**Cybersecurity 401**

**Module 2 - Data Security**

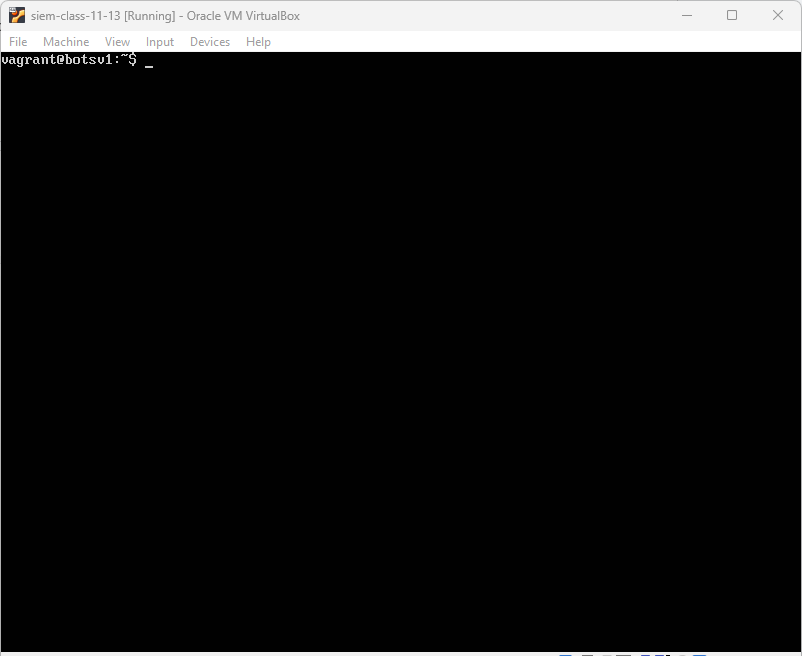
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# **Lab 11 - Foundational SIEM Operations**

# 

| Rodrigo Brasil 11/2023 |

### **Part 1: Staging Splunk**



Splunk VM deployed from code fellows resources:

<https://codefellows.github.io/ops-401-cybersecurity-guide/curriculum/#downloads-table>

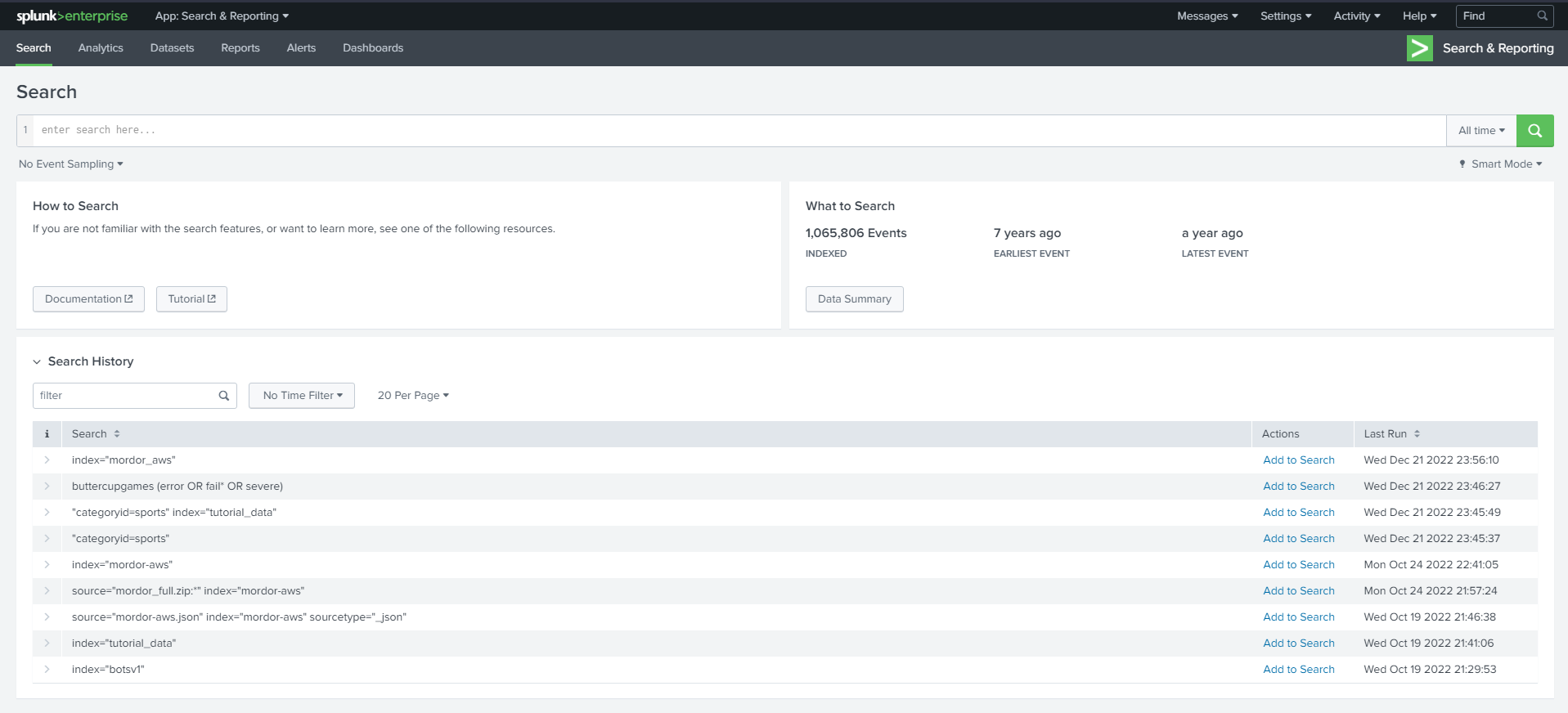


After deploying the machine, checked the machine IP using the command “**ip a**”

The IP for this machine is: “**192.168.1.5**”



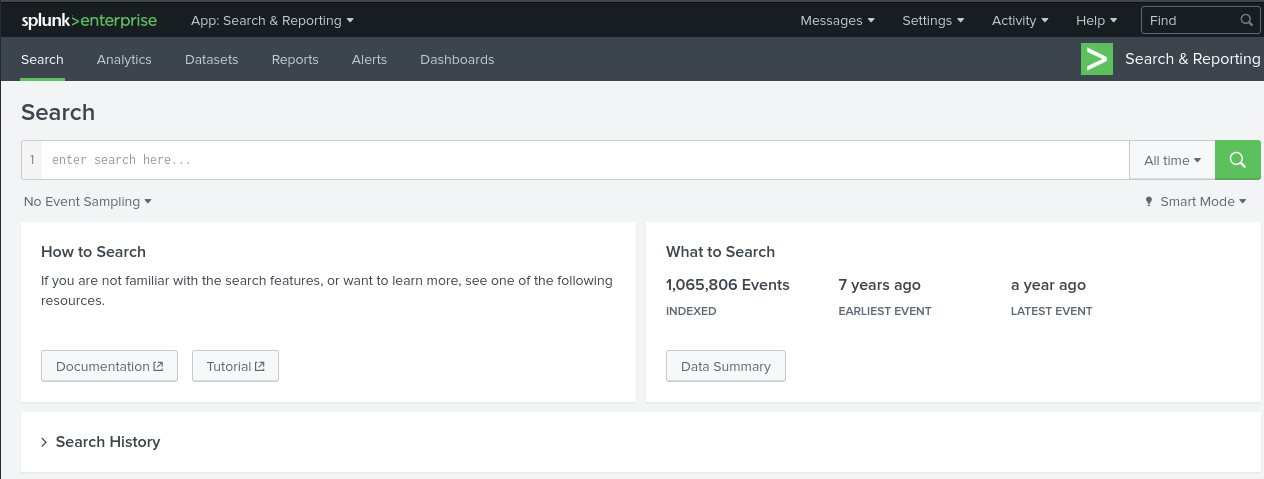
Using the IP gathered from the VM, on the browser typed the IP with the port 8000

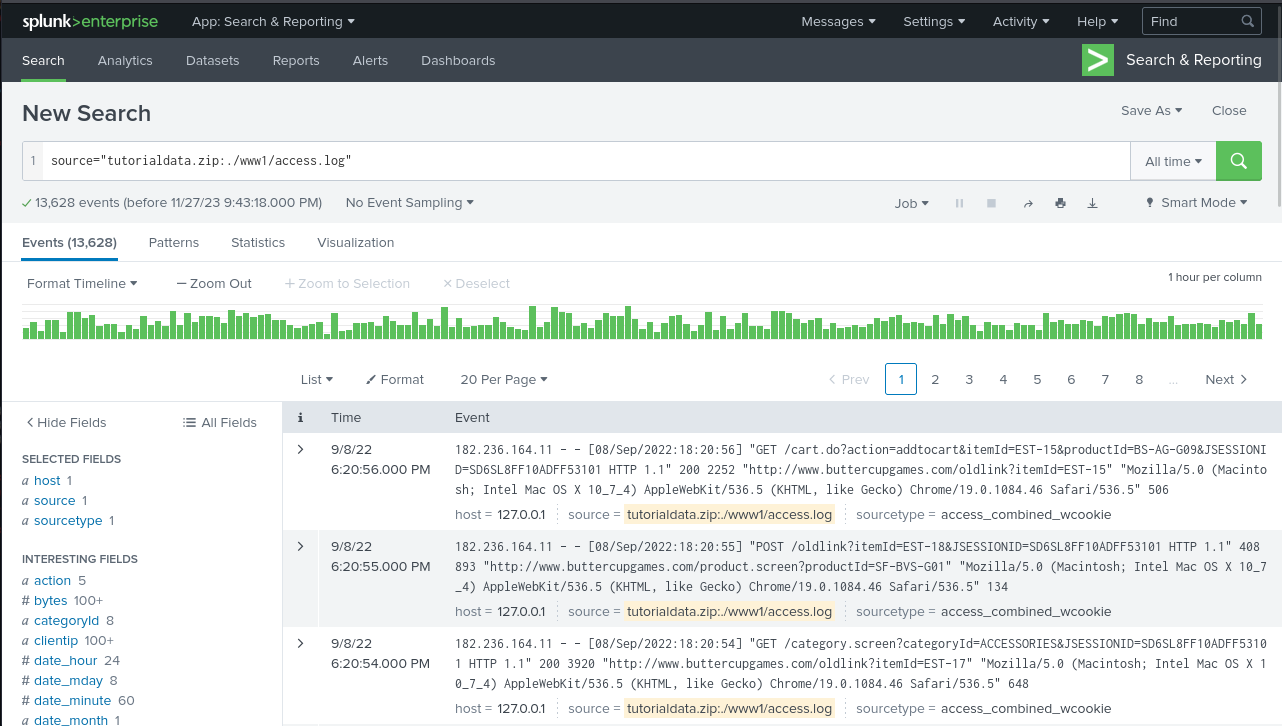


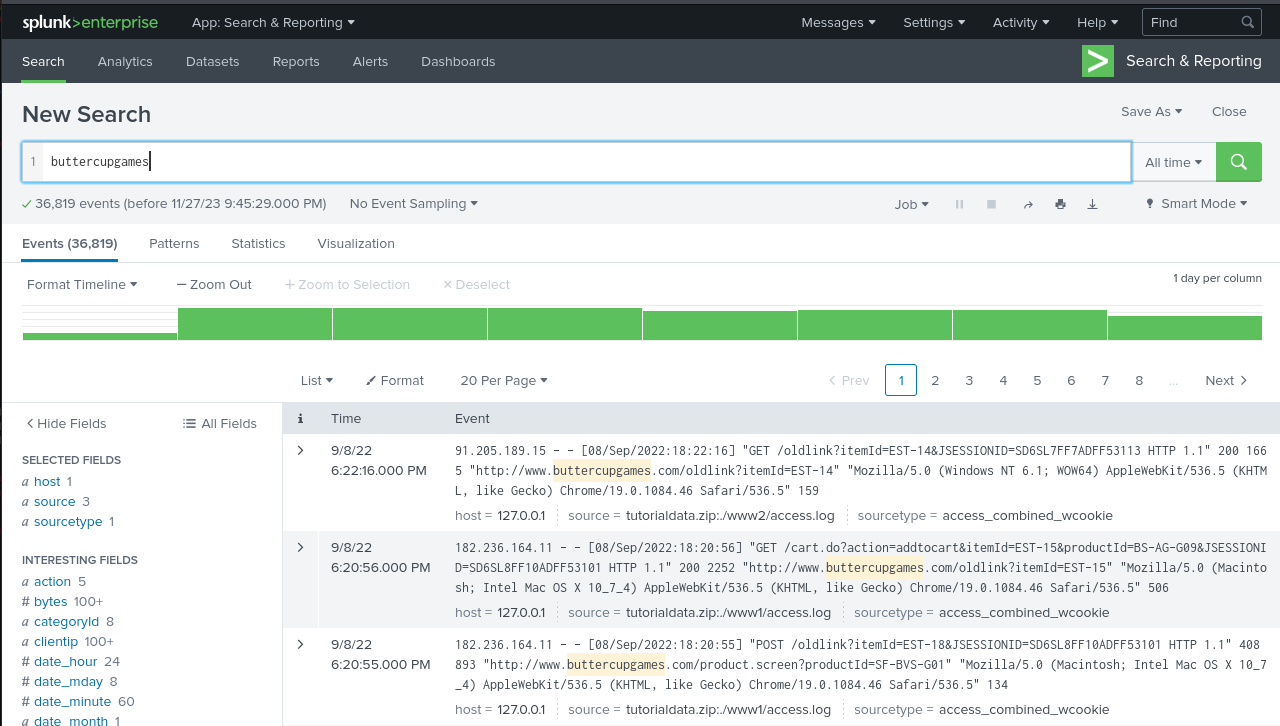
This is what the splunk UI looks like

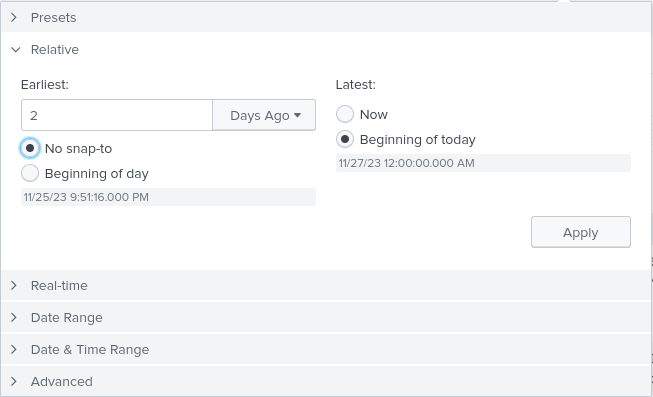
### 

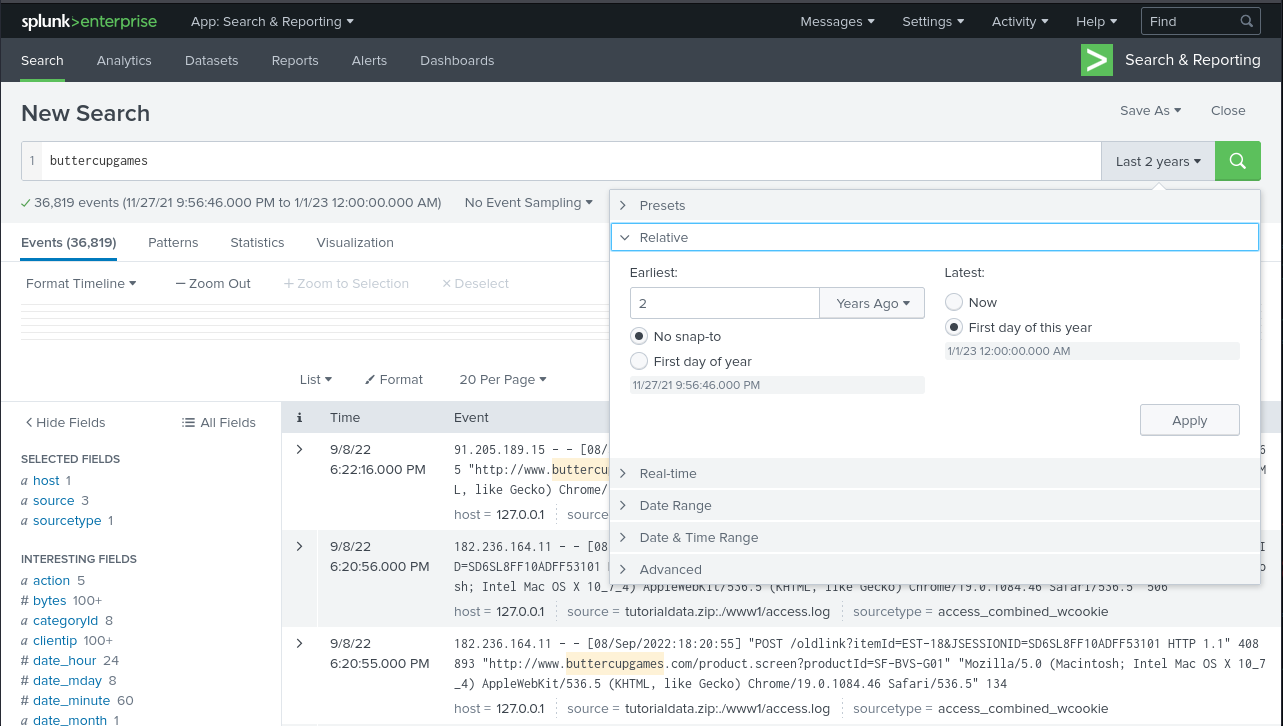
### **Part 2: Incident and Analysis**

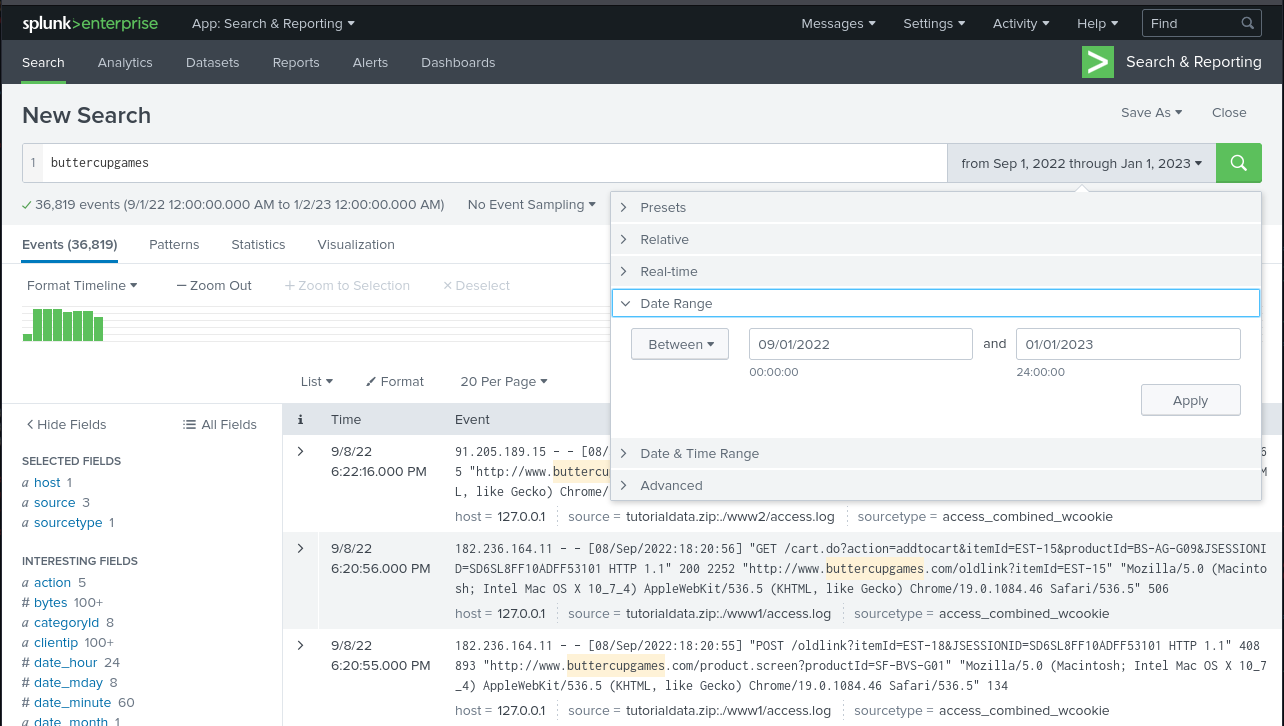


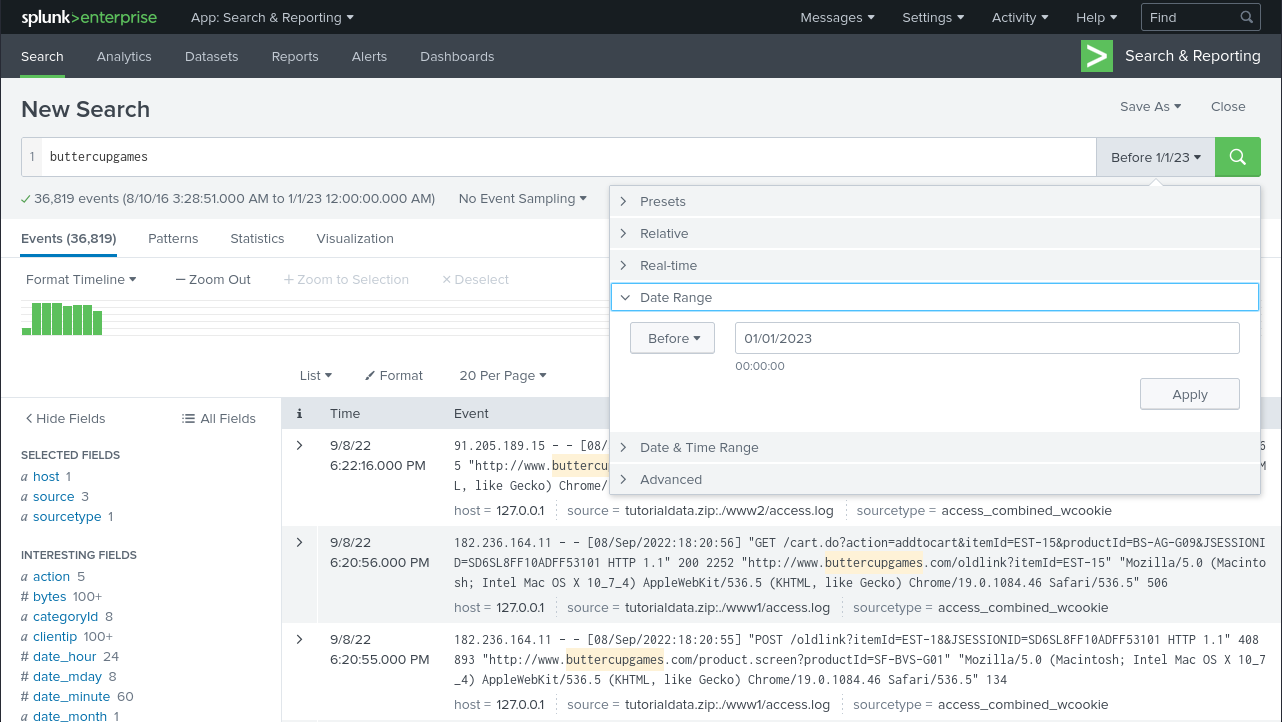


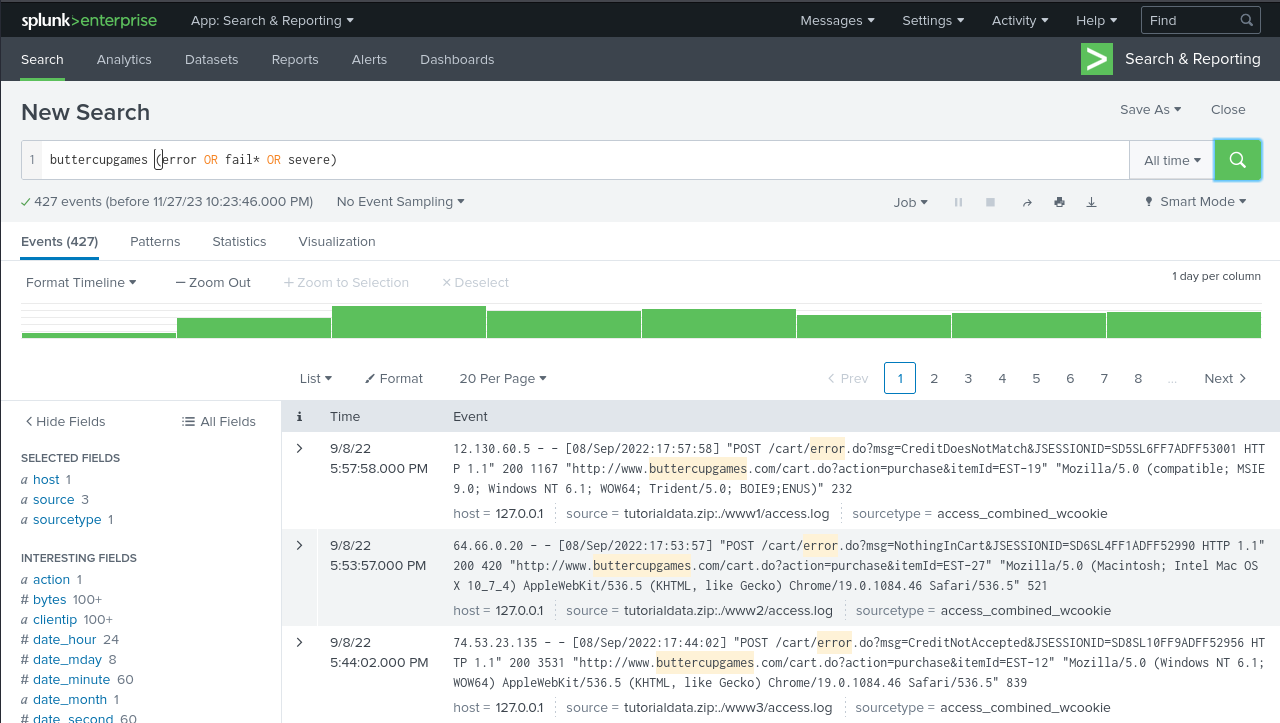












to find out how many errors have occurred on the Buttercup Games website

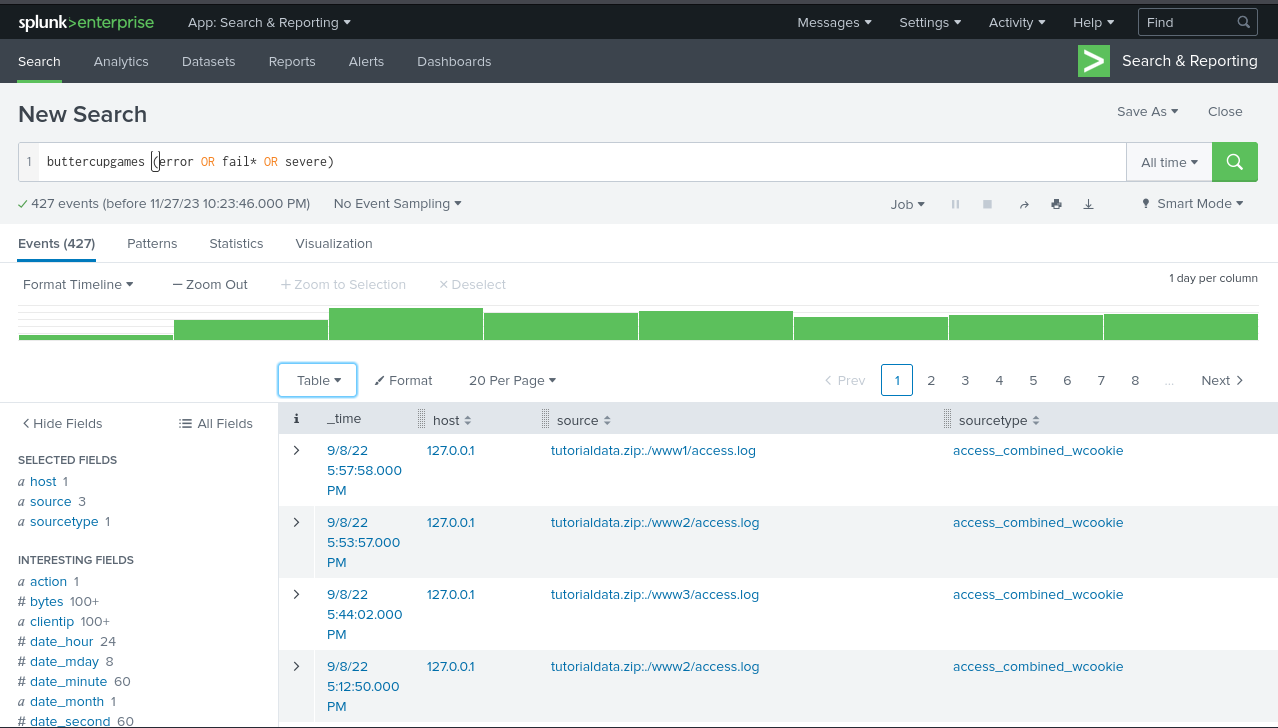
Start a new search.

Change the time range to All time.

To search for the terms error, fail, failure, failed, or severe, in the events that also mention buttercupgames, run the following search: “**buttercupgames (error OR fail\* OR severe)**”

Click the Search icon to the right of the time range picker to run the search.

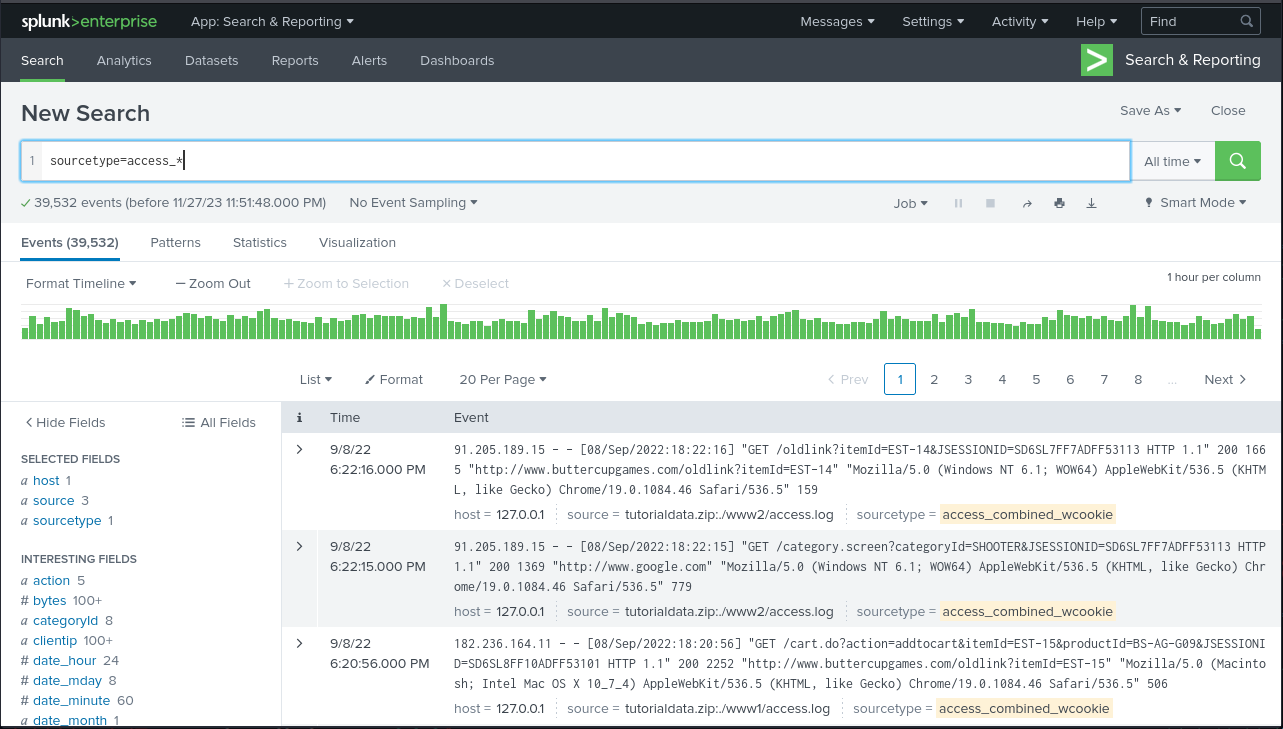
The asterisk ( \* ) character is used as a wildcard character to match fail, failure, failed, failing, and so forth

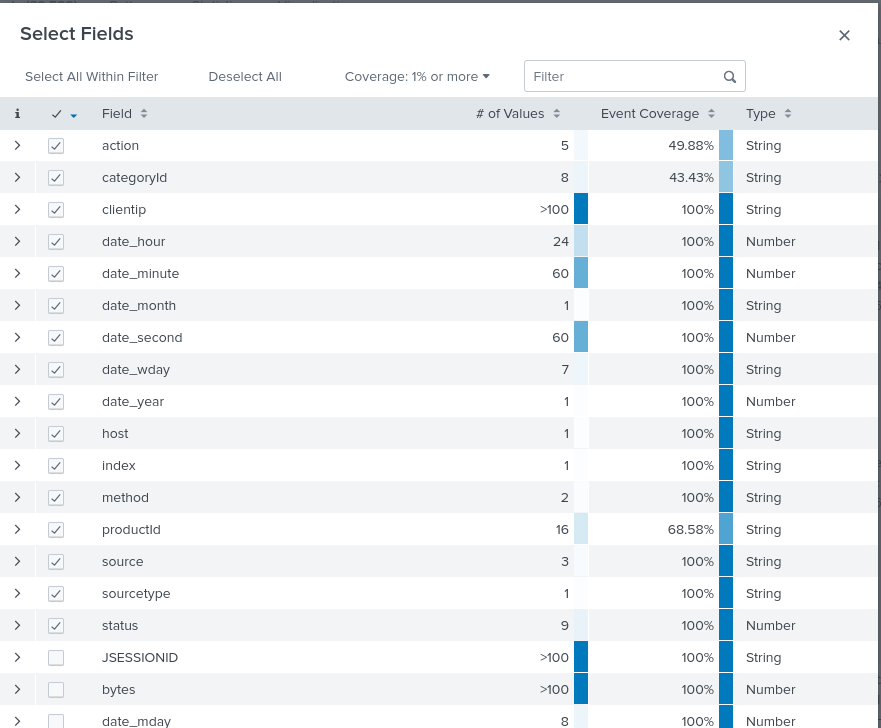


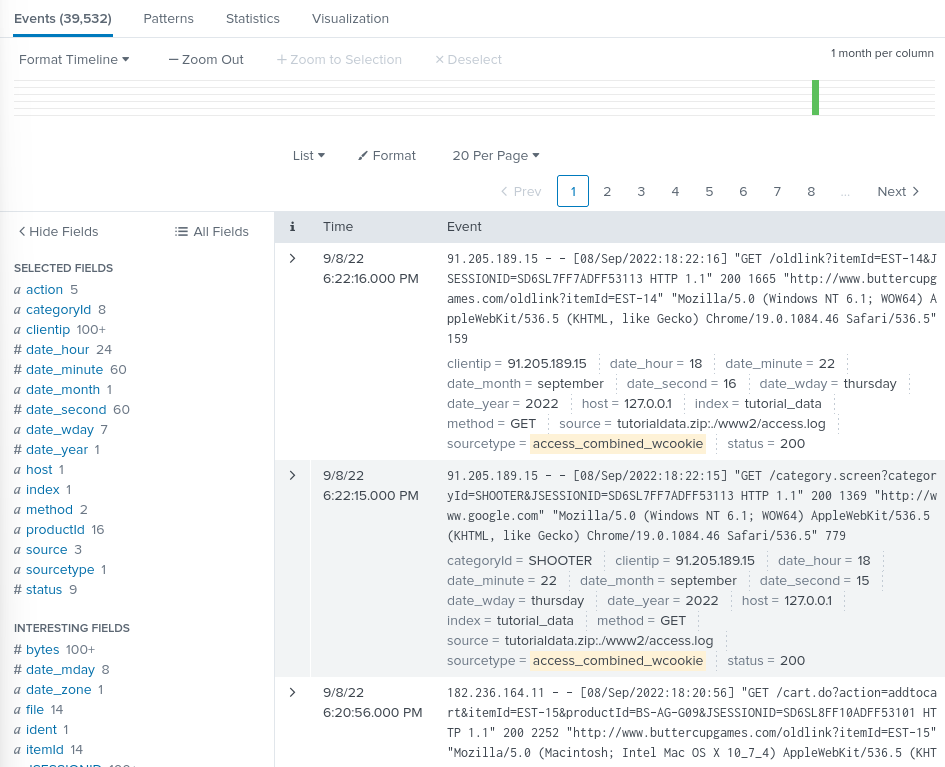
By default, the events appear as a list that is ordered starting with the most recent event. In each event, the matching search terms are highlighted

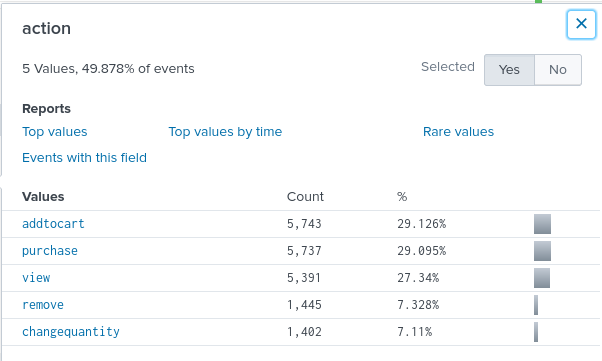
Select the List option and click Table.

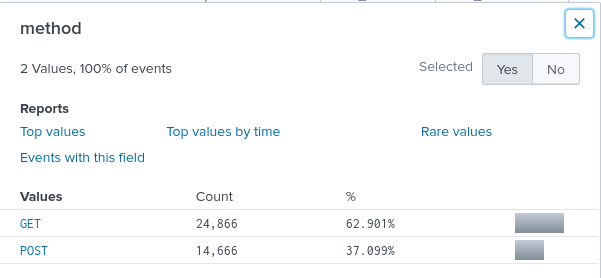
The display changes to show the event information column, the timestamp column, and columns for each of the Selected fields.



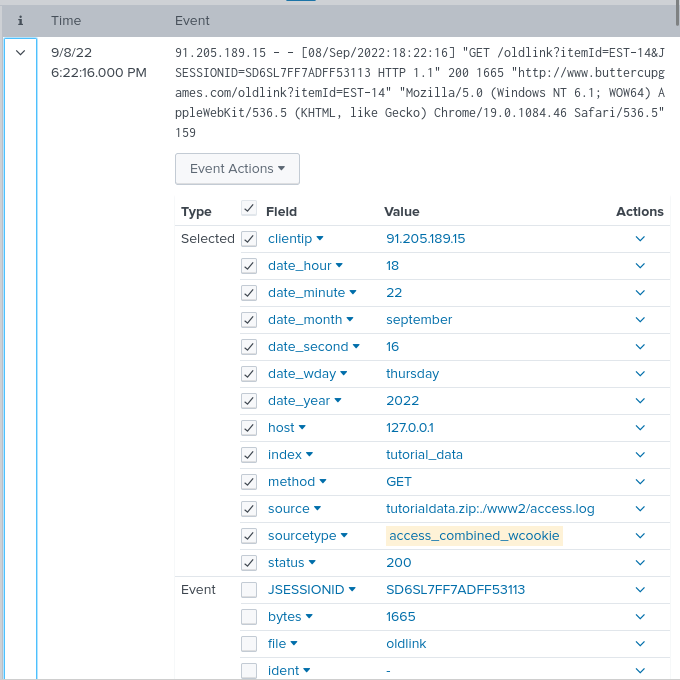


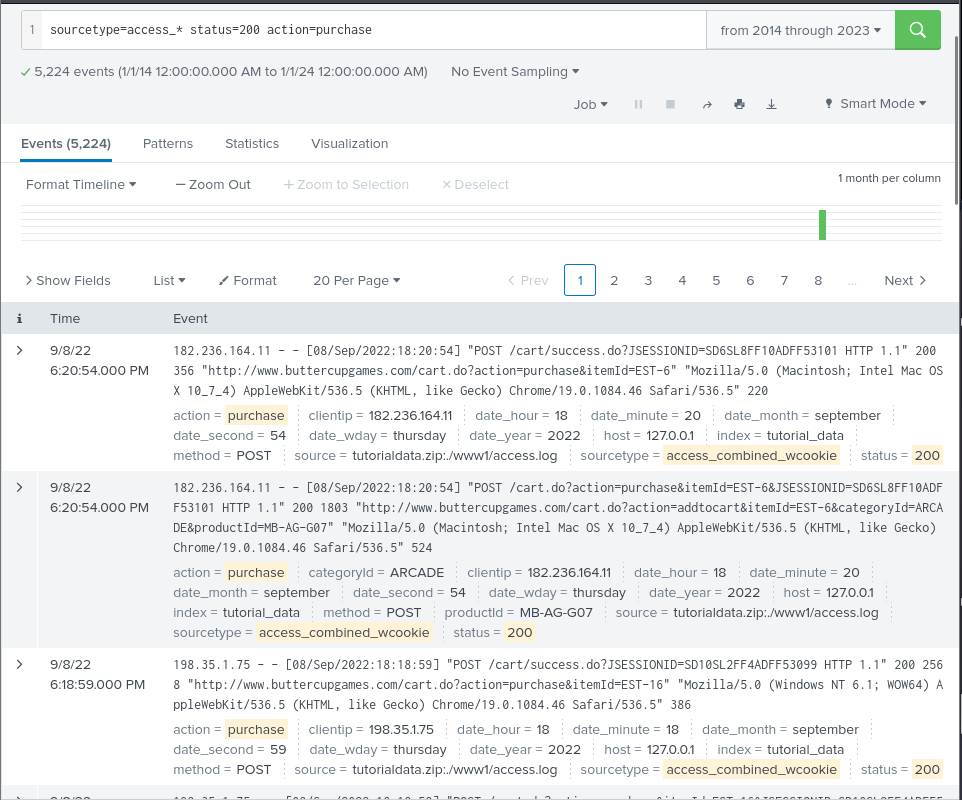




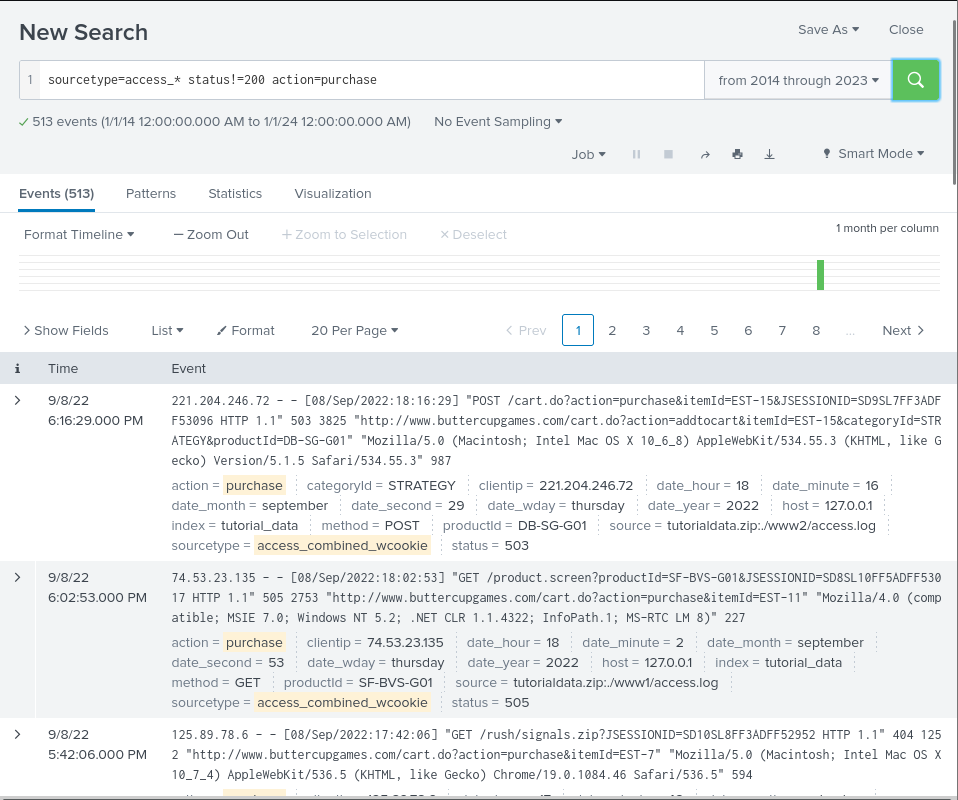




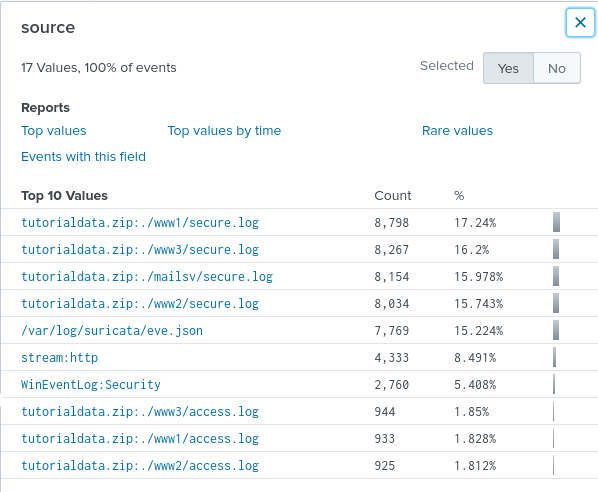


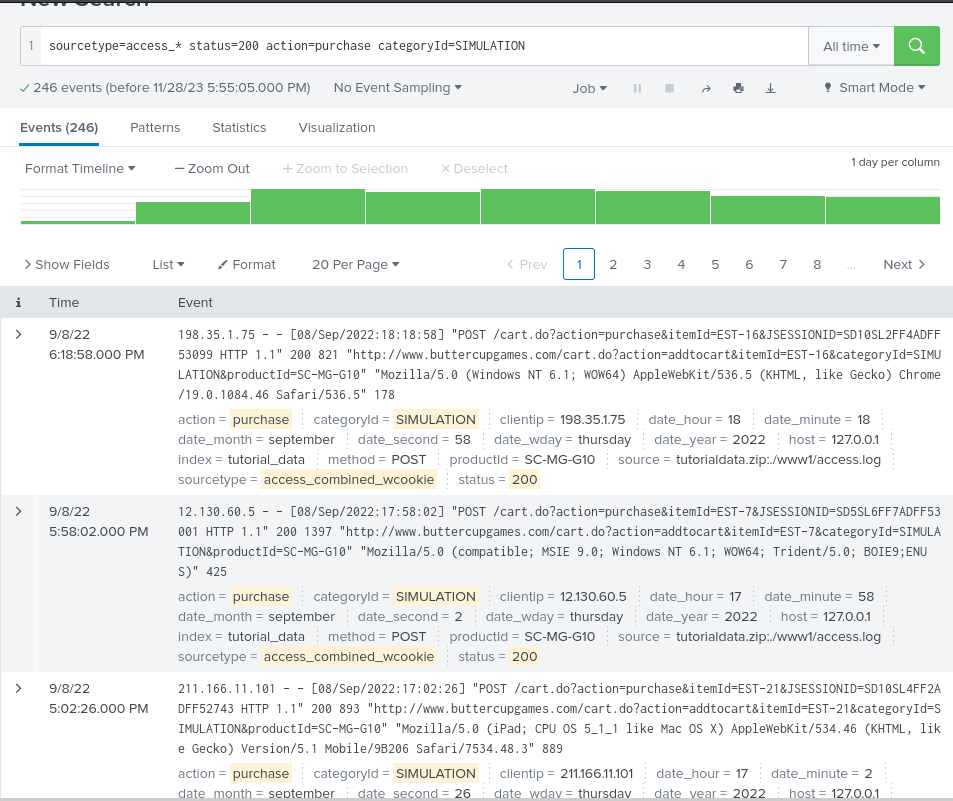


Successful purchases

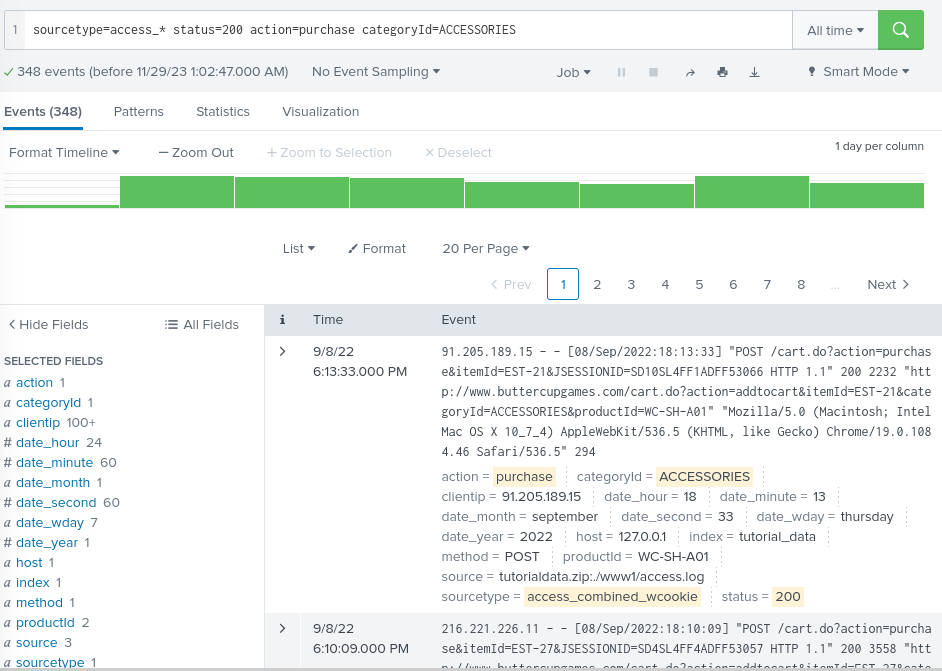


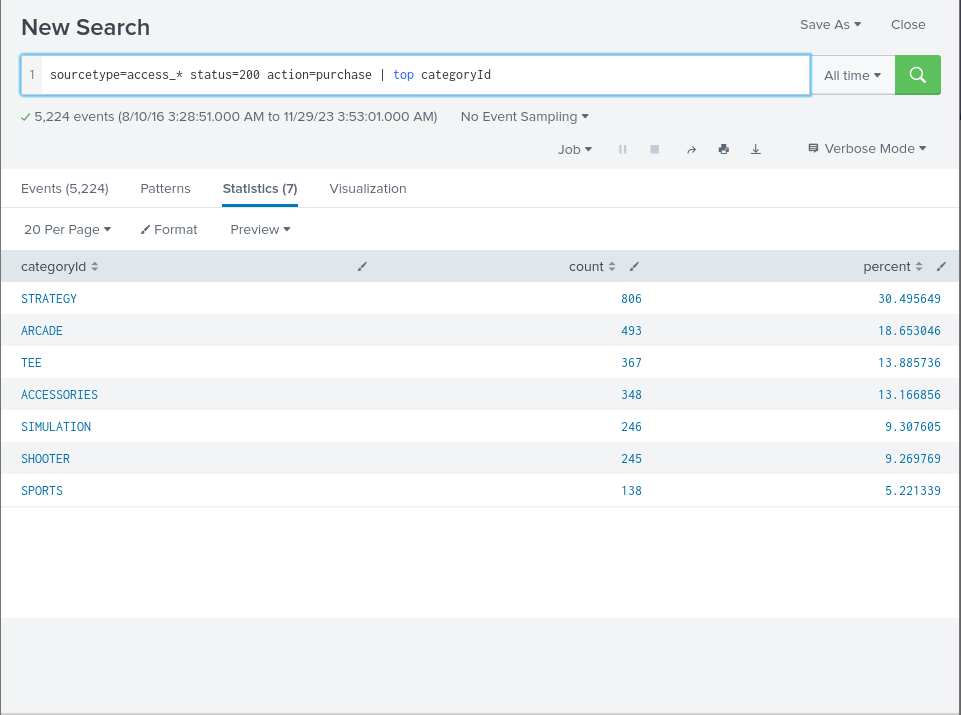
Failed purchases

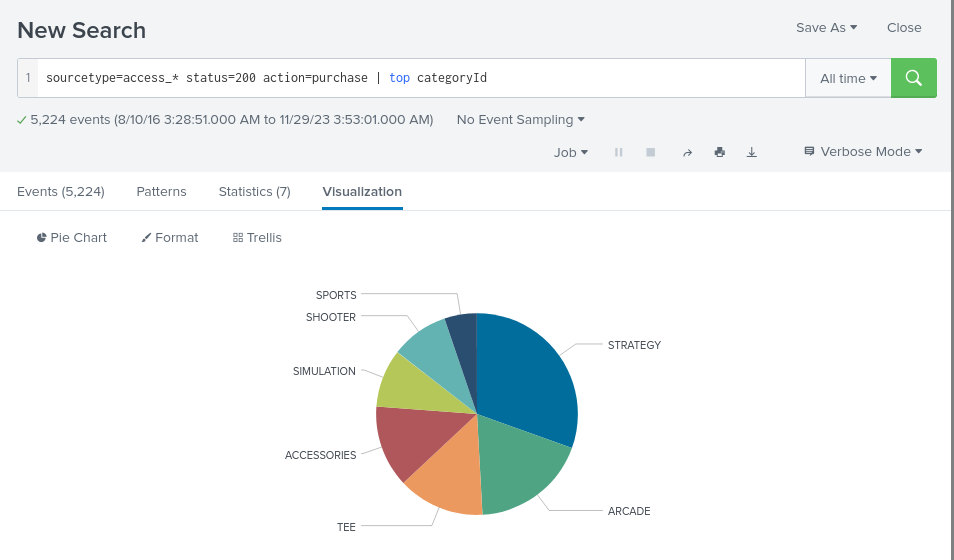


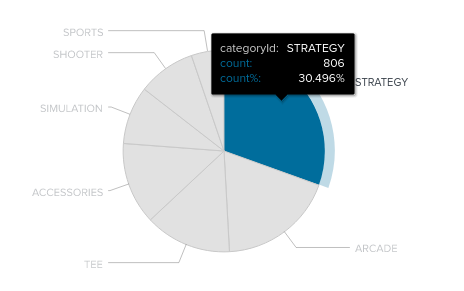


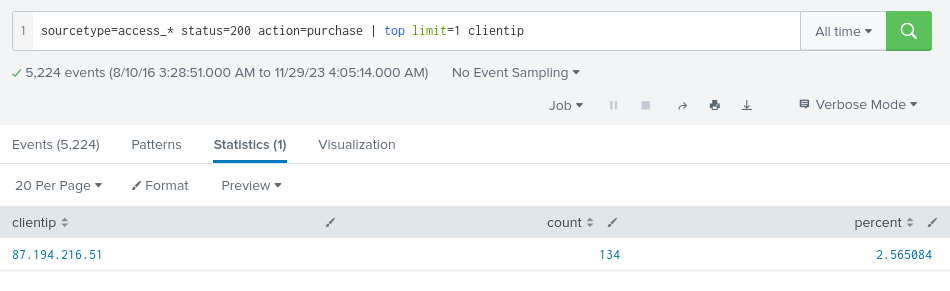
246 events

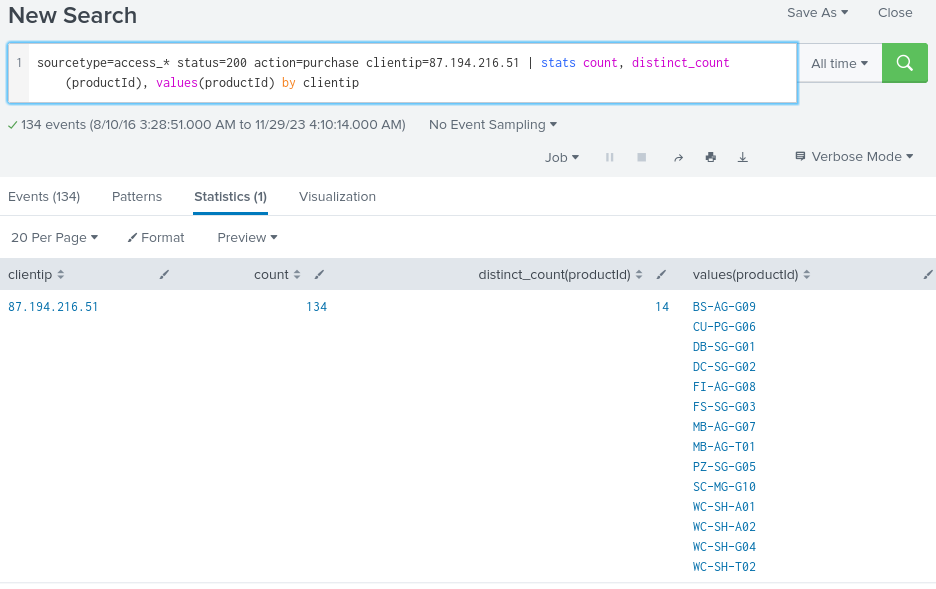


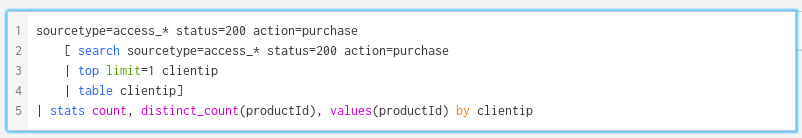




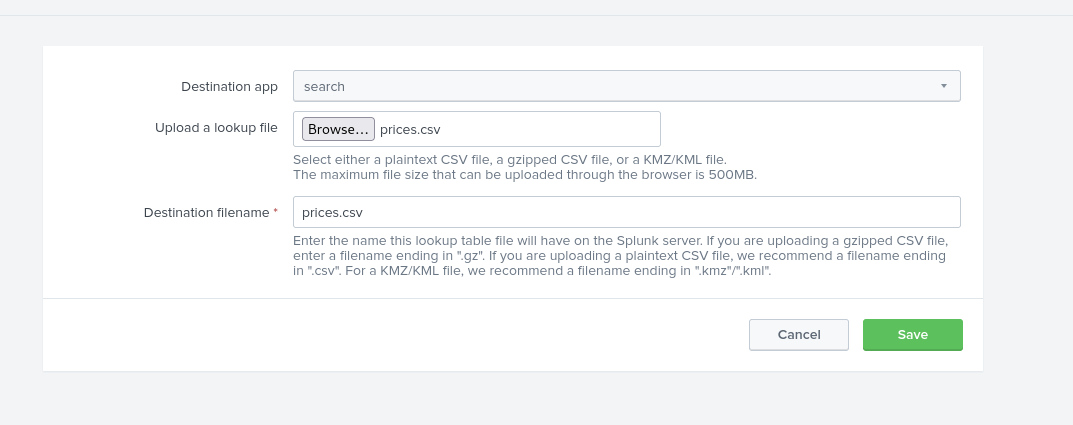


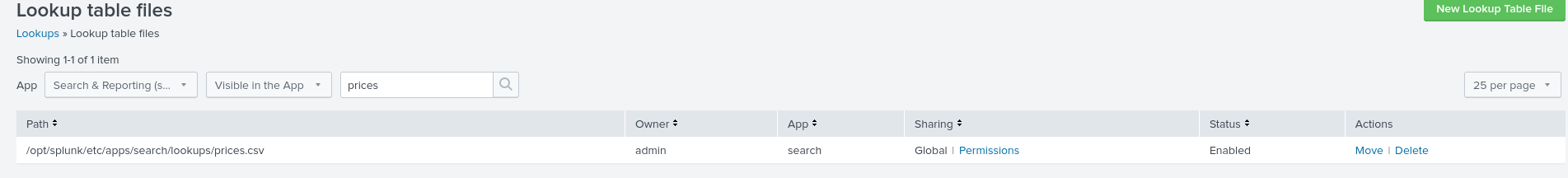


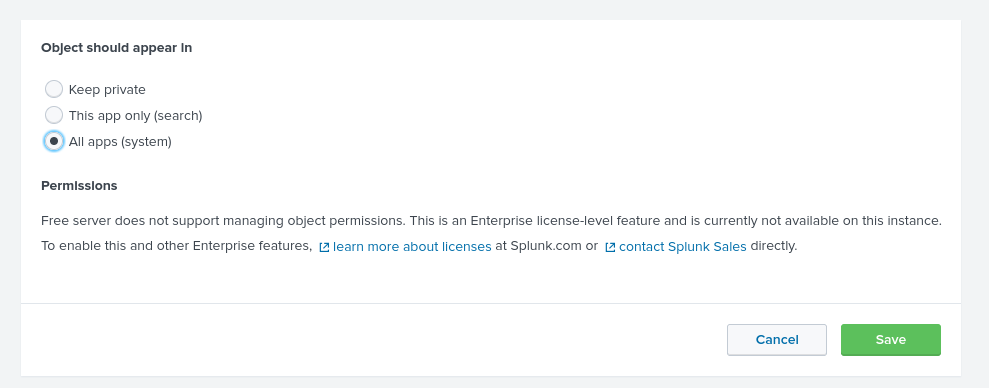


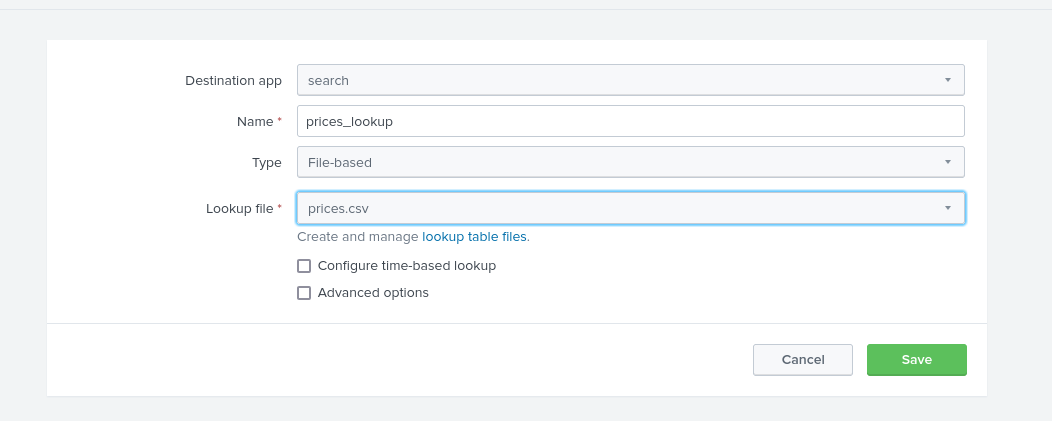


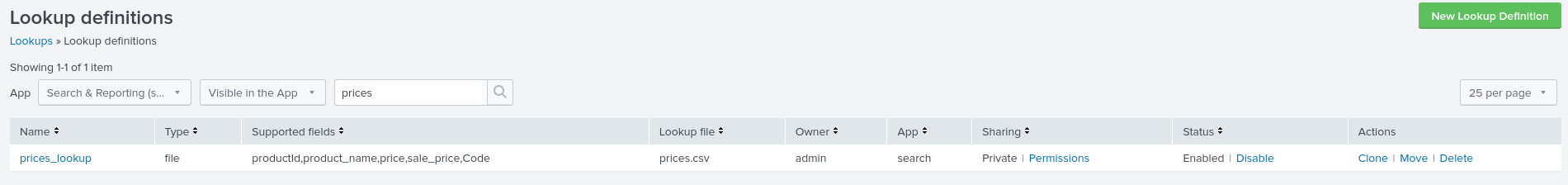
ctrl + \

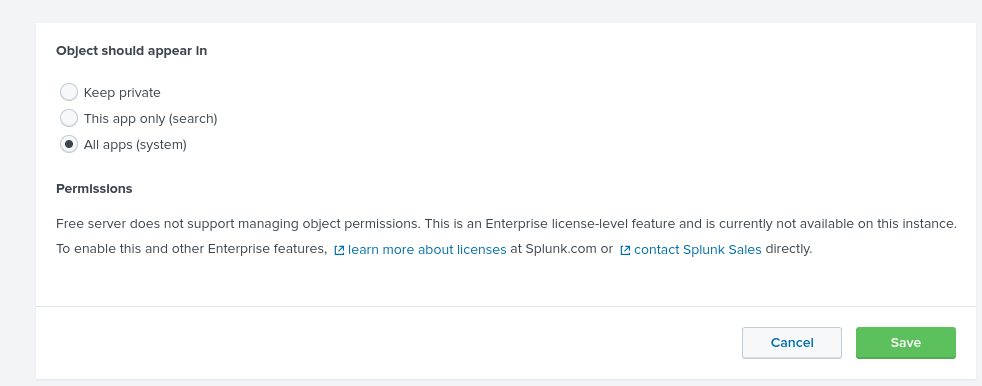


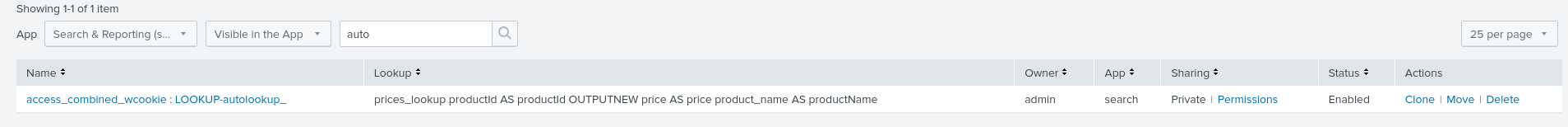












### 

### **Part 3: Reporting**

* Why would a security team benefit from SIEM implementation?
  + SIEM implementation provides security teams with a comprehensive and centralized solution for monitoring, detecting, and responding to security events. It plays a crucial role in enhancing the overall security posture of an organization by providing insights, automation, and the ability to respond swiftly to potential threats.
* What is an index?
  + index is a repository or storage location where Splunk stores and manages the data it ingests.
* What is a forwarder?
  + A forwarder refers to a software component responsible for collecting and forwarding log and event data from various sources to a Splunk indexer.
* How does a SIEM add value to an organization like Buttercup Games?
  + A SIEM system adds substantial value to organizations like Buttercup Games by providing advanced threat detection, incident response capabilities, compliance management, and overall visibility into the security landscape. It plays a crucial role in mitigating risks, protecting sensitive information, and ensuring the resilience of the organization against evolving cyber threats.