DHCP data

DHCP is the network protocol most client devices use to associate themselves with an IP network. Implemented via a DHCP server, which could be standalone or embedded in a router or other network appliance, DHCP provides network clients with critical network parameters including IP address, subnet mask, network gateway, DNS servers, WINS or other name servers, time servers (NTP), a host and domain name, and the address of other optional network services. DHCP logs show exactly which systems are connecting to a network, their IP and MAC addresses, when they connect and for how long. In the Common Information Model, DHCP data is typically mapped to the Network Sessions data model.

Application

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

- Processing DMCA notices

Sources

Guidance for onboarding data can be found in the Spunk 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 DHCP data.

- DHCP Insight