Unraveling the World of Security Data Aggregation

Posted on May 13, 2024

More than 30.6 billion records have been exposed in 2024 so far based on 8,839 publicly disclosed incidents. Intensifying cybersecurity efforts has thus become more critical than ever for organizations the world over. But that requires having the whole picture on hand, and that's only possible if users can take a closer look inside and outside their networks.

More often than not, painting the complete threat picture is an impossible feat to take on independently. Collecting, sifting through, and making sense of the massive data pool that effective cybersecurity requires is just too tedious even for an entire security team. They need the help of security data providers and a means to piece all the information they provide together to turn it into actionable intelligence. Enter security data aggregation.

At present, the number of security data aggregators is on the rise. But what makes a security data aggregation platform effective? Also, how can a technology aggregator determine which security data provider can contribute to its solution most?

A closer look at the platform's target users and their specific cybersecurity needs may be warranted at the onset. But, first off, let's define what security data is.

What Is Security Data and Who Needs It?

Security data, in this context, refers to information that organizations collect, process, and analyze to understand threat actor motives, targets, and attack behaviors so they can reduce risks, comply with regulatory requirements, and obtain in-depth insights based on forensic evidence. Examples of security data include threat intelligence, DNS records, network logs, incident data, and user behavior information, among others. It enables users to make faster, more informed, data-backed

decisions and shift from reactive to proactive security.

Security data can help several cybersecurity professionals, namely:

- Security and IT analysts can optimize prevention and detection aided by various data feeds in blocking bad IP addresses, URLs, domains, files, and other threat vectors.
- Security operations centers (SOCs) can prioritize incidents based on their risk and impact using security data.
- Computer security incident response teams (CSIRTs) can use security data to accelerate incident investigations, management, and prioritization and analyze root causes to determine an attack's scope.
- Intelligence analysts can uncover and track threat actors by looking at intrusion evidence and reviewing reports for better future detection.
- Executive management can understand risks, craft options to address them, and develop a more effective security road map.

Why the Need for Security Data?

Security data, as you may have already inferred from the user descriptions above, aids in:

- **Enhancing an organization's cybersecurity posture:** Knowledge about potential threats and their tactics, techniques, and procedures (TTPs) enables better security planning and targeted resource allocation, ultimately allowing businesses to defend against the most relevant threats.
- **Enabling a proactive cybersecurity approach:** Rather than reacting to cyber threats as they occur, security data identifies potential threats and vulnerabilities ahead of time, allowing businesses to mitigate risks before they can inflict any damage.
- **Improving incident response:** By understanding potential attackers' methods, businesses can proactively prepare and adapt their defenses. When a breach occurs, security data aids

in swift detection and targeted response, minimizing damage. Post-incident, it facilitates learning, refining preparations for future incidents.

- **Managing and reducing risks:** Security data provides insights into the most likely and most dangerous cyber threats. Armed with it, businesses can focus their resources on fortifying against specific threats, effectively reducing their overall risk and potential for damage, and enhancing their cybersecurity strategy.

Knowing who can benefit from security data and how by now, the next question is how does it form a cohesive picture? The answer lies in correlation—seeing each piece fit into the puzzle through a single dashboard, one that a security data aggregation platform can provide. But what is a security data aggregation platform, exactly?

What Is a Security Data Aggregation Platform?

A security data aggregation platform is like a one-stop shop for various kinds of cybersecurity information. So, instead of shopping for vulnerability management, antimalware, and other cybersecurity solutions one by one, organizations can opt for a single platform.

Security data aggregation platforms make acquiring threat information more efficient, providing vetted data for users. They also eliminate the need for manual data collection, allowing direct access to correlated threat information, providing actionable security intelligence and empowering immediate action.

While security data aggregation platforms may have varying components or partners, some are typically found in all, such as:

- Lists of indicators of compromise (IoCs)
- Vulnerability information sources
- Threat intelligence sources

- Domain intelligence sources
- DNS data sources
- Extended detection and response (xDR) intelligence sources
- Firewall services
- Cloud security services
- Virtual private network (VPN) services
- Virtual machine (VM) protection services

Some platforms also have solutions that provide security for specific industries like e-commerce, marketing, and more, of course.

Given the vast pool of aggregators with a wide array of partners, though, how would users know which is the right one?

What Makes a Security Data Aggregation Platform Good?

Not all security data aggregation platforms are created equal, but there are always certain criteria an ideal one should fulfill, including:

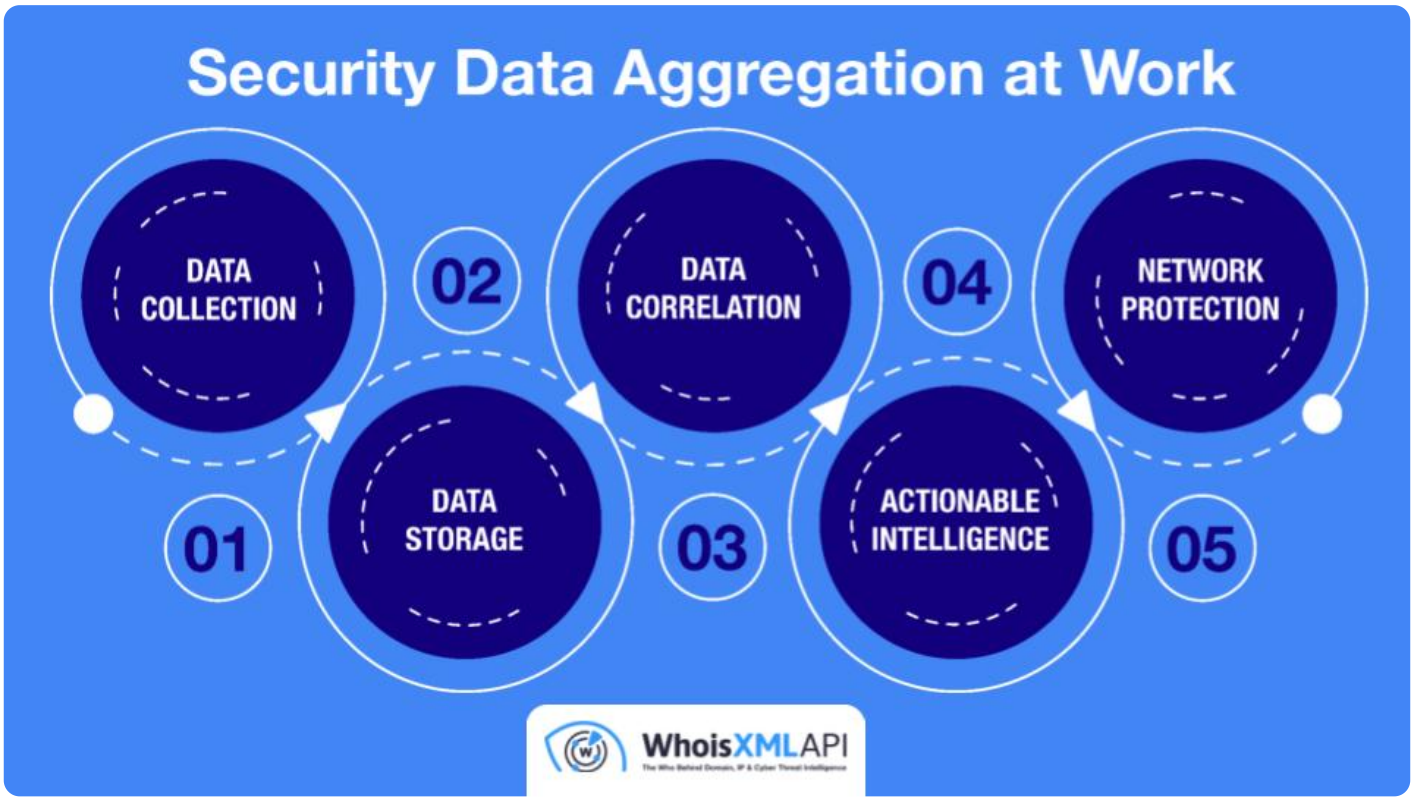
- **Provides easy access to diverse datasets:** The more relevant raw data from various sources, the better. Each dataset from sources with exhaustive coverage and regularly updated information, after all, can help organizations defend against bad actors. The more data a platform gives users access to, the stronger their defenses will be.
- **Has machine learning (ML) capabilities:** ML has the ability to recognize patterns and use them to predict threats before they can hit a network. IT security teams can also leverage ML-generated datasets to detect and evaluate a wide array of dangers, including advanced persistent threats (APTs), malware, ransomware, and zero-day exploits, adding practicality

to their intelligence. An essential aspect here is for the data to be well-formatted and consistent to ensure ML systems can ingest and use it effectively.

- **Provides automated incident response:** An attack can occur in seconds, and organizations should be able to keep up. An ideal platform must thus incorporate automated threat response capability. But that's not all. Automation can also serve other purposes. Automating security data collection and detection, for instance, relieves IT security teams of logging every threat that enters their attack surface.

- **Enables correlation:** A platform should be simple and easy to use. Apart from meeting an organization's security needs, it should also be able to map all the security data together in a way that translates to concrete actions like block access to and from specific domains or IP addresses.

Here's a simple chart that demonstrates how a security data aggregation platform typically works.

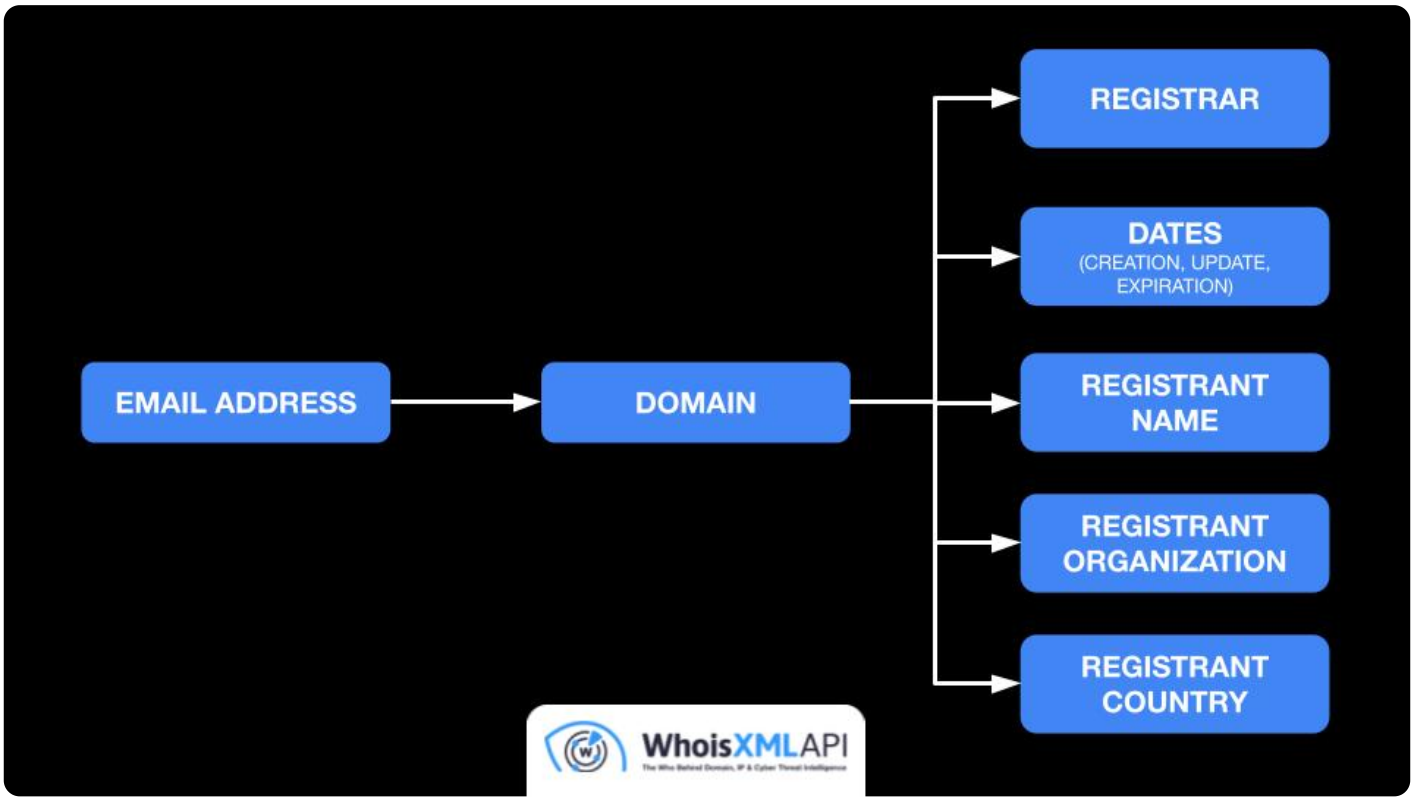


What Makes WhoisXML API a Good Security Data Partner?

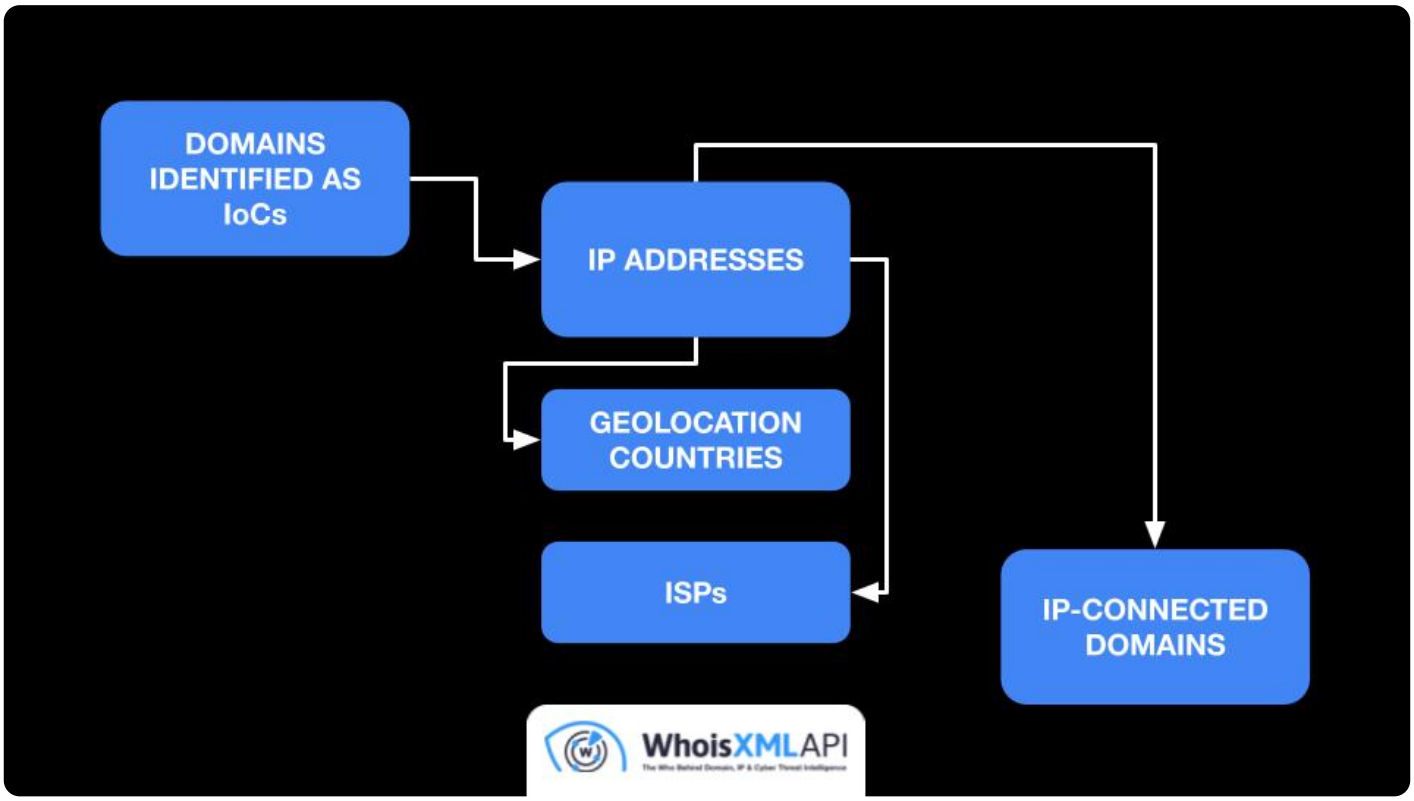
WhoisXML API has been providing security data, particularly domain, DNS, and threat intelligence to various aggregation platforms, such as Anomali ThreatStream, Cyware, Pangea, Query.AI, and Sumo Logic, in the past few years. Our data has been crucial in supporting users with threat detection and response, security investigations, digital risk mitigation, digital forensics, domain market research, and a wide range of other activities and use cases.

Our exhaustive intelligence sources that security data aggregation platforms can offer to their users comprises:

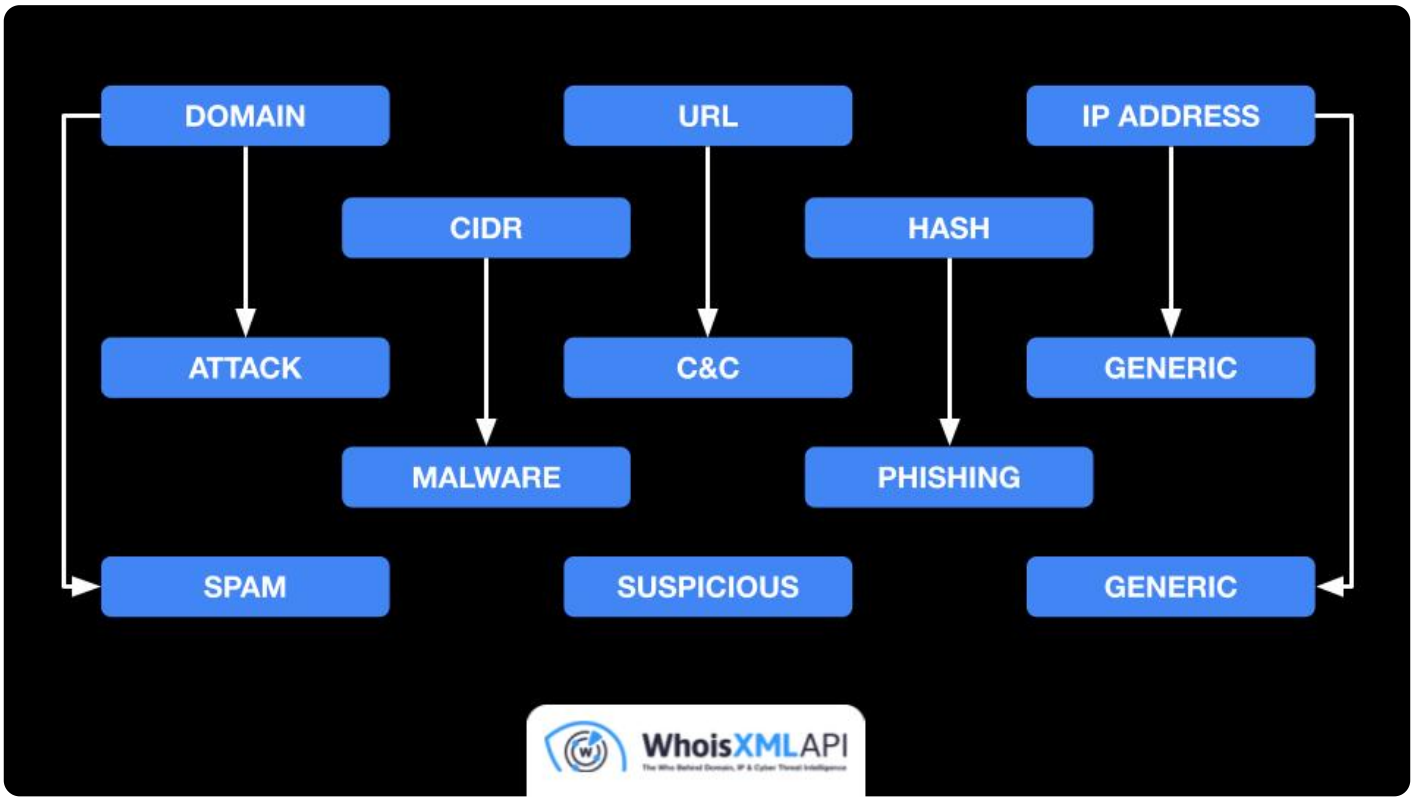
- **Domain intelligence:** Our WHOIS database tracks hundreds of millions of active domains across thousands of gTLDs and ccTLDs. On top of that, it contains complete information on registration and registrant data for billions of WHOIS records. WHOIS data is helpful in threat attribution.



- **IP and DNS data repositories:** Our IP database covers 99.5% of all IP addresses in use across hundreds of thousands of locations and ISPs. We also provide access to data for millions of IP netblocks. In addition, users can access more than a hundred billion DNS records. This data can aid users with threat infrastructure mapping and proactive attack vector identification.



- **Threat intelligence:** Our lists of IoCs identify the specific threat types (attack, command and control [C&C], generic, malware, phishing, spam, suspicious) millions of domains, URLs, IP addresses and hundreds of thousands of file hashes are associated with. Threat data is particularly helpful in threat blocking and breach prevention.



All of these data sources are regularly updated and continue to grow, made possible by our strong partnerships with ISPs, registrars, and other data providers. Security data aggregation platforms and their users can enjoy standardized data downloadable in different file outputs (JSON, XML, CSV, and PDF). Our APIs and databases come with programming libraries as well, making them easy to integrate into any platform. Best of all, platform users can customize their data consumption, depending on their current needs.

—

WhoisXML API domain, DNS, and threat intelligence has been helping organizations with various cybersecurity and business requirements for years now. And more can harness the insights and actionable intelligence it offers through security data aggregation platforms.

Ready to see how WhoisXML API's market-leading cyber intelligence sources can make your data security aggregation platform more attractive to security data users? Contact us now.

Disclaimer: this post was originally published on CircleID.com