In this report, we will discover SIEM Lab questions and answer made by Tayfun Mutlu.

NOTE: This lab provided by TryHackMe.

In the static lab attached, a sample dashboard and events are displayed. When a suspicious activiy happens, an Alert is triggered, which means some events match the condition of some rule already configured.

Question 1

Click on Start Suspicious Activity, which process caused the alert?

A screenshot of a computer

AI-generated content may be incorrect.(A process name is ‘cudominer.exe’ causes the alarm shows. Alarm says ‘Potential CryptoMiner Activity Observed, find and click on the triggered event to show the details.)

A blue and white rectangle with black text

AI-generated content may be incorrect.

Question 2

Find the event that caused the alert, which user was responsible for the process execution?

(We can see on events, the user ‘Chris.fort’ is caused the alert with using process ‘cudominer.exe’)

A screenshot of a computer

AI-generated content may be incorrect.

Question 3

What is the hostname of the suspect user?

(Host name of the suspect user is HR\_02. We are seeing this host name in events)

Question 4

Examine the rule and the suspicious process; which term matched the rule that caused the alert?

A blue and white rectangular object with black text

AI-generated content may be incorrect.(In rule page, we can see alert name, event id and log source. In here, the term is showns as ‘miner’ or ‘crypt’. So our term matches with one of this.)

Question 5

What is the best option for that represents the event? Choose from the following:

False-positive

True-positive

(True positive represents our event, because there was an alert and detection so something triggered the detection system. Detected event was real, upon investigation, we found the threat was actually there.)

Question 6

What is the FLAG?

(Flag is THM{000\_SIEM\_INTRO} as we see in Screenshot that given below.)

Conclusion

I analyzed suspicious crypto mining activity, identified relevant log attributes and verified detection logic using event correlation. This helped me practice threat classification (true vs false positive) and write clear investigation notes.