Threat Detection: Planning for a Secure Enterprise

Modality: On Demand

Duration: 16 Hours

About this Course:

Cybersecurity is the leading concern of small and large IT-based firms and organizations and cybercrime rates continue to rise with the advent of hybrid and cloud technologies. The annual damage from cybercrimes is anticipated to exceed $6 Trillion by the year 2021. These numbers clearly advocate the need for the implementation of robust cybersecurity strategies and measures to protect the viable information of business enterprises & organizations.

Besides this, the majority of cyber-attacks are caused by unmanaged devices, unapproved apps, and poor password protection practices. Focusing on Robust Threat Detection Planning for a Secure Business Enterprise, this course helps professionals and cybersecurity experts embrace digital transformation and implement cybersecurity strategies to mitigate security risks and resolve security threats and vulnerabilities.

This intermediate-level course provides an in-depth overview of modern threat detection methods and covers the key concepts of Threat Detection Monitoring & Mitigation Tools. Both on-premises and cloud solutions security is elaborated in this course including an overview of heuristic/behavioral detection methods.

Course Objectives:

The core objective of this course is to help professionals develop a better understanding and sound knowledge of the following key concepts:

- Fundamentals of Heuristic/Behavioral & Signature-Based Detection Methods
- On-Premises Mitigation and Threat Detection Tools Core Functionalities
- Windows Intrusion and Event Forwarding Detection
- Antimalware Scan Interface and Advanced Threat Analytics
- Core Features & Functionalities Cloud & Hybrid Mitigation & Threat Detection Tools
- Office 365 Threat Protection and Threat Intelligence
- Azure Auditing & Logging and Advanced Threat Detection
- Identifying the Significance of Business Threat Detection and Monitoring System
- Windows Defender Antivirus Layered Machine Learning Strategies

Audience:

- IT Support Officers & Experts
- Cybersecurity Officers
- Cybersecurity Professionals

Prerequisites:

Professionals planning to enroll in the Threat Detection: Planning for a Secure Enterprise course must comply with the following prerequisites:

- Basic Knowledge & Understanding of Current Cybersecurity Threats & Vulnerabilities
- Fundamental Knowledge of Hack Analysis on Networking Systems and Computers
- Basic Understanding of Risk Management

Course Outline:

Introduction to Threat Detection as Part of the Defense In-Depth Strategy

- An Overview of the Modern Cyber Threat Landscape
- Integrating Pre-Breach and Post-Breach Approaches to Mitigate Cyber Threats
- Comparing signature-based and behavioral heuristic detection methods
- Combating threat persistence
- Module Exam

Detecting Threats in On-Premises Environments

- Windows Event Forwarding and intrusion detection
- Microsoft Advanced Threat Analytics (ATA)
- Windows Defender Advanced Threat Protection (ATP)
- Microsoft Enterprise Threat Detection
- Microsoft Security Risk Detection
- AntiMalware Scan Interface (AMSI)
- Logging and Auditing
- Threat Detection Tools
- Module Exam

Detecting Threats in Hybrid and Cloud Environments

- Microsoft Cloud App Security and Office 365 Cloud App Security
- Office 365 Advanced Threat Protection
- Office 365 Threat Intelligence
- Azure Advanced Threat Detection
- Azure Logging and Auditing
- Microsoft Enterprise Mobility + Security (EMS)
- Microsoft 365
- Module Exam

Analyzing Threat Detection Solutions in Action

- Layered Machine Learning defenses in Windows Defender Antivirus
- Detecting persistent threats by using Windows Defender ATP
- Enterprise Threat Detection behavioral monitoring
- Microsoft comprehensive approach to cyber threat detection
- Module Exam

Course Completion

- Final Exam
- Labs?