EDUSUM

#1 Online Certification Guide

EC-COUNCIL 312-39 STUDY GUIDE PDF

Grab the EC-Council CSA Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

312-39

EC-Council Certified SOC Analyst (CSA)

100 Questions Exam – 70% Cut Score – Duration of 180 minutes

Table of Contents:

Get an Overview of the 312-39 Certification:

Who should take the **312-39 exam**? This is the first question that comes to a candidate's mind when preparing for the CSA certification. The 312-39 certification is suitable for candidates who are keen to earn knowledge on the Advanced and grab their EC-Council Certified SOC Analyst (CSA). When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But 312-39 study guide PDF is here to solve the problem. 312-39 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the EC-Council 312-39 Certification?

There are several reasons why one should grab the 312-39 certification.

- The CSA certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the **EC-Council Certified SOC Analyst (CSA)** is a powerful qualification for a prosperous career.

What is the EC-Council 312-39 CSA Certification Exam Structure?

Exam Name	EC-Council Certified SOC Analyst (CSA)
Exam Code	312-39
Exam Price	$250 (USD)
Duration	180 mins
Number of Questions	100
Passing Score	70%
Books / Training	**Courseware**
Schedule Exam	**Pearson VUE** OR **ECC Exam Center**
Sample Questions	**EC-Council CSA Sample Questions**
Practice Exam	**EC-Council 312-39 Certification Practice Exam**

Enhance Knowledge with 312-39 Sample Questions:

Question: 1

Harley is working as a SOC analyst with Powell Tech. Powell Inc. is using Internet Information Service (IIS) version 7.0 to host their website.

Where will Harley find the web server logs, if he wants to investigate them for any anomalies?

a) SystemDrive%inetpublogsLogFilesW3SVCN
b) SystemDrive%LogFilesinetpublogsW3SVCN
c) %SystemDrive%LogFileslogsW3SVCN
d) SystemDrive% inetpubLogFileslogsW3SVCN

Answer: b

Question: 2

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?

a) Strategic Threat Intelligence
b) Tactical Threat Intelligence
c) Functional Threat Intelligence
d) Operational Threat Intelligence

Answer: a

Question: 3

Bonney's system has been compromised by a gruesome malware. What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?

a) Complaint to police in a formal way regarding the incident
b) Turn off the infected machine
c) Leave it to the network administrators to handle
d) Call the legal department in the organization and inform about the incident

Answer: b

Question: 4

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

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: a

Question: 5

Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

a) Hybrid Attack
b) Bruteforce Attack
c) Rainbow Table Attack
d) Birthday Attack

Answer: d

Question: 6

Emmanuel is working as a SOC analyst in a company named Tobey Tech. The manager of Tobey Tech recently recruited an Incident Response Team (IRT) for his company. In the process of collaboration with the IRT, Emmanuel just escalated an incident to the IRT.

What is the first step that the IRT will do to the incident escalated by Emmanuel?

a) Incident Analysis and Validation
b) Incident Recording
c) Incident Classification
d) Incident Prioritization

Answer: c

Question: 7

Banter is a threat analyst in Christine Group of Industries. As a part of the job, he is currently formatting and structuring the raw data. He is at which stage of the threat intelligence life cycle?

a) Dissemination and Integration
b) Processing and Exploitation
c) Collection
d) Analysis and Production

Answer: b

Question: 8

A type of threat intelligent that find out the information about the attacker by misleading them is known as _____.

a) Threat trending Intelligence
b) Detection Threat Intelligence
c) Operational Intelligence
d) Counter Intelligence

Answer: c

Question: 9

According to the forensics investigation process, what is the next step carried out right after collecting the evidence?

a) Create a Chain of Custody Document
b) Send it to the nearby police station
c) Set a Forensic lab
d) Call Organizational Disciplinary Team

Answer: a

Question: 10

What does HTTPS Status code 403 represents?

a) Unauthorized Error
b) Not Found Error
c) Internal Server Error
d) Forbidden Error

Answer: d

What Study Guide Works Best in acing the EC-Council 312-39 CSA Certification?

The 312-39 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the CSA exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the EC-Council 312-39 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and utilize the EC-Council 312-39 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, 312-39 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven 312-39 Practice Test for Success!!!

Do you want to pass the 312-39 exam on your first attempt? Stop worrying; we, EduSum.com are here to provide you the best experience during your EC-Council Certified SOC Analyst preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **312-39 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.