SOCRadar®
Your Eyes Beyond

50 Free Online Tools for SOC Analysts

This guidebook provides SOC analysts with a list of 50 free online tools for cybersecurity tasks, covering categories like internet scanning engines, vulnerability databases, threat intelligence sharing platforms, phishing detection, sandboxes, and more. These tools can enhance threat detection, analysis, and response, offering accessible resources essential for securing digital assets and improving SOC efficiency.

50 Free Online Tools for SOC Analysts

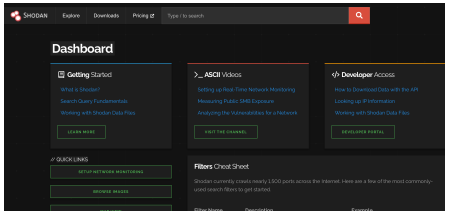
SOCRadar® Your Eyes Beyond

Internet Scanning Search Engines

Internet Scanning Search Engines are specialized tools that can scan and index devices, services, and systems connected to the internet. These services can provide valuable insights into the exposure of assets, and help SOC analysts discover unprotected devices and monitor the attack surface.

Shodan

Shodan enables the searching and analyzing of internet-connected devices, providing critical data for attack surface assessments.

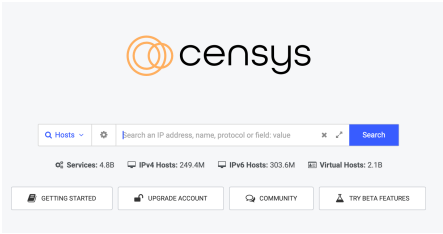


ZoomEye

ZoomEye acts as a cyberspace search engine, helping discover and monitor internet-exposed devices and activities for potential threats.

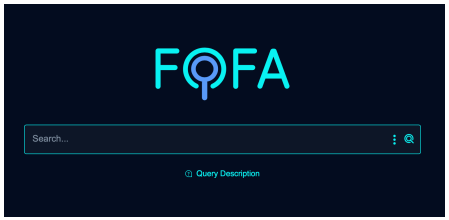
Censys

Censys conducts internet-wide scanning and data collection, offering comprehensive insights for security and compliance purposes.



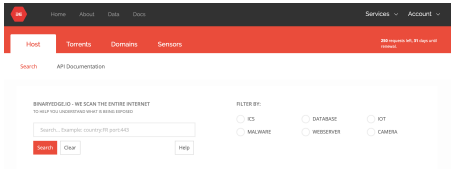
FOFA

FOFA is an advanced search engine for internet-connected devices, delivering valuable threat intelligence for enhanced cybersecurity.



BinaryEdge

BinaryEdge collects real-time data on open ports, services, and vulnerabilities, assisting in proactive threat detection and mitigation.



50 Free Online Tools for SOC Analysts

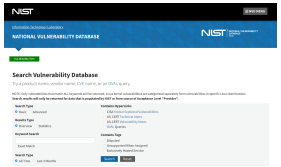
SOCRadar® Your Eyes Beyond

Vulnerability Databases

Vulnerability Databases are critical resources for cybersecurity professionals, providing centralized repositories of information on known security vulnerabilities.

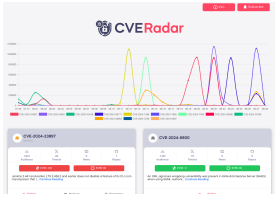
National Vulnerability Database (NVD)

A comprehensive and widely-used database maintained by NIST (National Institute of Standards and Technology), NVD provides detailed information on security vulnerabilities.



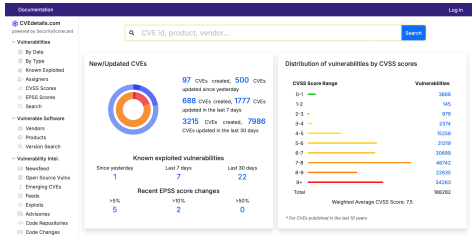
SOCRadar CVE Radar

CVE Radar, a free service on SOCRadar LABS, offers insights into trending cybersecurity vulnerabilities, helping organizations quickly identify and respond to the most pressing threats.



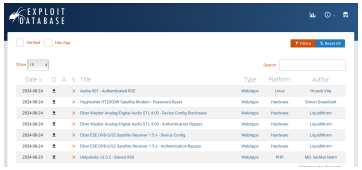
CVE Details

This platform aggregates CVE data and presents it in a user-friendly format, enabling users to analyze trends.



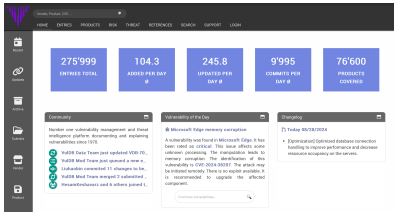
Exploit-DB

A public database that focuses on providing detailed information on security vulnerabilities along with proof-of-concept exploits. It's a valuable resource for both defensive and offensive security professionals.



Vulndb

A searchable database of security vulnerabilities that includes detailed reports and links to various sources, providing a comprehensive view of the vulnerability landscape.



50 Free Online Tools for SOC Analysts

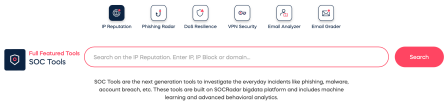
SOCRadar® Your Eyes Beyond

Threat Intelligence

Threat intelligence sharing platforms are essential tools for cybersecurity professionals, enabling them to collaborate, share, and analyze information on emerging threats. These platforms aggregate data from various sources, providing real-time insights.

SOCRadar LABS' SOC Tools

A suite of free tools developed by SOCRadar to assist SOC teams in investigating various cybersecurity incidents, including phishing, malware, and account breaches.



MISP (Malware Information Sharing Platform)

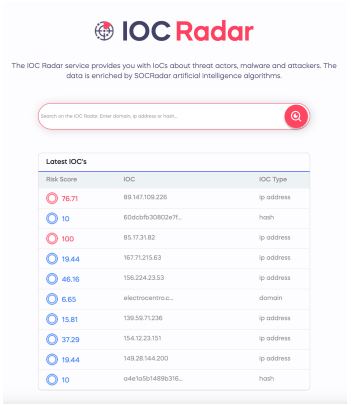
An open-source threat intelligence platform that facilitates the sharing, storing, and analyzing of threat indicators, helping organizations respond to threats more effectively.

SOCRadar Free CTI4SOC

is designed to assist SOC analysts in threat detection and analysis. It provides tools for effective threat hunting and analysis, enabling users to identify and respond to cyber threats more efficiently.

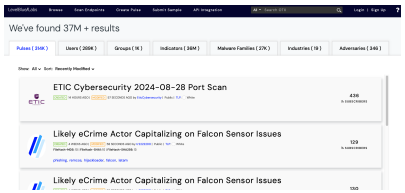
SOCRadar LABS' IOC

Radar provides IoCs about threat actors, malware and attackers, yielding results enriched by SOCRadar artificial intelligence algorithms.



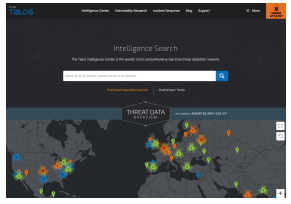
AlienVault Open Threat Exchange (OTX)

A community-powered platform where security professionals share and receive actionable threat intelligence to better understand emerging cyber threats.



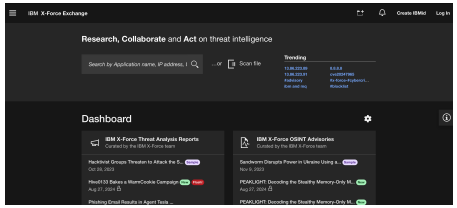
The Talos Intelligence Center

Cisco's Talos Intelligence Center offers a real-time threat detection network, where you can search by IP, URL, domain, network owner, or file SHA256.



IBM X-Force Exchange

A collaborative platform designed for the sharing, researching, and analyzing of threat intelligence, supporting organizations in identifying and mitigating risks.



50 Free Online Tools for SOC Analysts

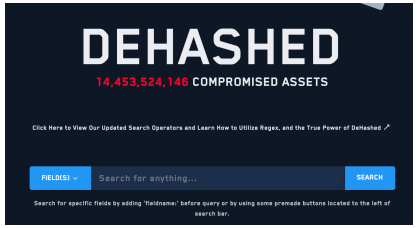
SOCRadar® Your Eyes Beyond

Credentials Search

Credential search services enable identifying if information such as usernames, passwords, or email addresses have been exposed in data breaches. SOC analysts use credential search services to monitor and detect compromised credentials, and prevent unauthorized access.

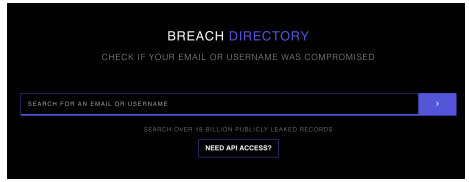
Dehashed

Search engine for finding leaked databases and exposed personal information. It allows tracking down compromised credentials and personal data across the web.



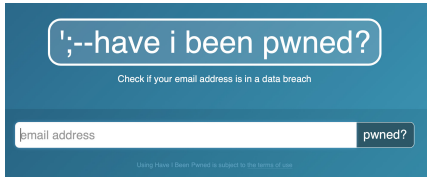
BreachDirectory

Searchable database of data breaches and leaked credentials, helping users identify if their accounts have been compromised in known security incidents.



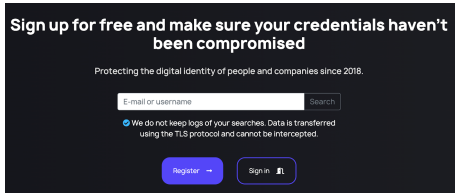
Have I Been Pwned (HIBP)

HIBP allows checking if email addresses have appeared in data breaches, providing a simple way to discover whether personal information has been exposed.



Leakcheck.io

Allows searching by email or username to check for compromised credentials, displaying sources, compromise dates, and whether key data fields like name, city, and password are included.



SOCRadar LABS Dark Web Report

A searchable database of security vulnerabilities that includes detailed reports and links to various sources, providing a comprehensive view of the vulnerability landscape.

50 Free Online Tools for SOC Analysts

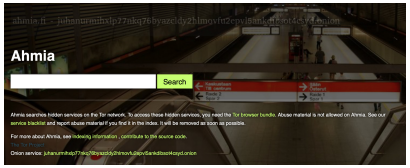
SOCRadar® Your Eyes Beyond

Dark Web

Dark Web search tools provide users with the ability to explore and navigate the hidden and anonymous sections of the internet, typically accessed through networks like Tor. SOC analysts utilize Dark Web search engines to monitor and investigate threats emerging from the dark web.

Ahmia

A search engine specifically designed for the Tor network, indexing hidden service websites to make them more accessible for users navigating the dark web. Ahmia is also available on the clearnet.

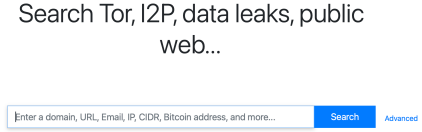


Torch

One of the oldest and largest search engines on the dark web, providing extensive indexing of hidden services for thorough exploration.

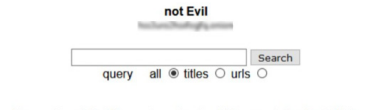
IntelX.io

A cybersecurity search engine and data archive offering access to a variety of datasets, including those from the dark web and domain registrants, making it a versatile tool for digital investigations.



Not Evil

A dark web search engine that focuses on indexing hidden service websites, providing an interface for searching the dark web. It's a popular service, but it has been mostly down recently.



Candle

An open-source search engine designed to search across the darknet, offering capabilities for users to find hidden services and content in the dark web ecosystem.

50 Free Online Tools for SOC Analysts

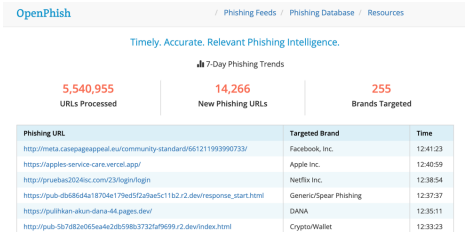
SOCRadar® Your Eyes Beyond

Phishing Detection and Analysis

Phishing detection and analysis tools aid the discovery of potential phishing attempts. SOC analysts use these tools to detect, analyze, and prevent phishing attacks, helping protect their organizations from cyber threats.

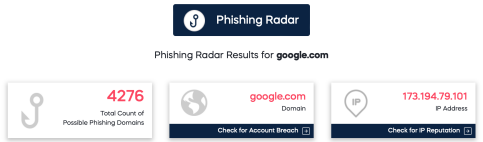
OpenPhish

OpenPhish provides an automated phishing detection system that delivers actionable intelligence to protect against phishing threats.



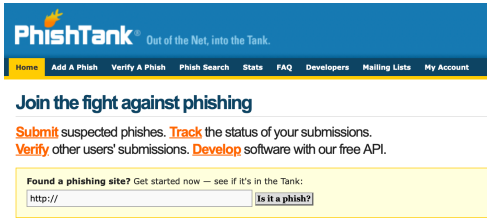
SOCRadar LABS Phishing Radar

SOCRadar LABS Phishing Radar enables users to search domain names, effectively detecting domain spoofing and phishing activities.



PhishTank

PhishTank is a community-driven platform where users can submit, verify, and share phishing data to enhance collective security.



URLScan.io

URLScan.io analyzes websites for phishing and malware, helping SOC analysts assess potential threats.

dnstwist

dnstwist is an online tool designed to identify domains that could be used in phishing attacks, safeguarding against domain spoofing.

50 Free Online Tools for SOC Analysts

SOCRadar® Your Eyes Beyond

Code Search

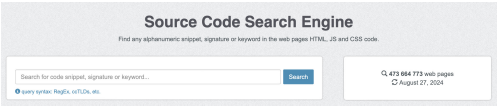
These tools enable SOC analysts to quickly locate and analyze code snippets across various repositories, aiding in threat detection and response.

Sourcegraph

Sourcegraph is a code search and navigation tool for both self-hosted and cloud code repositories, streamlining code exploration.

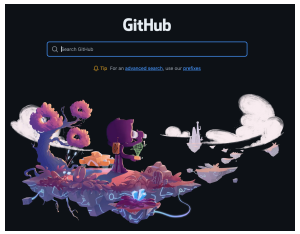
PublicWWW

PublicWWW offers code search across billions of files from thousands of code repositories, facilitating the discovery of code content.



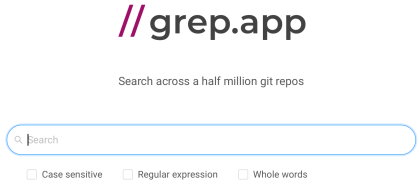
GitHub Code Search

GitHub Code Search allows users to search for code across public GitHub repositories, making it easier to find relevant code snippets.



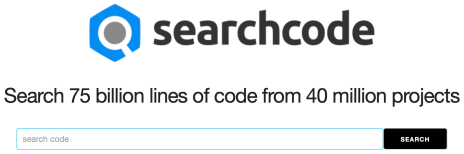
Grep.app

Grep.app is a code search engine that supports exact matches, regular expressions, and more, helping analysts locate specific code patterns.



SearchCode

SearchCode searches source code across hundreds of thousands of projects, providing a vast resource for code analysis and investigation.



50 Free Online Tools for SOC Analysts

SOCRadar® Your Eyes Beyond

Cloud Bucket Search

These tools assist SOC analysts in identifying, securing, and managing cloud storage buckets to prevent unauthorized access and data leaks.

AWSBucketDump

AWSBucketDump quickly enumerates AWS S3 buckets, allowing for efficient discovery and analysis of stored files.

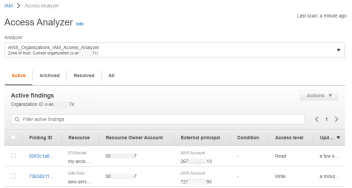
jordanpotti/
AWSBucketDump

Security Tool to Look For Interesting Files in S3 Buckets

10 Contributors · 3 Issues · 1k Stars · 239 Forks

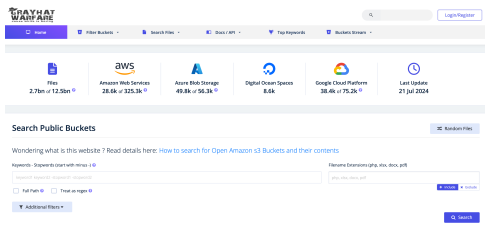
Amazon IAM Access Analyzer

Amazon IAM Access Analyzer enhances security by identifying and analyzing resource policies, helping detect unintended AWS resource access.



GrayHatWarfare

GrayHatWarfare provides an index of publicly accessible Amazon S3 buckets, offering a valuable resource for security analysis.

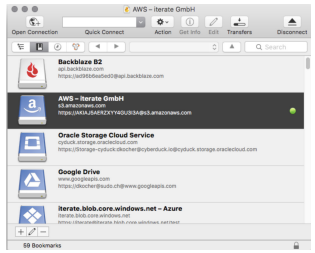


OpenBuckets

OpenBuckets is a tool designed to find and secure exposed cloud storage buckets across various services, ensuring data protection.

Cyberduck

Cyberduck is a versatile cloud storage browser that lets you connect to and manage files on services like Amazon S3, Google Drive, and Dropbox.



50 Free Online Tools for SOC Analysts

SOCRadar® Your Eyes Beyond

Custom GPT Agents

These custom GPT agents can assist SOC analysts by automating critical tasks, offering insights, and keeping them informed about cybersecurity developments.

NVD - CVE Research Assistant

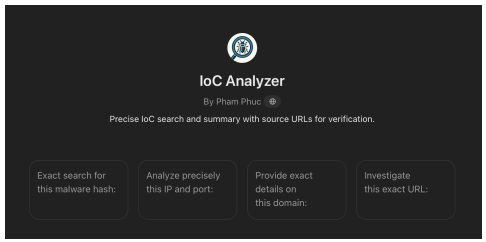
Offers expert information on CVEs and cybersecurity vulnerabilities from the National Vulnerability Database.

CyberNewsGPT

Provides the latest security news about cyber threats, hackings, breaches, vulnerabilities, and more, keeping SOC analysts informed of current events.

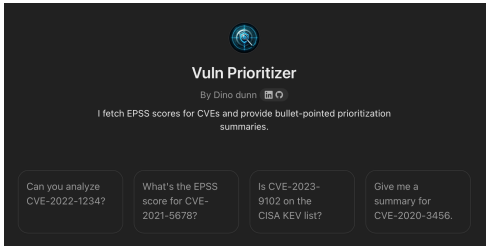
IOC Analyzer

Provides precise IoC search and summary with source URLs for verification, which is crucial for SOC analysts investigating incidents.



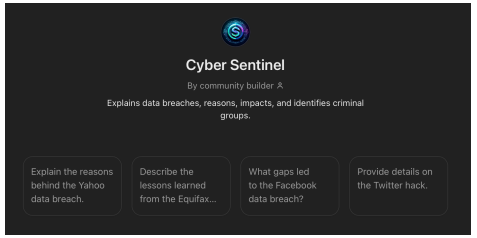
Vuln Prioritizer

Fetches EPSS scores for CVEs and provides prioritization summaries, helping SOC teams focus on the most critical vulnerabilities.



Cyber Sentinel

Explains data breaches, reasons, impacts, and lessons learned, providing valuable context for SOC analysts.



50 Free Online Tools for SOC Analysts

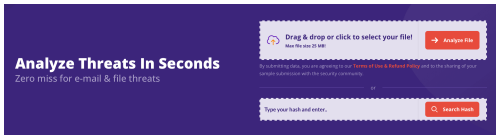
SOCRadar® Your Eyes Beyond

Sandboxes

SOC analysts utilize sandbox environments to safely analyze and monitor the behavior of suspicious files, URLs, as well as malware like ransomware, gaining critical information.

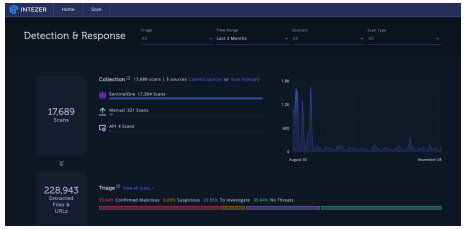
DocGuard

DocGuard is a cloud-based malware analysis service that can analyze files, URLs, and hashes, providing comprehensive threat assessments.



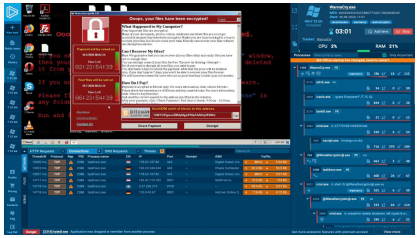
Intezer Analyze

Intezer Analyze is a cloud-based malware analysis platform that uses code genome mapping to detect and respond to threats, ensuring precise identification.



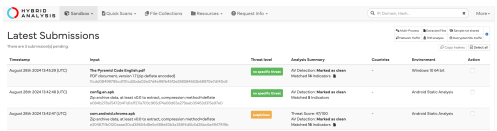
Any.run

Any.run is a malware analysis sandbox that enables users to execute and closely monitor suspicious files in a controlled environment.



Hybrid Analysis

Hybrid Analysis provides a malware analysis service that runs suspicious files in a sandbox, offering detailed insights into their behavior.



VirusTotal

VirusTotal analyzes suspicious files and URLs using multiple antivirus engines, helping SOC analysts detect and respond to threats.

50 Free Online Tools for SOC Analysts

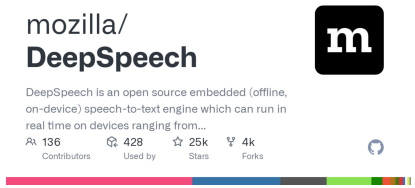
SOCRadar® Your Eyes Beyond

Bonus Category: AI Tools

These AI tools can assist SOC analysts in automating tasks, enhancing productivity, and enabling advanced analysis through machine learning and natural language processing.

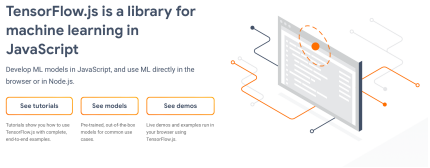
DeepSpeech

Open-source speech-to-text engine by Mozilla. It is a model trained by machine learning techniques; it also uses Google's TensorFlow for easier implementation.



TensorFlow

Open-source machine learning framework for building and deploying AI models. Users can develop ML models in JavaScript, and use it directly in the browser or in Node.js with its TensorFlow.js library.

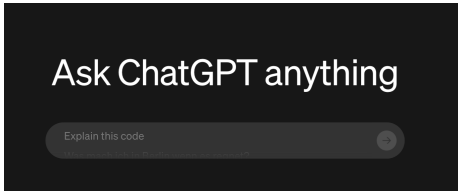


Anthropic's Claude

Highly capable AI assistant that can help with a wide range of tasks. It is highly efficient and is adept at complex tasks such as math and coding; it can also be used in business settings.

OpenAI's GPT-3, GPT-4 Models

OpenAI's GPT-3 and GPT-4 series, and the latest GPT-4o offer powerful language models with a wide range of applications.



Google's LaMDA

Google's LaMDA (Language Model for Dialogue Applications) is a conversational AI system that can engage in open-ended dialogue. It enables machines to have 'natural' conversations with humans.