LESSON: Threat Hunting Foundations

Before you Begin

This is the first module of the Threat Hunting and Intelligence (THI) course. Instructors should spend no more than the first 10 minutes of class with introductions of the Lead Instructor as by now the students should be well acquainted with the Associate Instructor. Take this opportunity to share your enthusiasm for threat hunting with the class and setting the ground level understanding that this is a proactively engaged practice that many companies fail to do properly.

The THI course mainly focuses on the idea of “finding more bad in better ways”, discovering compromised systems that your other security solutions did not alert to, malware that has alluded EDR and AV, identity and credential-based compromise, persistent and unique fraudulent abuse of systems and applications, and many other engaging topics. Think less in terms of vulnerabilities that can pose risks and potentially be a threat to the environment and more about advanced persistent threat (APT) tactics, techniques, and procedures (TTPs) and how you would go about discovering these behavioral indicators in a post-compromise scenario. How do we hunt an adversary that has already exploited a vulnerability? More often than not, adversaries, even advanced ones, will use very similar and known procedural level operations once they have gained initial access to an organization’s network.

Remember that in today’s time it’s not a question of “if” but “when”, more proactively you should assume when is now and always.

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 discover the active search process for undetected cyber threats within a network. The lesson explores the hypothesis-driven approach of threat hunting and the use of security tools and advanced analytics to identify sophisticated threats. Learners will examine key assumptions, such as network compromise, sophisticated adversaries, and a dynamic threat landscape. The lesson emphasizes the iterative six-step process of threat hunting. Learners will understand how data collection and management, key data sources, and log management tools like the ELK Stack improve cybersecurity throughout the threat hunting lifecycle. The lesson concludes by examining analytical models, such as the Diamond Model of Intrusion Analysis, methods like IoC-based hunting and machine learning, and the significance of establishing and updating baselines for effective threat hunting and incident response.

Objectives

- Define the concept of threat hunting.
- Describe the objectives and key aspects of threat hunting.
- Differentiate between threat hunting and traditional security monitoring.
- Explain the assumptions that govern threat hunting practices.
- Identify the main stages of the threat hunting process.
- Describe the challenges of establishing a threat hunting team.
- Identify common alternatives to a threat hunting team.
- Recognize the benefits of leveraging IR teams for threat hunting.
- Explain the structure of a threat hunting team, focusing on the responsibilities of a threat hunter.
- Recognize the significance of data collection and management in threat hunting.
- Identify key data sources for threat hunting.
- Define the data lifecycle.
- Describe the function of each component within the ELK Stack and its critical role in log searching.
- Explain how to set up the ELK Stack.
- Describe the Diamond Model of Intrusion Analysis within threat hunting.

- Identify different threat hunting methods.
- Recognize the benefits of the Pyramid of Pain model for IOC categorization.
- Explain the role of a baseline in threat hunting and the methods for establishing it.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
10 min	**Introductions**	● Lead Instructor should introduce themselves to the students and open the floor for initial ideas or thoughts.
2 min	**Lesson Opener:** Threat Hunting Foundations	● Introduce learners to the importance of threat hunting in cybersecurity. ● Explain the concept of progressive growth in Threat Hunting. Most organizations take a while to start and then mature this process.
5 min	**Real World Scenario:** Threat Hunting Foundations	● 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.
25 min	**Cyber Uncovered:** Introduction to Threat Hunting	● Provide a comprehensive definition of threat hunting, emphasizing its proactive nature in searching for undetected cyber threats within a network. ● Explain the objectives of threat hunting: Proactive identification, incident prevention, threat intelligence, and continuous improvement. ● Explore the key aspects of threat hunting, emphasizing the proactive approach, skilled expertise, and the continuous nature of the process. ● Compare threat hunting with traditional security monitoring, focusing on their definitions, approaches, goals, and the tools and techniques employed. ● Discuss the assumptions underlying threat hunting, including the assumption of compromise, sophistication of adversaries, and the dynamic threat landscape. ● Introduce the iterative threat hunting process. Examine the stages of preparation, hypothesis development, data collection and analysis, investigation, containment, and documentation and learning. ● 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:** Threat Hunting in an Organization	● Discuss the challenges of establishing a threat hunting team, highlighting resource requirements, operational demands, and organizational impact.

		● Present common alternatives to a threat hunting team, discussing outsourcing to specialized cybersecurity firms and utilizing automated threat hunting software. ● Highlight the trade-offs in terms of expertise, cost, flexibility, and limitations. ● Discuss the option of leveraging incident response teams for threat hunting, emphasizing the benefits of skill diversification and operational improvement in both reactive and proactive cybersecurity approaches. ● Introduce the structure of effective threat hunting teams, outlining roles such as threat hunter, security analyst, incident responder, forensic analyst, and intelligence analyst. ● Emphasize the diverse skills and perspectives each role brings. ● Explain the responsibilities of a threat hunter, highlighting proactive searching, threat identification, mitigation and response, effective communication, and the importance of continuous learning in staying ahead of evolving cyber threats. ● 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 min Pulse Check		
5 min Break		
20 min	**Cyber Uncovered:** Data Collection and Management	● Emphasize the crucial role of effective data collection and management in successful threat hunting, focusing on comprehensive coverage, timely access, and historical analysis. ● Introduce the key data sources for threat hunting, including network traffic, logs, endpoint data, and threat intelligence feeds. Discuss the importance of each source in threat detection. ● Clarify the concept of data storage and retention, addressing the challenges of prolonged storage and the balance required for compliance and legal standards. ● Discuss the data lifecycle in mature organizations, covering stages from creation to deletion or archiving. ● Emphasize the importance of each stage for effective data management. ● Introduce log management systems, highlighting their role in handling large volumes of log data. ● Discuss features such as log aggregation, real-time analysis, and reporting. ● Introduce the ELK Stack as an industry standard for log management. Emphasize its components (Elasticsearch, Logstash, Kibana, and Beats) and its role in collecting, indexing, and displaying logs. ● Explain each component of the ELK Stack, detailing Elasticsearch as a search engine, Logstash as a data processing engine, Kibana for GUI, and Beats as data collectors.

		● Guide learners through the setup of an ELK Stack, from Elasticsearch configuration to Logstash setup and Kibana integration. Stress the importance of additional steps for functional log management. ● Explain Elasticsearch configuration, distinguishing between single instances and clusters. Highlight relevant settings in the configuration file. ● Introduce Logstash configuration, emphasizing the need for configuration in using parser plugins for indexing and analyzing logs. ● Explore Logstash parser plugins, detailing their input, filter, and output sections. Emphasize their role in transforming diverse data formats into a structured form. ● Explain Kibana configuration, noting its relevance to SSL and connection to the Elasticsearch API. Mention its default settings and the way it is used with a reverse proxy like Nginx. ● Guide learners through the data ingestion process, explaining how the ELK Stack can be configured to receive data from multiple sources, including logs, metrics, or security-related events. ● Discuss the role of the ELK Stack in threat hunting, highlighting its usefulness in searching through logs for anomalies, even though it wasn't initially developed for SIEM services. ● 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.
25 min	**Lab:** Setting Up ELK for Data Collection	● This lab mainly pertains to setting up ELK for log ingestion and how to get systems to send beats (events/logs) to ELK. ● 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		
40 min	**Cyber Uncovered:** Conceptual Models and Establishing a Baseline	● Introduce the Diamond Model as a framework for analyzing cyber intrusions. ● Discuss the key questions related to each component: Adversary, capability, infrastructure, and victim. ● Discuss various threat hunting methods, including IoC-based hunting, hypothesis-driven approaches, and the use of machine learning and analytics in cyber intrusion analysis. ● Explain the Pyramid of Pain model, categorizing IoCs based on their difficulty for adversaries to change. ● Highlight the impact of different IoCs on threat hunting and intrusion analysis.

		● Break down the Pyramid of Pain, explaining the difficulty levels of changing different IoCs, from hash values to TTPs. Emphasize the value each level brings in threat hunting. ● Define a baseline in threat hunting and incident response, emphasizing its role in representing a system's standard operational state. ● Discuss how a baseline helps identify deviations that might signify security incidents. ● Highlight the importance of establishing a baseline and compare the detection of threats, response time, and incident analysis with and without baseline data. ● Emphasize the benefits of using a baseline for accurate threat detection. ● Discuss methods for baseline establishment, comparing manual establishment (time-consuming and expert-dependent) with automated tools (quicker, efficient, and algorithm-based). ● Emphasize the need for adjustments over time in baselines. Clarify that initial baselines may be affected by structural changes, role shifts, and technology updates, requiring continuous updates for effectiveness. ● 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:** Elastic Investigation	● This lab is used to hunt through existing logs on the log management system/SIEM (ELK). ● Take the opportunity to mention and differentiate between security engineering (setting up the tool) and security analysis (using the tool to find bad). ● 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**	● 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. ● Key take-aways: Proactivity, motivation, never settling for “good enough” security, and how visibility is key to threat hunting. These will be common discussion points throughout the rest of the course. ● Recommend that the students read-ahead and come prepared for the next lesson. ● Q&A
25 min	**Additional Time Filler (if needed)**	● Begin 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.