LESSON: Threat Hunting Tools and Techniques

Before you Begin

This is the 4th module of the Threat Hunting and Intelligence course, for reference Module 3 was the student's asynchronous content. One of the key points to highlight when discussing tools and techniques for threat hunting is one of environmental/organizational visibility. Hunting and detecting malicious activity becomes nearly impossible without adequate visibility to the behavioral aspects to the activity happening on a network. Whether you're hunting insider threats, malicious threat actors, APTs, fraudulent activity, or really anything; without proper visibility an analyst is going to be hamstrung to being much less valuable. Many different tools can enable visibility such as EDR, SIEM, AV, NDR, Sysmon, asset inventorying, amongst tons of others. These defensive layers not only help to actively defend your environment but they empower analysts to hunt, giving them valuable data to use to find more bad. Lacking adequate visibility, not retaining the data for necessary timeframes, the solutions being overly difficult to use, and a myriad of other problems present themselves in the real world and should be highlighted accordingly.

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. For this first module, take additional time to explain the purpose of the pulse check and encourage learners to provide their anonymous feedback. 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 explore the importance of indicators of compromise (IoCs) in identifying security breaches and aligning threat hunting tools with IoC types using the Pyramid of Pain model. They will learn to leverage hash values for malware association checks and cross-reference IP addresses and domain names with threat intelligence databases. Learners will understand adversary tactics and recognize tactics, techniques, and procedures (TTPs) through frameworks like MITRE ATT&CK. The lesson highlights the use of log management systems, SIEM solutions, and endpoint detection and response (EDR) tools for threat detection and response. Modern cybersecurity products like Splunk, ELK Stack, and CrowdStrike Falcon integrate these functionalities, while extended detection and response (XDR) solutions offer a holistic view of threats. Learners will discover Wazuh, an open-source security monitoring solution that evolved from OSSEC to enhance threat detection and compliance management. They will understand how visualization tools aid in detecting cybersecurity threats, with AI integration enhancing data processing efficiency. The lesson concludes by emphasizing the importance of aligning cybersecurity strategies with organizational objectives for robust defense mechanisms.

Objectives

- Recognize the significance of indicators of compromise (IoCs) within threat hunting.
- Discuss the factors that influence the selection of threat hunting tools.
- Analyze and illustrate different types of IoCs.
- Identify different types of tools used in threat hunting.
- Describe how modern cybersecurity products integrate multiple functionalities into unified solutions.
- Analyze the benefits and challenges of integrated solutions.
- Define extended detection and response (XDR) solutions and describe their main features.
- Define the main functionalities of OSSEC and its classification as a HIDS instead of an EDR.
- Describe Wazuh’s features and components.
- Compare and contrast between SIEM for monitoring and SIEM for hunting.
- Identify the components of a Wazuh deployment.
- Explain how to set up and use Wazuh for threat hunting.
- Define the concept of data visualization and recognize how it contributes to threat hunting.
- Describe Wazuh’s built-in visualization features.
- Identify data analytics and visualization tools, such as Power BI, Tableau, and Qlik.
- Explain how the integration of AI with data analytics tools enhances threat data analysis.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
5 min	**Lesson Opener:** Threat Hunting Tools and Techniques	● Introduce learners to the importance of threat hunting tools and techniques in cybersecurity.
5 min	**Real World Scenario:** Threat Hunting Tools and Techniques	● 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.
30 min	**Cyber Uncovered:** Hunting for IoCs	● Recap IoCs as digital footprints indicating potential security breaches or malicious activities, encompassing unusual activity patterns, suspicious file changes, and irregular network communications. ● Describe selecting tools in threat hunting based on IoC types, aligning tool complexity with IoC value according to the Pyramid of Pain. Provide examples like online databases for IP addresses and DNS analysis for domain names. ● Explain hash values generated from files or malware and their confirmation through comparison with databases like VirusTotal. Discuss the hunting approach and the ease with which adversaries can alter hash values. ● Detail how attackers modify hash values using a hex editor to change non-functional data, such as adding/removing code, altering metadata, or padding with non-functional data. ● Define suspicious IP addresses from server or network logs and confirm their validity through cross-referencing against threat intelligence databases. Discuss hunting approaches and adversary tactics for IP address alternation. ● Provide steps to look up IP addresses using AbuseIPDB, including opening the browser, entering the IP address, and analyzing findings on the search results page. ● Introduce suspicious domain names found in network logs and confirmations through analyzing registration details and reputation scores. Discuss hunting approaches and adversary tactics for domain name alternation. ● Outline steps to look up domain registration details using WHOIS lookup services, including accessing the website, entering the domain name, and reviewing the results. ● Define network artifacts as suspicious data streams or patterns detected through intrusion detection systems and explain confirmation methods and hunting approaches, including adversary tactics for altering traffic.

		● Emphasize the importance of inspecting network traffic beyond real-time monitoring, focusing on comparing data across different periods to identify signs of compromise. ● Define host artifacts found in file system logs, registry entries, or system audit logs and discuss confirmation methods, hunting approaches, and adversary tactics for altering host artifacts. ● Describe the process of identifying programs set to start automatically using Sysinternals' Autoruns and navigating the interface to view and analyze Autorun entries. ● Explain the process of identifying adversary tools in logs or network traffic and confirming their use through behavior analysis or comparison with known malicious tools. Discuss hunting approaches and adversary tactics for tool obfuscation. ● Introduce Shellter as a dynamic binary obfuscation tool tailored for Windows Portable Executables, explaining its capabilities and approach compared to traditional methods. ● Define TTPs identified through log analysis, network traffic patterns, and system behavior observations. Discuss confirmation methods, hunting approaches, and adversary tactics for TTP alteration. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class. There are specific prompts that you should ask learners to reflect on to apply the concepts learned to the real world scenario.
20 min	**Lab:** Obfuscating Code and Executables	● 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 in order to properly assess their knowledge and determine where they might need additional assistance.
5 min Break		
30 min	**Cyber Uncovered:** Tools for Threat Hunting	● Introduce three main types of tools in threat hunting: Log management systems, SIEM solutions, and EDR solutions, each serving distinct functions in threat detection and response. ● Discuss the role of log management systems in collecting and storing log data from various sources, facilitating historical data analysis while ensuring compliance and auditing requirements are met. ● Present SIEM solutions as tools that aggregate and analyze data from different sources in real time, provide correlation of events, and offer alerting for potential threats, often incorporating advanced features like AI and machine learning. ● Highlight the focus of EDR solutions on monitoring and responding to threats on endpoint devices, providing detailed forensic data and analysis capabilities while enabling real-time response and mitigation against attacks. ● Discuss the shift from standalone tools to integrated platforms in modern cybersecurity products, aiming to provide comprehensive

		security insights and streamlined operations by combining functionalities of log management, SIEM, and EDR solutions. ● Outline the benefits of integrated security solutions, such as enhanced visibility, simplified management, and cost efficiency, while also addressing challenges like overlapping features, complexity, and skill set requirements. ● Introduce extended detection and response (XDR) as an integrated security solution extending the capabilities of EDR by correlating data across multiple sources, offering a more holistic view of threats and enabling a coordinated response strategy. ● Describe the key components of an XDR solution: Agents, indexers, servers, and dashboards, each playing a crucial role in data collection, organization, storage, analysis, and visualization. ● Emphasize the importance of utilizing SIEM and EDR solutions for effective threat hunting as their integration enhances threat detection and response capabilities by cross-referencing events across various systems. ● Explain the significance of context in interpreting security events, providing examples of how different contexts can influence the interpretation of security events, such as failed login attempts. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class. There are specific prompts that you should ask learners to reflect on to apply the concepts learned to the real world scenario.
3-5 min Pulse Check		
5 min Break		
20 min	**Cyber Uncovered:** Hunting Using Wazuh	● Introduce OSSEC as an open-source tool for monitoring system logs, file integrity, and detecting unauthorized changes, highlighting real-time monitoring, file integrity checking, active response capabilities, and extensive platform support. Mention its role as the foundation for projects like Wazuh. ● Compare OSSEC with EDR, emphasizing OSSEC's focus on compliance, file integrity monitoring, and lack of real-time behavioral analysis and advanced remediation capabilities found in EDR solutions. ● Describe Wazuh as an open-source security monitoring solution, primarily a SIEM built on OSSEC, offering threat detection, incident response, compliance management, integration, and customization benefits. ● Explain Wazuh's components, including OSSEC integration, ELK Stack utilization, file integrity monitoring, vulnerability detection, and compliance management for enhanced threat detection and response. ● Differentiate between using a SIEM for monitoring and hunting, focusing on continuous surveillance and the detection of known threats versus proactive searching for sophisticated threats that evade standard monitoring.

		● Outline the components involved in a Wazuh deployment, including indexer, server, dashboard, and agents, and mention the complexity of installation, with instructions available through the installation assistant and official documentation. ● Detail the functionalities of the Wazuh server, such as displaying security events, compliance monitoring, system inventory, and threat intelligence integration, providing a comprehensive view of security data. ● Provide steps for deploying a Wazuh agent, including obtaining the agent package, installation, configuration, connection verification, and using the agent control program for status checking. ● Highlight the deployment, configuration, and functionality aspects of Wazuh agents on Windows, emphasizing their similarity to OSSEC agents and facilitating migration or understanding for users familiar with OSSEC. ● Explain the structure and purpose of the Wazuh agent configuration file (ossec.conf), divided into sections like <global>, <syscheck>, <rootcheck>, and <localfile>, with examples of settings and configurations. ● Describe the functionalities of Wazuh modules, including log data analysis, file integrity monitoring (FIM), and vulnerability detection, providing insights into system and network activities and alerting on potential security threats. ● Explain how to access data collected by Wazuh agents through the 'Security Events' section of the dashboard for a real-time overview or inspect individual agents by navigating to the 'Agents' section. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class. There are specific prompts that you should ask learners to reflect on to apply the concepts learned to the real world scenario.
5 min Break		
25 min	**Cyber Uncovered:** The Power of Visualization	● Define data visualization as the graphical representation of data to identify patterns, anomalies, and trends in threat hunting, aiding in quicker threat detection and decision-making. ● Discuss how effective data visualization speeds up threat detection, facilitates communication across teams, and improves decision-making by providing clear overviews of data. ● Explain the advanced visualization features in contemporary threat hunting platforms, including customizable dashboards, real-time data visualization, and interactive analysis tools. ● Describe Wazuh's graphical interfaces for aggregating and visualizing data from various sources, emphasizing their role in providing a unified view of an organization's security posture. ● Introduce dedicated data analytics and visualization tools designed to analyze large data sets and present findings visually, enhancing the capabilities of threat analysts.

		● Provide examples of data analytics and visualization tools like Power BI, Tableau, and Qlik, highlighting their features and capabilities for efficient threat identification. ● Explain how modern data analytics tools integrate AI technologies to analyze, interpret, and visualize large data sets more efficiently, augmenting human analysis with automation and predictive analysis. ● Discuss the role of AI in automated data visualization, intelligent data formatting, and interactive data exploration, enhancing the efficiency and accessibility of data analysis. ● Provide an example of interacting with data using natural language queries, such as Power BI's Natural Language Query feature, which leverages AI for immediate visualizations and insights. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class. There are specific prompts that you should ask learners to reflect on to apply the concepts learned to the real world scenario.
20 min	**Lab:** Asking Your Data	● 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 in order to properly assess their knowledge and determine where they might need additional assistance.
10 min	**Lesson Closure**	● 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. ● Key Take-aways: Tools and techniques are not what make the threat hunter, but without them, a threat hunter may be made entirely ineffective. Visibility and environmental awareness/context/knowledge is the most important subject to build upon while actively engaging. ● Recommend that the students read-ahead and come prepared for the next lesson. ● Q&A
25 min	**Open/Free Time**	● Continue discussing that this is close to the end of the program and open the door for career/industry questions. ● Circle back to content needing more depth of discussion. ● Find articles, blogs, research, etc. to utilize to discuss with the class. ● It is highly unlikely that you will find much extra time in the first 6 modules of this course.