

CYBLACK SOC ACADEMY

LOG ANALYSIS (SPLUNK)

Submitted by TEAM 1 (ALPHA TECH)

PRINCE ORUMA

ONYEKA VANESSA

DEBBIE AYOOLA

IVIE OSOIYE

KEHINDE OJUKO

MODUPE OJUGBELE

NDABEZINHLE REGAL SIBANDA

VERONICA OJUKWU

1.0 EXECUTIVE

SUMMARY3

2.0 ADD NEW

USERS.....3

2.1 ANALYSIS4

3.0 DASHBOARD AND ALERT

CREATION.....5

4.0 FIELD

EXTRACTION.....6

1.0 EXECUTIVE SUMMARY

After joining the Security Operations team at a medium-sized Organization (Alpha-Tech). My team has been tasked with analyzing OpenSSH log files to help identify any potential security threats.

The organization has recently experienced a few suspicious incidents, and management is keen on understanding if there are any patterns or anomalies in the SSH login attempts.

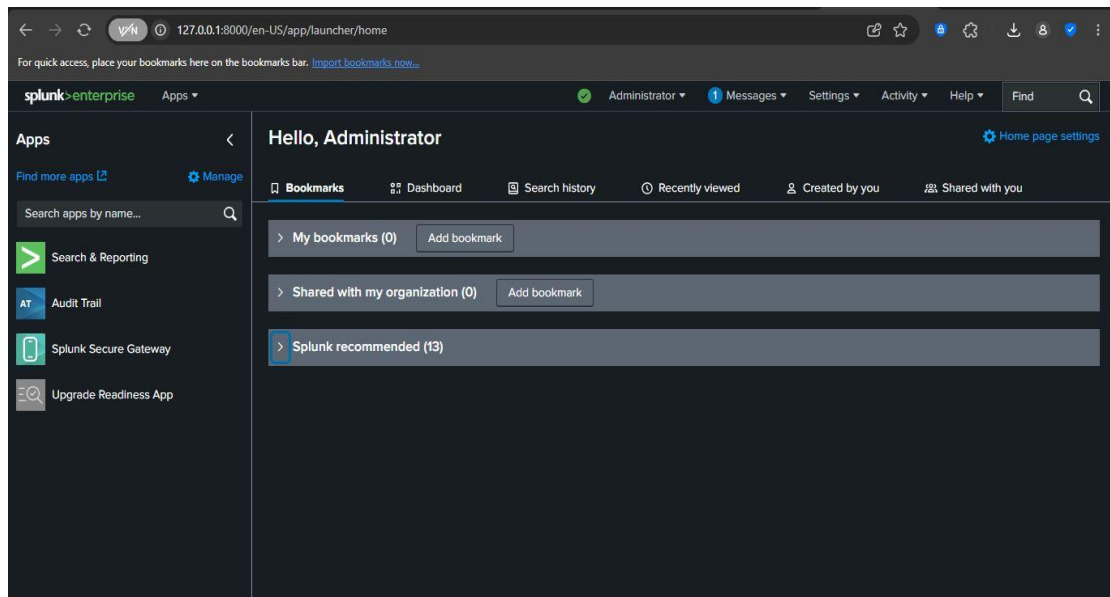
Our goal is to use Splunk Cloud to thoroughly analyze the provided OpenSSH log file, set up a dashboard and an alert in Splunk Cloud to help monitor similar activities in the future. Additionally, we are tasked to manage user accounts in Splunk Cloud as part of the assignment.

2.0 ADD NEW USERS

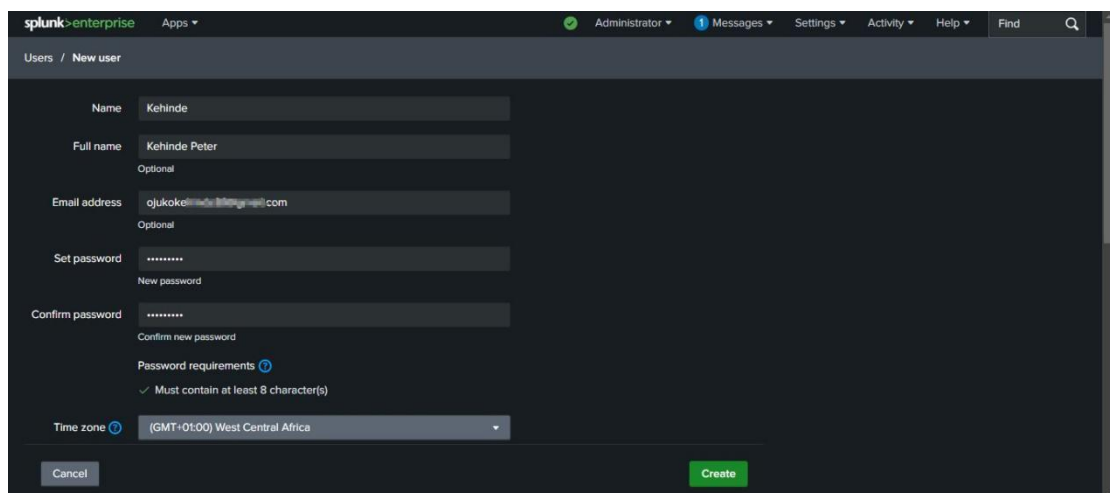
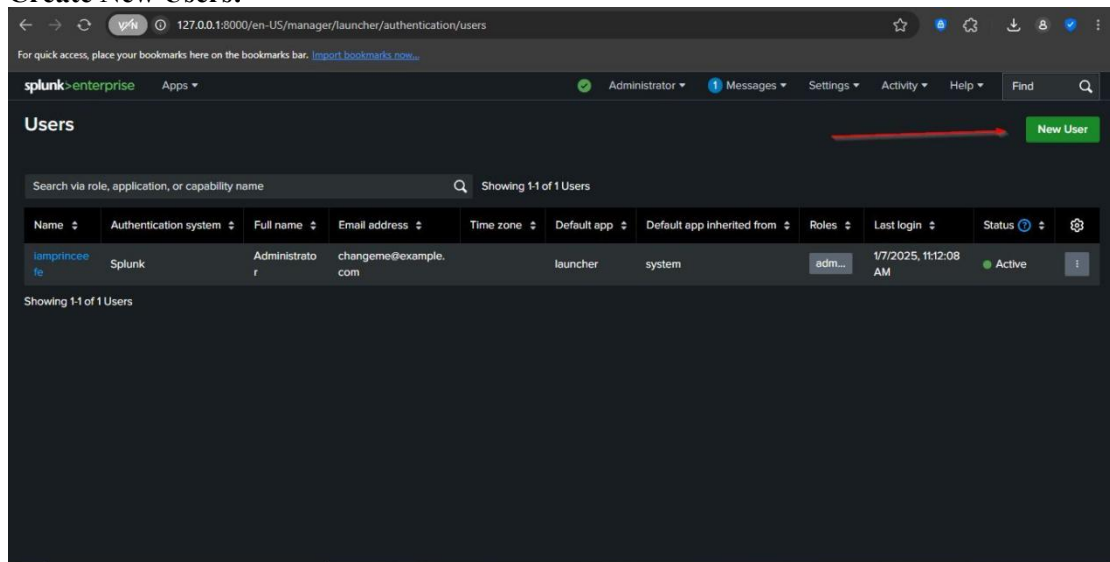
Firstly, we created a list of users and assigned appropriate roles based on the number of individuals in our team/group

We configured the time zone to West Africa Time (WAT), set the default app to “launcher(home)” and configured each user to change their password based on their first login.

Dashboard:



Create New Users:



Password requirements ⓘ
 ✓ Must contain at least 8 character(s)

Time zone ⓘ (GMT+01:00) West Central Africa

Default app ⓘ launcher (Home)

Assign roles ⓘ

Available item(s)
 1/6 Selected

- ☐ admin
- ☐ can_delete
- ☐ power
- ☒ splunk-system-role
- ☐ user
- ☐ user-kehinde

Selected item(s)
 0/0 Selected

☐ can_delete
☐ power
☒ splunk-system-role
☐ user
☐ user-kehinde

Create a role for this user. ☒

Require password change on next login ☒

Cancel Create

All Users Created:

Search via role, application, or capability name 🔍 Showing 1-8 of 8 Users									
Name ⬇	Authentication system ⬇	Full name ⬇	Email address ⬇	Time zone ⬇	Default app ⬇	Default app inherited from ⬇	Roles ⬇	Last login ⬇	Status ⓘ ⬇ ⚙
deborah	Splunk	Deborah Ayoola	ayooladeborahadeola@gmail.com	Africa/Algiers	launcher	system	can_delete		● Active ⓘ
lamprincefe	Splunk	Prince Oruma	princeorumaofficial@gmail.com	Africa/Algiers	launcher	system	admin	1/7/2025, 11:12:08 AM	● Active ⓘ
ivie	Splunk	Ivie Osoye	osoyeivie@gmail.com	Africa/Algiers	launcher	system	power		● Active ⓘ
kehinde	Splunk	Kehinde Peter	ojukokehinde38@gmail.com	Africa/Algiers	launcher	system	splunk-system-ro...		● Active ⓘ
modupe	Splunk	Modupe Ojugbele	holuwaseun588@gmail.com	Africa/Algiers	launcher	system	splunk-system-ro...		● Active ⓘ
regal	Splunk	Ndabezihle Regal Sibanda	sibandandabezihleregal@gmail.com	Africa/Algiers	launcher	system	power		● Active ⓘ
vanessa	Splunk	Vanessa Onyeka	onyekavanessa33@gmail.com	Africa/Algiers	launcher	system	admin		● Active ⓘ
veronica	Splunk	Veronica Ojukwu	veronpearla07@gmail.com	Africa/Algiers	launcher	system	can_delete		● Active ⓘ

2.1 ANALYSIS:

Next, we uploaded the provided OpenSSH log file into splunk cloud and conducted a detailed analysis of the log file by searching for anomalies like unusual IP's, and multiple failed login attempts.

The image shows two screenshots of the Splunk Enterprise interface. The top screenshot displays the 'Add Data' workflow, specifically the 'Review' step. It shows the following configuration:

- Input Type: Uploaded File
- File Name: OpenSSHnew_logs - OpenSSHnew_logs.csv
- Source Type: SSH Logs
- Host: DESKTOP-P95EP3H
- Index: Default

The bottom screenshot shows the 'New Search' results for the query: `source="OpenSSHnew_logs - OpenSSHnew_logs.csv" host="DESKTOP-P95EP3H" sourcetype="SSH Logs"`. The results show 2,001 events. The 'Events (2,001)' tab is selected, and the 'Timeline format' is chosen. The table below shows the first few events:

Time	Event
1/7/25 12:30:06.000 PM	Timestamp, Host, Process, PID, Message host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv sourcetype = SSH Logs
12/10/24 11:04:00.000 AM	12/10/2024 11:04:LabSZ,sshd,[25539]:,Failed password for invalid user user from 103.99.0.122 port 52683 ssh2 host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv sourcetype = SSH Logs
12/10/24 11:04:00.000 AM	12/10/2024 11:04:LabSZ,sshd,[25544]:,pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost= 183.62.140.253 user=root host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv sourcetype = SSH Logs
12/10/24 11:04:00.000 AM	12/10/2024 11:04:LabSZ,sshd,[25541]:,Received disconnect from 183.62.140.253: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv sourcetype = SSH Logs
12/10/24 11:04:00.000 AM	12/10/2024 11:04:LabSZ,sshd,[25541]:,Failed password for root from 183.62.140.253 port 36300 ssh2 host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv sourcetype = SSH Logs
12/10/24 11:04:00.000 AM	12/10/2024 11:04:LabSZ,sshd,[25539]:,pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost= 103.99.0.122 host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv sourcetype = SSH Logs
12/10/24 11:04:00.000 AM	12/10/2024 11:04:LabSZ,sshd,[25539]:,pam_unix(sshd:auth): check pass; user unknown host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv sourcetype = SSH Logs
12/10/24 11:04:00.000 AM	12/10/2024 11:04:LabSZ,sshd,[25539]:,input_userauth_request: invalid user user [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv sourcetype = SSH Logs
12/10/24 11:04:00.000 AM	12/10/2024 11:04:LabSZ,sshd,[25539]:,Invalid user user from 103.99.0.122

After analyzing the log file, we discovered the log contains multiple failed logins and authentication failures to a remote system.

The attacker was trying to connect with a root privilege over an SSH session and most of the SSH request and Authentication came from an IP that was consistent:

Failed login request from: 103.99.0.122

Authentication request from: 183.62.140.253

The attacker also tried to login using a username “user” that wasn’t recognized by the system.

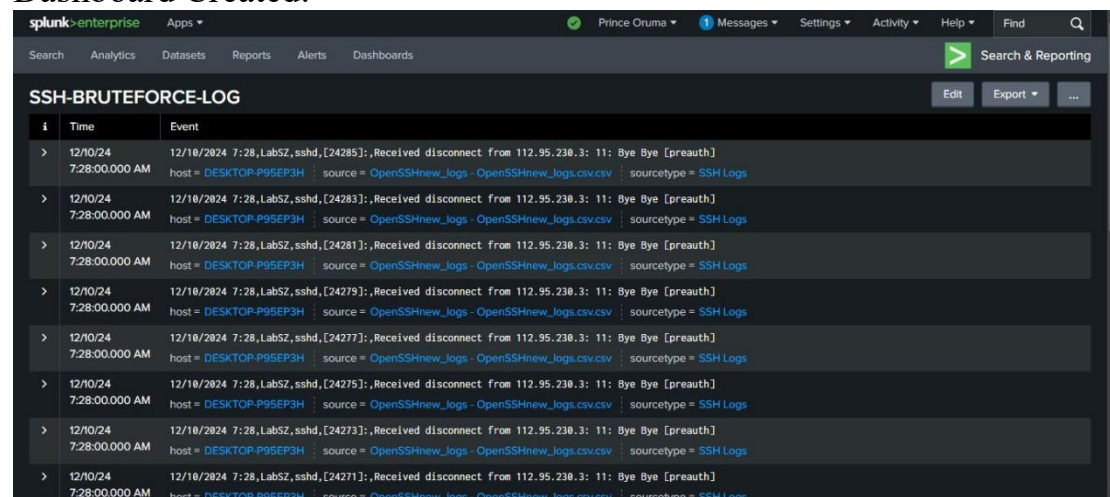
The timestamp of the log also signified a brute-force attack that was done with an automated tool

In conclusion, after thorough analysis on the log file we came to a conclusion that the log was originated from an attempted brute-force attack on a remote system through an SSH session.

3.0 DASHBOARD AND ALERT CREATION:

Next we created a dashboard using the search query ‘*Received disconnect from 112.95.230.3: 11: Bye Bye [preauth]*’ and configured an alert to run daily at 8am, expires at 24 hours, triggers when the number of results is greater than 2 and be received via email in plain text.

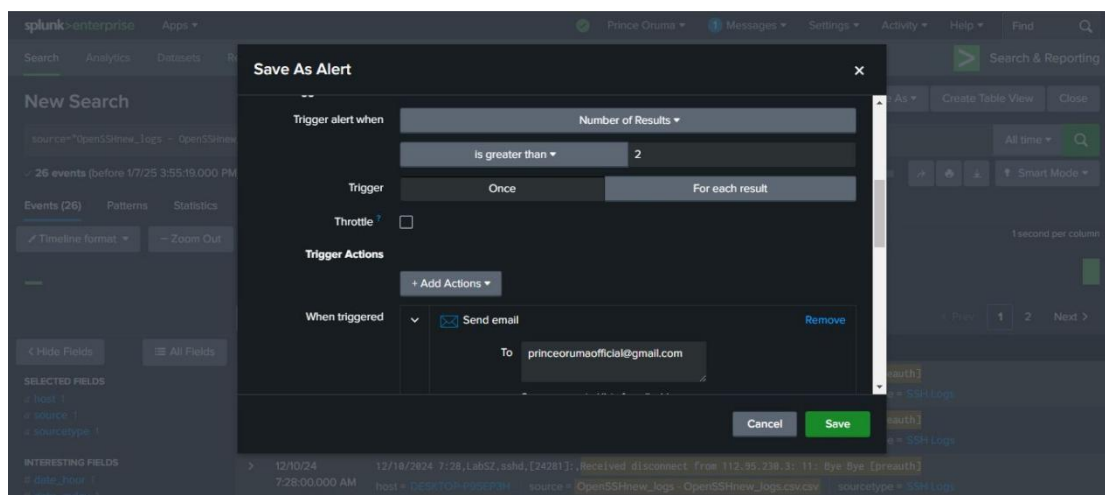
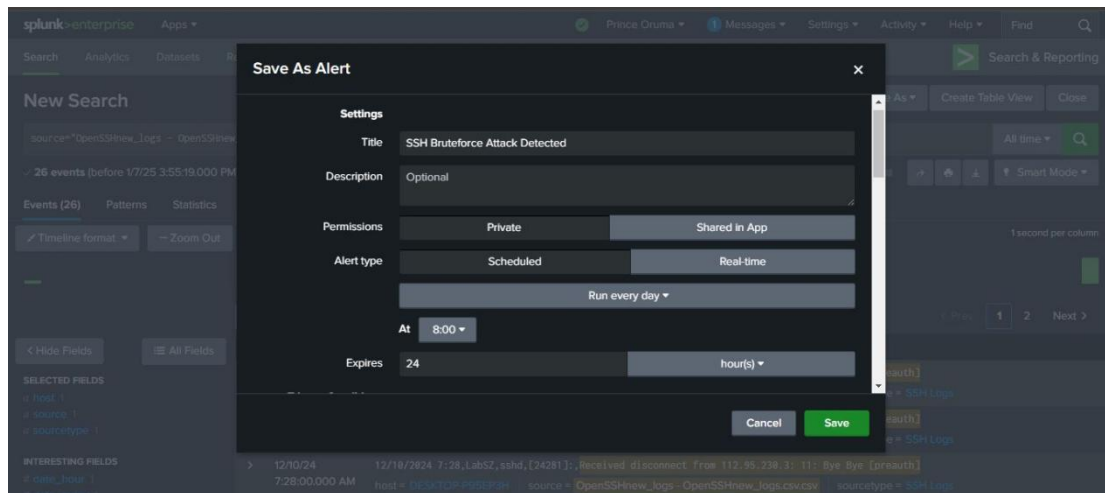
Dashboard Created:



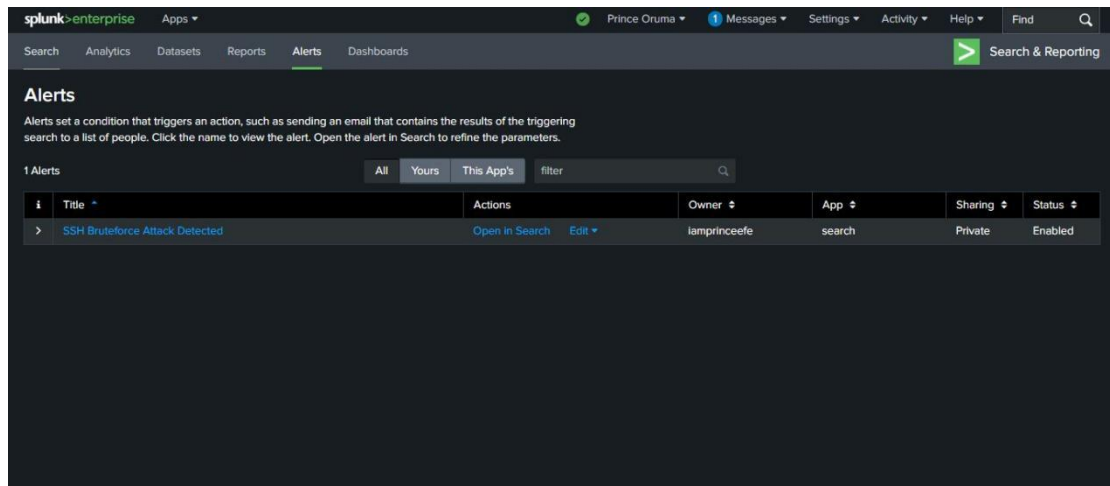
The screenshot shows the Splunk Enterprise interface with a dashboard titled "SSH-BRUTEFORCE-LOG". The dashboard displays a table of search results for the query "Received disconnect from 112.95.230.3: 11: Bye Bye [preauth]". The table has columns for Time, Event, and source. The results show multiple instances of the same event occurring at 7:28:00.000 AM on 12/10/24, all originating from the host DESKTOP-P95EP3H. The source is OpenSSHnew_logs - OpenSSHnew_logs.csv.csv, and the sourcetype is SSH Logs.

i	Time	Event
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,sshd,[24285];,Received disconnect from 112.95.230.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv.csv sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,sshd,[24283];,Received disconnect from 112.95.230.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv.csv sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,sshd,[24281];,Received disconnect from 112.95.230.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv.csv sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,sshd,[24279];,Received disconnect from 112.95.230.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv.csv sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,sshd,[24277];,Received disconnect from 112.95.230.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv.csv sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,sshd,[24275];,Received disconnect from 112.95.230.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv.csv sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,sshd,[24273];,Received disconnect from 112.95.230.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv.csv sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,sshd,[24271];,Received disconnect from 112.95.230.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv.csv sourcetype = SSH Logs

Create Alert:

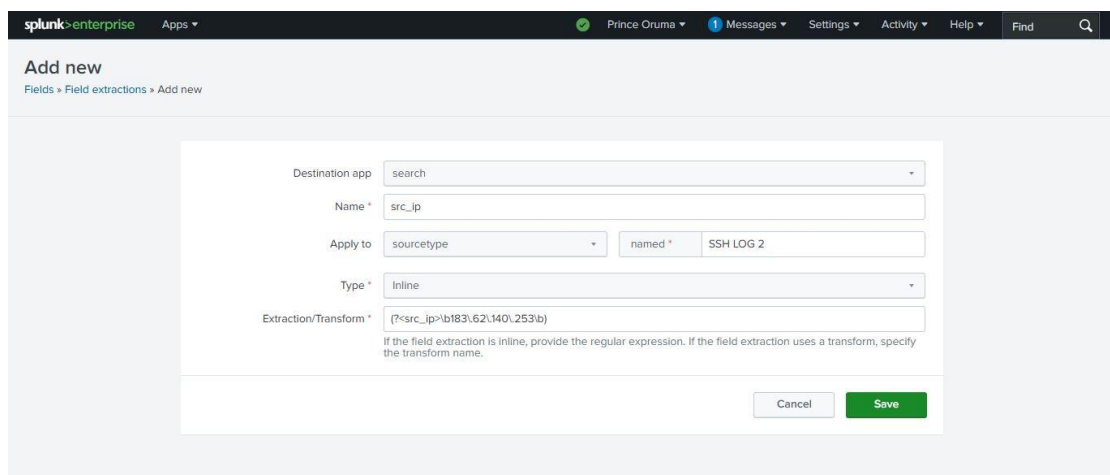
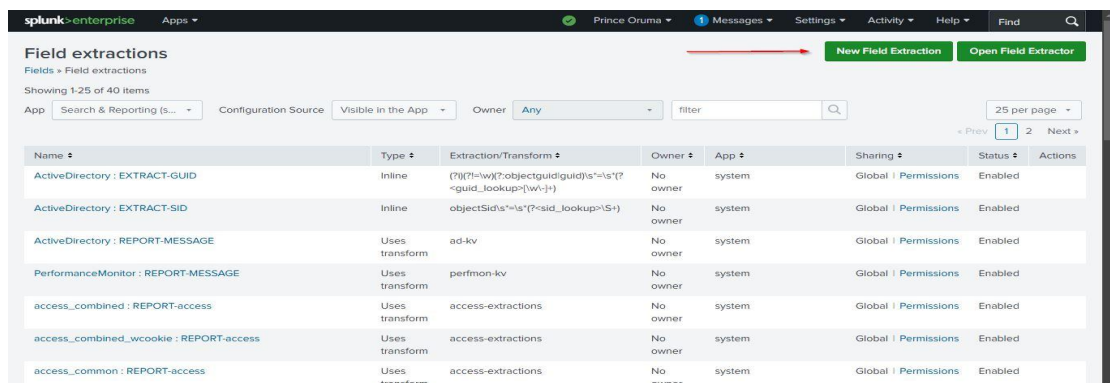


Alert Created:



4.0 FIELD EXTRACTION:

Next we configured a field extraction for the IP address **183.62.140.253** and named it “src_ip”



splunk>enterprise Apps ▾ Prince Oruma ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Apps

Find more apps [\[L\]](#) Manage

 🔍

Hello, Prince Oruma

[🔖 Bookmarks](#)
 [📊 Dashboard](#)
 [🕒 Search history](#)
 [⌚ Recently viewed](#)
 [👤 Created by you](#)
 [👥 Shared with you](#)

[⚙️ Home page settings](#)

Search & Reporting

AT Audit Trail

SG Splunk Secure Gateway

ER Upgrade Readiness App

SSH-BRUTEFORCE-LOG

[Open \[L\]](#)
 [↺ Change](#)
 [🗑 Remove](#)

i	Time	Event
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,ssh,[24285]:Received disconnect from 112.95.238.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv:cvs sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,ssh,[24283]:Received disconnect from 112.95.238.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv:cvs sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,ssh,[24281]:Received disconnect from 112.95.238.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv:cvs sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,ssh,[24279]:Received disconnect from 112.95.238.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv:cvs sourcetype = SSH Logs
>	12/10/24 7:28:00.000 AM	12/10/2024 7:28,LabSZ,ssh,[24277]:Received disconnect from 112.95.238.3: 11: Bye Bye [preauth] host = DESKTOP-P95EP3H source = OpenSSHnew_logs - OpenSSHnew_logs.csv:cvs sourcetype = SSH Logs