Leveraging IP Data to Enable Extensive Asset Discovery and Contextualization

Posted on June 17, 2024

Mirroring Sun Tzu's wisdom, "To know your enemy, you must become your enemy," today's cybersecurity landscape demands that security teams see their IT infrastructure through attackers' eyes. This proactive approach is vital, notably considering the Data Breach Investigations Report (DBIR) finding that 65% of data breaches stem from external sources.

Adopting an attacker mindset enables security teams to identify and address attack vectors early and continuously manage their attack surfaces. This strategy entails asking questions like, "What assets can threat actors see and use as entry points?" and "How can compromising these assets impact other assets?"

External attack surface management (EASM) solutions, especially when supplemented with IP intelligence, can help answer these and other related questions.

What Does IP Data Bring to the EASM Table?

Organizations rely on EASM solutions to gain a comprehensive view of their external attack surface. Since these platforms are only as valuable as the visibility they provide, they typically depend on combining internal and external data sources, such as vulnerability scans, network logs, and threat intelligence feeds.

In addition to these sources, IP data can also enhance EASM visibility, especially since threat actors often use IP address scans to identify active services and potential vulnerabilities during reconnaissance.

Integrating IP data comprising critical details, such as geolocation, IP netblocks, and network ownership, into EASM solutions helps verify asset ownership; add more context; and discover more IP addresses, domains, and subdomains.

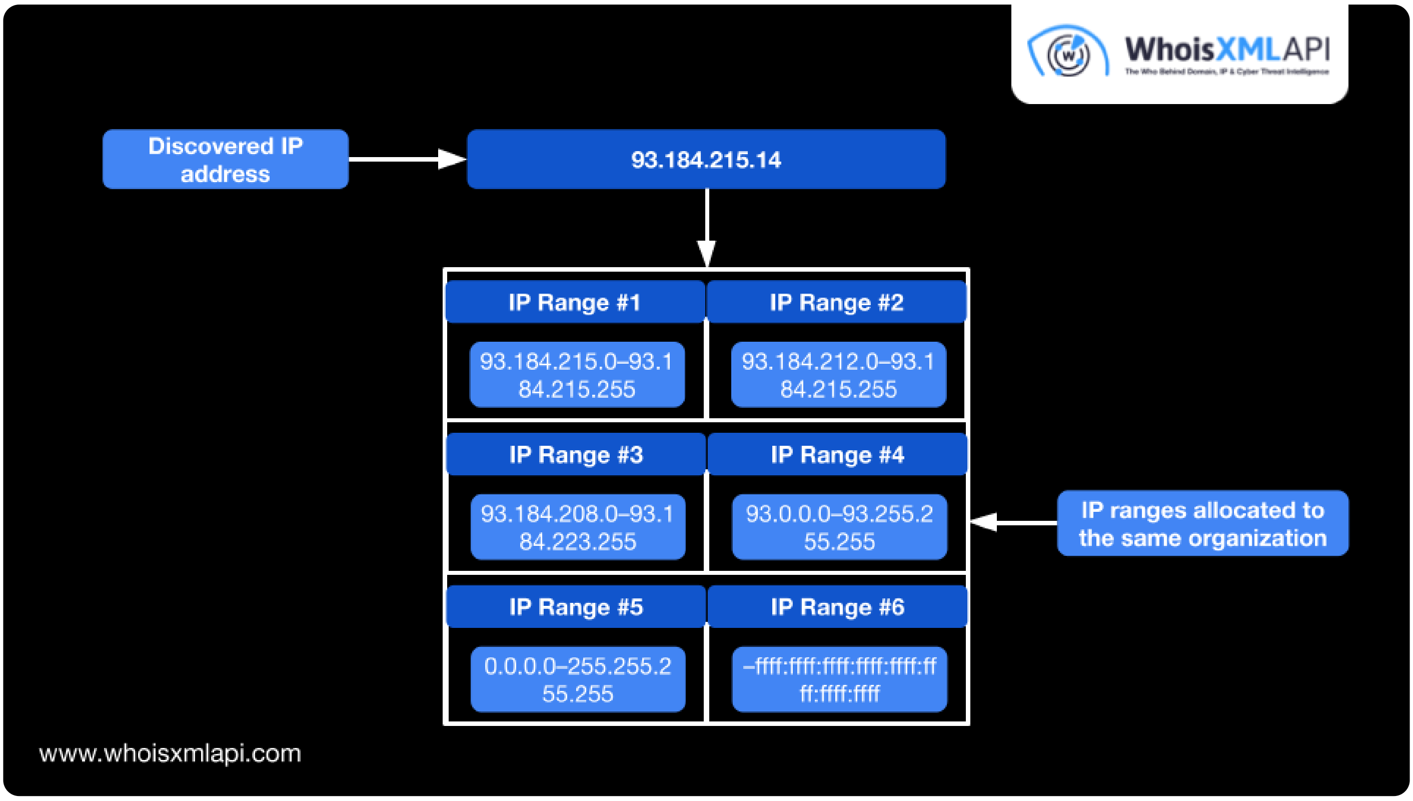
Add Ownership and Geolocation Context

IP netblocks data reveals the network contact’s name associated with an IP address block. This information helps with asset attribution, the process of verifying whether an asset belongs to the organization. It also includes geolocation information that adds more context to the asset in terms of origin.

Ultimately, understanding the ownership and location of IP addresses enables EASM solutions to effectively reduce false positives during asset discovery.

Discover Adjacent IP Addresses

When EASM platforms integrate IP netblocks data, they gain valuable insights beyond just a single IP address. They can discover other IP ranges allocated to the organization, thereby widening the asset discovery’s scope.

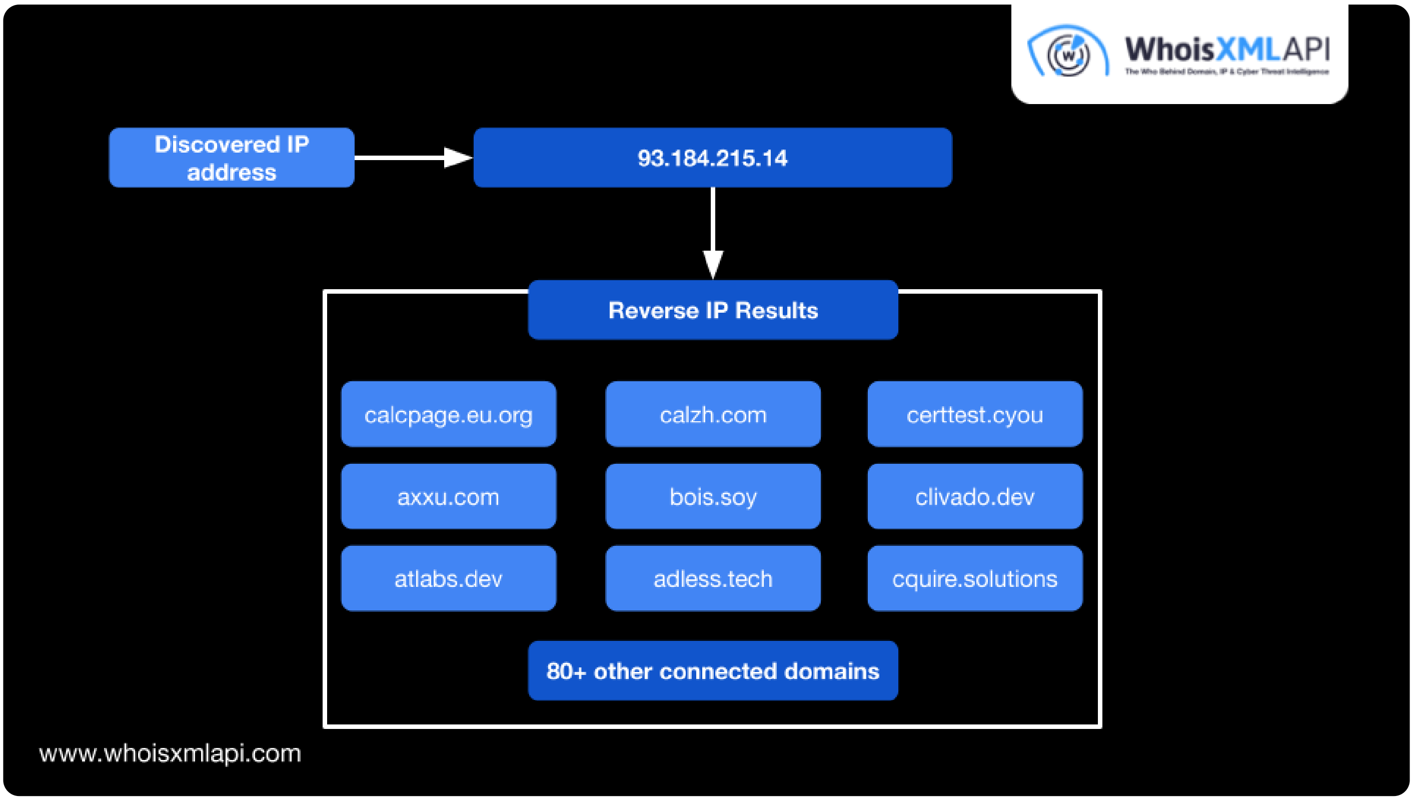


As a result, EASM solutions can discover unused or forgotten devices and services within the organization’s allocated IP range. Security teams can then take steps toward securing these previously unknown assets.

Find Connected Domains and Subdomains

Adjacent IP discovery using IP netblocks data is only one piece of the puzzle. EASM solutions can obtain a more complete picture when the IP addresses are mapped to linked domains and subdomains by tapping into reverse IP capabilities.

Reverse IP lookups query DNS records to reveal the domains associated with a particular IP address, allowing security teams to understand the purpose and functionality of the identified IP address.



Aside from expanding asset discovery, uncovering connected domains and subdomains also enables security teams to monitor them for vulnerabilities and security issues that may not be apparent from just looking at the IP address.

Conclusion

IP addresses play a crucial role in how people and businesses use the Internet. It’s no wonder that attackers target them to exploit vulnerabilities in connected systems or services. Therefore, creating an inventory of an organization’s IP addresses and connections is a crucial step in mitigating cyber threats and reducing attack surfaces.

Widen the EASM asset discovery scope of your solutions with IP data. Contact us now for more information about our IP intelligence.