Network access control data

Network access or admission control is a form of client/endpoint security that uses a locally installed software agent to pre-authorize connections to a protected network. NAC screens client devices for contamination by known malware and adherence to security policies such as running an approved OS with the most recent patches. Clients that fail NAC screens are rerouted to an isolated quarantine network until any detected problems are corrected. NAC data provides security teams with a detailed profile of a client’s state and activity. It can provide details into unauthorized device connections and be used to correlate users/IP to a physical network location. In the Common Information Model, NAC data is typically mapped to the Network Sessions data model.

Application

When your Splunk deployment is ingesting NAC data, you can use it to accomplish security and compliance use cases, such as the following:

- Monitoring NIST SP 800-53 rev5 control families
- Detecting AWS network ACL activity

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 NAC data.

- Technology Add-on for Cisco Secure Access Control Server (ACS)
- Aruba Networks Add-on for Splunk