Scenario: You have recently joined the Security Operations team at a medium-sized organization. As part of your first assignment, you are tasked with analyzing OpenSSH log files to help identify any potential security threats. The organization has recently experienced a few suspicious incidents, and management is keen on understanding if there are any patterns or anomalies in the SSH login attempts.

Objective:

Your goal is to use Splunk Cloud to thoroughly analyze the provided OpenSSH log file and create a comprehensive report covering all aspects of your work. You will also need to set up a dashboard and an alert in Splunk Cloud to help monitor similar activities in the future. Additionally, you will manage user accounts in Splunk Cloud as part of the assignment.

Tasks:

1. **User Management:**
    - **Add New Users:** Create a new user in Splunk Cloud for each group member. Ensure the following configurations:
        - **Time Zone:** Set the time zone to WAT (West Africa Time).
        - **Default App:** Set the default app to "launcher (home)."
        - **Password Policy:** Configure each user to change their password on the first login.
        - **Role Assignment:** Assign an appropriate role to each new user based on their responsibilities.
2. **Analysis:**
    - **Upload the Log File:** Load the provided OpenSSH log file into Splunk Cloud.
    - **Analyze the Data:** Conduct a detailed analysis of the log file. Look for anomalies such as unusual IP addresses, multiple failed login attempts, or any other indicators of potential security issues.
3. **Dashboard and Alert Creation:**
    - **Create a Dashboard:** Use the search query ***'Received disconnect from 112.95.230.3: 11: Bye Bye [preauth]'*** to create a dashboard in Splunk Cloud. Ensure the dashboard visualizes relevant data from the OpenSSH logs effectively.
    - **Configure an Alert:** Set up an alert based on the provided search query. The alert should:
        - Run daily at 8am.
        - Expire after 24 hours.
        - Trigger when the number of results is greater than 2.
        - Be received via email in plain text format.
        - **Include all group members as recipients:** Ensure that all members of your group are included as recipients of the alert email.
        - **Restrict Email Domain:** Configure Splunk to allow alert emails to be sent only to a particular domain.

4. **Field Extraction:**
    - **Create Field Extraction:** Configure a field extraction for the IP address ***'183.62.140.253'*** in Splunk Cloud. Name the extraction ***'src_ip'***.
5. **Reporting:**
    - Prepare and submit a well-organized report that includes your Splunk Cloud dashboard and alert configurations along with a comprehensive summary of all tasks completed.

Resources:

Create Free Splunk Cloud Account

How to create users in splunk cloud

How to upload log file to splunk

About Splunk Commands