PALO ALTO CORTEX XSOAR INTEGRATION

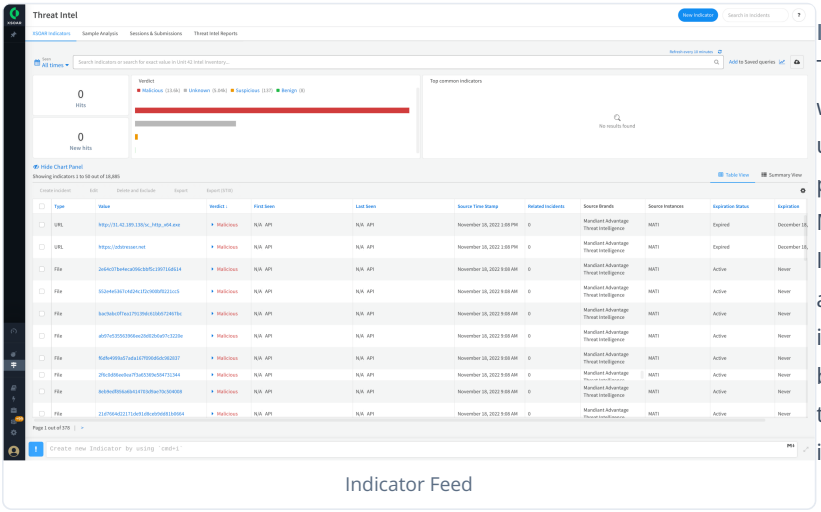
Developed By:	Mandiant
Latest Version:	1.1.1
Last Released:	September 22 2024
Key Contact:	**Support (https://docs.mandiant.com/home/mandiant-support-cases)**
Download:	**Mandiant Advantage Threat Intelligence Cortex XSOAR Integration (https://cortex.marketplace.pan.dev/marketplace/details/MandiantAdvantageThreatIntelligence/)**

Cortex XSOAR from Palo Alto Networks is a security orchestration, automation, and response (SOAR) platform. The Cortex SOAR Integration collects Indicators from the Mandiant Advantage Threat Intelligence (MATI) platform and adds them to the Cortex XSOAR indicator store for use during automated enrichment and investigations.

Cortex XSOAR unifies case management, automation, real-time collaboration, and threat intel management to serve security teams across the incident lifecycle.

For more information about this integration, explore the tabs that follow.

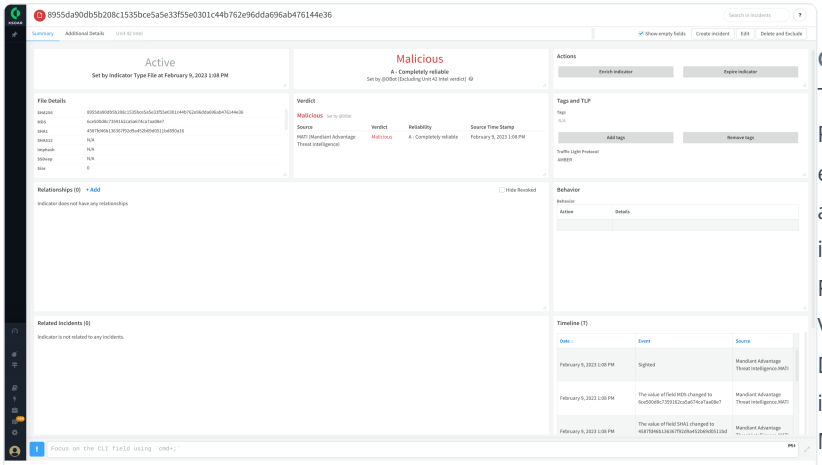
Features



Indicator Feed

Indicator Feed

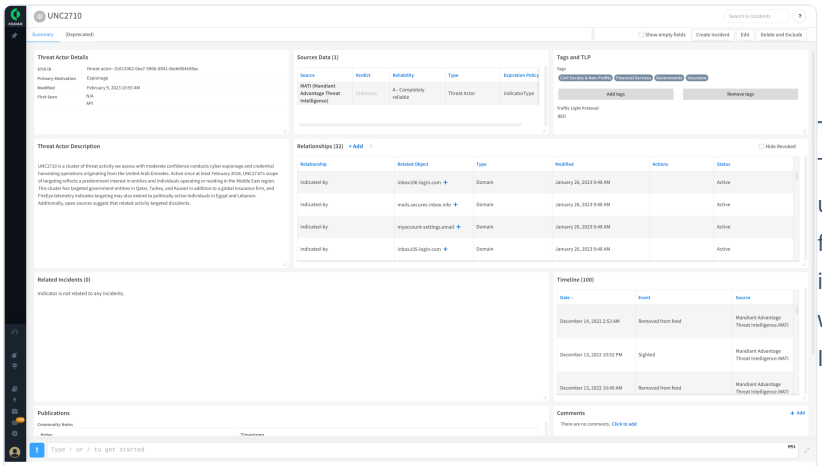
The integration features an Indicator Feed, which automatically fetches new and updated indicators from MATI and populates them into Cortex XSOAR. Malware Families, Threat Actors, and Indicators of Compromise (IOCs) can all be automatically ingested. If enabled, this integration will also create relationships between various indicators, to enable you to easily navigate through all available information.



Generic Reputation Commands

Generic Reputation Commands

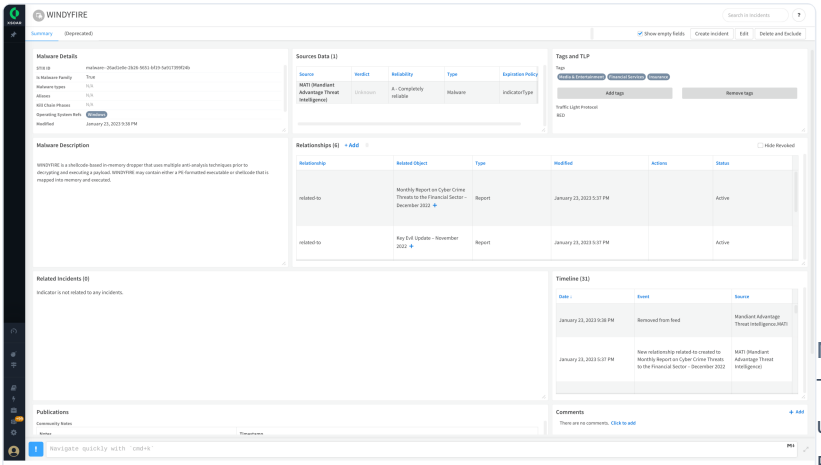
The integration supports Generic Reputation Commands, which lets you easily enrich an existing Indicator with additional information from MATI. This integration supports all available Generic Reputation Commands, including Common Vulnerabilities & Exposures (CVEs), File, Domain, URL, and IP. If enabled, this integration will also link to any associated Mandiant Advantage reports.



Threat Actor Lookup

Threat Actor Lookup

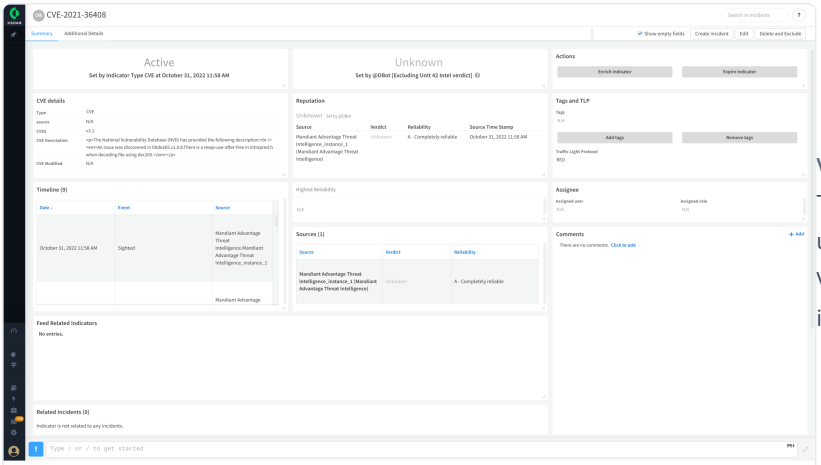
The integration features the ability to look up a Threat Actor by name. If an actor is found, this will populate the Threat Actor into Cortex XSOAR. If enabled, relationships will also be created to other Cortex XSOAR Indicators.



Malware Lookup

Malware Lookup

The integration features the ability to look up a Malware Family by name. If a Malware Family is found, it will be populated into Cortex XSOAR. If enabled, relationships will also be created to other Cortex XSOAR Indicators.



Vulnerability Lookup

Vulnerability Lookup

The integration features the ability to look up a Vulnerability by the CVE ID. If a Vulnerability is found, it will be populated into Cortex XSOAR.

Prerequisites

- An active Cortex XSOAR instance
- Network connectivity to **https://api.intelligence.mandiant.com** over port 443

This integration works with any edition of Cortex XSOAR, but limits and restrictions may apply to which features are available. See the **Cortex XSOAR License Documentation** (https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Licenses) for additional information on limits and restrictions.

Get API Key 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.

Setup and installation

Version 1.1.1 supersedes all previous versions of the Mandiant Advantage Threat Intelligence integration for Cortex XSOAR. Additionally, beginning with version 1.1.1 of this integration, feed and enrichment are split into two separate integrations.

To upgrade from a previous version of the Mandiant Advantage Threat Intelligence integration for Cortex XSOAR, consult the next section titled **Upgrade from a previous version**. For new installations of this integration, skip to the section titled **Install the integration**.

Upgrade from a previous version

To upgrade from an earlier version of this integration, follow these steps:

1. Note the instance name of your existing Mandiant Advantage Threat Intelligence integration instance. This is needed in step 4a.
2. Remove all instances of existing Mandiant Advantage Threat Intelligence integrations.
3. Optional: Remove the integration from your XSOAR server.
4. Remove all indicators created by the previous version of this integration. To do this:
    a. Open the Threat Intel page and perform an All Time search using this query: `source Instances:"INSTANCE_NAME"`, where *INSTANCE_NAME* is the name of your old integration instance (collected previously, in step 1).
    b. Select all indicators.
    c. Click **Delete and Exclude**.
    d. In the Delete and Exclude popup, select the **Do not add to exclusion list** checkbox and click **Delete and Exclude**.
5. Once the indicator deletion process completes, install the new version of the integration as outlined in the following section.

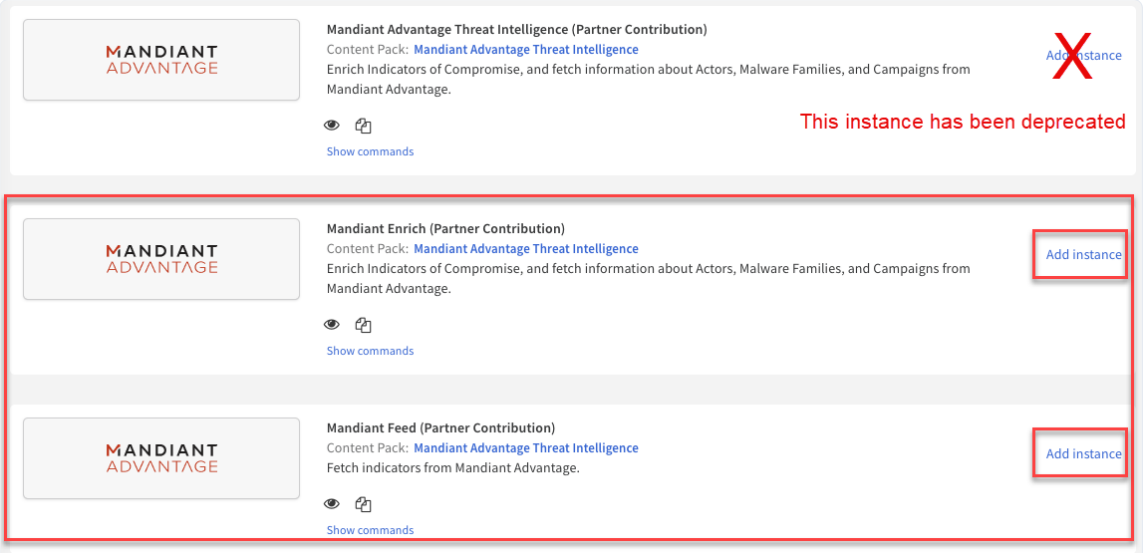
Install the integration

1. Install the Mandiant Advantage Threat Intelligence Cortex XSOAR Integration from the CORTEX Marketplace and

add the Mandiant Advantage Threat Intelligence Content Pack: **https://cortex.marketplace.pan.dev/marketplace/details/MandiantAdvantageThreatIntelligence/**

2. Click **Add Instance** for the instance of the integration that you want to add:
   - Mandiant Enrich
   - Mandiant Feed

> The Mandiant Advantage Threat Intelligence instance of this integration is deprecated and no longer used. It is retained for technical reasons related to Palo Alto Networks (PANW) requirements.



Integration Instance Settings

3. Configure each instance of the integration to suit your needs. Settings include fields such as **Name**, as well as **API Key** and **Secret Key** from the MATI platform.

> For integration-specific settings for each integration, see:
> - **MATI XSOAR Feed Integration (https://docs.mandiant.com/home/mati-xsoar-feed-integration)**
> - **MATI XSOAR Enrichment Integration (https://docs.mandiant.com/home/mati-xsoar-enrich-integration)**

4. Click **Save & exit**.

Set up Threat Score

The Mandiant Threat Score is included with the feed integration. To use this feature, you must add it to your indicator layouts in XSOAR. Follow these steps:

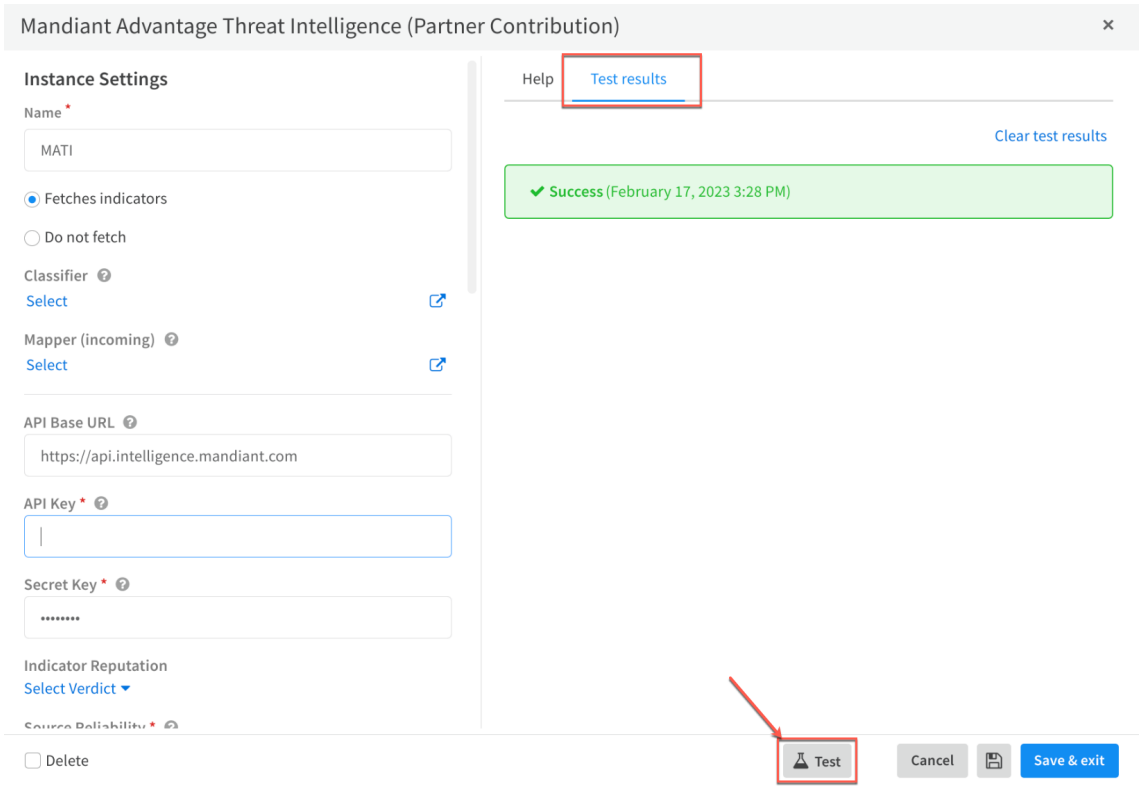
1. In your XSOAR environment, go to **Settings > Objects Setup > Indicators**.
2. Click **Field**, then click **New Field**.
3. Configure the Field using the following values:
   - **Field Type**: Select **Number**.
   - **Field Name**: Enter `Mandiant Threat Score`.
   - **Add to Indicator types**: Ensure that **Domain**, **IP**, **File**, **URL** are added.
   - **Indexing**: Enable **Make data available for search**.

- **Machine Name**: Enter `mandiantthreatscore`.

4. Save your changes.

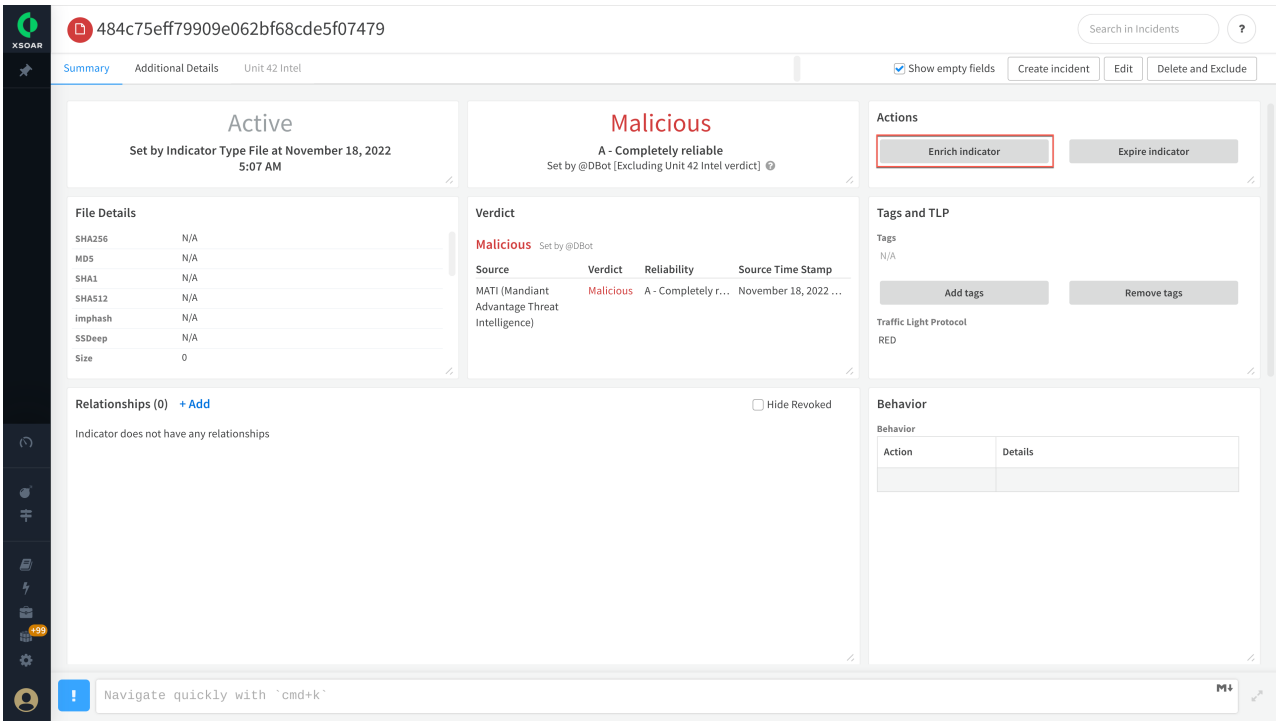
Verify connectivity

1. Navigate to the **Test results** tab and click **Test**.

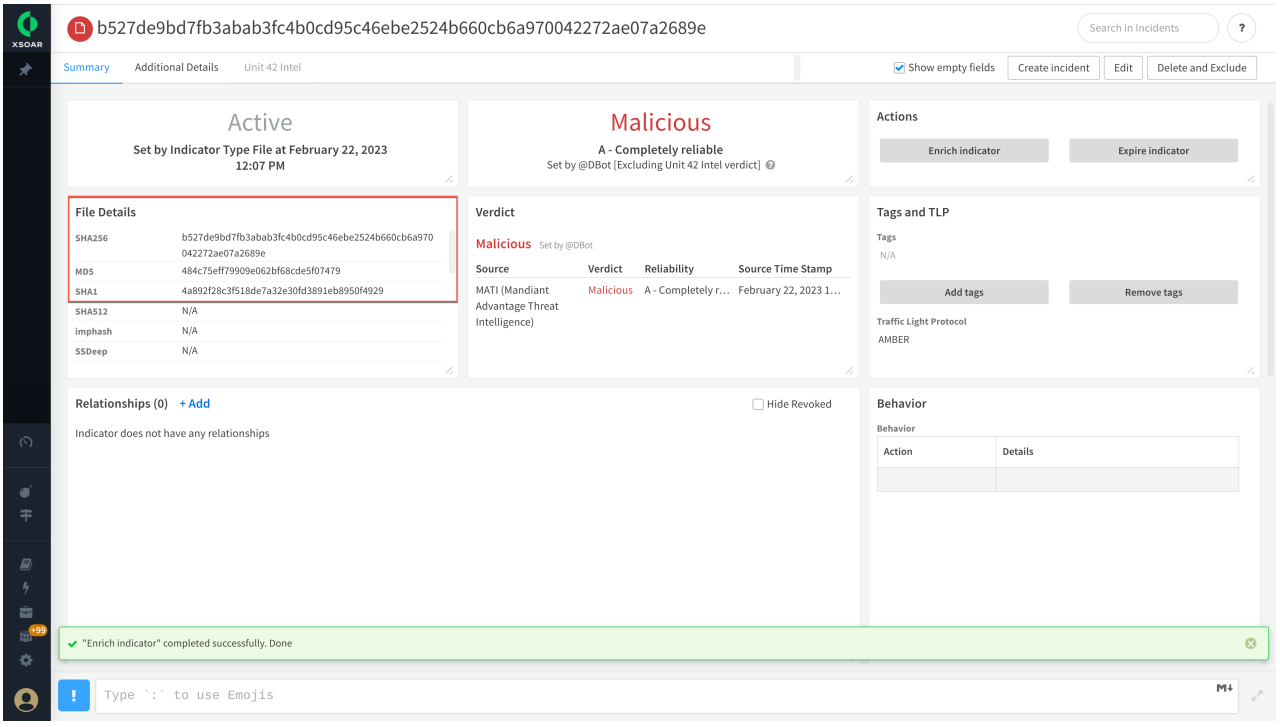


Indicator Enrichment

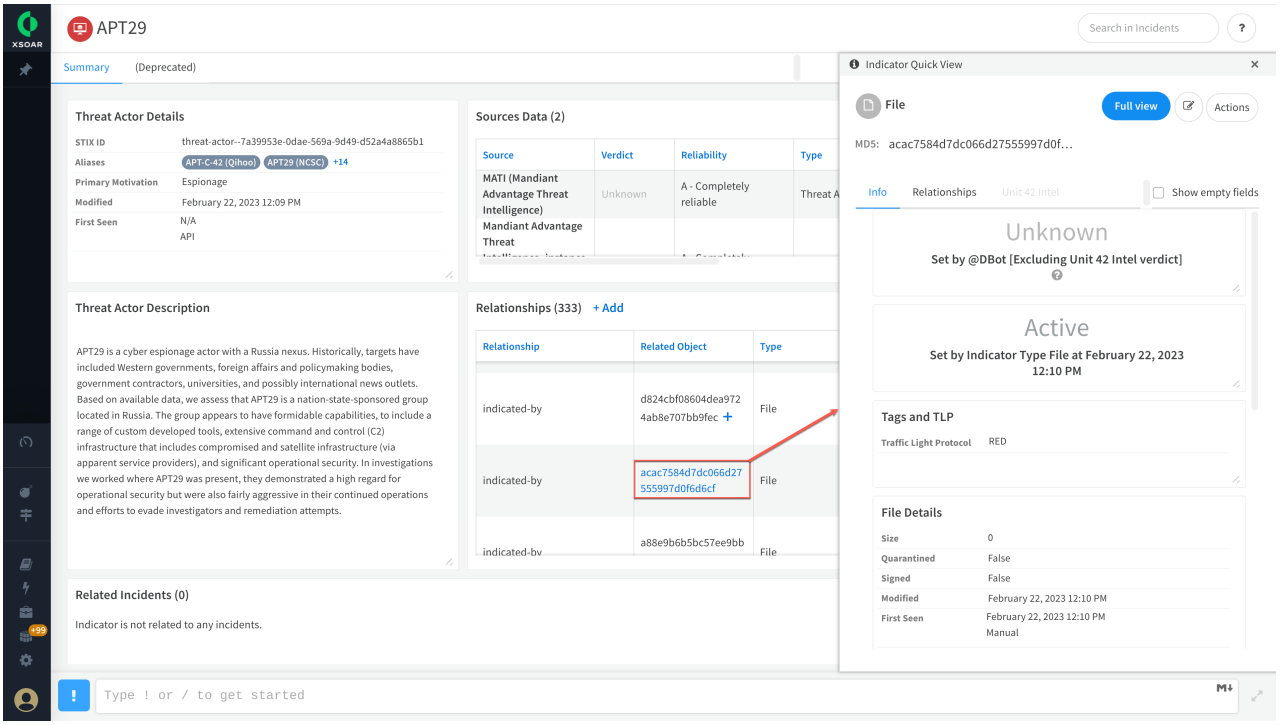
Indicators can be enriched with additional threat intelligence from Mandiant by clicking **Enrich Indicator**. This triggers an immediate pull request for the MATI API to collect any data associated with the indicator. Collected data may include reports, file hashes, verdict (benign, suspicious, or malicious), reliability, tags, and **traffic light protocol (TLP) (https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage)** status.



In this example, additional file details are included post-enrichment:



Items in the **Relationships** list are also populated with MATI data. This feature lets you pivot between threat actors, malware families, and other associated entities directly within Cortex XSOAR.



The ability to pivot and explore associated entities from the **Relationships** list requires the Threat Intelligence Management (TIM) license with your Cortex XSOAR subscription.

Troubleshooting

If an error occurs, provide the exact error message from Cortex XSOAR. If requested by Mandiant Support, also provide a Log Bundle from Cortex XSOAR. Instructions for creating and downloading a Log Bundle can be found in the **Cortex XSOAR Documentation (https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.5/Cortex-XSOAR-Administrator-Guide/Create-a-Log-Bundle)**.