FORTINET NSE 5 - EDR 5.0 STUDY GUIDE PDF

Fortinet NSE 5 FortiEDR Certification Questions & Answers

Details of the Exam-Syllabus-Questions

NSE 5 - EDR 5.0

Fortinet Network Security Expert 5 - Network Security Analyst

30 Questions Exam – Pass / Fail Cut Score – Duration of 60 minutes

Table of Contents:

Get an Overview of the NSE 5 - EDR 5.0 Certification:

Who should take the **NSE 5 - EDR 5.0 exam**? This is the first question that comes to a candidate's mind when preparing for the NSE 5 FortiEDR certification. The NSE 5 - EDR 5.0 certification is suitable for candidates who are keen to earn knowledge on the Network Security and grab their Fortinet Network Security Expert 5 - Network Security Analyst. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But NSE 5 - EDR 5.0 study guide PDF is here to solve the problem. NSE 5 - EDR 5.0 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Fortinet NSE 5 - EDR 5.0 Certification?

There are several reasons why one should grab the NSE 5 - EDR 5.0 certification.

- The NSE 5 FortiEDR certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the **Fortinet Network Security Expert 5 - Network Security Analyst** is a powerful qualification for a prosperous career.

What Is the Fortinet NSE 5 - EDR 5.0 NSE 5 FortiEDR Certification Exam Structure?

Section	**Objectives**
FortiEDR system	- Explain FortiEDR architecture and technical positioning - Perform installation process - Perform FortiEDR inventory and use system tools

Section	Objectives
	- Deploy FortiEDR multi-tenancy - Use API to carry out FortiEDR management functions
FortiEDR security settings and policies	- Configure communication control policy - Configure security policies - Configure playbooks - Explain Fortinet Cloud Service (FCS)
Events, forensics, and threat hunting	- Analyze security events and alerts - Configure threat hunting profiles and scheduled queries - Analyze threat hunting data - Investigate security events using forensics analysis
FortiEDR integration	- Deploy FortiXDR - Configure security fabric using FortiEDR
FortiEDR troubleshooting	- Perform FortiEDR troubleshooting - Perform alert analysis on FortiEDR security events and logs

Enhance Knowledge with NSE 5 - EDR 5.0 Sample Questions:

Question: 1

Which scripting language is supported by the FortiEDR action manager?

a) TCL
b) Bash
c) Perl
d) Python

Answer: d

Question: 2

Which security policy has all of its rules disabled by default?

a) Exfiltration Prevention
b) Execution Prevention
c) Device Control
d) Ransomware Prevention

Answer: c

Question: 3

What is true about classifications assigned by Fortinet Cloud Service (FCS)?

a) FCS revises the classification of the core based on its database.
b) The core only assigns a classification if FCS is not available.
c) FCS is responsible for all classifications.
d) The core is responsible for all classifications if FCS playbooks are disabled.

Answer: a

Question: 4

How does FortiEDR implement post-infection protection?

a) By insurance against ransomware
b) By preventing data exfiltration or encryption even after a breach occurs
c) By real-time filtering to prevent malware from executing
d) By using methods used by traditional EDR

Answer: b

Question: 5

What is the purpose of the Threat Hunting feature?

a) Execute playbooks to isolate affected collectors in the organization
b) Find and delete all instances of a known malicious file or hash in the organization
c) Delete any file from any collector in the organization
d) Identify all instances of a known malicious file or hash and notify affected users

Answer: d

Question: 6

What is the benefit of using file hash along with the file name in a threat hunting repository search?

a) It helps to check the malware even if the malware variant uses a different file name.
b) It helps to make sure the hash is really a malware.
c) It helps to find if some instances of the hash are actually associated with a different file.
d) It helps locate a file as threat hunting only allows hash search.

Answer: a

Question: 7

A FortiEDR security event is causing a performance issue with a third-party application. What must you do first about the event?

a) Investigate the event to verify whether or not the application is safe
b) Contact Fortinet support
c) Terminate the process and uninstall the third-party application
d) Immediately create an exception

Answer: a

Question: 8

What is the role of a collector in the communication control policy?

a) A collector is used to change the reputation score of any application that collector runs
b) A collector can quarantine unsafe applications from communicating
c) A collector blocks unsafe applications from running
d) A collector records applications that communicate externally

Answer: d

Question: 9

A company requires a global communication policy for a FortiEDR multi-tenant environment. How can the administrator achieve this?

a) An administrator creates a new communication control policy and shares it with other organizations.
b) A local administrator creates a new communication control policy and shares it with other organizations.
c) An administrator creates a new communication control policy for each organization.
d) A local administrator creates a new communication control policy and assigns it globally to all organizations.

Answer: c

Question: 10

Which connectors can you use for the FortiEDR automated incident response?

(Choose two.)

a) FortiSandbox
b) FortiSiem
c) FortiNAC
d) FortiGate

Answer: c, d

What Study Guide Works Best in Acing the Fortinet NSE 5 - EDR 5.0 NSE 5 FortiEDR Certification?

The NSE 5 - EDR 5.0 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the NSE 5 FortiEDR exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the Fortinet NSE 5 - EDR 5.0 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and Utilize the Fortinet NSE 5 - EDR 5.0 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.
Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, NSE 5 - EDR 5.0 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven NSE 5 - EDR 5.0 Practice Test for Success!!!

Do you want to pass the NSE 5 - EDR 5.0 exam on your first attempt? Stop worrying; we, NWExam.com are here to provide you the best experience during your Fortinet NSE 5 - FortiEDR 5.0 preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **NSE 5 - EDR 5.0 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.