Washington University of Science and Technology

SOC LAB

SPLUNK: 10 STEPS

Splunk is a data management platform that gathers, analyzes, and visualizes machine-generated data from various sources such as web servers, networks, sensors, and other databases. It allows users to create reports, dashboards, graphs, alerts, and other visualizations, facilitating insights and issue resolution.

Starting with Splunk for system auditing and analysis involves a few key steps. Here's a beginner-friendly guide:

1. Install Splunk:
   - Download the appropriate version of Splunk Enterprise from Splunk website.
   - Follow instructions. Splunk can be installed from Windows, Linux, and MacOS.
2. Familiarize Yourself with the Splunk Interface:
   - Once installed, navigate to http://<YourServerName>:8000 in your browser.
   - Explore the main features like Search & Reporting.
3. Add Data to Splunk:
   - To start analyzing system data, you need to add it to Splunk.
   - Go to "Settings" > "Add Data" on the Splunk Web interface.
   - Can add data from files and directories or receive data using forwarders.
4. Learn Basic Search Processing Language (SPL):
   - SPL is the query language you use in Splunk to search and analyze data.
   - Start with basic commands like search, stats, top, rare, and timechart.
5. Creating Your First Search:
   - In the Search & Reporting app, enter a basic SPL command to search your data. For example, index="_internal" |
6. Analyze and Visualize Data:
   - Use SPL to analyze data and identify patterns, anomalies, or events relevant to auditing.
   - Create visualizations like charts and graphs for better understanding.
7. Set Up Alerts for System Auditing:
   - In the Search & Reporting app, you can create alerts based on specific search criteria.
   - Set an alert for multiple failed login attempts to detect potential security breaches.
8. Creating Dashboards:
   - Dashboards are useful for monitoring systems in real time.
   - You can create custom dashboards with various panels displaying your system's security.
9. Understand and Implement Data Models:
   - It helps in structuring data and useful for complex analytical tasks and pivot tables.
10. Continuously Learn and Explore:
    - Splunk has a steep learning curve, so continuous learning is key.
    - Use resources like Splunk documentation, online forums, and community events.

Splunk is a powerful tool, and its full potential is realized when you become comfortable with the SPL and the various features it offers for data analysis and visualization.

Practice and Experiment

• The best way to learn Splunk is by practicing. Experiment with different types of data and SPL commands.

• Try to replicate real-world scenarios you might encounter in system auditing.