cs-sa07-24019
John_Mbithi_Mutave

Junior Security Analyst Intro

Introduction

Becoming a Junior Security Analyst marks the entry point into the dynamic and critical field of cybersecurity. This role is pivotal in safeguarding organizational assets, responding to threats, and ensuring resilience against cyber attacks. Below, we explore a typical day in the life of a Junior Security Analyst, their key responsibilities, and the qualifications necessary to excel in this role.

Responsibilities of a Junior Security Analyst

As a Junior Security Analyst, your daily responsibilities revolve around monitoring, analyzing, and responding to security incidents within an organization's network. Key tasks include:

Monitoring Security Systems: Continuously monitor security systems such as SIEM (Security Information and Event Management) tools, IDS (Intrusion Detection Systems), and firewalls to detect potential security breaches and suspicious activities.

Incident Response: Quickly respond to and investigate security incidents. This involves analyzing alerts, determining the scope and impact of incidents, and taking appropriate mitigation actions to contain and eradicate threats.

Vulnerability Assessment: Conduct regular vulnerability assessments and penetration testing to identify weaknesses in systems and networks. Recommend and implement corrective actions to strengthen security posture.

Security Awareness: Promote security awareness among employees through training sessions and communications, helping to reduce human error and improve overall security hygiene.

Documentation and Reporting: Maintain detailed logs and documentation of security incidents, investigations, and remediation efforts. Prepare reports for management and stakeholders outlining security risks and recommended improvements.

Qualifications Needed

To succeed as a Junior Security Analyst, certain qualifications and skills are essential:

Educational Background: A degree in Computer Science, Information Technology, Cybersecurity, or a related field provides foundational knowledge. Certifications such as CompTIA Security+, CEH (Certified Ethical Hacker), or equivalent demonstrate expertise.

Technical Skills: Proficiency in using security tools like SIEM, IDS/IPS, antivirus software, and network monitoring tools is crucial. Understanding of networking protocols, operating systems (Windows, Linux), and cloud environments (AWS, Azure) is beneficial.

Analytical Skills: Ability to analyze and interpret complex data from various sources to identify security threats and vulnerabilities.

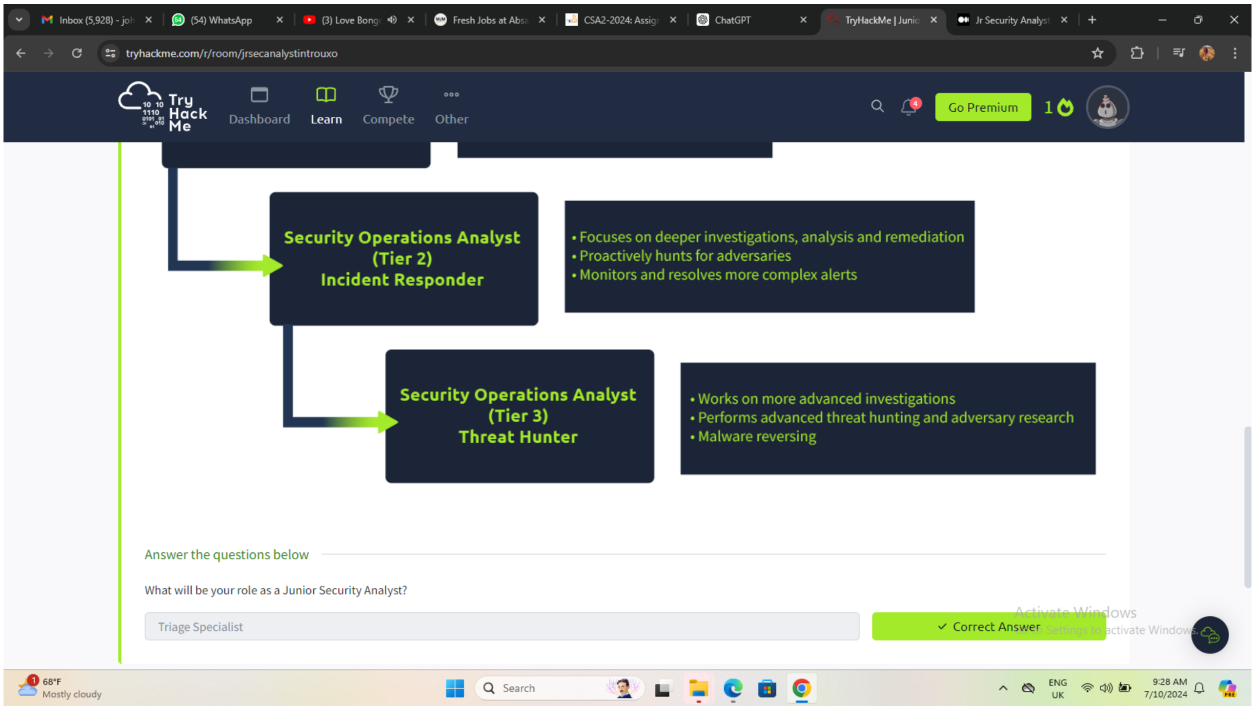
Communication Skills: Effective communication is essential for collaborating with team members, documenting findings, and presenting security reports to non-technical stakeholders.

Problem-Solving Abilities: A proactive approach to problem-solving and the ability to make quick, informed decisions under pressure are vital traits.

Overview of the task with screenshots

cs-sa07-24019

John_Mbithi_Mutave



Security Operations Analyst (Tier 2) Incident Responder

- Focuses on deeper investigations, analysis and remediation
- Proactively hunts for adversaries
- Monitors and resolves more complex alerts

Security Operations Analyst (Tier 3) Threat Hunter

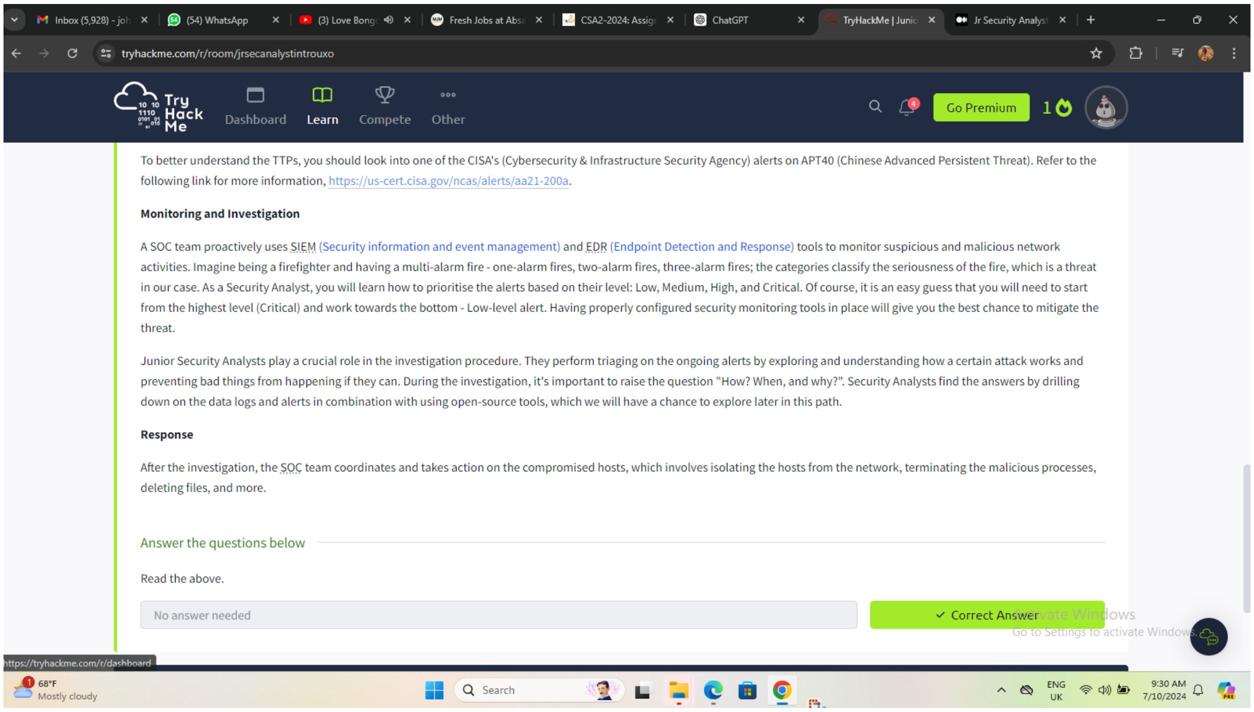
- Works on more advanced investigations
- Performs advanced threat hunting and adversary research
- Malware reversing

Answer the questions below

What will be your role as a Junior Security Analyst?

Triage Specialist

✓ Correct Answer



To better understand the TTPs, you should look into one of the CISA's (Cybersecurity & Infrastructure Security Agency) alerts on APT40 (Chinese Advanced Persistent Threat). Refer to the following link for more information, https://us-cert.cisa.gov/ncas/alerts/aa21-200a.

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. 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

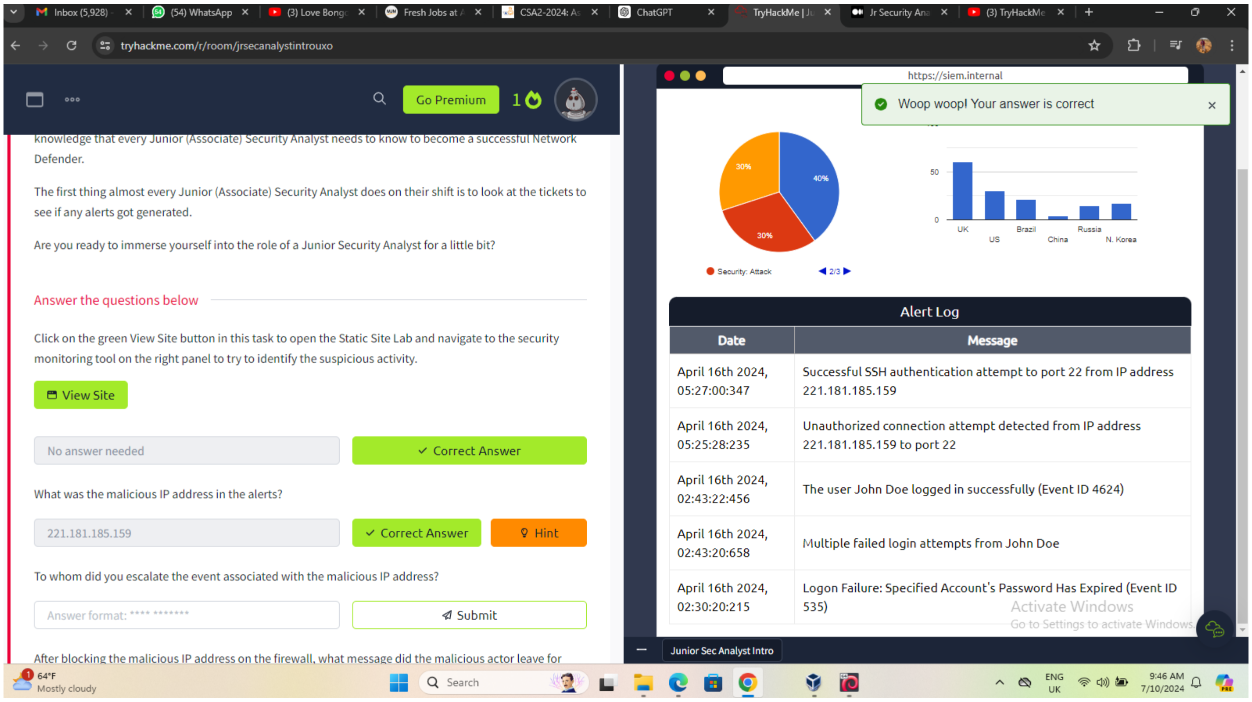
Read the above.

No answer needed

✓ Correct Answer

cs-sa07-24019

John_Mbithi_Mutave



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.

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?

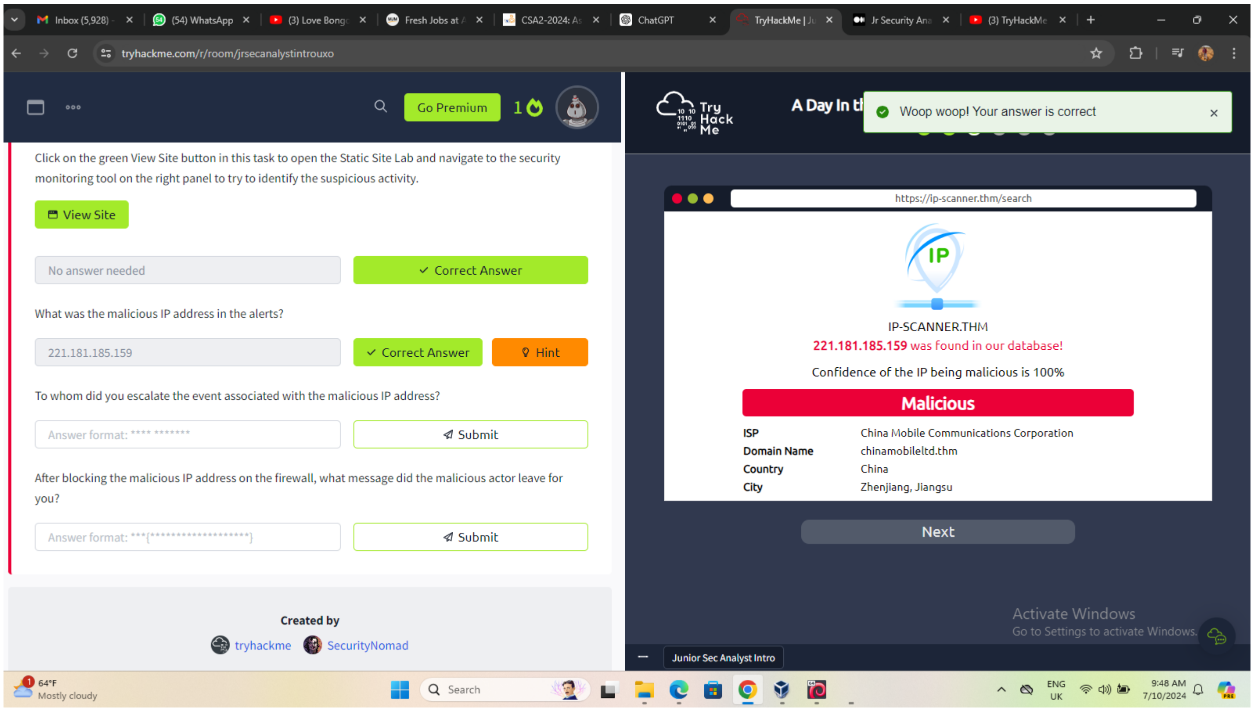
Answer format: **** *******

Submit

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

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)



tryhackme.com/r/room/jrsecanalystintrouxo
Go Premium
Try Hack Me
A Day In tl
Woop woop! Your answer is correct
https://ip-scanner.thm/search
IP
Next
Junior Sec Analyst Intro

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.

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

tryhackme SecurityNomad

IP-SCANNER.THM

221.181.185.159 was found in our database!

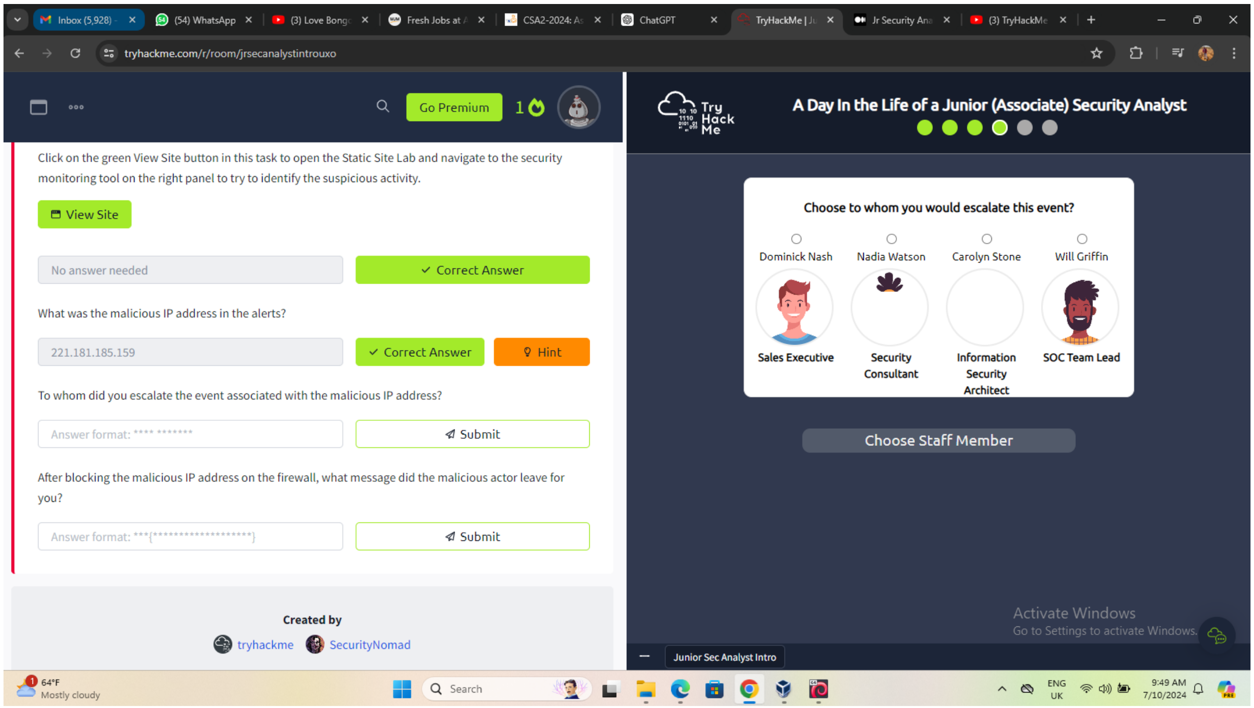
Confidence of the IP being malicious is 100%

Malicious

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

cs-sa07-24019

John_Mbithi_Mutave



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.

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

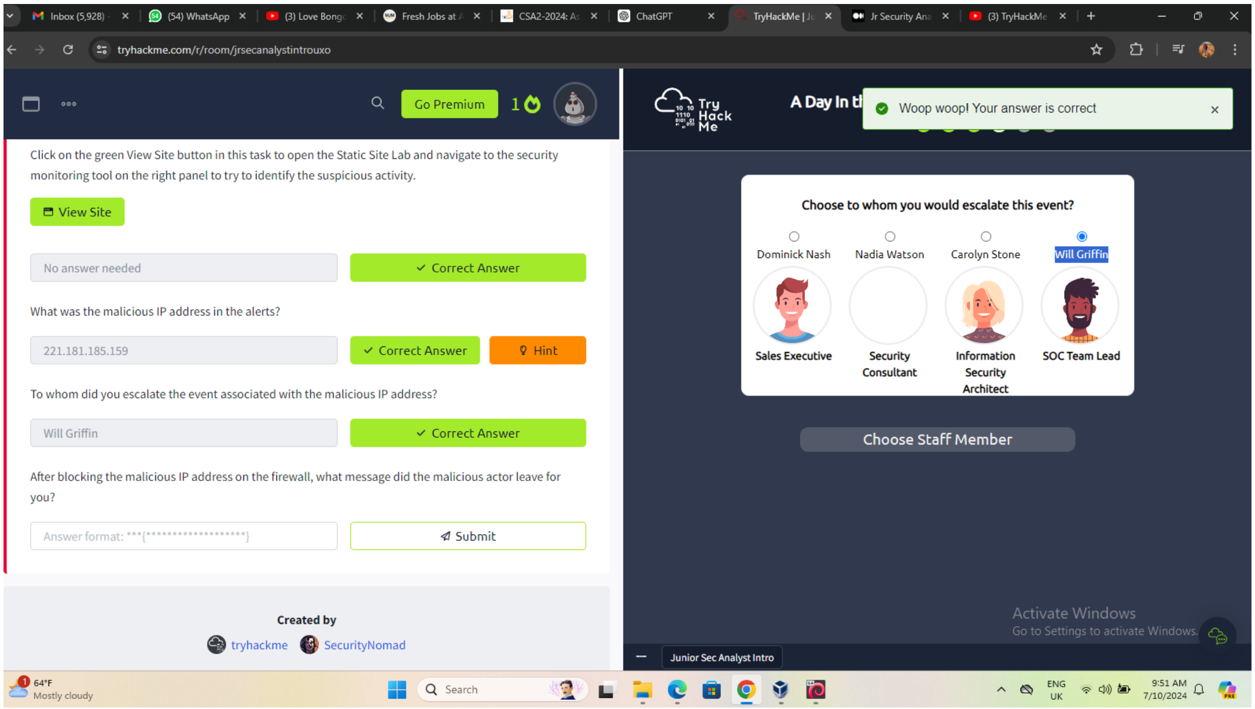
Created by

tryhackme SecurityNomad

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

Choose to whom you would escalate this event?

○ Dominick Nash ○ Nadia Watson ○ Carolyn Stone ○ Will Griffin



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.

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

Created by

tryhackme SecurityNomad

A Day In th

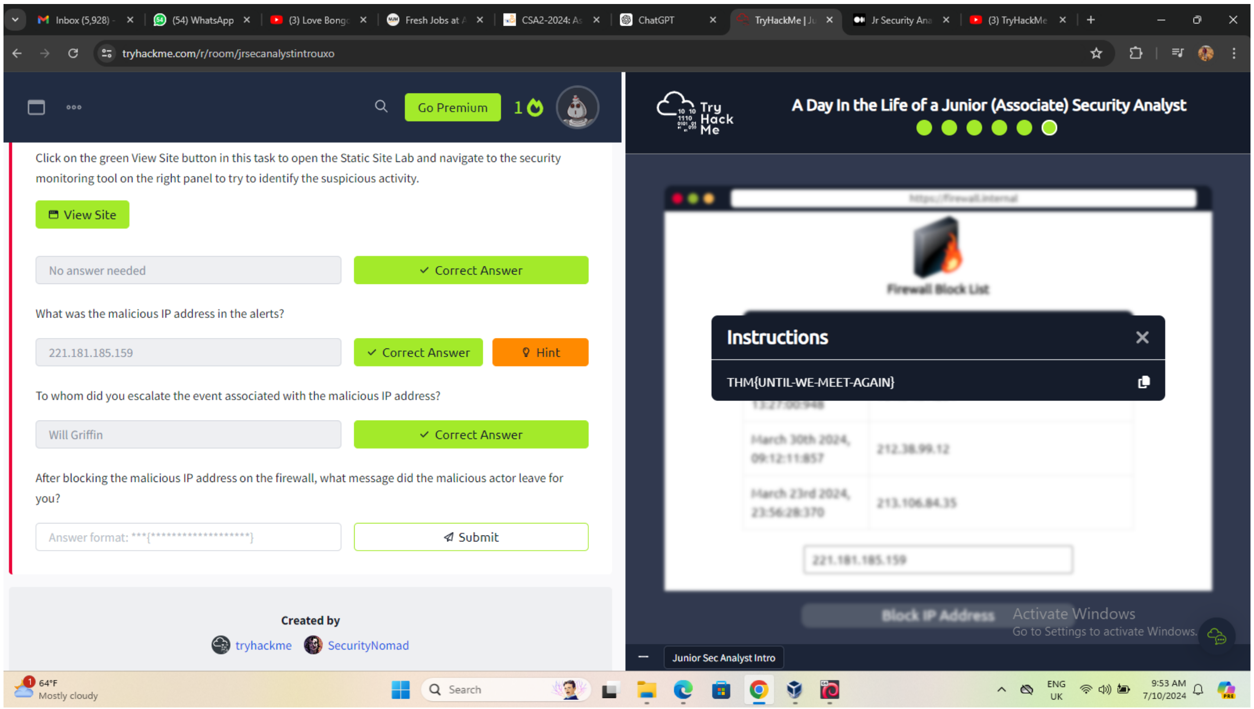
Woop woop! Your answer is correct

Choose to whom you would escalate this event?

○ Dominick Nash ○ Nadia Watson ○ Carolyn Stone ● Will Griffin

cs-sa07-24019

John_Mbithi_Mutave



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.

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

Created by

tryhackme SecurityNomad

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

https://firewall.internal

Firewall Block List

Instructions

THM{UNTIL-WE-MEET-AGAIN}

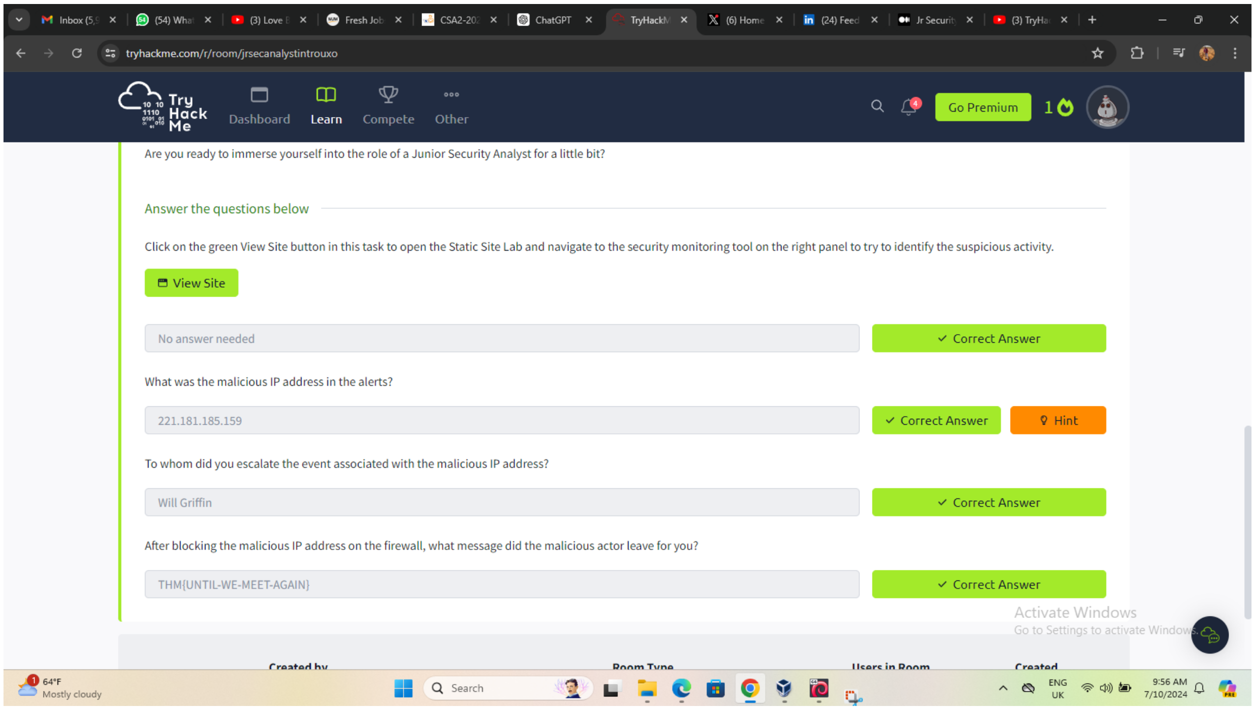
13:27:00:948	
March 30th 2024, 09:12:11:857	212.38.99.12
March 23rd 2024, 23:56:28:370	213.106.84.35

221.181.185.159

Block IP Address

Activate Windows
Go to Settings to activate Windows.

Junior Sec Analyst Intro



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.

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?

THM{UNTIL-WE-MEET-AGAIN}

✓ Correct Answer

Activate Windows
Go to Settings to activate Windows

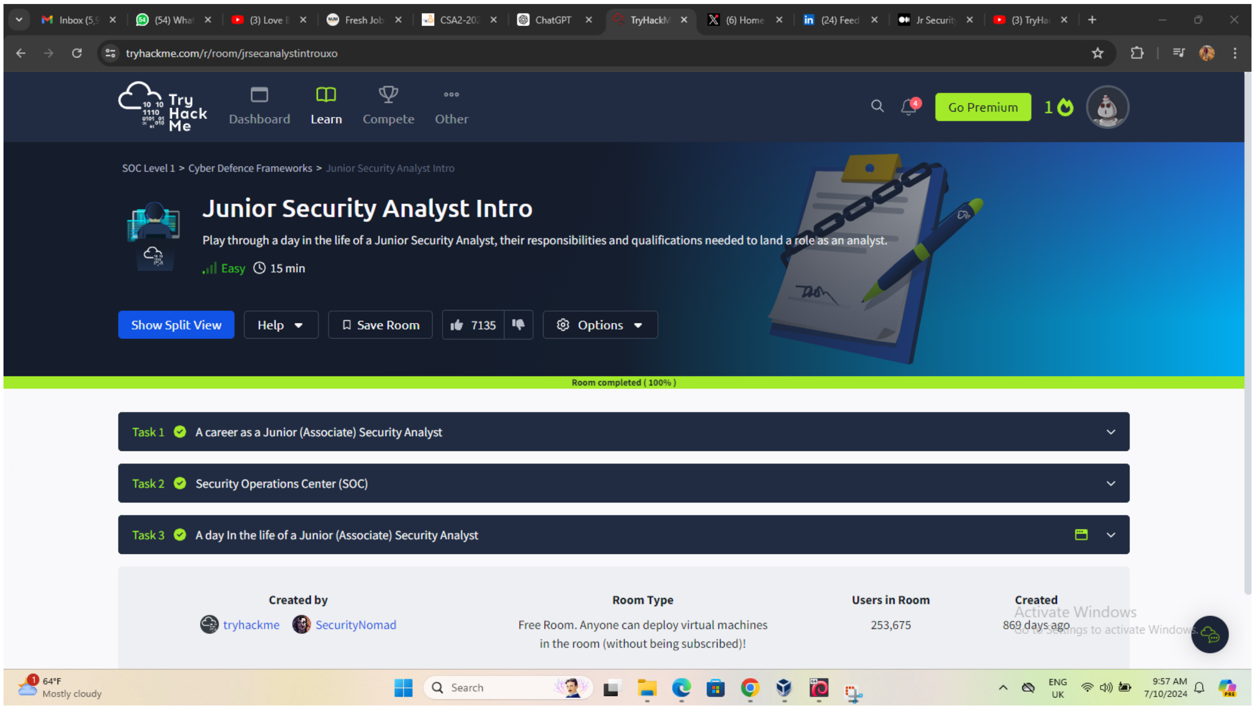
Created by

Room Type

Users in Room

Created

cs-sa07-24019
John_Mbithi_Mutave



SOC Level 1 > Cyber Defence Frameworks > Junior Security Analyst Intro

Junior Security Analyst Intro

Play through a day in the life of a Junior Security Analyst, their responsibilities and qualifications needed to land a role as an analyst.

Easy 15 min

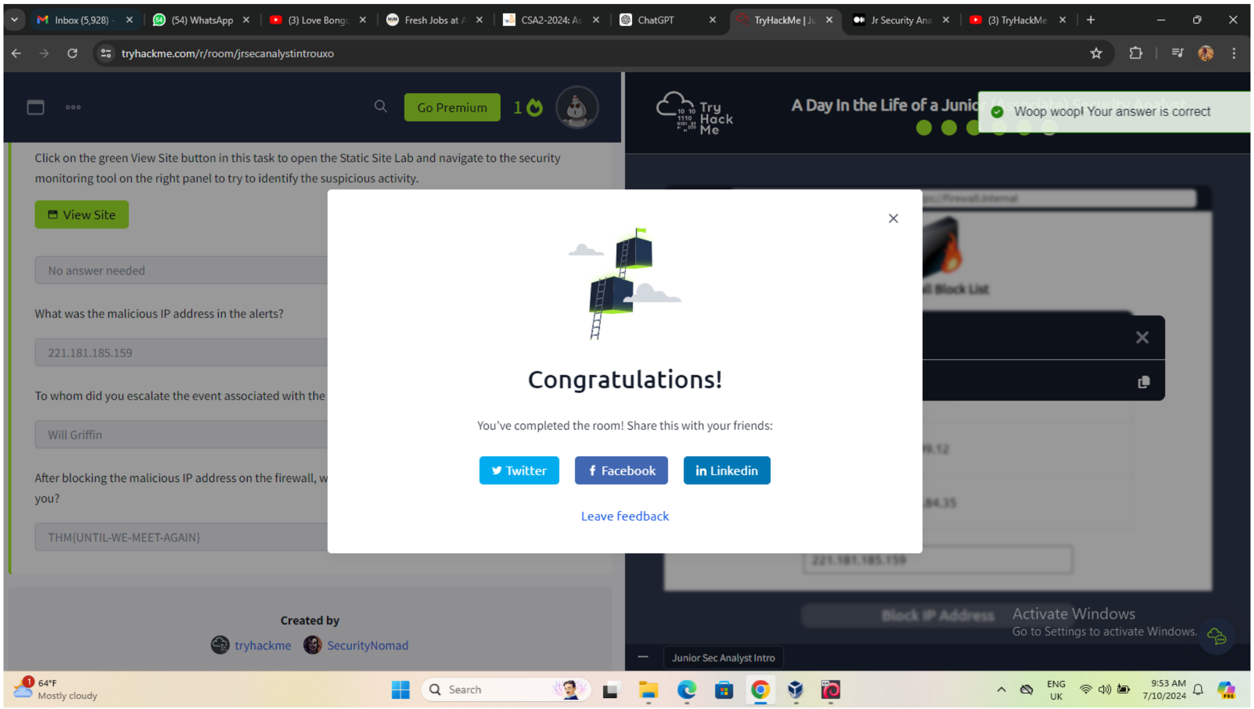
Room completed (100%)

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

Task 2 Security Operations Center (SOC)

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

Created by	Room Type	Users in Room	Created
tryhackme SecurityNomad	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	253,675	869 days ago



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

What was the malicious IP address in the alerts?

221.181.185.159

To whom did you escalate the event associated with the

Will Griffin

After blocking the malicious IP address on the firewall, w you?

THM{UNTIL-WE-MEET-AGAIN}

Congratulations!

You've completed the room! Share this with your friends:

Woop woop! Your answer is correct

Shareable Link - https://tryhackme.com/r/room/jrsecanalystintrouxo

Conclusion

In conclusion, a career as a Junior Security Analyst offers an exciting opportunity to contribute to the protection of sensitive data and critical infrastructure against evolving cyber threats. With the right blend of technical skills, educational background, and a passion for cybersecurity, aspiring analysts can make significant contributions to organizational security posture. Continuous learning and staying updated with industry trends are key to advancing in this dynamic field.