FORENOVA

MAI
DET
&
RES

TEC

RES

CON

PAR

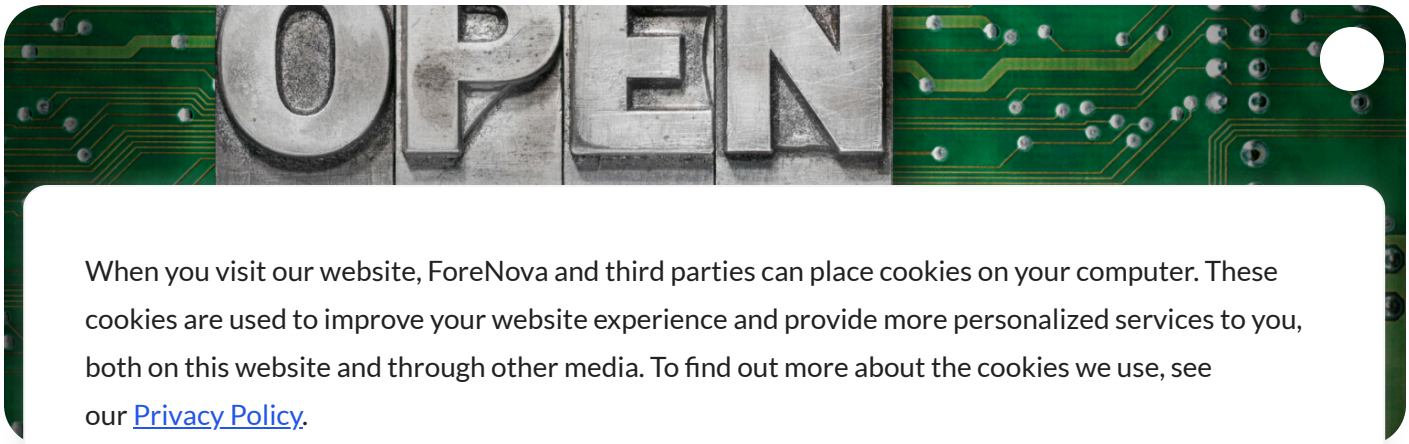

Table of Contents

April 29, 2024 | ForeNova

Top 10 Open-Source Intelligence Tools (OSINT)

Open-source intelligence (OSINT) involves gathering information from public sources to achieve various objectives, whether for IT security, detecting malicious activities, or collecting information for intelligence operations. Advanced techniques for OSINT help analysts sift through abundant data to find specific information.

Forenova Security, a global managed services provider, understands the importance of OSINT. Clients wanting to harness the power of open-source data leverage Forenova's services to help establish this critical business workflow.

What is Open-Source Intelligence (OSINT)?

OSINT tools help access, collate, and organize relevant data based on queries within the various tools. Organizations wanting to develop an OSINT practice should consider what approach they should take when leveraging these tools.

Th
th
C
h
fo
fi
c
w
d
a

A
fi

- Approximately 77 million terabytes of data are created each day.
- A total of 181 zettabytes of data will be generated in 2025.
- Videos account for over half of internet data traffic.

Much open-source data is bound to news, media, social media profiles, company websites, learning institutions, blogs, Wiki posts, and online publications.

Public information regarding previous cybersecurity threats, including data breaches, insider threats, and other criminal activities, is a standard search content piece for OSINT. Organizations can learn a great deal by studying previous attacks against other organizations.

How Vital are OSINT Tools for Cybersecurity, Journalism, and Law Enforcement Industries?

Many industries search, process, and rationalize open-source data. The modern-day news cycle requires journalists to be first with the big story. Often, a big tale starts with scattered information across several unconnected resources.

OSINT is ideal for journalists to use to capture story fragments and create a narrative based on the open-source information captured. Ultimately, this narrative becomes the lead news clip or the foundation for the blog.

Like journalism, cybersecurity benefits from accessing source-gathering tools using advanced search techniques. Gathering threats from previous cyberattacks, messages embedded within social media sites forecasting upcoming attacks are valuable snippets.

With nearly 20,000 security vendors globally, OSINT tools will help set a priority flag as part of their workflow.

Law enforcement also captures similar cybersecurity alerts as part of their investigations. Many law enforcement agencies capture open-source content through various online investigation tools, either specific to a criminal they are investigating or an organization under suspicion. News articles, publications, and podcasts are excellent sources of content law enforcement can add as artifacts to their cases. Leveraging OSINT tools helps expedite the data-capturing process more than just using a browser search page.

How are Open-Source Tools Regulated in Germany and the EU?

> Germany now has a federal open-source policy focusing on digital sovereignty. The Centre for Digital Sovereignty of Public Administration (ZenDiS) was created in 2022 to support this initiative.

- The German government is leading a digital transformation to increase its sovereignty with initiatives like OpenCoDE.de and a cloud strategy. This shift inspires public administrations and civil society to embrace open-source solutions.

- “Germany’s public sector has a robust open-source ecosystem, with many actors and vendors providing secure digital solutions.”

The coordination of open-source initiatives between state and federal levels is still evolving. German cities are expressing interest in utilizing open source despite potential challenges in co
p

- OSINT is frequently used with internal-only sources such as private telemetry data, dark web communities, and external intelligence-sharing services. Analysts have access to various tools

to assist with filtering and verifying this intelligence.
- OSINT techniques are legal and focus on gathering publicly available data. Malicious hackers use these tools for illegal attacks and by government agencies to improve cybersecurity defenses.

Discovery

Discovery tools analyze and uncover extensive information. Google, often seen as a standard search engine, can provide valuable insights in the hands of an OSINT expert and cybersecurity analyst.

Scrapping Tools

Scraping tools help gather and filter data from websites efficiently and securely. They ensure the removal of specific data while minimizing detection and eliminating unnecessary data interference.

Aggregation

Aggregation tools simplify data processing, securely analyze information, and provide actionable insights by connecting data fragments and presenting them in an easy-to-understand format.

What Are The Top Ten OSINTs in 2024?

Many tools are available for gathering OSINT data, including the OSINT Framework. The OSINT F
to

"Maltego offers a free version with limited features, known as Maltego CE. The desktop version, Maltego XL, costs $1,999 per instance. Server installations for large-scale commercial use start at $40,000 and include a complete training program."

Mitaka (Cybersecurity Tool)

Mitaka is a versatile tool that can function as a Chrome extension or Firefox add-on. It allows users to search multiple search engines for online indicators like IP addresses, domains, URLs, and hashes.

This tool helps identify malware, sketchy sites, and shady emails to increase awareness and security.

SpiderFoot (Online Investigation and Cybersecurity Tool)

SpiderFoot is a free tool for gathering and analyzing information from various sources. This tool gathers data on IP addresses, domains, and emails. The tool is available on GitHub, with a command-line interface and a web-based GUI.

Spyse (Cybersecurity Tool)

Spyse provides complete DAAS solutions for Internet security professionals, corporate administrators, SSL/TLS certificate providers, data centers, and business analysts.

"A
c

I

"I
p

Ir
fi
F
political analysts, news reporters, and security researchers.

Darksearch.Ai (Online Investigation Tool)

“For those new to the dark web, DarkSearch.ai is a helpful research platform. It is free to use and has a free API for automated searches. You can access DarkSearch.Ai from a web browser; Tor is unnecessary.”

Shodan (Digital Forensics Tool)

Shodan is a search engine designed to find information on devices that are not easily searchable, including those within the Internet of Things (IoT). Other OSINT tools like the Harvester use Shodan as a data source.

“A Freelancer license allows anyone to scan up to 5,120 IP addresses monthly on Shodan for $59. A Corporate license provides unlimited results and scanning of up to 300,000 IPs monthly for serious users for $899. The Corporate version also includes a vulnerability search filter and premium support.”

Babel Street X (Public Data Analysis)

Babel X is a search tool for the public internet that can search blogs, social media, message boards, news sites, and even the dark web, including Onion sites and some deep web content. It can geo-locate sources and perform text analysis to provide relevant results. Babel X can search in over 200 languages.

M
n s
o
b

M
T
c
O

M .doc, .ppt, .xls, and more. It can investigate various types of documents accessible through public

channels.

theHarvester (Public Data and Data Gathering Tool)

theHarvester is a tool for gathering public information outside of a network, making it useful for reconnaissance before penetration testing.

"This tool uses various search engines, including Bing, Google, dogpile, DNSdumpster, Exalead, Netcraft Data Mining, and AlienVault Open Threat Exchange. It can also access the Shodan search engine to find open ports on hosts. The tool collects emails, names, subdomains, IPs, and URLs."

theHarvester is available on GitHub for anyone to download. When cloning the tool, it is advisable to set up a separate Python environment in a virtual environment.

Searchcode (Data Gathering Tool)

Search code is a specialized search engine that delves deep into source code to gather intelligence for OSINT purposes. The engine, developed by a single individual, offers powerful search capabilities.

What is DarkGPT?

Developed with common attributes like ChatGPT, DarkGPT simply became a jailbroken version of

DarkGPT empowered the user to access several open-source data and private content embedded

within the public domain. DarkGPT can now query content restricted to ChatGPT, including dark art and dark aspects of human existence, and ask pointed questions about the dark side of a writer, director, or politician.

What is the Risk in OSINT Tools?

Attackers often use OSINT to execute a social engineering attack on employees from social media platforms or using email spear-phishing attacks. LinkedIn and other social networking sites are valuable sources of information for attackers, as they reveal personal details that can be used for phishing and password guessing.

Content shared on social media and professional networks may seem harmless at first. However, cyber attackers can exploit this information alongside existing vulnerabilities to launch cyber attacks.

Using cloud resources, attackers can scan for vulnerable assets, open ports, and misconfigured data stores. They can also find credentials and other information on GitHub, where developers sometimes unknowingly share sensitive data in their code.

Is Open-Source always better?

proactive security measures. By leveraging NovaMDR's expertise, SMEs can effectively navigate the complexities of open-source intelligence tools and enhance their cybersecurity posture with

confidence.

In essence, while open-source tools serve as powerful resources, the expertise and guidance provided by NovaMDR ensure that organizations can effectively harness the potential of these tools to bolster their security defenses and make informed decisions based on reliable intelligence.

Tags:

Cybersecurity

Share This Article

ForeNova

Related Posts

Cybersecurity

2024 Cybersecurity Recap

Cybersecurity in 2024 will see unprecedented breakthroughs and challenges. Massive ransomware attacks have already occurred, and Google's influence on ad...

READ MORE

ForeNova

19 Dec, 2024

Cybersecurity

Recap of the Largest Ransomware Attacks in 2024

Hackers focused their efforts on ransomware in 2024, leading to a surge in ransom demands. "With nearly 439 million dollars...

READ MORE

ForeNova

Cybersecurity

What is Computer Network Defense (CND)?

Cybersecurity is included among the top ten global issues both now and ahead in the World Economic Forum's (WEF) 2023...

READ MORE

ForeNova

ForeNova's security platform is designed to detect more cyber threats and attacks than ever before – even the previously unknown and undetected – across the entire IT landscape.

SERVICES

Nova MDR

COMPANY

Company Info

Contact Us

Impressum DE

Legal

RESOURCES

Blog

Terms of Use Privacy Policy Cookies