← Back Weekly challenge 4
Graded Quiz • 50 min **Due** Jul 2, 11:59 PM +08

Overview of logs	•	Congratulations! You passed!		
Overview of intrusion detection systems (IDS)		Grade Mook Latest bubmission of 1 to pass 80% or	Go to next item	
Overview of security information event management (SIEM)		received 190% EEK Gyade 1000 IIIEII 8E 4 higher Quiz - 50 min		
Review: Network traffic and logs		Review Learning Objectives		
using IDS and SIEM tools				
Video: Wrap-up 1 min		Which of the following refers to a record of events that occur within an organization's systems?	1/1 point	
Reading: Glossary terms from week 4		Log forw lesubmit your assignment		Try agair
10 min		Occurrences Jul 2, 11:59 PM +08 Attempts 3 every 24 hours		
Quiz: Weekly challenge 4 10 questions		Log sources Logs		
Quiz: Portfolio Activity: Finalize your incident handler's journal		Receive grade	Your grade	View Feedback
5 questions		Correct To Pass 80% or higher	100%	We keep your highest sco
Reading: Portfolio Activity Exemplar: Finalize your incident				
handler's journal	2. [Examine the following log: Dislike Report an issue	1/1 point	
Congratulations on completing		LoginEvent[2021/10/13 10:32:08.958711] auth_session_authenticator.cc:304 Regular		
Course 6!		user login 1		
	١	Which type of log is this?		
	(Network		
	(Authentication		
	(Application		
	(Location		
		⊘ Correct		
	3. [Fill in the blank: A syslog entry contains a header,, and a message.	1/1 point	
	(Object		
	(structured-data		
	(eXtensible Markup Language		
	(Control tag		
		⊘ Correct		
		Consider the following scenario:	1/1 point	
		A security analyst at a midsized company is tasked with installing and configuring a host-based intrusion detection system (HIDS) on a laptop. The security analyst installs the HIDS and wants to test whether it is worki	ng	
	ŗ	properly by simulating malicious activity. The security analyst runs unauthorized programs on the laptop, whic		
		the HIDS successfully detects and alerts on.		
	١	What is the laptop an example of?		
		An agent		
	(An endpoint		
	(A signature		
	(A log forwarder		
		⊘ Correct		
	5 \	Which rule option is used to indicate the number of times a signature is updated?	1/1	
			1/1 point	
		sid		
	(•) rev		
	(tep		
	(msg		
		⊘ Correct		
	٠, ١	Which combalis used to indicate a comment and in imposed in a Covington signature file?		
		Which symbol is used to indicate a comment and is ignored in a Suricata signature file?	1/1 point	
) \$		
		• #		
) : -		
	() >		
		⊘ Correct		
	-	Fill in the blank Surjects used the second forward for account and the second		
		Fill in the blank: Suricata uses the format for event and alert output.	1/1 point	
	`) HTML		
		HTTP		
		EVE JSON		
	(CEF		
		⊘ Correct		
	8. ¹	Which querying language does Splunk use?	1/1 point	
			± / ± polit	
		SIEM Processing Language Search Processing Language		
		Structured Querying Language Structured Querying Language		
		Structured Processing Language Structured Processing Language		
	`			
		⊘ Correct		
	9. \	What is the default method of search in Chronicle?	1/1 point	
		○ Non-normalized		
	Ì	UDM		
		YARA-L		
		Raw log		
	`			
		⊘ Correct		
	10.\	Which step in the SIEM process involves the processing of raw data into a standardized and structured format?	1/1 point	
		Normalize	-	
		Collect		
		O Index		
) Process		
	`	⊘ Correct		

?