40551: Enterprise Security Fundamentals

Duration: 1 Day

Method: Instructor-Led Training (ILT) | Live Online Training

Course Description

This course provides insight into security practices to improve the security posture of an organization. The course also examines the concept of Red Team vs. Blue Team security professionals, where one group of security pros, the red team, attacks some part or parts of a company's security infrastructure, and an opposing group, the blue team, defends against the attack. Both teams work to strengthen a company's defences. Since the goal of the two teams is to help the business attain a higher level of security, the security industry is calling this function, the Purple Team.

Target Audience

This course is intended for:

- IT Professionals that require a deeper understanding of Windows Security and wish to increase their knowledge level.

Prerequisites

To attend this course, candidates must have the following technical knowledge:

- The current cyber-security ecosystem
- Analysis of hacks on computers and networks
- Basic Risk Management

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Describe the current cybersecurity landscape.
- Describe the "assume compromise" philosophy.
- Identify factors that contribute to the cost of a breach.
- Distinguish between the responsibilities of red teams and blue teams.
- Identify typical objectives of cyber attackers.
- Describe a kill chain conducted by red teams.
- Describe the role, goals, and kill chain activities of the blue team in red team exercises.
- Describe the ways limiting how an attacker can compromise unprivileged accounts.
- Describe the methods used to restrict lateral movement.
- Describe how telemetry monitoring is used to detect attacks.
- Explain the concept of Confidentiality, Integrity, and Availability (CIA) triad.
- Describe the primary activities that should be included in organization preparations.
- Identify the main principles of developing and maintaining policies.

Course Topics

Module 1: Understanding the Cyber-Security landscape

- Current Cyber-Security Landscape
- Assume Compromise Philosophy

Module 2: Red Team: Penetration, Lateral Movement, Escalation, and Exfiltration

- Red Team versus Blue Team Exercises
- The Attackers Objective
- Red Team Kill Chain

Module 3: Blue Team Detection, Investigation, Response, and Mitigation

- The Blue Team
- Blue Team Kill Chain
- Restricting Privilege Escalation
- Restrict Lateral Movement
- Attack Detection

Module 4: Organizational Preparations

- CIA Triad
- Organizational Preparations
- Developing and Maintain Policies

LABS INCLUDED