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 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.

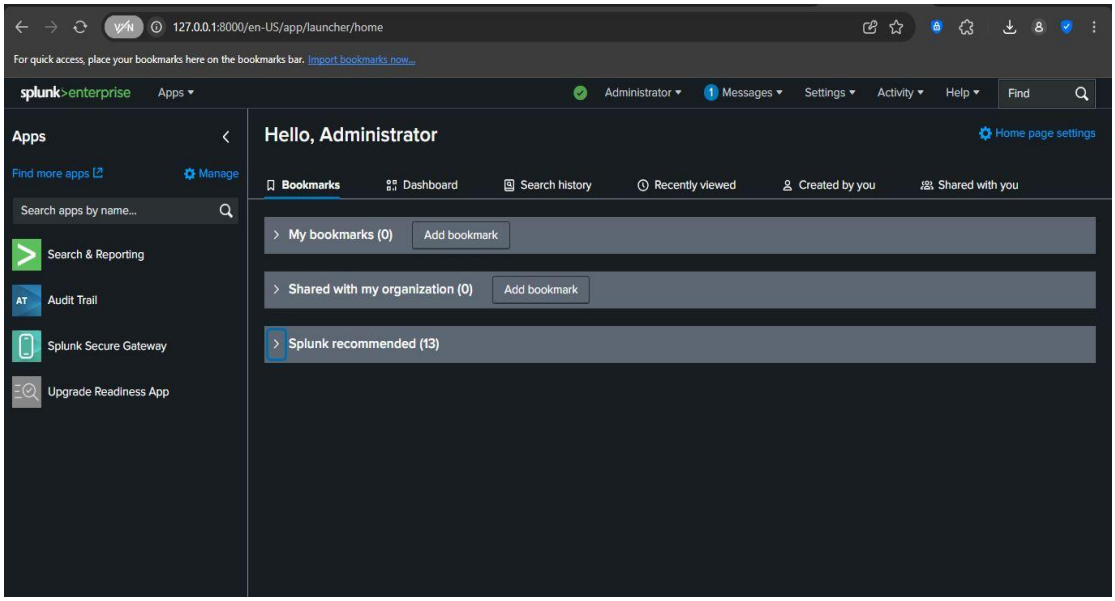
Our goal is to use Splunk Cloud to thoroughly analyze the provided OpenSSH log file, set up a dashboard and an alert in Splunk Cloud to help monitor similar activities in the future. Additionally, we are tasked to manage user accounts in Splunk Cloud as part of the assignment.

2.0 ADD NEW USERS

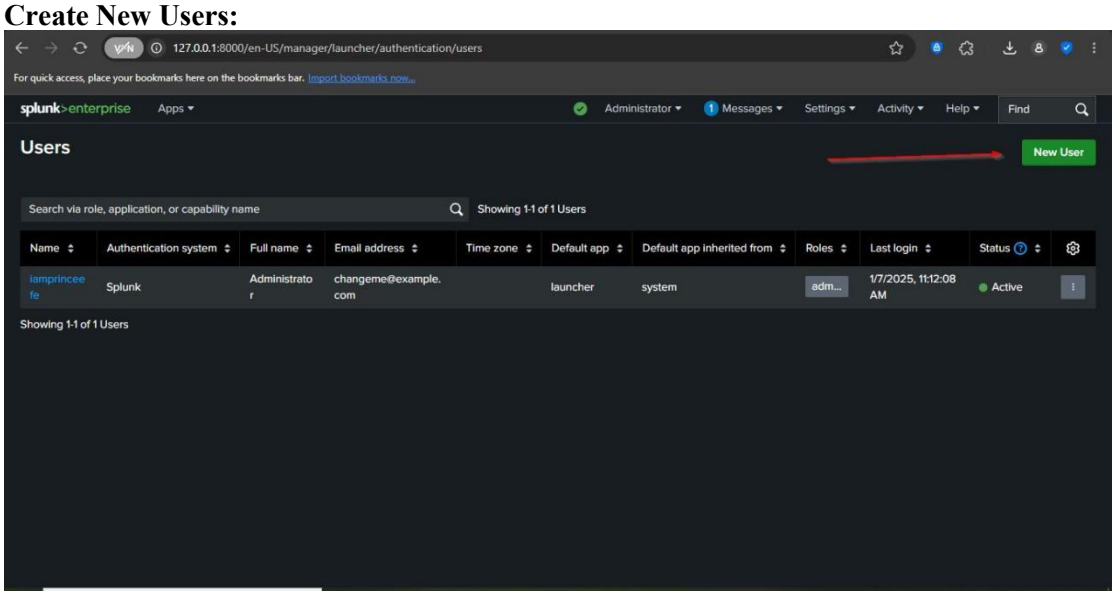
Firstly, we created a list of users and assigned appropriate roles based on the number of individuals in our team/group

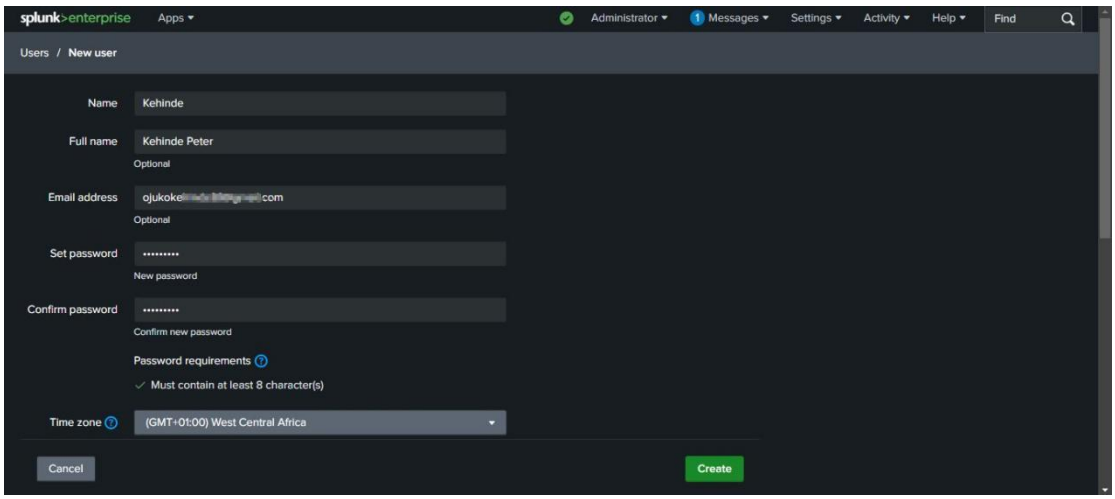
We configured the time zone to West Africa Time (WAT), set the default app to “laucher(home)” and configured each user to change their password based on their first login.

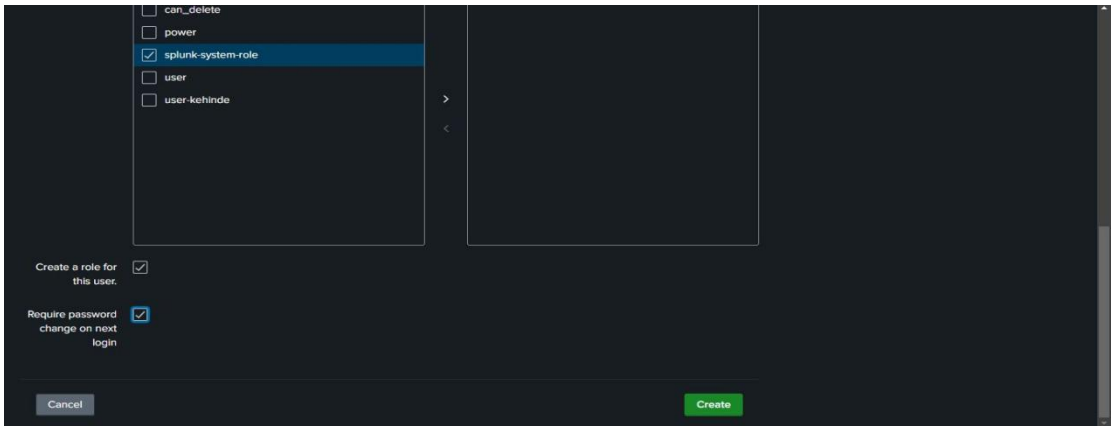
Dashboard:



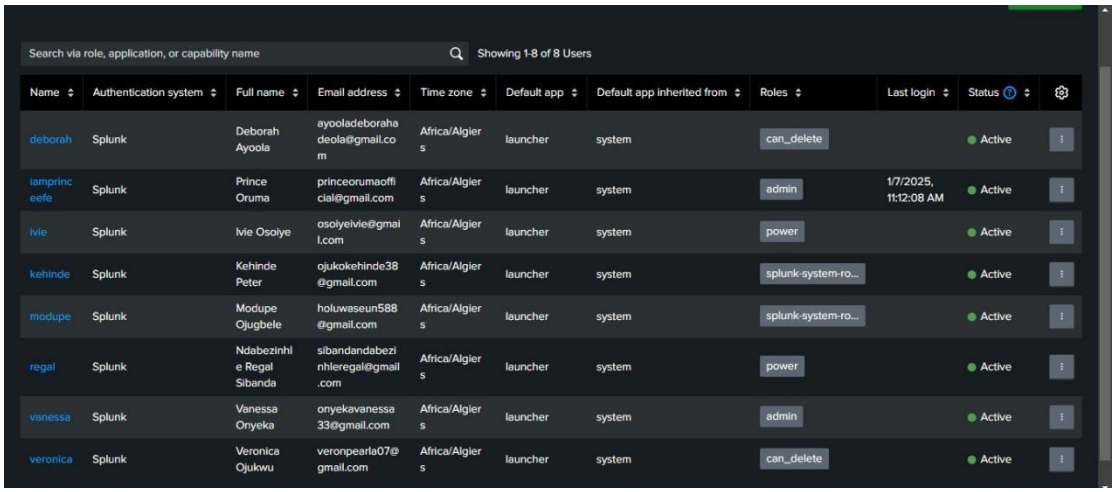
Create New Users:







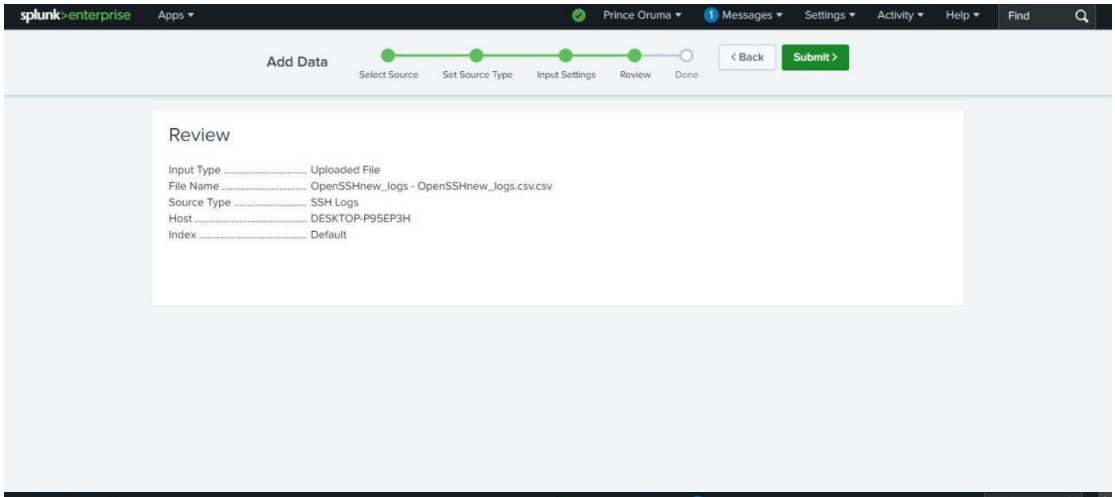
All Users Created:

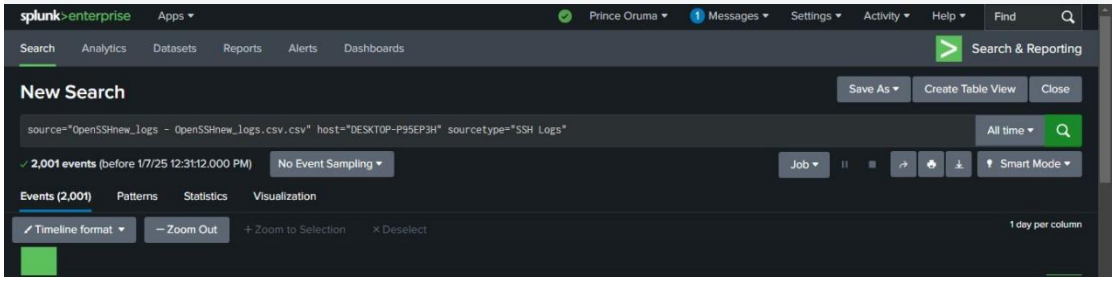


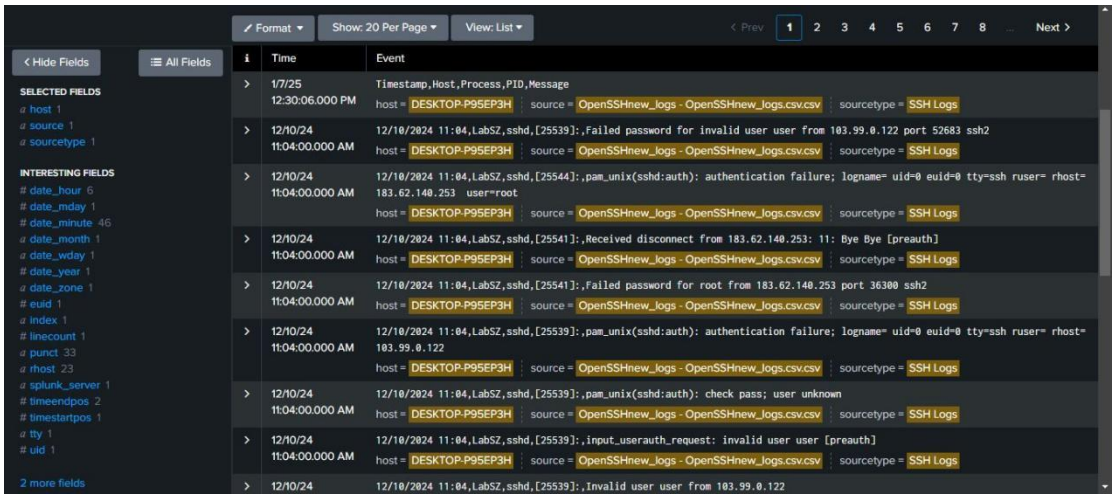
Name	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last login	Status
deborah	Splunk	Deborah Ayoola	ayooladeborahadeola@gmail.com	Africa/Algiers	launcher	system	can_delete		Active
iamprinceefe	Splunk	Prince Oruma	princeorumaofficial@gmail.com	Africa/Algiers	launcher	system	admin	1/7/2025, 11:12:08 AM	Active
ivie	Splunk	Ivie Osoiye	osoiyeivie@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	Ndabezinhle Regal Sibanda	sibandandabezinhleregal@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 unusua;l IP’s, and multiple failed login attempts.







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 recorgnized by the system.

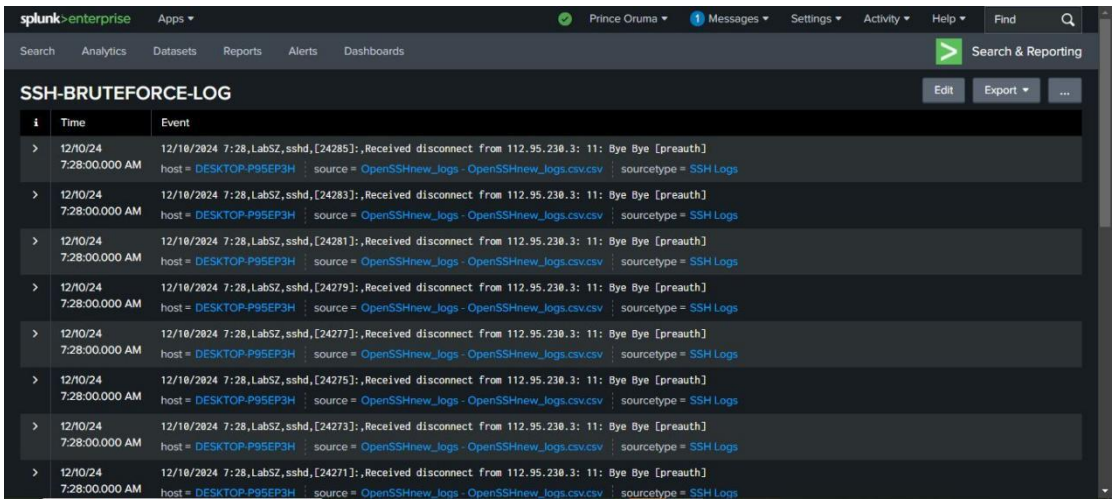
The timestamp of the log also signified a brute-force attack that was done with an automated tool

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.

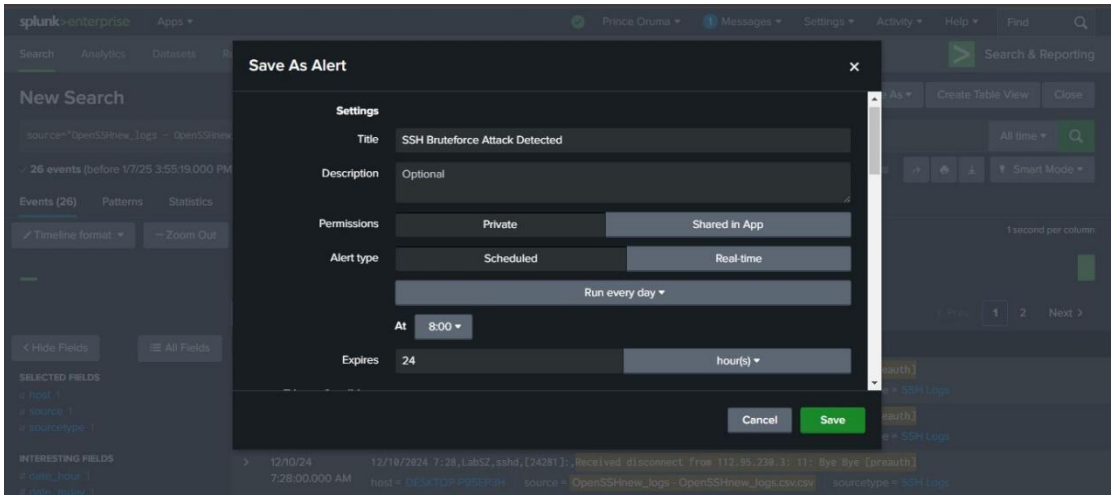
3.0 DASHBOARD AND ALERT CREATION:

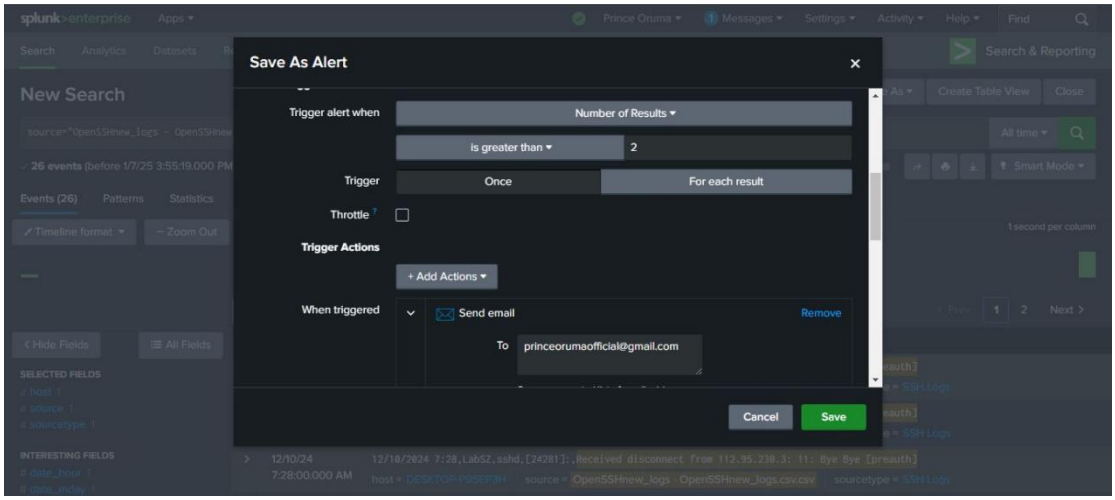
Next we created a dashboard using the search query ‘*Received disconnect from 112.95.230.3: 11: Bye Bye [preauth]*’ and configured an alert to run daily at 8am, expires at 24 hours, triggers when the number of results is greater than 2 and be received via email in plain text.

Dashboard Created:

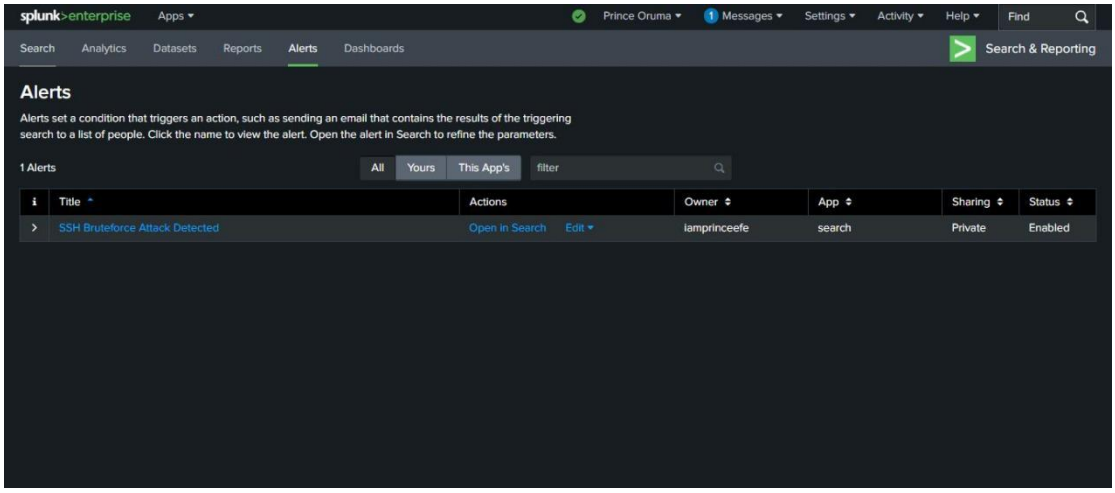


Create Alert:



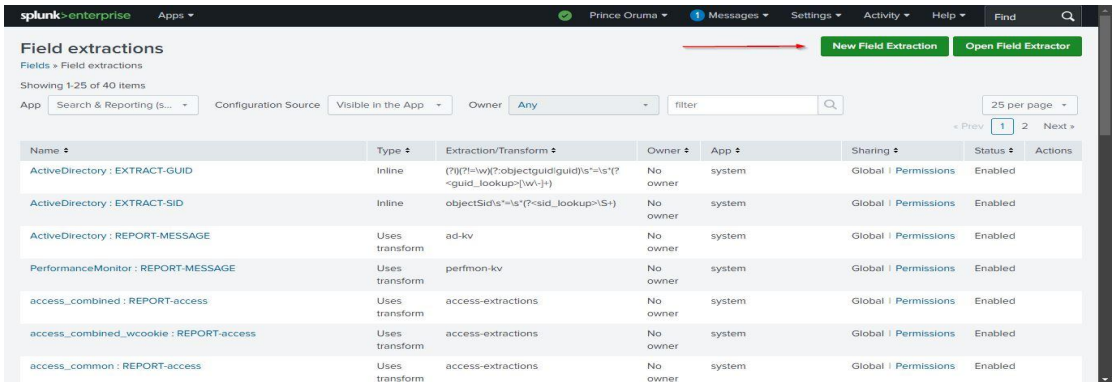


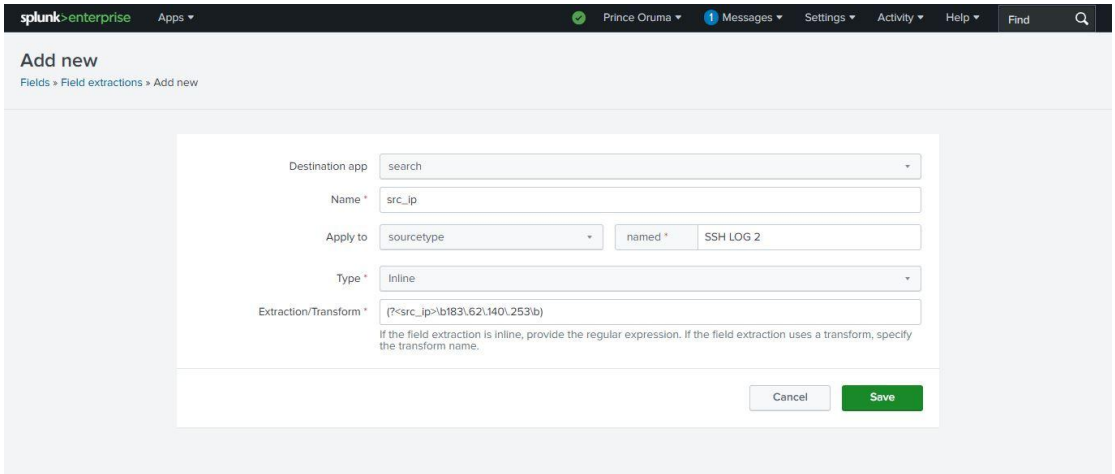
Alert Created:



4.0 FIELD EXTRACTION:

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





SSH LOG 2 : EXTRACT-src_ip	Inline	(?<src_ip>\b183\.62\.140\.253\b)	iamprinceefe	search	Private | Permissions	Enabled	Move | Delete

Dashboard: