

## THREAT INTELLIGENCE FAQ

We've compiled some frequently asked questions into this article.

### What is Mandiant Advantage?

Mandiant takes an intelligence-led, multi-vendor approach to XDR. The Mandiant Advantage platform enhances existing security controls and enables the SOC to improve efficiency and efficacy in finding malicious security incidents quickly and at scale. The platform gives security teams an early-knowledge advantage through the **Mandiant Intel Grid** (<https://www.mandiant.com/advantage/intel-grid>). The Intel Grid provides platform modules with current and relevant threat data and analysis expertise.

### Why was Mandiant Advantage Threat Intelligence created?

Mandiant Advantage Threat Intelligence (MATI) was built on the feedback from our customers and internal teams to deliver a data-driven experience to address key use cases through new capabilities. Our aim is to equip customers with everything we know, when we know it, in easily consumable formats.

### What is new or different about Mandiant Advantage Threat Intelligence for customers?

With MATI, you can continue to receive comprehensive intelligence into current, past, and possible future threat activity. Also, you can now know what we know about cyber threats and adversaries, when we know it. You'll have access to the same data and graph database that our intelligence analysts rely on, including the tools used by our expert Mandiant Incident Response team. Upgraded features and functionality that you'll experience with Threat Intelligence include the following:

- Real-time access to up-to-the-minute breach, adversary, machine, and operational intelligence
- Greater access and visibility across the threat landscape through open source and Mandiant threat data
- A scoring engine that helps teams better understand and prioritize threats, vulnerabilities, and their potential risk
- Simplified user experience with easy to use and digest charts, graphs, and report navigation
- Ability to overlay Mandiant Intelligence on web-based interfaces through the **browser plug-in** (<https://docs.mandiant.com/home/mati-browser-plugin>)
- Customers will see continued evolution in both Intelligence features and wider Mandiant Solutions capabilities introduced through the Mandiant Advantage platform.

### How does Mandiant keep threat intelligence content relevant to customer needs?

We evaluate usage of our platform, including search logs, to ensure that our threat intelligence content is responsive to the threats that are most relevant for customers. We may also audit search logs to make sure our customers are using our platform for their own security purposes, and not any other purpose.

### How will I be enabled and informed on new feature updates?

The Mandiant Advantage platform features this documentation portal which contains key customer-facing enablement content that is accessible from within the platform itself. Service Descriptions, Videos, How-to Guides, Release Notes, API info, FAQs, and more can be found here. The documentation site is accessed by clicking the help icon in the Mandiant Advantage platform web console. New and recently updated articles are captured in **Article updates** (<https://docs.mandiant.com/home/article-updates>).

### How can I provide feedback?

You can send feedback, questions, and requests to **Support** (<https://docs.mandiant.com/home/mandiant-support-cases>).

### Intelligence offerings available through Mandiant Advantage

What subscription levels are available?

- Fusion: Provides access to all available Mandiant Threat Intelligence reporting, indicators, and data
- Security Operations: Enhance threat monitoring, detection, and response
- Vulnerability: Assess, prioritize, and remediate vulnerabilities at enterprise scale effectively
- Digital Threat Monitoring (DTM): Protect your organization's brand, reputation, and sensitive data
- DTM Managed Service: Mandiant Analysts managing DTM on behalf of clients

What baseline features are included with these intelligence subscriptions?

- Mandiant Advantage Platform: Access to data, FINTEL, and features entitled with subscriptions
- IC-Score: A 0-100 rating representing our confidence that a particular indicator represents malicious activity
- Daily News Analysis: Daily analysis of cyber news, including Mandiant's judgment on accuracy
- Quarterly Briefings: General Intel briefing provided to subscribing organizations by our analysts
- Browser Plug-In: Automatically scan web pages for technical indicators and context with hyperlinks to associated Intel
- Intelligence API: Provides machine-to-machine integration with Mandiant's contextually rich Intel
- Indicators: Provided in various formats, gathered from multiple proprietary and public sources
- Support Services: Enablement and support to assure customers are onboarded successfully
- Email Notifications: Ability for users to set up delivery profiles to manage content notifications
- See the full Intelligence Subscription Service Description for further details in the [Service Descriptions](https://docs.mandiant.com/home/service-descriptions) (<https://docs.mandiant.com/home/service-descriptions>) section

### Are intelligence services offerings still available?

Yes, the following Intelligence Enablement, Intelligence Capability Development, and Executive Intelligence Briefing offerings are still available with MATI:

- Intelligence Coordination: Offers designated access to an Intelligence Enablement Manager (IEM). The IEM advises your Mandiant Intelligence consumption based on your concerns, growing needs, organizational goals, and available resources. The IEM can advise you throughout your maturity path.
- Intelligence Optimization: Offers unparalleled access to the data holdings of Mandiant and guidance on how to most effectively consume it through a designated Intelligence Optimization Analyst (IOA). IOAs are experienced Intelligence Analysts producing industry-leading threat Intel.
- Intelligence Jumpstart Workshop: Guides organizations in the identification and development of threat intelligence practices and capabilities.
- Intelligence Capability Assessment: Assess key threat intelligence capabilities to transform into an intelligence-led organization.
- Cyber Threat Diagnostic: Assess your cyber threat landscape based on an analysis of their log data correlated against Mandiant threat intelligence.
- Operational Intelligence Support: Work directly with you to identify emerging threats, integrate Mandiant Intelligence into operations, and mature capabilities.
- Advanced Intelligence Access: Through direct engagement, provides immediate access to raw FireEye threat data, analysis tools and finished intelligence.
- Cyber Intelligence Foundations: Train teams and develop essential knowledge and skills related to intelligence analysis.
- Expertise-on-Demand (see separate EoD Menu): "Ask and Analyst", Individual Finished Intel Reports, Threat Investigations, Custom Intel, Workshops.
- Executive Intelligence Briefings: Weekly Audiovisual Intelligence Analysis and Insights.

### How will I submit malware requests?

You have access to the **File Analysis** tab in Mandiant Advantage Threat Intelligence for submitting malicious samples.

### How will I submit On-Demand Intelligence (formerly Analyst Access) requests?

Please follow the instructions provided in the article "[How to submit an On-Demand Intelligence Access request \(https://docs.mandiant.com/home/expertise-service-how-to-make-a-request\)](https://docs.mandiant.com/home/expertise-service-how-to-make-a-request)" to successfully submit a request.

### Will I need to reconfigure my API connection or integration?

Integrations that use API v2 and v3 will continue to function. However, Mandiant is no longer maintaining these legacy APIs. We encourage all customers and partners to transition their integrations to **API v4** (<https://docs.mandiant.com/home/threat-intelligence-api-v4>) as the standard entry point for Mandiant Threat Intelligence.



For more information on existing integrations, see [Threat Intelligence Integrations \(https://docs.mandiant.com/home/threat-intelligence-integrations\)](https://docs.mandiant.com/home/threat-intelligence-integrations).

### What is "Digital Threat Monitoring" in the MATI platform?

This product in Mandiant Advantage enables you to detect and respond to external threats by monitoring the open, deep and dark web. It provides early warning of threat actors targeting your organization and notification of data and credential leaks so you can respond quicker. For more information, see [Digital Threat Monitoring \(https://docs.mandiant.com/home/digital-threat-monitoring\)](https://docs.mandiant.com/home/digital-threat-monitoring).