LESSON: Incident Response Planning

Primer

This module includes two short labs: the first lab focuses on Applying the Six Stages of Incident Response, while the second lab covers Initial Triage in a Windows Environment. We highly recommend that instructors plan ahead to allocate sufficient time for these labs to ensure students have ample opportunity to practice, especially the second lab as it requires a lot of investigation.

For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed for each lesson

- 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.
- 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. 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 gain an understanding of incident response, its critical importance, and the multifaceted process involved. They will recognize the potential consequences of unhandled incidents, ranging from severe data loss to legal penalties. The structure and composition of a computer security incident response team (CSIRT), including the collaboration with a security operations center (SOC), will be explored. Participants will delve into the intricacies of incident response strategies, playbooks, and the six stages outlined by the SANS incident response framework: Preparation, identification,

containment, eradication, recovery, and lessons learned. Practical aspects will be covered, such as asset definition, protection measures, the RACI matrix, and tools like Belkasoft Triage, F-Response, and KAPE, ensuring that learners grasp the complexities of incident identification, triage, and response in various environments, including cloud settings. The lesson will conclude by emphasizing the importance of external communication management and collaboration with cybersecurity firms, while highlighting common pitfalls to avoid during incident response.

Objectives

- Define the main goal of incident response.
- Recognize the risks involved in unhandled incidents.
- Describe the stages of the incident response process.
- Identify the roles and responsibilities of CSIRTs, SOCs, and non-technical positions in incident management.
- Recognize the importance of playbooks and incident response strategies and explain how they vary among organizations.
- List the aspects involved in the incident response preparation stage.
- Define organizational assets and identify the steps involved in asset protection.
- Recognize the significance of the RACI matrix in identifying incident response roles and responsibilities.
- Explain what a jump kit is and the tools and technologies it includes.
- Identify the strategies required for incident response in cloud environments.
- Recognize the importance of establishing internal and external incident handling communication channels.
- Identify different types of triggers involved in the incident identification stage.
- Recognize the importance of collaborative work between the CSIRT and the SOC for system monitoring.
- Define the concept of triage.
- Recognize the significance of log collection during the incident identification stage.
- Identify the most relevant artifacts for the triage process.
- Describe different triage tools and explain how they work.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
2 min	**Lesson Opener:** Incident Response Planning	● Introduce learners to the importance of incident response planning in cybersecurity.
5 min	**Real World Scenario:** Incident Response Planning	● 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.

5 min	**Lesson Companion:** Incident Response Planning	● Review the lesson companion, 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.
20 min	**Cyber Uncovered:** Incident Response Fundamentals	● Begin by emphasizing the critical role of incident response (IR) in cybersecurity, with the primary goal of managing and mitigating security incidents. ● Discuss the potential consequences of unhandled incidents, including data loss, financial damage, and reputational harm. ● Emphasize the effectiveness of even a basic incident response plan. ● Define key terms such as "event," "incident," and "breach." ● Ensure clarity on the distinctions between these terms and their implications for information security. ● Explore the proactive nature of incident response, which starts before an incident occurs. ● Cover aspects like planning, procedures, role definition, and communication strategies to enable swift and effective responses. ● Discuss the involvement of various personnel during an incident. ● Highlight the importance of a well-defined computer security incident response team (CSIRT) and their training and tools for efficient incident management. ● Clarify the roles of CSIRT and security operations center (SOC), emphasizing that they may not be composed of the same personnel or function as a single unit. ● Discuss the specific responsibilities of each team. ● Explore non-technical roles, such as public relations, and their significance during an incident. Introduce key individuals and teams involved, including the CEO, public relations, board of directors, system team, network team, NOC, help desk, and outsource advisors. ● Emphasize on the critical role both the Public Relations and Legal team play during the incident response ● Highlight the variability in incident response across organizations based on operational structures, regulatory requirements, and risk profiles. ● Provide examples, such as the priorities of a financial institution vs. a healthcare provider. ● Conclude by emphasizing the importance of incident playbooks. Discuss how these detailed guides provide step-by-step instructions for responding to specific security incidents, ensuring consistency and efficiency. ● Illustrate tailored scenarios, such as phishing attacks, ransomware infections, or data breaches. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Incident Response Fundamentals. There are specific prompts that you should ask

		learners to reflect on to apply this concept to the real world scenario.
5 min	**Real world scenario:** Incident Response Fundamentals	● 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.
5 min Break		
20 min	**Cyber Uncovered:** The Six Stages of IR	● Emphasize the significance of incident response and introduce the SANS Institute's framework. ● Highlight the six stages of incident response: Preparation, identification, containment, eradication, recovery, and lessons learned. ● Discuss the activities involved in the preparation stage, such as creating policies, developing plans, setting up communication protocols, and training the incident response team. ● Stress the importance of assessing risks and conducting simulations for readiness. ● Explore the identification stage, focusing on incident detection, immediate actions, and determining the incident scope. ● Discuss the role of security measures in initiating the response plan and reacting to the situation. ● Examine the containment stage, covering short-term and long-term strategies to stop immediate damage and prevent further spread. ● Discuss the careful and thorough execution required during the eradication stage to eliminate the incident root cause. ● Explore the recovery stage, explaining how affected systems and services are restored and brought back into operation. ● Discuss the importance of the lessons learned stage in reviewing, documenting, and improving the incident response plan and processes. ● Provide the ransomware incident example and discuss how the six stages of IR can be applied. ● Emphasize the specific actions taken at each stage, from preparation to lessons learned.

		● Compare the SANS incident response framework with the NIST incident response framework, highlighting similarities and differences. ● Discuss how both frameworks contribute to effective incident response. ● Address common pitfalls in incident response, focusing on the overlooked 'lessons learned' phase and the potential issues with premature threat eradication. ● Emphasize the importance of proper scoping for thorough incident removal. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
5 min	**Real World Scenario:** The Six Stages of IR	● 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.
20 min	**Lab:** Applying the Six Stages of IR	● 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 to properly assess their knowledge and determine where they might need additional assistance.
5 min	**Pulse Check**	● Before you launch the pulse check, explain each section clearly, and encourage the learners to participate in the survey. ● After administering the survey, share the poll results with learners and ask learners to provide feedback ● Encourage learners to attend office hours with the associate instructor.
5 min Break		
20 min	**Cyber Uncovered:** Preparation Stage	● Provide an overview of why incident preparation is crucial in cybersecurity. ● Highlight the key aspects that need to be identified and defined during the preparation phase. ● Define organizational assets and discuss their significance in achieving goals. ● Provide examples of tangible and intangible assets within an organization. ● Explain the characteristics of assets and their role in determining importance in security strategy. ● Discuss how understanding these characteristics can aid in incident response planning. ● Use the customer database example to illustrate steps taken during a data breach incident. ● Discuss the reasons why protecting critical assets like a customer database is important for a company. ● Introduce the RACI matrix and its components.

		● Provide a practical example of how the RACI matrix can be applied in incident response. ● Emphasize the importance of having tools tailored to an organization's technologies. ● Discuss the potential challenges and consequences that can arise if the IR team lacks preconfigured tools. ● Explain the concept of a 'jump kit' and its contents for incident response. ● Discuss the ways that maintaining a jump kit enhances the readiness of the CSIRT. ● Discuss the differences in responding to incidents in cloud environments compared to on-premises. ● Highlight the need for adapting measures and policies. ● Emphasize the importance of collaboration with DevOps and IT professionals when handling cloud-centric incidents. ● Explain the importance of predefined and secure communication alternatives during incidents. ● Discuss the reasons why it is crucial to have multiple redundant channels for effective incident response. ● Discuss the pressure and aspects that must be taken into consideration when managing external communications during incidents. ● Examine the reasons why organizations often rely on external cybersecurity firms and how internal IR teams coordinate with them. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on the preparation stage. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
	Real world scenario: Preparation Stage	● 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 to properly assess their knowledge and determine where they might need additional assistance.
5 min Break		
20 min	**Cyber Uncovered:** Identification Stage	● Explain the concept of continuous events within an organization's digital infrastructure. ● List and discuss the four triggers that can initiate the identification of a security incident. ● Discuss the importance of quick and efficient actions once a potential incident is identified. ● Explain the collaboration between CSIRT and SOC during incident identification. ● Discuss the challenges organizations face when managing multiple incidents simultaneously. ● Provide an example scenario in which an organization might need to triage multiple incidents. ● Define triage in the context of incident response.

		● Discuss the seven considerations during the triage process. ● Explain the importance of collecting logs and evidence as soon as an incident is identified. ● Discuss the significance of focusing on disk and memory images, network traffic captures, and application logs during an investigation. ● Introduce three tools used for incident response triage. ● Describe the process involved in BelkaSoft Triage, including key steps. ● Discuss the refinement options available within BelkaSoft, such as skin identification and hash comparison. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
5 min	**Real world scenario:** Preparation Stage	● 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 to properly assess their knowledge and determine where they might need additional assistance.
20 min	**Lab:** Initial Triage in Windows Environments	● 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 to properly assess their knowledge and determine where they might need additional assistance.
15 min	**Lesson Closure**	● Encourage learners to read ahead of time ● Provide learners additional resources to read / practice and assign homework (e.g., future labs) before you demonstrate the labs during the next class ● Spend some time to highlight what are the key takeaways from today's lesson ● Important topics covered during the class includes ○ Highlight the main purpose of the Incident Response ○ Reminder learning about the Benjamin Franklin Quote "By failing to prepare, you are preparing to fail" ○ Highlight the current unhandled incident reported in 2023 is $4.45 Million ○ Provide the main key takeaway when the incident response begins such as creating a plan, procedure and define roles and responsibilities ○ Summarize the key players in the CSIRT team such as IT professionals, security experts, decision makers and various stakeholders within an organization ○ Highlight the main difference between CSIRT and SOC ○ Provide the main key takeaway for Incident response Playbook

		○ Provide the main key takeaway of the six stages of IR ○ Highlight the main takeaway of the SANs and NIST Incident Response Framework ○ Provide a summary of IR pitfalls ○ provide the key takeaway for assets definition, valuation and protection ○ Highlight the importance of role and responsibilities before an incident occurs using RACI matrix ○ Highlight the main tools and technologies used for the IR investigations ○ Highlight the main triggers in the Incident Response such as IDS, Unusual System Behavior, user Reports, and External Notifications ○ Highlight the triage tools such as Belkasoft triage, F-Response, KAPE.
	Add Additional Time Filler	● Review using Kahoot or other similar platforms ● Conduct interview preparation conversations ● Continue discussions on real-world scenarios ● Demonstrate how to create users in Linux and grant them permissions ● Discuss different career paths in cybersecurity and highlight the roles that require Linux skills