# Reliable NSE6_EDR_AD-7.0 Test Labs | NSE6_EDR_AD-7.0 Trustworthy Exam Torrent


What's more, part of that Prep4sureExam NSE6_EDR_AD-7.0 dumps now are free: https://drive.google.com/open?id=1IViqh_gMo9_tCIiK55F85wHlgr9SKr8o

For candidates who are going to select the NSE6_EDR_AD-7.0 training materials for the exam, the pass rate for the NSE6_EDR_AD-7.0 training materials is important. With pass rate reaching 98.65%, the exam dumps have reached great popularity among the candidates, and we have received many good feedbacks from the buyers. In addition, NSE6_EDR_AD-7.0 Exam Materials are edited by professional experts, they possess the professional knowledge for the exam, therefore the quality can be guaranteed. We have free demo for you to have a try for NSE6_EDR_AD-7.0 training materials. You can have a try before buying.

## Fortinet NSE6_EDR_AD-7.0 Exam Syllabus Topics:

| Section | Weight | Objectives |
|---|---|---|
| Topic 1: FortiEDR Installation and Configuration | 25% | - Collector Agent installation methods<br>- Communication Manager setup<br>- Management Platform deployment<br>- Initial configuration and licensing<br>- Pre-installation requirements and planning |

| | | |
|---|---|---|
| Topic 2: Administration and Maintenance | 10% | - Upgrade and patch management<br>- User management and role-based access<br>- System monitoring and diagnostics<br>- Backup and recovery procedures<br>- Log management and export |
| Topic 3: FortiEDR Architecture and Components | 20% | - Communication Manager and Cloud Console<br>- Collector Agent components and functionality<br>- FortiEDR core architecture overview<br>- Management Platform architecture |
| Topic 4: Threat Detection and Response | 20% | - Automated threat remediation<br>- Incident response workflows<br>- Real-time threat blocking<br>- Event analysis and investigation<br>- Forensic data collection |
| Topic 5: Policy Management and Security Profiles | 25% | - Exclusion configuration<br>- Policy assignment and targeting<br>- Default security policies overview<br>- Custom policy creation and modification<br>- Application control rules |



## NSE6_EDR_AD-7.0 Trustworthy Exam Torrent & NSE6_EDR_AD-7.0 Valid Test Question

All these three NSE6_EDR_AD-7.0 real dumps formats contain the actual and updated Fortinet NSE 6 - FortiEDR 7.0 Administrator NSE6_EDR_AD-7.0 exam questions that will surely repeat in the upcoming NSE6_EDR_AD-7.0 exam and you can easily pass it with good scores. Today is the best time to learn new in-demand skills and upgrade your knowledge. Yes, you can do this easily. Just enroll in the Fortinet NSE 6 - FortiEDR 7.0 Administrator NSE6_EDR_AD-7.0 Exam and start preparation with Fortinet NSE 6 - FortiEDR 7.0 Administrator NSE6_EDR_AD-7.0 exam dumps. The updated, real, and verified Fortinet Dumps are ready for download. Just pay affordable Fortinet NSE 6 - FortiEDR 7.0 Administrator NSE6_EDR_AD-7.0 exam dumps charges and get the exam dumps file in your mailbox and start Prep4sureExam NSE6_EDR_AD-7.0 exam preparation.

## Fortinet NSE 6 - FortiEDR 7.0 Administrator Sample Questions (Q28-Q33):

**NEW QUESTION # 28**
Which two statements correctly describe the IoT probing process on FortiEDR? (Choose two answers)

- A. Collectors running on servers are always used for IoT probing.
- B. It identifies nearby devices by retrieving details such as hostname and IP address.
- C. Only healthy collectors participate in IoT probing.
- D. It captures all traffic from neighboring devices for deep packet inspection.

**Answer: B,C**

Explanation:
The correct answers are B and C .
The FortiEDR 7.0.0 Administration Guide explains that IoT device discovery continuously identifies newly connected non-workstation devices, such as printers, cameras, and media devices. During discovery, each relevant Collector periodically probes nearby neighboring devices. The guide states that nearby devices usually respond by providing information about themselves, including the device/host name and IP address .
This directly supports option B .
Option C is also correct because the guide states that Collectors in degraded , disabled , or isolated states do not take part in the IoT probing process. It also says FortiEDR uses the most powerful Collectors in each subnet and excludes weaker Collectors, including disabled and degraded Collectors.
Option A is wrong because the guide explicitly says Collectors running on servers do not take part in IoT probing. Option D is wrong because IoT probing is not described as deep packet inspection of all neighboring traffic; it is a discovery/probing process used to identify nearby devices and collect basic device information.
==========

**NEW QUESTION # 29**
An employee leaves the company and no longer has access to the FortiEDR system. You must ensure GDPR compliance regarding the employee's personal data stored in FortiEDR. Which two data types must be removed to meet GDPR requirements? (Choose two answers)

- A. Installed OS name
- B. Device and user name
- C. Installed applications
- D. IP address and MAC address

**Answer: B,D**

Explanation:
The correct answers are A. Device and user name and D. IP address and MAC address .
The FortiEDR 7.0.0 Administration Guide states that the GDPR feature is implemented in Administration > Settings > Personal Data Handling . It is used to remove relevant data for an employee or FortiEDR user who no longer has access to or uses the FortiEDR system. The guide explicitly identifies the personal data as device name, IP address, MAC address, and user name . It further states: "You must remove all device name, IP address, MAC address, and user name data from FortiEDR in order to fully comply with the GDPR standard." Therefore, installed applications and installed OS name are not the required GDPR personal data types in this FortiEDR procedure. The required removal is performed iteratively for the employee's/user's device name , IP address , MAC address , and user name . The guide also instructs administrators to continue removing the other required data: IP address, MAC address, and user name , and to delete any reports that may contain the user's data.

**NEW QUESTION # 30**
Refer to the exhibit.


An event exception is shown. Which two statements about the exception are true? (Choose two answers)

- A. A partial exception is applied to this event.
- B. The system owner can modify the trigger rules parameters.
- C. The exception is applied only on device C8092231196.
- D. FCS playbooks are enabled by Fortinet support.

**Answer: B,D**

Explanation:
The correct answers are C and D .
The exhibit shows an exception created/updated by FortinetCloudServices after the file Update.exe was classified as Good . This aligns with the FortiEDR Cloud Service behavior described in the guide. The guide states that once FCS is connected, it can enable

Tuning , which means automated security event exception
/allowlisting. After a triggered security event is reclassified as Safe, an automated cross-environment exception can be pushed downstream and the event expires, preventing it from triggering again.
Option C is correct because the Event Exceptions window includes Triggered Rules , and the guide states that when editing an exception, the administrator can modify the Collector Groups , Destinations , Users , and the pairs of rules and processes that define the exception in the Triggered Rules area.
Option D is the Fortinet/FCS-related statement supported by the guide's FCS behavior. The guide says FCS can enable follow-up actions, including Tuning through automated exceptions and Playbook Actions , and that playbook policy remediation actions are based on the final FCS determination.
Option A is wrong because the exhibit explicitly states "All the Raw Data Items are covered." A partial exception would mean not all raw data items are covered. The guide explains that if an exception does not cover all raw data items, FortiEDR displays a different indicator and distinguishes covered from non-covered raw data items.
Option B is wrong because the exception scope in the exhibit is set to All groups , All destinations , and All users . The comment references device C8092231196, but that is not the same as saying the exception applies only to that device.
═══════

**NEW QUESTION # 31**
Refer to the Exhibit:


Based on the event shown in the exhibit, which two statements about the event are true? (Choose two answers)

- A. Playbooks are configured for this event.
- B. The device is moved to isolation.
- C. The event has been blocked.
- D. The policy is in simulation mode.

**Answer: A,D**

Explanation:
The correct answers are A and B .
The exhibit shows the event classification as Malicious , classified by FortinetCloudServices , and the history states that device R2D2-kvm63 was moved from the Training Collector Group to the High Security Collector Group . This is a Playbook action. The FortiEDR guide explains that after classification changes, the Overview pane displays the history of automatic FortiEDR actions, including Playbook policy-related actions .
The guide specifically lists Move device to High Security Group under Investigation actions in Playbook policies. It states that a checkmark in a classification column means the device is automatically moved to the High Security Collector Group when a security event with that classification is triggered. So the exhibit proves that Playbooks are configured for this event.
The second correct answer is B because the triggered rule is under Training * Extended Detection . The FortiEDR guide states that the eXtended Detection Policy logs events and displays them in the Incidents tab, but no blocking options are provided for this policy.
Option C is wrong because moving a device to the High Security Collector Group is not the same as isolating the device. Isolation would block communication to/from the affected Collector. The exhibit shows a Collector Group move, not isolation.
Option D is wrong because Extended Detection does not block. The guide explicitly says Extended Detection events are logged and displayed, with no blocking options provided.
═══════

**NEW QUESTION # 32**
You are asked to configure a query to run every 15 minutes, automatically searching for specific registry modifications across all endpoints. Which FortiEDR feature must you configure? (Choose one answer)

- A. A new playbook trigger based on the registry change event
- B. A manual query linked to a policy override
- C. A communication control rule with a 15-minute delay
- D. A scheduled query defined within a threat hunting profile

**Answer: D**

Explanation:
The correct answer is C.
The FortiEDR guide explains that Threat Hunting searches across endpoint activity events, including registry activity. It states that Threat Hunting can search based on attributes of files, registry keys and values, network, processes, event log, and activity event types. This fits the requirement to search for specific registry modifications across endpoints.
The guide also explains that after filtering activity events, the query can be saved and defined as a Scheduled Query. It says: "Scheduled Query: Mark this option to automate the process of detecting threats so that this query is run automatically according to the schedule that you define." It also states that a security event is automatically created in the Incidents tab when matches are detected, and notifications can be sent through email, Syslog, and other configured methods.
The guide further states that the Repeat Every/On options define the frequency and schedule when the query runs. Therefore, a 15-minute recurring query is handled through the Scheduled Query capability in Threat Hunting, not Communication Control, policy override, or a manual Playbook trigger.
Strictly speaking, the guide calls this a scheduled query under Threat Hunting saved queries, not a "communication control rule" or "manual query." Option C is the intended answer.
==========

**NEW QUESTION # 33**
.....

We are now in a fast-paced era, and for this we have no right to choose. Just as a proverb says "Time is money." This is the reason why we must value time. That is to say, we should make full use of our time to do useful things. As examinee whose want to pass the NSE6_EDR_AD-7.0, you shouldn't waste your time on some useless books or materials. Our NSE6_EDR_AD-7.0 Materials are tool that can not only to help you save a lot of time, but also help you pass the NSE6_EDR_AD-7.0 exam. In this way, you can much time to complete your other goals and improve yourself better. What a rare opportunity it is! Never miss it because of your hesitation.

- 2026 Reliable NSE6_EDR_AD-7.0 Test Labs | Efficient NSE6_EDR_AD-7.0 Trustworthy Exam Torrent: Fortinet NSE 6 - FortiEDR 7.0 Administrator □ Search for 【 NSE6_EDR_AD-7.0 】 and download it for free on □ www.pdfvce.com □ website □NSE6_EDR_AD-7.0 Test Centres
- 2026 Reliable NSE6_EDR_AD-7.0 Test Labs | Efficient NSE6_EDR_AD-7.0 Trustworthy Exam Torrent: Fortinet NSE 6 - FortiEDR 7.0 Administrator □ Search for ➽ NSE6_EDR_AD-7.0 □ and download exam materials for free through [ www.exam4labs.com ] □Free NSE6_EDR_AD-7.0 Exam
- learn.csisafety.com.au, app.intigriti.com, www.notebook.ai, fortunetelleroracle.com, www.bandlab.com, savee.com, www.slideshare.net, www.impactio.com, learn.csisafety.com.au, faithlife.com, Disposable vapes

DOWNLOAD the newest Prep4sureExam NSE6_EDR_AD-7.0 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1IViqh_gMo9_tCIiK55F85wHlgr9SKr8o