LESSON: SIEM and SOAR

Before you Begin

This is the third week of this course. Instructors should be keeping pace with the lesson timings below. Instructors may want to spin up the first lab of the module to get it ready and stable before doing it live when the lab slide comes up.

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. 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 discuss the essential role of alerts in cybersecurity, serving as early warning systems to detect anomalies and potential threats based on predefined criteria. The process of alert generation, managed by SOC teams, and concepts like aggregation and correlation for enhanced attack detection will be explored. Real-time anomaly detection, dashboard significance for visual insights, and the integral role of SOAR, particularly the versatile Cortex XSOAR platform from Palo Alto, will be highlighted. The benefits of SOAR in security incident response, efficient case management, and the

triage and identification process will be emphasized. The lesson will conclude with an introduction to playbooks—sequences of actions that automate cybersecurity tasks—with a focus on creating them in Cortex XSOAR for streamlined incident response.

Objectives

- Define alerts in the context of cybersecurity.
- Identify the different alert types.
- Describe the alert flow.
- Differentiate between aggregation and correlation alerts.
- Recognize the importance of anomaly detection for early threat identification.
- Illustrate real-time anomaly detection.
- Explain what dashboards are.
- Analyze an event dashboard.
- Explain what SOAR is and how it works.
- Describe Cortex XSOAR's features.
- Identify the benefits of SOAR vs SIEM.
- Recognize SOAR's role in incident case management, triage, and identification.
- Define playbooks and recognize their significance in SOAR automation.
- Describe the main features of Cortex XSOAR playbooks.
- Explain how to create a playbook in Cortex XSOAR.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
< 2 min	**Lesson Opener:** SIEM and SOAR	● Introduce learners to the importance of mail security in cybersecurity.
< 5 min	**Real World Scenario:** SIEM and SOAR	● 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.
25 min	**Cyber Uncovered:** SIEM Alerts	● Explain to the students that while they learned how SIEM gathers information from applications and operating systems in the previous lesson, this module looks at how SIEM processes the collected information. ● Explain the concept of alerts as concise early warning messages in cybersecurity that detect anomalies, threats, or attacks based on predefined criteria. ● Highlight the importance of alerts in facilitating swift incident response and their transmission through various channels like email, SNMP, or directly into SIEM.

		● Explore various alert types, including those signaling internal/external cyberattacks, compromised user accounts or workstations, abuse of privileges, and fraud. ● Emphasize the critical role alerts play in identifying and responding to potential threats, preventing security breaches, and promptly addressing fraudulent activities. ● Break down the alert flow process, starting with log inspection to identify potentially malicious activity in system logs. ● Cover rule definition, rule testing to ensure alignment with attack patterns, fine-tuning to minimize false positives, and the final step of deploying optimized rules in the production environment. ● Introduce aggregation, explaining its role in consolidating logs with identical content within predefined fields and specific time frames. ● Discuss correlation, highlighting how alerts from different events are combined to identify similar suspicious behavior across system components or products. ● 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. ● Discuss the 3 C's of what a SIEM provides – Collection, Consolidation, Correlation.
30 min	**Lab:** Creating Alerts	● 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		
25 min	**Cyber Uncovered:** SIEM Trends and Dashboards	● Provide an overview of anomalies as unusual activities or patterns deviating from the norm, emphasizing their critical role in detecting potential security threats in cybersecurity. ● Explain how SIEM systems play a crucial role in identifying anomalies by monitoring network traffic, user behavior, and system logs. ● Highlight how SIEM enables security teams to respond quickly and mitigate potential cyberattacks. ● Break down the anomaly detection process, emphasizing the need for a deep dive into an organization's digital environment to scrutinize data for deviations from norms. ● Discuss the importance of studying timelines to understand how anomalies evolve for proactive threat mitigation. ● Provide a practical example of real-time anomaly detection using a query to display scanned logs of a website. ● Explain the components of the query, including the host, source, sampled time span, searched parameter, statistics filter, and condition.

		● Introduce dashboards as interactive tools that visually display key data and metrics, simplifying complex information for better understanding. ● Emphasize the role of dashboards in real-time security monitoring, analysis, and reporting within the context of SIEM. ● Detail the workflow of a SIEM dashboard, illustrating how it offers a powerful interface for cybersecurity professionals. ● Explain how event dashboards are valuable tools for visualizing and understanding data, enabling prompt identification and response to security incidents or anomalies. ● Present a specific example of a graph line dashboard covering a single day to illustrate how dashboards can provide insights into events and trends in real time. ● 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.
30 min	**Lab:** Dashboards	● 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 (wait for ~75% respondent rate then close the poll)		
5 min Break		
25 min	**Cyber Uncovered:** SOAR Introduction	● Start with an introduction to SOAR, defining it as a security orchestration, automation, and response framework designed to minimize human intervention during incident response. ● Explain that SOAR is not limited to SIEM data and highlight its integration with various security tools to automate incident response functions. ● Detail how SOAR acts as a structured data repository, receiving events from multiple sources similar to SIEM. ● Emphasize its strength in automating actions in response to specific events, streamlining incident response for more efficient threat mitigation and asset protection. ● Differentiate between SIEM and SOAR, noting that while SIEM provides data and alerts, SOAR takes action based on these alerts to streamline the response process. ● Stress that SOAR complements SIEM, forming a comprehensive approach to an organization's security strategy. ● Introduce Cortex XSOAR as a robust SOAR platform developed by Palo Alto, formerly known as Demisto. ● Highlight its pre-built and customizable automation capabilities, emphasizing its versatility through seamless integration with various technologies via API integration. ● Discuss the benefits of SOAR, focusing on its role in security incident response and the automation of repetitive security tasks.

		● Emphasize how SOAR accelerates incident handling and reduces the workload on cybersecurity professionals. ● Explain that SOAR solutions prevail in effective incident case management, autonomously initiating and concluding cases without human intervention. ● Stress the interoperability of SOAR platforms with other case management systems and the use of ticketing methods for streamlined case tracking and resolution. ● Describe the vital roles of triage and identification in cybersecurity for discerning and prioritizing alerts. ● Highlight how SOAR enhances this process by providing an additional triage layer beyond what the SIEM platform performs, aiding in determining critical alerts and bolstering incident response capabilities. ● 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 Break	
25 min	**Cyber Uncovered:** SOAR Automation	● Begin by introducing the central feature of SOAR, emphasizing its powerful automation capabilities in orchestrating and streamlining incident response processes. ● Explain how SOAR automates responses to detected threats, reducing the need for manual intervention while making security incident responses more manageable, faster, and efficient. ● Highlight how the automation feature sets SOAR apart in the cybersecurity landscape, providing a sophisticated and coordinated defense mechanism against cyberthreats. ● Define playbooks as sequences of predefined actions strategically designed to minimize the need for human intervention in repetitive cybersecurity tasks. ● Emphasize the flexibility of playbooks, allowing organizations to create them for autonomous operation or with human involvement at critical decision-making points. ● Discuss how playbooks can be tailored to various scenarios, incorporating conditions that guide their execution, making them valuable for incident response and security automation. ● Introduce the Palo Alto Cortex XSOAR playbooks as robust tools that seamlessly manage the entire incident lifecycle, simplifying complex cybersecurity processes. ● Highlight the user-friendly design of Cortex XSOAR playbooks, which makes them accessible to analysts of all levels (including junior analysts) and facilitates efficient incident response. ● Discuss the flexibility offered by Cortex XSOAR playbooks in assigning tasks with deadlines, contributing to organized and timely incident management. ● Provide a step-by-step guide for creating playbooks in Cortex XSOAR, including accessing playbooks, initiating playbook

		creation, naming and setting up, defining variables, designing workflow, testing and validation, and deployment and monitoring. ● 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.
10 min	**Lesson Closure**	● For this 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. The take-aways discussion should include key concepts such as alerts in cybersecurity, SOAR in incident response and utilizing playbooks. Students should review this information prior to moving to the next module. ● Recommend that the students read-ahead and come prepared for the next lesson. ● Q&A
	Additional Time Filler (if needed)	● Kahoot ● Discuss interview prep and questioning ● Use breakout rooms for additional lab practice ● Continue Real World Scenario Conversation