DATA SHEET

Analyst Access Request

An added benefit of your FireEye Threat Intelligence subscription

An Analyst Access request is an added benefit of your FireEye Threat Intelligence subscription in which you are given access to our threat and technical intelligence analysts. This access can be leveraged for specific questions regarding topics such as the following:

- Actor/Group attribution
- Risk assessment (related to specific threat actors, events or campaigns)
- Interpretation of media events/reporting
- Expansion of previous FireEye Threat Intelligence reporting
- Questions regarding adversary activity
- Domain and/or IP address intelligence requests
- Malware analysis (behavioral and/or limited reverse engineering)
- Network traffic analysis
- Drive-by exploitation capture/analysis
- Hostility check
- General threat or technical questions (malware, third-party reports)

It is important to note that Analyst Access work primarily involves leveraging our resources to answer specific questions and does not typically involve large amounts of custom intelligence creation.

What to Submit

When submitting an Analyst Access there are generally a few pieces of information that we like to have:

- Contact information: Your name, as well as an email and phone number at which to reach you.
- Context: Describe the "who, when, what, why, and how" behind your question or need. The more details you can provide us, the more effective and efficient we can be at quickly and specifically addressing your needs. This context should include related data points and information about the request.

  For example, the following requests provide actionable details and would offer the best chance of a maximally useful response from FireEye Threat Intelligence.
- "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."
- "We have read on your portal about DD4BC and are curious if you have seen them targeting anyone in our industry."
- "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."

Limitations

The following limitations apply to Analyst Access requests:

- No analysis of disk or memory images
- No on-site work
- Maximum of 50 IP addresses per request
- Maximum of 1 binary per request (exceptions can be made depending on need, pending a discussion with the assigned analyst)
- Maximum of 10MB of logs per request

If you have requests outside of these limitations, please work with your Intel Account Manager to help connect you with the appropriate resource.

How to Submit an Analyst Access request

1. FireEye Intelligence Portal: log in to **https://intelligence.fireeye.com**, and go to "Support > Analyst Access" to submit your request.
2. Email: Send an email to **analystaccess@fireeye.com** to initiate your request, which will be processed as our workload permits.
3. Phone: For urgent submissions, call **1-855-434-7339** to be connected with an analyst.

What to Expect

After you submit your request a FireEye Threat Intelligence analyst will reach out to you to discuss your request and to set expectations. In order to ensure the best experience possible please be prepared to answer follow-up questions and to provide details requested by the analyst(s) in a timely and complete fashion.

Turnaround time on the final deliverable varies but we will make every attempt to provide analysis within requested timeframe. Priority requests (provided to Level 3 Intelligence Optimization customers and submitted via phone) are placed at the front of the queue, while all other requests are handled in the order in which they are received.

Table 1. Analyst Access allocations.

The Intelligence Enablement Support levels provide the following number of Analyst Access requests per quarter:
Intelligence Coordination (L2) = 1 0 per quarter
Intelligence Optimization (L3) = 25 per quarter (includes two priority requests)

For questions about the Analyst Access process, or to see examples of Analyst Access requests and results, contact **intelligence-enablement@fireeye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.