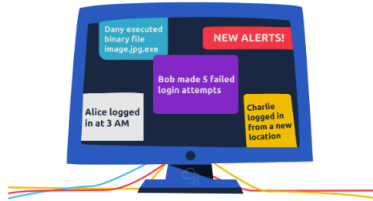


What would be a typical task that you will be doing as a security analyst? Click on "View Site" to follow along.

[View Site](#)



You are part of a *Security Operations Center (SOC)* responsible for protecting a bank. This bank's SOC uses a *Security Information and Event Management (SIEM)* system. A SIEM gathers security-related information and events from various sources and presents them via one system. For instance, you would be notified if there is a failed login attempt or a login attempt from an unexpected geographic location. Moreover, with the advent of machine learning, a SIEM might detect unusual behavior, such as a user logging in at 3 AM when he usually logs in only during work hours.

In this exercise, we will interact with a SIEM to monitor the different events on our network and systems in real-time. Some of the events are typical and harmless; others might require further intervention from us. Find the event flagged in red, take note of it, and click on it for further inspection.

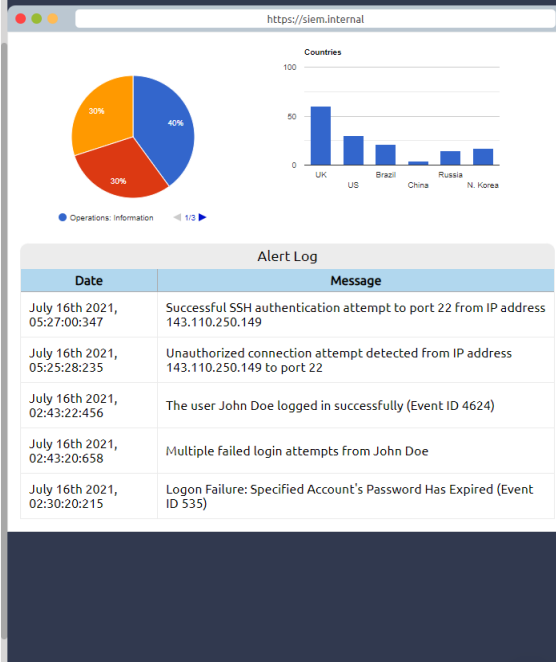
Next, we want to learn more about the suspicious activity or event. The suspicious event might have been triggered by an event, such as a local user, a local computer, or a remote IP address. To send and receive postal mail, you need a physical address; similarly, you need an IP address to send and receive data over the Internet. An IP address is a logical address that allows you to communicate over the Internet. We inspect the cause of the trigger to confirm whether the event is indeed malicious. If it is malicious, we need to take due action, such as reporting to someone else in the SOC and blocking the IP address.

**Answer the questions below**

What is the flag that you obtained by following along?

#### Instructions

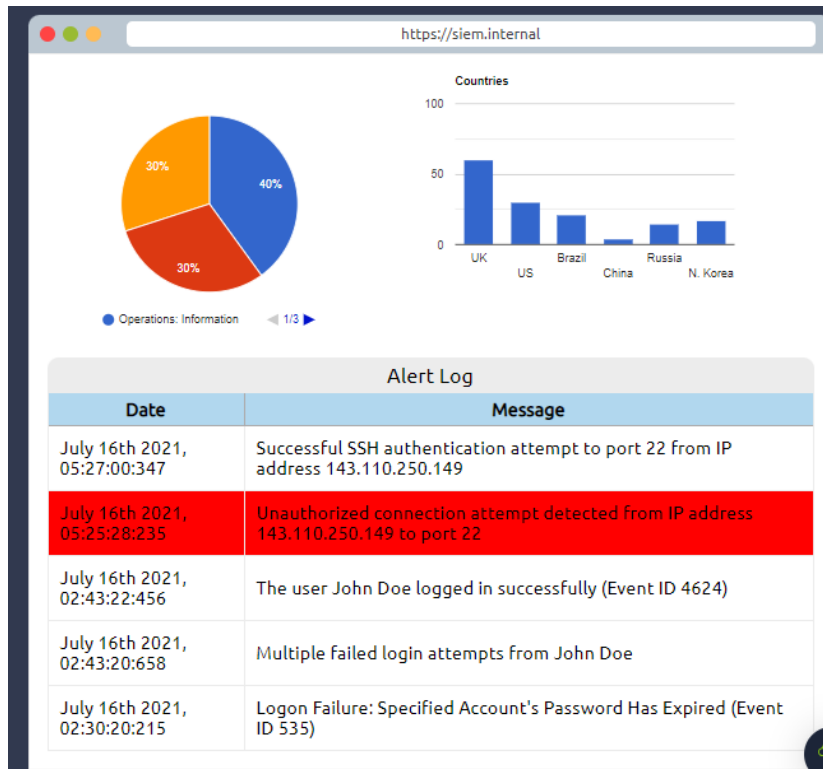
Inspect the alerts in your SIEM dashboard. Find the malicious IP address from the alerts, make a note of it, and then click on the alert to proceed.



#### 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.

From the list of the Alert Logs on the right side, there are alerts giving notices on recent activity.



Unauthorized connection attempt detected.

After selecting the option, the next step is to enter the IP to scan for its origin and information.

The screenshot shows the IP-Scanner.THM search interface with the URL <https://ip-scanner.thm>. It has a search bar with the IP address '143.110.250.149' and a 'Submit' button.

The screenshot shows the search results for the IP address 143.110.250.149. It indicates that the IP was found in the database with 100% confidence of being malicious. The results are categorized as 'Malicious' and include details about the ISP, domain name, country, and city.

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

#### 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!


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

Best to inform the Team Lead of the findings and report it.

Instruction:

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.

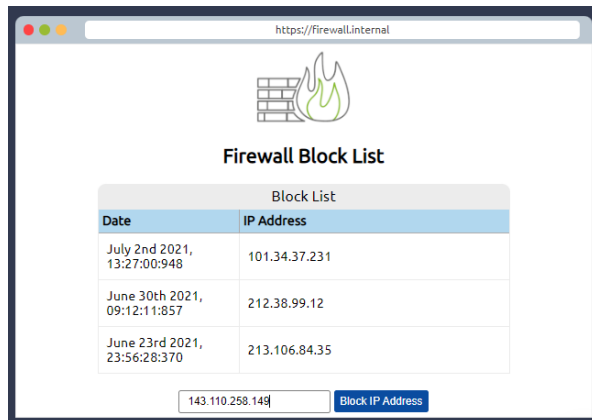
https://Firewall.Internal



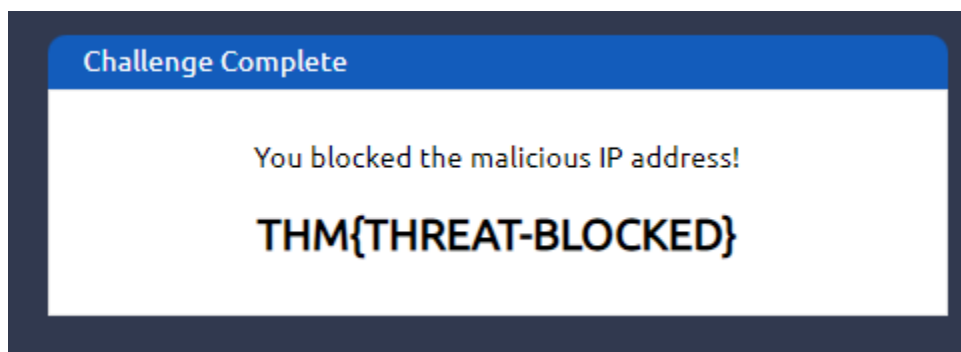
Firewall Block List

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



**143.110.250.149**



*Answer the questions below*

What is the flag that you obtained by following along?

THM{THREAT-BLOCKED}

Correct Answer