Mandiant

DIGITAL THREAT MONITORING

With Digital Threat Monitoring (DTM), you know about threats when we know about threats, giving you a leg-up in defending against cybersecurity attacks and vulnerabilities. DTM lets you take advantage of the collection infrastructure of Mandiant's Threat Intelligence to monitor for references to your organization or assets. Alerts are triggered in near real-time when your specified content is detected.

How DTM Works

DTM is continuously discovering, ingesting, and analyzing suspicious content from both the surface and dark web. DTM collects content from around the internet, including: paste sites (such as GitHub or Pastebin), forum posts, malicious email messages, and other sources. When DTM discovers suspicious content, it immediately ingests that content and normalizes it into a common format (also called a document or event). The content is run through our proprietary Machine learning (ML) pipeline which extracts entities (such as proper names, domain names, URLs, identities, organizations, and brands). The pipeline also provides content characterization (such as language, threat type, and industry).

DTM archives the documents and their associated ML extractions for searching/exploration of historical data in the Mandiant Advantage Threat Intelligence (MATI) platform. You can also choose to receive near real-time alerts based on conditions you define in a **Monitor**. The DTM alerting system lets define one or more Monitors with search conditions to match ingested data. When these conditions are met, an alert is created in near real-time for your Monitor.

DTM Use Cases

- Brand/reputation management
- Intellectual property (IP) protection
- Third-party/supply chain monitoring
- Fraud detection (payment cards, trademark infringement)
- Domain discovery/Network indicators (for example, typo-squatting)
- Data leaks
- Credential exploitation
- Illicit access/ransomware

The following video introduces Mandiant Advantage Digital Threat Monitoring and how to navigate through some of the basic features.

- Visibility to open web, deep web, and dark web to anticipate and respond to potential external threats.
- Machine Learning (ML) pipeline extracts entities (e.g., proper names, domain names, URLs, identities, organizations, brands, etc.), and provides content characterization (e.g., language, threat type, industry).
- Near real-time alerting system via Monitors that you define via search conditions to match ingested data.
- Monitor 200+ card forums, marketplaces, and ransomware sites
- Tailored to your organization via unique user keywords.