Cybersecurity

Module 19 Challenge Submission File

Let's Go Splunking!

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: The Need for Speed

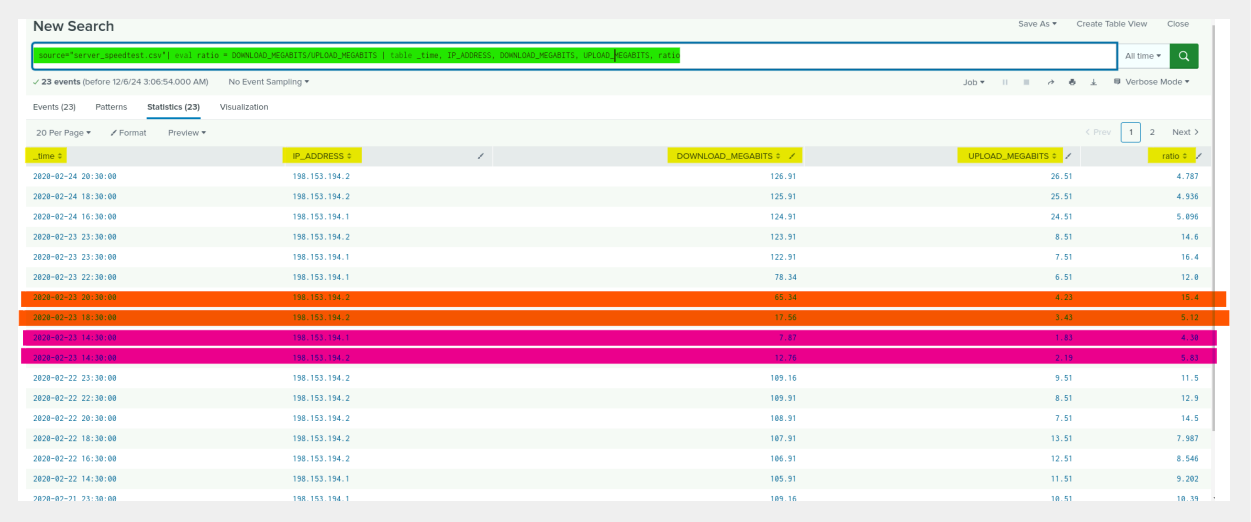
1. Based on the report you created, what is the approximate date and time of the attack?

Based upon the findings in the report, you can see download and upload speed dropped at 2:30pm on February 23, 2020

2. How long did it take your systems to recover?

Recovery began with a noticeable improvement in download speed, increasing from 17.56 Mbps to 65.34 Mbps, at 23:30:00 on February 23, 2020. This increase in speed is highlighted in orange in the screenshot. By 16:30:00 on February 24, 2020, both upload and download speeds had returned to normal.

Provide a screenshot of your report:



Step 2: Are We Vulnerable?

Provide a screenshot of your report:

Provide a screenshot showing that the alert has been created:

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

As observed, there is a significant spike in the number of events labeled "An account failed to log on" around 9:00 AM on February 21, 2020. Out of a total of 1,004 events, 124 occurred at this specific time, with similar numbers continuing in the hours that followed. Based on this pattern, it is reasonable to conclude that the attack likely began around 9:00 AM on February 21, 2020.

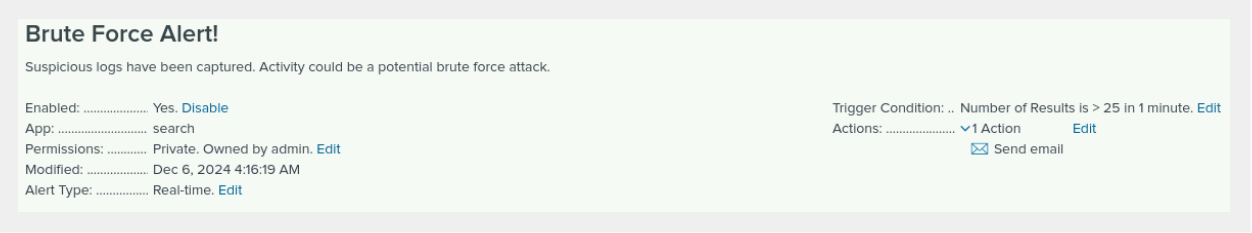
2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

Looking at the timeline of these events, we can observe that 124 failed logons is a significant spike. In the hours leading up to this, the highest number of bad logins was around 23, which we can consider normal behavior. (See screenshot for reference.)

Given that the brute force attack involved 124-135 logon attempts, I would establish a baseline of approximately 40 bad logons per hour. Based on this, I recommend the following ranges for assessing failed logon attempts per hour:

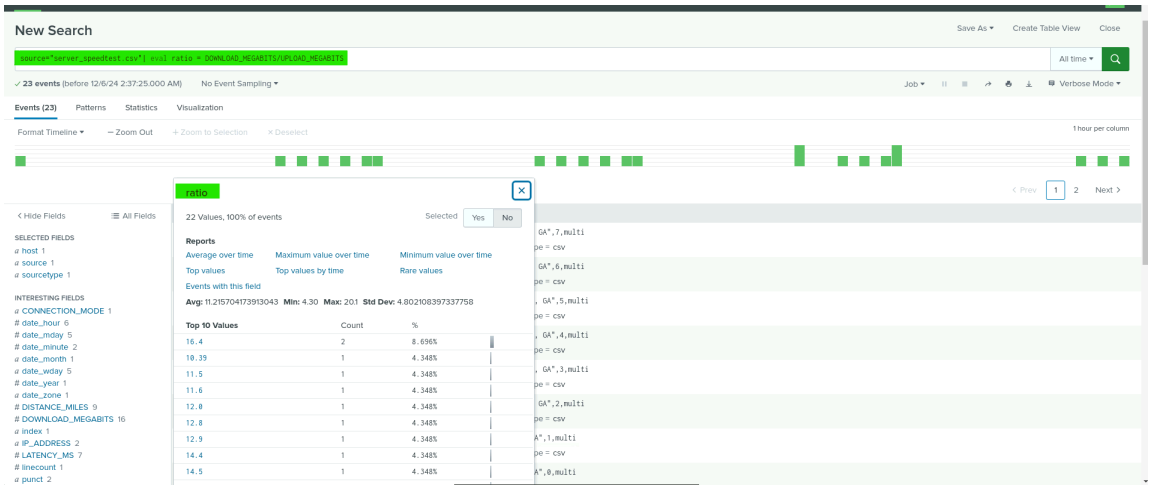
0-25 failed logons: Normal behavior.
25-50 failed logons: Worth investigating.
50+ failed logons: Critical. Events should be investigated as soon as possible.

3. Provide a screenshot showing that the alert has been created:

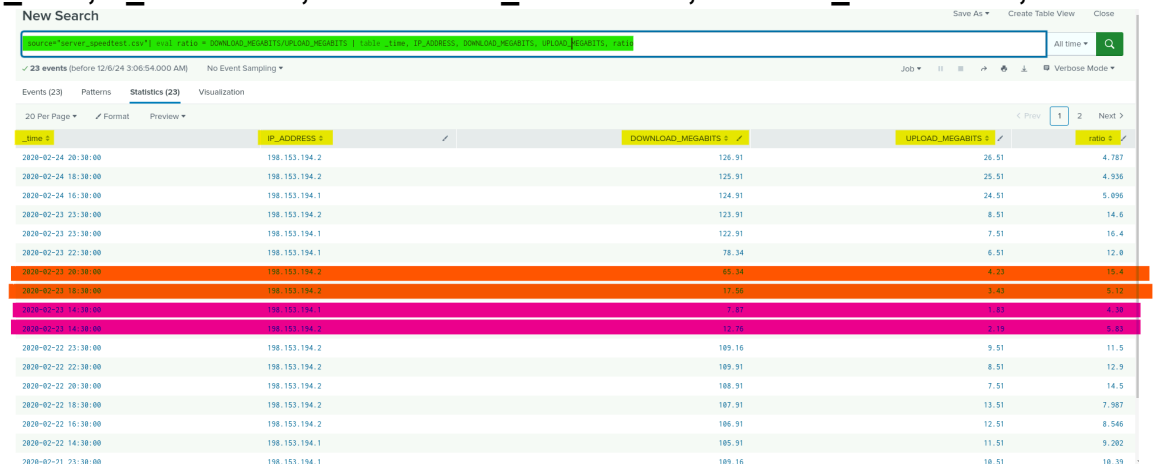


Detailed Work:
Your Task: Create a report to determine the impact of the DDOS attack on upload and download speed. Create an additional field to calculate the ratio of the upload speed to the download speed. To do so, complete the following steps:

Upload the following file containing the system speeds around the time of the attack: Speed Test File
Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.



Create a report using Splunk's table command to display the following fields in a statistics report: _time,IP_ADDRESS,DOWNLOAD_MEGABITS,UPLOAD_MEGABITS, ratio.



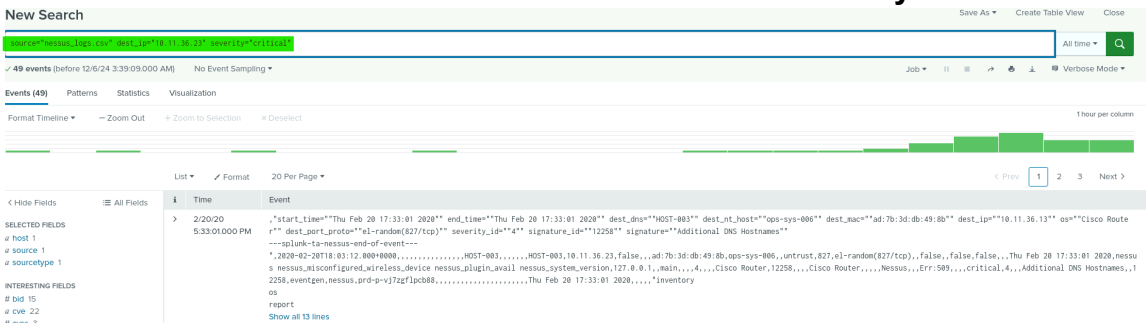
What was the approximate date and time of the attack?
Based on the report, the attack appears to have started at 14:30:00 on February 23, 2020, as indicated by the drop in download and upload speeds (highlighted in magenta in the screenshot).

How long did it take the systems to recover?
Recovery began with a noticeable improvement in download speed, increasing from 17.56 Mbps to 65.34 Mbps, at 23:30:00 on February 23, 2020. This increase in speed is highlighted in orange in the screenshot. By 16:30:00 on February 24, 2020, both upload and download speeds had returned to normal.

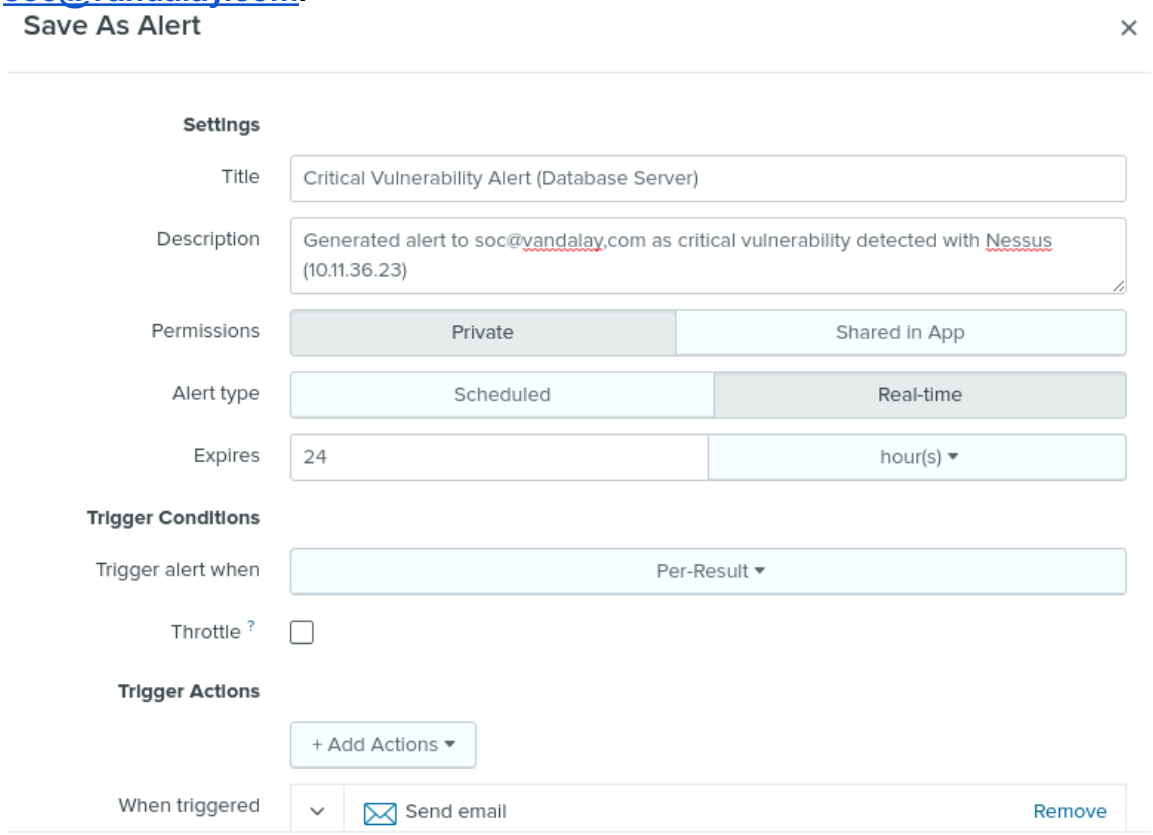
In summary:
The attack started at 14:30:00 on February 23, 2020.
Recovery began at 23:30:00 on February 23, 2020, with the increase in speed highlighted in orange.
Full recovery was achieved by 16:30:00 on February 24, 2020.

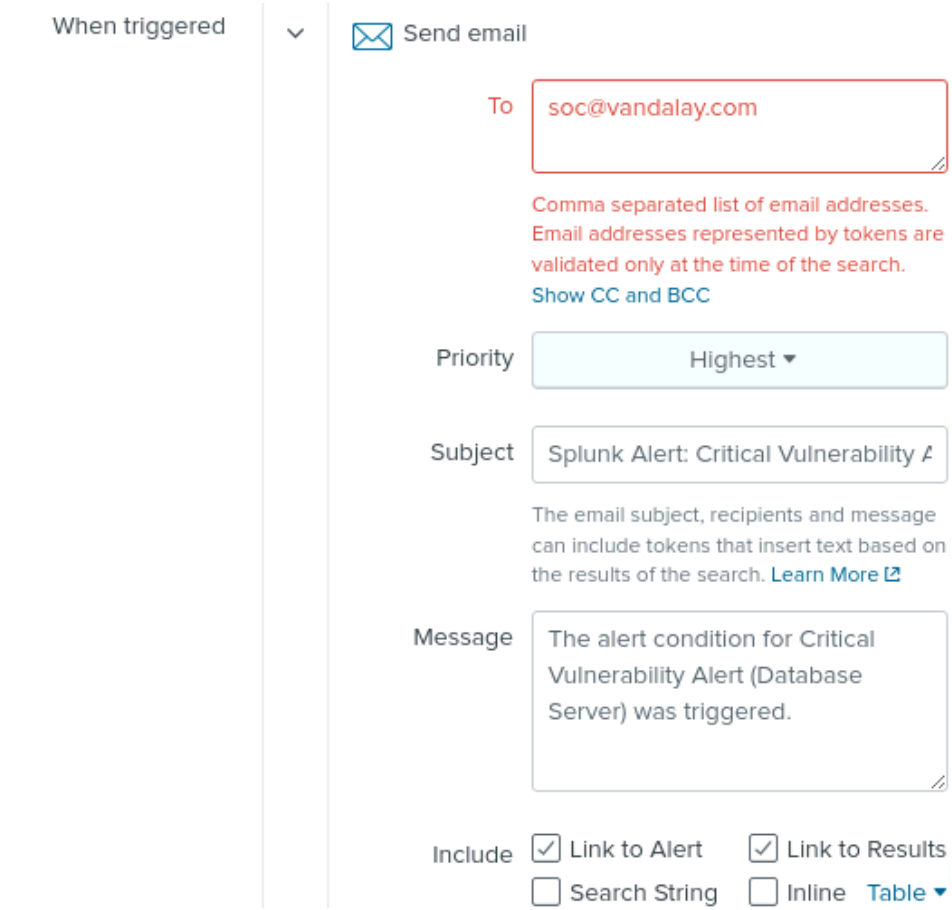
Are We Vulnerable?

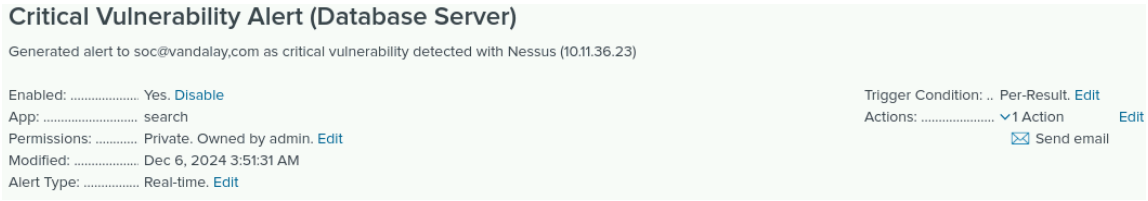
Create a report that shows the count of critical vulnerabilities from the customer database server.
The database server IP is 10.11.36.23.
The field that identifies the level of vulnerabilities is severity.



Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to soc@vandalay.com.

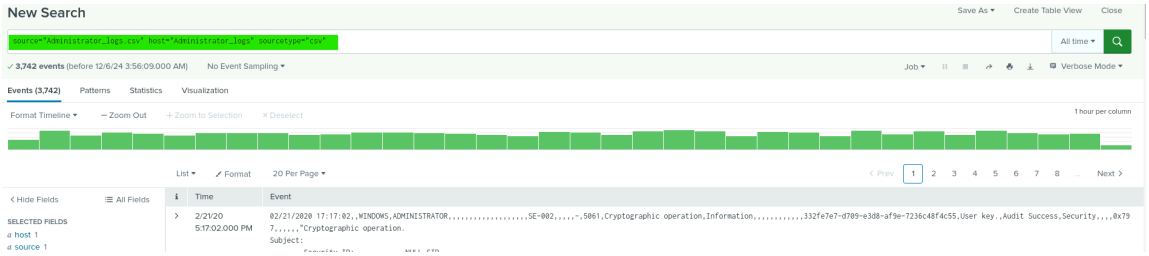




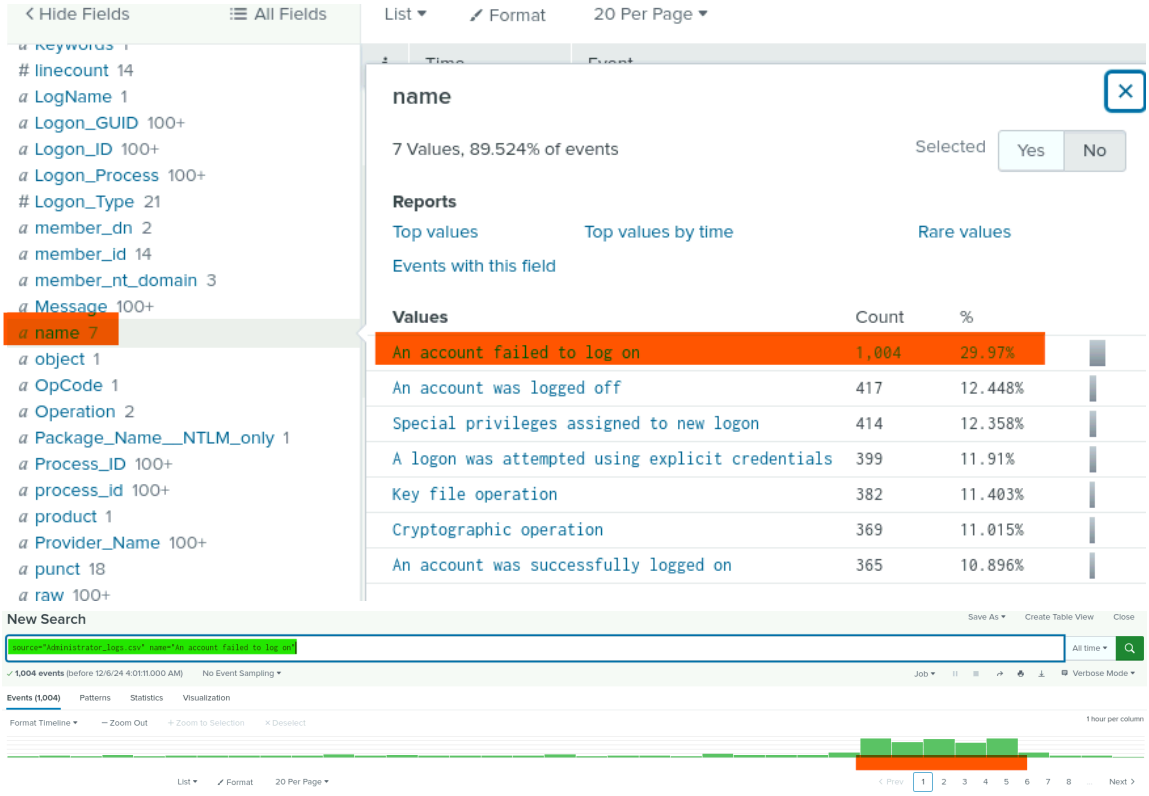


Step 3: Drawing the (Base)line

1. Upload the administrator login logs.

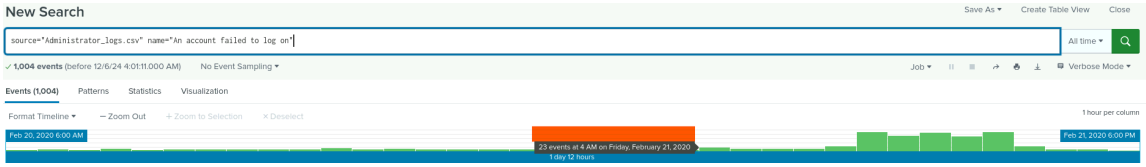


When did the brute force attack happen?



As observed, there is a significant spike in the number of events labeled "An account failed to log on" around 9:00 AM on February 21, 2020. Out of a total of 1,004 events, 124 occurred at this specific time, with similar numbers continuing in the hours that followed. Based on this pattern, it is reasonable to conclude that the attack likely began around 9:00 AM on February 21, 2020.

Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:



Looking at the timeline of these events, we can observe that 124 failed logons is a significant spike. In the hours leading up to this, the highest number of bad logins was around 23, which we can consider normal behavior. (See screenshot for reference.)

Given that the brute force attack involved 124-135 logon attempts, I would establish a baseline of approximately 40 bad logons per hour. Based on this, I recommend the following ranges for assessing failed logon attempts per hour:

0-25 failed logons: Normal behavior.
25-50 failed logons: Worth investigating.

50+ failed logons: Critical. Events should be investigated as soon as possible.

Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered. Provide a screenshot showing that the alert has been created.

Save As Alert

Settings

Title: Brute Force Alert!

Description: Suspicious logs have been captured. Activity could be a potential brute force attack.

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Expires: 30 day(s)

Trigger Conditions

Trigger alert when: Number of Results

is greater than 25

in 1 minute(s)

Trigger: Once | For each result

Throttle ?

Trigger Actions

+ Add Actions

When triggered

Send email — Remov

To: soc@vandalay.com

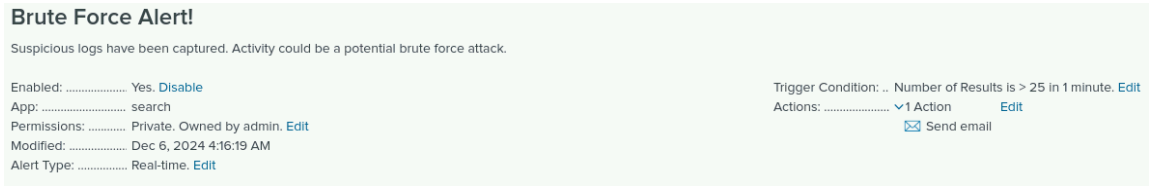
Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.
Show CC and BCC

Priority: Normal

Subject: Splunk Alert: Brute Force Alert!

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Message: The alert condition for Brute Force Alert! was triggered.



© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.