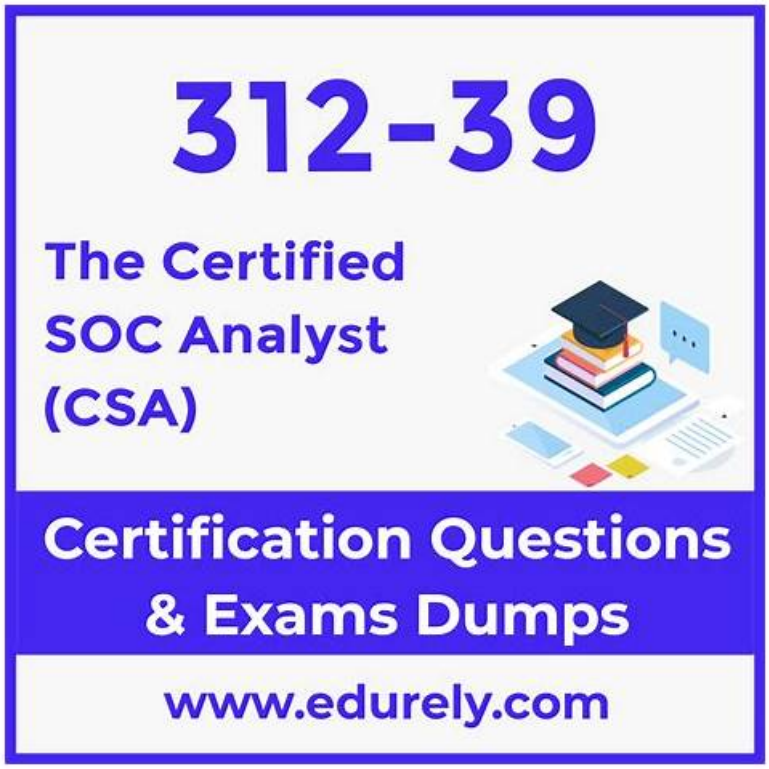
# Free PDF Quiz 312-39 - Certified SOC Analyst (CSA)– Professional Latest Test Materials




What's more, part of that PassLeader 312-39 dumps now are free: https://drive.google.com/open?id=1qZnqNpURngpmBgu9AYiSIwTfgovwhfXD

The result of your exam is directly related with the 312-39 learning materials you choose. So our company is of particular concern to your exam review. Getting the 312-39 certificate of the exam is just a start. Our 312-39 practice materials may bring far-reaching influence for you. Any demands about this kind of exam of you can be satisfied by our 312-39 training quiz. So our 312-39 practice materials are of positive interest to your future. Such a small investment but a huge success, why are you still hesitating?

EC-COUNCIL 312-39: Certified SOC Analyst (CSA) certification is an excellent choice for professionals who want to enhance their knowledge and skills in cybersecurity. Certified SOC Analyst (CSA) certification provides a comprehensive understanding of the security operations center and the role of SOC analysts in protecting an organization's IT infrastructure. The CSA certification is globally recognized and highly valued by employers, making it a valuable investment for professionals who want to advance their careers in cybersecurity.

EC-COUNCIL 312-39 Exam is a vendor-neutral certification, which means that it is not tied to any specific technology or product. Certified SOC Analyst (CSA) certification is recognized globally, and its holders are highly valued by employers. The CSA certification helps candidates to stand out in the competitive job market and improve their chances of getting hired or promoted in their current job.

**>> Latest 312-39 Test Materials <<**

## Latest Braindumps 312-39 Ebook | Reliable 312-39 Exam Dumps

Have you signed up for EC-COUNCIL 312-39 Exam? Will masses of reviewing materials and questions give you a headache? PassLeader can help you to solve this problem. It is absolutely trustworthy website. Only if you choose to use exam dumps PassLeader provides, you can absolutely pass your exam successfully. You spend lots of time on these reviewing materials you don't know whether it is useful to you, rather than experiencing the service PassLeader provides for you. So, hurry to take action.

## EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q118-Q123):

**NEW QUESTION # 118**
Which of the following Windows features is used to enable Security Auditing in Windows?

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

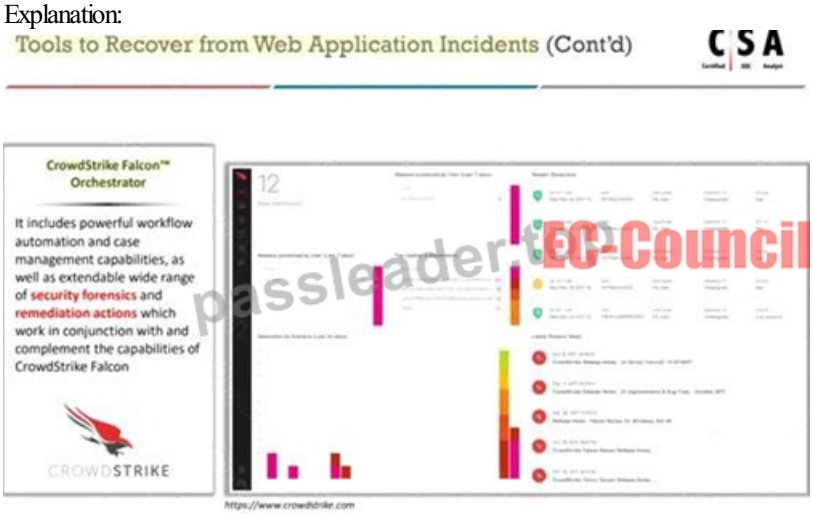
**Answer: B**

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 enableSecurity 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.
Reference: https://resources.infosecinstitute.com/topic/how-to-audit-windows-10-application-logs/

**NEW QUESTION # 119**
Which of the following tool is used to recover from web application incident?

- A. Symantec Secure Web Gateway
- B. CrowdStrike FalconTM Orchestrator
- C. Smoothwall SWG
- D. Proxy Workbench

**Answer: B**

Explanation:



**NEW QUESTION # 120**
Which of the following can help you eliminate the burden of investigating false positives?

- A. Ingesting the context data

- B. Not trusting the security devices
- C. Treating every alert as high level
- D. Keeping default rules

**Answer: A**

Explanation:
Ingesting context data can significantly reduce the burden of investigating false positives in a Security Operations Center (SOC). Context data provides additional information that can help differentiate between true threats and benign anomalies. By analyzing context data, such as user behavior, network traffic patterns, and threat intelligence, SOC analysts can apply a more targeted approach to threat detection. This allows for more accurate alerts, reducing the time and resources spent on investigating false positives.
References: The importance of context in threat detection is highlighted in EC-Council's resources, where it is stated that traditional security tools often generate a lot of noise and false positives, making it difficult for SOCs to distinguish real threats from benign events1. Additionally, leveraging threat intelligence and fine- tuning detection rules are recommended strategies for reducing false positives2. These practices are in line with the EC-Council's Certified SOC Analyst (CSA) course and study guides, which emphasize the need for context-aware security measures in modern SOC operations.

**NEW QUESTION # 121**
David is a SOC analyst responsible for monitoring critical infrastructure. He detects unauthorized applications running on a high-privilege Windows server accessible only by a restricted set of users. The applications were not part of approved deployments, and installations occurred outside business hours. Logs indicate potential system configuration changes around the same timeframe.
Which log should he examine to determine when and how these installations occurred?

- A. Application event log
- B. System event log
- C. Setup event log
- D. Security event log

**Answer: C**

Explanation:
The Setup event log is the most relevant Windows log for installation activity because it captures events related to software installation, servicing, and setup operations. For unauthorized application installs, the SOC needs timing, installer context, and evidence of package deployment or configuration changes driven by setup processes. The Setup log can contain MSI and update-related events, component installation records, and indications of system changes tied to installation workflows. The Security log is crucial for attribution (logons, privilege use, process creation if enabled), but it is not specifically focused on installer actions and may not capture full installation details unless advanced auditing is configured. The System log focuses on OS-level service and driver events (boot, service start/stop, hardware/driver issues) and may show related changes but is not the primary installation record. The Application log captures events written by applications themselves, which is inconsistent for installer tracing. In SOC practice, analysts often combine Setup log evidence with Security log context (who logged on, elevated rights, process lineage) and endpoint telemetry to identify the actor and technique, but the best single log for "when and how installs occurred" among these options is the Setup event log.

**NEW QUESTION # 122**
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 immediately escalate this issue to the management
- B. She should immediately contact the network administrator to solve the problem
- C. She should formally raise a ticket and forward it to the IRT
- D. She should communicate this incident to the media immediately

**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 # 123**
.....

You can use 312-39 guide materials through a variety of electronic devices. At home, you can use the computer and outside you can also use the phone. Now that more people are using mobile phones to learn our 312-39 study guide, you can also choose the one you like. We have three versions of our 312-39 Exam Braindumps: the PDF, the Software and the APP online. And you can free download the demo s to check it out.