Mandiant

# THREAT INTELLIGENCE INTEGRATIONS

Threat Intelligence Integrations are an important component of TAAM, allowing you to bring your threat intelligence information into the Validation Platform. Both threat intelligence Platforms (TIPs) and Threat Intelligence Feeds (TIFs) can be integrated, including:

| Integration Name | Vendor | Supported Version/API |
|---|---|---|
| **Anomali** (https://docs.mandiant.com/home/msv-anomali) | Anomali | 2.5.5+ |
| **CrowdStrike Intel** (https://docs.mandiant.com/home/msv-crowdstrike-intel) | CrowdStrike | API V1 and V2 |
| **Mandiant Threat Intelligence** (https://docs.mandiant.com/home/msv-mandiant-threat-intel) | Mandiant | API V4 |
| **Intel471** (https://docs.mandiant.com/home/msv-intel471) | Intel 471 | N/A |
| **Threat Connect** (https://docs.mandiant.com/home/msv-threat-connect) | Threat Connect | API V2 |
| **Threat Quotient** (https://docs.mandiant.com/home/msv-threat-quotient) | ThreatQuotient | N/A |

These integrations focus on adversaries rather than Indicators of Compromise (IOCs), and are used to populate the Threat Actor Library. Through API calls, the Validation Platform collects information. The following adversary types are available for the integrations listed:

| Threat Intelligence Integration | Threat Actor Group (Name) | Threat Actor (Malware) | Threat Actor Aliases | Threat Actor Country Data | Analyst Description | Tactics, Techniques, Procedures (TTPS) |
|---|---|---|---|---|---|---|
| Anomali | ✔ | | ✔ | ✔ | ✔ | ✔ |
| CrowdStrike Intel | ✔ | ✔ | ✔ | | ✔ | |
| Threat Connect | ✔ | | ✔ | ✔ | ✔ | ✔ |
| Mandiant Threat Intelligence | ✔ | | ✔ | ✔ | ✔ | ✔ |
| Intel471 | | ✔ | | | ✔ | |

By default, threat intel Integrations sync every 24 hours. These times can be adjusted, with a minimum frequency of 15 hours. You can also manually sync if necessary, or pause the integration.

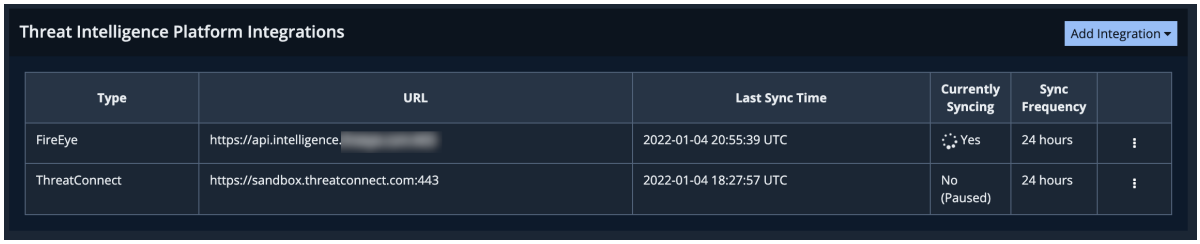


Some TIPs and TIFs have rate limits, including daily limits, on their APIs, so you do not want to sync too often. If you have reached your rate limit and try to sync, the sync fails silently because the APIs do not provide notification that the rate limit has been met. If you try to sync and it does not allow you to, wait a few hours and try again. If you cannot wait, you can try using an API key tied to a different account since rate limits are often by user.

When your integration syncs the first time, two things occur:

- Threat Actor profiles are created
- Two types of TAAM-specific Evaluations are created: General TAAM Evaluations and Priority TAAM Evaluations. For more information about these Evaluations, see **TAAM Evaluations (https://docs.mandiant.com/home/taam-evaluations)**.For more information about these Evaluations, see the TAAM Guide.

TAAM-specific integrations are managed on the Integrations page. All integrations support proxy use. See the Admin guide for additional information on setting up the proxy assignment.




Threat Intelligence Platform Integrations table on Integrations Page