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

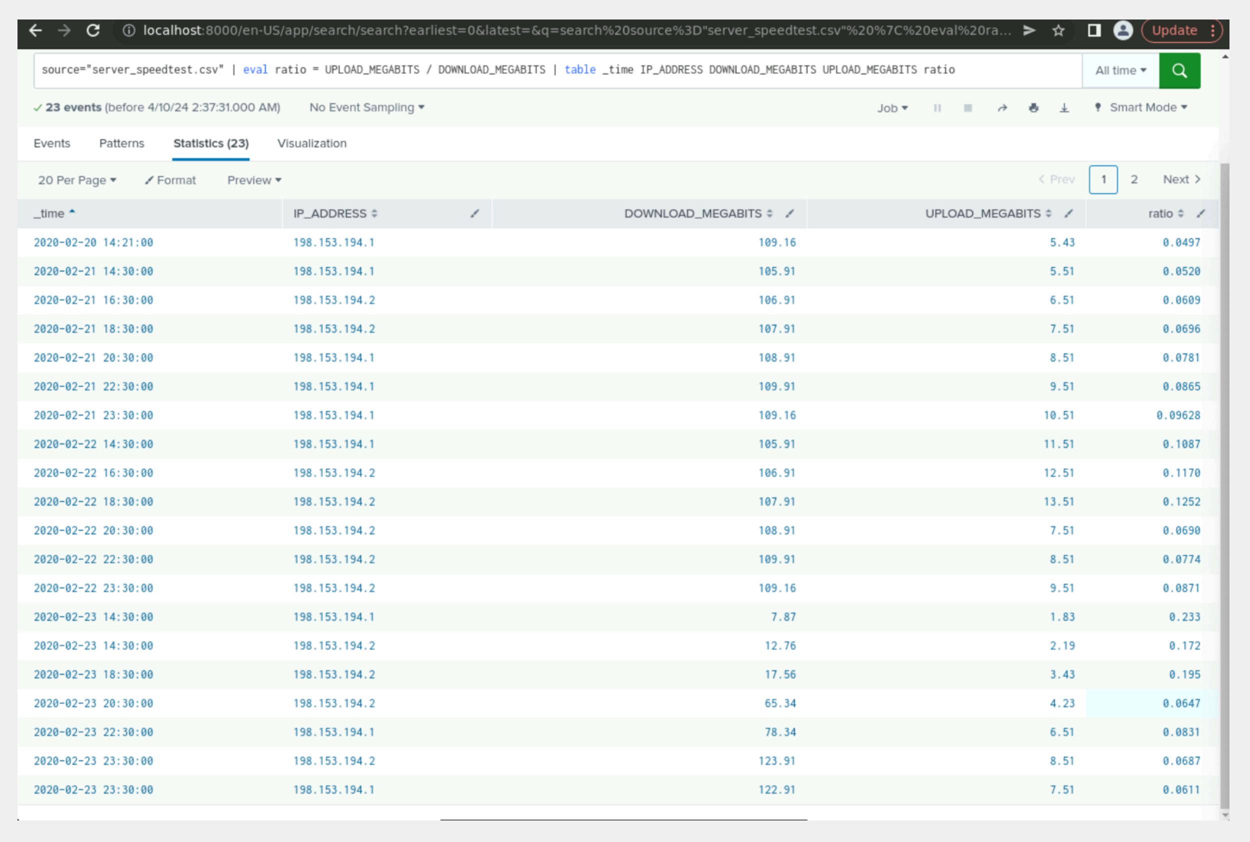
1. Based on the report you created, what is the approximate date and time of the attack?

```
2020-02-23 14:30
```

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

```
8 hours.
```

Provide a screenshot of your report:


localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search%20source%3D"server_speedtest.csv"%20%7C%20eval%20ra...
Update

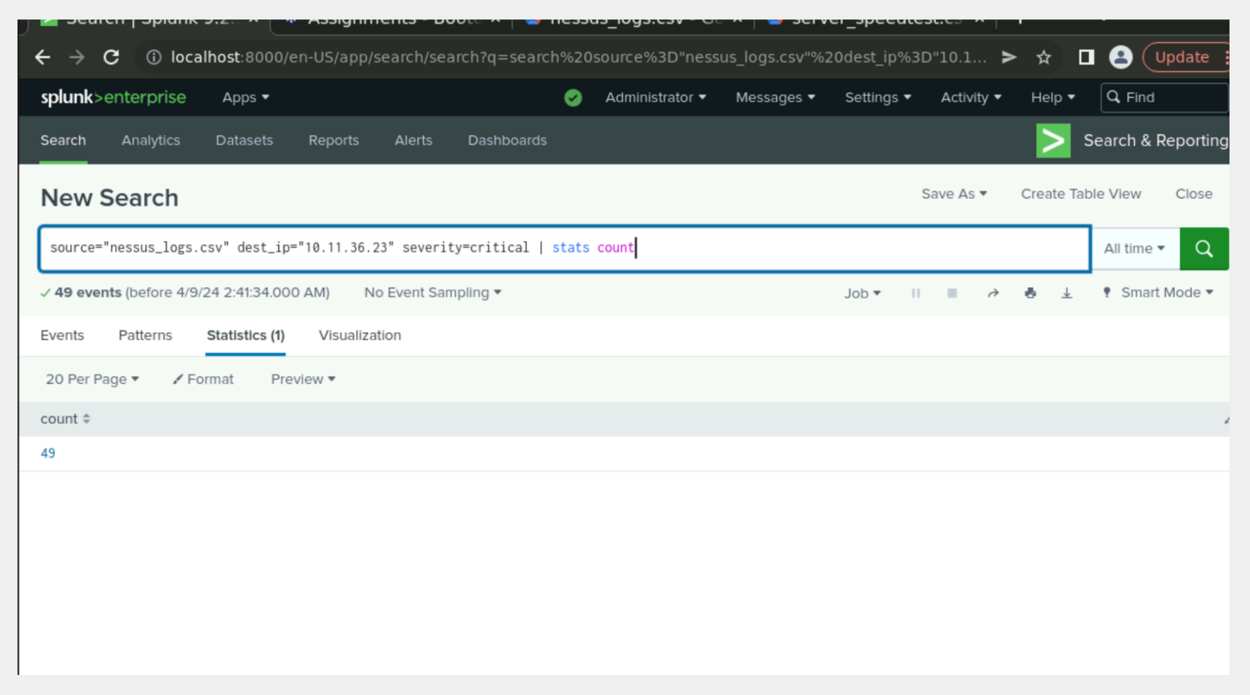
```
source="server_speedtest.csv" | eval ratio = UPLOAD_MEGABITS / DOWNLOAD_MEGABITS | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio
```

All time
✓ 23 events (before 4/10/24 2:37:31.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (23)
Visualization
20 Per Page
Format
Preview
Prev
1
2
Next

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	0.0497
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	0.0520
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	0.0609
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	0.0696
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	0.0781
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	0.1252
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0690
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611

Step 2: Are We Vulnerable?

Provide a screenshot of your report:

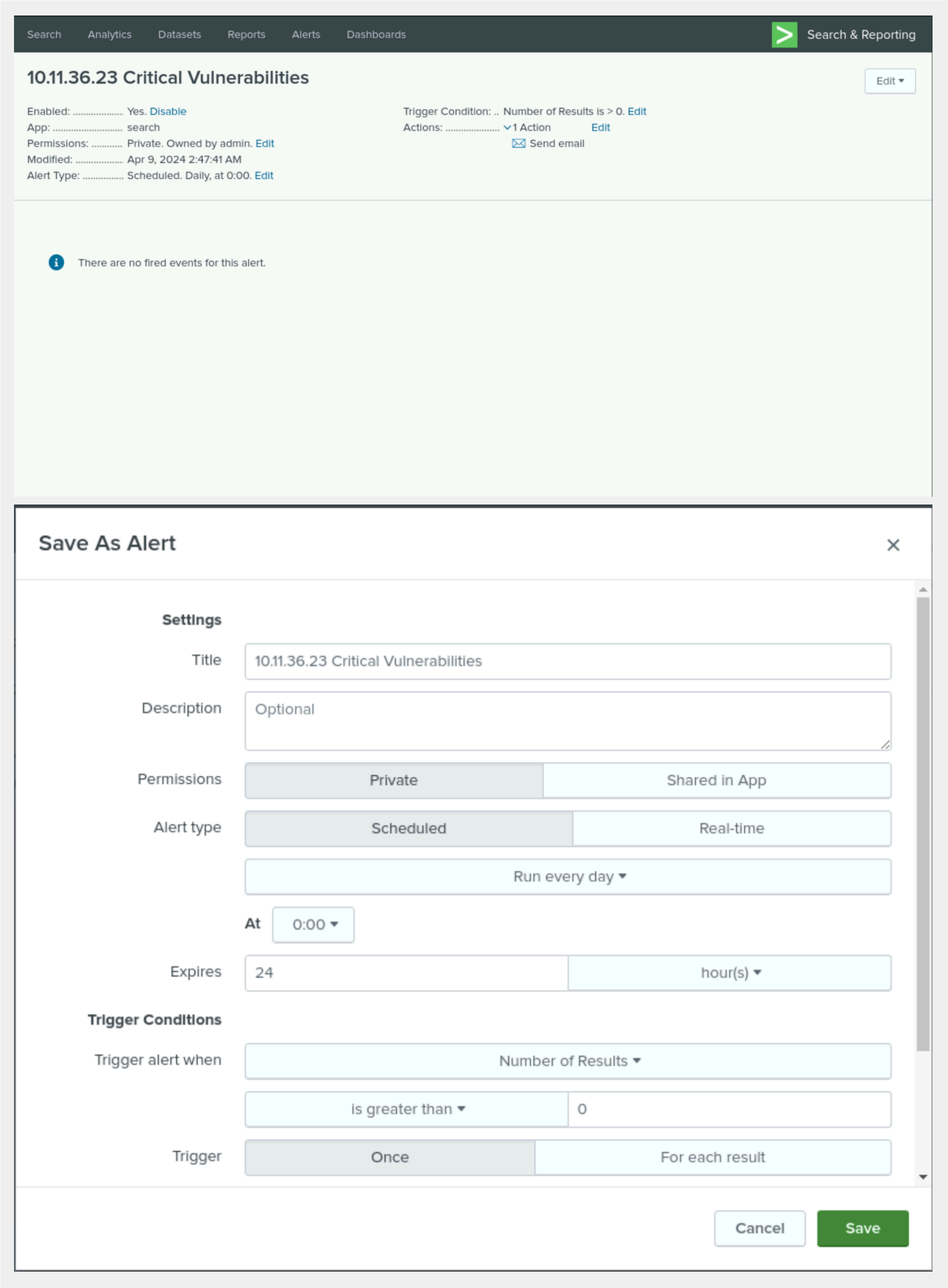


```
source="nessus_logs.csv" dest_ip="10.11.36.23" severity=critical | stats count
```

✓ 49 events (before 4/9/24 2:41:34.000 AM)

count
49

Provide a screenshot showing that the alert has been created:



10.11.36.23 Critical Vulnerabilities

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Apr 9, 2024 2:47:41 AM
Alert Type: .... Scheduled. Daily, at 0:00. Edit

Trigger Condition: .. Number of Results is > 0. Edit
Actions: .... ⌄1 Action Edit
✉ Send email

ℹ There are no fired events for this alert.

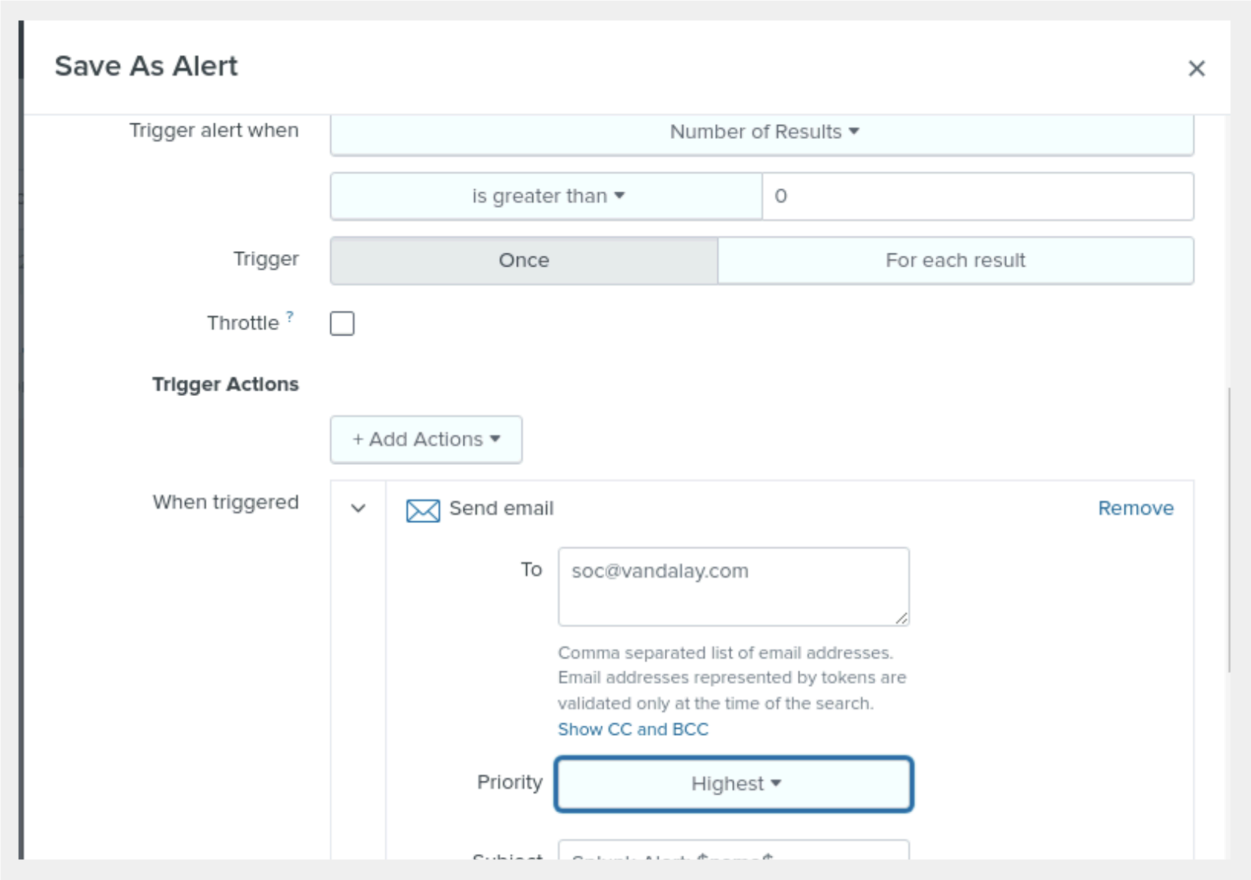
Save As Alert

Settings

Title	10.11.36.23 Critical Vulnerabilities	
Description	Optional	
Permissions	Private	Shared in App
Alert type	Scheduled	Real-time
	Run every day ▾	
	At 0:00 ▾	
Expires	24	hour(s) ▾

Trigger Conditions

Trigger alert when	Number of Results ▾	
	is greater than ▾	0
Trigger	Once	For each result



Save As Alert ×

Trigger alert when: Number of Results ▾

is greater than ▾ 0

Trigger: Once | For each result

Throttle ? □

Trigger Actions

+ Add Actions ▾

When triggered: Send email — Remove

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: Highest ▾

Subject: Splunk Alert: $name$

Step 3: Drawing the (Base)line

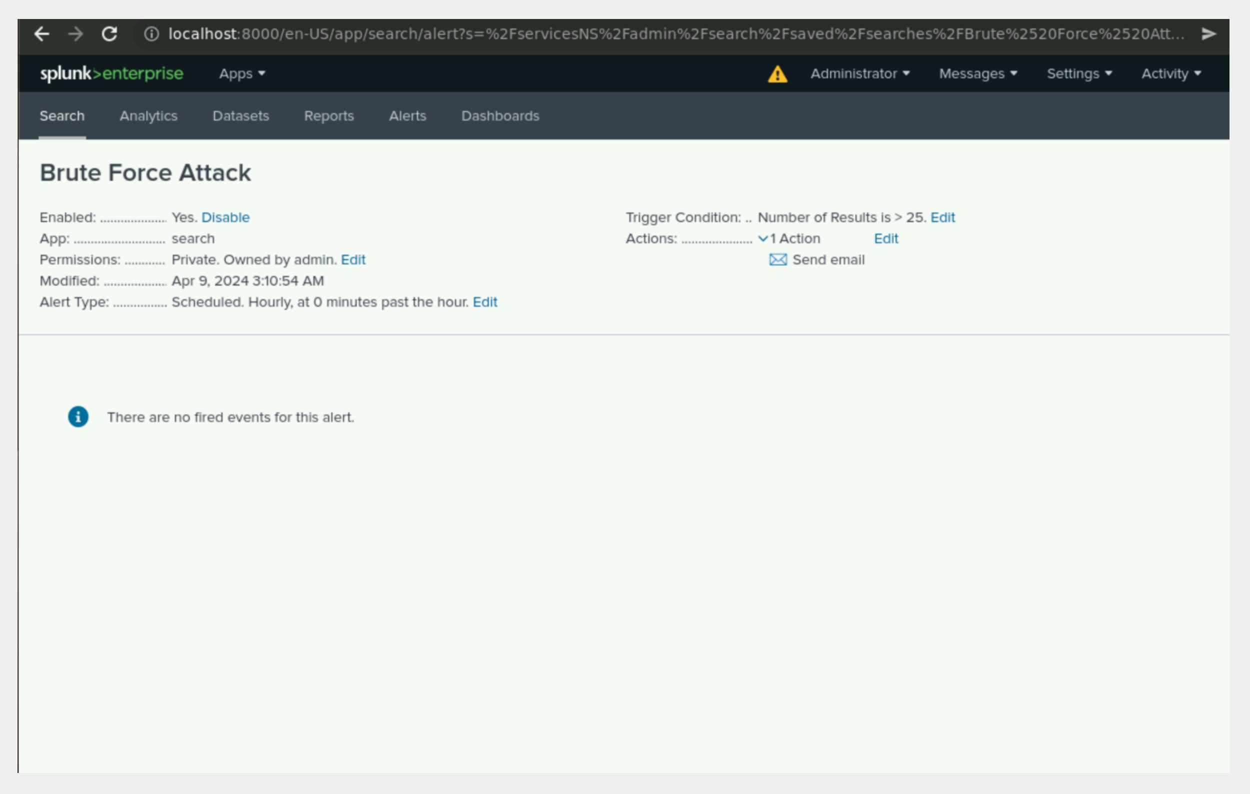
1. When did the brute force attack occur?

```
February 21, 2020 between 8AM and 2PM
```

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

```
Baseline is 5 to 25.  Threshold is higher than 25 in an hour.
```

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



localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FBrute%2520Force%2520Att...
splunk>enterprise
Apps ▾
Administrator ▾
Messages ▾
Settings ▾
Activity ▾
Search
Analytics
Datasets
Reports
Alerts
Dashboards

Brute Force Attack

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Apr 9, 2024 3:10:54 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 25. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.