**Fixit**

Fix the log parsing issue and analyze the logs in Splunk.

A computer with a screwdriver

Description automatically generated

Task 1

FIXIT Challenge

In this challenge room, you will act as John, who has recently cleared his third screening interview for the SOC-L2 position at MSSP Cybertees Ltd, and a final challenge is ready to test your knowledge, where you will be required to apply the knowledge to FIX the problems in Splunk.  
You are presented with a Splunk Instance and the network logs being ingested from an unknown device.

Pre-requisites  
This challenge is based on the knowledge covered in the following rooms:

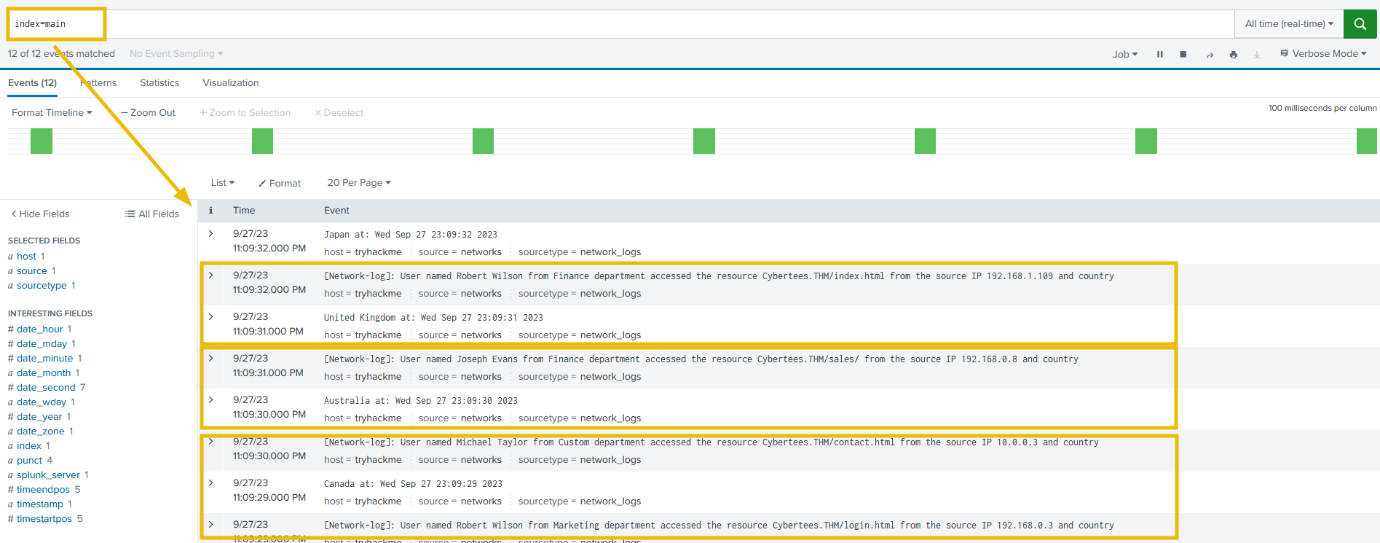
* [Regex](https://tryhackme.com/room/catregex)
* [Splunk: Exploring SPL](https://tryhackme.com/room/splunkexploringspl)
* [Splunk: Data Manipulation](http://tryhackme.com/jr/splunkdatamanipulation)

Room Machine  
Before moving forward, start the lab by clicking the Start Machine button. The lab will be accessible via split screen. If the VM is not visible, use the blue Show Split View button at the top-right of the page. Once the VM is in split screen view, you can click the + button to show it on a full screen. The VM will take 3-5 minutes to load properly. In this room, we will be working using the terminal of the VM and accessing the Splunk instance at MACHINE\_IP:8000.

**Note:** Splunk is installed in the /opt/splunk directory, and you will be working in the App called Fixit.  
  
Challenge: FIXIT  
This challenge is divided into three levels:

**Level 1: Fix Event Boundaries**

Fix the Event Boundaries in Splunk. As the image below shows, Splunk cannot determine the Event boundaries, as the events are coming from an unknown device.



**Level 2: Extract Custom Fields**

Once the event boundaries are defined, it is time to extract the custom fields to make the events searchable.

* Username
* Country
* Source\_IP
* Department
* Domain

**Sample Logs:**   
To create regex patterns, sample Network logs are shown below:

[Network-log]: User named Johny Bil from Development department accessed the resource Cybertees.THM/about.html from the source IP 192.168.0.1 and country

Japan at: Thu Sep 28 00:13:46 2023

[Network-log]: User named Johny Bil from Marketing department accessed the resource Cybertees.THM/about.html from the source IP 192.168.2.2 and country

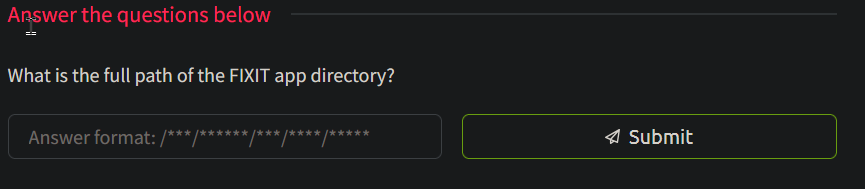
Japan at: Thu Sep 28 00:13:46 2023

[Network-log]: User named Johny Bil from HR department accessed the resource Cybertees.THM/about.html from the source IP 10.0.0.3 and country

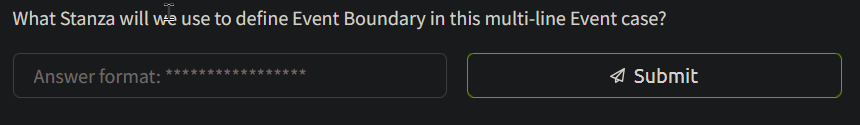
Japan at: Thu Sep 28 00:13:46 2023

Level 3: Perform Analysis on the FIXED Events  
Once the custom fields are parsed, we can use those fields to analyze the Event logs. Examine the events and answer the questions.

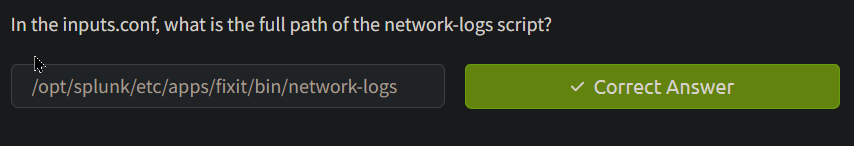
Happy Fixing!



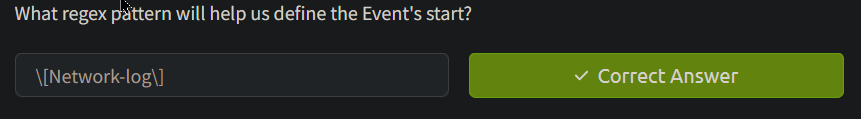




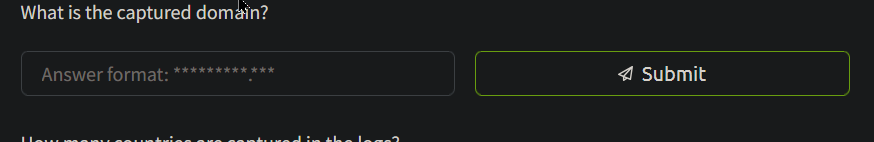
BREAK\_ONLY\_BEFORE





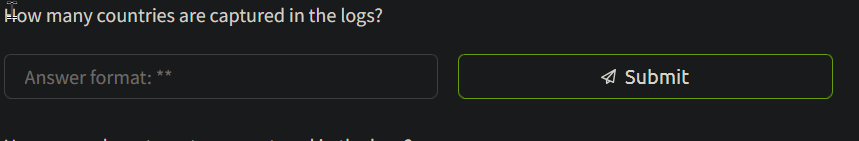






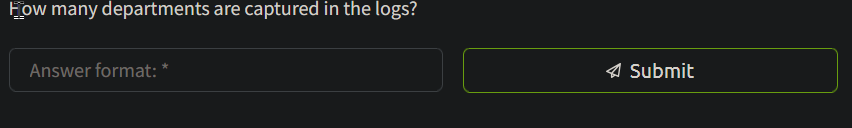
A screenshot of a computer

Description automatically generated



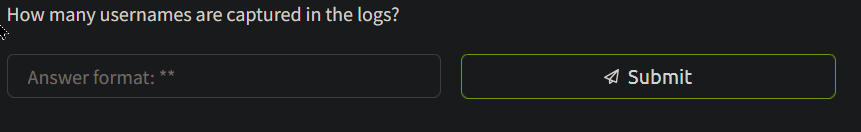
index=main  
|stats count by Country

Answer:12



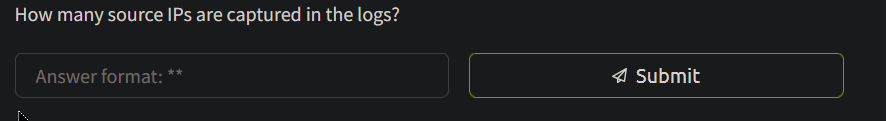
index=main  
|stats count by Department

Anaswer:6



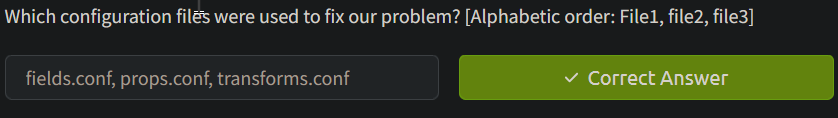
index=main  
|stats count by Username

Answer: 28

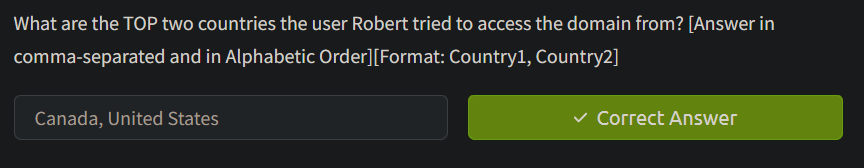


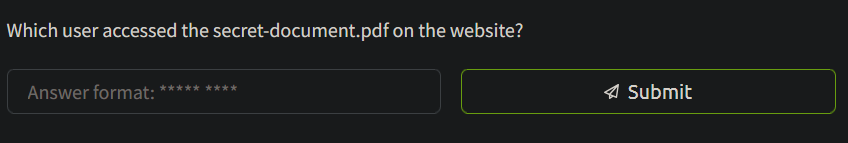
index=main  
|stats count by Source\_IP

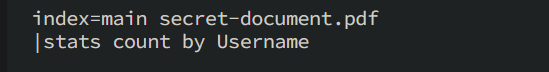
Answer:52



fields.conf, props.conf, transforms.conf







sarah hall