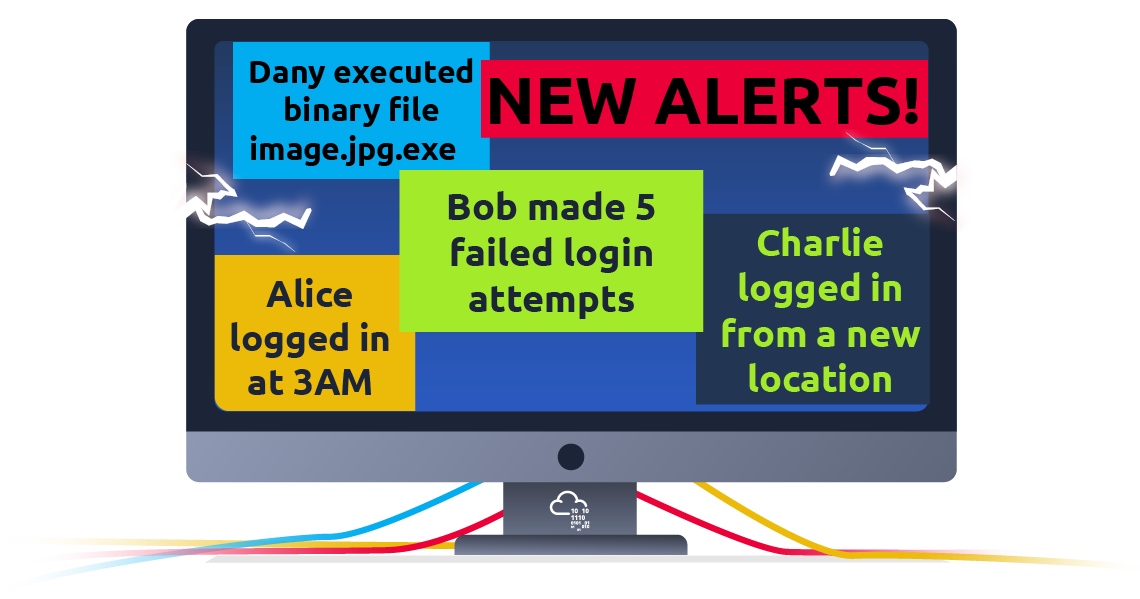
Task 3Practical Example of Defensive Security

The Scenario

Let us pretend you are a *Security Operations Center* (SOC) analyst responsible for protecting a bank. This bank's SOC uses a *Security Information and Event Management* (SIEM) tool, which gathers security-related information and events from various sources and presents them in one dashboard. If the SIEM finds something suspicious, an alert will be generated.



Not all alerts are malicious, however. It is up to the analyst to use their expertise in cyber security to investigate which ones are harmful.

For example, you may encounter an alert where a user has failed multiple login attempts. While suspicious, this kind of thing happens, especially if the user has forgotten their password and continues to try to log in.

Additionally, there might be alerts related to connections from unknown IP addresses. An IP address is like a home address for your computer on the Internet—it tells other computers where to send the information you request. When these addresses are unknown, it could mean that someone new is trying to connect or someone is attempting unauthorized access.

Simulating a SIEM

We have prepared a simplified, interactive simulation of a SIEM system to provide you with a hands-on experience similar to what cyber security analysts encounter.

To start this simulation, please click the "View Site" button below.

View Site

This action will open a "static site" on the right side of your screen. Follow the step-by-step instructions provided within the simulation to navigate through the events and locate the "flag." A flag is a series of characters with a format like this: "THM{RANDOM\_WORDS}". Use this flag to answer questions from rooms here in TryHackMe, like the one below.

What's next?

In this room, we've discussed the different subfields (SOC, Threat Intelligence, Malware Analysis, and DFIR) and experienced firsthand how to deal with alerts in a simulated SIEM environment. While we've covered a lot, the depth and complexity of this field mean there's more to learn and explore. The lessons learned here will serve as your foundation as cyber threats evolve, demanding continuous learning, vigilance, and adaptation.

Continue learning by checking out the next room in this series, "Search Skills." This room will teach you valuable techniques for searching for information online to aid your investigations and learning.

If you want to skip ahead and learn more about the topics discussed in this room, the following rooms are recommended:

* [Introduction to SIEM](https://tryhackme.com/r/room/introtosiem) - An Introduction to Security Information and Event Management
* [Security Operations](https://tryhackme.com/r/room/securityoperations) - Learn about the Security Operations Center (SOC): its responsibilities, services, and data sources
* [DFIR : An Introduction](https://tryhackme.com/r/room/introductoryroomdfirmodule) - Introductory room for the DFIR module
* [Intro to Malware Analysis](https://tryhackme.com/r/room/intromalwareanalysis) - What to do when you run into a suspected malware

Answer the questions below

What is the flag that you obtained by following along?

Top of Form

Your answer is too short. Please make sure it matches the answer format represented by underscores.

Bottom of Form