LESSON: Endpoint and Network Hunting

Before you Begin

Endpoint and Network Hunting is Module 5 of the Threat Hunting and Intelligence (THI) course. Be prepared to discuss previous incidents you have encountered in your own relevant experiences. Students seem to really love hearing about previous “war stories” or how you went about hunting through a large amount of data to discover an anomaly and what you did about it. Talk about actual threats you have encountered and mitigated or threat actors you have discovered and removed from the network. If this is not your typical day-to-day operations, as not every instructor works as an Incident Handler or Threat Hunter, consider generating some hypothetical scenarios or reading about previous incidents and how they were originally uncovered. Feel free to utilize the Real World Scenario to lean on a fictitious entity if you are wary of “sharing too much information” about your organization.

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 delve into endpoint threat hunting, identifying indicators of compromise (IoCs) by examining system misconfigurations, potential backdoors, and deviations from established baselines. They will learn to combat misconfigurations through regular audits and continuous monitoring. The lesson emphasizes the importance of combining network and endpoint hunting for comprehensive threat coverage, depth, and breadth of analysis, enhancing the detection of complex attacks. Techniques for detecting command and control (C2) communications, including anomaly detection and DNS monitoring, are discussed, focusing on open-source tools like iodine for DNS tunneling detection. Integration of user and entity behavior analytics (UEBA) into existing security infrastructures is highlighted for early threat detection and mitigation of insider threats, providing comprehensive threat detection and response solutions. The lesson concludes by underlining UEBA's versatility beyond cybersecurity, spanning fraud detection, regulatory compliance, and insider threat programs, demonstrating its value across various organizational domains.

Objectives

- Define the concept and goals of endpoint threat hunting.
- Analyze indicators of a potentially compromised system, including misconfigurations, backdoors, hidden user accounts, and baseline deviations.
- Describe best practices for preventing system misconfigurations.
- Define network threat hunting.
- Compare and contrast between network and endpoint threat hunting, describing the benefits of integrating the two practices.
- Explain how C2 communication works and how to detect this practice.
- Describe how iodine is used in DNS tunneling.
- Explain how to set up an iodine server and run a client.
- Define iodine DNS tunneling from a hunter’s perspective.
- Define UEBA and its main aspects.
- Identify common UEBA anomalies.
- Recognize the benefits of integrating UEBA into threat hunting.
- List examples of UEBA products.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
5 min	**Career Outcomes Content Reminder**	● Remind learners about the Career Outcomes module to ensure that they know that the materials are available and to complete the assigned modules. ● This module will help the learners do the following: ○ Prepare for the interview. ○ Construct questions to ask interviewers. ○ Use Big Interview to practice and sharpen interview skills. ● The Career Outcomes module can be found at the end of Week 2 of the Digital Forensics and Incident Response module. ● Students can reach out to their SSM for questions and help if they need it.
2 min	**Lesson Opener:** Endpoint and Network Hunting	● Introduce learners to the importance of endpoint and network hunting tools and techniques in cybersecurity.
5 min	**Real World Scenario:** Endpoint and Network Hunting	● 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:** Endpoint Threat Hunting	● Introduce endpoint threat hunting as the process of uncovering subtle, unusual activities on endpoints that may indicate a compromise, focusing on system misconfigurations, potential backdoors, and deviations from the baseline. ● Explain system misconfigurations as incorrect or suboptimal settings within a system's software or hardware configurations, leading to security vulnerabilities, and provide examples like unusual user account privileges and disabled security software. ● Define backdoors as covert access mechanisms that can come in various forms like services, user accounts, or scheduled tasks, and discuss how attackers exploit them to maintain unauthorized access to compromised systems. ● Explain hidden users in Windows operating systems, denoted by a dollar sign ('$') appended to their names, and discuss how attackers leverage hidden accounts for persistent access without detection. ● Describe the operational mix between user and service accounts on a system as a potential indication of compromised accounts, highlighting the difference between user and service accounts and how attackers exploit them. ● Discuss remote management services like RDP and VNC, their legitimate uses, and how attackers leverage them for

		unauthorized access, often enabling remote management features not intended for use. ● Highlight legitimate remote access software like TeamViewer and AnyDesk, discussing how attackers abuse them for malicious purposes, such as distributing malware through official channels. ● Explain security software tampering as attackers' attempts to neutralize security measures by shutting down security services or configuring exclusions within these services to evade detection. ● Provide strategies for dealing with security software tampering, including monitoring for unexpected shutdowns and regularly reviewing and auditing exclusion settings. ● Define the baseline in cybersecurity as the standard state of system and network activities and discuss how deviations from this baseline can indicate potential compromises, with examples like unapproved software installations and outdated software versions. ● Offer general strategies to prevent misconfigurations, such as conducting regular audits, utilizing configuration management tools, and implementing continuous monitoring and alerting solutions. ● 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:** Persistence Techniques Investigation	● 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:** Network Threat Hunting	● Introduce network threat hunting as a complementary practice to endpoint threat hunting, providing a macro view of the organizational security landscape by focusing on external communication and internal network traffic to detect threats. ● Compare network threat hunting to endpoint threat hunting, highlighting their respective focuses, data sources, and objectives, emphasizing the need for both methodologies to establish a comprehensive security posture. ● Discuss the benefits of combining network and endpoint threat hunting, including comprehensive coverage, depth and breadth of analysis, and enhanced detection capabilities, stressing the importance of leveraging both methodologies for effective threat detection. ● Define command and control (C2) communication as methods attackers use to remotely control compromised systems or networks within a target's infrastructure, emphasizing its critical role in cyberattacks.

		● Discuss common characteristics of C2 communication, such as obfuscation, low and slow data exfiltration, and dynamic domain generation, highlighting the challenges these characteristics pose to detection efforts. ● Explain the communication flow of C2 communication, from initial foothold establishment to command execution on compromised systems, providing insights into how attackers maintain control over compromised environments. ● Describe how adversaries utilize tunneling to protect C2 communication from detection, focusing on specific protocols like SSH, SSL/TLS, and IPSec, and their role in covertly moving data across a network. ● Discuss common methods for establishing C2 channels, including direct connections, social media channels, covert channels (e.g., DNS or HTTP), and encrypted communications, highlighting the sophistication of C2 mechanisms employed by threat actors. ● Outline the advantages of using HTTP and DNS for C2 communications, emphasizing their ubiquity, stealth, reliability, firewall evasion, and adaptability, underscoring the challenges they pose to detection efforts. ● Stress the importance of identifying and disrupting C2 communications in mitigating cyberthreats, providing an overview of approaches to C2 detection, including anomaly detection, DNS monitoring, beaconing detection, and traffic content analysis. ● Discuss various detection methods for identifying C2 communications, using the example of DNS tunneled C2 communication and emphasizing the importance of monitoring outbound network traffic for irregular patterns and indicators of malicious activity. ● Introduce various open-source tunneling tools used by adversaries for C2 communication, such as iodine, Socat, Chisel, reGeorg, and DNSCat2, emphasizing the need to comprehend how these tools work to improve detection capabilities. ● 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:** C2 Communication with iodine	● Introduce iodine as a high-performance tool facilitating DNS tunneling for transmitting data over DNS queries and responses, bypassing network firewalls and filters that do not closely scrutinize DNS traffic. ● Explain the client-server model of iodine operation, where the client initiates the tunnel and encodes outgoing data into DNS query payloads, which are routed through standard DNS pathways, allowing for data transmission.

		● Provide step-by-step instructions for setting up an iodine server, including registering a unique domain, configuring DNS settings, installing iodine software, and running the iodine server command with necessary parameters. ● Explain the process of running the iodine client, emphasizing the need for installation before execution and providing the command syntax with required parameters for initiating the client-side tunnel. ● Discuss how to identify C2 traffic created using iodine in Wireshark, highlighting indicators such as lengthy subdomains, increased query frequency, encoded data in DNS queries and responses, and destination domain consistency. ● Explain how iodine packets often feature unusually long subdomain strings due to the encoded data payload and how identifying DNS queries with extensive subdomain lengths can indicate potential DNS tunneling activity. ● Discuss the significance of a higher than normal frequency of DNS requests to a specific domain or subdomain as an indicator of active DNS tunneling, emphasizing the continuous communication between the client and server in iodine operation. ● Describe the presence of encoded information in the 'Data' section of DNS queries and responses as a method of covertly transferring tunnel data, highlighting the non-standard characters or patterns that may indicate encoded data. ● Emphasize the consistent targeting of the same domain in DNS requests as an indicator of DNS tunneling activity, explaining how repeated domain names in queries can be indicative of tunneling traffic. ● Discuss how adversaries can use tunneling protocols apart from iodine, such as SSH, HTTPS, ICMP, and others, to conceal their activities, highlighting that similar anomalies presented in the presence of iodine compared to regular DNS traffic will also be visible for other protocols. ● 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:** DNS Tunneling Investigation	● 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		
20 min	**Cyber Uncovered:**	● Introduce UEBA as a cybersecurity process utilizing advanced analytics to monitor and analyze user and entity behavior within a network, leveraging machine learning, data science, and

	User and Entity Behavior Analytics (UEBA)	statistical algorithms to detect anomalies indicative of potential security threats. ● Discuss the main aspects of UEBA, including behavioral profiling to establish baseline behaviors, anomaly detection to pinpoint unusual actions, and contextual analysis to enhance threat detection accuracy by understanding the context behind activities. ● Provide examples of common UEBA anomalies, such as unusual access times, geographic irregularities, excessive file downloads, and anomalous application use, highlighting how these deviations can signal various security threats. ● Outline the benefits of integrating UEBA into threat hunting, including early threat detection, reduced false positives, and insider threat mitigation, emphasizing UEBA's ability to detect subtle indicators of insider threats and improve operational efficiency. ● Discuss how UEBA is integrated into modern security platforms like SIEM, EDR, and XDR solutions, providing examples of UEBA products such as Rapid7 InsightIDR, Splunk User Behavior Analytics, and Aruba Introspect, and highlighting their capabilities in threat detection and response. ● Explain how UEBA extends beyond cybersecurity defense into domains such as fraud detection, regulatory compliance, and insider threat programs, emphasizing its analytical capabilities and potential to enhance operational integrity across organizations. ● 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	**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: Both endpoint artifacts and network activity can be viable sources for threat hunting. Neither is better than the other necessarily, but network activity will often be a little more difficult to make sense of due to encoding, encryption, and misuse of legitimate protocols. As previously mentioned, visibility and data are the lifeblood of a good threat hunting team. ● 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.
2 min	**Midpoint Course Survey**	● Allocate 2 minutes to facilitate the completion of the Midpoint Survey. ● Encourage learners to provide honest and constructive feedback about their learning experience.
3 min	**Discussion Board**	● Allocate 3 minutes to review the discussion board slides and how it impacts students' final grades.