PRATICAL NUMBER 5

QUESTION

How would you configure a SIEM system to monitor and alert on security incidents on a network?

ANSWER

Before we talk about configuring a SIEM system, I think it is important to have an idea of **true positive, true negative , false positive and false negative.**

True positive --This is an outcome where the model correctly predicts the positive class

True negative--This is an outcome where the model correctly predicts the negative class

False positive-This is an outcome where the model incorrectly predicts the positive class

False negative--This is an outcome where the model incorrectly predicts the negative class

For better understanding, the perfect example to combine all of this is a whatsapp notification

a notification from whatsapp stating you have a message, you log into your whatsapp and see the message is **TRUE POSITIVE**

a notification from whatsapp stating you have a message, you log into your whatsapp and didnt see the message is **TRUE NEGATIVE**

NO notification from whatsapp stating you have a message, you log into your whatsapp and see the message is **FALSE POSITIVE**

NO notifications and no messages on whatsapp is **FALSE NEGATIVE,**

To configure a SIEM system to monitor and alert on security incidents on a network;

<1>--The first step in configuring a SIEM is to identify which assets are to be monitored and protected and how critical it is to the organization and to determine how critical an instrument is to the organization can be calculated using qualitative and quantitative. This include calculating the single loss expectancy and annual rate of occurence.

<2>--The security incidents or scenarios should be identified include brute force attacks, malware infection, and data exfiltration

In accordance to this , one cant secure or protect what isn't known

<3>--Ensure logs are sent to the SIEM by syslog and sensitive data should be sent using encrypted channels.

<4>-- A SIEM rule should be created to define suspicious activity by analyzing patterns across different log sources.

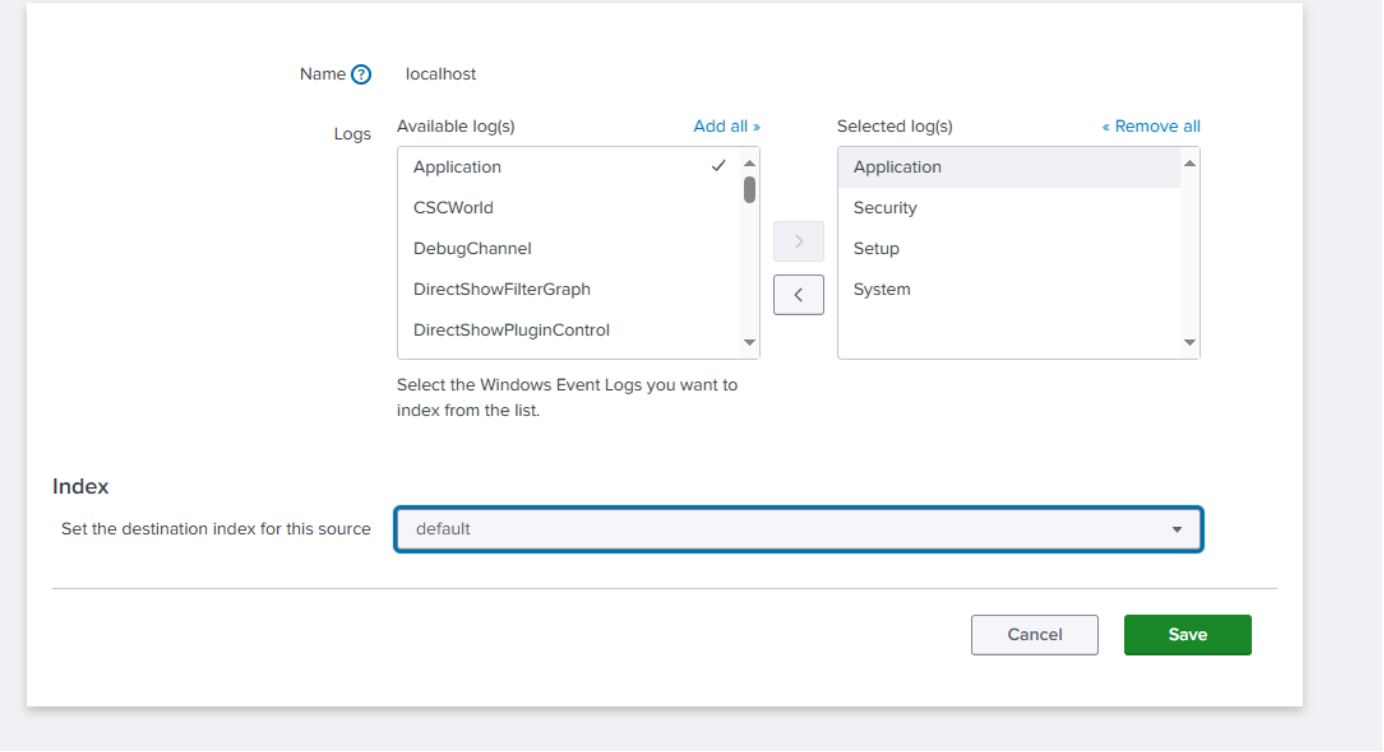
QUESTION 2

Set up a SIEM tool like Splunk Free or ELK Stack. Configure it to collect logs from various sources (firewalls, servers, endpoints). Create and customize alerts to trigger when certain suspicious activities are detected (e.g., a high number of failed login attempts or unusual outbound traffic).

ANSWER

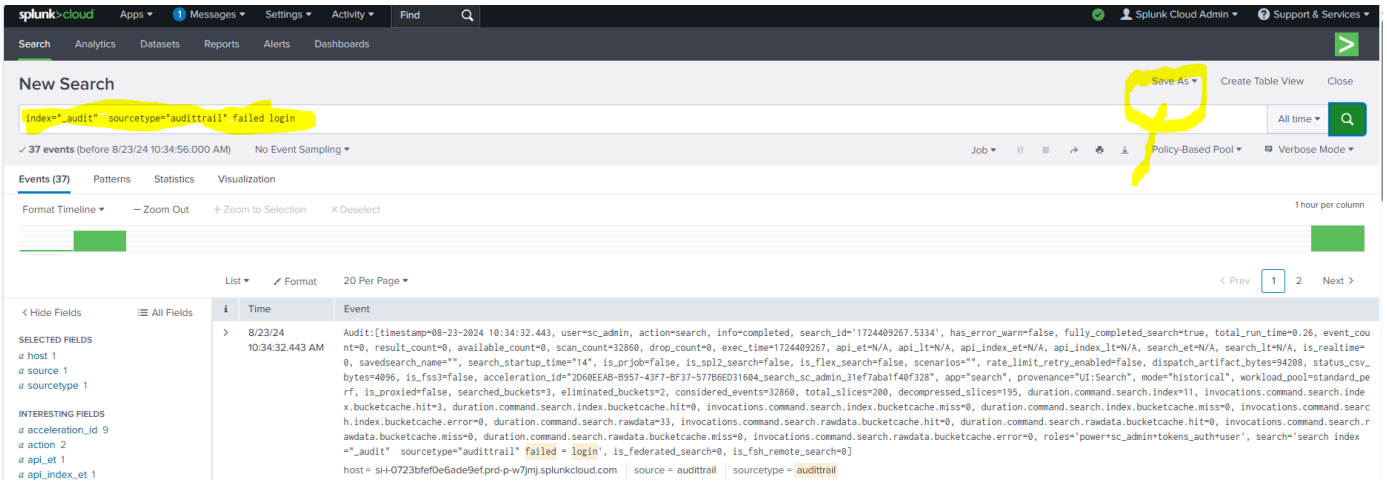
TO configure splunk to collect logs from various sources like firewalls, servers and endpoints

Kindly go to **settings- data input - local event log collection** and edit



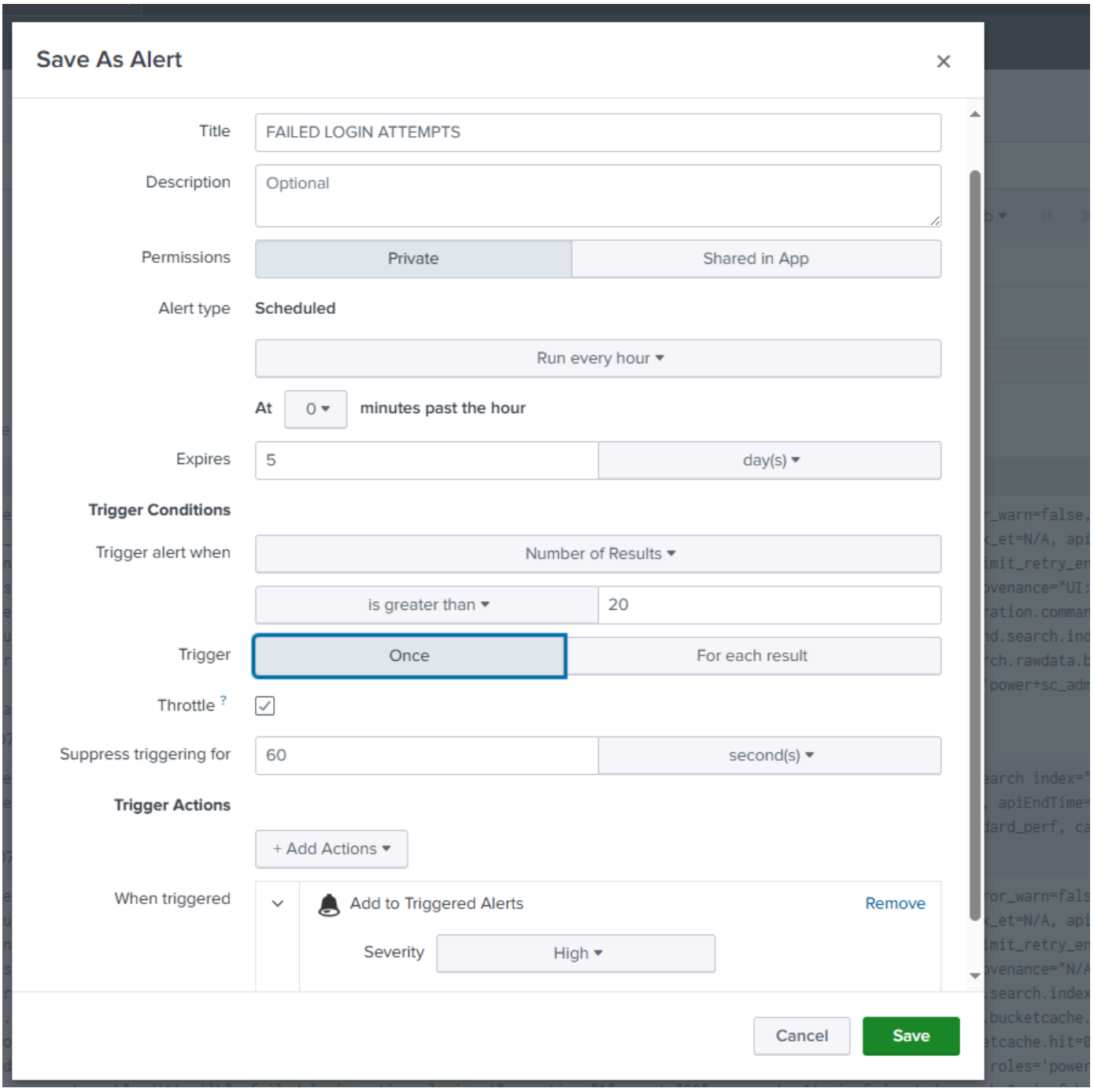
Then select **SAVE**

To create and customize alerts to trigger suspicious activities especially failed login attempts.

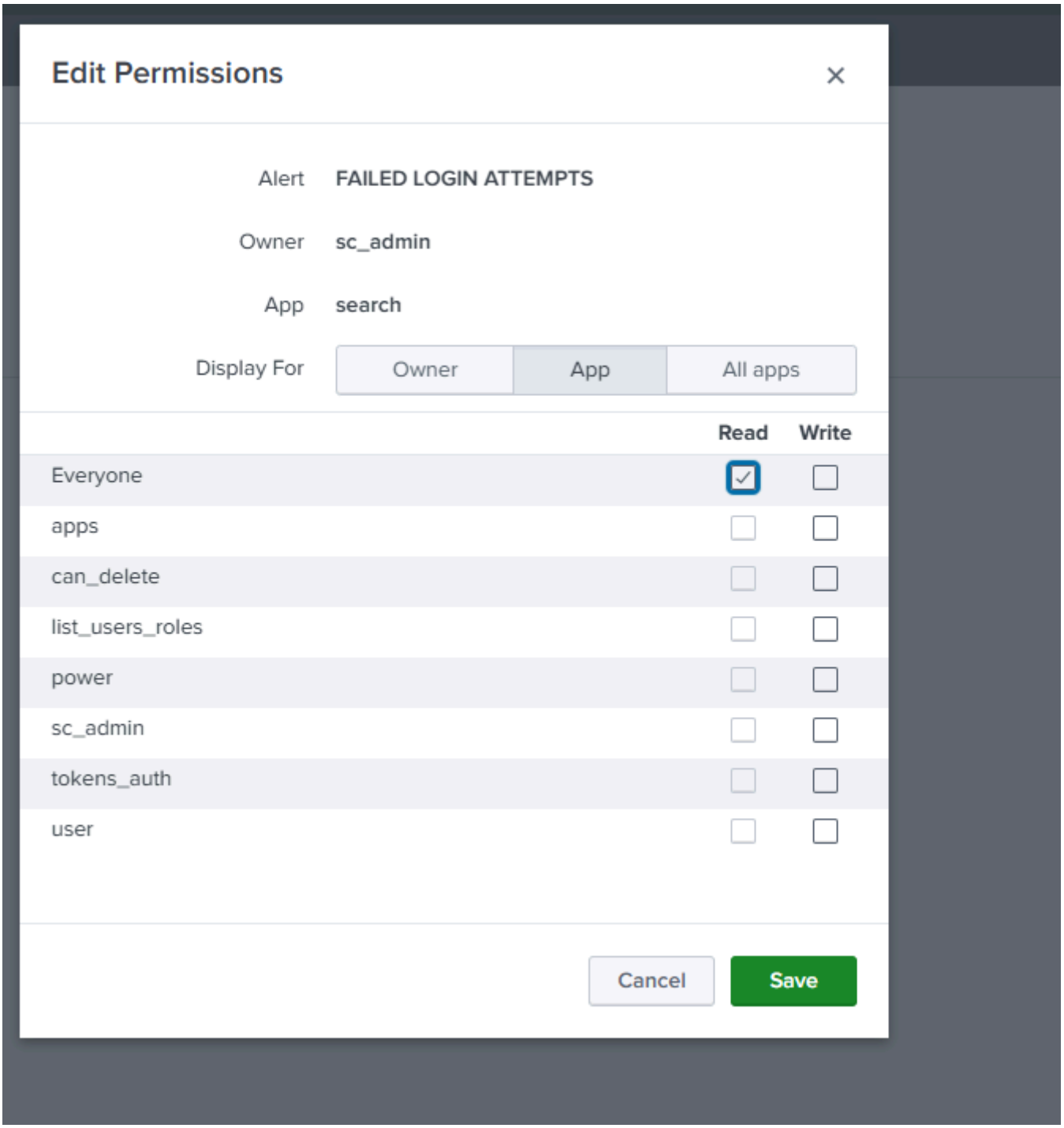


From the screenshot above which shows 37 events that indicates failed login attempts

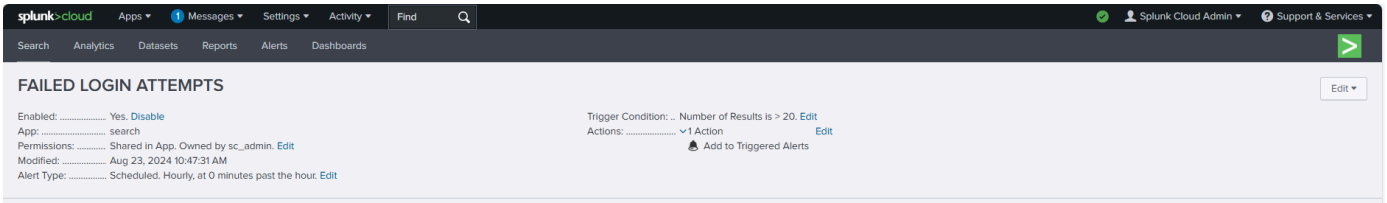
I will create and customize this alert by clicking the 'save as ' circled in the screenshot to detect high number of failed logins



I edited the permissions



I named it failed login attempts and customized alerts to trigger when there is a failed login attempts .



I set it to run every hour and expire after 5 days so i can create a new alert. I set it to trigger alert when the number of failed log in attempts is greaten than 20 and to trigger **ONCE.**