Mandiant

DIGITAL THREAT MONITORING FAQ

Here at Mandiant, we know Cybersecurity threats never sleep. That's why we designed the "always-on" threat monitoring and alerting capabilities of Digital Threat Monitoring (DTM). With DTM, you know about threats when we know about threats, giving you a leg-up in defending against Cybersecurity attacks and vulnerabilities. DTM enables you to benefit from the collection infrastructure of Mandiant Threat Intelligence and receive alerts when specific content is ingested.

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

What sources are used to collect DTM data?

Various sources are used to collect our data. This includes, but is not limited to: OSINT news/blogs, underground forums, code collaboration sites, Pastebin style sites, dark web shops, and domain registrations. We do not publish the exact sites/sources we collect from, but strive to only collect cybersecurity intelligence data from all such sources. The types of content we target includes, but is not limited to: credential dumps, threat news, bank identification number sales/dumps, for example.

We cover all major targets known to have the highest potential for impact to our customers. The list grows and shrinks as targets are retired and start up. With Research Tools, this will change as customers will be able to browse the list of targets and see what's covered.

Our collection covers web content, both on the open and dark web, primarily targeting sites used for communication by malicious actors. This includes marketplaces, forums, and paste sites that enable the generation of Threat Alert types covering different categories of customer interest.

When considering sources, it's important to note that data collection falls into three distinct categories:

- **Full Coverage**: We can see every item on this source. There can be one-off cases where we might miss a particular item but that should be the exception.
- **Partial coverage** (usually search-based): We can't see the full dataset so we have to somehow query the source, usually by searching, to extract the documents that have a likelihood to match. This technique is often used when there are limitations imposed by the source or by a third-party service we use to cover that source.
- **Capability**: A capability is something that's not directly tied to a source we might cover. It's an application we have built to solve a particular problem. For example, the DNS Teaser application analyzes domains that you provide to generate potential typo-squatted and look-like domains. We then attempt to resolve those generated domains to see whether their domain records changed, such as going from unregistered to registered or inactive to active.

Does DTM have full coverage of tweets?

Not at this time. We will be reviewing our X/Twitter coverage soon.

Does DTM have full coverage of GitHub?

No. For GitHub, we do NOT ingest every repository. Instead we use a search approach. We search GitHub using relevant cybersecurity keywords and then match that content against customer-defined keywords in Monitors.

How often is data collected?

Generally speaking, DTM is constantly collecting data 24x7. However, certain sources are collected on schedules that range from every few minutes to a few times per day.

How quickly are DTM Alerts created when my Monitor matches on a collected document?

DTM alerting operates in near real-time from when the data (document) is collected. The basic flow is as follows:

1. A document is collected from a source and ingested into our system.
2. The collected data undergoes analysis using Machine Learning.
3. The document is then matched against all Monitors in the DTM system.
4. An Alert is immediately generated for all Monitors that produce a hit/match.

Is it safe to include keywords and Monitor searches with my private data?

Yes. DTM is encrypted end-to-end. In transit, data is sent over TLS encrypted/verified connections. Data at rest is stored using hardware-level encryption that's adequate for Government Cloud-based standards. Moreover, your Monitor keywords/searches are not directly associated with your organization's name. Instead, the Monitors and their data are associated with a GUID that uniquely identifies your organization. The mapping between this GUID and your organization is stored in a separate, encrypted system. As a result, DTM Monitors do not provide any means to link your Monitor data/keywords to your organization name.

What purpose does Machine Learning serve in DTM?

Most ingested data (documents) are run through our Machine Learning pipeline. This pipeline uses advanced analysis/recognition techniques to identify both "things" within the documents, as well as "things" about documents, often called "classifications." Entities identified within documents are often called "entities" and usually correspond to person or place, for example. In other words, the analysis of a document might detect names, physical locations, or product names. Classifications are metadata about the document itself. For example, what type of content the document is, or what language it's written in. Both entities and classifications allow your Monitors to target specific things within our data with higher confidence of false positives.

Is it difficult to create new Monitors within DTM?

We strive to make this process as easy as possible but still provide a robust set of capabilities to meet advanced monitoring needs. To jumpstart Monitor creation, we provide a set of **Monitor Templates**, which encapsulates the most common use cases for Monitoring with DTM. We also let you create your own Monitor from scratch and advanced capabilities to use a query language syntax for advanced Monitoring uses.

For more information, see **How to Create DTM Monitors (https://docs.mandiant.com/home/dtm-creating-monitors)**.

Is there any limit to the number of Alerts my Monitors can generate?

We have no cap on the total number of Alerts Monitors can generate. However, we provide a safety mechanism that automatically disables Monitors that produce excessive Alerts within a given period of time. This mechanism is not a technical limitation but rather a feature to help our users create Monitors that do not accidentally produce more Alerts than feasible to consume and often indicate an invalid Monitor condition.

Can I delete Alerts?

Alerts serve as a record of indication, an audit history of sorts, and therefore cannot be deleted. However, Alerts have various states that you can set (new, read, closed), allowing you to control their lifecycle. Moreover, you can filter your view of Alerts based on their state (and other properties) allowing you to effectively delete them by setting their state to closed.

Can I search historical data in DTM?

Yes. We store all data we collect indefinitely and allow searching via **Research Tools**, available in Mandiant Advantage. Research Tools supports searching with a Lucene-style syntax so you can use single word terms or build complex queries to find the data (documents) you're looking for.

Is DTM available programmatically?

Yes. We provide a REST API for almost all operations that can be performed from DTM in Mandiant Advantage. This REST API uses JSON content to represent Monitors, Alerts, etc. For more details, please see the "API Access and Keys" section of your "Settings" in Mandiant Advantage.

When images are included in forum posts do we capture that content?

There is no image collection from Forums and Marketplaces.

Should we expect all content from Forums to be available in Research Tools?

The Mandiant collection systems attempt to capture all relevant content. For some targets, we do ignore Boards and Topics that have limited research and customer value. Examples include sexually explicit content or drug topics. Content is often modified or deleted from various forums as well - this can be a single post or an entire thread. We do everything we can to capture content before deletion or between modifications but it is impossible to capture everything.

Do we have coverage of Telegram, WhatsApp and Discord public chat content?

There is a current collection system gathering Telegram messages and is available in Mandiant Advantage. There is collection on WhatsApp but it has not been integrated with DTM yet. There is no Discord collection.

Does Mandiant search for credential dump repository?

There is no current support in the DTM product to display, search or alert on "stand-alone" credential data. There are some dumps that are manually curated internally by the research teams, but there's not really a "credential dump repository" out there that we monitor for DTM. We do monitor the places where we think credentials might show up - various pastes sites, telegram channels or samples of data that might show up in Forums. These documents have the potential to match customer monitors.

We do NOT cover **https://haveibeenpwned.com/** in DTM.

Do we process data dumps (leaks) and alert customers to any matched content?

No. Currently we do not do any dump analysis or dump indexing that feeds into DTM.

What about card dumps that are released within Card Shops and Markets? Why are these not covered?

There are sites that offer up tradition shop listings with items for sell and then at the same time they release small dumps of free items, most recently, dumps of full credit cards. Although these are very similar to a "shop listing" they aren't available in the same way a typical shop listing is presented in the system. Our automated scrapers do not pick them up. It requires a manual download of the dump, an inspection of the data format and some type of post-processing. These are not covered in DTM currently for this automation reason, but also because there is not a current mechanism to push these to Research Tools without essentially publishing the full credit card data to all customers. This is similar to the problem of how credentials are processed. Pushing the data requires some RBAC and redacting of fields or entire documents or document types to only the customers with a need to know.

Are Marketplaces, such as Genesis data covered in DTM?

Currently there are several card shops and other marketplaces covered by our collection and available internally in Bazaar. There are three types of listings we currently collect across all of the shops:

- **CC**: Credit cards (CC) for sale.
- **Accounts**: Access (credentials) to some type of online service (gmail, paypal, or Spotify).
- **Servers**: Access to a online server, usually through remote desktop protocol (RDP) or ssh (secure shell).

Currently Research Tools supports all shop listing content but not all fields are rendered. Use the JSON view for more detail.

Does DTM cover Ransomware?

In-depth coverage is generally covered in Mandiant Advantage Threat Intelligence (MATI) Fusion reporting.

DTM covers Ransomware from a couple of different angles.

1. DTM provides coverage on Ransomware naming and shaming sites, where actors leak content obtained from Ransomware related activities.
2. DTM provides coverage on many Forums with illicit content covering Ransomware topics from different angles. A search on the MATI, shows matches from Forums such as XSS, CenterClub, Sinister, RAMP, Breached and others.

Does DTM track exploits that are for sale?

DTM provides coverage on forums and markets where various cyber related elicit activity is occurring or expected to occur. Exploits might be discussed, rented, sold or purchased as part of this coverage but there is no guarantee of coverage. Often times high-value exploits are coveted and discussed in smaller sharing groups that might not be observed easily.

I've heard other vendors can provide full credit card numbers. I see lots of hits on customer bins but not the full card number. Why is that?

Most of the partial credit card numbers (BINs) we sees are from markets selling the full number to expected buyers. There is not benefit for the seller to expose the full card number to anyone other than the buyer. There are instances where competitors might purchase these card numbers and then provide these full numbers to attract potential customers.

There are other places where full credit card numbers might show up such as pastes or web content, but this is not the norm.

I see a lot of data in Research Tools but a lot of doesn't seem actionable. Why does Mandiant have Intel that's not actionable?

The data in Research Tools is provided to users intentionally in a raw state. The intent is provide customers with what we observe as we observe it. A given single piece of raw data is rarely actionable on its own. Often it needs some context and follow-on research or analysis before it is actionable or "actionable intel."

I see a burst of domain_discovery alerts and data with some domains are from the previous month. Any explanation for that?

As of April 2023, the bulk of the domain discovery events come from two different sources: Zonefiles IO and WhoisDS. Zonefiles occasionally has a monthly spike of events.

Why might an email appear as "invalid" when adding users to DTM alerts using Email Alert Notification Settings?

Email addresses will be set to `invalid` if any emails to that email address bounce or result in a complaint (such as being marked as spam). When this occurs, the recipient must work with their email provider/admin to remediate the bounce/complaint, and then go back into their DTM email notification settings and re-validate the `invalid` email address. To re-validate an email address from the email settings you have to remove and re-add the email address.

What if I have feedback, suggestions, or problems with DTM?

Please reach out to **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.