EDUSUM

#1 Online Certification Guide

GIAC GDSA

GIAC Defensible Security Architect Certification Questions & Answers

Exam Summary – Syllabus –Questions

GDSA

GIAC Defensible Security Architect

75 Questions Exam – 63% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your GDSA Certification Well:

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

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

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

GDSA GIAC Defensible Security Architect Certification Details:

Exam Name	GIAC Defensible Security Architect (GDSA)
Exam Code	GDSA
Exam Price	$979 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	63%
Books / Training	**SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GDSA Sample Questions**
Practice Exam	**GIAC GDSA Certification Practice Exam**

GDSA Syllabus:

Topic	Details
Cloud-based Security Architecture	- The candidate will show an understanding of the concepts involving cloud security, securing on-premise hypervisors, network segmentation, surface reduction, delivery models, and container security.
Data Discovery, Governance, and Mobility Management	- The candidate will demonstrate an understanding of file classification, Data Loss Prevention (DLP), database governance, and Mobile Device Management (MDM).
Data-Centric Security	- The candidate will demonstrate an understanding of the concepts involving data-centric security. Specifically, have an understanding of reverse proxies, web application firewalls, database firewalls, and database activity monitoring.
Fundamental Layer 3 Defense	- The candidate will demonstrate an understanding of the concepts related to securing basic Layer 3 hardware, protocols and services and have an awareness of common attack vectors. In particular, demonstrate a knowledge of CIDR, Layer 3 routing attacks and mitigations, Layer 2/3 benchmark and auditing tools, securing SNMP and NTP protocols, and bogon filtering.
Fundamental Security Architecture Concepts	- The candidate will demonstrate a basic understanding of the concepts of perimeter-focused deficiencies, presumption of compromise, Zero Trust Model, Intrusion Kill Chain, Diamond Model, software-defined networking, micro-segmentation, threat vector analysis and attack surface analysis.
IPv6	- The candidate will demonstrate an understanding of the concepts of IPV6. Specifically,have an understanding of addressing, dual stack systems, tunneling; and IPv6 router advertisement attacks and mitigation.
Layer 1/Layer 2 Defense	- The candidate will demonstrate an understanding of the concepts related to securing Layer 1 and Layer 2 services, applications and protocols and be aware of common vectors for these attacks. Specifically,have an understanding of the structure and deployment of VLANs, CDP, MAC spoofing, ARP cache poisoning, DHCP starvation, VLAN hopping, 802.1X, and NAC.

Topic	Details
Network Defenses	- The candidate will demonstrate an understanding of the concepts related to network defense. In particular, show a knowledge of NIDS, NIPS, network security monitoring, sandboxing, encryption, and DDOS protections.
Network Encryption and Remote Access	- The candidate will demonstrate an understanding of secure remote access, dual factor for all remote access VPNs and Jump Boxes.
Network Proxies and Firewalls	- The candidate will demonstrate an understanding of Web proxies,SMTP proxies, and next generation firewalls.
Zero Trust Endpoints	- The candidate will show an understanding of the concepts of securing Zero Trust Endpoints. In particular, demonstrate an understanding of patching via automation, end-user privilege reduction, host hardening, host IDS/IPS; endpoint firewalls, and scaling endpoint log collection.
Zero Trust Fundamentals	- The candidate will demonstrate an understanding of the concepts involving Zero Trust Architecture, credential rotation, and responding to pivoting adversaries and insider threats.
Zero Trust Networking	- The candidate will demonstrate a basic understanding of the concepts of Zero Trust Networking. Specifically, demonstrate an understanding of authenticating and encrypting endpoint traffic, Domain Isolation, Single Packet Authentication, red herring defenses, and proactive defenses to change attacker behaviors.

GIAC GDSA Sample Questions:

Question: 1

In the context of VLANs, what are the primary security concerns to address?
(Choose two)

a) VLAN hopping
b) Broadcast storm control
c) DHCP starvation
d) Quality of Service (QoS) tweaking

Answer: a, c

Question: 2

What is the primary function of a Network Intrusion Detection System (NIDS)?

a) Preventing all malware infections
b) Detecting potential network intrusions in real-time
c) Encrypting network traffic
d) Providing physical security for network devices

Answer: b

Question: 3

How does a host-based Intrusion Detection System/Intrusion Prevention System (IDS/IPS) contribute to the security of Zero Trust Endpoints?

a) By generating excessive logs to deter attackers
b) By encrypting data at rest and in transit
c) By monitoring and analyzing system activities for signs of malicious actions
d) By serving as the primary firewall at the network perimeter

Answer: c

Question: 4

What is the goal of authenticating and encrypting endpoint traffic in Zero Trust Networking?

a) To prevent all network communication
b) To allow unrestricted access to all devices
c) To verify the identity of users and devices and protect data from interception
d) To confuse attackers with false information

Answer: c

Question: 5

In the context of network proxies and firewalls, what is an essential characteristic of SMTP proxies?

a) They should enable all email attachments without scanning.
b) They provide detailed analysis and filtering of email traffic to identify threats.
c) They increase the speed of email delivery.
d) They are primarily used to enhance the user interface of email applications.

Answer: b

Question: 6

What are the purposes of using a sandbox in network defense?

a) Testing untrusted programs
b) Analyzing malware behavior
c) Storing sensitive information
d) Enhancing user experience

Answer: a, b

Question: 7

Which OSI model layer is synonymous with Layer 3 defense?

a) Facilitating data packet routing based on logical addressing and path determination.
b) Managing application-specific communications over the network efficiently.
c) Ensuring reliable data transfer with proper sequencing and error control mechanisms.
d) Establishing network connections and providing error detection at the data link level.

Answer: a

Question: 8

Which of the following is NOT a typical feature of Data Loss Prevention (DLP) solutions?

a) Content inspection
b) Contextual analysis
c) Data encryption
d) Decreasing storage use

Answer: d

Question: 9

When securing network protocols like SNMP and NTP, it is crucial to:

a) Ensure they are unmonitored
b) Utilize the least secure versions
c) Configure them with public access
d) Apply strong authentication and encryption

Answer: d

Question: 10

Which of the following are considered best practices for secure remote access?

a) Using outdated encryption standards
b) Regularly updating access policies
c) Allowing unlimited access attempts
d) Enforcing strong authentication mechanisms

Answer: b, d

Study Guide to Crack GIAC GIAC Defensible Security Architect GDSA Exam:

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

Reliable Online Practice Test for GDSA Certification

Make EduSum.com your best friend during your GIAC Defensible Security Architect exam preparation. We provide authentic practice tests for the GDSA exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual GDSA 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 GDSA exam.

Start Online practice of GDSA Exam by visiting URL
https://www.edusum.com/giac/gdsa-giac-defensible-security-architect