



Eric Mwenda

Junior Security Analyst Intro

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



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

An overview of the Security Operations Center (SOC) Three-Tier Model:



Answer the questions below

What will be your role as a Junior Security Analyst?

Triage Specialist

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.

McAfee's definition of a SOC, "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". The number of people working in the SOC can vary depending on the organisation's size.



Preparation and Prevention

As a Junior Security Analyst, you should stay informed of the current cyber security threats. It's crucial to detect and hunt threats, work on a security roadmap to protect the organisation, and be ready for the worst-case scenario.

Twitter and Feedly can be great resources to keep up 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.

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.

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

To be in the frontline is not always easy and can be very challenging as you will be working with various log sources from different tools that we will walk you through in this path. You will get a chance to monitor the network traffic, including IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) alerts, suspicious emails, extract the forensics data to analyze and detect the potential attacks, use open-source intelligence to help you make the appropriate decisions on the alerts.

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

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.

DONE

What was the malicious IP address in the alerts?

Ans: 221.181.185.159

the alerts.

One of the most exciting and rewarding things is when you are finished working on an incident and have 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 Completed

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](#) and [SecurityNomad](#)

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 174016 users

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

Woop woop! Your answer is correct.

Instructions

Inspect the alerts in your SIEM dashboard. Find the malicious IP address from the alerts, make note of it, and then click on the alert to proceed.

<https://siem.internal>

Operations: Information 40 (40%)

Countries

UK US Brazil China N. Korea

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)

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

Ans: will Griffin

Reason being he is the SOC Team Lead

the alerts.

One of the most exciting and rewarding things is when you are finished working on an incident and have 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 Completed

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](#) and [SecurityNomad](#)

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 174016 users

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

Instructions

We shouldn't worry too much if it was a failed authentication attempt, but you probably noticed the successful authentication attempt from the malicious IP address. Let's declare a small incident event and escalate it. There is some great staff working at the company, but you wouldn't want to escalate this to the wrong person who is not in charge of your team or department.

Choose to whom you would escalate this event?

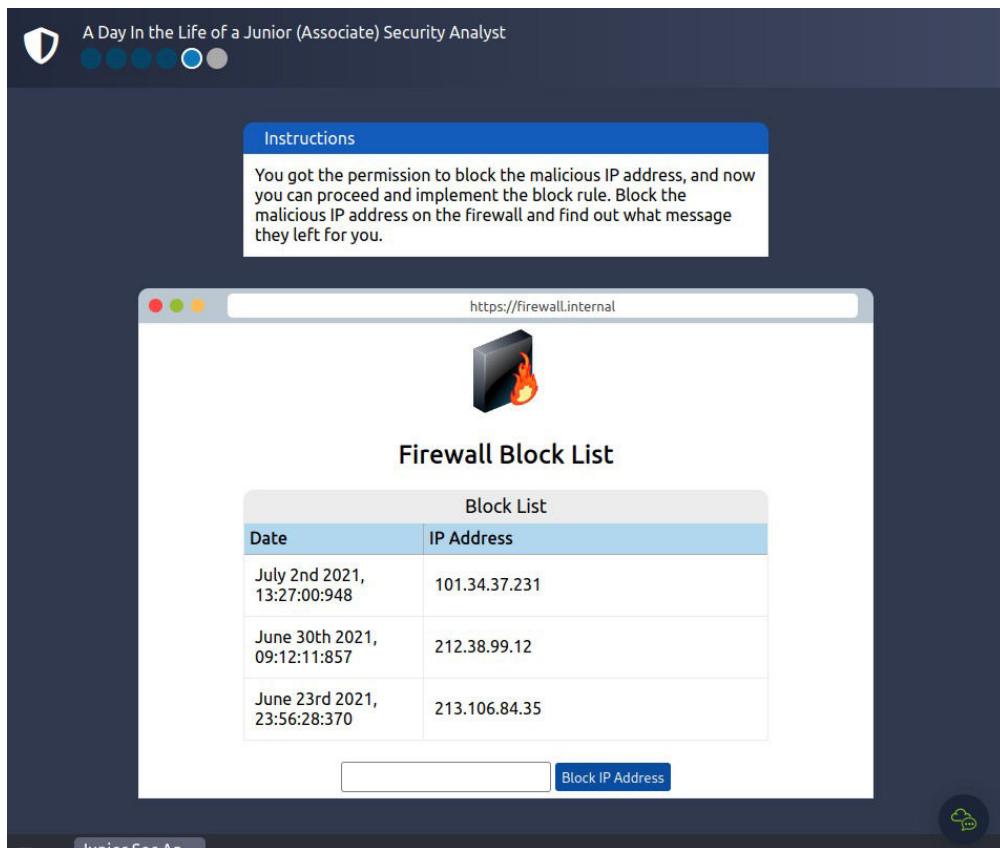
☐ Dominick Nash ☐ Nadia Watson ☐ Carolyn Stone ☒ Will Griffin

Sales Executive **Security Consultant** **Information Security Architect** **SOC Team Lead**

Choose Staff Member

After blocking the malicious IP address on the firewall, what message did the malicious actor leave for you? **Ans: THM{UNTIL-WE-MEET-AGAIN}**

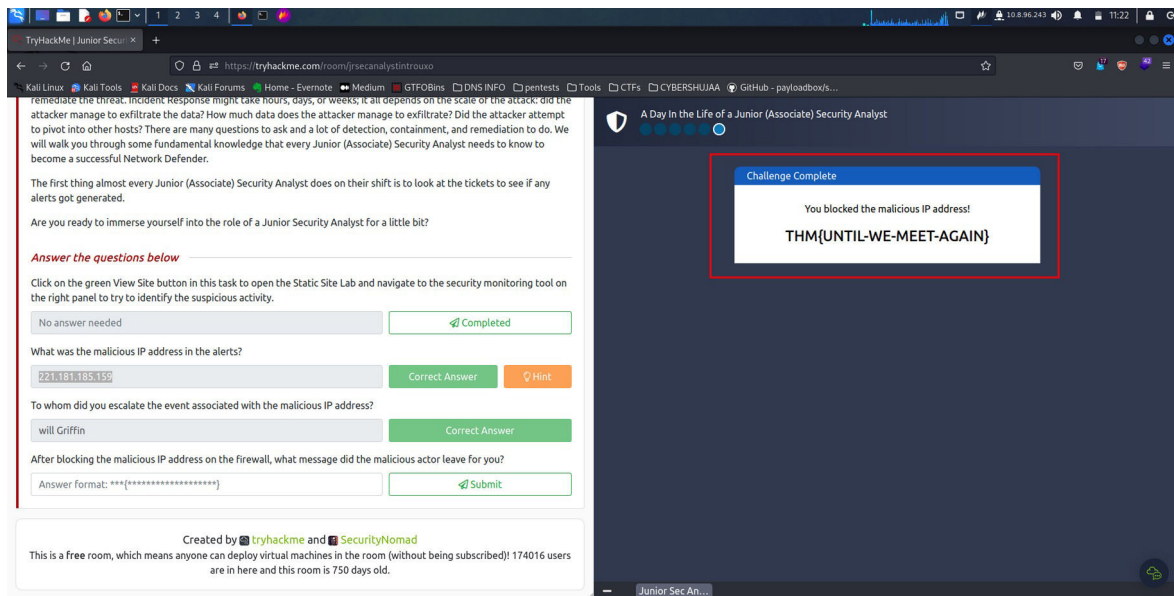
After escalating the event associated with the malicious IP address to Will Griffin, I was redirected to this page.



To block this the malicious IP address I had to add it on the input bar and click the Block IP Address.



By clicking the Block IP Address, I got the sent message the task demands. THM{UNTIL-WE-MEET-AGAIN}



Conclusion.

The Junior Security Analyst Intro room has introduced general tasks that a junior SOC analyst is likely to come across, such as monitoring the network and finding the unauthorized users and taking the necessary precaution of blocking them from the network. With this knowledge I believe I have a foundation of what to expect as a SOC analyst. Overall, this room serves as a good starting point for beginners in the field of SOC Analysis, fostering a solid understanding of fundamental security concepts and practices done in this centers.

Thank You.