SECURITY OPERATIONS

TryHackMe Room: Security Operations

Key Skill: Understanding how SOC handles threats in real time

---

🔎 What Security Operations Really Means

Security Operations = **doing security every single day**, not just planning it.

Core responsibilities:

- monitoring systems and logs
- detecting suspicious activity
- responding to alerts
- fixing weaknesses (patching, configs)
- working with SOC during incidents

Security Ops = **hands + eyes of cybersecurity**.

🔥 Lab Highlight — Blocking a Malicious Attack

In the simulation:

- we observed malicious traffic
- identified the attacking IP
- added firewall rules
- stopped the attacker

Flag: THM{ATTACK_BLOCKED}

This taught:

✔ how rules decide **PASS** vs **DROP**
✔ why blocking attacks early matters
✔ how SOC collaborates with network teams

🧱 Firewalls Matter

Firewalls decide:

Allow traffic?

Block traffic?

Log suspicious traffic?

Rules use things like:

- source IP
- destination IP
- port number
- protocol

<u>One bad rule = attackers walk in.</u>

🚨 Why SOC + Security Operations Must Work Together

<u>Security Operations:</u>

- fixes systems
- applies patches
- manages firewalls

<u>SOC:</u>

- detects threats
- investigates alerts
- escalates incidents

They constantly **communicate** during incidents.

🧠 Key Takeaways

- Security Ops is about **execution**, not theory
- Firewalls are the **first defensive layer**
- Stopping attacks early saves huge damage
- Collaboration is everything in security