Mandiant

MANDIANT MISP COLLECTOR

Developed By:	Mandiant
Latest Version:	2.3.0.8
Last Released:	June 3, 2026
Key Contact:	**Support** (https://docs.mandiant.com/home/customer-support)
Download:	**Docker**: **mandiant-misp-2308.tar** (https://dyzz9obi78pm5.cloudfront.net/app/image/id/6a2079dac071c4757e01ee68/n/mandiant-misp-2308.tar) (MD5: 0f1d4dfbc5c2c4ccc59f520712d9db93)
	Python: **mandiant-misp-2308.zip** (https://dyzz9obi78pm5.cloudfront.net/app/image/id/6a2079dc52b34d934405d5a0/n/mandiant-misp-2308.zip) (MD5: ce22f452ba51a5b40e2f781726f12334)

Overview

This integration collects intelligence from the Mandiant Threat Intelligence v4 API and ingests it into Malware Information Sharing Platform (MISP). The following intelligence is ingested:

- Each Mandiant-tracked Campaign, Threat Actor, and Malware Family is ingested as a MISP Event.
- Each MISP event contains an attribute with the Mandiant description of the intel object.
- Indicators of compromise (IOC) associated with each intel object are added to the MISP event as attributes.
- Each event is tagged with any known target industries, target countries, and motivations (Threat Actor objects only).
- Attack Patterns associated with each intel object are added to the event as a galaxy tag, enabling the MITRE ATT&CK Heat map view on the event page in the MISP interface.
- Where applicable, Threat Actors and Malware families that are associated with an intel object or indicator are correlated with MISP default Galaxy Clusters and added as MISP galaxy tags. Galaxy Clusters in the following MISP Galaxies are considered during correlation: Banker, Botnet, Malpedia, Ransomware, Rat, Stealer, and Threat Actor.

The integration is designed to run on a scheduled basis to ensure that local MISP instances contain the latest intelligence from Mandiant.

Docker

Prerequisites

- A server running the latest version of Docker (can be the MISP server). See the official **Docker documentation** (https://docs.docker.com/engine/install) for installation instructions.
- Docker Compose for container management: Version 2.x.x. See the official **Docker Compose** (https://docs.docker.com/compose/install) documentation for installation instructions.
- MISP: Version 2.5.0+ is recommended for full compatibility. The URL **api.mandiant.intelligence.com** can be accessed through HTTPS on port 443.
- MISP user: The user must be a System Administrator or a user with synchronization permission belonging to the same organization.

Installation

1. Download `mandiant-misp-2-3-0-7.tar` and transfer to your server.
2. Load the container.

```
docker load -i mandiant-misp-2308.tar
```

> The `mandiant-misp` image version 2.3.0.8 should be visible when you run the command `docker image ls | grep mandiant`.

3. Create an environment variables (.env) file using the following template:

```
MATI_API_KEY=
MATI_API_SECRET=
MISP_API_URL=
MISP_API_KEY=
MISP_VERIFY_SSL=true
MISP_ORGC_NAME=
MISP_ORGC_UUID=
IOC_LOOKBACK=
SYNC_MALWARE=true
SYNC_CAMPAIGNS=true
SYNC_ACTORS=true
EVENT_DISTRIBUTION=1
LOG_LEVEL=DEBUG
MIN_THREAT_SCORE=80
IDS_THRESHOLD=90
DISABLE_TO_IDS_FLAG=false
INTERVAL=360
CUSTOM_EVENT_TAG=
CUSTOM_ATTRIBUTE_TAG=
EVENT_THREAT_LEVEL=1
PROXY_ENABLED=false
PROXY_HOST=
PROXY_PORT=
PROXY_USER=
PROXY_PASS=
```

> If you're using the MISP Collector from the same machine as the MISP server, make the following initial updates to the applicable .env file:
>
> - MISP server .env file: `BASE_URL=https://machineIP`
> - MISP Collector .env file: `MISP_API_URL=https://machineIP`

> Run the container with the settings applicable to your environment. For more information on the settings, see the **Settings table (https://docs.mandiant.com/home/mati-mandiant-misp-collector#settings)**.

4. Create a `docker-compose.yml` file:

```
services:
  mandiant-misp:
    image: mandiant-misp:2.3.0.8
    env_file:
      - .env  # Use the .env file for environment variables
```

If you're using the MISP Collector from the same machine as the MISP server, the MISP Collector needs to be in the same Docker network as MISP server. In this scenario, create a `docker-compose.yml` file that defines the network as follows:

```
services:
  mandiant-misp:
    image: mandiant-misp:2.3.0.8
    networks:
      - misp-docker_default
    env_file:
      - .env  # Use the .env file for environment variables
networks:
  misp-docker_default:
    name: misp-docker_default
    external: true
```

5. Start the container:

```
docker compose up -d
```

Upgrade instructions

1. Load the new container image by running the following command:

```
docker load -i mandiant-misp-2308.tar
```

The `mandiant-misp` image version 2.3.0.8 should be visible when you run the command `docker image ls | grep mandiant`.

2. Use the `cd` command to navigate to the directory containing your `docker-compose.yml` file.
3. Edit the `docker-compose.yml` file:
   a. Open the `docker-compose.yml` file in a text editor.
   b. Locate the line that specifies the image version (for example, `image: mandiant-misp:2.3.0.8`).
   c. Change the version number to the desired new version (for example: `image: mandiant-misp:2.3.0.8`) and then save the file.
4. Run the following commands to apply the changes to Docker:

```
docker compose down
docker compose up -d
```

Troubleshooting

1. Use the `cd` command to navigate to the directory containing your `docker-compose.yml` file.
2. Run the following command:

```
docker compose logs -f
```

This command shows the logs for all the services defined in your `docker-compose.yml` file. The optional `-f` flag streams the logs, showing you real-time updates.
You can download a copy of your Docker Compose logs by redirecting the output of the `docker compose logs` command to a file using this command:

```
docker-compose logs -f > my-docker-compose-logs.txt
```

Python

Prerequisites

- MISP: Version 2.5.0+ is recommended for full compatibility. The URL **api.mandiant.intelligence.com** can be accessed through HTTPS on port 443.
- MISP user: The user must be a System Administrator or a user with synchronization permission belonging to the same organization.

Installation

1. Download the `mandiant-misp-v2308.zip` file and transfer it to your server.
2. Unzip the file.
3. Set environment variables by using your operating system's method for setting environment variables. This process varies depending on your OS (Linux, Windows, macOS).

```
MATI_API_KEY=
MATI_API_SECRET=
MISP_API_URL=
MISP_API_KEY=
MISP_VERIFY_SSL=
MISP_ORGC_NAME=
MISP_ORGC_UUID=
IOC_LOOKBACK=
SYNC_MALWARE=
SYNC_CAMPAIGNS=
SYNC_ACTORS=
EVENT_DISTRIBUTION=
LOG_LEVEL=
MIN_THREAT_SCORE=
IDS_THRESHOLD=
DISABLE_TO_IDS_FLAG=
INTERVAL=
CUSTOM_EVENT_TAG=
CUSTOM_ATTRIBUTE_TAG=
EVENT_THREAT_LEVEL=
PROXY_ENABLED=
PROXY_HOST=
PROXY_PORT=
PROXY_USER=
PROXY_PASS=
```

Configure settings applicable to your environment. For more information on the settings, see the **Settings table (https://docs.mandiant.com/home/mati-mandiant-misp-collector#settings)**.

4. Install the required Python libraries by opening a command prompt in the extracted app folder and running the following command:

```
pip install -r requirements.txt
```

5. In the same terminal, run the main Python script using the following command:

```
python main.py
```

Settings

Setting	Required	Default	Description
MATI_API_KEY	Yes		A valid Mandiant API Key
MATI_API_SECRET	Yes		A valid Mandiant API Secret
MISP_API_URL	Yes		The URL of the target MISP instance including the `https` prefix, for example, `https://misp.local`
MISP_API_KEY	Yes		A valid MISP API Key
MISP_VERIFY_SSL	No	True	If the MISP SSL certificate should be verified when connecting to the MISP API, allowed values: `true` or `false`
MIN_THREAT_SCORE	No	80	The minimum value of an indicators Threat Score to ingest
MISP_ORGC_NAME	No	Mandiant	Use to override the MISP creator organization name
MISP_ORGC_UUID	No	ae4bb2ec-b58b-449d-b606-b30c2e26d082	Use to override the MISP creator organization UUID
IOC_LOOKBACK	No	0	Used to calculate the earliest indicator last updated date to include when adding indicator attributes to a MISP event. If the value is zero, all indicators associated with the intelligence object are included
INTERVAL	No	360	The number of minutes to wait between each sync
CUSTOM_EVENT_TAG	No		The value of a custom MISP tag to be added to each event
CUSTOM_ATTRIBUTE_TAG	No		The value of a custom MISP tag to be added to each attribute
EVENT_THREAT_LEVEL	No	1	The MISP threat level to assign to each ingested event, must be `1`, `2`, or `3`
LOG_LEVEL	No	INFO	Defines the log level used by the application, allowed values: `INFO`, `DEBUG`, `WARNING`, `ERROR`
SYNC_CAMPAIGNS	No	True	Defines if MISP events are created from Mandiant Campaigns

Setting	Required	Default	Description
SYNC_MALWARE	No	False	Defines if MISP events are created from Mandiant Malware Families Mandiant tracks many thousands of Malware Families. Enabling this feature results in thousands of new events being added to your MISP instance.
SYNC_ACTORS	No	True	Defines if MISP events are created from Mandiant Threat Actors
EVENT_DISTRIBUTION	No	1	This setting determines the distribution level for events created from Mandiant data. Must be `0`, `1`, `2`, `3`, or `4`.
IDS_THRESHOLD	No	80	This setting defines the minimum threat score an indicator must have to automatically enable the IDS flag in your MISP instance
DISABLE_TO_IDS_FLAG	No	False	This setting allows you to enable or disable the `IDS_THRESHOLD` feature. When set to "True," the IDS flag will not be automatically applied based on the threat score, regardless of the `IDS_THRESHOLD` value
PROXY_ENABLED	No	False	If a proxy server should be used for connections to the Mandiant API, allowed values: `true` or `false`
PROXY_HOST	No		The value of the proxy server host to use
PROXY_PORT	No		The value of the proxy user to use if the proxy server requires authentication
PROXY_USER	No		The value of the proxy password to use if the proxy server requires authentication

Release Notes

- **v.2.3.0.8**
  - This release focuses on improving data accuracy and consistency when ingesting Mandiant Threat Intelligence into MISP.

    Key Fixes:

    - **Improved IOC Attribute Updates:** Fixed an issue where updated Indicators of Compromise (IOCs) from Mandiant were not consistently overwriting existing attributes in MISP. Key attributes such as Threat Score, Confidence, and Severity are correctly updated to reflect the latest intelligence.
    - **Accurate "Last Updated" Timestamp:** Resolved an issue with timestamp handling. The "Last Updated" field for events and attributes within MISP accurately reflects the time the information was last updated in the Mandiant source, distinct from the time it was ingested into MISP.
    - **Version Consistency:** Corrected internal version numbering to consistently reflect v2.3.0.8.
- **v.2.3.0.7**
  - Updated logic to ensure that when IoCs related to a parent object are changed and the parent is not, that these are ingested into MISP.
- **v.2.3.0.6**

    - **New Logic for Ingesting Threat Intelligence Data:** This release introduces a significant change in how threat intelligence data is processed.
        - **Campaigns, Malware Families, Threat Actors:** Each now gets its own dedicated event. This provides a clearer and more structured view of the data. These events include descriptions, associated indicators, and relevant tags like target industry, country, capability (for malware families), and motivation (for threat actors).
    - **Configuration Update:** The `settings.yml` file is now deprecated. Configuration is handled through Docker `.env` files, providing a more streamlined and consistent approach.
    - **Logging Update:** Logs are now written to `docker logs`, making it easier to access and manage log information.
    - **Bug Fixes:** This release includes fixes for several minor bugs identified in previous versions.

- **v.2.1.6**
    - Fixes an issue where Threat Actor Galaxy Cluster sync would fail when the `last_updated` value could not be read from the cache.

- **v.2.1.5**
    - Fixes an issue where Threat Actor Galaxy Cluster sync would fail when a source country was not included in the Mandiant API response.
    - Fixes an issue where Malware Family Galaxy Cluster sync would fail when the last_updated value could be read from the cache.

- **v2.1.0**
    - **New Features**
        - Introduced a new `log_level` setting and refined INFO logging to prevent log files from bloating unnecessarily.
        - Introduced a new `max_report_bytes` setting. When a Mandiant Report is greater than the value of this setting, the report content is split into equal size chunks and a MISP Event Report is added for each part. This setting is to work around a MISP-enforced max size of 64k for an Event Report.
        - Introduced a new `misp_sharing_group` setting to allow MISP Sharing Groups to be set on Events and Galaxy Clusters using the Sharing Group Name. When set, this setting overrides the Distribution level setting for MISP events.
        - Introduced a new `misp_distribution` setting to allow the MISP Distribution level to be set on Events and Galaxy Clusters.
        - Introduced a new `custom_tag` setting that adds the value of the setting as a MISP Tag on Events and Attributes created by the integration.
        - Added support for the new Threat Rating feature for Mandiant indicators. MISP indicator attributes now include a `threat_rating` and threat rating reason tag if a Threat Rating is returned by the Mandiant API.
        - Added new Galaxy Cluster relationships for MITRE ATT&CK Patterns used by a Threat Actor or Malware Family.
        - MISP events are created for Mandiant Campaigns, Threat Actors, and Malware Families. Events include associated TTPs as Galaxy associations (where found) and associated Indicators as attributes or objects.
        - Added `earliest_report` checkpoint to prevent legacy reports being ingested.
    - **Improvements**
        - Updated application to run in Python version 3.11.4.
        - Updated the Mandiant Threat Intel Client to version 0.1.20.
        - Added in-memory Galaxy Cluster caching to improve performance and reduce repetitive API calls to MISP.

        - Indicator attributes and objects are now periodically updated to reflect the latest IC-Score, Last Seen date, and threat rating telemetry.
        - ICS Network Activity and Operational Technology Phishing Roundup reports are now grouped into a single MISP event to prevent over-correlation in MISP.
    - **Bug Fixes**
        - Fixed an issue where log compression and rotation only ran at application startup. This process now runs at the start of each execution.

- **v2.0.2**
    - Fixed an issue where upgrades from versions 2.0.0.x to 2.0.1 would fail and the container would enter a continuous restart loop.

- **v2.0.1**
    - Added setting to control PyMISP logging levels for `stdout` output. The default setting is `CRITICAL`.
    - `SSL certificate stdout` warnings are now suppressed when the `misp_verify_ssl` setting is set to `False`.
    - Log files are now rotated daily. Rotated log files are compressed and old log files are removed after the number of days defined in the `runtime log_rotation_days` setting.

- **v2.0.0.9**
    - Fixed issue with rendering MISP event info when a Mandiant report title contains a \n newline character
    - Fixed a container crash when the Executive Summary in reports had a type of `None`
    - Updated timezone awareness for start and end date to avoid missing reports
    - Fixed an issue with Galaxy tagging for indicator attributes when an attributed association was not found in the local MISP galaxy
    - Fixed an issue caused by file indicators without SHA1 and SHA256 values

- **v2.0.0.8**
    - Fixed an issue where duplicate events were created for specific Mandiant Reports
    - Fixed an issue where reports could be missed by the sync process due to timezone awareness when calling the Mandiant API

- **v2.0.0.7**
    - Updated Mandiant Intel Client to v0.1.14
    - Additional indicator tagging available at the attribute level
    - Set IP address attribute type as `ip-src` for ICS Reports
    - Added IDS Flag for IoCs over threshold
    - Fixed failing Threat Actor Galaxy Cluster sync
    - Fixed container crash when exception is raised in Galaxy Cluster Sync

- **v2.0.0.6**
    - Added Third Party licenses folder and page in Config App
    - Updated Mandiant Threat Intel Client to v0.1.11
    - Added support in `docker-compose` to restart the container on reboot

- **v2.0.0.5**
    - Fixed an issue in settings validation when a Proxy is defined with no username or password
    - Fixed an issue where the Mandiant API returns the aliases key as list of strings instead of the expected list of dictionaries
    - Fixed an issue where the container crashes on `HTTP 405` response from MISP

- **v2.0.0.3**

- All interactions with MISP now use the PyMISP library
- Added utility to the Config application to remove duplicate events caused by legacy versions (1.1.x) of the integration
- Added additional error handling to prevent container crashes when connections to the Mandiant API fail
- Added Mandiant theming to the Config Application
- Removed dependencies on local cache files for incremental updates