## LESSON: Threat Detection, Prevention, and Response

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

* Checking with the students to see if they have any questions or need further clarification from any subject from the last class “Firewalls”.
* 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 regard 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 the concepts of network security management (NSM), encompassing intrusion detection systems (IDS) and intrusion prevention systems (IPS). They'll discover how IDS passively observes network activity, while IPS takes a proactive approach, examining traffic for patterns, malware, vulnerabilities, and behavior. Learners will understand the choice organizations make between IDS and IPS, considering potential impacts on network performance. Effective strategies for deploying IDS systems will be explored, including the use of multiple IDSs and TAB interfaces for traffic analysis. They will also gain insights into IPSs’ optimal placement and integration with advanced routers. The lesson covers behavior-based and content-based detection, protocol detection, and anomaly detection methods. Students will delve into network security rules and the structures of Snort and Suricata rules. Additionally, they will explore network detection and response (NDR) and managed detection and response (MDR) approaches, with examples illustrating their real-world applications, and understand the benefits of combining NDR and MDR for holistic security.

### Objectives

* Explain network security monitors (NSMs).
* Define intrusion detection systems (IDS).
* Define intrusion prevention systems (IPS).
* Compare and contrast between detection vs. prevention systems.
* Analyze IDS and IPS deployment strategies.
* Summarize popular solutions and methods for installing and configuring IDS and IPS.
* Describe the different network security methods used for detection.
* Compare and contrast IPSs vs. firewalls.
* Recognize the importance of protocol and anomaly detection in network security.
* Explain how IDS and IPS rules work and illustrate through examples.
* Summarize pattern-matching techniques used to identify threats in network traffic.
* Describe the features available to customize IDS and IPS systems.
* Explain the importance of false positive mitigation and traffic logging.
* Define network detection and response (NDR).
* Define managed detection and response (MDR).
* Compare and contrast NDR vs. MDR.
* List the key considerations when implementing NDR and MDR.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Lesson Opener:**  Threat Detection, Prevention, and Response | * Introduce learners to the importance of threat detection, prevention, and response in cybersecurity. |
| 5 min | **Real World Scenario:**  Threat Detection, Prevention, and Response | * 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. |
| 20 min | **Cyber Uncovered:**  Introduction to IPS/IDS | * Start by introducing the concept of network security monitors (NSMs) and highlight that they encompass various technologies, including IPS, IDS, and other monitoring systems. * Explain that NSMs are primarily responsible for network traffic inspection, analysis, and alert generation. * Emphasize that these systems are designed to offer comprehensive network monitoring and might incorporate visualization components for enhanced analysis. * Describe intrusion detection systems (IDS) as a security technology that monitors network traffic, identifies suspicious or unauthorized activities, and generates alerts when potential threats are detected. * Distinguish IDS from IPS by clarifying that it provides notifications without directly blocking the threats. * Cover the core elements of IDS, such as its ability to analyze data for known attack patterns or deviations from network norms and its role in generating alerts. * Differentiate between network-based IDS (NIDS) and host-based IDS (HIDS) and explain their respective focuses. * Discuss the detection methods employed by IDS, including signature-based (known patterns) and anomaly-based (deviations from normal) methods. * Explain that intrusion prevention systems (IPS) not only monitor network traffic and detect threats like IDSs, but also actively take measures to prevent or block detected threats. * Mention that IPSs provide a proactive defense mechanism by stopping potentially malicious activities. * Highlight the operations of IDS and IPS, emphasizing that IDS observes network traffic passively while IPS actively examines it. Clarify that IPS looks for irregular patterns, malware, known vulnerabilities, and may use behavior analysis to identify unusual network activity. * Mention that IPS can impact network performance, requiring careful configuration. * Present the crucial decision organizations face between deploying IDS, IPS, or a combination of both. * Provide a table or visual aid to help learners understand the differences between detection and prevention in terms of functionality, rule-based operation, handling false positives, traffic route, and network scope. * Explain the concepts of false positives (incorrectly flagging benign activities) and false negatives (missing genuine threats) and their impact on network security. * Clarify that true positives (accurately identifying threats) and true negatives (correctly recognizing benign activities) are the desired outcomes. * 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. |
| **5 min Break** | | |
| 20 min | **Cyber Uncovered:**  IDS/IPS Considerations | * Begin the lesson by explaining the significance of intrusion detection systems (IDS) in network security. * Discuss the importance of strategically positioning IDS within the network to effectively monitor traffic. * Explain how the placement can impact the system's performance and detection capabilities. * Explore the concept of using multiple IDSs in complex network environments for improved coverage. * Highlight scenarios where this strategy is particularly beneficial. * Introduce the concept of TAB interfaces and how they facilitate IDS traffic analysis by mirroring network traffic. * Explain how this technology aids in comprehensive network monitoring. * Address the limitations of placing an IDS at a network gateway, where switched traffic may bypass it. * Discuss why this placement might not be effective in certain situations. * Transition to intrusion prevention system (IPS) deployment strategies and their role in network security. * Explain that IPS should be placed on the network gateway or proxy to effectively block incoming and outgoing traffic. * Discuss the benefits of this strategic placement for proactive threat prevention. * Clarify that an IPS should be integrated as part of the traffic route, unlike an external device. * Emphasize how this integration enhances network security. * Describe how IPS actively blocks network traffic, focusing on patterns, malware, vulnerabilities, and behavior. * Discuss the significance of this feature in preventing potential security incidents. * Explain that IPS systems are often integrated into advanced routers, combining efficient traffic management with security measures. * Highlight the advantages of this integration in network security. * Provide an overview of popular network security solutions like Snort and Suricata. * Explain their features, real-time threat detection capabilities, and community support. * Discuss the installation options and cross-platform compatibility offered by Suricata. * Explain the two primary modes of operation for Suricata—IDS and IPS—and how organizations can choose between them based on their security goals. * Present pfSense as a versatile network security solution that can be installed as a firewall and router. * Describe the comprehensive package it provides and its integration with IDS/IPS tools like Suricata for enhanced security and threat detection capabilities. * Detail the steps involved in configuring Suricata in pfSense, focusing on interface selection, rule configuration, and alert settings. * Explain the user-friendly interface that simplifies the configuration process. * 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. |
| 10-15 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 | **Lab:**  Suricata Installation on pfSense | * 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. |
| 20-25 min | **Cyber Uncovered:**  IDS/IPS Detection Methods | * Begin by introducing the lesson's focus on network security detection methods. * Explain the concept of behavior-based detection, highlighting its attributes and typical use in firewalls. * Describe content-based detection and its role in examining packet payloads for malicious content in systems like intrusion prevention systems (IPS). * Transition to a comparison between IPS and firewalls, emphasizing the differences in their inspection methods and use cases. * Discuss the significance of protocol detection in network security and how it's employed to analyze packet headers for effective threat analysis. * Move on to the topic of anomaly detection in IDS and IPS systems, showcasing its role in identifying irregular network behavior and emerging threats. * Introduce the essential components of IPS/IDS rules, such as traffic specification, rule content, conditions, alerts, and metadata. * Provide examples of rule implementation to help students understand the practical application of rule structures. * Explain the structure of Snort rules, emphasizing key elements like rule action, protocol, source/destination, and rule options. * Transition to a closer look at Suricata rules, their customizability, and support for Snort and Emerging Threats (ET) rules. * Describe the importance of pattern matching in identifying specific threats in network traffic and its role in malware detection. * Discuss the significance of working with IPSs and IDSs, including fine-tuning, creating tailored rules, log analysis, rule adaptation, and continuous rule enrichment. * Delve into the challenges of false positives in network security and present mitigation strategies. * Emphasize the importance of logging traffic for network security investigations, discussing Suricata's built-in traffic logging capabilities. * Conclude by highlighting the role of analysts in responding to security alerts and incidents, explaining their workflow and the need for extensive analysis in certain cases. * **Provide learners with a 5 min break.** * 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. |
| 10-15 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 | **Lab:**  Anomaly Detection | * 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 | **Pulse Check** | * After the poll is concluded, spend a few minutes asking why students have selected their zones. Encourage them to share with each other. |
| 20 min | **Cyber Uncovered:**  Introduction to NDR & MDR | * Begin the lesson by introducing the concept of network detection and response (NDR) and its role in enhancing cybersecurity through real-time network traffic monitoring and threat response. * Highlight the key features of NDR, including traffic monitoring, anomaly detection, packet capture and analysis, behavior analysis, forensic capabilities, alerting, and real-time response. * Discuss the various use cases for NDR, such as detecting data breaches, identifying insider threats, monitoring network performance, and complying with regulatory requirements. * Transition to an overview of managed detection and response (MDR) services, explaining how MDR combines technology, expertise, and around-the-clock monitoring to protect organizations from security threats. * Explore the features of MDR, including the use of advanced security tools, skilled security analysts, 24/7 monitoring, and incident response capabilities. * Compare NDR and MDR, emphasizing that NDR is a technology or tool, while MDR is a comprehensive service that complements NDR with human expertise and monitoring. * Discuss the benefits of combining NDR and MDR, illustrating how NDR provides initial threat detection capabilities, while MDR offers human intelligence and response capabilities. * Move on to the key considerations for implementing NDR and MDR, covering aspects like network size, complexity, security needs, expert collaboration, and the importance of tailored solutions. * Conclude the lesson by providing real world examples of how MDR and NDR can be used to protect organizations from cyberthreats, showcasing their practical applications in different scenarios. * 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. |
| 10-15 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 | **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 DS/IPS Considerations, IDS/IPS Detection Methods, nad NDR and MDR * 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 |
| 5 min | **End-of-Course Survey** | * Allocate 5 minutes to facilitate the completion of the End-of-Course Survey. * Encourage learners to provide honest and constructive feedback about their learning experience. |

### 