

# **TryHackMe SOC Role in Blue Team Assignment**

**Course: CEH**

**Date Assigned: 5-11-2025**

**Due Date: 4-11-2025**

**Student Name: Praveen Kumar**

**Batch/Section: Super30 Batch**

**Instructor: Nitish kumar**

## Summary.

This lab provides practical insight into how a Security Operations Center (SOC) functions as the first line of defense in an organization's security posture. You begin by monitoring live security telemetry — logs from endpoints, servers, firewalls, SIEM dashboards, identity systems, and cloud services — to build an understanding of baseline network behavior and normal user activity. From there, you explore how SOC analysts detect threats in real time by triaging alerts, correlating logs, and using SIEM queries to identify suspicious behaviors, IOC matches, and anomalies that signal potential attacks.

You investigate simulated security events such as phishing attempts, malware execution, privilege escalation, lateral movement, and exfiltration to learn what patterns trigger alerts and why. Through hands-on threat hunting exercises, you practice pivoting across log sources, examining event timelines, mapping attacker activity to MITRE ATT&CK, and validating suspicious indicators. You also learn effective incident handling steps from alert verification and escalation to evidence collection, user communication, and documenting findings.

The lab covers essential SOC response workflows including account blocking, isolating compromised hosts, blocking malicious IPs/domains, and working with DFIR teams for deeper analysis. You gain understanding of playbooks, use cases, and rule tuning to reduce false positives and improve detection fidelity. Finally, you explore SOC collaboration practices, reporting, and strategies to harden the environment and stay ahead of adversary tactics. It's a full SOC lifecycle experience: monitor, detect, analyze, respond, recover the same structured approach used to protect real enterprise environments.

## The Contents of the Room

- **Task 1:** Introduction
- **Task 2:** Security Hierarchy
- **Task 3:** Meet the Blue Team
- **Task 4:** Advancing SOC Career
- **Task 5:** Final Challenge
- **Task 6:** Conclusion

## Task 1: Introduction to SOC




In your Junior Security Analyst Intro training, you learned the basics of what a SOC Level 1 analyst does in a team, such as monitoring alerts, investigating initial security incidents, and escalating suspicious actions. But merely learning the

duties of your role doesn't help much. To operate firmly and without hesitation in the real world as a professional, you must understand where a SOC stands in a business's security functions and how your role relates to the entire cybersecurity world.


The SOC serves as the central cybersecurity defense operations hub within an enterprise. It is your job as a SOC L1 analyst to work in frontline defense, where you constantly oversee protective resources, SIEM dashboards, endpoint logs, and network alerts. You have your work guided by senior analysts and security managers and are responsible for the accurate management of incidents and decision-making.

Anticipating the learning path, you understand the functions of leadership and support personnel around you, such as SOC Managers, Incident Response (IR) teams, Threat Intelligence specialists, and the Governance, Risk & Compliance (GRC) function. Knowing their duties allows you to work within the framework of collaboration and align your role for the most productive advancement in your career.




DashboardLearnPracticeCompete

Go Premium1



Learn > SOC Role in Blue Team



## SOC Role in Blue Team

Discover security roles and learn how to advance your SOC career, starting from the L1 analyst.

30 min9,420


Share your achievement


Save Room

91 Recommend

Options

Room completed (100%)

Task 1  Introduction



### Introduction

You've learned about a SOC L1 analyst role in the [Junior Security Analyst Intro](#) room. But where is it placed in a company structure? Who is overseeing your team? What other security departments exist? Which skills do you need to advance through your career ladder? Let's find out!

Answer the questions below

Let's find out!

No answer needed

✓ Correct Answer

## Task 2: Security Hierarchy

### Task 2 ✓ Security Hierarchy

#### Security Hierarchy

Cyber security priorities are different for every company. For law firms, the goal is the privacy of the legal documents. For factories, the availability of production lines. For hospitals, patient safety. That's why every company has a unique security approach and security team structure. Let's take a look at the high-level example of it:



**Q1.Which senior role typically makes key cyber security decisions?**

**Answer :** CISO

**Q2.What is the common name for roles like SOC analysts and engineers?**

**Answer :** Blue Team



**Q1.Which senior role typically makes key cyber security decisions?**

**Answer:** CISO

**Q2.What is the common name for roles like SOC analysts and engineers?**

**Answer:** Blue Team

Answer the questions below

Which senior role typically makes key cyber security decisions?

CISO

✓ Correct Answer

What is the common name for roles like SOC analysts and engineers?

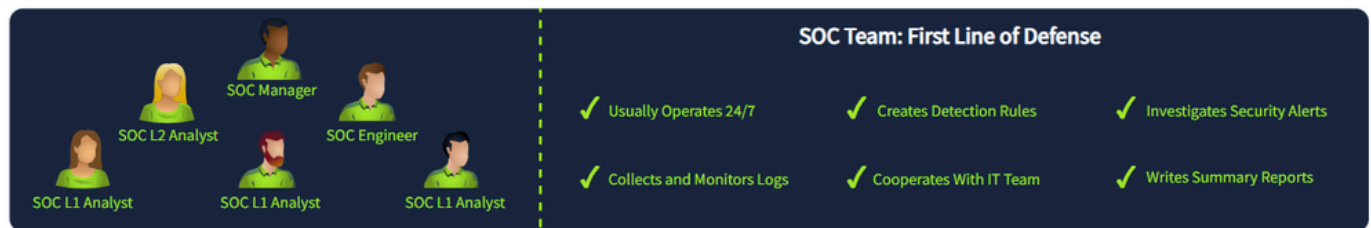
Blue Team

✓ Correct Answer

## Task 3: Meet the Blue Team

**Blue Team** is about defensive security, meaning it constantly monitors for attacks and tries to respond to them quickly. Depending on a company's size and sector, **Blue Team** can include a lot of different roles and subdepartments, usually counting 3 to 50 members total. Now, let's explore the most common **Blue Team** departments.

## Security Operations Center (SOC)



That's where you are most likely to start your cyber security journey! **SOC** is the central hub for an organization's cyber security - they are the first line of defense, work with various alerts, and handle most attacks. You can read more about **SOC** structure in [this room](#), but an efficient **SOC** is usually composed of the following roles:

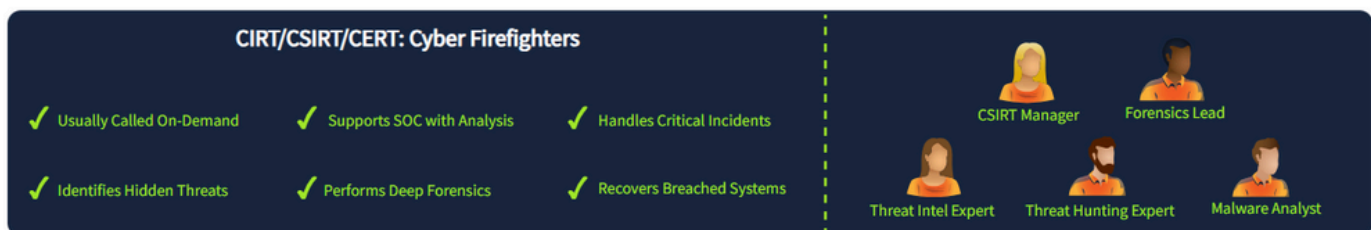


- **L1 Analysts:** Junior members who triage alerts and pass complex cases to L2
- **L2 Analysts:** Experienced members who investigate more advanced attacks
- **Engineers:** Experts in configuring security tools like **EDR** or **SIEM**
- **Manager:** A person who manages the whole **SOC** team

That's where you are most likely to start your cyber security journey! **SOC** is the central hub for an organization's cyber security - they are the first line of defense, work with various alerts, and handle most attacks. You can read more about **SOC** structure in [this room](#), but an efficient **SOC** is usually composed of the following roles:

- **L1 Analysts:** Junior members who triage alerts and pass complex cases to L2
- **L2 Analysts:** Experienced members who investigate more advanced attacks
- **Engineers:** Experts in configuring security tools like **EDR** or **SIEM**
- **Manager:** A person who manages the whole **SOC** team

## Cyber Incident Response Team (CIRT)



If **SOC** expertise is not enough or the incident goes out of control, you urgently call the "firefighters" - **CIRT**, also called **CSIRT** or **CERT**. The members should have a broad knowledge of cyber threats and handle breaches without depending on tools like **EDR** or **SIEM**. A **CIRT** job is stressful and responsible, but also rewarding. Here are a few **CIRT** examples:



- **JPCERT:** Japan's **CERT** handling nation-wide breaches
- **Mandiant:** A private team responding to global cyber incidents

If **SOC** expertise is not enough or the incident goes out of control, you urgently call the "firefighters" - **CIRT**, also called **CSIRT** or **CERT**. The members should have a broad knowledge of cyber threats and handle breaches without depending on tools like **EDR** or **SIEM**. A **CIRT** job is stressful and responsible, but also rewarding. Here are a few **CIRT** examples:

- **JPCERT:** Japan's **CERT** handling nation-wide breaches
- **Mandiant:** A private team responding to global cyber incidents
- **AWS CIRT:** Investigates security incidents of **AWS** customers

## Specialized Defensive Roles



Large companies, technology-focused startups, and government agencies often require narrow and specialized **Blue Team** roles - exciting and highly valuable, but requiring deep topic knowledge and broad experience in broader fields like **SOC** or **IT**. These narrow roles can include:



- **Digital Forensics Analyst:** Uncover hidden threats in disk and memory
- **Threat Intelligence Analyst:** Gather data about emerging threat groups
- **AppSec Engineer:** Maintain a secure software development lifecycle
- **AI Researcher:** Study **AI** threats and how to defend against them

Answer the questions below

Does Blue Team focus on defensive or offensive security?

Defensive

✓ Correct Answer

Which department handles active or urgent cyber incidents?

CIRT

✓ Correct Answer

🔍 Hint

## Q1.Does Blue Team focus on defensive or offensive security?

Answer: Defensive

## Q2.Which department handles active or urgent cyber incidents?

Answer: CIRT

## Task 4: Advancing SOC Career

### Task 4 ✓ Advancing SOC Career

#### SOC Path

Starting as a SOC L1 analyst may be a great option to broaden your cyber world awareness and better understand the more specialized roles. Moreover, even the entry-level SOC L1 role can be fun and engaging: You will deal with real attacks, protect the company from advanced threat groups, and learn a lot during the process. Let's see how you can start:

1. Gain core SOC skills and practice them. Related skills like red teaming or general IT would help, too!
2. Be proactive, try yourself in CTFs, stay in the loop of cyber news, and consider the SAL1 certification!
3. Prepare for an interview, learn the difference between an internal SOC and MSSP, and apply for a job!
4. After working for some time in a junior position, consider preparing and advancing to more senior roles!

#### Internal SOC vs MSSP

Not every organization has the expertise to operate a SOC on its own and relies on a Managed Security Services Provider (MSSP), a company that delivers outsourced security services, most commonly SOC, to its clients. Working at MSSP is typically high-pressure, but it is also a good option to quickstart your career. While we recommend applying for any open SOC position as your first job, it's also important to understand the differences:

Topic	Internal SOC	MSSP
 Scenario Example	You work in a SOC team of the bank and protect the bank's systems	You work for a global MSSP protecting its sixty customers in Europe



## Internal SOC vs MSSP

Not every organization has the expertise to operate a SOC on its own and relies on a Managed Security Services Provider (MSSP), a company that delivers outsourced security services, most commonly SOC, to its clients. Working at MSSP is typically high-pressure, but it is also a good option to quickstart your career. While we recommend applying for any open SOC position as your first job, it's also important to understand the differences:

Topic	Internal SOC	MSSP
Scenario Example	You work in a SOC team of the bank and protect the bank's systems	You work for a global MSSP protecting its sixty customers in Europe
Working Pace	You usually have calm shifts without too much time pressure	Your shift usually starts from a queue of urgent alerts to analyze
Security Tools	You work with just a few tools, but need to know them very well	You have to work with sixty diverse security tools and platforms
Incident Practice	You saw and learned from just two major cyber attacks last year	Every week, you deal with attacks and breaches, and can learn from it



### Next Steps

### Next Steps

Your most natural next step after L1 is to become a SOC L2 analyst, but you are free to choose another path! While handling a SIEM alert, you might notice that engineering work appeals to you more. During a cyber attack, you may be fascinated by CIRT actions. You may also find yourself well-suited as a manager and build your path to the CISO role. No matter what, your first year or two is to get real work experience, and to spend this time effectively, follow the tips below!



#### Learn From Every Alert

Understand why a rule triggered and use it to sharpen your detection skills



#### Think Like An Attacker

Ask "Why would the attackers do it" before triaging how did they do it



#### Verify Everything

Never assume. Always validate alerts and suspicious behavior in logs



#### Get Involved in Incidents

Real attacks teach lessons no lab can. They are worth a sleepless night

How would you call a cyber security company providing SOC services?

MSSP

✓ Correct Answer

Which role naturally continues your SOC L1 analyst journey?

SOC L2 Analyst

✓ Correct Answer

Q1.How would you call a cyber security company providing SOC services?

Answer: MSSP

Q2.Which role naturally continues your SOC L1 analyst journey?

Answer: SOC L2 Analyst

# Task 5: Final Challenge

Task 5

Final Challenge


### Final Challenge

For this task, imagine yourself as a CISO of TrySecureMe, a big multinational company. You oversee multiple departments and deal with incidents every month. This time, as many as seven incidents are happening at the same time, and you have to choose the right people to deal with every one of them. Do you know security roles well enough to complete this challenge?

**Website Instructions**

View Site

Open the attached website by clicking the **View Site** button above and consider resizing or opening it in full screen for a better view. Then, drag and drop the roles from the left to the incidents on the right. If your choices are correct, claim your flag and complete the task! You can reset the website at any time by clicking the **Reset** button.



Welcome to TrySecureMe!

Seven security tasks require an action, and you have to choose the right people to deal with every of them. Observe the roles on the left, drag the correct roles, and drop it on the corresponding scenario on the right.

Alice

Threat Researcher

Lucas

SOC L1 Analyst

SIEM created an alert about FW-NY-01 firewall brute-force. Who should triage the alert?

The HR manager Anna launched a phishing malware. Who should make a deep analysis?

The office in France was somehow hit with ransomware. Immediate response is required!

The servers storing the credit cards require PCI DSS audit. Who can help us here?

TryHackMe | Blue

TryHackMe | SOC Role in Blue T...

tryhackme.com/room/socroleinblueteam

Room progress ( 88% )

### Next Rooms in Path

1. Humans as Attack Vectors

2. Systems as Attack Vectors

Answer the questions below

Complete the room!

No answer needed

Complete

How likely are you to recommend this room to others?

1

2

3

4

5

6

7

8

9

10

Welcome to TrySecureMe!

Seven security tasks require an action, and you have to choose the right people to deal with every one of them. Observe the roles on the top, drag the correct roles, and drop it on the corresponding scenario below.

Susan

SOC L2 Analyst

Ben

Penetration Tester

Alice

Threat Researcher

SIEM created an alert about FW-NY-01 firewall brute-force. Who should triage the alert?

The HR manager Anna launched a phishing malware. Who should make a deep analysis?

The office in France was somehow hit with ransomware. Immediate response is required!

Our servers storing the credit cards require PCI DSS audit. Who can help us here?

Who can check the new version of tryhackme.thm for vulnerabilities?

The SIEM is unavailable due to a storage limit. Who can investigate the issue?

FIN7 threat group actively targets our company. Who can analyze their tactics?

SOC Role in Blue Team Web App

Type here to search

20°C Mostly clear

10:33 03-11-2025

Answer the questions below

What flag did you claim after completing the final challenge?

THM{trysecureme\_is\_secured!}

✓ Correct Answer

**Q1.What flag did you claim after completing the final challenge?**

**Answer:** THM{trysecureme\_is\_secured!}

## Task 6: Conclusion

### Task 6 ✓ Conclusion

Great job completing the challenge! Now you know how SOC team works, where it is placed in the security structure, and what you to do to start your career journey. Now, continue to the next rooms and learn what does SOC actually protect: humans and systems.

#### Next Rooms in Path

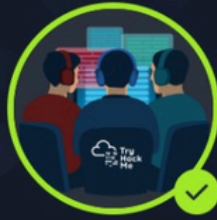
1. [Humans as Attack Vectors](#)
2. [Systems as Attack Vectors](#)

Answer the questions below

Complete the room!

No answer needed

✓ Correct Answer



You did it! 🎉 SOC Role in Blue Team complete!

Points earned 🎯 56	Completed tasks ✅ 6	Room type 👤 Walkthrough	Difficulty 📶 Easy	Streak 🔥 1
-----------------------	------------------------	----------------------------	----------------------	---------------

👤👤👤 81,493 users are actively learning this week

## Declaration

I declare that this work is my own and completed without unauthorized assistance.

Signature: Praveen Kumar

Date: 5-11-2025