

Room 2: Defensive Security Intro.

Summary:

- This room entails defensive security. It demonstrates how a special security team (Special Operations Center) can handle advances from malicious hackers.

Objective:

- To simulate defensive security through Security Information & Event Management (SIEM)

Tools Used:

- SIEM

Steps Taken:

- Used SIEM to demonstrate defensive security

Room progress (80%)

To start this simulation, please click the "View Site" button below.

[View Site](#)

This action will open a "static site" on the right side of your screen. Follow the step-by-step instructions provided within the simulation to navigate through the events and locate the "flag." A flag is a series of characters with a format like this: "THM{RANDOM_WORDS}". Use this flag to answer questions from rooms here in TryHackMe, like the one below.

What's next?

In this room, we've discussed the different subfields (SOC, Threat Intelligence, Malware Analysis, and DFIR) and experienced firsthand how to deal with alerts in a simulated SIEM environment. While we've covered a lot, the depth and complexity of this field mean there's more to learn and explore. The lessons learned here will serve as your foundation as cyber threats evolve, demanding continuous learning, vigilance, and adaptation.

Continue learning by checking out the next room in this series, "Search Skills." This room will teach you valuable techniques for searching for information online to aid your investigations and learning.

Answer the questions below

Operations: Information 1/3

Alert Log

Date	Message
undefined 7th 2025, 09:38:29:068	Successful SSH authentication attempt to port 22 from IP address 143.110.250.149
undefined 7th 2025, 09:35:12:103	Unauthorized connection attempt detected from IP address 143.110.250.149 to port 22
undefined 7th 2025, 07:18:55:283	The user John Doe logged in successfully (Event ID 4624)
undefined 7th 2025, 07:18:30:223	Multiple failed login attempts from John Doe
undefined 7th 2025, 07:08:46:226	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

Defensive Security

TryHackMe | Dashboard

Please Verify Your Email - johnn

TryHackMe | Defensive Security

tryhackme.com/room/defensivesecurityintro

Relaunch to update

Room progress (80%)

What's next?

In this room, we've discussed the different subfields (SOC, Threat Intelligence, Malware Analysis, and DFIR) and experienced firsthand how to deal with alerts in a simulated SIEM environment. While we've covered a lot, the depth and complexity of this field mean there's more to learn and explore. The lessons learned here will serve as your foundation as cyber threats evolve, demanding continuous learning, vigilance, and adaptation.

Continue learning by checking out the next room in this series, "Search Skills." This room will teach you valuable techniques for searching for information online to aid your investigations and learning.

Answer the questions below


What is the flag that you obtained by following along?

Submit

How likely are you to recommend this room to others?

you can proceed and implement the block rule. Block the malicious IP address on the firewall and find out what message they left for you.

https://firewall.internal



Firewall Block List

Block List	
Date	IP Address
July 2nd 2021, 13:27:00:948	101.34.37.231
June 30th 2021, 09:12:11:857	212.38.99.12
June 23rd 2021, 23:56:28:370	213.106.84.35

Block IP Address

Defensive Security

Flag(s):

- THM {THREAT – BLOCKED}

TryHackMe | Dashboard

Please Verify Your Email - johnn

TryHackMe | Defensive Security

tryhackme.com/room/defensivesecurityintro

Relaunch to update

Room progress (80%)

What's next?

In this room, we've discussed the different subfields (SOC, Threat Intelligence, Malware Analysis, and DFIR) and experienced firsthand how to deal with alerts in a simulated SIEM environment. While we've covered a lot, the depth and complexity of this field mean there's more to learn and explore. The lessons learned here will serve as your foundation as cyber threats evolve, demanding continuous learning, vigilance, and adaptation.

Continue learning by checking out the next room in this series, "Search Skills." This room will teach you valuable techniques for searching for information online to aid your investigations and learning.

Answer the questions below

What is the flag that you obtained by following along?

Submit

How likely are you to recommend this room to others?

A Day In the Life of a Junior (Associate) Security Analyst

Challenge Complete

You blocked the malicious IP address!

THM{THREAT-BLOCKED}

Defensive Security

Lessons Learned:

- I was able to enforce defensive security via SIEM