LESSON: Endpoint Detection and Response (EDR)

Primer

This is the first module of this course. Therefore, instructors should do the following:

- Introduce Themselves: Instructors should introduce themselves to students, highlighting their credentials and expertise to establish confidence and trust. Additionally, instructors can break the ice by asking students why they registered for the program and inviting them to share their hobbies and a fun fact about themselves.
- Review the Canvas System and syllabus: Spend some time reviewing the Canvas system, explaining the grading process, and going over the syllabus.
- Communication Protocols: Explain the methods available for students to reach out to instructors with questions or to share any information.

All the above points should be covered within 30 minutes.

For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed for each lesson

- 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.
- 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.
- Instructors should manage breaks based on need, considering both timing and duration. You may take a break if you feel the students need it or if a particularly challenging topic has just been covered.

Summary

In this lesson, learners will explore endpoint security solutions, understanding their vital role in protecting workstations and end-user devices. They'll delve into the endpoint security suite, gaining insights into its multifaceted protective measures and recognizing prominent industry vendors like Symantec, Check Point, Kaspersky, and McAfee. The lesson delves deep into the importance of antivirus software within endpoint security, emphasizing its role in threat detection and removal. Learners will unravel the intricacies of antivirus software, including specific and heuristic detection mechanisms, while also being introduced to ClamAV, an open-source, cross-platform antivirus solution for cost-effective endpoint protection. The lesson provides a clear understanding of false positives and false negatives, sheds light on zero-day vulnerabilities, and explores tactics employed by attackers to bypass antivirus software. Moreover, it emphasizes the significance of enhanced endpoint security in the modern digital landscape. The concept of antivirus signatures and their impact on malware detection is also thoroughly covered, as is the role of logical signatures, YARA rules, and the YARA rule structure in crafting precise pattern-matching rules for malware detection. Finally, learners will grasp the importance of PhishSigs, a specialized ClamAV database used to identify potentially malicious web content. Throughout the lesson, they'll gain a comprehensive understanding of vital concepts and technologies relevant to endpoint security and antivirus software.

Objectives

- Explain the concept of endpoint security.
- Identify key components of an endpoint security suite.
- Recognize common endpoint security vendors.
- Describe antivirus mechanisms.
- Recognize the key features and advantages of ClamAV.
- Evaluate the pros and cons of ClamAV as an endpoint security solution.
- Identify essential ClamAV configuration files.
- Recognize the impact of false positives and false negatives in antivirus software.

- Analyze the causes of false positives in antivirus software and recognize the risks associated with minimizing them.
- Explain zero-day vulnerabilities, their exploitation by hackers before patches are available, and their relevance in the cybersecurity landscape.
- Explain the evolution and key characteristics of endpoint detection and response (EDR).

- Identify essential endpoint security components and their roles in safeguarding networked workstations.
- Analyze the challenges and considerations related to device control and bring your own device (BYOD) policies.
- Differentiate between EDR and traditional antivirus (AV) software.
- Recognize the importance of signatures in antivirus software.
- Describe how to write and inspect signatures using Sigtool.
- Explain the concept of logical signatures.
- Summarize the concept and structure of YARA rules and their compatibility with ClamAV.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
20 min	**Introduction**	● The lead and associate instructor should introduce themselves to the learners ● Encourage the learners to post something about themselves in the chat window
10 min	**Canvas and Syllabus Overview**	● Review the key areas of the Canvas platform so that learners could have a better understanding of where to find the resources they will need for this course. ● Spend a few minutes reviewing the syllabus covering at a high level the expectations of the course
5 min	**Lesson Opener:** Endpoint Detection and Response (EDR)	● Introduce learners to the importance of endpoint detection and response (EDR) in cybersecurity.
5 min	**Real World Scenario:** Endpoint Detection and Response (EDR)	● 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. ● Read the real-world scenario aloud to the students while sharing your screen. This will help them stay engaged with the case as you go through the questions throughout the class.
10 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.
20 min	**Cyber Uncovered:** Endpoint Security Introduction	● Start the lesson by explaining the importance of endpoint security and how it protects workstations and end-user devices in today's digital landscape. ● Discuss the rise of BYOD environments and the need for security solutions to adapt to these complexities. ● Provide an overview of the endpoint security suite and its role in protecting endpoints.

		● Highlight key protective measures, such as antivirus/antimalware, data loss prevention, and application control/allowlisting. ● Introduce learners to some common vendors in the endpoint security industry, including Symantec, Check Point, Kaspersky, and McAfee. Discuss their significance in the market and their offerings. ● Delve into antivirus software and its role within endpoint security. ● Emphasize the need for regular signature updates to stay effective against evolving threats. ● Explain how antivirus solutions specialize in threat detection and removal. ● Describe how these solutions handle infected files, such as quarantine or deletion. ● Break down the different detection mechanisms within antivirus software, including specific detection, string/byte signatures, hash signatures, and heuristic detection. ● Highlight their importance in identifying various types of malware. ● Dive deeper into heuristic detection and how it explores unknown viruses. ● Discuss parameters like file structure and behavior and explain how sensitivity levels can be customized for endpoint protection. ● Encourage hands-on learning by allowing learners to explore antivirus software on their systems or by using virtual environments. ● Be prepared to discuss the implication 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.
20 min	**Cyber Uncovered:** ClamAV Introduction	● Begin the lesson by introducing ClamAV as an open-source and cross-platform antivirus software. ● Explain its importance in providing cost-effective protection across various operating systems. ● Discuss the flexibility of ClamAV, offering both command-line and graphical user interface options to cater to diverse user preferences. ● Emphasize the adaptability of ClamAV in aligning with specific security requirements. ● Highlight the benefits of ClamAV, including that it is a free antivirus solution that supports scheduled tasks for automation and provides an easy-to-use interface that simplifies antivirus management.

		● Discuss the regular virus database updates in ClamAV, highlighting the importance of staying protected against emerging threats. ● Explain ClamAV's robust virus detection capabilities, which ensure effective security, and mention that users have access to technical support for assistance. ● Address the drawbacks of ClamAV, including infrequent software updates, the absence of a 100% guarantee against viruses and threats, and its low processing speed that may affect system performance.Mention that ClamAV lacks a built-in host firewall and safe browsing capabilities, necessitating reliance on other tools for web security. ● Transition to ClamAV configuration files by introducing clamd.conf and its role in customizing the scan daemon's behavior and parameters for specific security needs. ● Continue with the freshclam.conf file, explaining its significance in adjusting the virus database update interval to ensure up-to-date protection against new threats. ● Conclude the lesson by discussing the Clamconf utility, which simplifies the management and customization of ClamAV settings by summarizing clamd.conf and freshclam.conf configuration files. Encourage learners to engage and experiment with these configurations through hands-on experience. ● Be prepared to discuss the implication 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.
10 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.
25 min	**Cyber Uncovered:** Antivirus Problems and Risks	● Begin the lesson by introducing the importance of false positives and false negatives in the realm of antivirus software. ● Explain how they can impact the effectiveness of security solutions. ● Discuss false positives, emphasizing that they occur when antivirus software mistakenly identifies legitimate files or applications as malicious threats. ● Explain the potential consequences of false positives, such as unnecessary alarms and disruption of regular operations. ● Move on to false negatives, explaining that they occur when antivirus software fails to detect actual viruses or malware. ● Highlight the risk associated with false negatives, as they can compromise system security.

		● Stress the significance of strong and accurate antivirus detection mechanisms in managing false positives and false negatives effectively. ● Transition to the causes of false positives in antivirus software. ● Discuss factors like heuristics, behavioral analysis, and machine learning as contributors to false positives. ● Explain how these factors can lead to misidentifying files as threats. ● Address the concept of zero-day vulnerabilities, defining them as recently discovered software weaknesses. ● Explain the critical nature of zero-day vulnerabilities and the need to address them promptly. ● Introduce antivirus bypass techniques used by attackers to evade detection. ● Discuss strategies like packing and encryption, code mutation, stealth techniques, disabling AV updates, and fileless attacks. ● Emphasize the importance of understanding these evasion techniques in the development of effective cybersecurity defenses. ● Discuss how security professionals must be aware of these tactics to enhance security measures. ● Conclude the lesson by summarizing the key points and reinforcing the significance of maintaining a balance between robust threat detection and minimizing false positives in antivirus software. ● Be prepared to discuss the implication 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.
20 min	**Lab:** Bypassing an Antivirus Application	● 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	**Pulse Check**	● Instructors are to spend a few minutes explaining the purpose of this poll as well as the zone. ● After the poll is concluded, spend a few minutes asking why students have selected their zones. Encourage them to share with each other. ● Future pulse checks should only take 3-5 min to administer.
10 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.
15 min	**Cyber Uncovered:** Endpoint Detection and Response	● Begin the lesson by introducing endpoint detection and response (EDR) and its significance in modern cybersecurity.

		● Explain the evolution from endpoint threat detection and response (ETDR) to EDR and the role it plays in monitoring and analyzing network endpoints. ● Discuss how EDR helps organizations identify and mitigate security threats by detecting and responding to suspicious or malicious activities at the host level. ● Emphasize the usefulness of EDR in scenarios requiring manual threat detection and analysis, where security professionals proactively search for threats in an environment. ● Transition to the components of endpoint security, starting with the internal firewall. Explain its role in actively monitoring and controlling network traffic and blocking potentially malicious connections. ● Move on to HIDS/HIPS (Host-Based Intrusion Detection System/Host-Based Intrusion Prevention System), discussing how these critical components work together to detect, protect against, and alert users or administrators about malicious activities or intrusion attempts on the host machine. ● Introduce the concept of a sandbox and its purpose in providing a controlled and isolated environment for running suspicious programs and files. Explain how it aids in analyzing potentially harmful code without risking the overall security of the system. ● Address device control and BYOD security, explaining how the security perimeter is broadened to include personal devices connected to the corporate network. Discuss the potential risks associated with personal devices and the need for strict device control policies. ● Conclude the lesson by comparing EDR and traditional antivirus (AV) solutions. Highlight how EDR goes beyond antivirus, offering advanced protection against sophisticated threats like advanced persistent threats (APTs). Discuss the differences in visibility and response requirements between EDR and AV solutions. ● Be prepared to discuss the implication 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.
20 min	**Cyber Uncovered:** YARA Rules and Signatures	● Start the lesson by introducing the concept of antivirus (AV) signatures and their importance in malware detection. ● Explain how antivirus software primarily relies on AV signatures to identify and detect malware by recognizing patterns of malicious code. ● Emphasize the significance of varying signature database formats among antivirus vendors and how this can impact the effectiveness of malware detection.

		● Move on to the topic of writing signatures, highlighting the use of Sigtool, a versatile tool used to create, inspect, and manage signatures. ● Explain the purpose of the --md5 flag in Sigtool and how it's used to generate MD5 hashes, a crucial cryptographic hash function, to verify file integrity. ● Describe the function of the full file path in signature writing or inspection, emphasizing its ability to specify the exact location of the file under scrutiny. ● Discuss how Sigtool can output signatures to a file named test.hdb and how this file can be used for various security and analysis purposes. ● Provide practical examples of Sigtool and ClamAV usage in signature generation and malware scanning, illustrating the real world application of the tool. ● Transition to the topic of logical signatures and how they combine multiple signatures using logical operators for precise pattern matching. ● Explain how logical signatures help identify complex threats through nuanced and adaptable pattern matching, enhancing the accuracy and effectiveness of antivirus detection. ● Discuss the significance of the EICAR file for testing antivirus software and the importance of excluding it from scanning to prevent false alarms and maintain database integrity. ● Introduce YARA rules, describing them as a method of defining specific patterns or characteristics to identify files containing malware based on predefined conditions. ● Explain how YARA rules enhance the accuracy and efficiency of malware detection by enabling security professionals to create custom rules tailored to their specific security needs. ● Describe the structure of YARA rules, including the rule name, strings specifying values to search for, and logical operators for complex pattern matching. ● Conclude the lesson by introducing YARA rule signatures in ClamAV, explaining their specific constraints and compatibility with custom rule sets, and highlighting their role in pattern matching and threat detection. ● Be prepared to discuss the implication 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.
10 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.
25 min	**Lab:** Configuring YARA Rules	● 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.
15 min	**Lesson Closure**	● For this first 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. The take-aways discussion should include key concepts such as the importance of endpoint detection and response (EDR) in cybersecurity and Address device control and BYOD security. Students should review this information prior to moving to the next module. ● Recommend that the students read-ahead and come prepared for the next lesson. ● Q&A
N/A	**Additional Time Filler (if needed)**	● Kahoot ● Discuss interview prep and questioning ● Use breakout rooms for additional lab practice ● Continue Real World Scenario Conversation