TH-200 OSTH

Foundational Threat Hunting

TH-200: Foundational Threat Hunting equips learners with the essential skills and mindset to operate on the defensive side of cybersecurity. In today's threat landscape, defenders must go beyond reactive security measures. Threat hunting is a proactive practice where security professionals seek out and identify threats before they can cause harm.

Threat Hunting Concepts and Practices	Learn about the different stages and types of threat hunts that enterprises use through an overview of basic objectives, concepts, and practices
Threat Actor Landscape Overview	Get an overview of various threat actors, with a focus on ransomware groups and Advanced Persistent Threats (APTs), and review in-depth discussions of several well-known actors
Communication and Reporting for Threat Hunters	Discover how threat hunters use the Traffic Light Protocol to receive and use threat intelligence to create reports
Hunting with Network Data	Use Network Indicators of Compromise (IoCs) with IDS/IPS tools like Suricata to monitor for suspicious activity, identify network compromises, and build practical threat-detection skills
Hunting on Endpoints	Hunt for threats with Endpoint IoCs and use intelligence- and hypothesis-based approaches to make your hunts more effective
Threat Hunting without IoCs	Hunt for threats without relying on known IoCs and focus on behavioral analysis and data correlation to detect advanced threats with tools like CrowdStrike Falcon