

GETTING STARTED WITH YOUR THREAT INTELLIGENCE SUBSCRIPTION

Are you a new Mandiant Advantage Threat Intelligence (MATI) subscriber? See the [Advantage Threat Intelligence QuickStart Guide](https://docs.mandiant.com/home/threat-intelligence-quick-start-guide) (<https://docs.mandiant.com/home/threat-intelligence-quick-start-guide>) for information that will allow you to quickly benefit from your subscription.

In addition to the QuickStart Guide, this Documentation portal also includes a number of guides and other resources to help you get the most out of your subscription:

- **Threat Intelligence Integrations** (<https://docs.mandiant.com/home/mati-threat-intelligence-integrations>): API integrations allow you to pull additional context and intelligence into your existing security tooling.
- **Threat Intelligence Guides** (<https://docs.mandiant.com/home/threat-intelligence-guides>): User guides walk you through how to use the MATI platform, including Threat Campaigns and File Analysis.
- **Threat Intelligence Resources** (<https://docs.mandiant.com/home/threat-intelligence-resources>): Additional articles to help you understand how MATI collects and enriches threat intelligence data, including threat actor tracking and attribution.

The **MATI platform** (<https://advantage.mandiant.com>) itself provides highly interactive visualizations and reports that make it easy to drill down to the information that's most relevant to your organization with **customizable dashboards** (<https://docs.mandiant.com/home/ma-custom-dashboard-widgets>) and continuously updated threat activity alerts.

Sample Finished Intelligence Reporting Guide

Below is a summarized list of the most popular finished intelligence reports. Availability may vary based on your Threat Intelligence subscription.

Understanding Key Threats

- **Actor profiles** (<https://advantage.mandiant.com/reports?reportType=Actor%20Profile>): In-depth analysis of key nation-state, criminal, and other malicious actors.
- **Malware profiles** (<https://advantage.mandiant.com/reports?reportType=Malware%20Profile>): Detailed analysis of malware types linked to notable threat activity.

Threat Landscape Analysis

- **Threats & environment by country & region** (<https://advantage.mandiant.com/reports?reportType=Country%20Profile>): Regular updates on the threat landscape facing organizations with a presence in specific countries and regions.
- **Threats & environment by industry** (<https://advantage.mandiant.com/reports?reportType=Malware%20Quarterly%20Industry%20Report,Industry%20Reporting>): Regular updates on the threat landscape facing organizations with a presence in specific industries.
- **Net assessments** (<https://advantage.mandiant.com/reports?q=%22net%20assessment%22&reportType=Trends%20and%20Forecasting,Net%20Assessment>): Overview of current threats in specific categories, such as nation-state intrusion operations.

Tracking New Activity

- **Event analysis** (<https://advantage.mandiant.com/reports?reportType=Event%20Coverage%20Implication>): Significant threat developments and Mandiant's analysis.
- **Research insights** (<https://advantage.mandiant.com/reports?reportType=Threat%20Activity%20Alert,Threat%20Activity%20Report>): Rapid insights into new collections.

Vulnerabilities & Exploitation

- **Weekly vulnerability exploitation trends** (<https://advantage.mandiant.com/reports?reportType=Weekly%20Vulnerability%20Exploitation%20Report>): Tracking developments in critical- and high-risk

vulnerabilities.

Malicious TTPs

- **Targeted intrusion lures** (<https://advantage.mandiant.com/reports?q=%22potential%20targeted%20malware%20infection%20lures%22&reportType=Trends%20and%20Forecasting>): Social engineering lure themes which have been, or may be, associated with targeted intrusion attempts.
- **Malware targeting** (<https://advantage.mandiant.com/reports?q=%22targeting%20update%22&reportType=Trends%20and%20Forecasting>): Changes in focus for malware with configured targeting behavior.
- **Operational technology-related phishing** (<https://advantage.mandiant.com/reports?q=%22operational%20technology%20phishing%20roundup%22&reportType=Event%20Coverage%2FImplication>): Malicious emails with content related to ICS and other operational technology.

Popular Intelligence

- **Weekly intelligence update** (<https://advantage.mandiant.com/reports?q=%22weekly%20intel%22&reportType=Executive%20Perspective>): Intelligence from the past week that is notable and of high interest to our customers.

Additional Resources

- The latest on cybersecurity threats and news from Mandiant are discussed weekly on **The Defender's Advantage Podcast** (<https://www.buzzsprout.com/1762840>).
- All Threat Intelligence customers will receive an email invitation to attend Mandiant's *Quarterly Threat Intelligence Briefing*.

Intelligence Training & Enablement

Your Advantage subscription includes an array of training and enablement content, and it is highly recommended that all customers review each module to get the best experience.

The following **In-Product Training & Content** is available in this Documentation portal:

- **Key Features Video**: Overview of key Mandiant Advantage features
There are two additional Browser Plugin videos:
 - **MATI Browser Plugin Onboarding** (<https://docs.mandiant.com/home/onboarding-mati-browser-plugin-overview>)
 - **Using the Browser Plugin with Splunk** (<https://docs.mandiant.com/home/how-to-use-mandiant-advantage-browser-plugin-with-splunk>)
This video is for version 1.0 of the plugin so is not 100% up-to-date
 - **Browser Plugin Overview** (<https://docs.mandiant.com/home/mati-browser-plugin>): Review documented details on the browser plugin
 - **Threat Intelligence Integrations** (<https://docs.mandiant.com/home/threat-intelligence-integrations>): Describes available integrations with other platforms
 - **On-Demand Training Modules** (<https://docs.mandiant.com/home/on-demand-intelligence-training>): A list of available Cyber Intelligence training modules available as paid options
 - **What's New** (<https://advantage.mandiant.com/whats-new>): Learn about the latest Advantage features
 - **Offerings and Services** (<https://www.mandiant.com/advantage/threat-intelligence/>): Deep dive on Mandiant Intelligence offerings
 - **FAQs** (<https://docs.mandiant.com/home/mati-threat-intelligence-faq>): Learn more about Advantage assets and Mandiant security techniques
- Additional **On-Demand** (<https://www.mandiant.com/advantage/academy/cyber-intelligence>) or **Instructor-Led**

(<https://www.mandiant.com/advantage/academy#course-formats>) training courses are available as paid options. We are highlighting popular options here to assure awareness and to fulfill the demand many organizations have for this knowledge.

- **Introduction to Threat Intelligence and Attribution:** Designed to provide insight into attribution methodology and demonstrate the proper handling of threat intelligence information
- **Hunt Mission Workshop:** How to employ a process framework to scope, execute, and validate the results of a network hunting operation and ensure each hunt mission improves security posture
- **Introduction to Cyber Crime for Executives:** Designed to educate senior leaders about cybercrime and incident response. Learners will review real-world intrusions, examining tactics and technologies
- **Cyber Intelligence Foundations:** How to apply the discipline of intelligence analysis to the cyber domain, including understanding the intelligence lifecycle and developing raw data into viable intel
- **Cyber Intelligence Research I – Scoping:** Teaches students to analyze, prioritize and fully understand requests for information (RFIs), and create a research plan that keeps their efforts on track
- **Cyber Intelligence Research II – OSINT:** Identify and develop pivot points or leads in investigations across multiple use cases. Review the basic functions of open-source tools and learn when and why to use them in their research
- **Cyber Intelligence Production:** How to convey analytic assessments and findings in intelligence reports and briefings covering strategic, operational, and technical intelligence products

Intelligence Services Options

In addition to expert training, organizations seeking additional best practices can leverage three additional Intelligence Services offerings to create a proactive security posture informing enterprise-wide decisions to reduce cyber risk:

Program Advisory: Help Assess, Design, and Enhance Customers' In-house Capabilities to be Intelligence-led

- **Assess:** Current-state capability across people, process, and technology; develop a strategic roadmap to reach the enterprise goals for intelligence
- **Design:** Target-state capability, including team size, required roles, responsibilities, processes, technical requirements, and cross-enterprise intelligence integration points
- **Enhance:** Organizational-wide CTI capabilities through strategy development, operational procedure implementation, and technical consultation

Applied Intelligence: Proactive Reporting and Direct Access to Intelligence Experts and Raw Data

- **Executive Intelligence Briefings:** Understand the big picture perspective on cyber threats and trends that should be top of mind for security leaders (delivered weekly).

- **Digital Threat Assessments:** Identify your external risk exposure related to your digital footprint, allowing results to be incorporated into your overall business risk profile (analyzed over 30 days).
- **Cyber Threat Profile:** Prioritize the external threats facing your organization and their methods of attack to understand your internal exposure and defensive posture (offered as a managed or unmanaged service).
- **On-Demand Analyst Support:** Provides customers with the flexibility to request actionable intelligence by world-class intelligence analysts, on a wide scope of time-bound organizational needs.
- **Proactive Analyst Support:** Receive tailored intelligence reporting at defined frequencies, tuned to your specific threat profile and operating environment (offered remotely on an annual basis).
- **Advanced Intelligence Access:** Pivot quickly to changes in your threat profile by incorporating raw data, global telemetry, and custom tooling into your operational workflows (offered on-site on an annual basis).

Technology Advisory: Optimizing Technical Solutions

- **Managed Threat Monitoring:** Leave the management of your digital footprint to Mandiant. We collect your keywords and proactively notify you of exposure and suggest mitigation strategies.
- **Mandiant Cyber Operations Platform:** The most realistic adversary emulation on the market. Our scalable, multi-purpose framework and infrastructure allows Mandiant experts to imitate malicious actors, by repurposing real-world APT payloads and custom-built attack packages to test cyber defense teams and help customers plug security gaps.
- **Custom Tooling:** Through the delivery of our various Mandiant Intelligence Services, we employ our homegrown private analyst tools. In addition, we create custom utilities for our customers to use and leverage during and after engagements. We also help our customers optimize their internal intelligence toolsets (TIPs).