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:

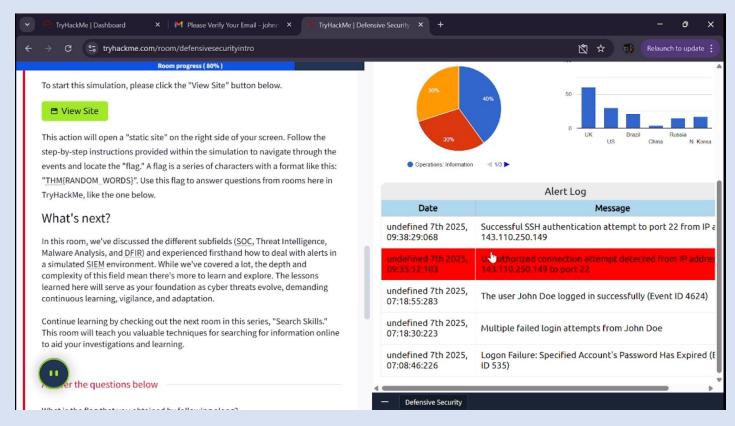
• To simulate defensive security through Security Information & Event Management (SIEM)

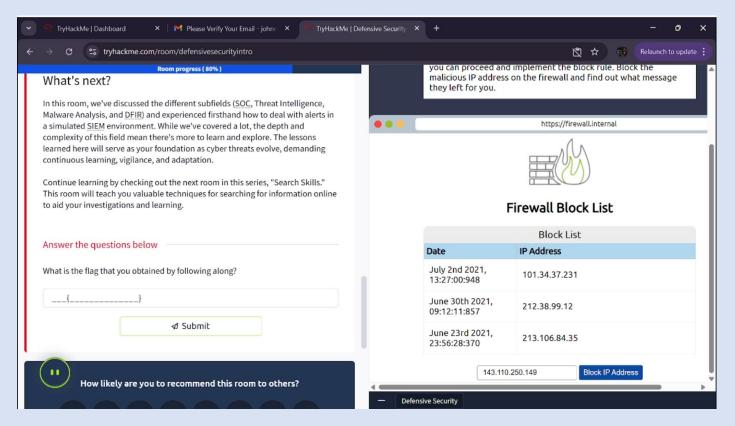
Tools Used:

SIEM

Steps Taken:

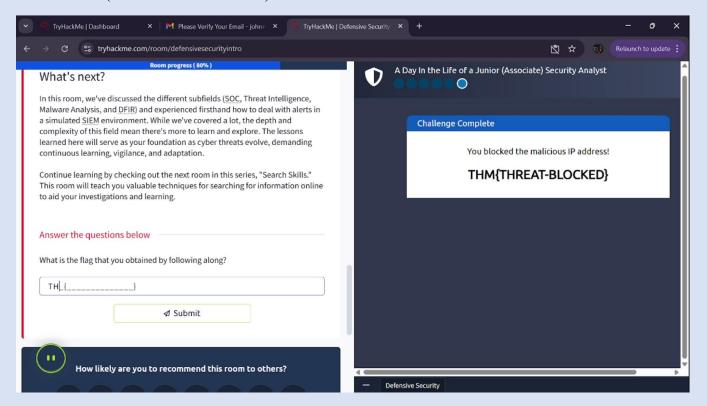
Used SIEM to demonstrate defensive security





Flag(s):

THM {THREAT – BLOCKED}



Lessons Learned:

• I was able to enforce defensive security via SIEM