Let's Go Splunking!

You have just been hired as an SOC analyst by Vandalay Industries, an importing and exporting company.

- Vandalay Industries uses Splunk for their security monitoring and have been experiencing a variety of security issues against their online systems over the past few months.
- You are tasked with developing searches, custom reports, and alerts to monitor Vandalay's security environment in order to protect them from future attacks.

System Requirements

You will use the Splunk app located in the web lab.

Your Objective

Utilize your Splunk skills to design a powerful monitoring solution to protect Vandalay from security attacks.

As you complete the assignment, fill out the M19 Challenge Submission FileLinks to an external site., which will be your Challenge deliverable. Remember to make a copy of this file before filling it out. Make sure to provide the following:

- Screen shots where indicated.
- Custom report results where indicated.

Topics Covered in This Assignment

- Researching and adding new apps
- Installing new apps
- Uploading files
- Splunk searching
- Using fields
- Custom reports
- Custom alerts

Let's get started!

Vandalay Industries Monitoring Activity Instructions

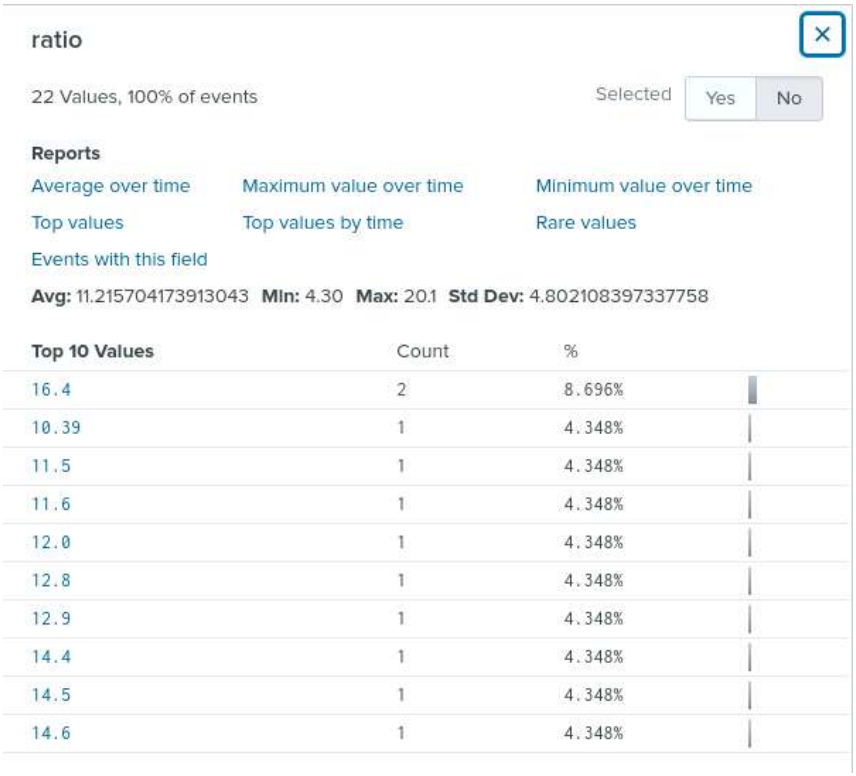
Step 1: The Need for Speed

Background: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandalay has been experiencing DDOS attacks against their web servers.

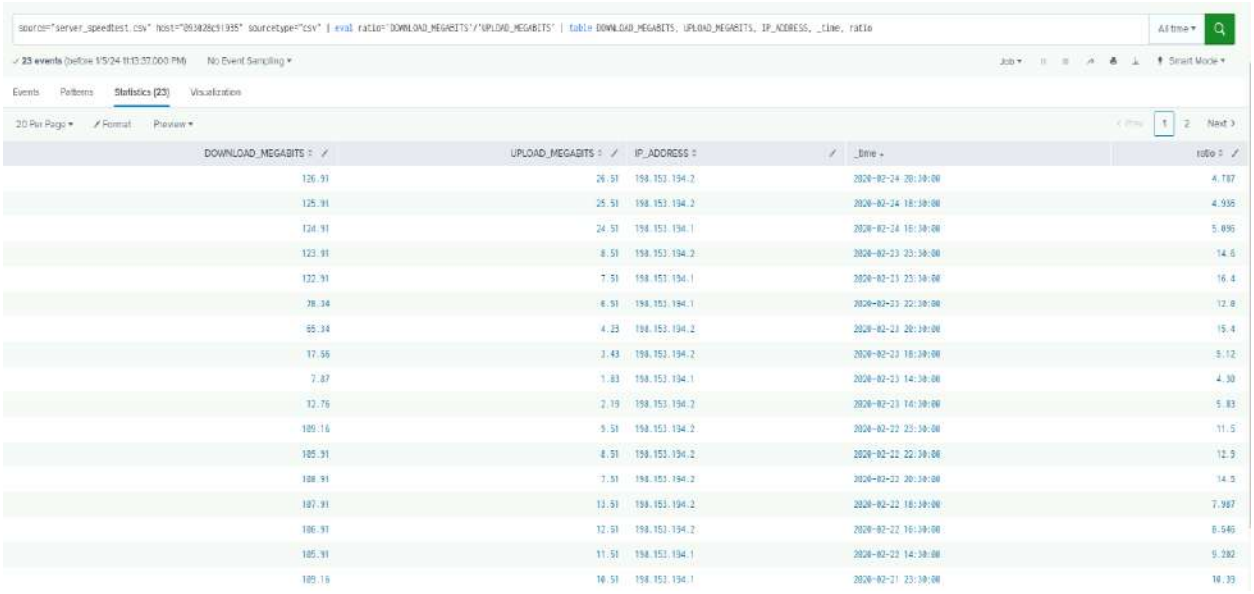
Not only were Vandalay web servers taken offline by a DDOS attack, but upload and download speed were also significantly impacted after the outage. Your networking team provided results of a network speed run around the time of the latest DDOS attack.

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:

1. Upload the following file containing the system speeds around the time of the attack:
    - Speed Test FileLinks to an external site.
2. Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.



3. 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



4. Answer the following questions in the M19 Submission File:
    - **(1)** Based on the report you created, what is the approximate date and time of the attack? 2020-02-23 14:30 (2:30 PM)
    - **(2)** How long did it take your systems to recover? 8 hours

Step 2: Are We Vulnerable?

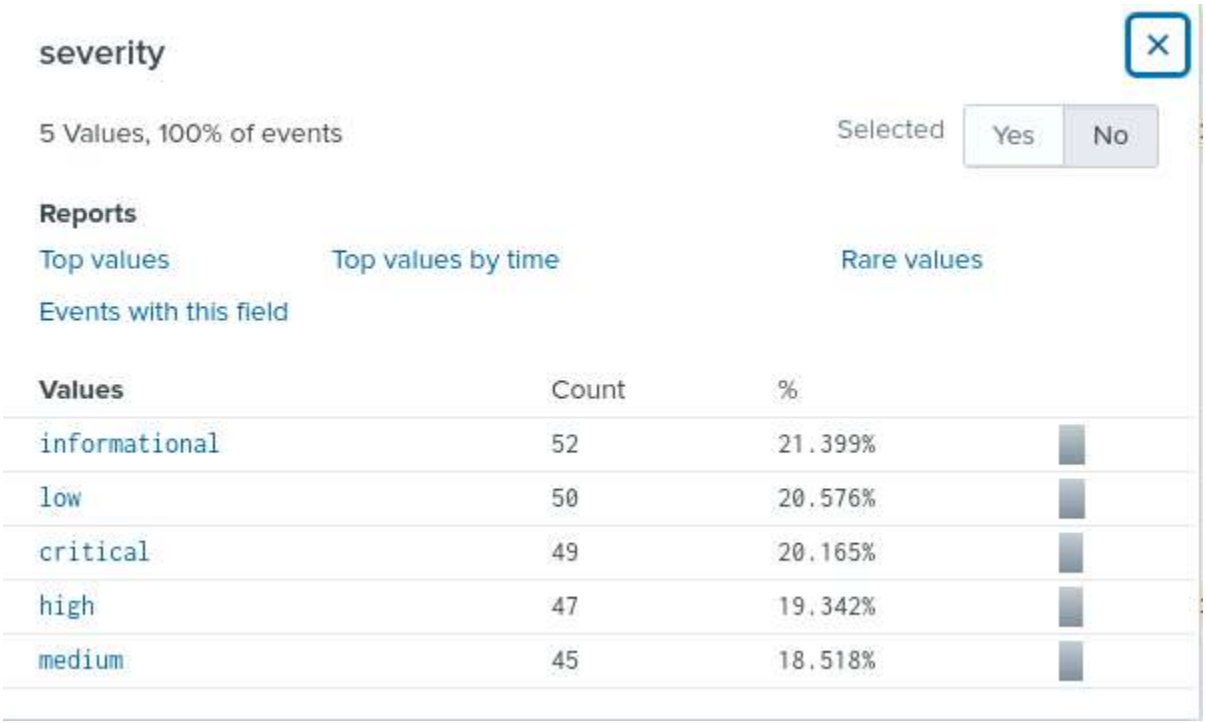
Background: Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

- For more information on Nessus, refer to the following link: https://www.tenable.com/products/nessus.

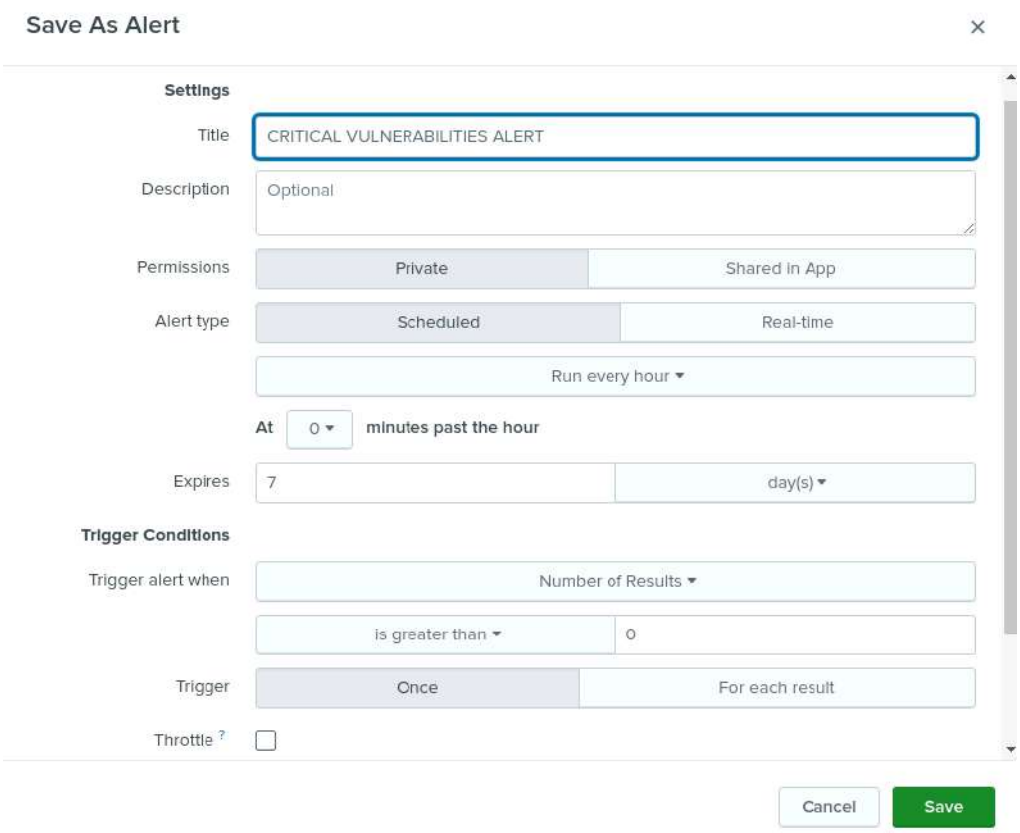
Your Task: Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server. To do so, complete the following steps:

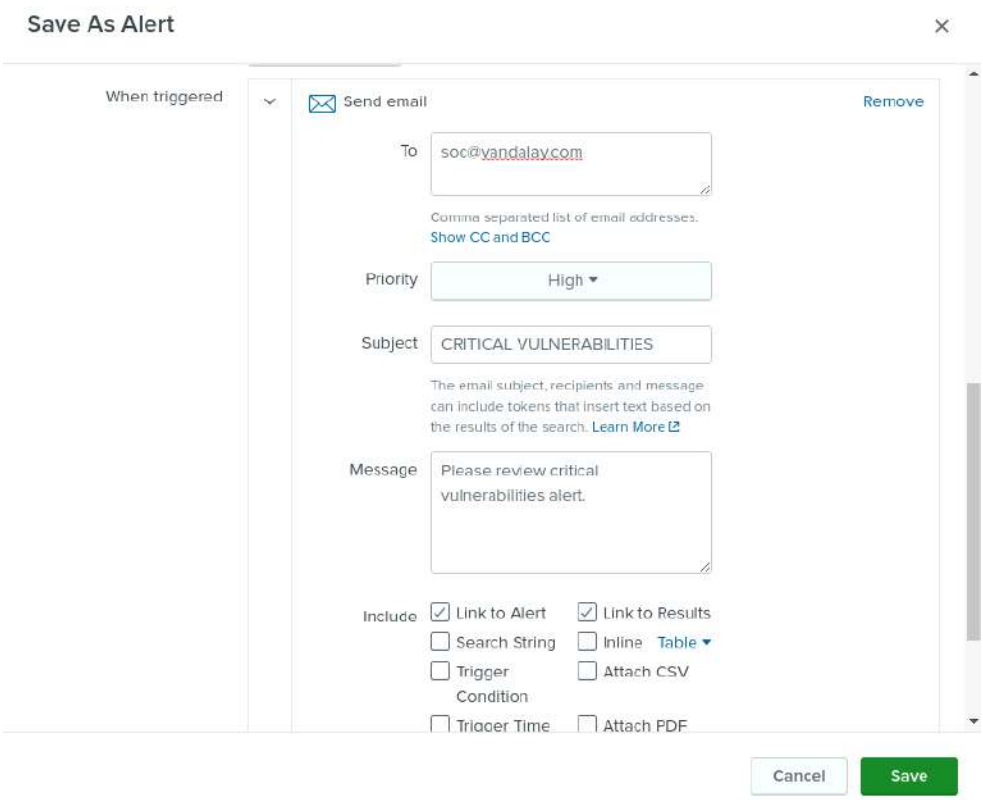
1. Upload the following file from the Nessus vulnerability scan:
    - Nessus Scan ResultsLinks to an external site.
2. Create a report that shows the count of critical vulnerabilities from the customer database server.
    - The database server IP is 10.11.36.23.

- The field that identifies the level of vulnerabilities is severity.

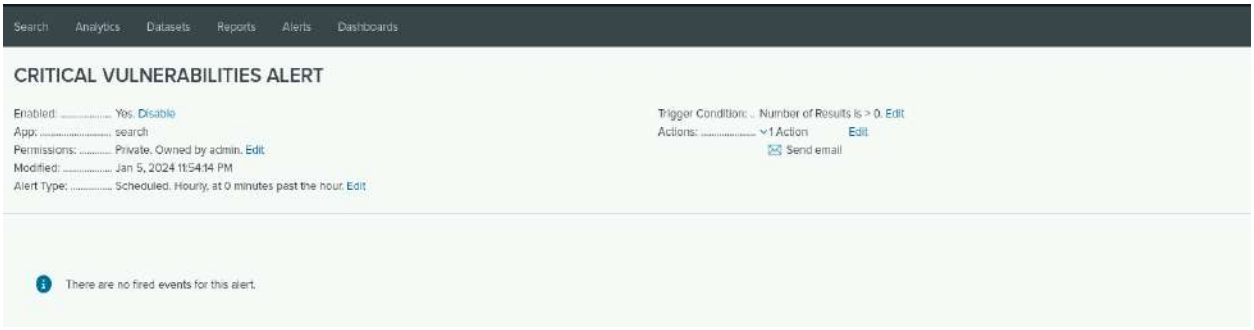


3. Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to soc@vandalay.com.


Save As Alert
Settings
Title
CRITICAL VULNERABILITIES ALERT
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every hour
At
0
minutes past the hour
Expires
7
day(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
0
Trigger
Once
For each result
Throttle
Cancel
Save



4. In your M19 Submission File, include a screenshot of your report and a screenshot showing that the alert has been created.



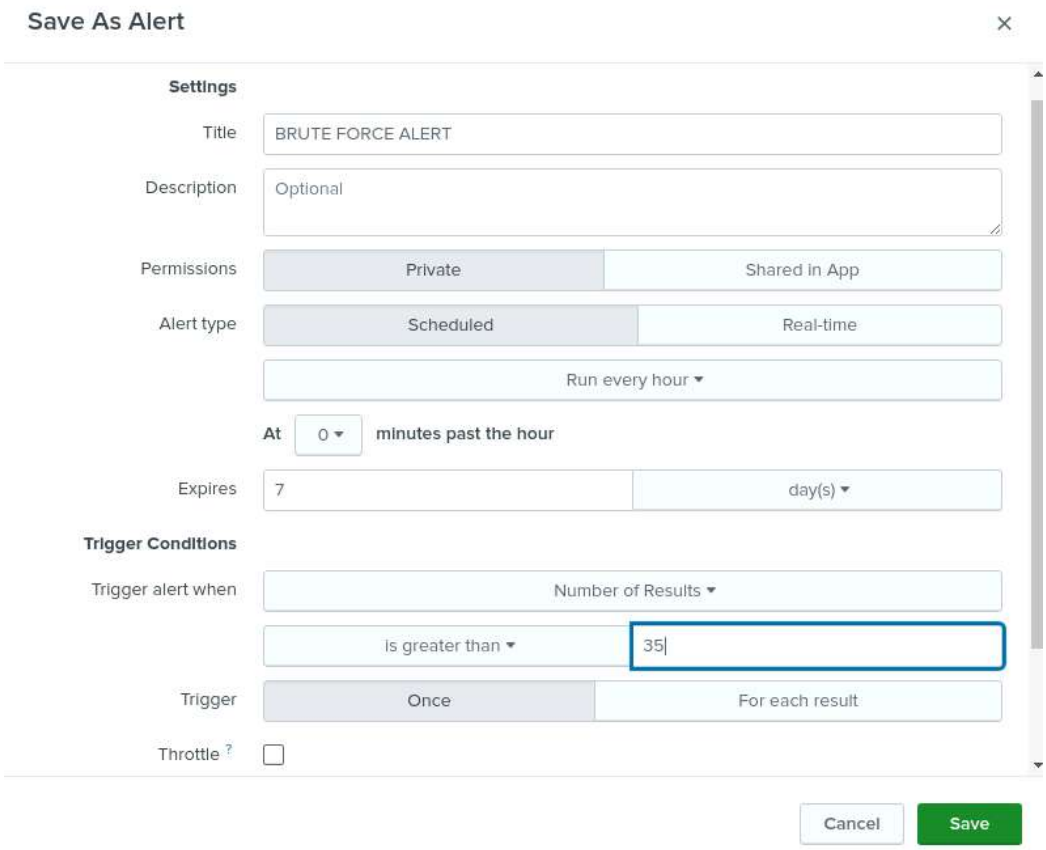
Step 3: Drawing the (Base)line

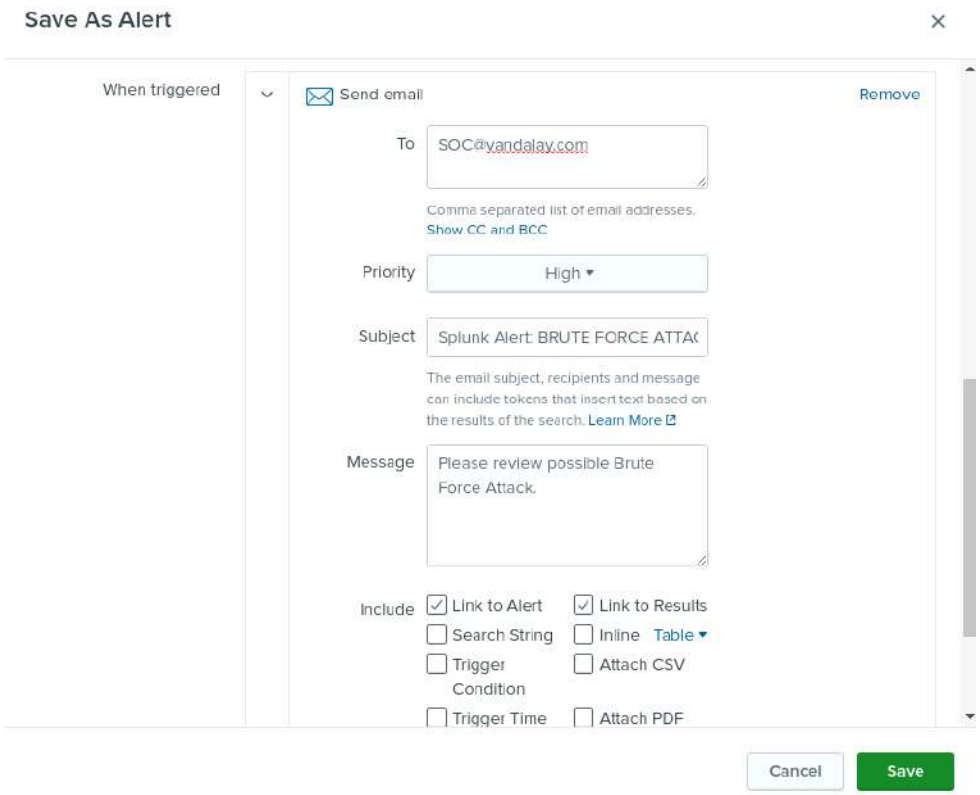
Background: A Vandaly server is also experiencing brute force attacks into their administrator account. Management would like you to set up monitoring to notify the SOC team if a brute force attack occurs again.

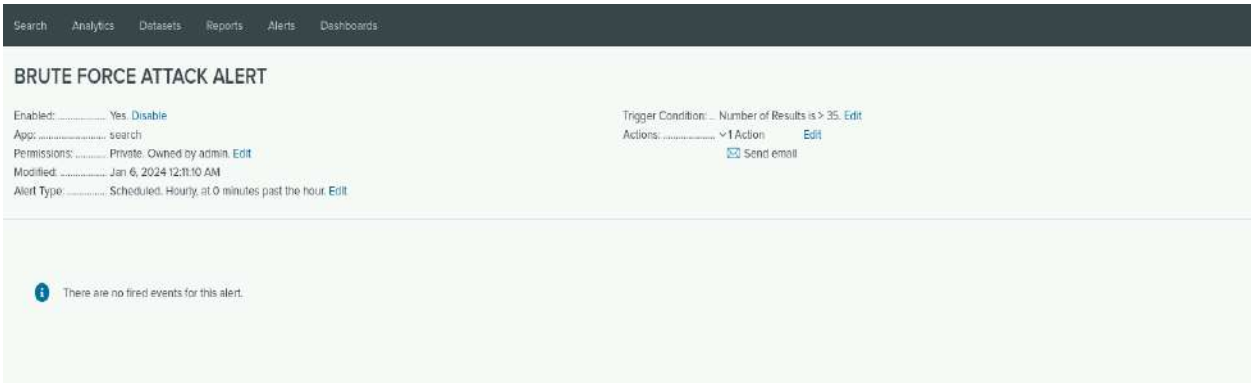
Your Task: Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring. To do so, complete the following steps:

1. Upload the following administrator login logs:
    - Admin LoginsLinks to an external site.
2. Answer the following in the M19 Submission File:
    - **(1)** When did the brute force attack occur? 2020-02-21 between 8:00 AM to 2:00 PM

    - **(2)** Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring. Baseline is 23; Threshold is 35
    - **(3)** 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
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every hour
At
0
minutes past the hour
Expires
7
day(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
35
Trigger
Once
For each result
Throttle
Cancel
Save


Save As Alert
When triggered
Send email
Remove
To
SOC@vandalay.com
Comma separated list of email addresses.
Show CC and BCC
Priority
High
Subject
Splunk Alert: BRUTE FORCE ATTAC
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More
Message
Please review possible Brute Force Attack.
Include
Link to Alert
Link to Results
Search String
Inline
Table
Trigger Condition
Attach CSV
Trigger Time
Attach PDF
Cancel
Save


Search
Analytics
Datasets
Reports
Alerts
Dashboards
BRUTE FORCE ATTACK ALERT
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Jan 6, 2024 12:11:10 AM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit
Trigger Condition: Number of Results is > 35. Edit
Actions: 1 Action Edit
Send email
There are no fired events for this alert.