Splunk Security Incident and Event Management(SIEM) Simulation

**Report On SIEM Tool in Cybersecurity and their Functions.**

Splunk Events by uploading a file(csv) containing logs of events.

This is the starting point of Splunk we see after uploading a log(csv) file.

A **SIEM (Security Information and Event Management)** tool is a cybersecurity platform that aggregates, correlates, and analyses log data from across an organization’s IT infrastructure (servers, networks, applications, etc.) to detect, investigate, and respond to threats in real time.

**Core Functions of a SIEM Tool**

1.**Log Collection & Aggregation**

What it does: Collects logs from firewalls, endpoints, cloud services, and other systems.

Example: Splunk ingests Windows Event Logs, Apache logs, and AWS CloudTrail data.

2. **Threat Detection & Correlation**

What it does: Uses rules/algorithms to link events (e.g., "5 failed logins + malware alert = brute-force attack").

3. **Real-Time Alerting**

What it does: Triggers alerts for suspicious activity (e.g., unauthorized access, data exfiltration).

Example: Email/SMS alerts for admin account lockout.

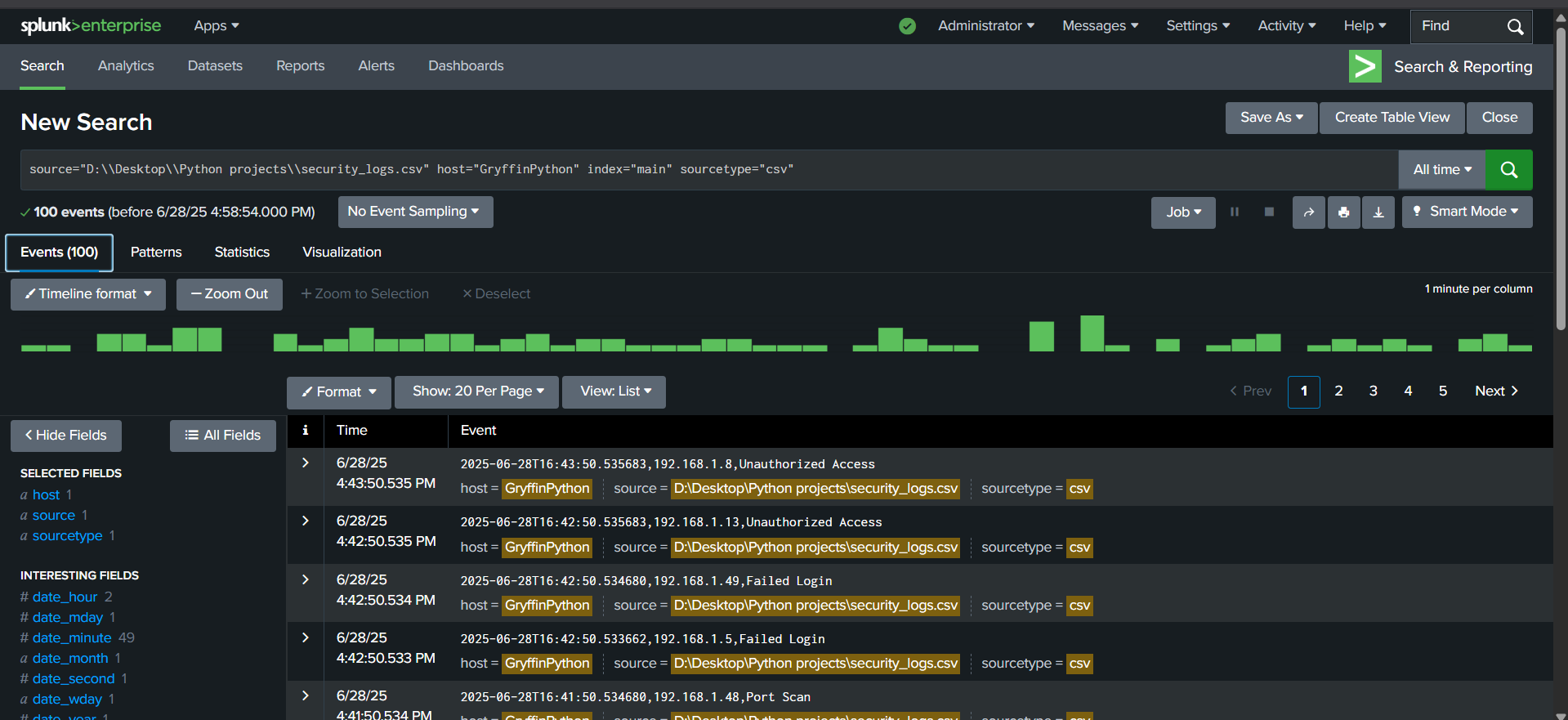
4. **Incident Investigation**

What it does: Provides forensic tools (timelines, dashboards) to trace attack origins.

5. **Compliance Reporting**

What it does: Generates reports for regulations (e.g., GDPR, HIPAA).

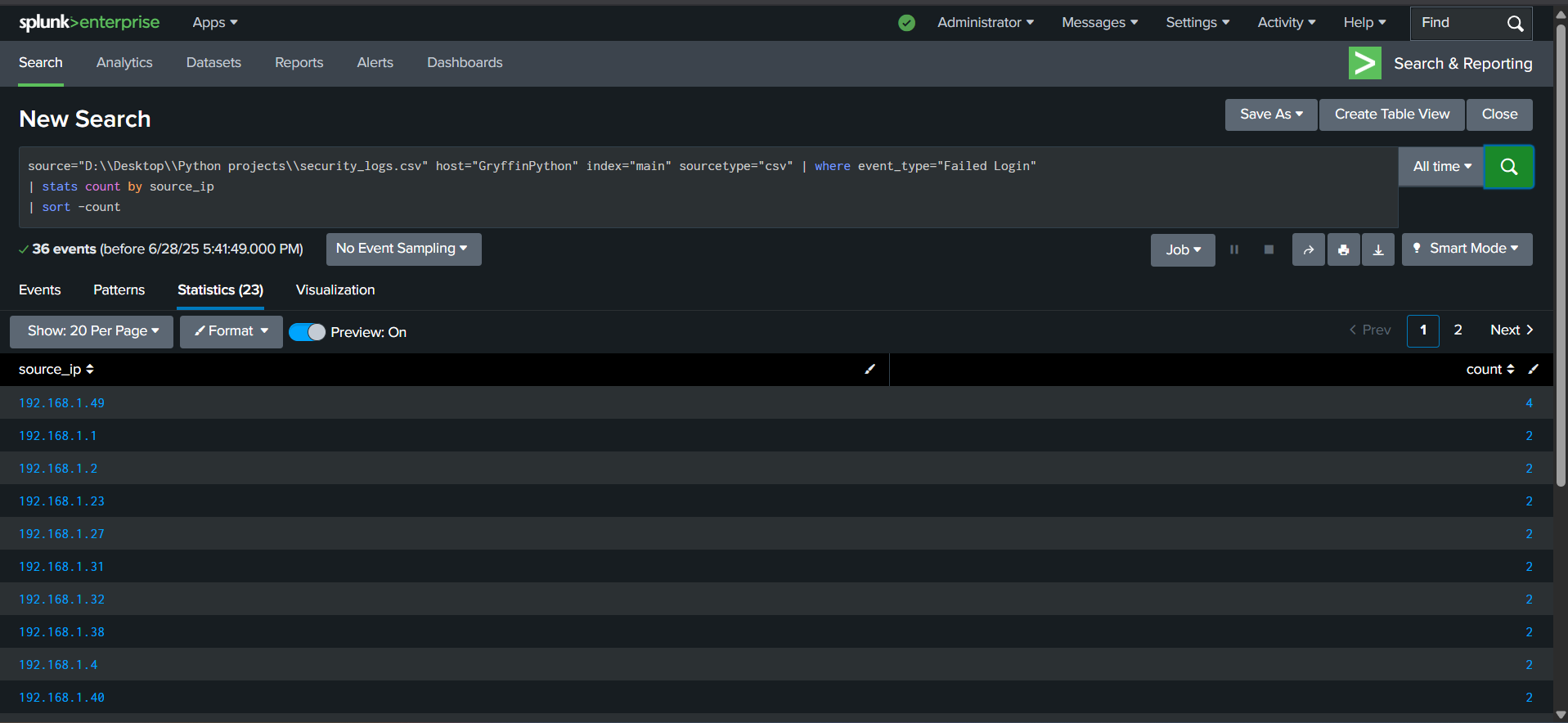
Example: Monthly audit of all privileged account access.



**Splunk Queries**

**Identify Failed Logins (Brute Force)**

Query: source="D:\\Desktop\\Python projects\\security\_logs.csv" index="main"| where event\_type="Failed Login"| stats count by source\_ip| sort -count



**Use Case**: Detect brute-force attacks.

**SOC Action**: Block IPs with count > 5

Mitigation:

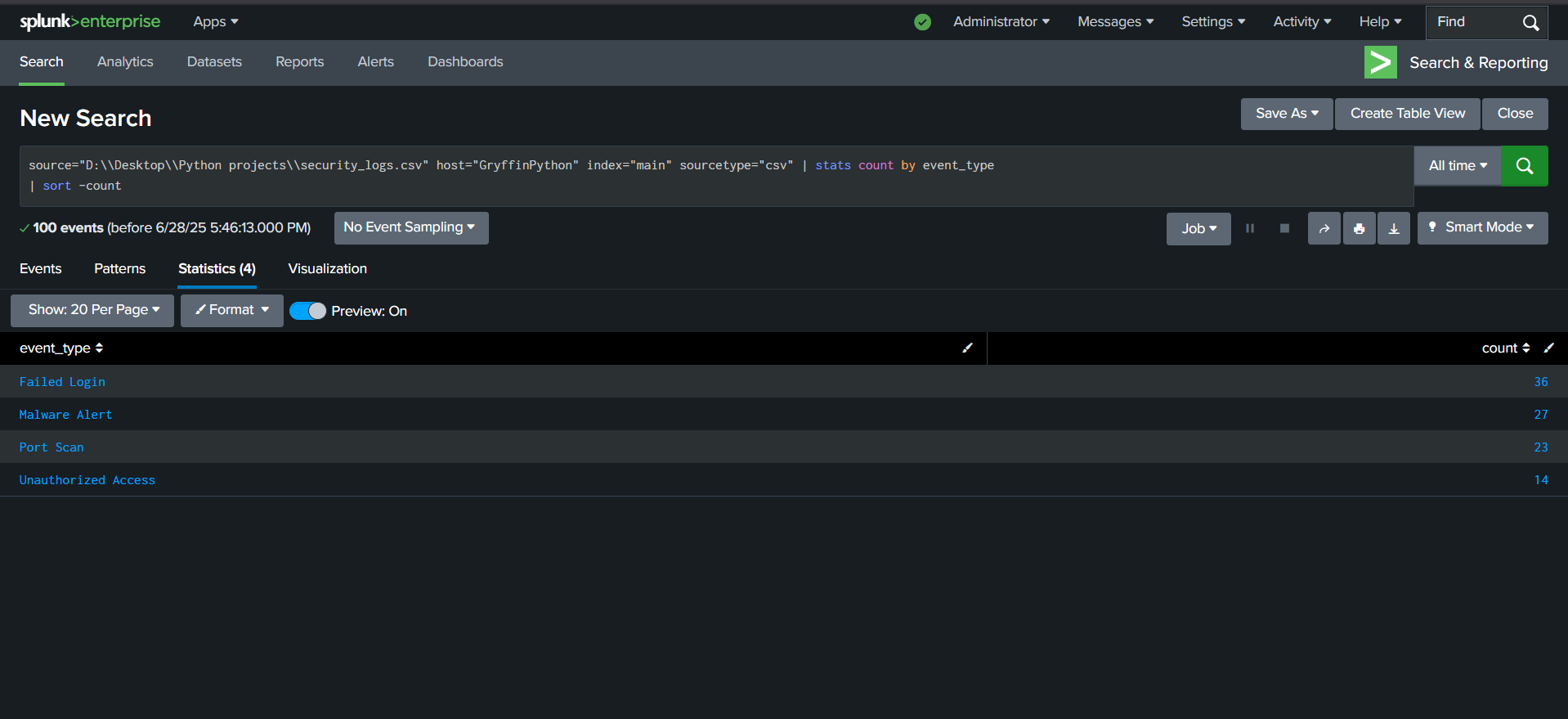
Block the IP at the firewall.

Reset passwords for targeted accounts.

Enforce MFA to prevent future attacks.

**Top Suspicious Event Types**

**source="D:\\Desktop\\Python projects\\security\_logs.csv" index="main"| stats count by event\_type| sort -count**

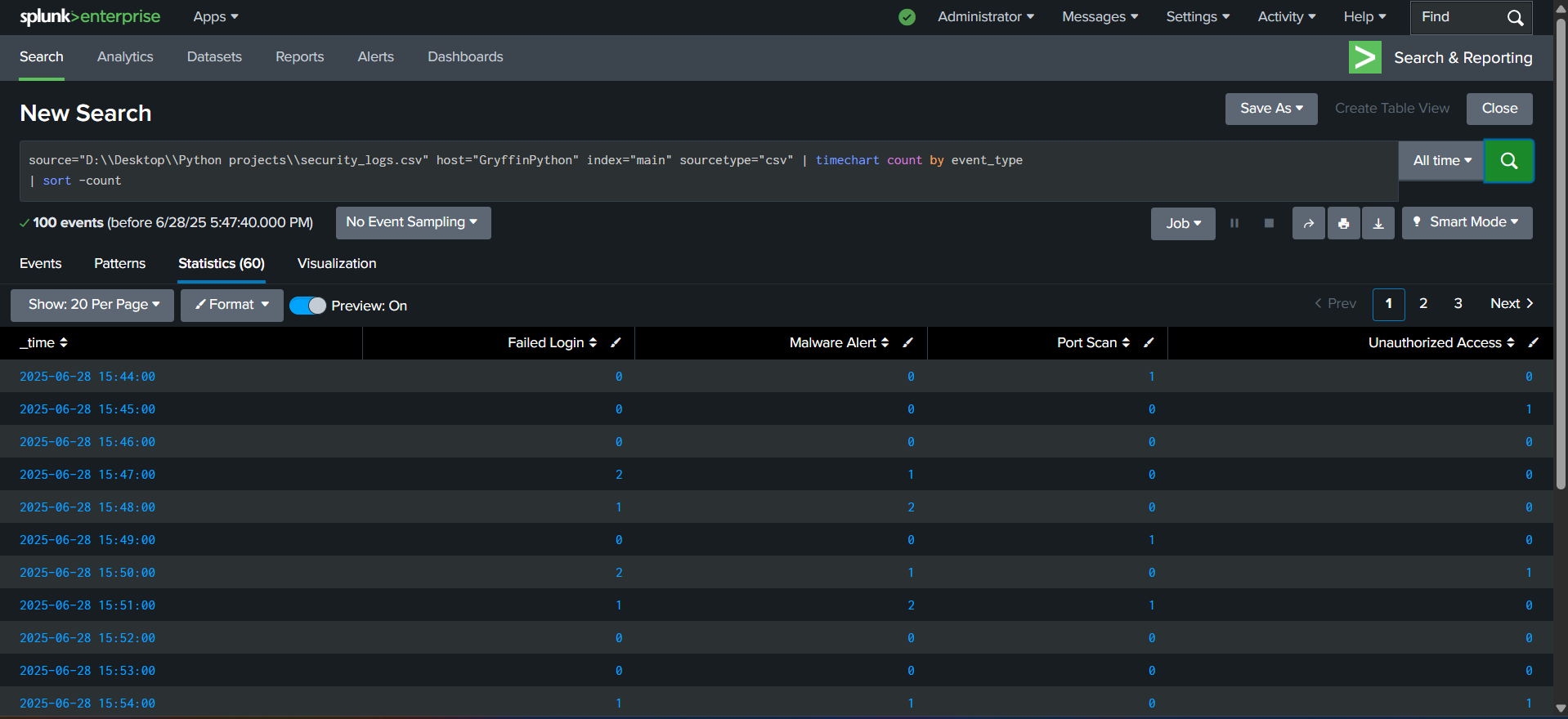
****

**Use Case:**

**Prioritize threats (e.g., "Malware Alert" > "Failed Login").**

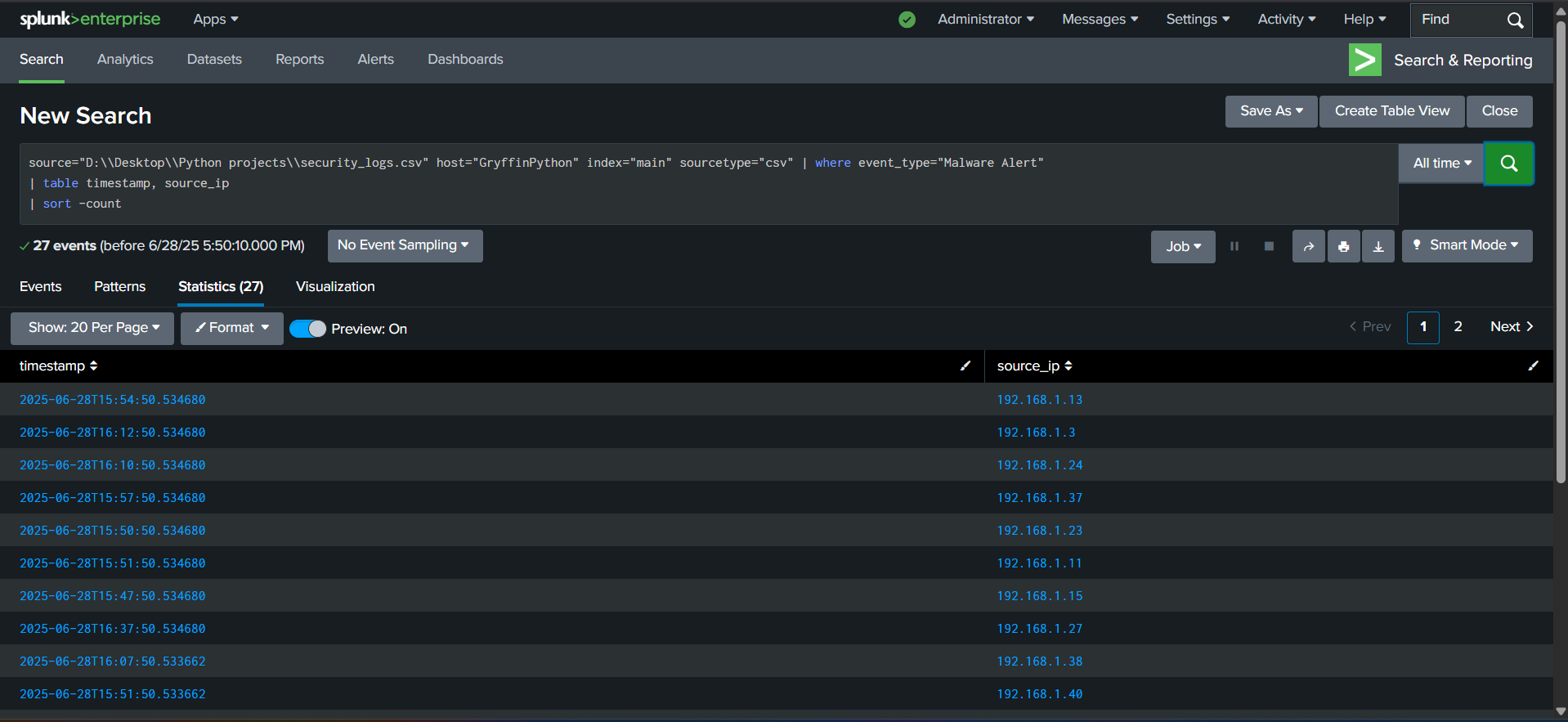
**Timeline of Security Events**

**Use Case: Visualize attack patterns over time.**

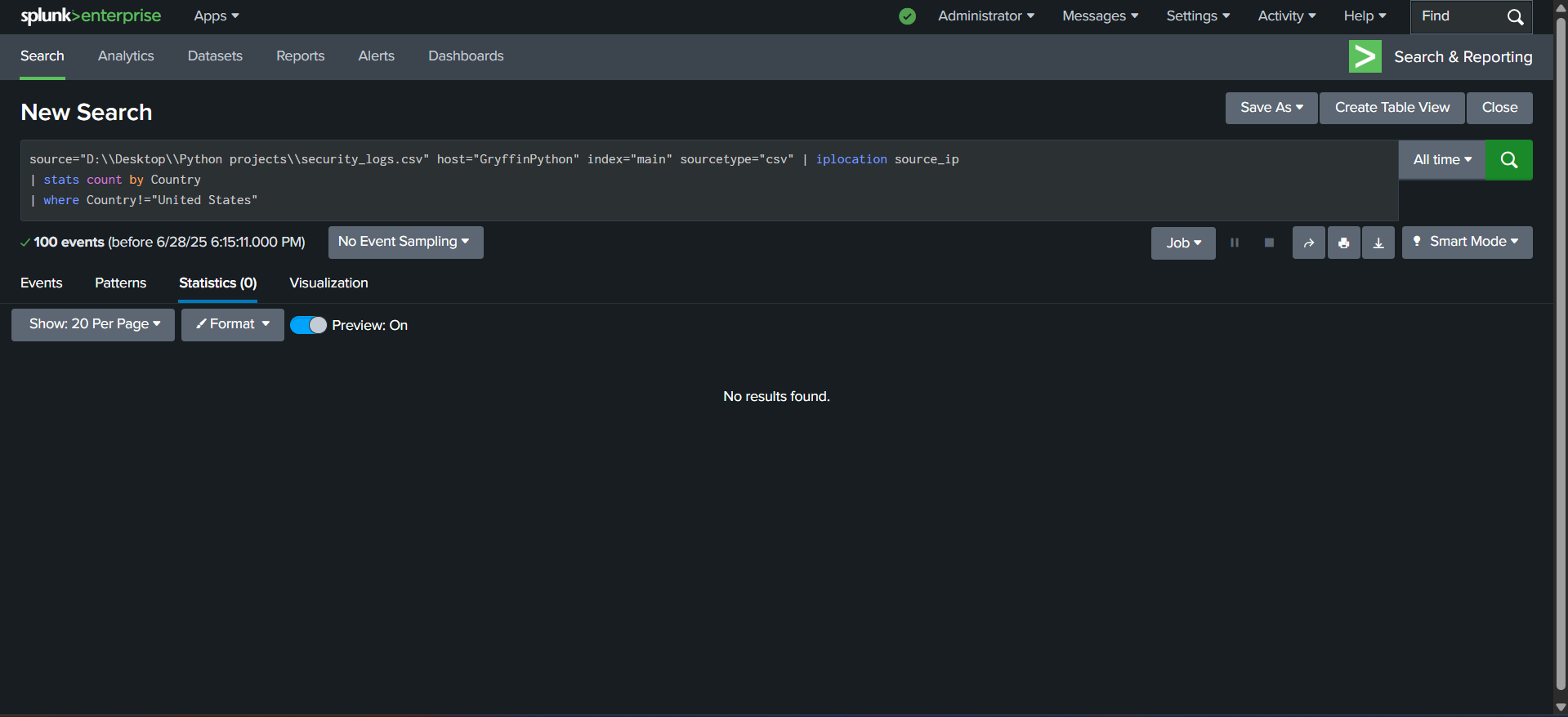
****

**Detect Malware Alerts**

**SOC Action: Isolate infected hosts (source\_ip).**

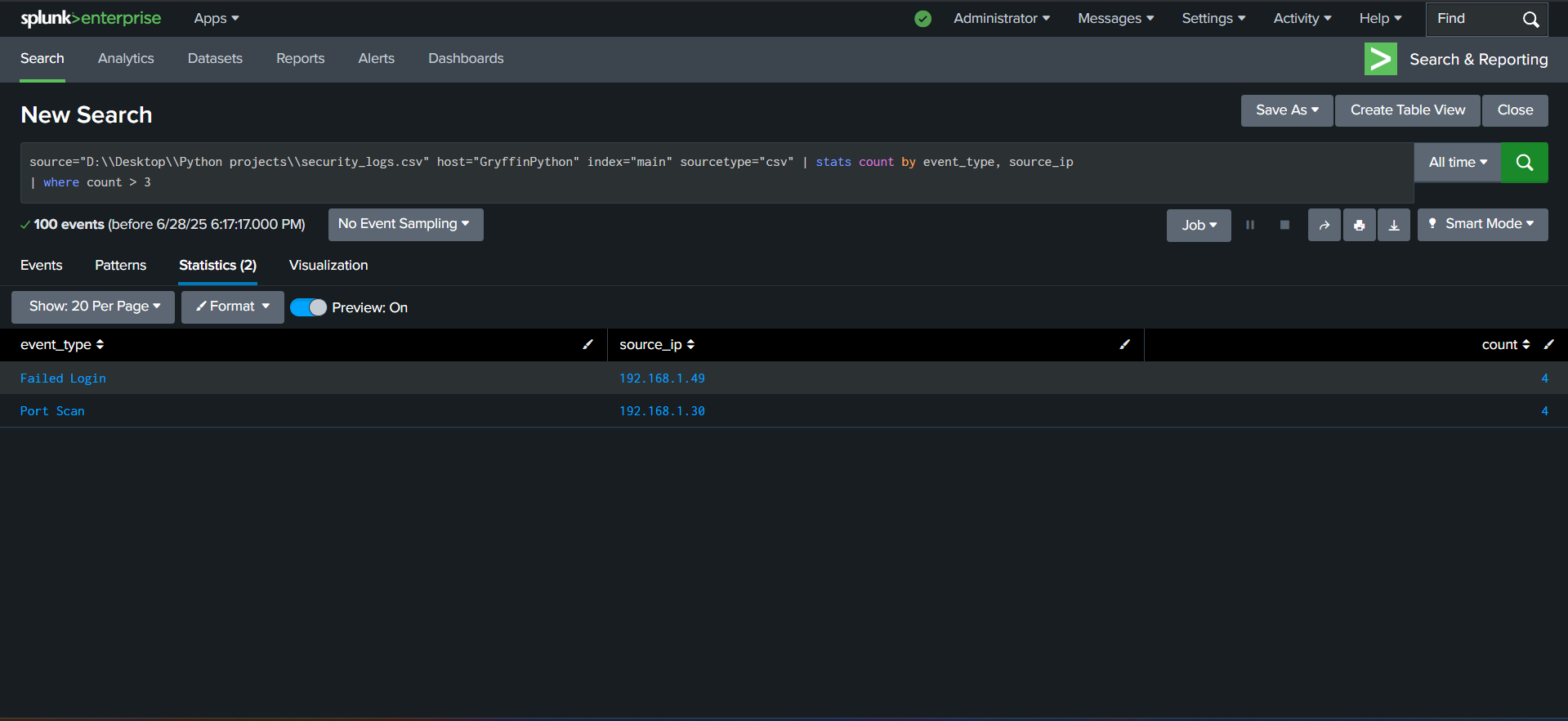
****

**Unusual Geographic IPs**



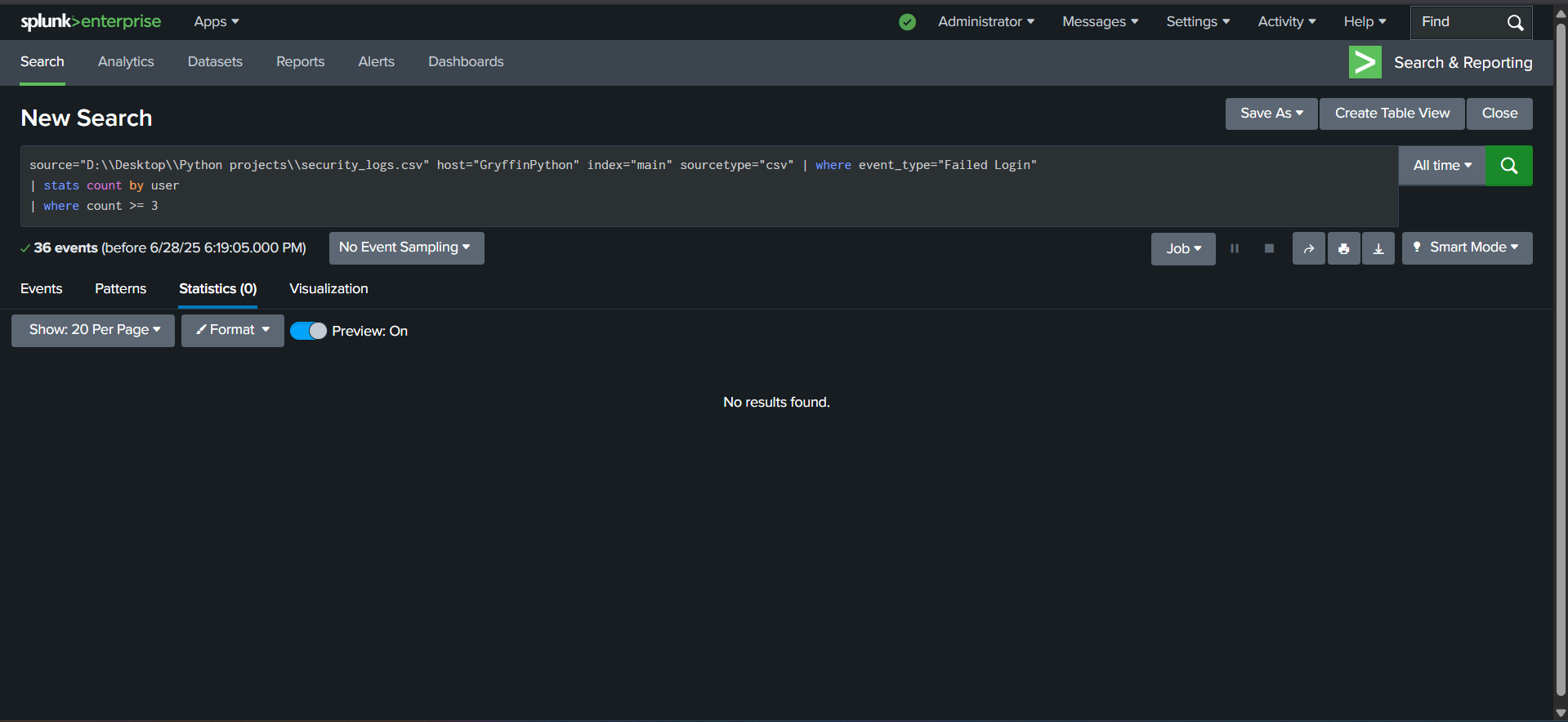
**Use Case**: Flag foreign IPs (e.g., Russia, China).

**High-Volume Events (Threshold Alert)**

****

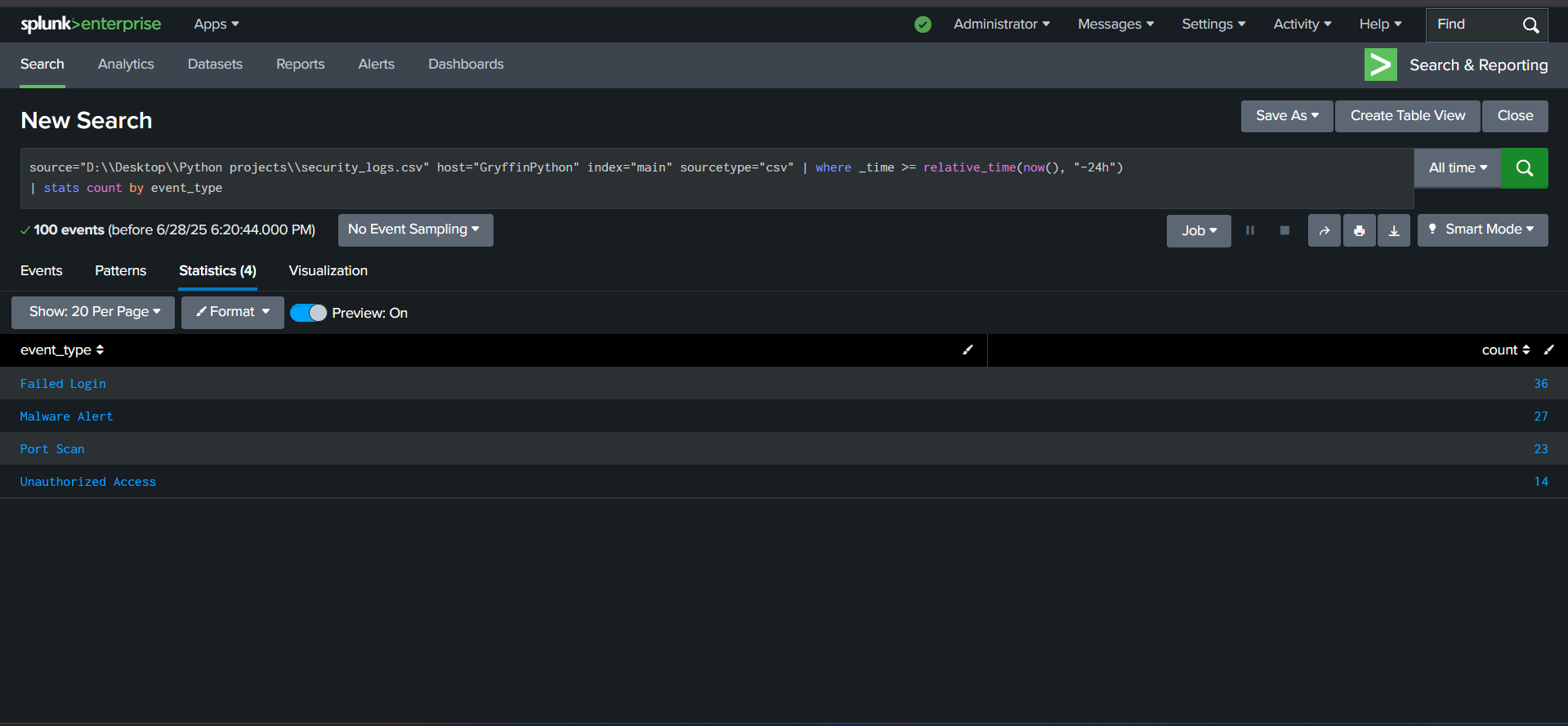
**SOC Action: Create a Splunk alert for count > 3.**

**Account Lockouts**

****

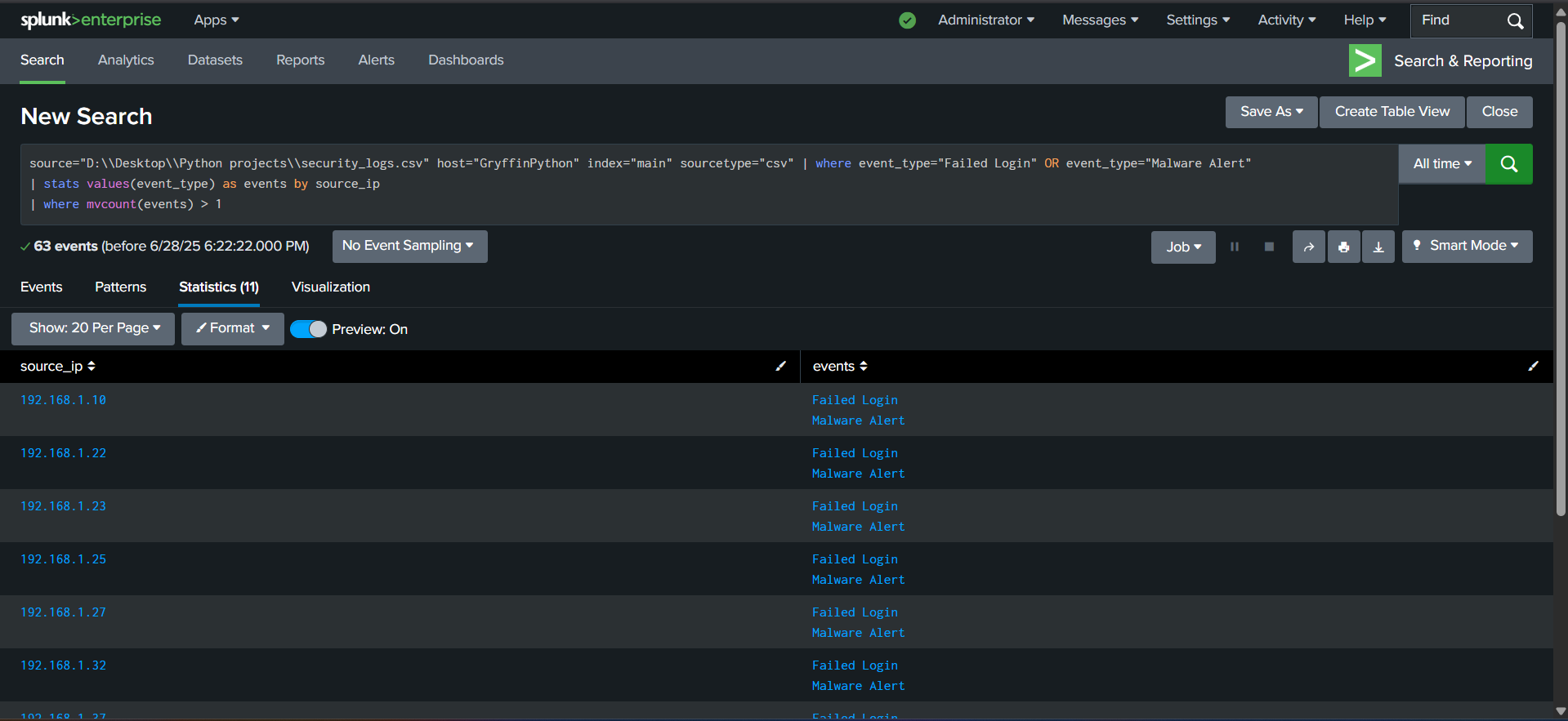
**Use Case: Identify compromised accounts.**

**Events in Last 24 Hours**

****

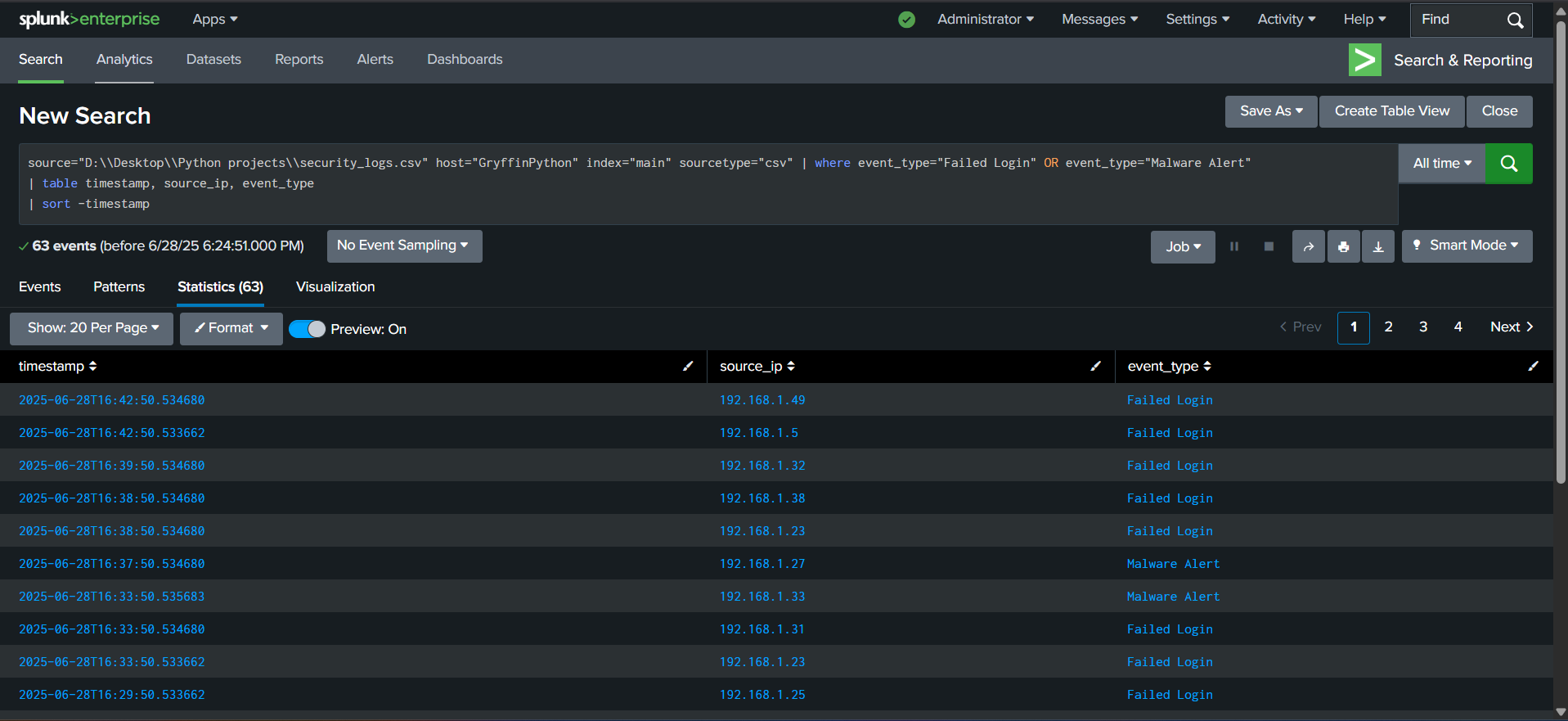
**Use Case: Daily threat summary.**

**Correlate Failed Logins + Malware**

****

**Use Case: Detect multi-stage attacks.**

**Generate an Incident Report**

****

**Export: Click Export > CSV for your incident report.**

**Splunk Dashboard**

This dashboard is made by accumulating multiple searches such as Brute force detection, Top malicious IP’s and Event Distribution in the logs present in the file.

The dashboard helps us in getting a clear summary of the logs that were made by the site that we are monitoring which allows us to learn more about the types of networks that were visiting the site we are monitoring.

Splunk dashboards are **interactive visualizations** that consolidate security data into actionable insights. They help SOC teams:

* **Monitor threats in real-time** (e.g., brute-force attacks, malware).
* **Correlate events** across logs (e.g., failed logins + geographic anomalies).
* **Streamline investigations** with drill-down capabilities.

Purpose:

Detect anomalies (e.g., spikes in failed logins).

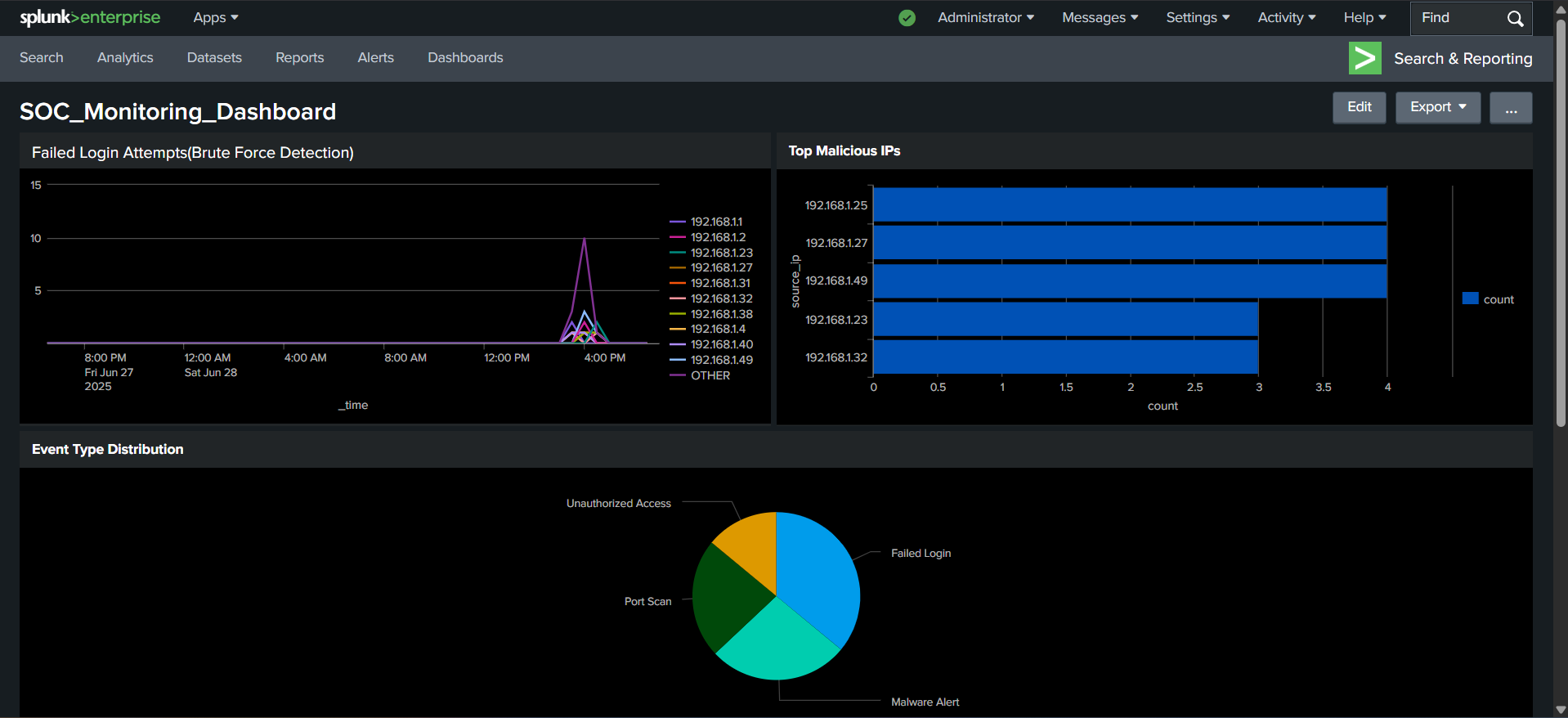
Prioritize incidents (e.g., malware vs. low-risk events).

3. Key Features of Your Dashboard

Real-Time Monitoring: Alerts update as new logs are ingested.

Custom Filters: Add time pickers or event-type dropdowns for deeper analysis.

Exportable Reports: Used for your internship deliverables (PDF/CSV).

****