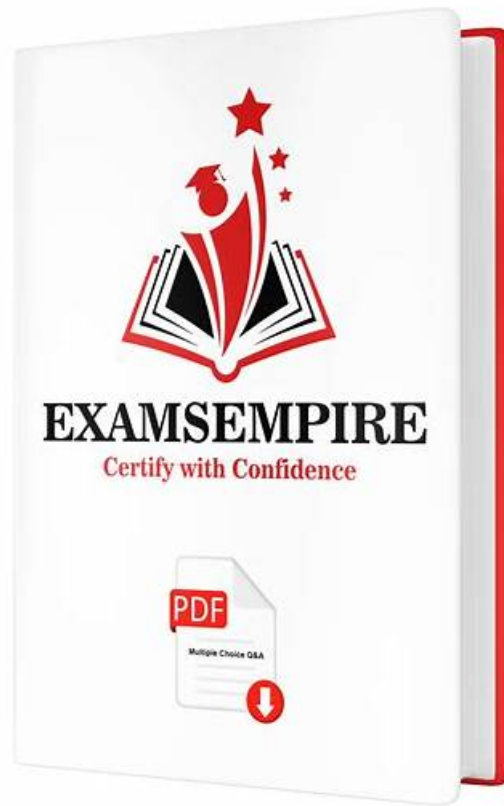


# Pass4sure GIAC GSOM Study Materials | GSOM Practice Test Fee



GSOM study materials can expedite your review process, inculcate your knowledge of the exam and last but not the least, speed up your pace of review dramatically. The finicky points can be solved effectively by using our GSOM exam questions. With a high pass rate as 98% to 100% in this career, we have been the leader in this market and helped tens of thousands of our loyal customers pass the exams successfully. Just come to buy our GSOM learning guide and you will love it.

If you want to take GIAC GSOM exam, PDFBraindumps GIAC GSOM exam dumps are your best tools. The dumps can help you pass GSOM test easily. And the dumps are very highly regarded. With our test questions and test answers, you don't need to worry about GSOM Certification. Because our dumps can solve all difficult problems you encounter in the process of preparing for the exam. Before you make a decision, you can download our free demo. For this, you will know whether our questions and answers fit to you or not.

>> **Pass4sure GIAC GSOM Study Materials** <<

## Real and Updated GIAC GSOM Exam Questions

No matter you are exam candidates of high caliber or newbies, our GIAC GSOM exam quiz will be your propulsion to gain the best results with least time and reasonable money. Not only because the outstanding content of GSOM Real Dumps that produced by our professional expert but also for the reason that we have excellent vocational moral to improve our GSOM learning materials quality.

## GIAC Security Operations Manager Sample Questions (Q83-Q88):

### NEW QUESTION # 83

Which metric can help in assessing the SOC's efficiency in identifying false positives?

Response:

- A. The total number of alerts in a year
- **B. The ratio of false positives to true positives**
- C. The number of high-priority incidents only
- D. The annual budget allocated to the SOC

**Answer: B**

#### **NEW QUESTION # 84**

Why is it important for a SOC to establish and track Key Performance Indicators (KPIs)?

Response:

- A. To ensure that all team members are overworked
- **B. To gauge the performance and impact of the SOC**
- C. To focus solely on the quantity of alerts processed
- D. To justify the elimination of the SOC

**Answer: B**

#### **NEW QUESTION # 85**

Why is it critical to have well-defined roles and responsibilities in incident response?

Response:

- **A. To assign specific tasks to team members based on their skills and expertise, ensuring efficient and effective response**
- B. To clearly delineate who is to be held accountable for the incident
- C. To ensure that no one in the organization takes any action, maintaining a clear chain of non-responsibility
- D. To prevent any single point of failure in the response process

**Answer: A**

#### **NEW QUESTION # 86**

In the context of SOC monitoring, what is the primary purpose of utilizing organizational-specific use cases during data source assessment?

Response:

- A. To reduce the volume of data collected
- B. To adopt a one-size-fits-all approach
- C. To decrease reliance on security frameworks
- **D. To align data collection with specific security needs**

**Answer: D**

#### **NEW QUESTION # 87**

How can the SOC use metrics to improve its strategic planning?

Response:

- A. By only tracking the number of alerts generated
- **B. By using metrics to identify trends, gaps, and areas for improvement**
- C. By focusing metrics solely on network traffic volumes
- D. By selecting arbitrary metrics that are easy to achieve

**Answer: B**

#### **NEW QUESTION # 88**

.....

- [illegible]