EC-COUNCIL 312-39

EC-Council CSA Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

312-39

EC-Council Certified SOC Analyst

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




EDUSUM

#1 Online Certification Guide

Table of Contents:

Discover More about the 312-39 Certification

Are you interested in passing the EC-Council 312-39 exam? First discover, who benefits from the 312-39 certification. The 312-39 is suitable for a candidate if he wants to learn about Advanced. Passing the 312-39 exam earns you the EC-Council Certified SOC Analyst title.

While preparing for the 312-39 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The 312-39 PDF contains some of the most valuable preparation tips and the details and instant access to useful **312-39 study materials just at one click.**

EC-Council 312-39 CSA Certification Details:

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**

312-39 Syllabus:

Topic
Security Operations and Management
Understanding Cyber Threats, IoCs, and Attack Methodology
Incidents, Events, and Logging
Incident Detection with Security Information and Event Management (SIEM)
Enhanced Incident Detection with Threat Intelligence
Incident Response

Broaden Your Knowledge with EC-Council 312-39 Sample Questions:

Question: 1

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: 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

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: 4

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: 5

What does HTTPS Status code 403 represents?

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

Answer: d

Question: 6

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: 7

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: 8

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: 9

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: 10

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

Avail the Study Guide to Pass EC-Council 312-39 CSA Exam:

- Find out about the 312-39 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **312-39 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the 312-39 training. Joining the EC-Council provided training for 312-39 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **312-39 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. 312-39 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the 312-39 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the 312-39 Certification

EduSum.Com is here with all the necessary details regarding the 312-39 exam. We provide authentic practice tests for the 312-39 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **312-39 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the EC-Council Certified SOC Analyst.

Start Online practice of 312-39 Exam by visiting URL
https://www.edusum.com/ec-council/312-39-ec-council-certified-soc-analyst