Mobile device data

Given the array of always-active sensors on mobile devices, these devices provide a flood of data. Security teams can expand the threat landscape by monitoring mobile device data for abnormal activity in regards to authentication, location, and application usage. Mobile device data provides physical parameters such as location, network MAC ID, device GUID, device type, and OS version. They also include network settings such as address, AP or cell-base station location, and link performance. Application-specific telemetry such as time in app, features used and internal state and debug parameters similar to those provided by conventional application servers. Insights into mobile application data can help developers deliver a better performing mobile app.

Application

When your Splunk deployment is ingesting mobile device data, you can use it to accomplish security and compliance use cases:

- Monitoring mobile device payments

Sources

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