Threat Detection: Planning for a Secure Enterprise

Modality: Self-Paced Learning

Duration: 16 Hours

SATV Value:

CLC:

NATU:

SUBSCRIPTION: Learn, Master

About this course:

By 2021, worldwide cybercrime damage is expected to reach $6 trillion—double what it cost businesses in 2015. Unapproved apps, unmanaged devices, poor password protection, and other security issues are leaving far too many organizations vulnerable to attack. And as organizations embrace digital transformation, it becomes increasingly urgent for the organization to increase control over their IT infrastructure and reduce security risks.

This course is an overview of threat detection as part of a defense in-depth strategy. You will learn how to protect, detect, and respond to cybercrime as you explore the capabilities of threat detection and mitigation tools.

Course Objective:

After completing this course, students will be able to:

- Describe signature-based and behavioral / heuristic detection methods
- List the capabilities of on-premise threat detection and mitigation tools
- Name the capabilities of hybrid and cloud threat detection and mitigation tools
- Recognize the importance of Enterprise threat detection monitoring

Audience:

- IT Support officer
- Cybersecurity officer
- Cybersecurity professional

Prerequisite:

- The current cybersecurity ecosystem
- Analysis of hacks on computers and networks
- Basic 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?