Threat Intelligence

Highlights

- Threat intelligence directly from the frontlines
- Curated by 500+ threat intelligence experts
- Backed by insights from 1,800+ incident response engagements annually
- AI infused threat intelligence to improve security and reduce toil
- 300+ Threat Actors Tracked
- Leverage Google's visibility across 5+ billion devices, 60+ billion URLs, 43 billion files, and 12 billion network indicators scanned daily for threats

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 threat intelligence directly from the front-lines providing organizations with up-to-the-minute updated threat intelligence to perform their security tasks faster and with more accuracy.

Focus on the threats that are most relevant to you

Yes, the global threat landscape is ever evolving, but how is your threat landscape changing? Mandiant Threat Intelligence allows you to focus on the threats that are most relevant to you. With a single dashboard, you can see an up-to-date view of who's targeting organizations like yours, active campaigns, malware, and relevant vulnerabilities. You can also receive daily or weekly notifications on changes to your threat landscape so you can better prepare your organization and stay ahead of the threats.

Make threat intelligence more actionable

To get the most value out of threat intelligence you need to be able to easily use it to protect your organization from attack or detect and respond from an existing breach. Mandiant Threat Intelligence integrates with the industry's leading security tools either via native integration or API allowing you to operationalize the threat intelligence quickly and easily. The browser plug-in puts threat intel into existing workflows. It overlays threat intelligence in your browser so you can learn more about a vulnerability, indicator, malware or threat actor without leaving your browser or workflow—including social media sites, SaaS based security consoles, etc.

Save time and reduce complexity with AI

Mandiant Threat Intelligence uses ML and AI throughout the product to help reduce toil by surfacing the most relevant information allowing staff restricted security teams to respond to attacks faster and share intelligence with ease to break down internal silos. The use of AI is most visible through Duet AI in Mandiant Threat Intelligence, an always-on AI collaborator that provides generative AI-powered assistance to help distill Mandiant's industry-leading corpus of threat intel into easy to comprehend summaries, allowing you to quickly understand how adversaries may be targeting your org and impacting the threat landscape.

Prioritize the threats with the greatest potential risk

Our days are filled with decisions and requests for our time. Mandiant Threat Intelligence can help you determine which threats or vulnerabilities require the most attention and which can wait. Threat campaigns and vulnerability intelligence provide actionable insight into active threat campaigns and vulnerability risk rating giving 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 confidently.

Optimize threat intelligence with our expertise

We can all use a little helping hand especially when it comes to securing the organization. Whether you need a dedicated onsite resource to provide up to the minute threat intelligence, a review of your cyber threat profile across the tactical, operational, and strategic levels, or just a quick request for information (RFI) about a threat, file or situation, Mandiant is here to help. Mandiant Threat Intelligence Services offer a full range of services to help you optimize your ability to consume, analyze and apply threat intelligence. Get expert assistance to help build a sustainable intelligence-led organization and improve your team's analytical and threat hunting capabilities.

Visibility into the open, deep and dark web to anticipate threats

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, important personnel, tech resources and trusted partners. Digital Threat Monitoring provides early visibility into external threat exposures by monitoring underground marketplaces, paste sites, blogs, forums, malware repositories and more to anticipate attacks and detect unknown data leaks and compromised credentials.

Minimize risk with prioritized patching

Faced with continuous expanding IT infrastructures, new applications and disparate geographical locations, the number of vulnerabilities to be addressed in your environment can feel overwhelming. 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. Threat Intelligence Vulnerability 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.

Simplified offerings to fit your organizational needs

Mandiant Threat Intelligence is offered in two subscriptions options.

Security operations center (SOC) personnel are under a constant barrage of security events requiring continuous attention and manual, laborious investigations. The Mandiant 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.

The **Security Operations subscription** includes:

- Global dashboards providing actor, malware and vulnerability activity trends
- Threat intelligence accessible via portal and browser plugin
- Dynamic actor and malware pivot views with MITRE ATT&CK map, object explorer and indicator downloads
- Access to open-source and Mandiant known indicators (IP, Domain, File Hash, URL) with maliciousness scoring metrics
- News analysis with Mandiant expert judgements and commentary
- Real-time visibility into the most active and relevant threat campaigns

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 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.

The **Fusion Subscription** includes:

- Mandiant Threat Intelligence 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

Threat Intelligence Product Portfolio

Access Types	Security Operations	Fusion
Browser Plug-in	●	●
API	●	●
Data Access		
Indicators – Open source and Mandiant proprietary	●	●
Threat actors – Open source and Mandiant proprietary	●	●
Malware and malware families – Open source and Mandiant proprietary	●	●
Active threat campaign data and view	●	●
Real time dashboards – Actor, malware and vulnerability	●	●
Vulnerability		
Public/known vulnerability descriptions	Add-on module	●
Mandiant risk and exploit rating	Add-on module	●
Mandiant vulnerability analysis	Add-on module	●
Digital Threat Monitoring (DTM)		
Dark web monitoring	Add-on module	●
Research tools and alerting	Add-on module	●
Analysis & Adversary Intelligence		
News analysis	●	●
Strategic reporting – Region, industry, trends		●
Adversary motivations, methods, tools, and behaviors		●
Reporting		●
Threat activity alerts, emerging threats and threat reporting		●
Mandiant research reporting		●