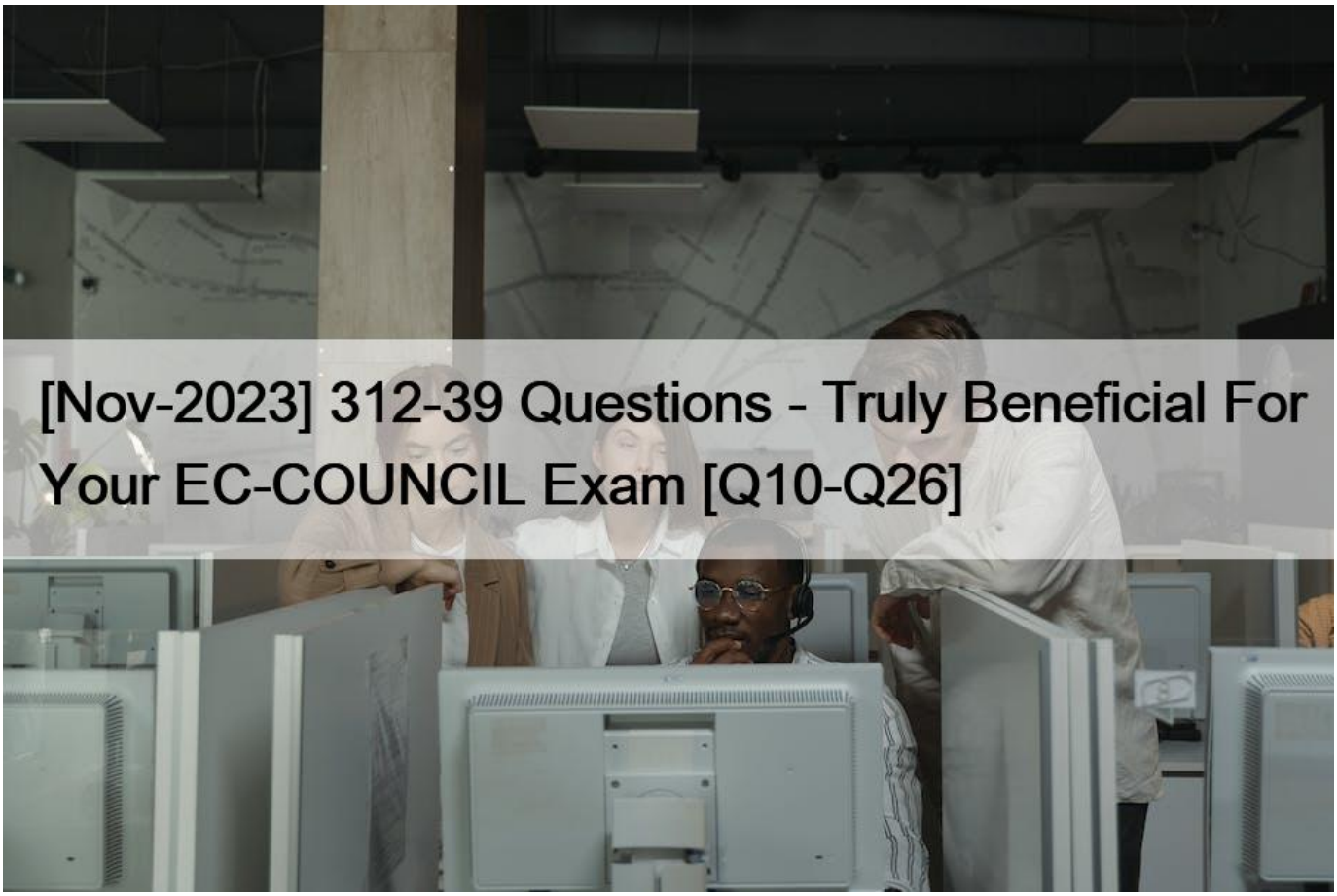
[Nov-2023 312-39 Questions - Truly Beneficial For Your EC-COUNCIL Exam [Q10-Q26



[Nov-2023 312-39 Questions - Truly Beneficial For Your EC-COUNCIL Exam Download EC-COUNCIL 312-39 Sample Questions

The Certified SOC Analyst (CSA) Exam is a certification exam offered by the EC-COUNCIL. 312-39 exam focuses on assessing the skills and knowledge of candidates in detecting, analyzing and responding to cybersecurity threats in a Security Operations Center (SOC) environment. The purpose of 312-39 exam is to validate the qualifications of candidates in providing a strong response to cybersecurity incidents and developing a secure SOC.

NEW QUESTION 10

Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?
* FISMA
* HIPAA
* PCI-DSS

* DARPA

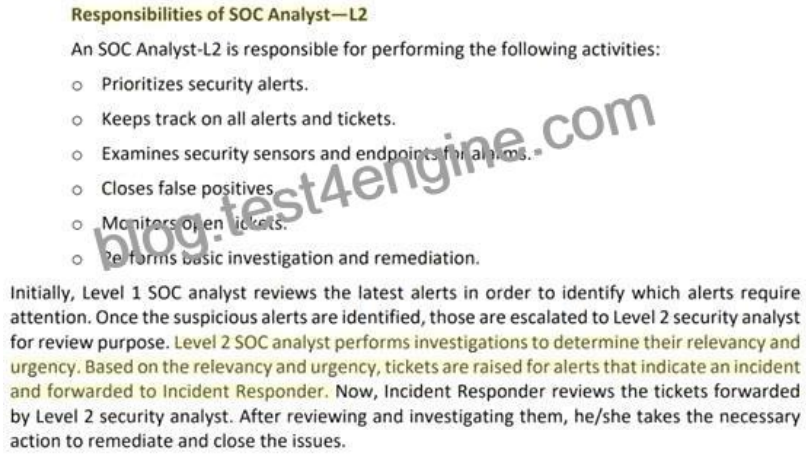
NEW QUESTION 11

Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?
* Rule-based detection
* Heuristic-based detection
* Anomaly-based detection
* Signature-based detection

NEW QUESTION 12

Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for further investigation and confirmation. Charline, after a thorough investigation, confirmed the incident and assigned it with an initial priority.

What would be her next action according to the SOC workflow?
* She should immediately escalate this issue to the management
* She should immediately contact the network administrator to solve the problem
* She should communicate this incident to the media immediately
* She should formally raise a ticket and forward it to the IRT



NEW QUESTION 13

Which of the following is a Threat Intelligence Platform?
* SolarWinds MS
* TC Complete
* Keepnote
* Apility.io

NEW QUESTION 14

John, a SOC analyst, while monitoring and analyzing Apache web server logs, identified an event log matching Regex /(.|(%|%25)2E)(.|(%|%25)2E)(/|(%|%25)2F||(%|%25)5C)/i.

What does this event log indicate?

* XSS Attack
* SQL injection Attack
* Directory Traversal Attack
* Parameter Tampering Attack

NEW QUESTION 15

Which of the following formula is used to calculate the EPS of the organization?
* EPS = average number of correlated events / time in seconds
* EPS = number of normalized events / time in seconds
* EPS = number of security events / time in seconds
* EPS = number of correlated events / time in seconds

NEW QUESTION 16

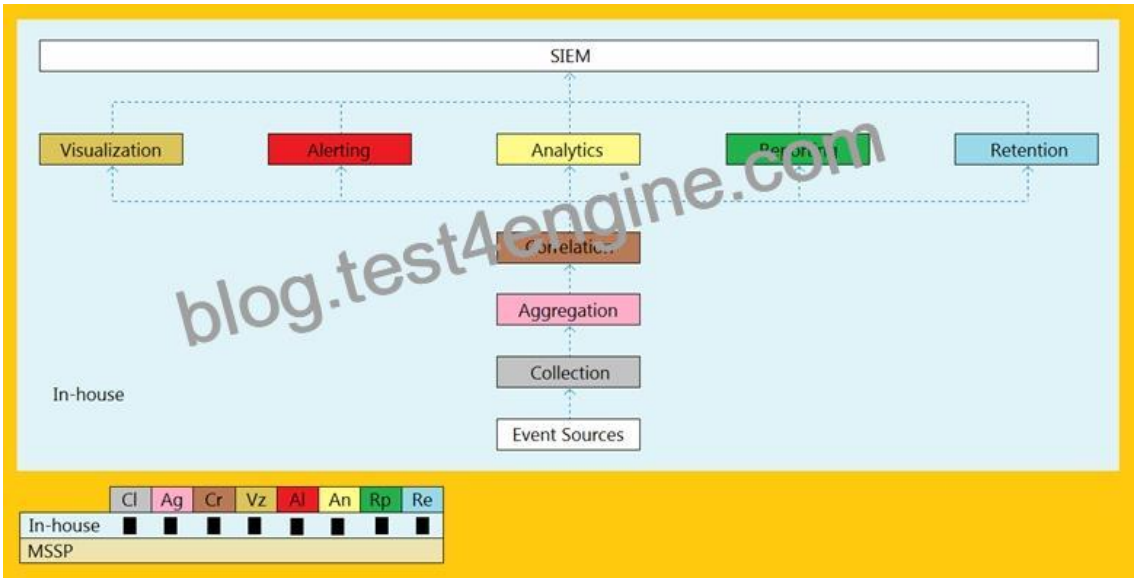
An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted code at the end of the company’s URL as follows:

http://technosoft.com.com/<script>alert(“WARNING: The application has encountered an error”);</script>.

Identify the attack demonstrated in the above scenario.
* Cross-site Scripting Attack
* SQL Injection Attack
* Denial-of-Service Attack
* Session Attack

NEW QUESTION 17

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

NEW QUESTION 18

Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?
* /etc/ossim/reputation
* /etc/ossim/siem/server/reputation/data
* /etc/siem/ossim/server/reputation.data
* /etc/ossim/server/reputation.data

NEW QUESTION 19

Which of the following process refers to the discarding of the packets at the routing level without informing the source that the data did not reach its intended recipient?
* Load Balancing
* Rate Limiting
* Black Hole Filtering
* Drop Requests

NEW QUESTION 20

Which of the following Windows Event Id will help you monitors file sharing across the network?
* 7045
* 4625
* 5140
* 4624

NEW QUESTION 21

Robin, a SOC engineer in a multinational company, is planning to implement a SIEM. He realized that his organization is capable of performing only Correlation, Analytics, Reporting, Retention, Alerting, and Visualization required for the SIEM implementation and has to take collection and aggregation services from a Managed Security Services Provider (MSSP).

What kind of SIEM is Robin planning to implement?
* Self-hosted, Self-Managed
* Self-hosted, MSSP Managed
* Hybrid Model, Jointly Managed
* Cloud, Self-Managed

SIEM Deployment Architecture Options: Cloud, Self-Managed

The cloud, self-managed SIEMs are the kind where only log collection and log aggregation are done in the MSSP, and the remaining methods and techniques like correlation, analytics, reporting, retention, alerting, and visualization of the data are performed inside the organization.

As the data are within the organization, the personalization of the visualization can be done as per the requirement of the staff. The maintenance of the SIEM is done as per the need, and unnecessary updates to the network can be omitted. By implementing the cloud technology in the SIEM, the data are way more secure compared to the storage in the physically accessed hardware storage units which consume a lot of places. These are some of the benefits for the organization by implementing cloud, self-managed SIEM.

Challenges that are faced by the organization if they want to implement this kind of SIEM in their network are that they may not get 24/7 monitoring on the log data. If the organization makes the staff work in shifts, then it will be a fruitful way of implementing a SIEM.

NEW QUESTION 22

A type of threat intelligent that find out the information about the attacker by misleading them is known as

.
* Threat trending Intelligence
* Detection Threat Intelligence
* Operational Intelligence
* Counter Intelligence

NEW QUESTION 23

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

NEW QUESTION 24

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

NEW QUESTION 25

Which of the following attack can be eradicated by converting all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums?
* Broken Access Control Attacks
* Web Services Attacks
* XSS Attacks
* Session Management Attacks

NEW QUESTION 26

Identify the HTTP status codes that represents the server error.
* 2XX
* 4XX
* 1XX
* 5XX

Truly Beneficial For Your EC-COUNCIL Exam: https://www.test4engine.com/312-39_exam-latest-braindumps.html]