McAfee 3 Day Advanced Threat Defence, Endpoint Detection and Response Course

BeSecure IT

Special Notices
Delegates are required to bring their own laptops for the course as we value hands on learning and each delegate will be provided a lab environment to work in, alongside real-world scenarios to facilitate learning.

Course Overview
The McAfee 4 Day Advanced Threat Defence, Endpoint Detection and Response Administration Course is designed to cover the configuration and day to day administration of the McAfee Intelligent Endpoint Solutions product suite, including:

- ePO Management Console
- Endpoint Security, including Adaptive Threat Prevention
- Data Exchange Layer
- Threat Intelligence Exchange
- Advanced Threat Defence
- Active Response

Main focuses will be on the integration of the solutions, through to more advanced use cases on how leverage the products to enable your IT Security team.

Delegates will learn how to

- Understand the use of each component
- Configure the policy set from a fresh install experience
- Install, Configure and deploy Endpoint Client software
- Perform day to day administration with confidence
- Leverage inter-component functionality to increase security and decrease workload

Outline

<u>ePO Management Console</u>

- Integrate the other solutions for reporting and management
- Leverage ePO Automation to reduce workload

<u>Endpoint Security</u>

- Introduce Endpoint Security Adaptive Threat Protection and its functions
- Understand its operational modes
- Configure policy and Deploy via the ePO Management Console
- Illustrate the reporting capabilities

<u>Data Exchange Layer</u>

- Discuss concepts and functions
- Walkthrough how to integrate with the ePO Management Console
- Deploy and configure DXL Broker
- Deploy and configure DXL Client
- Leverage additional DXL agent functionality

Threat Intelligence Exchange

- Understanding TIE and its function within the network
- Discuss the functions and workflow of a TIE detection
- Deploy and Configure TIE database server
- Discover how to integrate with ePO, DXL and ENS
- Work through how to provide relevant reporting information
- How to take action based on known and unknown files within your network

Advanced Threat Defence

- Understand how implementing an integrated sandbox solution can massively improve detection rates
- Understanding the threat workflow up to this point, and how the previous solutions react
- Configuring an image ready for ATD deployment and testing
- How to integrate with ePO, TIE and ENS
- Working through the network auto-immune response
- Testing the ATD sandboxing via manual upload and ENS/TIE submission

Active Response

- What is Endpoint Detection and Response
- Discuss the merits of an integrated Endpoint Detection and Response solution
- Understand the Active Response solution's architecture
- Integrate with ePO, TIE, ENS and ATD
- Discuss how you can leverage automated responses and rules to reduce the time between detection and remediation to minutes