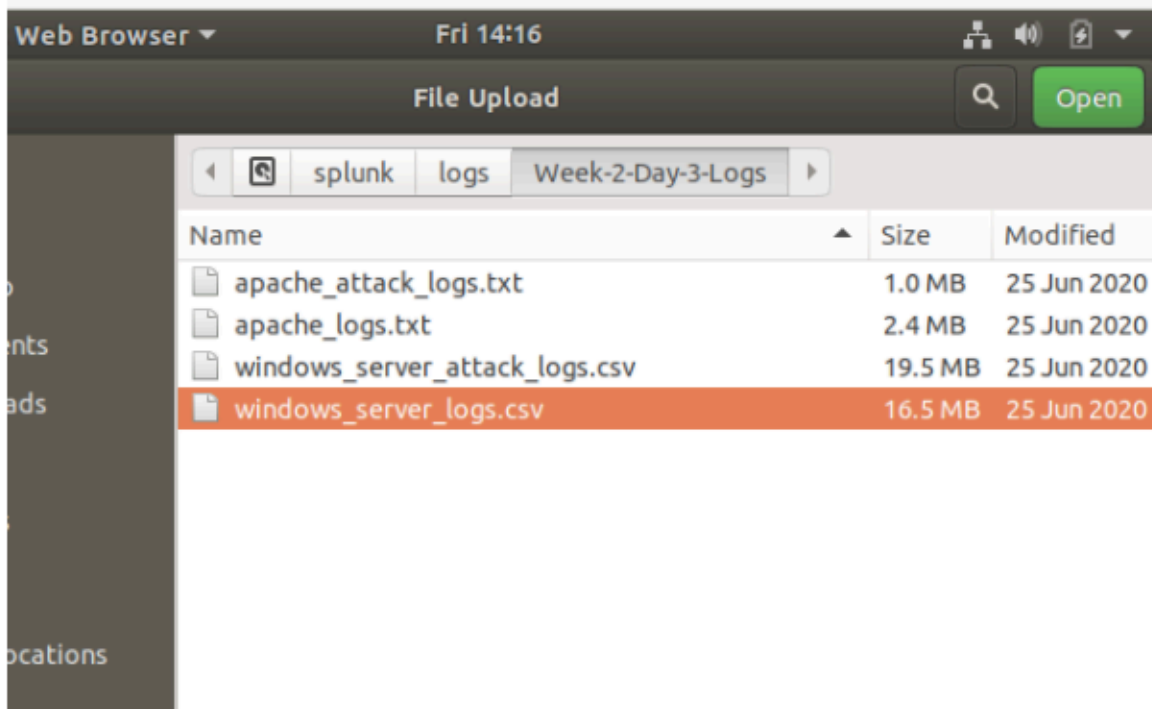


# Windows Event Logs

## 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. 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 under “Or get data in with the following methods.”
  - Then, click “Select File.”
  - Double-click the `windows_server_logs.csv` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory, as the following image shows:



3. You will 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 value, Splunk uses a random value to name the machine or device that generated the logs.
  - Update the value to "Windows\_server\_logs" and then select "Review."
5. On the "Review" page, verify that you've chosen the correct settings.
  - Select "Submit" to proceed with uploading your data into Splunk.

The screenshot shows the Splunk 'New Search' interface. At the top, the search bar contains the query: `source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"`. Below the search bar, it indicates **4,764 events** (before 5/7/25 2:01:47.000 AM) and shows a 'No Event Sampling' dropdown. The interface includes buttons for 'Save As', 'Create Table View', and 'Close'. Below the search bar, there are tabs for 'Events (4,764)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events' tab is active, showing a timeline view with a 'Timeline format' dropdown and a 'Zoom Out' button. The timeline shows a series of green bars representing events. Below the timeline, there are buttons for 'Format', 'Show: 20 Per Page', and 'View: List'. The 'View: List' button is selected, and the interface shows a list of events. The first event is from 3/24/20 at 11:59:54.000 PM, with the event text: `2020-03-24T23:59:54.000+0000,, "Domain_A user_f user_l",,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-4726,A user account was deleted,0,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_AUser_f`. The interface also shows a 'SELECTED FIELDS' section with `host 1`, `source 1`, and `sourcetype 1`, and an 'INTERESTING FIELDS' section with `Account_Domain 2` and `Account_Name 100+`.

- 
6. Once the file has successfully uploaded, a message that says "File has been uploaded successfully" will appear.
  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:
    - signature\_id

signature\_id

15 Values, 100% of events

Selected

Yes

No

Reports

Average over time

Maximum value over time

Minimum value over time

Top values

Top values by time

Rare values

Events with this field

Avg:

4475.4013434089

Min:

1102

Max:

4743

Std Dev:

879.9767461845869

Top 10 Values

Count

%

4672

342

7.179%

4743

340

7.137%

4648

337

7.074%

4739

329

6.906%

4624

323

6.78%

4718

321

6.738%

4726

318

6.675%

4673

317

6.654%

4720

313

6.57%

4689

309

6.486%

○ Signature

signature

15 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values	Count	%
Special privileges assigned to new logon	342	7.179%
A computer account was deleted	340	7.137%
A logon was attempted using explicit credentials	337	7.074%
Domain Policy was changed	329	6.906%
An account was successfully logged on	323	6.78%
System security access was removed from an account	321	6.738%
A user account was deleted	318	6.675%
A privileged service was called	317	6.654%
A user account was created	313	6.57%
A process has exited	309	6.486%

○

○ User

**user** ×

>100 Values, 100% of events Selected

**Reports**

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Top 10 Values	Count	%
<a href="#">user_l</a>	354	7.431%
<a href="#">user_a</a>	282	5.919%
<a href="#">user_m</a>	275	5.772%
<a href="#">user_i</a>	271	5.688%
<a href="#">user_f</a>	270	5.668%
<a href="#">user_e</a>	269	5.646%
<a href="#">user_h</a>	269	5.646%
<a href="#">user_c</a>	267	5.604%
<a href="#">user_d</a>	264	5.542%
<a href="#">user_b</a>	263	5.52%

○

## Status

**status** ×

2 Values, 100% of events Selected

**Reports**

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Values	Count	%
<a href="#">success</a>	4,622	97.019%
<a href="#">failure</a>	142	2.981%

○

## Severity

**severity** ×

2 Values, 100% of events Selected

**Reports**

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Values	Count	%
<a href="#">informational</a>	4,435	93.094%
<a href="#">high</a>	329	6.906%

○

## 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.

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

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

c. Take a screenshot of the report.

**Signature and ID Report**

source="windows\_server\_logs.csv" host="Windows\_server\_logs" sourcetype="csv" | stats count by signature, signature\_id | dedup signature\_id | table signature, signature\_id

✓ 4,764 events (before 5/7/25 2:20:02.000 AM) No Event Sampling

Events Patterns **Statistics (15)** Visualization

Show: 20 Per Page Format Preview: On

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

○ 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 Level Report**

source="windows\_server\_logs.csv" host="Windows\_server\_logs" sourcetype="csv" | stats count by severity | eventstats sum(count) as total | eval percentage=round((count/total)\*100, 2) | table severity, count, percentage

✓ 71,460 events (before 5/24/25 4:21:08.000 AM) No Event Sampling

Events Patterns **Statistics (2)** Visualization

Show: 20 Per Page Format Preview: On

severity	count	percentage
high	4935	6.91
informational	66525	93.09

○ 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.

**Success & Failure Rates of Windows Activities**

This report compares the success and failure rates of Windows activities based on the "status" field, helping to identify any patterns of failed attempts that might indicate suspicious activity.

[All time](#) 5,949 events (before 5/13/25 100:20:00 AM)

2 results 20 per page

status	count	percentage
failure	93	1.56
success	5856	98.44

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.

**Hourly Failed Windows Activity**

Helps spot anomalies like a sudden rise in failed logins, which could indicate brute-force attacks or unauthorized access attempts.

[All time](#) 2,130 events (before 5/12/25 11:18:01:000 PM)

24 results 20 per page

_time	count
2020-03-24 00:00	75
2020-03-24 01:00	75
2020-03-24 02:00	135
2020-03-24 03:00	60
2020-03-24 04:00	60
2020-03-24 05:00	150
2020-03-24 06:00	75
2020-03-24 07:00	105
2020-03-24 08:00	90
2020-03-24 09:00	135
2020-03-24 10:00	150
2020-03-24 11:00	75
2020-03-24 12:00	75
2020-03-24 13:00	75
2020-03-24 14:00	75
2020-03-24 15:00	30
2020-03-24 16:00	105
2020-03-24 17:00	60
2020-03-24 18:00	90
2020-03-24 19:00	60

- 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.

**(Normal Logs) High Rate of Failed Windows Activity Detected (Bases on Signature ID)**

Enabled: ..... Yes. [Disable](#)

App: ..... search

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

Modified: ..... May 14, 2025 5:24:09 PM

Alert Type: ..... Scheduled. Daily, at 18:00. [Edit](#)

Trigger Condition: .. Number of Results is > 105. [Edit](#)

Actions: ..... [1 Action](#) [Edit](#)

[Send email](#)

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

**An account was successfully logged on**

source="windows\_server\_logs.csv" host="Windows\_server\_logs" sourcetype="csv" signature\_id="4624" | bin \_time span=1h | stats count by \_time | where count > 225

✓ 4,845 events (before 5/26/25 3:32:41.000 AM) No Event Sampling Job

Events Patterns Statistics (5) Visualization

- Create an alert that's triggered when the threshold has been reached.
- The alert should trigger an email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).
- Design the alert based on the corresponding signature ID, as the signature name sometimes changes when the Windows system updates.

**An account was successfully logged on**

Enabled: ..... Yes. [Disable](#)

App: ..... search

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

Modified: ..... May 15, 2025 5:30:02 PM

Alert Type: ..... Scheduled. Weekly, Monday at 6:00. [Edit](#)

Trigger Condition: .. Number of Results is > 10. [Edit](#)

Actions: ..... ☒ Action [Edit](#)

☒ Send email

- Determine a baseline and threshold for the hourly count of the signature “a user account was deleted.”
- Design the alert based on the corresponding signature ID, as the signature name sometimes changes when the Windows system updates.

**Account Deletion Alert (4726)**

source="windows\_server\_logs.csv" host="Windows\_server\_logs" sourcetype="csv" signature\_id="4726" | bin \_time span=1h | stats count by \_time | where count > 255

✓ 4,770 events (before 5/26/25 3:43:57.000 AM) No Event Sampling Job

Events Patterns Statistics (3) Visualization

---

**Account Deletion Alert (4726)**

source="windows\_server\_logs.csv" host="Windows\_server\_logs" sourcetype="csv" signature\_id="4726" | bin \_time span=1h | stats count by \_time | where count > 255

✓ 4,770 events (before 5/26/25 3:43:57.000 AM) No Event Sampling Job

Events Patterns Statistics (3) Visualization

Show: 20 Per Page Format Preview: On

_time	count
2020-03-24 11:00	330
2020-03-24 13:00	315
2020-03-24 15:00	285

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



Save As Alert

Settings

Title

Account Deletion Alert (4726)

Description

This alert monitors for user account deletions (Signature ID 4726). It triggers if more than 3 deletions occur within an hour, helping detect potential unauthorized account removals.

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every week

On

Monday

at

6:00

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@VSI-company.com

Comma separated list of email addresses.

Cancel

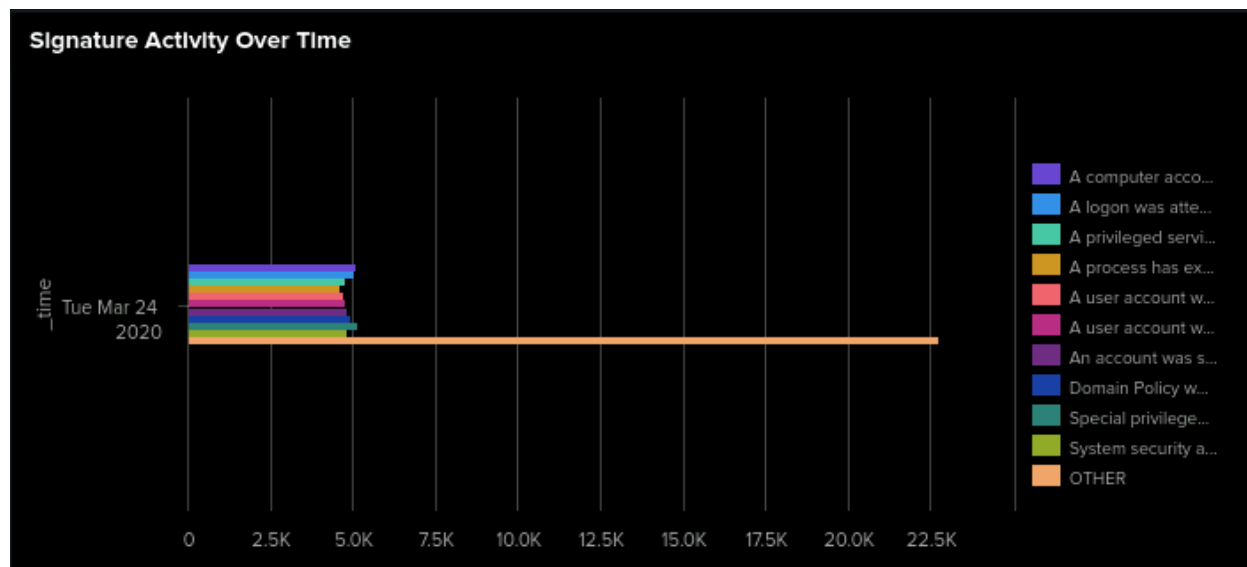
Save

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):

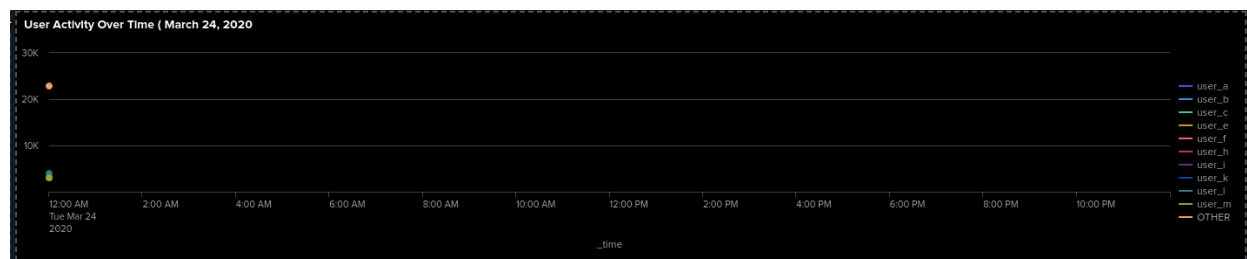
- A line chart that displays the different “signature” field values over time.

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

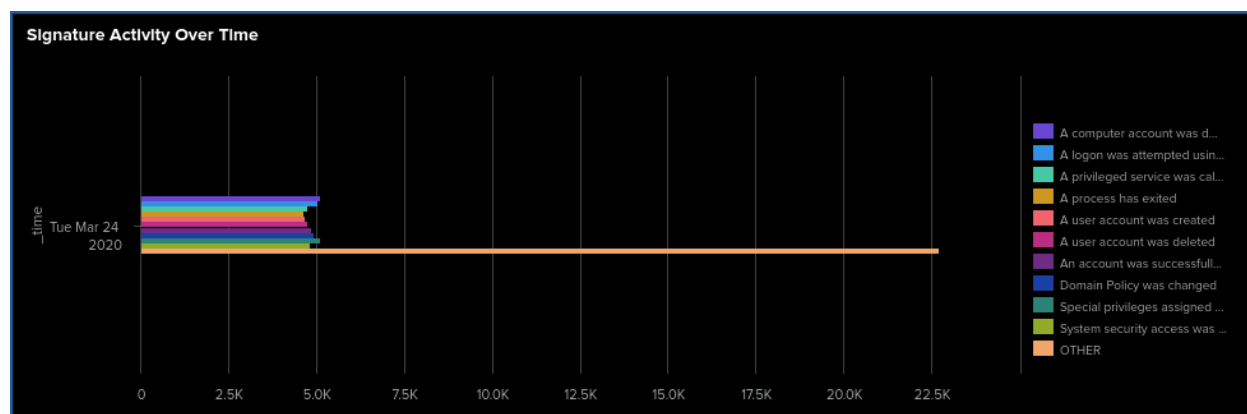
- b. Take a screenshot of the chart



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

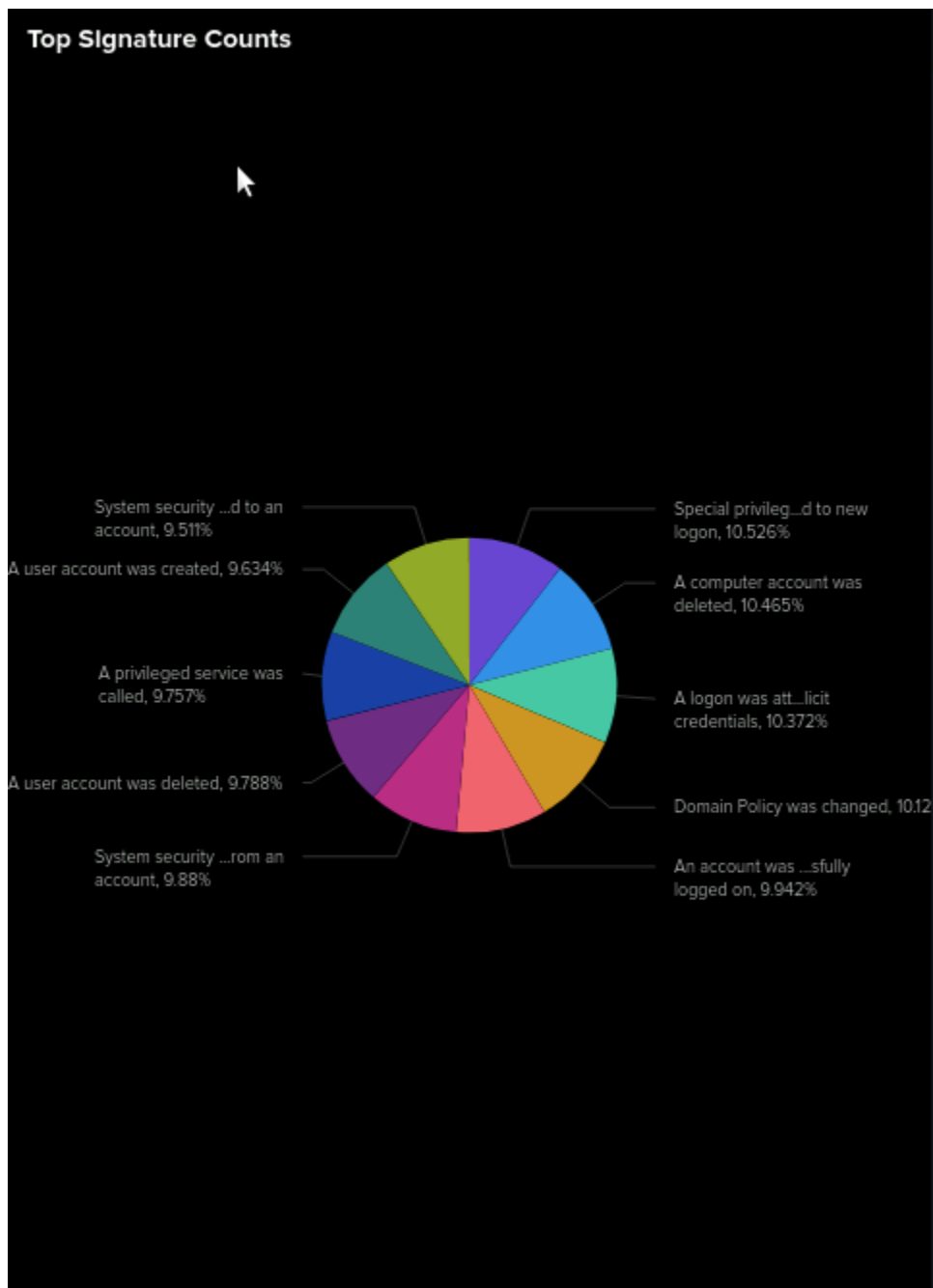


- Because a line graph doesn't necessarily provide the best visual for User Account Activity over time you could choose an alternative to provide you an alternative view



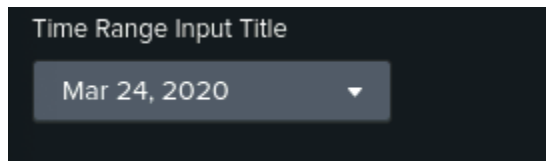
- Take a screenshot of the chart.

- Any visualization that illustrates the count of different signatures.



- Hint:** You can add brand-new custom visualizations by accessing this page inside your VM: [Additional Viz.](#)
  - Take a screenshot of the visualization.
- Any visualization that illustrates the count of different users.
- 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.
- 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.

## 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:

The screenshot shows a 'Review' page with the following configuration:

- 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

The screenshot shows the 'method' field analysis in Splunk. It displays 4 values representing 100% of the events. The 'Selected' button is set to 'Yes'. The table below shows the distribution of HTTP methods.

Values	Count	%
GET	3,157	70.202%
POST	1,324	29.442%
HEAD	15	0.334%
OPTIONS	1	0.022%

- Referer\_domain

referer\_domain

77 Values, 34.512% of events

Selected

Yes

No

Reports

[Top values](#)
[Top values by time](#)
[Rare values](#)

Events with this field

Top 10 Values

	Count	%	
<a href="#">http://www.semicomplete.com</a>	764	49.227%	<div></div>
<a href="#">http://semicomplete.com</a>	572	36.856%	<div></div>
<a href="#">http://www.google.com</a>	37	2.384%	<div></div>
<a href="#">https://www.google.com</a>	25	1.611%	<div></div>
<a href="#">http://stackoverflow.com</a>	15	0.966%	<div></div>
<a href="#">http://logstash.net</a>	6	0.386%	<div></div>
<a href="#">http://tuxradar.com</a>	6	0.386%	<div></div>
<a href="#">https://www.google.co.uk</a>	6	0.386%	<div></div>
<a href="#">https://www.google.com.br</a>	6	0.386%	<div></div>
<a href="#">http://kufli.blogspot.com</a>	5	0.322%	<div></div>

## ○ Status

status

7 Values, 100% of events

Selected

Yes

No

Reports

[Average over time](#)
[Maximum value over time](#)
[Minimum value over time](#)

[Top values](#)
[Top values by time](#)
[Rare values](#)

Events with this field

**Avg:** 232.40426951300867
 **Min:** 200
 **Max:** 500
 **Std Dev:** 73.59575528038513

Values	Count	%	
200	3,746	83.3%	<div></div>
404	679	15.099%	<div></div>
304	36	0.8%	<div></div>
301	29	0.645%	<div></div>
206	5	0.111%	<div></div>
403	1	0.022%	<div></div>
500	1	0.022%	<div></div>

## ○ Clientip

clientip

>100 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values	Count	%	
208.91.156.11	637	14.165%	
194.105.145.147	438	9.74%	
194.146.132.138	432	9.606%	
79.171.127.34	432	9.606%	
130.237.218.86	183	4.069%	
66.249.73.135	120	2.668%	
46.105.14.53	84	1.868%	
184.66.149.103	37	0.823%	
89.107.177.18	37	0.823%	
200.31.173.106	34	0.756%	

- Useragent

useragent

>100 Values, 99.978% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values	Count	%	
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)	1,296	28.826%	
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)	638	14.19%	
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	291	6.472%	
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	183	4.07%	
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	84	1.868%	
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	80	1.779%	
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	74	1.646%	
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	73	1.624%	
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	72	1.601%	
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	69	1.535%	

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

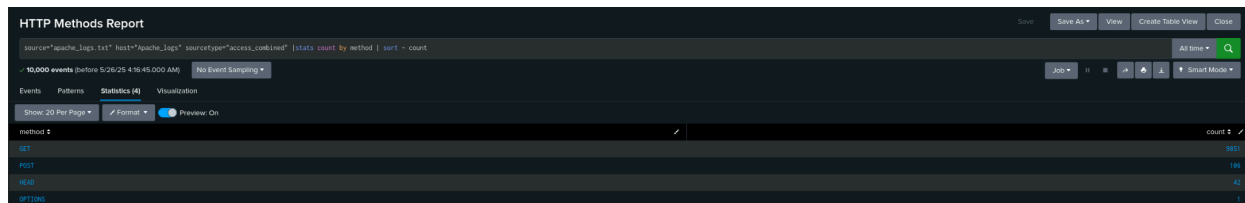
In this part, you will create reports, alerts, and dashboards to monitor for suspicious activity against VSI's Apache web server. To do so, complete the following steps:



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):

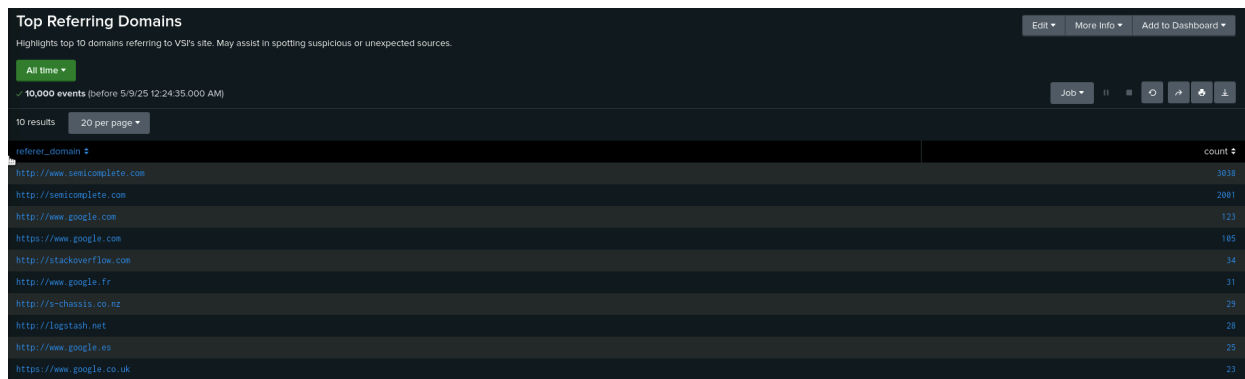
a. A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc.).



method	count
GET	1891
POST	104
HEAD	42
OPTIONS	1

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

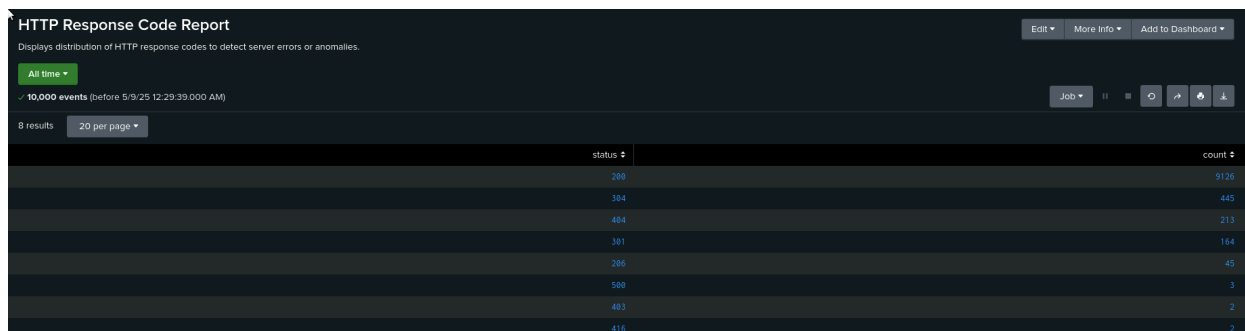
b. A report that shows the top 10 domains that refer to VSI's website.



referer_domain	count
http://www.semicomplete.com	3038
http://www.google.com	2081
https://www.google.com	123
http://stackoverflow.com	185
http://www.google.fr	34
http://s-chassis.co.nz	31
http://logstash.net	29
http://www.google.es	28
https://www.google.co.uk	23

■ This will assist VSI with identifying suspicious referrers.

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

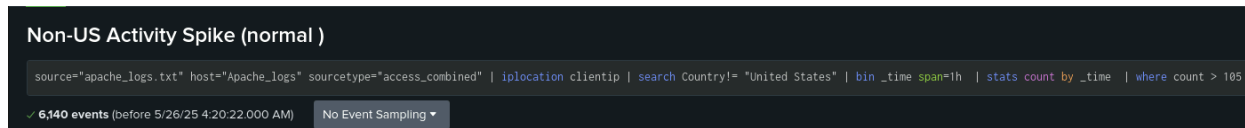


status	count
200	9126
304	445
404	213
301	164
206	45
500	3
403	2
416	2

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

○ **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.

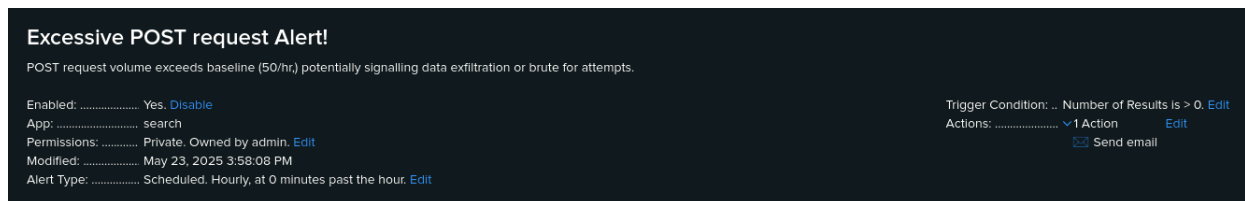


- The alert should trigger an email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).

- b. 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](mailto:SOC@VSI-company.com).



- **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`.

- b. A geographical map showing the location based on the "clientip" field.

- 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](#).

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

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

f. A 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>).



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.

## 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. Use the app/scenario below as an example of an add-on
  - **Whois XML IP Geolocation API:** App details [here](#) | Install Instructions: [Whois XML IP Geolocation API](#)
3. **Be sure to grab screenshots of your add-on app!**

Name ▾	Folder name ▾	Version ▾	Update checking ▾	Visible ▾	Sharing ▾	Status ▾	Actions
SplunkDeploymentServerConfig	SplunkDeploymentServerConfig		Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
SplunkForwarder	SplunkForwarder		Yes	No	App   Permissions	Disabled   Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App   Permissions	Disabled   Enable	
ThreatHunting	ThreatHunting	1.5.1	Yes	Yes	Global   Permissions	Enabled	Launch app   Edit properties   View objects   View details on Splunkbase

