EDUSUM

#1 Online Certification Guide

GIAC GSOM

GIAC Security Operations Manager Certification Questions & Answers

Exam Summary – Syllabus –Questions

GSOM

GIAC Security Operations Manager (GSOM)

75 Questions Exam – 66% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your GSOM Certification Well:

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

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

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

GSOM GIAC Security Operations Manager Certification Details:

Exam Name	GIAC Security Operations Manager (GSOM)
Exam Code	GSOM
Exam Price	$979 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	66%
Books / Training	**LDR551: Building and Leading Security Operations Centers**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GSOM Sample Questions**
Practice Exam	**GIAC GSOM Certification Practice Exam**

GSOM Syllabus:

Topic	Details
Continuous Improvement	- The candidate will demonstrate an understanding of using post-incident data along with automation, analytic testing, and adversarial emulation to optimize SOC operations and ensure future growth.
Cyber Defense Theory, Threat Intel, and Defensible Architecture	- The candidate will demonstrate an understanding of fundamental cyber defense theory, cyber threat intelligence, and defensible security architecture concepts.
Data Source Assessment and Collection	- The candidate will demonstrate an understanding of utilizing business operations knowledge, organizational specific use cases, and industry frameworks to plan, prioritize, and orchestrate secure and efficient data collection and enrichment to support SOC monitoring operations.
Managing Alert Creation and Processing	- The candidate will demonstrate knowledge of alert creation, prioritization, and classification to support efficient SOC triage efforts. The candidate will demonstrate an understanding of implementing best practices to ensure timely and manageable SOC alert response.
Managing Incident Response Execution	- The candidate will demonstrate knowledge of techniques for performing effective investigations and methods to support the success of each phase of the incident response cycle.
Preparing for Incident Response	- The candidate will demonstrate an understanding of the preparation requirements for successful incident response, fundamental knowledge of the incident response cycle, and the role that incident response plays in the overall SOC operations.
Proactive Detection and Analysis	- The candidate will demonstrate familiarity with the threat hunting process, active defense techniques, and how community sourced resources can be utilized to supplement gaps in the SOC detection capabilities.
SOC Analytics and Metrics	- The candidate will demonstrate knowledge of using metrics, goals, and analytics to measure the progress and effectiveness of SOC operations to generate and implement a strategic plan that guides continuous maturity of the SOC.
SOC Design and Planning	- The candidate will demonstrate an understanding of how to assess the business goals, operational requirements, relevant threats, potential attack paths, and risk profile of an

Topic	Details
	organization to design and staff an effective SOC program.
SOC Tools and Technology	- The candidate will demonstrate knowledge of common SOC tools and technology, how they are utilized to support SOC operations, and the proper implementation practices to secure these resources.

GIAC GSOM Sample Questions:

Question: 1

In designing a defensible security architecture, which elements are critical? (Choose two)

a) Assuming that all network traffic is benign until proven otherwise
b) Implementing security at different layers (e.g., perimeter, network, host)
c) Regular testing and updates to security controls
d) Relying solely on antivirus software for endpoint protection

Answer: b, c

Question: 2

When assessing data sources for SOC monitoring, what is an important consideration related to organizational specific use cases?

a) Implementing the same use cases across different organizations
b) Customizing data collection methods to fit these use cases
c) Choosing use cases that are easiest to implement, regardless of relevance
d) Avoiding the use of use cases to simplify data collection

Answer: b

Question: 3

How can industry frameworks assist in the planning and prioritization of data collection for SOC monitoring?

a) By providing specific data sources to collect from, regardless of organizational context
b) By offering best practices and standards for structuring data collection
c) By eliminating the need for organizational input
d) By mandating uniform data collection processes across industries

Answer: b

Question: 4

Effective alert creation should:
(Select all that apply)

a) Generate a high volume of alerts to increase the chances of detecting incidents
b) Utilize contextual information to enhance alert relevancy
c) Incorporate thresholds to prevent alert fatigue
d) Be configurable and adaptable over time

Answer: b, c, d

Question: 5

Defensible security architecture typically includes which of the following features?

a) Single layer of security at the network perimeter
b) Neglecting the importance of data encryption
c) Isolation of IT systems for easier management
d) Strong emphasis on endpoint security

Answer: d

Question: 6

Why is it important to integrate endpoint detection and response (EDR) tools into SOC operations?

a) To provide detailed visibility into endpoint activities and potential threats
b) To replace the need for a SIEM system
c) To monitor and manage desktop environments only
d) To focus solely on external threats and ignore internal anomalies

Answer: a

Question: 7

What role does 'Threat Hunting' play in cyber defense?

a) It passively waits for alerts from other security tools
b) It involves actively looking for indicators of compromise within an environment
c) It is solely focused on external threat intelligence gathering
d) It disregards any anomalous activity that does not match known patterns

Answer: b

Question: 8

Analytic testing within SOC operations can help identify:

a) The best cybersecurity insurance policies
b) Future trends in employee behavior
c) Weaknesses in the incident response plan
d) The most efficient software update schedules

Answer: c

Question: 9

Which of the following best describes the role of automation in optimizing SOC operations post-incident?

a) Automates routine tasks to reduce human error
b) Replaces the need for human analysis entirely
c) Increases the incidence of false positives
d) Decreases the speed of incident response

Answer: a

Question: 10

To effectively detect advanced persistent threats (APTs), a SOC should:

(Choose two)

a) Rely exclusively on signature-based detection
b) Utilize behavioral analysis to identify subtle indicators of compromise
c) Engage in continuous information sharing with similar organizations
d) Assume APTs cannot bypass traditional security measures

Answer: b, c

Study Guide to Crack GIAC Security Operations Manager GSOM Exam:

- Getting details of the GSOM 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 GSOM 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 GSOM 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 GSOM 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 GSOM practice tests is must. Continuous practice will make you an expert in all syllabus areas.