EDUSUM

#1 Online Certification Guide

GIAC GCDA

GIAC Certified Detection Analyst Certification Questions & Answers

Exam Summary – Syllabus –Questions

GCDA

GIAC Certified Detection Analyst (GCDA)

75 Questions Exam – 79% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your GCDA Certification Well:

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

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

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

GCDA GIAC Certified Detection Analyst Certification Details:

Exam Name	GIAC Certified Detection Analyst (GCDA)
Exam Code	GCDA
Exam Price	$979 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	79%
Books / Training	**SEC555: SIEM with Tactical Analytics**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GCDA Sample Questions**
Practice Exam	**GIAC GCDA Certification Practice Exam**

GCDA Syllabus:

Topic	Details
Alert Analysis	- The candidate will demonstrate an understanding of how to analyze endpoint security logs, augment intrusion detection alerts, analyze vulnerability information, correlate malware sandbox logs, handle alerts efficiently, identify which alerts to retain and identify staff training opportunities.
Device Discovery	- The candidate will demonstrate an understanding of how an environment can be more fully understood through the use of active and passive device discovery and how this understanding can be used to create baselines and detect anomolous behavior.
Endpoint Logging Analysis	- The candidate will demonstrate an understanding of how to discover abnormal activity, establish baselines and optimize logging to find anomalous behavior through the use of endpoint logs, events of interest and host-based firewalls.
Endpoint Logging Collection	- The candidate will demonstrate an understanding of how to identify attacks and analyze logs in both Windows and Linux environments and employ scripting to reduce log noise as well as establish collection strategies, both agentless and agent-oriented in these environments.
Log Aggregation and Parsing	- The candidate will demonstrate an understanding of how log filters and message brokers can be used during data queuing and storage to enhance log retention and search response times, demonstrate an understanding of the methods and techniques used to perform analysis, analytical reporting, and alerting through the use of visualizations and detection dashboards.
Log Collection	- The candidate will demonstrate an understanding of how data gathering strategies, event rates, storage requirements and staffing requirements inform SIEM planning and event logging device architecture, log monitoring for assets, data gathering and preservation strategies and techniques of log collection.
Log Output and Storage	- The candidate will demonstrate an understanding of data queuing, resiliency and storage as well as how to perform analytical reporting and alerting through the use of visualizations and detection dashboards.
Network Service Log	- The candidate will demonstrate an understanding of how

Topic	Details
Analysis	to identify attacker characteristics, determine anomalous behavior and establish baseline behavior in common network protocol traffic such as SMTP, DNS, HTTP and HTTPS.
Network Service Log Collection & Enrichment	- The candidate will demonstrate an understanding of detection methods and relevance to log analysis, analyzing common application logs, application of threat intelligence to generic network logs, correlation of network datasets and establishment of network baseline activity.
Post-Mortem Analysis	- The candidate will demonstrate an understanding of how to use virtual machines and malware sandboxes, configure systems to generate event log alerts after compromise, identify unusual time-based activity and re-analyze network traffic after an incident.
Software Monitoring	- The candidate will demonstrate an understanding of how to identify authorized and unauthorized software, treat scripting tools and command line parameters as a special kind of software and source collection methodology.
User Monitoring	- The candidate will demonstrate an understanding of how to utilize behavior analytics when analyzing user logons, built-in accounts and system services based on patterns, use network data to discover unauthorized use or assets, configure enterprise wide baseline collection and establish large scale persistence monitoring.

GIAC GCDA Sample Questions:

Question: 1

In the context of network service log collection, what aspects should be enriched to improve log analysis?

(Choose two)

a) Font styles to highlight different levels of log importance.
b) Geo-location information to trace the origin of network traffic.
c) User and entity behavior analytics (UEBA) for identifying insider threats.
d) Sound effects to indicate the severity of log events.

Answer: b, c

Question: 2

How does analyzing logs help in identifying attacks specifically in Linux environments?

a) By detecting unusual access patterns to sensitive files.
b) By tracking the uptime of the system.
c) By monitoring the version control history of deployed applications.
d) By observing the frequency of system reboots.

Answer: a

Question: 3

What are key considerations in planning storage requirements for log collection?
(Choose two)

a) The retention period for different types of logs.
b) The resolution of the monitors used to view the logs.
c) The anticipated growth in data volume.
d) The number of users who will access the logs.

Answer: a, c

Question: 4

How can monitoring software help in identifying unauthorized software?
(Choose two)

a) By changing the desktop theme when unauthorized software is detected.
b) By playing alert tones in different musical keys based on the software category.
c) By scanning system directories and comparing found applications against a whitelist.
d) By maintaining an inventory of authorized applications and alerting on deviations.

Answer: c, d

Question: 5

What purposes do detection dashboards serve in log output analysis?
(Select all that apply)

a) To consolidate and summarize key findings from log data.
b) To provide interactive mechanisms for deeper investigation of alerts.
c) To recommend culinary dishes based on log patterns.
d) To facilitate real-time monitoring and situational awareness.

Answer: a, b, d

Question: 6

Which factors should be considered when monitoring logs for assets?

(Choose two)

a) The criticality of the assets being monitored.
b) The favorite colors of the security analysts.
c) The geographic location of the assets.
d) The compliance requirements related to the assets.

Answer: a, d

Question: 7

Why is it beneficial to use virtual machines for post-mortem analysis?

a) To ensure the analysis environment can be easily replicated or restored.
b) To enhance the graphical interface of the analysis tools.
c) To improve the coffee-making process for analysts.
d) To increase the office space for post-mortem analysts.

Answer: a

Question: 8

Why is it important to analyze user logon patterns in behavior analytics?

a) To design personalized desktop themes for users.
b) To identify potential unauthorized access or compromised credentials.
c) To select appropriate background music for user logon events.
d) To forecast the cafeteria menu based on user preferences.

Answer: b

Question: 9

How can alert analysis identify staff training opportunities?

a) By assessing the frequency of alerts during off-hours.
b) By tracking the number of alerts generated per day.
c) By calculating the mean time to resolve alerts across the team.
d) By determining which alerts are ignored or mishandled by staff.

Answer: d

Question: 10

What is a source collection methodology in the context of software monitoring?

a) A technique to gather information on the provenance and purpose of installed software.
b) A strategy to collect the best desktop wallpapers from various sources.
c) A method to compile the greatest hits of software-related music.
d) A system to categorize software by the color of its icon.

Answer: a

Study Guide to Crack GIAC Certified Detection Analyst GCDA Exam:

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

Reliable Online Practice Test for GCDA Certification

Make EduSum.com your best friend during your GIAC Certified Detection Analyst exam preparation. We provide authentic practice tests for the GCDA exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual GCDA exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the GCDA exam.

Start Online practice of GCDA Exam by visiting URL
https://www.edusum.com/giac/gcda-giac-certified-detection-analyst