

ELASTIC SIEM INTEGRATION

This feature is released as a Public Preview. Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to [Support](#). (<https://docs.mandiant.com/home/mandiant-support-cases>)

The Mandiant Advantage integration for Elastic SIEM lets you retrieve Indicators of Compromise (IOCs) from Mandiant Advantage Threat Intelligence (MATI). These indicators can be used for correlation in Elastic SIEM to help discover potential threats. MATI gives you access to unparalleled visibility and expertise to understand the threats that matter most to your business.

Prerequisites

- An Elasticsearch instance for storing and searching your data.
 - You can use Elasticsearch Service on Elastic Cloud (recommended), or self-manage the Elastic Stack on your own hardware.
- API access Key ID and Secret generated from the MATI platform to authenticate requests from Elastic.
- Network connectivity to <https://api.intelligence.mandiant.com> over port 443

Compatibility

- This integration has been tested against the MATI API v4.

Get API Key ID and Secret



To obtain a **Service API Key** (which is tied to an organization rather than an individual user) for use with third-party security technologies such as a SIEM, contact [Support](#) (<https://www.mandiant.com/support>).

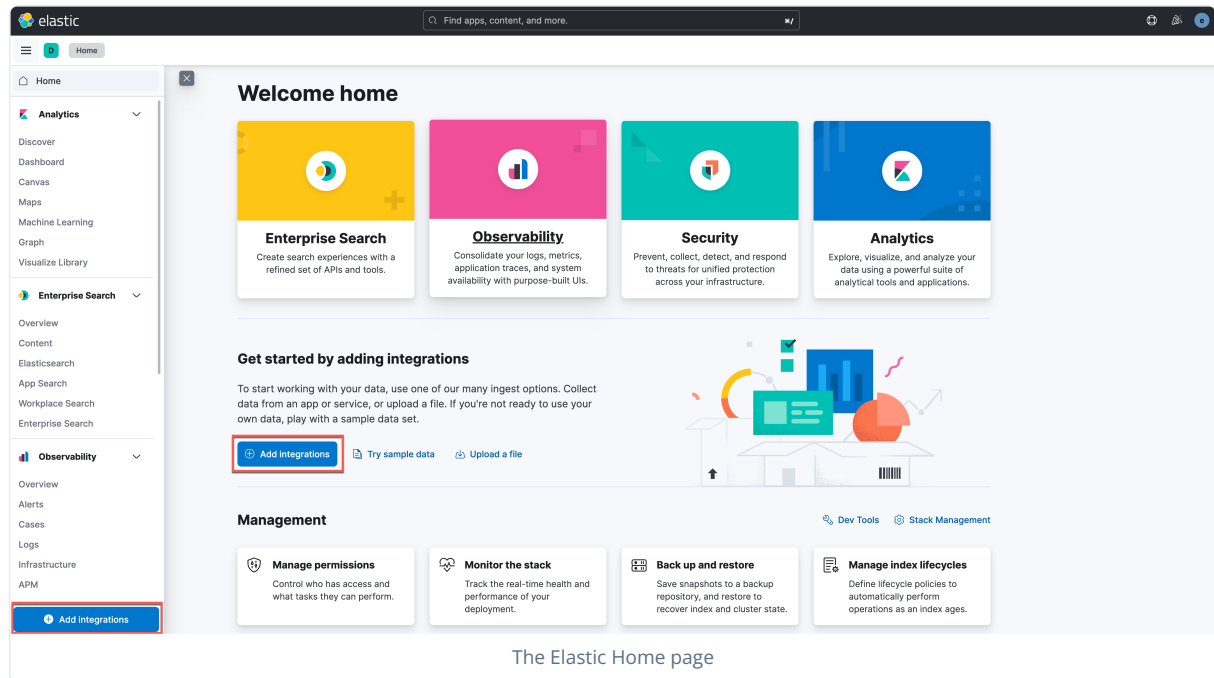
To obtain an API Key ID and Secret for an individual user account, perform the following:

1. Navigate to the Mandiant Threat Intelligence web console.
2. Click **Account Settings**.
3. Select **API Access and Keys** from the navigation menu.
4. Click **Get Key ID and Secret**.
5. Copy and store the displayed values in a secure location.

Installation

Complete the following workflow to set up and install the integration.

1. Log into the Elastic SIEM web console.
2. Click **Add Integration**.

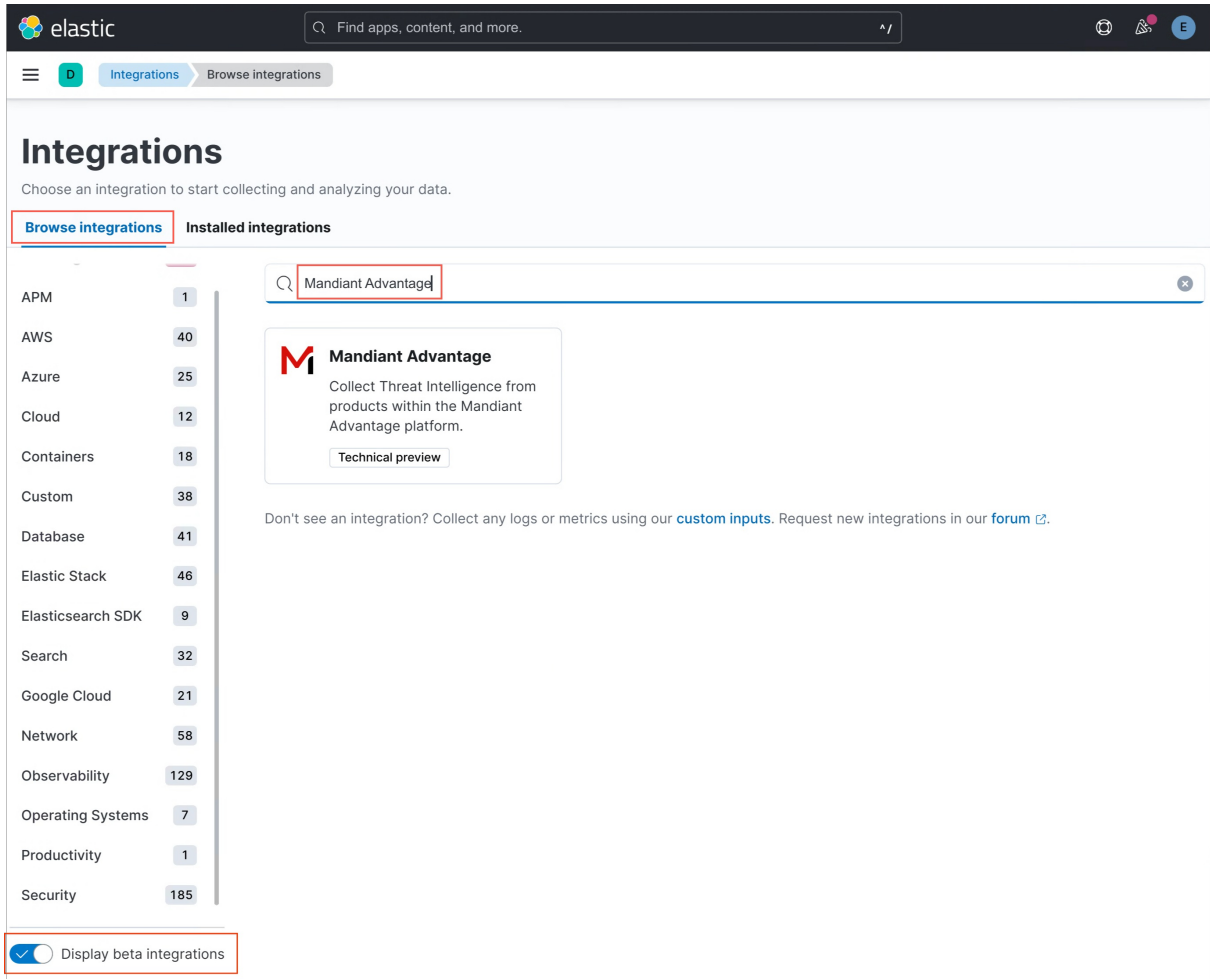


3. Navigate to the **Browse integrations** tab.
4. Enter "Mandiant Advantage" in the **Search** field.



Be sure the option to **Display beta integrations** is enabled.

5. Click **Mandiant Advantage**.



elastic Find apps, content, and more.

Integrations Browse integrations

Integrations

Choose an integration to start collecting and analyzing your data.

Browse integrations Installed integrations

APM 1

AWS 40

Azure 25

Cloud 12

Containers 18

Custom 38

Database 41

Elastic Stack 46

Elasticsearch SDK 9

Search 32

Google Cloud 21

Network 58

Observability 129

Operating Systems 7

Productivity 1

Security 185

Display beta integrations

Mandiant Advantage

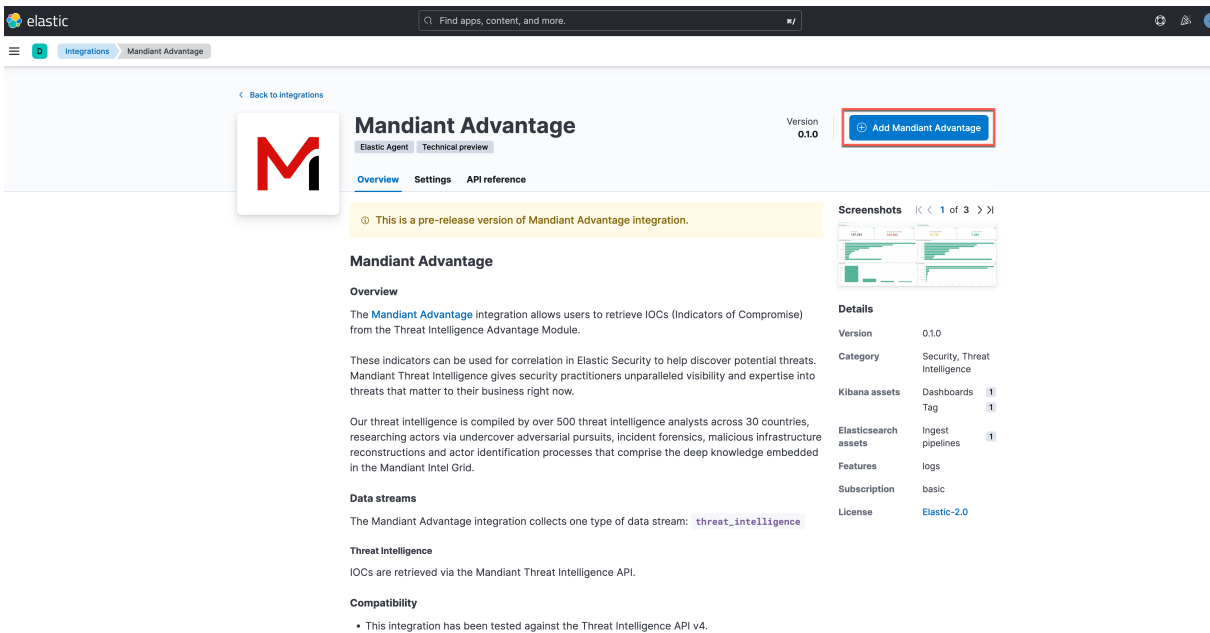
M **Mandiant Advantage**

Collect Threat Intelligence from products within the Mandiant Advantage platform.

Technical preview

Don't see an integration? Collect any logs or metrics using our [custom inputs](#). Request new integrations in our [forum](#).

6. Click **Add Mandiant Advantage**.



elastic Find apps, content, and more.

Integrations Mandiant Advantage

Back to Integrations

M **Mandiant Advantage** Version 0.1.0 **Add Mandiant Advantage**

Elastic Agent Technical preview

Overview Settings API reference

This is a pre-release version of Mandiant Advantage integration.

Mandiant Advantage

Overview

The **Mandiant Advantage** integration allows users to retrieve IOCs (Indicators of Compromise) from the Threat Intelligence Advantage Module.

These indicators can be used for correlation in Elastic Security to help discover potential threats. Mandiant Threat Intelligence gives security practitioners unparalleled visibility and expertise into threats that matter to their business right now.

Our threat intelligence is compiled by over 500 threat intelligence analysts across 30 countries, researching actors via undercover adversarial pursuits, incident forensics, malicious infrastructure reconstructions and actor identification processes that comprise the deep knowledge embedded in the Mandiant Intel Grid.

Data streams

The Mandiant Advantage integration collects one type of data stream: `threat_intelligence`

Threat Intelligence

IOCs are retrieved via the Mandiant Threat Intelligence API.

Compatibility

- This integration has been tested against the Threat Intelligence API v4.

Details

Version	0.1.0
Category	Security, Threat Intelligence
Kibana assets	Dashboards 1 Tag 1
Elasticsearch assets	Ingest pipelines 1
Features	logs
Subscription	basic
License	Elastic-2.0

Screenshots 1 of 3

7. Enter an **Integration name**.

8. Optional: Enter a **Description** for the integration.

[< Cancel](#)

M Add Mandiant Advantage integration

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings
Choose a name and description to help identify how this integration will be used.

Integration name
ti_mandiant_advantage-1

Description Optional

[> Advanced options](#)

Collect data from Mandiant Advantage products 2 errors [Change defaults](#) [^](#)

Settings
The following settings are applicable to all inputs below.

Enable request tracing
 [×](#)
The request tracer logs requests and responses to the agent's local file-system for debugging configurations. Enabling this request tracing compromises security and should only be used for debugging. See [documentation](#) for details.

9. Enter your **Threat Intelligence API Key ID** and **Threat Intelligence API Key Secret** generated from the MATI platform.

Mandiant Threat Intelligence
Collect IOCs from Mandiant Threat Intelligence

Threat Intelligence API Key ID

Threat Intelligence API Key ID is required
Key ID for the Threat Intelligence API.

Threat Intelligence API Key Secret

Threat Intelligence API Key Secret is required
Key Secret for the Threat Intelligence API.

Interval
1h
Interval at which the indicators will be pulled. Supported units for this parameter are h/m/s.

Initial Interval
720h
The time in the past to start the collection of Indicator data from, based on an indicators last_update date. NOTE: Supported units for this parameter are h/m/s.

Minimum IC-Score Optional
80
Indicators that have an IC-Score greater than or equal to the given value will be collected. Indicators with any IC-Score will be collected if the value is set to 0.

Preserve original event
 [×](#)

10. Choose where to add the integration.

- To add this integration to a new set of hosts, click the **New Hosts** tab.
 - Enter a **New agent policy name** to create an Agent policy for the new hosts.
 - Click **Save and continue** to complete the integration installation.

2 Where to add this integration?

New hosts Existing hosts

Create agent policy
Add this integration to a new set of hosts by creating a new agent policy. You can add agent in the next step.

New agent policy name
Agent policy 1

Collect system logs and metrics ⓘ

> [Advanced options](#)

Cancel Preview API request **Save and continue**

- To add this integration to an existing set of hosts, click the **Existing hosts** tab.
 - Select which **Agent policy** to apply.
 - Click **Save and continue** to complete the integration installation.

2 Where to add this integration?

New hosts **Existing hosts**

Agent policy
Agent policies are used to manage a group of integrations across a set of agents.

Agent policy
Elastic-Agent (elastic-package) ▼

0 agents are enrolled with the selected agent policy.

Cancel Preview API request **Save and continue**

API details and usage

Elastic SIEM documentation defines data sources as Data Streams and data storage locations as Log References.

Data streams


- The Mandiant Advantage integration collects one type of data stream: `threat_intelligence`
 - IOCs are retrieved from the `threat_intelligence` for correlation and analysis in Elastic SIEM using the MATI API v4.

Log References


- IOCs retrieved using the MATI API v4 over time can be viewed in the `Threat Intelligence` logs.

API usage parameters

The integration lets you control the timing of API queries and filter the number of IOCs that are ingested.

 Elastic SIEM does not support manual or ad hoc API calls.

- Update the **Initial interval** to modify the frequency of API calls.
 - The time in the past to start collecting Indicator data from MATI, based on an Indicator's `last_update` date.
 - Supported units for this parameter are hours, minutes, and seconds. The default value is 720 hours (equivalent to 30 days).

 You may reduce this interval if you don't want as much historical data to be ingested when the integration first runs.

Mandiant Threat Intelligence
Collect IOCs from Mandiant Threat Intelligence

Threat Intelligence API Key ID

Threat Intelligence API Key ID is required
Key ID for the Threat Intelligence API.

Threat Intelligence API Key Secret

Threat Intelligence API Key Secret is required
Key Secret for the Threat Intelligence API.

Interval

Interval at which the indicators will be pulled. Supported units for this parameter are h/m/s.

Initial Interval

The time in the past to start the collection of Indicator data from, based on an indicators last_update date. NOTE: Supported units for this parameter are h/m/s.

Minimum IC-Score Optional

Indicators that have an IC-Score greater than or equal to the given value will be collected. Indicators with any IC-Score will be collected if the value is set to 0.

Preserve original event

- Update the **Minimum IC-Score** filter to control the number Indicators pulled into Elastic SIEM.
 - Indicators that have an Indicator Confidence Score (IC-Score) greater than or equal to the given value will be collected.



For more information, see [Understanding IC-Score](https://docs.mandiant.com/home/understanding-ic-score) (<https://docs.mandiant.com/home/understanding-ic-score>).

- Indicators with any IC-Score will be collected when the value is set to 0.



To ensure that only high-confidence Indicators are ingested, this value should be set to 80.

Mandiant Threat Intelligence
Collect IOCs from Mandiant Threat Intelligence

Threat Intelligence API Key ID

Threat Intelligence API Key ID is required
Key ID for the Threat Intelligence API.

Threat Intelligence API Key Secret

Threat Intelligence API Key Secret is required
Key Secret for the Threat Intelligence API.

Interval

Interval at which the indicators will be pulled. Supported units for this parameter are h/m/s.

Initial Interval

The time in the past to start the collection of Indicator data from, based on an indicators last_update date. NOTE: Supported units for this parameter are h/m/s.

Minimum IC-Score Optional

Indicators that have an IC-Score greater than or equal to the given value will be collected. Indicators with any IC-Score will be collected if the value is set to 0.

Preserve original event

