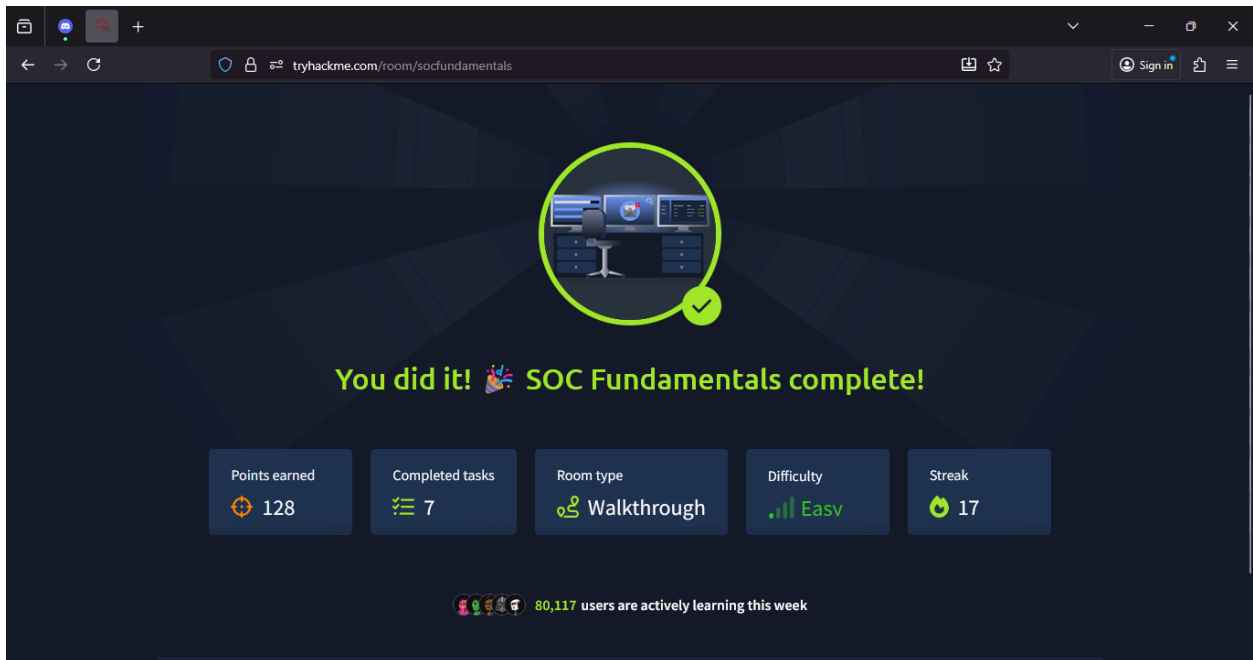


SOC Fundamentals Lab



tryhackme.com/room/socfundamentals

Sign in

You did it! 🎉 SOC Fundamentals complete!

Points earned: 128

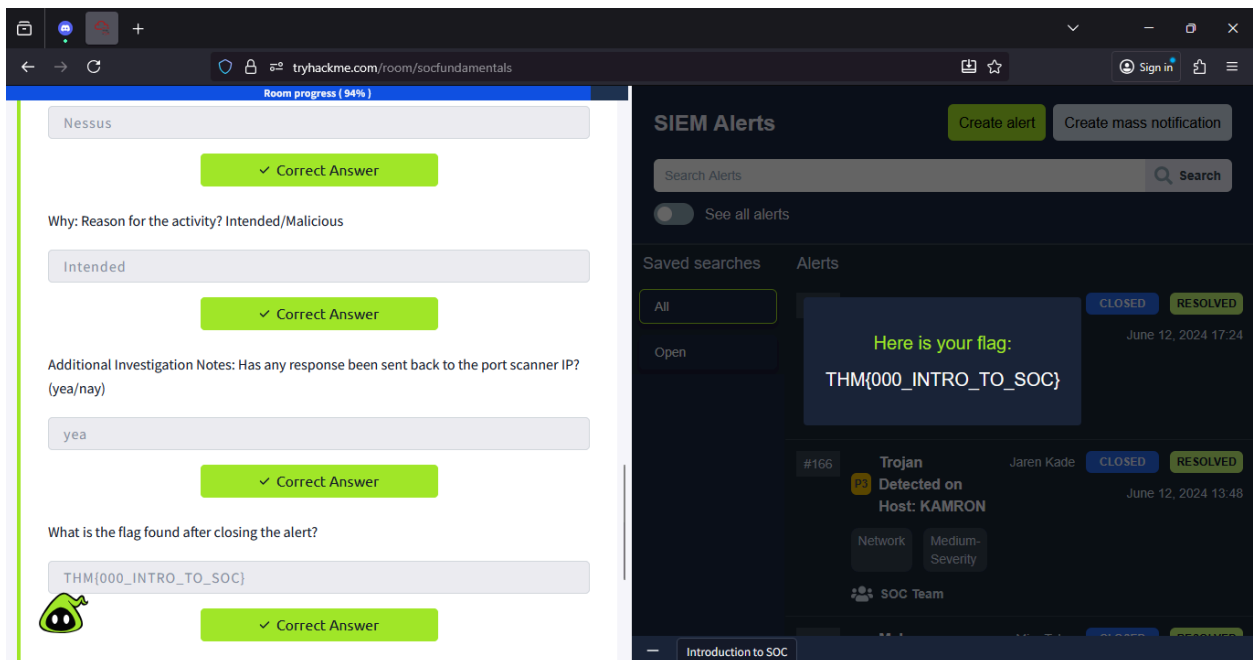
Completed tasks: 7

Room type: Walkthrough

Difficulty: Easy

Streak: 17

80,117 users are actively learning this week



tryhackme.com/room/socfundamentals

Sign in

Room progress (94%)

Nessus

✓ Correct Answer

Why: Reason for the activity? Intended/Malicious

Intended

✓ Correct Answer

Additional Investigation Notes: Has any response been sent back to the port scanner IP? (yea/nay)

yea

✓ Correct Answer

What is the flag found after closing the alert?

THM{000_INTRO_TO_SOC}

✓ Correct Answer

SIEM Alerts

Create alert Create mass notification

Search Alerts Search

See all alerts

Saved searches Alerts

All Open

Here is your flag:
THM{000_INTRO_TO_SOC}

June 12, 2024 17:24

#166 Trojan Jaren Kade CLOSED RESOLVED

Detected on Host: KAMRON

June 12, 2024 13:48

Network Medium-Severly

SOC Team

Introduction to SOC

tryhackme.com/room/socfundamentals

Room progress (94%)

SIEM solution, where you can see all the associated logs for this alert. You are tasked to view the logs individually and answer the question to the 5 Ws given below.

Note: The vulnerability assessment team notified the SOC team that they were running a port scan activity inside the network from the host: 10.0.0.8

Answer the questions below

What: Activity that triggered the alert?

Port Scan

✓ Correct Answer

When: Time of the activity?

June 12, 2024 17:24

✓ Correct Answer

Where: Destination host IP?

10.0.0.3

✓ Correct Answer

Who: Source host name?

Nessus

✓ Correct Answer

Why: Reason for the activity? Intended/Malicious

tryhackme.com/room/socfundamentals

Room progress (94%)

Task 7 Conclusion

This room helped us learn some exciting facts about the SOC team. We saw its responsibilities and the pillars, People, Process, and Technology, that mature any SOC environment. This room focused on understanding how People, Processes, and Technology play their roles in the day-to-day SOC use cases. Lastly, we got our hands on a practice lab and solved a real-world SOC alert as a level 1 Analyst.

Answer the questions below

I understand the fundamentals of a SOC.

No answer needed

✓ Correct Answer

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

Submit now

tryhackme.com/room/socfundamentals

Room progress (94%)

Task 7 Conclusion

This room helped us learn some exciting facts about the SOC team. We saw its responsibilities and the pillars, People, Process, and Technology, that mature any SOC environment. This room focused on understanding how People, Processes, and Technology play their roles in the day-to-day SOC use cases. Lastly, we got our hands on a practice lab and solved a real-world SOC alert as a level 1 Analyst.

Answer the questions below

I understand the fundamentals of a SOC.

No answer needed

✓ Correct Answer

Thank you!

Your feedback helps us improve our content! We appreciate the time you took to share your thoughts!


✓ Close

tryhackme.com/room/socfundamentals

Go Premium 17

Dashboard Learn Practice Compete

Cyber Security 101 > Defensive Security > SOC Fundamentals



SOC Fundamentals

Learn about the SOC team and their processes.

45 min 55,771

Show Split View

Save Room

891 Recommend

Options


Room progress (94%)

Task 1 Introduction to SOC

Technology has made our lives more efficient, but with this efficiency comes more responsibility. Modern-day fears have come a long way from the exploitation of physical assets. The critical data, called secrets, are no longer stored in physical files. Organizations carry tons of confidential data in their network and systems. Any unauthorized disruption, loss, or modification to this data may cause them a huge damage. Threat actors discover and exploit new vulnerabilities in these networks and systems daily, becoming a major concern in cyber security. Traditional security practices may not be enough to prevent many of these threats. Dedicated a whole team to managing your organization's security is important.

tryhackme.com/room/socfundamentals

Room progress (94%)



This room will delve into some key concepts of SOC, one of the most important fields in defensive security.

Learning Objectives

- Building a baseline for SOC (Security Operations Center)
- Detection and response in SOC
- The role of People, Processes, and Technology
- Practical exercise

Answer the questions below

What does the term SOC stand for?

Security Operations Center

✓ Correct Answer

Task 2 ✓ Purpose and Components

Task 3 ✓ People

tryhackme.com/room/socfundamentals

Room progress (94%)

People, Process, and Technology coexist in a SOC environment. A team of professional individuals working on state-of-the-art security tools in the presence of proper processes is what makes a mature SOC environment.

In the upcoming tasks, we will discuss each of these pillars individually and examine how they are important parts of SOC.

Answer the questions below

The SOC team discovers an unauthorized user is trying to log in to an account. Which capability of SOC is this?

Detection

✓ Correct Answer

What are the three pillars of a SOC?

People, Process, Technology

✓ Correct Answer

Task 3 ✓ People

Task 4 ✓ Process

tryhackme.com/room/socfundamentals

Room progress (94%)

and correlate the data from multiple data sources to perform a proper analysis.

- **SOC Analyst (Level 3):** Level 3 Analysts are experienced professionals who proactively look for any threat indicators and support in the incident response activities. The critical severity detection reported by Level 1 and Level 2 Analysts are often security incidents that need detailed responses, including containment, eradication, and recovery. This is where Level 3 analysts' experience comes in handy.
- **Security Engineer:** All analysts work on security solutions. These solutions need deployment and configuration. Security Engineers deploy and configure these security solutions to ensure their smooth operation.
- **Detection Engineer:** Security rules are the logic built behind security solutions to detect harmful activities. Level 2 and 3 Analysts often create these rules, while the SOC team can sometimes also utilize the detection engineer role independently for this responsibility.
- **SOC Manager:** The SOC Manager manages the processes the SOC team follows and provides support. The SOC Manager also remains in contact with the organization's CISO (Chief Information Security Officer) to provide him with updates on the SOC team's current security posture and efforts.

Note: The roles in the SOC team can increase or decrease depending on the size and criticality of the organizations.

Answer the questions below


Alert triage and reporting is the responsibility of?

SOC Analyst (Level 1)

✓ Correct Answer

Hint

Which role in the SOC team allows you to work dedicatedly on establishing rules for alerting security solutions?

 Detection Engineer

✓ Correct Answer

tryhackme.com/room/socfundamentals

Room progress (94%)

Sign in

Why?

After the investigation, it was found that the file was downloaded from a pirated software-selling website. The investigation with the user revealed that they downloaded the file as they wanted to use a software for free.

Reporting

The detected harmful alerts need to be escalated to higher-level analysts for a timely response and resolution. These alerts are escalated as tickets and assigned to the relevant people. The report should discuss all the 5 Ws along with a thorough analysis, and screenshots should be used as evidence of the activity.

Incident Response and Forensics

Sometimes, the reported detections point to highly malicious activities that are critical. In these scenarios, high-level teams initiate an incident response. The incident response process is discussed in detail in the [Incident Response](#) room. A few times, a detailed forensics activity also needs to be performed. This forensic activity aims to determine the incident's root cause by analyzing the artifacts from a system or network.


Answer the questions below

At the end of the investigation, the SOC team found that John had attempted to steal the system's data. Which 'W' from the 5 Ws does this answer?

Who

✓ Correct Answer

The SOC team detected a large amount of data exfiltration. Which 'W' from the 5 Ws does this answer?

What

✓ Correct Answer

tryhackme.com/room/socfundamentals

Room progress (94%)

Sign in

correlating them with multiple log sources and alerts us in case of a match with any of the rules. Modern SIEM solutions surpass this rule based detection analysis, providing us with user behavior analytics and threat intelligence capability. Machine learning algorithms support this to enhance the detection capabilities.

Note: The SIEM solution only provides the **Detection** capabilities in a SOC environment.

- **EDR:** Endpoint Detection and Response (EDR) provides the SOC team with detailed real-time and historical visibility of the devices' activities. It operates on the endpoint level and can carry out automated responses. EDR has extensive detection capabilities for endpoints, allowing you to investigate them in detail and respond with a few clicks.
- **Firewall:** A firewall functions purely for network security and acts as a barrier between your internal and external networks (such as the Internet). It monitors incoming and outgoing network traffic and filters any unauthorized traffic. The firewall also has some detection rules deployed, which help us identify and block suspicious traffic before it reaches the internal network.

Several other security solutions play unique roles in a SOC environment, such as Antivirus, EPP, IDS/IPS, XDR, SOAR, and more. The decision on what Technology to deploy in the SOC comes after careful consideration of the threat surface and the available resources in the organization.


Answer the questions below

Which security solution monitors the incoming and outgoing traffic of the network?

Firewall

✓ Correct Answer

Do SIEM solutions primarily focus on detecting and alerting about security incidents? (yea/nay)

yea

✓ Correct Answer