DUMPSBOSS.

Fortinet NSE 6FortiEDR 7.0 Administrator

Fortinet NSE6_EDR_AD-7.0

Version Demo

Total Demo Questions: 4

Total Premium Questions: 43

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, FortiEDR Introduction	2
Topic 2, FortiEDR Architecture	1
Topic 3, FortiEDR Communication	4
Topic 4, FortiEDR Deployment	4
Topic 5, FortiEDR Security Policies	7
Topic 6, FortiEDR Events	5
Topic 7, FortiEDR Threat Hunting	5
Topic 8, FortiEDR Playbooks	3
Topic 9, FortiEDR Exclusions	2
Topic 10, FortiEDR Integrations	10
Total	43

QUESTION NO: 1

An analyst must repeatedly search all endpoints for a registry modification and wants a security event to be raised when the condition is found. The search must run automatically every 15 minutes. Which configuration meets this requirement? (Choose one answer)

A. A scheduled query within a threat hunting profile

B. A Communication Control policy with a recurring rule

C. An Application Control entry based on the registry path

D. A playbook action that searches the registry

ANSWER: A

Explanation:

A **scheduled query within a threat hunting profile** is correct. FortiEDR Threat Hunting allows an administrator to define filters for endpoint activity, save the query, and schedule recurring execution. A scheduled query can identify the specified registry activity across the endpoint estate and generate a security event when matching results are found.

A playbook responds to an existing event; it does not provide the recurring threat-hunting search required in this scenario. Communication Control and Application Control are enforcement features rather than scheduled endpoint-activity query mechanisms.

QUESTION NO: 2

An administrator creates an enabled Application Control entry by using only the hash of a known unwanted executable. Which two statements describe the expected matching behavior? (Choose two answers)

A. The entry can match the executable after it is copied to another directory.

B. The entry can match the executable after its file name is changed.

C. The entry matches only when the original file path is retained.

D. The entry requires a configured signer before it can be enabled.

ANSWER: A B

Explanation:

A hash-based Application Control entry identifies the specific file content represented by that hash. Therefore, the entry can match the same executable even when it is copied to a different directory or renamed. A file name and path are not required when the application definition uses the hash attribute alone.

A path-only definition is location-specific, while a file-name, path, and signer definition is evaluated using those configured attributes. Neither approach provides the same content-specific matching behavior as a hash-only entry.

QUESTION NO: 3

A company requires a global communication policy for a FortiEDR multi-tenant environment. Which recommendation must you make? (Choose one answer)

A. Create a separate communication control policy for each organization.

B. Create a new communication control policy and apply it to multiple organizations.

C. Create a new communication control policy and delegate it to other organizations.

D. Create a new communication control policy and assign it globally to all organizations.

ANSWER: A

Explanation:

Create a separate communication control policy for each organization. In a FortiEDR multi-tenant deployment, Communication Control is managed within the context of an individual organization rather than from the Hoster view. The Hoster view provides cross-organization visibility and selected centralized administration functions, but the Communication Control window is not available there. Consequently, a hoster administrator cannot define one Communication Control policy and directly apply, delegate, or assign it across every tenant organization.

The appropriate operational approach is therefore to switch to each organization and configure the required Communication Control policy independently. This keeps communication rules—such as controls over endpoint network connections—scoped to the tenant that owns the endpoints and policy configuration. It also aligns administration with FortiEDR's tenant separation model, where organization-specific settings are maintained in the applicable organization view. Fortinet's FortiEDR documentation provides the product documentation set and the Administration Guide used to manage organizations and policies: FortiEDR 7.0 documentation and FortiEDR 7.0 Administration Guide.

QUESTION NO: 4

FortiEDR IoT device discovery is enabled for a subnet containing workstations and servers. Which two Collector characteristics make a Collector suitable to participate in probing nearby devices? (Choose two answers)

A. The Collector is healthy and installed on a non-server endpoint.

B. The Collector is active on the subnet that is being probed.

C. The Collector is isolated to preserve the endpoint during investigation.

D. The Collector is installed on a server with access to all subnets.

ANSWER: A B

Explanation:

IoT probing uses suitable active Collectors to discover neighboring devices and retrieve basic information such as host name and IP address. A healthy Collector can participate in this process, while a degraded, disabled, or isolated Collector is not selected.

Collectors installed on servers are not used for IoT probing. Consequently, a healthy non-server endpoint Collector is an appropriate candidate, whereas Collector health alone is insufficient when the Collector is installed on a server.