

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+

The screenshot shows a web browser window displaying a TryHackMe room. The browser's address bar shows the URL <https://tryhackme.com/room/jrsecanalystintrouxo>. The room's title is "Junior Security Analyst Intro". A green arrow points to a box labeled "Security Operations Analyst (Tier 3) Threat Hunter". To the right of this box, a list of responsibilities is shown: "Works on more advanced investigations", "Performs advanced threat hunting and adversary research", and "Malware reversing". A green notification box says "Woop woop! Your answer is correct." Below this, a question is asked: "What will be your role as a Junior Security Analyst?". The answer "Triage specialist" is entered in a text box, and a green button labeled "Correct Answer" is visible. Below the question, there are two task cards: "Task 2: Security Operations Center (SOC)" and "Task 3: A day in the life of a Junior (Associate) Security Analyst". At the bottom, a message states: "This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 128354 users are in here and this room is 6 months old." A green badge icon and a message "You've started a streak. Keep it going for 6 days for a badge!" are also visible.

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.

The screenshot shows a web browser window with the URL <https://tryhackme.com/room/jrsecanalystintrouxo>. The browser's address bar shows the URL and a 80% zoom level. The page content is titled "Monitoring and Investigation" and contains the following text:

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. Imagine being a firefighter and having a multi-alarm fire - one-alarm fires, two-alarm fires, three-alarm fires; the categories classify the seriousness of the fire, which is a threat in our case. As a Security Analyst, you will learn how to prioritise the alerts based on their level: Low, Medium, High, and Critical. Of course, it is an easy guess that you will need to start from the highest level (Critical) and work towards the bottom - Low-level alert. Having properly configured security monitoring tools in place will give you the best chance to mitigate the threat.

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.

Answer the questions below

Read the above.

No answer needed Correct Answer

Woop woop! Your answer is correct.

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

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.

managed to remediate the threat. Incident Response might take hours, days, or weeks; it all depends on the scale of the attack: did the attacker manage to exfiltrate the data? How much data does the attacker manage to exfiltrate? Did the attacker attempt to pivot into other hosts? There are many questions to ask and a lot of detection, containment, and remediation to do. We will walk you through some fundamental knowledge that every Junior (Associate) Security Analyst needs to know to become a successful Network Defender.

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.

Are you ready to immerse yourself into the role of a Junior Security Analyst for a little bit?

Answer the questions below

Click on the green View Site button in this task to open the Static Site Lab and navigate to the security monitoring tool on the right panel to try to identify the suspicious activity.

No answer needed Correct Answer

What was the malicious IP address in the alerts?

221.181.185.159 Correct Answer Hint

To whom did you escalate the event associated with the malicious IP address?

Answer format: ***** Submit

After blocking the malicious IP address on the firewall, what message did the malicious actor leave for you?

Dashboard:

Woop woop! Your answer is correct.

Operations: Information 1/3

Alert Log

Date	Message
July 16th 2021, 05:27:00:347	Successful SSH authentication attempt to port 22 from IP address 221.181.185.159
July 16th 2021, 05:25:28:235	Unauthorized connection attempt detected from IP address 221.181.185.159 to port 22
July 16th 2021, 02:43:22:456	The user John Doe logged in successfully (Event ID 4624)
July 16th 2021, 02:43:20:658	Multiple failed login attempts from John Doe

knowledge that every Junior (Associate) Security Analyst needs to know to become a successful Network Defender.

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.

Are you ready to immerse yourself into the role of a Junior Security Analyst for a little bit?

Answer the questions below

Click on the green View Site button in this task to open the Static Site Lab and navigate to the security monitoring tool on the right panel to try to identify the suspicious activity.

No answer needed Correct Answer

What was the malicious IP address in the alerts?

221.181.185.159 Correct Answer Hint

To whom did you escalate the event associated with the malicious IP address?

Will Griffin Correct Answer

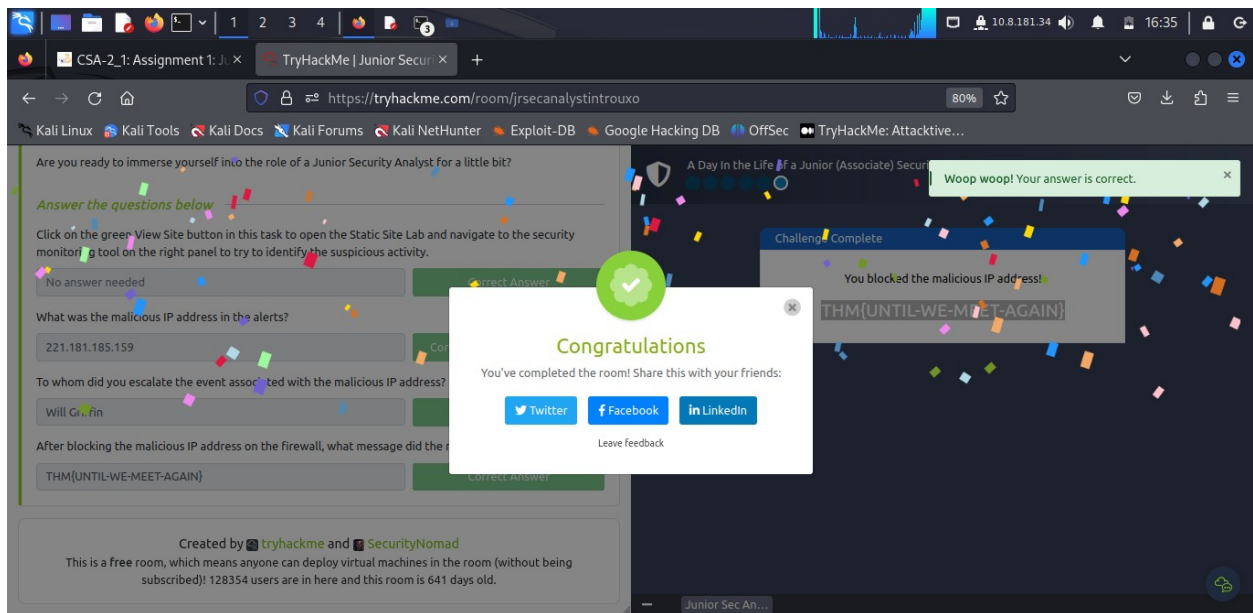
After blocking the malicious IP address on the firewall, what message did the malicious actor leave for you?

Answer format: *****(*****
Submit

Instructions: You got the permission to block the malicious IP address, and now you can proceed and implement the block rule. Block the malicious IP address on the firewall and find out what message they left for you.

Firewall Block List

Date	IP Address
July 2nd 2021, 13:27:00:948	101.34.37.231
June 30th 2021, 09:12:11:857	212.38.99.12
June 23rd 2021, 23:56:28:370	213.106.84.35



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>