Mandiant

UNDERSTANDING IC-SCORE

Threat intelligence is often difficult to leverage in practice due to the high level of noise and lack of coverage provided by most feeds. A typical organization has to purchase multiple subscriptions and develop ad-hoc methods to evaluate and clean those inputs before they can be used to detect threats.

To overcome this problem, Mandiant assesses and labels indicators of compromise (IOCs) or simply, indicators with an Indicator Confidence Score (IC-Score). The goal of IC-Score is to provide a one-stop solution for customers that intelligently aggregates the (sometimes conflicting) information from a variety of **open-source and Mandiant-proprietary intelligence sources** **(https://docs.mandiant.com/home/mati-ic-score-source-descriptions)** into a single rating. Through the use of machine learning, each source of intelligence is assigned a confidence based on the quality of the intelligence they provide, leveraging both human assessments and large-scale data-driven methods. Ultimately, IC-Score captures the probability that a given indicator is associated with malicious activity (a true positive).

What is IC-Score?

The IC-Score represents the probability that the indicator is malicious (a true positive). To calculate the final probability of maliciousness, the underlying machine learning model incorporates all information available about the indicator, weighted by the learned confidence for each source of information. Since there are only two possible outcomes (malicious or benign), all indicators start with a score of 50% when no information is available – equivalent to a coin flip between whether the indicator is malicious or not. With each additional piece of information, that baseline score is pushed toward either a 0% probability of malicious (a known benign) or a 100% probability of maliciousness (a known malicious). The range of possible scores is interpreted as follows:

Score	Interpretation
`<= 40%`	Known benign/noise
`> 40% and < 60%`	Indeterminate/unknown
`>= 60% and < 80%`	Suspicious
`>= 80%`	Known malicious

Indicator Aging Information

The IC-Score system incorporates new information, refreshes enrichment data, and ages-off old information during specific scoring events, enumerated below:

- A new observation of the indicator on one of our OSINT sources or proprietary Mandiant monitoring systems
- Specific timeout periods associated with each of the source and enrichment for the indicator

The timeout periods are set based on the **last seen** date of the indicator on the respective source or enrichment. That is, after a specified number of days when the indicator was last observed from a given source or when the information was updated by the enrichment service, Mandiant considers the information to be stale and stop considering it as an active factor in calculating the score.

The following table describes important timestamp attributes associated with an indicator.

Attribute	Description
First seen	The timestamp when an indicator was first observed from a given source.
Last seen	The timestamp when an indicator was most recently observed from a given source.
Last updated	The timestamp when an indicator's IC-Score or other metadata was most recently updated due to indicator aging, new observations, or other management processes.

Where is IC-Score used?

IC-Score is used extensively in:

- **Mandiant Advantage Threat Intelligence (MATI)** **(https://docs.mandiant.com/home/mati-getting-started)**
- **Digital Threat Monitoring (DTM)** **(https://docs.mandiant.com/home/dtm-digital-threat-monitoring)**
- **Mandiant Advantage Attack Surface Management (MA-ASM)** **(https://docs.mandiant.com/home/asm-getting-started)**