Home Lab Setup & SIEM Implementation Using Splunk

Prepared by:

Kripesh Acharya
Kripeshacharya2025@gmail.com

September 2024

Table of Contents

Abstract

This report outlines the implementation of a Security Information and Event Management (SIEM) system using Splunk in a home lab environment. The project involved installing Splunk Enterprise, integrating and parsing various log files, and conducting security analysis. Key activities included monitoring logs, detecting suspicious events using Search Processing Language (SPL), and creating dashboards and alerts to enhance security visibility and response.

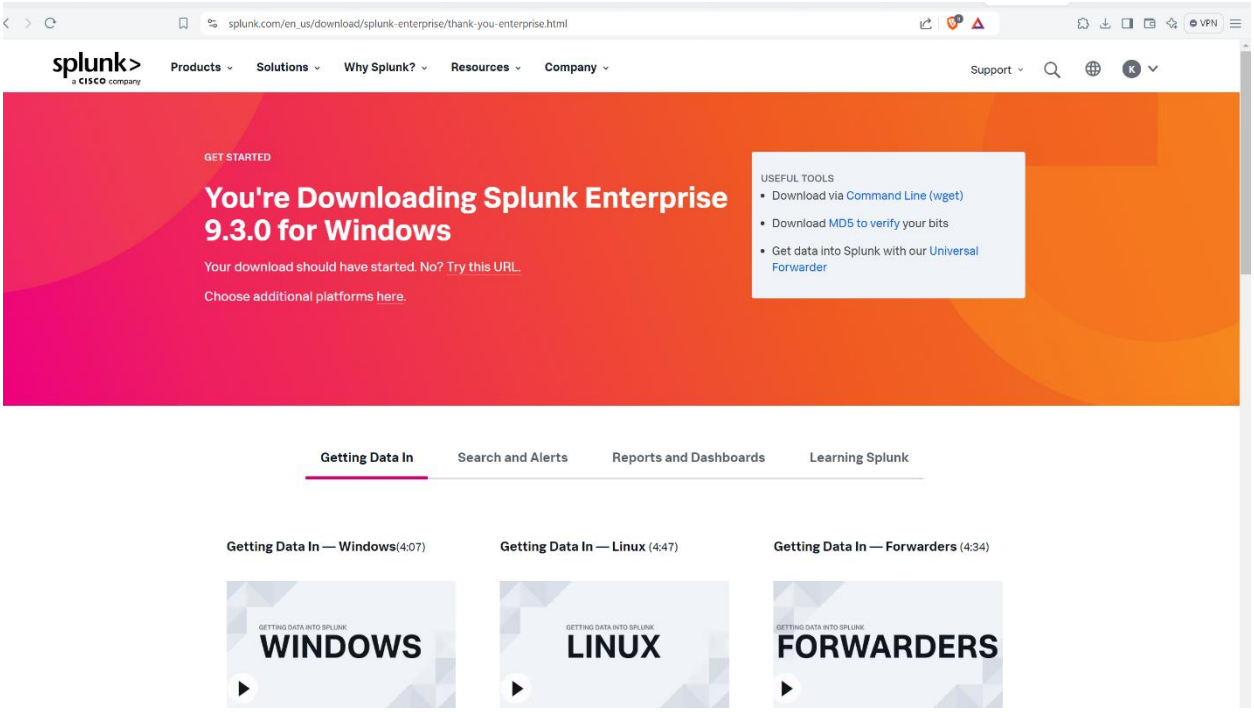
1. Introduction

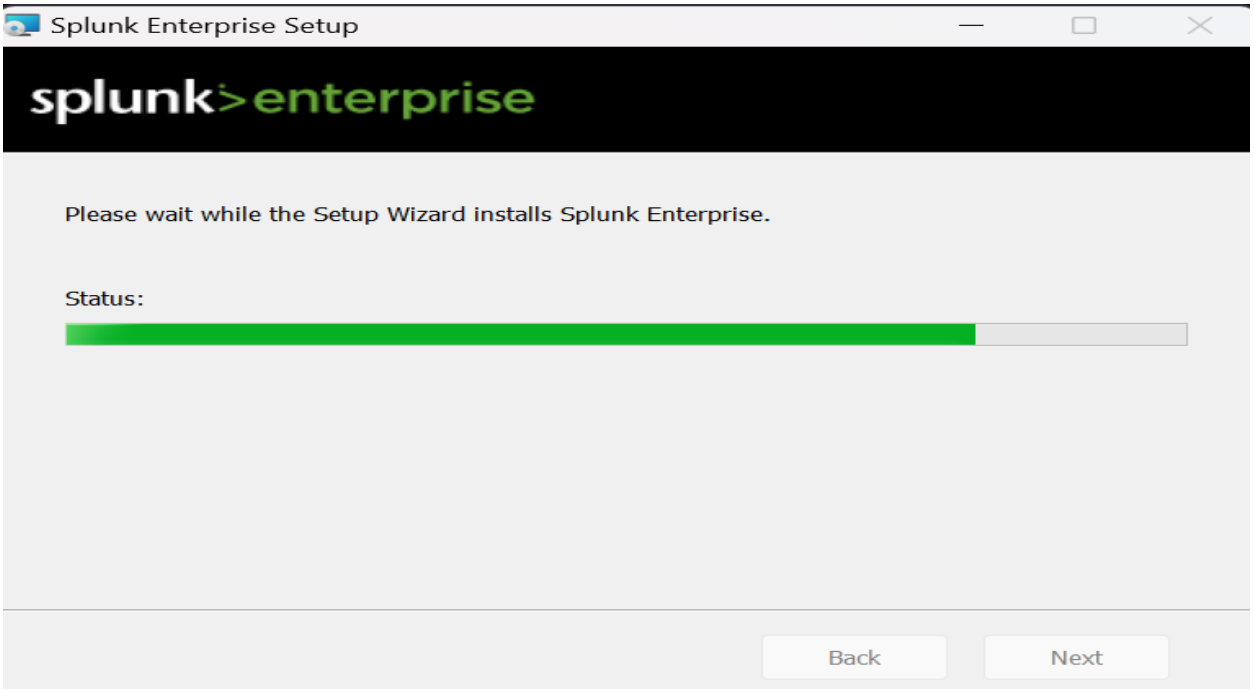
With the increasing complexity of security threats, effective monitoring and analysis of log data are crucial. This project focuses on setting up a SIEM solution using Splunk, a leading platform for handling large volumes of machine-generated data. The goal was to gain practical experience in log management, data integration, and security analysis within a controlled home lab environment.

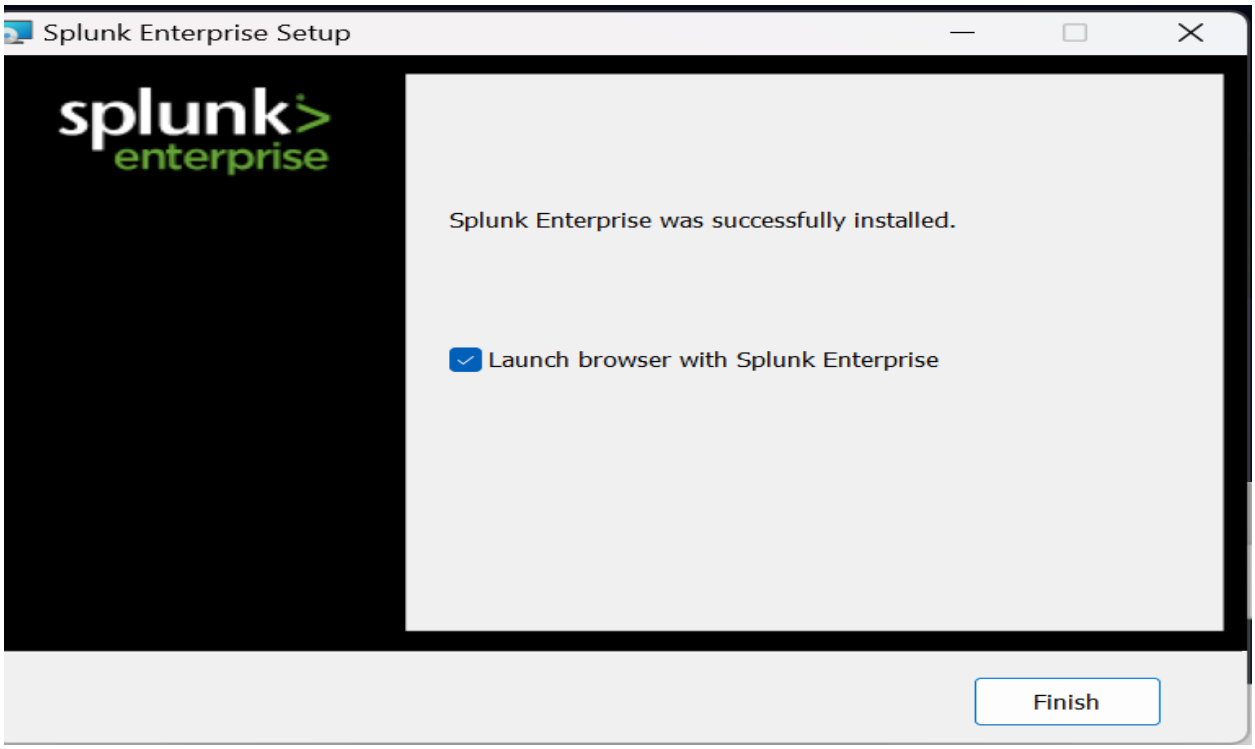
2. Project Implementation

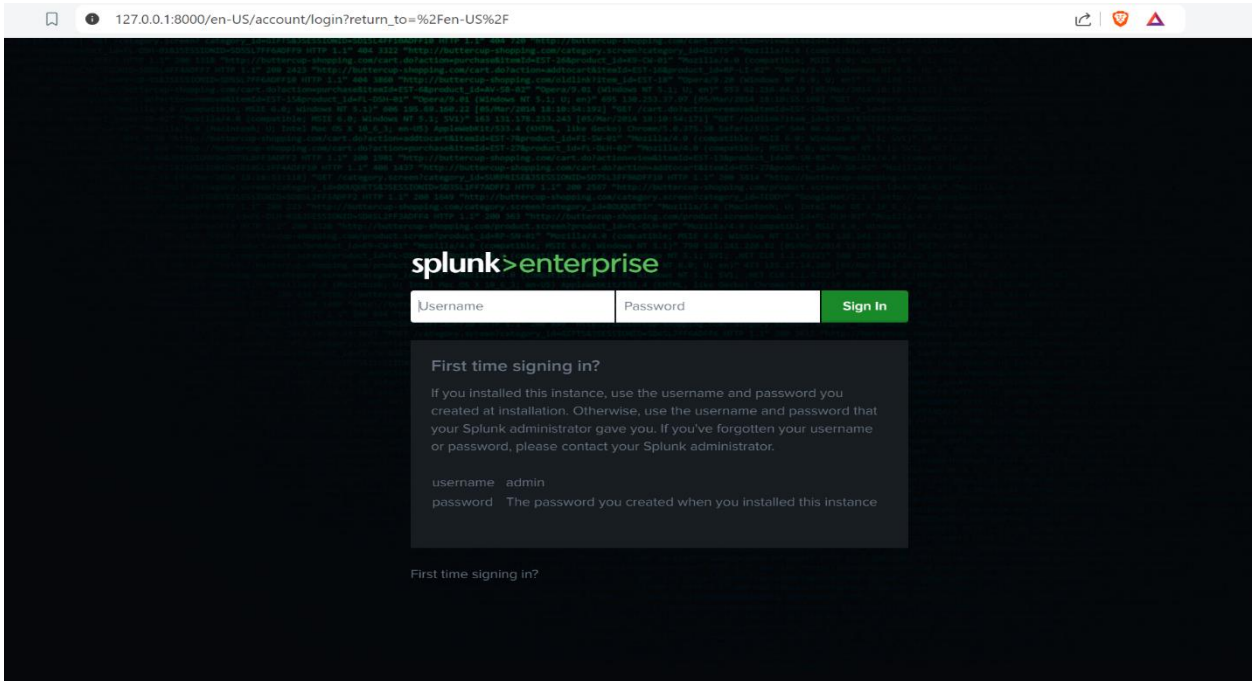
2.1 Installation and Initial Setup

The project began with the download and installation of Splunk Enterprise from the official website. The setup was performed on a Windows system.






Splunk Enterprise Setup
splunk> enterprise
Splunk Enterprise was successfully installed.
Launch browser with Splunk Enterprise
Finish


127.0.0.1:8000/en-US/account/login?return_to=%2Fen-US%2F
splunk>enterprise
Username
Password
Sign In
First time signing in?
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.
username admin
password The password you created when you installed this instance
First time signing in?

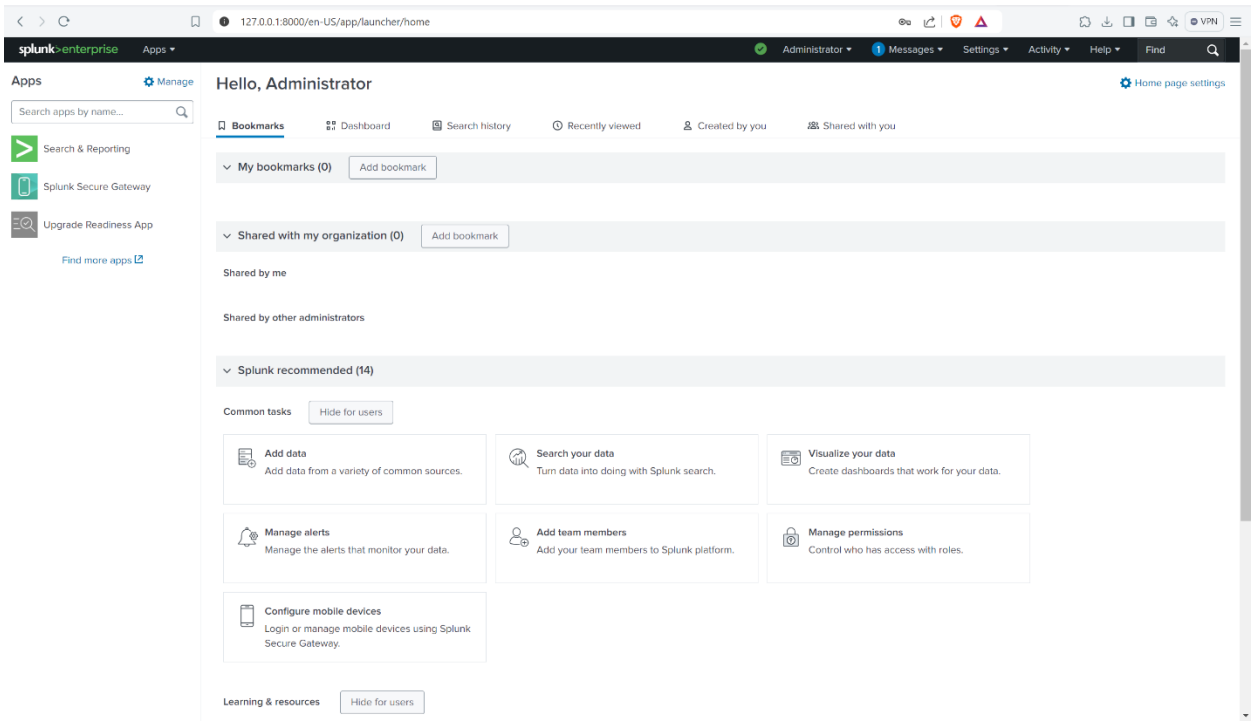


Fig: Splunk Enterprise Initial Setup

After the initial setup, it's important to ensure that Splunk is configured to start automatically and continues to monitor data without interruption.

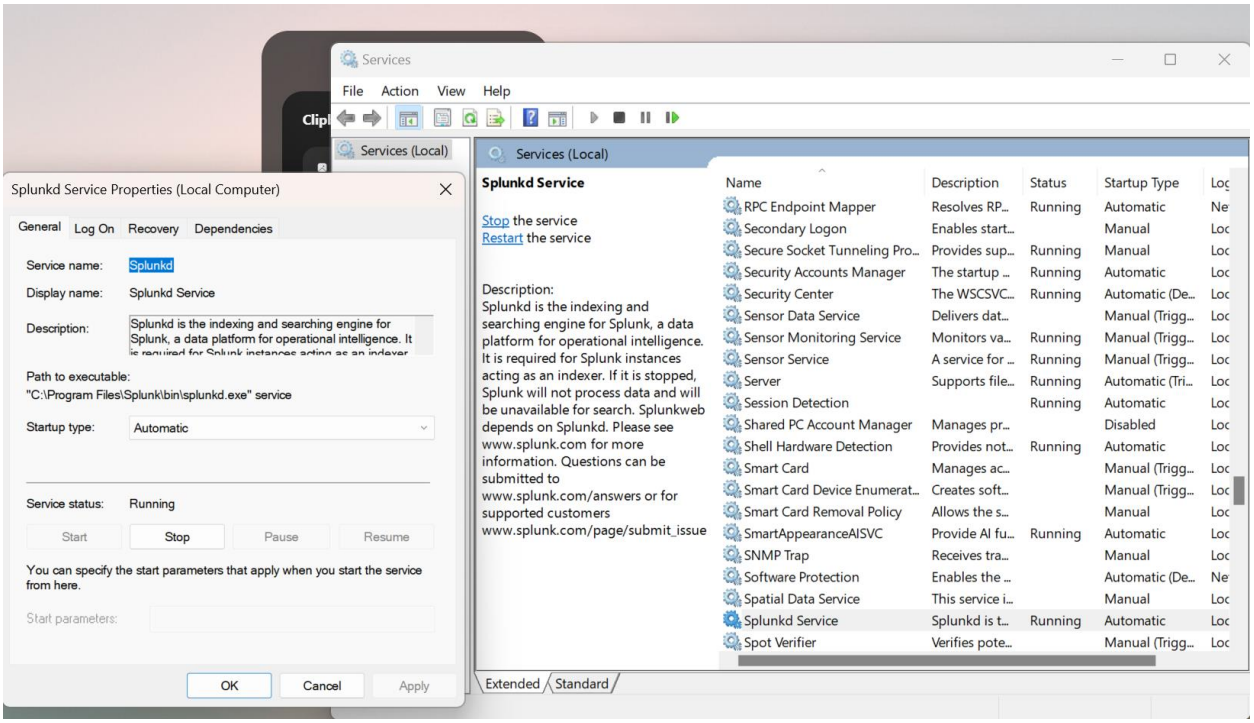


Fig: Verify Application Startup Status

After verifying that Splunk is starting up correctly, the next step involves configuring and selecting the appropriate log collections. In this case only Application, Security and System was selected.

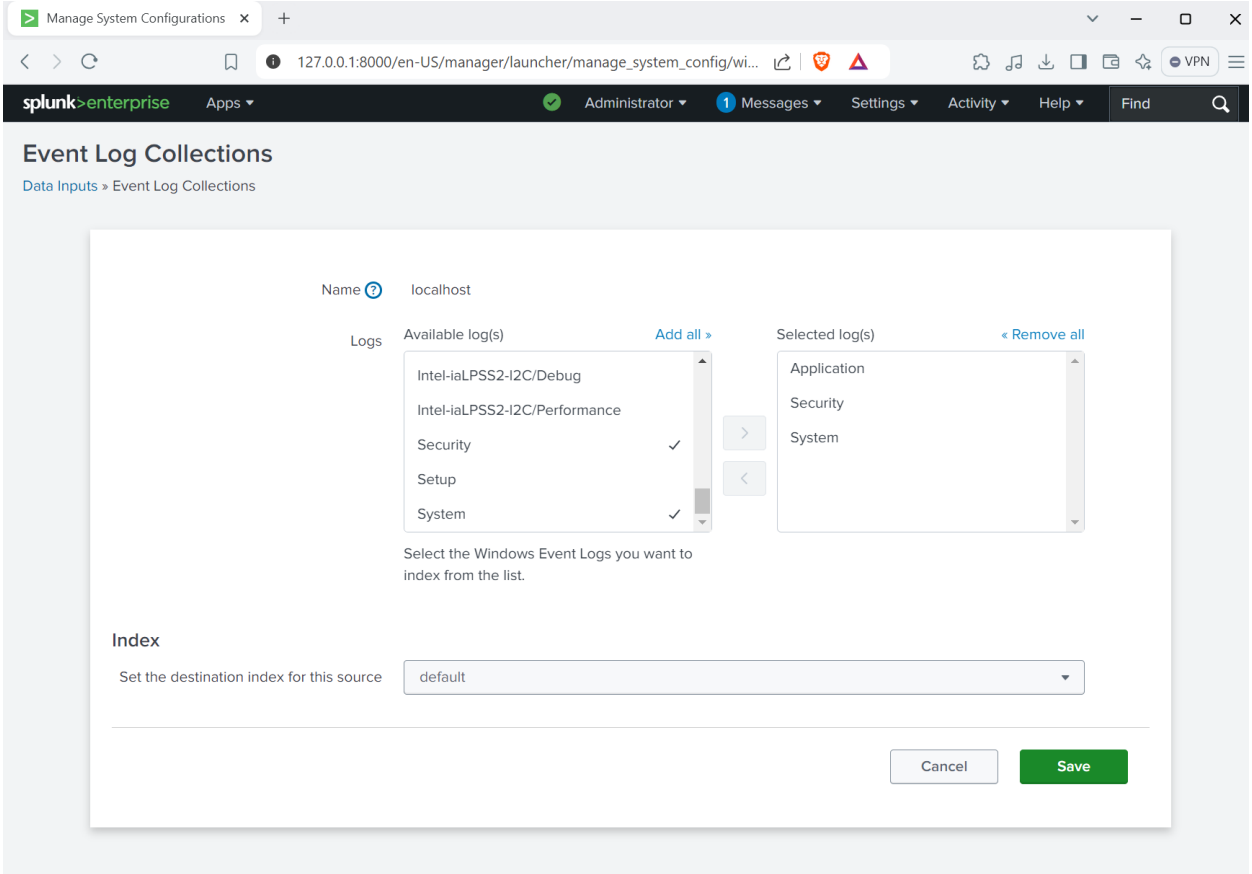
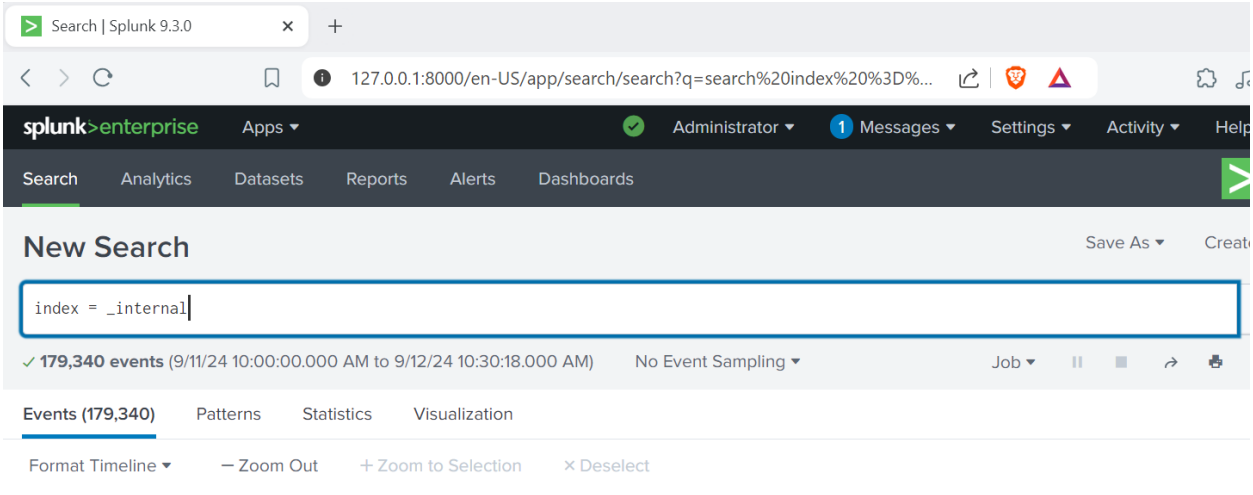


Fig: Log Collection Selection

To test its detection capabilities, the Windows Event Security logs were cleared and Splunk was checked to see if it generated an alert for this action.



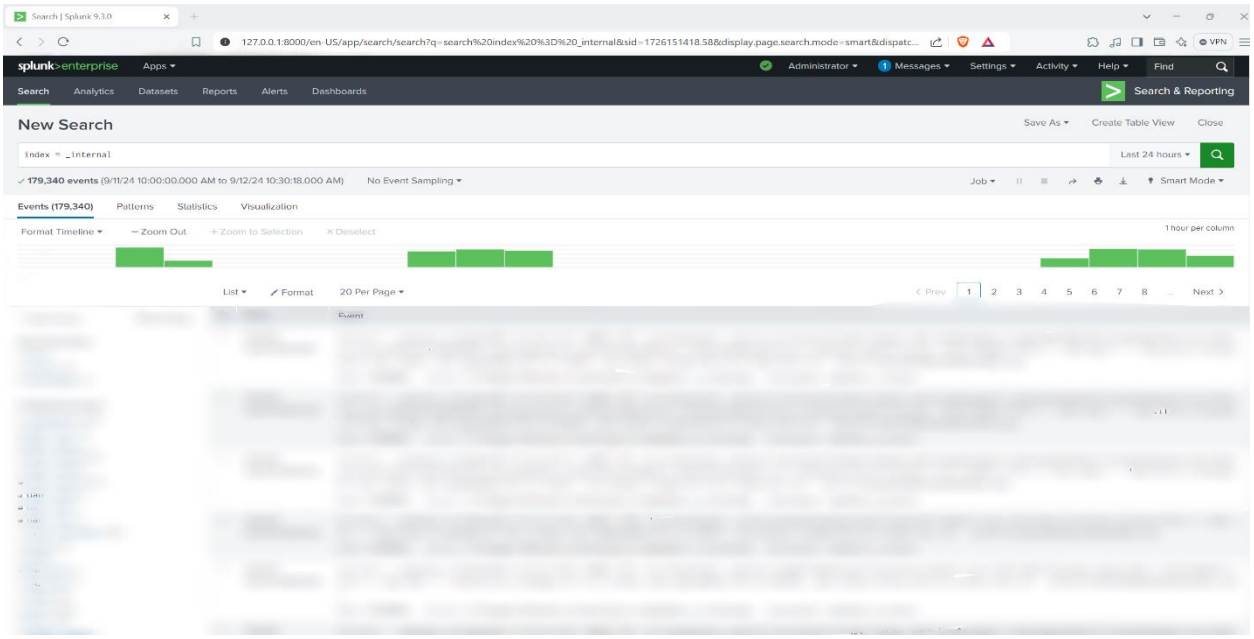


Fig: Internal System Alerts

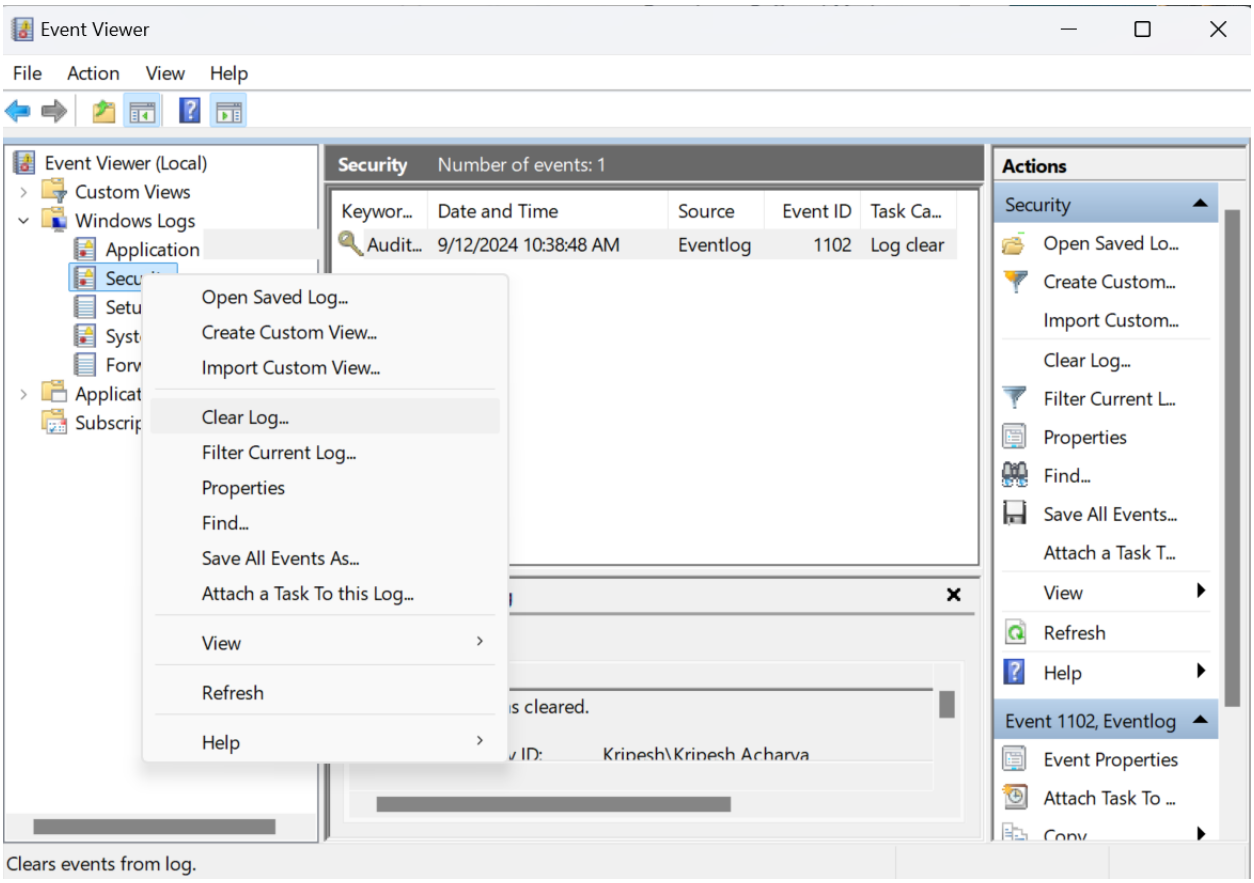


Fig: Security Log Cleared

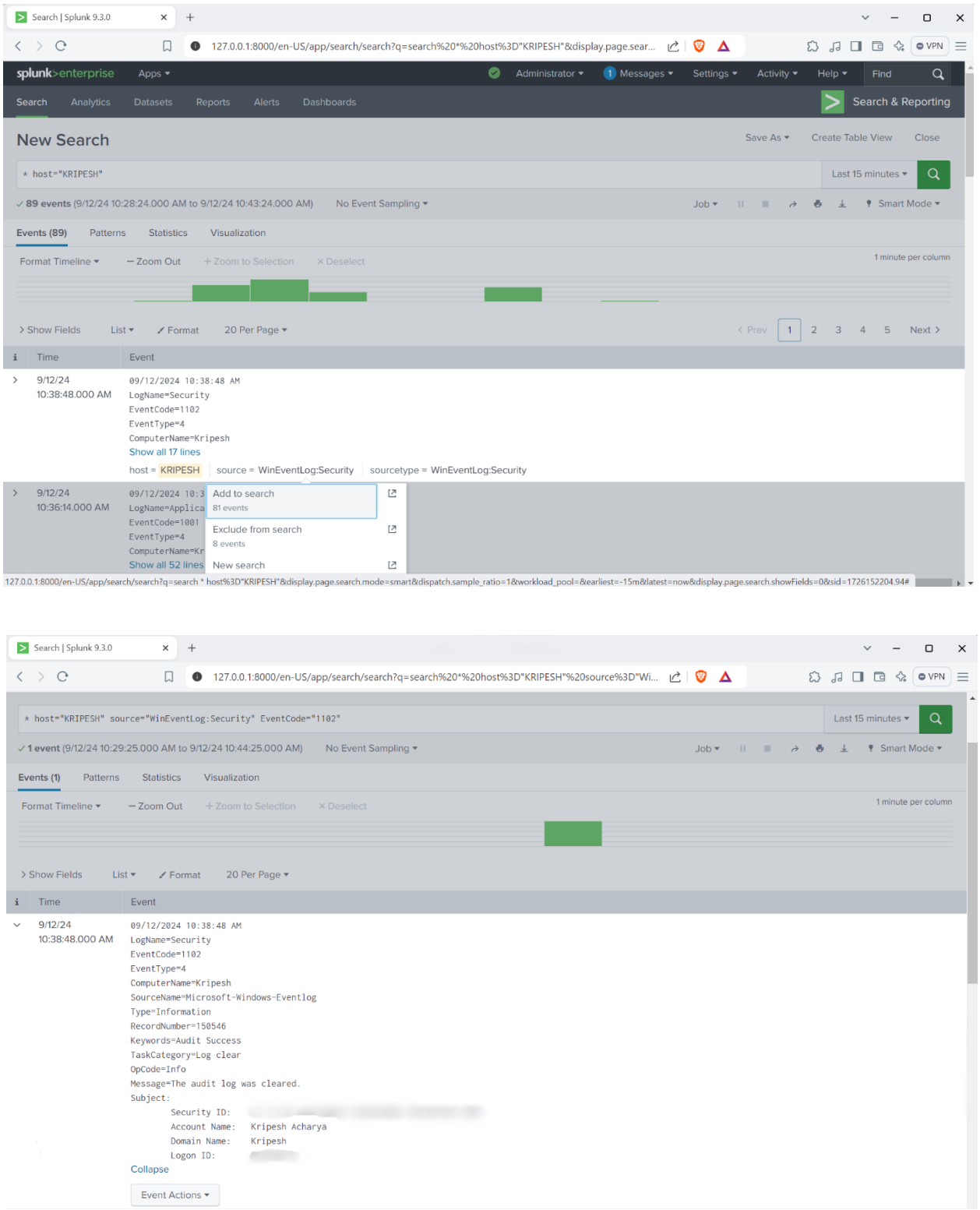


Fig: Windows Event Security Log Detected

After successfully detecting the log-cleared alert, a new dashboard was created to facilitate easy viewing of similar alerts in the future.

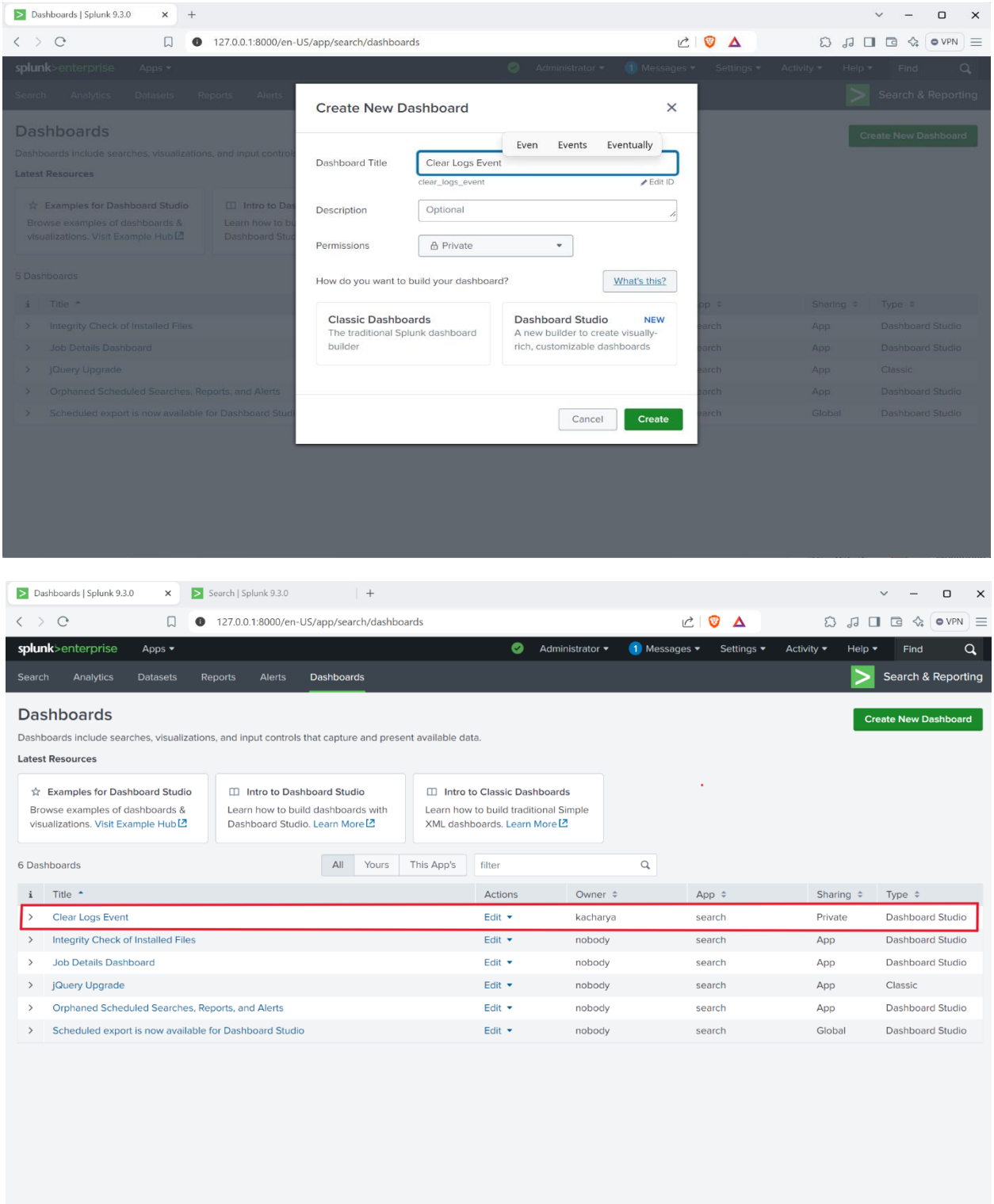
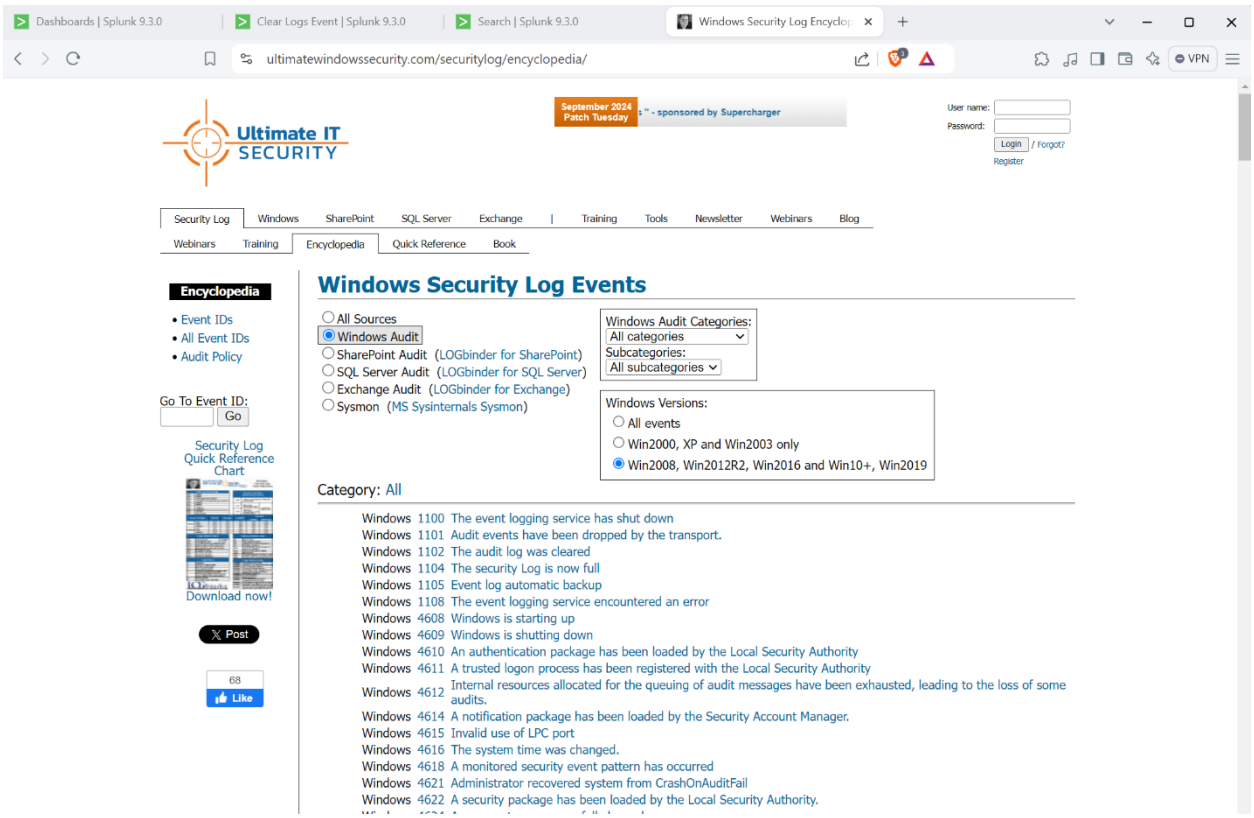


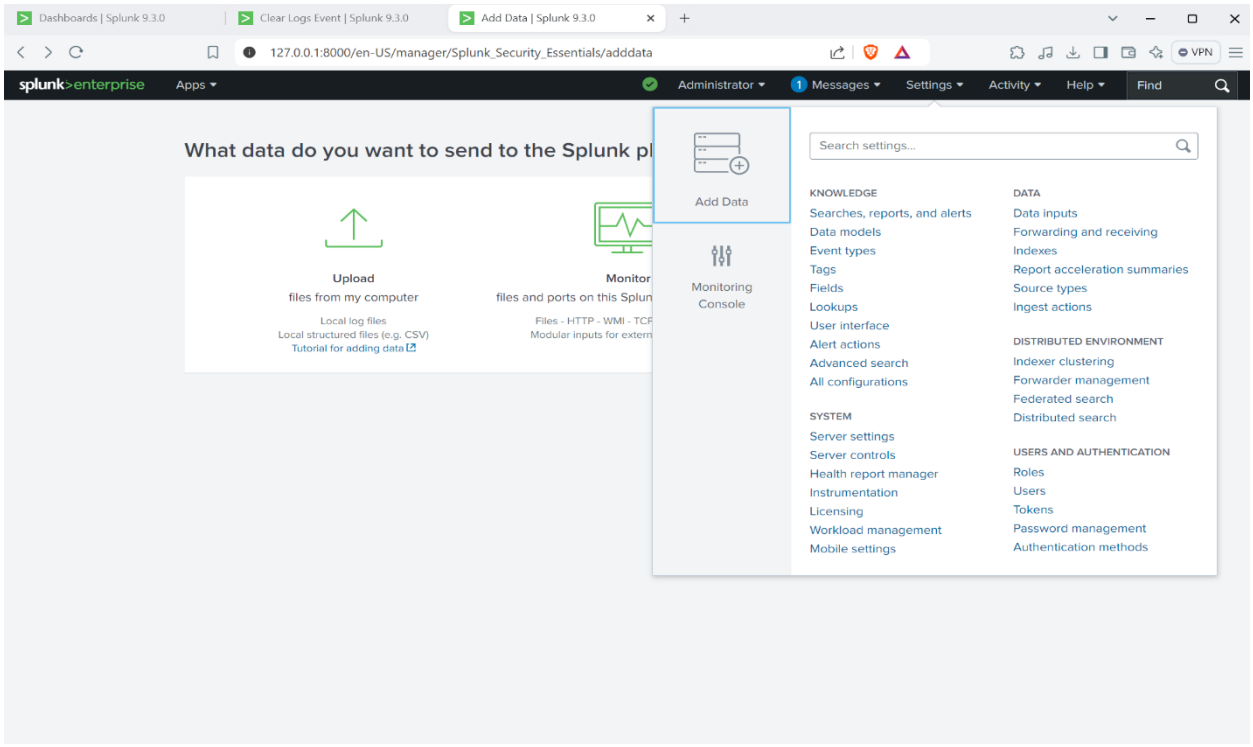
Fig: Dashboard Created

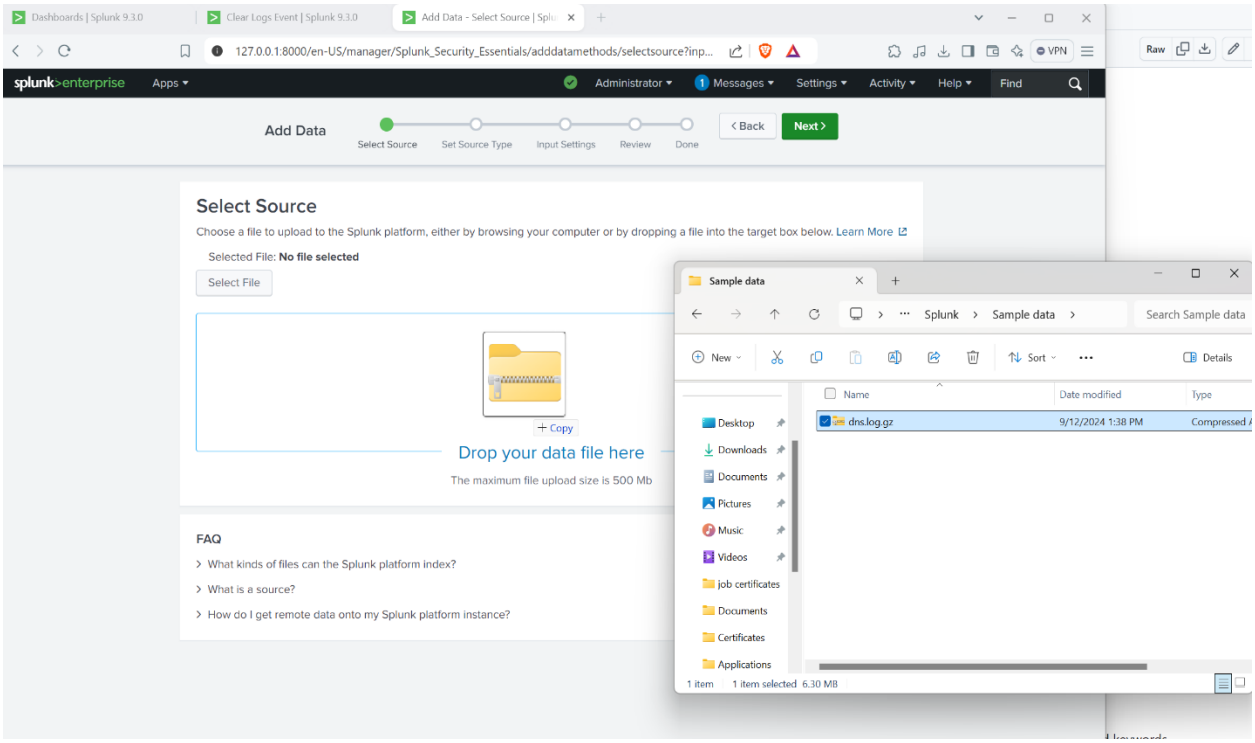
UltimateWindowsSecurity.com can be referred to for details on event log IDs and other important information related to Windows security events.

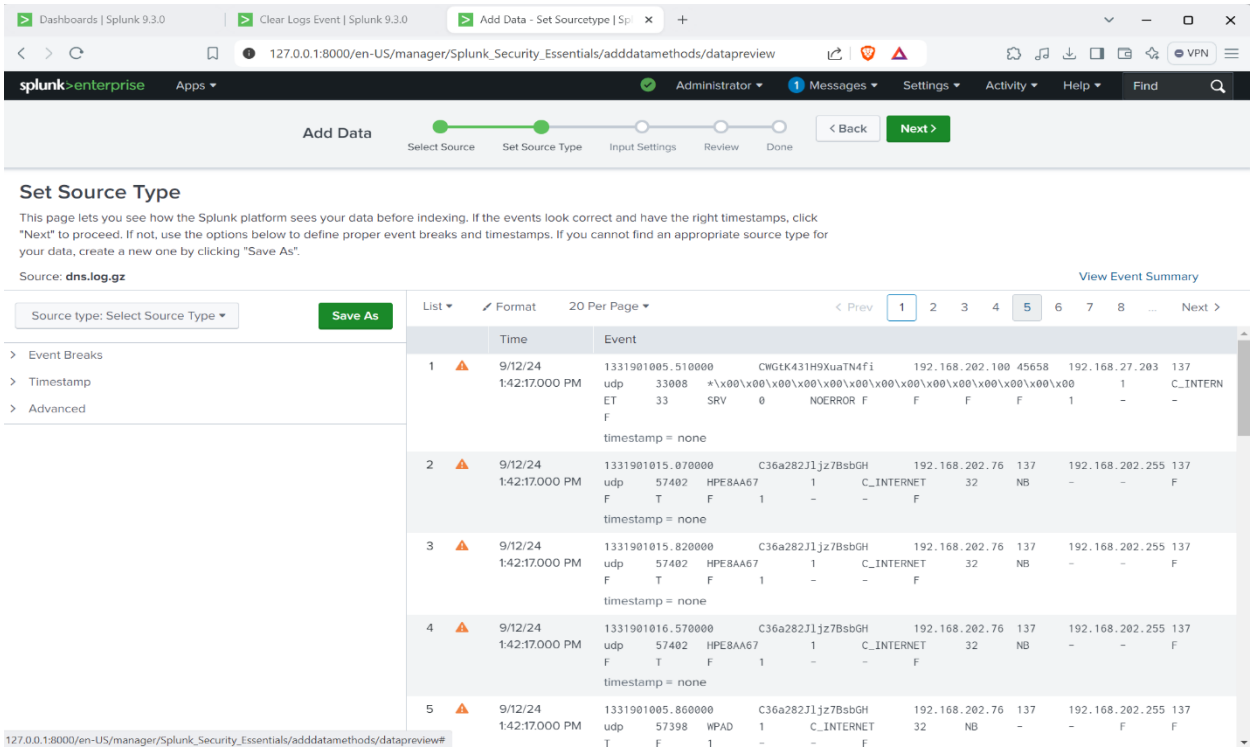


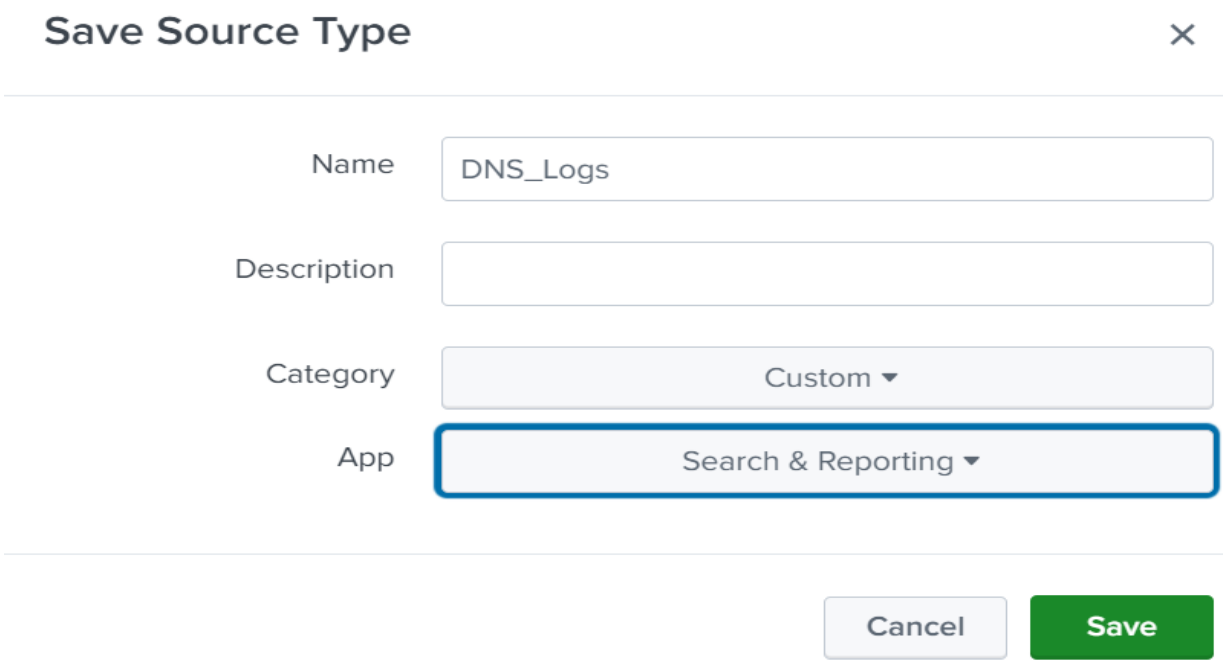
2.2 Log Collection and Integration

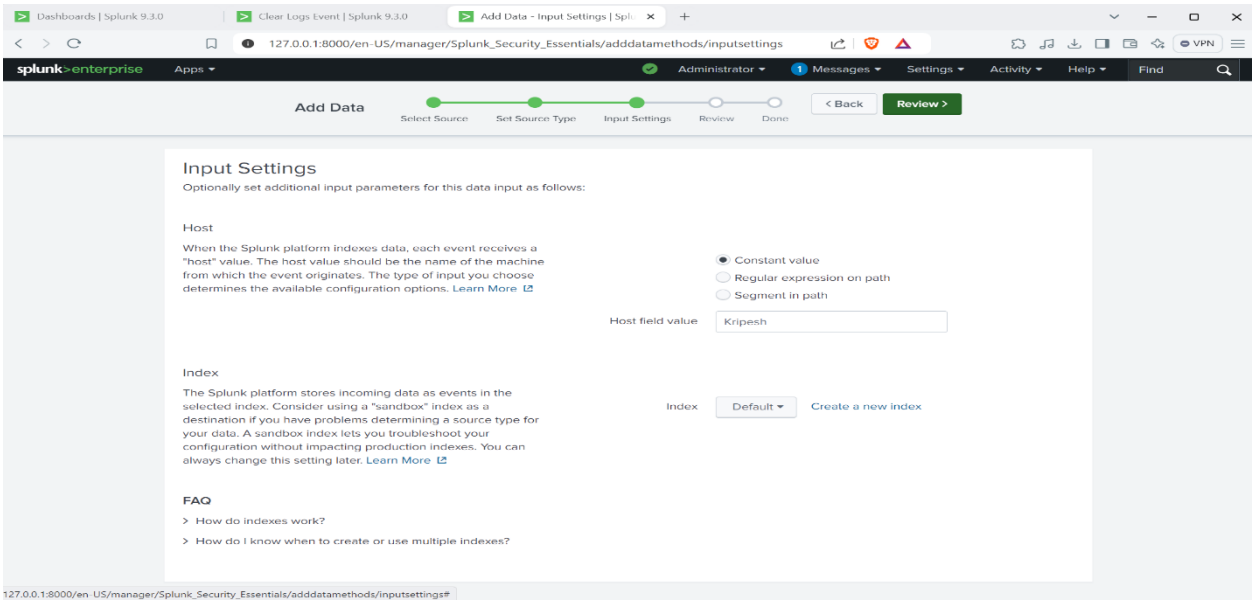
Logs from various sources, including DNS, FTP, and SSH, were collected and integrated into Splunk. This involved adding log files to the system and ensuring they were correctly indexed and searchable. The next step involves adding log files into Splunk for security analysis. The first log data imported into the application is the DNS log. This includes configuring the data input, ensuring proper indexing, and setting up necessary parsing rules to facilitate effective analysis and detection of security events.

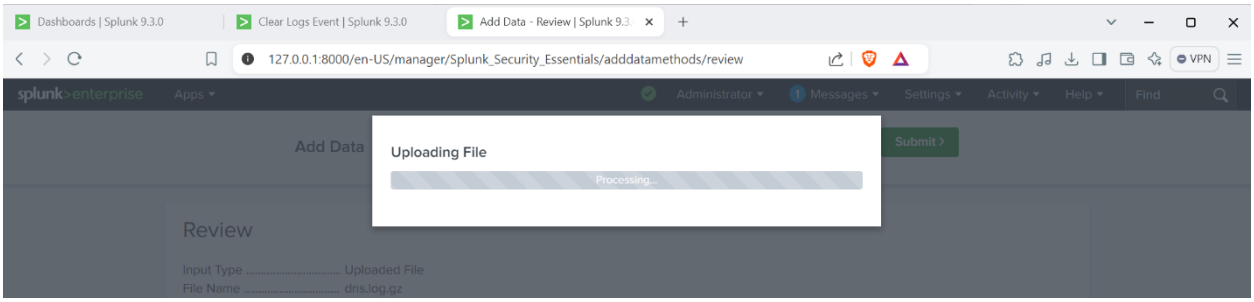

Dashboards | Splunk 9.3.0
Clear Logs Event | Splunk 9.3.0
Add Data | Splunk 9.3.0
127.0.0.1:8000/en-US/manager/Splunk_Security_Essentials/adddata
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
What data do you want to send to the Splunk pl
Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data
Monitor
files and ports on this Splun
Add Data
Monitoring Console
Search settings...
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Health report manager
Instrumentation
Licensing
Workload management
Mobile settings
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
Ingest actions
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Federated search
Distributed search
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password management
Authentication methods


Add Data - Select Source | Splu
127.0.0.1:8000/en-US/manager/Splunk_Security_Essentials/adddatamethods/selectsource?inp...
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
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
Select File
Drop your data file here
The maximum file upload size is 500 Mb
FAQ
What kinds of files can the Splunk platform index?
What is a source?
How do I get remote data onto my Splunk platform instance?
Sample data
Splunk > Sample data
Search Sample data
dns.log.gz
9/12/2024 1:38 PM
1 item
1 item selected 6.30 MB


Dashboards | Splunk 9.3.0
Clear Logs Event | Splunk 9.3.0
Add Data - Set Sourcetype | Spl
127.0.0.1:8000/en-US/manager/Splunk_Security_Essentials/adddatamethods/datapreview
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
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: dns.log.gz
View Event Summary
Source type: Select Source Type
Save As
Event Breaks
Timestamp
Advanced
List
Format
20 Per Page
Prev
Next
Time
Event
9/12/24 1:42:17.000 PM
timestamp = none
127.0.0.1:8000/en-US/manager/Splunk_Security_Essentials/adddatamethods/datapreview#


Save Source Type
Name
DNS_Logs
Description
Category
Custom
App
Search & Reporting
Cancel
Save





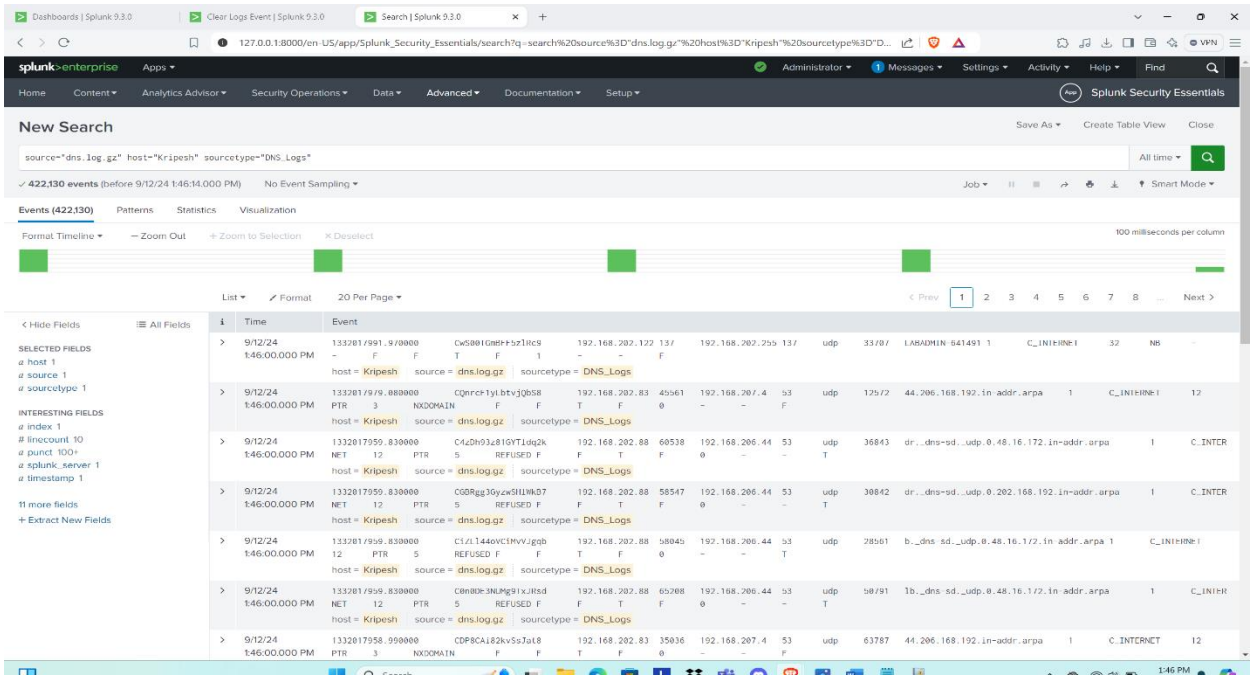
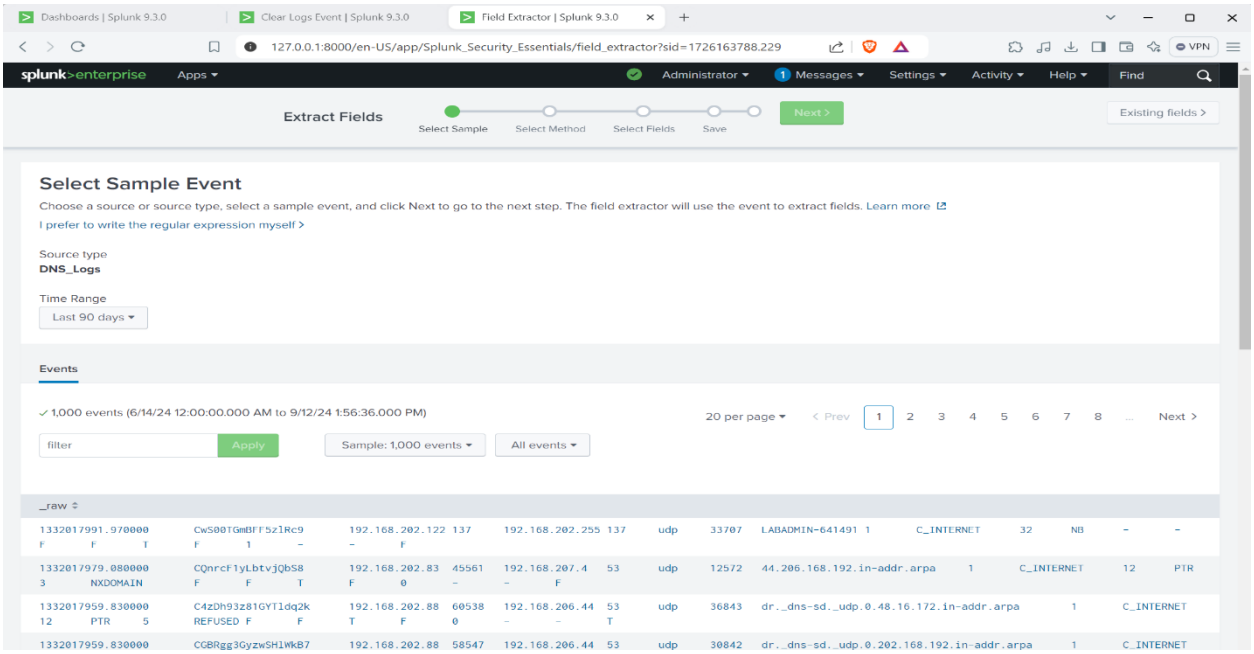
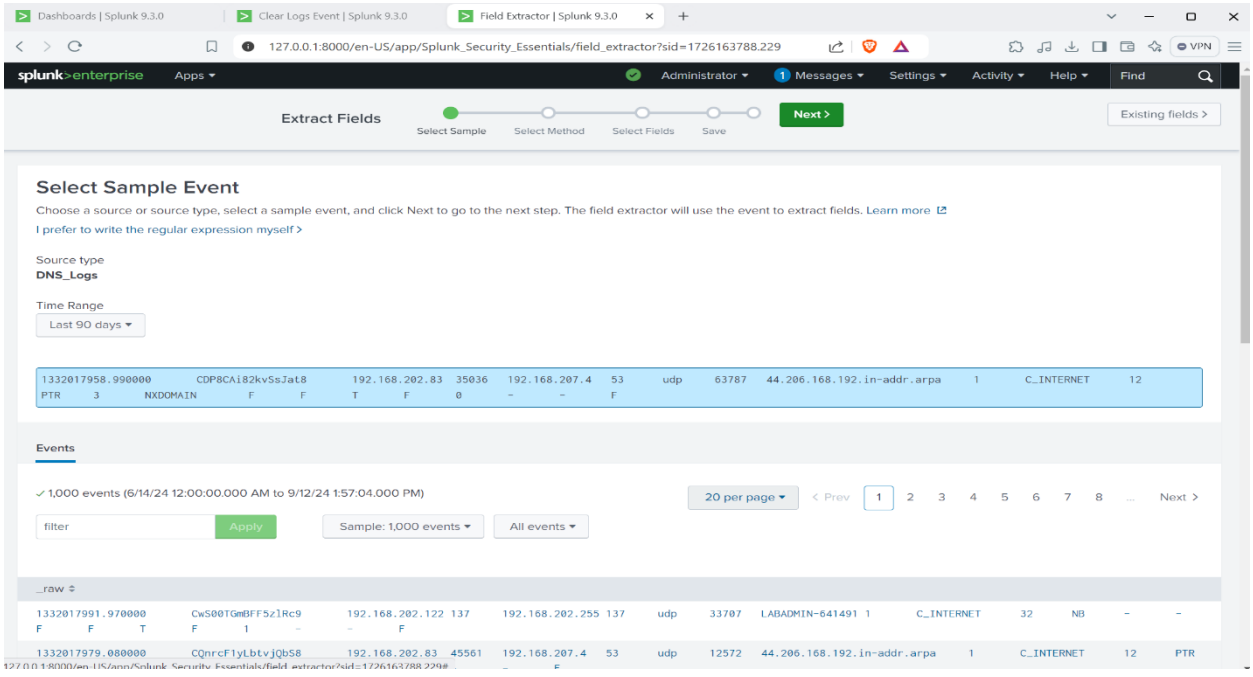


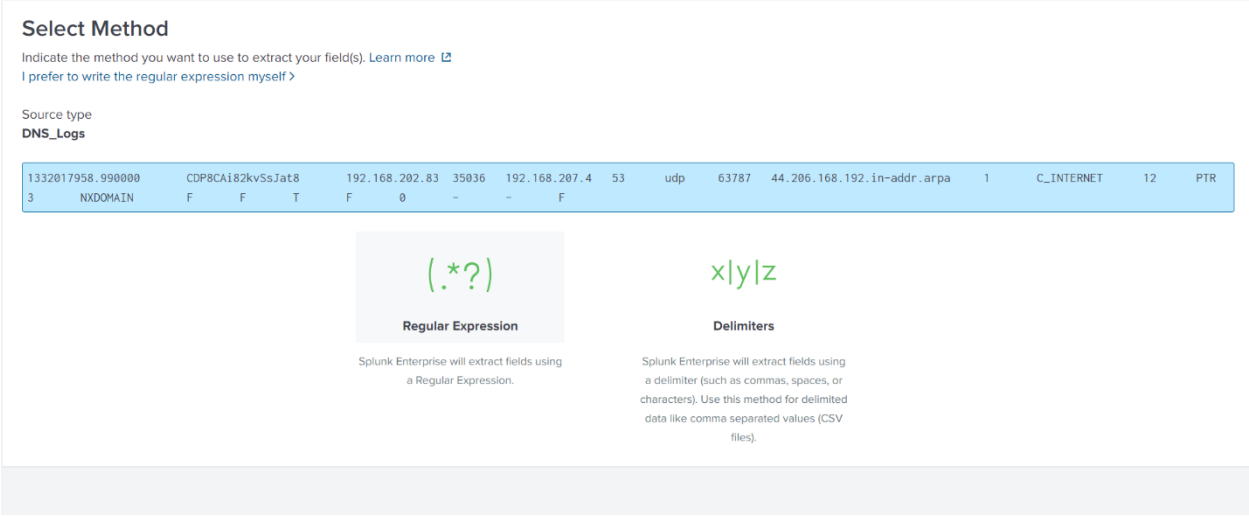
Fig: DNS Log File Uploaded Successfully

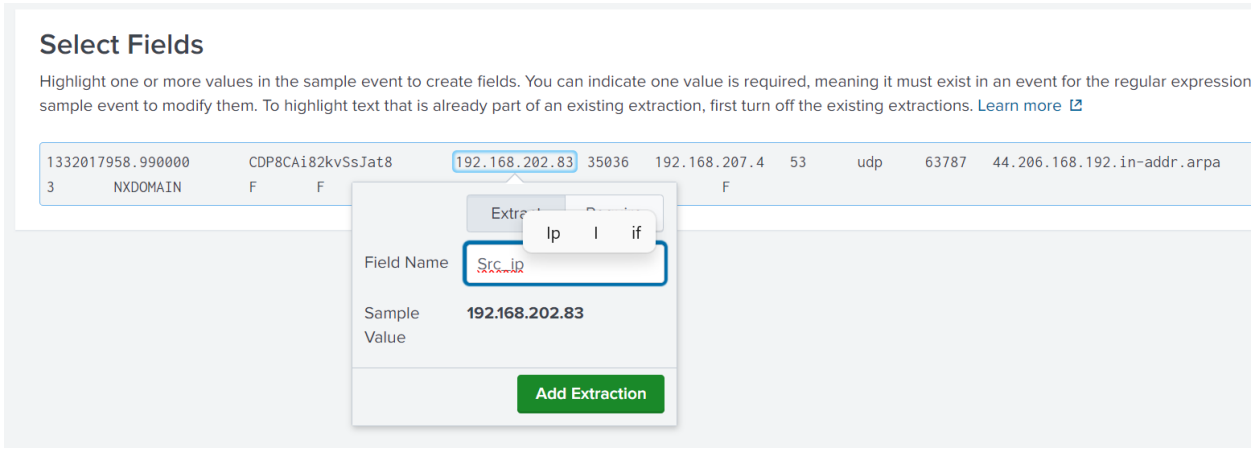
2.3 Data Parsing and Security Analysis

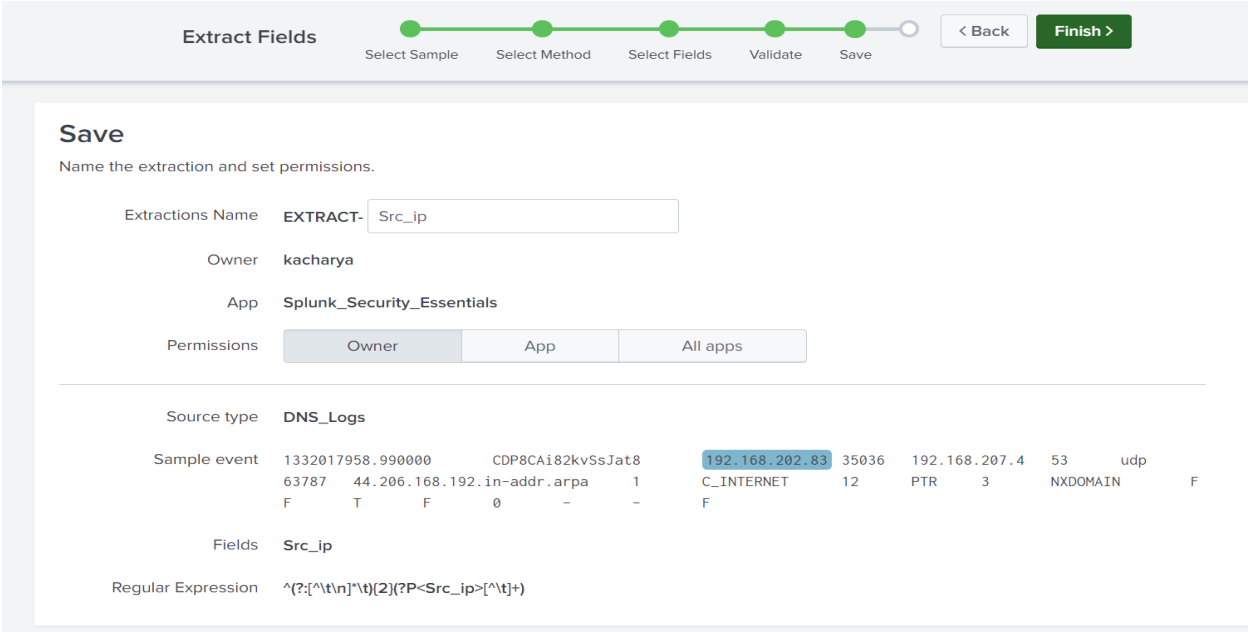
Data parsing was performed to structure the logs appropriately. Security analysis was conducted using Splunk's Search Processing Language (SPL) to identify and investigate suspicious events. This process included filtering and querying the log data to uncover potential security issues. The next step after uploading the log file is to select a sample event and parse the data. This ensures that the data is structured appropriately, making it easier to use later in Search Processing Language (SPL) queries for effective analysis and reporting.






Select Method
Indicate the method you want to use to extract your field(s). Learn more
I prefer to write the regular expression myself >
Source type
DNS_Logs
1332017958.990000 CDP8CAi82kvSsJat8 192.168.202.83 35036 192.168.207.4 53 udp 63787 44.206.168.192.in-addr.arpa 1 C_INTERNET 12 PTR
3 NXDOMAIN F F T F 0 - - F
(.*?)
Regular Expression
Splunk Enterprise will extract fields using a Regular Expression.
x|y|z
Delimiters
Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).


Select Fields
Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more
1332017958.990000 CDP8CAi82kvSsJat8 192.168.202.83 35036 192.168.207.4 53 udp 63787 44.206.168.192.in-addr.arpa
3 NXDOMAIN F F F
Extract
Regex
Ip I if
Field Name
Src_ip
Sample Value
192.168.202.83
Add Extraction


Extract Fields
Select Sample
Select Method
Select Fields
Validate
Save
< Back
Finish >
Save
Name the extraction and set permissions.
Extractions Name
EXTRACT-
Src_ip
Owner
kacharya
App
Splunk_Security_Essentials
Permissions
Owner
App
All apps
Source type
DNS_Logs
Sample event
1332017958.990000 CDP8CAi82kvSsJat8 192.168.202.83 35036 192.168.207.4 53 udp
63787 44.206.168.192.in-addr.arpa 1 C_INTERNET 12 PTR 3 NXDOMAIN F
F T F 0 - - F
Fields
Src_ip
Regular Expression
^(?:[^\t\n]*\t){2}(?P<Src_ip>[^\t]+)

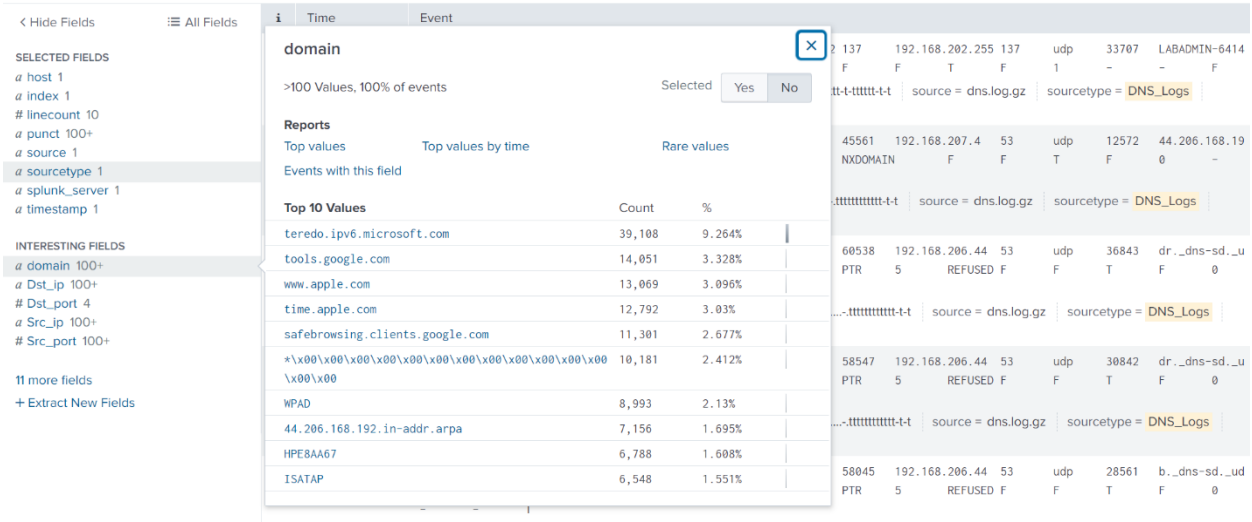


Fig: Data Parsed from the Log Event Sample

After the data is parsed, it is analyzed for further investigation using Search Processing Language and commands. This step helps in querying the data to identify and investigate security events and anomalies.

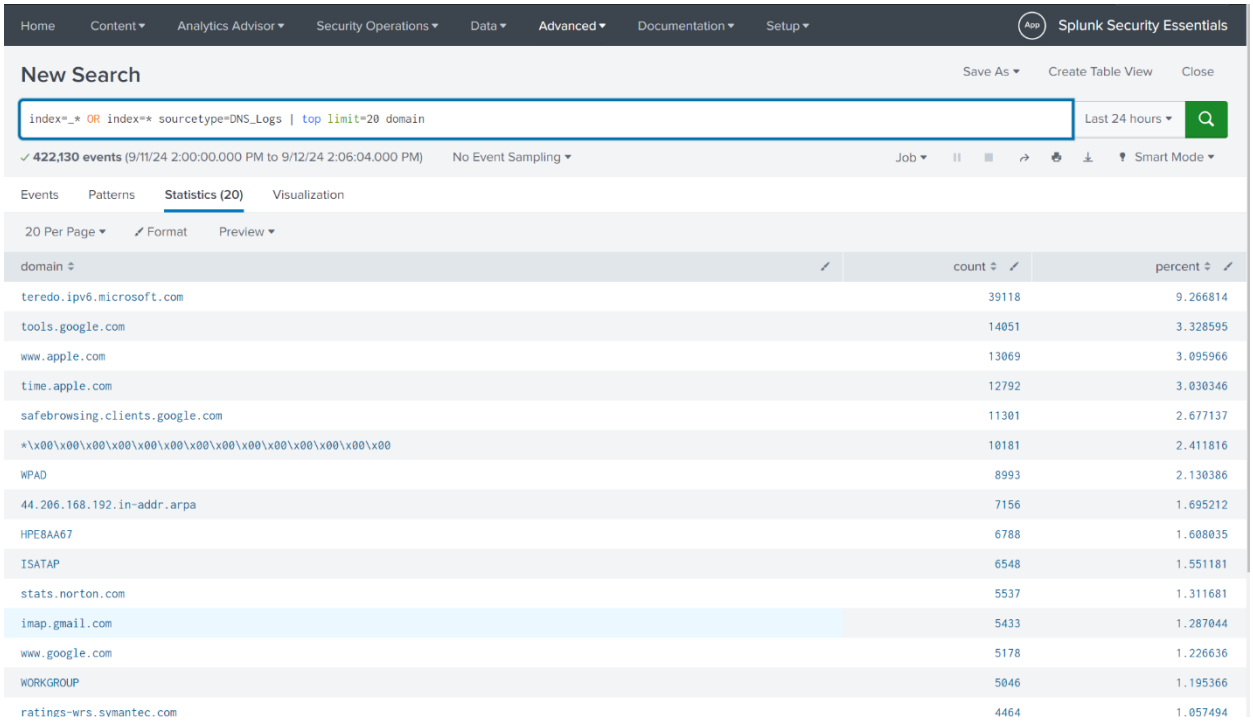
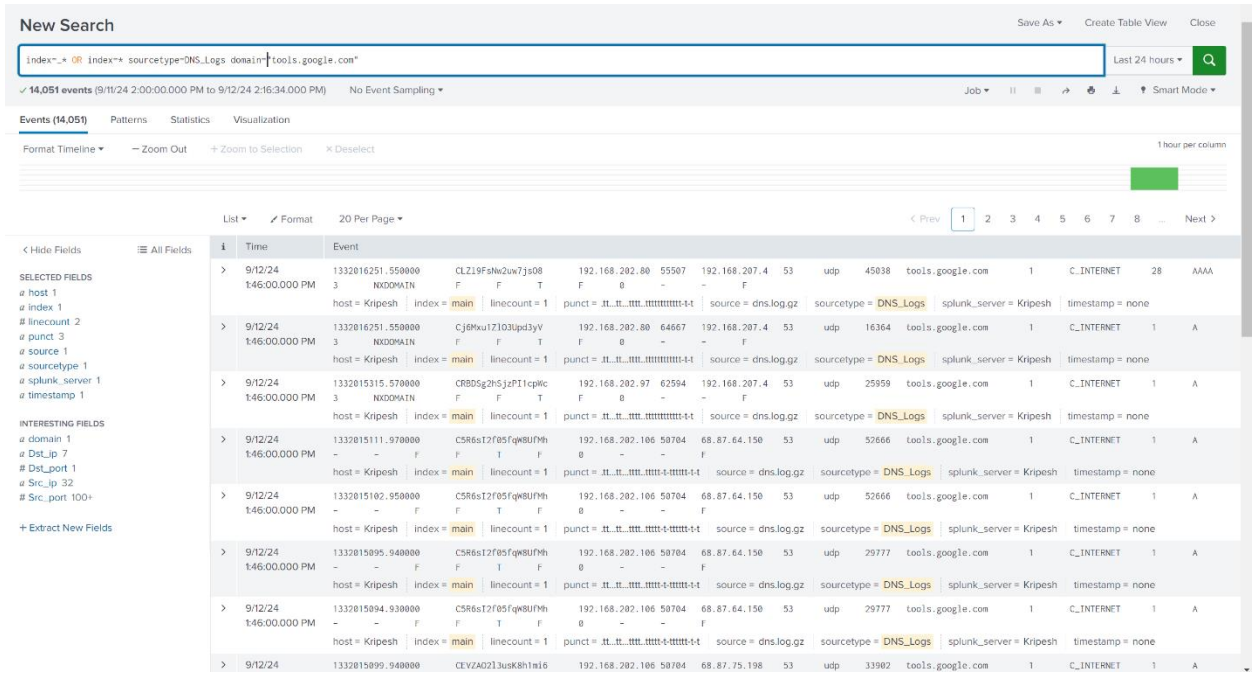
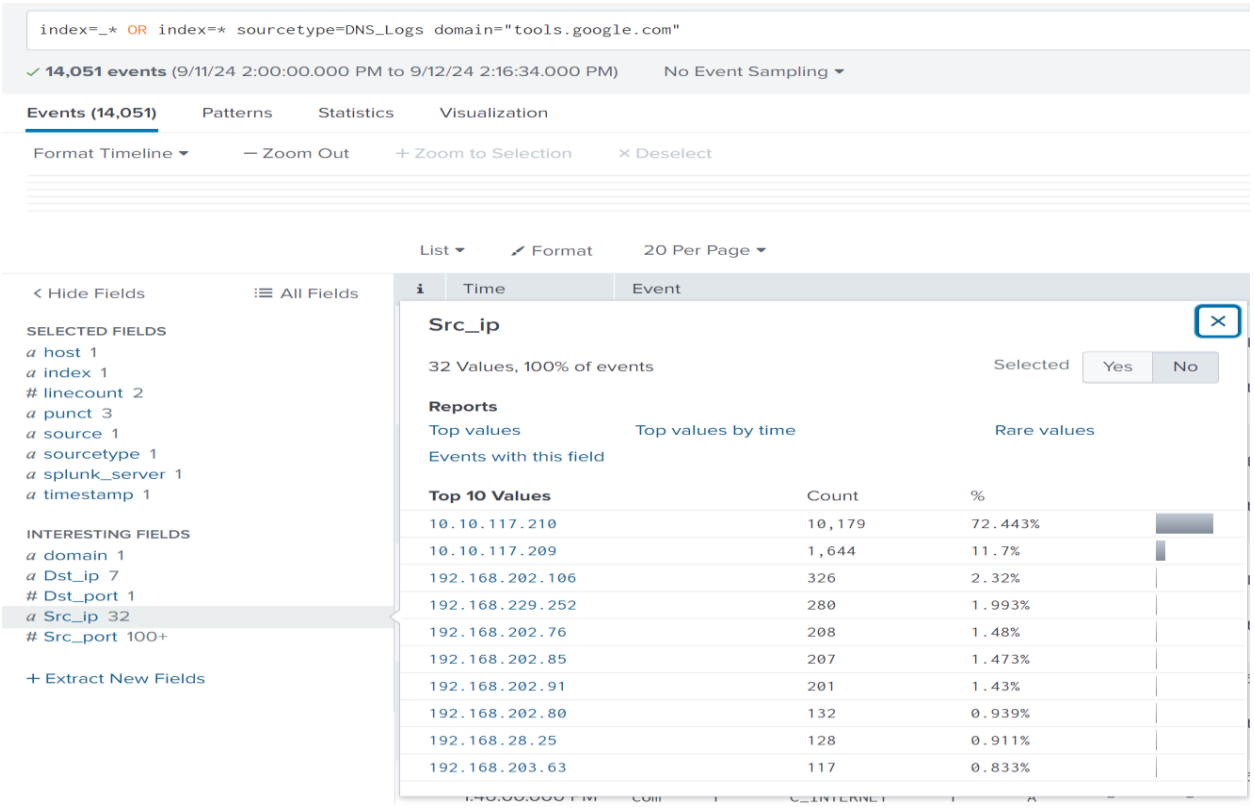


Fig: Looking For top 20 Domain mostly visited





In the above figure, to determine which users visited a particular site the most, a query was executed to identify and list the top users based on their visit frequency to the specified site.

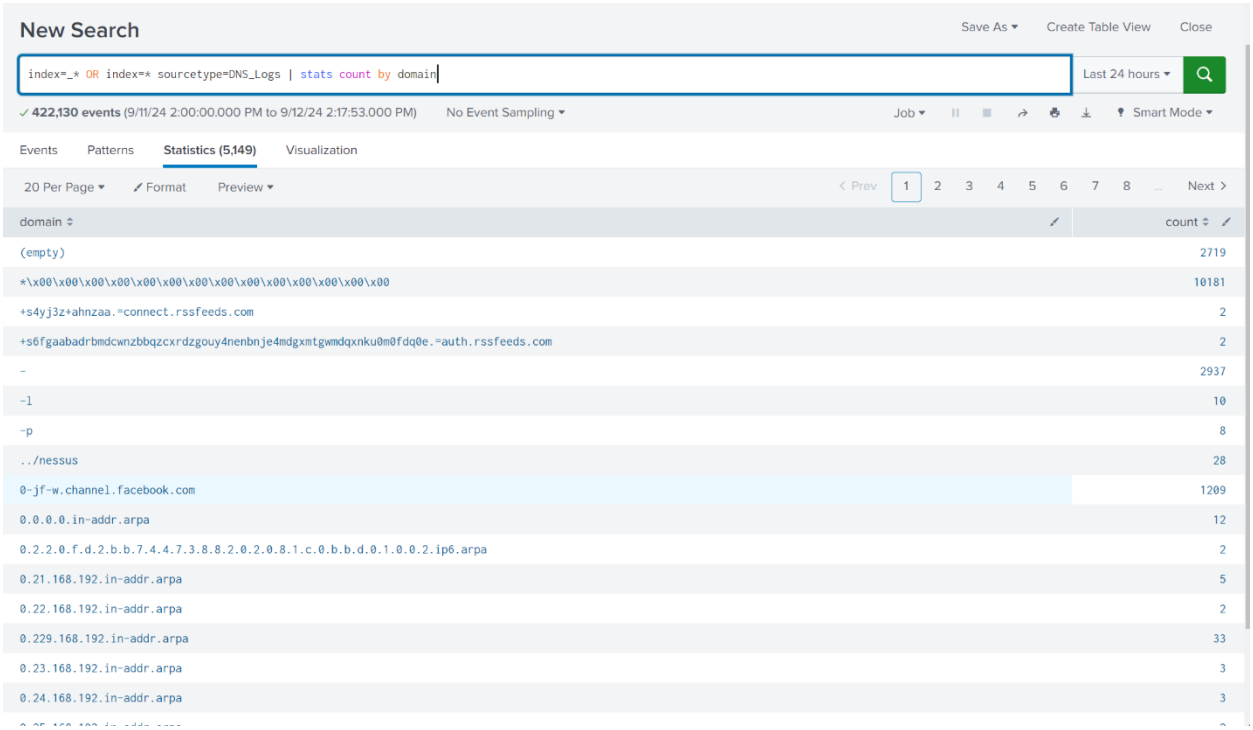
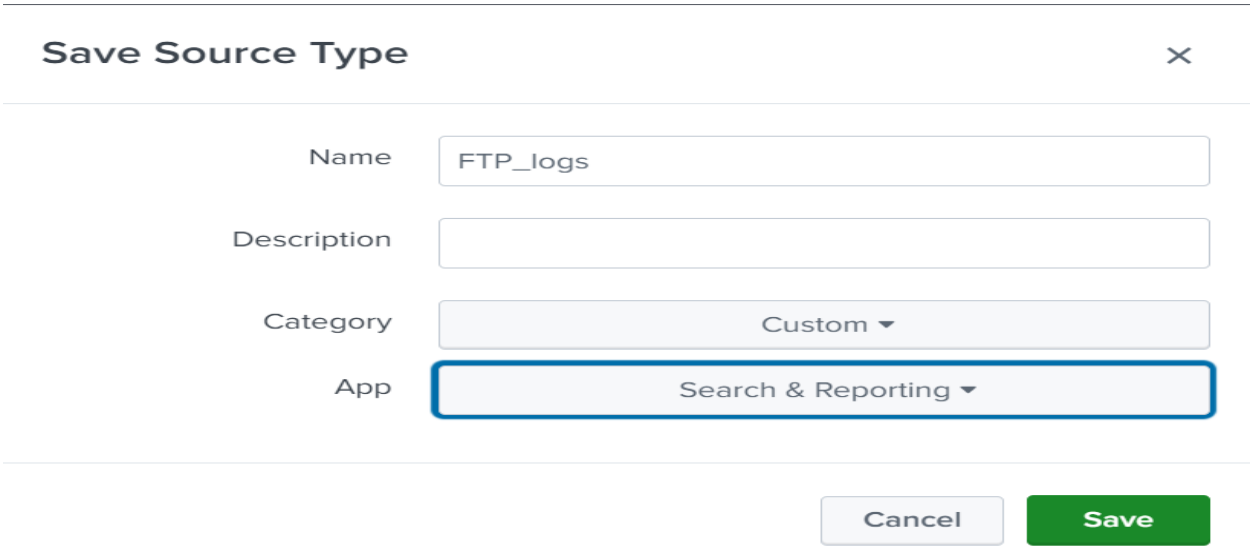


Fig: Query Executed to View Total Statistics Number of Domain

Similarly, the analysis was also conducted on the FTP log data to identify key patterns and user activity, using similar queries to extract valuable insights for further investigation.



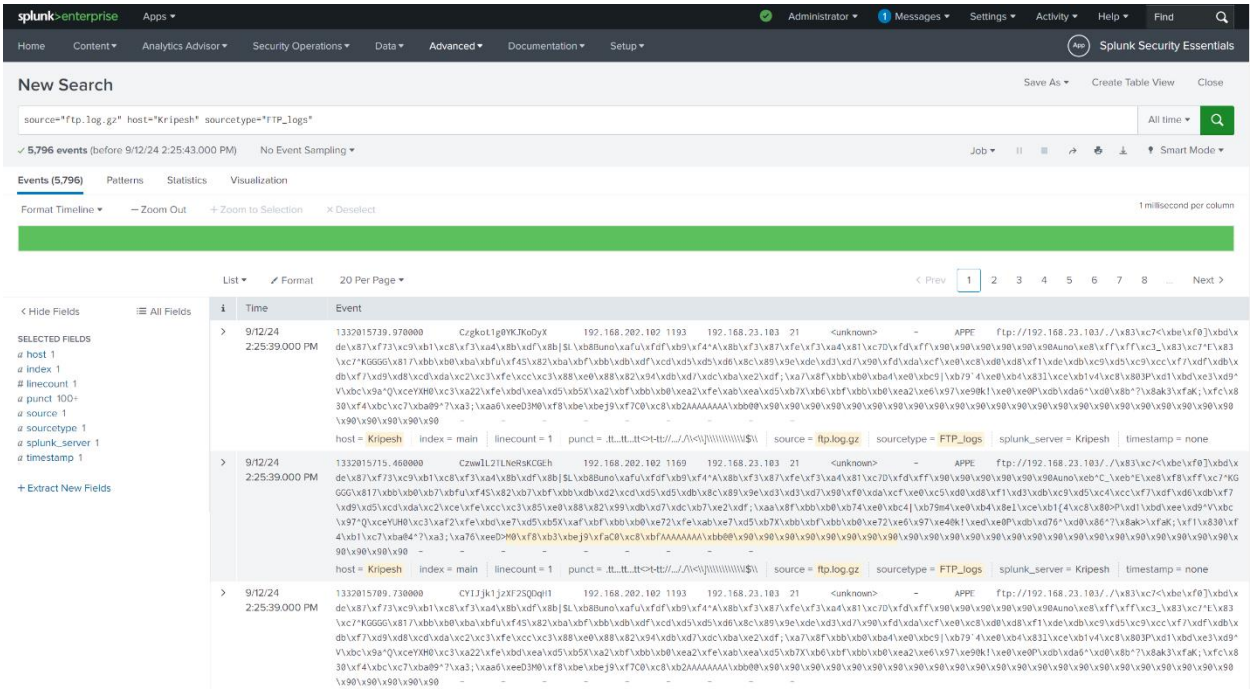
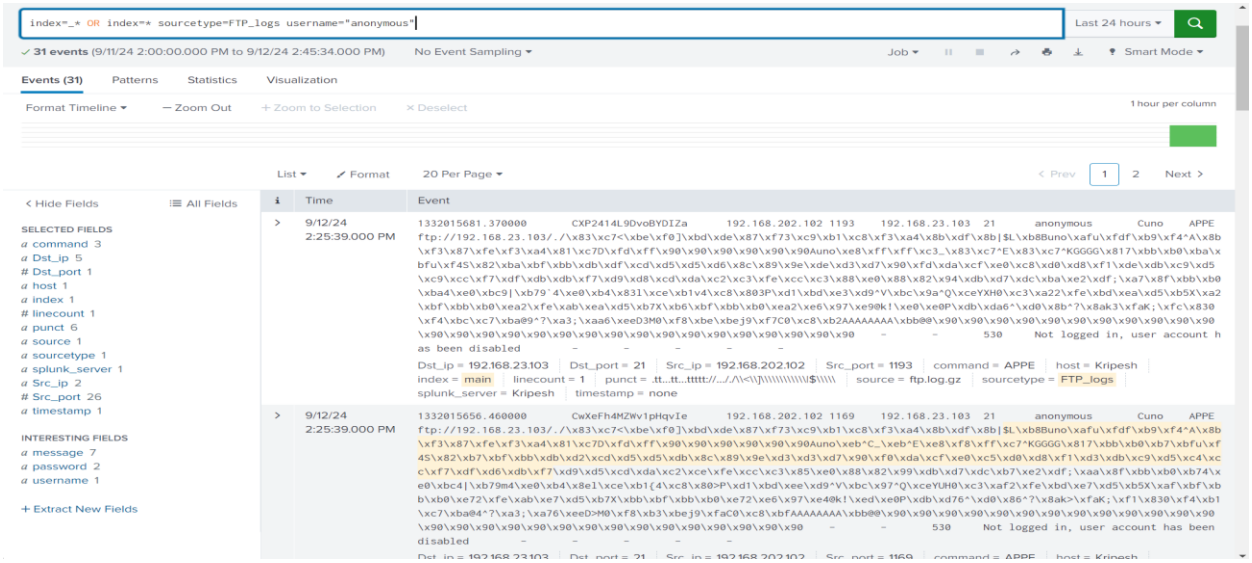
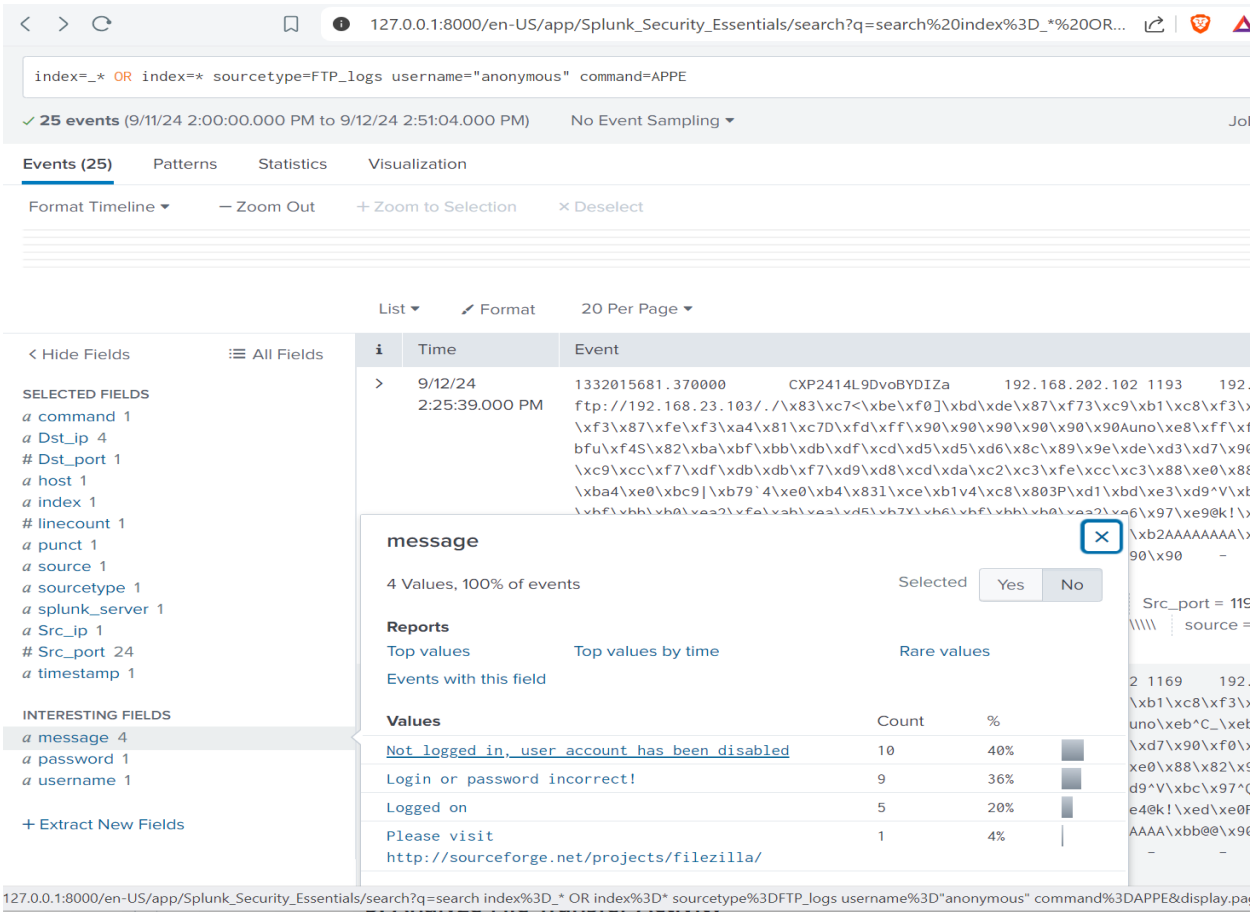


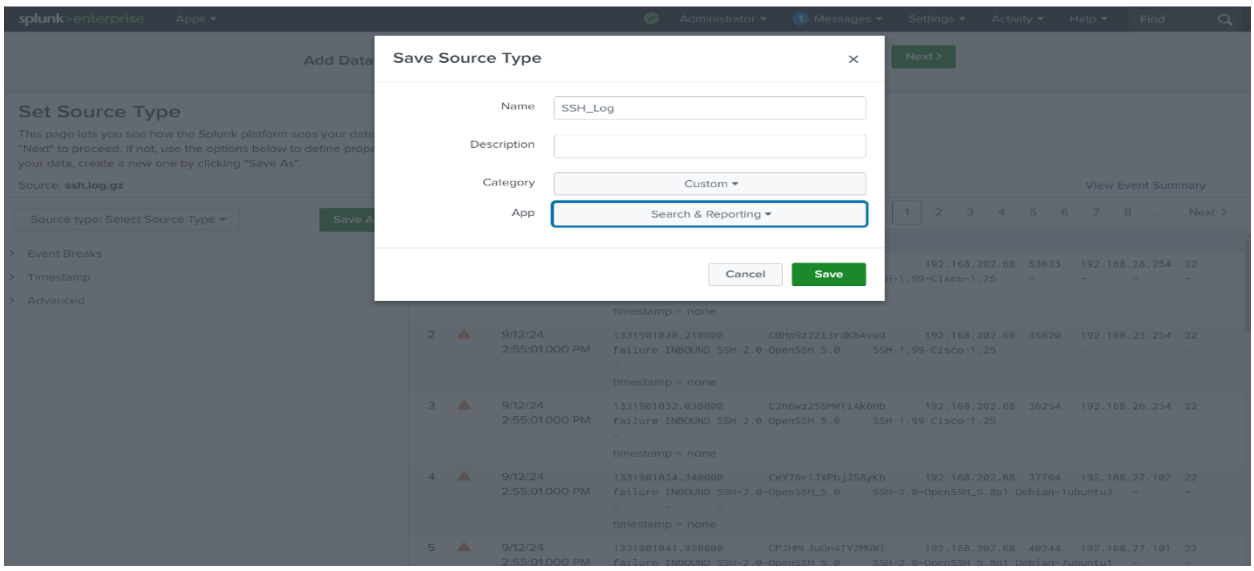
Fig: FTP Log data Uploaded

The user "anonymous" had attempted to send files multiple times, raising suspicion. The username was filtered, and the status of each attempt was checked based on the server logs to determine if any of the file transfers were successful.





In the same way, the SSH log file was analyzed to investigate user activity and identify any potential security issues, focusing on suspicious login attempts and unusual behavior patterns.



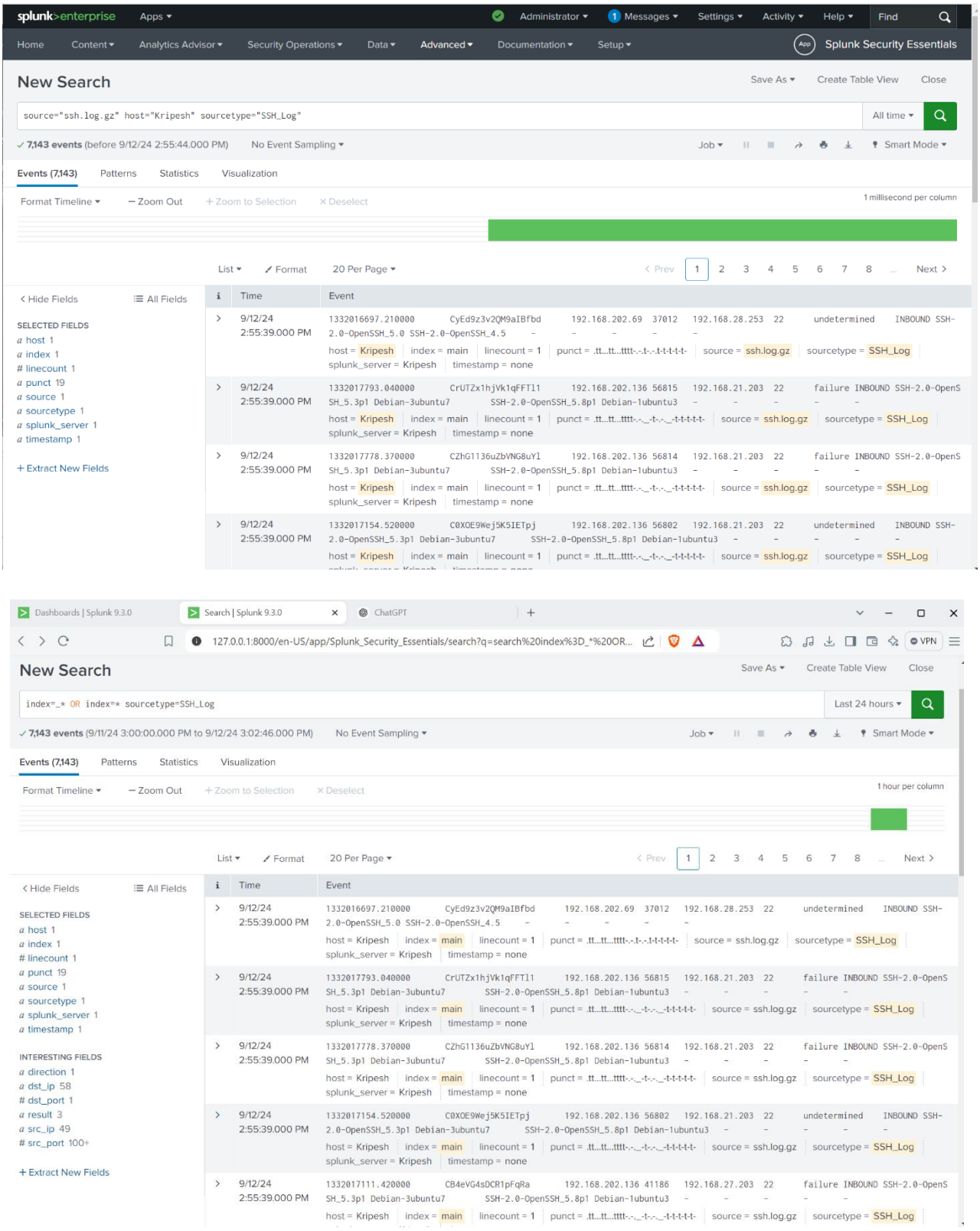
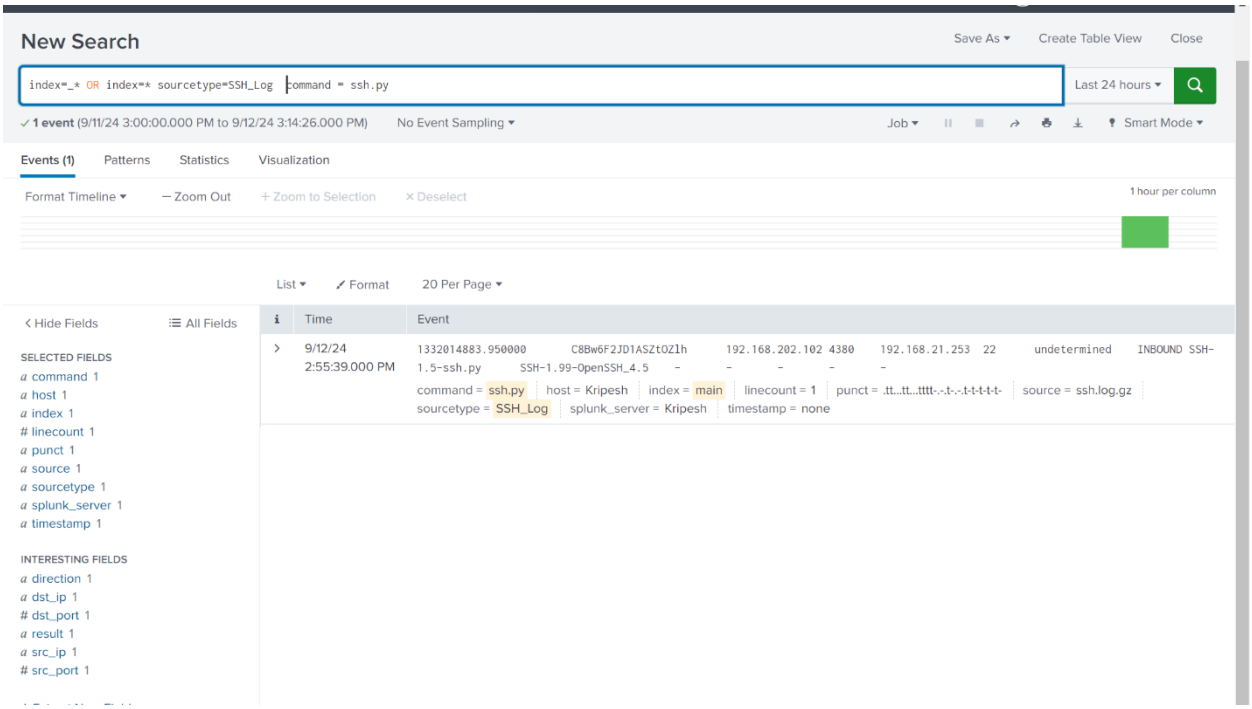


Fig: SSH Log after applying Data Parsing



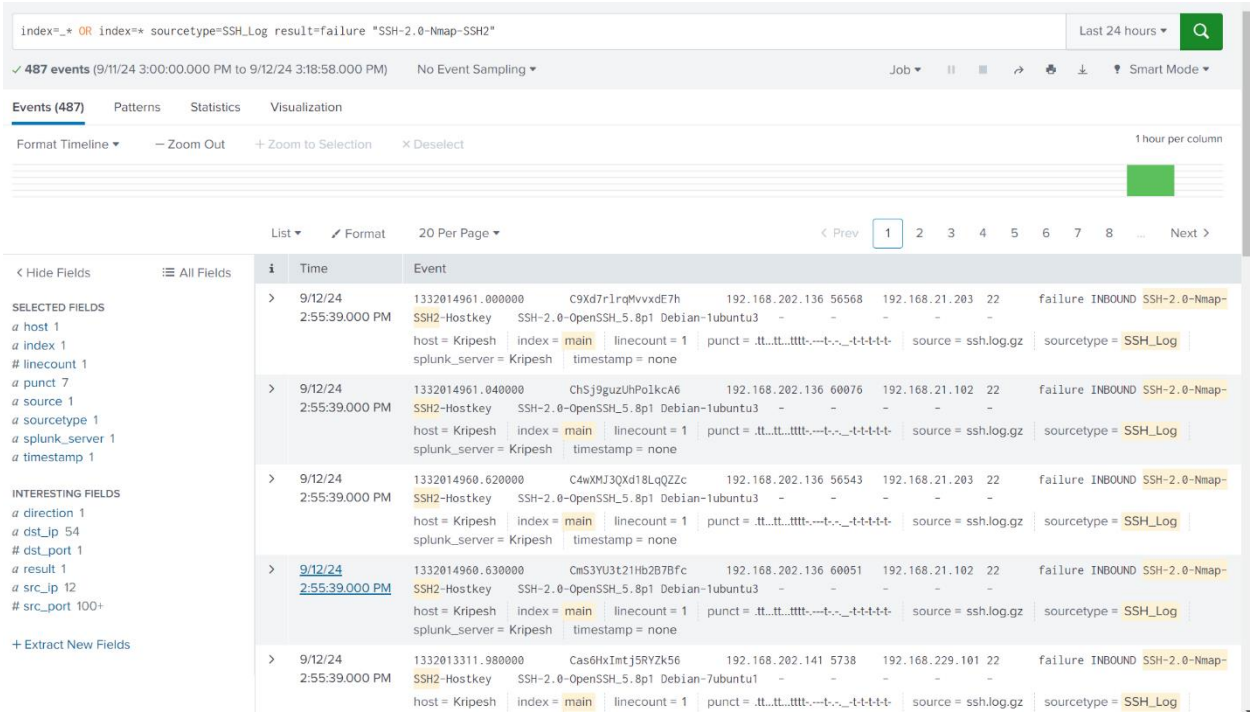


Fig: Investigating suspicious Events

2.4 Dashboard Creation

A custom dashboard was created in Splunk to provide a visual representation of the collected log data. This dashboard facilitated easy access to critical information and trends.

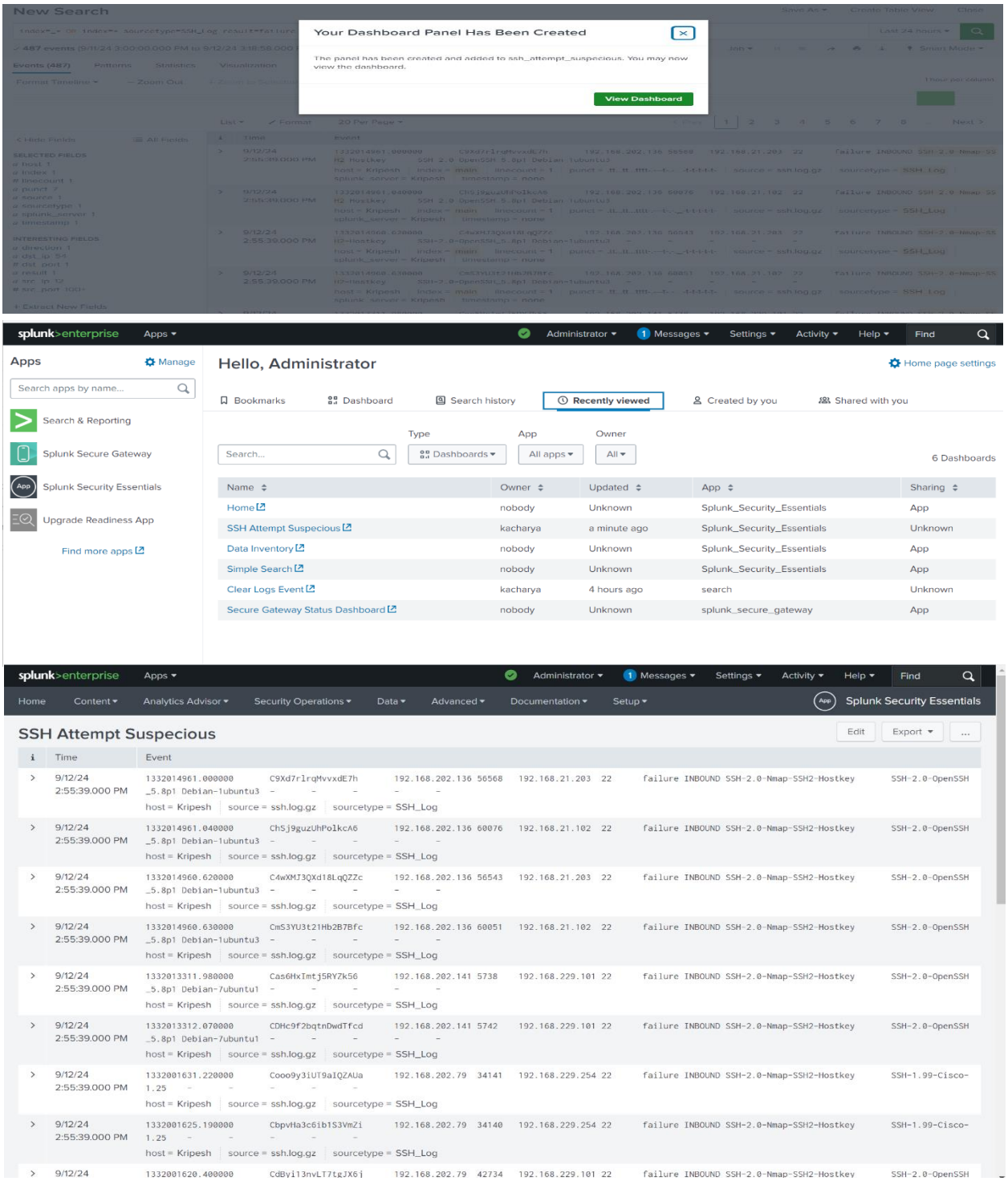


Fig: Dashboard Created

2.5 Reporting, Scheduling and Alerting

After Dashboard creation, the next step involved creating a comprehensive report based on the analysis, scheduling regular reports for continuous monitoring, and setting up alerts to notify of any suspicious activities or security events in real-time.

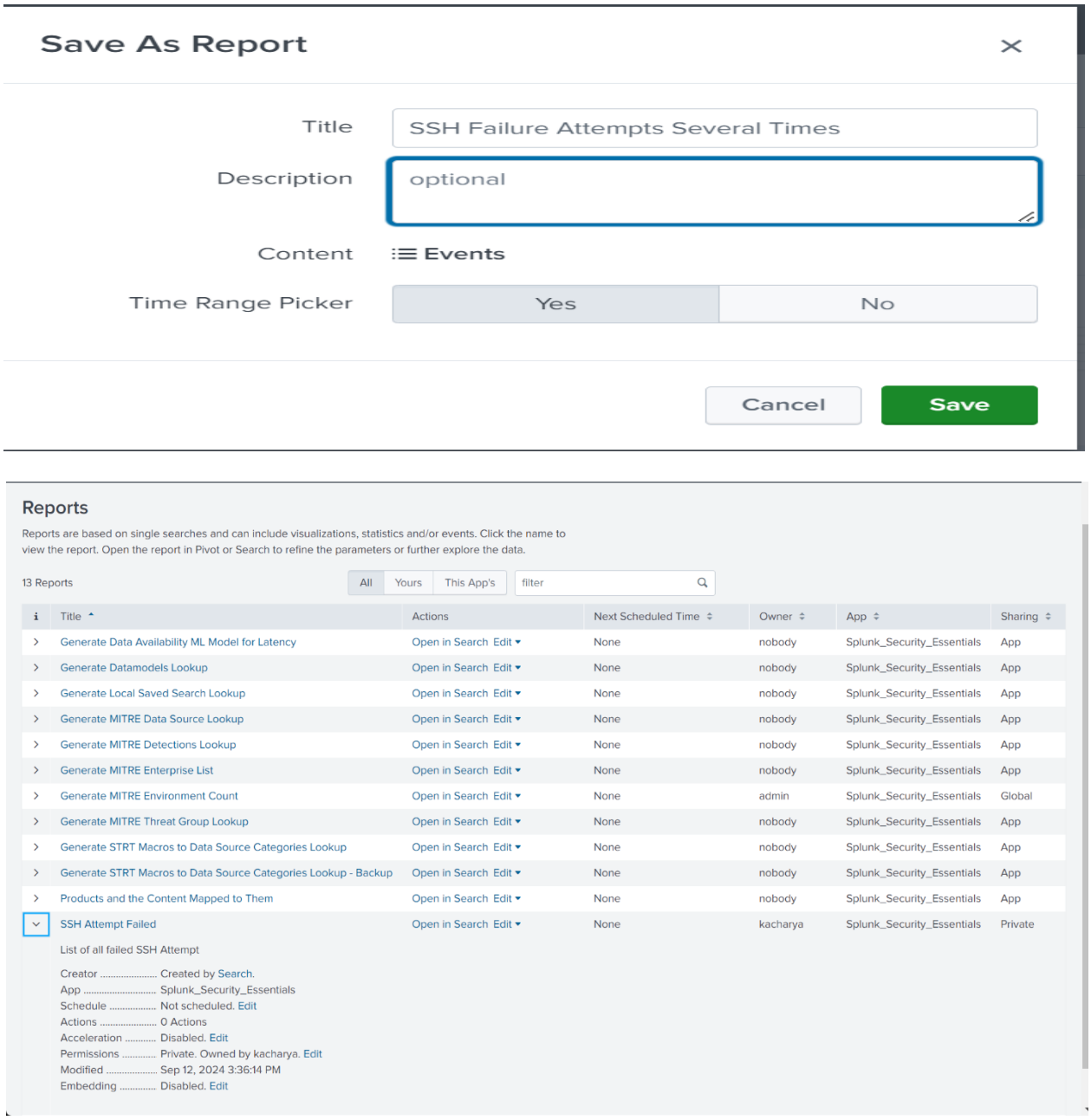


Fig: Report Created

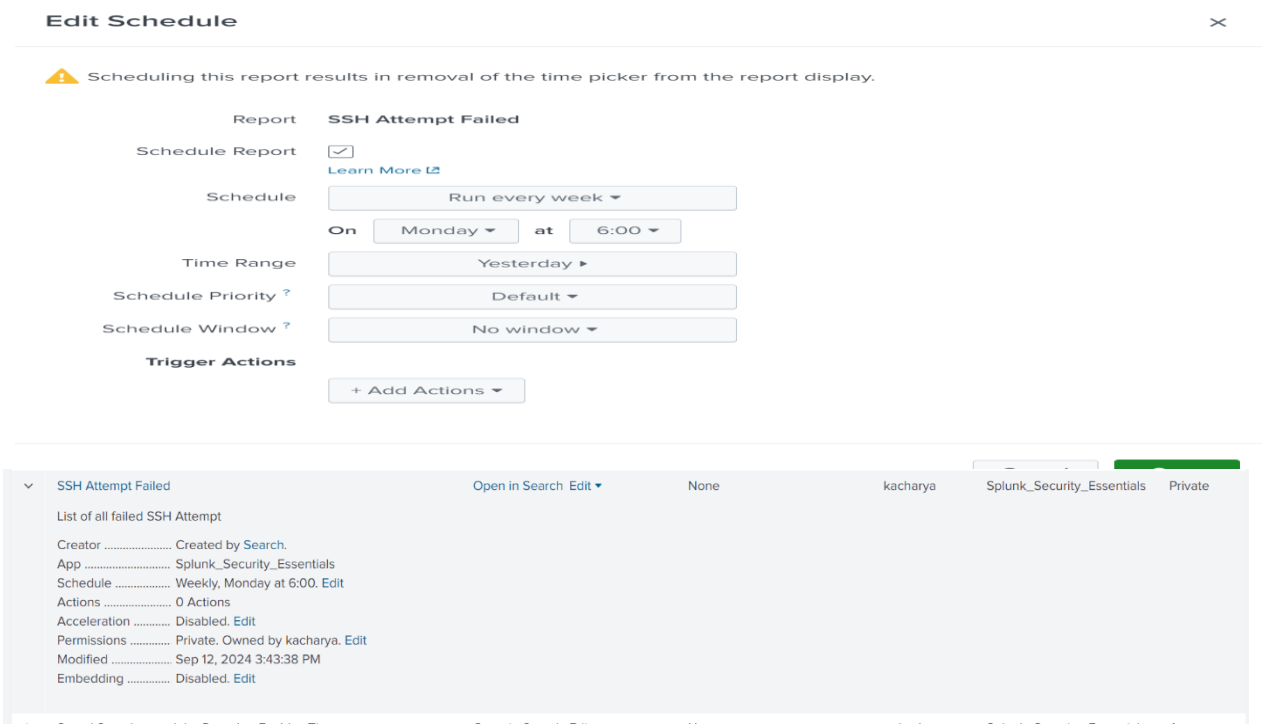


Fig: Scheduling a Report

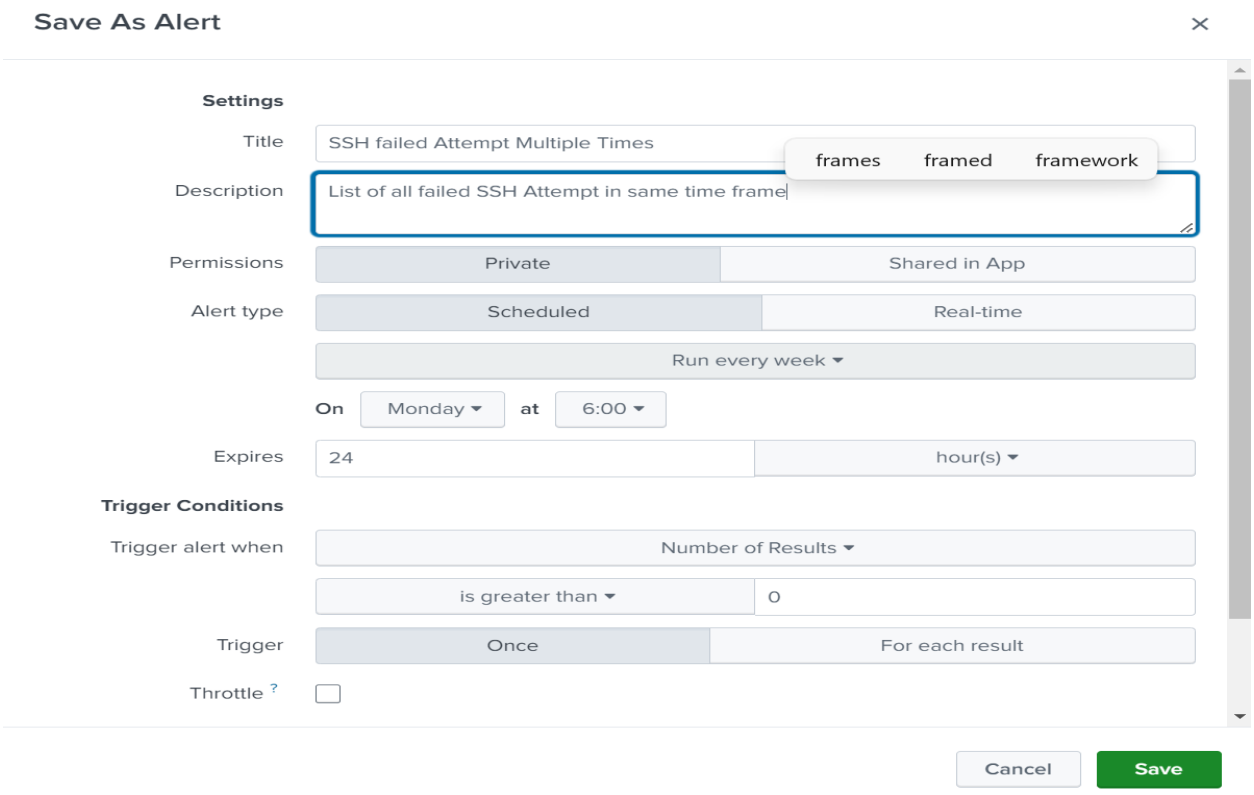


Fig: Creating an Alert

2.6 Continuous Monitoring

The last step is to implement continuous monitoring, ensuring that logs are regularly analyzed, reports are generated, and alerts are triggered automatically to detect and respond to any ongoing or emerging security threats.

3.Learning Resources

- **LetsDefend Learning Platform**: Provided hands-on training and practical knowledge on using Splunk for SIEM.
- **Rajneesh Gupta YouTube Channel**: Offered tutorials and insights into Splunk functionalities and best practices.

4. Conclusion

The project successfully demonstrated the capabilities of Splunk as a SIEM tool in a home lab setting. Through installation, log management, data analysis, and dashboard creation, valuable insights into security monitoring and incident response were gained. The use of SPL and alerting mechanisms enhanced the ability to detect and address suspicious activities effectively.