Network protocol data

Network protocols describe the structure of data that flows through networks. In most cases, network ports are assigned to specific protocols for both security and performance reasons. Some protocols operate at a lower level of the computing stack and are used to direct packet routing, such as TCP, UDP or IP. Other protocols, such as HTTP, HTTPS and TNS describe how packets are structured for applications such as web services, databases, and a wide range of client-based applications. Application traffic can be monitored for usage, performance, and availability, and can provide visibility into specific user data.

Network protocols are an important source for identifying advanced persistent threats, analyzing traffic flows for unusual activity, and identifying potential data exfiltration. Aggregating and analyzing flow records also can show anomalous traffic patterns and flow destinations that are indicative of a breach, such as an APT phoning home to a command and control server for instructions, additional malware code, or copying large amounts of data to an attacker’s system. The data can also be used to detect traffic related to DDoS, malicious domains, and unknown domains or locations. In the Common Information Model, network protocol data is typically mapped to the Network traffic data model.

Application

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

- Complying with the Markets in Financial Instruments Directive II

Sources

Guidance for onboarding data can be found in the Spunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud).