Contents

Installation of Splunk and Creation of Fortigate Firewall Dashboard

Project Objective: The primary objective of this project is to install Splunk Enterprise, configure it to ingest logs from a Fortigate firewall, and create a comprehensive dashboard to visualize and monitor firewall activities. This includes tracking and displaying metrics such as blocked traffic, allowed traffic, top sources and destinations of traffic, top blocked categories, and overall firewall performance metrics.

Scope:

- Install and configure Splunk Enterprise.
- Ingest and parse Fortigate firewall logs into Splunk.
- Create searches and queries to extract relevant data.
- Design and implement a dashboard to visualize firewall activities and metrics.
- Configure alerts for critical security events.

Deliverables:

1. Installed and configured Splunk Enterprise.
2. A functional Splunk dashboard displaying various Fortigate firewall metrics.
3. Search queries used to generate the dashboard panels.
4. Documentation detailing the setup process, search queries, and dashboard features.

Stakeholders:

- IT Security Team
- Network Administrators
- SOC Analysts
- IT Management

Milestone:

1: Splunk Installation and Configuration

Install Splunk Enterprise on a designated server.

Configure initial settings and ensure Splunk is operational.

2: Data Ingestion and Parsing

Set up data ingestion from Fortigate firewall to Splunk.

Parse and normalize the log data to extract relevant fields.

3: Dashboard Creation

Develop search queries to extract necessary metrics.

Design and implement the dashboard panels.

4: Alerts Configuration and Final Testing

Configure alerts for critical firewall events.

Final testing and validation of the dashboard.

Complete project documentation.

Tools and Technologies:

- Fortigate Firewall
- Splunk Enterprise
- Fortigate Add-on for Splunk
- Splunk Dashboard Editor

Assumptions:

Access to Fortigate firewall logs.

Server or cloud instance for installing Splunk.

Basic understanding of Splunk search processing language (SPL).

Risks and Mitigations

Risk: Installation issues due to software compatibility.

Mitigation: Ensure all system requirements are met before installation.

Risk: Data ingestion issues due to log format changes.

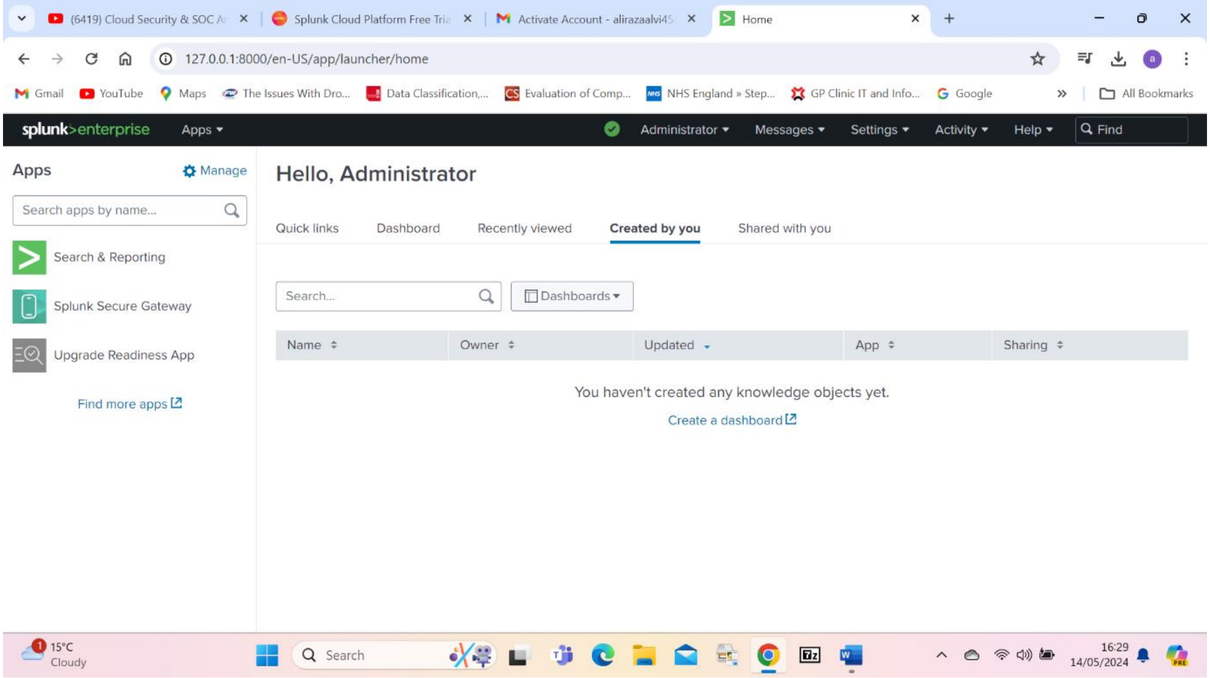
Mitigation: Regularly update the Fortigate add-on for Splunk and monitor log ingestion.

Risk: Performance issues due to large data volumes.

Mitigation: Implement data archiving and index optimization strategies.

Splunk Installation and Configuration:

Download and install Splunk Enterprise on the designated server.



You haven't created any knowledge objects yet.

Splunk enterprise

Configure Splunk to start at boot and set up admin credentials.

Verify that Splunk is running correctly and accessible via the web interface.

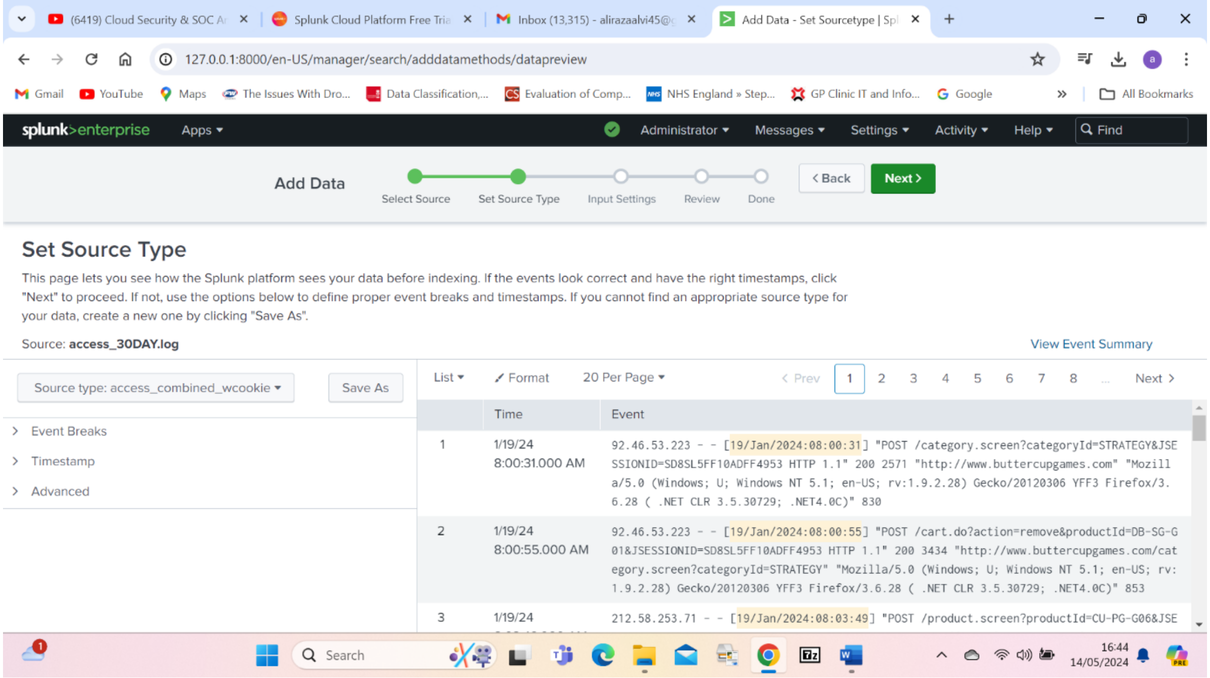
Data Ingestion:

Set up a data input in Splunk to receive logs from the Fortigate firewall.

Ensure logs are being indexed correctly in Splunk.

1- Download Splunk enterprise free trial version
2- Download and paste tmp folder on desktop(log data) (splk.it/f1data)
3- In Splunk home tab click on add data
4- Upload access_30DAY file available in tmp folder
5- While uploading data in host field value put web application
6- Put index as test click save
7- After save u will an option for add more data click that
8- Now choose file linux_s_30DAY file from tmp folder
9- In source type u have to choose operating system and there will be Linux secure
10- With next tab u need to change the host field name to Linux server
11- All done with data upload now click start search button n you will see the data upload
12- Install Splunk universal forwarder to receive the logs of local machine
13- Configure the forwarder at 127.0.0.1 and give any random port in my case its 9997
14- Download the data file botsv1 file

15- Copy this folder and go to C drive of computer and go to program files and go to the Splunk folder and the etc and then app and paste it in apps folder
16- Now click on apps and find more apps
17- Download Fortinet Fortigate on Splunk
18- Download infosec app for Splunk
19- Download ta Suricata



Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

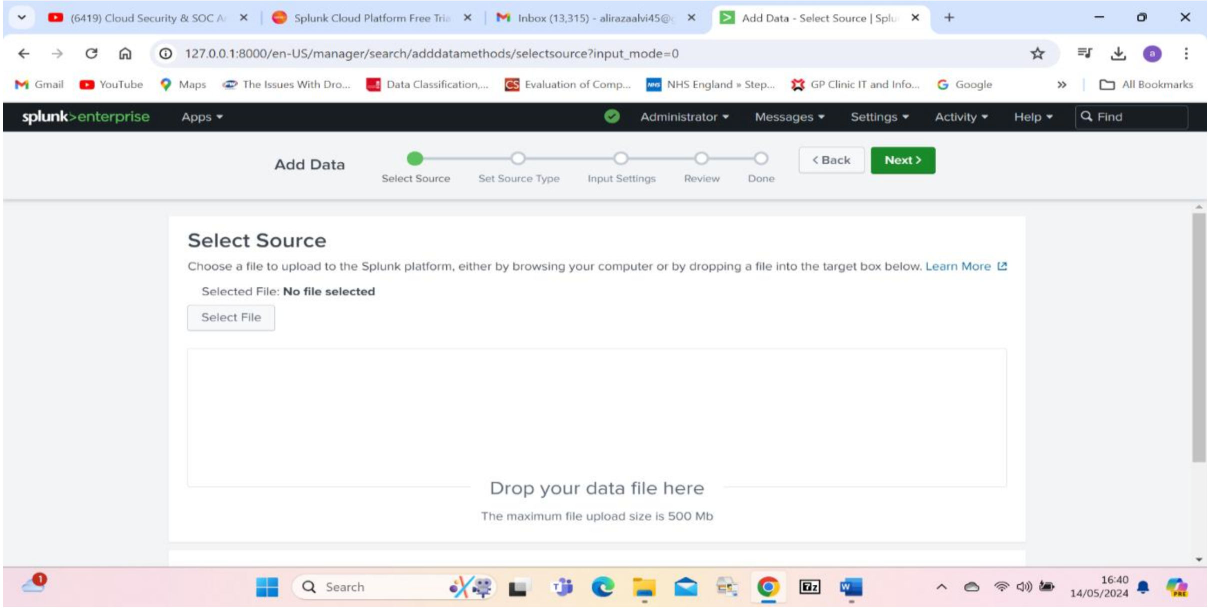
Source: **access_30DAY.log**

View Event Summary

Source type: access_combined_wcookie

	Time	Event
1	1/19/24 8:00:31.000 AM	92.46.53.223 - - [19/Jan/2024:08:00:31] "POST /category.screen?categoryId=STRATEGY&JSESSIONID=SD8SL5FF10ADFF4953 HTTP 1.1" 200 2571 "http://www.buttercupgames.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 830
2	1/19/24 8:00:55.000 AM	92.46.53.223 - - [19/Jan/2024:08:00:55] "POST /cart.do?action=remove&productId=DB-SG-G01&JSESSIONID=SD8SL5FF10ADFF4953 HTTP 1.1" 200 3434 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 853
3	1/19/24	212.58.253.71 - - [19/Jan/2024:08:03:49] "POST /product.screen?productId=CU-PG-G06&JSE

Data ingestion



Select Source

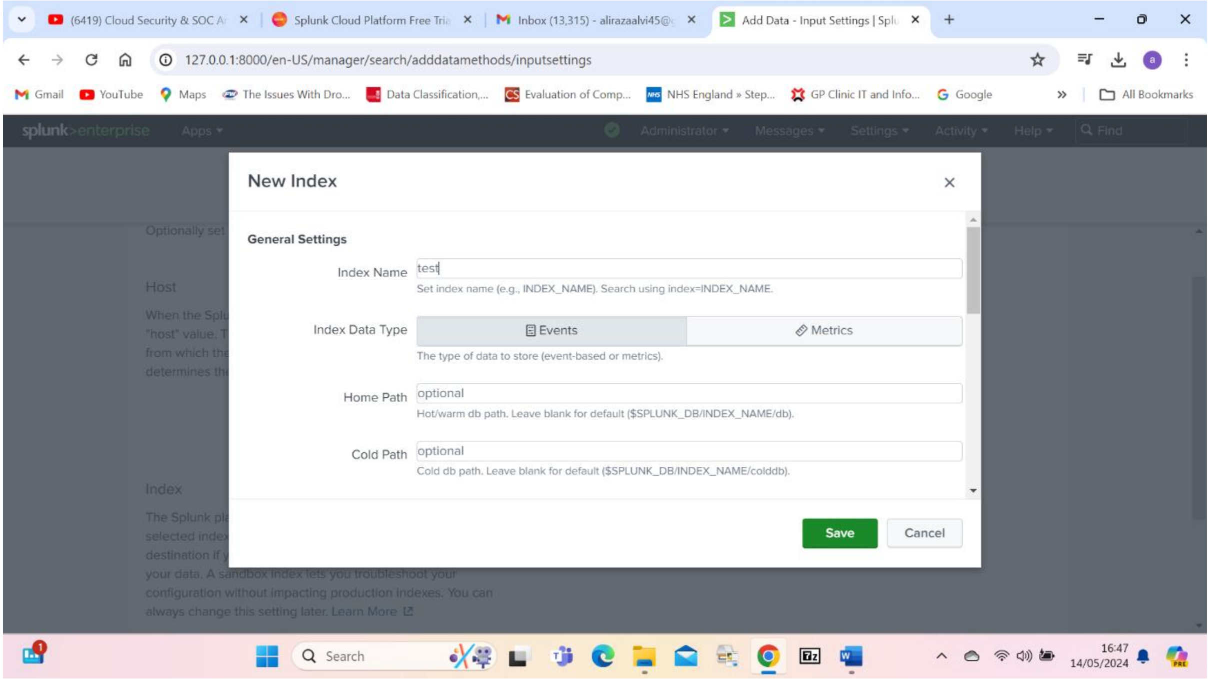
Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: **No file selected**

Drop your data file here

The maximum file upload size is 500 Mb

Data ingestion



New Index

General Settings

Index Name: test
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Data Parsing and Field Extraction:

Install the Fortigate Add-on for Splunk to parse the logs.

Verify that all relevant fields (e.g., source IP, destination IP, action, service, etc.) are being extracted correctly.

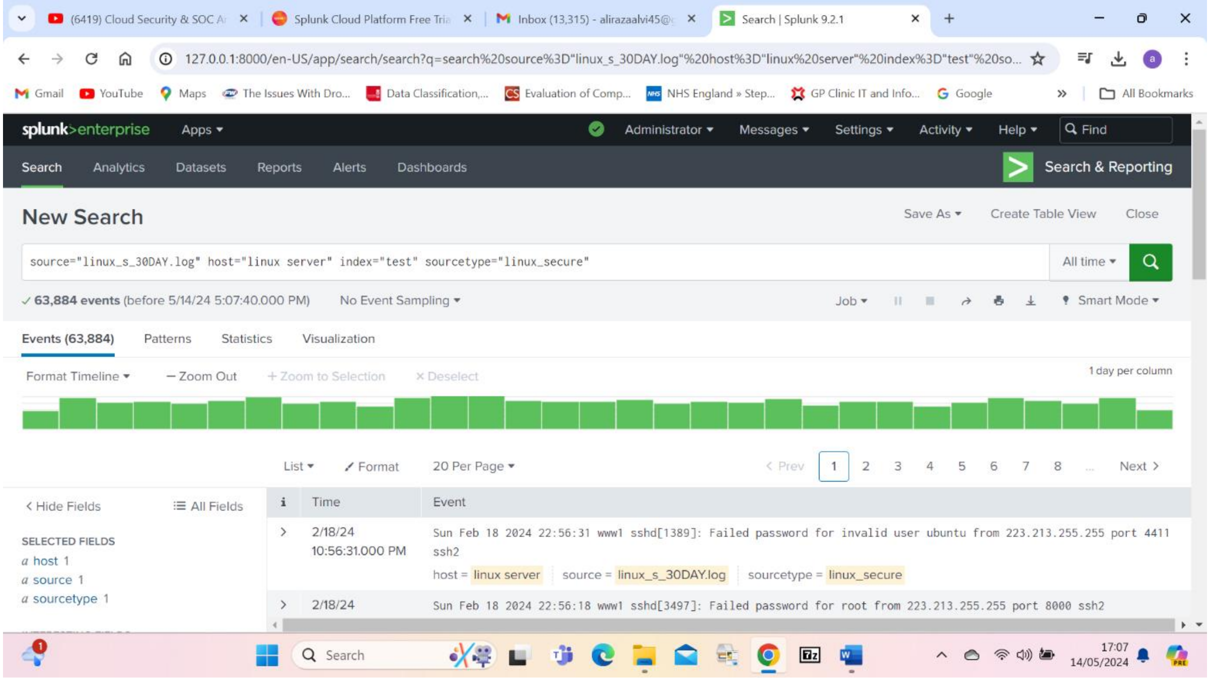
Write search queries in Splunk's Search Processing Language (SPL) to extract relevant information from the network traffic logs.

Use SPL commands to perform aggregations, filtering, and calculations as needed.

Some more queries for practice and check the data parsing

1. Enter a search that returns all web application events that include a purchase action with a web status of 200
index=test sourcetype=access_combined_wcookie action=purchase status=200
2. Enter a search that returns all web application events that include a purchase action where product ID is WC-SH-G04
index=test sourcetype=access_combined_wcookie action=purchase productId=WC-SH-G04
3. case 3:The team is only looking for successful purchases, so change your search to only return those.
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do
4. The team is only looking for unsuccessful purchases, so change your search to only return those.
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=error.do
5. Status not equal to 200 and got error
index=test sourcetype=access_combined_wcookie action=purchase status!=200 file="error.do"

6. You will see fields that do not matter to the team. Use the fields command to only return the action, JSESSIONID and status fields. Does your search run faster using the command?
Ans: index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields action, JSESSIONID, status
7. Now tell the difference:
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields - action, JSESSIONID, status
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields-action, JSESSIONID, status
8. Write a query to provide a statistics of the above activity by JSESSIONID
index=test sourcetype=access_combined_wcookie | fields action, JSESSIONID, status | stats count by JSESSIONID
9. Write a query to provide a statistics of the products purchased by productId. Use the fields command to only return the action, productid and status fields
index=test sourcetype=access_combined_wcookie | fields action, productId, status | stats count by productId
10. Find the statistics of the productid and clientip
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields action, productId, status, clientip | stats count by productId, clientip
11. Find the list of clientips who have visited the URL "Buttercupgames.com" and rename the count as events.
index=test sourcetype=access_combined_wcookie action=purchase status=200 referer_domain="http://www.buttercupgames.com" | stats count by clientip | rename count as events | sort –events.



127.0.0.1:8000/en-US/app/search/search?q=search%20source%3D"linux_s_30DAY.log"%20host%3D"linux%20server"%20index%3D"test"%20so...

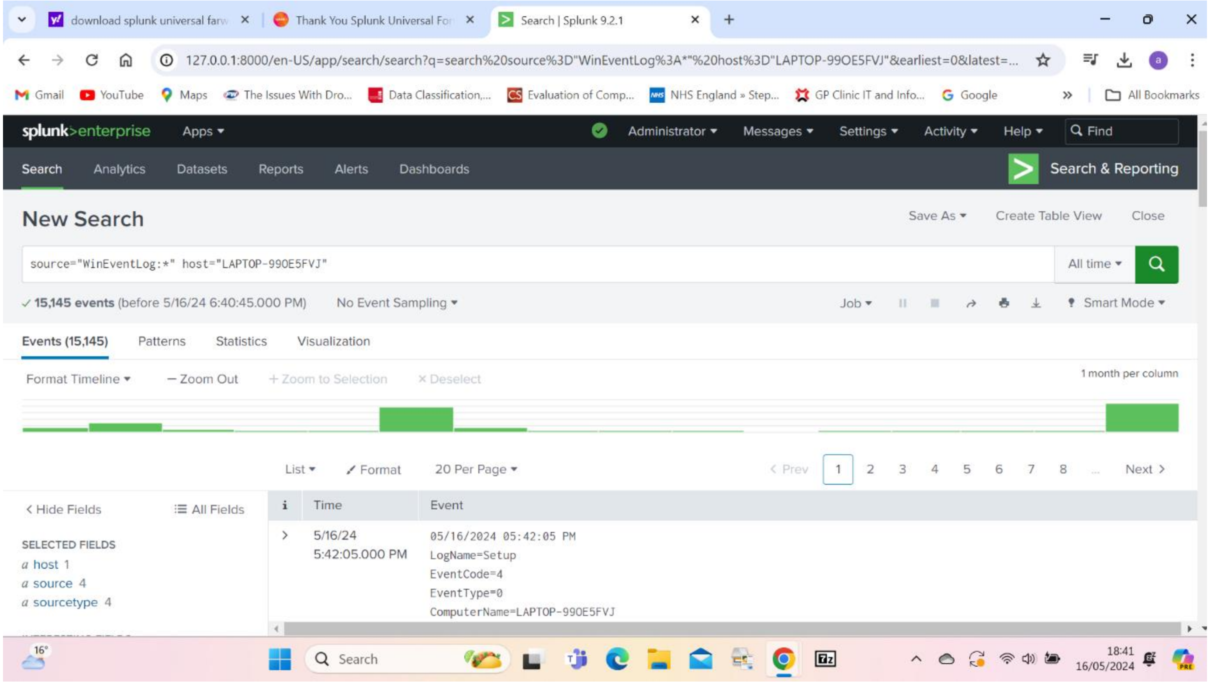
```
source="linux_s_30DAY.log" host="linux server" index="test" sourcetype="linux_secure"
```

✓ 63,884 events (before 5/14/24 5:07:40.000 PM) No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

i	Time	Event
>	2/18/24 10:56:31.000 PM	Sun Feb 18 2024 22:56:31 www1 sshd[1389]: Failed password for invalid user ubuntu from 223.213.255.255 port 4411 ssh2 host = linux server source = linux_s_30DAY.log sourcetype = linux_secure
>	2/18/24	Sun Feb 18 2024 22:56:18 www1 sshd[3497]: Failed password for root from 223.213.255.255 port 8000 ssh2

Local machine logs



New Search

```
source="WinEventLog:*" host="LAPTOP-990E5FVJ"
```

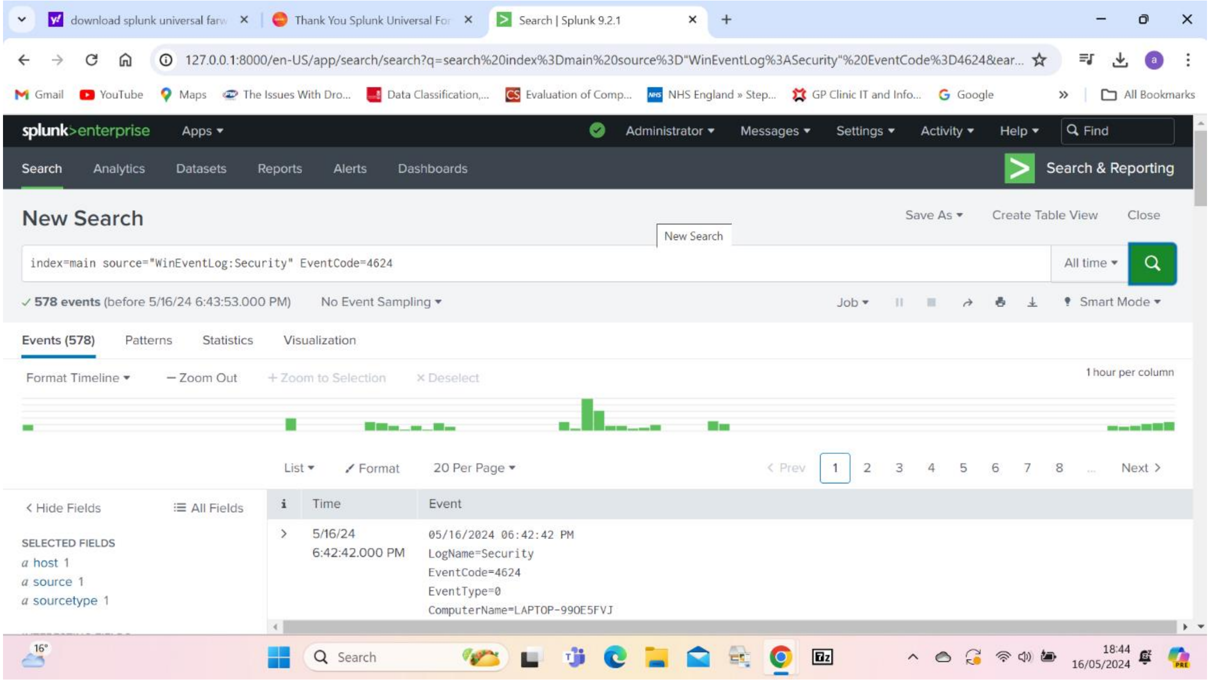
✓ 15,145 events (before 5/16/24 6:40:45.000 PM) No Event Sampling

SELECTED FIELDS
a host 1
a source 4
a sourcetype 4

5/16/24 5:42:05.000 PM

```
05/16/2024 05:42:05 PM
LogName=Setup
EventCode=4
EventType=0
ComputerName=LAPTOP-990E5FVJ
```

Local windows logs



New Search

```
index=main source="WinEventLog:Security" EventCode=4624
```

✓ 578 events (before 5/16/24 6:43:53.000 PM) No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

5/16/24 6:42:42.000 PM

```
05/16/2024 06:42:42 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=LAPTOP-990E5FVJ
```

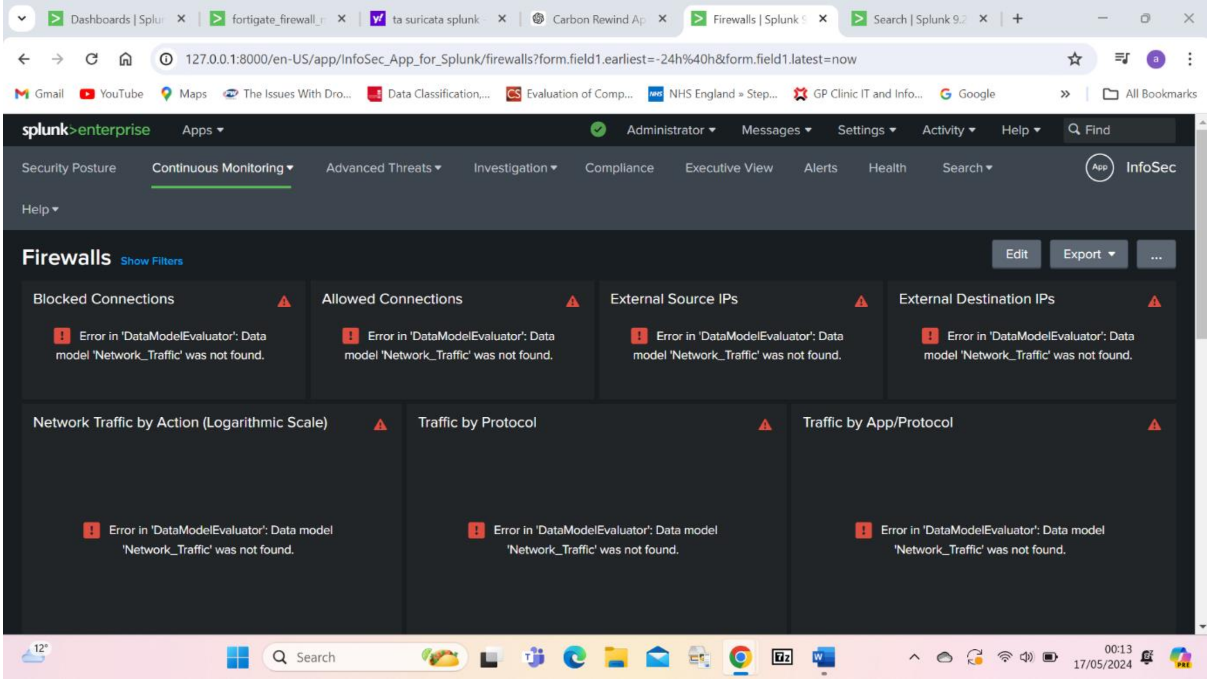
Windows log event 4624

Fortigate Firewall queries

1. index=botsv1 sourcetype= fortigate _traffic action=blocked |stats count(action) (for blocked connections)
2. index=botsv1 sourcetype= fortigate _traffic action=allowed |stats count(action) for allowed connections
3. index=botsv1 sourcetype= fortigate _traffic action=teardown |stats count(action) for teardown connections
4. index=botsv1 sourcetype=fortigate_traffic src_ip!=10.0.0.0/8 src_ip!=192.168.0.0/16 src_ip!=172.16.0.0/12 |stats count by src_ip (for external sourceip)
5. index=botsv1 sourcetype=fortigate_traffic dest_ip!=10.0.0.0/8 dest_ip!=192.168.0.0/16 dest_ip!=172.16.0.0/12 |stats count by dest_ip (for destination ip)
6. index=botsv1 sourcetype=fortigate_traffic action=* |timechart count by action (for network traffic by action by logrethmic scale)
7. index=botsv1 sourcetype=fortigate_traffic transport=* | timechart count by transport (by protocoal)
8. index=botsv1 sourcetype=fortigate_traffic app=* | timechart count by app traffic (by app)
9. index=botsv1 sourcetype=fortigate_traffic action=blocked OR action=teardown | stats count by src_ip dest_port | iplocation src_ip | geostats sum(count) by dest_port (for blocked incoming traffic by destination port)
10. index=botsv1 sourcetype=fortigate_traffic action=blocked |stats count by src_ip |rename src_ip as Blocked_Country | iplocation Blocked_Country |stats sum(count) as count by Country |sort - count |head 10 (for top countries by blocked connections)
11. index=botsv1 sourcetype=fortigate_traffic action=blocked |stats count by src_ip |rename src_ip as Blocked_USERS | iplocation Blocked_Country |sort - count |head 10 (for top sources blocked by connection)

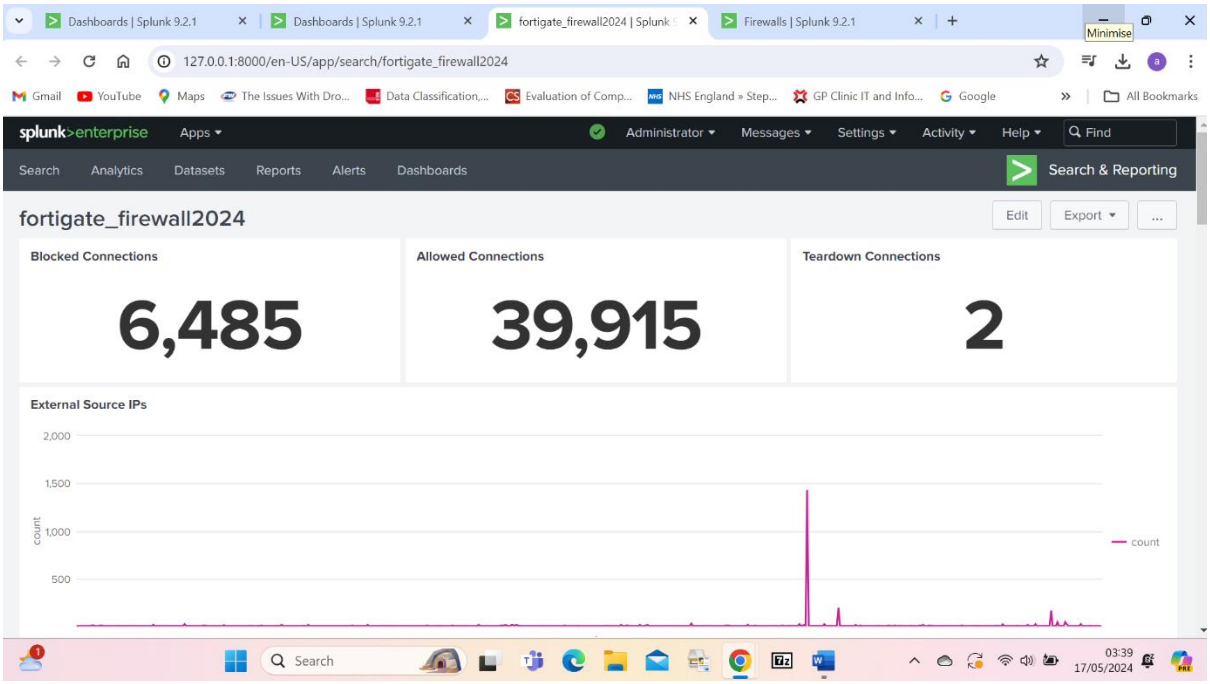
Dashboard Design:

Create a new dashboard in Splunk.

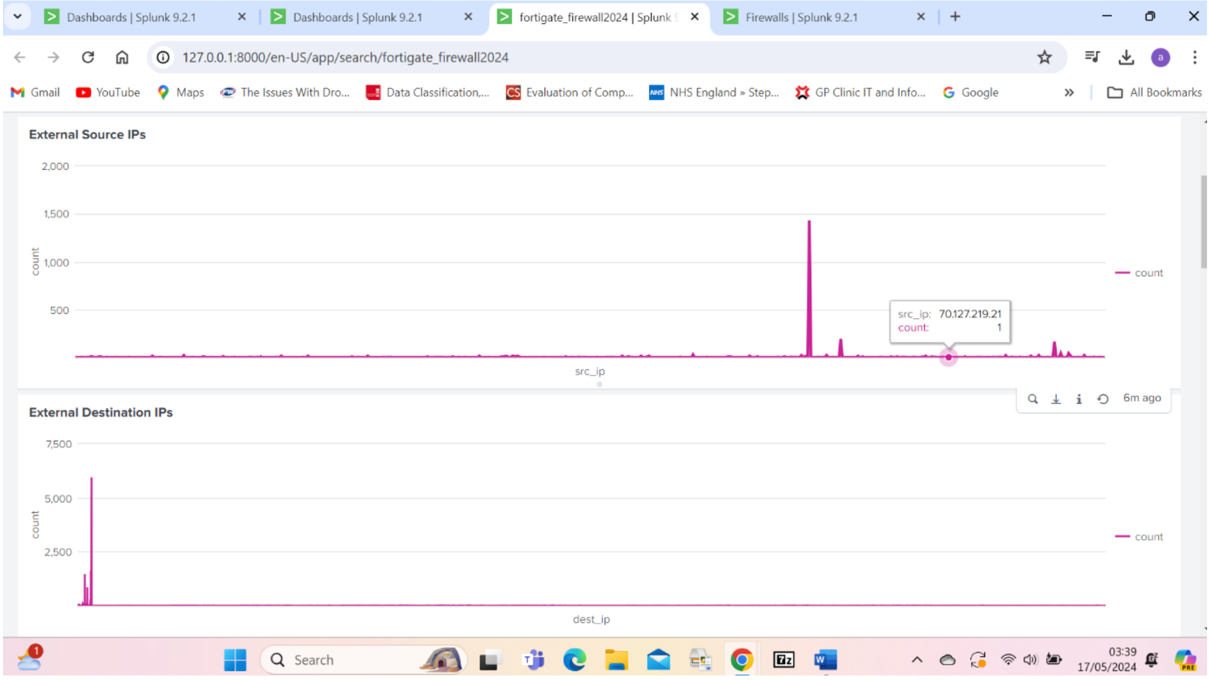


Error in 'DataModelEvaluator': Data model 'Network_Traffic' was not found.

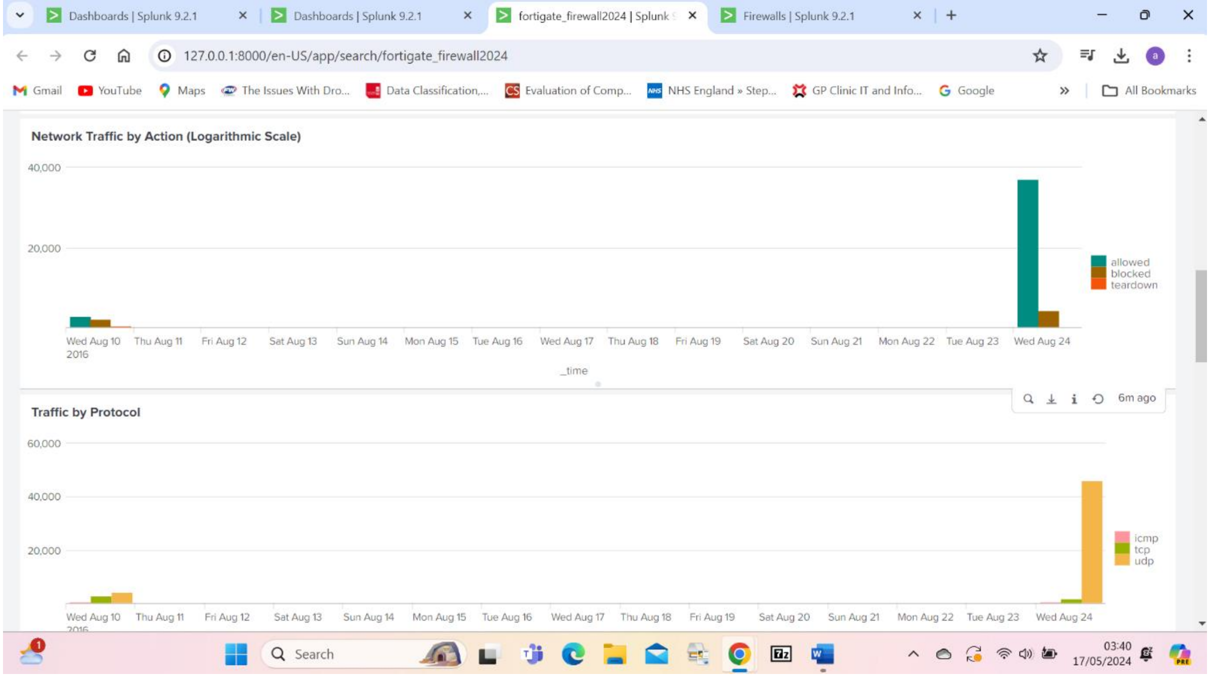
Fortigate Firewall Dashboard example



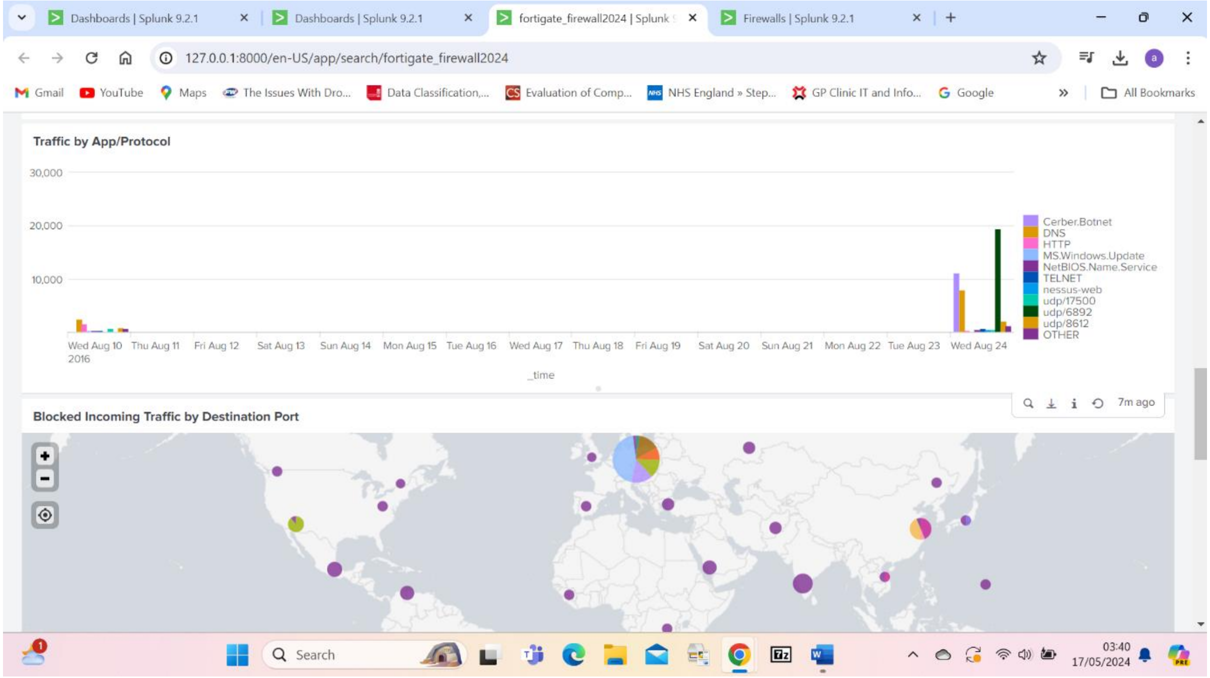
Fortigate Firewall Dashboard



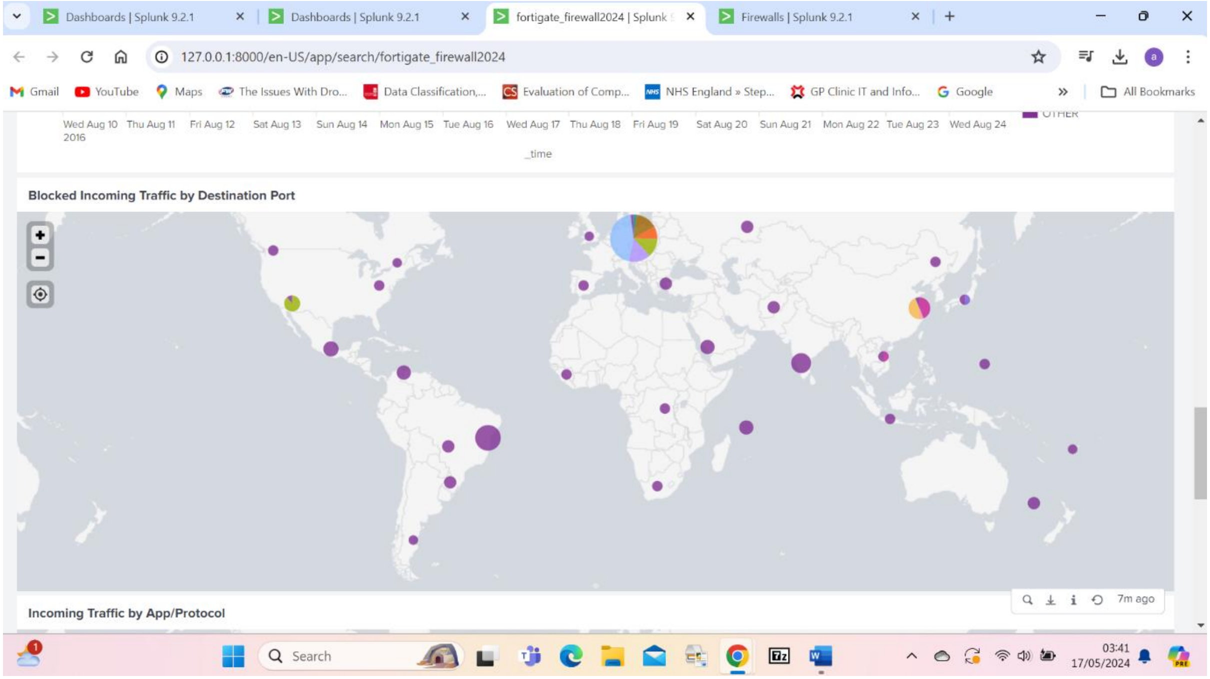
Fortigate Firewall Dashboard



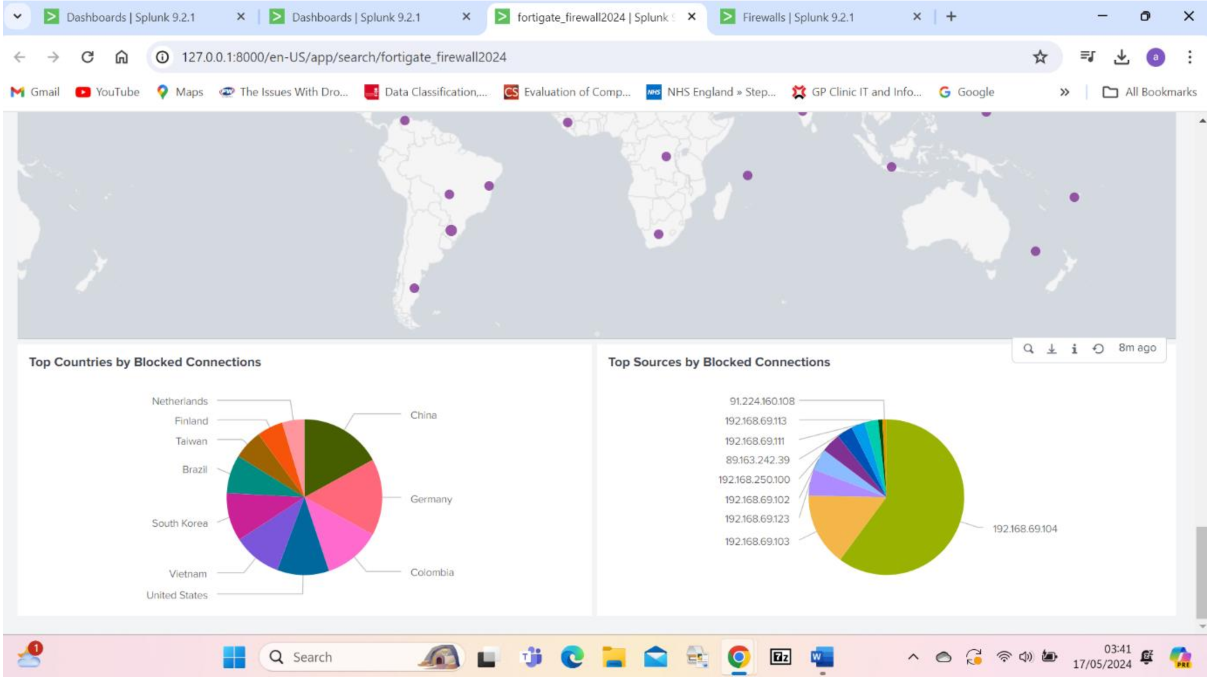
Fortigate Firewall Dashboard



Fortigate Firewall Dashboard



Fortigate Firewall Dashboard



Fortigate Firewall Dashboard

Alerts Configuration:

Set up alerts for critical events such as multiple blocked attempts from the same IP, unusual traffic patterns, etc.

Define alert thresholds and notification methods.

Testing and Validation:

All the data has been tested and Validate that the dashboard displays accurate and timely data.

Test alerts to ensure they trigger as expected.