# Braindumps 312-39 Downloads & New 312-39 Exam Pattern


2026 Latest Exam4Labs 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1fea9pj8CjEyxtt_MUFsbnau_51X98f5z

Three versions of 312-39 exam dumps are provided by us. Each version has its own advantages. 312-39 PDF version is printable and you can take it with you. 312-39 Soft test engine can stimulate the real exam environment, so that it can release your nerves while facing the real exam. 312-39 Online Test engine can be used in any web browsers, and it can also record your performance and practicing history. You can continue your practice next time.

One of the key benefits of earning the CSA certification is that it helps professionals to stand out in a crowded job market. Certified SOC Analyst (CSA) certification is globally recognized and is highly valued by employers in the field of cybersecurity. It is also a great way to demonstrate to potential employers that you are committed to your professional development and are willing to invest in your career.

## 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.

- **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.

- **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.



## Top Braindumps 312-39 Downloads | Pass-Sure New 312-39 Exam Pattern: Certified SOC Analyst (CSA) 100% Pass

Most of the candidates remain confused about the format of the actual 312-39 exam and the nature of questions therein. So our 312-39 exam questions can perfectly provide them with the newest information about the exam not only on the content but also on the format. And to help them adjust to the real exam, we also developed the Software verson of the 312-39 learning prep which can simulate the real exam.

EC-COUNCIL 312-39 Certified SOC Analyst (CSA) certification exam is a crucial step for IT and security professionals who aim to build a career in security operations centers (SOC). Certified SOC Analyst (CSA) certification is designed to validate the candidate's knowledge and skills related to SOC operations, including threat detection, response, and mitigation. 312-39 Exam focuses on a wide range of topics, including security operations, incident management, threat intelligence, and risk management.

## EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q114-Q119):

**NEW QUESTION # 114**
Which of the following Windows features is used to enable Security Auditing in Windows?

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

**Answer: A**

Explanation:
To enable Security Auditing in Windows, the Local Group Policy Editor is used. This feature allows administrators to configure security policies and audit settings on a local computer. Here's how you can enable Security Auditing using the Local Group Policy Editor:
* Press Win + R, type gpedit.msc, and press Enter to open the Local Group Policy Editor.
* Navigate to Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy.
* Here, you will find a list of audit policies that you can configure for both success and failure events.
* By enabling these policies, you can specify which security-related events you want to audit, such as account logon events, object access, policy change, privilege use, and more.
References: The process described above is aligned with the best practices and guidelines provided by Microsoft and other authoritative sources on Windows security auditing, such as:
* Microsoft's official documentation on Security Auditing1.
* Guides on how to enable Security Auditing in Active Directory environments2.
* Articles detailing the essentials of Windows event log security auditing3. These references are part of the learning resources for the EC-Council SOC Analyst course and provide comprehensive information on the subject.

**NEW QUESTION # 115**
Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for furtherinvestigation 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?

- A. She should communicate this incident to the media immediately
- B. She should immediately escalate this issue to the management

- C. She should formally raise a ticket and forward it to the IRT
- D. She should immediately contact the network administrator to solve the problem

**Answer: C**

Explanation:
Once an L2 SOCAnalyst like Charline confirms an incident, the SOC workflow dictates that the incident must be formally documented. This involves raising a ticket in the incident management system. The ticket should include all relevant details from the investigation, such as the nature of the incident, the affected systems, and the initial priority assigned. After raising the ticket, the L2 Analyst should forward it to the Incident Response Team (IRT). The IRT will then take over the incident to conduct a deeper analysis, perform containment measures, eradicate the threat, and recover systems to normal operation.
References:
Certified SOC Analyst Training | CSA Certification - EC-Council1
Managing the SOC and Responding to Incidents Effectively - EC-Council2
Crafting an Effective Incident Report: A Guide for SOC Analysts3
Certified SOC Analyst - CERT - EC-Council4

**NEW QUESTION # 116**
Jason, a SOC Analyst with Maximus Tech, was investigating Cisco ASA Firewall logs and came across the following log entry:
May 06 2018 21:27:27 asa 1: %ASA -5 - 11008: User 'enable_15' executed the 'configure term' command What does the security level in the above log indicates?

- A. Normal but significant message
- B. Warning condition message
- C. Critical condition message
- D. Informational message

**Answer: A**

Explanation:

**NEW QUESTION # 117**
In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

- A. Evidence Handling
- B. Eradication
- C. SystemsRecovery
- D. Evidence Gathering

**Answer: B**

Explanation:
The eradication stage is where the root cause of the incident is determined from the forensic results. This stage involves not only removing the threat from the affected systems but also identifying and fixing the vulnerabilities that were exploited. It's crucial to understand how the incident occurred to prevent future occurrences. After the containment stage, where the immediate threat is isolated, eradication ensures that the threat is completely removed and that the root cause is addressed.
References: The EC-Council's Certified Incident Handler (E|CIH) program outlines the stages of incident handling and response, which include preparation, identification, containment, eradication, recovery, and lessons learned. Theeradication stage specifically deals with eliminating the threat and addressing the root cause based on forensic analysis. This information is covered in the E|CIH program and can be found in the official EC-Council learning resources1.
Reference: https://www.eccouncil.org/wp-content/uploads/2019/02/ECIH-V2-Brochure.pdf

**NEW QUESTION # 118**
A multinational financial institution notices unusual network activity during a routine security audit. The SOC detects multiple failed login attempts, followed by a successful access attempt using an administrator's credentials from an unrecognized IP address. Shortly after, sensitive customer records are accessed without authorization. The company suspects a breach and calls in the forensic

investigation team. During evidence collection, the forensic team creates a detailed record that tracks every individual who handled the evidence, its storage location, and timestamps of transfers. What is this process called?

- A. Data Imaging
- B. Digital Fingerprinting
- C. Incident Documentation
- D. Chain of Custody

**Answer: D**

Explanation:
Chain of custody is the formal process used to document and preserve evidence integrity by recording who collected the evidence, who accessed it, where it was stored, and when it changed hands. In SOC and forensic operations, chain of custody is essential for maintaining evidentiary reliability, especially in cases with regulatory, legal, or disciplinary implications. It ensures that evidence has not been altered, tampered with, or mishandled, and it supports defensible conclusions about what occurred. Incident documentation is broader and includes timelines, decisions, actions taken, and communications, but it does not specifically track evidence handling transfers. Data imaging is the creation of a forensic copy of storage media (disk image), a separate technical step that may be recorded within chain-of-custody logs. Digital fingerprinting refers to generating hashes or other identifiers to confirm file integrity; again, it is a technique used within evidence handling, but the tracking record of handlers, locations, and transfers is chain of custody. For SOC analysts, correctly maintaining chain of custody is critical when responding to breaches involving sensitive customer records and potential compliance investigations.

**NEW QUESTION # 119**
.....