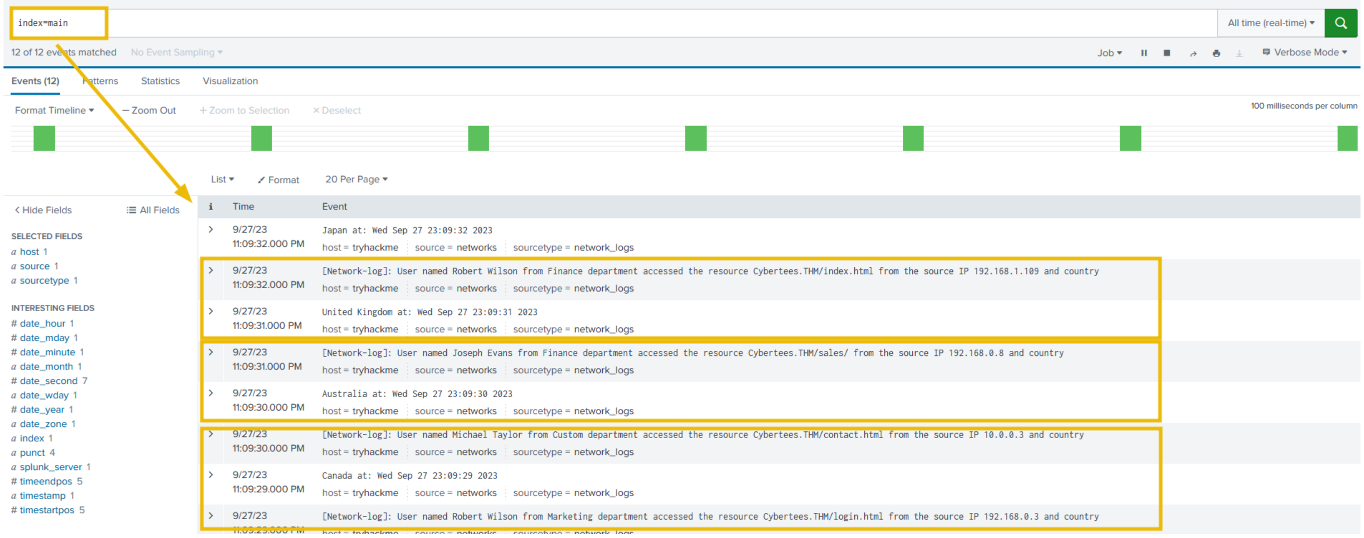
Level 1: Fix Event Boundaries

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.



```
index=main
12 of 12 events matched
```

i	Time	Event
>	9/27/23 11:09:32.000 PM	Japan at: Wed Sep 27 23:09:32 2023 host = tryhackme source = networks sourcetype = network_logs
>	9/27/23 11:09:32.000 PM	[Network-log]: User named Robert Wilson from Finance department accessed the resource Cybertees.THM/index.html from the source IP 192.168.1.109 and country host = tryhackme source = networks sourcetype = network_logs
>	9/27/23 11:09:31.000 PM	United Kingdom at: Wed Sep 27 23:09:31 2023 host = tryhackme source = networks sourcetype = network_logs
>	9/27/23 11:09:31.000 PM	[Network-log]: User named Joseph Evans from Finance department accessed the resource Cybertees.THM/sales/ from the source IP 192.168.0.8 and country host = tryhackme source = networks sourcetype = network_logs
>	9/27/23 11:09:30.000 PM	Australia at: Wed Sep 27 23:09:30 2023 host = tryhackme source = networks sourcetype = network_logs
>	9/27/23 11:09:30.000 PM	[Network-log]: User named Michael Taylor from Custom department accessed the resource Cybertees.THM/contact.html from the source IP 10.0.0.3 and country host = tryhackme source = networks sourcetype = network_logs
>	9/27/23 11:09:29.000 PM	Canada at: Wed Sep 27 23:09:29 2023 host = tryhackme source = networks sourcetype = network_logs
>	9/27/23 11:09:29.000 PM	[Network-log]: User named Robert Wilson from Marketing department accessed the resource Cybertees.THM/login.html from the source IP 192.168.0.3 and country host = tryhackme source = networks sourcetype = network_logs

Level 2: Extract Custom Fields

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

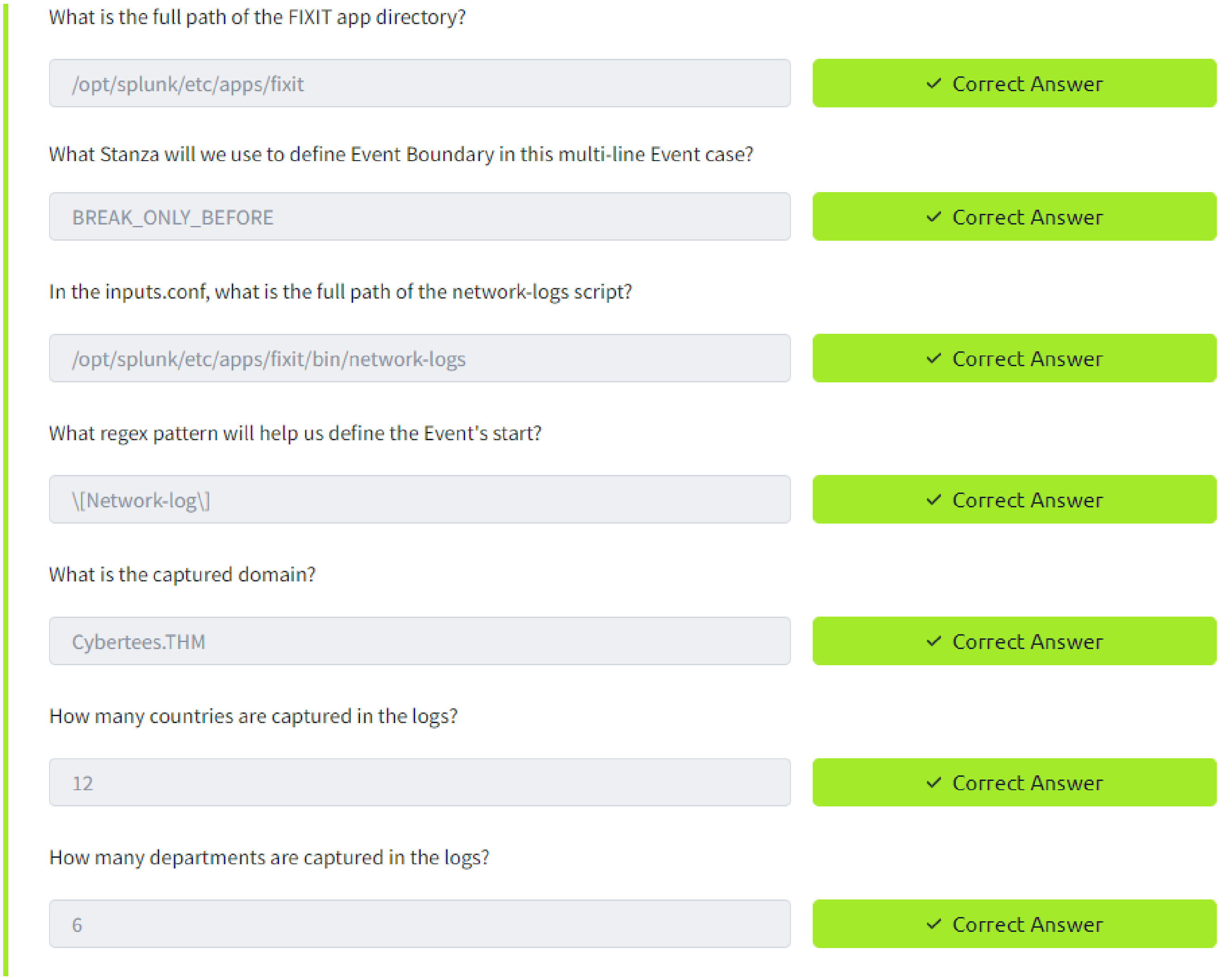
- Username
- Country
- Source_IP
- Department
- Domain

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!



What is the full path of the FIXIT app directory?

/opt/splunk/etc/apps/fixit

What Stanza will we use to define Event Boundary in this multi-line Event case?

BREAK_ONLY_BEFORE

In the inputs.conf, what is the full path of the network-logs script?

/opt/splunk/etc/apps/fixit/bin/network-logs

What regex pattern will help us define the Event's start?

\[Network-log\]

What is the captured domain?

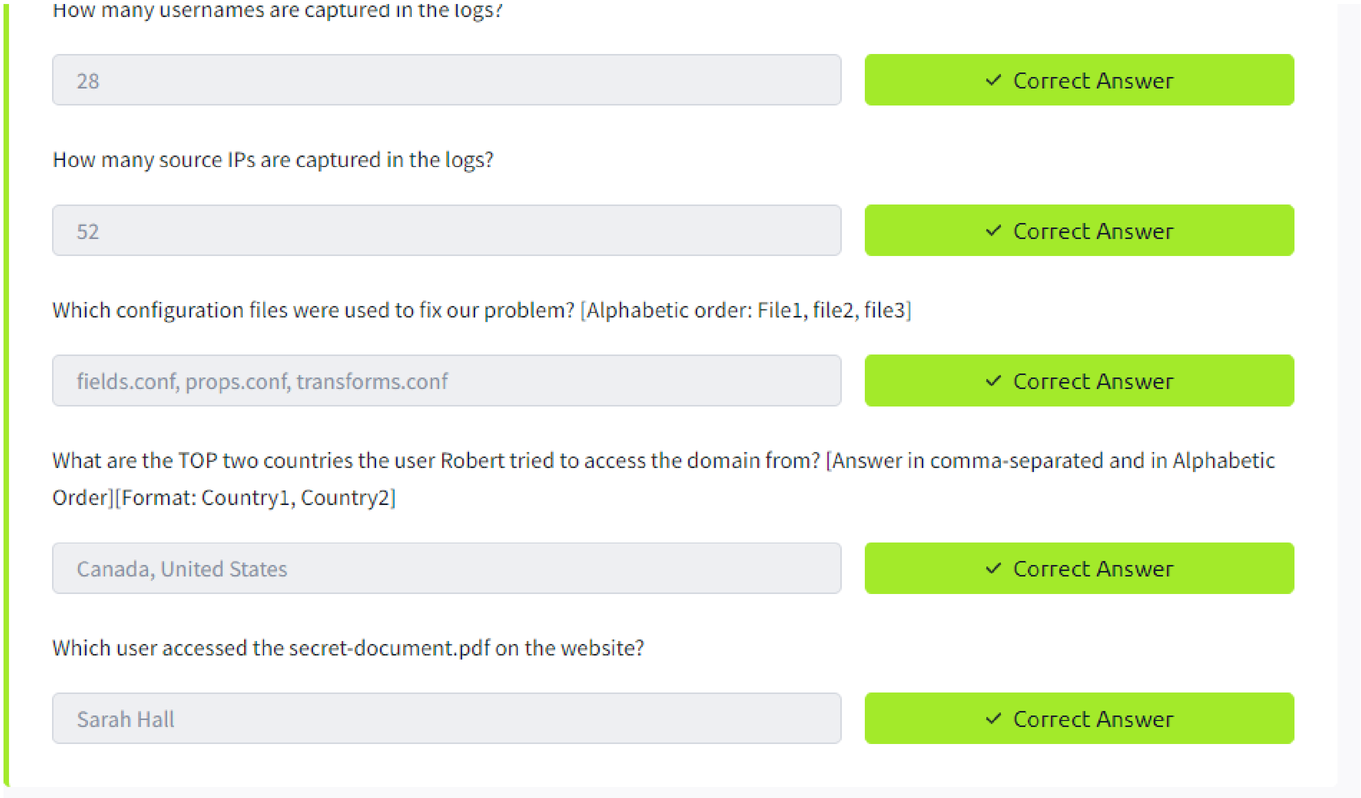
Cybertees.THM

How many countries are captured in the logs?

12

How many departments are captured in the logs?

6



How many usernames are captured in the logs?

28

How many source IPs are captured in the logs?

52

Which configuration files were used to fix our problem? [Alphabetic order: File1, file2, file3]

fields.conf, props.conf, transforms.conf

What are the TOP two countries the user Robert tried to access the domain from? [Answer in comma-separated and in Alphabetic Order][Format: Country1, Country2]

Canada, United States

Which user accessed the secret-document.pdf on the website?

Sarah Hall