FORTINET NSE 5 - EDR 5.0

Fortinet NSE 5 FortiEDR Certification Questions & Answers

Exam Summary – 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:

Know Your NSE 5 - EDR 5.0 Certification Well:

The NSE 5 - EDR 5.0 is best suitable for candidates who want to gain knowledge in the Fortinet Network Security. Before you start your NSE 5 - EDR 5.0 preparation you may struggle to get all the crucial NSE 5 FortiEDR materials like NSE 5 - EDR 5.0 syllabus, sample questions, study guide.

But don't worry the NSE 5 - EDR 5.0 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 NSE 5 - EDR 5.0 syllabus?
- How many questions are there in the NSE 5 - EDR 5.0 exam?
- Which Practice test would help me to pass the NSE 5 - EDR 5.0 exam at the first attempt?

Passing the NSE 5 - EDR 5.0 exam makes you Fortinet Network Security Expert 5 - Network Security Analyst. Having the NSE 5 FortiEDR certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Fortinet NSE 5 - EDR 5.0 NSE 5 FortiEDR Certification Details:

Exam Name	Fortinet NSE 5 - FortiEDR 5.0
Exam Code	NSE 5 - EDR 5.0
Exam Price	$200 USD
Duration	60 minutes
Number of Questions	30
Passing Score	Pass / Fail
Recommended Training	**NSE 5 Training FortiEDR**
Exam Registration	**PEARSON VUE**
Sample Questions	**Fortinet NSE 5 - EDR 5.0 Sample Questions**

Practice Exam	Fortinet Network Security Expert 5 - Network Security Analyst Practice Test

NSE 5 - EDR 5.0 Syllabus:

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

Fortinet NSE 5 - EDR 5.0 Sample Questions:

Question: 1

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: 2

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

(Choose two.)

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

Answer: c, d

Question: 3

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: 4

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: 5

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: 6

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: 7

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: 8

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: 9

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: 10

Which scripting language is supported by the FortiEDR action manager?

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

Answer: d

Study Guide to Crack Fortinet NSE 5 FortiEDR NSE 5 - EDR 5.0 Exam:

- Getting details of the NSE 5 - EDR 5.0 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 NSE 5 - EDR 5.0 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 Fortinet provided training for NSE 5 - EDR 5.0 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 NSE 5 - EDR 5.0 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 NSE 5 - EDR 5.0 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for NSE 5 - EDR 5.0 Certification

Make NWExam.com your best friend during your Fortinet NSE 5 - FortiEDR 5.0 exam preparation. We provide authentic practice tests for the NSE 5 - EDR 5.0 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual NSE 5 - EDR 5.0 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 NSE 5 - EDR 5.0 exam.

Start Online practice of NSE 5 - EDR 5.0 Exam by visiting URL
https://www.nwexam.com/fortinet/nse-5-edr-5-0-fortinet-nse-5-fortiedr-5-0-nse-5-network-security-analyst