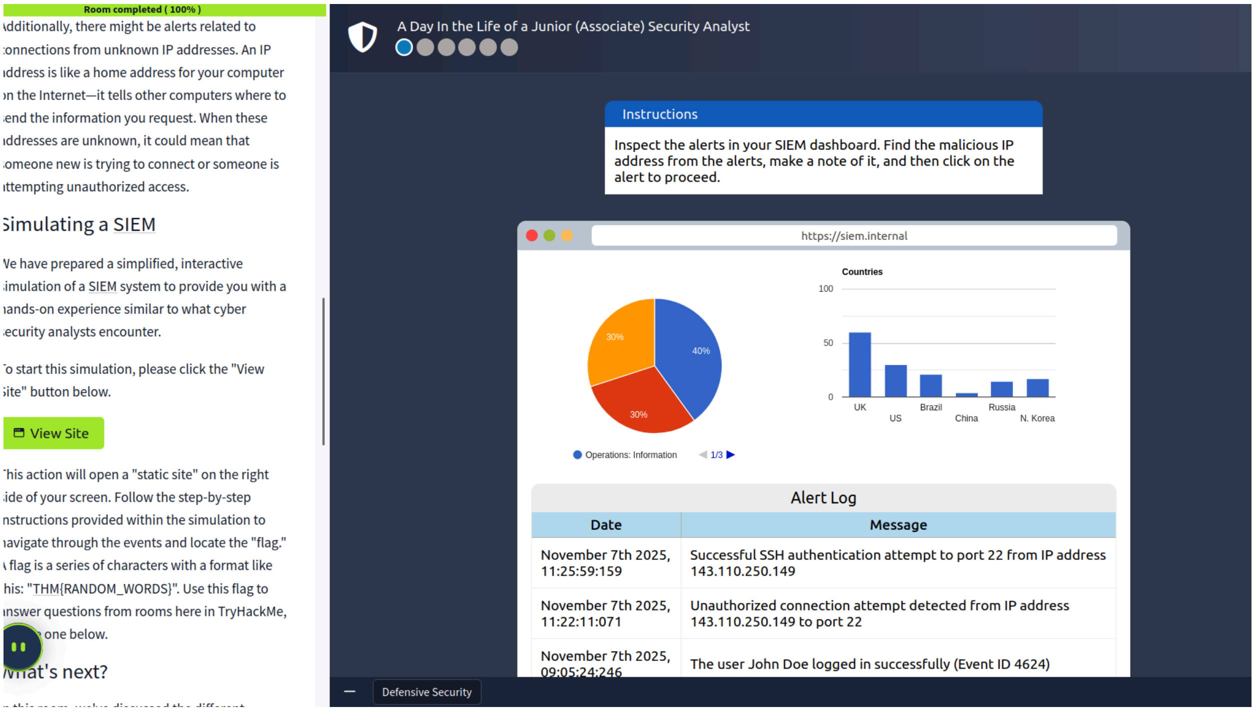
task:1

🖥️ Step 1: Launch the SIEM

- Clicked **"View Site"** to open the SIEM simulation interface.
- Observed several logs and alerts.



Room completed (100%)

dditionally, there might be alerts related to onnections from unknown IP addresses. An IP ddress is like a home address for your computer n the Internet—it tells other computers where to end the information you request. When these ddresses are unknown, it could mean that omeone new is trying to connect or someone is ttempting unauthorized access.

imulating a SIEM

Ve have prepared a simplified, interactive imulation of a SIEM system to provide you with a ands-on experience similar to what cyber ecurity analysts encounter.

o start this simulation, please click the "View ite" button below.

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

hat's next?

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

Instructions

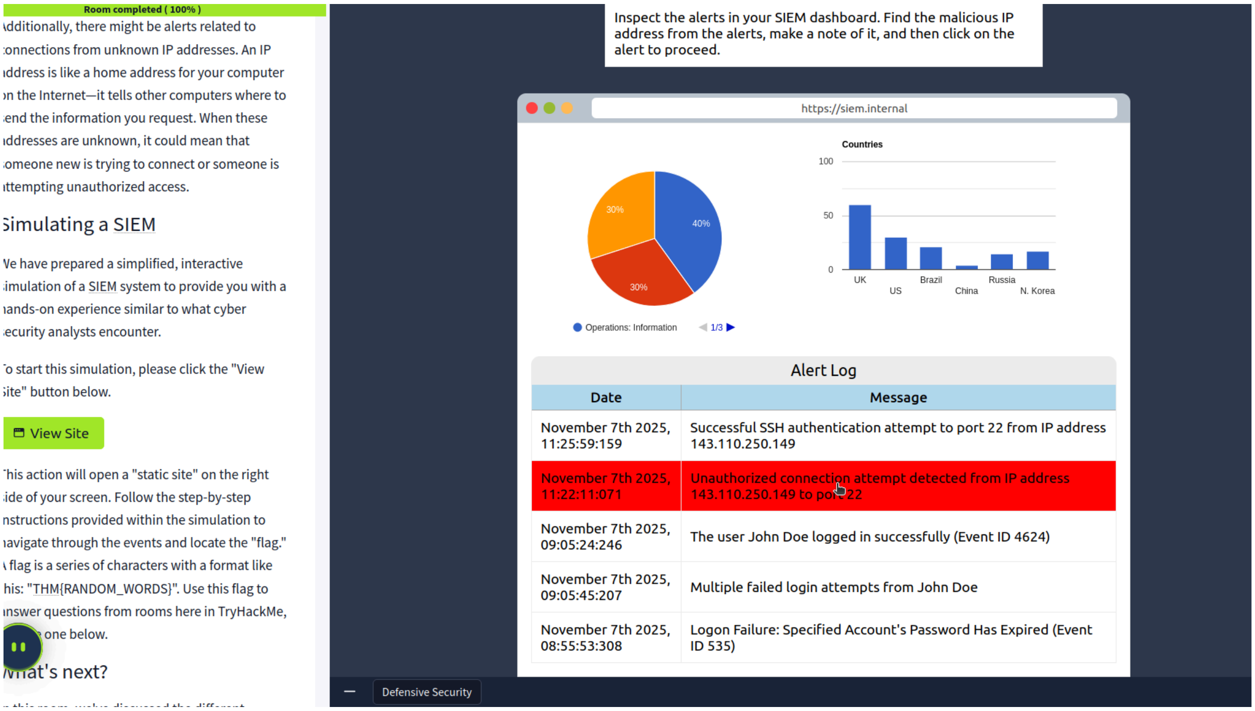
Inspect the alerts in your SIEM dashboard. Find the malicious IP address from the alerts, make a note of it, and then click on the alert to proceed.

Alert Log

Date	Message
November 7th 2025, 11:25:59:159	Successful SSH authentication attempt to port 22 from IP address 143.110.250.149
November 7th 2025, 11:22:11:071	Unauthorized connection attempt detected from IP address 143.110.250.149 to port 22
November 7th 2025, 09:05:24:246	The user John Doe logged in successfully (Event ID 4624)

🚨 Step 2: Identify Suspicious Activity

- Found an alert for a **successful login attempt** from a **suspicious unknown IP address**.
- Recognized this as a potential **unauthorized access**.



ıdditionally, there might be alerts related to :onnections from unknown IP addresses. An IP ıddress is like a home address for your computer ›n the Internet—it tells other computers where to ;end the information you request. When these ıddresses are unknown, it could mean that ;omeone new is trying to connect or someone is ıttempting unauthorized access.

Simulating a SIEM

Ve have prepared a simplified, interactive ;imulation of a SIEM system to provide you with a ıands-on experience similar to what cyber ;ecurity analysts encounter.

'o start this simulation, please click the "View ;ite" button below.

'his action will open a "static site" on the right ;ide of your screen. Follow the step-by-step nstructions provided within the simulation to ıavigate through the events and locate the "flag." ٨ flag is a series of characters with a format like his: "THM{RANDOM_WORDS}". Use this flag to ınswer questions from rooms here in TryHackMe, one below.

Vhat's next?

n this room, we've discussed the different

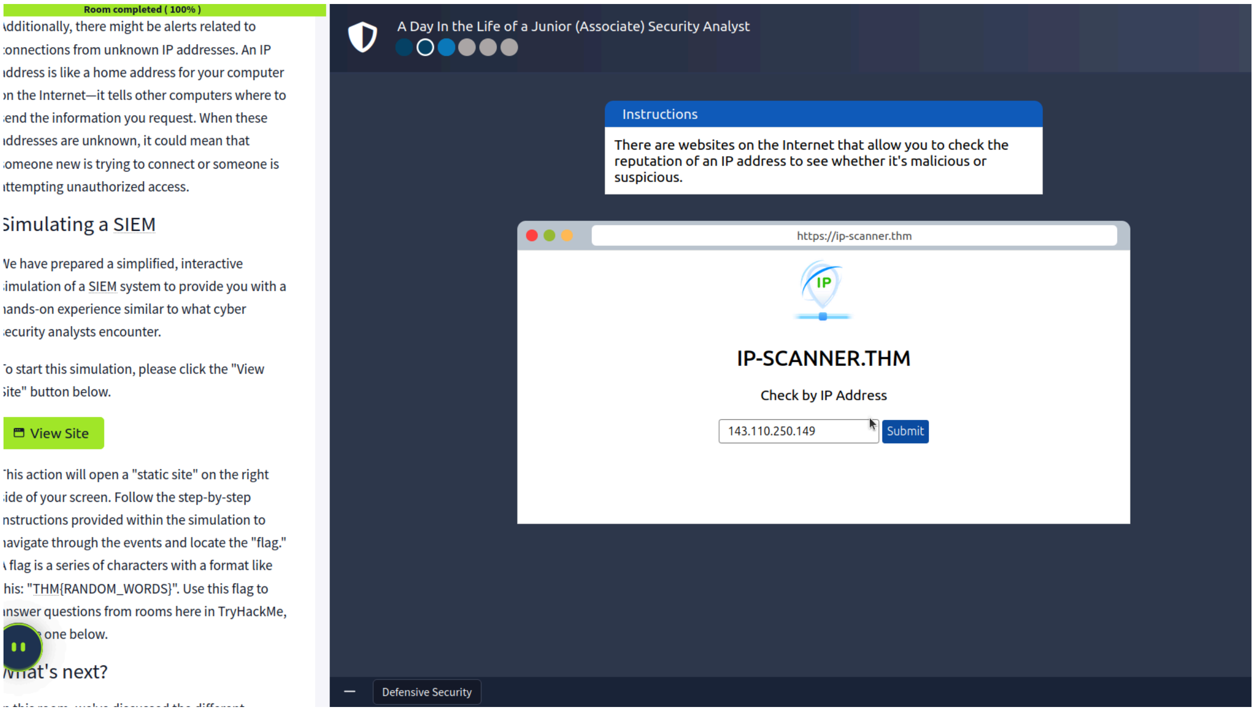
Inspect the alerts in your SIEM dashboard. Find the malicious IP address from the alerts, make a note of it, and then click on the alert to proceed.

Alert Log

Date	Message
November 7th 2025, 11:25:59:159	Successful SSH authentication attempt to port 22 from IP address 143.110.250.149
November 7th 2025, 11:22:11:071	Unauthorized connection attempt detected from IP address 143.110.250.149 to port 22
November 7th 2025, 09:05:24:246	The user John Doe logged in successfully (Event ID 4624)
November 7th 2025, 09:05:45:207	Multiple failed login attempts from John Doe
November 7th 2025, 08:55:53:308	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

🕵️ Step 3: Investigate the IP Address

- Scanned the IP.
- Confirmed it was flagged as **malicious**.



Room completed (100%)

\dditionally, there might be alerts related to :onnections from unknown IP addresses. An IP ıddress is like a home address for your computer ɔn the Internet—it tells other computers where to ;end the information you request. When these ıddresses are unknown, it could mean that ;omeone new is trying to connect or someone is ıttempting unauthorized access.

Simulating a SIEM

Ve have prepared a simplified, interactive ;imulation of a SIEM system to provide you with a ıands-on experience similar to what cyber ;ecurity analysts encounter.

'o start this simulation, please click the "View ;ite" button below.

View Site

'his action will open a "static site" on the right ;ide of your screen. Follow the step-by-step nstructions provided within the simulation to ıavigate through the events and locate the "flag." \ flag is a series of characters with a format like his: "THM{RANDOM_WORDS}". Use this flag to ınswer questions from rooms here in TryHackMe, one below.

Vhat's next?

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

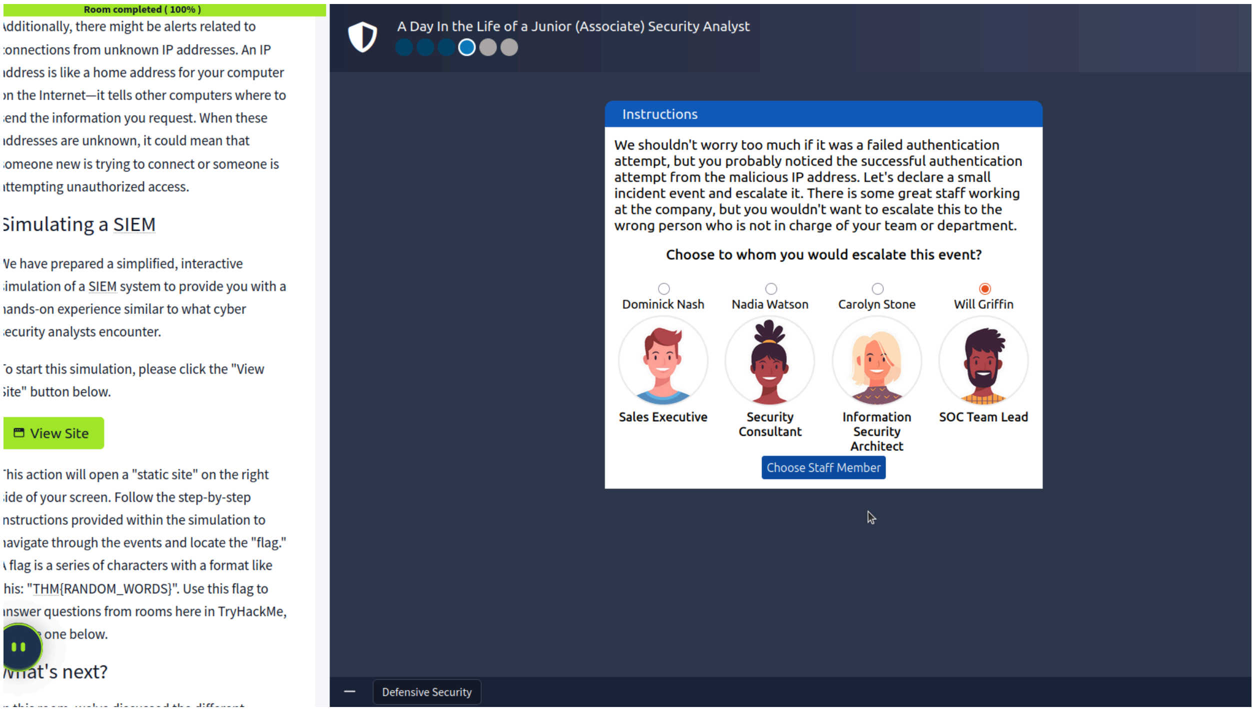
143.110.250.149

Submit

Defensive Security

📈 Step 4: Escalate the Incident

- From the list of employees, the correct escalation path was:
  ✅ **Will Griffin – SOC Team Lead**



Room completed (100%)

dditionally, there might be alerts related to onnections from unknown IP addresses. An IP ddress is like a home address for your computer n the Internet—it tells other computers where to end the information you request. When these ddresses are unknown, it could mean that omeone new is trying to connect or someone is ttempting unauthorized access.

imulating a SIEM

Ve have prepared a simplified, interactive imulation of a SIEM system to provide you with a ands-on experience similar to what cyber ecurity analysts encounter.

o start this simulation, please click the "View ite" button below.

View Site

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

at's next?

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?

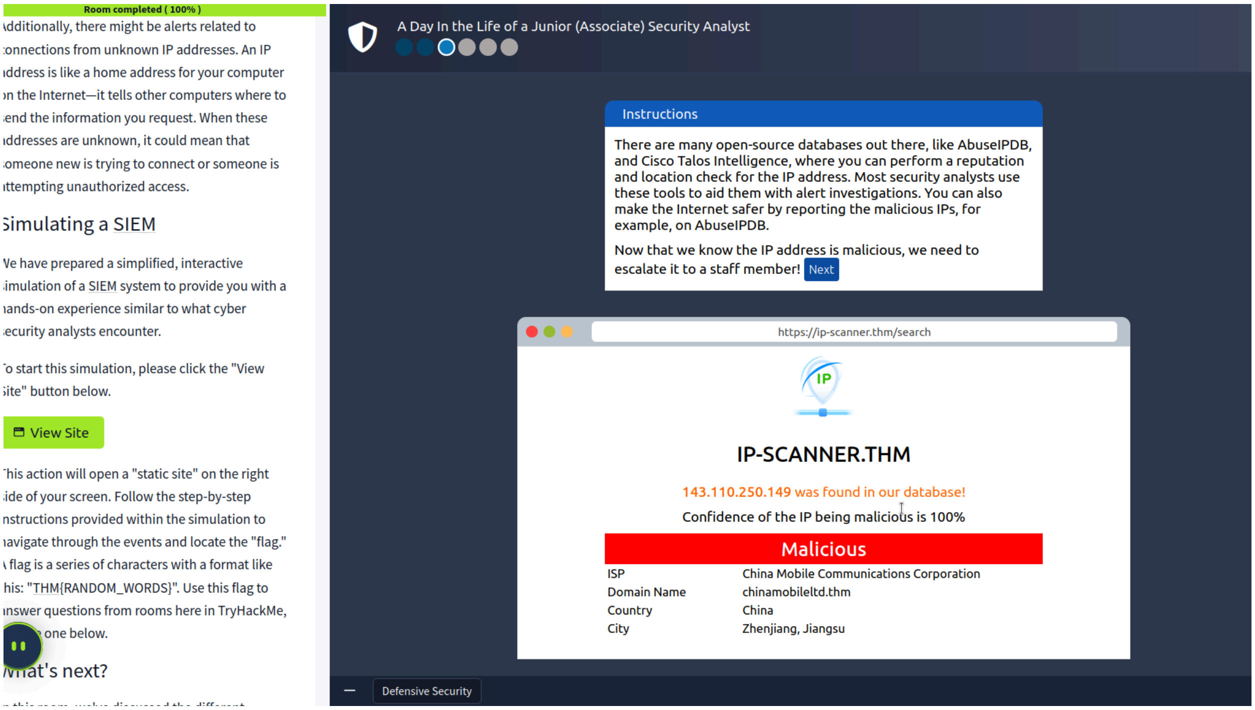
○ Dominick Nash – Sales Executive
○ Nadia Watson – Security Consultant
○ Carolyn Stone – Information Security Architect
● Will Griffin – SOC Team Lead

Choose Staff Member

Why?

- SOC (Security Operations Center) is the right team to handle malicious activity.

- Will Griffin's role matches the responsibility for incident response.



Room completed (100%)

dditionally, there might be alerts related to onnections from unknown IP addresses. An IP ddress is like a home address for your computer n the Internet—it tells other computers where to end the information you request. When these ddresses are unknown, it could mean that omeone new is trying to connect or someone is ttempting unauthorized access.

imulating a SIEM

e have prepared a simplified, interactive imulation of a SIEM system to provide you with a ands-on experience similar to what cyber ecurity analysts encounter.

o start this simulation, please click the "View ite" button below.

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

at's next?

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

Instructions

There are many open-source databases out there, like AbuseIPDB, and Cisco Talos Intelligence, where you can perform a reputation and location check for the IP address. Most security analysts use these tools to aid them with alert investigations. You can also make the Internet safer by reporting the malicious IPs, for example, on AbuseIPDB.

Now that we know the IP address is malicious, we need to escalate it to a staff member! Next

https://ip-scanner.thm/search

IP-SCANNER.THM

143.110.250.149 was found in our database!

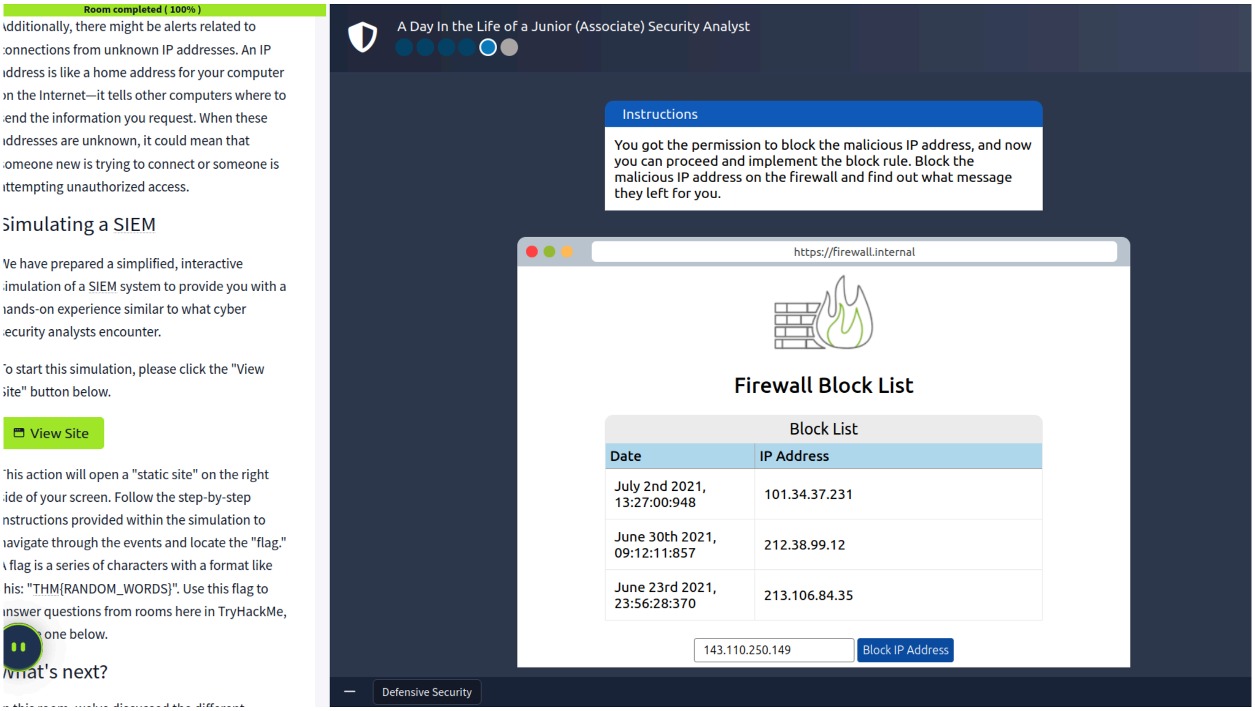
Confidence of the IP being malicious is 100%

Malicious

ISP	China Mobile Communications Corporation
Domain Name	chinamobileltd.thm
Country	China
City	Zhenjiang, Jiangsu

🔒 Step 5: Block the IP Address

- Used the firewall interface to block the malicious IP.
- After blocking, a flag was revealed.


Room completed (100%)
View Site
A Day In the Life of a Junior (Associate) Security Analyst
https://firewall.internal
Block IP Address
Defensive Security

ıdditionally, there might be alerts related to :onnections from unknown IP addresses. An IP ıddress is like a home address for your computer ın the Internet—it tells other computers where to ;end the information you request. When these ıddresses are unknown, it could mean that ;omeone new is trying to connect or someone is ıttempting unauthorized access.

Simulating a SIEM

Ve have prepared a simplified, interactive ;imulation of a SIEM system to provide you with a ıands-on experience similar to what cyber ;ecurity analysts encounter.

'o start this simulation, please click the "View ;ite" button below.

'his action will open a "static site" on the right ;ide of your screen. Follow the step-by-step nstructions provided within the simulation to ıavigate through the events and locate the "flag." ι flag is a series of characters with a format like his: "THM{RANDOM_WORDS}". Use this flag to ınswer questions from rooms here in TryHackMe, one below.

What's next?

Instructions

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.

Firewall Block List

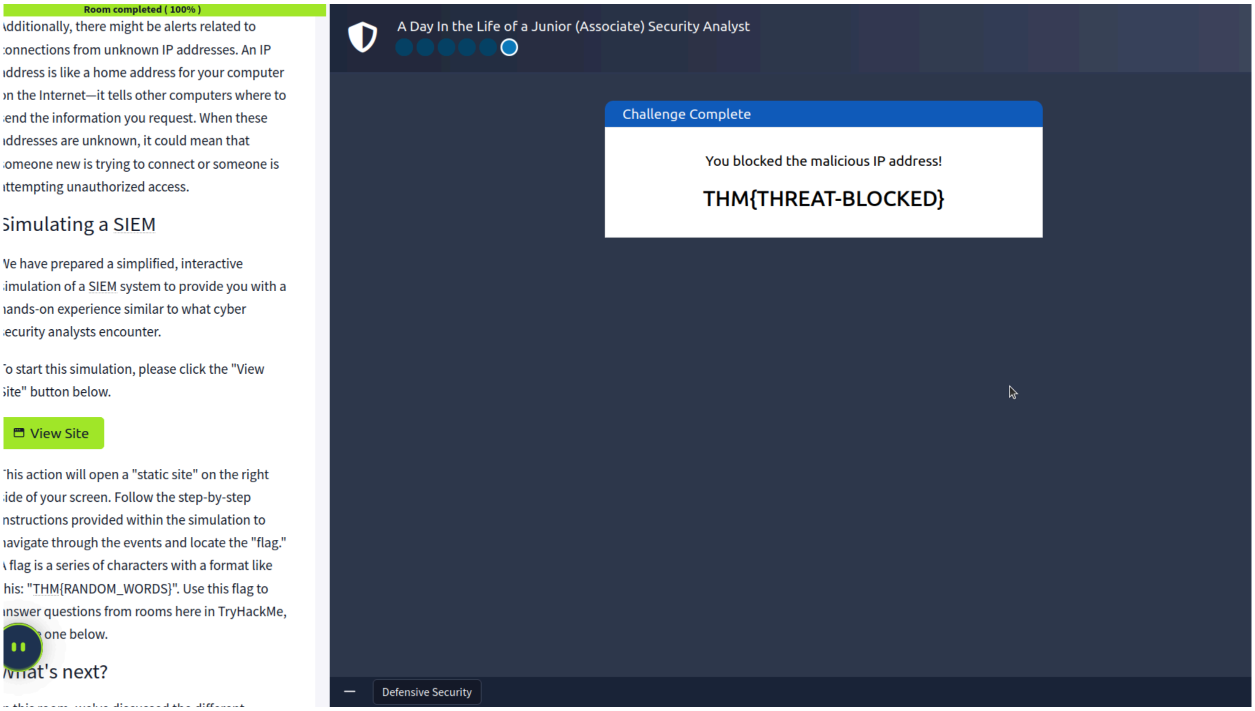
Block List

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

143.110.250.149

🚩 Final Flag

- **Flag Obtained**: `THM{THREAT-BLOCKED}`
- Submitted the flag successfully to complete the room.



Room completed (100%)

dditionally, there might be alerts related to onnections from unknown IP addresses. An IP ddress is like a home address for your computer n the Internet—it tells other computers where to end the information you request. When these ddresses are unknown, it could mean that omeone new is trying to connect or someone is ttempting unauthorized access.

imulating a SIEM

Ve have prepared a simplified, interactive imulation of a SIEM system to provide you with a ands-on experience similar to what cyber ecurity analysts encounter.

o start this simulation, please click the "View ite" button below.

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

at's next?

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

Challenge Complete

You blocked the malicious IP address!

THM{THREAT-BLOCKED}