DNS data

The domain name system (DNS) is the internet’s phone book, providing a mapping between system or network resource names and IP addresses. DNS has a hierarchical name space that typically includes three levels: a top-level domain (TLD) such as .com, .edu or .gov; a second-level domain such as “google” or “whitehouse;” and a system level such as “www” or “mail.” DNS nameservers operate in this hierarchy either by acting as authoritative sources for particular domains, such as a company or government agency, or by acting as caching servers that store DNS query results for subsequent lookup by users in a specific location or organization; for example, a broadband provider caching addresses for its customers.

DNS server logs provide operations teams with a record of traffic, the type of queries, how many are locally resolved either from an authoritative server or out of cache, and a picture of overall system health. Logs can also reveal an unusually high number of requests from external sources and whether an organization’s servers have been compromised. Finally, DNS data can provide detection of unknown domains, malicious domains, and temporary domains. In the Common Information Model, DNS data is typically mapped to the Network Resolution data model.

Application

When your Splunk deployment is ingesting DNS data, you can use it to accomplish security and compliance and IT Ops use cases.

- Monitoring a network for DNS exfiltration
- Monitoring DNS queries
- Detecting host redirection attacks

Sources

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with DNS data.

- Technology Add-on for Unbound DNS
- Splunk Add-on for ISC BIND