Mandiant

Digital Threat Monitoring

Highlights

- Monitor 200+ card forums, marketplaces and ransomware sites
- Tailored to your organization via unique user keywords
- Unlimited users
- Offered as a managed service or self-managed

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

Cyber criminals conduct their work on the open, deep, and dark web. To find them, you need to know where to look, have the right access and understand what they are saying. If you could access these conversations and filter the noise to see what they're saying about you, your organization, or your partners, you could anticipate and plan for threats or learn if you were already compromised.

- **Open web:** Also known as the surface or clear web, this is easily accessible data indexed by search engines—but it only comprises 10% of available information
- **Deep web:** Most online information falls into this category, where data is not indexed by search engines; this includes academic networks and information that requires payment or registration.
- **Dark web:** This section of the internet requires special software (such as TOR) and configurations to access and criminal forums and marketplaces are typically hosted here (the "underground").

Mandiant Advantage Digital Threat Monitoring watches the open, deep and dark web so you can detect and respond to potential external threats. Leveraging industry-leading threat intelligence, Digital Threat Monitoring not only knows where to look and listen for cyber criminal discussions but helps access private encrypted channels and understand the languages and slang/codes used by cyber criminals. Digital Threat Monitoring removes the noise and false positives using machine learning-driven language processing, entity recognition and filters. In just a few minutes per day, you could learn of a data and credentials leak or if malicious actors are targeting your organization, VIPs and vendors.

Protect what matters most to the organization

With visibility across unground markets, blogs, paste sites and more, Digital Threat Monitoring can help you anticipate threats and detect previously unknown leaks. Using unique and tailored keywords, you can focus the monitoring to protect your:

Brand
Prevent the loss of customers, revenue, and trust

VIPs
Prevent targeted attacks and better mitigate hacktivism

Technical resources
Mitigate extortion and data loss

Trusted relationships
Prevent a conduit to a data breach or disruption of your supply chain

Value-added managed option

While every organization could benefit from monitoring for potential threats, targeting and data leaks, not every organization has the resources, time or skills to do so. With Managed Digital Threat Monitoring, Mandiant analysts will triage alerts and highlight data you prioritize or need to act on.

A designated analyst manages all your keywords and monitors, saving your team setup and tuning time. The analyst provides monthly reports and touchpoint meetings to both provide insight into trends in activity and further tailor analyst support. They work with you to monitor, detect and make informed decisions about external threats across the internet, including the deep, dark web. The designated analyst will help triage, prioritize and provide contextual analysis so you can effectively mitigate the effect of data leaks, ransomware and other cyber threats.

	Digital Threat Monitoring	Managed Digital Threat Monitoring
Onboarding	Yes	Yes
Unlimited Users	Yes	Not Applicable
Intelligence Portal Access	Yes (Free)	Yes (Free)
Threat Alert Notifications	Yes	Yes
Keyword Categories	All	All
Keyword Management	Self-Managed	Mandiant
Monitoring/Triaging Alerts	Self-Managed	Mandiant
Intelligence Investigations	Available as part of the Expertise on-Demand service	Mandiant
Summary Reports	Not included	Monthly
Service Review Meetings	Not included	Monthly
Urgent Findings Notice	Not included	Included
Takedowns and Disruption	Coming Soon	Included

Digital Threat Monitoring is an essential part of Mandiant's digital risk protection solution, giving you the ability to identify high-risk attack vectors, malicious orchestration from the deep and dark web, and attack campaigns on the open web. Mandiant's digital risk protection solution also provides contextual information on threat actors and their tactics, techniques and procedures to provide a complete cyber threat profile that helps you protect your digital assets, supply chain and brand.

Digital Risk Protection

Cyber Threat Profile Service