GIAC GSOC

GIAC Security Operations Certified Certification Questions & Answers

Exam Summary – Syllabus –Questions

GSOC
GIAC Security Operations Certified
75 Questions Exam – 67% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your GSOC Certification Well:

The GSOC is best suitable for candidates who want to gain knowledge in the GIAC Cyber Defense. Before you start your GSOC preparation you may struggle to get all the crucial GIAC Security Operations Certified materials like GSOC syllabus, sample questions, study guide.

But don't worry the GSOC 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 GSOC syllabus?
- How many questions are there in the GSOC exam?
- Which Practice test would help me to pass the GSOC exam at the first attempt?

Passing the GSOC exam makes you GIAC Security Operations Certified. Having the GIAC Security Operations Certified certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GIAC GSOC GIAC Security Operations Certified Certification Details:

Exam Name	GIAC Security Operations Certified (GSOC)
Exam Code	GSOC
Exam Price	$979 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	67%
Books / Training	**SEC450: Blue Team Fundamentals: Security Operations and Analysis**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GSOC Sample Questions**
Practice Exam	**GIAC GSOC Certification Practice Exam**

GSOC Syllabus:

Topic	Details
Analytic Design and Tuning	- The candidate will understand how to design, enrich, test, share, and improve analytics.
Blue Team Defense Concepts	- The candidate will be able to explain the purpose of a SOC / Blue Team, its role in organizational risk, and common SOC monitoring and incident response methods.
Endpoint Defense	- The candidate will be familiar with common endpoint attacks, how to defend against them, and how endpoints log events.
HTTP(S) Analysis and Attacks	- The candidate will understand how to identify common attacks against HTTP(S) traffic, and how to defend against them.
Interpreting Events	- The candidate will be familiar with common events in Windows and Linux, how those events are represented and located in logs, and how to extract information from potentially malicious files.
Intrusion Triage and Analysis	- The candidate will understand how to prioritize incidents, and how to include organizational factors in analysis and response.
Network Traffic Analysis	- The candidate will have a high-level understanding of the architecture and monitoring of enterprise networks, how to review network traffic, and identify and protect against DNS attacks.
Operational Improvement	- The candiate will understand how to improve Blue Team operational efficiency through automation of tasks, orchestration of response, and training.
Protocol Attacks and Analysis	- The candidate will understand the purpose of common network protocols (such as SMTP, SMB, DHCP, ICMP, FTP, and SSH), common attack tactics, how to defend against them.
SOC Management Systems	- The candidate will be familar with the role and function of common Incident Management Systems, Threat Intelligence Platforms, and SIEMs.

GIAC GSOC Sample Questions:

Question: 1

For effective network traffic analysis, what should be considered when monitoring encrypted traffic?

(Choose Three)

a) The increase in CPU usage due to encryption and decryption processes
b) The possibility of encrypted malware communication
c) The certificate authority (CA) issuing the certificates
d) Establishing baselines for normal encrypted traffic patterns
e) Ignoring encrypted traffic as it is always secure

Answer: b, c, d

Question: 2

During the sharing phase of analytics, what is an effective practice for fostering understanding and engagement among stakeholders?

(Choose Three)

a) Utilizing interactive visualizations
b) Providing detailed technical documentation to all stakeholders regardless of their background
c) Tailoring the presentation to the audience's level of expertise
d) Offering actionable insights based on the data
e) Limiting access to data to prevent information overload

Answer: a, c, d

Question: 3

Which two sources of information are critical for analyzing Windows system events?

(Choose Two)

a) The Application log in Event Viewer
b) The Security log in Event Viewer
c) The Recycle Bin's metadata
d) The Windows Update log

Answer: a, b

Question: 4

Why is it crucial to secure SSH communications, particularly for administrative access?

a) Because securing SSH is mandated by all data protection regulations
b) Because SSH is commonly used over untrusted networks
c) Because unsecured SSH can provide an attacker with elevated privileges and access to sensitive areas of the network
d) Because SSH does not support strong encryption

Answer: c

Question: 5

Which factor is crucial when prioritizing incident response?

a) The phase of the moon
b) The personal interest of the responding analyst
c) The geographic location of the attacker
d) The incident’s potential impact on the organization

Answer: d

Question: 6

What is a crucial factor in a SOC's success in improving an organization's security posture?

a) Conducting regular and comprehensive training for SOC staff
b) Isolating the SOC team from the rest of the IT department to avoid biases
c) Limiting the SOC's access to essential systems only
d) Focusing exclusively on external threat intelligence

Answer: a

Question: 7

In the context of analytics enrichment, which of the following is considered a best practice?

a) Ignoring data source reliability
b) Incorporating external data sources for enhanced insights
c) Using only internal data to avoid external biases
d) Enriching data at random intervals

Answer: b

Question: 8

What advantage does integrating a Threat Intelligence Platform with a SIEM offer to a SOC?

a) It provides a direct marketing channel to potential clients.
b) It transforms the SIEM into an autonomous AI entity.
c) It enables correlation of external threat data with internal event data for enhanced analysis.
d) It allows the SOC to broadcast threat alerts on television.

Answer: c

Question: 9

How do Threat Intelligence Platforms (TIPs) enhance the effectiveness of a SOC?

a) By replacing the need for human analysts
b) By providing actionable intelligence on emerging threats
c) By functioning as the primary data storage solution
d) By automating all incident response actions

Answer: b

Question: 10

When securing endpoints, which two measures are effective in preventing unauthorized access?

(Choose Two)

a) Enabling auto-run features for external media
b) Implementing full disk encryption
c) Applying strong, unique passwords for each endpoint
d) Allowing users to install their applications to ensure they have tools they prefer

Answer: b, c

Study Guide to Crack GIAC GIAC Security Operations Certified GSOC Exam:

- Getting details of the GSOC 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 GSOC 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 GIAC provided training for GSOC 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 GSOC 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 GSOC practice tests is must. Continuous practice will make you an expert in all syllabus areas.