Eccouncil 312-39 Practice Questions

Shared by Jacobs on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Sarah, a financial analyst at a multinational corporation, is suspected of leaking sensitive financial data to an unauthorized external party. The SOC team observed anomalous data transfer patterns originating from her account, flagged by the SIEM, indicating potential data exfiltration. The incident response team must contain the incident swiftly to minimize data loss and protect critical assets. As a SOC analyst, which should be prioritized as the initial containment measure?

Options:

A- Access control
B- Change passwords regularly
C- Isolate the storage
D- Data-Centric Audit and Protection (DCAP)

Answer:

A

Explanation:

Initial containment for suspected data exfiltration by a specific user account should prioritize immediately restricting that account's ability to access and transfer data. ''Access control'' is the broad containment category that includes disabling the account, suspending sessions, revoking tokens, removing access to sensitive shares, and applying conditional access blocks. This is the fastest way to stop ongoing data loss while preserving evidence for investigation. ''Change passwords regularly'' is a general security hygiene practice, not an initial incident containment action, and it may not stop exfiltration quickly if active sessions or tokens remain valid. ''Isolate the storage'' can be appropriate if a particular repository is being actively exfiltrated, but it can be disruptive to business operations and may not address the actor's continued access paths across other systems. DCAP is a programmatic capability for monitoring and controlling data access over time; it is valuable, but it is not the immediate first step when the SOC must rapidly stop suspected exfiltration. From a SOC playbook view, the initial action is to reduce attacker/insider access immediately (account restriction), then scope what data was accessed, preserve logs, and coordinate with HR/legal for insider procedures.

Question 2

Question Type: MultipleChoice

Which option best Windows features is used to enable Security Auditing in Windows?

Options:

A- Bitlocker
B- Windows Firewall
C- Local Group Policy Editor
D- Windows Defender

Answer:

C

Question 3

Question Type: MultipleChoice

Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.

Options:

A- Dictionary Attack
B- Rainbow Table Attack
C- Bruteforce Attack
D- Syllable Attack

Answer:

A

Question 4

Question Type: MultipleChoice

Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?

Options:

A- /etc/ossim/reputation
B- /etc/ossim/siem/server/reputation/data
C- /etc/siem/ossim/server/reputation.data
D- /etc/ossim/server/reputation.data

Answer:

D

Question 5

Question Type: MultipleChoice

The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk.

What kind of threat intelligence described above?

Options:

A- Tactical Threat Intelligence
B- Strategic Threat Intelligence
C- Functional Threat Intelligence
D- Operational Threat Intelligence

Answer:

B

Question 6

Question Type: MultipleChoice

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?

Options:

A- show logging | access 210
B- show logging | forward 210
C- show logging | include 210
D- show logging | route 210

Answer:

C

Question 7

Question Type: MultipleChoice

Which of the following tool can be used to filter web requests associated with the SQL Injection attack?

Options:

A- Nmap
B- UrlScan
C- ZAP proxy
D- Hydra

Answer:

B

Question 8

Question Type: MultipleChoice

Which encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal?

Options:

A- Unicode Encoding
B- UTF Encoding
C- Base64 Encoding

D- URL Encoding

Answer:

D

Question 9

Question Type: MultipleChoice

What does [-n] in the following checkpoint firewall log syntax represents?

fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification_scheme_file] [-m unification_mode(initial|semi|raw)] [-a] [-k (alert name|all)] [-g] [logfile]

Options:

A- Speed up the process by not performing IP addresses DNS resolution in the Log files
B- Display both the date and the time for each log record
C- Display account log records only
D- Display detailed log chains (all the log segments a log record consists of)

Answer:

A

Question 10

Question Type: MultipleChoice

Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?

Options:

A- Containment --> Incident Recording --> Incident Triage --> Preparation --> Recovery --> Eradication --> Post-Incident Activities
B- Preparation --> Incident Recording --> Incident Triage --> Containment --> Eradication --> Recovery --> Post-Incident Activities
C- Incident Triage --> Eradication --> Containment --> Incident Recording --> Preparation -->

Recovery --> Post-Incident Activities
D- Incident Recording --> Preparation --> Containment --> Incident Triage --> Recovery --> Eradication --> Post-Incident Activities

Answer:

B

Explanation:

The correct flow of stages in an Incident Handling and Response (IH&R) process typically follows a structured approach that begins withPreparation, which is crucial for an effective response to incidents. This is followed byIncident Recording, where details of the incident are documented.Incident Triageis the next stage, where incidents are prioritized based on their impact.Containmentstrategies are then employed to limit the spread of the incident.Eradicationinvolves removing the threat from the affected systems.Recoveryis the process of restoring systems to normal operation. Finally,Post-Incident Activitiesinvolve learning from the incident and improving future response efforts.

References:The stages of the IH&R process are outlined in various EC-Council resources, including the EC-Council's Certified Incident Handler (E|CIH) program and related training materials, which emphasize the importance of a structured and methodical approach to incident handling and response123.

Question 11

Question Type: MultipleChoice

In which log collection mechanism, the system or application sends log records either on the local disk or over the network.

Options:

A- rule-based
B- pull-based
C- push-based
D- signature-based

Answer:

C

Explanation:

In a push-based log collection mechanism, the system or application actively sends (or ''pushes'') log records to a designated storage location, which can be either on the local disk or over a network to a remote server. This is in contrast to a pull-based mechanism, where the log records are retrieved (or ''pulled'') by the management server from the devices.

The push-based mechanism is often used for real-time monitoring and alerting because it allows for immediate transfer of log data as events occur. This method ensures that log records are consistently and reliably sent to a central repository without the need for a third-party service to request or retrieve them.

References:The EC-Council's Certified SOC Analyst (CSA) program includes the study of various log collection mechanisms as part of its curriculum. The CSA study materials provide detailed explanations of push-based and other log collection mechanisms, emphasizing their role in effective security operations center (SOC) monitoring and incident response. For further information, please refer to the official EC-Council CSA study guides and related course materials.

Question 12

Question Type: MultipleChoice

Which option best is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?

Options:

A- FISMA
B- HIPAA
C- PCI-DSS
D- DARPA

Answer:

C

Explanation:

PCI-DSS stands for Payment Card Industry Data Security Standard. It is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. The PCI-DSS is a widely recognized set of

guidelines that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

References:The EC-Council's Certified SOC Analyst (CSA) course materials and study guides include information on various security standards, including PCI-DSS, which is specifically focused on the protection of account data.The course would cover the importance of adhering to such standards to ensure the security and integrity of sensitive payment card information1234.