Junior Security Analyst Intro

Introduction

Now the learner is ready for a Junior Security Analyst role where they will be a Triage Specialist – this role basically makes a security analyst spend a lot of time triaging or monitoring the event logs and alerts.

Activities

Task 1: A career as a Junior (Associate) Security Analyst

The responsibilities for a Junior Security Analyst or Tier 1 SOC Analyst include:

- Monitor and investigate the alerts (most of the time, it's a 24x7 SOC operations environment)
- Configure and manage the security tools
- Develop and implement basic IDS (Intrusion Detection System) signatures
- Participate in SOC working groups, meetings
- Create tickets and escalate the security incidents to the Tier 2 and Team Lead if needed

The qualifications for this role are:

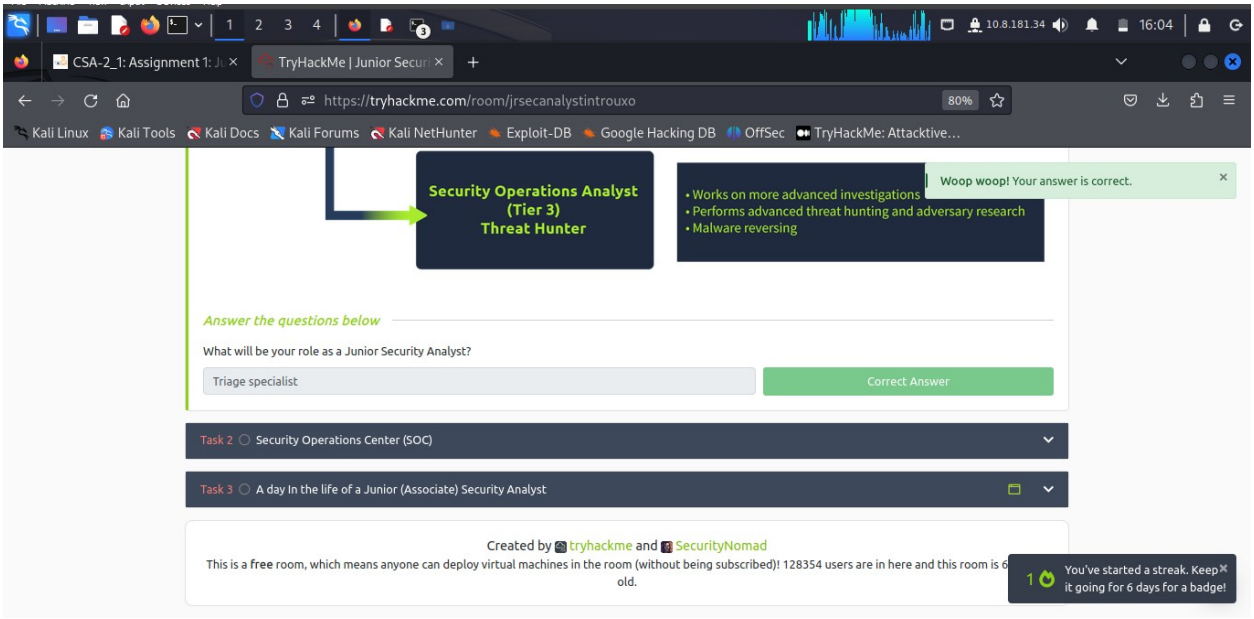
0-2 years of experience with Security Operations

Basic understanding of Networking (OSI model or TCP/IP model), Operating Systems (Windows, Linux), Web Applications.

Scripting/programming skills are a plus

Desired certification:

CompTIA Security+



Task 2: Security Operations Center(SOC)

The core function of a SOC (Security Operations Center) is to investigate, monitor, prevent, and respond to threats in the cyber realm 24/7 or around the clock.

Security operations teams are charged with monitoring and protecting many assets, such as intellectual property, personnel data, business systems, and brand integrity. As the implementation component of an organisation's overall cyber security framework, security operations teams act as the central point of collaboration in coordinated efforts to monitor, assess, and defend against cyberattacks.

Preparation and Prevention

As a Junior Security Analyst, you should stay informed of the current cyber security threats (staying updated on **X** with the news related to Cybersecurity).

Prevention methods include gathering intelligence data on the latest threats, threat actors, and their **TTPs (Tactics, Techniques, and Procedures)**. It also includes the maintenance procedures like updating the firewall signatures, patching the vulnerabilities in the existing systems, block-listing and safe-listing applications, email addresses, and IPs.

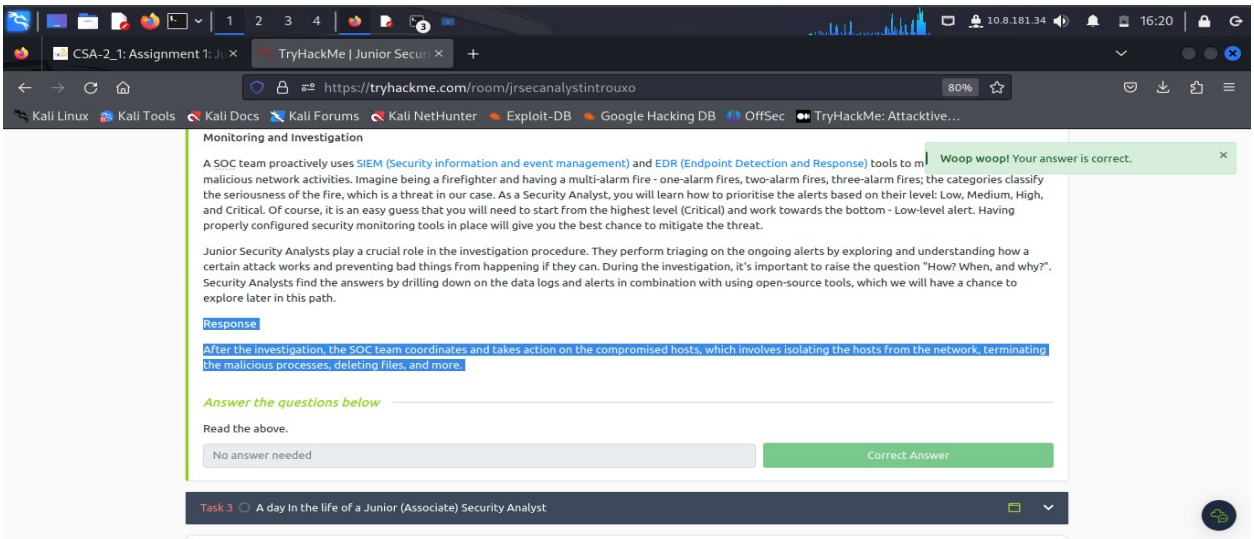
Monitoring and Investigation

A SOC team proactively uses **SIEM (Security information and event management) and EDR (Endpoint Detection and Response)** tools to monitor suspicious and malicious network activities.

Junior Security Analysts play a crucial role in the investigation procedure. They perform triaging on the ongoing alerts by exploring and understanding how a certain attack works and preventing bad things from happening if they can. During the investigation, it's important to raise the question "How? When, and why?". Security Analysts find the answers by drilling down on the data logs and alerts in combination with using open-source tools, which we will have a chance to explore later in this path.

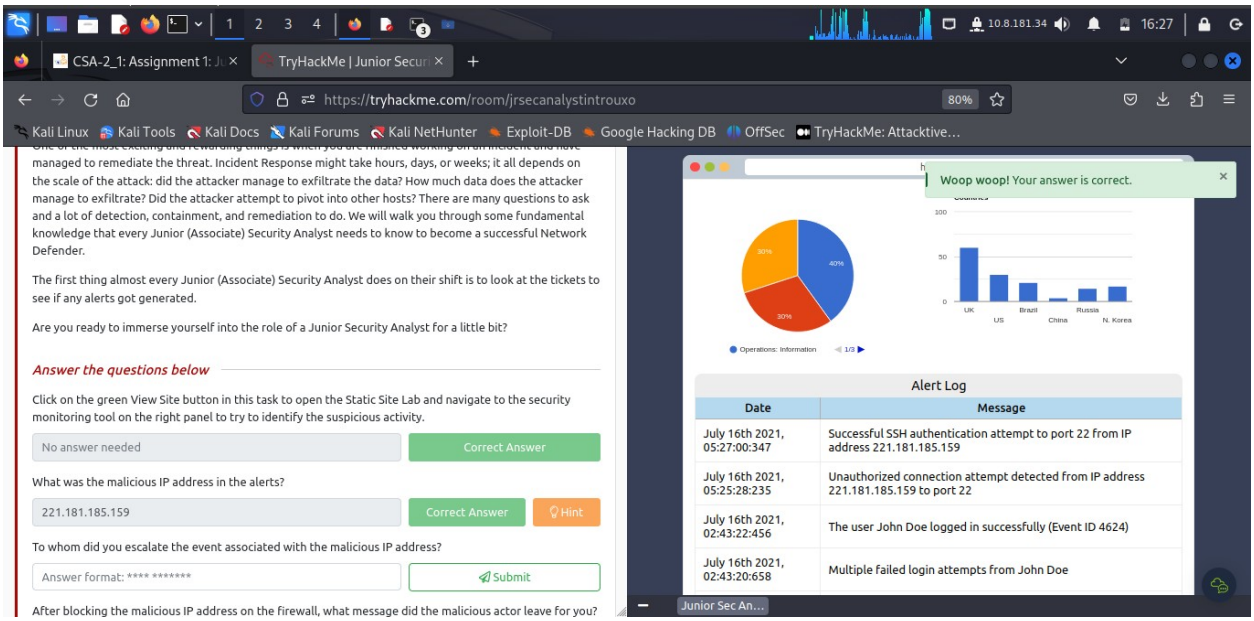
Response

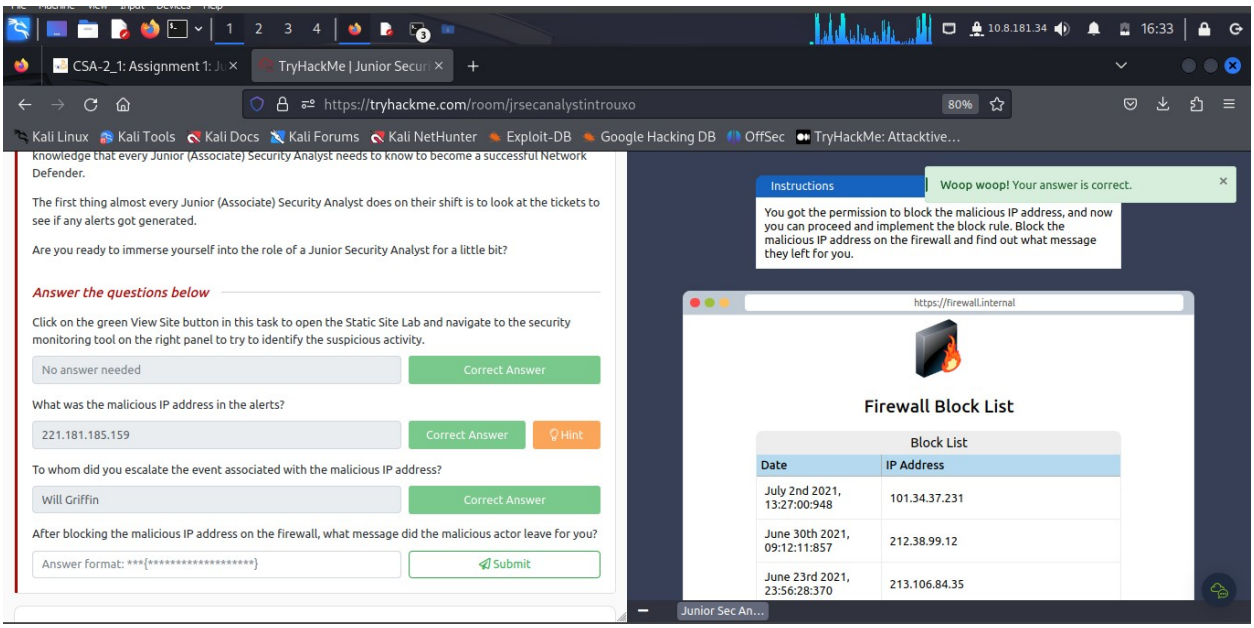
After the investigation, the SOC team coordinates and takes action on the compromised hosts, which involves isolating the hosts from the network, terminating the malicious processes, deleting files, and more.

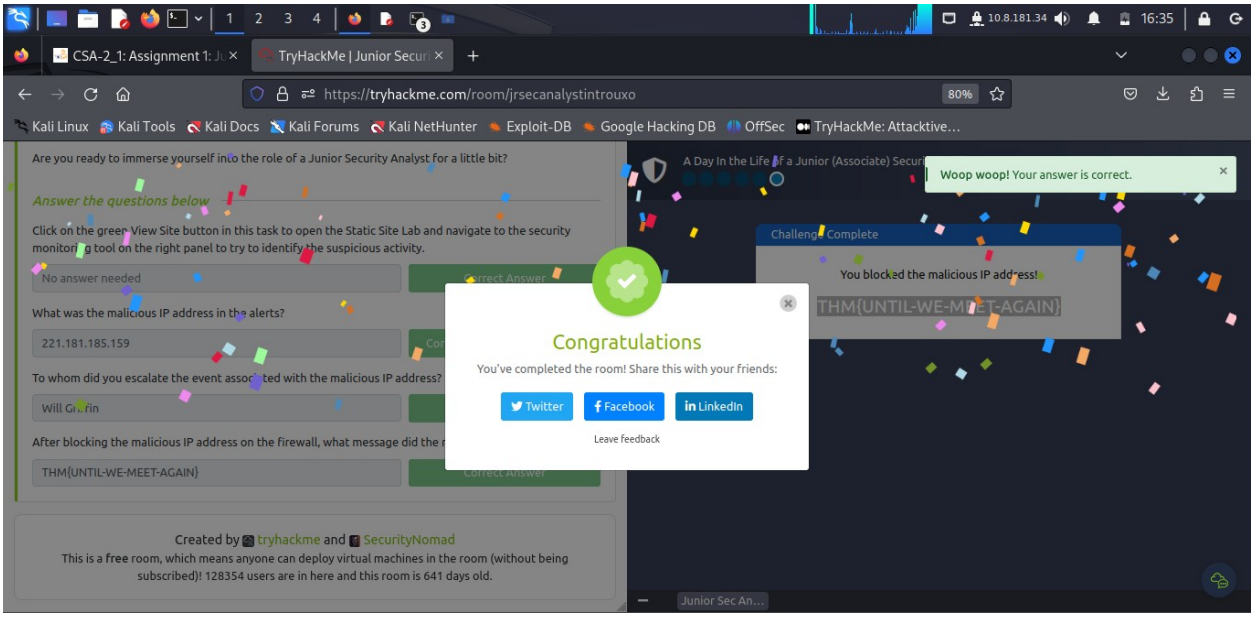


Task 3: A day in the life of a Junior(Associate) Security Analyst

The first thing almost every Junior (Associate) Security Analyst does on their shift is to look at the tickets to see if any alerts got generated.







Conclusion

In this task the Junior Security Analyst was able to know the right qualifications, roles and what is done either in SOC as an entry security analyst or becoming advanced security analyst that's transitioning from Tier 1 to Tiers 2 and 3 of this role of Security analysis.

Completion Link: https://tryhackme.com/room/jrsecanalystintrouxo