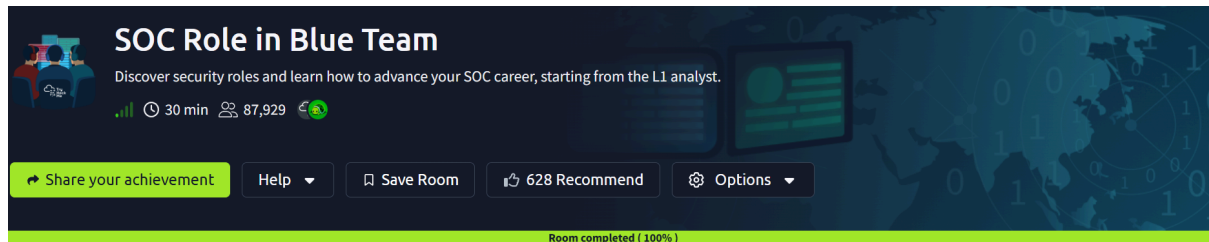


## SOC Role in Blue Team Write-up

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



### 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!

#### Learning Objectives

- Understand the concept and purpose of the Blue Team
- Explore a place of the SOC within the company structure
- Find out about your career path as a SOC L1 analyst

#### Prerequisites

- Complete the Junior Security Analyst Intro room(<https://tryhackme.com/room/jrsecanalystintrouxo>)
- Remind yourself of SOC Roles and Processes(<https://tryhackme.com/room/socfundamentals>)

### 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:



Looking at the diagram above, top executives like the CEO usually focus on global business objectives and don't manage technical aspects. That's why they hire a Chief Information Security Officer (CISO) or a similar role who knows the business needs and can create the most suitable security departments.

### Security Departments

In tiny companies, the IT department takes the role of securing the company. Small to medium-sized companies may have a generic "Information Security" team that does all sorts of tasks. For this room, we will focus on bigger companies with a CISO overseeing multiple security teams, each handling a specific task. For example:

- **Red Team:** Offensive security experts, pentesters, or ethical hackers who look for security issues
- **GRC Team:** Specialists managing policies and ensuring compliance with regulations like PCI DSS
- **Blue Team:** Defensive security experts like SOC analysts, engineers, or incident responders

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

**Answer: CISO**

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

**Answer: Blue Team**

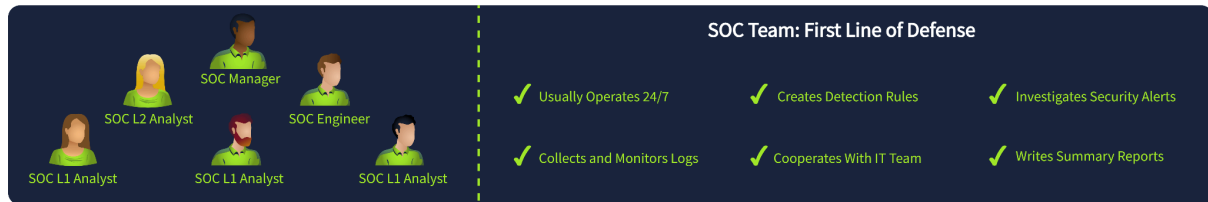
### Task 3 Meet the Blue Team

A **blue team** comprises cyber security and technology professionals whose aim is to protect an information system from impending cyber threats by performing and implementing defensive actions.

**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.

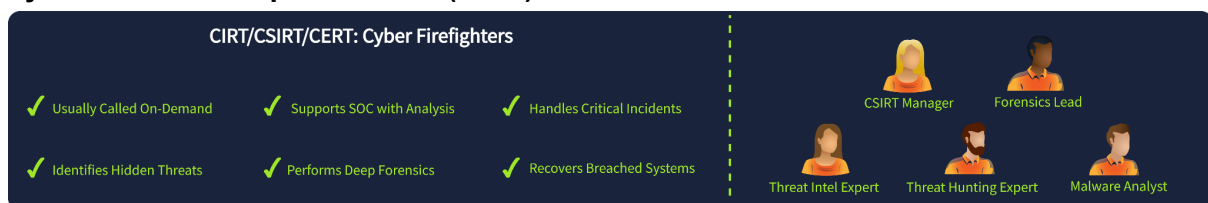
## Security Operations Center (SOC)



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(<https://tryhackme.com/room/socfundamentals>) , 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**(Endpoint detection and response (EDR) is a series of tools that monitor devices for activity that could indicate a threat.) or **SIEM**(Security Information and Event Management system that is used to aggregate security information in the form of logs, alerts, artifacts and events into a centralized platform that would allow security analysts to perform near real-time analysis during security monitoring.)
- 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(<https://www.jpcert.or.jp/english/>) : Japan's CERT handling nation-wide breaches

Mandiant(<https://cloud.google.com/security/mandiant>) : A private team responding to global cyber incidents

AWS CIRT(<https://aws.amazon.com/security-incident-response/>) : 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

**Does Blue Team focus on defensive or offensive security?**

**Answer:** **Defensive**

**Which department handles active or urgent cyber incidents?**

**Answer:** **CIPT**

## 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 <u>SOC</u>	MSSP
<b>Scenario Example</b>	You work in a <u>SOC</u> team of the bank and protect the bank's systems	You work for a global MSSP protecting its sixty customers in Europe
<b>Working Pace</b>	You usually have calm shifts without too much time pressure	Your shift usually starts from a queue of urgent alerts to analyze
<b>Security Tools</b>	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

### 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?

Answer: **MSSP**

Which role naturally continues your SOC L1 analyst journey?

Answer: **SOC L2 Analyst**

### Task 5 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

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 one of them. Observe the roles on the top, drag the correct roles, and drop it on the corresponding scenario below.




**Robert**  
CERT Lead




**Ben**  
Penetration Tester




**Susan**  
SOC L2 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!



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?

What flag did you claim after completing the final challenge?

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

## 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.



**Nick**  
GRC Auditor



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?



**Lucas** | SOC L1 Analyst



**Susan** | SOC L2 Analyst



**Robert** | CERT Lead



**Ben** | Penetration Tester



**Eugen** | SOC Engineer



**Alice** | Threat Researcher

## 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.

Congratulations - All assignments are correct!



The answer to the TryHackMe question is:

`THM{trysecureme_is_secured!}`



Robert | CERT Lead



Nick | GRC Auditor



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



Ben | Penetration Tester



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



Eugen | SOC Engineer



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



Alice | Threat Researcher

### 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

- Humans as Attack Vectors
- Systems as Attack Vectors