SOC Tools

Analysis Tools For Detecting and Responding to Threats

OSINT
OSINT framework focused on gathering information from free tools or resources.

https://osintframework.com/

VirusTotal
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.

https://www.virustotal.com/

OTX (AlienVault)
Open Threat Exchange (OTX) is among our most useful threat intelligence tools.

https://otx.alienvault.com/

HYBRID ANALYSIS
This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.

https://hybrid-analysis.com/

RISKIQ
RiskIQ Community brings petabytes of internet intelligence directly to your fingertips. Investigate threats by pivoting through attacker infrastructure data.

https://community.riskiq.com/

ANY.RUN
ANY.RUN is an interactive online malware analysis service created for dynamic as well as static research of multiple types of cyber threats.

https://any.run/

MX TOOLBOX
All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool. Input a domain name or IP Address or Host Name.

https://mxtoolbox.com/

Internet Storm Center
It uses a distributed sensor network that takes in over 20 million intrusion detection log entries per day to generate alerts regarding security threats.

https://isc.sans.edu/

DOMAINTOOLS
Find information on any domain name or website. Large database of whois information, DNS, domain names, name servers, IPs, and tools for searching.

https://whois.domaintools.com/

SHODAN
Shodan is a search engine that lets the user find specific types of computers (webcams, routers, servers, etc.) connected to the internet using a variety of filters.

https://www.shodan.io/

AbuseIPDB
AbuseIPDB is a project dedicated to helping combat the spread of hackers, spammers, and abusive activity on the internet. AbuseIPDB provides a central blacklist to report and find IP addresses that have been associated with malicious activity online.

https://www.abuseipdb.com/

DigitalSide Threat-Intel
This site contains a set of Open Source Cyber Threat Intellegence information, monstly based on malware analysis and compromised URLs, IPs and domains.

https://osint.digitalside.it/

Nothink!
SNMP, SSH, Telnet Blacklisted IPs from Matteo Cantoni's Honeypots.

http://www.nothink.org/

ThreatTracker
A Python script designed to monitor and generate alerts on given sets of IOCs indexed by a set of Google Custom Search Engines.

https://github.com/michael-yip/ThreatTracker

DNSdumpster
DNSdumpster is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.

https://dnsdumpster.com/

IBM X-Force Exchange
IBM X-Force Exchange is a threat intelligence sharing platform enabling research on security threats, aggregation of intelligence, and collaboration with peers.

https://exchange.xforce.ibmcloud.com/

Omar Al-Harbi