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

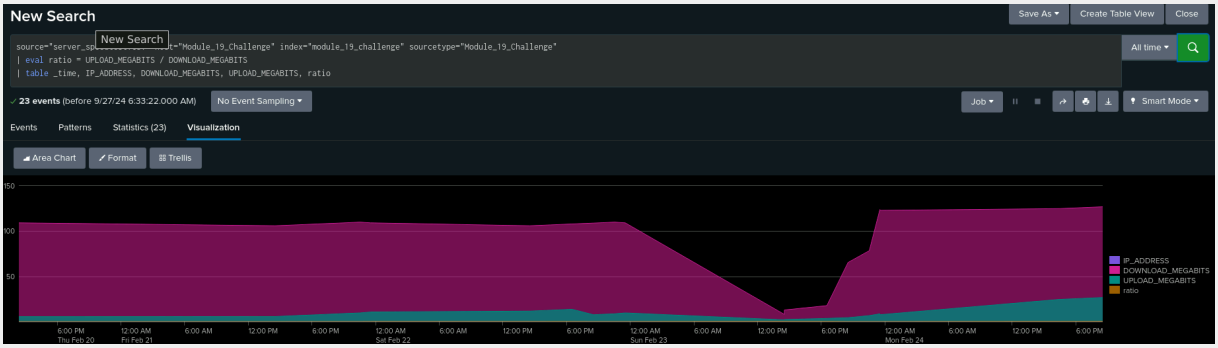
1. Based on the report you created, what is the approximate date and time of the attack?

```
The attack time was approximately 2/23/2020 2:30 PM,GMT
```

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

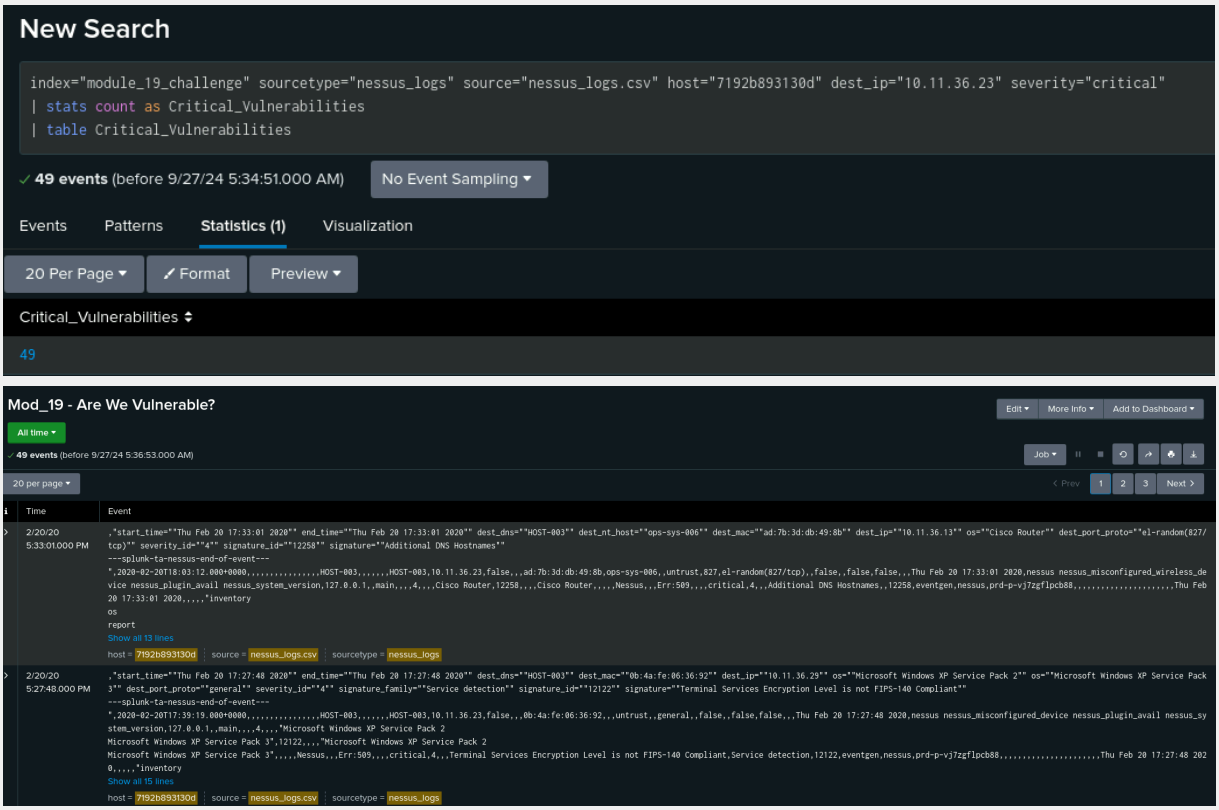
```
It took approximately 9hrs for our systems to recover.
```

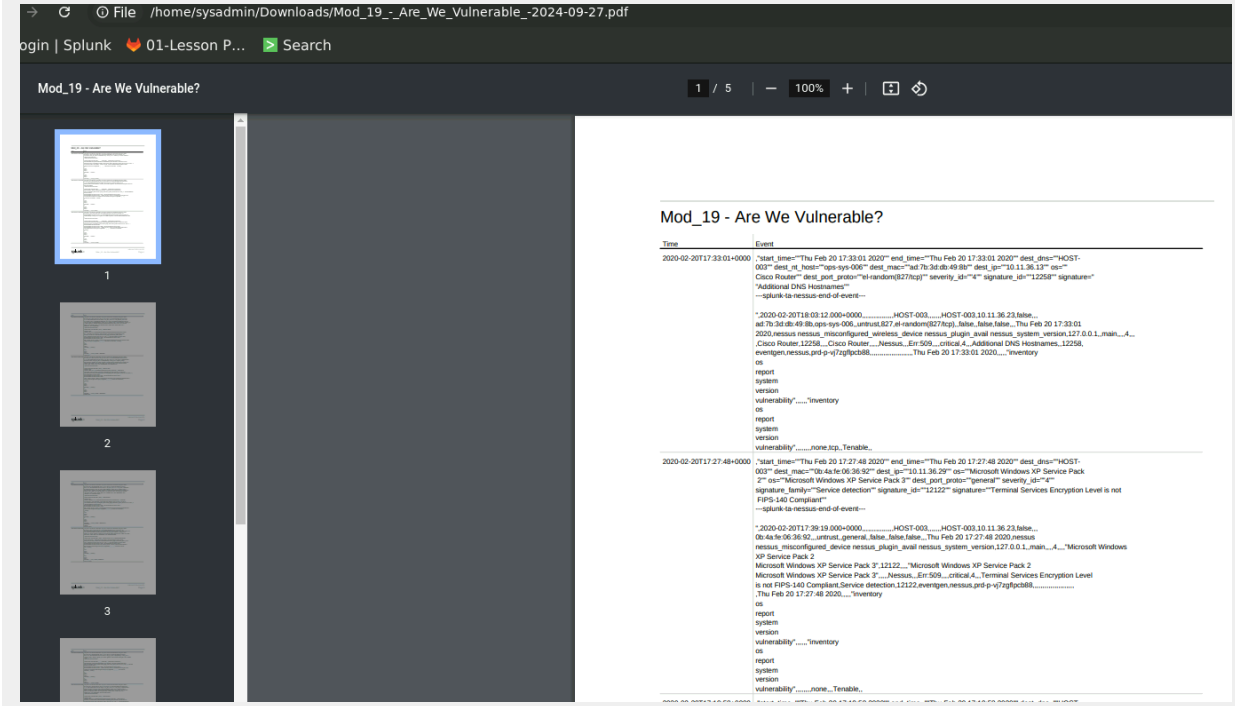
Provide a screenshot of your report:



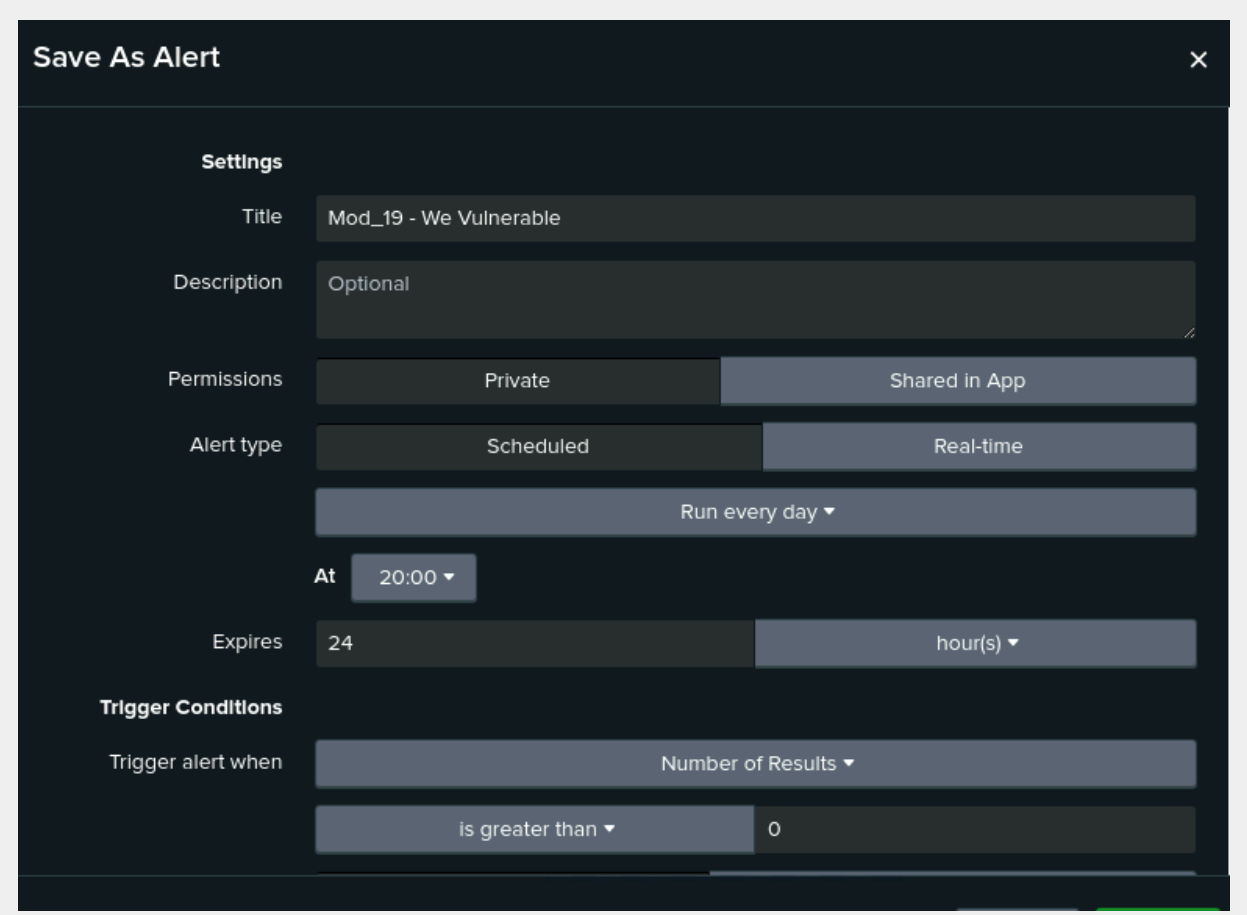
Step 2: Are We Vulnerable?

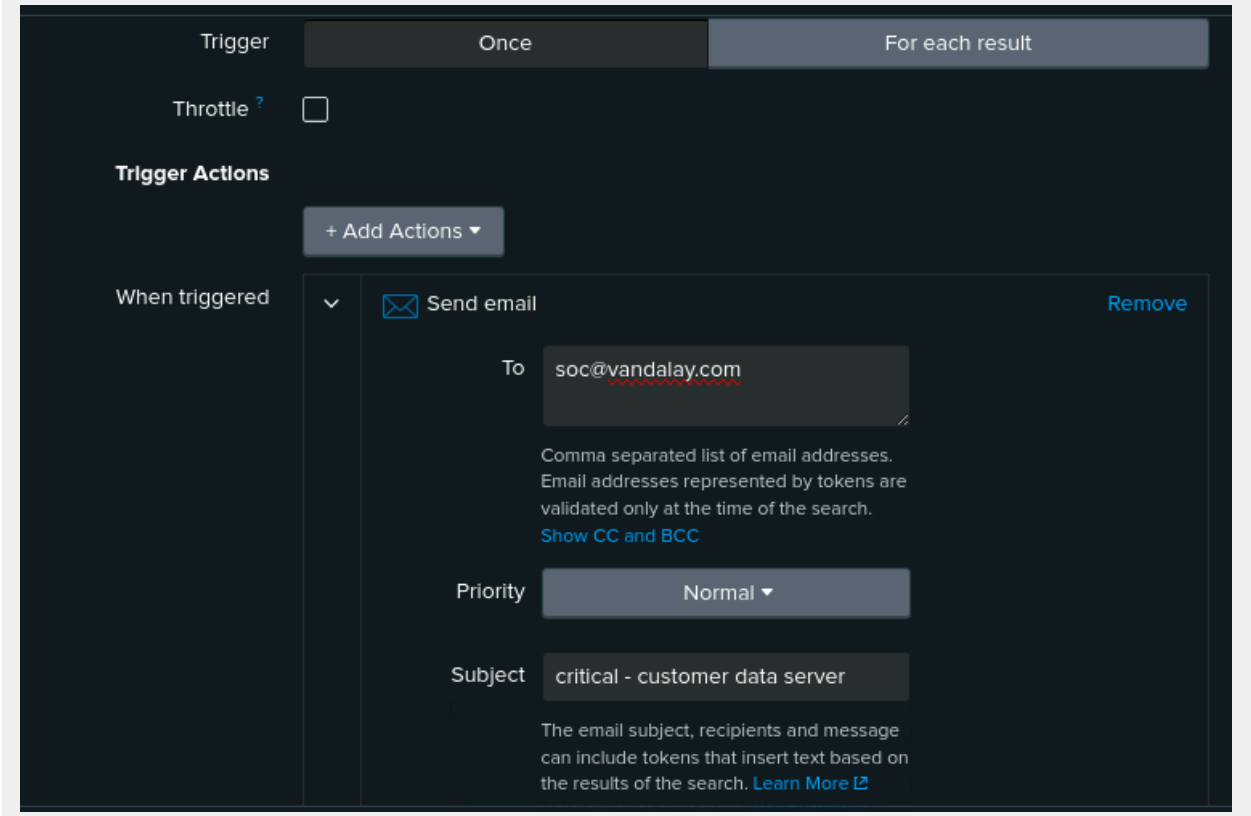
Provide a screenshot of your report:

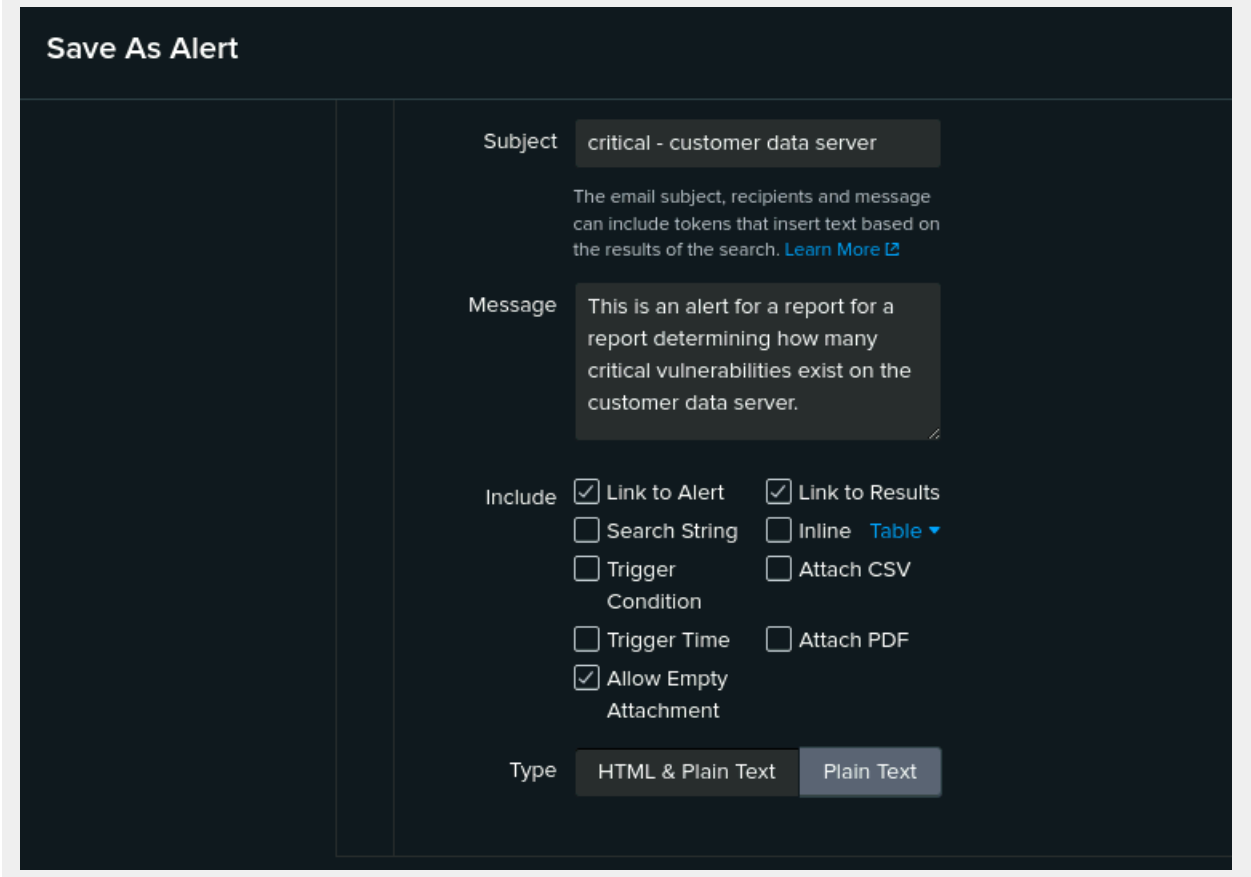


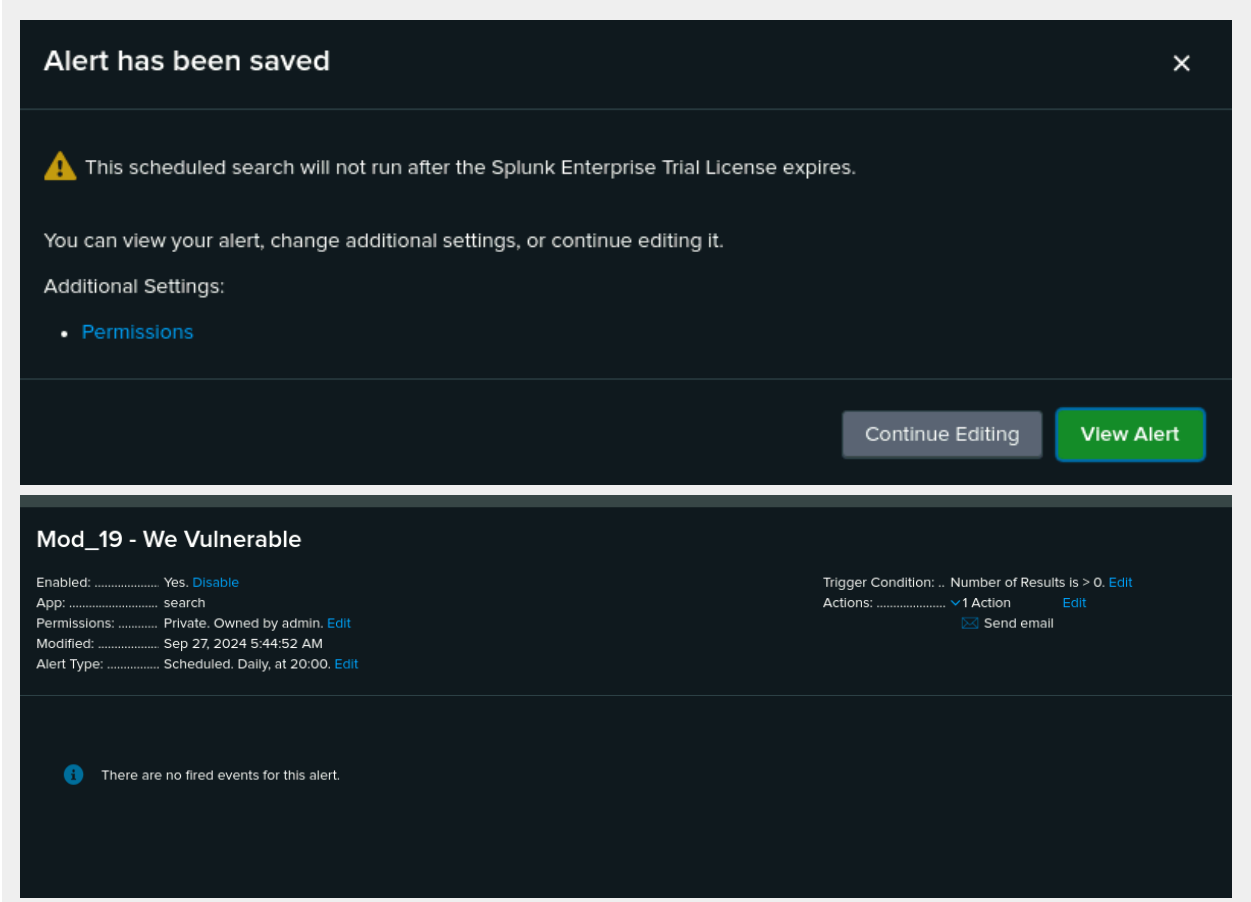


Provide a screenshot showing that the alert has been created:


Save As Alert
Settings
Title
Mod_19 - We Vulnerable
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every day
At
20:00
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
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
critical - customer data server
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

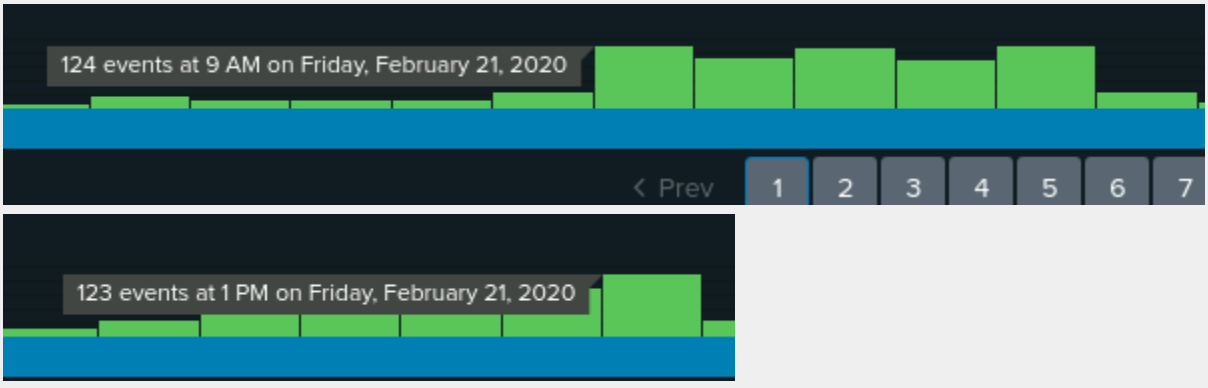

Save As Alert
Subject
critical - customer data server
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More
Message
This is an alert for a report for a report determining how many critical vulnerabilities exist on the customer data server.
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



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

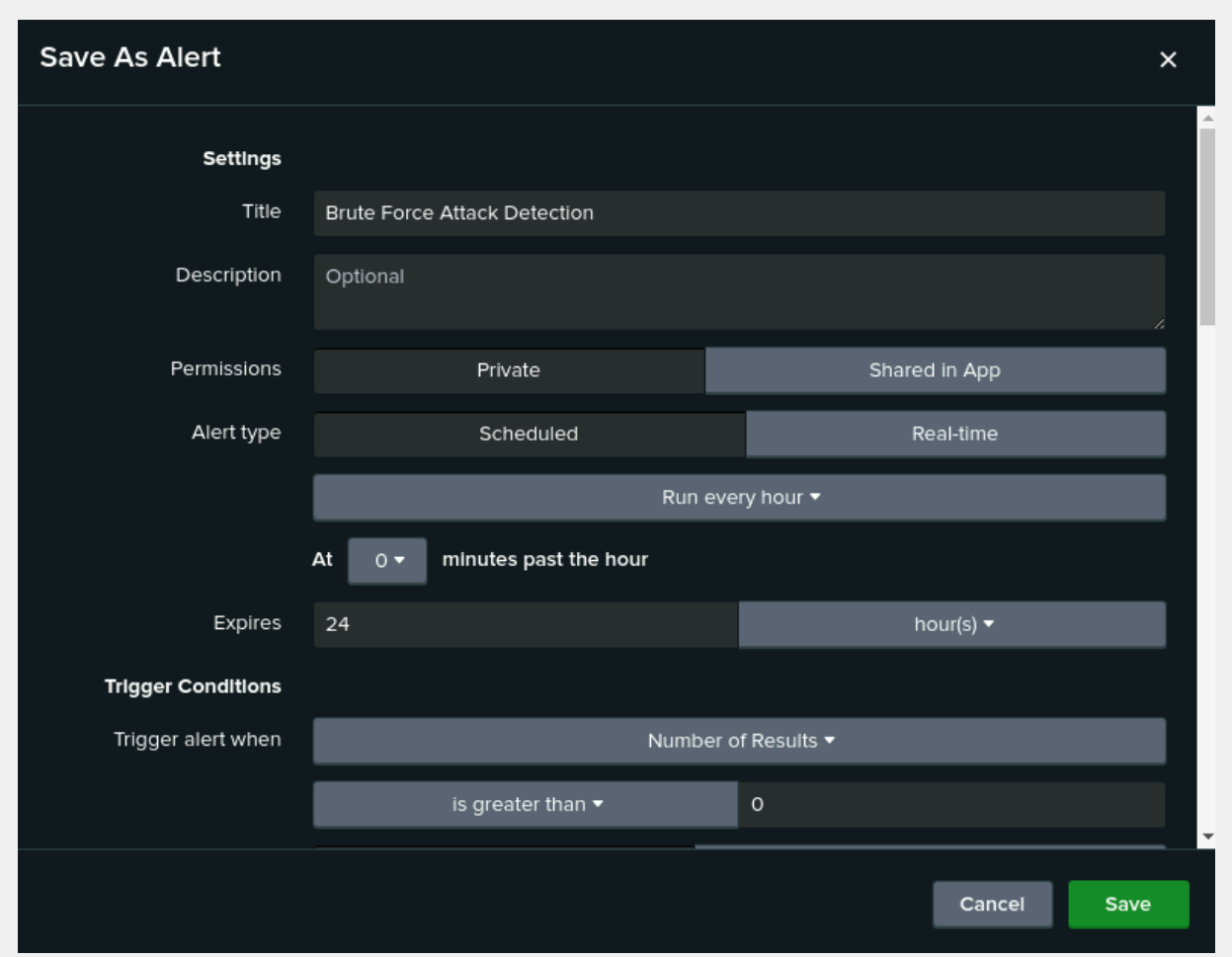
Between
9am Friday 21/02/2020 (124 events) - 1pm Friday 21/02/2020 (123 events)

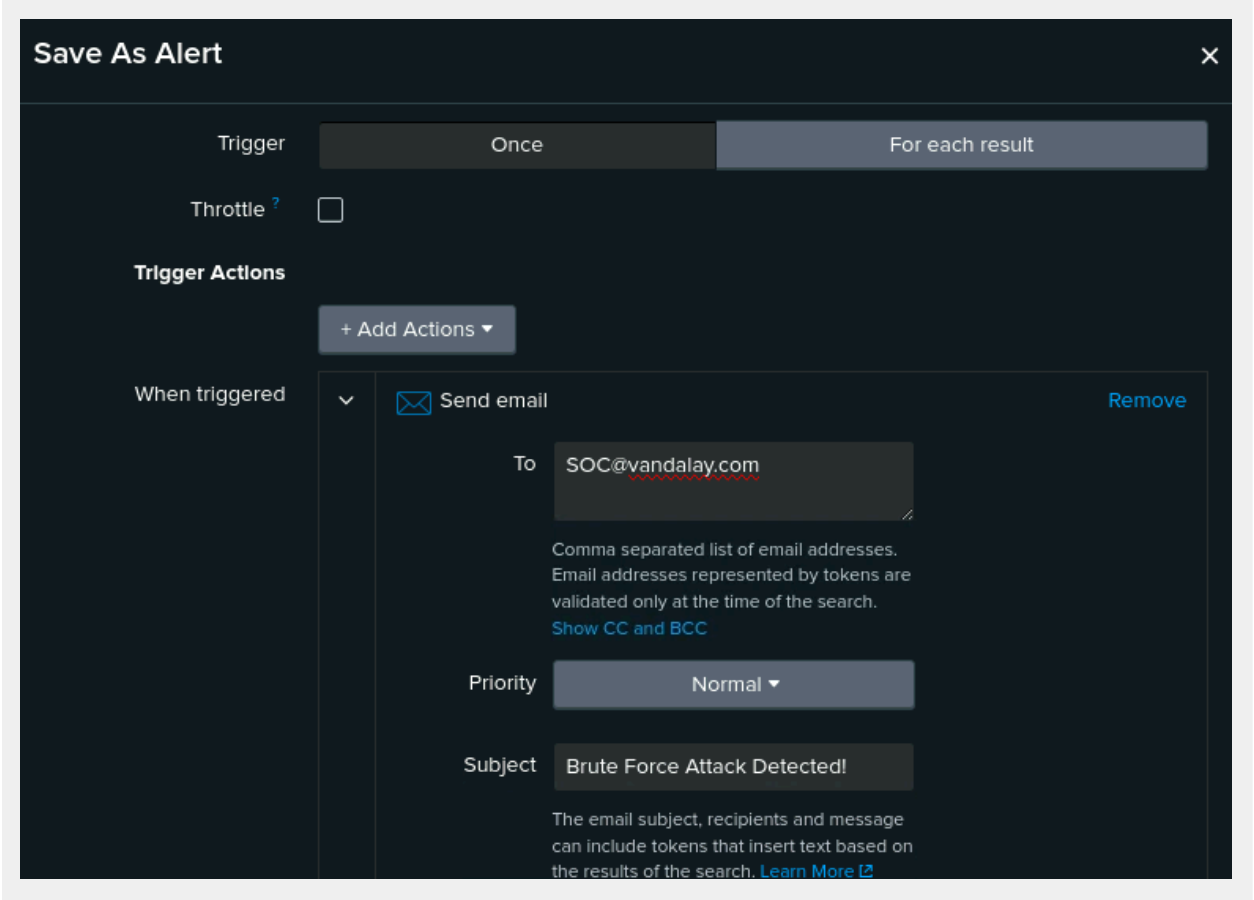


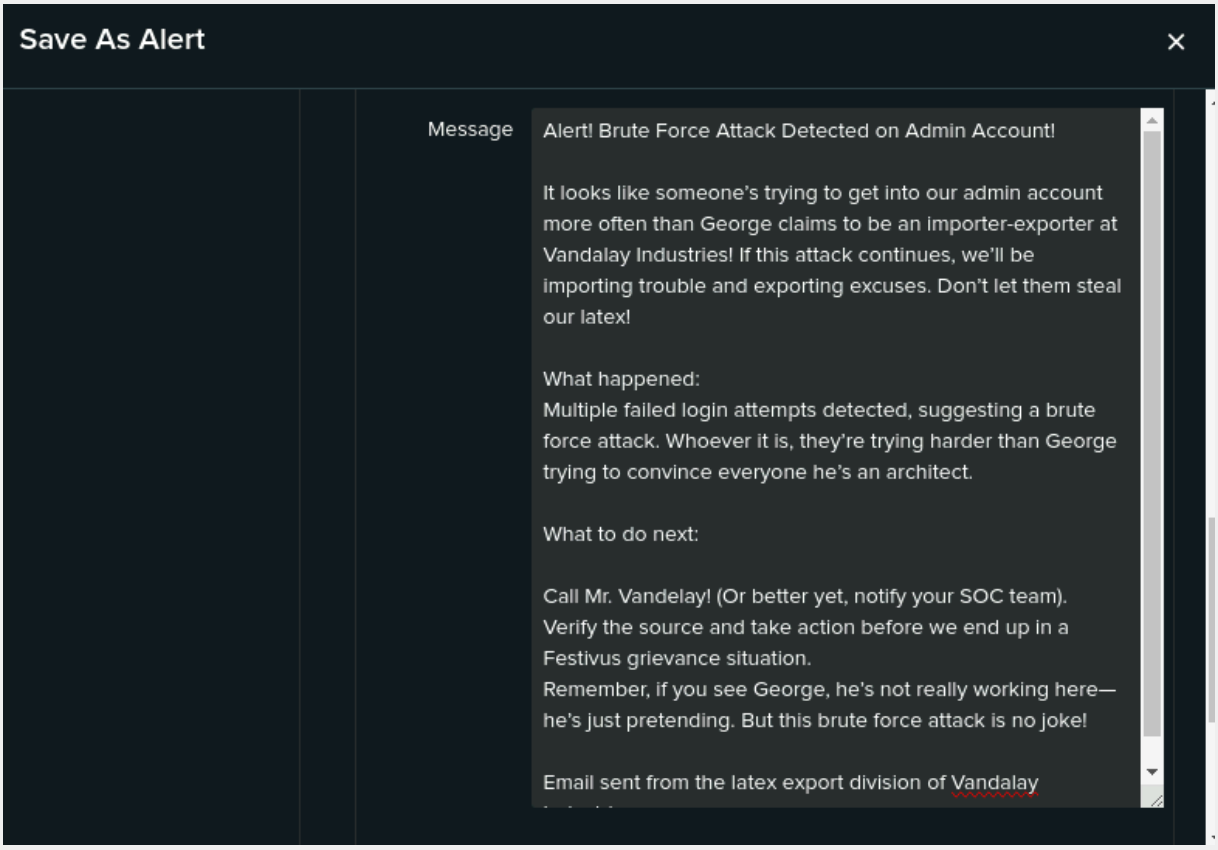
2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

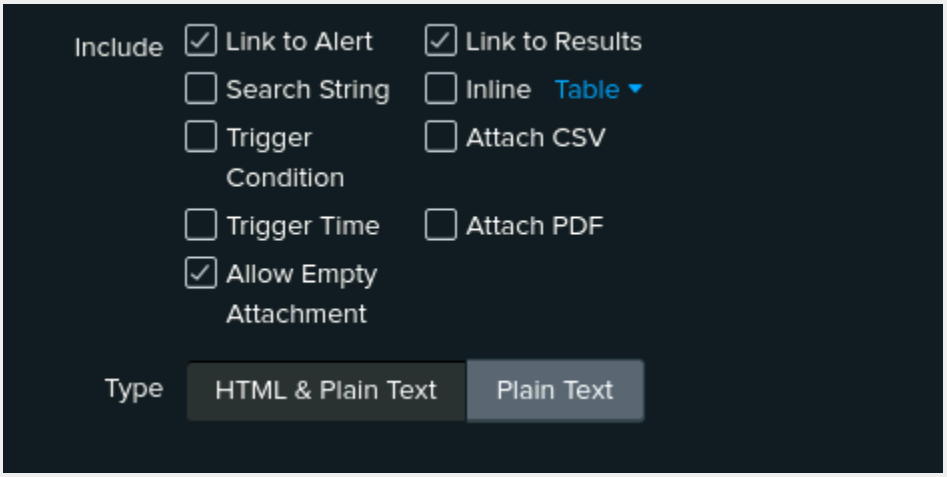
```
The normal baseline would be around 15 failed logins per hour. So I would
set the alert at 18 per hour to avoid too many false positives.
```

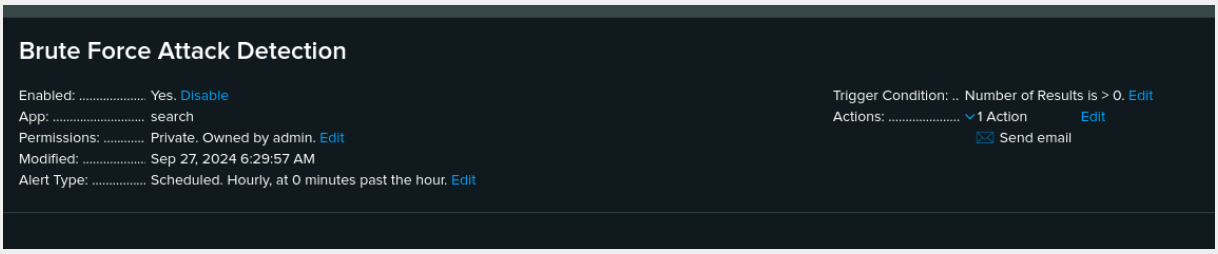
3. Provide a screenshot showing that the alert has been created:


Save As Alert
Settings
Title
Brute Force Attack Detection
Description
Optional
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
0
Cancel
Save


Save As Alert
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
Normal
Subject
Brute Force Attack Detected!
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More


Save As Alert
Message
Alert! Brute Force Attack Detected on Admin Account!
It looks like someone's trying to get into our admin account more often than George claims to be an importer-exporter at Vandalay Industries! If this attack continues, we'll be importing trouble and exporting excuses. Don't let them steal our latex!
What happened:
Multiple failed login attempts detected, suggesting a brute force attack. Whoever it is, they're trying harder than George trying to convince everyone he's an architect.
What to do next:
Call Mr. Vandelay! (Or better yet, notify your SOC team).
Verify the source and take action before we end up in a Festivus grievance situation.
Remember, if you see George, he's not really working here—he's just pretending. But this brute force attack is no joke!
Email sent from the latex export division of Vandalay


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


Brute Force Attack Detection
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Sep 27, 2024 6:29:57 AM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit
Trigger Condition: Number of Results is > 0. Edit
Actions: 1 Action Edit
Send email