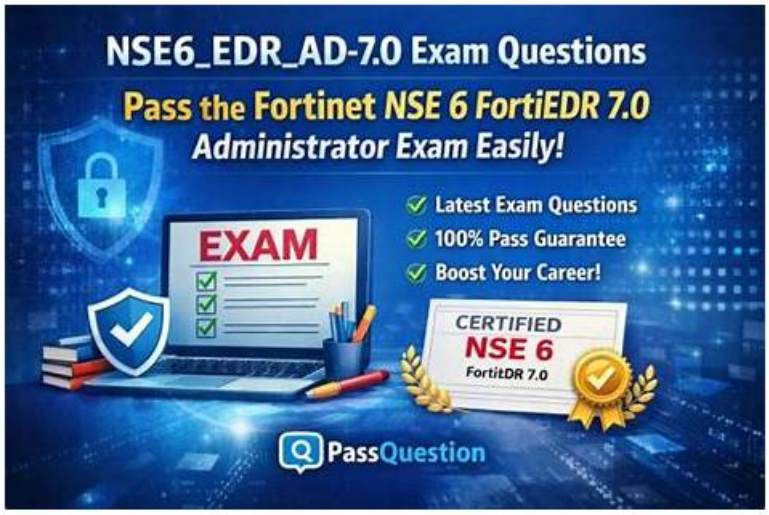
Practice NSE6_EDR_AD-7.0 Exam Pdf - 100% Pass 2026 NSE6_EDR_AD-7.0: Fortinet NSE 6 - FortiEDR 7.0 Administrator First-grade Test Registration



To keep pace with the times, we believe science and technology can enhance the way people study. Especially in such a fast-pace living tempo, we attach great importance to high-efficient learning. Therefore, our NSE6_EDR_AD-7.0 study materials base on the past exam papers and the current exam tendency, and design such an effective simulation function to place you in the Real NSE6_EDR_AD-7.0 Exam environment. We promise to provide a high-quality simulation system with advanced NSE6_EDR_AD-7.0 study materials to help you pass the exam with ease.

Fortinet NSE6_EDR_AD-7.0 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: FortiEDR System Architecture and Deployment	25%	- Architecture and technical positioning - Installation and deployment process - Multi-tenancy deployment - API-based management operations - Inventory management and system tools
Topic 2: Monitoring and Troubleshooting	10%	- Log and alert troubleshooting - Performance and issue diagnosis - System monitoring and health checks
Topic 3: Security Settings and Policies	25%	- Fortinet Cloud Service (FCS) integration - Communication control policies - Playbooks creation and management - Security policies configuration
Topic 4: Events, Forensics, and Threat Hunting	25%	- Forensic analysis and incident investigation - Threat hunting data interpretation - Security event and alert analysis - Threat hunting profiles and queries
Topic 5: Integration and Security Fabric	15%	- Fortinet Security Fabric integration - FortiXDR deployment and configuration

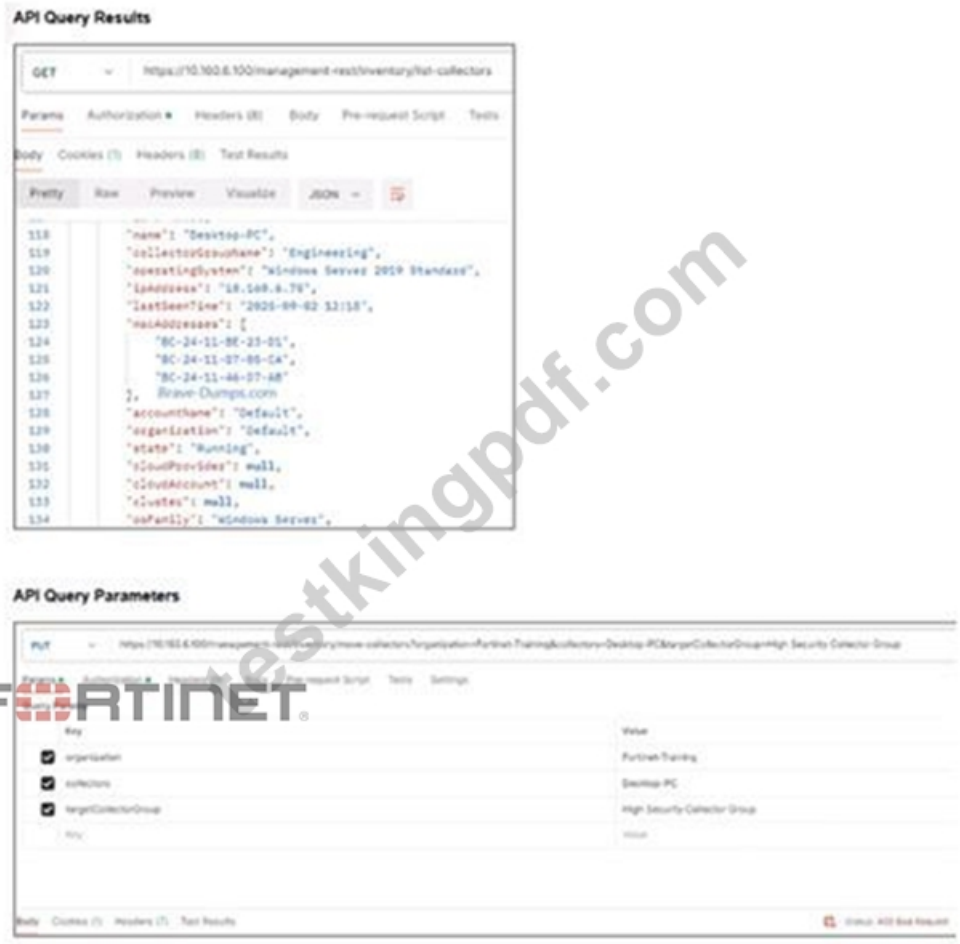
>> Practice NSE6_EDR_AD-7.0 Exam Pdf <<

Test NSE6_EDR_AD-7.0 Registration, NSE6_EDR_AD-7.0 Latest Braindumps Sheet

Nowadays, the development of technology is quickly. Also, our NSE6_EDR_AD-7.0 exam guide will keep advancing. A lot of reforms have applied to the content and formats of our NSE6_EDR_AD-7.0 learning guide according to our professional experts constantly efforts. We just hope that you will have a better experience when you study on our NSE6_EDR_AD-7.0 Actual Exam. Act from now if you are still hesitating, our NSE6_EDR_AD-7.0 study materials will enable you embrace a bright future.

Fortinet NSE 6 - FortiEDR 7.0 Administrator Sample Questions (Q14-Q19):

NEW QUESTION # 14
Refer to the exhibits.



You are attempting to move a collector into the High Security Collector Group for isolation but encounter an error in the API request as shown in the exhibit. To successfully isolate the collector, which API parameter must you correct? (Choose one answer)

- A. Change the HTTP method in the request from PUT to POST.
- B. Set the organization parameter to Default.
- C. Set the target collector group parameter to Engineering group.
- D. Update the authorization credentials in the API header.

Answer: B

Explanation:
The correct answer is A. Set the organization parameter to Default .
From the first exhibit, the API query result for the Collector shows:
* Collector name: Desktop-PC
* Collector group name: Engineering
* Organization: Default
* State: Running
But in the second exhibit, the API request is using:
* organization = Fortinet-Training
* collectors = Desktop-PC
* targetCollectorGroup = High Security Collector Group
That organization value is wrong. The Collector belongs to the Default organization, so the API request must reference the

Collector's actual organization. Otherwise FortiEDR cannot locate or move that Collector under the organization specified in the request.
The FortiEDR guide confirms that Collector Groups are used to assign different FortiEDR policies to different Collectors, and that Collectors can be moved between groups/organizations in the Inventory workflow. In Hoster view, FortiEDR shows Collectors from all organizations and allows moving Collectors between organizations, but the organization context must match the Collector being managed.
Option B is wrong because the exhibit shows the API request is authorized; the failure is a 400 Bad Request , not an authentication failure. Option C is wrong because the endpoint shown is already a move/update operation using PUT, and the issue is not the HTTP method. Option D is wrong because Engineering is the current Collector Group. The goal is to move the Collector to High Security Collector Group , so changing the target back to Engineering would not isolate or harden the Collector.

NEW QUESTION # 15
Refer to the exhibit:
Process exclusion

You configured an execution prevention exclusion with both File Name = app.exe and Path = C:\Tools. What will FortiEDR do? (Choose one answer)

- A. Exclude only app.exe when it is running from C:\Tools.
- B. Exclude app.exe whenever it appears.
- C. Exclude all files in C:\Tools.
- D. Exclude only signed versions of app.exe.

Answer: A

Explanation:
The correct answer is B. Exclude only app.exe when it is running from C:\Tools.
The FortiEDR 7.0.0 Administration Guide explains that the Exclusion Manager is used to define which processes, files, or domains are excluded from Security Policies monitoring. For Process Exclusions, FortiEDR does not inspect actions performed by specific processes, and those processes are identified by the attributes defined by the administrator.
The guide further explains that process/source attributes can include File Name, Path, Hash, and Signer. It also states that when an exclusion contains multiple conditions, an AND relationship exists between the conditions. If an OR relationship is required, a separate exclusion must be created.

In this exhibit, both conditions are selected:
File Name = app.exe
Path = C:\Tools
Because FortiEDR applies an AND relationship between multiple exclusion conditions, the exclusion applies only when both conditions match. Therefore, FortiEDR excludes app.exe only when it is located/running from C:\Tools.
Option A is wrong because no Signer condition is selected. Option C is wrong because that would apply if only the file name were used broadly. Option D is wrong because FortiEDR is not excluding every file in C:
\Tools; it is excluding the process that matches both the file name and path conditions.

NEW QUESTION # 16
Which two statements correctly describe the IoT probing process on FortiEDR? (Choose two answers)

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

Answer: A,B

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 # 17
Refer to the exhibit.

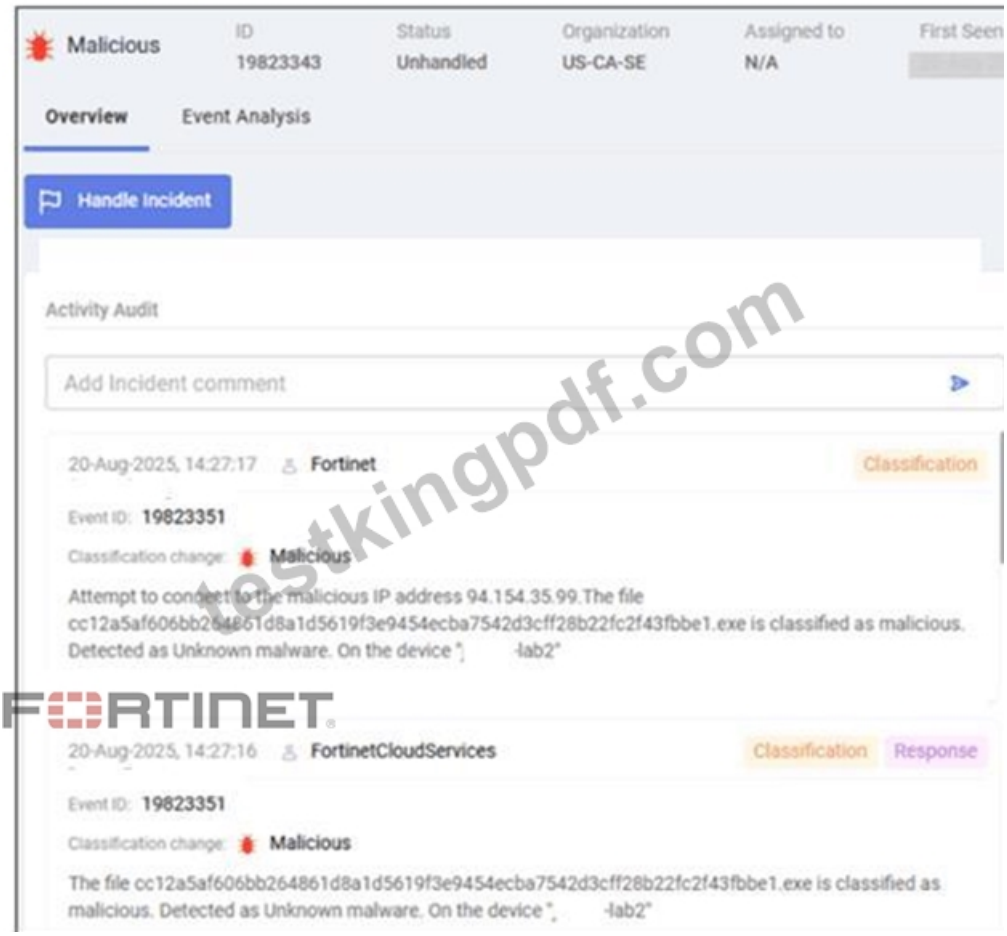
An event exception is shown. Which two statements about the exception are true? (Choose two answers)

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

Answer: A,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 # 18
Refer to the exhibit.



Based on the exhibit, which two observations are true? (Choose two answers)

- A. FCS has classified this as malicious.
- B. EDR has never encountered this malware before.
- C. FortiEDR has classified this as suspicious.
- D. This incident has been resolved.

Answer: A,B

Explanation:
The correct answers are C and D .
The exhibit shows the incident classification as Malicious . In the Activity Audit, the entry from FortinetCloudServices states: "Classification change: Malicious" and also says the file is classified as malicious. This directly proves that FCS classified the event as malicious . The FortiEDR guide explains that the audit history shows the chronology for classifying the security event and displays details when FortiEDR Cloud Service (FCS) reclassifies a security event after its initial classification by the Core.
The exhibit also states that the file was "Detected as Unknown malware." This supports option D in the exam wording: FortiEDR/FCS has classified the file as malicious, but it is being identified as unknown malware , meaning it was not recognized as a known malware family/signature at the time of classification.
The guide explains that FCS enhances classification using data enrichment, automated and manual analysis, file analysis, sandboxing, machine learning flow analysis, commonality analysis, crowdsourced data deduction, and other methods, so "unknown malware" can still be classified malicious by FCS.
Option A is wrong because the exhibit shows Malicious , not Suspicious. Option B is wrong because the incident status is Unhandled , not resolved or handled.
═══════

NEW QUESTION # 19

.....

These Fortinet NSE6_EDR_AD-7.0 exam practice tests identify your mistakes and generate your result report on the spot.To make your success a certainty, TestkingPDF offers free updates on our Fortinet NSE6_EDR_AD-7.0 real dumps for up to three months. It means all users get the latest and updated Fortinet NSE6_EDR_AD-7.0 practice material to clear the Fortinet NSE 6 - FortiEDR 7.0 Administrator NSE6_EDR_AD-7.0 certification test on the first try. We are a genuine brand working to smoothen up your NSE6_EDR_AD-7.0 exam preparation.

Test NSE6_EDR_AD-7.0 Registration: https://www.testkingpdf.com/NSE6_EDR_AD-7.0-testking-pdf-torrent.html

- NSE6_EDR_AD-7.0 Reliable Dumps Questions □ NSE6_EDR_AD-7.0 Exam Cram □ Dump NSE6_EDR_AD-7.0 File □ Easily obtain free download of ▷ NSE6_EDR_AD-7.0 ◁ by searching on { www.testkingpass.com } □Practice Test NSE6_EDR_AD-7.0 Pdf
- 2026 NSE6_EDR_AD-7.0 – 100% Free Practice Exam Pdf | Professional Test NSE6_EDR_AD-7.0 Registration □ Immediately open ✔ www.pdfvce.com □✔□ and search for 「 NSE6_EDR_AD-7.0 」 to obtain a free download □ □NSE6_EDR_AD-7.0 Reliable Dumps Questions
- Web-Based Practice Exams to Evaluate Fortinet NSE6_EDR_AD-7.0 Exam Preparation □ Search on 《 www.examdiscuss.com 》 for 【 NSE6_EDR_AD-7.0 】 to obtain exam materials for free download □ □NSE6_EDR_AD-7.0 Reliable Test Tutorial
- NSE6_EDR_AD-7.0 Reliable Test Tutorial □ Detailed NSE6_EDR_AD-7.0 Answers □ NSE6_EDR_AD-7.0 Test Sample Online □ Easily obtain [NSE6_EDR_AD-7.0] for free download through { www.pdfvce.com } □Latest NSE6_EDR_AD-7.0 Learning Material
- 2026 NSE6_EDR_AD-7.0 – 100% Free Practice Exam Pdf | Professional Test NSE6_EDR_AD-7.0 Registration □ Immediately open 【 www.prepawaypdf.com 】 and search for 【 NSE6_EDR_AD-7.0 】 to obtain a free download □ □Valid NSE6_EDR_AD-7.0 Exam Dumps
- NSE6_EDR_AD-7.0 Test Sample Online □ NSE6_EDR_AD-7.0 Exam Cram □ NSE6_EDR_AD-7.0 Test Papers □ □ Download 「 NSE6_EDR_AD-7.0 」 for free by simply entering 【 www.pdfvce.com 】 website □Practice Test NSE6_EDR_AD-7.0 Pdf
- NSE6_EDR_AD-7.0 Reliable Dumps □ Latest NSE6_EDR_AD-7.0 Exam Objectives □ NSE6_EDR_AD-7.0 Exam Cram □ Enter □ www.exam4labs.com □ and search for ▸ NSE6_EDR_AD-7.0 ◂ to download for free □Dump NSE6_EDR_AD-7.0 File
- High Pass-Rate Practice NSE6_EDR_AD-7.0 Exam Pdf - Effective Test NSE6_EDR_AD-7.0 Registration - Practical NSE6_EDR_AD-7.0 Latest Braindumps Sheet □ Search for ✔ NSE6_EDR_AD-7.0 □✔□ and obtain a free download on ⇛ www.pdfvce.com ⇚ □NSE6_EDR_AD-7.0 Reliable Cram Materials
- NSE6_EDR_AD-7.0 Hottest Certification □ New NSE6_EDR_AD-7.0 Exam Prep □ Practice Test NSE6_EDR_AD-7.0 Pdf □ Search for ☀ NSE6_EDR_AD-7.0 □☀□ and obtain a free download on ➽ www.testkingpass.com □ □ □Dump NSE6_EDR_AD-7.0 File
- First-grade Practice NSE6_EDR_AD-7.0 Exam Pdf Provide Prefect Assistance in NSE6_EDR_AD-7.0 Preparation ↕ Open 《 www.pdfvce.com 》 enter ➤ NSE6_EDR_AD-7.0 □ and obtain a free download □New NSE6_EDR_AD-7.0 Exam Prep
- 2026 NSE6_EDR_AD-7.0 – 100% Free Practice Exam Pdf | Professional Test NSE6_EDR_AD-7.0 Registration □ The page for free download of ➠ NSE6_EDR_AD-7.0 □ on 《 www.prepawaypdf.com 》 will open immediately □New NSE6_EDR_AD-7.0 Exam Prep
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, fortunetelleroracle.com, Disposable vapes