Navigating Today's OSINT Ecosystem Effectively

Posted on April 11, 2024

Organizations of all types have long been relying on open-source intelligence (OSINT) for various business purposes, most notably cybersecurity. There's a growing need for it. In fact, experts predict that the worldwide OSINT market revenue will reach US$38.07 billion by 2028 from US$12.2 billion in 2023. And that's not surprising given that 75% of security professionals have seen the volume of cyber attacks rise in the past year alone.

But the OSINT ecosystem is vast, comprising hundreds if not thousands of disparate types, sources, tools, and techniques. Navigating it can be a challenge. Organizations not only need to know what information to gather but also which vendor to tap and how to piece all the details together to come up with concrete cybersecurity measures.

Why the Need for OSINT?

OSINT, defined as data that is available to the general public, is essential to keeping cyber threats and attacks at bay. While many think it is limited to information obtained from web searches or the Surface Web, that is most definitely not the case. In fact, OSINT can come from several sources, including the Dark Web and vulnerability databases. It can also be sourced using various tools that identify the technologies a website uses, a target's domain and DNS infrastructure, and many more.

How Does OSINT Gathering Work?

The OSINT gathering process requires two things—a clear strategy and framework for acquiring

and using the right data, tools, and techniques for collecting and processing the information. It can be a tedious process.

Many cybersecurity professionals consider the OSINT Framework a definitive guide to effective and comprehensive threat intelligence gathering. It is a compilation of the OSINT data points any specialist may wish to gather to beef up any investigation, along with possible sources and tools, for the first two stages of the OSINT cycle.

What Is the OSINT Cycle and How Does It Work?

The OSINT cycle has five steps that cybersecurity professionals should conduct in a continuous loop if they are to thwart today's cyber threats.

Let’s tackle them one by one.

1. Direction: Involves crafting prerequisites and a question outline to get a clear idea on what

information is required, what sources to use, and what the results will accomplish. As mentioned earlier, cybersecurity teams can be guided by the OSINT Framework.

2. Collection: The actual information gathering phase using a security team's preferred methodologies and resources. This phase may include collecting data from using news articles, social networks, and other free tools although they can only go so far. Organizations may need to enrich them with domain, DNS, and threat intelligence given that the ultimate goal is to protect their network, notably from online threats.

3. Processing: Involves refining the information gathered by organizing it into a centralized evidence repository, chronology, or report.

4. Analysis: Includes analyzing the data and creating a final report. This step lets security teams understand and anticipate events using the data gathered. Threat intelligence enrichment can help with this stage in that it gives more actionable insights into a threat (e.g., what domains and IP addresses to block, etc.).

5. Dissemination: Involves distributing the report and guidelines to end users.

Just How Big Is the Current OSINT Ecosystem?

The OSINT ecosystem comprises various intertwined and often distinct players and resources, such as:

- **Search engines:** Google would probably be top of mind for many intel gatherers but they may also consider Bing and DuckDuckGo, along with region-specific engines like Yandex and Baidu.

- **OSINT aggregation tools and platforms:** Platforms like Maltego and OWASP AMASS can aid in obtaining more information about specific web properties like domain names and IP addresses, including ownership data and connections, which are critical to attack surface mapping.

- **Domain, DNS, and threat intelligence:** APIs like the ones WhoisXML API offers that can be readily integrated into existing cybersecurity solutions and already accessible via aggregation tools and platforms (e.g., Maltego and OWASP AMASS) are good sources of timely and relevant information on digital properties under investigation. Those with specific requirements, meanwhile, can consider using web-based tools to obtain the same data.

- **Vulnerability intelligence sources:** The National Vulnerability Database, CVE, and Common Weakness Enumeration (CWE) pages are extensive repositories of vulnerabilities and their corresponding solutions and mitigations. Tools like Sploitus, a specially crafted exploit and hack tool search engine, are also useful for gathering more information on specific exploits threat actors can use in attacks.

- **Other tools and data aggregators:** Other tools also exist to enable metadata search, code search, people and identity investigation, phone number research, email search and verification, social media listening, image analysis, geospatial research and mapping, and wireless network detection and packet analysis, among others.

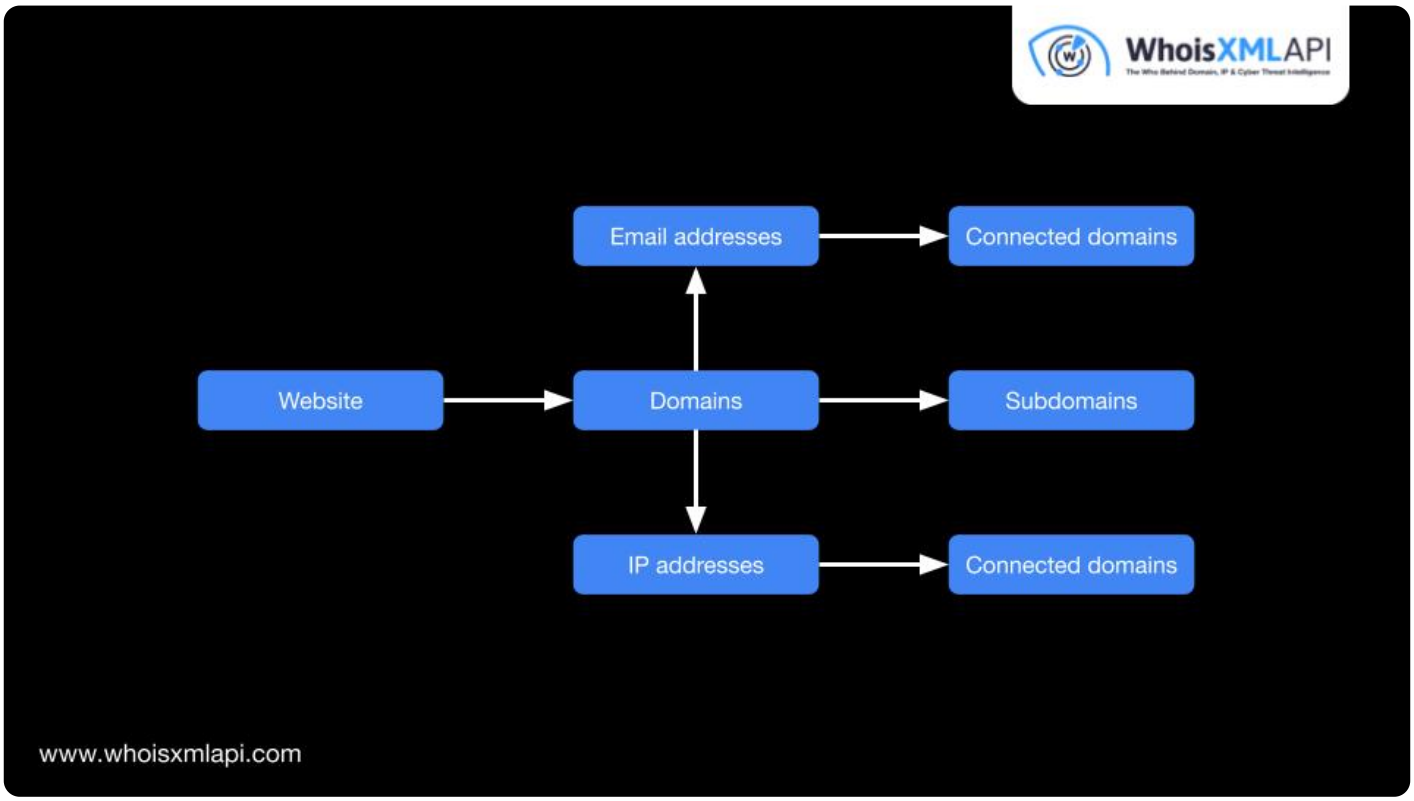
What Cybersecurity Processes Can OSINT Help With?

The entire myriad of OSINT tools, techniques, and sources can help organizations with several cybersecurity tasks. We named at least five here.

Ethical Hacking and Penetration Testing

Security professionals use OSINT to identify potential weaknesses in friendly networks so they can be remediated before threat actors can exploit them. Some of the weaknesses they may find include accidental sensitive data leaks through social media, open ports or unsecured Internet-connected devices, unpatched software, and leaked or exposed assets on pastebins and such.

Pen testers and ethical hackers often start by listing all of an organization's public-facing assets. Apart from looking at potential exposure vectors like too much information on social networks, they can also look at dangling DNS records, system and application vulnerabilities, forgotten subdomains, open ports, and other weaknesses present in their client's web infrastructure.



External Threat Identification

The Internet is an excellent source of insights into the most pressing and emerging threats. It can give security researchers an idea on the vulnerabilities threat actors are actively exploiting or insights into ongoing attacks.

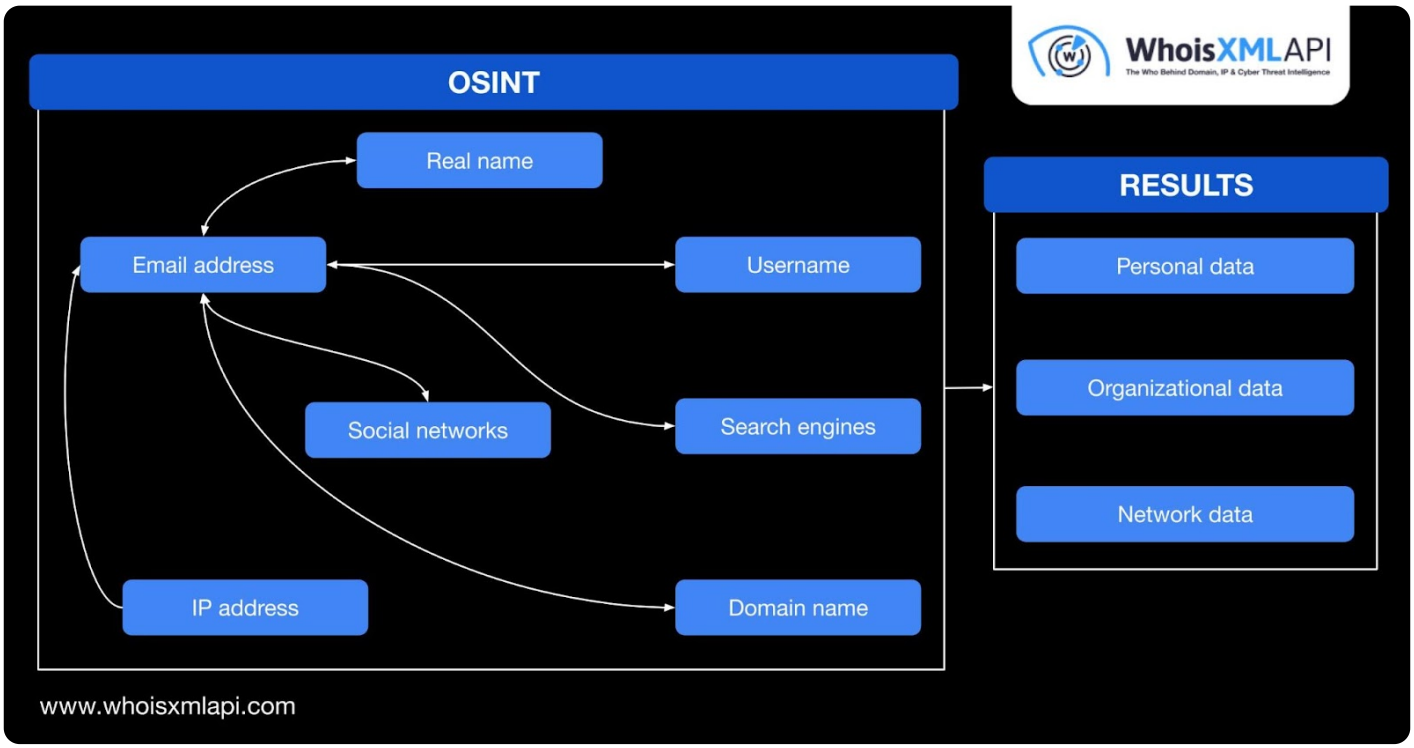
OSINT, such as that obtained from threat intelligence feeds, can help security teams identify which of the digital properties (e.g., domains, IP addresses, etc.) threat actors utilized in attacks are

actually malicious.

Fraud Detection

OSINT is also useful in fraud investigations. Apart from the usual social media analysis, digital footprinting, financial transaction analysis, and Dark Web exploration, APIs accessible via platforms like Maltego can shed more light on how expansive a particular threat's infrastructure is.

Security teams can, for instance, enhance personal (e.g., attacker's name connected to an email address) and organizational (e.g., attacker's company) information research with network data like WHOIS and DNS record details for better security.

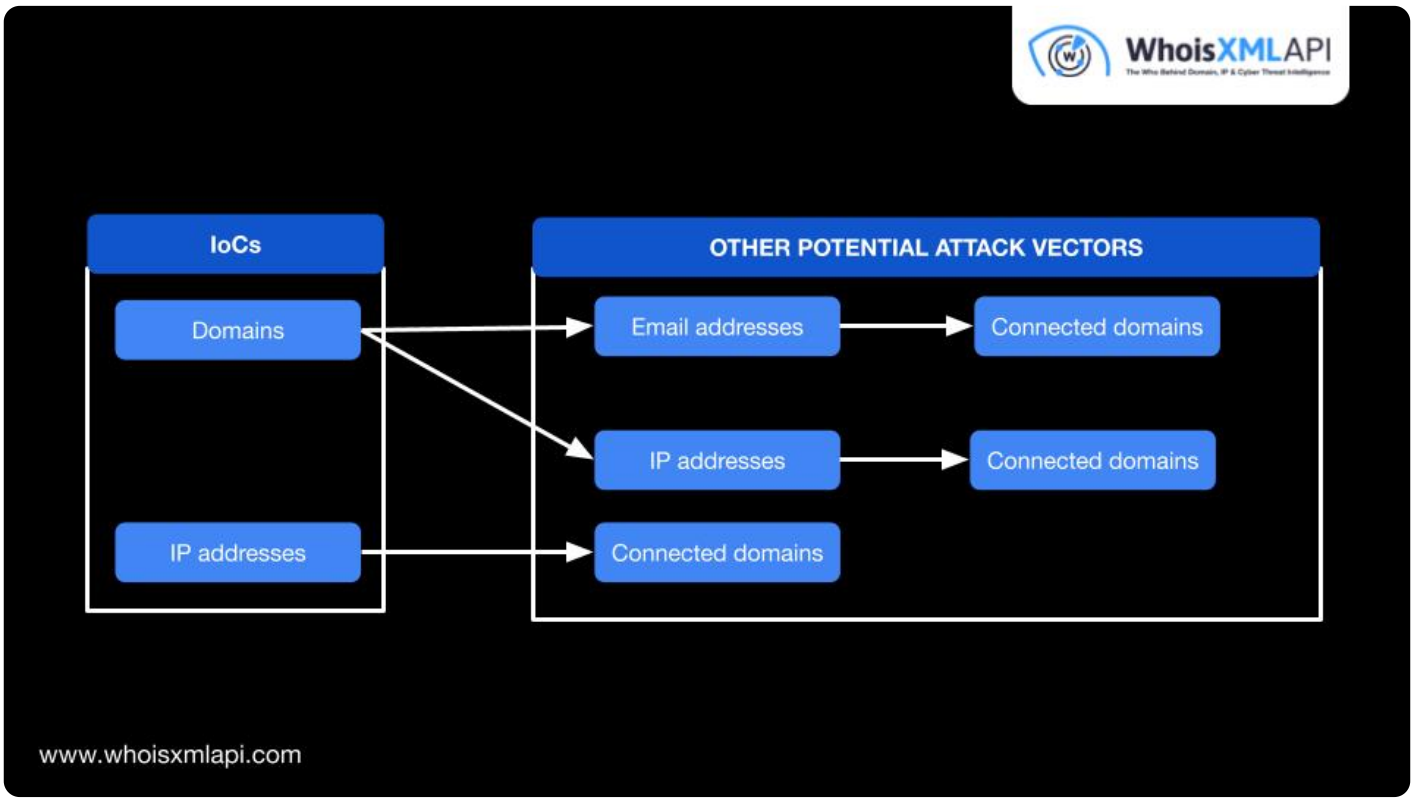


Security Breach Prevention

A single security breach can cost an organization an average of US$4.45 million in 2023. And the

expenses can keep adding up even after remediation and restoration due to fines, investigations, and lawsuits. Security operations center (SOC) and incident response teams armed with operational threat intelligence, including OSINT, can, however, make more timely and informed decisions to prevent such an issue.

SOCs and incident responders can identify other potential attack vectors (e.g., connected domains, subdomains, IP addresses, etc.) not yet published in lists of indicators of compromise (IoCs) that are worth noting and blocking.



Supply Chain Protection

Protecting networks should not stop at what's under an organization's direct control. Security teams also need to oversee who has access to their systems, applications, and data through their entire supply chain. They need to monitor their vendors, partners, consultants, and practically every third party they grant network access to aided by OSINT. They need to keep in mind that in

2023 alone, supply chain attacks and zero-day exploitation led to a 72% increase in the number of compromise incidents.

Knowing all the components that make up connected third-party networks is possible with the help of OSINT tools that use domain and DNS intelligence. Supplementing that information with real-time threat intelligence is even better in that organizations can prioritize severing ties to digital properties that can put their own networks in danger.

Putting All the OSINT Puzzle Pieces Together

OSINT platforms can help security analysts and researchers map and analyze connections between various OSINT data points related to an attack or a threat actor. But the tools may not work as well if they do not integrate domain, DNS, and threat intelligence to tell the complete story so organizations can thwart attacks targeting their networks.

Instead of relying on disparate tools for web, archive, and social network searches and then manually mapping them to email addresses, domains, IP addresses, and other network details, platform integration significantly eases and hastens the process when every OSINT source is already in place. While web searches provide real-world data (e.g., personal and organizational details), built-in domain and DNS APIs can give users insights into their network connections. Together, they can not only identify who may be behind a threat but also what network connections to sever to stop attacks in their tracks.

It's one thing to collect as much personal, organizational, and network information on an attacker. It's another to put all the puzzle pieces together in a way that can provide real-time cybersecurity insights efficiently and rapidly.

Ready to see how WhoisXML API's market-leading cyber intelligence sources can complete the OSINT picture? Contact us now.