

Overview - Threat Defense Operations

Note
5m

✓ Status Incomplete

Do you wonder how Cyber Security professionals detect suspicious behavior on their company network? What tools, technologies, and processes do they utilize to detect a potential threat? The course Threat Defense Operations explores some of these questions, and much more.

In this course, you will learn how to use strategic as well as tactical intelligence to safeguard the security posture of an organization. You will also learn how frameworks like MITRE ATT&CK and Cyber Kill Chain can be used to continuously improve network defense. As you work through this course, you will develop relevant knowledge and skills that are needed to detect, analyze, and mitigate various types of threats in a modern digital landscape.

By the end of this course, you will be able to:

- Explore how to extract Tactical and Strategic Intelligence and consume it during Incident Response and Threat Hunting
- Acquire skill set for Intrusion Analysis and Dissemination of Intelligence, and understand Indicators of Compromise
- Explain the Threat Hunting life-cycle and create a few hypotheses for your Hunting program
- Understand and utilize frameworks like MITRE ATT&CK and Cyber Kill Chain to track and analyze cyber intrusions
- Understand and utilize security information and event management (SIEM) in the overall monitoring system of the organization

So, let’s proceed and begin with the course!

←

Previous
Course Reflection

Next
Understanding Cyber Threat Intelligence

→

W07D4 📅

Thu Aug 8

- > Lectures (1)
- < Work (7)
7 hrs
- </> Project: Encryption


 [Course Reflection](#)

 [Overview - Threat Defense Operations](#)

 [Understanding Cyber Threat Intelligence](#)

 [Threat Intelligence Platforms and Their Usage](#)

 [Threat Actors and Their Tactics](#)

 [Cyber Kill Chain & Intrusion Analysis](#)

> **Other** (1)

[W07D4 Schedule »](#)