COMPREHENSIVE DEMONSTRATION: SPLUNK SECURITY INCIDENT AND EVENT MANAGEMENT TOOL (SIEM)

By Snehal Borhade

INDEX

COMPREHENSIVE DEMONSTRATION: SPLUNK SECURITY INCIDENT AND EVENT MANAGEMENT TOOL (SIEM)

Abstract

This project, titled "A Comprehensive Demonstration of Splunk SIEM," provides an in-depth exploration of Splunk's Security Information and Event Management (SIEM) capabilities. Splunk is a powerful platform for searching, monitoring, and analyzing machine-generated data via a web-style interface. Our demonstration focuses on key functionalities that are essential for effective security management, including events, dashboards, lookups, reports, and alerts. We begin by showcasing how Splunk processes and indexes large volumes of data, transforming raw data into meaningful events. This foundational step enables the extraction of actionable insights from diverse data sources. We then delve into the creation and customization of dashboards, illustrating how Splunk's intuitive interface allows for real-time visualization of critical metrics and trends.Through this comprehensive demonstration, we aim to illustrate the robust features of Splunk SIEM and its application in real-world scenarios. This project serves as a valuable resource for security professionals seeking to leverage Splunk for enhanced visibility and control over their IT environments.

Purpose

The purpose of the project titled "A Comprehensive Demonstration of Splunk SIEM" is to provide a detailed and practical understanding of Splunk's Security Information and Event Management (SIEM) capabilities.This project helps to understand and explore various aspects of splunk. This project is a basic overview of how logs are monitored,analyzed and visualized in the cyber-security industry.To demonstrate practical applications of Splunk in a real-world security environment. By showcasing how Splunk can be used to visualize data, enrich event information, and generate actionable insights, the project aims to provide a hands-on learning experience.

Approach

The approach for the project titled "A Comprehensive Demonstration of Splunk SIEM" involves a systematic and structured methodology to explore and demonstrate the various functionalities of Splunk.Setting up data inputs ,explore basic and advanced search commands to filter and extract relevant information from the events,Set up real-time dashboards to monitor critical events and system performance indicators,Demonstrate how to use lookups in searches to enhance the value and meaning of the data.

Procedure

Brief overview :

SIEM

SIEM stands for Security Incident and Event Mananegement. SIEM (Security Information and Event Management) tools are essential for collecting and managing security-relevant data, which is crucial during investigations. These tools enhance network visibility by providing comprehensive awareness of activities occurring between devices on a network. The insights derived from SIEM tools enable security teams to swiftly investigate and respond to security incidents. With numerous advantages, SIEM tools significantly improve the efficiency and effectiveness of security teams in incident response and management.SIEM (Security Information and Event Management) tools provide comprehensive access to event and activity data across a network, including real-time monitoring. Given that networks can connect to hundreds of different systems and devices, SIEM tools are designed to ingest and centralize this vast amount of data for easy access and analysis. These tools continuously monitor systems and networks in real-time, applying detection rules to identify potential malicious activity. When an activity matches a rule, an alert is generated and sent to security teams for evaluation. Additionally, SIEM tools serve as data retention systems, offering access to historical data which can be retained or deleted based on the organization's requirements. SIEM tools are primarily used by Security analyst and SOC analyst for monitoring data and access logs. Security analyst Continuously monitor the network for suspicious activity and anomalies.Respond to alerts generated by SIEM tools based on predefined detection rules , to correlate events from various sources to understand the full context of a security incident. SIEM is also used to investigate the root cause of security incidents by analyzing the logs and data collected by the SIEM tool.Maintain audit trails for all activities and access logs to support compliance audits.

SOC analyst is Security Operation Centre analyst who is responsible for monitoring every factor related to security I.e incoming and outgoing data, access to that data,log entries etc. Act as the first responders to security incidents, leveraging SIEM alerts to quickly assess and prioritize threats.

They utilize advanced analytics and threat intelligence integrated into the SIEM to detect sophisticated threats and use insights gained from SIEM data to train and develop the skills of team members, enhancing overall SOC capabilities.
There are many siem tools available such as QRadar, Splunk , Arcsight etc. The one demonstrated in this project is splunk.

Splunk

Splunk is a leading platform for operational intelligence, providing powerful tools for searching, monitoring, and analyzing machine-generated data from a variety of sources. Designed to handle large volumes of data in real-time, Splunk transforms raw data into valuable insights, enabling organizations to make informed decisions and respond swiftly to security threats and operational issues. Splunk's robust features include data ingestion, indexing, and real-time search capabilities. It supports the creation of detailed dashboards, reports, and alerts, which facilitate proactive monitoring and analysis. With its ability to handle diverse data sources and formats, Splunk is widely used for security information and event management (SIEM), IT operations, business analytics, and more. By leveraging Splunk, organizations can gain comprehensive visibility into their IT infrastructure, enhance security posture, and drive operational efficiency, making it an essential tool for modern enterprises.
There are various features used in Splunk which helps use to categorize,monitor and visualiza data. It provides comprehensive view of the functions going on within the company.Some Features within splunk are events, lookups,dashboard,reports,alerts,logs ,indexes,forward cluster.

Splunk interface:

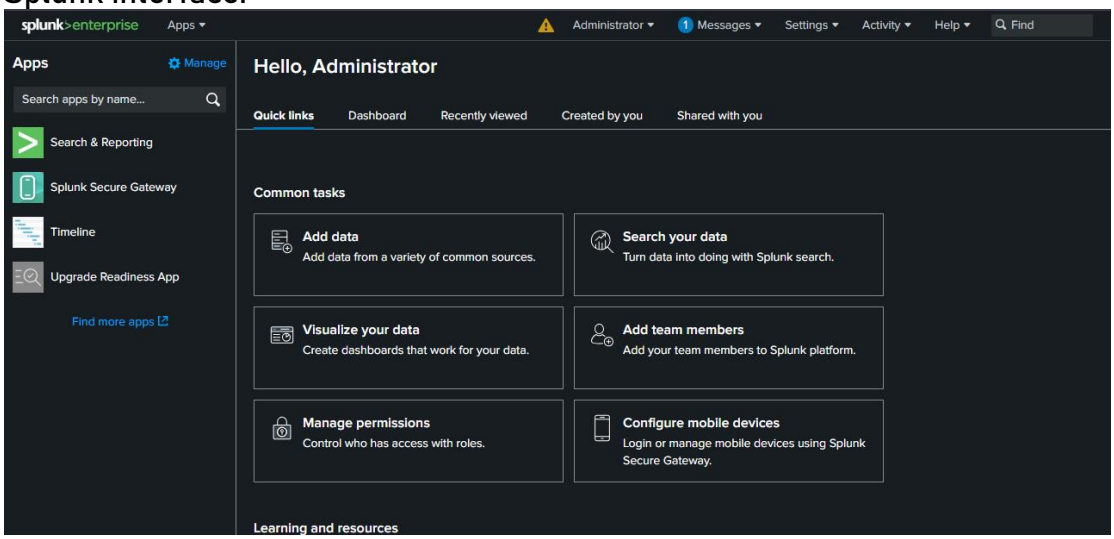

Fig.1 interface

To input data:

We can input data in various way by uploading a file or using by making indexes. If we upload a data file it can be selected by source.

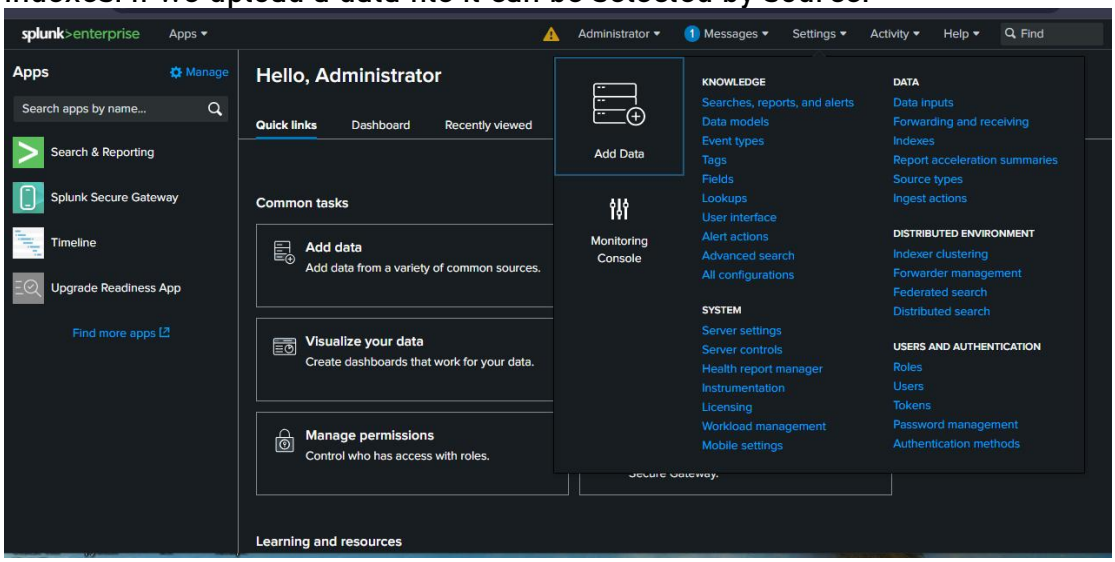

Fig.2 input data 1

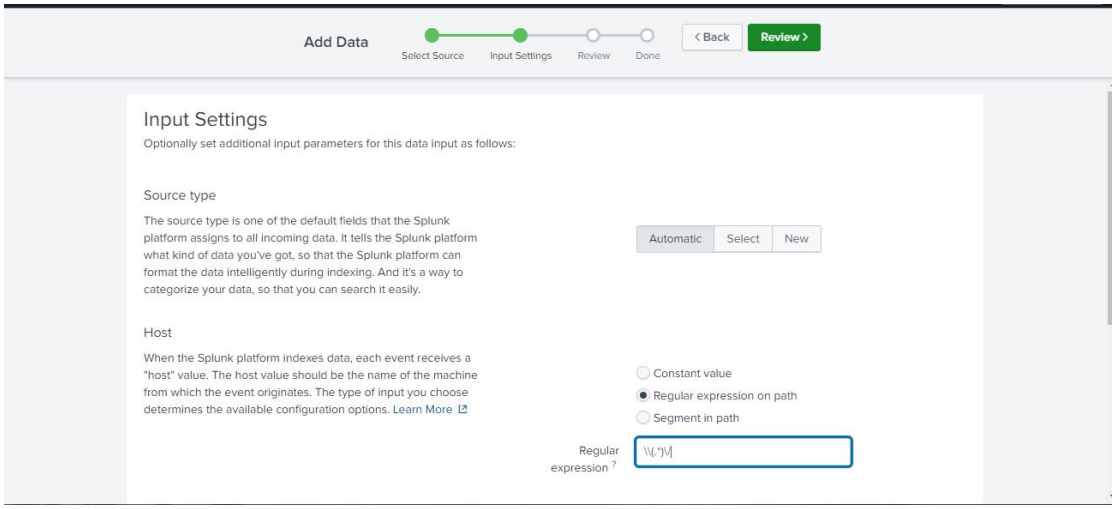

Fig.3 input data 2

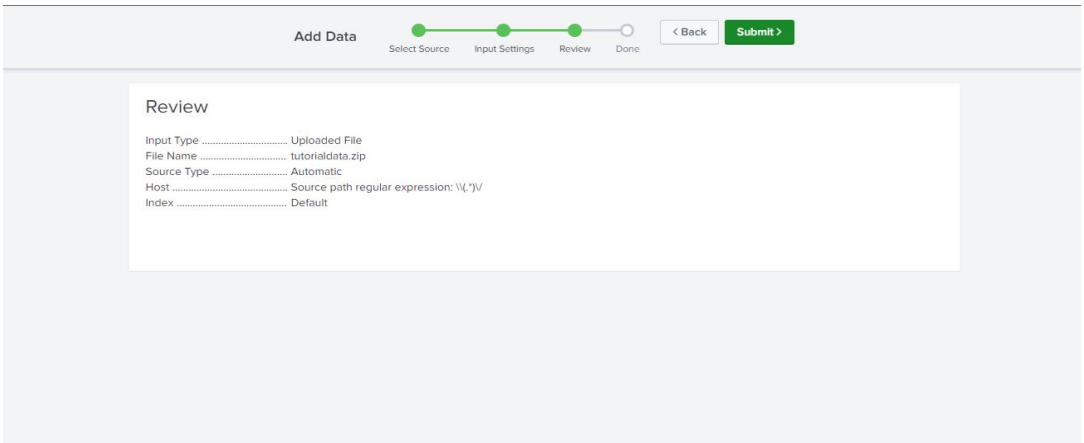

Fig.4 input data 3

Once the data is upoaded it can be searched by its soucrce:

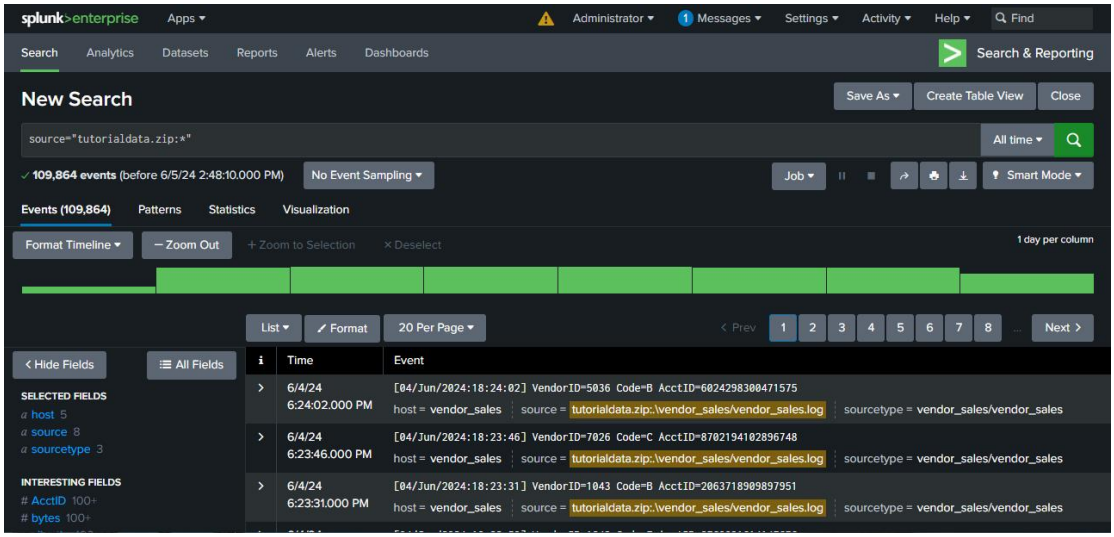

Fig5.Search

Search feature is used to search through the data and get results for our specific keyword.In Splunk, the search feature is the core functionality that allows users to query and analyze large volumes of machine-generated data. It enables users to search for specific events, patterns, or trends within their data sets. The search feature supports a powerful query language that enables complex searches and filtering based on various criteria such as time, source, and event type.Users can utilize search commands to manipulate and analyze their data, performing functions like aggregation, filtering, and visualization. Splunk's search feature also supports real-time searching, allowing users to monitor data as it streams in, and historical searching, enabling analysis of past events.Overall, the search feature in Splunk provides users with the ability to extract valuable insights from their data, facilitating proactive monitoring, troubleshooting, and decision-making.

To create event:

In Splunk, events represent individual occurrences or entries in the data being analyzed. Each event typically contains timestamped information about a specific action, event, or log entry. Splunk's event feature organizes and indexes these events, making them searchable and analyzable.When we create an event we highlight the fields we want to be noticing more. Fro eg. We can create a event or highlight the areas which has failed password entry. We further can also make another event that will show failed entry or login for valid user and invalid user.

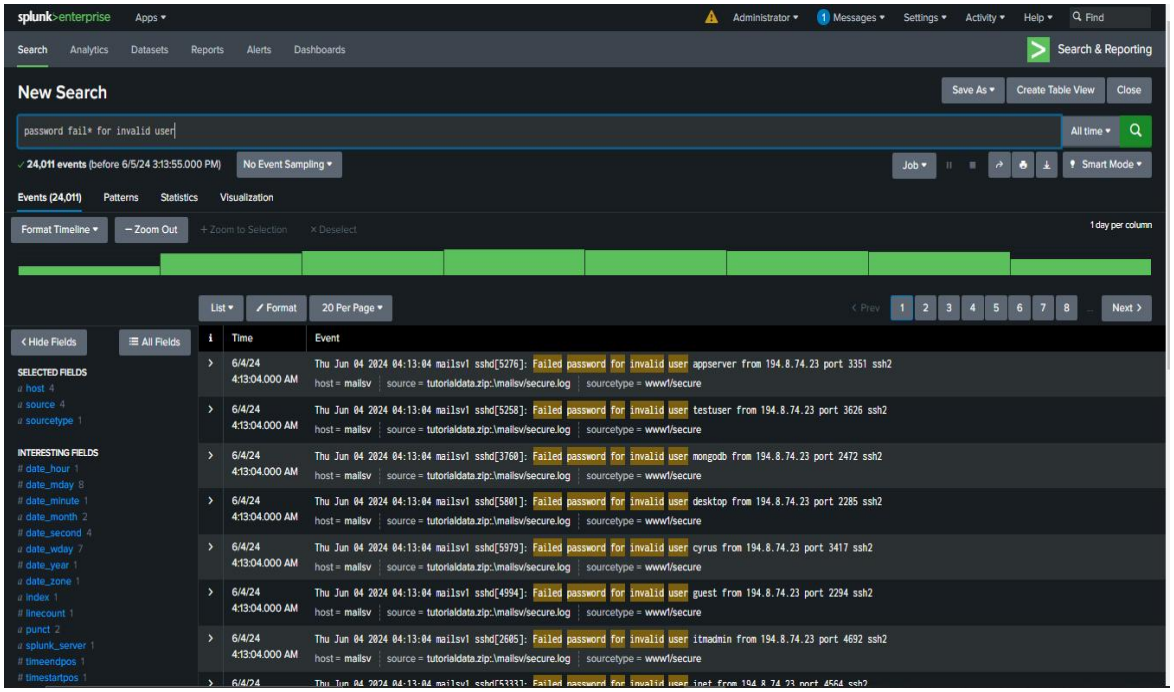

Fig6 event 1

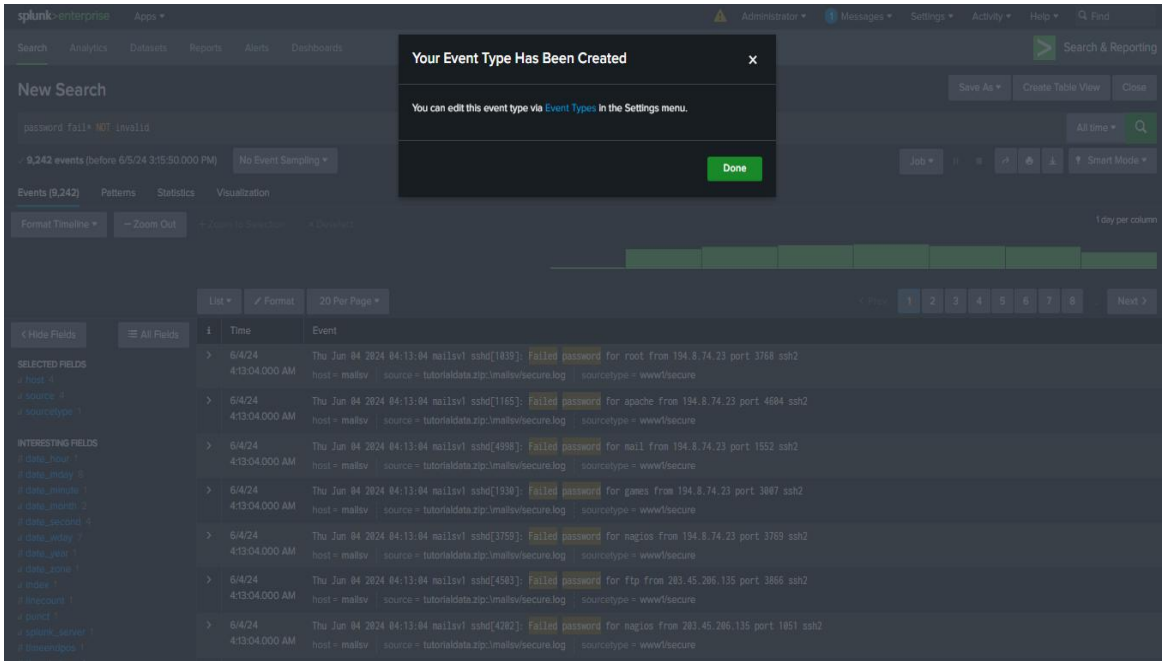

Fig7 event 2

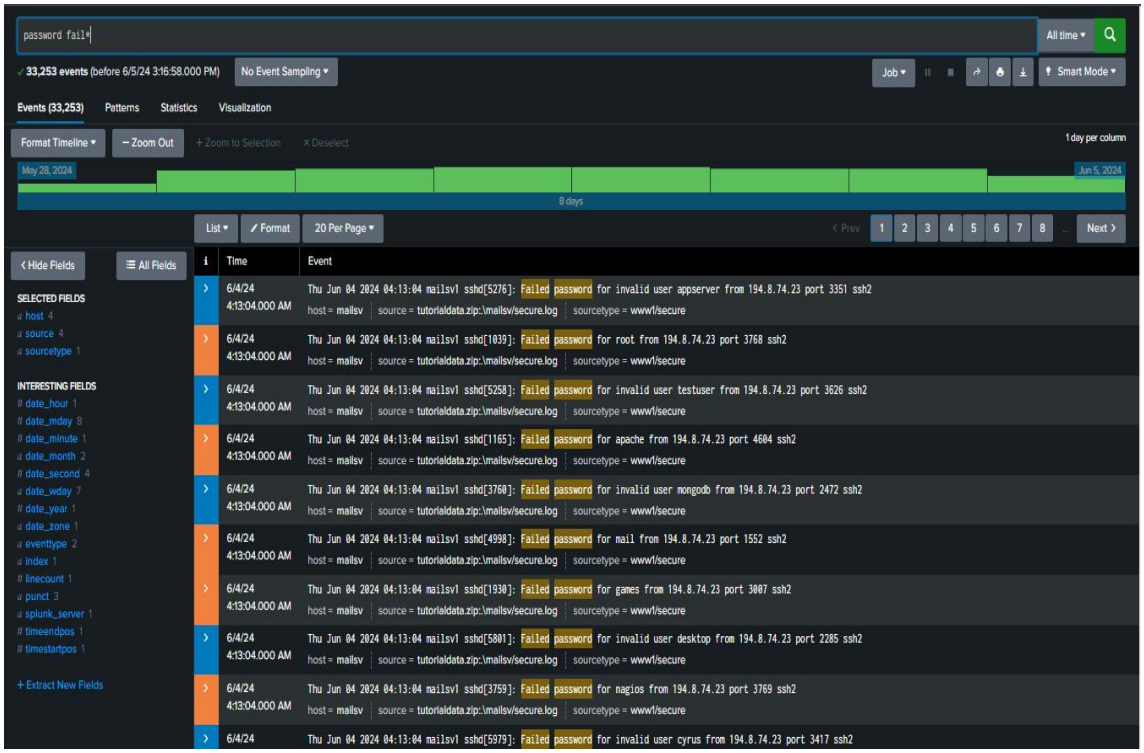

Fig8. event 3

Here password fail by invalid user is shown by orange and by valid user in blue. We can set color, name, description and value for how critical it is.
We can also set permissions for event type. Permission is giving rights to other users or apps to write or read our event.

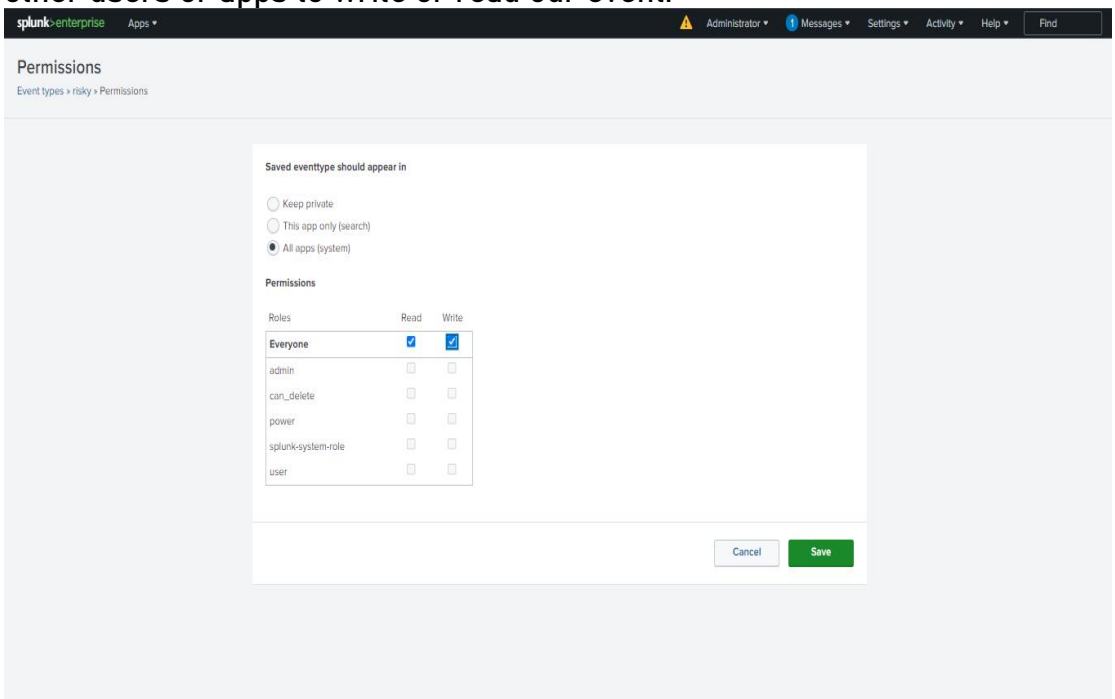

Fig9. event permissions

Count by event type :

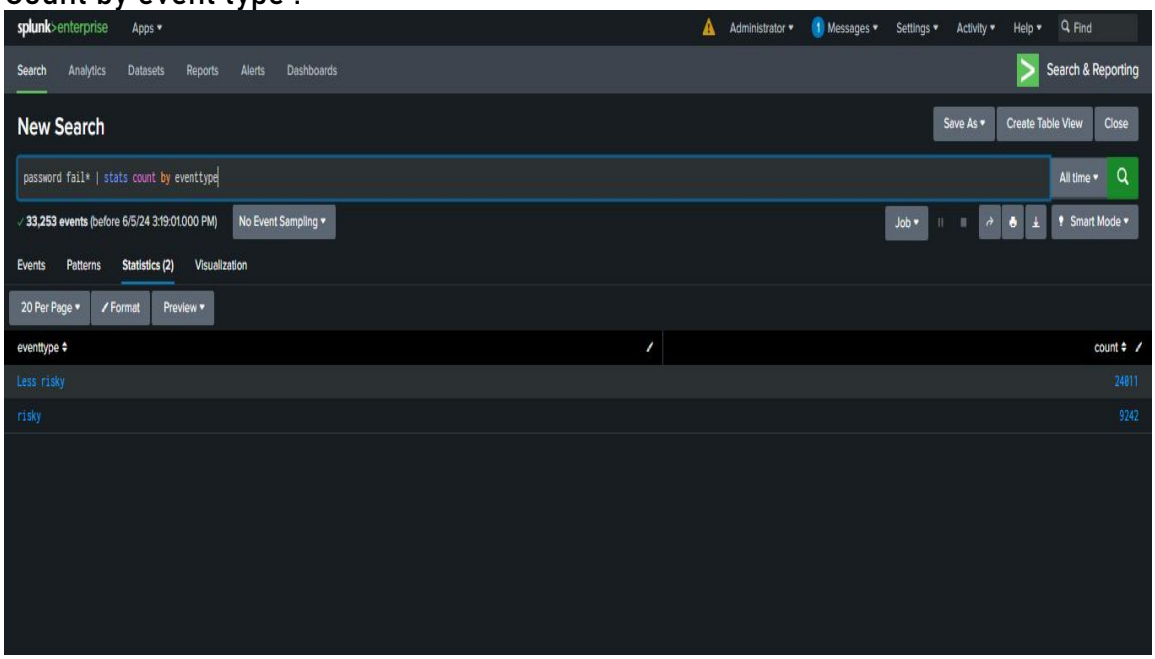

Fig10. event count

We can also create tables and visualisation using command table and then specifying columns we want. :

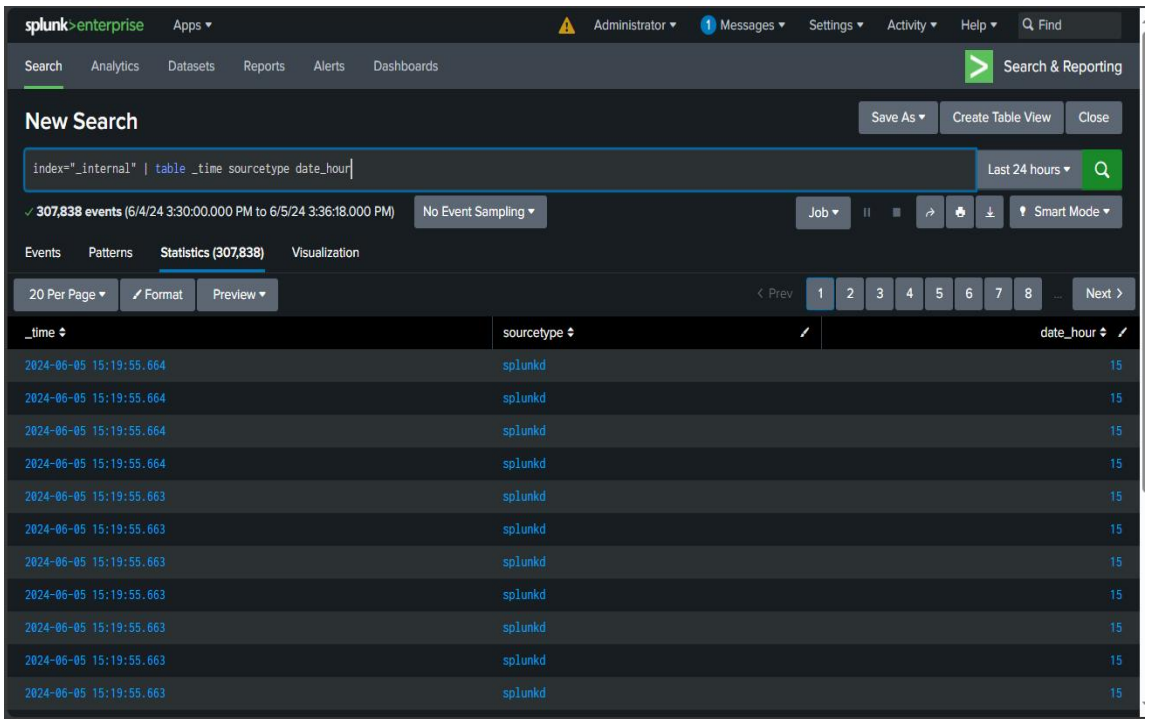

Fig11. table

Here we have used table command to get table of time,source-type and date.

To visualize this data we can simply choose visualize:

Fig12. table_visualize

Visualization provide various pattern options such as bar chart , line chart , pie chart , bubble , geographical etc.

Jobs:

It keeps record of all the searches we have done. The search can be deleted,stored, scheduled, paused and restart from here. This option can be found in activity section.

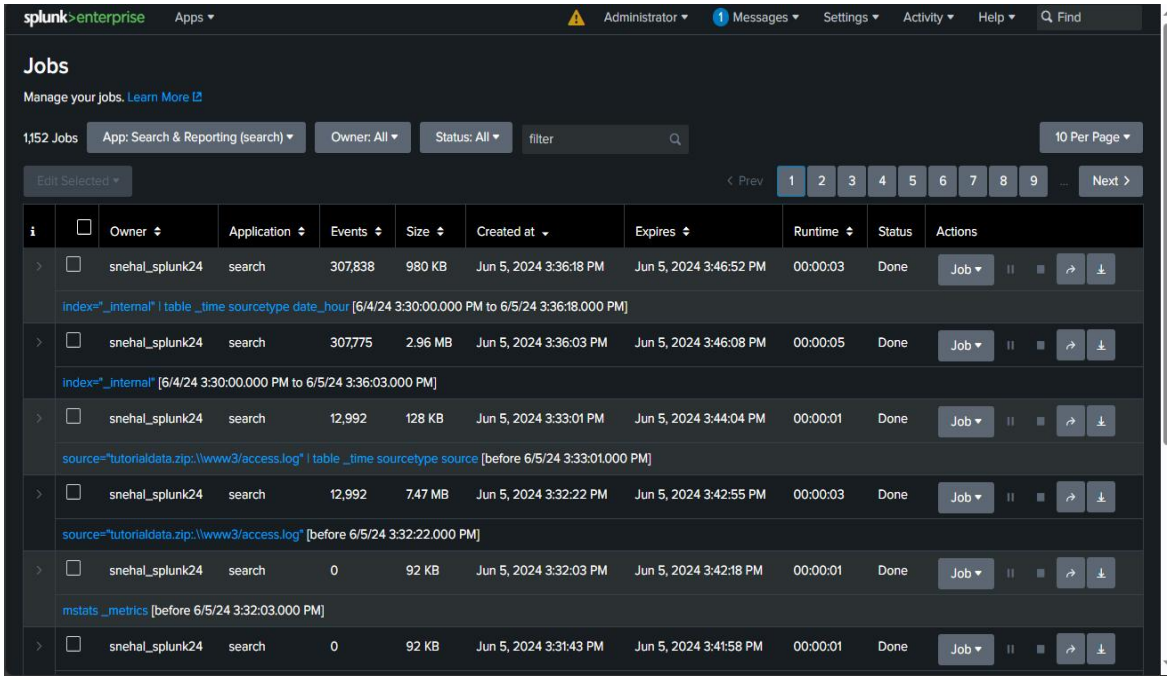

Fig13. Jobs

Report :

In Splunk, the report feature allows users to create structured summaries of data analysis and insights for further review or distribution. Reports in Splunk are customizable and can be tailored to specific needs and requirements.Reports in Splunk enable users to summarize data findings from searches, dashboards, or saved events. Users can aggregate data using various statistical functions, such as count, sum, average, and more.Reports can include visualizations such as charts, graphs, and tables to present data in a clear and understandable format. Users can customize the appearance and layout of visualizations to suit their preferences.Splunk allows users to schedule the generation and distribution of reports at predefined intervals. Users can schedule reports to be sent via email or saved to a shared location, ensuring stakeholders receive timely updates and insights.Splunk reports offer flexibility in terms of customization. Users can customize report parameters, data filters, and time ranges to focus on specific aspects of the data. Additionally, users can add annotations, comments, and descriptions to provide context and insights into the data presented in the report.

We can save our search as report to create a report.

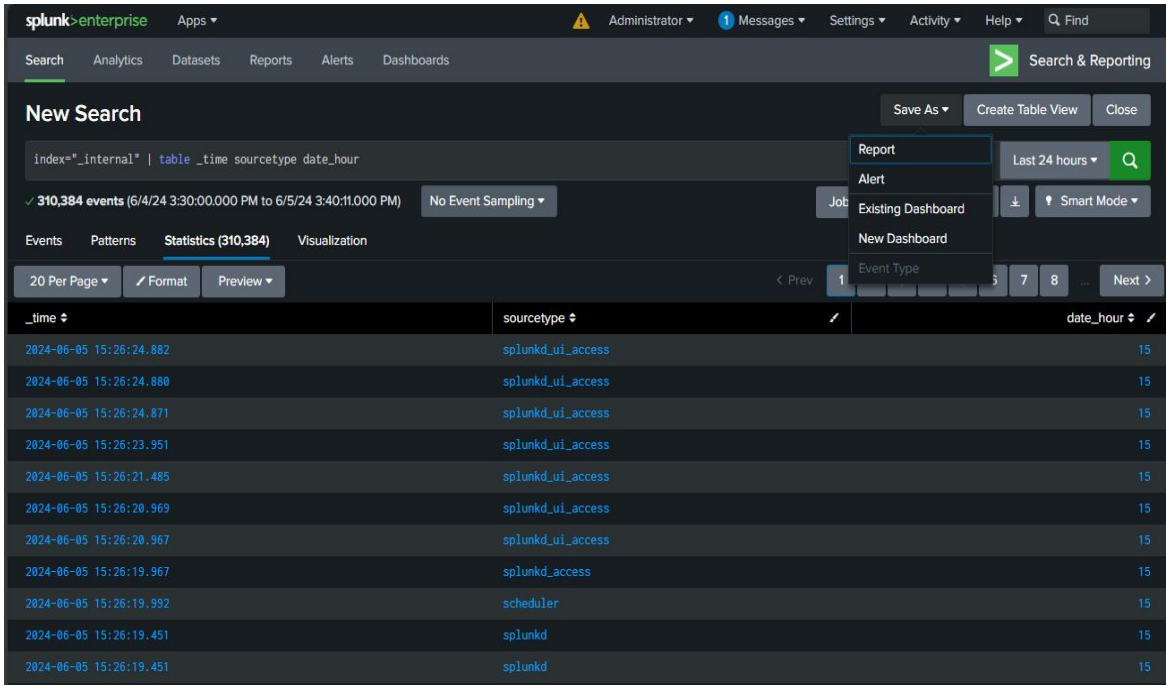

Fig14. Reports

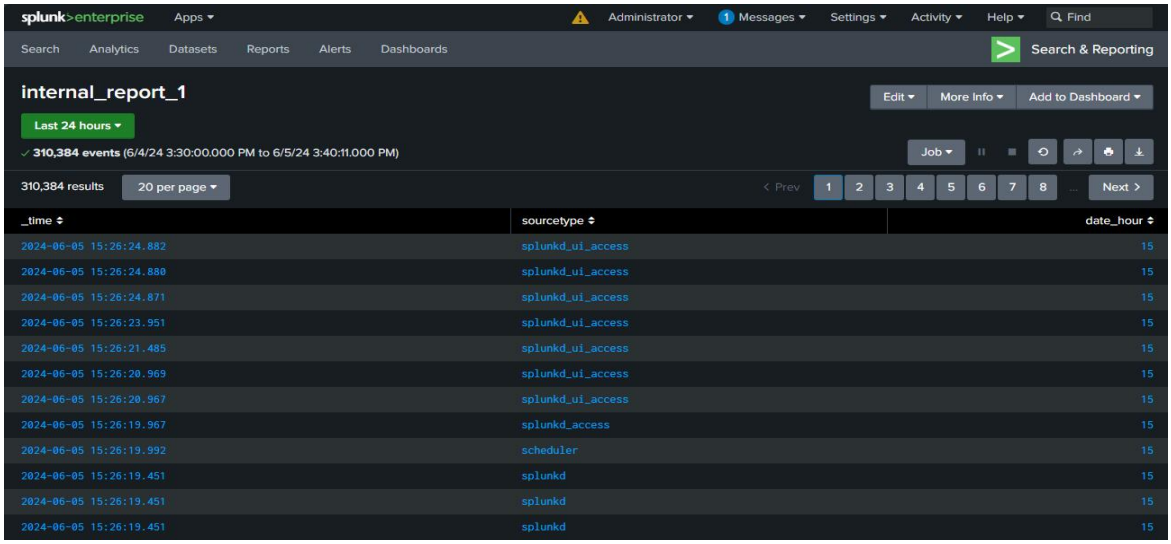

Fig15. Reports

Fig16. Reports

All reports can be seen in the reports section. We can edit , give permissions and delete our report from here. We can schedule report so as to obtain it weekly ,daily monthly as so on.

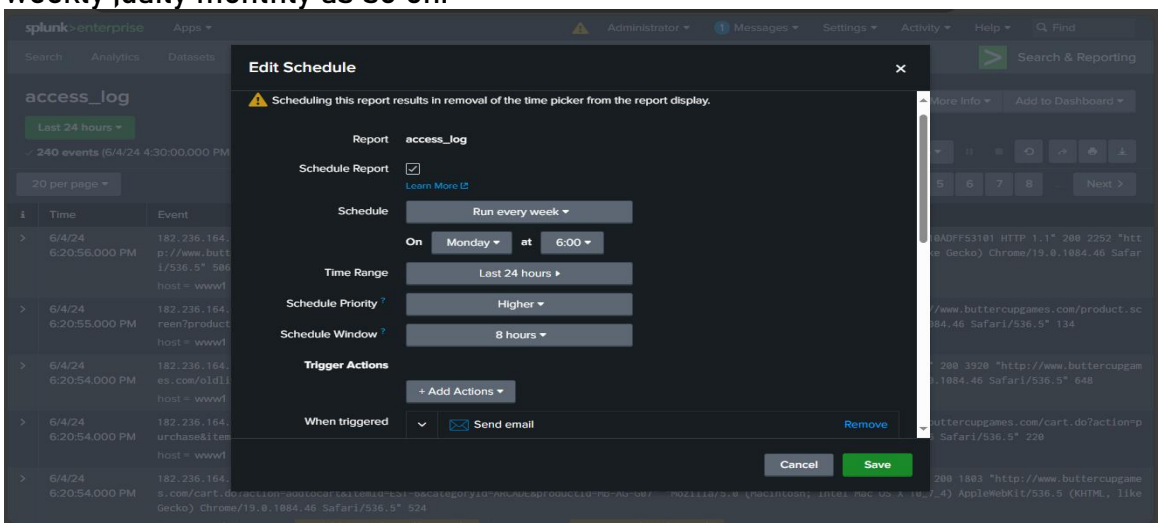

Fig. Reports schedule

Dashboard :

The dashboard feature in Splunk offers users a comprehensive and interactive platform to visualize and monitor key metrics and trends within their data. Users can create customized dashboards with various visualizations such as charts, graphs, maps, and tables to present data in a visually appealing and intuitive format. Dashboards can be tailored to specific use cases, allowing users to focus on relevant information and insights. With real-time data updates and the ability to drill down into specific details, Splunk dashboards empower users to quickly identify patterns, anomalies, and opportunities for optimization. Whether used for operational monitoring, security analysis, or business intelligence, Splunk dashboards provide a centralized hub for data-driven decision-making and actionable insights.

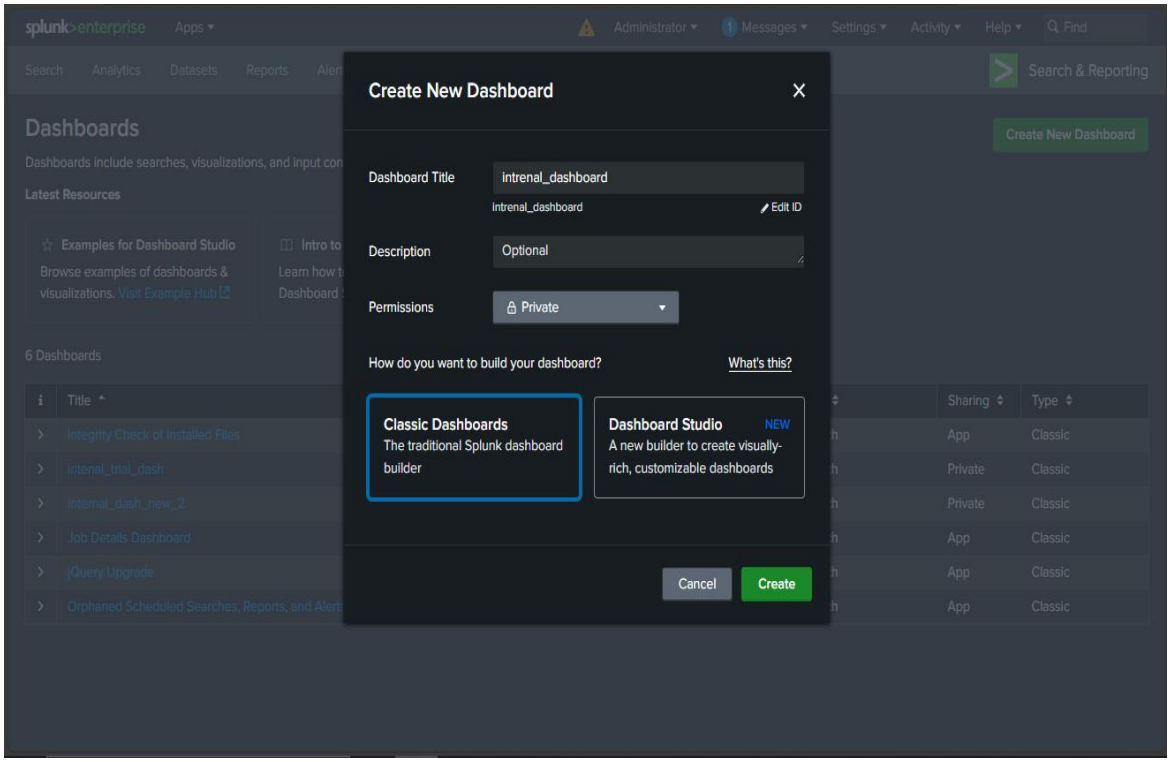

Fig17. Dashboards

We can set title , description , permissions and choose how we want to build your dashboard

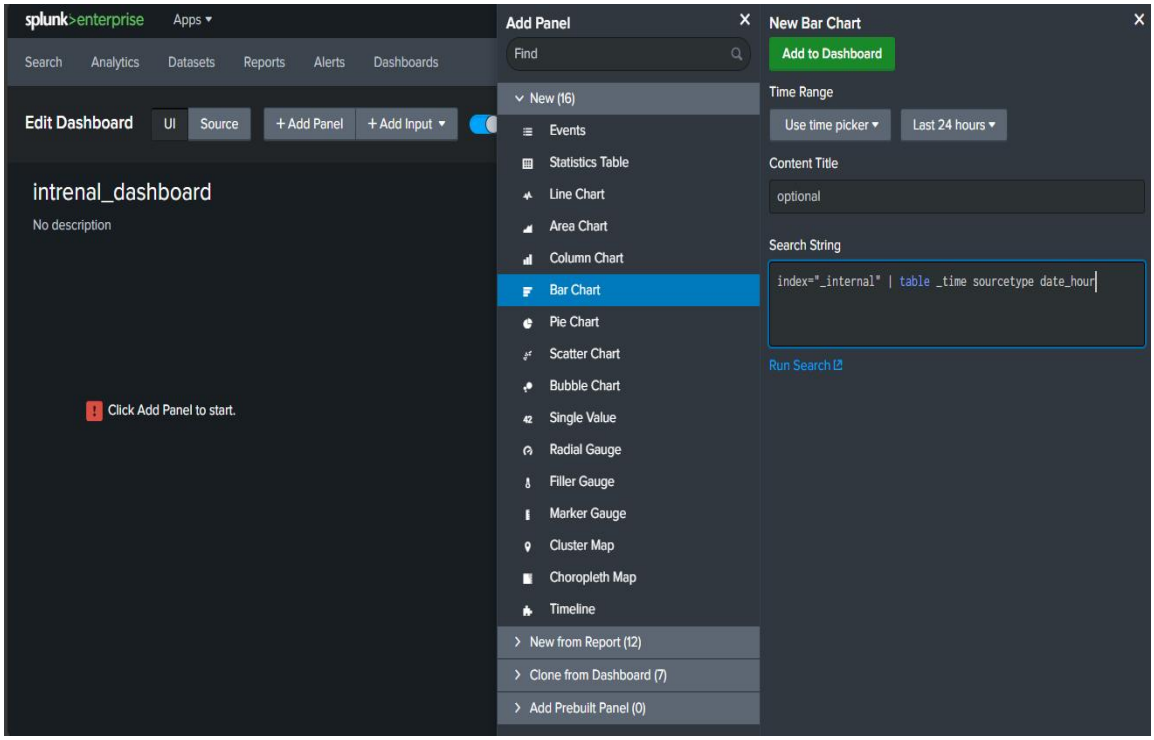

Fig18. Dashboards_panels

We need to add panel in dashboard once it is created. The panels ia panel is a visual component or element within a dashboard that displays specific data or information. Panels are used to present data in a visual format, such as charts, graphs, tables, maps, or single value visualizations, allowing users to quickly interpret and analyze the data.

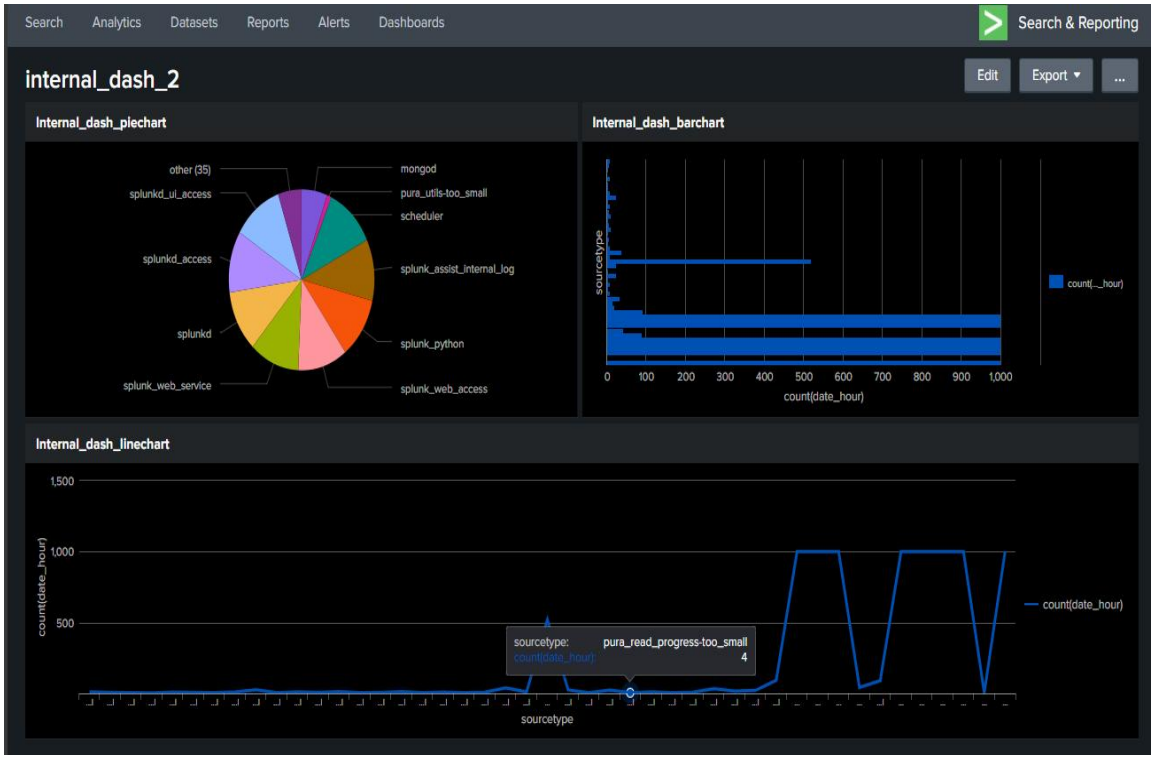

Fig19. Dashboards_visualisation

Here we have added 3 panels and visualized them.

Lookup

A lookup is a feature in which we take data from 2 different datasets to represent desired data output.The lookup feature in Splunk allows users to enrich and augment their data by integrating external reference datasets into their analysis. With lookups, users can enhance the context and relevance of their data by cross-referencing it with supplementary information from external sources such as CSV files, databases, or custom tables. This capability enables users to correlate and analyze data more comprehensively, leading to deeper insights and more informed decision-making. Lookups in Splunk can be used for various purposes, including adding geographical information to IP addresses, enriching user activity logs with additional attributes, or performing entity resolution across different data sets. By leveraging the lookup feature, users can unlock the full potential of their data and gain valuable insights that would otherwise be inaccessible.

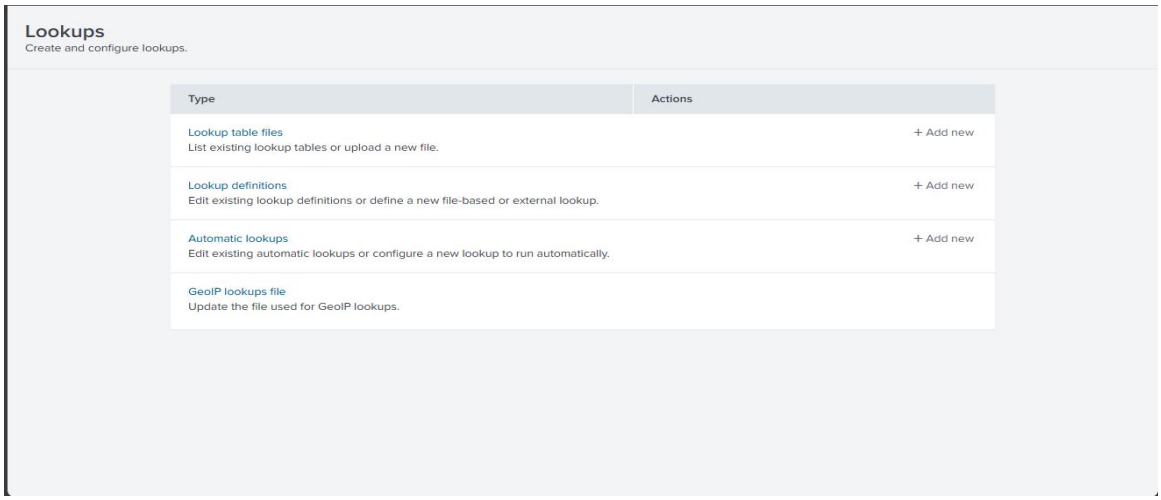

Fig20. Lookups

To create a lookup first we will select lookup table files and then create a lookup by adding external csv data file.

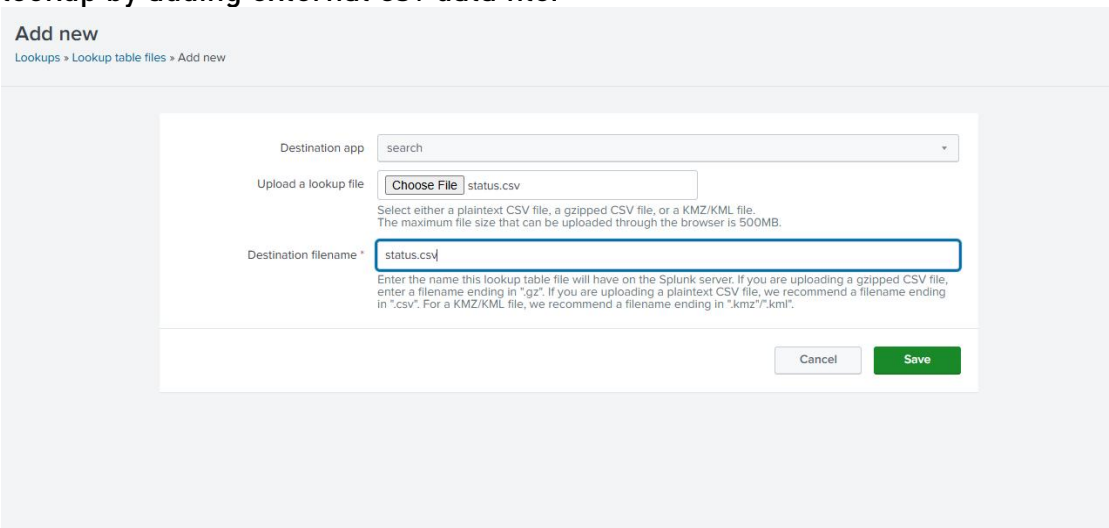

Fig21. new Lookups

Added csv file has few status codes and descriotion separaed by comma.

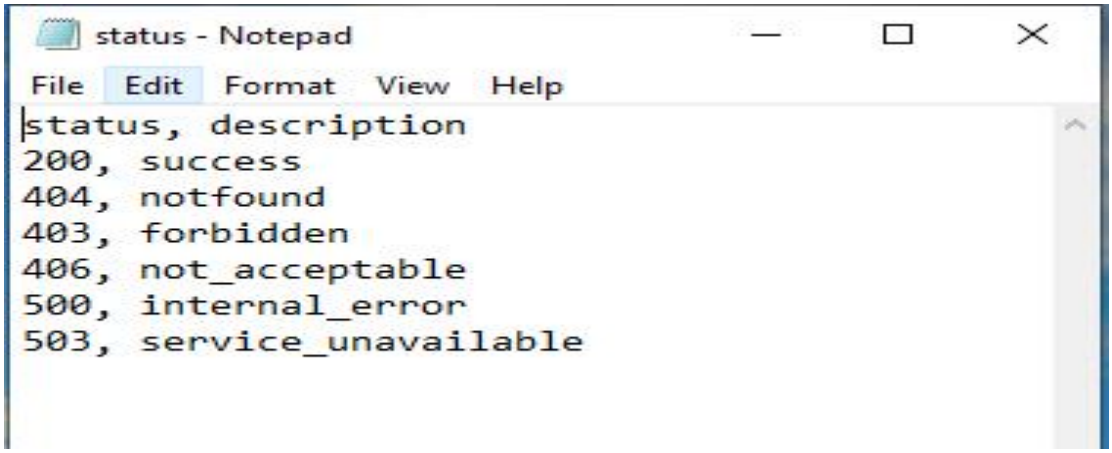

Fig22. csv file

Created lookups can be seen in the lookup table files.

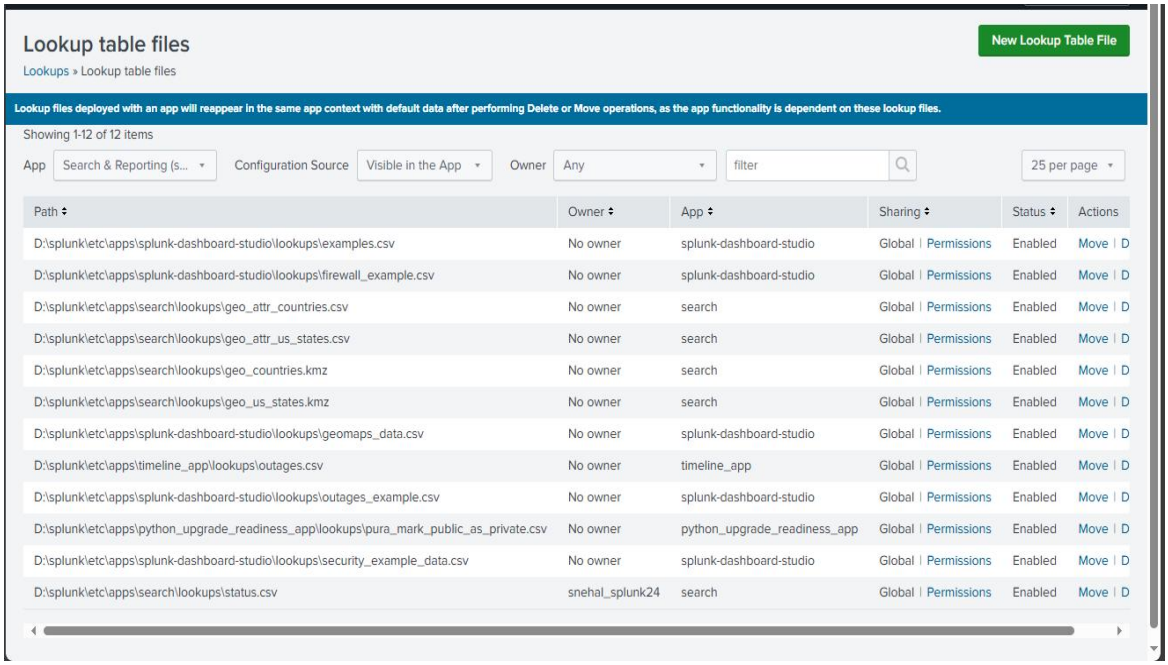

Fig23. table_ file

A lookup command is used to invoke field valu lookups.
Syntax:
Lookup <lookup-table-name><lookup-field1>AS<event-field1>, <lookup-field2>AS<event-field2>OUTPUTNEW<lookup-destfield1>AS<event-destfield>

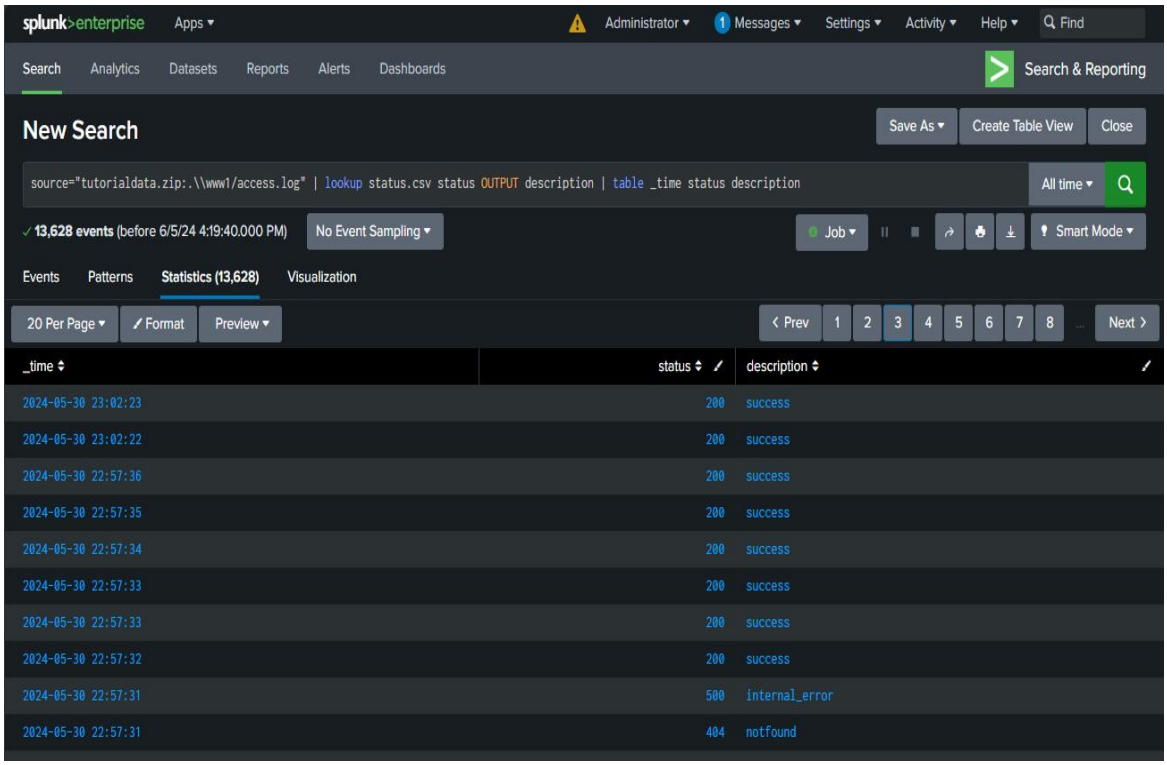

Fig24. lookup command

Lookup definition

A lookup definition provides a lookup name and a path to find the lookup table. Lookup definitions can include extra settings such as matching rules, or restrictions on the fields that the lookup is allowed to match. One lookup table can have multiple lookup definitions.

All lookup types require a lookup definition. After you create a lookup definition you can invoke the lookup in a search with the `lookup` command.

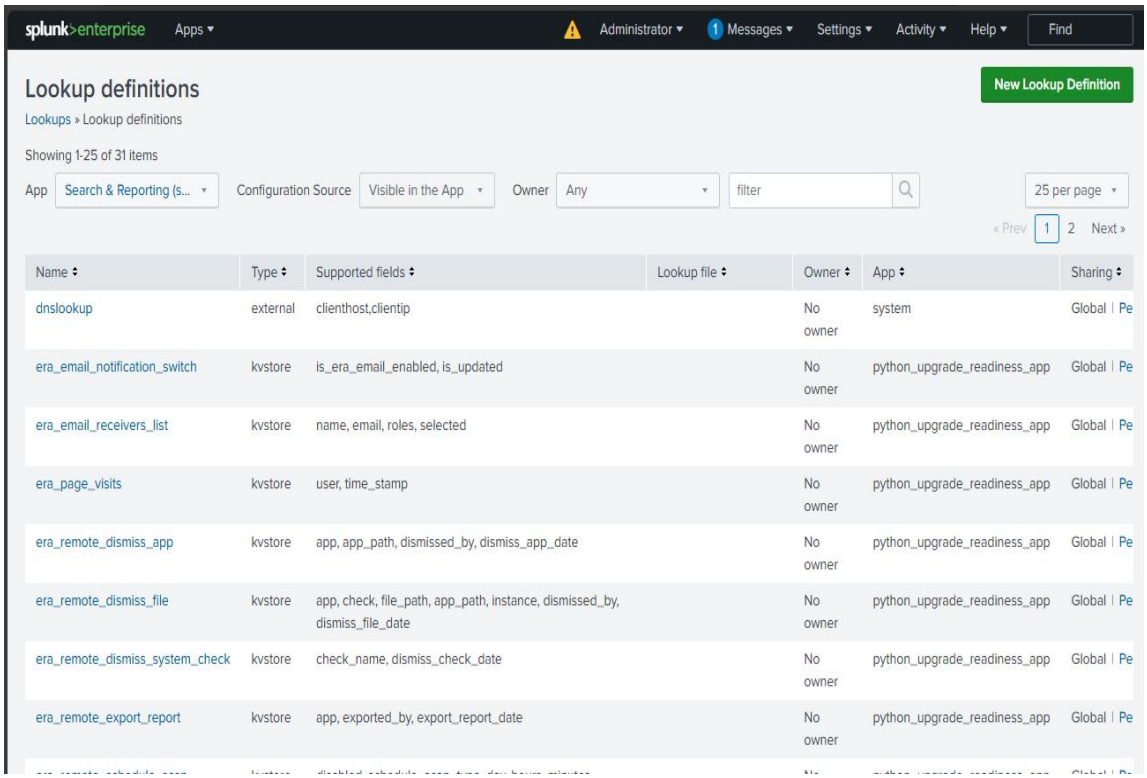

Fig25. lookup definition

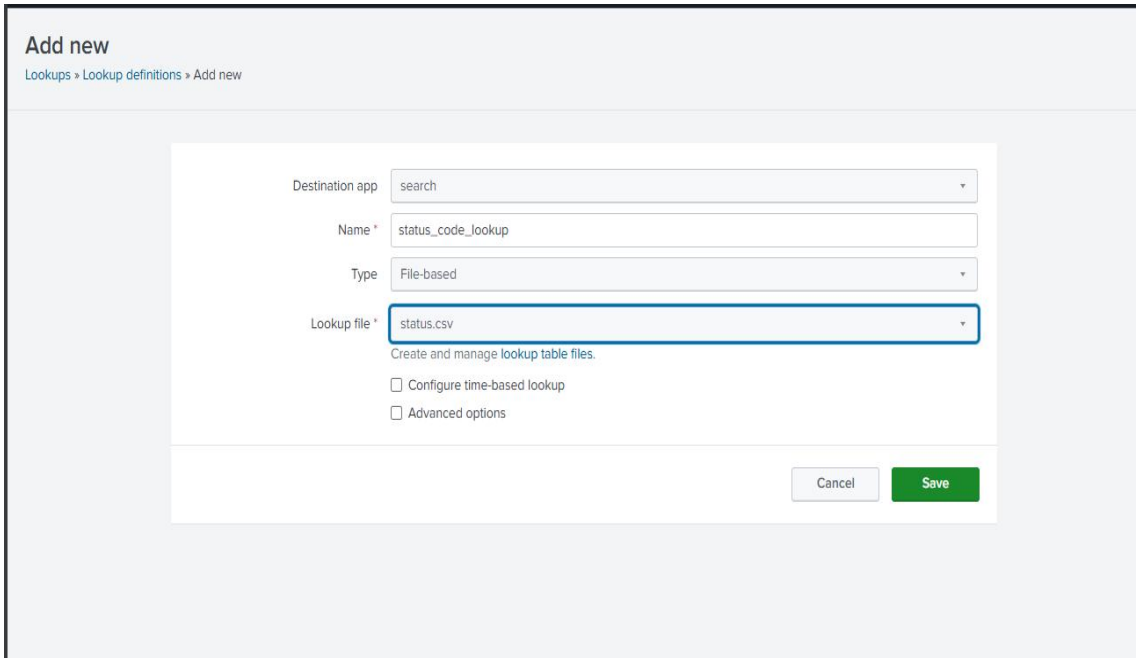

Fig26. lookup definition

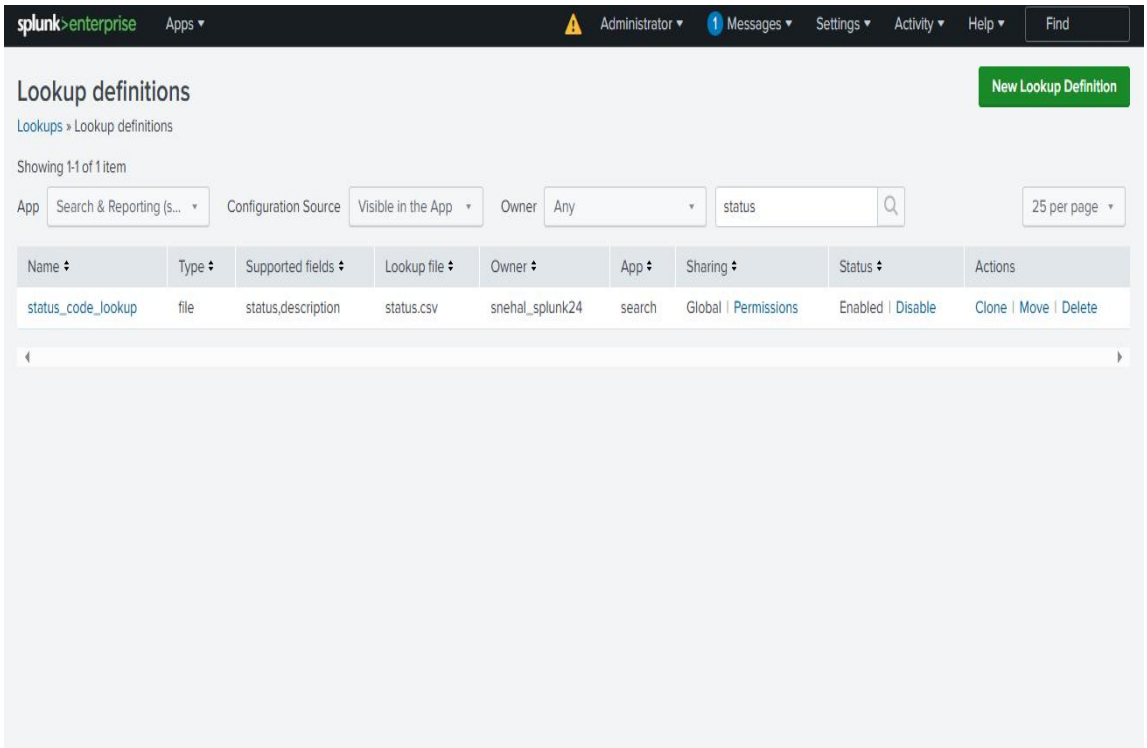

Fig27. lookup definition

Automatic lookup

Use automatic lookups to apply a lookup to all searches at search time. After you define an automatic lookup for a lookup definition, you do not need to manually invoke it in searches with the `lookup` command.

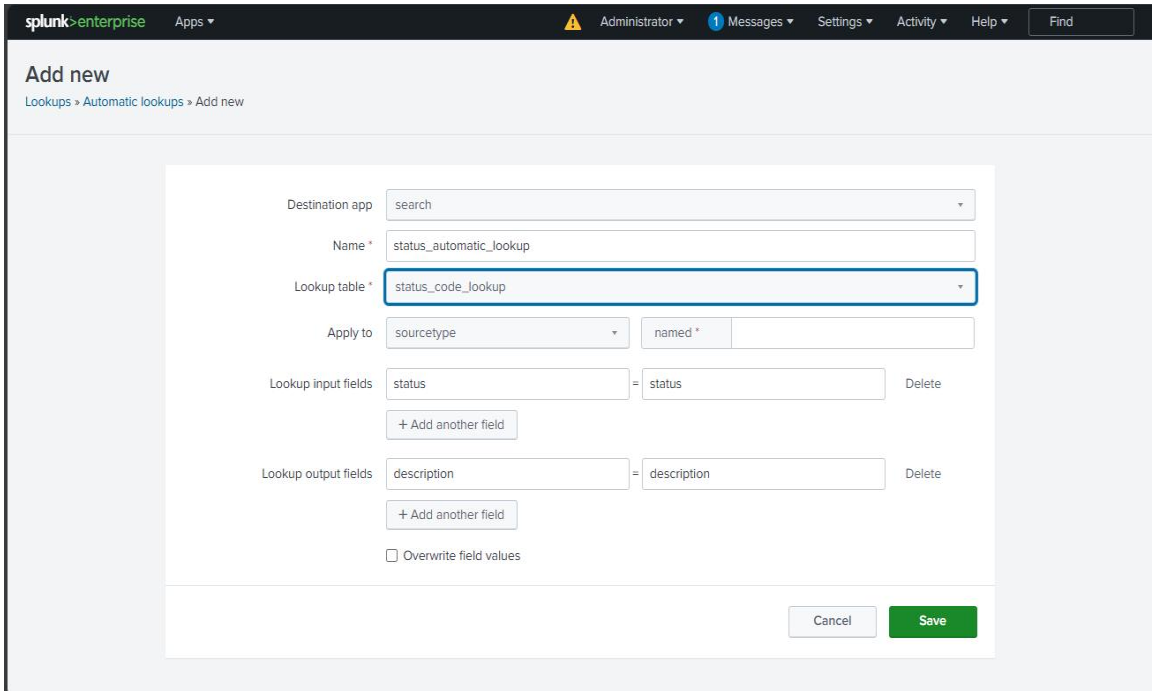

Fig28. Automatic lookup1

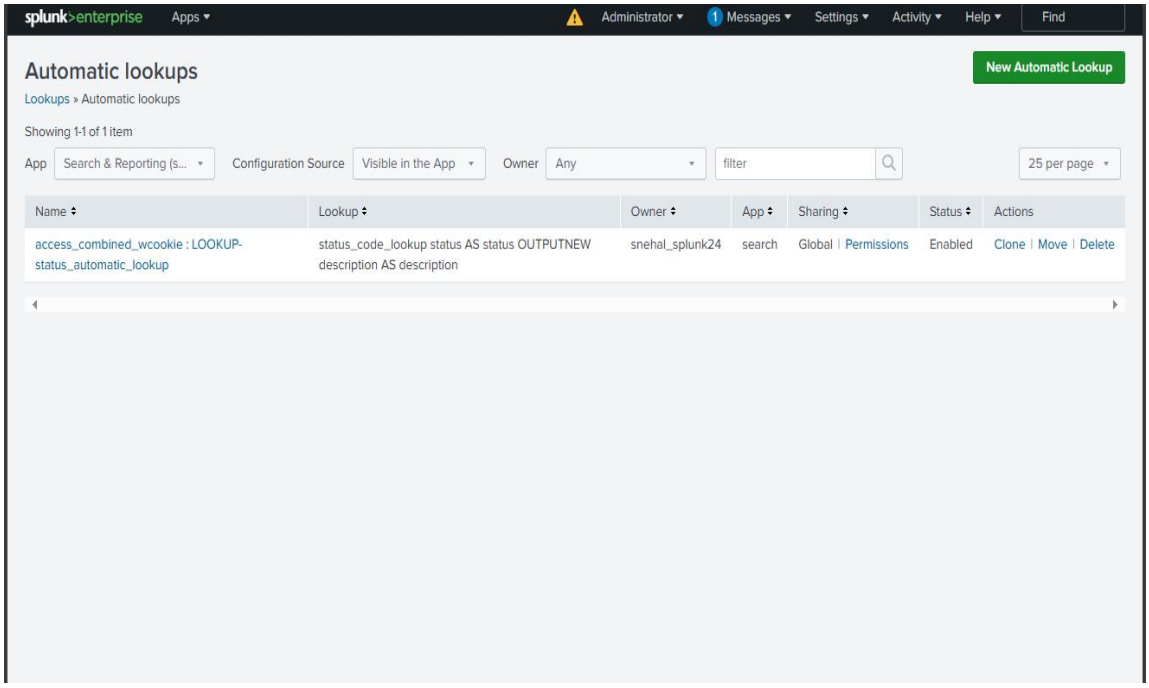

Fig29. Automatic lookup2

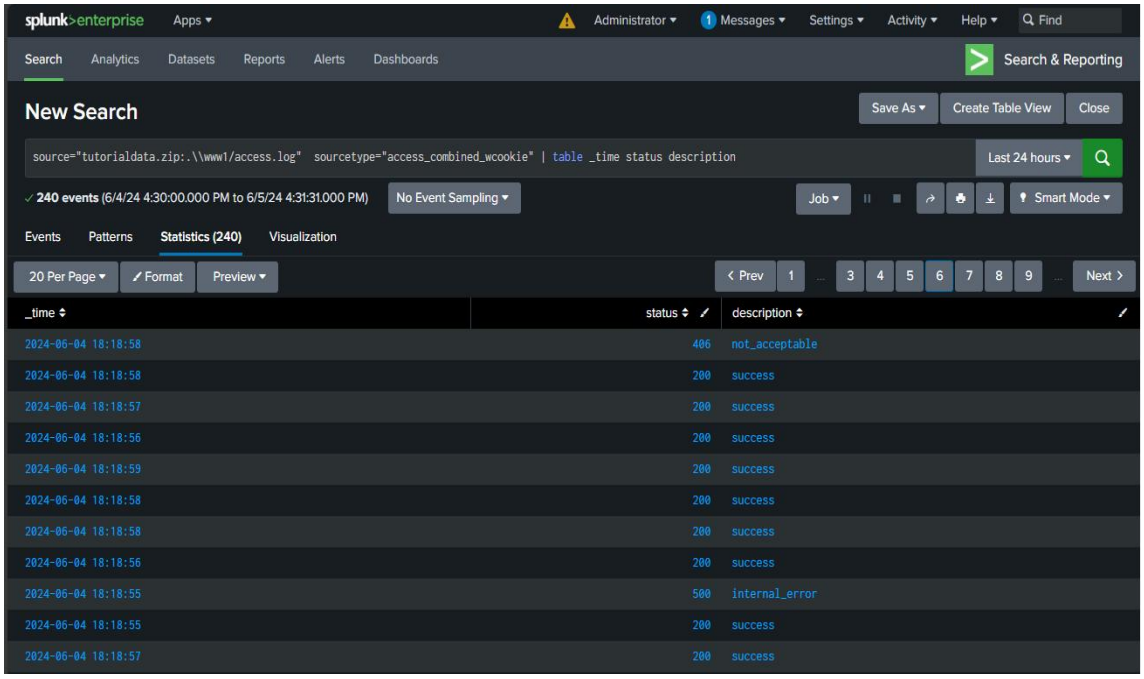

Fig30. Automatic lookup3

Here , no lookup command was used ,but still the data from external file was used to display status and description.

To create an alert:

We can save our search as alert to create an alert.The alert feature in Splunk empowers users to proactively monitor their data for specific conditions or events and receive notifications when these conditions are met. Users can create alerts based on predefined criteria, such as threshold values, patterns, or anomalies detected in their data. When an alert condition is triggered, Splunk can automatically send notifications via email, SMS, or other channels, alerting users and stakeholders to potential issues or opportunities in real-time. Alerts can be customized with various parameters, including severity levels, suppression conditions, and escalation actions, ensuring that users receive timely and relevant notifications tailored to their specific needs. By leveraging the alert feature in Splunk, users can stay informed, respond quickly to critical events, and take proactive measures to address emerging challenges or capitalize on opportunities in their data. We can write our query in search bar and save it as alert.

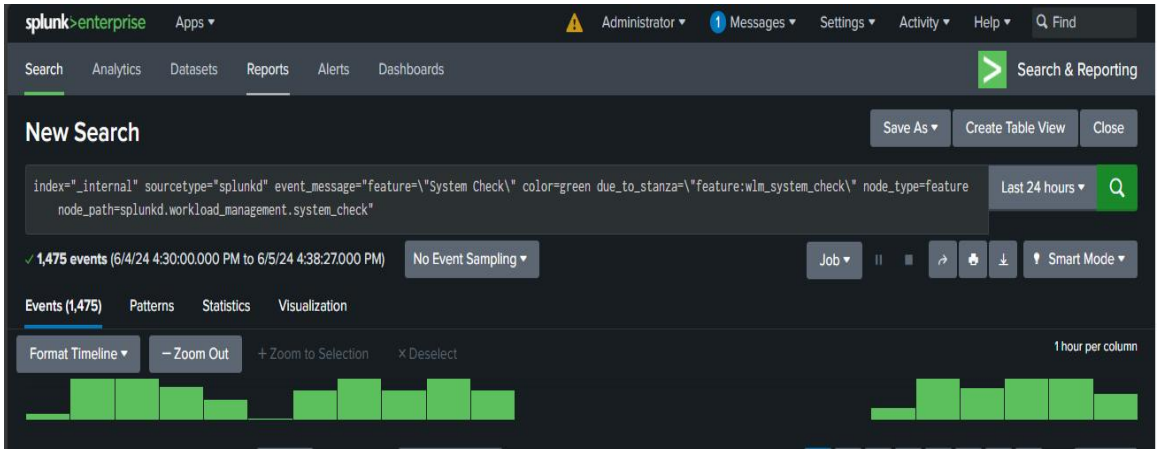

Fig31. Alert_definition

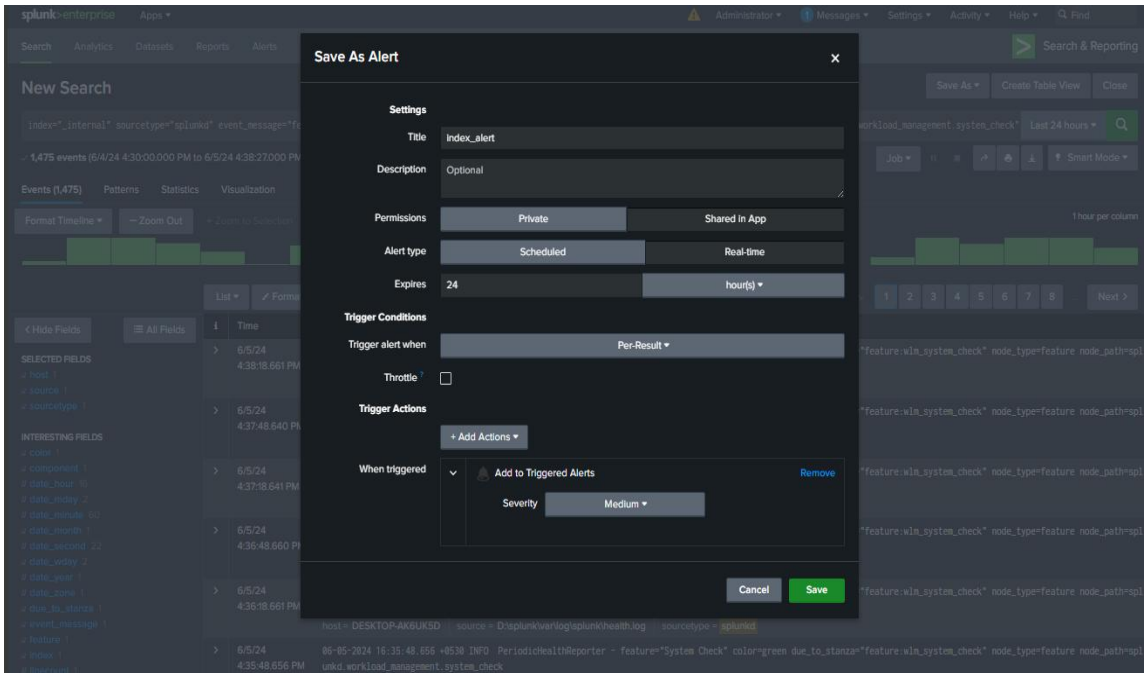

Fig32. Alert_definition

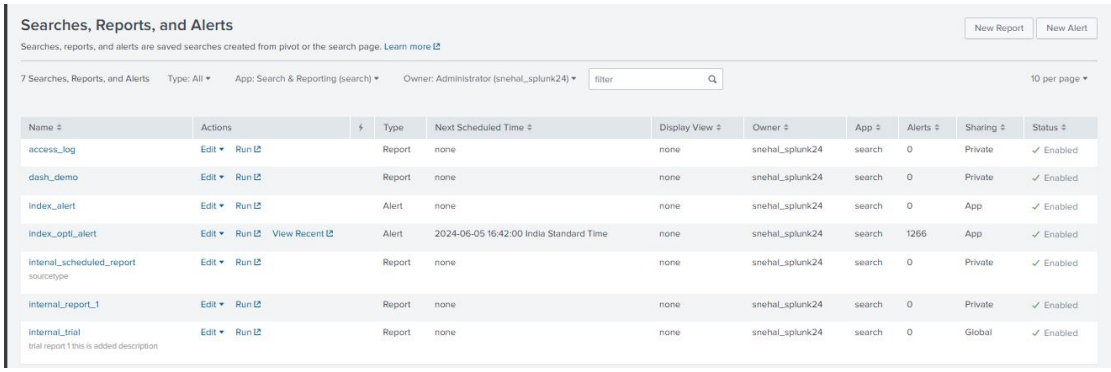

Fig33. Alert

Indexes:
Indexes in Splunk serve as repositories for storing and organizing data ingested into the platform. They provide a structured and efficient way to store and retrieve data, enabling users to quickly search, analyze, and visualize large volumes of machine-generated data. Splunk indexes can be configured to accommodate diverse data types and sources, including logs, metrics, and event data. Users can define index settings such as retention periods, access controls, and data segmentation to optimize storage and performance according to their specific requirements. Indexes play a critical role in enabling fast and reliable data retrieval, supporting various use cases such as security monitoring, IT operations, and business analytics. By effectively managing indexes, users can efficiently leverage the full capabilities of Splunk to derive actionable insights and drive informed decision-making from their data.

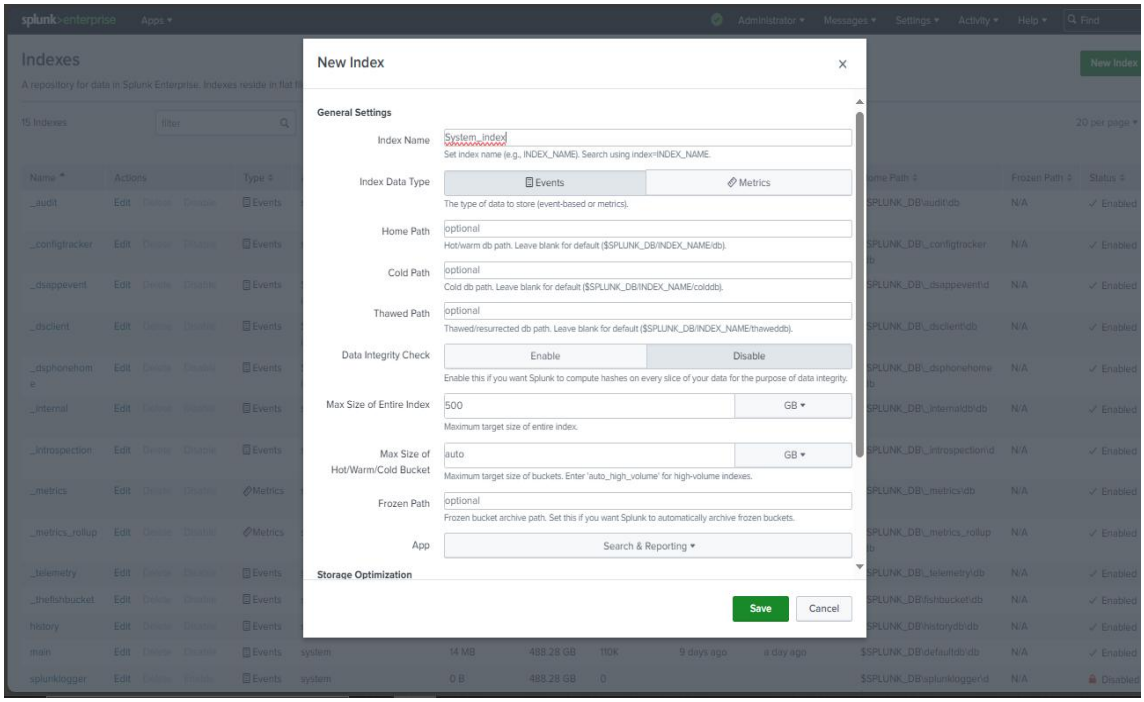

Fig34. Create Indexes

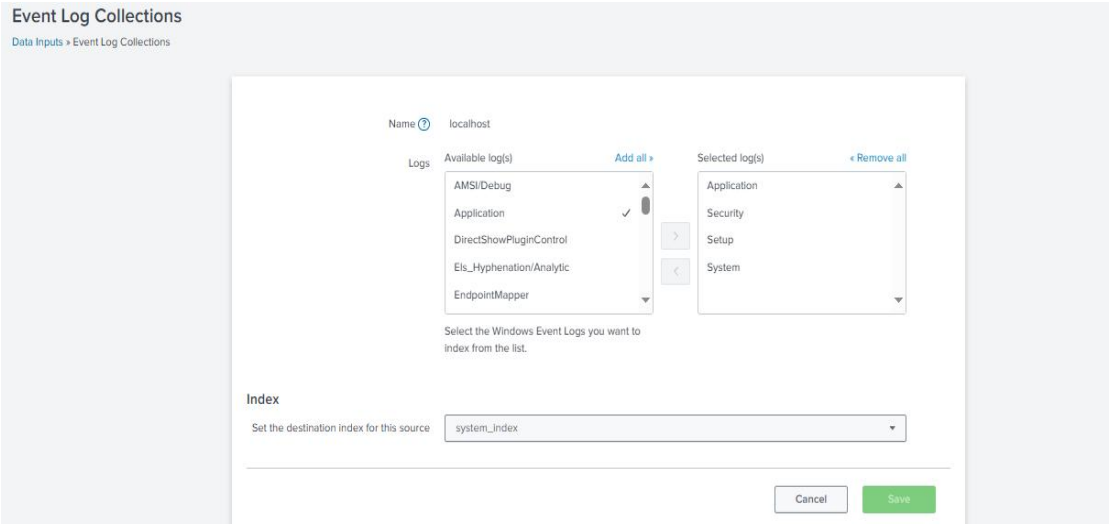

Fig35. event_log_collection

The log collection feature in Splunk enables users to gather, aggregate, and index log data from diverse sources across their IT infrastructure. Splunk provides a versatile platform for collecting logs from applications, servers, network devices, and other systems, allowing users to centralize their log data in one location for easy access and analysis. With support for various log formats and protocols, including syslog, Windows Event Logs, and APIs, Splunk offers flexibility in capturing log data from virtually any source. Users can configure log collection settings to specify which logs to collect, how frequently to collect them, and where to store them within Splunk indexes. By leveraging Splunk's log collection capabilities, organizations can gain comprehensive visibility into their IT environment, streamline troubleshooting and monitoring processes, and extract valuable insights from their log data to support business objectives and security initiatives.

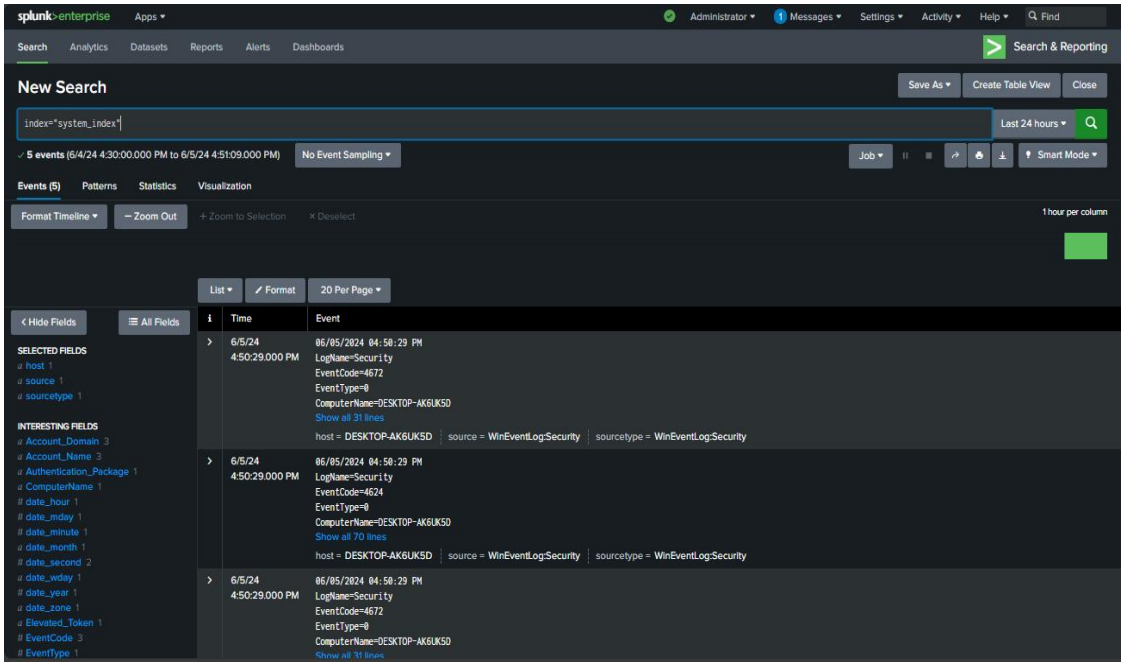

Fig35. windows_log

Conclusion

In conclusion, the project "A Comprehensive Demonstration of Splunk SIEM" has provided an extensive exploration of Splunk's diverse functionalities, including event management, dashboard creation, lookup integration, report generation, and alert configuration. Through this comprehensive demonstration, we have showcased how Splunk serves as a powerful platform for security information and event management, empowering organizations to effectively monitor, analyze, and respond to security threats and operational challenges. By leveraging Splunk's capabilities, users can gain deep insights into their data, visualize key metrics and trends, enrich data analysis with external references, generate actionable reports, and proactively detect and mitigate security incidents through automated alerts. Overall, this project underscores the significance of Splunk as a leading solution for operational intelligence and security management, enabling organizations to enhance their security posture, optimize operational efficiency, and make informed decisions based on data-driven insights.