**🛡️ Task 2 Report: Log Analysis using SIEM Tool (Splunk Cloud)**

**1. Objective**

The objective of this task is to analyze log files using a SIEM (Security Information and Event Management) tool to detect unusual or potentially malicious behavior. In this case, we use **Splunk Cloud** to ingest and analyze access logs.

### ****2. Tool Used****

* **SIEM Tool**: Splunk Cloud
* **Log Source**: sample\_access.log
* **Log Type**: Web server access logs
* **Sourcetype**: access

### ****3. Search Queries Used****

Here are the Splunk search queries used for the analysis:

**Query 1: All events from access log**

source="sample\_access.log" sourcetype="access"

**Purpose**: Basic extraction of all access log events.

**Query 2: Identify all HTTP POST requests**

source="sample\_access.log" sourcetype="access" method=POST

**Purpose**: Find all POST requests to check for login attempts or data submission.

**Query 3: Find failed login attempts**

source="sample\_access.log" sourcetype="access" status=401

**Purpose**: Detect unauthorized login attempts using HTTP 401 status.

**Query 4: Check for admin page access attempts**

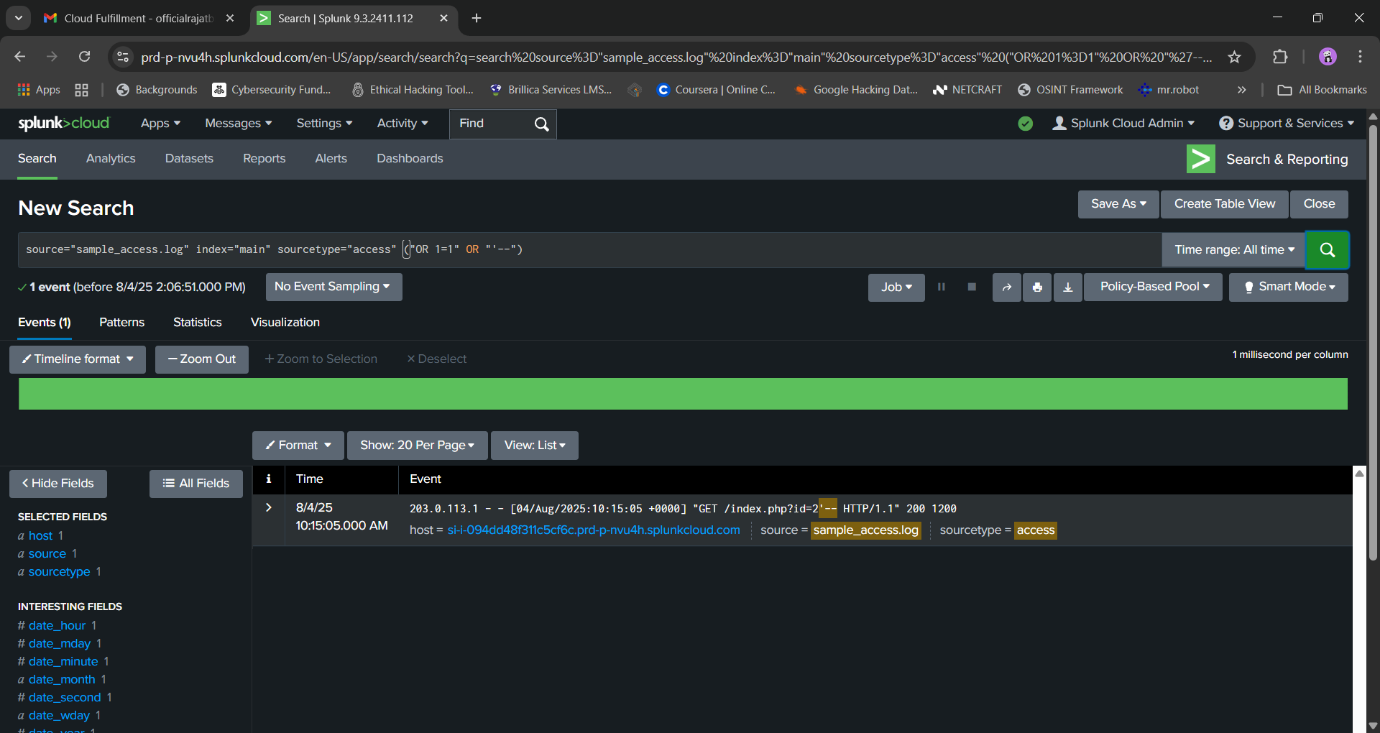
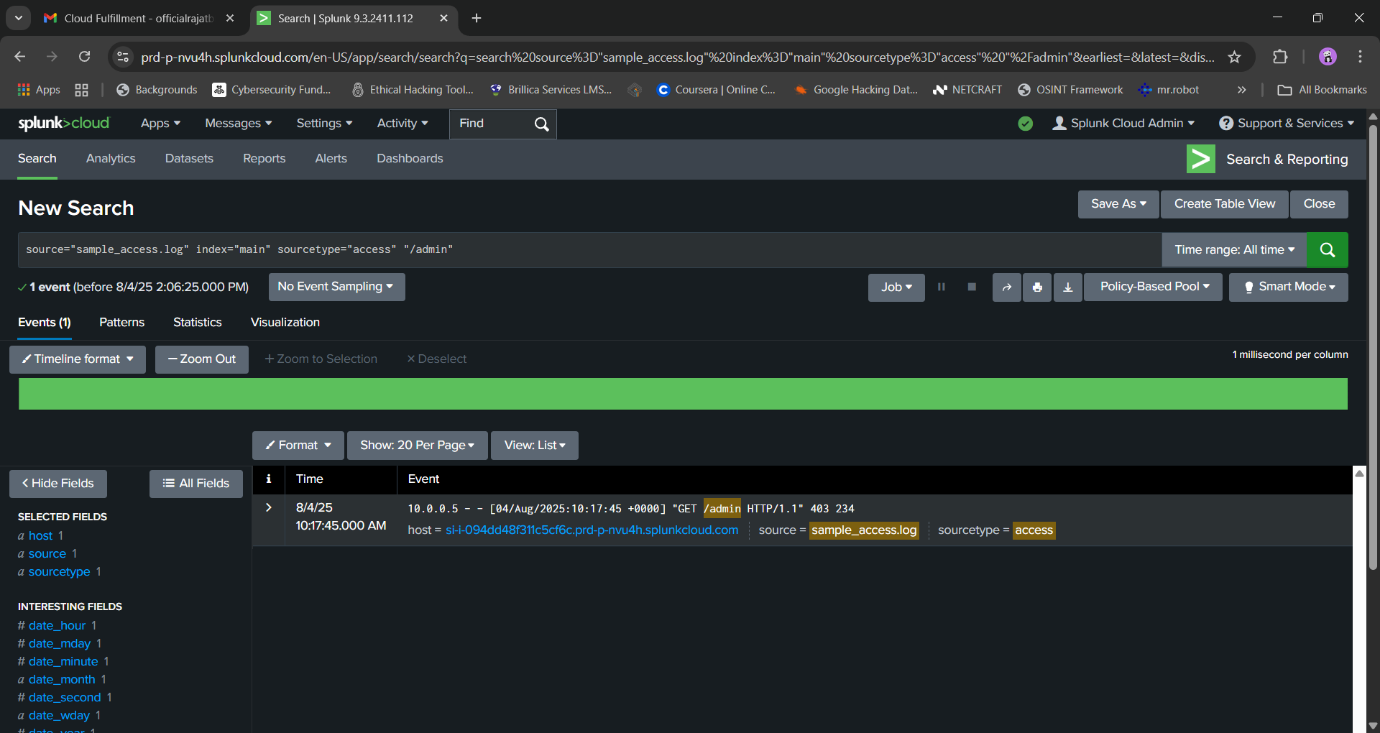
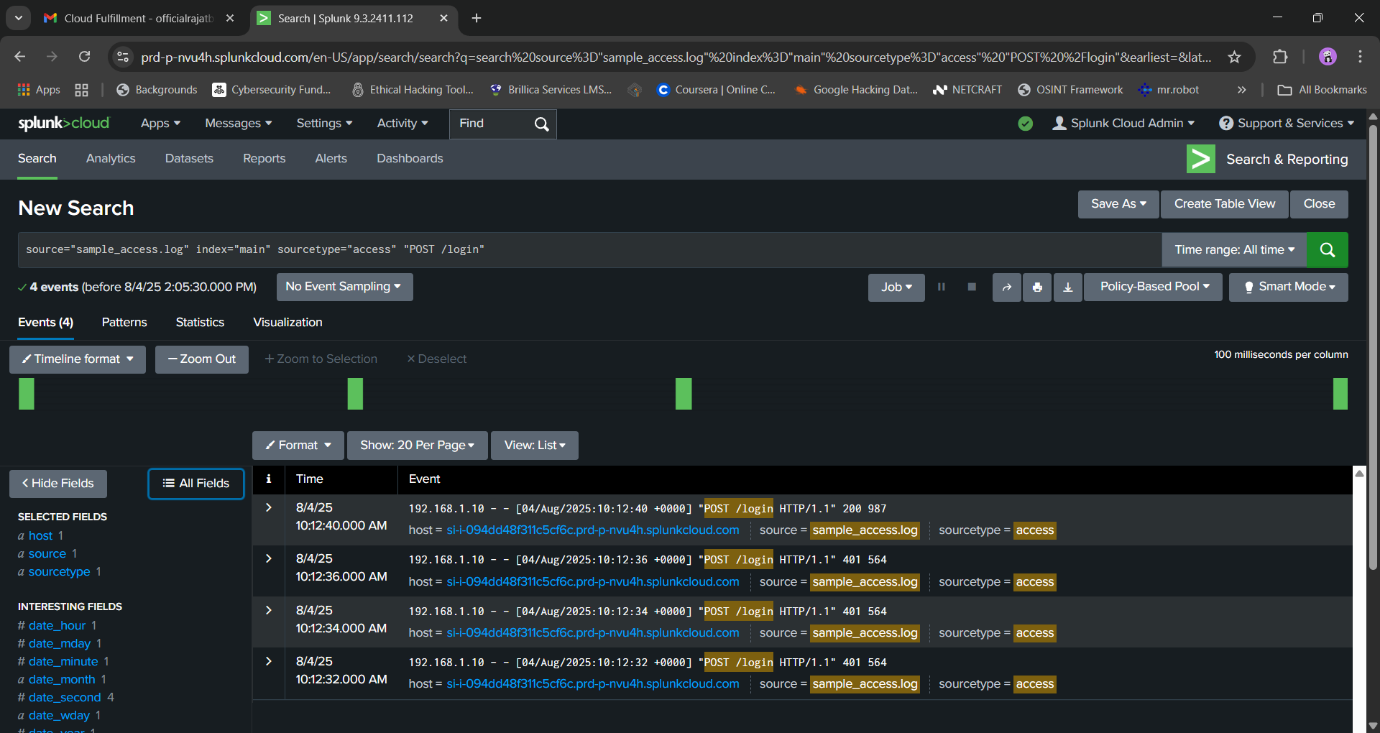
source="sample\_access.log" sourcetype="access" uri="/admin"

**Purpose**: See if anyone is trying to access restricted /admin endpoints.

**Query 5: SQL Injection Indicators**

source="sample\_access.log" sourcetype="access" uri="\*' OR '1'='1\*"

**Purpose**: Detect possible SQL Injection attempts in the request URL.



### ****4. Observations from Logs****

* Multiple failed login attempts (status code 401), possible brute force attempts.
* Suspicious requests to /admin endpoint.
* One or more SQL-like patterns in request parameters, indicating a possible SQL Injection attempt.
* Some successful login attempts followed by POST requests.

### ****6. Conclusion****

The access logs show signs of potential security incidents such as failed login attempts, SQL injection patterns, and access to restricted URLs. These need to be further investigated and monitored.