## LESSON: Microsoft Endpoint Security

**Before you Begin**

In this module, there are a variety of technologies that will be covered during the lesson such as host encryption, application control, and host-based firewall services for Windows. For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed:

* Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
* Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
* Ensure learners are given opportunities for breaks throughout the lesson. The pacing guide below provides recommended breaks. However, there are additional breaks added in the slide deck, please use them if needed.
* For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regards to the lesson.
* Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
* At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.

### Summary

In this lesson, learners will gain a comprehensive understanding of encryption algorithms, encryption keys, and their role in ensuring the confidentiality and security of sensitive information. They will explore BitLocker, a powerful encryption tool provided by Microsoft for full-disk encryption, and learn about the importance of managing BitLocker recovery keys for data recovery, disaster resilience, user support, and regulatory compliance. The lesson will also cover AppLocker, a robust application control feature in Microsoft Windows, and how its implementation allows organizations to enforce policies that only permit authorized applications, thereby reducing the risk of malware infections and unauthorized software installations. Learners will delve into Windows Firewall as a critical defense mechanism for network protection, application control, and network visibility, and understand how to configure and manage Windows Firewall settings through Group Policy in a domain environment for centralized and efficient network security management.

### Objectives

* Define the concept of encryption and its purpose in protecting data on a computer.
* Identify BitLocker as a built-in encryption tool in Windows and explain its primary function to encrypt entire drives.
* Describe the importance of managing BitLocker recovery keys and the various methods available to do so.
* Apply AppLocker rules to allow or deny specific applications from running on a Windows device within a domain environment in a given scenario.
* Evaluate whether a set of AppLocker policies meets specific security requirements for a domain environment.
* Create a policy using AppLocker that only allows authorized software to run on a Windows device within a domain environment.
* Create Windows Firewall rules.
* Configure Windows Firewall settings to manage both external and internal traffic.
* Apply Windows Firewall settings through Group Policy to multiple computers in a domain.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| **Estimated Time** | **Lesson Portion** | **Directions** |
| 5 min | **Lesson Opener:**  Microsoft Endpoint Security | * Introduce learners to Microsoft Endpoint Security. |
| 5 min | **Real World Scenario:**  Microsoft Endpoint Security | * Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| 40 min | **Cyber Uncovered:**  Host Encryption | * Describe encryption algorithms as mathematical procedures used to transform data. * Discuss how encryption algorithms make data unreadable to unauthorized parties. * Provide examples of commonly used encryption algorithms, such as AES and RSA. * Define encryption keys and their role in the encryption and decryption processes. * Differentiate between symmetric and asymmetric encryption keys. * Introduce BitLocker as a full-disk encryption feature in Windows operating systems. * Discuss the difference between partial and full-disk encryption. * Explain how BitLocker uses symmetric key encryption to protect data. * Emphasize the secure encryption capabilities for internal and external storage devices. * Explore the multiple authentication methods supported by BitLocker. * Discuss its seamless integration with Windows operating systems. * Explain the benefits of using BitLocker for data protection. * Discuss the purpose of recovery keys in maintaining data accessibility. * Explain scenarios where recovery keys are essential, such as forgotten passwords or system failures. * Explain saving recovery keys to a file and secure storage options. * Discuss the option to print recovery keys and proper physical storage. * Introduce Active Directory integration for centralized recovery key management. * Be prepared to discuss the implications of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 30 min | **Lab:**  Bitlocker | * Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| 5 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 35 min | **Cyber Uncovered:**  AppLocker | * Begin by highlighting the increasing challenges organizations face in protecting their systems from malicious software and unauthorized applications. * Explain the importance of application security and the need for a solution like AppLocker. * Introduce AppLocker as a built-in feature in Microsoft Windows designed to control application execution. * Emphasize that AppLocker enables organizations to define and enforce policies regarding which applications are allowed or blocked. * Explain the application control feature, allowing granular control over applications based on file paths, hash values, publisher information, and digital signatures. * Discuss the rule-based policies, highlighting the ability to create rules based on attributes such as file name, publisher, or version. * Describe the flexibility of rule creation and the different rule types supported by AppLocker, such as executable rules, Windows Installer rules, script rules, and DLL rules. * Discuss the enhanced security provided by AppLocker, preventing the execution of unauthorized or malicious applications and reducing the risk of malware infections. * Highlight the policy consistency achieved through standardized application control, minimizing the risk of configuration drift and unauthorized software installations. * Explain the granular control offered by AppLocker, allowing administrators to define specific rules based on unique security requirements. * Explain the process of creating AppLocker policies using the Group Policy Management Console or Windows PowerShell cmdlets. * Guide the learners through the steps of rule definition, enforcement, and the importance of thorough testing and fine-tuning before deploying policies to production environments. * Walk learners through the steps of opening the Group Policy Management Console, editing the Default Domain Policy, navigating to the Application Identity policy, and enabling it. * **Provide learners with a 5 minute break if needed.** * Present the "Allow" rule for "Firefox Web Browser" as an example, including the rule type, path, and action. * Discuss the "Deny" rule for "Chrome Web Browser," explaining the rule type, publisher, and action. * Guide learners through the general steps of opening the Group Policy Management Console, creating or editing a Group Policy Object (GPO), navigating to the AppLocker settings, and creating the "Allow" and "Deny" rules. * Emphasize the importance of applying the GPO to the appropriate organizational units (OUs) or devices, testing the rules, and monitoring and refining them based on feedback. * Explain the steps for evaluating whether a set of AppLocker policies meets specific security requirements for a domain environment. * Discuss aspects such as understanding security requirements, assessing existing policies, policy analysis, rule coverage, testing and validation, compliance checks, regular review and updates, and documentation and reporting. |
| 5 min | **Pulse Check** | * After the poll is concluded, review the results with the learners. Encourage those in the red zone to attend office hours and/or to reach out to the instructors for assistance. |
| 5 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 40 min | **Cyber Uncovered:**  Windows Firewall | * Introduce Windows Firewall as a software-based network security solution included in Microsoft Windows operating systems. * Explain that Windows Firewall acts as a barrier between computers or networks and potential threats by monitoring and controlling inbound and outbound network traffic. * Discuss the key features and capabilities of Windows Firewall. * **Provide learners with a 5 minute break if needed.** * Explain that Windows Firewall can be accessed through the Windows Security settings or the Control Panel, with advanced configuration options available in the Windows Defender Firewall with Advanced Security console. * Describe how administrators can define inbound and outbound rules based on specific criteria, such as port numbers, protocols, IP addresses, or applications. * Highlight the importance of regularly monitoring Windows Firewall logs, reviewing and updating rules as needed, and applying the latest security updates for ongoing protection. * **Provide learners with a 5 minute break if needed.** * Explain how Windows Firewall settings can be configured and deployed using Group Policy for consistent firewall rules and configurations across the domain. * Provide step-by-step instructions for configuring Windows Firewall settings via Group Policy. * Be prepared to discuss the implications of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 30 min | **Lab:**  Configuring Windows Firewall | * Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| 10 min | **Lesson Closure** | * For this lesson, spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson and what they should do to prepare for the next module. Complete a high level review of how host encryption, application control, and the Windows Firewall can be used to better secure the endpoint. * You will be able to use the data collected in the pulse check to help with the lesson closure. Remind those learners that reported being in the “red zone” to take advantage of office-hours. * Recommend that the learners ensure they submit all of the assignments on-time to ensure the appropriate credit is provided to them. * Recommend that the students read-ahead and come prepared for the next lesson. * Q&A |
|  | **Additional Time Filler (if needed)** | * Kahoot * Discuss interview prep and questioning * Use breakout rooms for additional lab practice * Continue Real World Scenario Conversation |