Cisco: Identity Services

Cisco Identity Services Engine (ISE) is a security policy management and control platform. It automates and simplifies access control and security compliance for wired, wireless, and VPN connectivity. You can use the Splunk platform to analyze Cisco ISE syslog data directly or use it as a contextual data source to correlate with other communication and authentication data. In the Common Information Model, Cisco Identity Services data can be mapped to any of the following data models, depending on the field: Alerts, Authentication, Change, Endpoint, Network Traffic.

Configuration

Guidance for onboarding data can be found in the Spunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Source type: cisco:ise:syslog
- Add-on or app:
  - Splunk Add-on for Cisco Identity Services (Supported Add-On)
  - Splunk for Cisco Identity Services (Unsupported App)

Application

When your Splunk deployment is ingesting Cisco Identity Services data, you can use the data to achieve the following:

- Processing DMCA notices