



## Intro to Defensive Security

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

<https://tryhackme.com/room/defensivesecurity>

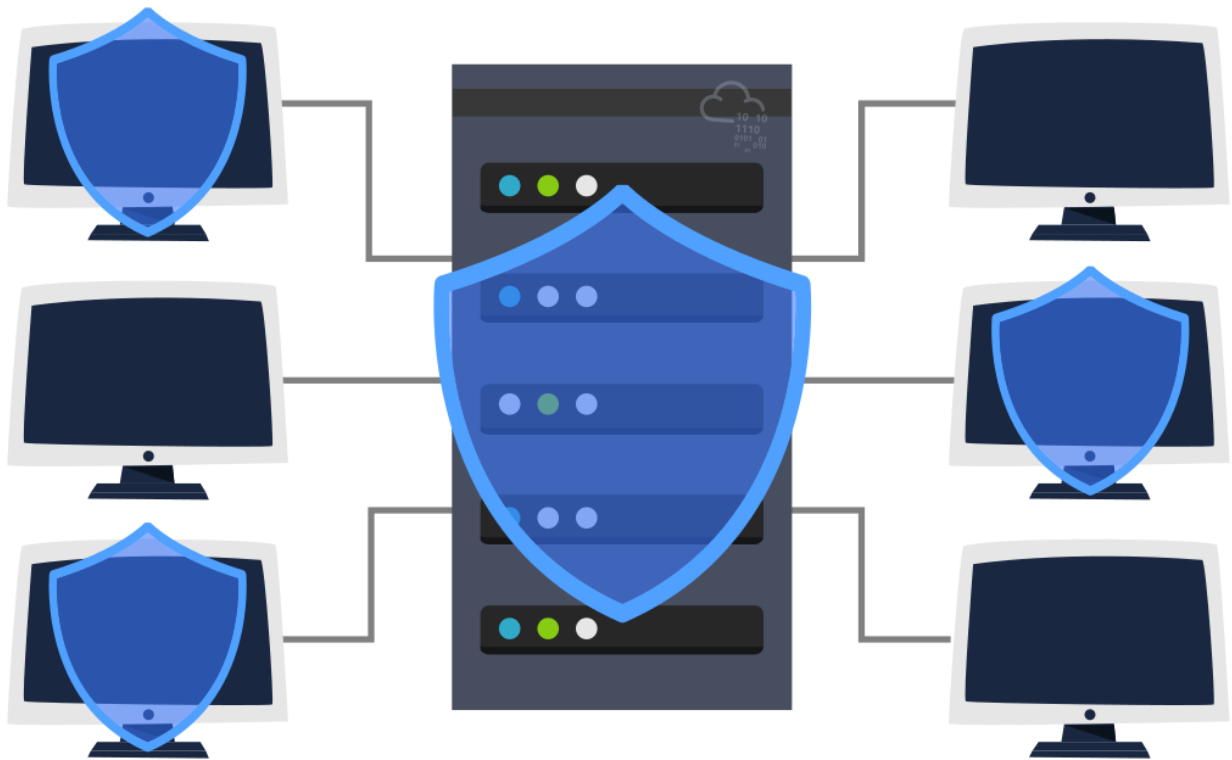
## Task 1 Introduction to Defensive Security

Offensive security focuses on one thing: breaking into systems. Breaking into systems might be achieved through exploiting bugs, abusing insecure setups, and taking advantage of unenforced access control policies, among other things. Red teams and penetration testers specialize in offensive security.

Defensive security is somewhat the opposite of offensive security, as it is concerned with two main tasks:

1. Preventing intrusions from occurring
2. Detecting intrusions when they occur and responding properly

Blue teams are part of the defensive security landscape.



Some of the tasks that are related to defensive security include:

- User cyber security awareness: Training users about cyber security helps protect against various attacks that target their systems.
- Documenting and managing assets: We need to know the types of systems and devices that we have to manage and protect properly.
- Updating and patching systems: Ensuring that computers, servers, and network devices are correctly updated and patched against any known vulnerability (weakness).
- Setting up preventative security devices: firewall and intrusion prevention systems (IPS) are critical components of preventative security. Firewalls control what network traffic can go inside and what can leave the system or network. IPS blocks any network traffic that matches present rules and attack signatures.
- Setting up logging and monitoring devices: Without proper logging and monitoring of the network, it won't be possible to detect malicious activities and intrusions. If a new unauthorized device appears on our network, we should be able to know.

There is much more to defensive security, and the list above only covers a few common topics.

In this room, we cover:

- Security Operations Center (SOC)
- Threat Intelligence
- Digital Forensics and Incident Response (DFIR)
- Malware Analysis

Answer the questions below

Which team focuses on defensive security?

Blue Team

## Task 2 Areas of Defensive Security

In this task, we will cover two main topics related to defensive security:

- Security Operations Center (SOC), where we cover Threat Intelligence

- Digital Forensics and Incident Response (DFIR), where we also cover Malware Analysis

## Security Operations Center (SOC)

A *Security Operations Center* (SOC) is a team of cyber security professionals that monitors the network and its systems to detect malicious cyber security events. Some of the main areas of interest for a SOC are:

- **Vulnerabilities:** Whenever a system vulnerability (weakness) is discovered, it is essential to fix it by installing a proper update or patch. When a fix is not available, the necessary measures should be taken to prevent an attacker from exploiting it. Although remediating vulnerabilities is of vital interest to a SOC, it is not necessarily assigned to them.
- **Policy violations:** We can think of a security policy as a set of rules required for the protection of the network and systems. For example, it might be a policy violation if users start uploading confidential company data to an online storage service.
- **Unauthorized activity:** Consider the case where a user's login name and password are stolen, and the attacker uses them to log into the network. A SOC needs to detect such an event and block it as soon as possible before further damage is done.
- **Network intrusions:** No matter how good your security is, there is always a chance for an intrusion. An intrusion can occur when a user clicks on a malicious link or when an attacker exploits a public server. Either way, when an intrusion occurs, we must detect it as soon as possible to prevent further damage.

Security operations cover various tasks to ensure protection; one such task is threat intelligence.



## Threat Intelligence

In this context, *intelligence* refers to information you gather about actual and potential enemies. A *threat* is any action that can disrupt or adversely affect a system. Threat intelligence aims to gather information to help the company better prepare against potential adversaries. The purpose would be to achieve a *threat-informed defense*. Different companies have different adversaries. Some adversaries might seek to steal customer data from a mobile operator; however, other adversaries are interested in halting the production in a petroleum refinery. Example adversaries include a nation-state cyber army working for political reasons and a ransomware group acting for financial purposes. Based on the company (target), we can expect adversaries.



Intelligence needs data. Data has to be collected, processed, and analyzed. Data collection is done from local sources such as network logs and public sources such as forums. Processing of data aims to arrange them into a format suitable for analysis. The analysis phase seeks to find more information about the attackers and their motives; moreover, it aims to create a list of recommendations and actionable steps.

Learning about your adversaries allows you to know their tactics, techniques, and procedures. As a result of threat intelligence, we identify the threat actor (adversary), predict their activity, and consequently, we will be able to mitigate their attacks and prepare a response strategy.

## Digital Forensics and Incident Response (DFIR)

This section is about Digital Forensics and Incident Response (DFIR), and we will cover:

- Digital Forensics
- Incident Response
- Malware Analysis

### Digital Forensics

Forensics is the application of science to investigate crimes and establish facts. With the use and spread of digital systems, such as computers and smartphones, a new branch of forensics was born to investigate related crimes: computer forensics, which later evolved into, *digital forensics*.

In defensive security, the focus of digital forensics shifts to analyzing evidence of an attack and its perpetrators and other areas such as intellectual property theft, cyber espionage, and possession of unauthorized content. Consequently, digital forensics will focus on different areas such as:

- File System: Analyzing a digital forensics image (low-level copy) of a system's storage reveals much information, such as installed programs, created files, partially overwritten files, and deleted files.
- System memory: If the attacker is running their malicious program in memory without saving it to the disk, taking a forensic image (low-level copy) of the system memory is the best way to analyze its contents and learn about the attack.
- System logs: Each client and server computer maintains different log files about what is happening. Log files provide plenty of information about what happened on a system. Some traces will be left even if the attacker tries to clear their traces.

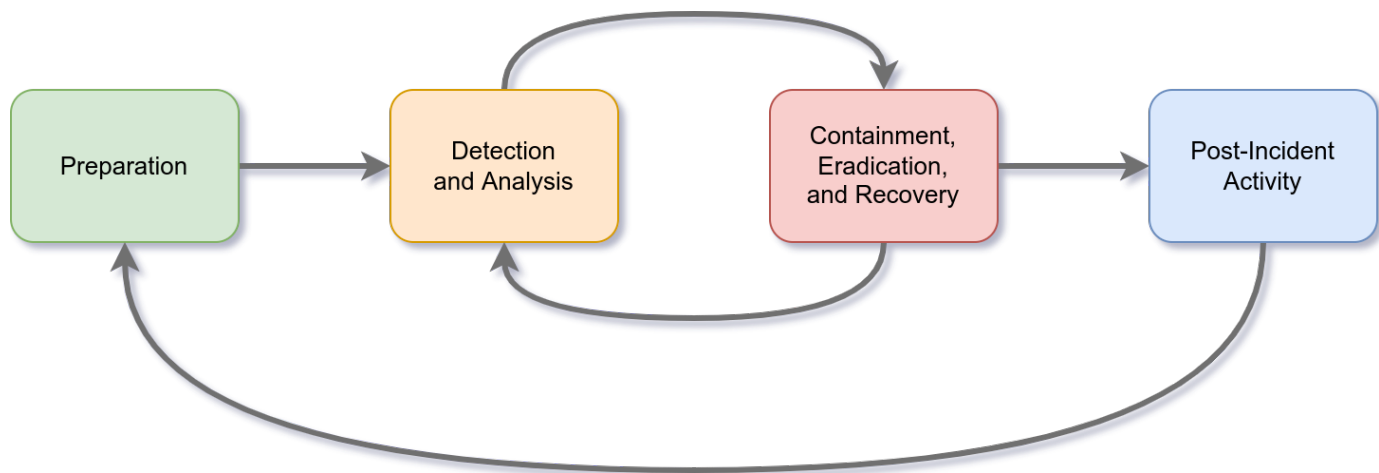
- Network logs: Logs of the network packets that have traversed a network would help answer more questions about whether an attack is occurring and what it entails.

## Incident Response

An *incident* usually refers to a data breach or cyber attack; however, in some cases, it can be something less critical, such as a misconfiguration, an intrusion attempt, or a policy violation. Examples of a cyber attack include an attacker making our network or systems inaccessible, defacing (changing) the public website, and data breach (stealing company data). How would you *respond* to a cyber attack? Incident response specifies the methodology that should be followed to handle such a case. The aim is to reduce damage and recover in the shortest time possible. Ideally, you would develop a plan ready for incident response.

The four major phases of the incident response process are:

1. Preparation: This requires a team trained and ready to handle incidents. Ideally, various measures are put in place to prevent incidents from happening in the first place.
2. Detection and Analysis: The team has the necessary resources to detect any incident; moreover, it is essential to further analyze any detected incident to learn about its severity.
3. Containment, Eradication, and Recovery: Once an incident is detected, it is crucial to stop it from affecting other systems, eliminate it, and recover the affected systems. For instance, when we notice that a system is infected with a computer virus, we would like to stop (contain) the virus from spreading to other systems, clean (eradicate) the virus, and ensure proper system recovery.
4. Post-Incident Activity: After successful recovery, a report is produced, and the learned lesson is shared to prevent similar future incidents.



## Malware Analysis

Malware stands for malicious software. *Software* refers to programs, documents, and files that you can save on a disk or send over the network. Malware includes many types, such as:

- Virus is a piece of code (part of a program) that attaches itself to a program. It is designed to spread from one computer to another; moreover, it works by altering, overwriting, and deleting files once it infects a computer. The result ranges from the computer becoming slow to unusable.
- Trojan Horse is a program that shows one desirable function but hides a malicious function underneath. For example, a victim might download a video player from a shady website that gives the attacker complete control over their system.
- Ransomware is a malicious program that encrypts the user's files. Encryption makes the files unreadable without knowing the encryption password. The attacker offers the user the encryption password if the user is willing to pay a "ransom."



Malware analysis aims to learn about such malicious programs using various means:

1. Static analysis works by inspecting the malicious program without running it. Usually, this requires solid knowledge of assembly language (processor's instruction set, i.e., computer's fundamental instructions).
2. Dynamic analysis works by running the malware in a controlled environment and monitoring its activities. It lets you observe how the malware behaves when running.

Answer the questions below

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?

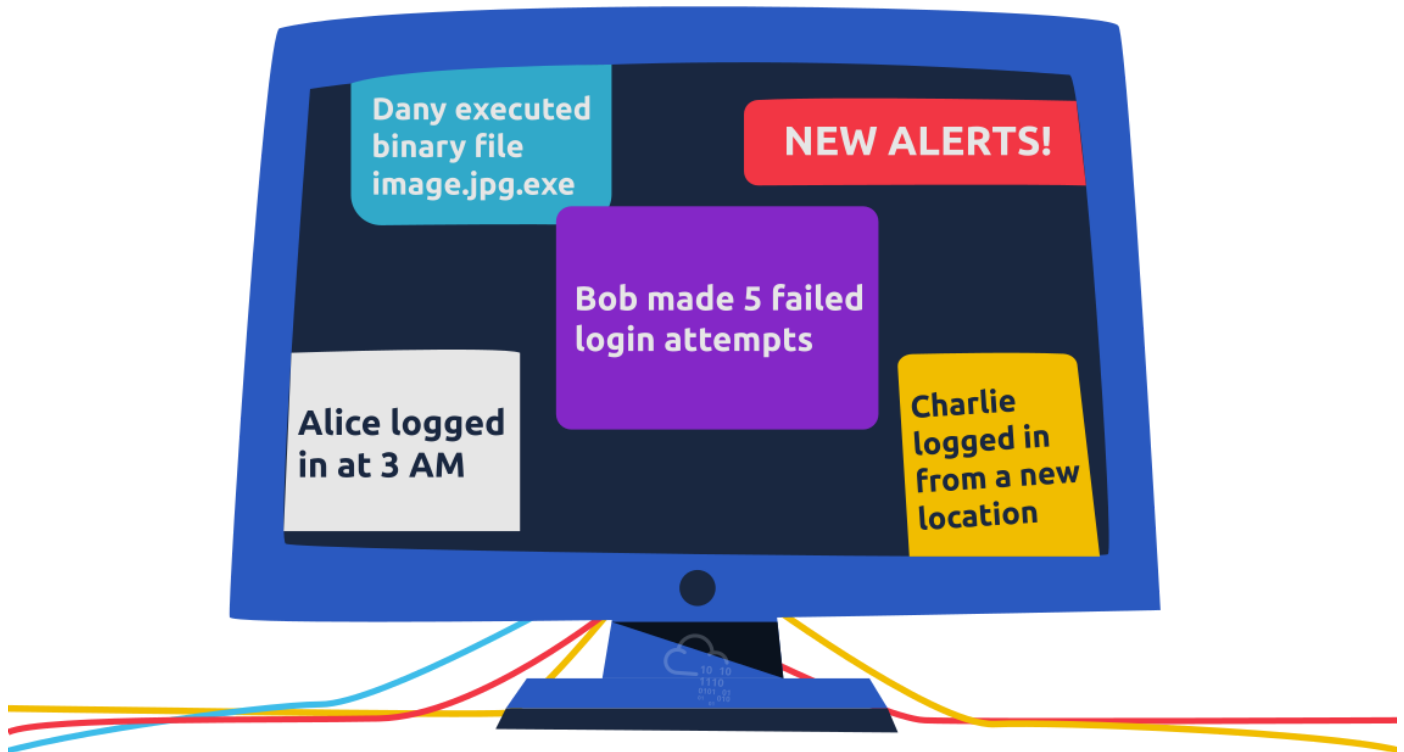
Digital Forensics and Incident Response

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



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

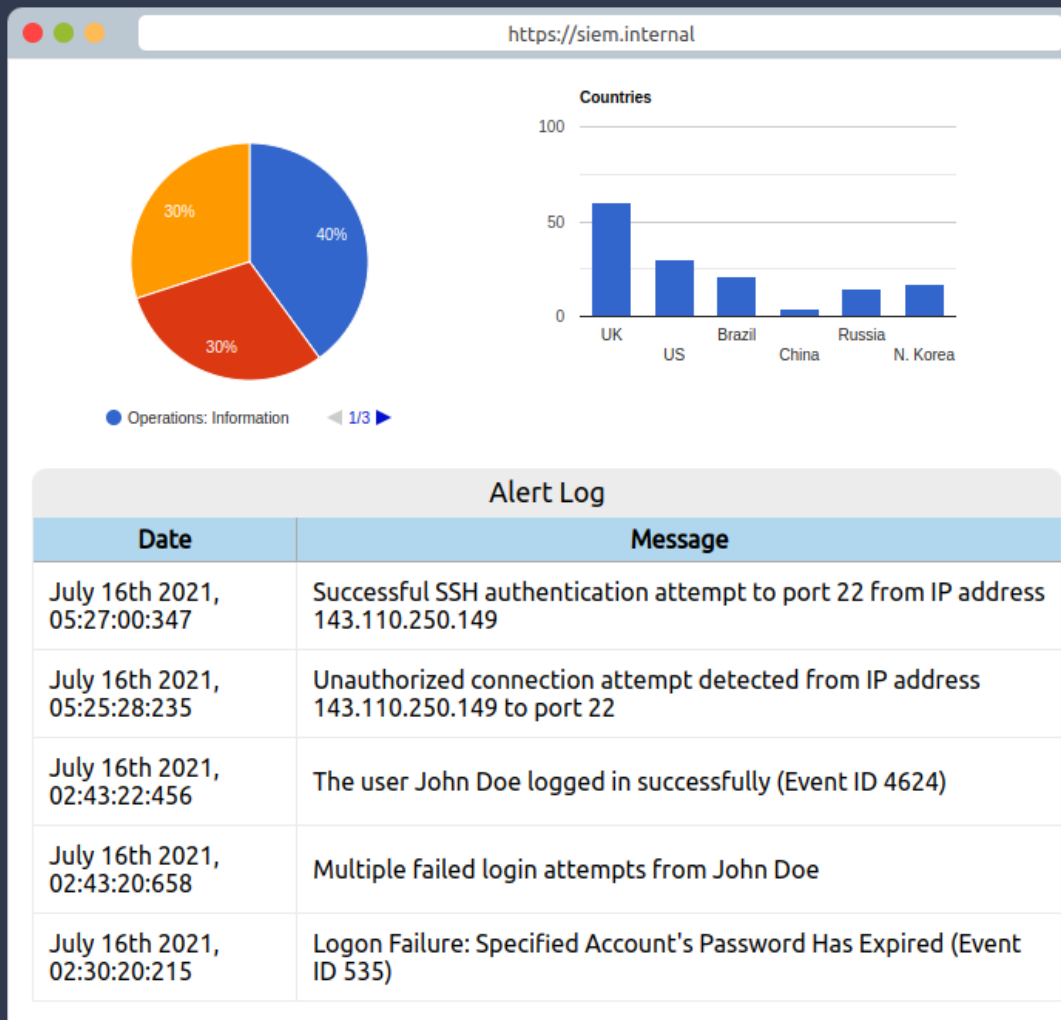
What is the flag that you obtained by following along?

THM{THREAT-BLOCKED}



## 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

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.

The screenshot shows a web browser window with the address bar displaying `https://ip-scanner.thm`. The page features a logo with a blue shield and a green 'IP' inside. Below the logo, the text 'IP-SCANNER.THM' is prominently displayed. Underneath, it says 'Check by IP Address'. There is a text input field containing the IP address '143.110.250.149' and a blue 'Submit' button to its right.

https://ip-scanner.thm



## IP-SCANNER.THM

Check by IP Address

### 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


### 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](#)

### 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.

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

### Challenge Complete

You blocked the malicious IP address!

**THM{THREAT-BLOCKED}**