

Intro to Defensive Security

Introducing defensive security and related topics, such as threat intelligence, SOC, DFIR, and SIEM.

Task 1 Introduction to Defensive Security

Question	Answer
Which team focuses on defensive security?	Blue Team

Task 2 Areas of Defensive Security

Question	Answer
What would you call a team of cyber security professionals that monitors a network and its systems for malicious events?	Security Operations Center
What does DFIR stand for?	Digital Forensics and Incident Response
Which kind of malware requires the user to pay money to regain access to their files?	ransomware

Task 3 Practical Example of Defensive Security

What is the flag that you obtained by following along?


Answer: **THM{THREAT-BLOCKED}**




→ I Inspected the alerts in my SIEM dashboard and found the malicious IP address from the alerts to be that of unauthorised connection attempt from 143.110.250.149 to port 22(ssh port)

Alert Log	
Date	Message
July 14th 2024, 08:09:39:109	Successful SSH authentication attempt to port 22 from IP address 143.110.250.149
July 14th 2024, 08:06:24:149	Unauthorized connection attempt detected from IP address 143.110.250.149 to port 22
July 14th 2024, 05:49:05:235	The user John Doe logged in successfully (Event ID 4624)
July 14th 2024, 05:49:34:200	Multiple failed login attempts from John Doe
July 14th 2024, 05:39:01:278	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

- I clicked on the alert to further inspect
- Then i inputted the IP address so the IP scanner can check the reputation of the IP address to see whether it's malicious or suspicious



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



Instructions

There are websites on the Internet that allow you to check the reputation of an IP address to see whether it's malicious or suspicious.

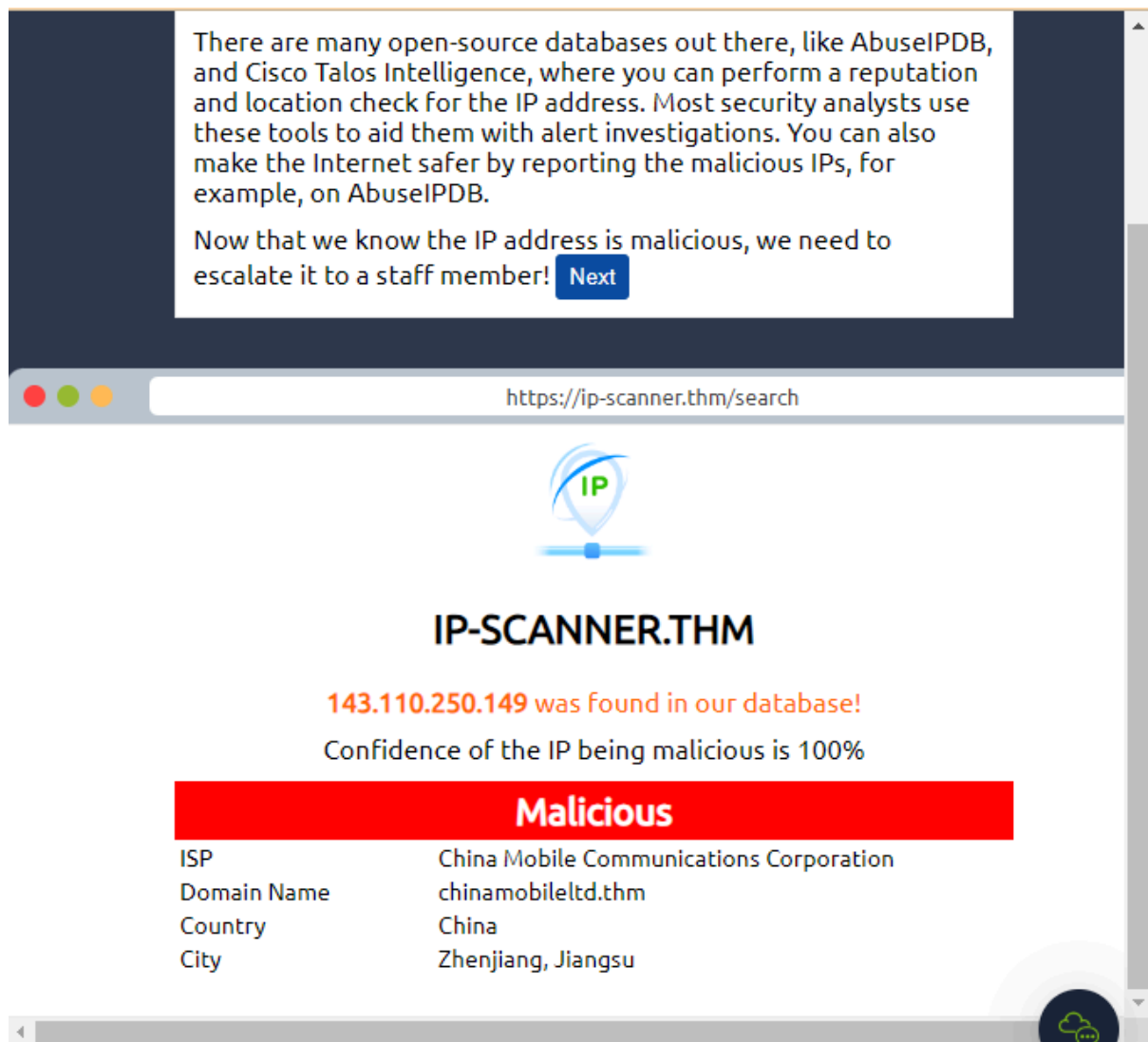
<https://ip-scanner.thm>




IP-SCANNER.THM

Check by IP Address

→ The scanner proved that the IP address is malicious




→ I clicked on next to escalate the alert to the SOC team lead


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


Instructions


We shouldn't worry too much if it was a failed authentication attempt, but you probably noticed the successful authentication attempt from the malicious IP address. Let's declare a small incident event and escalate it. There is some great staff working at the company, but you wouldn't want to escalate this to the wrong person who is not in charge of your team or department.

Choose to whom you would escalate this event?

☐ Dominick Nash

Sales Executive

☐ Nadia Watson

Security Consultant

☐ Carolyn Stone

Information Security Architect

☒ Will Griffin

SOC Team Lead


Choose Staff Member

Defensive Security

→ Next, i blocked the malicious IP address

You got the permission to block the malicious IP address, and now 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



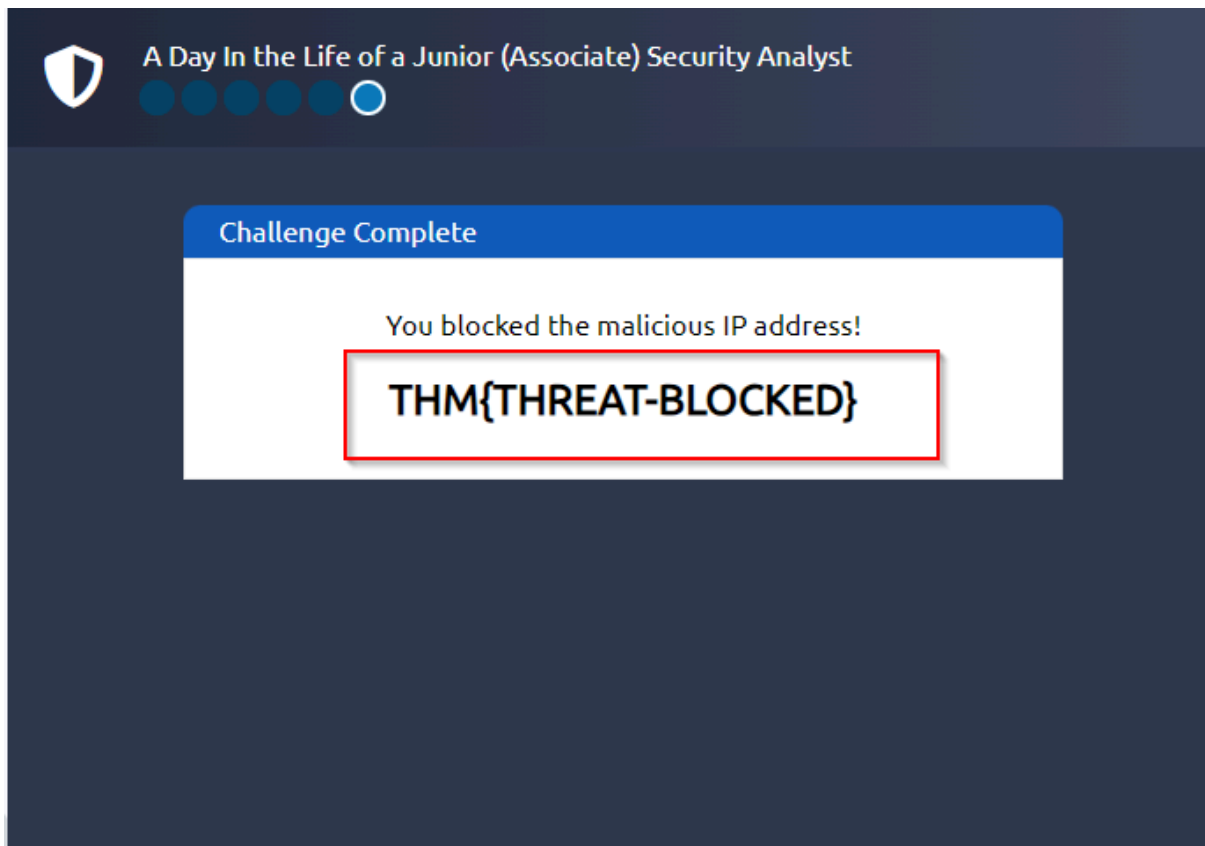
Firewall Block List

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

→ Finally, i got the flag



END!!!