The Value of Open Source Intelligence (OSINT) for application pen tests

Open source intelligence is actionable intelligence gathered from available data or information, collected, analyzed, and distributed in a timely manner to a wide range of audiences to address a specific information requirement.

Intelligence sources may be categorized as “overt” (publicly available) or “covert” (not publicly available). Open source intelligence deals only with public data sources that are widely available and legal to access.

These include the World Wide Web, Facebook, Twitter, Instagram, LinkedIn, etc., traditional media sources outlets like newspapers, magazines, television, and radio, public government data, academic and online tools, professional publications, commercial data, and technical literature. Threat actors also have access to the same open source feeds and other public sources.

The Open Source Intelligence Cycle

The development of intelligence from public data sources follows the open source intelligence cycle, which may be summarized:

- Planning and Direction–Establishing intelligence collection requirements.
- Data Collection–Collecting data and information from publicly available sources.
- Data Processing–Validating data to confirm usefulness.
- Data Analysis and Production–Transforming the data as accurate, complete, and relevant intelligence that addresses the identified intelligence requirements.
- Intelligence Distribution–Distributing the intelligence to the right audience at the right time to support strategic decision-making.
- Evaluation and Feedback–Collecting feedback on the effectiveness and impact of the OSINT cycle to facilitate continuous improvement.

Intelligence must have a goal or reason. Successful intelligence initiatives begin with a clearly defined goal, purpose, and intended use case that guides the data collection process along with defining a success criteria.

If intelligence is not collected, data becomes irrelevant. The intelligence community operatives collect data, which functions as an input in the open source intelligence cycle. Data validation, correlation, analysis, and production, intelligence operatives transform the raw data into usable intelligence that meets the defined success factors and goals.

Leveraging OSINT in Defining Pen Testing Engagements

Intelligence and security personnel rely on publicly available information sources for timely and accessible cyber threat data. Historical data is available on the web, including in knowledge bases like MITRE ATT&CK. Security teams can also access public threat intelligence feeds that are continuously updated with new reports from the community.

Social Media accounts and the internet are great open source intelligence sources. Millions of people use them daily. Their updates are constant. And they're all public. Search-ability operatives can use software technology and artificial intelligence automation technologies to search and filter for specific types of information on the web and on Social Media Platforms. Automation-Intelligence and Security Operatives can use software and AI automation technologies and machine learning to monitor the web and Social Media Platforms at scale. Intelligence agencies use social engineering to collect unofficial or non-public data information. These data collectors try to gather hand intelligence around currently exposed cyber attacks, phishing attacks, or a new attack surface not seen before in the wild.

Many source intelligence gathering efforts also include public disclosures of lawsuits along with organizations that fail to report a breach in a timely manner.

- The law firm Tycko & Zeilichei LLP has sued both Capital One and GitHub, claiming that both companies failed to protect users' personal information. In addition, the complaint highlights that Paige A. Thompson allegedly stole the data in March and then posted about the theft on GitHub in April. As a result, the stolen data stayed on GitHub.com for nearly 3 months.The law firm also alleged that Capital One should have known that hackers stole personal information when the information was first taken in March.
- The most recent hack was discovered when Uber disclosed it had been breached. Hackers stole information, including names, email addresses, phone numbers, credit card details, and driver's license numbers. The hackers could gain access to an internal GitHub repository used by Uber employees. From there, they accessed other repositories containing sensitive information, such as a code for the company's self-driving cars. This information included source code for the company' autonomous vehicles, along with proprietary information about the company's mapping technology.
- Three out of every 1,000 commits to GitHub leaked a secret, a frequency 50% higher than 2020. More than half of the secrets comprised credentials for accessing data storage services, cloud providers, a private encryption key, or a development tool, while another 10% comprised credentials for messaging systems and version-control platforms.
  Additional OSINT Context Press Releases and Product Release Notes
  Pen testers will analyze several open source intelligence data sources to factor into a client engagement. The tester coordinator during the project collection **phase will** research if the client is currently leveraging as an example; GitHub within AWS.
  If the client is currently using this platform, the pen tester could create a subsection of

the engagement to focus on testing for any known or unknown vulnerabilities similar to the CapitalOne security breach.

Pen testing firms use OSINT to capture current and updated security vulnerabilities happening in near time or a current breach in cyber threat intelligence from hackers on the dark-net. Firms like CYBRI access specialized search engines like Shoban.IO and Censys.IO to collect OSINT data. Patterns of vulnerabilities, leakage vulnerabilities, and social engineering attacks often are well documented on these two search engines.

What Is Open Source Penetration Testing

Open source penetration testing is an engagement that helps you understand how vulnerable your organization's infrastructure is." Open source penetration testing is a method of assessing the security of an information system by simulating targeted attacks."

- This type of testing allows you to find out how vulnerable your network is to cyberattacks.
- The primary goal of such tests is to identify the main weak points, the most effective attack patterns, and the potential impact of the attack.

CYBRI's Expertise

Clients often will engage 3rd party pen testing firms like CYBRI to perform engagements specific to compliance mandates, validating the security integrity of a new application or platform, or re-test a critical element within their infrastructure shortly after a redesign or major code update.

Cloud Penetration Testing

Cyber attacks on cloud infrastructure have grown just as quickly as cloud technology adoption has. Hackers target cloud technologies with the specific goal of stealing sensitive information and disrupting business operations.

CYBRI's Cloud penetration testing services cover all aspects of your Cloud infrastructure, from user roles/IAM, network and infrastructure, business logic, and configuration security. We ensure that each aspect of your cloud infrastructure maintains a strong cybersecurity posture by scheduling your quarterly or annual pen tests with our easy-to-use BlueBox platform.

Network & Infrastructure Penetration Testing

The moment you connect your system to the internet, you are inherently at risk of facing cyber-attacks. You must secure your network infrastructure to ensure you don't fall prey to any malicious attack.

Our pen testers will navigate your network infrastructure as a simulated hacker or attempt to breach your network to assess the strength of your security. We target your firewalls and other network devices to find the weakest point of entry and then move laterally to find all exploits.

What makes CYBRI one of the Premier penetration testing companies?

Our outstanding penetration testing company services have attracted several clients that range from small startups to huge multinational companies. We are dedicated to improving cybersecurity across the board, so our services to your organization continue even after the pen test report has been delivered.

No matter the size of your organization, we will assess all of your cybersecurity needs from scratch to provide security measures tailored to your business needs. Our experts are always available to all of our clients in an advisory capacity should you wish to contact us.

Discuss your project with Us!

Click here to go to our site, fill out the form and the engagement team will contact you shortly!

https://cybri.com/red-team/