

Splunk: Analyzing Impact, vulnerability and drawing Baselines for alerts

Task 1 Analyzing the Impact of the DDOS Attack

Task 2 Are We Vulnerable?

Task 3 Drawing the Baseline

Let's go Splunking!

Scenario 1

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

1. 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.
2. You are tasked with developing searches, custom reports and alerts to monitor Vandalay's security environment in order to protect them from future attacks.

Your Objective

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

Task 1: Analyzing the Impact of the DDOS Attack

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 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.

Task: Create a report to determine the impact that the DDOS attack had on download and upload speed. Additionally, create an additional field to calculate the ratio of the upload speed to the download speed.

1. Upload: Upload the file of the system speeds around the time of the attack.

The screenshot shows the 'Add Data' wizard in Splunk Enterprise. The progress bar at the top indicates the process is complete, with steps: Select Source, Set Source Type, Input Settings, Review, and Done. A green checkmark and the message 'File has been uploaded successfully.' are displayed. Below the message, there are several action buttons: 'Start Searching' (highlighted in green), 'Extract Fields', 'Add More Data', 'Download Apps', and 'Build Dashboards'. Each button has a brief description and a link to learn more.

Add Data | Select Source | Set Source Type | Input Settings | Review | Done | < Back | Next >

✓ **File has been uploaded successfully.**
Configure your inputs by going to Settings > [Data Inputs](#)

- Start Searching** | Search your data now or see [examples and tutorials](#).
- Extract Fields** | Create search-time field extractions. [Learn more about fields](#).
- Add More Data** | Add more data inputs now or see [examples and tutorials](#).
- Download Apps** | Apps help you do more with your data. [Learn more](#).
- Build Dashboards** | Visualize your searches. [Learn more](#).

2. Create Field: Create a field called SpeedRatio showing the ratio between the upload and download speeds.

The screenshot shows the Splunk search results page. The search bar contains the query: `source="server_speedtest.csv" host="speedtestserver" sourcetype="speedtest" | eval SpeedRatio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS'`. The results show 23 events. A visualization of the data is displayed as a bar chart. Below the chart, a table lists the events. The table has columns for Time and Event. The first event is from 2/24/20 8:30:00.000 PM, and the second is from 2/24/20 6:30:00.000 PM. Both events show a SpeedRatio value of 0.2089 and 0.2026 respectively. The table also shows the host and source for each event.

source="server_speedtest.csv" host="speedtestserver" sourcetype="speedtest" | eval SpeedRatio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' | All time

✓ 23 events (before 6/13/22 11:55:02.000 PM) No Event Sampling

Events (23) | Patterns | Statistics | Visualization

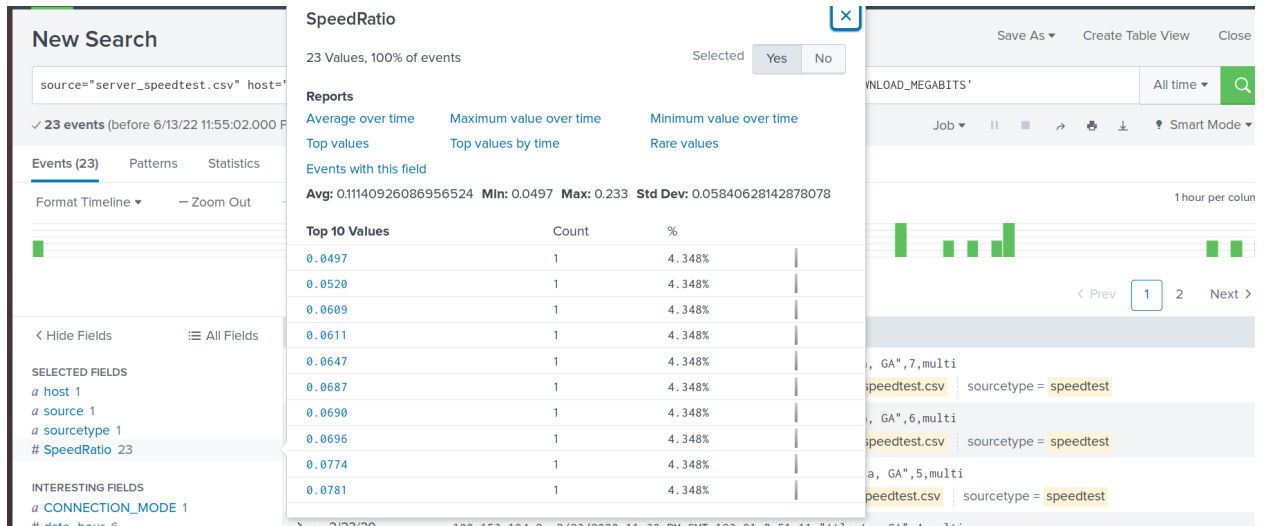
Format Timeline | Zoom Out | Zoom to Selection | Deselect | 1 hour per column

List | Format | 20 Per Page

i	Time	Event
>	2/24/20 8:30:00.000 PM	198.153.194.2,2/24/2020 8:30 PM,GMT,126.91,26.51,14,"Atlanta, GA",7,multi SpeedRatio = 0.2089 host = speedtestserver source = server_speedtest.csv sourcetype = speedtest
>	2/24/20 6:30:00.000 PM	198.153.194.2,2/24/2020 6:30 PM,GMT,125.91,25.51,13,"Atlanta, GA",6,multi SpeedRatio = 0.2026 host = speedtestserver source = server_speedtest.csv sourcetype = speedtest

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
SpeedRatio 23

INTERESTING FIELDS



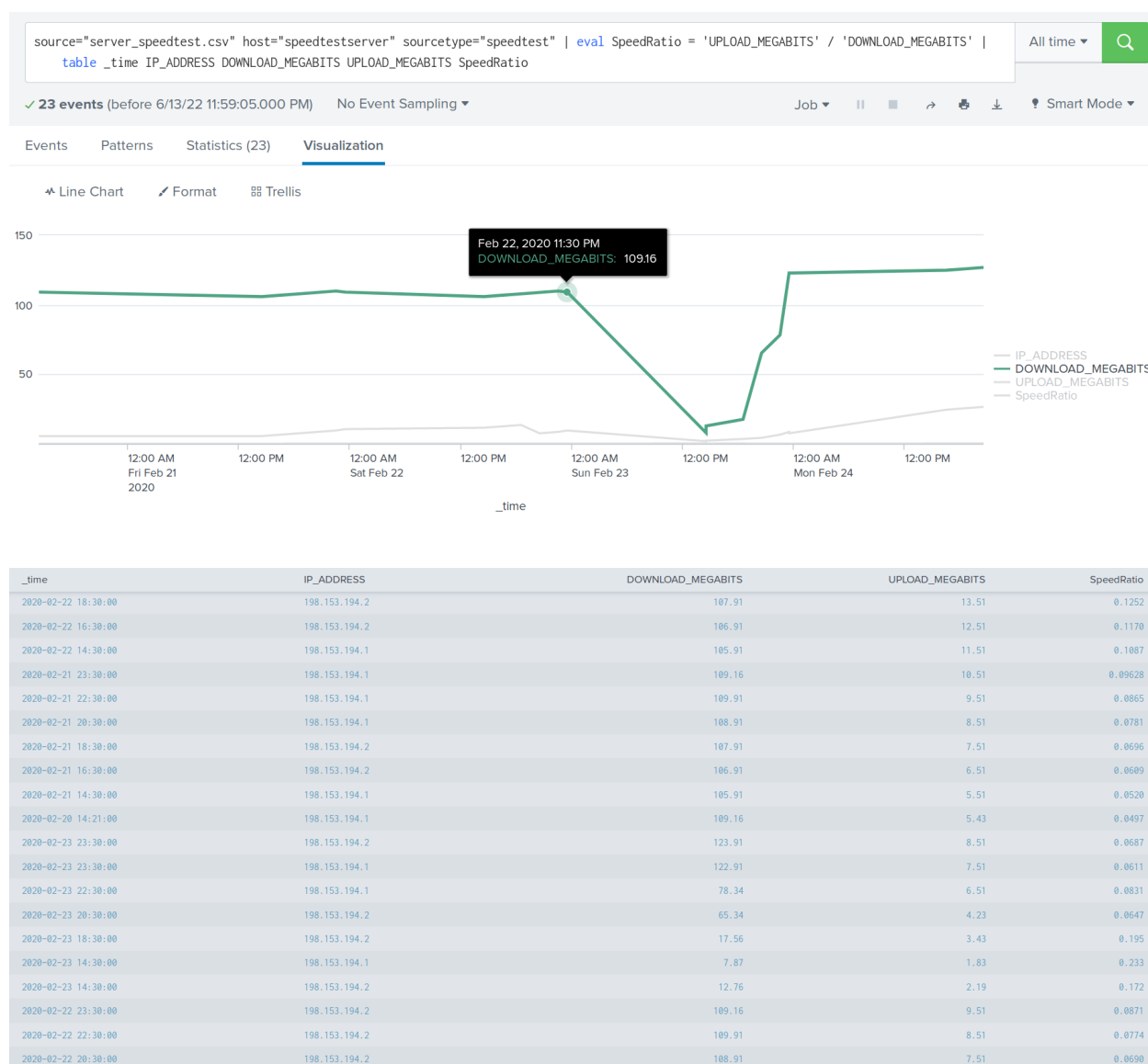
3. Create Statistic Report: Create a table displaying the following fields:

- Time
- IP_ADDRESS
- DOWNLOAD_MEGABITS
- UPLOAD_MEGABITS
- Ratio

The screenshot displays the Splunk interface with a search for `source="server_speedtest.csv" host="speedtestserver" sourcetype="speedtest" | eval SpeedRatio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS SpeedRatio`. The search results show 23 events. A table visualization is open, displaying the following data:

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	SpeedRatio
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	0.1252
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865

4. Use visualizations



5. Conclusions based on the report created:

:

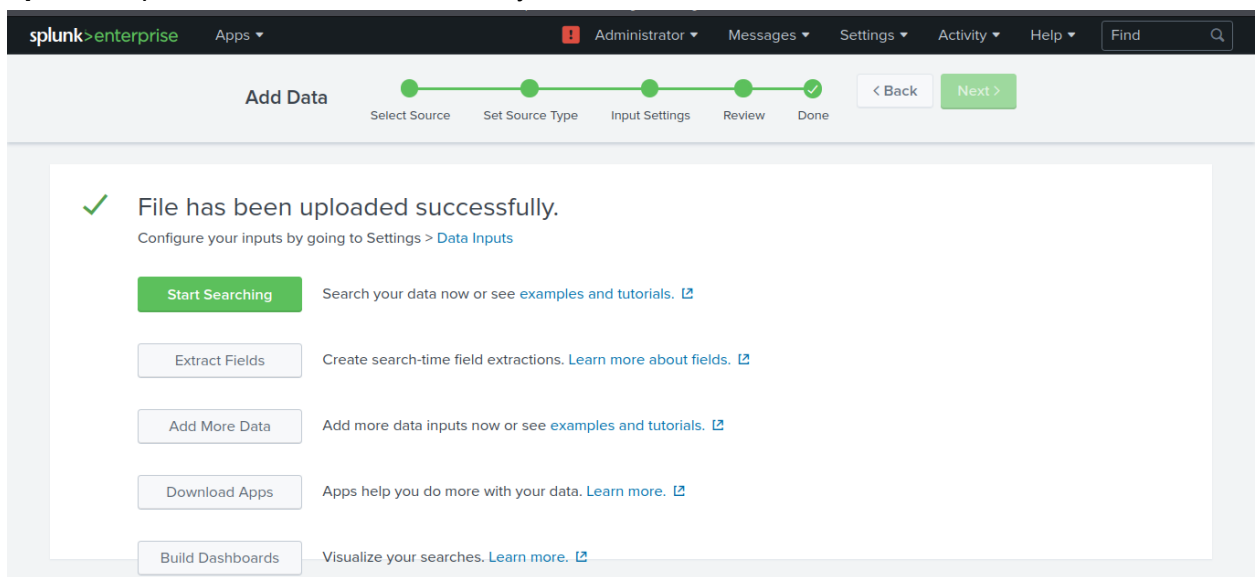
- The attack began on February 22, 2020 at 11:30 pm. The lowest speed was reached on February 23, 2020 at 02:30 pm. The full recovery was restored on February 23 at 11:30 pm.
- the systems needed 24 hours to recover

Task 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.

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.

1. Upload: Upload the Nessus vulnerability scan.



2. **Vulnerabilities Count:** Create a report that shows the count of critical vulnerabilities from the customer database server.

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A 'Search & Reporting' button is on the right. The main content area displays a report titled 'Dataserver Vulnerabilities count'. It has buttons for 'Edit', 'More Info', and 'Add to Dashboard'. Below the title, it says 'All time' and '✓ 49 events (before 1/10/22 9:56:12.000 PM)'. There are icons for job status, refresh, and other actions. A pagination bar shows '20 per page' and '1' of 3 pages. The report content is a table with columns 'i', 'Time', and 'Event'. The first row shows a search result for a vulnerability event on 2/20/20 at 5:33:01.000 PM. The event details include start and end times, destination DNS, host, MAC address, IP address, OS (Cisco Router), destination port and protocol (827/tcp), severity ID (4), and a signature. The signature is a long string of text including 'splunk-ta-nessus-end-of-event', a timestamp, host information, and a list of vulnerabilities. The report ends with 'os report' and a link to 'Show all 13 lines'.

3. **Alert:** Build an alert that monitors every day for critical vulnerabilities. Emailed alert to soc@vandalay.com

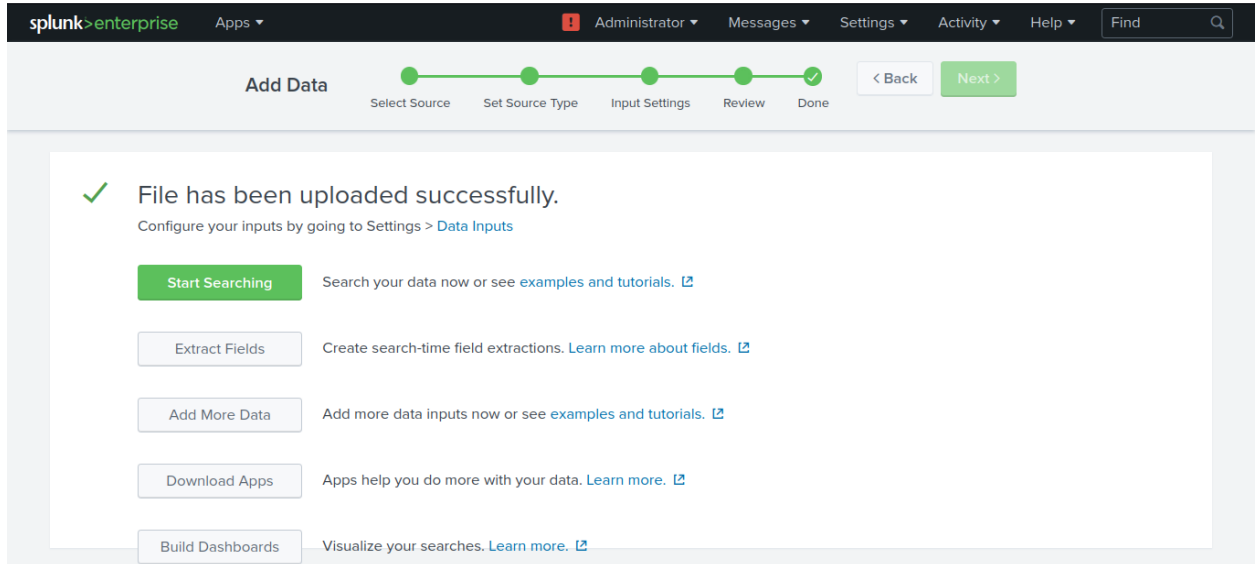
The screenshot shows the Splunk Enterprise interface for an alert configuration. The top navigation bar is the same as in the previous screenshot. The main content area displays an alert configuration titled 'Dataserver Critical Vulnerabilities discovered'. It has an 'Edit' button. The configuration details are as follows: Enabled: Yes, Disable; App: search; Permissions: Private, Owned by andres; Modified: Jan 10, 2022 10:03:06 PM; Alert Type: Scheduled, Daily, at 0:00. The Trigger Condition is 'Number of Results is > 0'. The Actions are '1 Action' and 'Send email'. Below the configuration details, there is a message: 'There are no fired events for this alert.'

Task 3: Drawing the Baseline

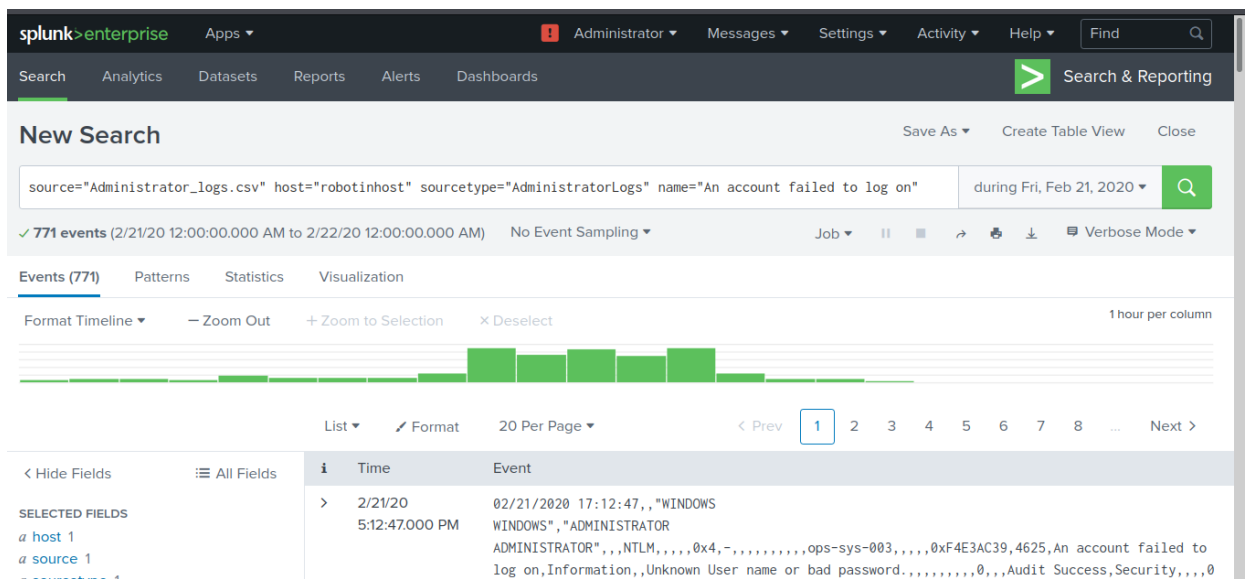
Background: A Vandalay server is also experiencing brute force attacks into their administrator account. Management would like you to set up monitoring to notify the SOC team if a brute force attack occurs again.

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.

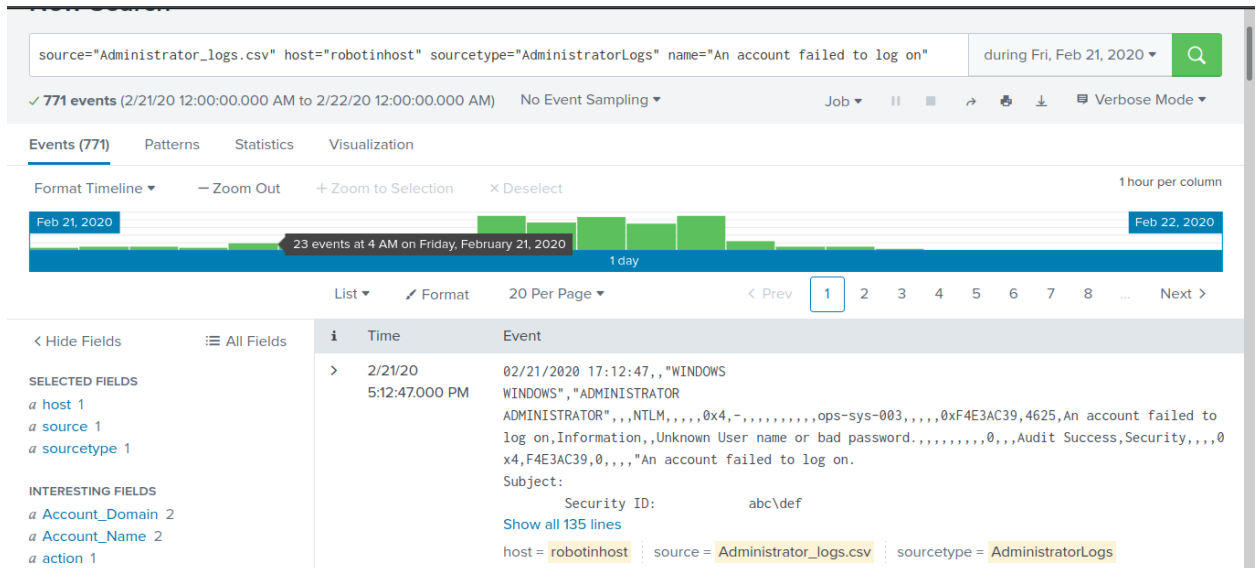
1. **Upload:** Upload the administrator login logs.



2. **Conclusion:** The brute force attack occurs On February 21 from 9:00 AM to 1:00 PM



3. **Baseline and Threshold:** The average failed attempt is under 23 for an hour. The range 8 to 20 failed attempts for an hour. The baseline is 20 and the threshold will be set at 23.



- Alert:** Create an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Brute Force Attack alert

The amount of failed login attempts has reach the count of 23 in an hour

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by andres. [Edit](#)

Modified: Jan 10, 2022 9:06:03 PM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 23. [Edit](#)

Actions: 1 Action [Edit](#)

[Send email](#)

i There are no fired events for this alert.