LESSON: Cyber Threat Intelligence

Before you Begin

This is the second module of the Threat Hunting and Intelligence course. Instructors should highlight how cyber threat intelligence (CTI) empowers organizations to operate at a higher level than without, allowing a proactive and threat-informed defensive strategy that encompasses how adversaries actually operate and function. The cybersecurity industry contains a plethora of useful resources, frameworks, blogs, research, groups, etc. that can be exceedingly beneficial for organizations of all industries and sizes. Empowering both employee and executive level stakeholders with awareness to the latest threats, incident response teams with contextualized information to work more efficiently, threat hunters to hunt more effectively, fraud analysts to find more fraudulent activity, or whatever the use-case at hand may be; CTI can be one of the most empowering forces that an organization can employ.

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 world of cyber threat intelligence (CTI), analyzing information to enhance decision-making and threat hunting processes. Learners will examine diverse threat intelligence sources like open-source intelligence, social media, and the dark web, providing crucial data such as indicators of compromise (IoCs) and tactics, techniques, and procedures (TTPs). The lesson presents various threat intelligence types, including strategic, tactical, operational, and technical, each with unique sources. Learners will grasp how to integrate threat intelligence feeds into security products and platforms to enhance threat hunting capabilities. They will also learn the importance of automating threat intelligence parsing and correlating it with organizational vulnerabilities for proactive defense. The lesson concludes by exploring hypothesis-driven hunting and practical strategies like purple teaming for improved detection and response.

Objectives

- Define the threat intelligence process and recognize its importance.
- Identify different types of threat intelligence and sources.
- Describe the main features of open-source, commercial, and governmental threat intelligence.
- Recognize the significance of threat feeds within threat intelligence.
- Identify public threat intelligence platforms.
- Describe the role of CTI parsing and correlation in automating and optimizing threat hunting.
- Identify standardized languages for sharing threat intelligence.
- Describe the MITRE ATT&CK framework and compare it with other CTI platforms.
- Define the concept of a hunting hypothesis and its role in proactive hunting.
- Compare and contrast between hypothesis-driven and data-driven hunting.
- Identify the steps involved in the hypothesis development process.
- Exemplify the use of hypotheses in threat hunting through a use case.
- Recognize testing detection capabilities as a practical alternative to threat hunting in resource-limited environments.
- Identify the role of hypotheses in verifying detection capabilities.
- Discuss the consequences of misconfigured security services.
- List misconfiguration issues in security services.
- Explain how purple teaming can improve detection and response capabilities.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions

2 min	**Lesson Opener:** Cyber Threat Intelligence	● Introduce learners to the importance of threat intelligence in cybersecurity.
5 min	**Real World Scenario:** Cyber Threat Intelligence	● Explain how when companies start to use cyber threat intelligence that the teams may lack purpose and initially establishing the “why” you are collecting and using the intelligence can be a big game changer for growth and maturity. ● Lean into the notion that better usage of cyber threat intelligence would greatly empower Bright Wash Manufacturing’s capability to fight off advanced threats. ● 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.
40 min	**Cyber Uncovered:** Cyber Threat Intelligence (CTI) Overview	● Provide a comprehensive definition of cyber threat intelligence, emphasizing its goal of informing decision-makers. ● Explain the different CTI sources available, such as open-source intelligence and social media, and its outputs, including IoCs and TTPs. ● Highlight the importance of threat intelligence in enhancing threat hunting activities, providing context to security alerts, anticipating attacker methods, and enhancing situational awareness. ● Compare threat hunting with and without threat intelligence, discussing efficiency, security, and approach differences. ● Emphasize the benefits of using threat intelligence for efficient and proactive threat hunting. ● Introduce different types of threat intelligence (strategic, tactical, operational, technical) and their characteristics and sources (government reports, security bulletins, etc.). ● Define open-source threat intelligence as derived from publicly available sources like hacker forums and social media. ● Discuss its importance in gathering information about potential or current attacks. ● Provide examples of open-source intelligence sources, including security blogs, open databases, and technical documentation. ● Highlight their value in offering expert insights and analyses on cyber threats. ● Present commercial threat intelligence sources as specialized services providing real-time information on emerging cyber threats. ● Compare commercial threat intelligence sources with open-source intelligence, emphasizing benefits like specialization and expert analysis. ● Define governmental threat intelligence sources, offering insights into national and international cyber threats. ● Highlight their importance for organizations, especially those responsible for critical infrastructure.

		● 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:** CTI Feeds and Platforms	● Provide a comprehensive definition of threat feeds, highlighting their concise and actionable nature compared to blog posts and whitepapers. ● Discuss how CTI feeds assist in immediate threat detection and response. ● Describe the integration of threat intelligence feeds into security products like CrowdStrike and Proofpoint. Highlight the benefits and potential limitations of relying on a limited set of data sources. ● Introduce publicly available threat intelligence platforms like AlienVault OTX and IBM X-Force Exchange. ● Discuss their features and benefits in sharing threat intelligence with security professionals. ● Emphasize the importance of automating the parsing of threat intelligence to maximize efficiency and effectiveness in threat hunting. ● Discuss how automation speeds up detection, ensures consistency, and facilitates scalability. ● Explain the significance of correlating threat intelligence with organizational infrastructure for a proactive approach to threat hunting. ● Highlight the importance of prioritizing defenses based on specific vulnerabilities and assets. ● Present STIX and TAXII as the formats used to share threat intelligence. Explain STIX as a standardized language for describing cyber threat information and TAXII as a protocol for securely exchanging threat information. ● Analyze the provided example of STIX data in JSON format, emphasizing its structured and machine-readable nature for describing cyber threats. ● Define STIX Relationships as connections linking various cyber threat intelligence elements to depict a comprehensive understanding of cyber threats. Discuss their importance in contextualizing threat intelligence. ● Introduce the MITRE ATT&CK framework as a significant knowledge source of adversary TTPs. Discuss its role in identifying and mitigating threats effectively. ● Explain the components of the ATT&CK framework, including tactics, techniques, procedures, threat groups, and software. Highlight their importance in understanding adversary behavior. ● Compare MITRE ATT&CK with other CTI platforms, with an emphasis on their focus, structure, usage, community involvement, and integration 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.
20 min	**Lab:** Collecting Cyber Threat Intelligence	● The STIX lab helps solidify the usage of a common language amongst disparate data sources/entities/vendors to allow sharing and usage of information in a standard format. ● Highlighting that STIX is simply just a known implementation of JSON can be valuable here. Walk through that they are simply key:value pairs the lead to relationships and entity building. ● 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 min Pulse Check		
5 min Break		
30 min	**Cyber Uncovered:** Hypotheses for Threat Hunting	● Provide a comprehensive definition of a hunting hypothesis, emphasizing its role in guiding the hunt for cyber threats within an organization's network. ● Explain how hypotheses are created based on existing threats, vulnerabilities, and historical data. ● Provide examples of hypotheses, such as identifying unknown malware, compromised credentials, or established persistence in the network. Highlight the predictive nature of hypotheses in threat hunting. ● Mention that the main role of hypotheses is to create focus and clarity amidst vast amounts of information. Explain how hypotheses determine methodology and provide a structured framework for analysis in proactive hunting. ● ● Mention that hypotheses can also be based on data rather than just threat intelligence. ● Outline the process of hypothesis development, including reviewing threat intelligence, developing preliminary hypotheses, collecting relevant data, analyzing and testing hypotheses, refining them based on insights, and documenting findings. ● Present the provided phishing scenario faced by a financial services company, including context about increased phishing attempts, industry trends, and data breach reports. ● Describe the hypothesis development process based on the phishing scenario, such as identifying APT groups targeting the financial services company to gain access to sensitive data. ● Outline potential hunting steps for validating the phishing scenario hypothesis, including email analysis, monitoring threat intelligence feeds, assessing employee training, and increasing network monitoring.

		● Discuss the expected outcomes if the hypothesis is true, such as identifying specific APT groups and enhancing defensive strategies. ● Explain the response if the hypothesis is not supported, focusing on general cybersecurity measures and employee training. ● 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		
20 min	**Cyber Uncovered:** Detection Capabilities Testing	● Introduce the concept of testing detection capabilities as an alternative to threat hunting in resource-limited environments. ● Explain how detection capabilities testing offers a structured approach to identify vulnerabilities and assess system defenses. ● Define the detection capabilities hypothesis, emphasizing its focus on identifying and neutralizing potential threats to validate proactive defense strategies. Mention that it validates detection mechanisms rather than actively hunting threats. ● Provide examples of detection hypotheses, such as detecting unusual outbound traffic patterns, unauthorized system changes, or access requests from atypical geographical locations. ● Explain the dangers of misconfigured security services and how they can be as dangerous as skilled attackers by failing to detect intrusions and creating false security. ● Outline the forms misconfiguration can take, including inadequate coverage, false negatives, and alert fatigue, and their implications for network security. ● Define purple teaming as a collaboration between the red team (attack simulation) and the blue team (defense) to improve detection and response capabilities. ● Describe the process of conducting a gap analysis after purple teaming, including identifying and analyzing current detection capabilities and structuring a plan to address areas attackers could exploit. ● 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:** Validating Detection Rules	● The lab's main goal is to help learners conceptualize the idea of testing and validating detection rules. The instructor should explain that a detection needs to be validated and ensure that it will alert when appropriate, highlighting the importance of the discussion from the previous section. ● 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: CTI is the lifeblood of a strong and mature cybersecurity department and even more so to enable effective threat hunting at broad scope. Without the proper awareness being imparted to the appropriate audiences, many things will go missed and unattended to. ● Recommend that the students read-ahead and come prepared for the next lesson. ● Q&A
25 min	**Additional Time Filler (if needed)**	● 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.