10 OSINT TOOLS FOR CTI

To help **optimize cyber threat research**, these tools enable you to capture open-source information relevant to specific data points in your investigation.

In some cases, APIs are also available, so you can integrate the capabilities into your CTI environment.

Exploitalert

Exploitalert is a site where you can search for exploits and find available patches, mitigation measures, etc., to monitor exploits in real time.
The **exploitalert API** can be integrated into your CTI or security software.

AUTHENTIC8

GreyNoise

GreyNoise Intelligence helps you identify and triage potential cyberthreats, and eliminate false positives. The tool captures data on IP addresses behind scan and attack traffic to help classify IP intent. You can integrate the GreyNoise API with common security products to quickly sift through alerts, and see a visualization of the full context behind scanner IPs under investigation.

Censys

Censys helps you identify exposures that attackers are likely to exploit. On a daily basis, the platform analyzes all devices connected to the internet, adding new IPs and removing old ones. Using the Censys web interface or API, you can query hosts and certificates to monitor your organization's exposure to threats.

ThreatMiner

This threat intelligence portal enables you to research indicators of compromise (IOCs) to have a better understanding of attack origins. Beyond just data points, **ThreatMiner** provides valuable context about IOCs to help you discern potential value of information as intelligence.

AttackerKB

AttackerKB is a web portal that crowdsources critical assessments on cyberthreats to help you triage security efforts. Insights from this forum can give you better understanding on which vulnerabilities are relevant to your business, and the level of urgency and impact.

VirusTotal

VirusTotal aggregates data from over 70 antivirus scanners and URL/domain blacklisting services to raise global awareness about potentially harmful content. You can use VirusTotal reports for your CTI research, and also upload files to their platform to share helpful information on known cyber threats.

Microsoft Defender TI

Microsoft Defender TI streamlines CTI workflows to detect, understand, prioritize and respond to cyberthreats more rapidly. The platform aggregates critical data sources and analysis on IOCs to give organizations greater ability to proactively defend vulnerabilities and prevent exploits.

AUTHENTIC8

DomainTools

DomainTools provides a “Whois Lookup” database to obtain details about domains going back to 1995. Searching on domain name or IP address, you can find information about the registrant, IP location, IP history, activity dates and more.

DNSdumpster

DNSdumpster can help you map a cyberattacker's entire threat surface based on DNS records. Based on a domain name, you can identify hosts and all associated subdomains to gain a broader perspective about adversaries.

Shodan

Shodan enables you to assess vulnerabilities from a device perspective. You can monitor which devices on your network are connected to the internet, where they are located and who is using them.

2022 saw a **61%** rise in phishing attacks; a **21%** increase in the number of newly discovered vulnerabilities; and an average of **277** days for security teams to identify and contain a breach (source).

Increasing the efficiency and effectiveness of CTI research is more critical than ever, and these OSINT tools can help.