Mandiant

ON-DEMAND INTELLIGENCE ACCESS

On-Demand Intelligence Access provides Intelligence customers the ability to have our expert analyst team develop succinct, tailored deliverables answering the customer's questions. Customers use the **Ask an Expert system (https://docs.mandiant.com/home/mati-experise-service-how-to-make-a-request)** to submit requests to us, and our experts develop a response using all the resources that empower Mandiant Intelligence—our technical and threat intelligence analysts, their extended access to threat data, and subject matter expertise. The nature of the requests must be related to cyber threats, but can vary in scope, topic, and expected result. Additionally, customers receive enablement support to assist them in integrating and obtaining maximum value from On-Demand Intelligence Access.

When an On-Demand Intelligence Access user submits an intelligence request through the Ask an Expert system, our team will work with the user to scope a response deliverable, and our team will provide the requested deliverable on a jointly established timeline as feasible. This paper describes the typical experience of using the Ask an Expert system.

Ask An Expert

Analyst Access: Example Topics and Requests

The following represent example topics and sample customer requests, but more robust samples are available upon request:

- Actor/Group attribution
  - "We're currently investigating a recent APT28 campaign and are looking for any recent activity, campaigns, targeting verticals by industry and country, as well as newly developed capabilities or changes in TTPs."
- Risk assessment (related to specific threat actors, events, or campaigns)
  - "In light of the UK and Russia geo-political tensions which could spill into the Cyber space we'd like to get a brief piece on the threat landscape around this and approaches Russia and associated actors can use against UK/UK based institutions. E.g. actors, TTP's, known IOC's etc."
- Interpretation of media events/reporting
  - "The attached article mentions the use of a new campaign targeting POS terminals. We have concerns regarding this as we operate POS terminals in a similar environment. Please tell us what you can about this kind of attack, including this specific campaign, and how we can protect ourselves."
- Expansion of previous Mandiant Intelligence reporting
  - "Regarding this actor's claims of access to the dataset seen in 18-02002535, are there any further details on its sale or status? Has the data been validated?"
- Questions regarding adversary activity
  - "We have read on your portal about DD4BC and are curious if you have seen them targeting anyone in our industry."
- Domain and/or IP address intelligence requests
  - "We have observed suspicious traffic going to [domain] for several months. The domain appears to have active registration and resolves to two IP addresses that do not host any other domains. Do you have any additional information about this domain or what might be causing this suspicious traffic?"
- Malware analysis (Behavioral and/or limited reverse engineering)
  - "In the past week we've seen a few hundred messages with an apparently hostile attachment. We'd like IOCs for the attachment and campaign, both for mitigation and for greater understanding of the attack in general, especially as it pertains to motive. We've attached a sample email and attachment from the attack."

- Analysis of customer provided network traffic
  - "Attached is a PCAP of a Struts exploitation attempt. We have noted widespread exploitation attempts of CVE-2017-5638 starting Nov. 2 from the below IP addresses. Questions for Analysts:
    - What is the significance of the string "[redacted]"? What is its expected content?
    - Is it associated with another campaign?
    - What are the IOCs associated with the attempted payload?"
- Drive-by exploitation capture/analysis
  - "We have a user who accidentally clicked on this URL. I would like to request an analysis and better understand the nature of this link, if malware was installed, etc."
- Hostility check against binary or domain
  - "One of our executives is part of an industry planning committee and received (and opened) a suspicious PDF with a title related to the committee's activities. VirusTotal does not identify it as hostile, but did mention several instances of JavaScript, and an unspecified "automatic action" Please check for hostility."

Mandiant Receipt and Processing

Once received, the request is processed and prioritized by Mandiant intelligence teams to determine scope, expectations, and proper resource assignments. Generally, these requests are processed in the order in which they are received. An acknowledgement that the request was received by Mandiant will be sent to the customer.

In emergencies where a request needs immediate attention, users are encouraged to contact Mandiant's team through the provided phone hotline to confirm their request is processed quickly. Such urgent cases could include, for example, a tactical intelligence request associated with an internal breach response at the user's organization. Mandiant Intelligence cannot guarantee that we will be able to deliver responses more quickly than is typical upon request, but we do work with each user to scope an appropriate response timeframe, and will as feasible take into account unusually urgent circumstances when scoping.

Questionable or hostile attachments should be archived (.7z or .zip) and password protected (otherwise, we may not receive a request or it may be delayed due to technical issues). For all requests, any relevant artifacts and context must be provided to Mandiant by the customer.

Coordination

After submission, a Mandiant Intelligence analyst may contact the customer to discuss the request, gather more details, and set expectations. To ensure the best experience possible the customer should be prepared to answer follow-up questions, and to provide details requested by the Mandiant analyst(s) in a timely and complete fashion. Identifying a preferred contact method or phone number by the customer is also helpful to our teams.

Research and Analysis

To fulfill the request, varying levels of analysis and research is needed. This work does not typically involve a high level of custom intelligence development, extensive analysis over large amounts of data, or additional collection activity. The On-Demand Intelligence Access service was designed to answer customer requests with specificity and expedience. See below for what is generally considered out-of-scope for this service.

Resolution

Deliverables or content provided to the customer to resolve the request will vary, depending upon the nature of the request itself. All responses are provided with any additional or supporting intelligence available at the time of the request.

Resolution time on the final deliverable varies, but Mandiant teams will make every attempt to provide analysis within

requested timeframe. As discussed above, our team will work with each user to confirm a timeline is feasible for the agreed-upon scope of their request.

Upon receipt of the response and any related deliverables, the customer will have the opportunity to provide feedback, confirm that expectations have been met, and the request will be closed. Mandiant requests customers confirm receipt of responses and consider whitelisting our e-mails to avoid delay.

Out-of-Scope

To maximize the value On-Demand Intelligence Access provides users, we accept a wide scope of requests that require different types and levels of work. Consequently, our team will work with each submitter to confirm what is feasible within the scope of the service. In many cases, the maximum scope that one deliverable can cover is what is feasible for an expert analyst leading execution to develop and deliver remotely, using Mandiant resources, within 8 total hours of work. However, additional resources or support from other experts are commonly required in combination with the leading analyst's work, and may factor into request scope limitations. Due to the flexibility of this service, these needs vary significantly based on the nature of a request.

Customers can often have us perform larger projects by using multiple On-Demand Intelligence Access entitlements at once. We will confirm when this approach is possible and approved by the submitter during the Coordination phase described above.

Based on this scope description, the following are examples of requests considered out-of-scope for this service.

- Access to any customer information or data outside of the established communication channels in this service description.
- Direct access, configuration, development, or modification of customer-owned technology, systems, and/or data.
- Direct incident response services or consult, including security event investigations or breach notifications related to the customer organization or infrastructure. (Customers often use Analyst Access to obtain intelligence related to incident response efforts, but direct incident response services such as damage assessment are outside the scope of these entitlements.)
- Analysis of disk or memory images
- Use of Mandiant technology to deliver or disseminate intelligence on behalf of the customer to other parties.
- More than 50 IP addresses or 1 binary file for analysis per request *
- An excess of 10MB of security log data for analysis per request. *

* Larger requests may be feasible to cover by using multiple entitlements at once, as described above.