Physical card reader data

Most organizations use automated systems to secure physical access to facilities. Historically, these have been simple magnetic strips affixed to employee badges; however, locations with stringent security requirements may use some form of biometric reader or digital key. Regardless of the technology, the systems compare an individual’s identity with a database and activate doors when the user is authorized to enter a particular location.

Badge readers record information such as user ID, date and time of entry, and sometimes a photo for each access attempt. The data can be used to detect attempted breaches and be correlated to system and network logs to identify potential insider threats and provide overall situational awareness. It can also be used to detect access at unusual times and locations or for unusual durations.

Application

When your Splunk deployment is ingesting physical card reader data, you can use it to accomplish security and compliance use cases.

- Monitoring badges for facilities access

Sources

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