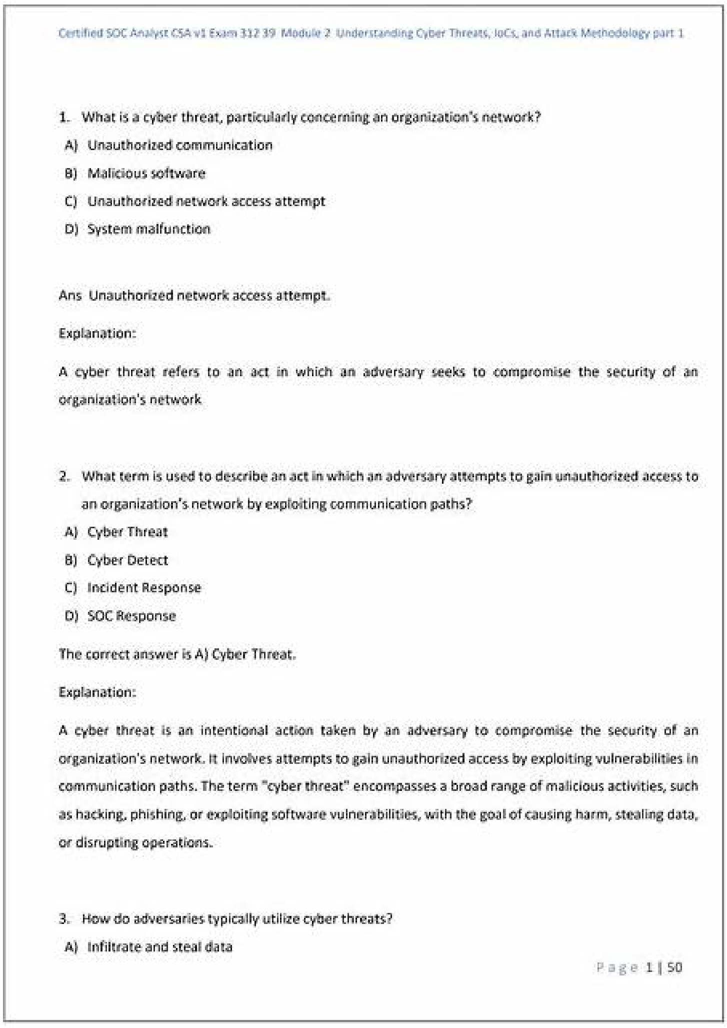
Reliable 312-39 Exam Labs | 312-39 Intereactive Testing Engine



Certified SOC Analyst CSA v1 Exam 312 39 Module 2 Understanding Cyber Threats, IoCs, and Attack Methodology part 1

1. What is a cyber threat, particularly concerning an organization's network?

A) Unauthorized communication

B) Malicious software

C) Unauthorized network access attempt

D) System malfunction

Ans Unauthorized network access attempt.

Explanation:

A cyber threat refers to an act in which an adversary seeks to compromise the security of an organization's network

2. What term is used to describe an act in which an adversary attempts to gain unauthorized access to an organization's network by exploiting communication paths?

A) Cyber Threat

B) Cyber Detect

C) Incident Response

D) SOC Response

The correct answer is A) Cyber Threat.

Explanation:

A cyber threat is an intentional action taken by an adversary to compromise the security of an organization's network. It involves attempts to gain unauthorized access by exploiting vulnerabilities in communication paths. The term "cyber threat" encompasses a broad range of malicious activities, such as hacking, phishing, or exploiting software vulnerabilities, with the goal of causing harm, stealing data, or disrupting operations.

3. How do adversaries typically utilize cyber threats?

A) Infiltrate and steal data

Page 1 | 50

2026 Latest BraindumpQuiz 312-39 PDF Dumps and 312-39 Exam Engine Free Share: https://drive.google.com/open?id=1G-3Ll49I5TkxhehtSaok-3XxkVDZ9_Ss

As we all know, certificates are an essential part of one's resume, which can make your resume more prominent than others, making it easier for you to get the job you want. For example, the social acceptance of 312-39 certification now is higher and higher. If you also want to get this certificate to increase your job opportunities, please take a few minutes to see our 312-39 Study Materials. Carefully written and constantly updated content can make you keep up with the changing direction of the exam, without aimlessly learning and wasting energy.

EC-COUNCIL 312-39 Certification Exam is designed for security professionals, SOC analysts, incident response team members, and network administrators who want to improve their skills and knowledge in security operations. 312-39 exam tests the candidate's ability to detect and respond to security incidents, manage security events, analyze threat intelligence, and perform continuous monitoring of security systems. By passing the CSA certification exam, professionals can demonstrate their expertise in security operations and become eligible for higher-paying job roles in the cybersecurity industry.

>> Reliable 312-39 Exam Labs <<

Free PDF 312-39 - Certified SOC Analyst (CSA) Marvelous Reliable Exam Labs

There is no exaggeration that you can be confident about your coming exam just after studying with our 312-39 preparation materials for 20 to 30 hours. Tens of thousands of our customers have benefited from our exam materials and passed their 312-39 exams with ease. The data showed that our high pass rate is unbelievably 98% to 100%. Without doubt, your success is 100% guaranteed with our 312-39 training guide. You will be quite surprised by the convenience to have an overview just by clicking into the link, and you can experience all kinds of 312-39 versions.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q56-Q61):

NEW QUESTION # 56
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. Incident Triage
- B. Post-Incident Activities
- C. Incident Disclosure
- D. Incident Recording and Assignment

Answer: A

Explanation:

NEW QUESTION # 57
Which of the following directory will contain logs related to printer access?

- A. /var/log/cups/accesslog file
- B. /var/log/cups/access_log file
- C. /var/log/cups/Printer_log file
- D. /var/log/cups/Printeraccess_log file

Answer: B

Explanation:
* Planning and budgeting: This is the initial phase where you determine the scope, objectives, and financial resources available for the lab.
* Physical location and structural design considerations: Selecting a suitable location and designing the lab to meet operational needs and security requirements.
* Work area considerations: Organizing the space efficiently for different tasks such as evidence analysis, storage, and administrative work.
* Human resource considerations: Identifying the roles, responsibilities, and qualifications required for lab personnel.
* Physical security recommendations: Implementing measures to protect sensitive data and physical assets within the lab.
* Forensics lab licensing: Ensuring that the lab and its personnel are compliant with relevant laws, regulations, and industry standards.
References: While I can't refer to specific EC-Council SOC Analyst courses or study guides, these steps are generally accepted as part of the process for setting up a computer forensics lab. For detailed guidance, it's best to consult the official EC-Council resources and materials provided for the SOC Analyst certification.
Graphical user interface Description automatically generated with low confidence

NEW QUESTION # 58
Identify the type of attack, an attacker is attempting on www.example.com website.

- A. Session Attack
- B. Denial-of-Service Attack
- C. SQL Injection Attack
- D. Cross-site Scripting Attack

Answer: D

NEW QUESTION # 59
Which of the following Windows features is used to enable Security Auditing in Windows?

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

Answer: B

NEW QUESTION # 60
John, a threat analyst at GreenTech Solutions, wants to gather information about specific threats against the organization. He started collecting information from various sources, such as humans, social media, chat room, and so on, and created a report that contains malicious activity.
Which of the following types of threat intelligence did he use?

- A. Technical Threat Intelligence
- B. Operational Threat Intelligence
- C. Strategic Threat Intelligence
- D. Tactical Threat Intelligence

Answer: B

Explanation:
Operational threat intelligence involves gathering detailed information about specific threats to an organization. It is often derived from various sources, including human intelligence, social media, chat rooms, and other platforms where data about malicious activities can be collected. This type of intelligence is focused on understanding the specifics of a threat, such as the tactics, techniques, and procedures (TTPs) of threat actors, and is used to inform the organization about imminent or ongoing attacks.
In the scenario described, John, a threat analyst, is collecting information from diverse sources to create a report on malicious activity. This aligns with the practices of operational threat intelligence, which is concerned with the details of particular threats and activities, rather than broader strategic trends or technical indicators.
References:The EC-Council's Certified Threat Intelligence Analyst (C|TIA) program provides comprehensive training on the different types of threat intelligence, including operational threat intelligence. The program covers the methodologies for collecting, analyzing, and disseminating threat intelligence, which are relevant to the activities performed by John in the scenario1.

NEW QUESTION # 61
......

BraindumpQuiz's 312-39 exam training materials evoke great repercussions in the examinees, and has established a very good reputation, which means that choosing BraindumpQuiz 312-39 exam training materials is to choose success. After you buy our 312-39 VCE Dumps, if you fail to pass the certification exam or there are any problems of learning materials, we will give a full refund. What's more, after you buy our 312-39 exam, we will provide one year free renewal service.

312-39 Intereactive Testing Engine: https://www.braindumpquiz.com/312-39-exam-material.html

- 312-39 Exam Vce □ 312-39 Exam Vce □ 312-39 Actual Questions □ Search for ➡ 312-39 □□□ and download exam materials for free through ✔ www.pass4test.com □✔□ □312-39 Exam Vce
- Certification 312-39 Questions □ Certification 312-39 Questions □ 312-39 Exam Study Guide □ Search for （312-39） and download it for free immediately on ✔ www.pdfvce.com □✔□ □312-39 Valid Exam Camp Pdf
- 312-39 Test Passing Score □ 312-39 Prep Guide □ 312-39 Exam Study Guide □ Open □ www.examcollectionpass.com □ enter ⇛ 312-39 ⇚ and obtain a free download □312-39 Exam Vce
- Tips to Crack EC-COUNCIL 312-39 Exam Easily □ Download 【312-39】 for free by simply searching on " www.pdfvce.com " □312-39 Test Quiz
- 312-39 Sample Exam □ 312-39 Exam Quick Prep □ Latest Study 312-39 Questions □ Easily obtain free download of ✔ 312-39 □✔□ by searching on 《www.practicevce.com》 □312-39 Exam Quick Prep
- High Pass-Rate Reliable 312-39 Exam Labs - Leader in Certification Exams Materials - Effective 312-39 Intereactive Testing Engine □ Copy URL ▹ www.pdfvce.com ◃ open and search for ➤ 312-39 □ to download for free □312-39

Exam Quick Prep

- Pass Guaranteed 2026 EC-COUNCIL - Reliable 312-39 Exam Labs ⏲ Copy URL □ www.exam4labs.com □ open and search for 「 312-39 」 to download for free □312-39 Latest Dumps Ebook
- New 312-39 Test Discount 〰 Latest 312-39 Braindumps Free □ 312-39 Sample Exam □ Open ➤ www.pdfvce.com □ enter □ 312-39 □ and obtain a free download □New 312-39 Test Discount
- Salient Features of Desktop 312-39 Certified SOC Analyst (CSA) Practice Tests Software □ Search for □ 312-39 □ and download it for free on □ www.pdfdumps.com □ website □312-39 Pdf Files
- 100% Pass Quiz 2026 EC-COUNCIL 312-39: Trustable Reliable Certified SOC Analyst (CSA) Exam Labs □ Simply search for ☀ 312-39 □☀□ for free download on ▶ www.pdfvce.com ◀ □Latest 312-39 Exam Forum
- 312-39 Latest Dumps Ebook ✳ Certification 312-39 Questions □ 312-39 Test Passing Score □ Search for ▹ 312-39 ◃ and download it for free on “ www.testkingpass.com ” website □312-39 Latest Dumps Ebook
- www.stes.tyc.edu.tw, bbs.t-firefly.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.4001179958.org, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of BraindumpQuiz 312-39 dumps for free: https://drive.google.com/open?id=1G-3Ll49I5TkxhehtSaok-3XxkVDZ9_Ss