

SIE300-M1-1-Lab-Advanced Notifications Lab

Due No due date

Points 3

Questions 3

Time Limit None

Allowed Attempts 3

Instructions

Abstract

Notifications in a SIEM are often overlooked because there are too many and often they aren't in email- where business is normally done. Instead of sending a simple email for an alert, this lab will extend the functionality of alerts through a webhook.

Exercise Objective(s):

By the end of this lab, the student should be able to:

EO1: Configure alert notifications for critical events

System Requirements & Configuration

System Requirements

Your VirtualBox Environment. This is the Splunk environment created in a previous lab. If necessary, repeat the **SIE100-M3-1-Lab-Splunk Install** to create a new Splunk Virtual Machine. Additional labs in SIE200 may also be necessary to ensure all data is present.

Network Requirements

This lab should be done on local Virtual Machines with internet access. Set the network to NAT or NAT Network.

Software Requirements

The Slack webhook alert from Splunkbase will be installed and an account will need to be created (if the student does not currently have one) during the lab.

Procedure – Detailed Lab Steps

Lab Execution

[Chat](#)

Base Lab

Go to www.slack.com (<http://www.slack.com/>)

Select “**Try for Free**” in the upper right-hand corner.

Sign in to the Slack account if applicable and skip to step 5; otherwise, set one up for free by clicking “**My team isn’t on Slack yet**”.

Enter the email address into the box provided and then enter the 6 digit verification code that was sent to the email.

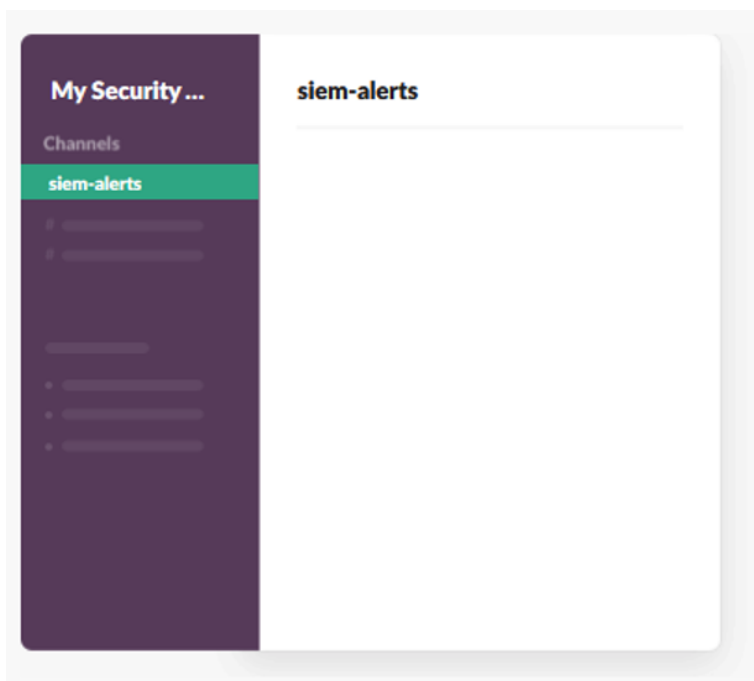
Click **Create a Workspace**.

What's the name of your company or team?

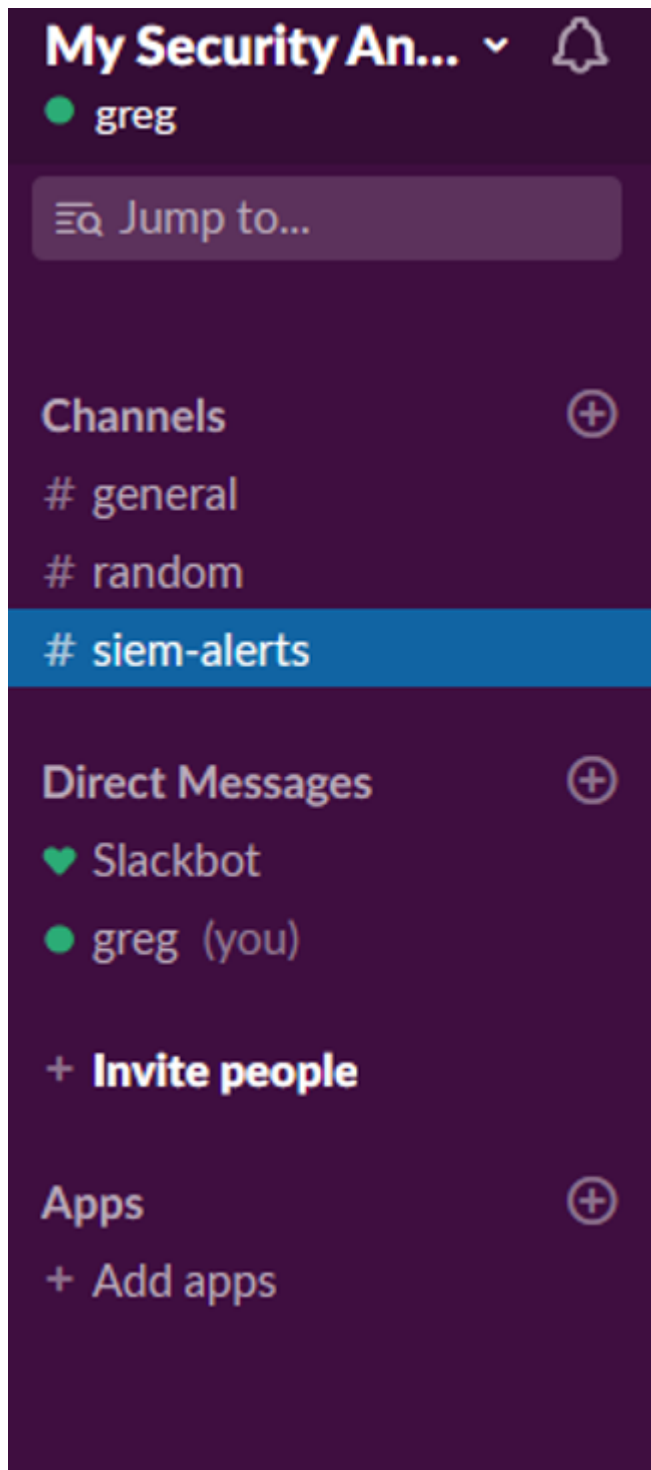
My Security Analyst Team

Next

Enter **SIEM-alerts** when asked what the team is currently working on.



Click Next until this is completed, skipping the step to add teammates.



Start the Splunk VM, and use a browser to access the Splunk Console.

Choose **Splunk Apps**, and download the **Slack Notification Alert app**

Install the App inside of the Splunk instance. Please reference previous module labs if unsure how to do this.

Once the app has been installed, it will prompt to open the app, and then set it up. This screen should see this screen next:

Slack Alert Action
Configure the Slack API

Server

Webhook URL
In order to obtain the Webhook URL you have to create a new incoming webhook integration for your Slack instance. See [Incoming Webhooks Docs](#) for details.

Sender Name
This name will appear in slack as the user sending the message

Sender Icon
The avatar/icon shown by the sender of the slack message. This URL needs to be accessible from the internet.


Follow the screenshots below to set up the webhook (step by step instructions can be found at this link: <https://api.slack.com/messaging/webhooks> (<https://api.slack.com/messaging/webhooks>)).

Create a Slack App ×

App Name

Don't worry; you'll be able to change this later.

Development Slack Workspace

 My Security Analyst Team ▼

Your app belongs to this workspace—leaving this workspace will remove your ability to manage this app. Unfortunately, this can't be changed later.

By creating a Web API Application, you agree to the [Slack API Terms of Service](#).

Incoming Webhooks

Activate Incoming Webhooks

☒ On

Incoming webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details. You can include [message attachments](#) to display richly-formatted messages.

Each time your app is installed, a new Webhook URL will be generated.

If you deactivate incoming webhooks, new Webhook URLs will not be generated when your app is installed to your team. If you'd like to remove access to existing Webhook URLs, you will need to [Revoke All OAuth Tokens](#).

Add New Webhook to Workspace

This app was created by a member of your workspace, My Security Analyst Team.

Splunk SIEM is requesting permission to access the My Security Analyst Team Slack workspace



What will Splunk SIEM be able to view?



Content and info about you



View information about your identity

Where should Splunk SIEM post?



Splunk SIEM requires a channel to post to as an app

siem-alerts

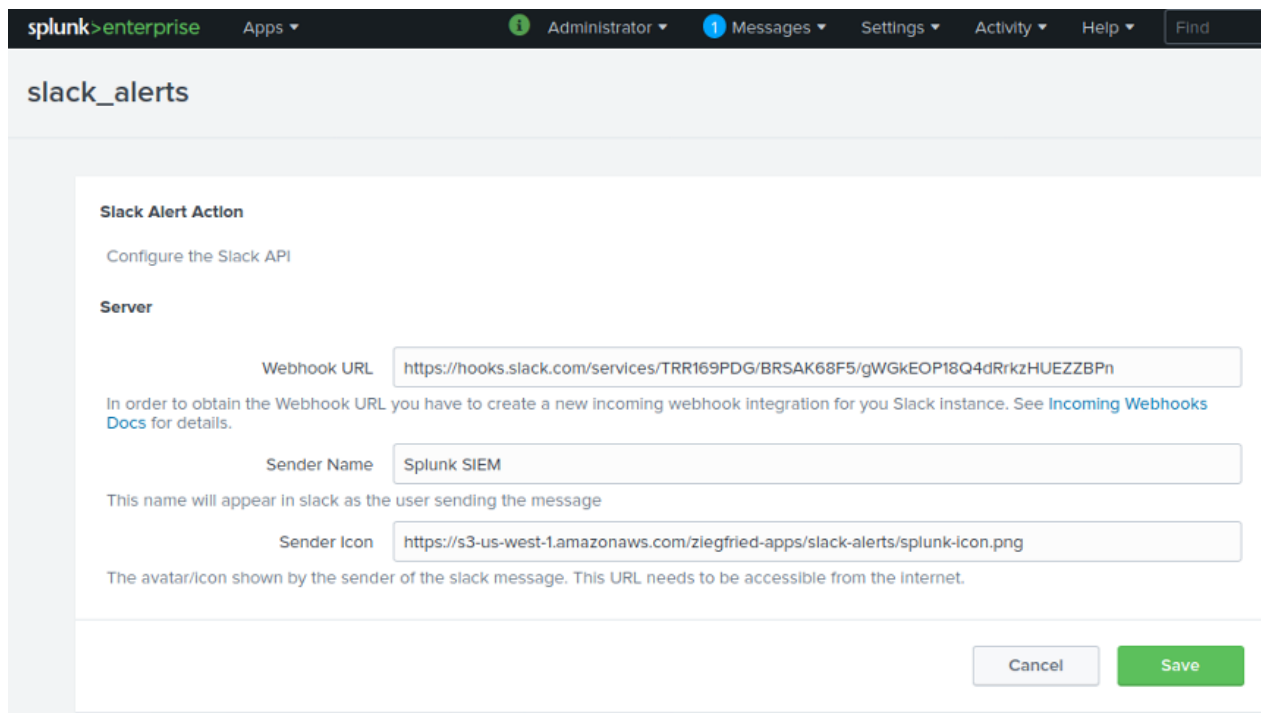


Cancel

Allow

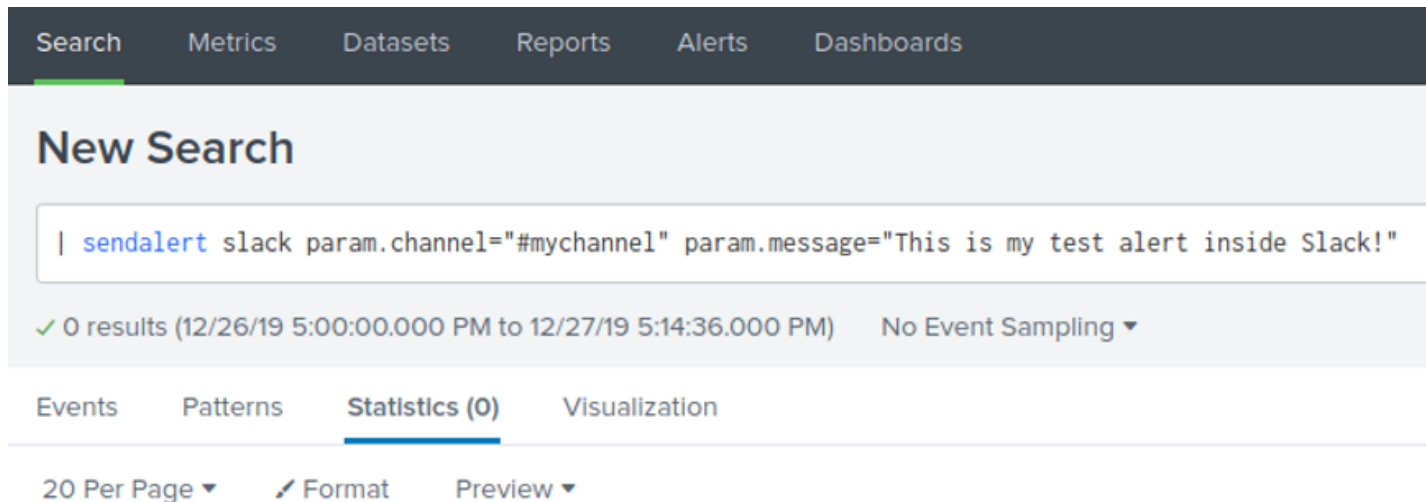
Webhook URL	Channel	Added By
https://hooks.slack.com/services/TRR1 <button>Copy</button>	#siem-alerts	greg Dec 27, 2019

After the webhook is created, copy the **Webhook URL** and paste it into Splunk.



The screenshot shows the 'slack_alerts' configuration page in Splunk. The page has a header with 'splunk>enterprise' and navigation links for Apps, Administrator, Messages, Settings, Activity, Help, and Find. The main content area is titled 'slack_alerts' and contains a 'Slack Alert Action' section. This section includes a 'Server' subsection with the following fields: 'Webhook URL' (https://hooks.slack.com/services/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), 'Sender Name' (Splunk SIEM), and 'Sender Icon' (https://s3-us-west-1.amazonaws.com/zlegfried-apps/slack-alerts/splunk-icon.png). There are 'Cancel' and 'Save' buttons at the bottom right.

Go back to search and search for `| sendalert slack param.channel="#mychannel" param.message="This is my test alert inside Slack!"`



The screenshot shows the Splunk Search interface. The top navigation bar includes Search, Metrics, Datasets, Reports, Alerts, and Dashboards. The main heading is 'New Search'. Below it, a search bar contains the query: `| sendalert slack param.channel="#mychannel" param.message="This is my test alert inside Slack!"`. Below the search bar, it shows '0 results (12/26/19 5:00:00.000 PM to 12/27/19 5:14:36.000 PM)' and 'No Event Sampling'. At the bottom, there are tabs for Events, Patterns, Statistics (0), and Visualization. Below the tabs, there are controls for '20 Per Page', 'Format', and 'Preview'.

Open the tab with Slack. There should be an alert in the SIEM-alerts channel.



greg 5:01 PM
joined #siem-alerts.



greg 5:10 PM
added an integration to this channel: **Splunk SIEM**



Splunk SIEM APP 5:14 PM
This is my test alert inside Slack!

Message #siem-alerts

Create a new file input using the same method as the previous module inside of **/var/log/**. This time call the file **advanced_log.log**.

Set up an alert that searches for *** source="/var/log/advance_log.log"** and alerts if the number of logs is over 5 for the past 15 minutes.

Use the Slack Alert as the Action for the alert. Modify the file to trigger the alert: **echo "This is test notification to Slack" >> /var/log/advanced_log.log**

New Search

* source="/var/log/advanced_log.log"

✓ 13 events (12/27/19 5:21:13.000 PM to 12/27/19 5:36:13.000 PM) No Event Sampling ▼

Events (13) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼

< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a eventtype 1
a index 1
linecount 1
a punct 1
a splunk_server 1
a timestamp 1
a unix_category 1
a unix_group 1

i	Time	Event
>	12/27/19 5:36:09.000 PM	This is a test notification to Slack host = siem source = /var/log/advanced_log.log sourcetype = config_file
>	12/27/19 5:36:09.000 PM	This is a test notification to Slack host = siem source = /var/log/advanced_log.log sourcetype = config_file
>	12/27/19 5:36:09.000 PM	This is a test notification to Slack host = siem source = /var/log/advanced_log.log sourcetype = config_file
>	12/27/19 5:36:08.000 PM	This is a test notification to Slack host = siem source = /var/log/advanced_log.log sourcetype = config_file
>	12/27/19 5:36:08.000 PM	This is a test notification to Slack host = siem source = /var/log/advanced_log.log sourcetype = config_file



Splunk SIEM

APP

5:57 PM

Testing alerting

Testing alerting

Testing alerting

Testing alerting

Testing alerting

Questions

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	<u>Attempt 2</u>	less than 1 minute	3 out of 3
	<u>Attempt 1</u>	19,546 minutes	2 out of 3

Score for this attempt: 3 out of 3

Submitted Sep 28, 2022 at 8:03pm

This attempt took less than 1 minute.

Correct!

Question 1

1 / 1 pts

Severity is often subjective and due to this, not very useful in prioritizing.

True

False

Question 2**1 / 1 pts**

These are reasons to remediate except this one:

- ☐ Mitigate risk
- ☐ Reduce dwell time and evict adversaries
- ☐ Reduce attack surface
- ☒ Encourage known risky staff to stay inside corporate network

Correct!**Question 3****1 / 1 pts**

Automation, if done right, is like adding people to your staff.

- ☒ True
- ☐ False

Correct!**Quiz Score: 3 out of 3**

Have specific feedback?

Tell us here! ([https://flatironschoolforms.formstack.com/forms/canvas_feedback?](https://flatironschoolforms.formstack.com/forms/canvas_feedback?CourseID=5338&LessonID=28275&LessonType=quizzes&CanvasUserID=10700&Course=None)

[CourseID=5338&LessonID=28275&LessonType=quizzes&CanvasUserID=10700&Course=None](https://flatironschoolforms.formstack.com/forms/canvas_feedback?CourseID=5338&LessonID=28275&LessonType=quizzes&CanvasUserID=10700&Course=None))