

Apache Dashboard

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.

Reports:

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?
 - On the attack day, high severity events triple in proportion (from 6.91% → 20.22%)
 - This spike in severity, despite fewer total logs, is a red flag and strongly suggests malicious or disruptive activity
 - While the normal day has 13x more logs, most are low-risk ("informational").
 - The attack day has far fewer logs, but every fifth event is high severity, which increases its operational risk profile.



Report Analysis for Failed Activities (done)

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

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 a 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"`.

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?

Baseline Comparison **From the normal day (Mar 24):**

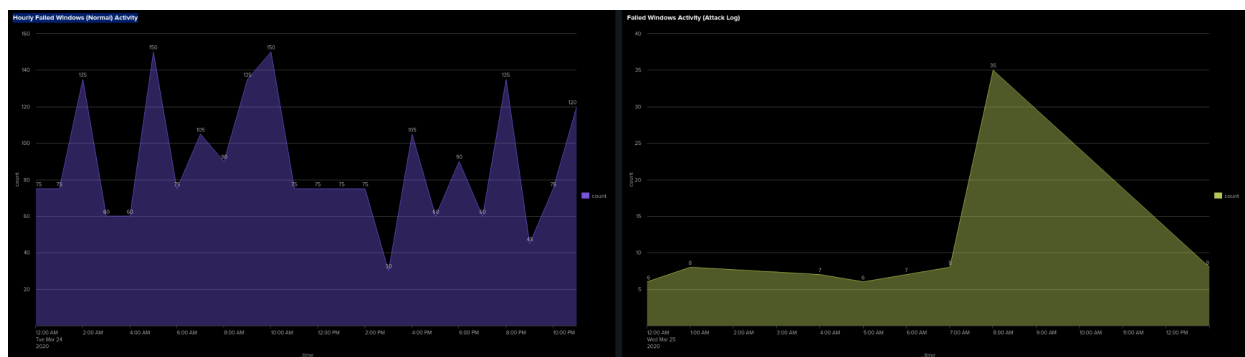
- Average = 79.5 failures/hour
- Standard Deviation = 31.45
- Normal Threshold = ~48–111 failures/hour

The attack day shows lower overall hourly counts but:

08:00 am shows a significant spike to 35 failures, which:
Is still below the baseline threshold from the normal day, but stands out against other hours on the attack day, where failures averaged between 6–8.

This may indicate:

- A low-and-slow attack pattern (deliberately keeping activity under detection thresholds)
- A targeted brute-force attempt spiking only during one hour



Alert Analysis for Successful Logins (done)

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for a 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"`.
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?

On the **normal day**, successful logins were high-volume but followed a **regular and expected pattern**.

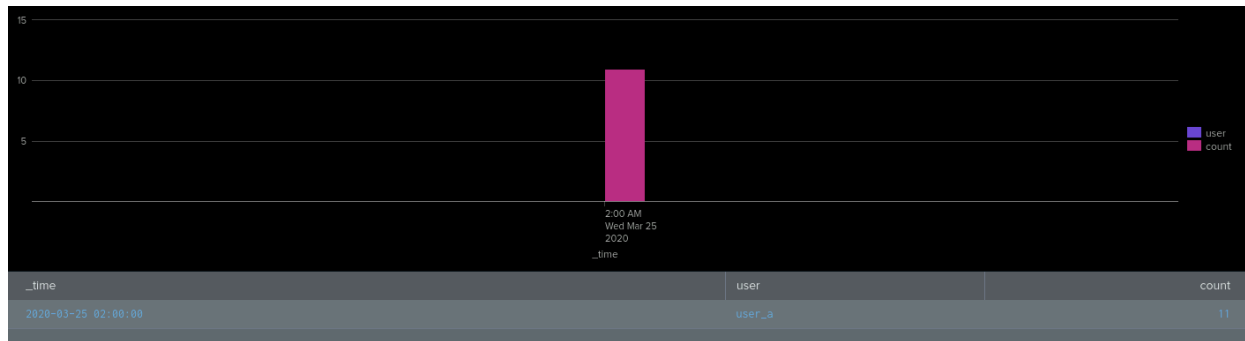
On the **attack day**, the **frequency of logins during off-hours** and their alignment with **previously failed attempts** suggest **unauthorized access**.

Recommendation: Investigate accounts active during attack day logins and consider implementing **MFA**, account lockout policies, or anomaly-based detection rules.

Hour	Count
00:00	11
01:00	15
02:00	14
03:00	14
04:00	12
05:00	9
06:00	11
07:00	15

08:00	16
13:00	15

After determining the frequency of logins during off-hours on the day of the attack I located the users most active during this period and found that User_a had attempted to log in a total of 11 times matching the 2 am spike



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 a 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?

On the normal day of March 24, 2020, account deletions occurred in high-volume bursts during specific hours, exceeding 255 deletions per hour, indicating scheduled administrative maintenance activities.

- 11:00 - 330 deletions
- 13:00 - 315 deletions
- 15:00 - 285 deletions

The large spikes in deletions suggest planned administrative activity, likely scheduled user cleanup or deprovisioning by authorized personnel.

According to the Data:

The account deletion alerts on the attack day (**March 25, 2020**) show consistent activity across multiple hours with moderate volume, indicating unauthorized or suspicious behavior possibly aimed at covering tracks or disrupting access.

- 13 distinct hours with deletion events
- Highest: 17 deletions at 05:00
- Others range from 1 to 14 deletions/hr
- The deletion volume is lower per hour but persistent and frequent (potential red flag.)
- Indicating **stealthy malicious behavior**, likely trying to avoid detection by:
 - Deleting accounts gradually
 - Possibly removing compromised accounts or covering attacker traces

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?
 - Yes, there is a noticeable increase in the frequency of high-severity events and account deletions during early hours on the attack day.
- What signatures stand out?
 - 4624 (successful logins)
 - 4726 (account deletions)

These are abnormally high compared to the normal day logs, indicating potentially malicious access and cleanup.
- What time did each signature's suspicious activity begin and stop?
 - 4624: Unusual surge starts around 00:00 and continues hourly until 13:00.
 - 4726: Spikes begin at 00:00 and persist hourly until 13:00, peaking around 05:00–08:00.
- What is the peak count of the different signatures?
 - 4624 (logins): 16 successful logins in a single hour.
 - 4726 (deletions): 17 deletions in an hour during the attack..

Dashboard Analysis for Users

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

- Does anything stand out as suspicious?
 - Yes, multiple users are active in high volumes during non-standard hours, many of whom do not appear in normal-day data.
- Which users stand out?
 - user_a (11 logins in one hour)
 - user_c, user_e, user_n

Their frequency and distribution indicate potential lateral movement or automated account use.
- What time did each user's suspicious activity begin and stop?
 - Most activity occurs between 00:00 and 13:00.

- user_a: Notable spike at 02:00.
- user_n, user_e: Active across multiple hours including 01:00 and 08:00.
- What is the peak count of the different users?
 - user_a: 11 logins at 02:00
 - user_c and user_e: 3 logins at 01:00

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

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

- Does anything stand out as suspicious?
 - Yes, the pie and bar charts show that 4624 and 4726 dominate the attack-day activity, which is inconsistent with normal operational patterns.
- Do the results match your findings from the time chart for signatures?
 - Yes, the same signatures that stood out in the time chart (logins and deletions) are clearly overrepresented in graphical summaries, confirming abnormal behavior.

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

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

- Does anything stand out as suspicious?
 - Yes. Several users with little or no prior history are active during off-hours and show high activity counts.
- Do the results match your findings from the time chart for users?
 - Yes. Users like user_a, user_e, and user_n consistently appear as top users across both visualization methods, reinforcing their anomalous behavior.

Dashboard Analysis for Users with Statistical Charts

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

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

Advantages:

- Allows precise comparison of user activity counts.
- Easier to sort, filter, and perform trend analysis.
- Better for exporting and auditing.


Disadvantages:

- Lacks intuitive visual cues.
- Doesn't highlight temporal anomalies as clearly as time charts or bar graphs.
- Can be overwhelming without proper grouping or thresholds.

Part 3: Load Apache Attack Logs

In this part, you will upload Apache attack logs 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_attack_logs.txt` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory.
 - Click the green "Next" button on the top right.
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 a page called "Input Settings."
 - 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 "Apache_logs" and then select "Review."
5. At the "Review" page, verify that you've chosen the correct settings.
 - Select "Submit" to proceed with uploading your data into Splunk.
6. Once the file has been uploaded, a message that says "File has been uploaded successfully" will appear.
7. Select "Start Searching."
8.  **Important:** After the search data populates, select "All Time" for the time range.

WindWindow

Part 4: Analyze Apache Attack Logs

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

Report Analysis for Methods

1. Access the "Reports" tab, and select "Yours" to view the reports that you created on Day 1.
2. Select the report that analyzes the different HTTP methods.
3. Select "Edit" > "Open in Search."
4. Take note of the percentage and count of the various methods.
5. Change the source from `source="apache_logs.txt"` to `source="apache_attack_logs.txt"`.
6. Select "Save."

7. Review the updated results, and answer the following questions in the review document:

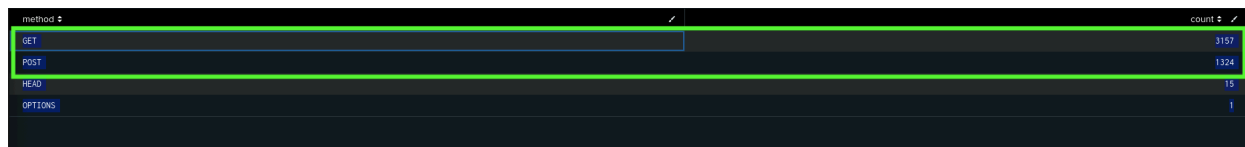
1. Did you detect any suspicious changes in HTTP methods? If so, which one?

Yes — the **POST** method shows a notably high count (1324), which may indicate suspicious or malicious activity.

2. What is that method used for?

The **POST** method is used to submit data to a server (e.g., login forms, uploads). A high number of POST requests may signal:

- Brute force login attempts
- Exploit attempts (e.g., file uploads, web shells)
- Data exfiltration



method	count
GET	3157
POST	1324
HEAD	15
OPTIONS	1

This increase suggests that an attacker may be attempting to exploit input forms or APIs on the server.

Report Analysis for Referrer Domains

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that analyzes the different referrer domains.
3. Select “Edit” > “Open in Search.”
4. Take note of the different referrer domains.
5. Change the source from `source="apache_logs.txt"` to `source="apache_attack_logs.txt"`.
6. Select “Save.”
7. Review the updated results, and answer the following question in the review document:

- Did you detect any suspicious changes in referrer domains?
- Yes. Most of the traffic is coming from **semicomplete.com** (over 1,300 hits total), which looks unusual compared to other more normal referrers like Google or Stack Overflow.
- This could mean someone is testing or attacking the site using tools that link back to **semicomplete.com**, which is known to be related to test or security tools.

referrer_domain	count
http://www.semicomplete.com	764
http://semicomplete.com	572
http://www.google.com	37
https://www.google.com	25
http://stackoverflow.com	15
http://logstash.net	6
http://tuxradar.com	6
https://www.google.co.uk	6
https://www.google.com.br	6
http://kufli.blogspot.com	5

Report Analysis for HTTP Response Codes

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that analyzes the different HTTP response codes.
3. Select “Edit” > “Open in Search.”
4. Take note of the different HTTP response codes.
5. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt"`.
6. Select “Save.”
7. Review the updated results, and answer the following question in the review document:

- Did you detect any suspicious changes in HTTP response codes?
- Yes. Most responses are normal (200 = OK), but there are **679 "404 Not Found"** errors, which could mean someone is scanning the site for missing or hidden pages.
- Also, there's **1 "403 Forbidden"** and **1 "500 Internal Server Error"**, which could be signs of attempted attacks or misconfigurations.

status	count
200	3746
404	679
304	36
301	29
206	5
403	1
500	1

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

Alert Analysis for International 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 international activity.
3. Select “Open in Search.”
4. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt"`.
5. Review the updated results, and answer the following questions in the review document:
 - Did you detect a suspicious volume of international activity?
 - **Yes. There was a big spike at 8 PM on March 25, 2020,**
 - If so, what was the count of events in the hour(s) it occurred?
 - **937 events in just one hour.**
 - Would your alert be triggered for this activity?
 - **Yes, if the threshold was below 900, the alert would definitely trigger.**
 - After reviewing, would you change the threshold you previously selected?
 - **Yes. Based on this spike, it may be a good idea to lower the threshold slightly to catch large activity bursts earlier.**

time	count
2020-03-25 00:00	120
2020-03-25 01:00	108
2020-03-25 09:00	107
2020-03-25 20:00	937

Alert Analysis for HTTP POST Activity

1. Access the “Alerts” tab, and select “Yours” to view the alerts you created on Day 1.
2. Select the alert for suspicious volume of HTTP POST activity.
3. Select “Open in Search.”

4. Change the source from `source="apache_logs.txt"` to `source="apache_attack_logs.txt"`.
5. Review the updated results, and answer the following questions in the review document:
 - Did you detect any suspicious volume of HTTP POST activity?
 - Yes, there was a large spike in **POST requests**.
 - If so, what was the count of events in the hour(s) it occurred?
 - There were **600 POST requests** in a single hour.
 - When did it occur?
 - On **March 25, 2020, at 8:00 PM**.
 - After reviewing, would you change the threshold that you previously selected?
 - Yes — I would **lower the threshold to around 400** to detect smaller, earlier spikes.

Dashboard Setup

1. Access the Apache Web Server Monitoring dashboard.
 2. Select “Edit.”
 3. For each panel that you created, access the panel and complete the following steps:
 - Select “Edit Search.”
 - Change the source from `source="apache_logs.txt"` to `source="apache_attack_logs.txt"`.
 - Select “Apply.”
 4. Save the whole dashboard.
 5. Change the time on the whole dashboard to “All Time.”
- On **March 25, 2020, at 8:00 PM**.

