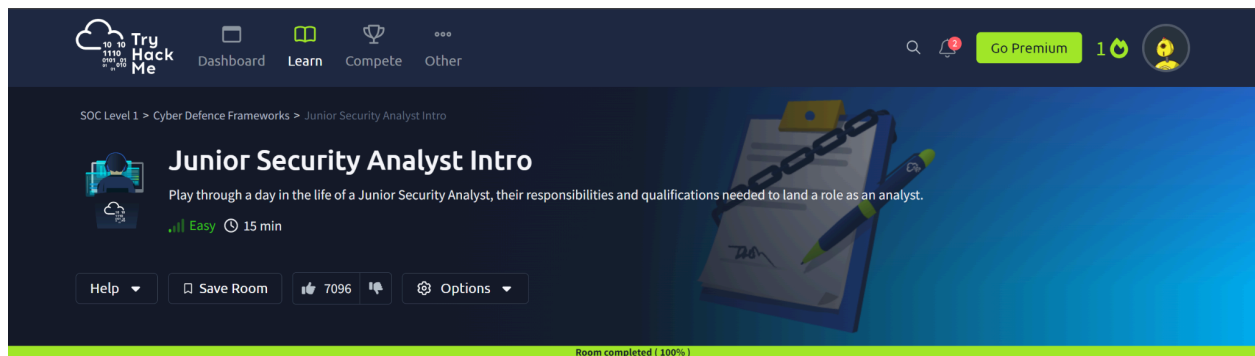


# JUNIOR SECURITY ANALYST INTRO

## ASSIGNMENT REPORT



**Peter Kinyumu,**  
**cs-sa07-24067,**  
**July 8th, 2024.**

## 1. INTRODUCTION

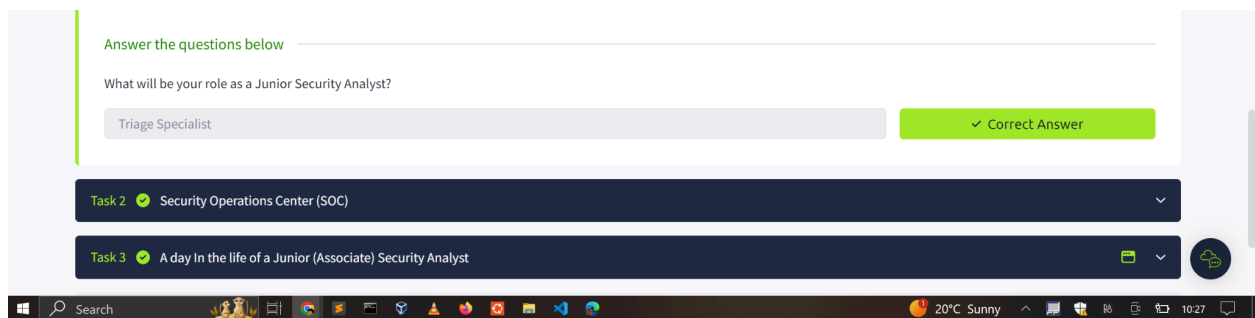
This room helps us understand the career of an Associate Security Analyst. It takes us through the responsibilities of a Junior Security Analyst, the required qualifications, the three-tiered model of the Security Operation Center, the responsibilities of SOC, and finally, a day in the life of a Junior Security Analyst.

## 2. ANSWERS TO QUESTIONS

### A career as a Junior(Associate) Security Analyst

#### a. What will be your role as a Junior Security Analyst?

- **Triage Specialist**



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

#### a. What was the malicious IP address in the alerts?

- **221.181.185.159**

CSA2-2024: Assignment 1: Junior Security Analyst Intro

tryhackme.com/room/jrsecanalystintro

Crackmes Gmail YouTube Maps

Go Premium 1

View Site

No answer needed Complete

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?

Answer format: \*\*{\*\*\*\*\*} Submit

See the highlighted IP from the log message.  
Created by

Alert Log

Date	Message
April 16th 2024, 05:27:00:347	Successful SSH authentication attempt to port 22 from IP address 221.181.185.159
April 16th 2024, 05:25:28:235	Unauthorized connection attempt detected from IP address 221.181.185.159 to port 22
April 16th 2024, 02:43:22:456	The user John Doe logged in successfully (Event ID 4624)
April 16th 2024, 02:43:20:658	Multiple failed login attempts from John Doe
April 16th 2024, 02:30:20:215	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

Junior Sec Analyst Intro

CSA2-2024: Assignment 1: Junior Security Analyst Intro

tryhackme.com/room/jrsecanalystintro

Crackmes Gmail YouTube Maps

Go Premium 1

View Site

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?

Answer format: \*\*{\*\*\*\*\*} Submit

Created by

A Day In the Life of a Junior (Associate) Security Analyst

https://ip-scanner.thm/search

IP-SCANNER.THM

221.181.185.159 was found in our database!

Confidence of the IP being malicious is 100%

Malicious

ISP	China Mobile Communications Corporation
Domain Name	chinamobiletd.thm
Country	China
City	Zhenjiang, Jiangsu

Next

Junior Sec Analyst Intro

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

- Will Griffin

CSA2-2024: Assignment 1: Junior Security Analyst | TryHackMe | Junior Security Analyst Intro

tryhackme.com/r/room/jrsecanalystintrouxo

Crackmes Gmail YouTube Maps

Go Premium 1

View Site

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

Escalate to SOC lead

Created by

Tru Hack Me

A Day In the Life of a Junior (Associate) Security Analyst

Choose to whom you would escalate this event?

Dominick Nash Sales Executive

Nadia Watson Security Consultant

Carolyn Stone Information Security Architect

Will Griffin SOC Team Lead

Choose Staff Member

Junior Sec Analyst Intro

17°C Sunny 08:49

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

● THM{ UNTIL-WE-MEET-AGAIN }

CSA2-2024: Assignment 1: Junior Security Analyst | TryHackMe | Junior Security Analyst Intro

tryhackme.com/r/room/jrsecanalystintrouxo

Crackmes Gmail YouTube Maps

Go Premium 1

View Site

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

Block IP address

Created by

Me

https://firewallInternal

Firewall Block List

Block List

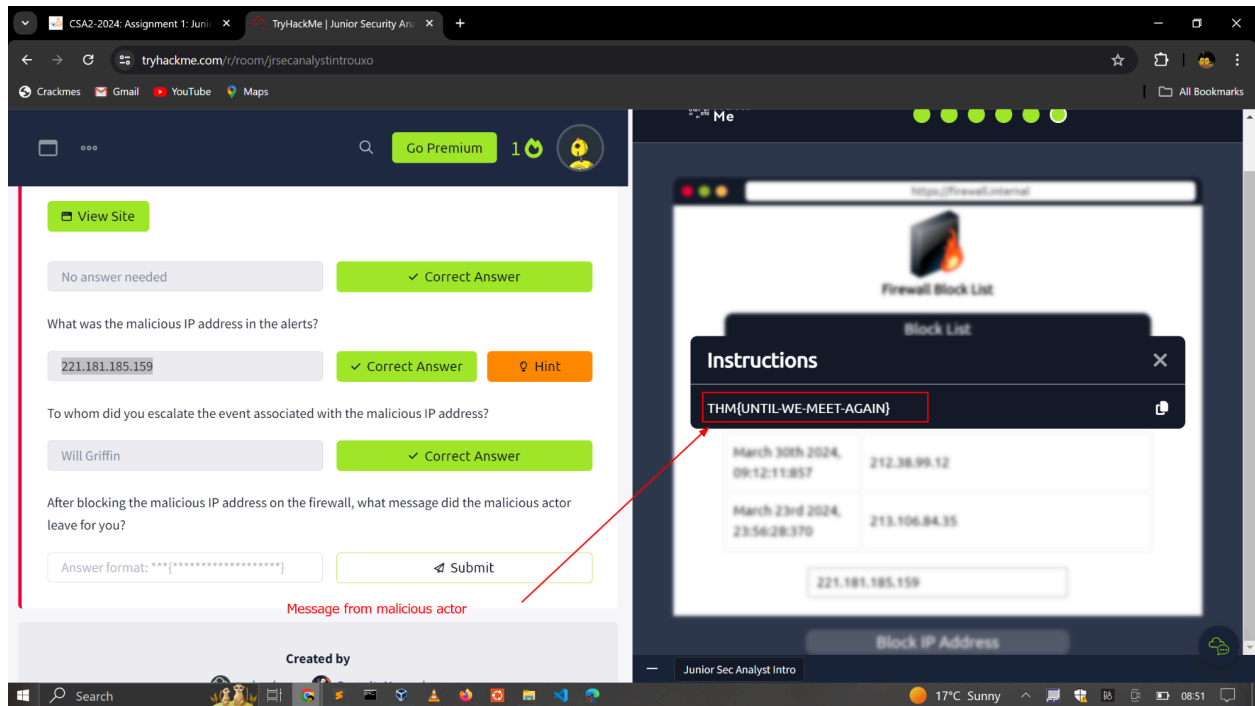
Date	IP Address
April 2nd 2024, 13:27:00:948	101.34.37.231
March 30th 2024, 09:12:11:857	212.38.99.12
March 23rd 2024, 23:56:28:370	213.106.84.35

221.181.185.159

Block IP Address

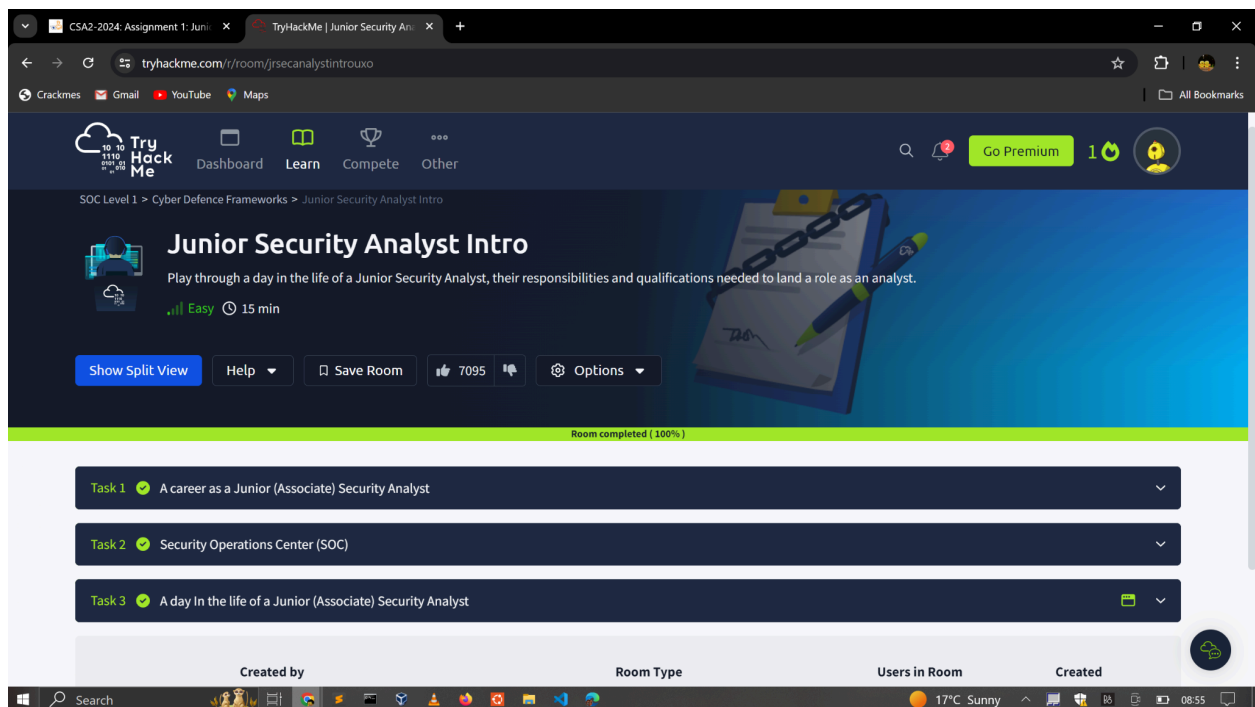
Junior Sec Analyst Intro

17°C Sunny 08:52



### 3. MODULE COMPLETION

<https://tryhackme.com/p/c1ph3rbnuk>



## **4. CONCLUSION**

This assignment has helped me understand the role of a Junior Security Analyst, from the responsibilities involved, like monitoring and investigating alerts, to required qualifications, such as Networking and Operating systems. I also enjoyed the practical tour in “A day in the life of a Junior Security Analyst”. I now have a solid grasp of what to expect when working as an Associate Security Analyst.