Rumos valorizamos profissionais!

Microsoft Security Workshop: Planning for a Secure Enterprise – Improving Detection (40553)

- **Formato do curso:** Presencial e Live Training
- **Localidade:** Lisboa
- **Data:** 16 Set. 2020 a 16 Set. 2020
- **Preço:** 490€
- **Horário:** Laboral - 9h30 - 17h30
- **Duração:** 7 horas

In this course, you will learn about the modern cyber threat landscape and the corresponding detection and prevention methods and a number of customer-managed and Microsoft-managed solutions that provide threat detection capabilities for on-premises workloads.

You will also learn about the most prominent Microsoft-managed services that provide threat detection capabilities for hybrid and cloud-based workloads. And finally, you will step through a number of different scenarios that illustrate how these solutions respond to a number of actual cyberattacks, with description of a Microsoft-recommended comprehensive approach to implementing cybersecurity in hybrid environments.

Destinatários

This course is intended for IT Professionals that require a deeper understanding of Windows Security and to increase their knowledge level through a predominately hands-on experience with Microsoft threat detection tools for hybrid and cloud-based workloads.

Pré-requisitos

This workshop is part of a larger series of Workshops offered by Microsoft on the practice of Security. While it is not required that you have completed any of the other courses in the Security Workshop series before taking this workshop, it is highly recommended that you start with the first course in the series, Microsoft Security Workshop: Enterprise Security Fundamentals.
This workshop requires that you meet the following prerequisites:
In addition to their professional experience, students who take this training should already have the following technical knowledge:

- Experience with Windows Client and Server administration, maintenance, and troubleshooting.

- Basic experience and understanding of Windows networking technologies, to include Windows Firewall network setting, DNS, DHCP, WiFi, and cloud services concepts.
- Basic experience and understanding of Active Directory, including functions of a domain controller, sign on services, and an understanding of group policy.
- Knowledge of and relevant experience in systems administration, using Windows Server 2012 R2 and 2016.

Learners who take this training can meet the prerequisites by obtaining equivalent knowledge and skills through practical experience as a Security Administrator, System Administrator, or a Network Administrator.

Programa

An Overview of the Modern Cyber Threat and Cyber Security Landscape

By 2021, worldwide cybercrime damage is expected to reach $6 trillion —double what it cost businesses in 2015. As digital transformation sweeps the globe, the imminent threat of cybercrime grows alongside it. As a result, new techniques in cybersecurity are being developed to mitigate the increased levels of risks. Despite a wide variety of cyberattacks, most of them can be categorized based on their primary characteristics and their objectives. There is also a common set of methods and tactics that cyberattacks rely on in order to evade detection. These methods and tactics, in turn, shape the modern approach to cyber security. In this module, you will learn about the modern cyber threat landscape and the corresponding detection and prevention methods.

Lessons

- An overview of the modern cyber threat landscape
- Detection and prevention in the modern cyber threat landscape

Detecting Threats in On-Premises Environments

This module will provide an overview of a number of customer-managed and Microsoft-managed solutions that provide threat detection capabilities for on-premises workloads. It is important to note that these solutions are also available when running cloud-hosted Infrastructure as a Service (IaaS) workloads, regardless of the cloud hosting provider, as long as the IaaS environment satisfies solution prerequisites.

Lessons

- Windows Event Forwarding (WEF) and Intrusion Detection
- Windows Defender Advanced Threat Protection (ATP)
- Microsoft Advanced Threat Analytics (ATA)
- Microsoft Enterprise Threat Detection (ETD)
- Integrating programming and scripting technologies with threat detection
- Logging, Auditing, and Monitoring with Windows-based tools

Lab : Lab: Threat detection with Windows Event Forwarding

- Configure Windows Event Forwarding and creating a subscription
- Using WEF to detect threats

Detecting Threats in Hybrid and Cloud Environments

As organizations move their workloads to the Microsoft cloud, they can fully realize benefits offered by a wide range of its services. Most of these services deliver functionality superior to equivalent on-premises technologies. Customers can take advantage of enhanced security through advanced threat detection capabilities provided by services like Azure Active Directory (Azure AD), Azure Security Center, and Azure Log Analytics. These security services and capabilities provides a straightforward and effective way to understand what is happening within customers' hybrid and cloud deployments in real time. In this module, you will learn about the most prominent Microsoft-managed services that provide threat detection capabilities for hybrid and cloud-based workloads.

Lessons

- Microsoft Office 365 and SaaS Related Offerings
- Azure Advanced Threat Detection
- Microsoft Enterprise Mobility and Security Offerings
- Azure Logging and Auditing

Analyzing Threat Detection Solutions in Action

Cybersecurity solutions presented in the previous modules of this course combine extensive pre-breach endpoint security to prevent potential attacks with a post-breach detection and remediation functionality in order to minimize impact of an attack already in progress. To better understand the nature of these solutions and the benefits they offer, it is worthwhile to examine their response to real-life exploits. In this module, you will step through a number of different scenarios that illustrate how these solutions respond to a number of actual cyberattacks. The module will conclude with description of a Microsoft-recommended comprehensive approach to implementing cybersecurity in hybrid environments.

Lessons

- 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

Lab : Lab: Improving Detection

- Deploying Microsoft ATA
- Using Microsoft ATA for Threat Detection