Summer 2020

Splunk Software Platform Data Transformation

Shanell Hurst

ABSTRACT

Machine data can be harvested from virtually any device in a structured or unstructured format. The amount of information collected can be massive, confusing and challenging to interpret. Data compilation has the ability to tell a story about events that have taken place. Splunk's software platform can demystify obscurity by allowing users to view machine data in an understandable format, correlate information with log files, send alerts as well as pinpoint sources for troubleshooting and problem resolution. I implemented different forwarder instances on various servers located in both public facing and virtual environments. Indexers were created to store, process and classify events from the machine data received. This platform provides a graphical user interface where data can be further parsed and searched. The distribution will also allow future students to experience how to transform machine data into statistics and visualizations, query input with Splunk Processing Language (SPL), create triggered events for alerting, create reports as well as monitor events in real time.