TH-200: Foundational Threat Hunting

Duration: 90 Days

Course Description:

OffSec's Foundational Threat Hunting (TH-200) eq cybersecurity professionals with the practical skills and knowledge needed to effectively detect and respond to threats. This course covers core threat hunting concepts, exploring the methodologies used by enterprises to track and mitigate adversaries. Key areas include understanding the threat actor landscape, with a focus on ransomware and Advanced Persistent Threats (APTs) and utilizing bo network and endpoint Indicators of Compromise (IoCs) f proactive threat detection.

Course Outlines:

Threat Hunting Concepts and Practices

- This module provides an overview of the basic objectives, concepts and practices of cyber threat hunting. It covers how enterprises implement threat hunting and the different stages and types of threat hunts.

Threat Actor Landscape Overview

- This module provides an overview of different types of threat actors with an emphasis on ransomware actors and Advanced Persistent Threats (APTs). It includes number of more in-depth discussions of well-known threat actors.

Communication and Reporting for Threat Hunters

- This module introduces the way in which threat hunters receive and use threat intelligence and create threat reports. It covers the concept of the Traffic Light Protocol but does not cover IoCs.

Hunting with Network Data

- This module explores using Network Indicators of Compromise (IoCs) for proactive threat hunting. It highlights the role of Intrusion Detection Systems (IDand Intrusion Prevention Systems (IPS), like Suricata, in monitoring for suspicious activities. Practical methods to identify signs of compromise in networks are covered, followed by hands-on exercises to develop threat detection skills.

Hunting on Endpoints

- This module provides an introduction to cyber threat hunting utilizing Endpoint IoCs. It covers intelligence-based and hypothesis-based threat hunting as well as considerations that improve the effectiveness of a hunt.

Threat Hunting without IoCs

- This module teaches threat hunting techniques that don' rely on known IoCs. It covers custom threat hunting, focusing on behavioral analysis and data correlation to detect advanced threats. Tools like CrowdStrike Falcon are used to apply these methods in practical scenarios