

10 of the Best Open Source Threat Intelligence Feeds

By Walker Banerd

Published: 2019-04-30 · Archived: 2026-04-06 00:44:34 UTC

In our quest to help security operations and incident response teams work more effectively, we've created a list of the top 10 open source threat intelligence feeds.

Each threat feed listed here integrates seamlessly with our [Morpheus AI SOC solution](#), as do dozens of the top enterprise and subscription-based threat intelligence platforms.

1. Department of Homeland Security: [Automated Indicator Sharing](#)

Private companies are able to report cyber threat indicators with the DHS, which are then distributed via the Automated Indicator Sharing website. This database helps reduce the effectiveness of simple attacks by exposing malicious IP addresses, email senders, and more.

2. FBI: [InfraGard Portal](#)

The FBI's InfraGard Portal provides information relevant to 16 sectors of critical infrastructure. Private and public sector organizations can share information and security events, and the FBI also provides information on cyber attacks and threats that they are tracking.

3. [Abuse.ch](#)

Swiss-based abuse.ch, a Bern University project, collaborates with Spamhaus, serving IT experts and law enforcement. It tracks botnets, operates MalwareBazaar, URLhaus, and YARAify, focusing on malware like Emotet, Dridex, and malicious SSL certificates, sharing indicators of compromise.

4. SANS: [Internet Storm Center](#)

The Internet Storm Center, formerly known as the Consensus Incidents Database, came to prominence in 2001, when it was responsible for the detection of the "Lion" worm. It uses a distributed sensor network that takes in over 20 million intrusion detection log entries per day to generate alerts regarding security threats. The site also provides analysis, tools, and forums for security professionals.

5. VirusTotal: [VirusTotal](#)

VirusTotal uses dozens of antivirus scanners, blacklisting services, and other tools to analyze and extract data from files and URLs submitted by users. The service can be used to quickly check incidents like suspected phishing emails, and every submission is retained in its database to build a global picture of cyber threats.

6. Cisco: [Talos Intelligence](#)

The Talos threat intelligence team protects Cisco customers, but there is a free version of their service available. Talos' unmatched tools and experience provide information about known threats, new vulnerabilities, and emerging dangers. Talos also provides research and analysis tools.

7. VirusShare: [VirusShare Malware Repository](#)

VirusShare is an online repository of malware created and maintained by J-Michael Roberts, a digital forensics examiner. The site gives researchers, incident responders, and forensic investigators access millions of malware samples.

8. Google: [Safe Browsing](#)

The Safe Browsing service identifies dangerous websites and shares the information to raise awareness of security risks. Safe Browsing finds thousands of unsafe sites every day, many of which are legitimate sites that have been compromised by hackers.

9. National Council of ISACs: [Member ISACs](#)

While some ISAC feeds are quite expensive, others are free. The National Council of ISACs provides a comprehensive list.

10. The Spamhaus Project: [Spamhaus](#)

Spamhaus is a European non-profit that tracks cyber threats and provides real-time threat intelligence. Spamhaus has developed comprehensive block-lists for known spammers and malware distributors, which they provide to ISPs, email service providers, and individual organizations.

[Morpheus AI](#), D3's [autonomous SOC](#) solution integrates with hundreds of [leading SOC tools](#), including [threat intelligence platforms](#) to automatically enrich alerts and incidents with contextual data. [Schedule a demo today](#) to learn from one of our SOC automation experts how D3 can seamlessly bring threat intelligence into your security operations workflows.

Source: <https://d3security.com/blog/10-of-the-best-open-source-threat-intelligence-feeds/>