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

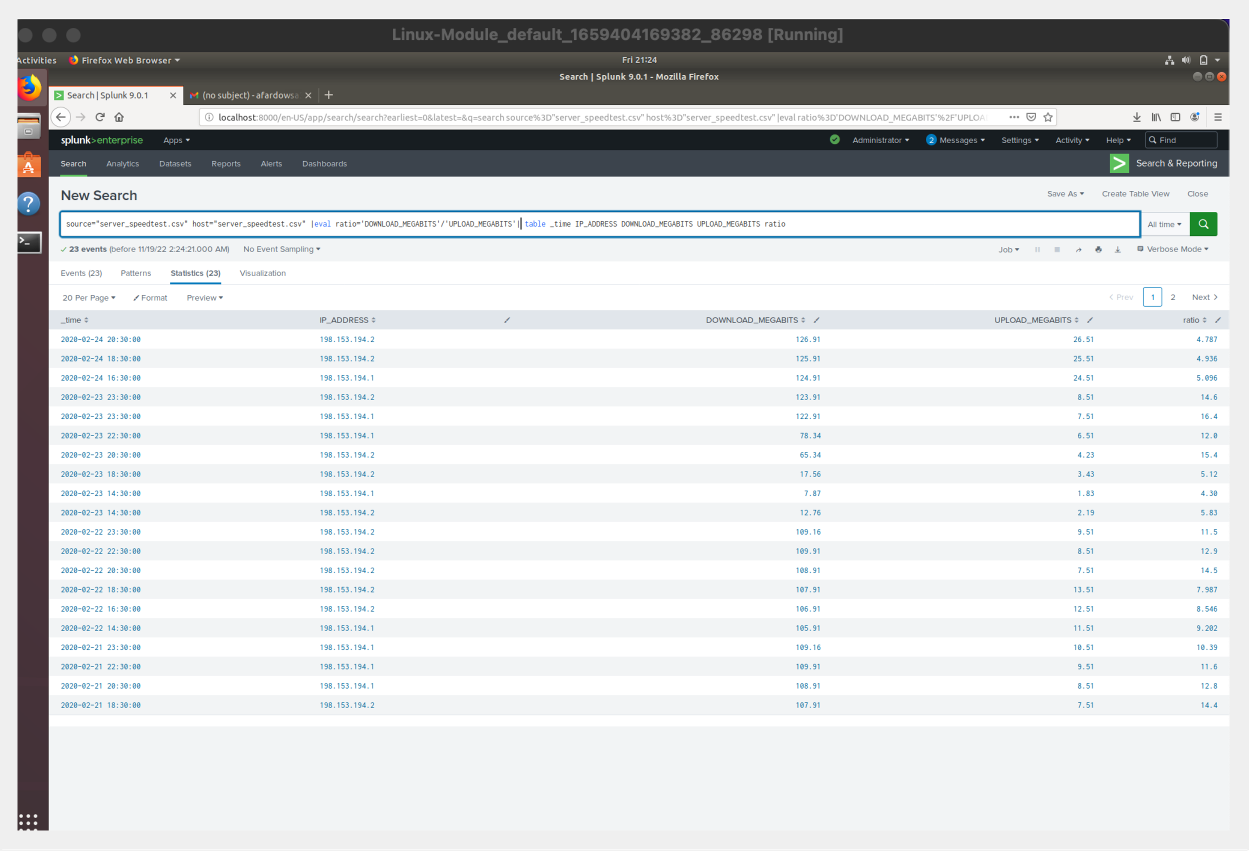
1. Based on the report you created, what is the approximate date and time of the attack?

```
02/23/20 at 2:20
```

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

```
8 hours from 02/23/2020 14:30:00 to 02/23/2020 22:30:00
```

Provide a screenshot of your report:



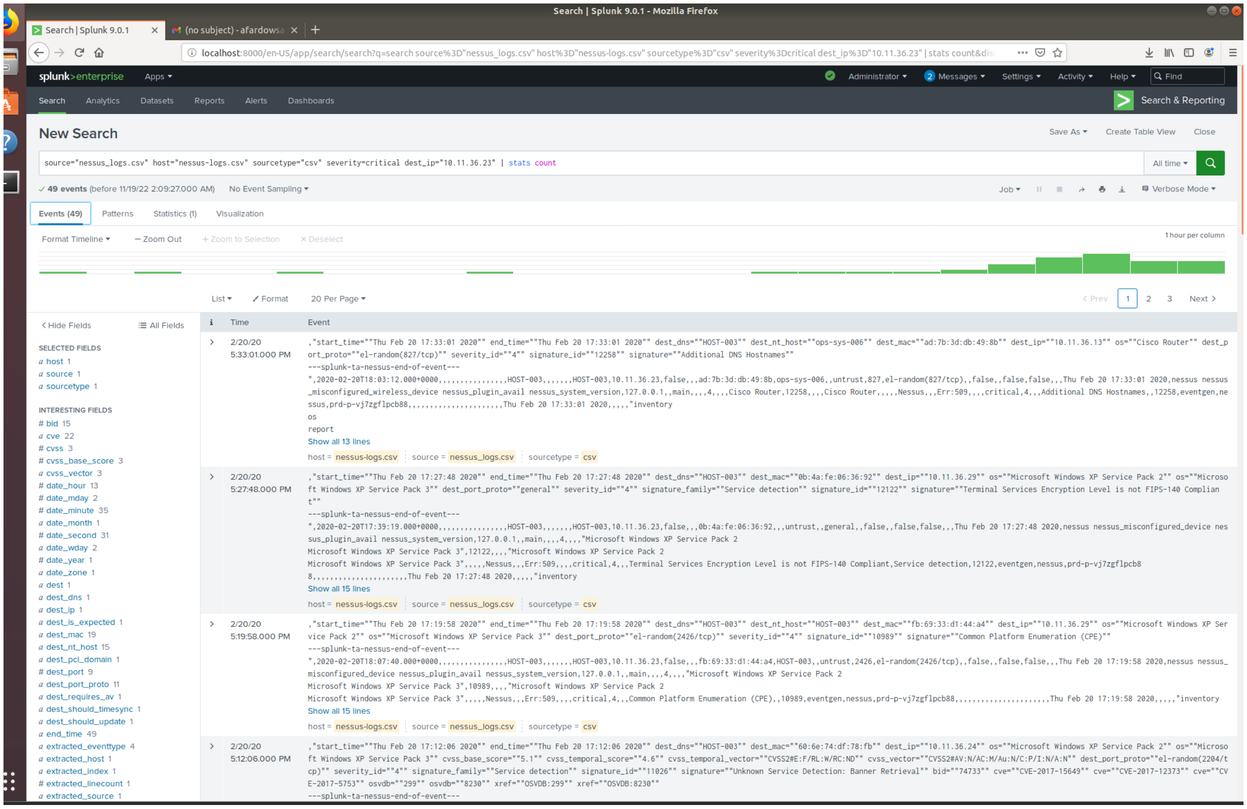
```
source="server_speedtest.csv" host="server_speedtest.csv" |eval ratio='DOWNLOAD_MEGABITS'/'UPLOAD_MEGABITS'| table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio
```

✓ 23 events (before 11/19/22 2:24:21.000 AM) No Event Sampling

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	4.787
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	4.936
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	5.096
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	14.6
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	16.4
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	12.0
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	15.4
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	5.12
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	4.30
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	5.83
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	11.5
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	12.9
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	14.5
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	7.987
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	8.546
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	9.202
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	10.39
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	11.6
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	12.8
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	14.4

Step 2: Are We Vulnerable?

Provide a screenshot of your report:



```
source="nessus_logs.csv" host="nessus-logs.csv" sourcetype="csv" severity=critical dest_ip="10.11.36.23" | stats count
```

✓ 49 events (before 11/19/22 2:09:27.000 AM) No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bid 15
a cve 22
# cvss 3
# cvss_base_score 3
a cvss_vector 3
# date_hour 13
# date_mday 2
# date_minute 35
a date_month 1
# date_second 31
a date_wday 2
# date_year 1
a date_zone 1
a dest 1
a dest_dns 1
a dest_ip 1
a dest_is_expected 1
a dest_mac 19
a dest_nt_host 15
a dest_pci_domain 1
# dest_port 9
a dest_port_proto 11
a dest_requires_av 1
a dest_should_timesync 1
a dest_should_update 1
a end_time 49
a extracted_eventtype 4
a extracted_host 1
a extracted_index 1
# extracted_linecount 1
a extracted_source 1

2/20/20 5:33:01.000 PM

```
,"start_time=""Thu Feb 20 17:33:01 2020"" end_time=""Thu Feb 20 17:33:01 2020"" dest_dns=""HOST-003"" dest_nt_host=""ops-sys-006"" dest_mac=""ad:7b:3d:db:49:8b"" dest_ip=""10.11.36.13"" os=""Cisco Router"" dest_p
ort_proto=""el-random(827/tcp)"" severity_id=""4"" signature_id=""12258"" signature=""Additional DNS Hostnames""
---splunk-ta-nessus-end-of-event---
",2020-02-20T18:03:12.000+0000,,,,,,,,,,,,,,,HOST-003,,,,,,HOST-003,10.11.36.23,false,,,ad:7b:3d:db:49:8b,ops-sys-006,,untrust,827,el-random(827/tcp),,false,,false,false,,,Thu Feb 20 17:33:01 2020,nessus nessus
_misconfigured_wireless_device nessus_plugin_avail nessus_system_version,127.0.0.1,,main,,,,4,,,,Cisco Router,12258,,,,Cisco Router,,,,,Nessus,,,Err:509,,,,critical,4,,,Additional DNS Hostnames,,12258,eventgen,ne
ssus,prd-p-vj7zgflpcb88,,,,,,,,,,,,,,,,,,,,,Thu Feb 20 17:33:01 2020,,,,,"inventory
os
report
```

Show all 13 lines
host = nessus-logs.csv | source = nessus_logs.csv | sourcetype = csv

2/20/20 5:27:48.000 PM

```
,"start_time=""Thu Feb 20 17:27:48 2020"" end_time=""Thu Feb 20 17:27:48 2020"" dest_dns=""HOST-003"" dest_mac=""0b:4a:fe:06:36:92"" dest_ip=""10.11.36.29"" os=""Microsoft Windows XP Service Pack 2"" os=""Microso
ft Windows XP Service Pack 3"" dest_port_proto=""general"" severity_id=""4"" signature_family=""Service detection"" signature_id=""12122"" signature=""Terminal Services Encryption Level is not FIPS-140 Complian
t""
---splunk-ta-nessus-end-of-event---
",2020-02-20T17:39:19.000+0000,,,,,,,,,,,,,,,HOST-003,,,,,,HOST-003,10.11.36.23,false,,,0b:4a:fe:06:36:92,,,untrust,,general,,false,,false,false,,,Thu Feb 20 17:27:48 2020,nessus nessus_misconfigured_device nes
sus_plugin_avail nessus_system_version,127.0.0.1,,main,,,,4,,,,"Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3",12122,,,,"Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3",,,,,Nessus,,,Err:509,,,,critical,4,,,Terminal Services Encryption Level is not FIPS-140 Compliant,Service detection,12122,eventgen,nessus,prd-p-vj7zgflpcb8
8,,,,,,,,,,,,,,,,,,,,,Thu Feb 20 17:27:48 2020,,,,,"inventory
```

Show all 15 lines
host = nessus-logs.csv | source = nessus_logs.csv | sourcetype = csv

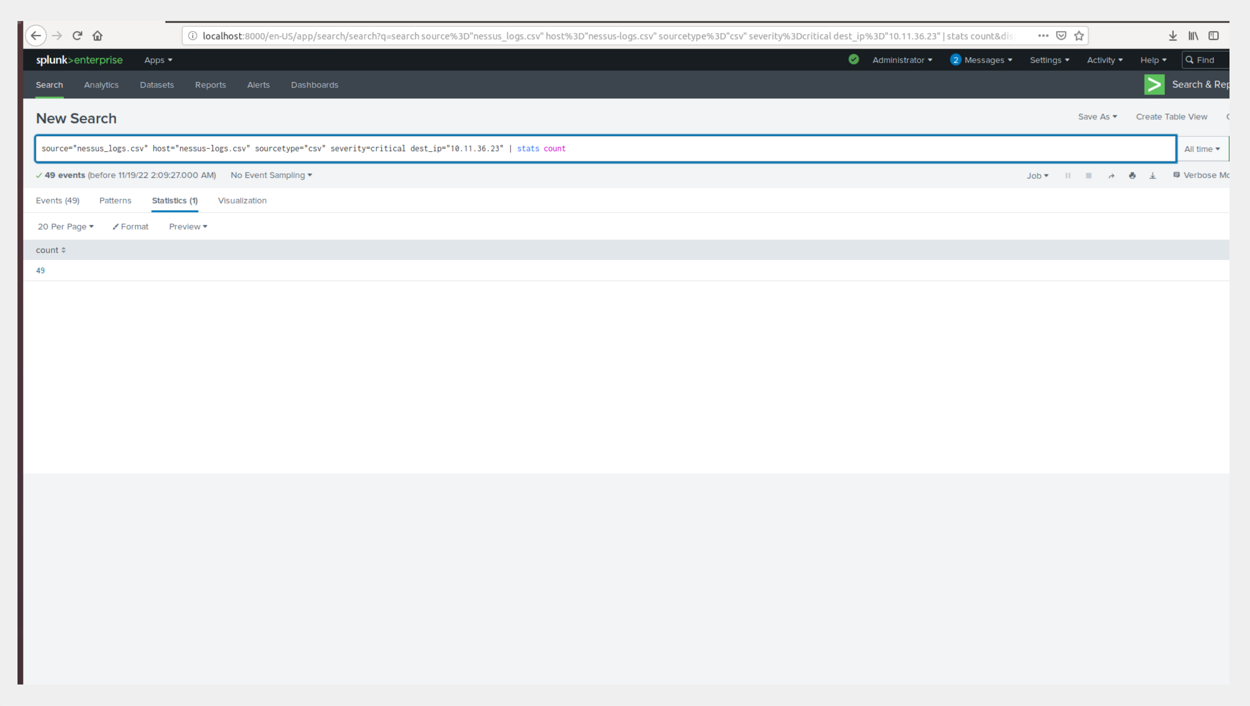
2/20/20 5:19:58.000 PM

```
,"start_time=""Thu Feb 20 17:19:58 2020"" end_time=""Thu Feb 20 17:19:58 2020"" dest_dns=""HOST-003"" dest_nt_host=""HOST-003"" dest_mac=""fb:69:33:d1:44:a4"" dest_ip=""10.11.36.29"" os=""Microsoft Windows XP Ser
vice Pack 2"" os=""Microsoft Windows XP Service Pack 3"" dest_port_proto=""el-random(2426/tcp)"" severity_id=""4"" signature_id=""10989"" signature=""Common Platform Enumeration (CPE)""
---splunk-ta-nessus-end-of-event---
",2020-02-20T18:07:40.000+0000,,,,,,,,,,,,,,,HOST-003,,,,,,HOST-003,10.11.36.23,false,,,fb:69:33:d1:44:a4,HOST-003,,untrust,2426,el-random(2426/tcp),,false,,false,false,,,Thu Feb 20 17:19:58 2020,nessus nessus_
misconfigured_device nessus_plugin_avail nessus_system_version,127.0.0.1,,main,,,,4,,,,"Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3",10989,,,,"Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3",,,,,Nessus,,,Err:509,,,,critical,4,,,Common Platform Enumeration (CPE),,10989,eventgen,nessus,prd-p-vj7zgflpcb88,,,,,,,,,,,,,,,,,,,,,Thu Feb 20 17:19:58 2020,,,,,"inventory
```

Show all 15 lines
host = nessus-logs.csv | source = nessus_logs.csv | sourcetype = csv

2/20/20 5:12:06.000 PM

```
,"start_time=""Thu Feb 20 17:12:06 2020"" end_time=""Thu Feb 20 17:12:06 2020"" dest_dns=""HOST-003"" dest_mac=""60:6e:74:df:78:fb"" dest_ip=""10.11.36.24"" os=""Microsoft Windows XP Service Pack 2"" os=""Microso
ft Windows XP Service Pack 3"" cvss_base_score=""5.1"" cvss_temporal_score=""4.6"" cvss_temporal_vector=""CVSS2#E:F/RL:W/RC:ND"" cvss_vector=""CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N"" dest_port_proto=""el-random(2204/t
cp)"" severity_id=""4"" signature_family=""Service detection"" signature_id=""11026"" signature=""Unknown Service Detection: Banner Retrieval"" bid=""74733"" cve=""CVE-2017-15649"" cve=""CVE-2017-12373"" cve=""CV
E-2017-5753"" osvdb=""299"" osvdb=""8230"" xref=""OSVDB:299"" xref=""OSVDB:8230""
---splunk-ta-nessus-end-of-event---
```

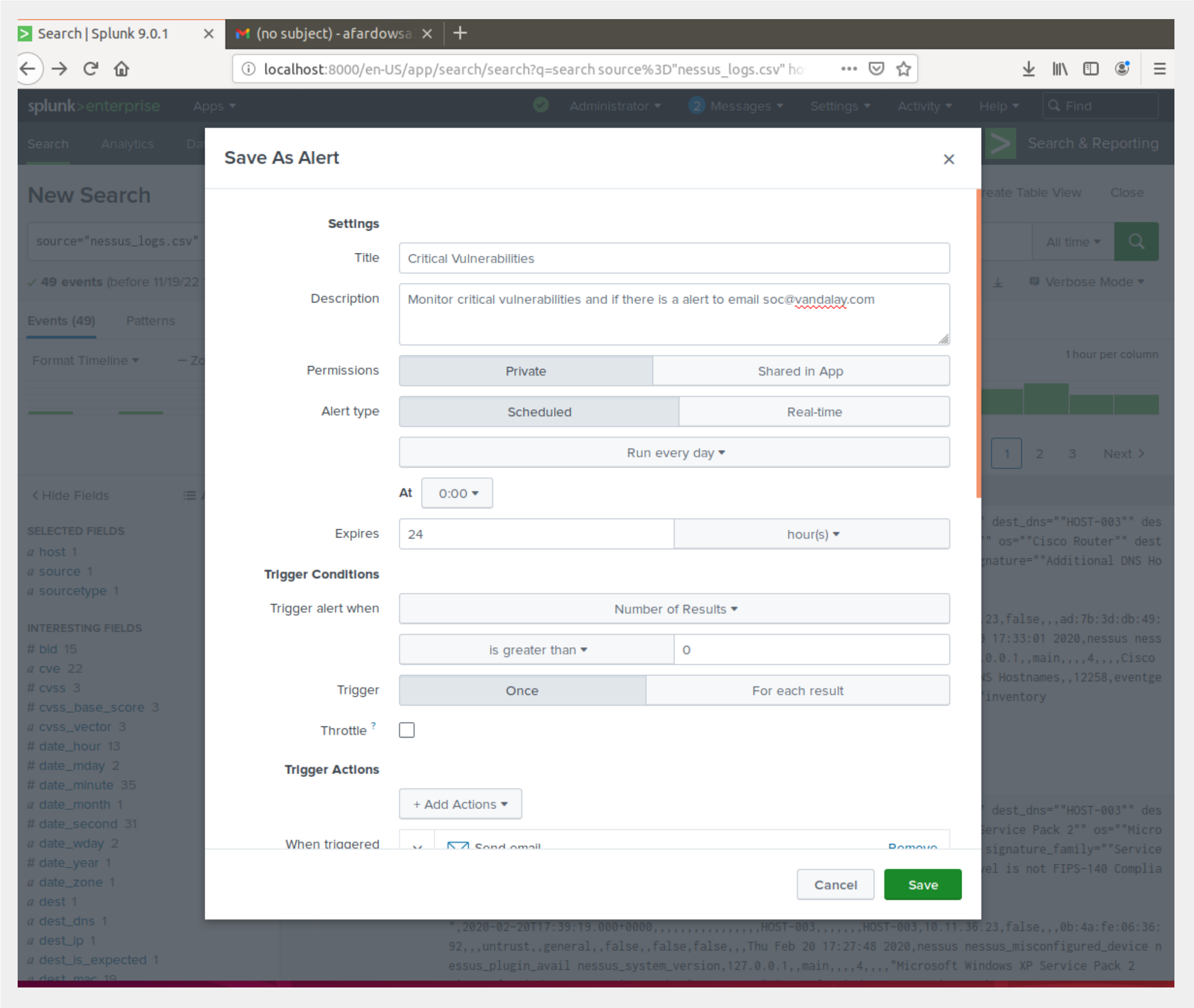


```
source="nessus_logs.csv" host="nessus-logs.csv" sourcetype="csv" severity=critical dest_ip="10.11.36.23" | stats count
```

✓ 49 events (before 11/19/22 2:09:27.000 AM) No Event Sampling

count
49

Provide a screenshot showing that the alert has been created:



Save As Alert

Settings

Title: Critical Vulnerabilities

Description: Monitor critical vulnerabilities and if there is a alert to email soc@vandalay.com

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

Throttle ? □

Trigger Actions

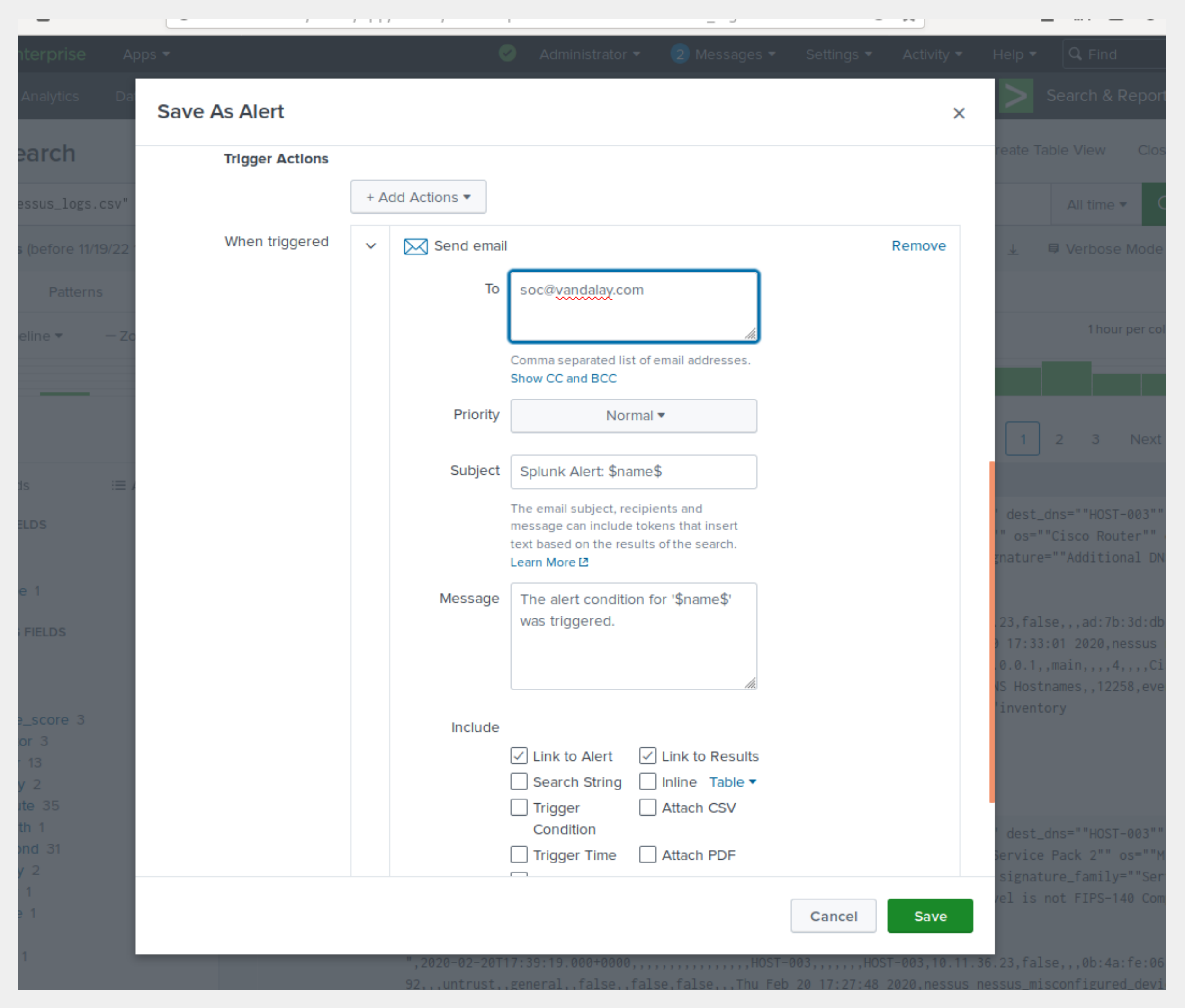
+ Add Actions

When triggered: Send email Remove

```
source="nessus_logs.csv"
✓ 49 events (before 11/19/22
```

```
a host 1
a source 1
a sourcetype 1
# bid 15
a cve 22
# cvss 3
# cvss_base_score 3
a cvss_vector 3
# date_hour 13
# date_mday 2
# date_minute 35
a date_month 1
# date_second 31
a date_wday 2
# date_year 1
# date_zone 1
a dest 1
a dest_dns 1
a dest_ip 1
a dest_is_expected 1
```

```
" dest_dns=""HOST-003"" des
" os=""Cisco Router"" dest
nature=""Additional DNS Ho
.23,false,,,ad:7b:3d:db:49:
17:33:01 2020,nessus ness
0.0.1,,main,,,,4,,,,Cisco
S Hostnames,,12258,eventge
inventory
" dest_dns=""HOST-003"" des
ervice Pack 2"" os=""Micro
signature_family=""Service
el is not FIPS-140 Complia
",2020-02-20T17:39:19.000+0000,,,,,,,,,,,,,,HOST-003,,,,,,HOST-003,10.11.36.23,false,,,0b:4a:fe:06:36:
92,,,untrust,,general,,false,,false,false,,,Thu Feb 20 17:27:48 2020,nessus nessus_misconfigured_device n
essus_plugin_avail nessus_system_version,127.0.0.1,,main,,,,4,,,,"Microsoft Windows XP Service Pack 2
```



Save As Alert

Trigger Actions

When triggered: Send email

To: soc@vandalay.com

Comma separated list of email addresses.
Show CC and BCC

Priority: Normal ▾

Subject: Splunk Alert: $name$

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 '$name$' was triggered.

Include

☑ Link to Alert ☑ Link to Results
☐ Search String ☐ Inline Table ▾
☐ Trigger Condition ☐ Attach CSV
☐ Trigger Time ☐ Attach PDF

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

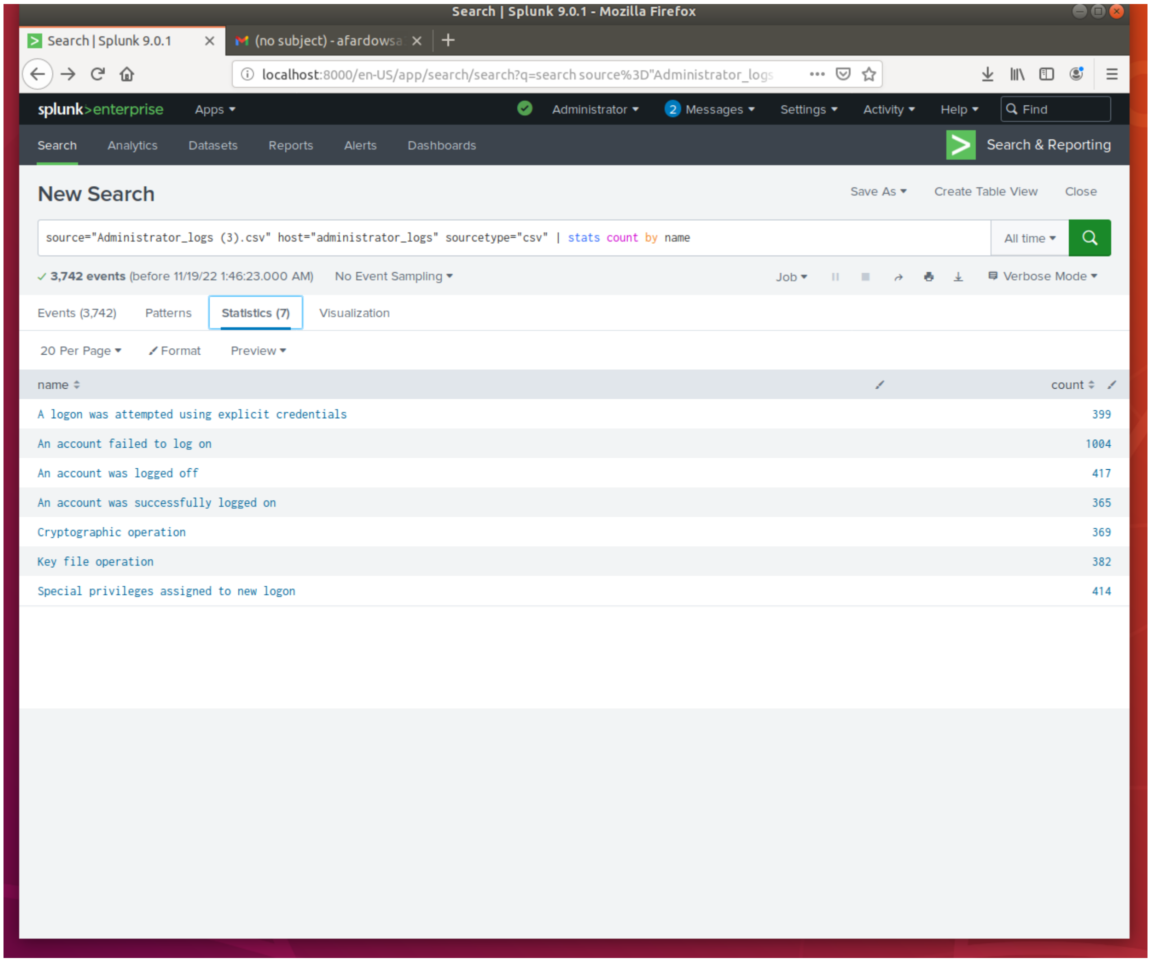
```
2/21/20 5:17:02
```

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

```
I put a baseline of more than 20 failed login attempts for every hour. More than 20 it’s will alert SOC@vandalay.com of a brute force attack.
```

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

4.

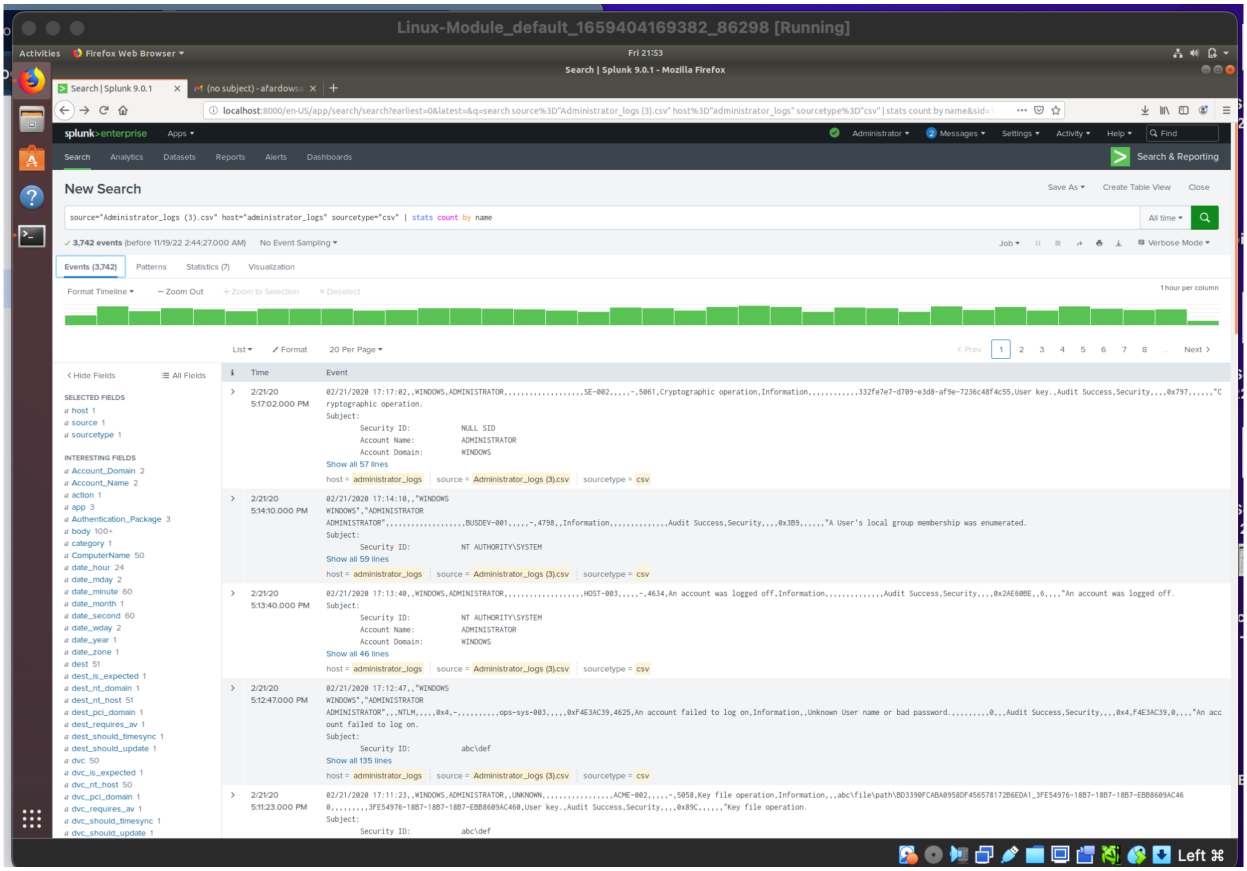


New Search

```
source="Administrator_logs (3).csv" host="administrator_logs" sourcetype="csv" | stats count by name
```

✓ 3,742 events (before 11/19/22 1:46:23.000 AM)

name	count
A logon was attempted using explicit credentials	399
An account failed to log on	1004
An account was logged off	417
An account was successfully logged on	365
Cryptographic operation	369
Key file operation	382
Special privileges assigned to new logon	414



```
source="Administrator_logs (3).csv" host="administrator_logs" sourcetype="csv" | stats count by name
```

✓ 3,742 events (before 11/19/22 2:44:27.000 AM) No Event Sampling

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Account_Domain 2
- a Account_Name 2
- a action 1
- a app 3
- a Authentication_Package 3
- a body 100+
- a category 1
- a ComputerName 50
- a date_hour 24
- a date_mday 2
- a date_minute 60
- a date_month 1
- a date_second 60
- a date_wday 2
- a date_year 1
- a date_zone 1
- a dest 51
- a dest_is_expected 1
- a dest_nt_domain 1
- a dest_nt_host 51
- a dest_pci_domain 1
- a dest_requires_av 1
- a dest_should_timesync 1
- a dest_should_update 1
- a dvc 50
- a dvc_is_expected 1
- a dvc_nt_host 50
- a dvc_pci_domain 1
- a dvc_requires_av 1
- a dvc_should_timesync 1
- a dvc_should_update 1

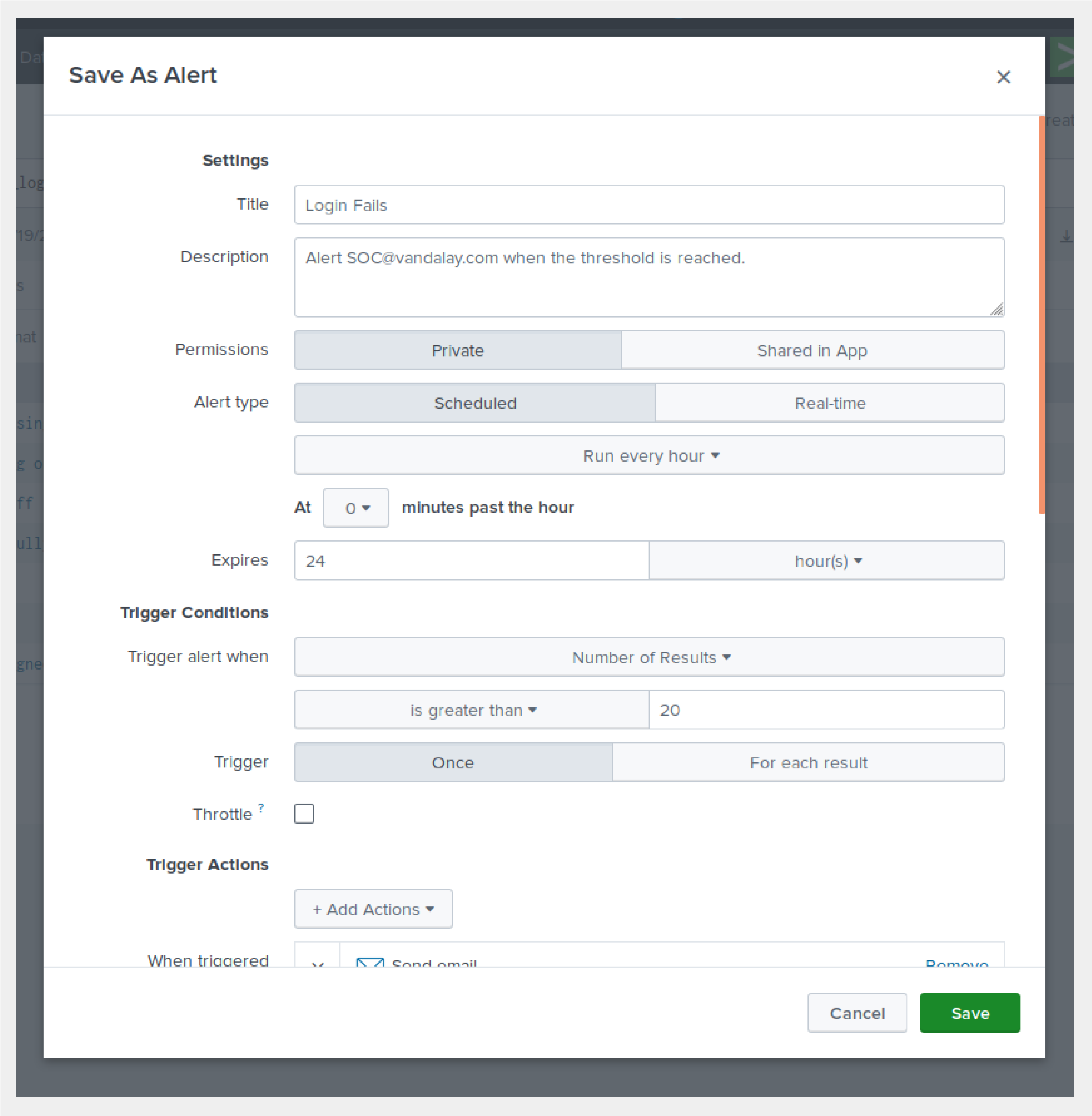
```
i  Time                  Event
>  2/21/20               02/21/2020 17:17:02,,WINDOWS,ADMINISTRATOR,,,,,,,,,,,,,,,,,,SE-002,,,,,-,5061,Cryptographic operation,Information,,,,,,,,,,,,332fe7e7-d709-e3d8-af9e-7236c48f4c55,User key.,Audit Success,Security,,,,0x797,,,,,,"C
   5:17:02.000 PM        ryptographic operation.
                         Subject:
                                 Security ID:            NULL SID
                                 Account Name:           ADMINISTRATOR
                                 Account Domain:         WINDOWS
                         Show all 57 lines
                         host = administrator_logs   source = Administrator_logs (3).csv   sourcetype = csv

>  2/21/20               02/21/2020 17:14:10,,"WINDOWS
   5:14:10.000 PM        WINDOWS","ADMINISTRATOR
                         ADMINISTRATOR",,,,,,,,,,,,,,,,,,BUSDEV-001,,,,,-,4798,,Information,,,,,,,,,,,,,,Audit Success,Security,,,,0x3B9,,,,,,"A User's local group membership was enumerated.
                         Subject:
                                 Security ID:            NT AUTHORITY\SYSTEM
                         Show all 59 lines
                         host = administrator_logs   source = Administrator_logs (3).csv   sourcetype = csv

>  2/21/20               02/21/2020 17:13:40,,WINDOWS,ADMINISTRATOR,,,,,,,,,,,,,,,,,,HOST-003,,,,,-,4634,An account was logged off,Information,,,,,,,,,,,,,,Audit Success,Security,,,,0x2AE60BE,,6,,,,"An account was logged off.
   5:13:40.000 PM        Subject:
                                 Security ID:            NT AUTHORITY\SYSTEM
                                 Account Name:           ADMINISTRATOR
                                 Account Domain:         WINDOWS
                         Show all 46 lines
                         host = administrator_logs   source = Administrator_logs (3).csv   sourcetype = csv

>  2/21/20               02/21/2020 17:12:47,,"WINDOWS
   5:12:47.000 PM        WINDOWS","ADMINISTRATOR
                         ADMINISTRATOR",,,NTLM,,,,,0x4,-,,,,,,,,,,,ops-sys-003,,,,,0xF4E3AC39,4625,An account failed to log on,Information,,Unknown User name or bad password.,,,,,,,,,0,,,Audit Success,Security,,,,0x4,F4E3AC39,0,,,,"An acc
                         ount failed to log on.
                         Subject:
                                 Security ID:            abc\def
                         Show all 135 lines
                         host = administrator_logs   source = Administrator_logs (3).csv   sourcetype = csv

>  2/21/20               02/21/2020 17:11:23,,WINDOWS,ADMINISTRATOR,,UNKNOWN,,,,,,,,,,,,,,,,,ACME-002,,,,,-,5058,Key file operation,Information,,,abc\file\path\BD3390FCABA0958DF456578172B6EDA1_3FE54976-18B7-18B7-18B7-EBB8609AC46
   5:11:23.000 PM        0,,,,,,,,,3FE54976-18B7-18B7-18B7-EBB8609AC460,User key.,Audit Success,Security,,,,0x89C,,,,,,"Key file operation.
                         Subject:
                                 Security ID:            abc\def
```



Save As Alert

Settings

Title: Login Fails

Description: Alert SOC@vandalay.com when the threshold is reached.

Permissions: [✓ Private] Shared in App

Alert type: [✓ Scheduled] Real-time

Run every hour ▾

At 0 ▾ minutes past the hour

Expires: 24 hour(s) ▾

Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than ▾ 20

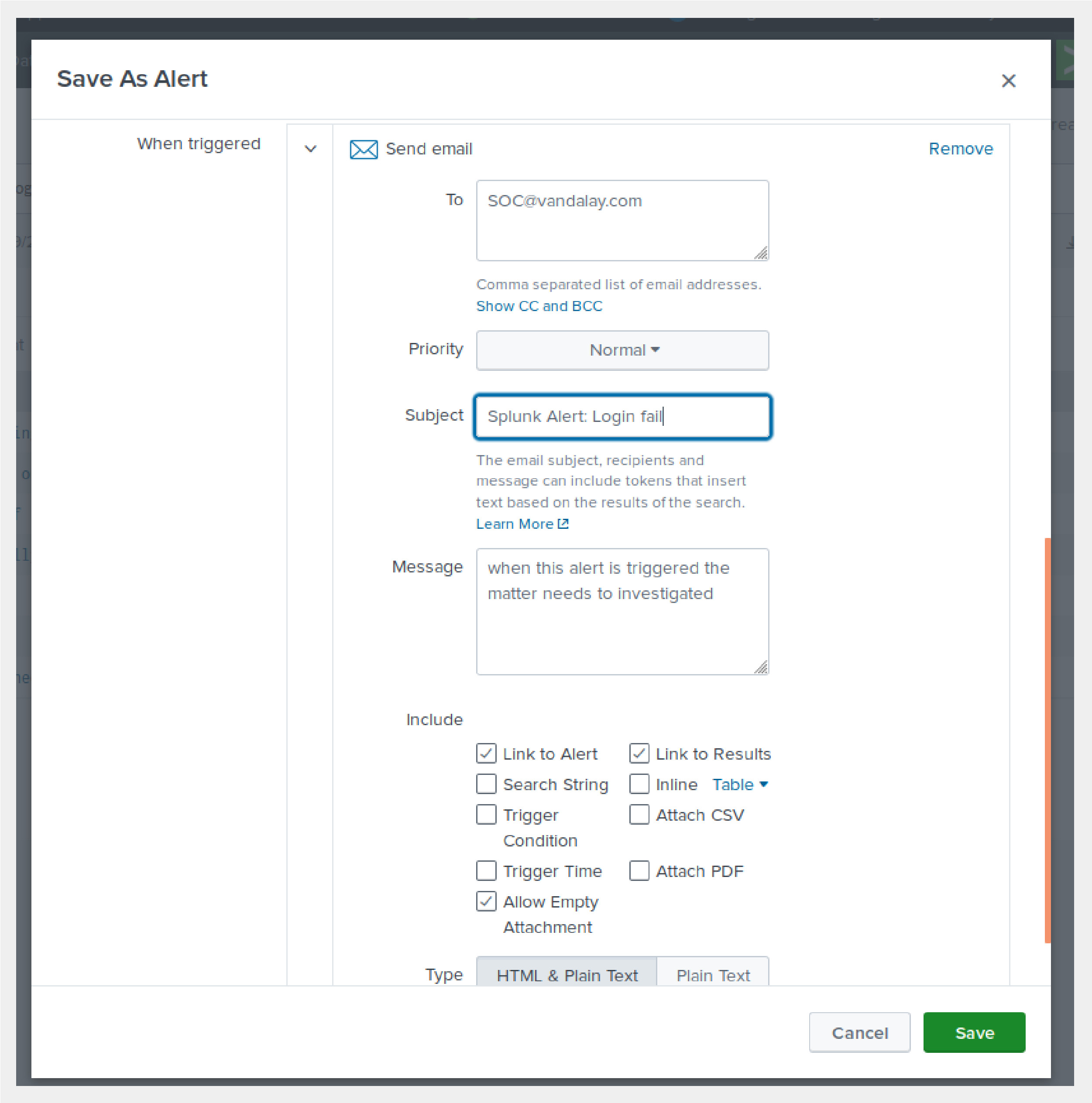
Trigger: [✓ Once] For each result

Throttle ? □

Trigger Actions

+ Add Actions ▾

When triggered: Send email Remove



Save As Alert ×

When triggered

Send email Remove

To: SOC@vandalay.com

Comma separated list of email addresses.

Show CC and BCC

Priority: Normal ▾

Subject: Splunk Alert: Login fail

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

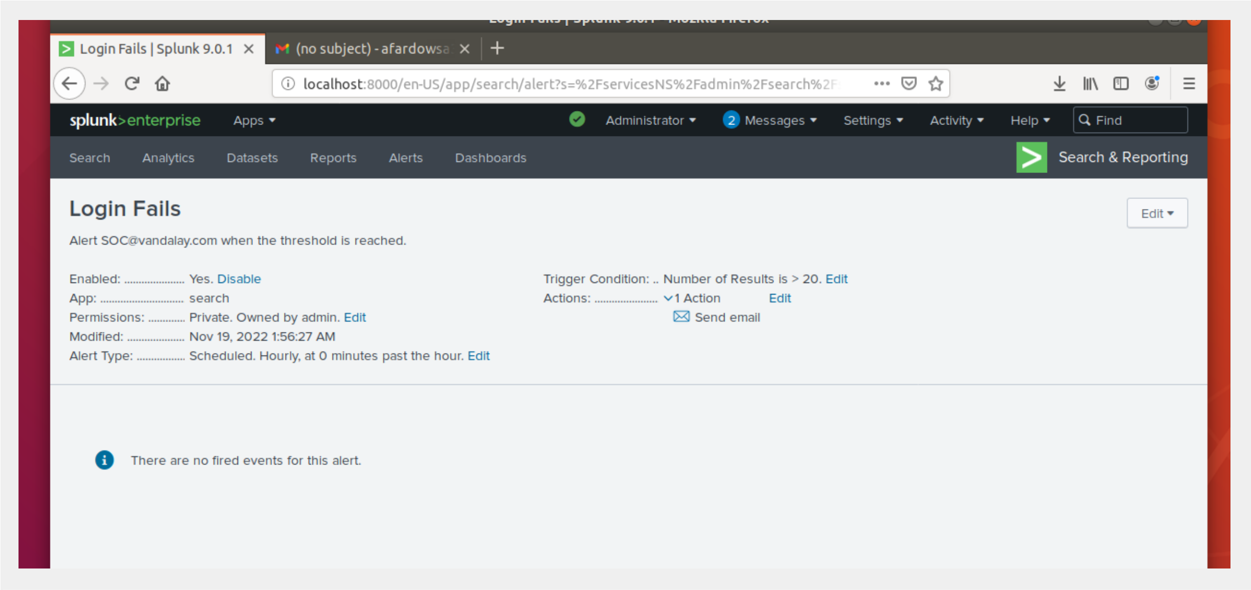
Message: when this alert is triggered the matter needs to investigated

Include

☑ Link to Alert	☑ Link to Results
☐ Search String	☐ Inline Table ▾
☐ Trigger Condition	☐ Attach CSV
☐ Trigger Time	☐ Attach PDF
☑ Allow Empty Attachment	

Type: HTML & Plain Text | Plain Text

Cancel Save



Login Fails

Alert SOC@vandalay.com when the threshold is reached.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Nov 19, 2022 1:56:27 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 20. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.