LESSON: Enhancing Threat Hunting Capabilities

Before you Begin

Module 8 is the final content-based module of the Threat Hunting and Intelligence (THI) class. Start the night with prefacing the schedule and what to expect for the last two modules of class the following week. Cloud threat hunting is an aspect of the cybersecurity industry that is still very much in the beginning stages. Competent threat hunting as a whole is very rare to find at any given organization. When you interlace the nuanced ways companies are using cloud environments and the speed in which businesses operate and shift it's inevitable that creating a strong threat hunting program well versed in how to hunt adversaries in the cloud can be very difficult. Using cloud-native technology can help and assist in the meantime, but similar to our traditional security monitoring, these tools will put you in a reactive state. As with all threat hunting, visibility into actions taken against systems and applications is still paramount, but now with the added complexity of shared responsibility, which makes the entire concept of threat hunting very difficult. Understanding how the applications run and work, and more importantly how they may be abused and what that abuse may look like in the logs, is another key factor.

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 process of adapting threat hunting strategies to address new vulnerabilities and attack vectors resulting from cloud migration. They will discover the unique aspects of cloud environments and understand the specific security challenges introduced by serverless computing. The lesson emphasizes the shared responsibility model in cloud security and how threat hunting practices differ across infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) models. Learners will discuss the importance of leveraging tools designed for cloud environments, such as cloud native security platforms (CNSPs), cloud access security brokers (CASBs), and advanced logging services, to effectively hunt for threats. Additionally, they will explore cloud-specific logging solutions provided by major cloud service providers (CSPs), focusing on essential cloud events for security analysis. The lesson highlights the importance of structured methodology in threat hunting, exemplified by the Threat Hunting Maturity Model (THMM). The lesson concludes by exploring continuous improvement strategies and aligning threat hunting with strategic objectives for proactive security practices.

Objectives

- Recognize the impact of cloud infrastructure on threat hunting.
- Identify the main considerations related to cloud-based threat hunting, focusing on the challenges of serverless computing.
- Describe the main characteristics of different cloud service models, including IaaS, PaaS, and SaaS.
- Identify cloud-based hunting tools, events, and behaviors.
- Recognize the benefits of cloud logging services and differentiate them from log management systems.
- Identify the logging solutions of different cloud service providers (CSPs).
- Describe important security events that are unique to the cloud.
- Define cloud-native security platforms (CNSPs).
- Identify various CNSPs and compare them with XDR solutions.
- Recognize the significance of cloud access security brokers (CASBs) in cloud-based hunting.
- Match threat behaviors in the cloud with threat hunting practices.
- Compare and contrast threat hunting with and without a strong methodology.
- Define the Threat Hunting Maturity Model (THMM) and recognize its relevance in the evolving cybersecurity landscape.

- Describe each stage of the THMM and explain how organizations can advance to the next stage.
- Describe the main actions required to advance in the Maturity Model.
- Explain how to define threat hunting objectives and differentiate them from threat hunting hypotheses.
- List examples of threat hunting objectives and effectiveness measurements.
- Discuss the importance of documenting threat hunting processes and aligning them with the organization's business goals.
- Describe the process of risk assessment in threat hunting.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
2 min	**Lesson Opener:** Enhancing Threat Hunting Capabilities	● Introduce learners to the importance of enhancing threat hunting capabilities in cybersecurity.
5 min	**Real World Scenario:** Enhancing Threat Hunting Capabilities	● 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:** Threat Hunting and the Cloud	● Discuss the impact of cloud migration on threat hunting practices, emphasizing the need for adaptation to effectively secure increasingly cloud-based services. ● Explain the unique considerations in cloud threat hunting, such as decentralized perimeters, dynamic scalability, complex configurations, and the shared responsibility model, highlighting the challenges posed by these characteristics. ● Present serverless computing as a unique challenge in cloud infrastructure due to its dynamic nature, discussing security concerns like event injection attacks and unauthorized function invocations. Explain the difficulties in monitoring and analyzing serverless function executions. ● Emphasize the importance of adapting threat hunting strategies to align with the shared responsibility model in cloud environments, where security obligations are divided between the cloud provider and the customer, highlighting the need for collaboration with cloud service providers. ● Detail threat hunting practices in IaaS models, where customers are responsible for the infrastructure built upon the cloud provider's foundational services, covering network traffic analysis, system and application log monitoring, vulnerability scanning, and the detection of unauthorized changes. ● Discuss threat hunting considerations in PaaS models, where customers focus on developing and managing applications without dealing with underlying infrastructure complexities,

		highlighting application-level threat hunting, analysis of application behavior, and monitoring data access and usage patterns. ● Explain threat hunting practices in SaaS models, where cloud providers manage complete applications, focusing on monitoring user activities and authentication logs, analyzing data access logs, and ensuring proper configurations and permissions. ● Introduce tools tailored for cloud-based threat hunting, including cloud logging services, cloud-native security platforms (CNSPs), and cloud access security brokers (CASBs), outlining their features and roles in proactive threat detection and mitigation. ● Highlight the granularity of cloud-specific events and behaviors that extend beyond traditional OS capabilities, emphasizing their significance in providing deeper insights into user activities, security settings adjustments, and network traffic unique to cloud services. ● Present a comprehensive approach to threat hunting in the cloud, emphasizing the vast and intricate data sources available and the importance of incorporating cloud-specific data into threat hunting practices, while still relying on data management, understanding threat behavior, and generating alerts. ● 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		
30 min	**Cyber Uncovered:** Cloud Threat Hunting Tools	● Discuss the importance of logging in cloud environments, highlighting the specialized services offered by cloud service providers (CSPs) to facilitate extensive logging and real-time monitoring of cloud resources and applications. ● Compare cloud logging services with traditional log management systems, discussing differences in scope, integration, scalability, analytics, and alerting capabilities. ● Detail logging solutions provided by major CSPs (Amazon Web Services, Microsoft Azure, Google Cloud Platform), focusing on their functionalities, such as monitoring performance metrics, tracking user activity, and aggregating log data. ● Discuss key events specific to cloud environments, including cloud API interactions, configuration and state changes, serverless function executions, and their significance in threat hunting. ● Explain cloud-native security platforms (CNSPs) as comprehensive solutions designed to protect cloud-native applications and infrastructure, including features such as comprehensive coverage, integration with cloud ecosystems, automated security policies, and advanced threat detection. ● Provide an overview of integrated security solutions offered by major cloud providers (AWS Security Hub, Azure Security Center,

		Google Cloud Security Command Center), highlighting their features and benefits. ● Compare CNSPs with extended detection and response (XDR) solutions in terms of protection scope, primary objective, integration focus, and security approach. ● Introduce cloud access security brokers (CASBs) as security policy enforcement points positioned between cloud service consumers and providers, explaining their role in ensuring secure and compliant cloud service usage. ● Discuss common threat behaviors in the cloud, including unauthorized access, misconfiguration exploitation, insider threats, and API vulnerability exploitation. ● Present threat hunting activities and objectives corresponding to cloud threat behaviors, such as analyzing access logs, conducting configuration audits, employing user and entity behavior analytics (UEBA), and performing API security testing. ● 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:** Monitoring Lambda Functions	● 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.
3-5 min Pulse Check		
5 min Break		
30 min	**Cyber Uncovered:** Threat Hunting Maturity Model	● Discuss the evolution of threat hunting over time, emphasizing how it is influenced by technological advancements, organizational learning, and the changing cybersecurity landscape. ● Compare adopting a structured methodology in threat hunting to merely accumulating and reviewing extensive security data, highlighting differences in efficiency, effectiveness, learning, and adaptability. ● Present the Threat Hunting Maturity Model (THMM) as a framework for categorizing an organization's ability to proactively search for and isolate advanced threats that evade existing security solutions. ● Describe the stages of the THMM, from minimal to leading, each characterized by specific traits and capabilities, providing examples of organizations at each stage. ● Explain the characteristics of the minimal stage, where organizations lack formal threat hunting activities and rely solely on basic security measures and incident response. ● Detail the characteristics of the initial (ad-hoc) stage, involving sporadic, manual efforts without formal processes or tools, focusing on ad-hoc analyses when specific threats are suspected.

		● Discuss the procedural stage, where organizations begin to develop standard procedures for threat hunting, utilizing basic tools and techniques to systematically search for threats. ● Explain the characteristics of the innovative stage, where threat hunting integrates advanced analytics, machine learning, and automation to enhance efficiency and effectiveness. ● Describe the leading stage, representing a fully integrated threat hunting program with real-time analysis, a dedicated team, and a strategic, intelligence-led approach. ● Provide guidance on advancing from one stage to the next in the THMM, emphasizing the need to enhance organizational threat detection and response capabilities and cultivate a proactive, intelligence-driven security culture. ● 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		
30 min	**Cyber Uncovered:** Advancing in the Maturity Model	● Outline the steps for advancing from ad-hoc threat hunting to a comprehensive program, including establishing clear objectives and scope, implementing supporting processes and tools, and conducting continuous evaluation and iteration. ● Explain the importance of defining threat hunting objectives, comparing them to hypotheses, and highlighting their role in guiding hunting activities aligned with the organization's security strategy. ● Differentiate between threat hunting hypotheses and objectives: hypotheses guide investigative efforts, while objectives define the scope and direction of hunting activities. ● Provide examples of threat hunting objectives, including detecting undiscovered malware, identifying insider threats, ensuring compliance, and maintaining an awareness of the threat landscape. ● Highlight the significance of establishing clear objectives for measuring threat hunting effectiveness and ensuring alignment with organizational security goals. ● Present examples of metrics for measuring threat hunting effectiveness, such as detection rate of unknown threats, mean time to identify/respond, and coverage of attack surface. ● Explain the transition from ad-hoc to procedural threat hunting stages, emphasizing the need to formalize processes, roles, and responsibilities for consistent and repeatable hunting activities. ● Emphasize the importance of aligning threat hunting with the organization's risk management strategy and business goals to ensure focused efforts and impactful outcomes. ● Define risk assessment as a systematic process for identifying, analyzing, and evaluating threats to organizational assets, emphasizing its relevance to threat hunting.

		● Present the risk assessment flow, outlining steps from identifying threats to developing mitigation strategies, highlighting its role in prioritizing threat hunting activities. ● Discuss the application of risk assessment to prioritize threat hunting activities, focusing on assets and threats with the highest risk potential to allocate resources effectively. ● 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.
10 min	**Lab:** Understanding Threat Hunting and Risk Management	● 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: Cloud environments are still rife with opportunities for misconfigurations and issues that can lead to wide scale data theft or operations impacting attacks. Threat actors are consistently shifting their tactics to cloud environments to ensure that they are maximizing what they can get from the opportunities available. Most organizations are still making egregious DevSecOps mistakes and even when things are configured properly attackers may still find nuanced ways to attack the applications being hosted in various cloud environments. ● 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.