Mandiant

INDICATOR THREAT SCORE AND CONFIDENCE SCORE SOURCE DESCRIPTIONS

The Indicator Confidence Score (IC-Score) and Indicator Threat Score source descriptions help to contextualize why an Indicator has the score that it does. The descriptions show which categories of systems provided the confidence or threat assessments about an Indicator. Findings from the following Mandiant-proprietary and third-party sources are combined with an assessment of the source's data quality to determine the IC-Score or Threat Score for an Indicator.

For more information, see **Understanding IC-Score** (https://docs.mandiant.com/home/understanding-ic-score) and **Indicator Threat Score Methodology** (https://docs.mandiant.com/home/mati-indicator-threat-score-methodology).

Source	Description
Botnet Monitoring	The Botnet Monitoring category contains malicious verdicts from proprietary systems that monitor live botnet traffic, configurations, and command & control (C2) for indications of botnet infection.
Bulletproof Hosting (https://en.wikipedia.org/wiki/Bulletproof_hosting)	The Bulletproof Hosting category contains sources that monitor registration and usage of bulletproof hosting infrastructure and services. These entities often provide services for illicit activities that are resilient to remediation or takedown efforts.
Crowdsourced Threat Analysis	Crowdsourced Threat Analysis combines malicious verdicts from a wide variety of threat analysis services and vendors. Each responding service is treated as a unique response in this category with its own associated confidence.
FQDN Analysis	The fully qualified domain name (FQDN) Analysis category contains malicious or benign verdicts from multiple systems that perform analysis of a domain. This analysis includes the examination of a domain's IP resolution, registration, and whether the domain appears to be typosquatted.
Google: Safe Browsing	Safe Browsing (WebRisk) is a Google service that provides real-time information about the safety of websites. This assessment is constantly updated by scanning billions of URLs daily and is powered by the same technology that protects Google customers.
GreyNoise Context	The GreyNoise Context source provides a malicious or benign verdict based on data derived from **GreyNoise Context service** (https://docs.greynoise.io/reference/noisecontextip-1). This service examines contextual information about a given IP address, including ownership information and any benign/malicious activity observed by GreyNoise infrastructure.
GreyNoise RIOT	The GreyNoise RIOT source assigns benign verdicts based on the **GreyNoise RIOT service** (https://docs.greynoise.io/reference/riotip). This service identifies known benign services that cause common false positives based on observations and metadata about the infrastructure and services. The service provides two levels of confidence in its benign designation which we incorporate as separate appropriately weighted factors in our score.

Source	Description
Knowledge Graph	The Mandiant Knowledge Graph contains Mandiant Intelligence assessments of indicators derived from analysis of cyber intrusions and other threat data. This source contributes both benign and malicious verdicts to the indicator score.
Malware Analysis	The Malware Analysis category contains verdicts from multiple proprietary static and dynamic malware analysis systems, including Mandiant's MalwareGuard machine learning model.
MISP: Dynamic Cloud Hosting (DCH) Provider	The MISP: Dynamic Cloud Hosting (DCH) Provider provides benign verdicts based on multiple MISP lists that define network infrastructure associated with cloud hosting providers. Infrastructure associated with DCH providers can be reused by numerous entities, which makes it less actionable.
MISP: Educational Institution	The MISP: Education Institution category provides benign verdicts based on the MISP list of university domains from around the world. An indicator's presence on this list indicates a legitimate association with a university and suggests the indicator should be considered benign.
MISP: Internet Sinkhole	The MISP: Internet Sinkhole category provides benign verdicts based on the MISP list of known sinkhole infrastructure. Since sinkholes are used to observe and/or contain previously malicious infrastructure, the appearance on known sinkhole lists reduces the indicator score.
MISP: Known VPN Hosting Provider	The MISP: Known VPN Hosting Provider category provides benign verdicts based on multiple MISP lists identifying known VPN infrastructure, including the VPN-IPv4 and VPN-IPv6 lists. VPN infrastructure indicators are assigned a benign verdict due to the large number of users that are associated with these VPN services.
MISP: Other	The MISP: Other category serves as a default category for newly added MISP lists or other one-off lists that do not naturally fit into more specific categories.
MISP: Popular Internet Infrastructure	The MISP: Popular Internet Infrastructure category provides benign verdicts based on MISP lists for popular web services, email services, and Content Delivery Network (CDN) services. The indicators on these lists are associated with common web infrastructure and should be considered benign.
MISP: Popular Website	The MISP: Popular Websites category provides benign verdicts based the popularity of a domain across multiple domain popularity lists, including Majestic 1 Million, Cisco Umbrella, and Tranco. Presence across multiple popularity lists increases the confidence that the domain is benign.
MISP: Trusted Software	The MISP: Trusted software category provides benign verdicts based on MISP lists of file hashes that are known to be legitimate or otherwise cause false positives in threat Intel feeds. Sources include MISP lists like nioc-filehash and common-ioc-false-positives.
Spam Monitoring	Spam Monitoring contains proprietary sources that collect and monitor indicators related to identified spam and phishing activity.
Tor	The Tor source assigns benign verdicts based on multiple sources that identify Tor infrastructure and Tor exit nodes. Tor node indicators are assigned a benign verdict due to the sheer volume of users associated with a Tor node.
URL Analysis	The URL Analysis category contains malicious or benign verdicts from multiple systems that perform analysis of a URL's content and hosted files.