TryHackMe Walkthrough – Blue Team Fundamentals Room

# 🔗 Room URL

https://tryhackme.com/room/blueteamfundamentals

# 🧾 Summary

This room introduces the core responsibilities of Blue Team operations. It covers incident detection, triage, SIEM fundamentals, and basic response techniques. Ideal for anyone preparing for a SOC role or cybersecurity analyst position.

# 🛠️ Tools & Topics Covered

- SIEM Tools (Splunk, ELK)  
- Log analysis  
- MITRE ATT&CK Framework  
- Threat Intelligence  
- Incident Triage

# 🔍 Key Concepts Learned

1. The role of a Blue Team in a cybersecurity defense strategy.  
2. How attackers are detected using behavioral anomalies and log data.  
3. The structure and usage of SIEM tools in an enterprise setting.  
4. Mapping real-world attacks using MITRE ATT&CK.  
5. How to document an incident timeline and respond efficiently.

# 🎯 Practical Exercises

- Interpreted log files to detect brute force and lateral movement attacks  
- Used Splunk queries to build real-time dashboards  
- Analyzed threat actor behavior using ATT&CK techniques

# 🧠 What I Learned

- How to think like a defender using detection logic and correlation  
- Ways to reduce alert fatigue using priority-based triage  
- Real-world use of SIEM platforms to detect malicious activity  
- Blue Team responsibilities in a SOC workflow