Get 2022 Updated Free EC-COUNCIL 312-39 Exam Questions & Answer [Q12-Q32

Get 2022 Updated Free EC-COUNCIL 312-39 Exam Questions and Answer
312-39 Dumps PDF and Test Engine Exam Questions

Career Prospects

Those candidates who achieve the passing score in the certification exam are entitled to earn the CSA certification as well as membership privileges. The certified individuals are in high demand with numerous job openings that they can explore. Without a doubt, this EC-Council certificate is a highly rewarding option that allows the professionals to take up different job roles. Some career paths that they can explore include a Security & Network Administrator, a Network Defense Analyst, a Security & Network Engineer, a Network Security Specialist, a Network Defense Technician, a Network Security Operator, and a Cybersecurity Analyst, among others.

EC-COUNCIL 312-39 Exam Syllabus Topics:

TopicDetailsTopic 1- Able to escalate incidents to appropriate teams for additional assistance- Able to make use of varied, disparate, constantly changing threat informationTopic 2- Gain understating of SOC and IRT collaboration for better incident response- Gain knowledge of the Centralized Log Management (CLM) processTopic 3- Gain hands-on experience in SIEM use case development process- Plan, organize, and perform threat monitoring and analysis in the enterpriseTopic 4- Gain knowledge of integrating threat intelligence into SIEM- Able to recognize attacker tools, tactics, and proceduresTopic 5-

Able to develop threat cases (correlation rules), create reports- Gain a basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities

To achieve the desired success, it is expedient to gain competence in the exam topics. This means that the first place to start your preparation is to go through these domains. The details of the sections covered in the certification test are enumerated below: **Incidents, Logging, and Events: 21%**It requires that the test takers possess the relevant skills in describing local & centralized logging concepts. It also covers their understanding of the fundamentals of incidents, logging, and events. **Understanding Attack Methodology, Cyber Threats, and IoCs: 11%**It covers the students' skills in explaining the terms of cyberattacks and threats. Besides that, you will need to have some understanding of network-level attacks, host-level attacks, network-level attacks, indicators of compromise, as well as application-level attacks, among others. **Security Operations & Management: 5%**It requires that the applicants have a good understanding of the SOC fundamentals and know how to describe the components of SOC, which includes people, processes, as well as technology. The individuals should also understand the process of implementing SOC. **Incident Response: 29%**It focuses on one's knowledge of different incident response process phases. Also, it covers the ways to respond to different network security incidents, application security incidents, email security incidents, insider incidents, and malware incidents. **Incident Detection with SIEM (Security Information & Event Management): 26%**It evaluates your understanding of the fundamental concepts of SIEM, SIEM deployment, and handling alert triaging & analysis concept. It also covers the skills and ability to explain various SIEM solutions as well as various use case examples for application-level, host-level, and network-level incident detection.

NO.12 Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?
* Containment -> Incident Recording -> Incident Triage -> Preparation -> Recovery -> Eradication -> Post-Incident Activities
* Preparation -> Incident Recording -> Incident Triage -> Containment -> Eradication -> Recovery -> Post-Incident Activities
* Incident Triage -> Eradication -> Containment -> Incident Recording -> Preparation -> Recovery -> Post-Incident Activities
* Incident Recording -> Preparation -> Containment -> Incident Triage -> Recovery -> Eradication -> Post-Incident Activities

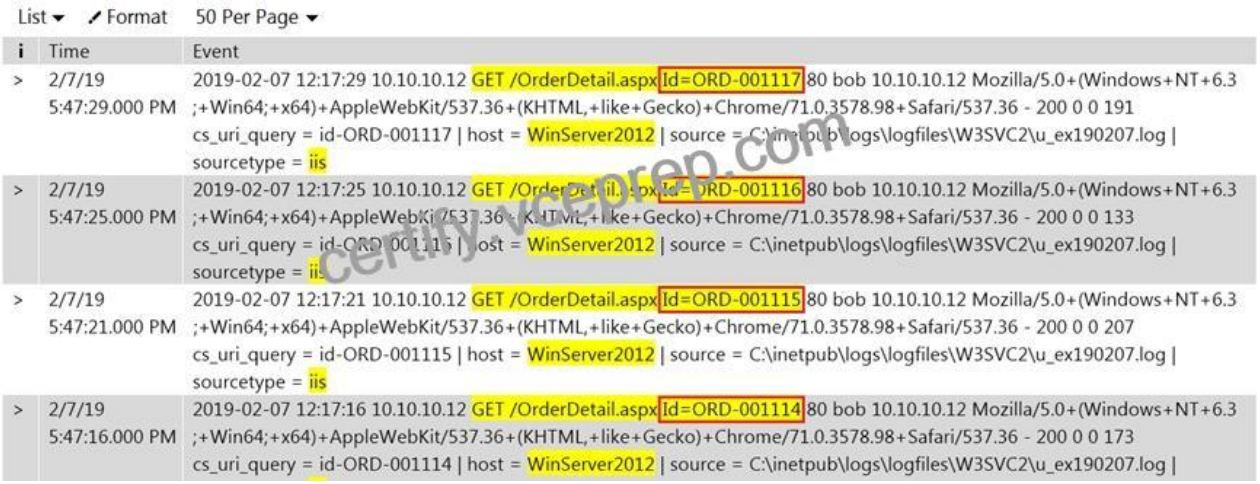
NO.13 What does the HTTP status codes 1XX represents?
* Informational message
* Client error
* Success
* Redirection

NO.14 In which log collection mechanism, the system or application sends log records either on the local disk or over the network.
* rule-based
* pull-based
* push-based
* signature-based

NO.15 The Syslog message severity levels are labelled from level 0 to level 7.

What does level 0 indicate?
* Alert
* Notification
* Emergency
* Debugging

NO.16 Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.


List ▾ Format 50 Per Page ▾

i	Time	Event
>	2/7/19 5:47:29.000 PM	2019-02-07 12:17:29 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001117 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3 ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 191 cs_uri_query = id-ORD-001117 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log | sourcetype = iis
>	2/7/19 5:47:25.000 PM	2019-02-07 12:17:25 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001116 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3 ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 133 cs_uri_query = id-ORD-001116 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log | sourcetype = iis
>	2/7/19 5:47:21.000 PM	2019-02-07 12:17:21 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001115 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3 ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 207 cs_uri_query = id-ORD-001115 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log | sourcetype = iis
>	2/7/19 5:47:16.000 PM	2019-02-07 12:17:16 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001114 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3 ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 173 cs_uri_query = id-ORD-001114 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log |

What does this event log indicate?
* Directory Traversal Attack
* XSS Attack
* SQL Injection Attack
* Parameter Tampering Attack

NO.17 Which of the following command is used to enable logging in iptables?
* $ iptables -B INPUT -j LOG
* $ iptables -A OUTPUT -j LOG
* $ iptables -A INPUT -j LOG
* $ iptables -B OUTPUT -j LOG

NO.18 Which of the following tool is used to recover from web application incident?
* CrowdStrike FalconTM Orchestrator
* Symantec Secure Web Gateway
* Smoothwall SWG
* Proxy Workbench

NO.19 Which of the log storage method arranges event logs in the form of a circular buffer?
* FIFO
* LIFO
* non-wrapping
* wrapping

NO.20 Which of the following attacks causes sudden changes in file extensions or increase in file renames at rapid speed?
* Ransomware Attack
* DoS Attack
* DHCP starvation Attack
* File Injection Attack

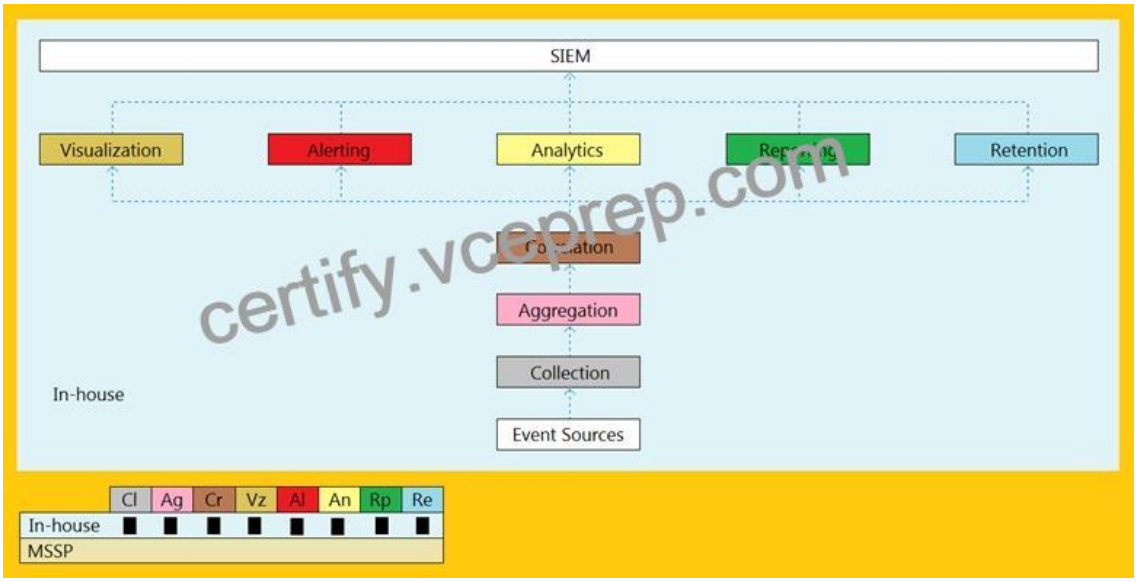
NO.21 Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex

/((%3C)|<)((%69)|i|(% 49))((%6D)|m|(%4D))((%67)|g|(%47))[n]+((%3E)|>)/|.

What does this event log indicate?
* Directory Traversal Attack
* Parameter Tampering Attack
* XSS Attack
* SQL Injection Attack

NO.22 Which of the following Windows Event Id will help you monitors file sharing across the network?
* 7045
* 4625
* 5140
* 4624

NO.23 An organization is implementing and deploying the SIEM with following capabilities.



What kind of SIEM deployment architecture the organization is planning to implement?
* Cloud, MSSP Managed
* Self-hosted, Jointly Managed
* Self-hosted, Self-Managed
* Self-hosted, MSSP Managed

NO.24 What does Windows event ID 4740 indicate?
* A user account was locked out.
* A user account was disabled.
* A user account was enabled.
* A user account was created.

NO.25 Which of the following formula represents the risk?
* Risk = Likelihood * Severity * Asset Value
* Risk = Likelihood * Consequence * Severity
* Risk = Likelihood * Impact * Severity
* Risk = Likelihood * Impact * Asset Value

NO.26 According to the Risk Matrix table, what will be the risk level when the probability of an attack is very low and the impact of that attack is major?
* High
* Extreme
* Low
* Medium

NO.27 Which of the following stage executed after identifying the required event sources?
* Identifying the monitoring Requirements
* Defining Rule for the Use Case
* Implementing and Testing the Use Case
* Validating the event source against monitoring requirement

NO.28 Peter, a SOC analyst with Spade Systems, is monitoring and analyzing the router logs of the company and wanted to check the logs that are generated by access control list numbered 210.

What filter should Peter add to the ‘show logging’ command to get the required output?
* show logging | access 210
* show logging | forward 210
* show logging | include 210
* show logging | route 210

NO.29 Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?
* Netstat Data
* DNS Data
* IIS Data
* DHCP Data

NO.30 Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?
* $ tailf /var/log/sys/kern.log
* $ tailf /var/log/kern.log
* # tailf /var/log/messages
* # tailf /var/log/sys/messages

NO.31 Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?
* Windows Event Log
* Web Server Logs
* Router Logs
* Switch Logs

NO.32 David is a SOC analyst in Karen Tech. One day an attack is initiated by the intruders but David was not able to find any suspicious events.

This type of incident is categorized into?
* True Positive Incidents
* False positive Incidents
* True Negative Incidents
* False Negative Incidents

Verified 312-39 exam dumps Q&As with Correct 102 Questions and Answers:
https://www.vceprep.com/312-39-latest-vce-prep.html]