

# Junior Security Analyst Intro

## Introduction

In today's digital landscape, organizations face an ever-evolving array of cyber threats that can compromise sensitive data, disrupt operations, and inflict financial and reputational damage. To counter these threats, many organizations have established Security Operation Centers (SOCs) as a centralized hub for monitoring, detecting, analyzing, and responding to cybersecurity incidents. A SOC plays a critical role in an organization's defense strategy by providing continuous surveillance and leveraging advanced technologies and skilled personnel to safeguard information assets.

The primary objective of a SOC is to ensure the confidentiality, integrity, and availability of an organization's information systems. By integrating people, processes, and technology, a SOC can identify and mitigate security threats in real-time, thereby minimizing potential damage and ensuring swift recovery from incidents. This report delves into the various aspects of SOC operations, including its functions, types, models, and best practices, highlighting the importance of a well-structured SOC in strengthening an organization's cybersecurity posture. Tasks involved in this room were few and here is how I went about them.

What will be your role as a Junior Security Analyst?

Triage Specialist

✓ Correct

After reading through the notes within the room, the role of a Junior Security Analyst will be a Triage specialist where he or she will spend a lot of the time triaging the event logs and alerts



In the Junior Security Analyst role, you will be a Triage Specialist. You will spend a lot of time triaging or monitoring the event logs and alerts.

The responsibilities for a Junior Security Analyst or Tier 1 SOC Analyst include:

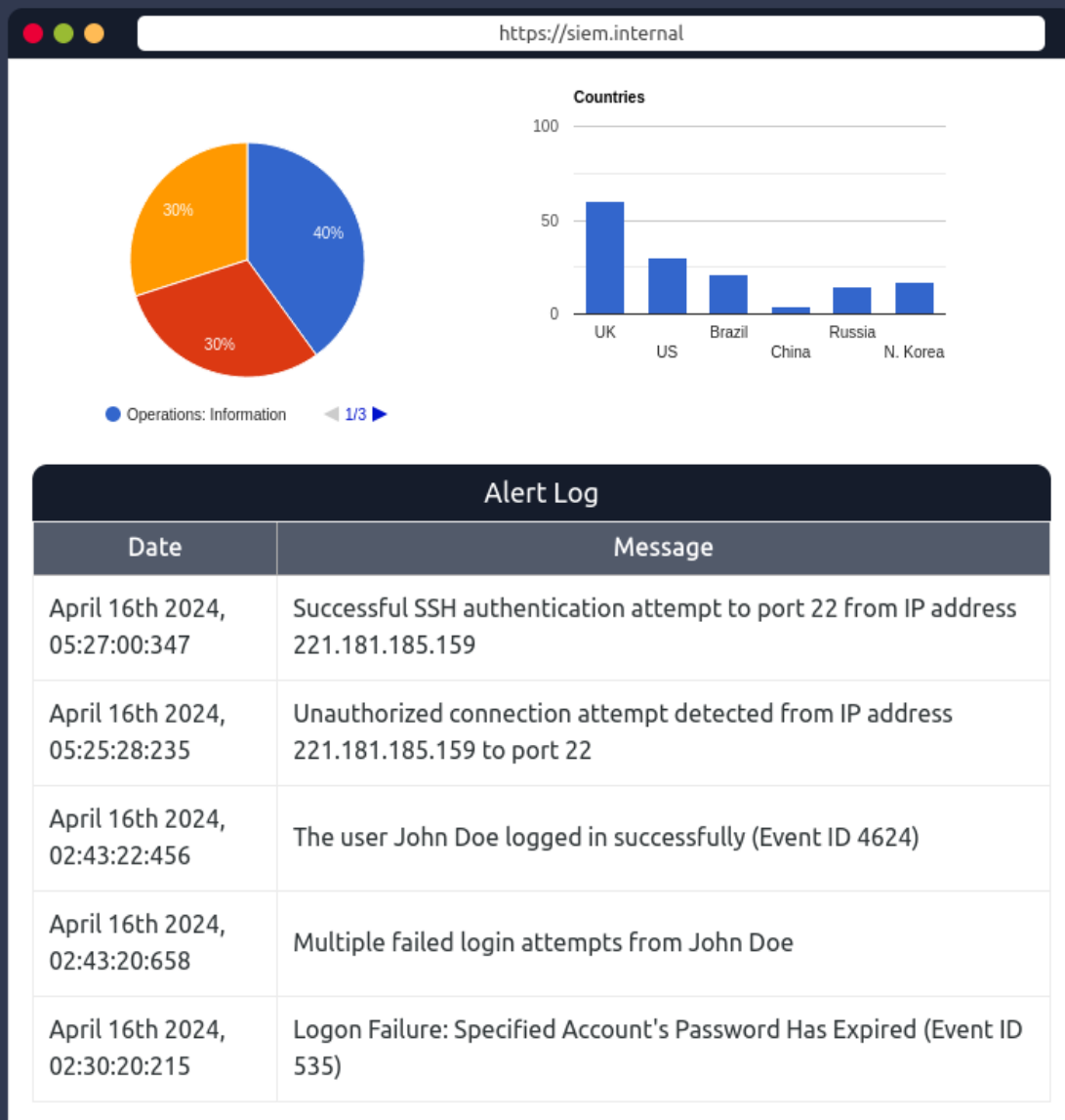
- Monitor and investigate the alerts (most of the time, it's a 24x7 SOC operations environment)
- Configure and manage the security tools
- Develop and implement basic IDS (Intrusion Detection System) signatures
- Participate in SOC working groups, meetings

What was the malicious IP address in the alerts?

221.181.185.159

✓ Correct

Going through the event logs, on April 16th 2024 there was an unauthorized connection attempt detected as seen from the alert log image below.







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

Will Griffin

✓ Correct

As seen from the image below, I escalated this event to Will Griffin who is the SOC Team Lead.

Choose to whom you would escalate this event?

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Dominick Nash	Nadia Watson	Carolyn Stone	Will Griffin
			
Sales Executive	Security Consultant	Information Security Architect	SOC Team Lead

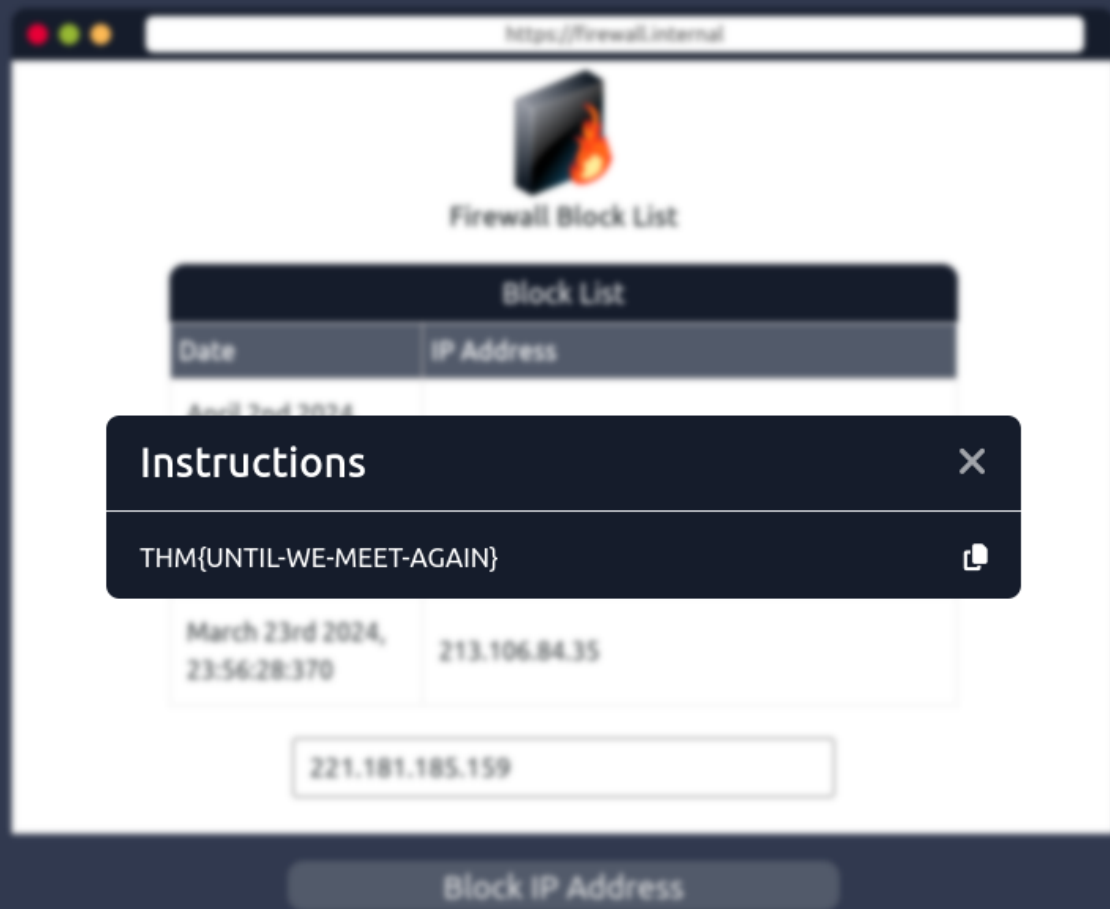
Choose Staff Member

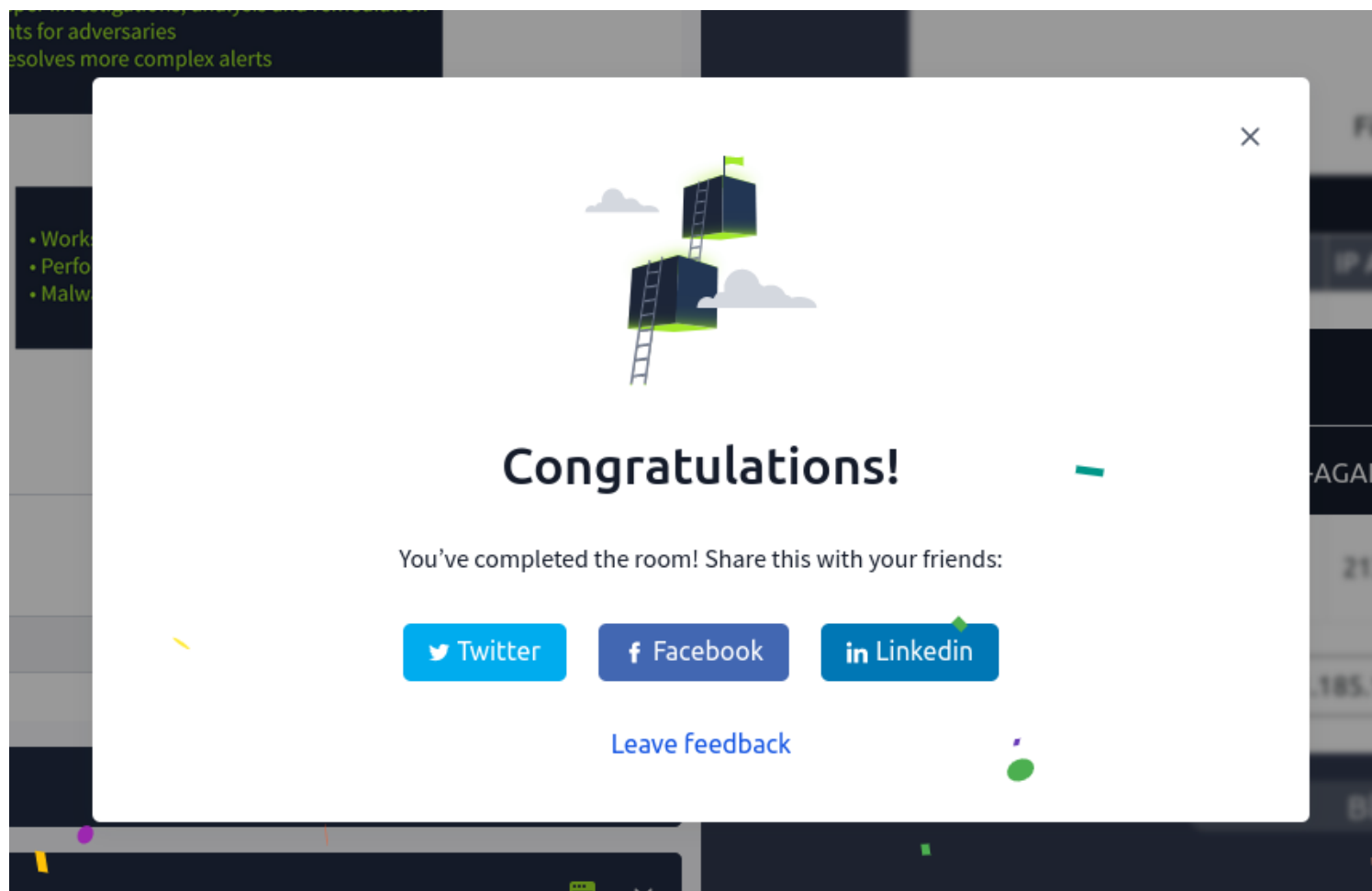
After blocking the malicious IP address on the firewall, what message did the malicious actor leave for you?

THM{UNTIL-WE-MEET-AGAIN}

✓ Correct

After successfully blocking the IP address I was able to retrieve a flag as seen below.





<https://tryhackme.com/r/room/jrsecanalystintrouxo>

## Conclusion

In conclusion, the establishment and operation of a Security Operation Center (SOC) is a cornerstone of an organization's cybersecurity strategy. As cyber threats continue to grow in sophistication and frequency, the role of the SOC becomes increasingly vital. By providing continuous monitoring, rapid incident response, and proactive threat intelligence, a SOC enables organizations to stay ahead of potential threats and minimize the impact of security incidents.

Different SOC models, whether internal, external, hybrid, or co-managed, offer unique advantages and can be tailored to meet the specific needs and resources of an organization. The implementation of comprehensive playbooks further enhances the effectiveness of a SOC by providing clear, actionable steps for responding to various types of security incidents.

Ultimately, a well-functioning SOC not only protects an organization's critical assets but also fosters a culture of security awareness and resilience. By investing in a robust SOC framework and continuously evolving to address new threats, organizations can ensure they remain vigilant and prepared in the face of an ever-changing cybersecurity landscape.

This was an easy room giving an overview and introductory environment of what it means to be a SOC Junior Sec Analyst.