Exam4Future

Fortinet NSE 5 - FortiEDR 5.0 Exam

Fortinet NSE5_EDR-5.0

Version Demo

Total Demo Questions: 5

Total Premium Questions: 50

Buy Premium PDF

https://exam4future.com

support@exam4future.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiEDR Architecture	10
Topic 2, FortiEDR Deployment	2
Topic 3, FortiEDR Configuration	5
Topic 4, FortiEDR Security Policies	14
Topic 5, FortiEDR Threat Hunting	10
Topic 6, FortiEDR Incident Response	9
Total	50

QUESTION NO: 1

The FortiEDR axe classified an event as inconclusive, out a few seconds later FCS revised the classification to malicious. What playbook actions ate applied to the event?

A. Playbook actions applied to inconclusive events

B. Playbook actions applied to handled events

C. Playbook actions applied to suspicious events

D. Playbook actions applied to malicious events

ANSWER: D

Explanation:

Playbook actions applied to malicious events is correct because FortiEDR uses the event's updated classification when FortiGuard Cloud Services (FCS) returns a definitive verdict. An initial inconclusive classification represents a temporary state while further reputation, intelligence, or cloud-based analysis is pending. When FCS subsequently determines that the activity is malicious, FortiEDR updates the event classification to malicious and applies the playbook actions configured for malicious events. This ensures the configured automated response aligns with the final threat verdict, such as collecting additional evidence, isolating a device, terminating a process, or notifying designated responders, depending on the organization's playbook configuration. The short delay in receiving the FCS verdict does not cause the event to remain governed by its earlier inconclusive state; the malicious verdict is the actionable classification for the event. Administrators should therefore ensure that the malicious-event playbook contains the response actions appropriate for confirmed threats and is tested against their operational requirements. Fortinet's FortiEDR documentation describes event classification, cloud-assisted analysis, and playbook-driven response behavior in the FortiEDR 5.0 Administration Guide. Fortinet also provides current threat-intelligence context through FortiGuard Labs.

QUESTION NO: 2

Which two statements are true about the FortiEDR Threat Hunting Repository? (Choose two.)

A. It stores endpoint data for threat-hunting investigations

B. It enables centralized searches across managed endpoints

C. It directly blocks processes on a collector

D. It replaces the FortiEDR Core for policy evaluation

ANSWER: A B

Explanation:

The Threat Hunting Repository stores collected endpoint information that can be used for historical investigation and threat hunting. It enables analysts to search centrally across the organization rather than needing to examine each managed endpoint independently.

The repository supports investigation of indicators and endpoint activity, but it is not the component that enforces a block action on an endpoint. Enforcement remains the responsibility of the Collector working with the Core. See the FortiEDR 5.0 Administration Guide for Threat Hunting and architecture information.

QUESTION NO: 3

What is the primary purpose of the FortiEDR Central Manager?

A. Provide centralized administration of FortiEDR organizations and policies

B. Enforce process-blocking actions directly on endpoints

C. Store all threat-hunting telemetry

D. Perform file remediation on offline collectors

ANSWER: A

Explanation:

The FortiEDR Central Manager provides centralized administration for the FortiEDR environment. Administrators use it to manage organizations, users, collector groups, policies, and other FortiEDR configuration settings from a common management interface.

The Central Manager is an administration component. It does not replace the Core for event analysis or the Collector for endpoint monitoring and enforcement. See the FortiEDR 5.0 Administration Guide for Central Manager administration details.

QUESTION NO: 4

What does a FortiEDR threat hunting profile determine?

A. The amount and type of telemetry collected for threat hunting

B. The administrator role required to access the console

C. The classification assigned by FortiGuard Cloud Services

D. The network ports used by the Central Manager

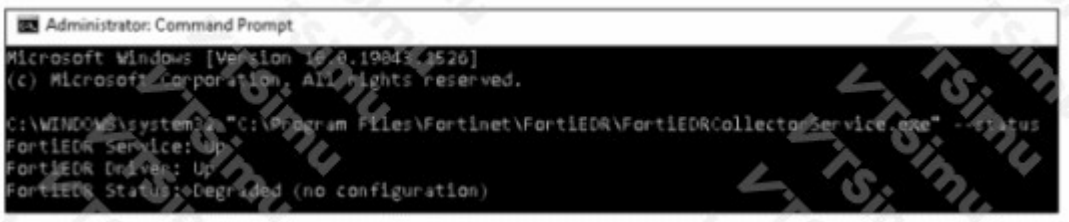
ANSWER: A

Explanation:

A threat hunting profile determines the scope of endpoint information that the FortiEDR Collector gathers for threat-hunting and investigation use. Profiles provide a balance between the amount of available telemetry and the endpoint resources required to collect it. For example, a more comprehensive profile supplies broader investigative visibility but can require more processing, storage, and bandwidth than a lighter profile. See the FortiEDR 5.0 Administration Guide for threat-hunting configuration information.

QUESTION NO: 5

Refer to the exhibit.



Based on the FortiEDR status output shown in the exhibit, which two statements about the FortiEDR collector are true? (Choose two.)

A. The collector device has windows firewall enabled

B. The collector has been installed with an incorrect port number

C. The collector has been installed with an incorrect registration password

D. The collector device cannot reach the central manager

ANSWER: B D

Explanation:

The collector has been installed with an incorrect port number, and the collector device cannot reach the central manager. FortiEDR Collectors must establish communication with their assigned Central Manager using the connection details supplied at installation or deployment, including the manager address and communication port. The status output indicates that this management connection cannot be established and identifies a port mismatch as the relevant configuration issue. Consequently, the Collector cannot complete its connection to the Central Manager. Correct Central Manager reachability is essential for Collector registration, receiving security policies, reporting events, and maintaining normal operational status. After confirming network routing and name resolution as applicable, the administrator should verify that the configured Central Manager port matches the port on which the Central Manager is listening, then confirm that the required path is reachable from the endpoint. Fortinet's FortiEDR documentation describes the Collector–Central Manager architecture and the connection configuration used by deployed Collectors. See the FortiEDR 5.0 documentation and the FortiEDR 5.0 Administration Guide.