Fortinet NSE6_EDR_AD-7.0 NSE 6 Practice Questions

Shared by Glass on 17-08-2026

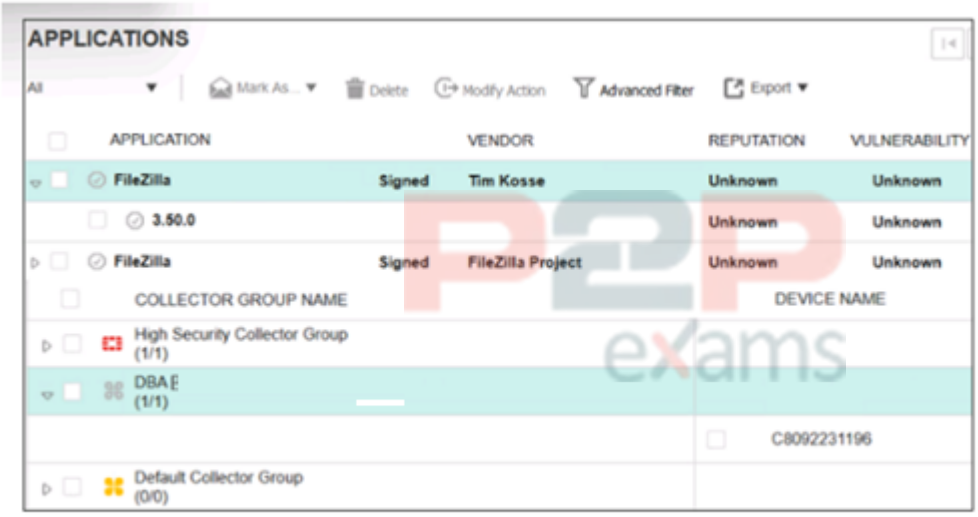
For More Free Questions and Preparation Resources

Check the Links on Last Page

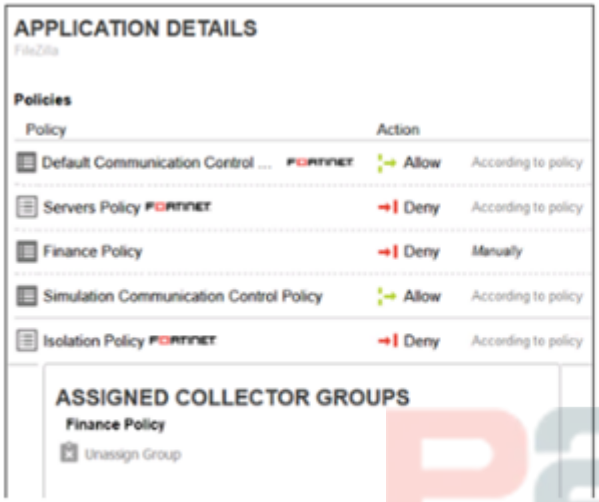
Question 1

Question Type: MultipleChoice

Refer to the exhibits.



Application Details



The application policy logs and application details are shown. Collector C8092231196 is a member of the Finance group. In this scenario, what must you do to block the FileZilla application? (Choose one answer)

Options:

A- Assign the Simulation Communication Control Policy to the DBA group.
B- Deny the application in the Finance policy.
C- Assign the Finance policy to the DBA group.
D- Assign the Finance policy to a broader collector group, such as the Default Collector Group.

Answer:

B

Explanation:

The correct answer is B. Deny the application in the Finance policy.

The FortiEDR 7.0.0 Administration Guide states that Communication Control policies define the actions to be taken for a given application or application version. It also states that each Communication Control policy applies to specific Collector Groups, and all devices that belong to those Collector Groups follow that policy. A Collector Group can be assigned to only one Communication Control policy.

In the exhibit, the Collector C8092231196 is stated to be a member of the Finance group. Therefore, to block FileZilla for that Collector, the application action must be set to Deny under the Finance policy, because that is the policy context that applies to the Collector's group.

The guide also explains that you can modify a policy action for an application/version so that the selected application is explicitly set to Allow or Deny for the relevant policy. When modified this way, the Application/Version Details area shows the action as manually changed and excluded from the original policy action.

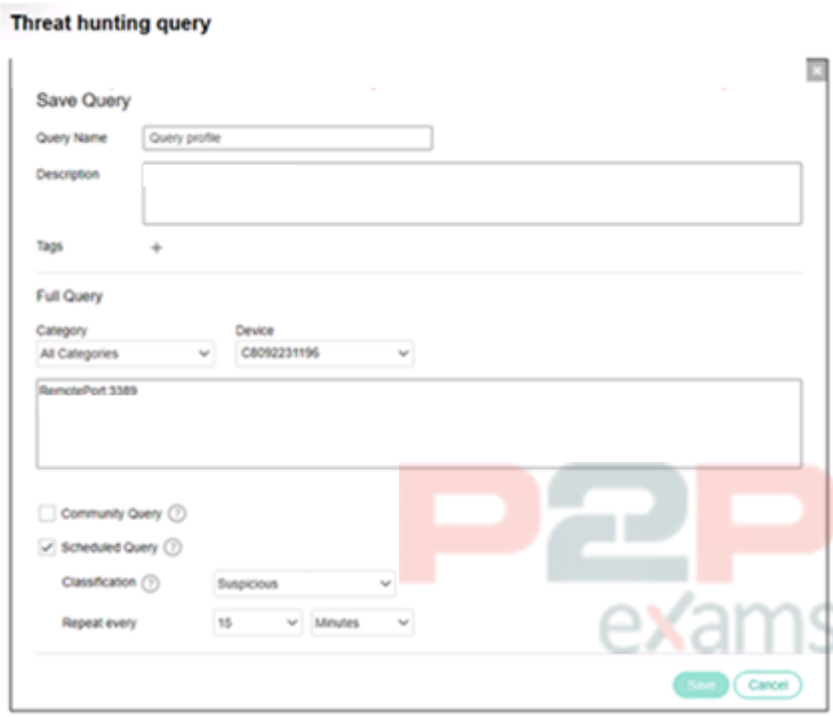
Option A is wrong because assigning a Simulation Communication Control Policy to the DBA group does not affect a Collector in the Finance group. Option C is wrong because assigning the Finance policy to the DBA group would affect DBA Collectors, not the Finance Collector in the scenario. Option D is wrong because assigning the Finance policy to a broader group such as Default Collector Group is unnecessary and could over-broaden the policy impact. The precise action is to deny FileZilla in the policy that applies to the Collector's own group: Finance policy.

=========

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



Based on the exhibit, which statement about this threat hunting query is true? (Choose one answer)

Options:

A- A security incident will be generated whenever the device attempts an RDP connection.
B- The query is limited to detecting network activity and does not inspect process behavior.
C- The query is configured as a global hunting rule and is automatically visible across all organizations.
D- RDP connections will be automatically blocked and classified as suspicious.

Answer:

A

Explanation:

The correct answer is A.

The exhibit shows a FortiEDR Threat Hunting saved query using RemotePort:3389, scoped to a specific device, with Scheduled Query enabled, classification set to Suspicious, and a repeat interval of 15 minutes. TCP port 3389 is the standard RDP port, so the query is designed to detect RDP-related network activity for the selected endpoint.

The FortiEDR guide states that saving a Threat Hunting query can define it as a scheduled query to automate threat detection. It further states that when a scheduled query runs and detects matches, a security event is automatically created in the Incidents tab, and notifications are sent according to the security event configuration.

Option B is too absolute and therefore wrong. The specific query shown uses a network field, but Threat Hunting itself can search activity events across files, registry, network, processes, and event logs. Option C is wrong because the Community Query checkbox is not selected, so it is not configured as a shared community/global query. The guide states that Community Query must be selected to share the query with the FortiEDR community, including other organizations.

Option D is wrong because a scheduled Threat Hunting query generates an incident; it does not automatically block RDP unless additional playbook actions are configured. The guide says scheduled queries generate security events and may trigger configured playbook actions, but the query itself is not a blocking control.

=========

Question 3

Question Type: MultipleChoice

A collector attempts to access a known malicious website. FortiEDR is configured for eXtended detection with FortiAnalyzer. What two roles does Fortinet Cloud Services (FCS) perform in this process? (Choose two answers)

Options:

A- FCS sends a log record to FortiAnalyzer.
B- FCS sends OS metadata to the FortiEDR manager.
C- FCS correlates and analyzes the collected logs.
D- FCS identifies if a malicious event has taken place and reports the detection incident.

Answer:

C, D

Explanation:

The correct answers are C and D.

The guide states that for eXtended Detection Source integration, FortiEDR connects to external systems to collect activity logs. The aggregated data is then sent to Fortinet Cloud Services (FCS), where it is correlated and analyzed to detect malicious indications. Those malicious indications result in security events for eXtended Detection policy rule violations.

For FortiAnalyzer/FortiAnalyzer Cloud specifically, the guide states that this integration is used

to correlate data between FortiEDR and the Fortinet Security Fabric and issue eXtended Detection alerts.

Option A is wrong because FCS does not send the original log record to FortiAnalyzer. FortiAnalyzer is the external source whose data is correlated with FortiEDR data. Option B is wrong because OS metadata is collected by the Collector and handled through FortiEDR components; the FCS role here is cloud-side enrichment, correlation, and detection, not sending OS metadata back to the manager.

==========

Question 4

Question Type: MultipleChoice

Refer to the exhibits.

What happens when the net user command runs on an endpoint? (Choose one answer)

Options:

A- It triggers an immediate endpoint alert.

B- It blocks CLI commands by default.
C- It triggers an incident when the query matches the target process (net.exe).
D- It triggers FortiEDR rules because the activity is not suspicious.

Answer:

C

Explanation:

The correct answer is C.

The exhibit shows a Threat Hunting saved query named CLI Command with the query:

Target.Process.Filename ('net.exe')

It is configured as a Scheduled Query, classified as Suspicious, and set to repeat every 15 minutes. The FortiEDR guide states that saving a Threat Hunting query allows it to be defined as a scheduled query to automate threat detection. When the scheduled query runs and detects matching activity, a security event is automatically created in the Incidents tab.

The guide also states that scheduled queries run automatically according to the configured schedule, and each time a match is detected, FortiEDR generates a security event in the Incidents tab and sends notifications according to the security event configuration.

So, when the endpoint runs:

net user edruser password! /ADD

FortiEDR records the relevant process activity, and when the scheduled query runs, it matches the target process net.exe and creates an incident/security event. It is not immediate by default because the query is scheduled every 15 minutes. It also does not block CLI commands by default unless playbook actions or policy controls are configured. The activity is treated according to the saved query classification, which in the exhibit is Suspicious.

=========

Question 5

Question Type: MultipleChoice

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)

Options:

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

Answer:

C

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.

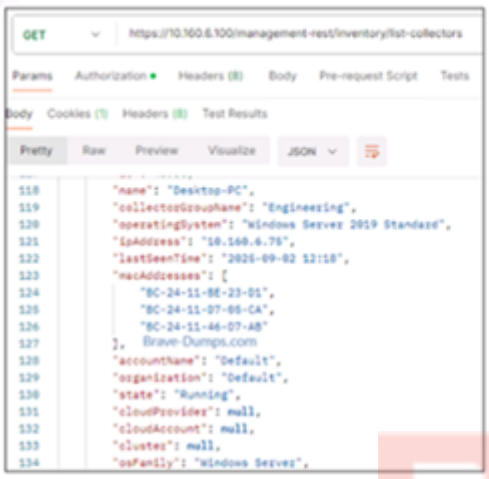
=========

Question 6

Question Type: MultipleChoice

Refer to the exhibits.

API Query Results



API Query Parameters

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? (Select one answer)

Options:

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

Answer:

A

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.

=========

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

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

Options:

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

Answer:

C, 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.

=========

Question 8

Question Type: MultipleChoice

Which two Python commands are supported when using FortiEDR Connect to directly access a protected device shell? (Select two answers)

Options:

A- %upload_file
B- %ipconfig_all
C- %psexec
D- %timestamp

Answer:

A, B

Explanation:

The correct answers are A. %upload_file and B. %ipconfig_all.

The FortiEDR 7.0.0 Administration Guide states that FortiEDR Connect opens a console that provides direct access to a FortiEDR-protected device through a remote shell connection. This allows administrators to respond to incidents, run commands and scripts, collect and download forensic data, and remediate threats. The guide also states that the FortiEDR Connect terminal has a prompt where commands can be typed, and the Help button displays the supported commands and their parameters.

The guide further confirms that FortiEDR Connect supports FortiEDR-specific commands, Windows command-line access through %cmd, and Python commands.

For the exact command list, Fortinet's official FortiEDR Connect technical tip lists the supported commands. In that list, %ipconfig_all is explicitly described as returning extended IP information, and %upload_file is explicitly described as uploading a file to the specified path. (Fortinet Community)

Options C. %psexec and D. %timestamp are not listed as supported FortiEDR Connect commands in the official Fortinet command list. Therefore, they must not be selected.

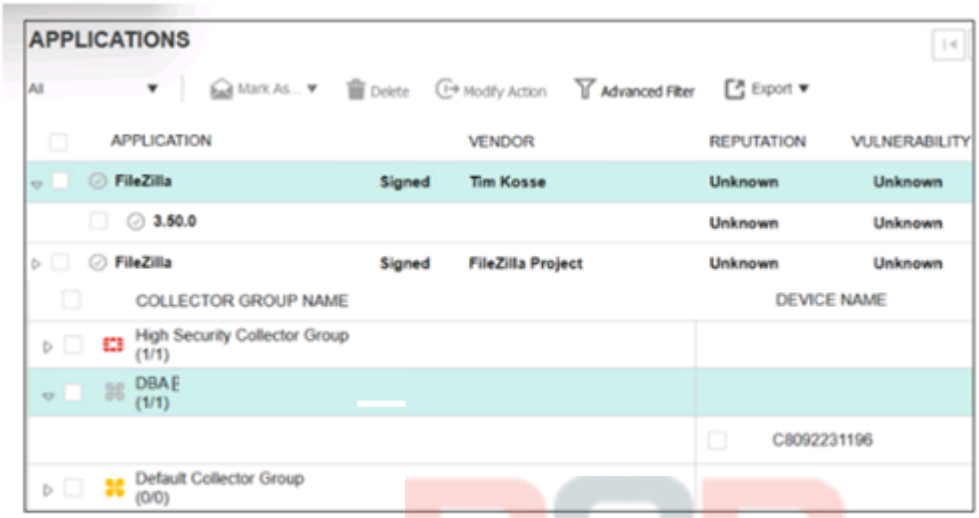
=========

=========

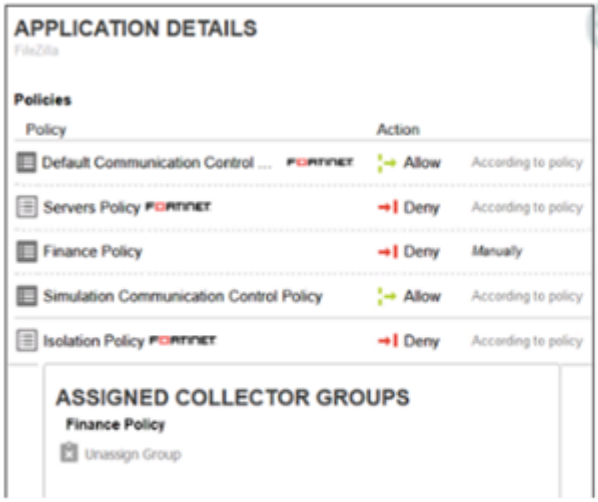
Question 9

Question Type: MultipleChoice

Refer to the exhibits.



Application Details



The application policy logs and application details are shown. Collector C8092231196 is a member of the Finance group. In this scenario, what must you do to block the FileZilla application? (Select one answer)

Options:

A- Assign the Simulation Communication Control Policy to the DBA group.
B- Deny the application in the Finance policy.
C- Assign the Finance policy to the DBA group.
D- Assign the Finance policy to a broader collector group, such as the Default Collector Group.

Answer:

B

Explanation:

The correct answer is B. Deny the application in the Finance policy.

The FortiEDR 7.0.0 Administration Guide states that Communication Control policies define the actions to be taken for a given application or application version. It also states that each Communication Control policy applies to specific Collector Groups, and all devices that belong to those Collector Groups follow that policy. A Collector Group can be assigned to only one Communication Control policy.

In the exhibit, the Collector C8092231196 is stated to be a member of the Finance group. Therefore, to block FileZilla for that Collector, the application action must be set to Deny under the Finance policy, because that is the policy context that applies to the Collector's group.

The guide also explains that you can modify a policy action for an application/version so that the selected application is explicitly set to Allow or Deny for the relevant policy. When modified this way, the Application/Version Details area shows the action as manually changed and excluded from the original policy action.

Option A is wrong because assigning a Simulation Communication Control Policy to the DBA group does not affect a Collector in the Finance group. Option C is wrong because assigning the Finance policy to the DBA group would affect DBA Collectors, not the Finance Collector in the scenario. Option D is wrong because assigning the Finance policy to a broader group such as Default Collector Group is unnecessary and could over-broaden the policy impact. The precise action is to deny FileZilla in the policy that applies to the Collector's own group: Finance policy.

=========

Question 10

Question Type: MultipleChoice

You added three new applications to FortiEDR using only the Path attribute. What are two expected outcomes of this configuration? (Select two answers)

Options:

A- These applications will be disabled until explicitly enabled.
B- Only applications in the specified directory paths will be blocked.
C- These applications will be blocked only if the file name also matches.
D- All instances of these applications will be blocked, regardless of location.

Answer:

A, B

Explanation:

The correct answers are A and B.

The FortiEDR 7.0.0 Administration Guide states that newly added applications are disabled by default, which means they are not blocked unless enabled. The guide further explains that the default state can be changed by enabling the Enable Default application state option in the Application Control Manager settings. Therefore, option A is correct.

Option B is also correct because Application Control allows an application to be defined by Hash or by any combination of File Name / Path / Signer. The guide says that the Path field specifies the path to the executable file of the application to be blocked. When using path-based matching, the enforcement is tied to the specified path criteria, not to every possible location of the same file.

Option C is wrong because the file name does not also need to match when only the Path attribute is used. Option D is wrong because blocking all instances regardless of location applies when only the File Name field is used, not when the match is path-specific. The guide explicitly states that if only the File Name field is filled, the application is blocked no matter where the executable appears.

Question 11

Question Type: MultipleChoice

A collector triggers a suspicious security incident that is initially flagged as potentially malicious. The environment is connected to the FortiEDR Cloud Service (FCS) for classification. How does FCS process the event for accurate classification? (Choose one answer)

Options:

A- By data processing, comprehensive automated analysis, and comprehensive manual analysis
B- By relying solely on the FortiGate firewall policies
C- By comparing the event against only local signatures
D- By correlating collector logs only

Answer:

A

Explanation:

The correct answer is A.

The FortiEDR 7.0.0 Administration Guide states that the FortiEDR Cloud Service (FCS) enriches and enhances system security by performing deep, thorough analysis and investigation about the classification of a security event. It determines the exact classification of security events with a high degree of accuracy.

The guide further explains that the FCS classification process is performed through data enrichment and enhanced deep analysis and investigation enabled by automated and manual processes. These processes may include intelligence services, static and dynamic file analysis, sandboxing, flow analysis through machine learning, commonality analysis, crowdsourced data deduction, and more.

Therefore, FCS does not rely only on FortiGate firewall policies, local signatures, or raw Collector log correlation. It performs enriched cloud-based automated and manual analysis to classify the incident accurately.

=========

Question 12

Question Type: MultipleChoice

You find third-party software on a user's computer that does not appear in the application list on the communication control console. Which two statements are true about this situation? (Select two answers)

Options:

A- The application has not made any connection attempts.
B- The application is blocked by the security policies.
C- The application is ignored because its reputation score is acceptable to the security policy.
D- The application is allowed in all communication control policies.

Answer:

A, D

Explanation:

The best answers are A and D, but be careful: A is directly verified by the guide; D is the only remaining statement that can be true in policy context, but it is weaker than A.

The FortiEDR 7.0.0 Administration Guide states that the Communication Control tab identifies communicating applications detected in the organization. More specifically, the Applications page lists ''all communicating applications detected in your organization that have ever attempted to communicate.'' Therefore, if software exists on a user's computer but does not appear in the Communication Control application list, the most direct explanation is that it has not attempted external communication.

The guide also explains that FortiEDR Communication Control reduces the scope of administration because Security/IT only needs to handle applications that communicate externally. It also states that non-authorized applications can still execute, and only their outgoing communication is prevented. This confirms that the Communication Control application list is not a full software inventory; it is a list of applications that have communicated or attempted communication.

Option B is not correct. If an application were blocked due to FortiEDR security-policy enforcement after a connection attempt, FortiEDR would generate security-event visibility in the Incidents workflow, not simply hide the application from Communication Control. FortiEDR Collectors send communication-related data for Communication Control, and security events are sent for enforcement/monitoring purposes.

Option C is also wrong. Reputation score affects policy decisions and application risk evaluation, but it does not cause an application to be ignored or excluded from the application list. The guide says each application in the Applications page shows a reputation indicator, which proves reputation is displayed for listed applications rather than used to hide them.

For option D, if the application has never attempted communication, Communication Control has no observed communication event to list. In exam logic, this can be interpreted as the application is not currently being denied by Communication Control policies. However, the stronger technical truth is this: Communication Control does not list installed software; it lists applications that have attempted to communicate.

=========

Question 13

Question Type: MultipleChoice

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

Options:

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.

=========