Junior Security Analyst Intro: TryHackMe

Name: Daniel Mwendwa Mwithui

ADM NO. CS-SA04-23080

Program: Security Analyst

Date of submission:28th July2023

Introduction

Welcome to the junior security analyst training module on TryHackMe! In this assignment, we will dive into the world of cybersecurity and explore the essential roles and responsibilities of a security analyst within a Security Operations Center (SOC). Throughout this module, we will discuss the key functions of Tier 1 (Triage), Tier 2 (Incident Responder), and Tier 3 (Threat Hunter) personnel. By the end of this assignment, you will gain a comprehensive understanding of the critical tasks involved in each role, and how they collectively contribute to strengthening an organization's cybersecurity defenses.

Security operation Center

Security Operations Center (SOC) is a team or a facility in an organization responsible for investigating, monitoring, preventing, and responding to cybersecurity threats. Their main job is to detect and respond to any potential security incidents or breaches to protect the organization's data and systems.

The SOC team is divided into the following three TIERS

1. **Tier 1**: The Tier 1 team members are often referred to as "Triage Analysts" or "Security Analysts." Their primary responsibility is to be the first line of defense when it comes to monitoring security alerts and handling initial incidents. This is where junior security analysts lie. They are at the beginner level

Responsibilities:

- Monitoring: They constantly monitor security alerts and notifications from various security tools, such as intrusion detection systems and firewalls.

- Alert Triage: They assess the alerts and categorize them based on severity and potential impact to determine which incidents require immediate attention.
- Incident Identification: Tier 1 analysts identify and analyze security incidents that could indicate potential threats or breaches.
- Basic Troubleshooting: They perform basic incident analysis and attempt to resolve straightforward security issues using predefined procedures and playbooks.
- Escalation: If an incident is beyond their expertise or requires more in-depth investigation, they escalate it to Tier 2 for further analysis and response.

2. **Tier 2**: Tier 2 team members are often referred to as "Incident Responders" or "Security Engineers." Their role is to provide more specialized support in incident investigation, containment, and mitigation.

Responsibilities:

- Incident Investigation: Tier 2 analysts conduct in-depth investigations of escalated incidents to understand the root cause and extent of the compromise.
- Containment and Eradication: They work to contain the incident, prevent it from spreading further, and remove the threat from affected systems.
- Advanced Analysis: These analysts possess a deeper understanding of cybersecurity threats and are capable of analyzing more complex attack vectors.
- Incident Documentation: They document the entire incident response process, detailing the actions taken and the lessons learned for future reference.

- Collaboration: Tier 2 teams often collaborate with Tier 1 analysts and communicate with external stakeholders, such as legal, compliance, or law enforcement agencies.

3. **Tier 3**: The Tier 3 team members are known as "Threat Hunters" or "Security Researchers." Their primary focus is on proactively searching for advanced and persistent threats that may have evaded traditional security measures.

Responsibilities:

- Proactive Threat Hunting: Tier 3 analysts continuously search for signs of advanced threats and adversaries within the network using various techniques and threat intelligence.

- Incident Response Optimization: They contribute to improving incident response processes, tools, and playbooks based on their findings and experience.

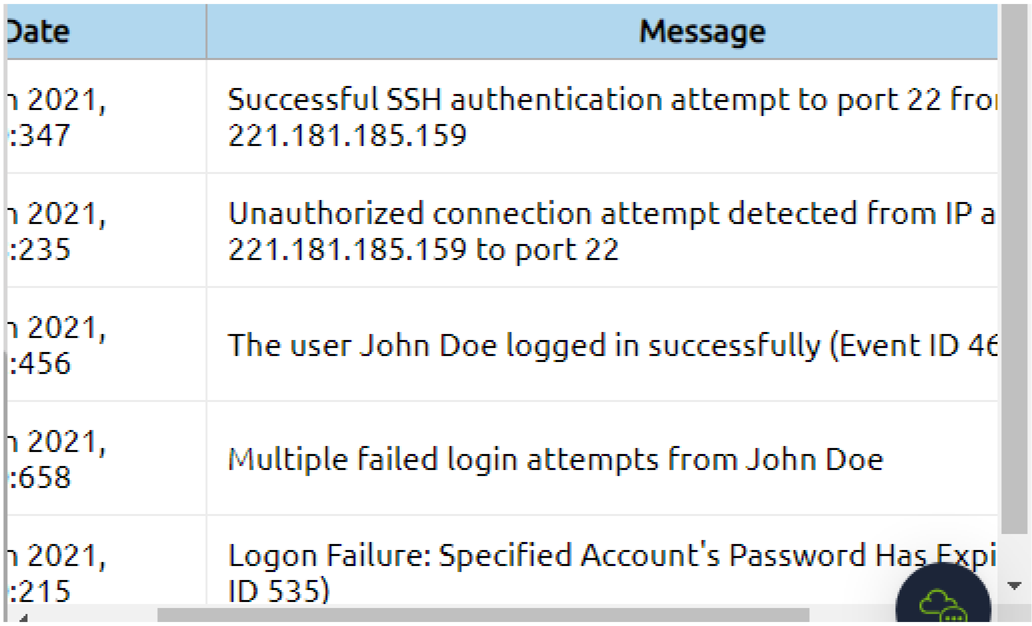
- Malware Analysis: Threat hunters often conduct in-depth malware analysis to understand the behavior and capabilities of new threats.

- Threat Intelligence Integration: They incorporate threat intelligence from various sources into the SOC's detection and response capabilities.

- Knowledge Sharing: Tier 3 personnel often share their findings with Tier 1 and Tier 2 teams to enhance their understanding of emerging threats.

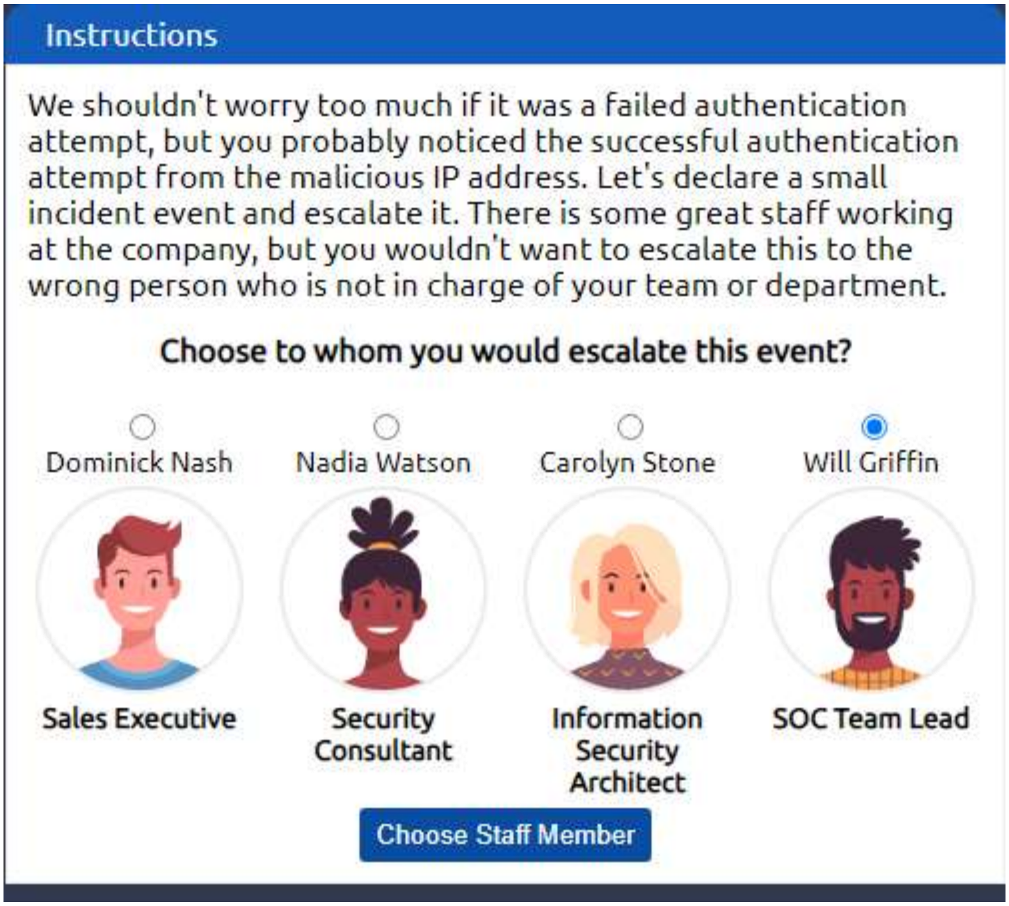
Module completion

To complete this module, we are going to use attached security monitoring tool to answer the questions that follow. See the screenshots below. From the alert log, we are going to select the alert with unauthorized connection attempt and select it.



Date	Message
n 2021, :347	Successful SSH authentication attempt to port 22 fro 221.181.185.159
n 2021, :235	Unauthorized connection attempt detected from IP a 221.181.185.159 to port 22
n 2021, :456	The user John Doe logged in successfully (Event ID 4€
h 2021, :658	Multiple failed login attempts from John Doe
h 2021, :215	Logon Failure: Specified Account's Password Has Expi ID 535)

To escalate the incidence, we should consider a person in the above tier like tier 2 security engineer or threat hunters tier 3. From the list provided, security lead is the most appropriate staff to report the incidence to.



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?

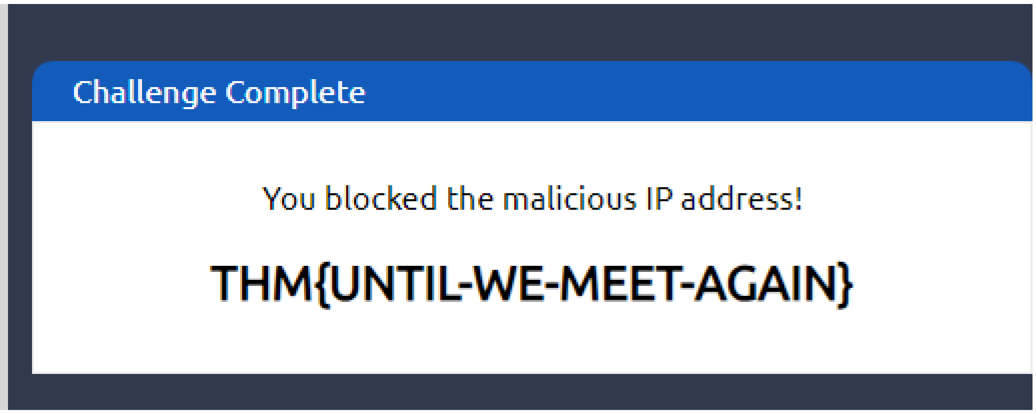
○ Dominick Nash — Sales Executive

○ Nadia Watson — Security Consultant

○ Carolyn Stone — Information Security Architect

● Will Griffin — SOC Team Lead

Now let us go on and block the IP address.



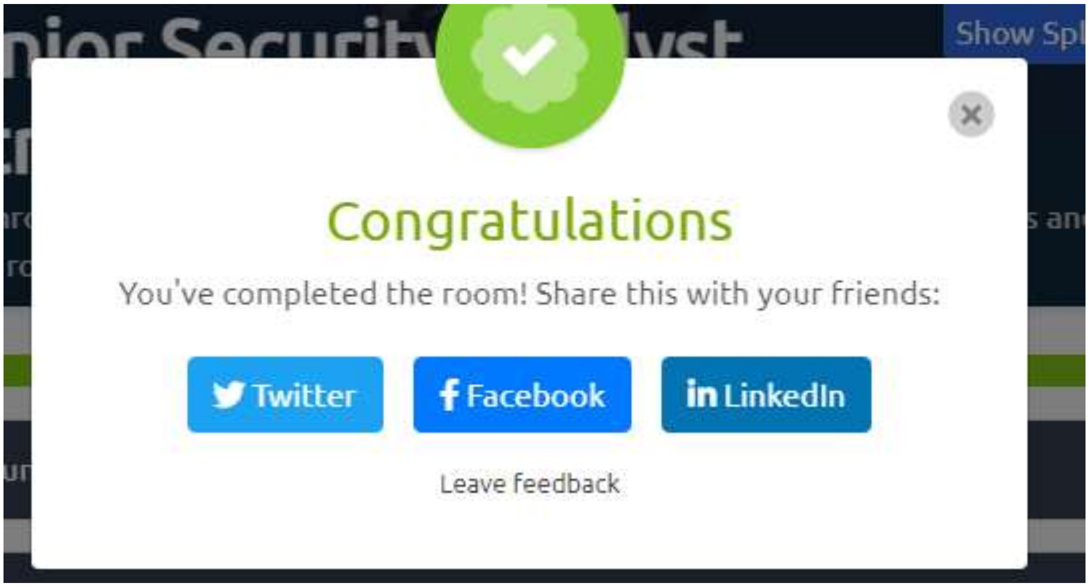
Challenge Complete

You blocked the malicious IP address!

THM{UNTIL-WE-MEET-AGAIN}

Here is completion for this module and link

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



Congratulations

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

Conclusion

Completing this junior security analyst training module has been an enlightening experience. We have learned about the vital roles of Tier 1 (Triage), Tier 2 (Incident Responder), and Tier 3 (Threat Hunter) personnel within a Security Operations Center. Understanding the distinct responsibilities of each tier has given us valuable insights into how security analysts work collaboratively to detect, respond, and proactively defend against cyber threats. As we move forward in our cybersecurity journey, this knowledge will undoubtedly play a crucial role in securing digital infrastructures and safeguarding sensitive information. With continued practice and learning, we can contribute effectively to the ever-evolving landscape of cybersecurity and SOC specifically.