LESSON: SIEM Introduction

Primer

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

- Checking with the student to see if they have any questions or need further clarification from any subject from the last class “Mail Security” and self study module.
- 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.
- Instructors should manage breaks based on need, considering both timing and duration. You may take a break if you feel the students need it or if a particularly challenging topic has just been covered.

Summary

In this lesson, learners will discuss key cybersecurity threat terminology, including threats, vulnerabilities, risks, and assets. They will delve into asset-centric security considerations, focusing on

continuous monitoring of hardware, software, data, and communications. Students will gain an understanding of various security components and tools, such as network access control, network behavior analysis, firewall, identity management, web application firewall, VPN, intrusion detection and prevention, endpoint detection and response, mail relay, and endpoint protection security. The lesson will introduce learners to the roles of security operations centers (SOCs) and network operations centers (NOCs) in managing security incidents and network operations. Students will learn about the significance of security information and event management (SIEM) systems, differentiating between SIM, SEM, and SIEM, and the components that make up a comprehensive SIEM solution. They will also understand the SIEM workflow, involving data collection, parsing, evaluation, correlation, and inspection for effective security threat response. Furthermore, the lesson will provide insights into popular SIEM solutions like QRadar, ArcSight, AlienVault, and Splunk, highlighting their unique features for enhanced cybersecurity. Students will explore the components of Splunk, including the search head, indexers, and forwarders, and the installation processes for different operating systems. Finally, they will learn about Splunk plugins, their categories (add-ons and apps), and how these plugins extend and customize Splunk for various cybersecurity, IT operations, and business intelligence needs.

Objectives

- Define cybersecurity threat-related terminology.
- Identify the assets that must be monitored to prevent and identify vulnerabilities and threats.
- Describe the components and tools utilized in organizations' security strategies.
- Differentiate between security operations centers (SOCs) and network operations centers (NOCs).
- Describe SIEM systems and their vital role in cybersecurity.
- Compare and contrast SIM, SEM, and SIEM solutions.
- Explain the components, features, and workflow of SIEM systems.
- Identify popular SIEM solutions.
- Identify the components included in Splunk.
- Explain how to install Splunk on Linux and Windows.
- Describe the different types of Splunk plugins.
- Explain the structure of log data.
- Define log collectors.
- Describe application, OS, and external logs.
- Define, categorize, and illustrate Windows event logs.
- Identify different log-gathering methods.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
5-8 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: ○ Incorporate LinkedIn into their job search strategy. ○ Follow step-by-step instructions on how to build a robust LinkedIn profile utilizing the information they've collected for their technical resume. ● The Career Outcomes module can be found at the end of Week 2 of Designing Your Cybersecurity Infrastructure. ● Students can reach out to their SSM for questions and help if they need it. ● Emphasize on how important is linkedIn for job hunting and networking
5 min	**Lesson Opener:** SIEM Introduction	● Introduce learners to the importance of SIEM in cybersecurity.
5 min	**Real World Scenario:** SIEM Introduction	● 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	**Cyber Uncovered:** Security Measures	● Begin the lesson by explaining that a foundational understanding of cybersecurity and security measures is essential before diving into more complex topics like security information and event management (SIEM). ● Emphasize the importance of having a strong grasp of foundational security for various reasons, including: ○ Holistic Understanding: Explain that SIEM processes alerts from different infrastructures. Without a basic understanding, learners might miss their significance. ○ Contextual Analysis: Stress the need to recognize and understand the context of alerts for effective threat assessment. ○ Efficient Response: Highlight how foundational knowledge helps ensure faster threat mitigation and containment. ○ Optimizing Configuration: Explain that proper SIEM setup requires knowledge of underlying security measures. ○ Knowledge Integration: Discuss the interconnected nature of cybersecurity aspects and how understanding the basics ensures a cohesive approach. ○ Avoiding Misinterpretations: Mention the risk of misreading SIEM data without foundational knowledge, leading to overlooked threats or false alarms. ● Define key cybersecurity threat terminology, including threats, vulnerabilities, risks, and assets. Ensure learners have a clear understanding of these fundamental concepts. ● Explain the concept of continuous monitoring for proactive identification and to address potential vulnerabilities and threats. ● Discuss the importance of deploying a multifaceted security strategy to safeguard valuable assets. Describe various security components and tools, including network access control, network

		behavior analysis, firewall, identity management, web application firewall (WAF), virtual private network (VPN), intrusion detection and prevention (IDS/IPS), endpoint detection and response (EDR), mail relay, and endpoint protection security. ● Present the roles of security operations centers (SOCs) and network operations centers (NOCs) in protecting organizational assets. Explore the functions of both teams and highlight the interplay between cybersecurity and network reliability. ● 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.
20 min	**Cyber Uncovered:** Introduction to SIEM	● Start the lesson by introducing SIEM (Security Information and Event Management) and its vital role in cybersecurity. Explain that SIEM is used to collect logs, create alerts, and analyze data. ● Discuss the key features and differences among SIM, SEM, and SIEM. Use the provided comparison table to help learners understand the distinctions and choose the right solution for their cybersecurity needs. ● Explore the essential components and features of SIEM systems, including the database, correlation engine, collectors, management center, application programming interface (API), filters, rules, active lists, reports, and trends. ● Break down the SIEM workflow into five key stages: Collection, parsing, evaluation, correlation, and inspection. Use icons or visual aids to help learners understand each step. ● Introduce four popular SIEM solutions, namely QRadar, ArcSight, AlienVault, and Splunk. Highlight their unique features and capabilities using icons or visual representations. ● 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	**Pulse Check**	● After the poll is concluded, spend a few minutes asking why students have selected their zones. Encourage them to share with each other.
10-15 min	**Break**	● Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.
20 min	**Cyber Uncovered:** Splunk Installation	● Start by introducing Splunk as a powerful software platform used for searching, monitoring, and analyzing large volumes of machine-generated data. ● Explain its importance in various domains, including IT operations, security monitoring, and business analytics. ● Explore the key components of Splunk, which include the search head (user interface for data search and access), indexers (core

		components for data ingestion and indexing), and forwarders (collectors for data forwarding). ● Walk through the Splunk installation process on Linux, emphasizing compatibility with various operating systems. Provide an example installation command and explain the importance of starting the Splunk daemon for data handling and analysis. ● Explain that the installation process on Windows closely resembles that on Linux for a consistent user experience. Mention that administrators should provide system credentials for proper configuration and permissions. ● Emphasize the importance of installing Splunk forwarders on all platforms, including Linux, Windows, and macOS, to ensure comprehensive data collection and forwarding. ● Discuss Splunk plugins, categorizing them into add-ons and apps. Explain how add-ons enhance specific functionalities like data collection and parsing, while apps provide comprehensive solutions with dashboards, reports, and visualizations. ● 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.
20-25 min	**Lab:** Splunk Deployment	● 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.
10-15 min	**Break**	● Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.
20 min	**Cyber Uncovered:** Log Collection and Types	● Start by explaining the fundamental importance of log data in cybersecurity and network monitoring. Describe how log data provides valuable insights into network activity, user actions, and system events. ● Discuss the key components of log data, including date/time timestamps, destination hostname, process ID, action, login user, source IP, source port, and protocol. ● Explain the significance of each component in understanding log entries. ● Introduce log collectors as vital components in SIEM environments. Explain their role in gathering real-time log data and securely transmitting it for analysis. ● Mention the specific ports used for secure transmission and the importance of log normalization and parsing. ● Explain the placement of log collectors in network architecture. ● Describe how they operate between less secure DMZ segments and more secure LAN areas to ensure comprehensive and secure log management.

		● Provide examples of log sources in IT environments, including application logs, OS logs, and external logs. ● Explain how integrating these logs into centralized log management systems like SIEMs enhances threat detection capabilities. ● Dive into Windows event logs, classifying system events into distinct categories with assigned severity types. ● Discuss event categories, categorized information, severity identification, and how security events offer insights into authentication, access control, and policy enforcement. ● Explore common security event IDs found in Windows event logs, such as 4624 (Successful User Login), 4625 (Failed User Login Attempt), 4672 (Special Privileges Assignment), 4700 (Scheduled Task Enablement), 1116 (Windows Defender Malware Detection Event), and 5031 (Firewall Service Event). ● Explain their significance in security monitoring. ● Describe different types of event log classifications, including information logs, warning logs, error logs, success audit logs, and failure audit logs. ● Explain how each log type provides insights into system events and security issues. ● Conclude by discussing the importance of log gathering in detailed system monitoring and threat detection. ● Highlight the role of tools like Splunk and SIEM systems in streamlining this process. ● Explain key methods for comprehensive data capture, including syslog, direct file recording, and database retrievals. ● 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:** Search Events	● 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. ● Explain to the students how they can leverage AI in cybersecurity.
10-15 min	**Break**	● Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break.
2-3 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 Review Discussion Board Slides and how it impacts students' final grades.

15 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 identify the assets that must be monitored to prevent and identify vulnerabilities and threats. In addition, describe SIEM systems and their vital role in cybersecurity. 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
N/A	**Additional Time Filler (if needed)**	● Kahoot ● Discuss interview prep and questioning ● Use breakout rooms for additional lab practice ● Continue Real World Scenario Conversation