Exploit Prediction Scoring System (EPSS) severity metrics. Security practitioners are then better equipped to make more informed decisions without added capital or operational spend expenditures.

What's included?

- Global dashboards providing actor, malware and vulnerability activity trends
- Access to Open Source Indicators with Mandiant indicator confidence score
- Open-source intelligence (OSINT)-based vulnerability views and scoring
- News analysis with Mandiant expert judgements and commentary
- Threat intelligence accessible via portal and browser plugin

Benefits

For security analysts, incident responders, security operations managers and intelligence analysts

- **Alert prioritization and triage.** Use up to the minute updated threat intelligence to prioritize and contextualize security event information, reducing alert fatigue and improving overall SOC efficiency
- **Detect hidden threats.** Download indicators and expand your detection tools to uncover threat actors or malware activities that could be lingering unseen in your environment
- **Accelerate response.** Empower security analyst teams with a MITRE ATT&CK based actor behavior insights to understand potential attack progress and help formulate the right response

Mandiant Advantage Threat Intelligence Security Operations

Increase SOC efficiency and effectiveness

Security operations center (SOC) personnel are under a constant barrage of security events requiring continuous attention and manual, laborious investigations. The Mandiant Advantage Threat Intelligence Security Operations subscription offers security analysts and incident responders with up-to-the-minute actor, malware and vulnerability tracking to help them prioritize alerts and understand the attacker, capabilities and motivations behind their threat events. By correlating SOC-generated alerts with Mandiant a well as with OSINT indicators, security teams get direct guidance during triage, investigation and response improving both speed and security effectiveness while reducing overall alert fatigue. Anticipate, identify and respond to threats with more confidence by understanding the current and relevant threat campaigns affecting your industries, regions and peers. The Security Operations subscription also helps security teams with historical detection of emerging cyber threats by providing detailed actor or malware indicators data, made available via Mandiant Advantage as well as the API.

What's included?

- Mandiant Advantage Threat Intelligence Free
- Dynamic actor and malware pivot views with MITRE ATT&CK map, object explorer and indicator downloads
- Access to Mandiant known indicators (IP, Domain, File Hash, URL) with maliciousness scoring metrics
- News analysis with Mandiant expert judgements and commentary
- Quarterly Threat Briefings and basic support (provisioning plus onboarding)
- Real-time visibility into the most active and relevant threat campaigns

Benefits

- **Uncover unknown risks.** Customizable, scalable access to frontline finished intelligence. Identify global threats, outside of your organization's perimeter, powered by Mandiant's breach intelligence
- **Informed cyber defense.** Improve security strategy with a holistic situational awareness of vulnerabilities, threat actors, their activity and potential impact to your business
- **Understand priorities.** Alleviate alert fatigue with instant access to the specific threats that matter to your organization as and when they occur to help prioritize security activities and effectively prevent attacks
- **Reduce threat risks.** Enhance security controls and emulate actor specific tactics during red team exercises

Mandiant Advantage Threat Intelligence Fusion

Comprehensive threat intelligence for the entire security organization

To understand more about their adversaries, security teams are often looking at mountains of public threat information that is often vendor influenced. It can lead to data overload and necessitate reconciling unknown trusted data with internally discovered threat profiles. The Fusion subscription from Mandiant Advantage is the only source of threat intelligence your security team needs. It provides full, unlimited access to Mandiant Threat Intelligence, including ongoing, past and predictive threat activity. Fusion gives security teams an unrivalled, strategic view of the threat landscape, one that combines multiple threat facets such as cyber crime, cyber espionage, strategic intelligence, cyber physical intelligence and intelligence related to adversary operations. Access thousands of finished intelligence (FINTEL) reports based on strategic analysis from Mandiant experts, third-party global telemetry, Mandiant incident response and technical research findings all from one searchable view.

What's included?

- Mandiant Advantage Threat Intelligence Free, Security Operations, Vulnerability and Digital Threat Monitoring capabilities
- Filter by report types, region, industry, actor or malware name
- Finished intelligence reports with full narrative covering strategic to tactical analysis research and context

Benefits

For vulnerability analysts, IT/system or data owners, risk managers and intelligence analysts

- **Visibility.** Review vulnerability data by technology, actors and exploit source
- **Prioritize.** Analyze data by risk and exploit rating to focus on the vulnerabilities that matter now
- **Notifications.** Get notified of zero-day vulnerabilities
- **Quick installation.** Integrates with your vulnerability scanners via Browser Plugin or API

Mandiant Advantage Vulnerability (Additional Module)

Maximize threat surface reduction efforts

Faced with continuous expanding IT infrastructures, new applications and disparate geographical locations, vulnerability risk analysts can feel overwhelmed by the number of vulnerabilities to be addressed in their environment. Analyzing vulnerability information can be a labor-intensive process and even when armed with a simplified vulnerability rating system, it can be hard to know where to start. The Threat Intelligence Vulnerability subscription from Mandiant Advantage allows security risk teams to assess, prioritize and remediate discovered vulnerabilities at enterprise scale by unique scoring mechanism based on ease of exploitation, likelihood of the exploit and perceived threat or impact.

What's included?

- Mandiant vulnerability views and scoring including exploit ratings, risk ratings, zero-day assessment and activity observed from our frontline experts
- Comprehensive vulnerability reports including CVE IDs, vulnerable technologies, exploit vectors and relevant reports
- Quarterly Threat Briefings and basic support (provisioning plus onboarding)

Benefits

For intelligence analysts, legal counsel, public relations/ corporate communications, executives and senior leadership

- **External threat visibility.** Identify threats to assets outside of your organization’s perimeter, including the dark web
- **Simple setup.** With your search parameters defined, Advantage will continuously monitor multiple forums, social media, paste sites and actor related posts
- **Reliable.** Reduce false positives or negatives with an industry trusted and protected portal
- **Accelerate response.** Prepare response to limit further damage and defend enterprise assets or information

Mandiant Advantage Digital Threat Monitoring (Additional Module)

Early warning on external threat exposures

Traditional cyber defenses typically focus on assets or events that exist within your network. But in today’s highly connected world, you also need to protect assets that extend beyond your perimeter—such as your organization’s brand, identities and partner community. The Digital Threat Monitoring subscription from Mandiant Advantage provides early visibility into external threat exposures your assets face with dark web peace of mind monitoring. This allows you to defend against the risks that threaten your brand, infrastructure and high-value partnerships. You can identify breaches, exposures and digital threats across the open, deep and dark web using customized keyword search terms. You can subsequently automate, analyze and generate threat alerts on potentially significant matches.

What's included?

- Customized keyword-driven research tools for tailored, scalable reconnaissance and dark web monitoring
- Optional Access to Mandiant Analyst for setup, triage and investigation via Managed DTM, On Demand Support or Expertise On Demand
- Threat alerts via the Alerts Dashboard including the status, source, severity attributes and insights to help manage your monitored assets.
- Quarterly Threat Briefings and basic support (provisioning plus onboarding)

The Mandiant Advantage Threat Intelligence Portfolio

	Free	Security Operations	Fusion
ACCESS TYPES			
Mandiant Advantage Platform and Browser Plug-in	○	○	○
API	○	○	○
DATA ACCESS			
Indicators - Open Source - with Mandiant Scoring	○	○	○
Threat Actors - Open Source and Publicly Known	○	○	○
Malware and Malware Families - Open Source	○	○	○
Real Time Dashboards - Actor, Malware, and Vulnerability	○	○	○
Indicators - Mandiant Proprietary - with Scoring and Context		○	○
Threat Actors - Mandiant Proprietary - UNC, Temp, APT, FIN		○	○
Malware and Malware Families - Mandiant Proprietary		○	○
Live Actor & Malware Pivot Views - MITRE ATT&CK and Graph		○	○
Active threat campaign data and view		○	○
VULNERABILITY			
Public / Known Vulnerability Descriptions	○	○	○
Mandiant Risk and Exploit Rating	+ Vulnerability Module		○
Mandiant Vulnerability Analysis	+ Vulnerability Module		○
DIGITAL THREAT MONITORING (DTM)			
Dark Web Monitoring	+ Digital Threat Monitoring		○
Research Tools and Alerting	+ Digital Threat Monitoring		○
ANALYSIS & ADVERSARY INTELLIGENCE			
News Analysis	○	○	○
Quarterly Intelligence Threat Briefing		○	○
Strategic Reporting - Region, Industry, Trends			○
Adversary Motivations, Methods, Tools, and Behaviors			○
Reporting			○
Threat Activity Alerts, Emerging Threats, and Trend Reporting			○
Mandiant Research Reporting			○

Vulnerability and Digital Threat Monitoring can be purchased independently.

Learn more at **www.mandiant.com/intelligence**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT NOW PART OF Google Cloud