Deep packet inspection data

Deep Packet Inspection (DPI) is a fundamental technique used by firewalls to inspect headers and the payload of network packets before passing them down the network subject to security rules. DPI provides information about the source and destination of the packet, the protocol, other IP and TCP/UDP header information, and the actual data. In the Common Information Model, deep packet inspection data is typically mapped to the Network Traffic Data model.

DPI provides raw information of everything transmitted over a network, including things that aren’t necessarily part of or difficult to extract from a log, such as database query results. PCAP data can also be used to provide and identify:

- DNS session analysis for malicious domain communications from each endpoint
- Abnormal amounts of traffic or sessions
- Abnormal amounts of domain and host communications
- Known malicious traffic from a host
- Expired SSL certification analysis
- Abnormal host communications (internal and external)

Application

Detection

- Detecting the use of randomization in cyberattacks
- Monitoring a network for DNS exfiltration
- Detecting UDP amplification abuse
- Monitoring employee network traffic
- Monitoring command line interface actions
- Detecting software supply chain attacks

Investigation

- Investigating a ransomware attack
- Analyzing wire data from databases

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 deep packet inspection data.

- Splunk App for Stream
- PCAP Analyzer for Splunk
- Zeek App for Splunk