Cybersecurity

Activity Guide

Designing Your Defensive Solution

Today, you will create a monitoring solution to protect VSI. Specifically, you will:

1. **Load and analyze Windows logs.**
2. **Create reports, alerts, and dashboards for the Windows logs.**
3. **Load and analyze Apache logs.**
4. **Create reports, alerts, and dashboards for the Apache logs.**
5. **Install an add-on Splunk application for additional monitoring.**

Resources

- Splunkbase
- Splunk Documentation
- Splunk Add-Ons Guide

Instructions

- Today, you will play the role of an SOC analyst at a small company called **Virtual Space Industries (VSI)**, which designs virtual-reality programs for businesses.
- VSI has heard rumors that a competitor, **JobeCorp**, may launch cyberattacks to disrupt VSI's business.
- As an SOC analyst, you are tasked with using Splunk to monitor potential attacks on your systems and applications.
- The VSI products that you have been tasked with monitoring include:
    - An Apache web server, which hosts the administrative webpage

    - A Windows operating system, which runs many of VSI’s back-end operations
- Your networking team has provided you with past logs to help you develop baselines and create reports, alerts, dashboards, and more.

You’ve been provided the following logs on your machine:

- **Windows Server Logs**
    - This server contains intellectual property of VSI’s next-generation virtual-reality programs.
- **Apache Server Logs**
    - This server is used for VSI’s main public-facing website, vsi-company.com.

Complete the following five parts in order to accomplish your Day 1 tasks.

Part 1: Load and Analyze Windows Logs

In this first part, you will upload and analyze Windows security logs that represent “regular” activity for VSI into your Splunk environment.

- Update the value to “Windows_server_logs” and then select “Review.”
- On the “Review” page, verify that you’ve chosen the correct settings.
    - Select “Submit” to proceed with uploading your data into Splunk.
- Once the file has successfully uploaded, a message that says “File has been uploaded successfully” will appear.
- Select “Start Searching.”
- ⚠ **Important:** After the data populates on the search, select “All Time” for the time range.
- Briefly analyze the logs and the available fields, specifically examining the following important fields:
    - signature_id
    - signature
    - user
    - status
    - severity

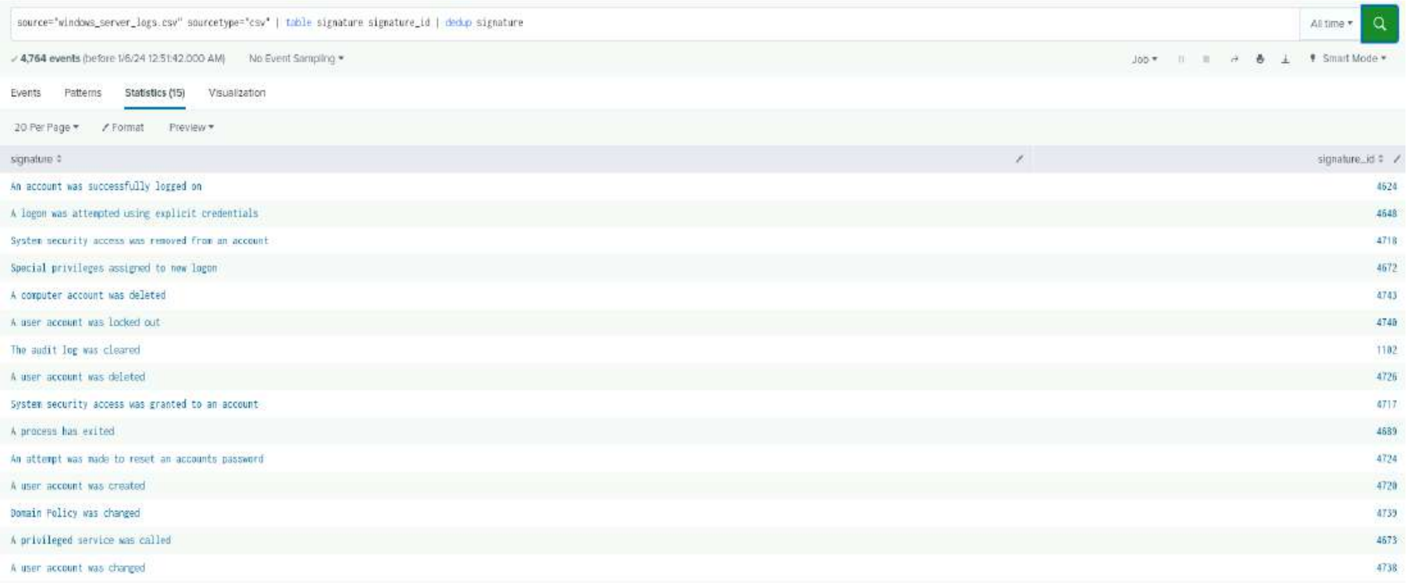
Part 2 Create Reports, Alerts, and Dashboards for the Windows Logs

In this part, you will create reports, alerts, and dashboards to monitor for suspicious activity against VSI's Windows server. Design the following deliverables to protect VSI from potential attacks by JobeCorp:

1. **Reports:** Design the following **reports** to assist VSI in quickly identifying specific information and **be sure to grab screenshots of each report**:
   - A report with a table of signatures and associated signature IDs.
     a. This will allow VSI to view reports that show the ID number associated with the specific signature for Windows activity.

     b. **Hint:** Research how to remove the duplicate values in your SPL search.

     c. Take a screenshot of the report



```
source="windows_server_logs.csv" sourcetype="csv" | table signature signature_id | dedup signature
```

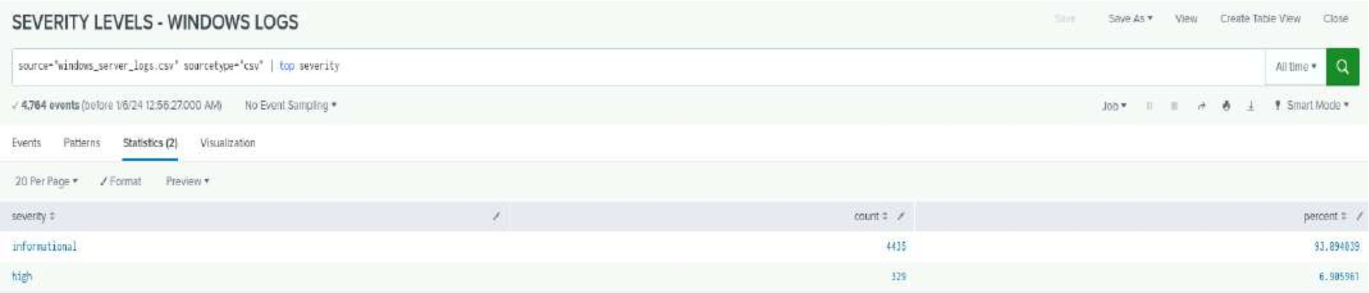
✓ 4,764 events (before 1/6/24 12:51:42.000 AM)

signature	signature_id
An account was successfully logged on	4624
A logon was attempted using explicit credentials	4648
System security access was removed from an account	4718
Special privileges assigned to new logon	4672
A computer account was deleted	4743
A user account was locked out	4740
The audit log was cleared	1102
A user account was deleted	4726
System security access was granted to an account	4717
A process has exited	4689
An attempt was made to reset an accounts password	4724
A user account was created	4720
Domain Policy was changed	4739
A privileged service was called	4673
A user account was changed	4738

- A report that displays the severity levels, and the count and percentage of each.

    a. This will allow VSI to quickly understand the severity levels of the Windows logs being viewed.

    b. Take a screenshot of the report.



SEVERITY LEVELS - WINDOWS LOGS

```
source="windows_server_logs.csv" sourcetype="csv" | top severity
```

✓ **4,764 events** (before 1/6/24 12:56:27.000 AM) No Event Sampling ▾

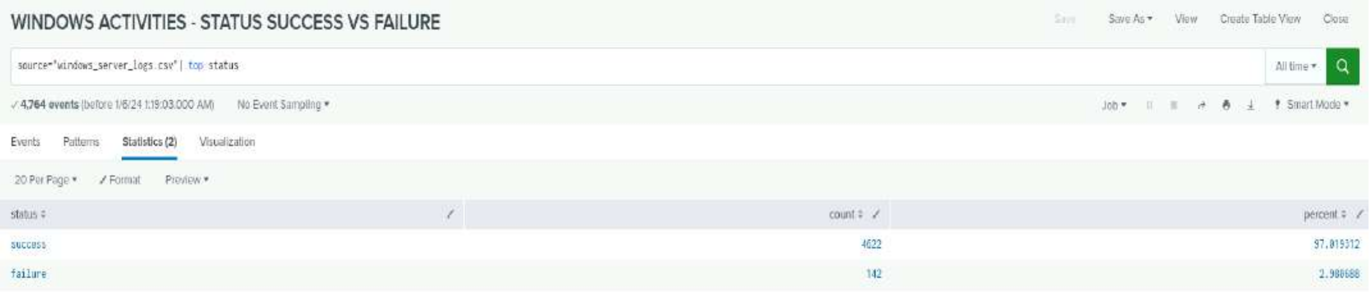
severity	count	percent
informational	4435	93.094039
high	329	6.905961

- A report that provides a comparison between the success and failure of Windows activities.

    a. This will show VSI if there is a suspicious level of failed activities on their server.

    b. **Hint:** Check the “status” field for this information.

    c. Take a screenshot of the report.



WINDOWS ACTIVITIES - STATUS SUCCESS VS FAILURE

```
source="windows_server_logs.csv" | top status
```

✓ **4,764 events** (before 1/6/24 1:19:03.000 AM) No Event Sampling ▾

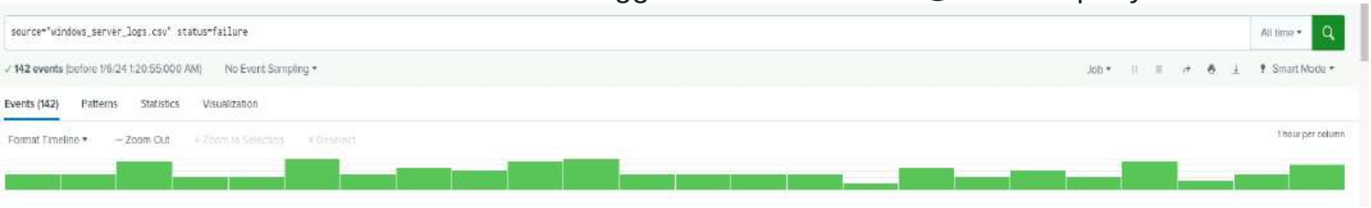
status	count	percent
success	4622	97.019312
failure	142	2.980688

2. **Alerts:** Design the following **alerts** to notify VSI of suspicious activity, and keep this information on hand as you will include it in your presentation:

   - Determine a baseline and threshold for the hourly level of failed Windows activity.

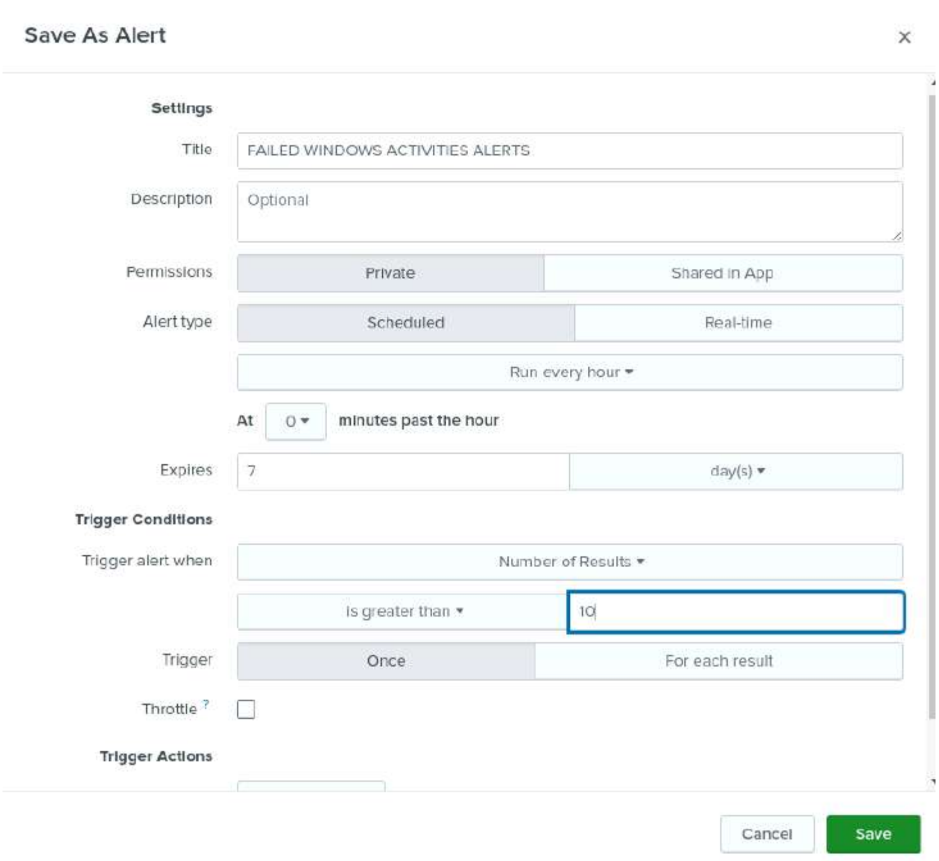
     a. Create an alert that's triggered when the threshold has been reached.

     b. The alert should trigger an email to SOC@VSI-company.com.



```
source="windows_server_logs.csv" status=failure
```

✓ 142 events (before 1/6/24 1:20:55.000 AM) No Event Sampling ▾



Save As Alert

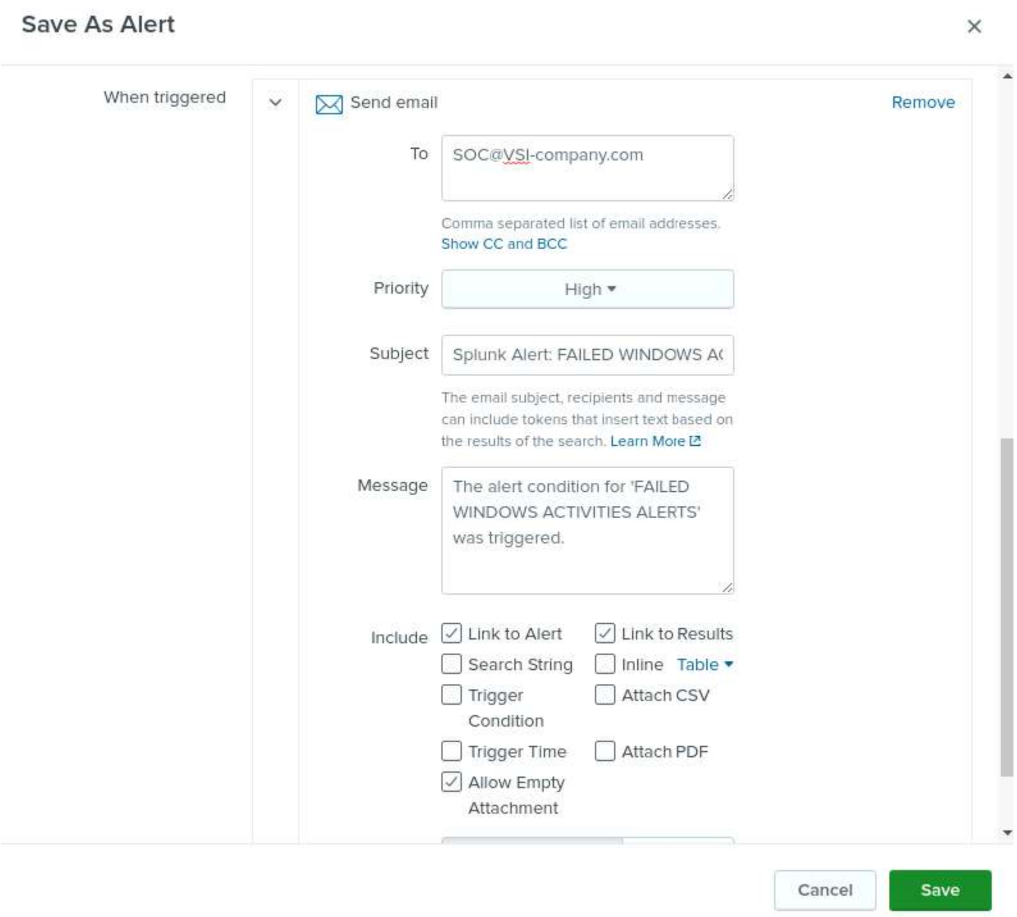
Settings

Title	FAILED WINDOWS ACTIVITIES ALERTS
Description	Optional
Permissions	Private
Alert type	Scheduled
	Run every hour ▾
At	0 ▾ minutes past the hour
Expires	7 day(s) ▾

Trigger Conditions

Trigger alert when	Number of Results ▾
	is greater than ▾ 10
Trigger	Once
Throttle ?	□

Trigger Actions



Save As Alert ×

When triggered

Send email — Remove

To: SOC@VSI-company.com

Comma separated list of email addresses.
Show CC and BCC

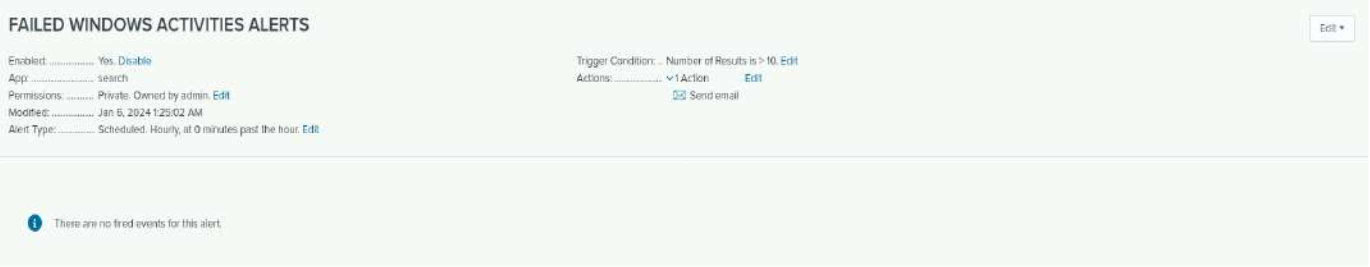
Priority: High ▾

Subject: Splunk Alert: FAILED WINDOWS A(

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 'FAILED WINDOWS ACTIVITIES ALERTS' was triggered.

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



FAILED WINDOWS ACTIVITIES ALERTS

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jan 6, 2024 1:25:02 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 10. Edit
Actions: .... ∨ 1 Action Edit
Send email

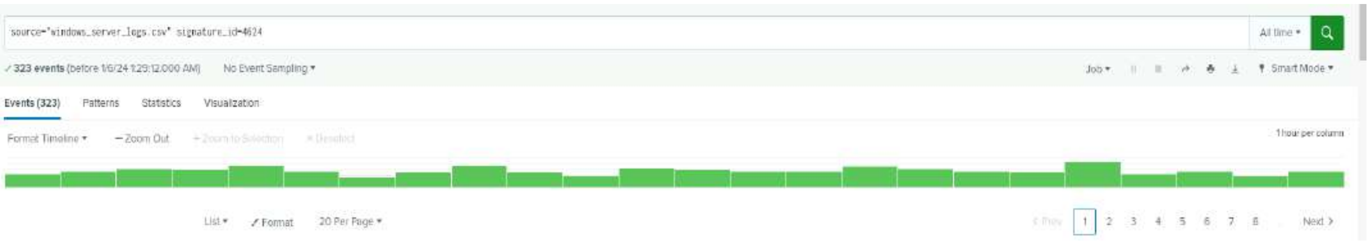
There are no fired events for this alert.

- Determine a baseline and threshold for the hourly count of the signature “an account was successfully logged on.”

  a. Create an alert that’s triggered when the threshold has been reached.

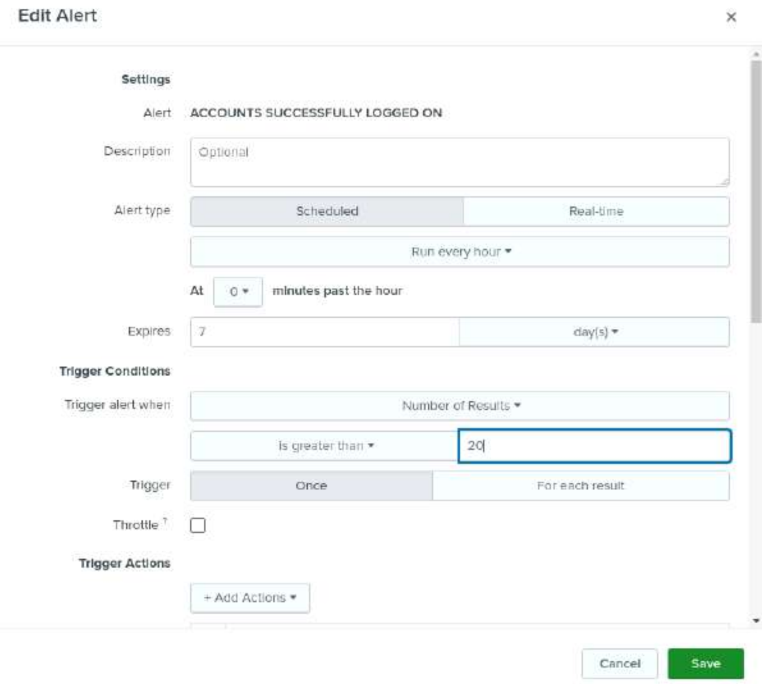
  b. The alert should trigger an email to SOC@VSI-company.com.

  c. Design the alert based on the corresponding signature ID, as the signature name sometimes changes when the Windows system updates.



```
source="windows_server_logs.csv" signature_id=4624
```

✓ 323 events (before 1/6/24 1:29:12.000 AM)



Edit Alert

Settings

Alert: ACCOUNTS SUCCESSFULLY LOGGED ON

Description: Optional

Alert type: [✓ Scheduled] Real-time

Run every hour ▾

At 0 ▾ minutes past the hour

Expires: 7 day(s) ▾

Trigger Conditions

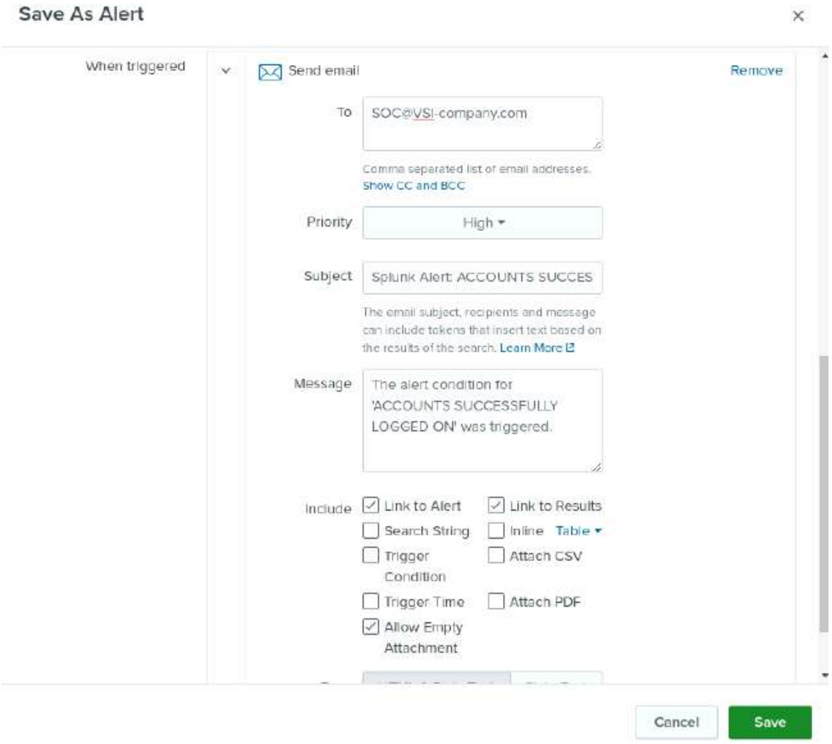
Trigger alert when: Number of Results ▾

is greater than ▾ 20

Trigger: [✓ Once] For each result

Throttle ? □

Trigger Actions



Save As Alert

When triggered: Send email

To: SOC@VSI-company.com

Comma separated list of email addresses.
Show CC and BCC

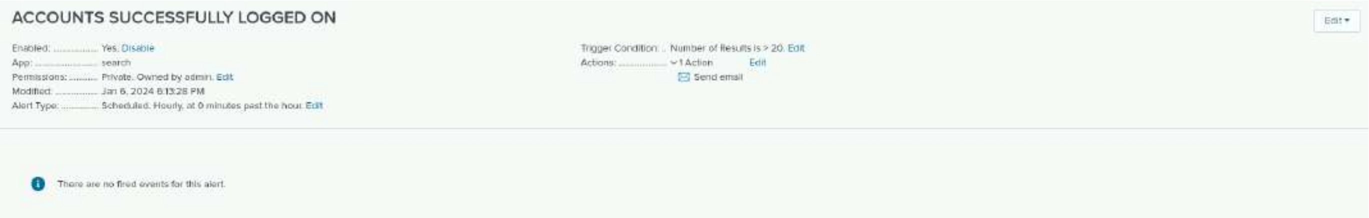
Priority: High ▾

Subject: Splunk Alert: ACCOUNTS SUCCES

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 'ACCOUNTS SUCCESSFULLY LOGGED ON' was triggered.

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



ACCOUNTS SUCCESSFULLY LOGGED ON

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jan 6, 2024 6:13:28 PM
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

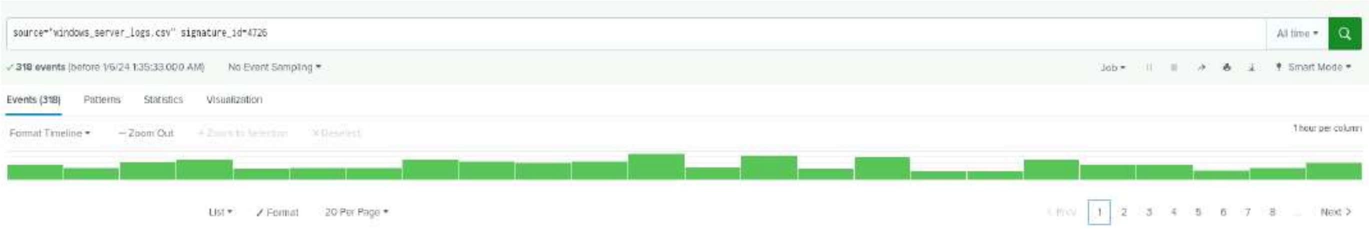
There are no fired events for this alert.

- Determine a baseline and threshold for the hourly count of the signature "a user account was deleted."

    a. Design the alert based on the corresponding signature ID, as the signature name sometimes changes when the Windows system updates.

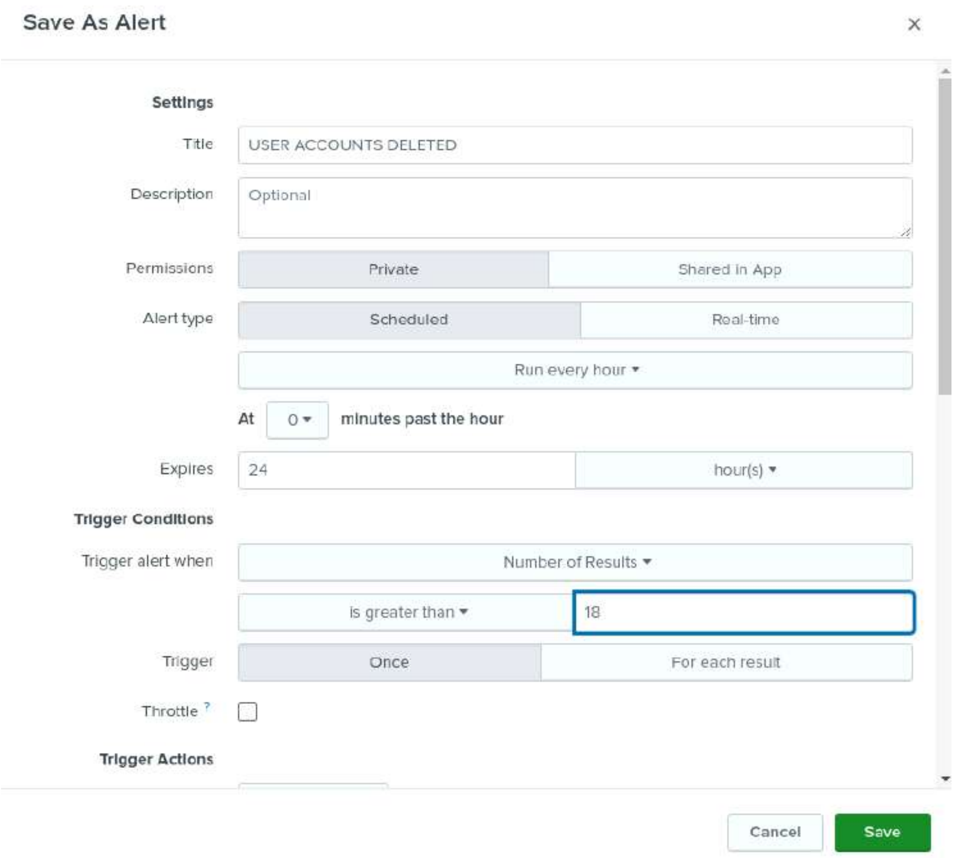
    b. Create an alert that's triggered when the threshold has been reached.

    c. The alert should trigger an email to SOC@VSI-company.com.



```
source="windows_server_logs.csv" signature_id=4726
```

✓ 318 events (before 1/6/24 1:35:33.000 AM) No Event Sampling ▾



Save As Alert

Settings

Title: USER ACCOUNTS DELETED

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

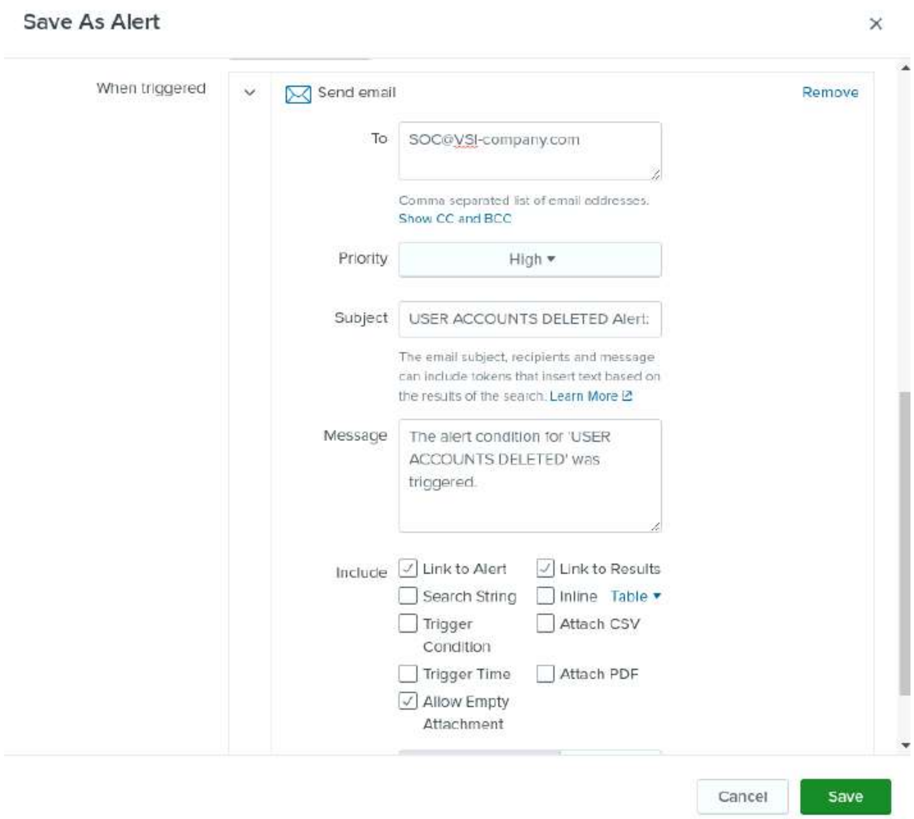
Trigger alert when: Number of Results ▾

is greater than ▾ 18

Trigger: [✓ Once] For each result

Throttle ? □

Trigger Actions



Save As Alert

When triggered: Send email

To: SOC@VSI-company.com

Comma separated list of email addresses.
Show CC and BCC

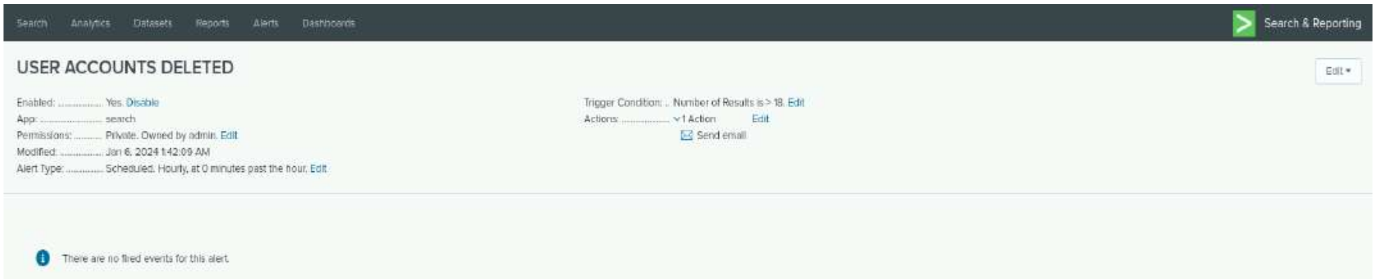
Priority: High ▾

Subject: USER ACCOUNTS DELETED Alert:

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 'USER ACCOUNTS DELETED' was triggered.

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



USER ACCOUNTS DELETED

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jan 6, 2024 1:42:09 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 18. Edit
Actions: .... ⌄1 Action Edit
✉ Send email

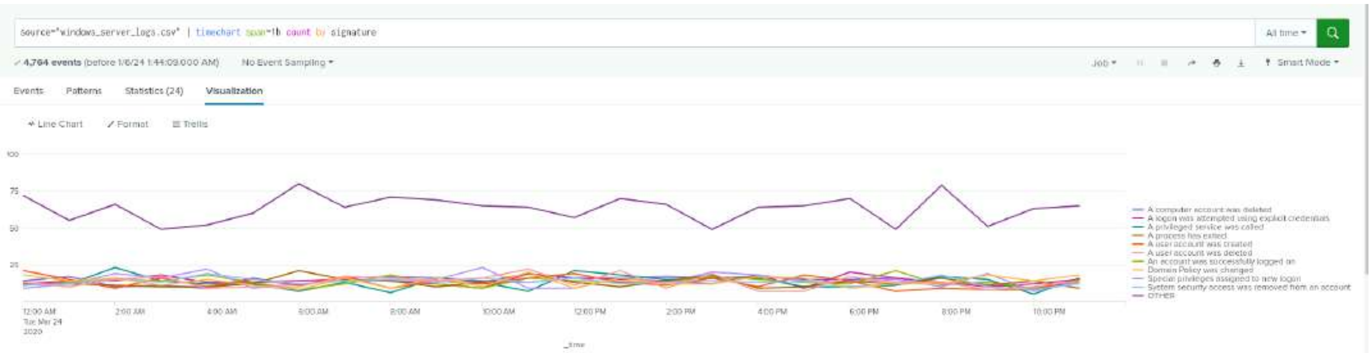
There are no fired events for this alert.

3. **Visualizations and dashboards:** Design the following visualizations, and add them to a dashboard called “Windows Server Monitoring” (be creative with your visualizations, and make sure to grab screenshots of each):

   ○ A line chart that displays the different “signature” field values over time.

   a. **Hint:** Add the following after your search: `timechart span=1h count by signature`.

   b. Take a screenshot of the chart.



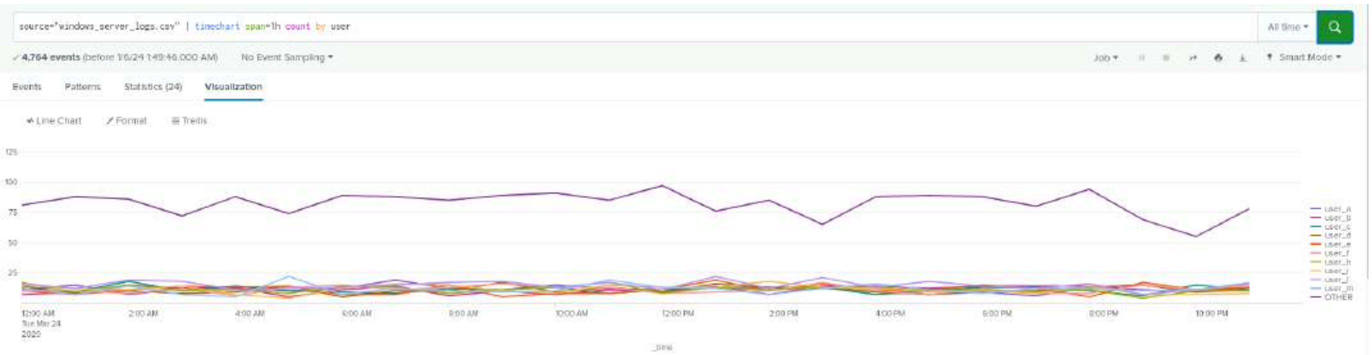
```
source="windows_server_logs.csv" | timechart span=1h count by signature
```

✓ 4,764 events (before 1/6/24 1:44:09.000 AM)

All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (24)
Visualization
Line Chart
Format
Trellis
100
75
50
25
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER

   ○ A line chart that displays the different “user” field values over time.

   a. Take a screenshot of the chart.



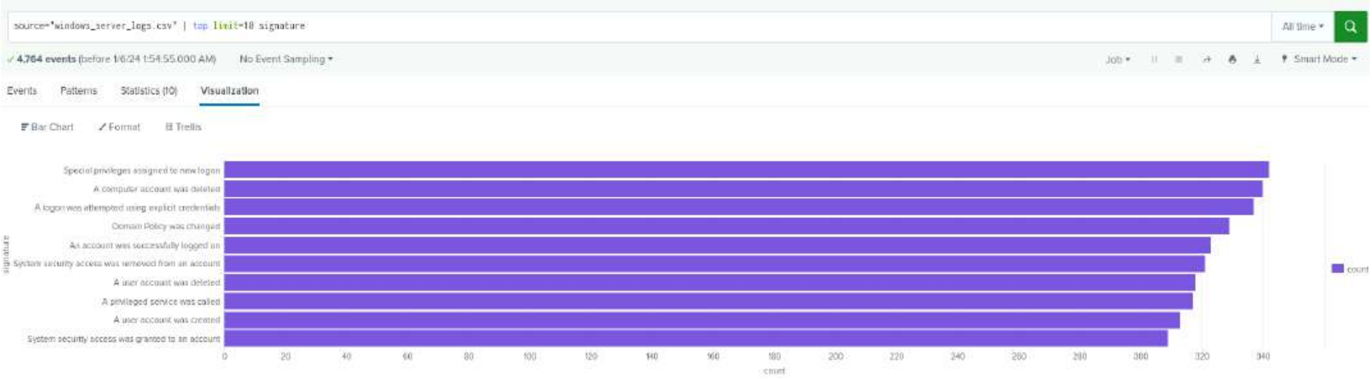
```
source="windows_server_logs.csv" | timechart span=1h count by user
```

✓ 4,764 events (before 1/6/24 1:49:46.000 AM)

- Any visualization that illustrates the count of different signatures.

   a. **Hint:** You can add brand-new custom visualizations by accessing this page inside your VM: Additional Viz.

   b. Take a screenshot of the visualization.



```
source="windows_server_logs.csv" | top limit=10 signature
```

✓ **4,764 events** (before 1/6/24 1:54:55.000 AM) No Event Sampling ▾

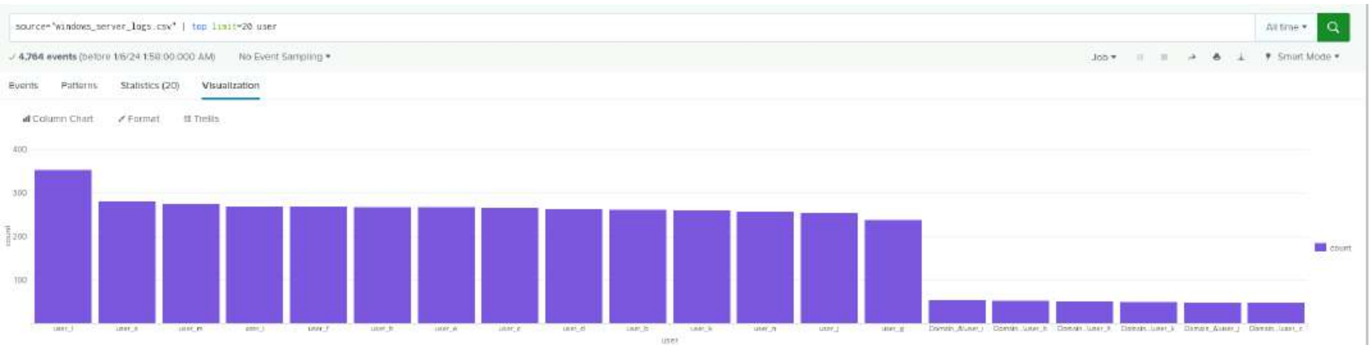
All time ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (10)
Visualization
Bar Chart
Format
Trellis
Special privileges assigned to new logon
A computer account was deleted
A logon was attempted using explicit credentials
Domain Policy was changed
An account was successfully logged on
System security access was removed from an account
A user account was deleted
A privileged service was called
A user account was created
System security access was granted to an account
signature
0
20
40
60
80
100
120
140
160
180
200
220
240
260
280
300
320
340
count
count

- Any visualization that illustrates the count of different users.

   a. Take a screenshot of the visualization.

- Any single-value visualization of your choice that analyzes any single data point,e.g., radial gauge, marker gauge, or a custom visualization from http://localhost:8000/en-US/manager/search/appsremote?content=visualizations&type=app.

   a. Take a screenshot of the visualization.

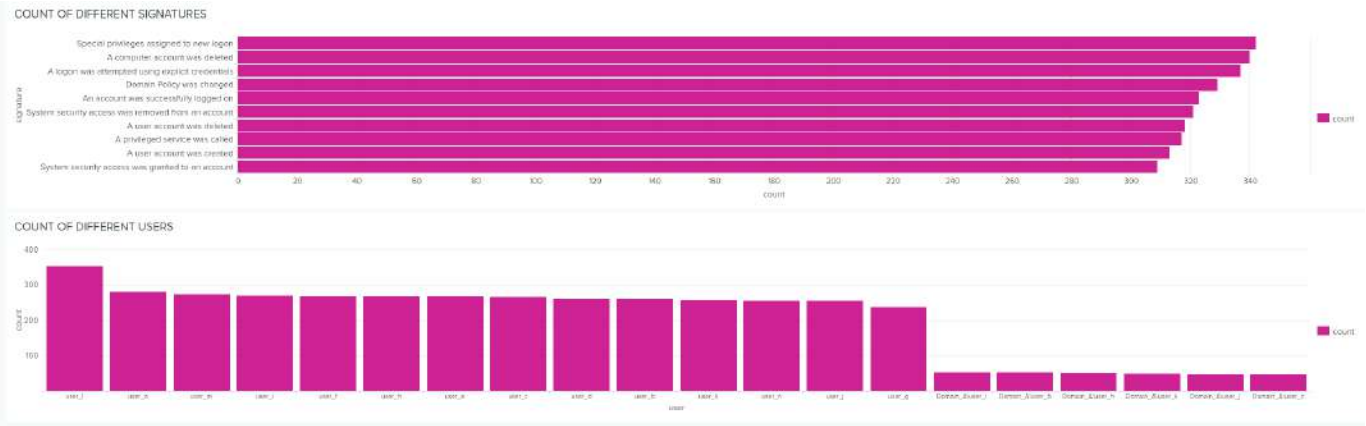


```
source="windows_server_logs.csv" | top limit=20 user
```

✓ **4,764 events** (before 1/6/24 1:58:00.000 AM) No Event Sampling ▾

4. On your dashboard, add the ability to change the time range for all visualizations.

- Be sure to title all of your panels appropriately.
- Organize the panels on your dashboard as you see fit.

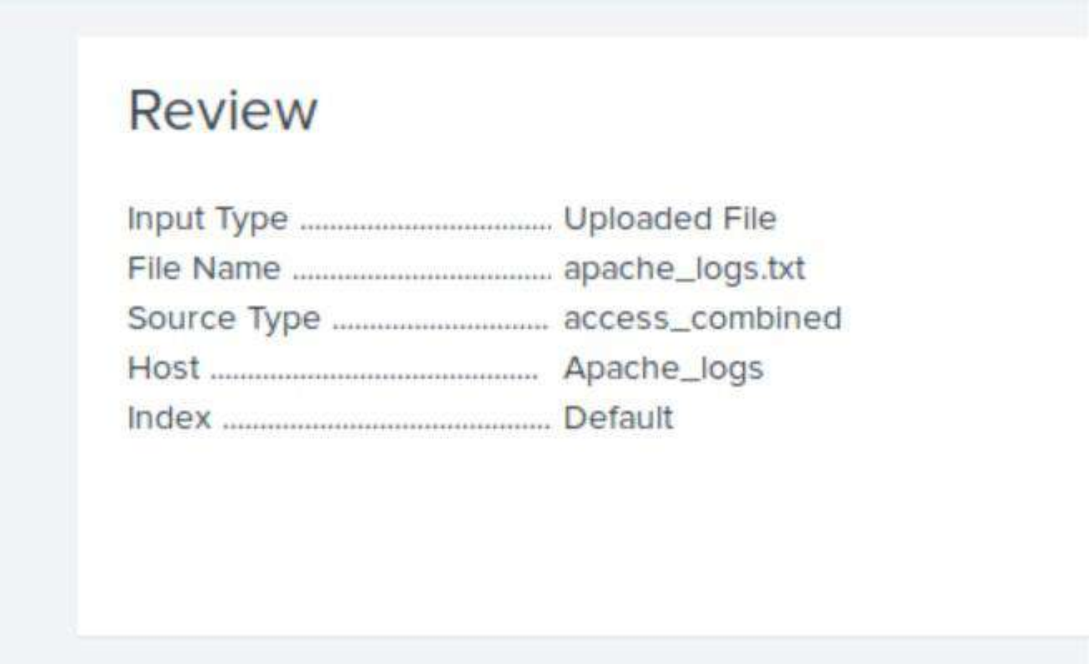

COUNT OF DIFFERENT SIGNATURES
signature
Special privileges assigned to new logon
A computer account was deleted
A logon was attempted using explicit credentials
Domain Policy was changed
An account was successfully logged on
System security access was removed from an account
A user account was deleted
A privileged service was called
A user account was created
System security access was granted to an account
0
20
40
60
80
100
120
140
160
180
200
220
240
260
280
300
320
340
count
count
COUNT OF DIFFERENT USERS
400
300
200
100
count
user_l
user_a
user_m
user_i
user_f
user_h
user_e
user_c
user_d
user_b
user_k
user_n
user_j
user_g
Domain_&user_i
Domain_&user_b
Domain_&user_h
Domain_&user_k
Domain_&user_j
Domain_&user_e
user
count

Part 3: Load and Analyze Apache Logs

In this part, you will upload and analyze Apache web server logs that represent “regular” activity for VSI into your Splunk environment. To do so, complete the following steps:

1. Return to the “Add Data” option within Splunk.
2. Since you will upload the provided log file, select the “Upload” option.
    - Click “Select File.”
    - Select the `apache_logs.txt` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory.
    - Click the green “Next” button in the top right.
3. You’ll be brought to the “Set Source Type” page.
    - You don’t need to change any configurations on this page.
    - Select “Next” again.
4. You’ll be brought to the “Input Settings” page.
    - This page contains optional settings for how the data is input.
    - In the “Host” field, Splunk uses a random value to name the machine or device that generated the logs.
    - Update the value to “Apache_logs” and then select “Review.”

5. On the “Review” page, verify that you’ve chosen the correct settings, as the following image shows:



Review

Input Type .... Uploaded File
File Name .... apache_logs.txt
Source Type .... access_combined
Host .... Apache_logs
Index .... Default

   - Select “Submit” to proceed with uploading your data into Splunk.

6. Once the file has successfully uploaded, a message that says “File has been uploaded successfully” will appear on the screen.

7. Select “Start Searching.”

8. ⚠ **Important:** After the data populates on the search, select “All Time” for the time range.

9. Briefly analyze the logs and the available fields, specifically examining the following important fields:

   - method
   - referer_domain
   - status
   - clientip
   - useragent

Part 4: Create Reports, Alerts, and Dashboards for the Apache Logs

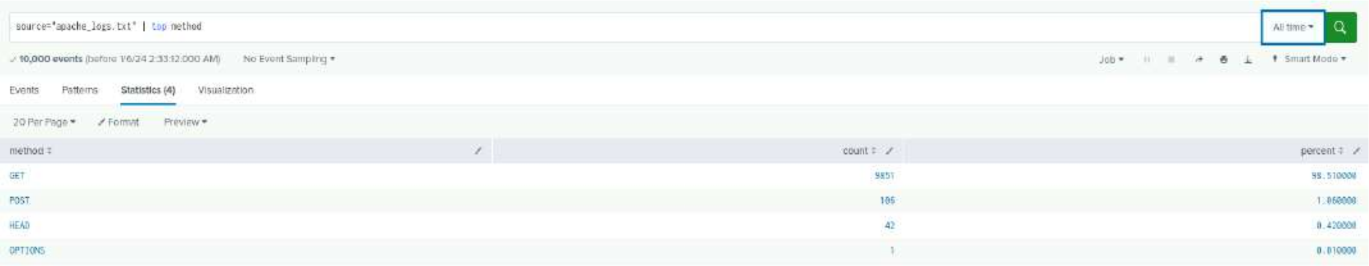
In this part, you will create reports, alerts, and dashboards to monitor for suspicious activity against VSI's Apache web server. To do so, complete the following steps:

1. Design the following deliverables to protect VSI from potential attacks by JobeCorp:

    - **Reports:** Design the following **reports** to assist VSI in quickly identifying specific information (make sure to grab screenshots of each report):

        a. A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc.).

        - This will provide insight into the type of HTTP activity being requested against VSI's web server.



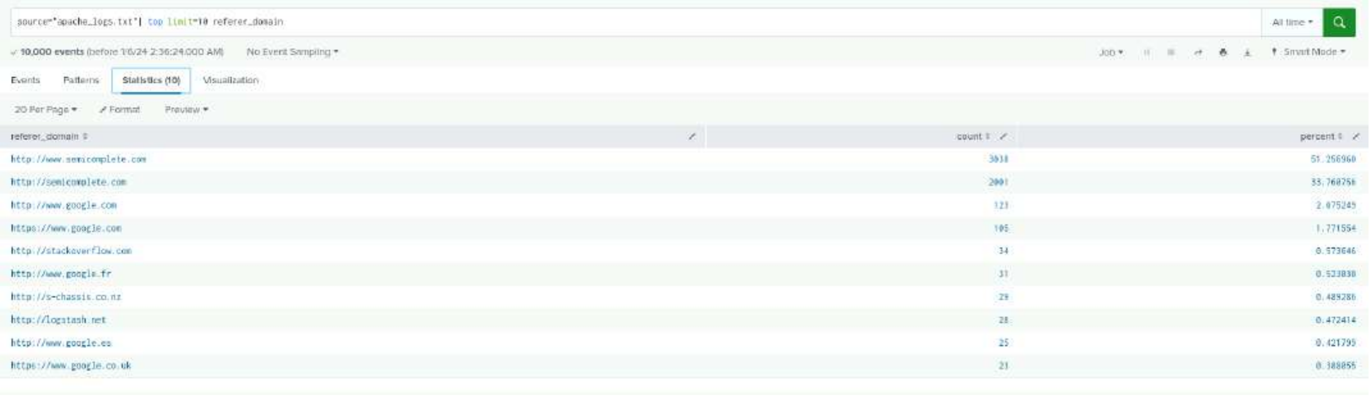
```
source="apache_logs.txt" | top method
```

✓ 10,000 events (before 1/6/24 2:33:12.000 AM)

method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000

        b. A report that shows the top 10 domains that refer to VSI's website.

        - This will assist VSI with identifying suspicious referrers.



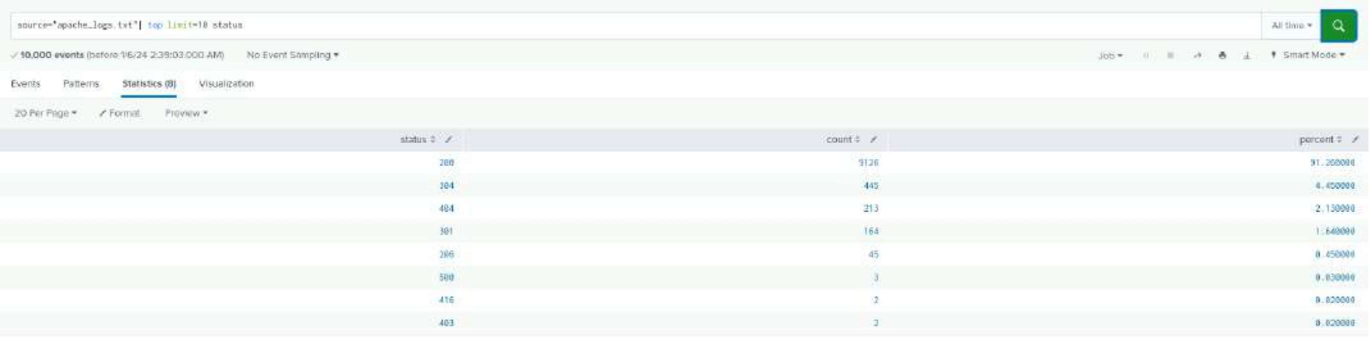
```
source="apache_logs.txt"| top limit=10 referer_domain
```

✓ 10,000 events (before 1/6/24 2:36:24.000 AM)

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421798
https://www.google.co.uk	23	0.388055

c. A report that shows the count of each HTTP response code.

- This will provide insight into any suspicious levels of HTTP responses.



```
source="apache_logs.txt"| top limit=10 status
```

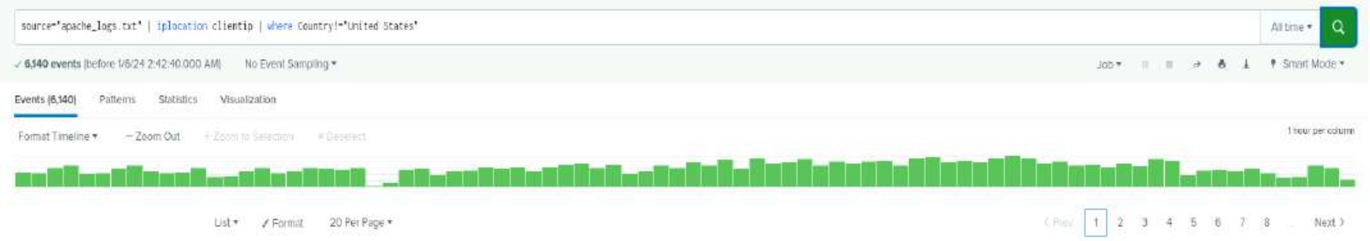
✓ **10,000 events** (before 1/6/24 2:39:03.000 AM)

status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

○ **Alerts:** Design the following **alerts**:

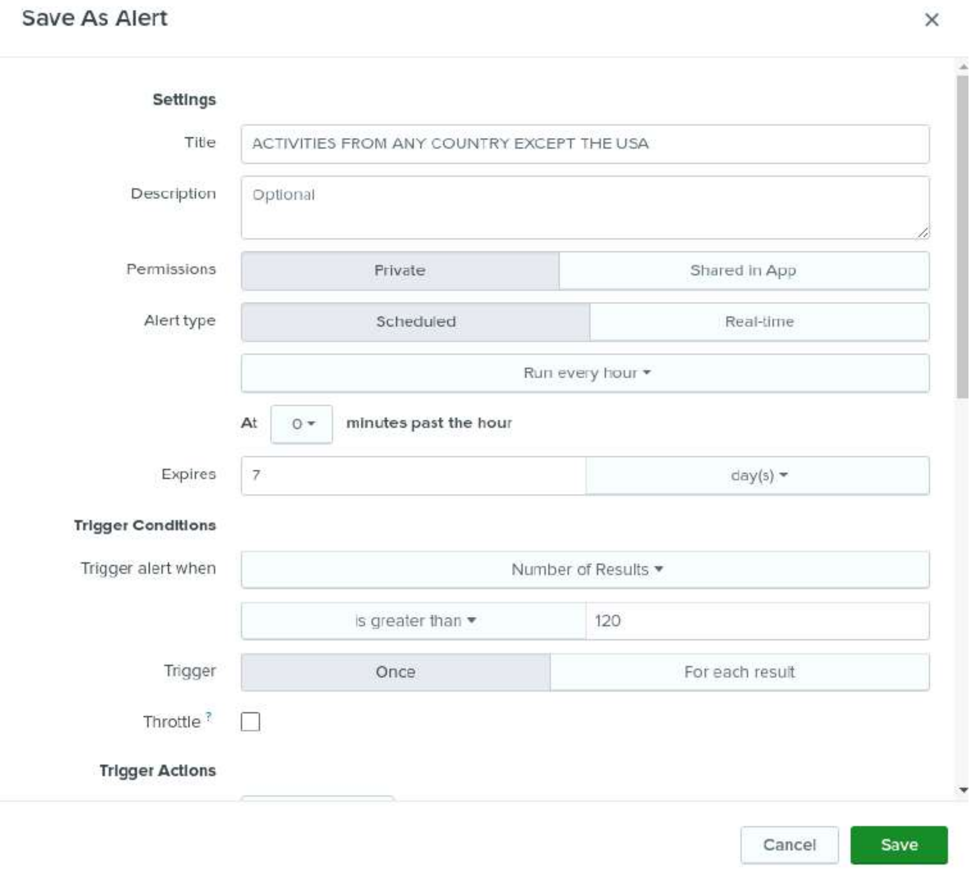
a. Determine a baseline and threshold for hourly activity from any country besides the United States.

- Create an alert that's triggered when the threshold has been reached.
- The alert should trigger an email to SOC@VSI-company.com.



```
source="apache_logs.txt" | iplocation clientip | where Country!="United States"
```

✓ **6,140 events** (before 1/6/24 2:42:40.000 AM)



Save As Alert ×

Settings

Title: ACTIVITIES FROM ANY COUNTRY EXCEPT THE USA

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

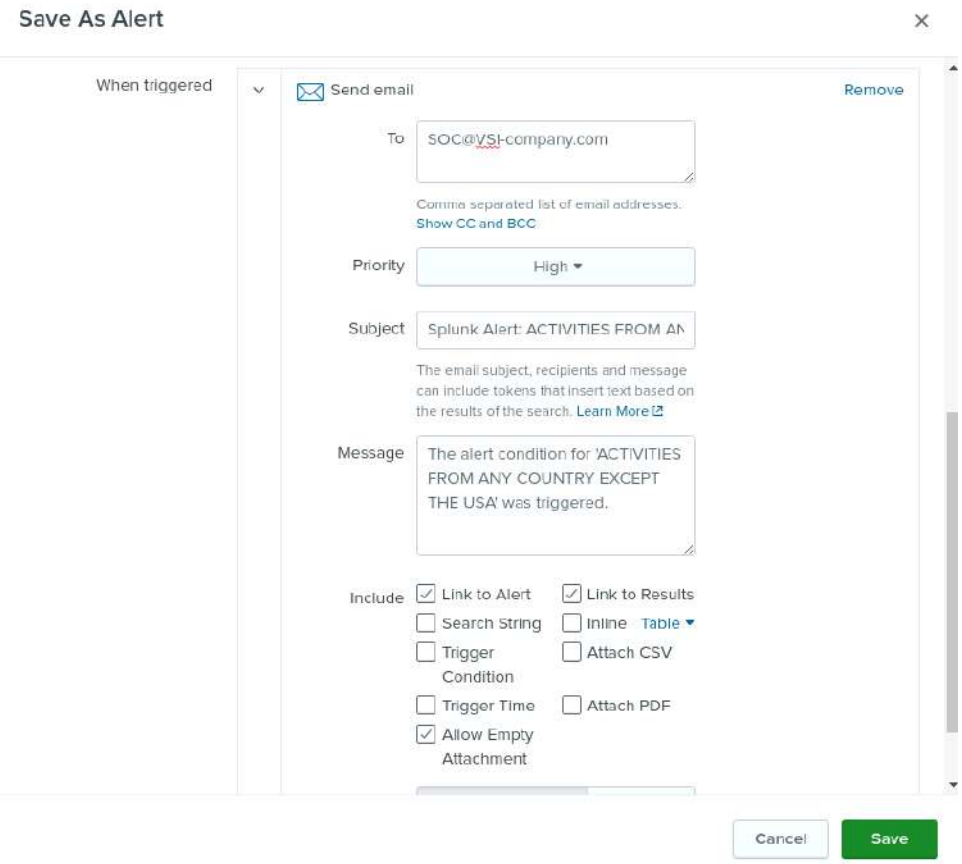
Trigger alert when: Number of Results ▾

is greater than ▾ 120

Trigger: [✓ Once] For each result

Throttle ? □

Trigger Actions



Save As Alert ×

When triggered: Send email — Remove

To: SOC@VSI-company.com

Comma separated list of email addresses.
Show CC and BCC

Priority: High ▾

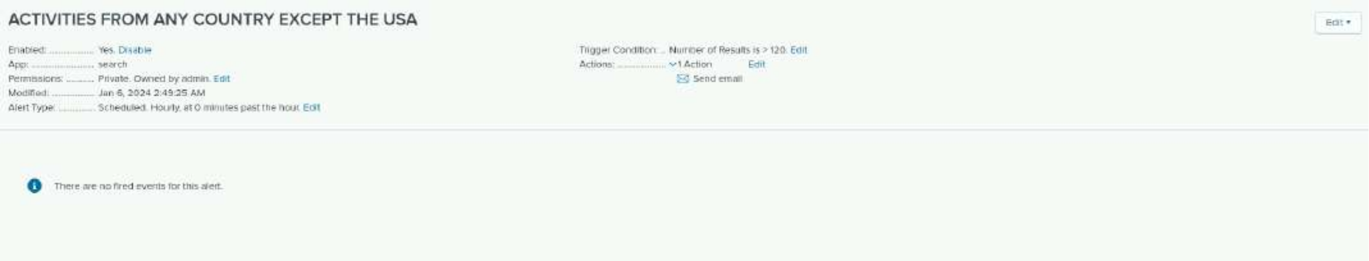
Subject: Splunk Alert: ACTIVITIES FROM AN

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 'ACTIVITIES FROM ANY COUNTRY EXCEPT THE USA' was triggered.

Include:

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



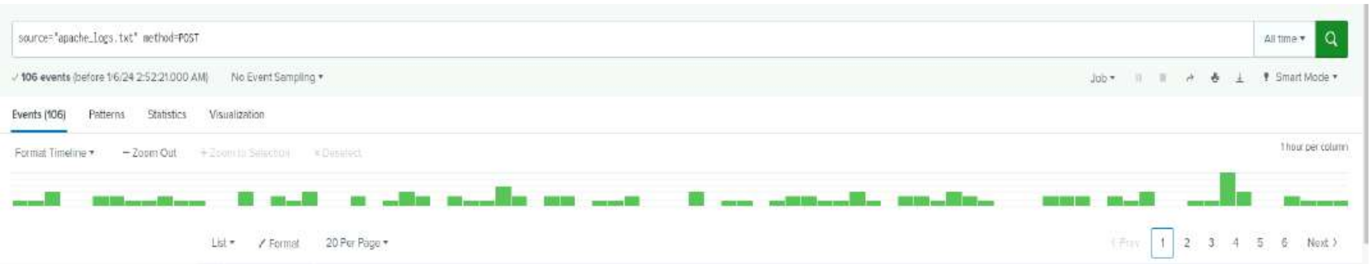
ACTIVITIES FROM ANY COUNTRY EXCEPT THE USA

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jan 6, 2024 2:49:25 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 120. Edit
Actions: .... ⌄1 Action Edit
Send email

There are no fired events for this alert.

- Determine an appropriate baseline and threshold for the hourly count of the HTTP POST method.
    - Create an alert that’s triggered when the threshold has been reached.
    - The alert should trigger an email to SOC@VSI-company.com.

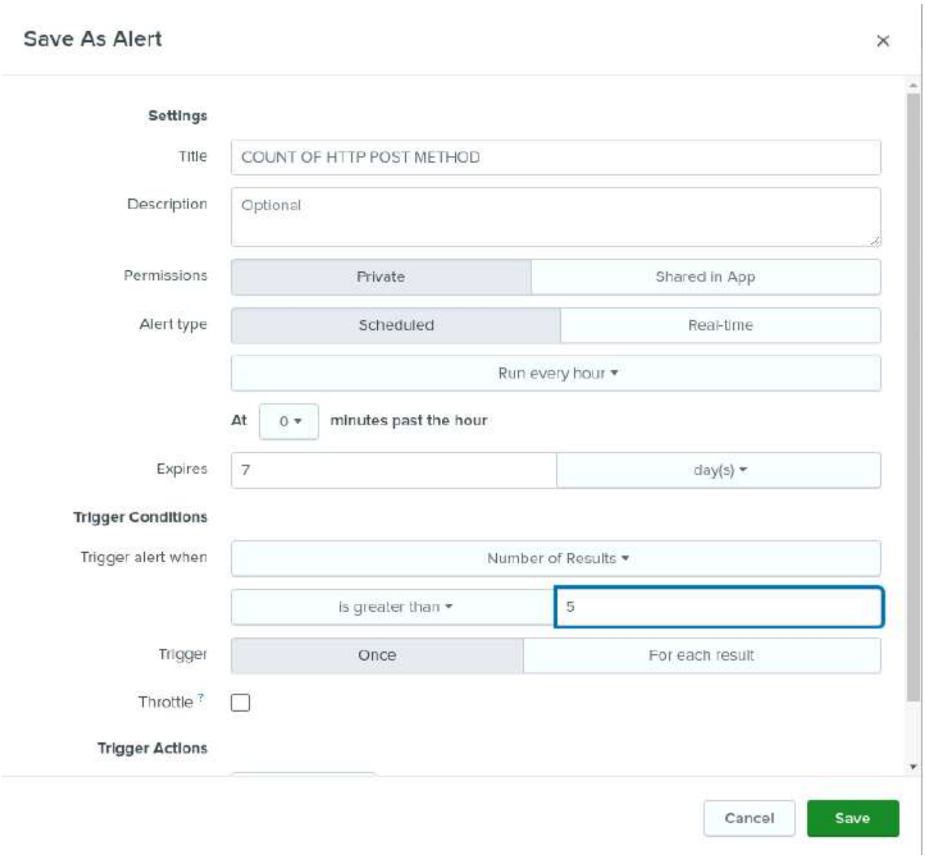


```
source="apache_logs.txt" method=POST
```

✓ 106 events (before 1/6/24 2:52:21.000 AM) No Event Sampling ▾

Events (106)

1 hour per column



Save As Alert

Settings

Title: COUNT OF HTTP POST METHOD

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

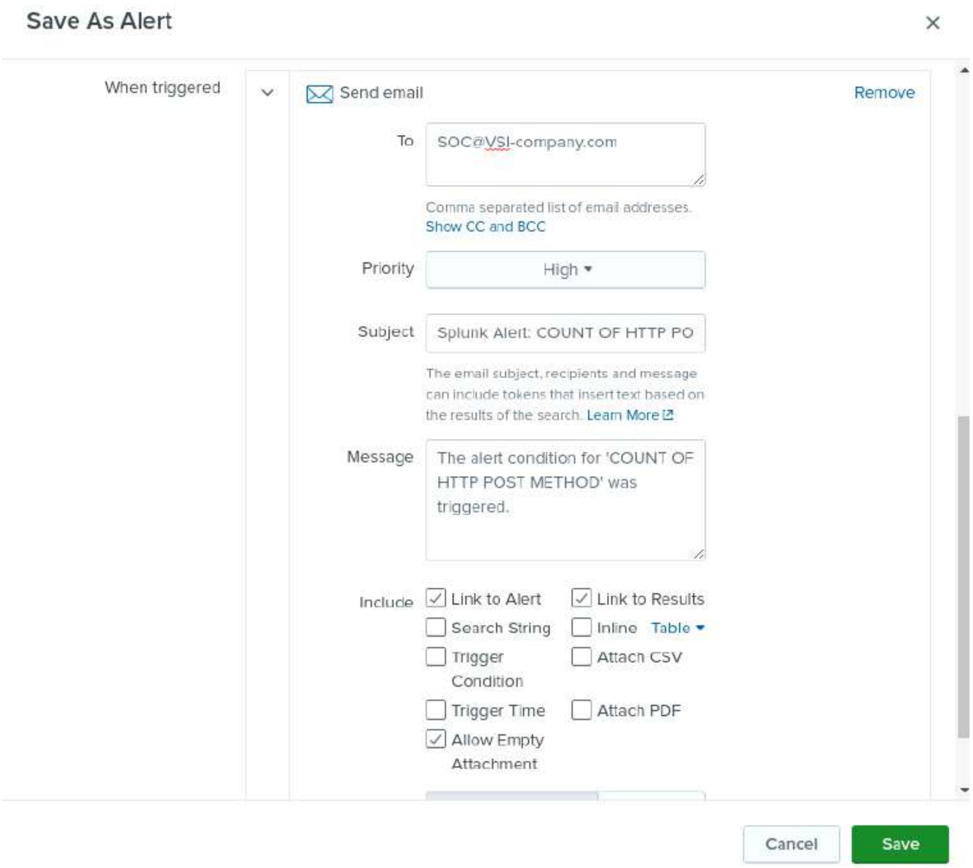
Trigger alert when: Number of Results ▾

is greater than ▾ 5

Trigger: Once | For each result

Throttle ? □

Trigger Actions



Save As Alert

When triggered: Send email

To: SOC@VSI-company.com

Comma separated list of email addresses.
Show CC and BCC

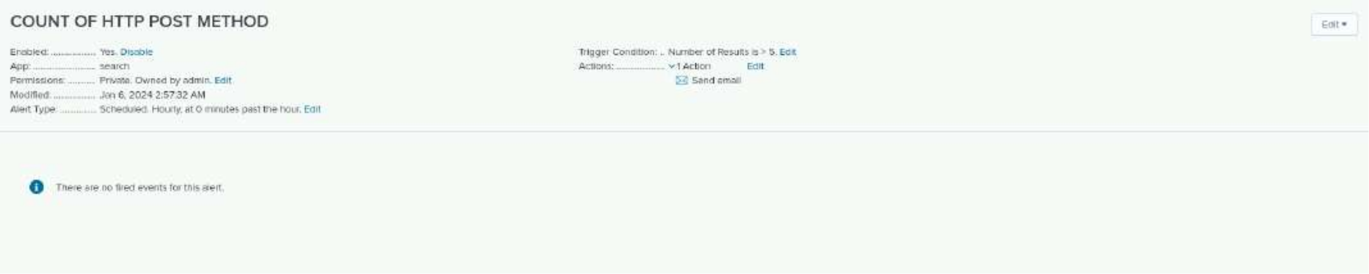
Priority: High ▾

Subject: Splunk Alert: COUNT OF HTTP PO

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 'COUNT OF HTTP POST METHOD' was triggered.

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



COUNT OF HTTP POST METHOD

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jan 6, 2024 2:57:32 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

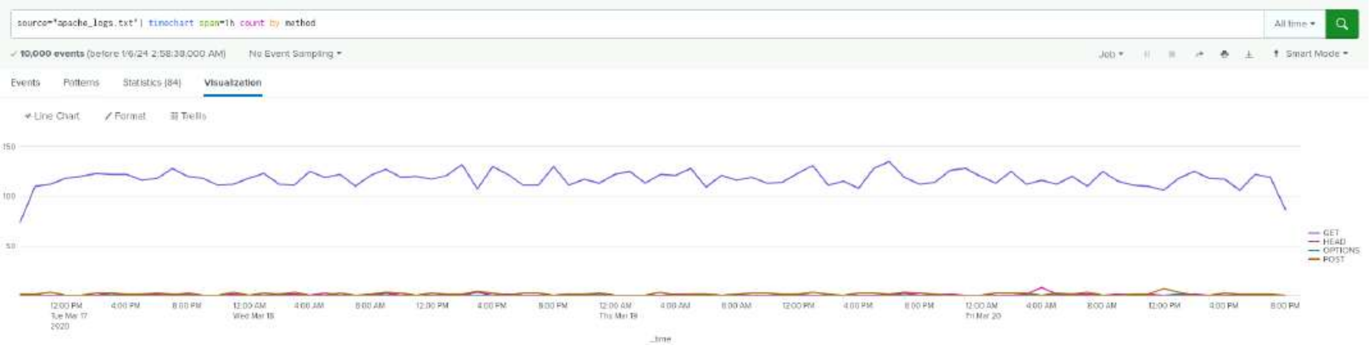
Trigger Condition: .. Number of Results is > 5. Edit
Actions: .... ∨ 1 Action Edit
Send email

There are no fired events for this alert.

- **Visualizations and dashboards:** Design the following **visualizations**, and add them to a **dashboard** called “Apache Web Server Monitoring” (be creative with your visualizations, and make sure to grab screenshots of each):

  a. A line chart that displays the different HTTP “methods” field values over time.

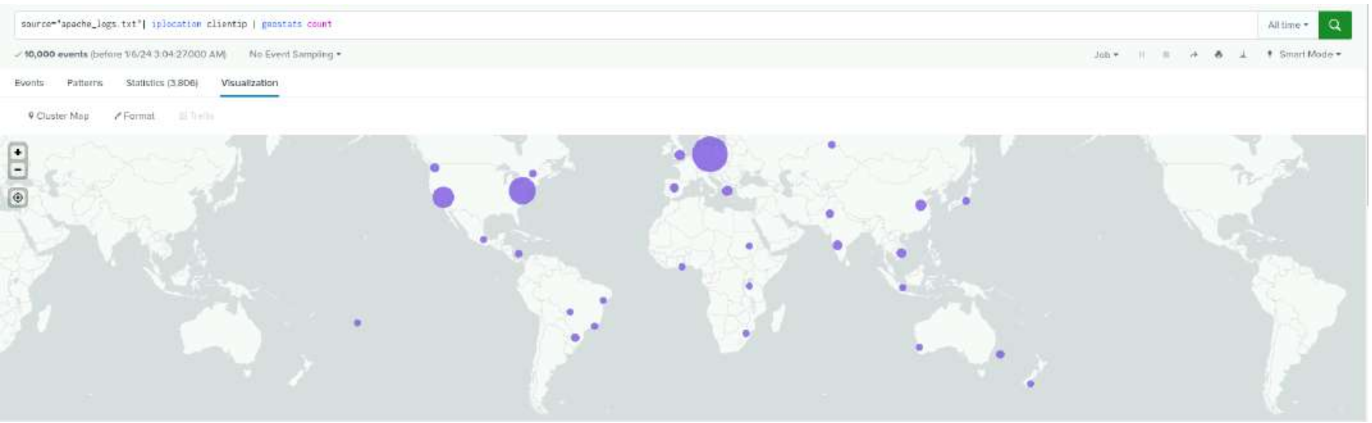
  - **Hint:** Add the following after your search: `timechart span=1h count by method`.



```
source="apache_logs.txt" | timechart span=1h count by method
```

✓ 10,000 events (before 1/6/24 2:58:38.000 AM)

  b. A geographical map showing the location based on the “clientip” field.

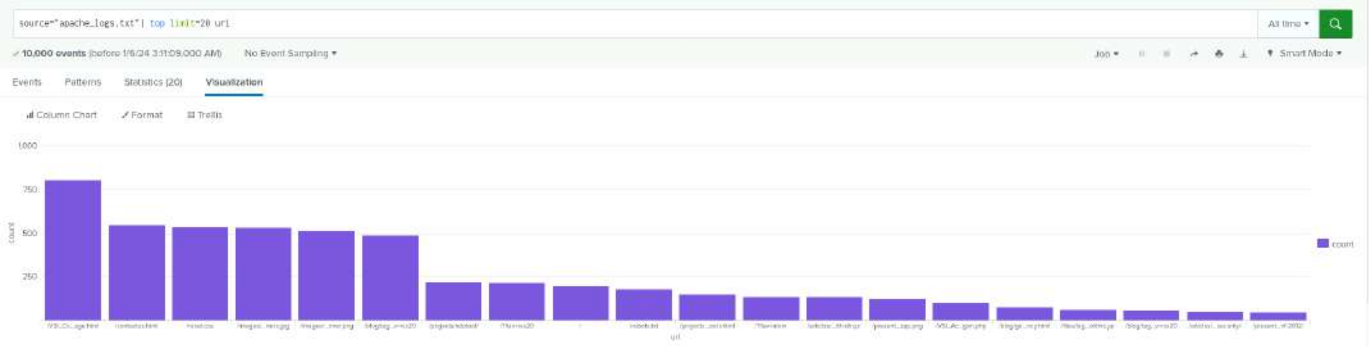


```
source="apache_logs.txt"| iplocation clientip | geostats count
```

✓ 10,000 events (before 1/6/24 3:04:27.000 AM)

c. Any visualization of your choice that displays the number of different URIs.

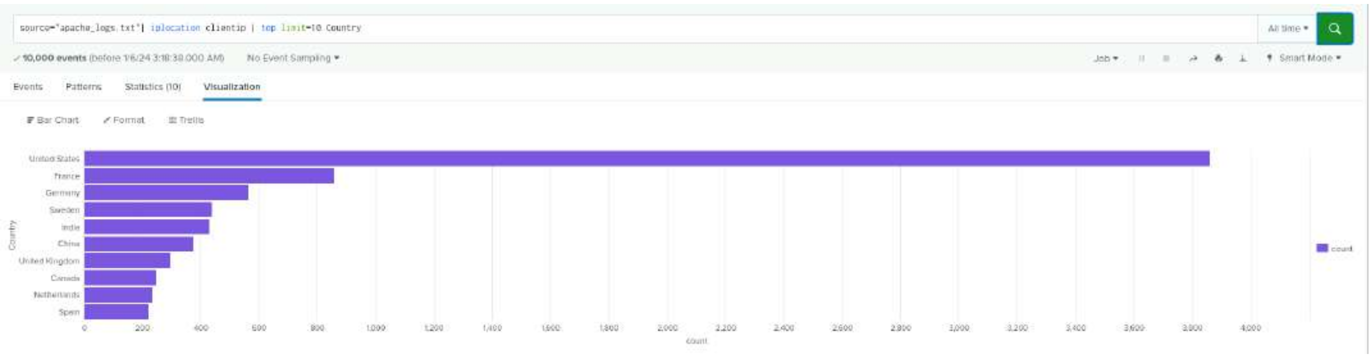
   - **Hint:** You can add brand-new custom visualizations by accessing this page inside your VM: Additional Viz.



```
source="apache_logs.txt"| top limit=20 uri
```

✓ 10,000 events (before 1/6/24 3:11:09.000 AM) No Event Sampling ▾

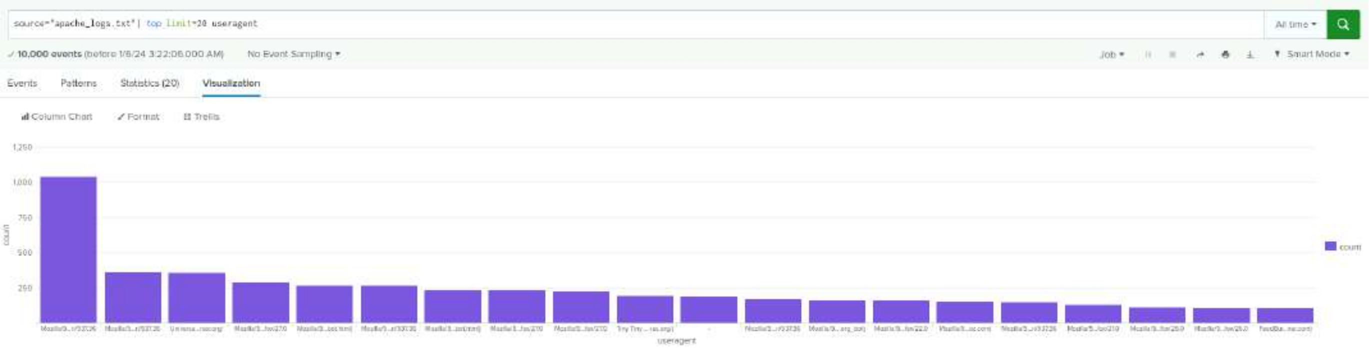
d. Any visualization of your choice that displays the count of the top 10 countries that appear in the log.



```
source="apache_logs.txt"| iplocation clientip | top limit=10 Country
```

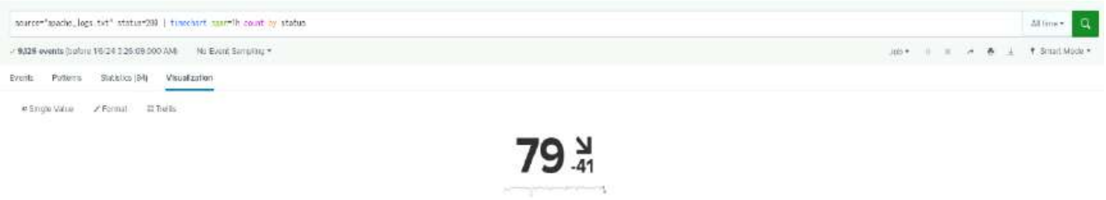
✓ 10,000 events (before 1/6/24 3:18:38.000 AM) No Event Sampling ▾

e. Any visualization that illustrates the count of different user agents.



```
source="apache_logs.txt"| top limit=20 useragent
```

✓ 10,000 events (before 1/6/24 3:22:06.000 AM) No Event Sampling ▾

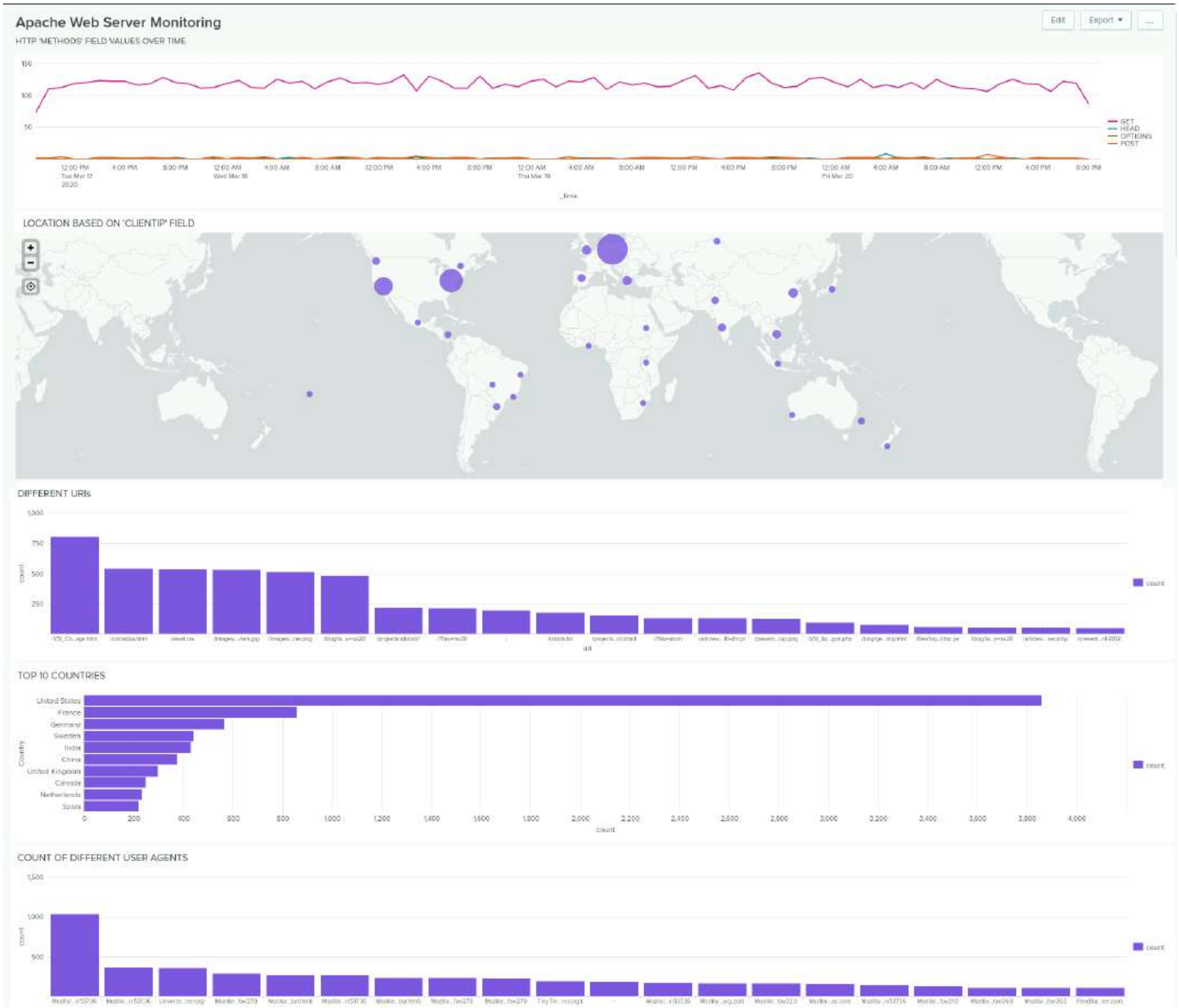


```
source="apache_logs.txt" status=200 | timechart span=1h count by status
```

✓ 9,326 events (before 1/6/24 3:26:09.000 AM) No Event Sampling ▾

f. A single-value visualization of your choice that analyzes any single data point: e.g., radial gauge, marker gauge, or a custom visualization.

2. On your dashboard, add the ability to change the time range for all visualizations.
   - Be sure to title all of your panels appropriately.
   - Organize the panels on your dashboard as you see fit.



Apache Web Server Monitoring

HTTP 'METHODS' FIELD VALUES OVER TIME

LOCATION BASED ON 'CLIENTIP' FIELD

DIFFERENT URIs

TOP 10 COUNTRIES

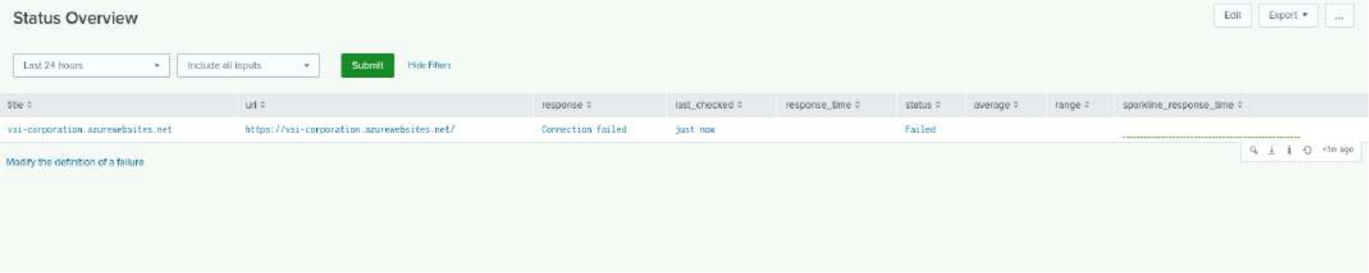
COUNT OF DIFFERENT USER AGENTS

Part 5: Install an Add-On Splunk Application for Additional Monitoring

NOTE: Splunkbase requires a verified email address to access. You will need to log into https://www.splunk.com/ for an email verification prompt. For first time registrations you will need to log out and back in for an e-mail verification prompt.

In this part, your team will choose a Splunk add-on app to provide additional monitoring for VSI's systems. To do so, complete the following steps:

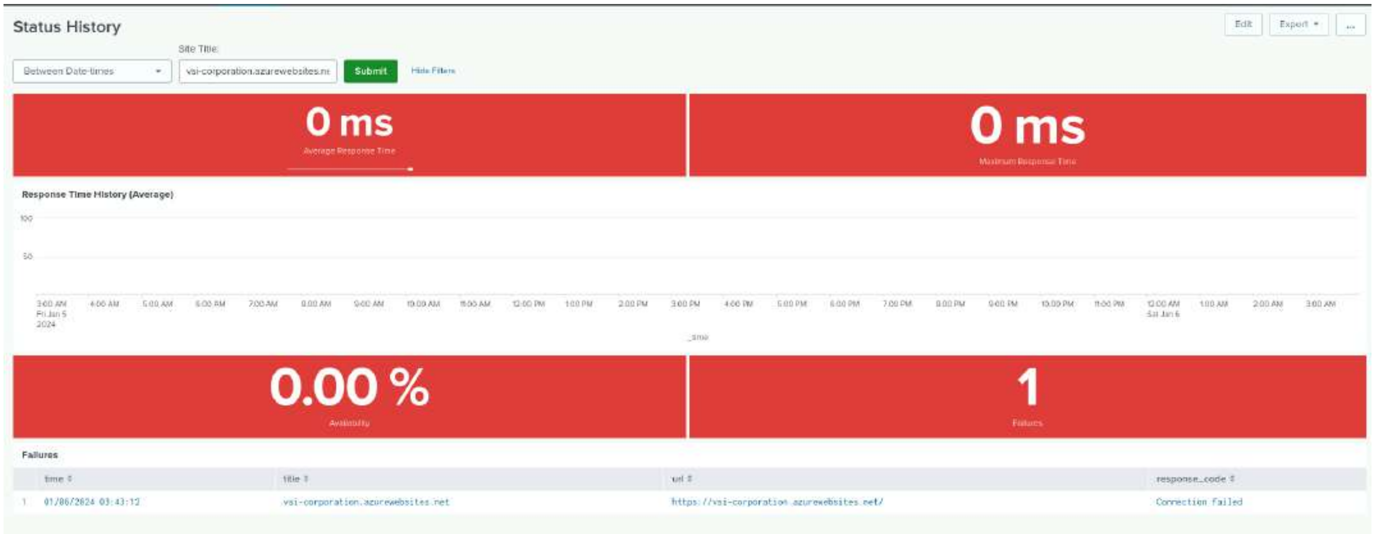
1. First, select any **ONE** of the Splunk add-on apps from https://splunkbase.splunk.com/ to provide additional security monitoring for VSI.
    - You can choose any app from Splunkbase as long as you are able to meet the following requirements:
        - You must be able to install and use the add-on app.
        - You must be able to describe a scenario that illustrates how the app's features will protect VSI.
    - Use the following guide to install your add-on app: Choosing your own add-on app from Splunkbase.
2. You are also welcome to choose one of these Splunk add-on apps with a pre-defined scenario:
    - **Website Monitoring:** App details here **| Install Instructions:** Website Monitoring App
    - **Whois XML IP Geolocation API:** App details here **| Install Instructions:** Whois XML IP Geolocation API
    - **Website Input:** App details here **| Install Instructions:** Website Input
3. **Be sure to grab screenshots of your add-on app!**



Status Overview

title ⇕	url ⇕	response ⇕	last_checked ⇕	response_time ⇕	status ⇕	average ⇕	range ⇕	sparkline_response_time ⇕
vsi-corporation.azurewebsites.net	https://vsi-corporation.azurewebsites.net/	Connection failed	just now		Failed			

Modify the definition of a failure



Status History

Site Title: vsi-corporation.azurewebsites.ne

0 ms
Average Response Time

0 ms
Maximum Response Time

Response Time History (Average)

0.00 %
Availability

1
Failures

Failures

	time ⇕	title ⇕	url ⇕	response_code ⇕
1	01/06/2024 03:43:12	vsi-corporation.azurewebsites.net	https://vsi-corporation.azurewebsites.net/	Connection failed

Cybersecurity

Activity Guide

Monitoring and Analyzing Attacks

Today, you will determine whether your monitoring solution protected VSI. Specifically, you will:

1. **Load Windows attack logs.**
2. **Analyze Windows attack logs.**
3. **Load Apache attack logs.**
4. **Analyze Apache attack logs.**
5. **Create project presentations.**

Resources

- Splunkbase
- Splunk Documentation
- Splunk Add-Ons Guide

Instructions

Welcome to Day 2 of your Defensive Security project!

Part 1: Load Windows Attack Logs

In this first part, you will upload Windows attack logs into your Splunk environment. To do so, complete the following steps:

1. Select the “Add Data” option within Splunk.
2. Since you will upload the provided log file, select the “Upload” option.
   - Click “Select File.”
   - Select the `windows_server_attack_logs.csv` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory.
   - Click the green “Next” button on the top right.

Part 2: Analyze Windows Attack Logs

In this part, you will review the reports, alerts, and dashboards that you created on Day 1 and analyze the results. To do so, complete the following steps:

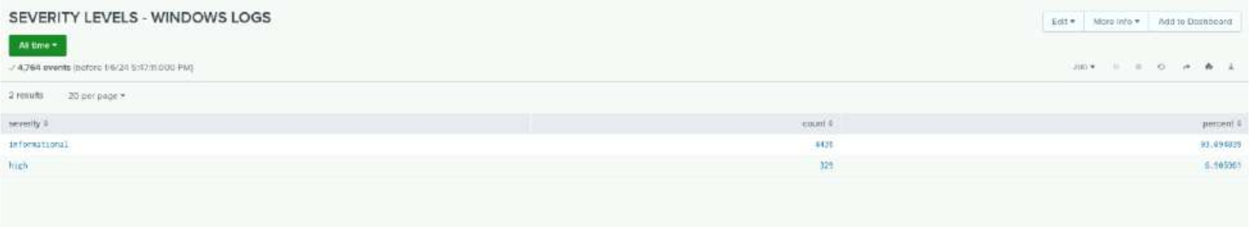
Report Analysis for Severity

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that you created to analyze the different severities.
3. Select “Open in Search.”
4. Take note of the percentages of different severities.
5. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
6. Select “Save.”
7. Review the updated results, and answer the following question in the Project 3 Review Questions document:
   - Did you detect any suspicious changes in severity?

Note: You will use this same document for the remaining review questions.

Report Analysis for Failed Activities

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that you created to analyze the different activities.
3. Select “Open in Search.”
4. Take note of the failed activities percentage.
5. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
6. Select “Save.”

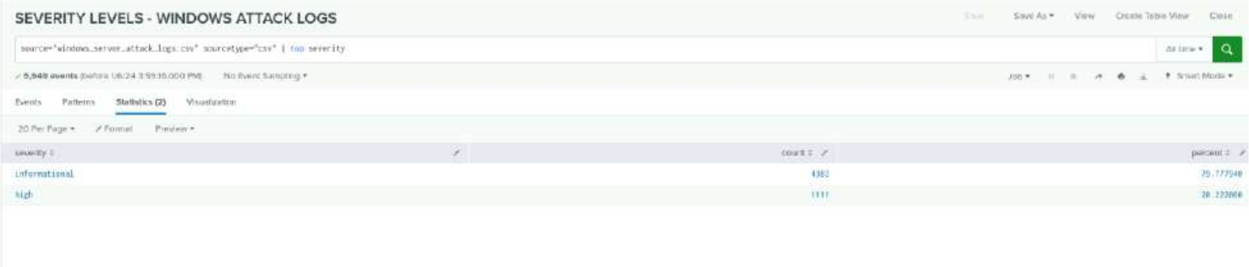


SEVERITY LEVELS - WINDOWS LOGS

✓ 4,764 events (before 1/6/24 5:47:11.000 PM)

2 results

severity	count	percent
informational	4435	93.094039
high	329	6.905961



SEVERITY LEVELS - WINDOWS ATTACK LOGS

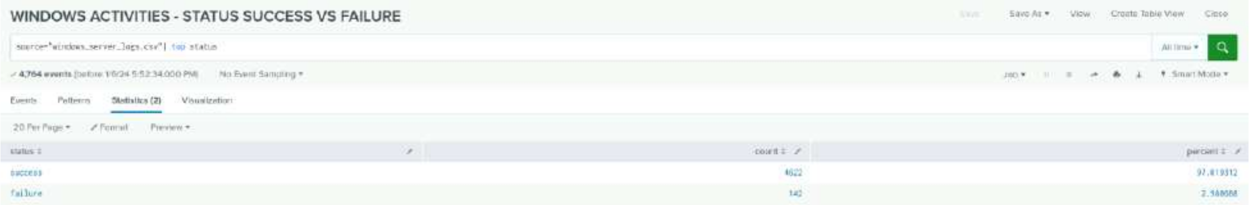
```
source="windows_server_attack_logs.csv" sourcetype="csv" | top severity
```

✓ 5,494 events (before 1/6/24 3:59:18.000 PM)

severity	count	percent
informational	4383	79.777940
high	1111	20.222060

Severity levels from the attack logs increased from 329 to 1111 for ‘high’ severity (around 13.3%). ‘Informational’ slightly increased from 4383 to 4435 (around 13.3%).

7. Review the updated results, and answer the following question in the review document:
    - ○ Did you detect any suspicious changes in failed activities

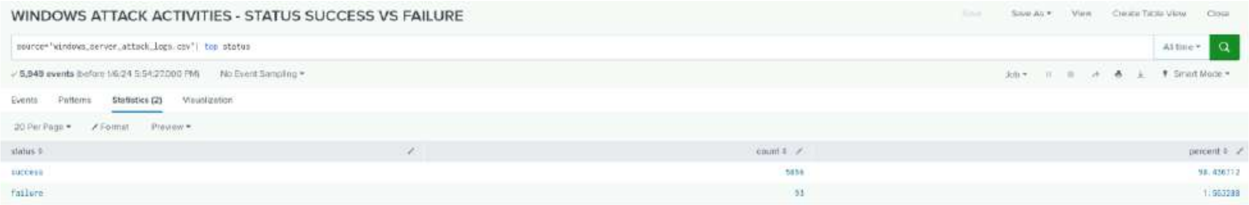


WINDOWS ACTIVITIES - STATUS SUCCESS VS FAILURE

```
source="windows_server_logs.csv"| top status
```

✓ 4,764 events (before 1/6/24 5:52:34.000 PM)

status	count	percent
success	4622	97.019312
failure	142	2.980688



WINDOWS ATTACK ACTIVITIES - STATUS SUCCESS VS FAILURE

```
source="windows_server_attack_logs.csv"| top status
```

✓ 5,949 events (before 1/6/24 5:54:27.000 PM)

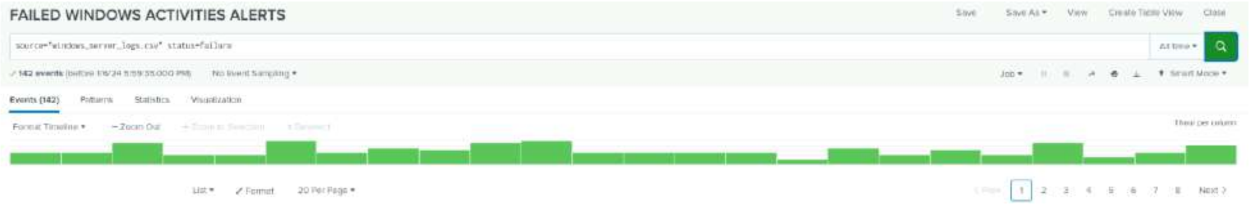
status	count	percent
success	5856	98.436712
failure	93	1.563288

Success rate increased from 97% to 98%, while failure rate reduced from approximately 2.9% to 1.5%.

Now, you will review the alerts that you created on Day 1 and analyze the results.

Alert Analysis for Failed Windows Activity

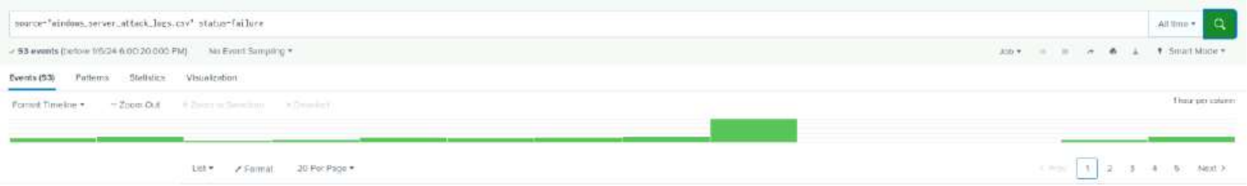
1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of failed activities.
3. Select “Open in Search.”
4. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.



FAILED WINDOWS ACTIVITIES ALERTS

```
source="windows_server_logs.csv" status=failure
```

✓ 142 events (before 1/6/24 5:59:35.000 PM)



```
source="windows_server_attack_logs.csv" status=failure
```

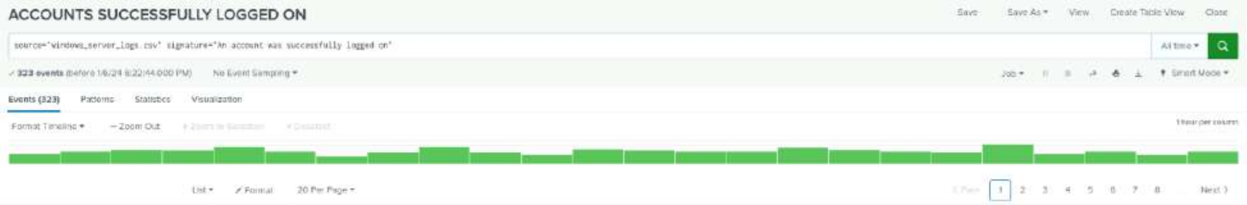
✓ 93 events (before 1/5/24 6:00:20.000 PM)

5. Review the updated results, and answer the following questions in the review document (*note that your alerts will not trigger; this is a theoretical exercise*):
    - ○ Did you detect a suspicious volume of failed activity?
    - ○ If so, what was the count of events in the hour(s) it occurred?
    - ○ When did it occur?
    - ○ Would your alert be triggered for this activity?
    - ○ After reviewing, would you change your threshold from what you previously selected?

On March 25, 2020 at 8:00 AM, there was a high rate of login failures (35 events), which is a lot more than the threshold of 10 events. This would have triggered the ‘Failed Windows Activities alert’ which had a threshold of 10. I would not change the threshold, as it alerted us to suspicious activity (Not false positive).

Alert Analysis for Successful Logins

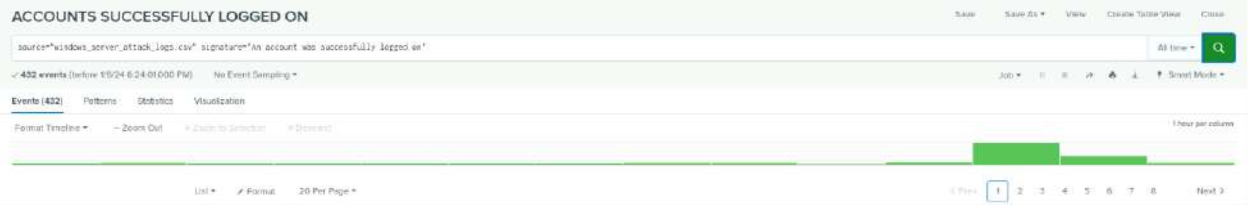
1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of successful logins.
3. Select “Open in Search.”
4. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.



ACCOUNTS SUCCESSFULLY LOGGED ON

```
source="windows_server_logs.csv" signature="An account was successfully logged on"
```

✓ 323 events (before 1/6/24 8:22:44.000 PM)



ACCOUNTS SUCCESSFULLY LOGGED ON

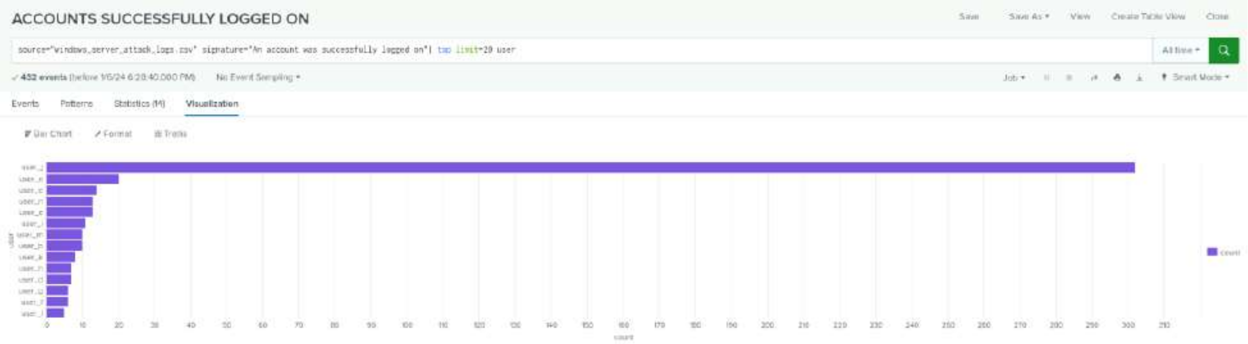
```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on"
```

✓ 432 events (before 1/5/24 6:24:01.000 PM) No Event Sampling ▾

Events (432)

5. Review the updated results, and answer the following questions in the review document:
   - ○ Did you detect a suspicious volume of successful logins?
   - ○ If so, what was the count of events in the hour(s) it occurred?
   - ○ Who is the primary user logging in?
   - ○ When did it occur?
   - ○ Would your alert be triggered for this activity?
   - ○ After reviewing, would you change your threshold from what you previously selected?

On March 25, 2020 at 11:00 AM, there was a high rate of successfully logged on accounts (196 events) and 77 events at 12PM, which are a lot more than the threshold of 20 events set. This would have triggered the ‘ACCOUNTS SUCCESSFULLY LOGGED ON’ alert which had a threshold of 20. I would not change the threshold, as it alerted us to suspicious activity (Not false positive).



ACCOUNTS SUCCESSFULLY LOGGED ON

```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on"| top limit=20 user
```

✓ 432 events (before 1/5/24 6:28:40.000 PM) No Event Sampling ▾

Statistics (14)

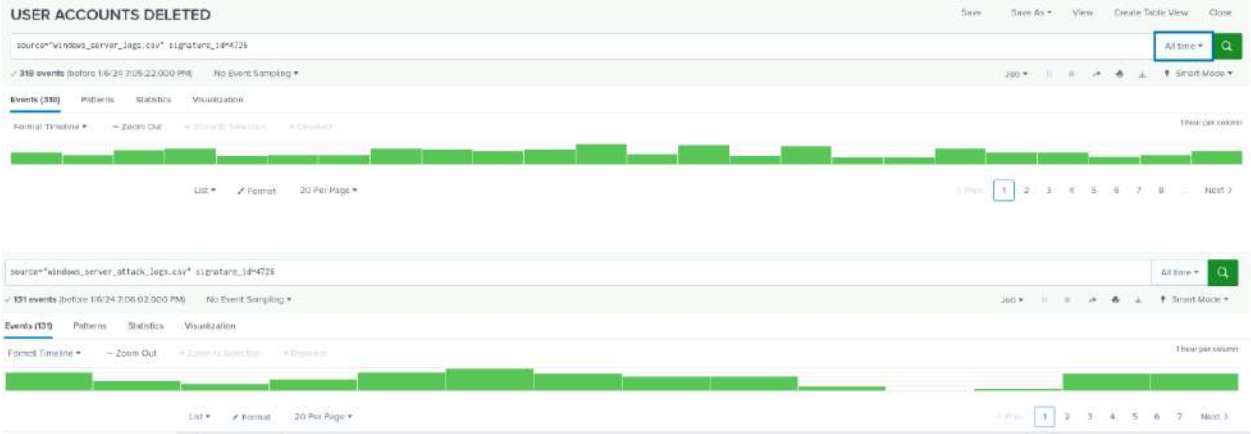
According to the above, the primary user logging in is user j.

Alert Analysis for Deleted Accounts

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.

2. Select the alert for suspicious volume of deleted accounts.
3. Select “Open in Search.”
4. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
5. Review the updated results, and answer the following question in the review document:
    - Did you detect a suspicious volume of deleted accounts?

Next, you will view your dashboard and analyze the results.



USER ACCOUNTS DELETED

```
source="windows_server_logs.csv" signature_id=4726
```

✓ 318 events (before 1/6/24 7:05:22.000 PM)

Events (318)

```
source="windows_server_attack_logs.csv" signature_id=4726
```

✓ 131 events (before 1/6/24 7:06:02.000 PM)

Events (131)

After reviewing the events, there was no suspicious activity detected. This would not have triggered the ‘USER ACCOUNTS DELETED’ alert which had a threshold of 18. I would not change the threshold.

Dashboard Setup

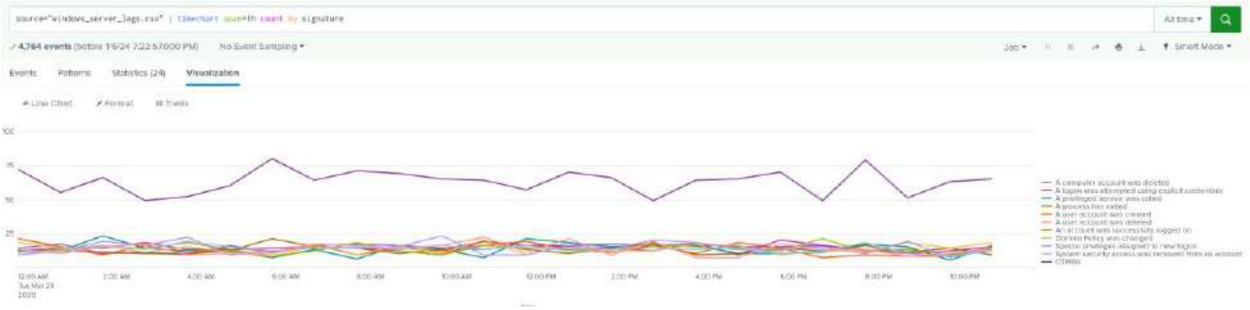
1. Access the Windows Web Server Monitoring dashboard.
    - Select “Edit.”
2. For each panel that you created, access the panel and complete the following steps:
    - Select “Edit Search.”
    - Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
    - Select “Apply.”
    - Save the dashboard.

- Change the time on the whole dashboard to “All Time.”

Dashboard Analysis for Time Chart of Signatures

Analyze your new dashboard results, and answer the following questions in the review document:

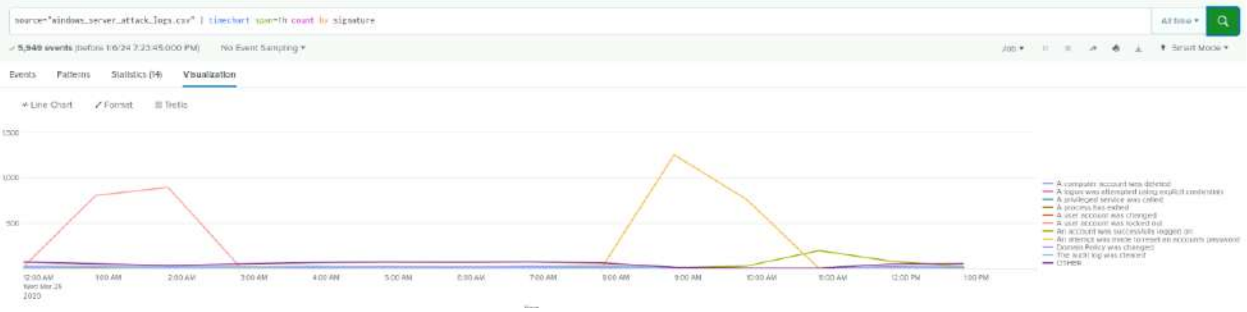
- Does anything stand out as suspicious?
- What signatures stand out?
- What time did each signature’s suspicious activity begin and stop?
- What is the peak count of the different signatures?



```
source="windows_server_logs.csv" | timechart span=1h count by signature
```

✓ 4,764 events (before 1/6/24 7:22:57.000 PM) No Event Sampling ▾

All time ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (24)
Visualization
Line Chart
Format
Trellis
100
75
50
25
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER



```
source="windows_server_attack_logs.csv" | timechart span=1h count by signature
```

✓ 5,949 events (before 1/6/24 7:23:45.000 PM) No Event Sampling ▾

All time ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (14)
Visualization
Line Chart
Format
Trellis
1,500
1,000
500
12:00 AM
Wed Mar 25
2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was changed
A user account was locked out
An account was successfully logged on
An attempt was made to reset an accounts password
Domain Policy was changed
The audit log was cleared
OTHER

Dashboard Analysis for Users

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?

“A user account was locked out” peaked on March 25, 2020 at 1:00 AM at 805 events and at 2:00 AM at 896 events.

“An attempt was made to resent accounts password” peaked on March 25, 2020 at 9:00 AM at 1258 events and at 10:00 AM at 761 events.

“An account successfully logged” on March 25, 2020 at 11:00 AM with 196 events and at 12:00 PM at 77 events.

- Which users stand out?

“A user account was locked out” signature stands out for suspicious activity.

“An attempt was made to reset an accounts password” signature stands out for suspicious activity.

“An account was successfully logged on” stands out for suspicious activity.

- What time did each user’s suspicious activity begin and stop?

“A user account was locked out” peaked on March 25, 2020 at 1:00 AM at 805 events and at 2:00 AM at 896 events. The suspicious activity stopped at 3:00 AM on March 25, 2020.

“An attempt was made to resent accounts password” peaked on March 25, 2020 at 9:00 AM at 1258 events and at 10:00 AM at 761 events. The suspicious activity stopped at 11:00 AM on March 25, 2020.

“An account successfully logged” on March 25, 2020 at 11:00 AM with 196 events and at 12:00 PM at 77 events. The suspicious activity stopped at 1:00 PM on March 25, 2020.

Cybersecurity

Project 3 Review Questions

Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes. Suspicious changes in severity between windows server logs to windows server attack logs:

‘High’ drastically increased from 329 events to 1111 events. This is an increase from 7% to 20%.

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes, there was an increase on March 25, 2020 at 8:00 AM at 35 events.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes, there was an increase on March 25, 2020 - from 8 events at 7:00 AM to 35 events at 8:00 AM.

- If so, what was the count of events in the hour(s) it occurred?

```
March 25, 2020 at 8:00 AM at 35 events
```

- When did it occur?

```
March 25, 2020 at 8:00 AM
```

- Would your alert be triggered for this activity?

```
Yes, this would have triggered my alert that was set at a threshold of 10
events.
```

- After reviewing, would you change your threshold from what you previously selected?

```
No, I would not change my threshold. It correctly alerted me to suspicious
activity. Furthermore, historical data shows that previous events have not
surpassed 10.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes. On March 25, 2020 at 11:00 AM and 12:00 PM
```

- If so, what was the count of events in the hour(s) it occurred?

```
On March 25, 2020, there were 196 events at 11:00 AM and 77 events at 12:00
PM
```

- Who is the primary user logging in?

```
User_j
```

- When did it occur?

On March 25, 2020, there were 196 events at 11:00 AM and 77 events at 12:00 PM

- Would your alert be triggered for this activity?

Yes, this would have triggered my alert that had a threshold of 20 events.

- After reviewing, would you change your threshold from what you previously selected?

No, I would not change my threshold. It correctly alerted me to suspicious activity. Furthermore, historical data shows that previous events have not surpassed 20. At 10:00 AM, there were 23 events by user_j which would have alerted me to the start of an attack.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

3 events occurred at 9:00 AM, 0 events occurred at 10:00 AM and 1 event occurred at 11:00 AM on March 25, 2020. This is way below the benchmark of 20 based on historical data.

Based on historical data, there is an average number of approximately 14 events per hour. 0-3 events are way below this.

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes

- What signatures stand out?

Signatures that stand out:

```
- A user account was locked out
- An attempt was made to reset an accounts password
- An account was successfully logged on
```

- What time did it begin and stop for each signature?

```
- A user account was locked out: Wednesday, March 25, 2020 at 12:00 AM to
3:00 AM

- An attempt was made to reset an accounts password: Wednesday March 25,
2020 at 8:00 AM to 11:00 AM

- An account was successfully logged on: Wednesday, March 25, 2020 at 10:00
AM to 1:00 PM
```

- What is the peak count of the different signatures?

```
- A user account was locked out: 896 events
- An attempt was made to reset an accounts password: 1258 events
- An account was successfully logged on: 196 events
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes
```

- Which users stand out?

```
- User_a
- User_k
- User_j
```

- What time did it begin and stop for each user?

```
- User_a: Wednesday, March 25, 2020 at 12:00 AM to 3:00 AM
- User_k: Wednesday, March 25, 2020 at 8:00 AM to 11:00 AM
- User_j: Wednesday, March 25, 2020 at 10:00 AM to 1:00 PM
```

- What is the peak count of the different users?

```
- User_a: 984 events
- User_k: 1256 events
- User_j: 196 events
```

Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

```
Yes
```

- Do the results match your findings in your time chart for signatures?

```
No.

- A user account was locked out: 1811 events
- An attempt was made to reset an accounts password: 2128 events
- An account was successfully logged on: 432 events
```

Dashboard Analysis for Users with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

```
Yes
```

- Do the results match your findings in your time chart for users?

```
No.

- User_a: 1878 events
- User_k: 2118 events
- User_j: 398 events
```

Dashboard Analysis for Users with Statistical Charts

- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

```
source="windows_server_attack_logs.csv" | top user

Advantages:
-Quick Identification: Easily identifies the most frequently occurring
users, helping you quickly spot high-impact or suspicious activities.
-Simplicity: Simple and straightforward query for a quick overview.

Disadvantages:
-Lack of Context: Doesn't provide information about when these events
occurred or how they've changed over time.
-Limited Details: Only shows the top users without additional details on the
distribution or patterns.

source="windows_server_logs.csv" | timechart span=1h count by user

Advantages:
-Temporal Insight: Provides a time-based perspective, allowing you to see
how user activity changes over hourly intervals.
-Patterns and Trends: Helps in identifying patterns, trends, and anomalies
in user behavior over time.

Disadvantages:
-Less Immediate: May require more time to analyze compared to a simple top
list.
-Complexity: The timechart introduces a level of complexity, especially for
those who are not familiar with time-based visualizations.

For a quick snapshot of the most common users, the first report may suffice.
To understand how user activity evolves over time and detect temporal
patterns, the second report provides a more comprehensive view.
```

Apache Web Server Log Questions

Report Analysis for Methods

- Did you detect any suspicious changes in HTTP methods? If so, which one?

```
Yes, high increase in POST requests. This increased by 28%, while GET
requests reduced by 28%.
```

- What is that method used for?

```
POST - A POST request in HTTP is a method employed to send information from
a client to a web server, commonly utilized for tasks such as form
submissions or creating data on the server.

GET - An HTTP GET request is a way for a client to request data from a web
server by specifying parameters in the URL, typically used for retrieving
information without modifying anything on the server.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
No suspicious activity detected
```

Report Analysis for HTTP Response Codes

- Did you detect any suspicious changes in HTTP response codes?

```
Yes, status 404 increased from 213 to 679, an increase of approximately 13%.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, a suspicious increase in events on March 25, 2020 at 8:00 PM, mostly
originating from Ukraine
```

- If so, what was the count of the hour(s) it occurred in?

```
937 events on March 25, 2020 at 8:00 PM
```

- Would your alert be triggered for this activity?

Yes, my alert would’ve triggered it. This is way above my threshold of 120 events.

- After reviewing, would you change the threshold that you previously selected?

No. My threshold would have correctly alerted me to suspicious activity. This threshold was determined after analyzing historical trends.

Alert Analysis for HTTP POST Activity

- Did you detect any suspicious volume of HTTP POST activity?

Yes, a suspicious increase on March 25, 2020 at 8:00 PM

- If so, what was the count of the hour(s) it occurred in?

1296 events on March 25, 2020 at 8:00 PM

- When did it occur?

Wednesday, March 25, 2020 at 8:00 PM

- After reviewing, would you change the threshold that you previously selected?

No. My threshold of 5 events would have correctly alerted me to suspicious activity. This threshold was determined after analyzing historical trends.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, a suspicious increase in POST and GET requests was noticed.

- Which method seems to be used in the attack?

```
   -  POST
   -  GET
```

- At what times did the attack start and stop?

```
Increase in GET requests started on March 25, 2020 at 5:00 PM to 7:00 PM,
while increase in POST requests began at 7:00 PM to 9:00 PM.
```

- What is the peak count of the top method during the attack?

```
   -  GET: 729 events
   -  POST: 1296 events
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, an increase in activity on March 25, 2020 at 8:00 PM
```

- Which new location (city, country) on the map has a high volume of activity? (**Hint**: Zoom in on the map.)

```
Ukraine, specifically Kiev and Kharkiv
```

- What is the count of that city?

```
   -  Kiev - 440 events
   -  Kharkiv - 432 events
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, increase in activities with the following URIs:
 -  /VSI_Account_logon.php
 -  /files/logstash/logstash-1.3.2-monolithic.jar
```

- What URI is hit the most?

```
 -  /VSI_Account_logon.php: 1323 events

 -  /files/logstash/logstash-1.3.2-monolithic.jar: 638 events
```

- Based on the URI being accessed, what could the attacker potentially be doing?

```
 -  /VSI_Account_logon.php: Potential brute-force attacks, such as
    credential stuffing or password spraying.

 -  /files/logstash/logstash-1.3.2-monolithic.jar: This could indicate
    attempts to exploit vulnerabilities or perform remote code execution.
```