The Key to Effective External Asset Discovery

Posted on March 20, 2024

The external attack surface management (EASM) industry has exploded over the years. As of Q1 2023, dozens of vendors have been competing against each other, and more have since entered the market.

However, an EASM solution is only as good as the asset visibility it provides. After all, EASM platform users can't effectively manage what they can't see. For this reason, external asset discovery is the foundation of EASM, dictating the overall effectiveness of an EASM strategy or solution.

How Does External Asset Discovery Work?

Building an effective EASM solution hinges on giving users the automated capability to find all of their assets, allowing them to easily perform all of the asset discovery phases—asset mapping, validation, and monitoring. These processes require the EASM tool to rely on a high-quality intelligence source stack that provides expanded asset coverage.

While any EASM solution can be designed to perform modern asset discovery, the question is, does it have access to the data required for extensive asset visibility? Here's how such a data requirement plays out in the asset discovery process.

Asset Mapping

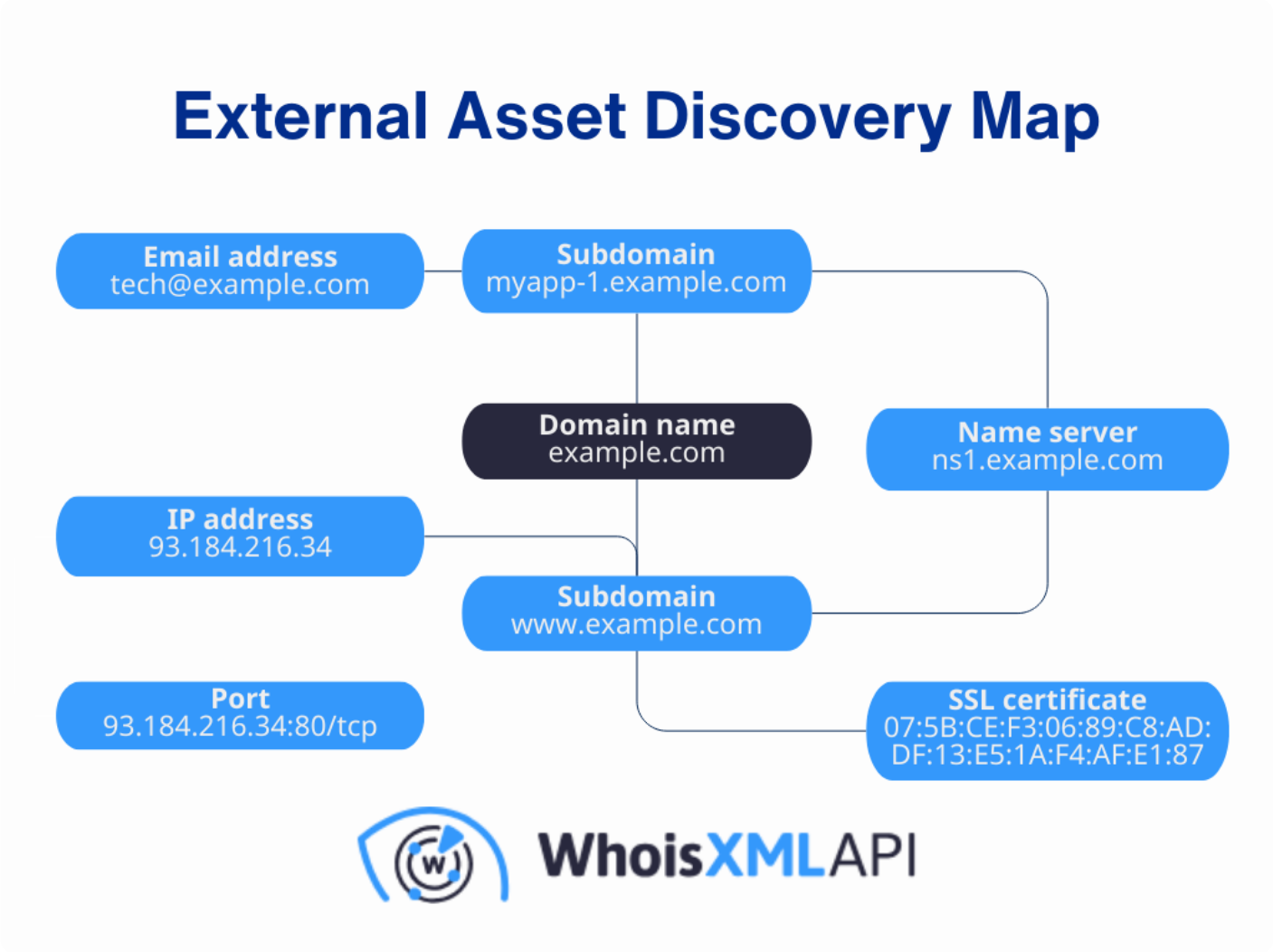
External asset discovery begins by feeding your EASM solution with the Internet-facing assets already on your user's radar. That starting point can generally be an organization's domain name,

hostname, or any external asset already known and visible to it.

The EASM solution should then be able to map known assets to all other connected external assets, including those that may have been forgotten or previously unknown. For example, the tool can find subdomains, IP addresses, name servers, and Secure Sockets Layer (SSL) certificates associated with the organization's domain name. These public-facing assets are commonly plagued with various security risks and exploitable vulnerabilities.

The crucial discovery of the user's potentially vulnerable external assets requires EASM tools to access domain, IP, and DNS intelligence. Only then can it thoroughly perform these essential asset mapping processes, to name a few:

- Domain to subdomain
- Subdomain to IP address
- Subdomain to name server
- Domain/Subdomain to SSL certificate
- Email address to mail server
- Domain to IP address
- IP address to domain
- IP address to Automated System number (ASN)
- IP address to location
- IP address to netblock



In the simplified example above, the domain example[.]com led to the discovery of two subdomains, an IP address, a port, a name server, an SSL certificate, and an email address. Any of these assets can be unsecured and vulnerable to cyber attacks, hence the importance of identifying them.

Asset Validation

The next step is to enable users to analyze the assets discovered by adding business and ownership context. The goal is to validate their authenticity and utility.

- **Authenticity:** During external asset discovery, EASM tools identify a vast number of Internet-facing resources potentially linked to the user's organization. But not all the assets discovered are necessarily legitimate or even relevant to the company's operations. For example, an EASM solution may detect a previously unknown domain resolving to the organization's IP address. When the tool gleans context from a WHOIS database, it could determine, for example, that a former employee registered the domain.

- **Utility:** It is also essential for platform users to determine if the assets identified are still in use by enriching them with DNS and Internet-related intelligence. For example, organizations may find dangling subdomains created initially for services that have already been decommissioned. They may also discover hostnames with expired SSL certificates.

By gleaning context through an EASM tool, security teams can validate external assets based on the above-mentioned criteria. As a result, they can distinguish between authorized assets (i.e., those under their control and actively used) and unauthorized assets (e.g., dangling subdomains, forgotten cloud instances, or resources provisioned by rogue employees). Asset validation also enables them to prioritize how to address potential security risks efficiently.

Asset Monitoring

Finally, asset discovery should be a never-ending process. As changes in the platform user's business operations continue to emerge (e.g., remote work setup, cloud adoption, new services, etc.), new assets are constantly created. Your user's existing assets rarely remain the same either. IP addresses are constantly reallocated, which comes with changes in ASNs, geolocations, and other IP-related data. Meanwhile, WHOIS and DNS records get updated all the time.

Therefore, an organization's attack surface is never static. As such, EASM solutions must be able to continuously capture this dynamic nature by tapping into up-to-date cyber intelligence, including:

- **WHOIS data:** Helps EASM tool users monitor domain ownership changes and identify expiring domain names.

- **IP data:** Obtaining up-to-date IP intelligence enables EASM solutions to identify and provide the current geographical location and network provider of the user's IP assets.
- **DNS data:** Continuously monitoring an organization's DNS records through EASM helps immediately identify unauthorized changes to DNS records, find orphaned DNS entries, and keep track of new subdomains added to its DNS zone.

Conclusion

External asset discovery is a crucial part of EASM. If your EASM solution falls short in this area, users may get blindsided by attackers exploiting vulnerabilities in unseen and thus unprotected assets. The key is for EASM tools to leverage in-depth domain, DNS, and IP intelligence that enables more comprehensive asset mapping, accurate asset validation, and constant asset monitoring.

Ready to see how WhoisXML API's market-leading cyber intelligence sources can enhance your external asset discovery? Contact us now.