LESSON: Dealing with Advanced Persistent Threats (APTs)

Before you Begin

This is the 7th module of the Threat Hunting and Intelligence (THI) course, Module 6 is the student's asynchronous content. This is also the second to last module that has slides and content, with the last week of the course dedicated to the Hands-On Certification and Security+ discussions. The topic of hunting for Advanced Persistent Threats (APTs) is an important one that will require students to think about the situation quite a bit more deeply than surface-level thinking such as hashes and domain names. The concept of living-off-the-land and the difficulty in determining truly malicious actions and those that mirror them but were otherwise benign actions in the logs is something that cannot be overstated enough. Understanding APTs and how they operate often helps to answer a common question, "why hasn't anyone been able to create a tool to stop attacks from happening?", because to do so would be to stomp on many legitimate operations within corporate environments.

The key factor when considering APT type threat actors is the notion of *persistence* which is indicated in the name. Many threat actors can be relatively rudimentary in terms of technicality but still successfully compromise seemingly secure environments. Contrarily, they can operate with exceptionally advanced tactics such as exploitation of zero-day vulnerabilities and other advanced TTPs. No matter how they decide to infiltrate the organization, they wish to persist as long as necessary to meet operational goals and if they were to lose access they would be persistent in attempting to regain their access. Many organizations will face similar APT groups wishing to compromise a large number of entities, but many organizations will also face persistent actors not seen by other organizations due to their unique applications and data sets. The answer to "why these particular organizations?" is that it helps to achieve the goals of the threat actor group.

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 critical role of indicators of compromise (IoCs) in identifying potential security breaches by aligning threat hunting tools with the types of IoCs using the Pyramid of Pain model. They will learn about the effectiveness of hash values in malware association and the importance of cross-referencing IP addresses and domain names with threat intelligence databases. The lesson emphasizes utilizing log management systems, SIEM solutions, and extended detection and response (XDR) solutions for comprehensive threat detection and response. Learners will discover how integrating SIEM and EDR enhances threat detection capabilities, exemplified by versatile open-source security monitoring solutions like Wazuh. The lesson concludes by highlighting the significance of data visualization in transforming complex data sets into understandable formats and integrating AI into data analytics for enhanced threat understanding.

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 PowerBI, 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
2 min	**Lesson Opener:** Dealing with Advanced Persistent Threats (APTs)	● Introduce learners to the importance of advanced persistent threats (APTs) in cybersecurity.
5 min	**Real World Scenario:** Dealing with Advanced Persistent Threats (APTs)	● 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:** Understanding APTs	● Define advanced persistent threats (APTs) as groups or entities engaged in sophisticated, prolonged cyber espionage or cyberattacks against specific targets, often state-sponsored or highly organized criminal actors. ● Highlight common characteristics of APTs, including their state-sponsored or organized nature, targeted operations, sophisticated methodologies, and long-term persistence in networks. ● Compare APTs with opportunistic attackers across various aspects, such as objectives, resources, tactics, target selection, and duration and persistence, emphasizing the strategic nature and advanced capabilities of APTs. ● Discuss the strategic risk posed by APTs to national security and corporate competitiveness, emphasizing the need for responses beyond typical IT security measures and the importance of collaborative approaches involving public-private partnerships and international cooperation. ● Provide examples of notorious APTs, including APT1 (Comment Crew), APT28 (Fancy Bear), APT29 (Cozy Bear), APT38 (Lazarus Group), and APT41 (Wicked Panda), highlighting their attributed origins and notable cyber activities. ● Explain the significance of naming APTs in cyberthreat intelligence, describing various naming taxonomies and conventions, including animal-based naming conventions like bears (Russian APTs), pandas (Chinese APTs), kittens (Iranian APTs), and tigers (Southeast Asian APTs).

		● Discuss the importance of identifying APTs in enhancing organizational security postures, including tailored security measures, strategic resource allocation, collaborative defense enhancement, and proactive threat hunting. ● Present a case study on Volt Typhoon, a group associated with the People's Republic of China (PRC) state-sponsored actors, detailing their targeting of U.S. critical infrastructure for espionage and potential disruptive or destructive cyber activities. ● Describe observations related to Volt Typhoon's activities since mid-2021, including their targeting of critical infrastructure organizations across various U.S. territories, their focus on espionage and maintaining undetected access, and their use of stealth tactics and compromised network equipment. ● Explain the collaborative response to Volt Typhoon's activities, including the issuance of a joint cybersecurity advisory (CSA) by the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) to help organizations identify and mitigate potential compromises. ● 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:** Hunting for APTs	● Introduce the topic of hunting for APTs, highlighting the need for a nuanced approach due to their unique characteristics, including stealth, persistence, sophistication, and targeted nature. ● Discuss common APT attack techniques, such as spear phishing, exploiting zero-day vulnerabilities, and living off the land (LOTL), emphasizing how these techniques differ from those employed by opportunistic attackers and the challenges they pose for detection. ● Define living off the land (LOTL) as a technique where attackers use legitimate tools and protocols already present on the target's system or network for malicious activities, providing examples of LOTL utilities commonly used on Windows systems. ● Detail the capabilities of Certutil and WMI in executing malicious activities, including downloading and decoding files and executing commands on remote systems, illustrating how these tools can be abused by attackers. ● Explain the challenges in detecting LOTL techniques, including the use of legitimate tools, minimal footprint, and blending in with normal activity, highlighting why traditional security solutions struggle to identify these techniques. ● Present strategies for combating LOTL techniques, including behavioral analysis, anomaly detection, and enhanced logging and monitoring, emphasizing the importance of proactive threat hunting practices.

		● Introduce Sysmon as a tool for enhancing logging on Windows systems, highlighting its ability to capture comprehensive system activity logs and establish baselines of normal activity. ● Discuss how Sysmon can be used for threat hunting, enabling security teams to capture detailed system activity logs, establish baselines, and implement complex detection rules tailored to specific APT techniques. ● Provide an example of a Sysmon rule for detecting LOTL activities involving the execution of PsExec, illustrating how such rules can be used to identify the unauthorized use of administrative tools and command-line utilities.
3-5 min Pulse Check		
5 min Break		
20 min	**Cyber Uncovered:** Hunting Using Honeypots	● Introduce hunting using honeypots as a proactive defense measure against APTs, highlighting their ability to detect infiltration attempts early and provide valuable insights into attack methodologies. ● Define honeypots as deliberately vulnerable systems designed to lure cyberattackers, explaining their purpose of detecting, deflecting, or studying hacking attempts, and their role as decoys to divert attackers from real targets. ● Discuss the classification of honeypots based on their level of interaction and complexity, including low, medium, and high interaction levels, and how each serves different security objectives. ● Explain the categorization of honeypots based on the types of assets they simulate, such as application, service, and client honeypots, and their respective roles in attracting and analyzing cyberthreats. ● Present the two main reasons for deploying honeypots: production honeypots, which mimic actual services to detect threats and protect real assets, and research honeypots, which gather detailed information about threats to improve cybersecurity knowledge. ● Define honeynets as networks of interconnected honeypots designed to simulate real network environments and attract sophisticated attackers, explaining their role in capturing detailed information about threats and attack methodologies. ● Compare honeypots and honeynets in terms of complexity, objective, deployment, risk management, data collection, and use cases, highlighting their respective strengths and suitability for different security needs. ● Discuss the strategic approach to effectively deploying honeypots, whether through custom instances tailored to specific threats or dedicated honeypot solutions with preconfigured settings and built-in alerting mechanisms. ● Introduce several dedicated honeypot solutions, including Kippo, Cowrie, Dionaea, Glastopf, and Honeyd, explaining their features

		and intended use cases for capturing different types of cyberthreats. ● Outline the steps involved in setting up a dedicated honeypot solution, including designating an environment, setting up the virtual environment, configuring vulnerable services, implementing monitoring and alerting, and testing the honeypot. ● Explain the configuration aspects of a dedicated honeypot, focusing on network placement and accessibility, system and service simulation, and logging and monitoring settings. ● Highlight the insights that can be gained from honeypots, including understanding attack patterns and techniques, APT behavior, vulnerability identification, and the assessment of security posture, emphasizing their role in enhancing organizational defenses against APTs. ● 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:** Setting Up a Honeypot	● 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:** Adversary Simulation	● Introduce adversary simulation as a proactive defense technique against APTs, emphasizing its role in replicating real-world adversary actions within an organization's network. ● Discuss the importance of adversary simulation in gaining insights into APT penetration methods, identifying vulnerabilities, and enhancing detection and response capabilities. ● Compare adversary simulation and penetration testing in terms of objectives, approach, focus, and outcome, highlighting how simulation mimics real-world APT behavior for long-term engagement. ● Present different methods of simulating adversary actions, including scripts, emulation software, and red team exercises, explaining their suitability for various security assessments. ● Introduce the APTSimulator project as a collection of scripts designed to simulate APT activities within a network environment, emphasizing its role in testing security controls and incident response capabilities against APT attack techniques. ● Describe MITRE Caldera as a cybersecurity framework for automating adversary simulation, enabling organizations to test their defenses against realistic threats in a controlled environment. ● Explain the components of Caldera, including the server, agents, adversary profiles, and plugins, detailing how they work together to simulate adversary behavior.

		● Discuss the role of Caldera agents as endpoints for executing tasks that simulate real-world attacker actions, emphasizing their deployment and management via the Caldera server. ● Explain how Caldera's built-in adversary profiles mimic the operational patterns of real-world threat actors, providing a targeted approach to testing and improving defense mechanisms. ● Describe Caldera operations as tailored simulations designed to test specific aspects of an organization's cybersecurity defenses, providing a comprehensive overview of the system's resilience against APTs. ● Outline the steps involved in using Caldera for APT hunting, including adversary profile customization, operation design, and result analysis, emphasizing the iterative process of enhancing security posture based on simulation results. ● 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:** Adversary Simulation Using Caldera	● 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: APTs operate in ways that are much more difficult to detect, but they are not ghosts on the box/wire. They do still have many telltale signs of being in the environment and leave trails of what actions they took while there. You may need enhanced logging or well functioning tools to be able to discover them in addition to active threat hunting to assist in processing the data. ● 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.