Mandiant

INDICATOR THREAT SCORE METHODOLOGY

Threat Score is the evolution of IC Score, and it is the recommended default for assessing the impact of an Indicator. IC Score continues to be supported for backward compatibility.

Indicator Threat Score is a measure of the likelihood that an Indicator poses a genuine threat to an organization. It combines Confidence and Severity scoring models to provide a simple and easily understood metric. It lets you focus and filter only on Indicators with both a high Confidence score and a high Severity Level.

- **Confidence**: Degree of certainty that an Indicator is malicious. In other words, is the Indicator benign or malicious?

  An indicator can be 100% malicious in intent but not something that actually needs to be worried about. For example, a spammer sending a generic spam email can be entirely malicious. But seeing those Indicators in your system doesn't mean you have any problems that need to be addressed.

- **Severity**: Potential impact or damage an Indicator could cause for an organization. In other words, should you care about this Indicator?

The goal is to reduce noise and simplify workflows so you can focus on higher-order activities with greater impact, such as Threat Modeling.

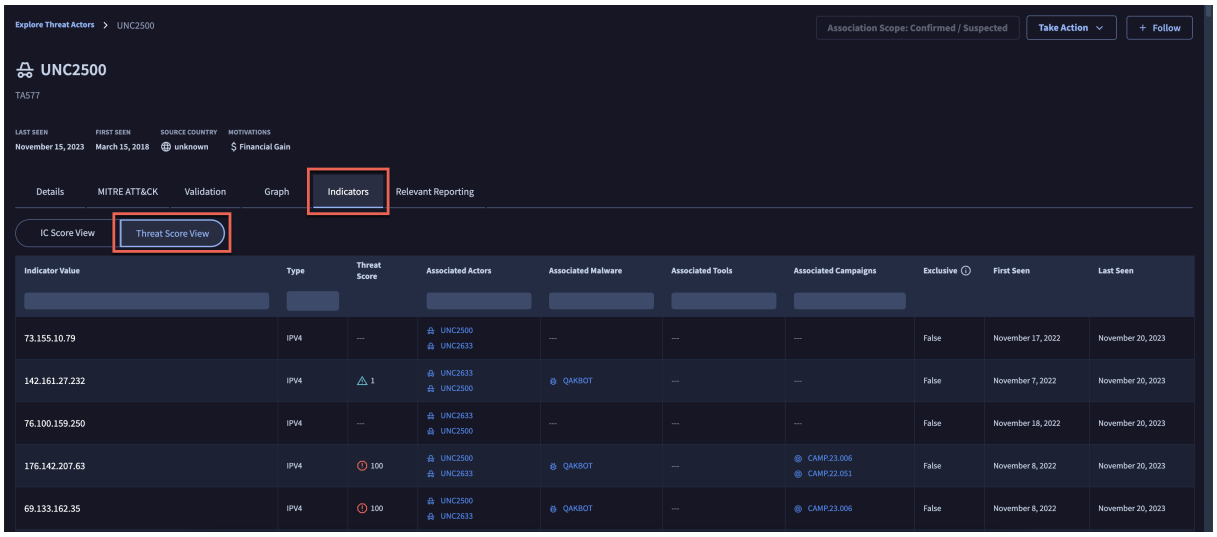
Indicator Threat Score is an analytical score from 0 to 100 that reflects the likelihood of a threat being malicious to an organization. The following are suggested actions based on Indicator Threat Score:

Indicator Threat Score	Suggested Action
Higher than 60	Alert and investigate
40 to 60	Flag as suspicious and worthy of investigation
Less than 40	Ignore as noise
0	Ignore as benign

Explore Indicator Threat Score

Use the following workflow to explore Indicator Threat Score details for an Indicator. This example focuses on an Indicator associated with a Threat Actor.

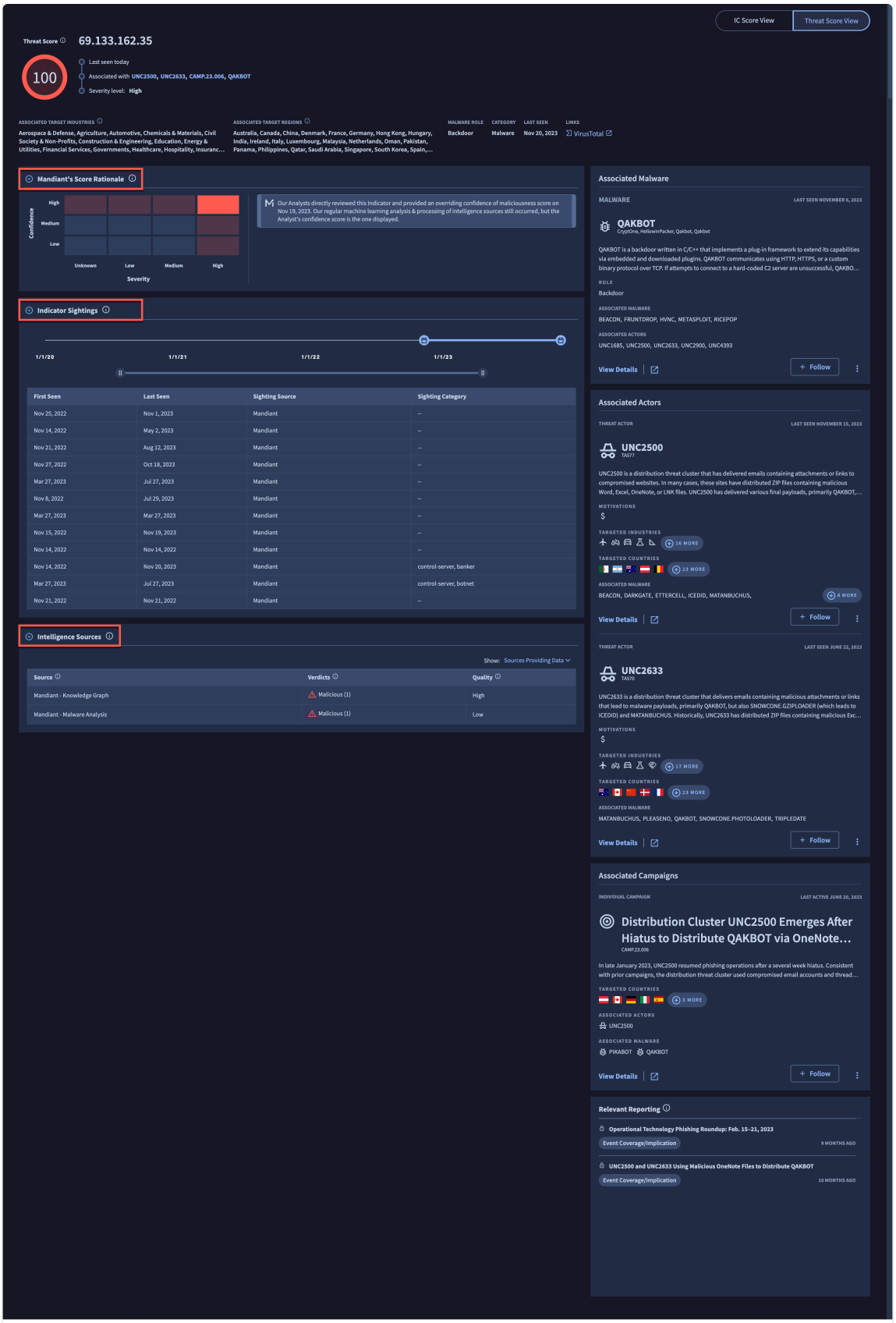
1. Navigate to the Threat Intelligence Dashboard.
2. Click **Explore > Threat Actors**.
3. Select the **Indicators** tab.
4. Click **Threat Score View**.



5. Click any hyperlinked **Indicator Value** to view details associated with calculating its Indicator Threat Score. The specific context and components of the Indicator Threat Score are described in the following sections:
    a. **Mandiant's Score Rationale**: Displays a heat map containing Confidence and Severity Levels.
    b. **Indicator Sightings**: Shows a timeline of Indicator sightings, including a slider that lets you zoom in or out as desired.
        i. Indicator sightings list the different sources which were observed on the displayed dates as malicious, either an analyst or by an automated system.

> These sightings are not always attributed to an Actor, Campaign, or Malware due to lack of corroborating evidence required to release more detailed attribution.

    c. **Intelligence Sources**: Provides detailed context for determining the Indicator Threat Score for this Indicator.
        i. **Source**: The source of the evaluation, which may be either directly from Mandiant or from open source threat data feeds.
        ii. **Verdicts**: Summarized count of malicious or benign verdict responses for each source category.
        iii. **Quality**: Mandiant's assessment of the data quality of the source used in the scoring model.
    d. Widgets are also displayed with additional details related to Malware, Actors, Campaigns, and Relevant Reports that are associated with the Indicator.



Threat Score View of Indicator details

Understand Threat Score Calculation

Indicator Threat Score combines Confidence and Severity scoring models to provide a simple and easily understood metric.

Confidence

The Confidence score of an Indicator captures the degree of certainty in the quality of its malicious content given existing evidence and observation.

Confidence is modeled using a form of semi-supervised learning called weak supervision. This model closely mirrors how an analyst might ask questions to gather and weigh relevant alert information before applying their final judgment.

Confidence Level is calculated using the Indicator Confidence Score (IC-Score) as its foundation. Confidence Level is rated on a linear scale where 0 is no confidence and 100 is full confidence.

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

Confidence Levels are mapped as follows:

- **High**: Confidence Score between 71 - 100
- **Medium**: Confidence Score between 31 - 70
- **Low**: Confidence Score between 0 - 30

Severity

The Severity score of an Indicator categorizes the impact of malicious activities possible for high-confidence alerts. Severity is assessed using additional context, enrichments, and expert judgment downstream of Confidence.

Within the scoring framework, the Confidence score helps initially remove any obvious noise. Any available Mandiant context is then used by the Severity scoring model to further divide Indicators iteratively into the following Severity Levels:

- High
- Medium
- Low
- Benign

As part of the Severity scoring model for an Indicator, at least one of the following Severity Reasons is collectively used to categorize the Severity Level for each Indicator.

> Severity Reasons are directly exposed in the API only.

- **benign**: Known benign Indicators.
- **lowConfidence**: Indicators with a IC-Score less than 80.
- **osint**: Indicators which are only sourced from third-party sources.
- **adwareSource**: Indicators identified as adware.
- **spamSource**: Indicators identified as Spam.
- **scannerSource**: Indicators identified as known internet scanners.
- **cryptoSource**: Indicators identified as known Crypto Miners.
- **attributed**: Indicators with a Mandiant attribution (Actor, Malware, Tool, or Campaign).

- **highPrevalence**: Indicators which are highly prevalent.
- **fintel**: Indicators which are referenced in Mandiant Finished Intel reports.

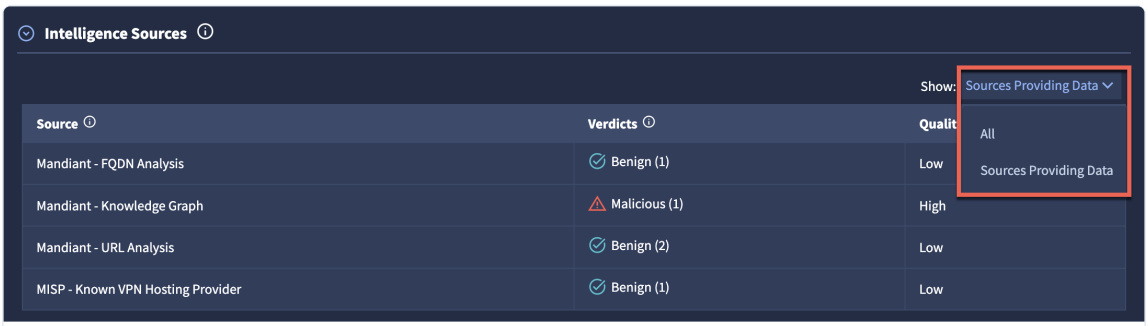
Finally, the Severity Level is used as a multiplier to assign Indicator Threat Scores as weighted values of the original IC-Score. In other words, a Severity Level of High uses a multiplier of 1.0 and Benign uses a multiplier of 0, while Medium and Low fall between these benchmarks.

Review Intelligence Sources

Intelligence sources used to derive Verdicts for Indicator Threat Score originate either directly from Mandiant or from open source threat data.

The **Intelligence Sources** table displays the **Source** and its contributing data source for each **Verdict** displayed. You can choose to display all data sources or only those that contribute to the Verdict.

- Click the **Sources Providing Data** drop-down to select one of the following:
  - **All**: Displays all available data sources, regardless of which contributed to a given Verdict.
  - **Sources Providing Data**: Displays only the data sources that contributed to Verdicts for this Indicator.



Intelligence Sources table in Threat Score View details

The following list includes each **Source** categorized with all available data sources that may be used to contribute to a particular finding.

The displayed list of Sources and their contributing data sources will vary according to the type of Indicator being viewed.

1. Mandiant
   a. Bulletproof Hosting
   b. FQDN Analysis
   c. Knowledge Graph
   d. Malware Analysis
   e. Spam Monitoring
   f. URL Analysis
2. Google
   a. Safe Browsing
3. Crowdsourced Threat Analysis
4. MISP
   a. Dynamic Cloud Hosting (DCH) Provider

   b. Educational Institution
   c. Internet Sinkhole
   d. Known VPN Hosting Provider
   e. Popular Internet Infrastructure
   f. Popular Website
   g. Other

5. Open Source Threat Data Feeds
   a. Aa419
   b. Benkow
   c. Cryptolaemus
   d. Cybercrimetracker
   e. Digitalside
   f. Feodos
   g. Fumik0
   h. Futex.re
   i. Magpie
   j. Malshare
   k. Malwaredomainlist
   l. Openphish
   m. Phishing Database
   n. Phishstats
   o. Phishtank Valid Online
   p. Tds Harvester
   q. Urlhaus
   r. Viriback
   s. Vxvault Virilist