

312-39 Reliable Torrent | 312-39 Reliable Test Question

Σημαντικά γεγονότα	
20/4/2026	Σαρνέντης, Βιοκαρπέντ, Γενική Συνέλευση
20/4/2026	Bally's Intralot, Sunrise, Phoenix, Interlife, Ekron, δημοσίευση αποτελεσμάτων χρήσης 2025
20/4/2026	Σαρνέντης, σύνθεση αποτελεσμάτων α' τριμήνου 2026
21/4/2026	Τράπεζα Πειραιώς, Ανδρομέδα, Προοδευτική, Γενική Συνέλευση
21/4/2026	Πλαστικά Θράκης, Λαοκάμ, Qualica, Μουζάκης, EIS, δημοσίευση αποτελεσμάτων χρήσης 2025
21/4/2026	Παπουτσάκης, αποκοπή μερίσματος
22/4/2026	Kip-Kip, Ευρώπη, Real Cons., δημοσίευση αποτελεσμάτων χρήσης 2025
22/4/2026	Αεροδρόμιο Αθηνών, TREK, αποκοπή μερίσματος
22/4/2026	Autohellas, Aegean, Γενική Συνέλευση
23/4/2026	Τράπεζα Ελλάδος, αποκοπή μερίσματος
24/4/2026	S&P, αξιολόγηση ελληνικής οικονομίας
24/4/2026	Autohellas, αποκοπή μερίσματος
27/4/2026	Logismos, ΣΙΔΗΡΑ, Μυλωνάουλη, δημοσίευση αποτελεσμάτων χρήσης 2025
28/4/2026	Aegean, αποκοπή μερίσματος
28/4/2026	Jumbo, Space Hellas, Βιοκαρπέντ, CNL Capital, Αλουριά, δημοσίευση αποτελεσμάτων χρήσης 2025
28/4/2026	Eurobank, BriQ, Γενική Συνέλευση
29/4/2026	EYAO, Τρία Άλφα, Alpha R.E., Ελευνά, Δάσις, Frigoglass, δημοσίευση αποτελεσμάτων χρήσης 2025
29/4/2026	Y/KNOT, έναρξη διαπραγμάτευσης νέων μετοχών
30/4/2026	Aktor, EYΔΑΠ, Galaxy Mezz, Ιατρική Αθηνών, Σελμιπορία, Ελαστρον, Medicon, δημοσίευση αποτελεσμάτων χρήσης 2025
30/4/2026	Τράπεζα Πειραιώς, Mermeren, δημοσίευση αποτελεσμάτων α' τριμήνου 2026
30/4/2026	Εθνική Τράπεζα, MIG, Intertech, Μιλκ Κέδρος, Γενική Συνέλευση
4/5/2026	Allwyn, έναρξη διαπραγμάτευσης νέων μετοχών από επανεξέταση μερίσματος
4/5/2026	Σαρνέντης, αποκοπή δικαιώματος στο μέρισμα
5/5/2026	Optima Bank, Γενική Συνέλευση
6/5/2026	BriQ, αποκοπή δικαιώματος στο μέρισμα
7/5/2026	Eurobank, Titan, Coca Cola, δημοσίευση αποτελεσμάτων α' τριμήνου 2026
8/5/2026	Fitch, αξιολόγηση ελληνικής οικονομίας
8/5/2026	OTE, Εθνική Τράπεζα, δημοσίευση αποτελεσμάτων α' τριμήνου 2026
8/5/2026	Coca Cola, Tiván, Γενική Συνέλευση
11/5/2026	Τράπεζα Κύπρου, Premia, δημοσίευση βασικών αποτελεσμάτων α' τριμήνου 2026
11/5/2026	Eurobank, αποκοπή δικαιώματος στο μέρισμα
11/5/2026	ΕΛΒΑΛΧΑΚΟΡ, Γενική Συνέλευση
12/5/2026	MSCI, αναδιάρθρωση δεκτών
12/5/2026	ΔΕΗ, Austriacard, Optima Bank, δημοσίευση αποτελεσμάτων α' τριμήνου 2026
12/5/2026	ΟΛΘ, Orilina, Allwyn, Γενική Συνέλευση
13/5/2026	Novat, Performance, Γενική Συνέλευση
14/5/2026	HelleniQ Energy, δημοσίευση αποτελεσμάτων α' τριμήνου 2026
14/5/2026	ΟΛΘ, αποκοπή μερίσματος
14/5/2026	Ελλάκτωρ, Γενική Συνέλευση
15/5/2026	Τράπεζα Κύπρου, Γενική Συνέλευση
15/5/2026	Orilina, αποκοπή δικαιώματος στο μέρισμα
15/5/2026	Τράπεζα Κύπρου, Γενική Συνέλευση
18/5/2026	Αεροδρόμιο Αθηνών, δημοσίευση αποτελεσμάτων α' τριμήνου 2026
19/5/2026	Foulris, δημοσίευση αποτελεσμάτων α' τριμήνου 2026
19/5/2026	Πλαστικά Θράκης, Alpha Trust, Γενική Συνέλευση
20/5/2026	Quest, ΕΛΒΑΛΧΑΚΟΡ, δημοσίευση αποτελεσμάτων α' τριμήνου 2026

BONUS!!! Download part of Lead2Passed 312-39 dumps for free: <https://drive.google.com/open?id=1mvyhOrntKzdMCH0HiypWj93UkyILbt8f>

Test your knowledge of the 312-39 exam dumps with Lead2Passed Certified SOC Analyst (CSA) (312-39) practice questions. The software is designed to help with Certified SOC Analyst (CSA) (312-39) exam dumps preparation. Certified SOC Analyst (CSA) (312-39) practice test software can be used on devices that range from mobile devices to desktop computers. We provide the Certified SOC Analyst (CSA) (312-39) exam questions in a variety of formats, including a web-based practice test, desktop practice exam software, and downloadable PDF files.

The Certified SOC Analyst (CSA) certification exam is ideal for professionals who want to enhance their knowledge and skills in the area of cybersecurity. Certified SOC Analyst (CSA) certification exam is designed to provide a comprehensive understanding of the various security threats and vulnerabilities that organizations face today. Professionals who pass the certification exam will be equipped with the necessary skills to identify and respond to security incidents, perform threat analysis, and monitor security systems. Certified SOC Analyst (CSA) certification exam also covers the best practices for managing and responding to security incidents, which is essential for any organization that wants to ensure the security of its network and data.

To prepare for the CSA certification exam, candidates are required to have a solid understanding of cybersecurity concepts and technologies. They should also have experience working in a SOC environment and be familiar with the tools and techniques used to detect and respond to security incidents. EC-Council provides a training program to help candidates prepare for the exam. This training program covers all the topics that are included in the exam and provides hands-on experience in using the tools and techniques used by SOC analysts.

The CSA certification is an intermediate-level certification that is ideal for professionals who are looking to advance their career in the cybersecurity field. It is particularly relevant for those who work in SOC environments, such as security analysts, incident responders, and SOC managers.

>> 312-39 Reliable Torrent <<

Pass Guaranteed Quiz EC-COUNCIL - 312-39 - Fantastic Certified SOC Analyst (CSA) Reliable Torrent

Our 312-39 exam materials have three different versions: the PDF, Software and APP online. All these three types of 312-39 learning quiz win great support around the world and all popular according to their availability of goods, prices and other term you can think of. 312-39 practice materials are of reasonably great position from highly proficient helpers who have been devoted to their quality over ten years to figure your problems out and help you pass the exam easily.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q34-Q39):

NEW QUESTION # 34

Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:
`http://www.terabytes.com/process.php/../../../../etc/passwd`

- A. Form Tampering Attack
- B. SQL Injection Attack
- C. Denial-of-Service Attack
- **D. Directory Traversal Attack**

Answer: D

Explanation:

NEW QUESTION # 35

Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive. Identify the stage in which he is currently in.

- A. Post-Incident Activities
- B. Incident Disclosure
- **C. Incident Triage**
- D. Incident Recording and Assignment

Answer: C

Explanation:

The stage of incident handling that involves incident analysis and validation to determine if the incident is a true incident or a false positive is known as Incident Triage. This stage is critical as it helps in prioritizing incidents based on their severity, impact, and urgency. The process of triage typically includes an initial assessment to confirm the validity of an incident, categorize its type, and determine the appropriate response.

References: The EC-Council's SOC Analyst course outlines the incident handling and response process, which includes the triage stage as a key component¹². This is further supported by the NIST framework, which details the stages of incident response, including detection and analysis, where triage is a fundamental activity¹. The Certified SOC Analyst (CSA) training also emphasizes the importance of incident triage in the overall security operations center (SOC) workflow³.

NEW QUESTION # 36

David Reynolds, a SOC analyst at a healthcare organization, is investigating suspicious login attempts flagged by the SIEM. To mitigate brute-force risk on targeted endpoints, he collaborates with IT to implement an automatic account lockout policy that temporarily disables accounts after multiple failed login attempts.

Within the SOC's eradication strategy, which category of measures does this action align with?

- A. Physical security measures
- B. Network security measures
- C. Host security measures
- **D. Authentication and authorization measures**

Answer: D

Explanation:

Account lockout is an identity control that directly strengthens authentication by limiting repeated password guessing attempts. It sits

within authentication and authorization measures because it governs how accounts can authenticate and how access is granted or denied based on login outcomes. In SOC terms, brute-force attacks target the authentication surface; lockout policies reduce attacker attempts and can prevent successful compromise by forcing a pause or administrative intervention after repeated failures. While the policy may be implemented on hosts or via directory services, its purpose is to control identity access behavior, not network segmentation or physical protections. Host security measures typically refer to endpoint hardening, patching, EDR controls, and local configuration baselines. Network security measures include firewall rules, segmentation, and traffic filtering. Physical security includes facility and device access controls. Because the action is specifically about controlling login attempts and access to accounts, it is best categorized as authentication and authorization. In practice, SOC teams complement lockout policies with MFA, conditional access, password spraying detection, and monitoring for "failures followed by success" patterns to reduce both brute-force success and user disruption.

NEW QUESTION # 37

A leading e-commerce company relies on backend servers for processing customer transactions. You are working with their cybersecurity team as a SOC analyst. One morning, you notice a sharp increase in CPU utilization on one of your backend servers. Your team scans and monitors the server and finds that an unknown process is running, consuming excessive resources. You further perform detailed forensic analysis and identify the presence of an unrecognized scheduled task that triggers a PowerShell script connecting to an unknown IP address. What should you do to confirm whether this is an active attack?

- A. Check file integrity and detect recent unauthorized changes
- B. Review user access logs for unauthorized activity
- C. Analyze the network logs to identify external connections
- D. Analyze the system logs for unauthorized changes

Answer: C

Explanation:

The strongest "must-be-true" confirmation for an active attack in this scenario is evidence of command-and-control (C2) or other suspicious external communication. You already have a scheduled task launching PowerShell and attempting to connect to an unknown IP address, which is a high-signal indicator of malicious automation. The fastest way to validate ongoing activity is to analyze network telemetry (firewall/proxy logs, netflow, EDR network events) to confirm whether outbound connections are occurring, how frequently, and whether data is being transferred. Network logs can reveal destination IP/port, protocols, connection success/failure, volume, and timing correlation with the scheduled task triggers. File integrity checks and system logs are useful for understanding persistence and modifications, but they may lag behind or miss short-lived network beacons. User access logs help attribute activity but do not directly confirm an active external control channel. From a SOC triage and containment perspective, confirming external connections enables immediate actions such as blocking the destination, isolating the host, and scoping for other systems contacting the same IPs/domains. Therefore, network log analysis is the most direct next step to confirm active malicious behavior.

NEW QUESTION # 38

A security team is configuring a newly deployed SIEM system. With limited resources, they must prioritize monitoring scenarios that provide the greatest security benefit. The team understands an effective SIEM relies on well-defined use cases tailored to the organization's environment. Which factor should guide their selection of use cases?

- A. Prioritize use cases that address zero-day attacks
- B. Select use cases based on the availability and quality of data from existing data sources
- C. Implement as many use cases as the SIEM supports to cover all threats
- D. Focus on use cases required to meet industry compliance standards

Answer: B

Explanation:

Use cases should be selected based on the availability and quality of data because detections cannot work without reliable telemetry. In SOC engineering, the first constraint is data: what sources exist, how complete they are, how quickly they arrive, and whether fields are parsable and consistent. Choosing use cases that your environment can actually support produces faster time-to-value, fewer false positives, and fewer blind spots.

Prioritizing "zero-day" use cases is too vague and often unrealistic, because zero-days vary widely and require strong behavioral telemetry and baselines. Implementing as many use cases as possible spreads resources thin and increases noise, creating alert fatigue. Compliance-driven use cases are important, but if the underlying data is missing or poor quality, compliance rules will still fail

operationally and can create a false sense of security. A mature approach is: start with high-value, high-feasibility detections that match available data (identity compromise, suspicious admin actions, endpoint malware, critical network anomalies), then expand as data coverage improves. Therefore, data availability and quality should guide initial use case selection.

NEW QUESTION # 39

.....

After using our 312-39 study materials, you will feel your changes. These changes will increase your confidence in continuing your studies on 312-39 real exam. Believe me, as long as you work hard enough, you can certainly pass the exam in the shortest possible time. The rest of the time, you can use to seize more opportunities. As long as you choose 312-39 simulating exam, we will be responsible to you.

312-39 Reliable Test Question: <https://www.lead2passed.com/EC-COUNCIL/312-39-practice-exam-dumps.html>

- TOP 312-39 Reliable Torrent: Certified SOC Analyst (CSA) - High Pass-Rate EC-COUNCIL 312-39 Reliable Test Question Open { www.testkingpass.com } enter ▷ 312-39 ◁ and obtain a free download 312-39 New Dumps Pdf
- 312-39 New Dumps Pdf 312-39 Test Certification Cost 312-39 Reliable Dumps Sheet Download 312-39 for free by simply entering ➡ www.pdfvce.com website Valid 312-39 Test Simulator
- 312-39 Reliable Torrent | Efficient 312-39: Certified SOC Analyst (CSA) 100% Pass Search on ▷ www.easy4engine.com ◁ for 312-39 to obtain exam materials for free download Test 312-39 Score Report
- Free PDF Quiz EC-COUNCIL - Useful 312-39 Reliable Torrent Enter ▷ www.pdfvce.com ◁ and search for ✓ 312-39 ✓ to download for free Test 312-39 Score Report
- Valid 312-39 Exam Tutorial 312-39 Real Question (M) 312-39 Valid Exam Syllabus Simply search for ✓ 312-39 ✓ for free download on 《 www.practicevce.com 》 Reliable 312-39 Test Prep
- Test 312-39 Score Report 312-39 Exam Overviews Reliable 312-39 Braindumps Free The page for free download of ☀ 312-39 ☀ on ✓ www.pdfvce.com ✓ will open immediately Test 312-39 Questions
- Trustable 312-39 learning materials - 312-39 preparation exam - www.prep4away.com ⇌ Immediately open ⇒ www.prep4away.com ⇐ and search for ▷ 312-39 ◁ to obtain a free download Valid 312-39 Test Simulator
- Topping 312-39 Practice Quiz: Certified SOC Analyst (CSA) Supply You the Most Veracious Exam Brain Dumps - Pdfvce Easily obtain free download of 312-39 by searching on ▷ www.pdfvce.com ◁ 312-39 Latest Test Practice
- Free PDF 2026 EC-COUNCIL 312-39: Certified SOC Analyst (CSA) Reliable Torrent Simply search for 312-39 for free download on (www.practicevce.com) 312-39 Dump Torrent
- 312-39 Reliable Torrent | 100% Pass | Latest Questions Search for ➡ 312-39 and download exam materials for free through [www.pdfvce.com] Reliable 312-39 Test Prep
- Easy to Use and Compatible www.troytecdumps.com EC-COUNCIL 312-39 Exam Questions Formats Search for 312-39 and easily obtain a free download on [www.troytecdumps.com] Reliable 312-39 Test Prep
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, bbs.t-firefly.com, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New 312-39 dumps are available on Google Drive shared by Lead2Passed: <https://drive.google.com/open?id=1mvyhOrntKzdMCH0HiypWj93UkyILbt8f>