EC-COUNCIL 312-39

EC-Council CSA Certification Questions & Answers

Exam Summary – Syllabus –Questions

312-39
EC-Council Certified SOC Analyst (CSA)
100 Questions Exam – 70% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your 312-39 Certification Well:

The 312-39 is best suitable for candidates who want to gain knowledge in the EC-Council Advanced. Before you start your 312-39 preparation you may struggle to get all the crucial CSA materials like 312-39 syllabus, sample questions, study guide.

But don't worry the 312-39 PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the 312-39 syllabus?
- How many questions are there in the 312-39 exam?
- Which Practice test would help me to pass the 312-39 exam at the first attempt?

Passing the 312-39 exam makes you EC-Council Certified SOC Analyst (CSA). Having the CSA certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

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	Details	Weights
Security Operations and Management	- Understand the SOC Fundamentals - Discuss the Components of SOC: People, Processes and Technology - Understand the Implementation of SOC	5%
Understanding Cyber Threats, IoCs, and Attack Methodology	- Describe the term Cyber Threats and Attacks - Understand the Network Level Attacks - Understand the Host Level Attacks - Understand the Application Level Attacks - Understand the Indicators of Compromise (IoCs) - Discuss the Attacker's Hacking Methodology	11%
Incidents, Events, and Logging	- Understand the Fundamentals of Incidents, Events, and Logging - Explain the Concepts of Local Logging - Explain the Concepts of Centralized Logging	21%
Incident Detection with Security Information and Event Management (SIEM)	- Understand the Basic Concepts of Security Information and Event Management (SIEM) - Discuss the Different SIEM Solutions - Understand the SIEM Deployment - Learn Different Use Case Examples for Application Level Incident Detection - Learn Different Use Case Examples for Insider Incident Detection - Learn Different Use Case Examples for Network Level Incident Detection - Learn Different Use Case Examples for Host Level Incident Detection - Learn Different Use Case Examples for Compliance - Understand the Concept of Handling Alert Triaging and Analysis	26%
Enhanced Incident Detection with Threat Intelligence	- Learn Fundamental Concepts on Threat Intelligence - Learn Different Types of Threat Intelligence - Understand How Threat Intelligence Strategy is Developed - Learn Different Threat Intelligence Sources from which Intelligence can be Obtained	8%

Topic	Details	Weights
	- Learn Different Threat Intelligence Platform (TIP) - Understand the Need of Threat Intelligence-driven SOC	
Incident Response	- Understand the Fundamental Concepts of Incident Response - Learn Various Phases in Incident Response Process - Learn How to Respond to Network Security Incidents - Learn How to Respond to Application Security Incidents - Learn How to Respond to Email Security Incidents - Learn How to Respond to Insider Incidents - Learn How to Respond to Malware Incidents	29%

EC-Council 312-39 Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 6

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: 7

What does HTTPS Status code 403 represents?

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

Answer: d

Question: 8

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: 9

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: 10

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

Study Guide to Crack EC-Council CSA 312-39 Exam:

- Getting details of the 312-39 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 312-39 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the EC-Council provided training for 312-39 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 312-39 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 312-39 practice tests is must. Continuous practice will make you an expert in all syllabus areas.