Contents

IDS Dashboard Creation with Suricata in Splunk

Project Objective

To set up an Intrusion Detection System (IDS) using Suricata and visualize the data in Splunk through a comprehensive dashboard.

Introduction

This project aims to integrate Suricata IDS with Splunk to monitor and analyse network traffic for potential security threats. The data collected by Suricata will be ingested into Splunk, where custom dashboards and alerts will be created for real-time monitoring and analysis.

Environment Setup

Prerequisites

- Splunk Enterprise
- Suricata IDS
- Sufficient disk space and memory
- Administrative access to the network and systems being monitored

Installation

Splunk Installation

1-Download Splunk

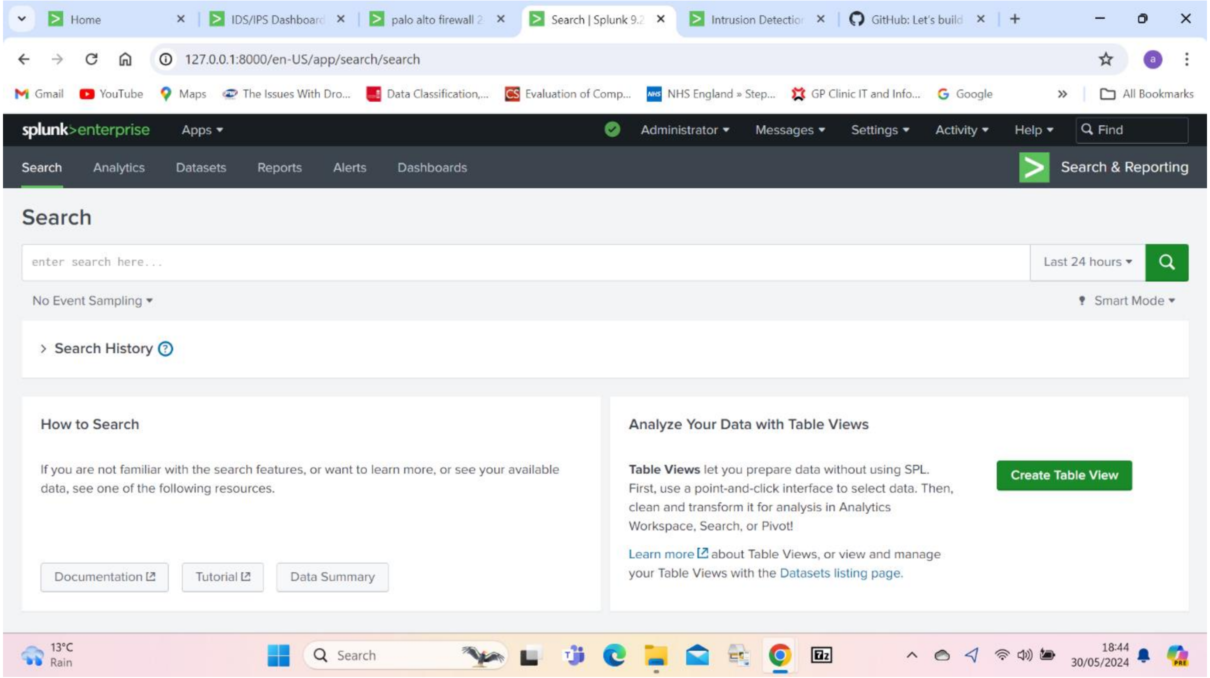
Visit the **Splunk website** and download the Splunk installer for your operating system.

2-Install Splunk:

Follow the installation instructions provided on the Splunk website.

3-Start Splunk:

Start the Splunk service using the appropriate command for your OS.



How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

Splunk enterprise

Suricata Installation

1-Download Suricata:

Visit the **Suricata website** and download the latest version of Suricata.

2-Install Suricata:

Follow the installation instructions provided on the Suricata website.

3-Configure Suricata:

Edit the **suricata.yaml** configuration file to set the appropriate network interfaces and logging options.

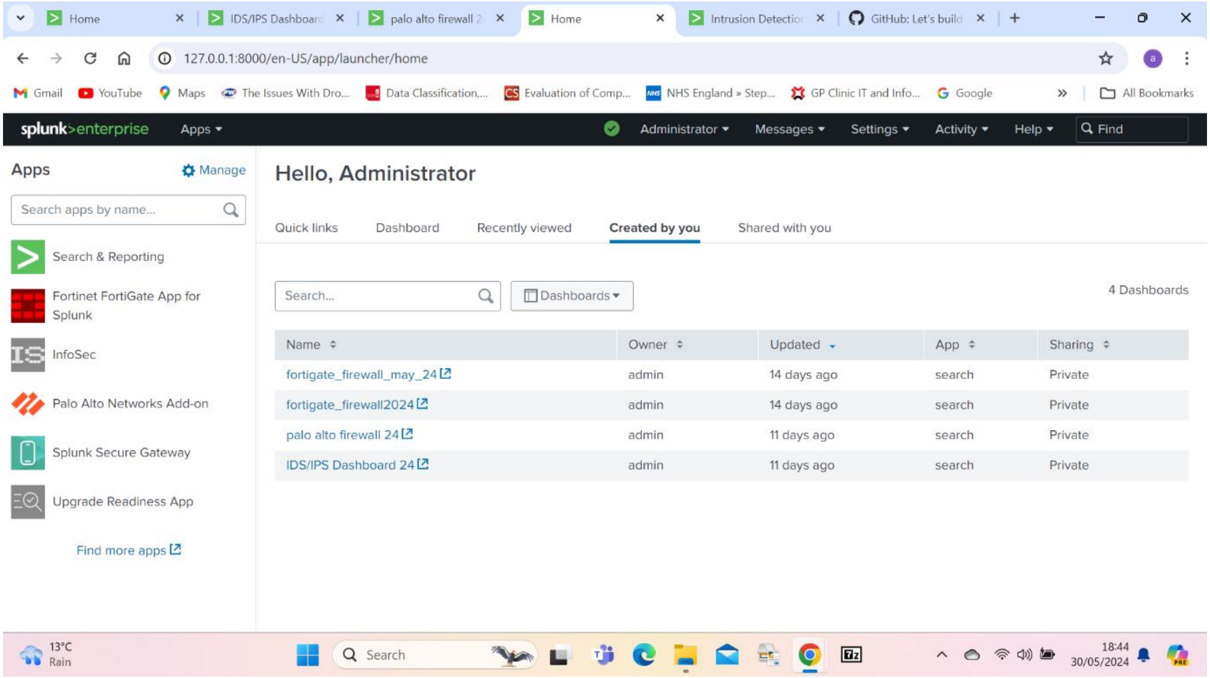
3. Suricata Configuration

Installation

Install Suricata using the package manager or by building it from source. For example, on Ubuntu:

Configuration

Configure the **suricata.yaml** file to enable JSON output and specify the network interfaces to monitor.



Hello, Administrator

Name	Owner	Updated	App	Sharing
fortigate_firewall_may_24	admin	14 days ago	search	Private
fortigate_firewall2024	admin	14 days ago	search	Private
palo alto firewall 24	admin	11 days ago	search	Private
IDS/IPS Dashboard 24	admin	11 days ago	search	Private

Infosec for IDS

4. Splunk Configuration

Installation

Install Splunk Enterprise or Splunk Cloud as per the official Splunk Installation Guide.

Data Ingestion

1-Set Up Data Inputs:

In Splunk, go to **Settings > Data Inputs > Files & Directories**

Add the directory where Suricata logs are stored (e.g., **/var/log/suricata**).

2-Configure Source Type:

Set the source type to **json_suricata** for Suricata JSON logs.

5. Data Parsing and Field Extraction

Use Splunk's Field Extractor to create field extractions for the Suricata logs.

Some Queries for Practice and Check the Data Parsing

index=suricata | stats count by alert.signature

index=suricata | table timestamp src_ip dest_ip proto alert.signature index=suricata | timechart span=1h count by alert.severity

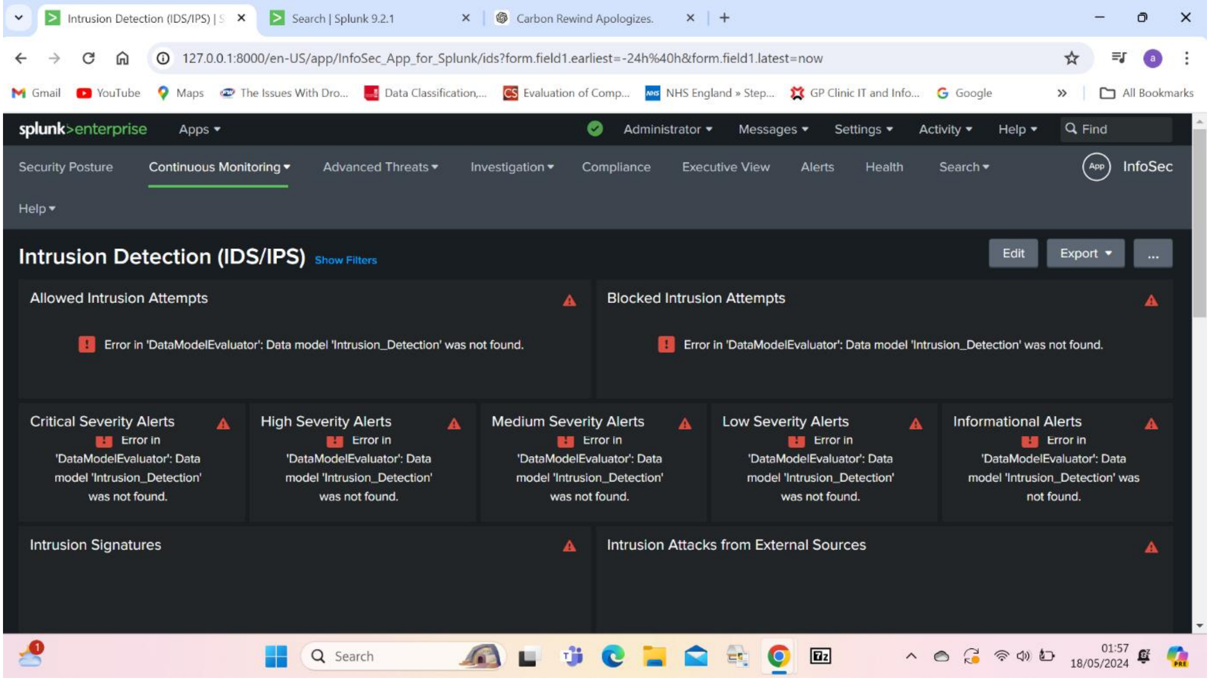
6. Dashboard Design

Creating the Dashboard

1-Create a New Dashboard:

In Splunk, go to **Dashboards** and click **Create New Dashboard**.

Name the dashboard **IDS Dashboard**.



Intrusion Detection (IDS/IPS) Show Filters

Allowed Intrusion Attempts

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

Blocked Intrusion Attempts

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

Critical Severity Alerts

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

High Severity Alerts

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

Medium Severity Alerts

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

Low Severity Alerts

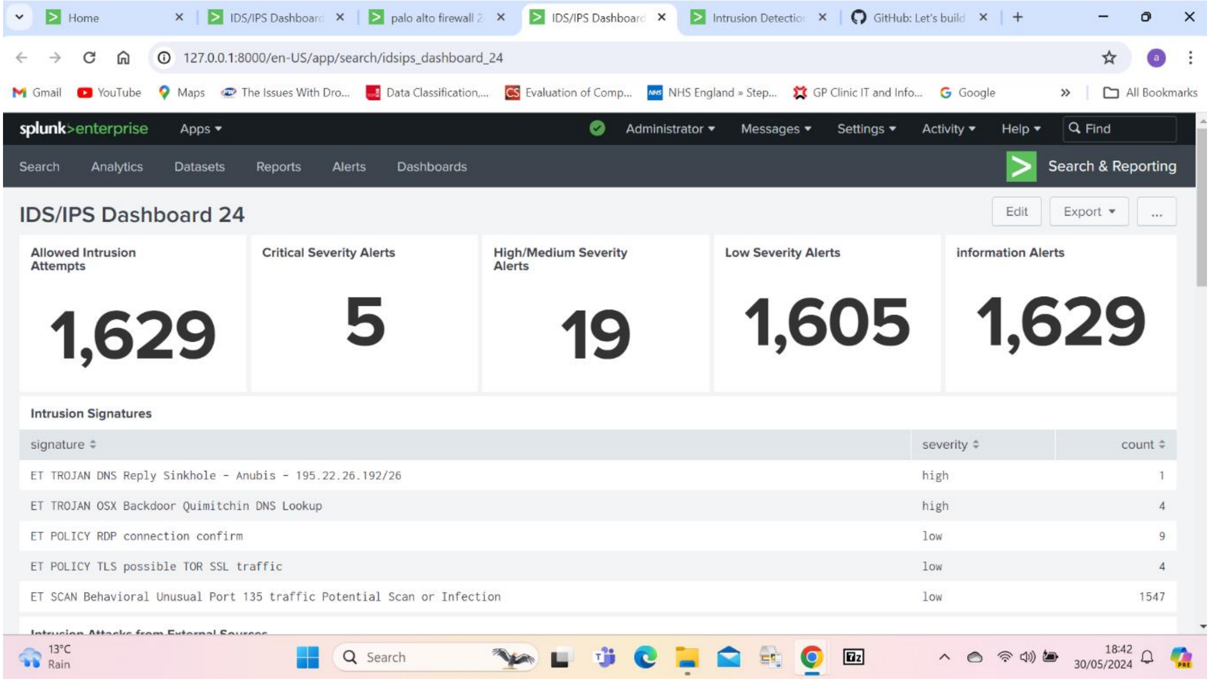
Error in 'DataModelEvaluator': Data model 'Intrusion_Detection' was not found.

Informational Alerts

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

Intrusion Signatures

Intrusion Attacks from External Sources



IDS/IPS Dashboard 24

Allowed Intrusion Attempts	Critical Severity Alerts	High/Medium Severity Alerts	Low Severity Alerts	information Alerts
1,629	5	19	1,605	1,629

Intrusion Signatures

signature	severity	count
ET TROJAN DNS Reply Sinkhole - Anubis - 195.22.26.192/26	high	1
ET TROJAN OSX Backdoor Quimitchin DNS Lookup	high	4
ET POLICY RDP connection confirm	low	9
ET POLICY TLS possible TOR SSL traffic	low	4
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection	low	1547

Intrusion Attacks from External Sources

Adding Panels

1-Add Panel for Top Alerts:

Add a new panel with the following query:

index=suricata | top alert.signature

2-Add Panel for Alerts Over Time:

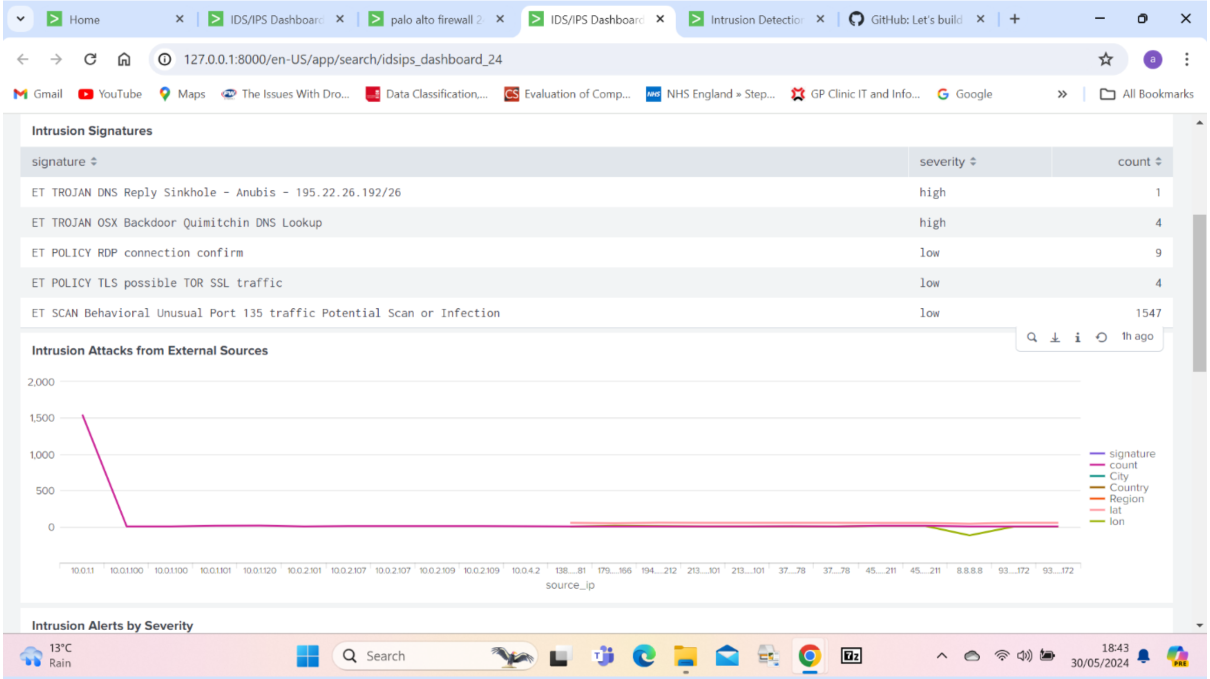
Add a timechart panel with the following query:

index=suricata | timechart span=1h count by alert.signature

3-Add Panel for Source IPs:

Add a table panel with the following query:

index=suricata | top src_ip

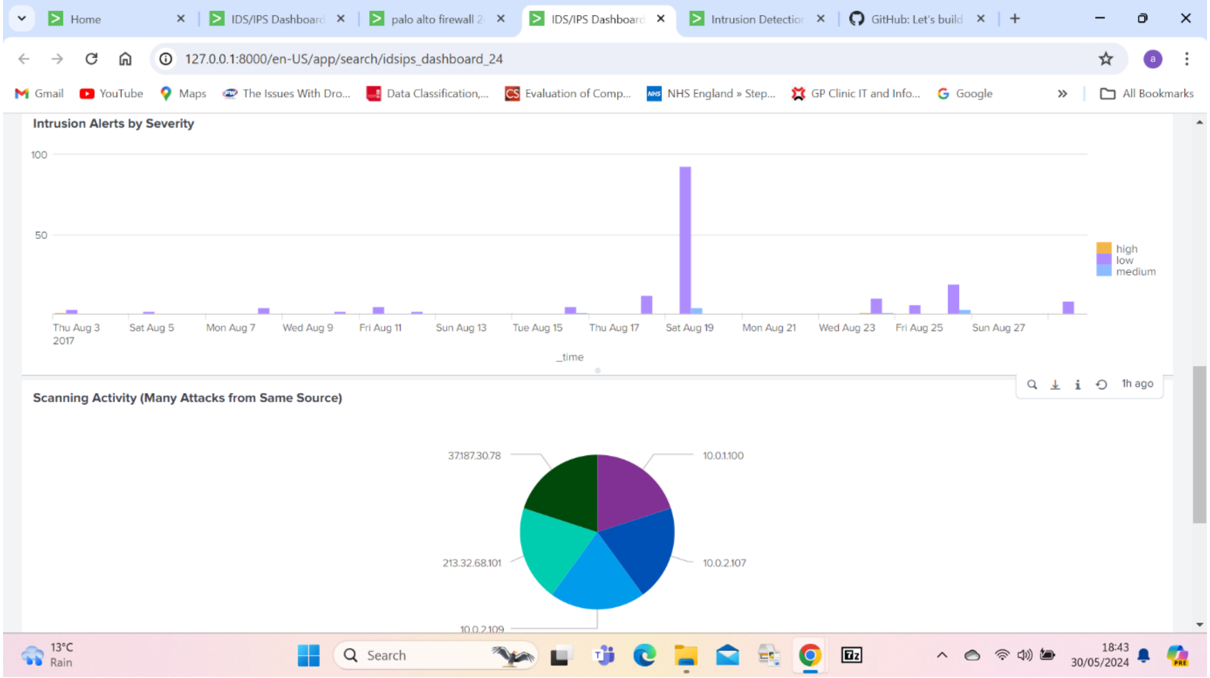


Intrusion Signatures

signature ⇕	severity ⇕	count ⇕
ET TROJAN DNS Reply Sinkhole - Anubis - 195.22.26.192/26	high	1
ET TROJAN OSX Backdoor Quimitchin DNS Lookup	high	4
ET POLICY RDP connection confirm	low	9
ET POLICY TLS possible TOR SSL traffic	low	4
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection	low	1547

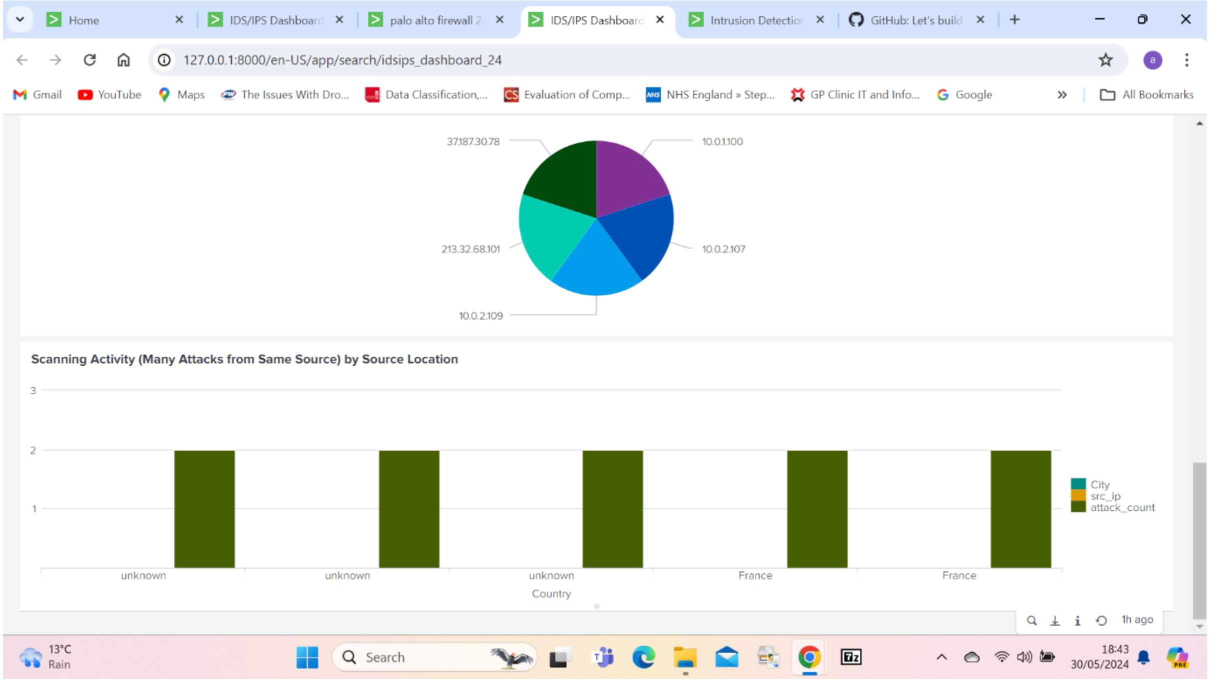
Intrusion Attacks from External Sources

Intrusion Alerts by Severity



Intrusion Alerts by Severity

Scanning Activity (Many Attacks from Same Source)



7. Alerts Configuration

Configure alerts to notify you of critical IDS events.

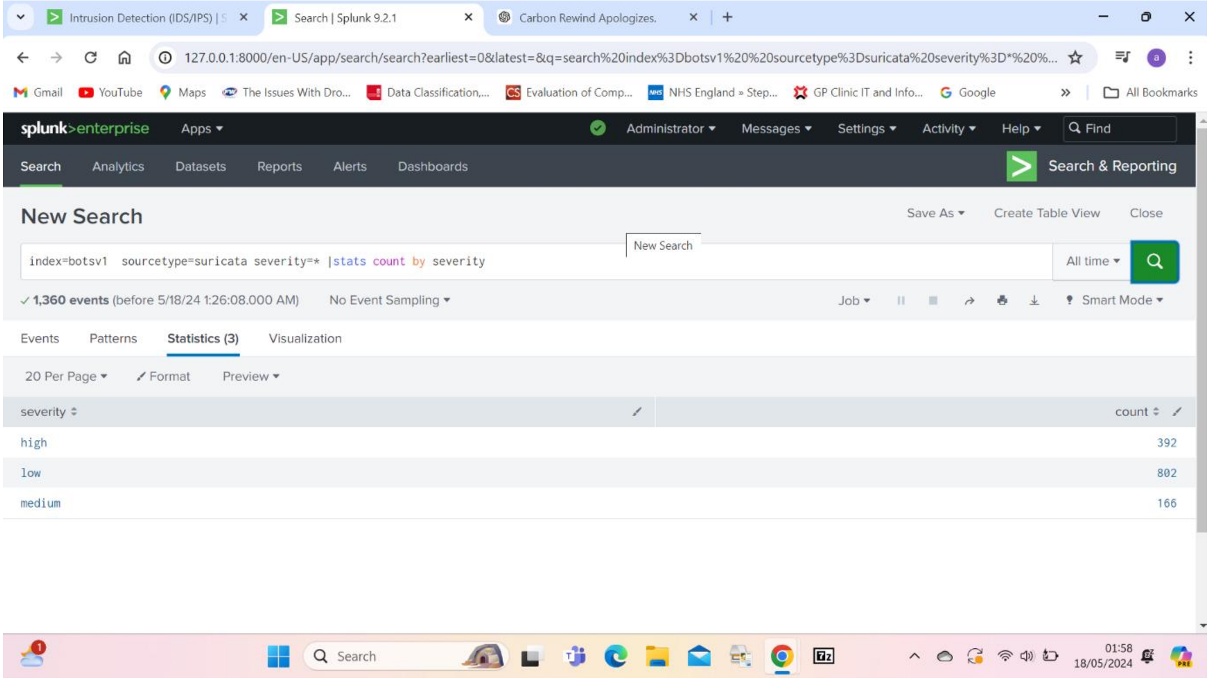
Creating an Alert

1-Create New Alert:

Go to **Settings > Searches, Reports, and Alerts**.

Create a new alert with the following query:

index=suricata alert.severity=high



```
index=botsv1  sourcetype=suricata severity=* |stats count by severity
```

✓ 1,360 events (before 5/18/24 1:26:08.000 AM) No Event Sampling

severity	count
high	392
low	802
medium	166

2-Set Alert Conditions:

Set the alert to trigger when the number of events exceeds a threshold.

3-Configure Alert Actions:

Set up email notifications or other actions.

8. Testing and Validation

Test the IDS setup by generating test traffic and verifying that the alerts and dashboards are functioning as expected.

9. Conclusion

This project demonstrated the integration of Suricata IDS with Splunk, including setup, configuration, data ingestion, dashboard creation, and alerting. The resulting IDS dashboard provides valuable insights into network security threats.