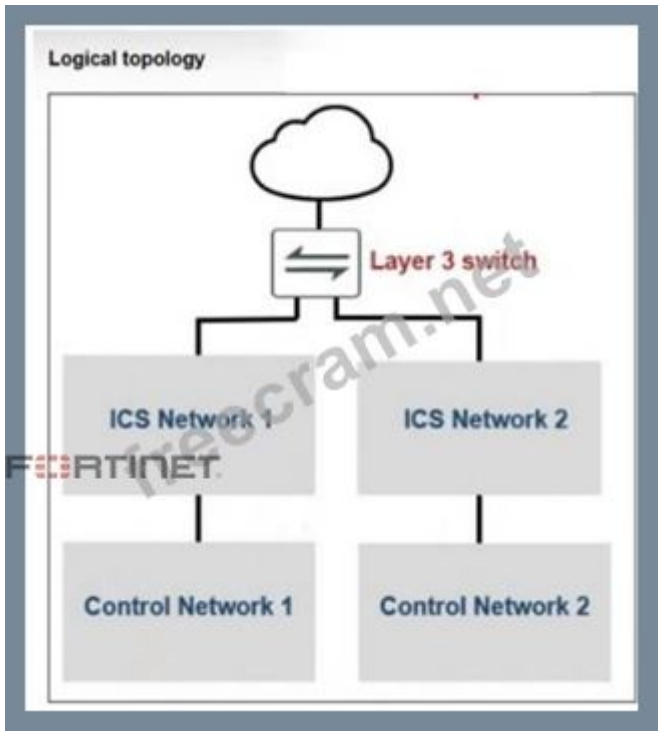
Fortinet.NSE6_OTS_AR-7.6.v2026-07-13.q17

Exam Code:	NSE6_OTS_AR-7.6
Exam Name:	Fortinet NSE 6 - OT Security 7.6 Architect
Certification Provider:	Fortinet
Free Question Number:	17
Version:	v2026-07-13
# of views:	106
# of Questions views:	174
https://www.freecram.net/torrent/Fortinet.NSE6_OTS_AR-7.6.v2026-07-13.q17.html	

NEW QUESTION: 1
Refer to the exhibit. A partial OT network is shown. You must improve the security of this OT network and implement internal segmentation between network 1 and network 2. How can you achieve the segmentation? (Choose one answer)

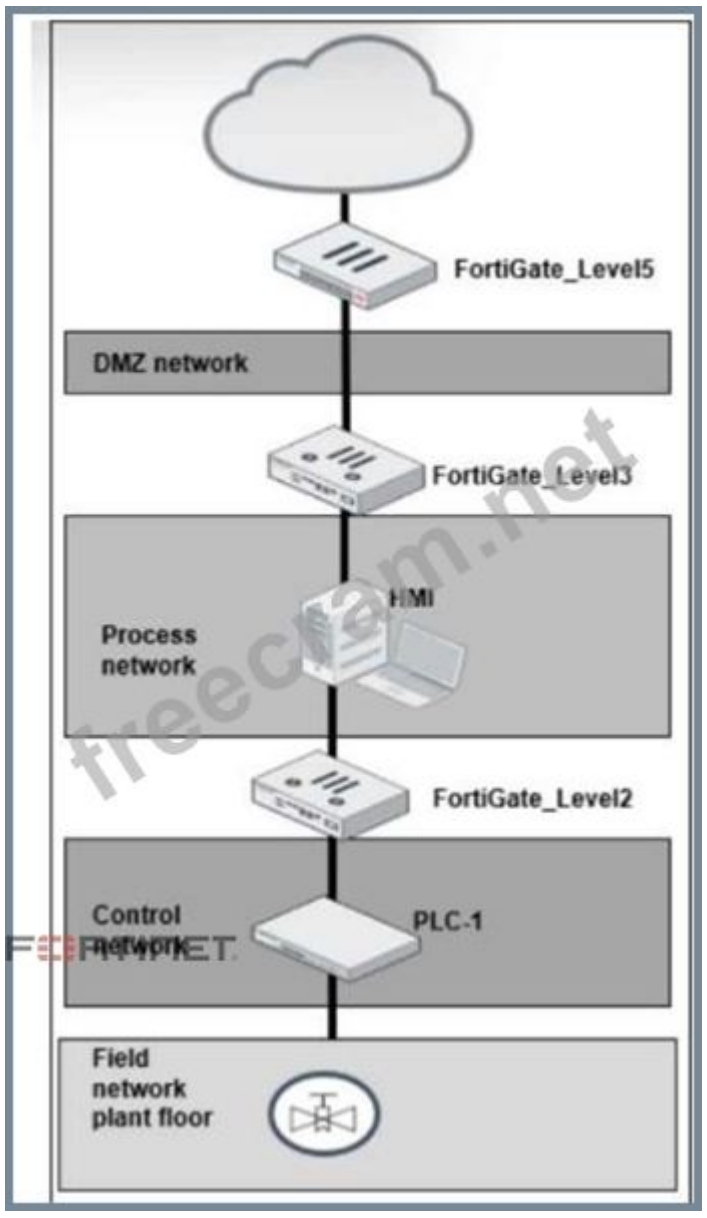


A. You can configure universal ZTNA.
B. You can configure one traffic VDOM.
C. You can configure an explicit software switch.
D. You can configure forward domain IDs for each network.
Answer: (SHOW ANSWER)
The correct answer is D. You can configure forward domain IDs for each network. The study guide explains that in FortiGate transparent mode, "all interfaces belong to the same broadcast domain, even interfaces with different VLAN IDs" and then states that you should "use this command to subdivide into multiple broadcast domains" with set forward-domain <domain_ID>. It further explains that "interfaces with the same domain ID belong to the same broadcast domain"

and "traffic arriving on one interface is broadcast only to interfaces in the same forward domain ID." This is exactly the mechanism used to separate one internal network from another and improve segmentation.
The other options do not match this requirement. Universal ZTNA is described as controlling user access to applications, not segmenting two internal OT networks. An explicit software switch is for controlling intra-switch or intra-VLAN traffic inside the same software switch broadcast domain, which is more aligned with microsegmentation than separating two routed internal networks. One traffic VDOM does not create segmentation by itself; segmentation with VDOMs requires multiple VDOMs, not one. Therefore, the best choice for segmenting network 1 and network 2 in this scenario is to assign separate forward domain IDs.

NEW QUESTION: 2
During layer 2 polling, which two pieces of information are gathered by FortiNAC to identify a device? (Choose two answers)
A. Where it was learned
B. The MAC-to-IP correlation learned
C. The system name learned
D. The time it was learned
Answer: (SHOW ANSWER)
According to the OT Security 7.6 Architect study guide section on Asset Management, specifically regarding FortiNAC Visibility:
Layer 2 Polling Data: Because each physical address is unique, FortiNAC identifies hosts as they connect to the network. The information gathered during this process fills in the physical address and location information in the database.
Visibility Components: The guide states that the physical address learned, the time it was learned, and where it was learned from provide the foundation of endpoint visibility in the form of "what, where, and when" information. This confirms that Where it was learned (Option A) and The time it was learned (Option D) are correct.
Exclusions:
Layer 3 Polling: The MAC-to-IP correlation (Option B) is explicitly defined as a function of Layer 3 polling, where the correlated IP address is added to the database record for the corresponding MAC address.
DHCP Fingerprinting: The host name or system name (Option C) and the operating system are gathered via DHCP fingerprinting, not layer 2 polling.

NEW QUESTION: 3
Refer to the exhibit.



A simplified OT network is shown. You want to optimize the protection of this OT network. Which two controls must you implement? (Choose two answers)

A. Offline IDS on FortiGate_Level3.

B. IPS on FortiGate_Level5.

C. Virtual patching on FortiGate_Level2.

D. OT signature on FortiGate_Level5.

Answer: (SHOW ANSWER)

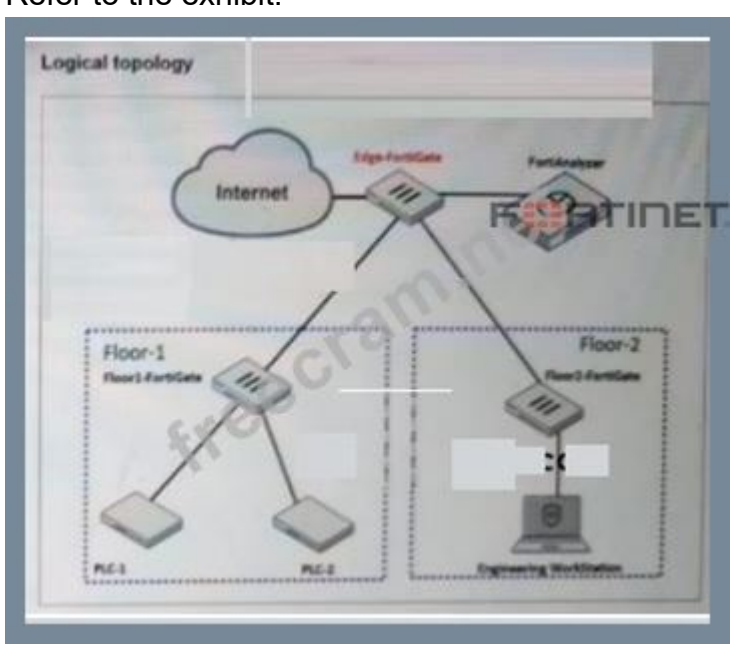
The correct answers are B. IPS on FortiGate_Level5 and C. Virtual patching on FortiGate_Level2.

The study guide explains that "the first line of defense is securing the IT side of your network" and that FortiGate should be placed to protect ICS environments and stop threats from propagating from IT into OT. It also states that IPS improves OT security because "today's threat landscape requires IPS to block a wider range of threats and improve OT security" and that in IPS mode, vulnerable devices are protected. This makes FortiGate_Level5, at the upper boundary near the DMZ and external connectivity, the correct place to implement IPS as a primary protection control.

The study guide also states in the Purdue model section that "Level 2 consists of the processes and programs that control the PLCs, RTUs, and IEDs found at Level 1" and that "it is necessary to segment, or even microsegment, these servers with firewall segmentation, along with policies that include application control and virtual patching." In addition, the virtual patching section says "Virtual patching protects OT devices that have not yet been updated against vulnerability exploits" and applies when traffic related to the vulnerable device reaches the firewall policy. Since FortiGate_Level2 sits between the process network and the control network, it is the right enforcement point for virtual patching to protect the PLC-side assets.

Option A is not one of the best answers because offline IDS only detects and logs attacks; the guide says "no traffic flows through FortiGate" in offline IDS mode, whereas IPS can actually block threats. Option D is also not the best answer because OT signatures are enabled within the IPS framework, but the stronger control explicitly described for this design is to deploy IPS at the upper boundary and virtual patching closer to vulnerable OT devices.

NEW QUESTION: 4
Refer to the exhibit.



A partial OT network is shown. You want to configure an automated alert sent by FortiAnalyzer when an attack occurs on a FortiGate device. Which two configurations must you implement? (Choose two answers)
A. You must configure a stitch on the root FortiGate.
B. You must configure a LOCALHOST task in the FortiAnalyzer playbook.
C. You must configure an intrusion prevention security profile on all FortiGate devices.
D. You must configure an event handler on FortiAnalyzer.
Answer: A,D (LEAVE A REPLY)
The correct answers are A and D. The study guide provides a direct use case called Attack Detection and Automated Alert. It states: "A downstream FortiGate detects an attack and sends logs to FortiAnalyzer. FortiAnalyzer parses the logs and notifies the root FortiGate. The root FortiGate triggers the action, which in this case, is a notification to the administrator." The same slide also explicitly shows "Stitches configured on root FortiGate." This confirms that to send the automated alert, you must configure the automation stitch on the root FortiGate.
The second required configuration is an event handler on FortiAnalyzer. The guide explains that "Event handlers generate events" and that "FortiAnalyzer uses event handlers to filter all incoming logs. If logs match the conditions configured in an event handler, FortiAnalyzer generates an event." Since FortiAnalyzer must detect the attack from the received logs before notifying the root FortiGate, an event handler is required on FortiAnalyzer.
Option B is incorrect because the study guide does not identify a LOCALHOST task as the required configuration for this attack-alert flow. Option C is also incorrect because the question asks what must be configured to enable the automated alert workflow. An IPS profile may detect some attacks, but the required automation path in the study guide is specifically event handler on FortiAnalyzer + stitch on the root FortiGate.

NEW QUESTION: 5
You want to protect OT devices that are not updated against known vulnerabilities so you apply virtual patching to the firewall policies. What must you check to confirm that the OT devices are virtually patched? (Choose one answer)
A. The output of the CLI command get virtual-patch profile

B. The OT View page
C. The output of the CLI command get rule otvp status
D. The Asset Identity List page
Answer: (SHOW ANSWER)
The correct answer is C. The output of the CLI command get rule otvp status. In the Virtual Patching section, the study guide shows the workflow where FortiGate queries FortiGuard for device-specific vulnerabilities, receives OT virtual patching signatures, maps them to the device MAC address, and then explicitly displays the CLI verification command get rule otvp status together with fields such as Rule-name, Vuln_type, and Cve. This is the direct confirmation mechanism shown in the guide for checking whether OT devices have virtual patching rules associated with them.
The other options are less accurate for confirmation. The OT View page is for Purdue-level visualization, and the Asset Identity List page shows device and asset information, but neither is presented in the guide as the command or control used to verify virtual patching status. The study guide specifically uses get rule otvp status as the status check tied to virtual patching behavior.

NEW QUESTION: 6
For the installation of your first FortiGate device, you want to minimize the impact in your OT network. Therefore, you deploy it initially as an offline IDS. Which two statements about this deployment are correct? (Choose two answers)
A. The FortiGate device acts as a network sensor.
B. The cybersecurity visibility increases with the security profiles.
C. Attacks, including zero-day attacks, are blocked.
D. OT traffic flows through the FortiGate device.
Answer: (SHOW ANSWER)
Deploying a FortiGate in offline IDS (also known as one-arm sniffer mode) is a common strategy in OT environments for several reasons found in the study guide:
Priority of Availability: In OT, availability and safety are critically important and prioritized higher than in IT. An offline IDS minimizes impact because it does not sit in the direct path of production traffic.
Network Sensor Role: In this mode, the FortiGate is connected to a mirror/SPAN port on a switch. It acts as a network sensor, receiving a copy of the traffic rather than having the traffic flow through it. This confirms Statement A is correct and Statement D is incorrect.
Passive vs. Active: The guide explicitly states that in OT environments, passive methods are preferred over active methods to avoid negatively impacting performance or causing process interruptions.
Depth of Visibility: Even though the device is offline, you apply security profiles (such as IPS, Application Control, and Antivirus) to the sniffer interface. This allows the FortiGate to analyze the copied traffic and provide deep visibility into the OT assets and their behaviors. This confirms Statement B is correct.
Detection vs. Prevention: An IDS (Intrusion Detection System) is passive; it can detect threats but cannot reset connections or drop packets to block attacks. Therefore, it cannot block zero-day attacks, making Statement C incorrect.

NEW QUESTION: 7
You want to automate some tasks in your OT network. Which three configurations are directly available in a new basic event handler on FortiAnalyzer? (Choose three answers)
A. Send alert email
B. Create a report
C. Quarantine an attacker
D. Automatically create an incident
E. Automation stitch

Answer: (SHOW ANSWER)

According to the OT Security 7.6 Architect study guide regarding FortiAnalyzer Event Management:

Notification Options: When configuring a new event handler, FortiAnalyzer provides several built-in notification methods to alert administrators when specific log criteria are met. The most common and direct method is Send alert email (Option A).

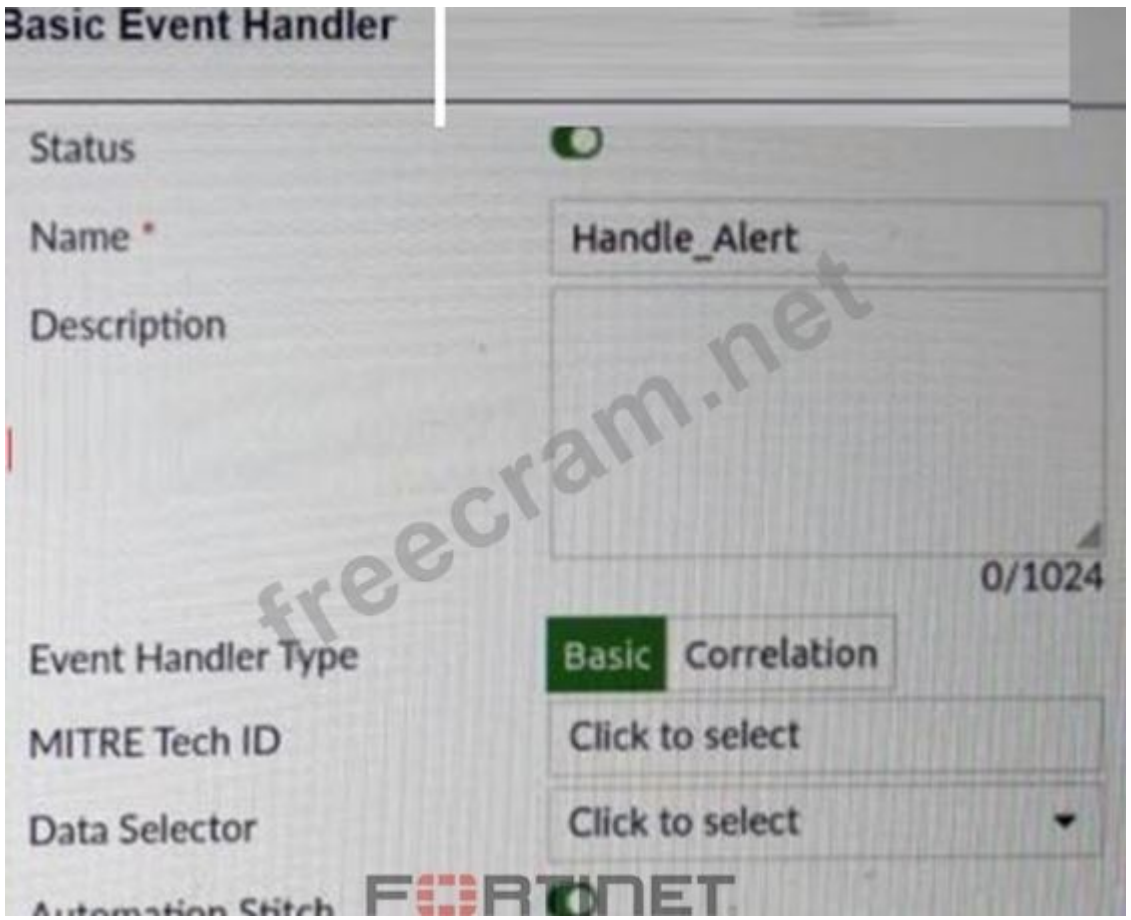
Incident Management: To streamline the SOC workflow, an event handler can be configured to Automatically create an incident (Option D) based on the triggered event. This moves the event into the Incident Manager for further analysis.

Security Fabric Integration: In the 7.6 architecture, event handlers can directly trigger an Automation stitch (Option E). This allows the FortiAnalyzer to notify the root FortiGate to take action (like running a CLI script or changing a policy) across the Security Fabric.

Exclusions: Create a report (Option B) is typically a task performed by a Playbook or a scheduled report job, not a direct setting inside the basic event handler configuration. Quarantine an attacker (Option C) is an action that results from an automation stitch or playbook, but it is not a direct configuration toggle within the event handler itself.

NEW QUESTION: 8

Refer to the exhibit.



A basic event handler is shown. You have enabled Automation Stitch to automate the handling of an alert. Which two steps must you take to use this automation stitch? (Choose two answers)

A. You must configure Action on FortiAnalyzer.

B. You must configure a Playbook task on FortiAnalyzer.

C. You must configure a FortiAnalyzer event handler trigger on FortiGate.

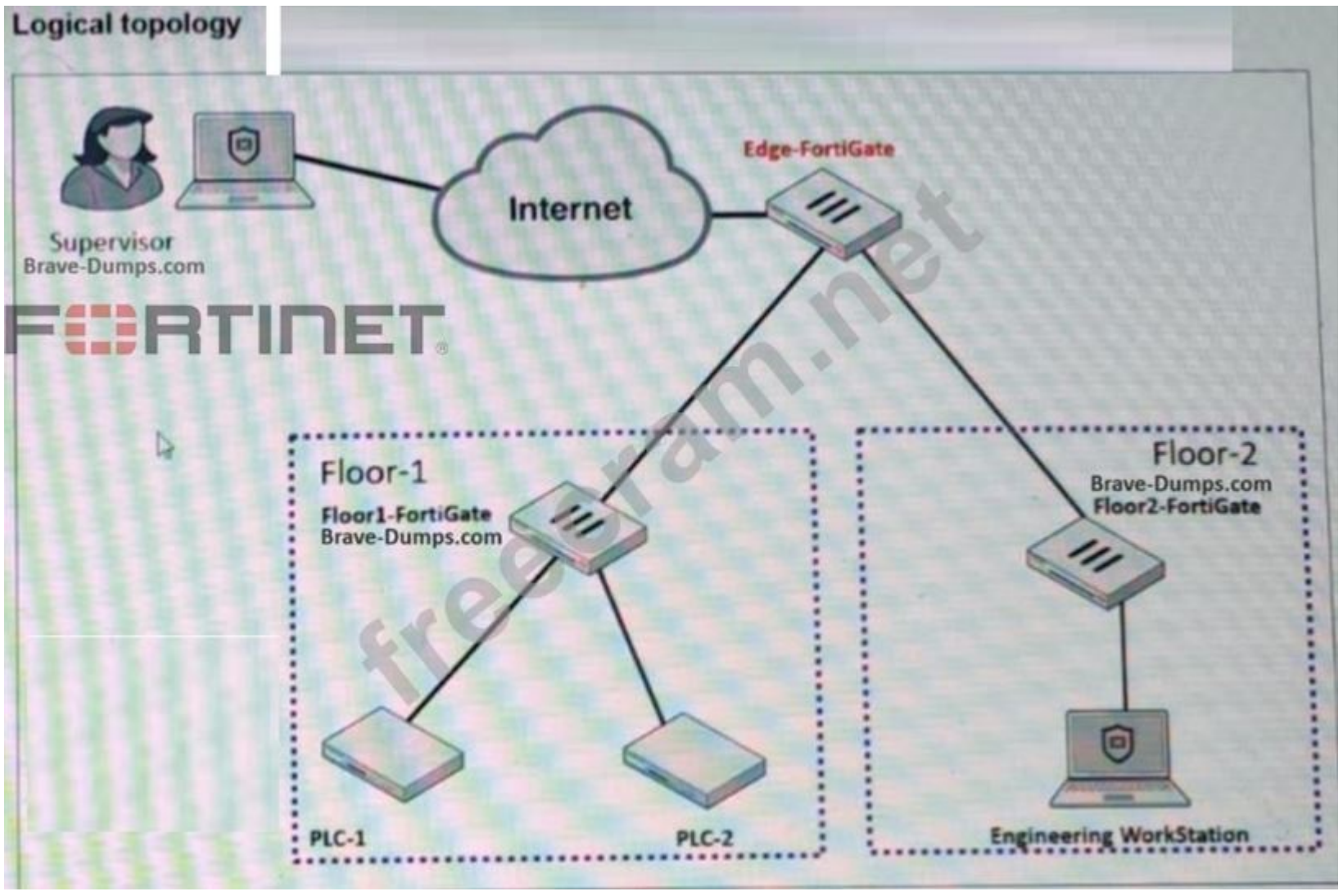
D. You must configure Rules on FortiAnalyzer.

Answer: (SHOW ANSWER)

The correct answers are C and D.

Option D is correct because the study guide states that the configuration of an event handler can include "Rules" and explains that "Rules are granular conditions" and "Event handlers can have one or more rules." It further states that "FortiAnalyzer uses event handlers to filter all incoming logs" and "If logs match the conditions configured in an event handler, FortiAnalyzer generates an event." Therefore, to use the automation stitch, you must define the rules on FortiAnalyzer so the event handler can actually generate the event that starts the automation flow.
Option C is also correct. The study guide explains that "When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification" to the FortiGate side, and in the attack-detection example it says "FortiAnalyzer parses the logs and notifies the root FortiGate" and then "The root FortiGate triggers the action." It also explicitly shows "Stitches configured on root FortiGate." This means the FortiGate must have the corresponding automation trigger configured for the FortiAnalyzer event handler notification.
Option A is incorrect because the study guide does not describe configuring an Action on FortiAnalyzer as the required step for this FortiAnalyzer-to-FortiGate automation-stitch flow. Option B is also incorrect because playbooks are a different FortiAnalyzer automation mechanism; the question specifically refers to using the Automation Stitch option in the event handler.

NEW QUESTION: 9
Refer to the exhibit.



A partial OT network is shown. You want to provide the supervisor with secure remote access. Which two features can you implement on Edge-FortiGate? (Choose two answers)
A. IPsec
B. FortiToken

C. SD-WAN
D. FSSO
Answer: (SHOW ANSWER)
Based on the exhibit and the OT Security 7.6 Architect standards for Secure Remote Access:
Secure Tunneling (Statement A): The exhibit shows a Remote PC connecting through a VPN Cloud to the Edge-FortiGate. In the Fortinet architecture, IPsec VPN is the primary method for establishing a secure, encrypted tunnel for remote administrators or supervisors to access the internal OT segments (Level 2/3) from an external location.
Multi-Factor Authentication (Statement B): Secure remote access in OT environments (aligned with IEC 62443 standards) requires strong authentication. The study guide emphasizes the use of FortiToken to provide Two-Factor Authentication (2FA) for VPN users, ensuring that compromised credentials alone are not enough to gain access to critical infrastructure.
FSSO (Statement D): Fortinet Single Sign-On is generally used for identifying internal users already on the network to apply identity-based policies; it is not the primary mechanism for establishing the remote connection itself.
SD-WAN (Statement C): While SD-WAN can manage the path of the VPN traffic, it is a WAN optimization and reliability feature, not a "secure remote access" feature for a supervisor in the context of authentication and encryption.

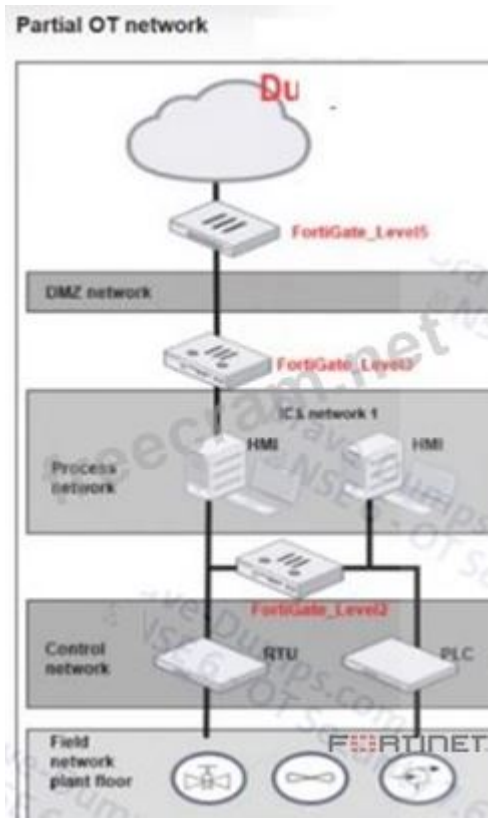
NEW QUESTION: 10
Refer to the exhibits.
Partial Basic Event Handler page

Creation of a trigger

A partial Basic Event Handler page on FortiAnalyzer and the creation of a trigger in a FortiGate device are shown. To improve the protection of your OT network, you want to automate the handling of compromised devices notified through FortiAnalyzer. You have configured an event handler named Alert_trigger as shown in the exhibit. When you create the trigger on the FortiGate device, the Event handler name field does not provide the Alert_trigger option. What two actions must you perform to make the Alert_trigger option available? (Choose two answers)
A. You must click + Create in the Event handler name field.
B. You must authorize the FortiGate device on FortiAnalyzer.

C. You must configure the FortiAnalyzer setting on the FortiGate device.
D. You must configure the trigger on the root FortiGate.
Answer: (SHOW ANSWER)
The correct answers are C and D.
Option C is correct because the study guide explains that when "a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification" and, in the Security Fabric workflow, "FortiAnalyzer parses the logs and notifies the root FortiGate." This means FortiGate must first have the FortiAnalyzer connection configured so it can consume FortiAnalyzer event handlers and use them in automation. The wizard message in the exhibit also points to this requirement by indicating that a FortiAnalyzer connection must be configured.
Option D is also correct because the study guide explicitly says that in this automation flow "the root FortiGate triggers the action" and shows "Stitches configured on root FortiGate." Therefore, if you want the FortiAnalyzer event handler to appear and be usable for automation, the trigger must be configured on the root FortiGate, not on an arbitrary downstream FortiGate.
Option A is incorrect because + Create is only a GUI control and does not solve the missing-event-handler visibility problem. Option B is not identified in the study guide as the requirement for making a FortiAnalyzer event handler available in the FortiGate automation trigger list.

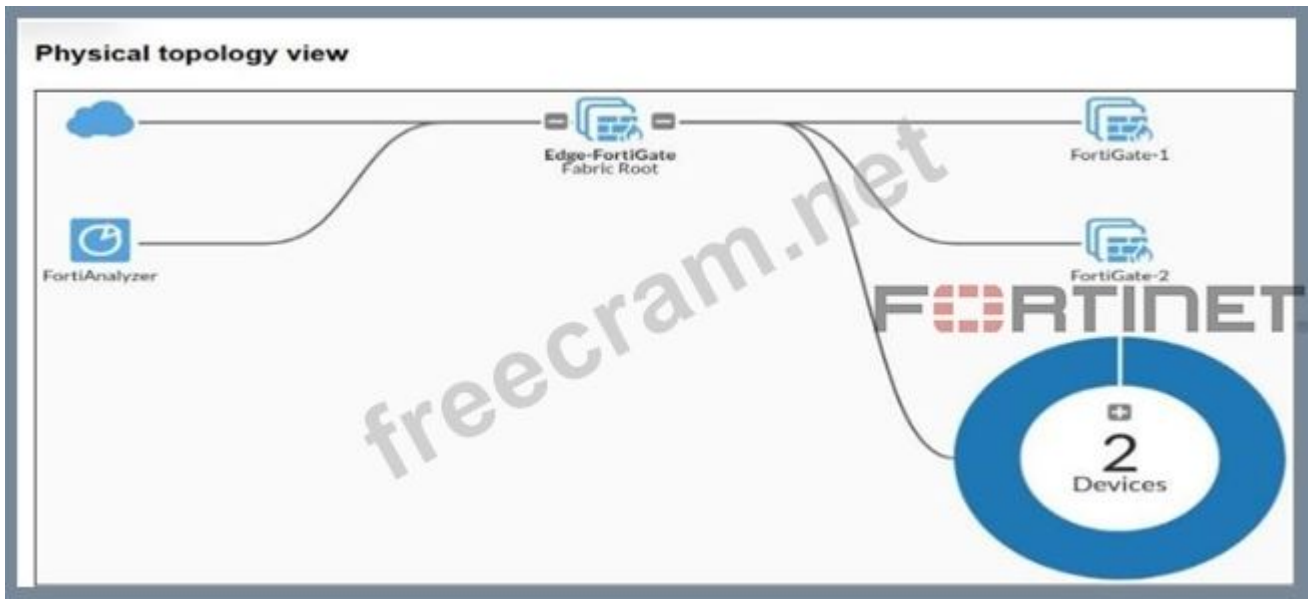
NEW QUESTION: 11
Refer to the exhibit.



A partial OT network is shown. In this OT network, you must add additional security measures to detect OT protocols and, therefore, increase the traffic visibility. Which security sensor must you implement to detect the OT protocols in this network? (Choose one answer)
A. Device detection on all the FortiGate interfaces.
B. Inline IDS on FortiGate_Level3.
C. Application sensor set to monitor on all the FortiGate devices.
D. IPS sensor on FortiGate_Level5.
Answer: (SHOW ANSWER)
The correct answer is C. Application sensor set to monitor on all the FortiGate devices.

The study guide clearly explains that application control is the feature used to identify OT protocols. It states that "application control detects the protocols used in applications like Modbus, IEC 104, and the contents of the telecontrol messages" and also says "You can use application control signatures to detect OT protocols." It further shows an example where a Modbus application control profile is enabled on a firewall policy "for OT protocol visibility in the monitor status." This directly matches the requirement in the question, which is to detect OT protocols and increase traffic visibility.
The other options do not fit the requirement as precisely. Device detection is for identifying devices and collecting endpoint information, not for detecting industrial protocols. Inline IDS and IPS are focused more on detecting or blocking attacks, exploits, protocol abnormalities, and known vulnerabilities. While IPS can inspect some OT traffic, the study guide distinguishes it from application control by stating that IPS signatures tend to detect exploits, whereas application control signatures tend to provide protocol detection at various levels. Therefore, the required security sensor for OT protocol detection and traffic visibility is the application sensor in monitor mode.

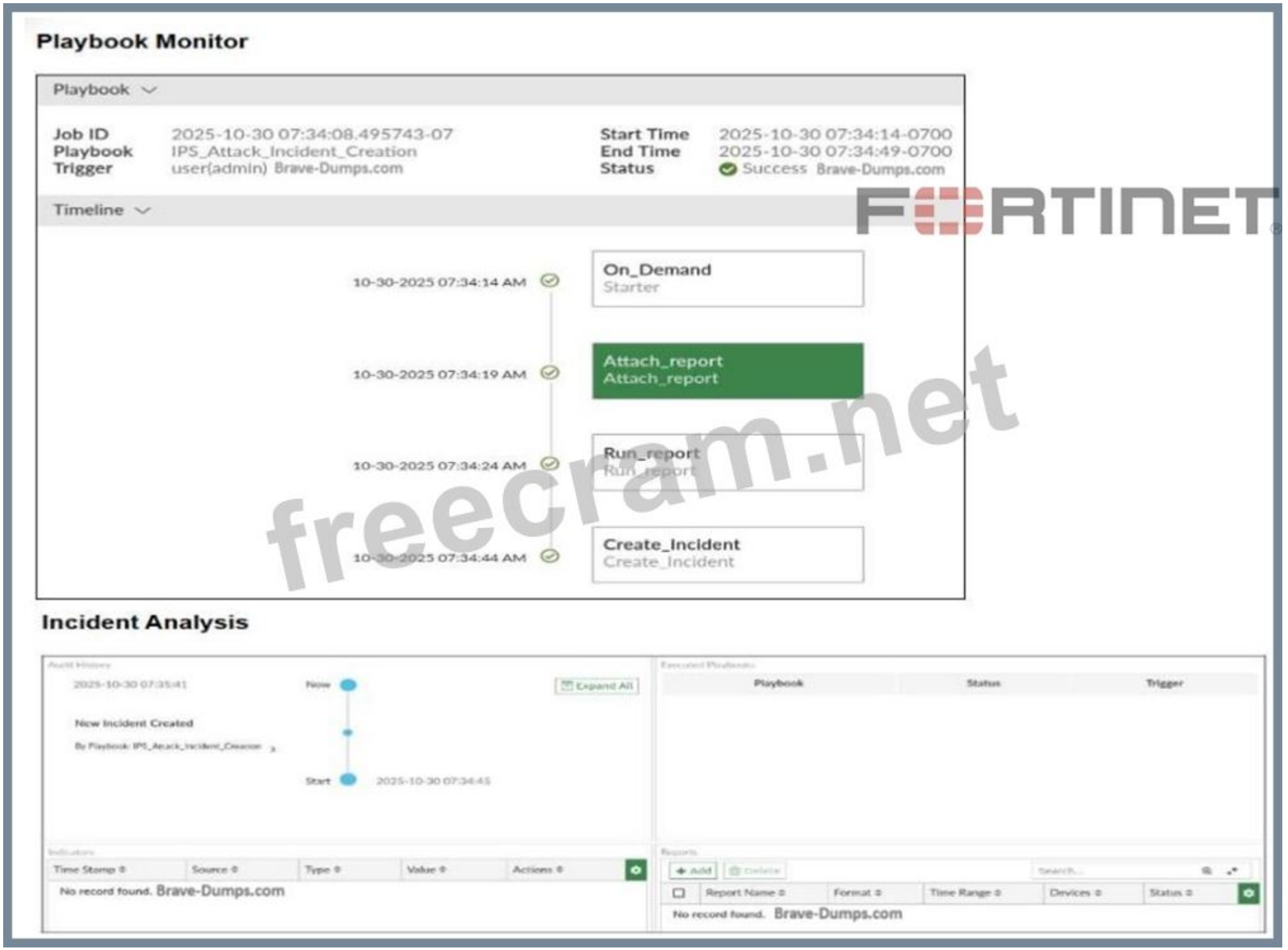
NEW QUESTION: 12
Refer to the exhibit.



Why is the OT View tab not available in the Asset Identity Center section of the FortiGate-1 device? (Choose one answer)
A. You must enable the Purdue Levels feature on the FortiGate-1 device.
B. Device Detection is not enabled on the FortiGate-1 interface.
C. The OT View tab is only available on the root FortiGate.
D. You must enable Security Fabric Connection on the interfaces of the FortiGate-1 device.
Answer: (SHOW ANSWER)
The correct answer is A. The study guide states that "The OT view is not available by default. You must enable it in the Feature Visibility section of the GUI or using the CLI command shown on this slide" and shows config system settings → set gui-ot enable. It also says that "After you enable the feature, the Asset Identity Center contains an Asset Identity List tab and an OT View tab." This directly explains why the OT View tab is missing: the feature that enables the Purdue-style OT display has not been enabled yet.
The OT View is the view that displays devices in a Purdue diagram, and the Asset Identity List also shows the current Purdue level for each device. Because the answer options do not explicitly say enable OT View in Feature Visibility, option A is the intended match, since it refers to enabling the Purdue-related OT display feature. Option B is incorrect because device detection affects visibility of devices, not whether the OT View tab exists. Option C is not supported by the study guide, and option D is also not given as the requirement for showing the OT View tab.

NEW QUESTION: 13

Refer to the exhibits.



The Playbook Monitor dashboard and the analysis of the corresponding incident analysis are shown. You created the playbook with the objective of automatically attaching the report to the incident that was created. Which two statements are correct? (Choose two answers)

A. You must wait for the report to be generated and attached to the incident.

B. Only the Create_Incident task was executed.

C. The tasks in the playbook must be reordered.

D. The playbook was triggered manually.

Answer: (SHOW ANSWER)

The correct answers are C and D.

Option D is correct because the Playbook Monitor clearly shows the starter as On_Demand and the trigger as user(admin). The study guide states that "ON_DEMAND: The playbook runs when an administrator manually starts it" and also notes that to run it manually, you select the playbook and click Run. This exactly matches the exhibit, so the playbook was manually triggered.
Option C is also correct. The study guide explains that "tasks run one after another" and that "if needed, the output of one task can be used by the tasks that follow it." It also gives an example where workflow logic matters, such as creating an incident and then attaching details to it. In the exhibit, the sequence shown is Attach_report, then Run_report, then Create_Incident, while the incident analysis shows no report attached. Since the report must exist and the incident must already be available before it can be attached properly, the task order is wrong and must be reordered.
Option B is incorrect because the monitor shows multiple tasks completed successfully, not only Create_Incident. Option A is not the best answer because the main problem demonstrated by the exhibits is not simply waiting time, but the incorrect workflow order. The playbook completed successfully, yet the report is still not attached, which indicates a design issue in the task sequence rather than just a delay.

NEW QUESTION: 14
What are two advantages provided by industrial Ethernet? (Choose two answers)
A. Encryption
B. Real-time control
C. Remote access
D. Determinism
Answer: (SHOW ANSWER)
The correct answers are B. Real-time control and D. Determinism. The study guide defines industrial Ethernet as the "use of Ethernet and TCP/IP as transport mechanisms for industrial protocols" and states that it provides "real-time control," "low latency," and "determinism (meaning reliable and predictable data delivery)" in harsh environments. It further explains that industrial Ethernet "provides deterministic communication between machine controllers, actuators, sensors, and other units." These statements directly confirm that the two key advantages are real-time control and determinism.
The other options are not supported by the study guide as core advantages of industrial Ethernet. Encryption is not listed as one of the benefits in this section, and remote access is discussed elsewhere in the OT architecture but not as a defining advantage of industrial Ethernet itself. The guide is explicit that the main benefits here are predictable delivery and real-time communication, which are essential in industrial control environments where timing and reliability matter.

NEW QUESTION: 15
Refer to the exhibit.

Event Brave-Dumps.com	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler Brave-Dumps.com	Device Name
Schneider.Electric.Modicon.	Mitigated	IPS	16	Medium	a day ago	an hour ago	Default-Malicious-Code-Detection-By-Threat	Edge-FortiGate
Triangle.Research.Nano-10.I	Mitigated	IPS	6	Medium	19 hours ago	19 hours ago	Default-Malicious-Code-Detection-By-Threat	Edge-FortiGate

Based on the information provided on the partial Event Monitor page shown in the exhibit, how was the attack detected? (Choose one answer)
A. Automatically by a stitch
B. Manually by an administrator
C. Automatically by a playbook
D. Automatically by an event handler
Answer: (SHOW ANSWER)
The correct answer is D. Automatically by an event handler. The study guide explicitly states that "Event handlers generate events on FortiAnalyzer" and "FortiAnalyzer uses event handlers to filter all incoming logs. If the logs received match the conditions set in the event handlers, FortiAnalyzer generates an

event." It also says "You can view all generated events on the Event Monitor page." This directly matches the exhibit, which is showing entries on the Event Monitor page. Therefore, the attack shown there was detected automatically through an event handler.
The guide also explains the detection flow: "FortiAnalyzer receives logs," "FortiAnalyzer parses logs," and "FortiAnalyzer generates an event if a rule is matched in an event handler." In addition, the Event Monitor view includes the Handler column, which identifies the event handler that generated the event. That is why the attack is not considered manually detected, and it is not primarily detected by a playbook or stitch. Playbooks and stitches are used for subsequent automation actions, but the event appearing in Event Monitor is created by the event handler mechanism.

NEW QUESTION: 16
Refer to the exhibits.

Log details related to the event

A partial Incident Analysis page and the log details related to the event are shown. An attack is reported on your OT network. You analyze the corresponding incident. Based on the information provided on the Incident Analysis page and the log details, which two statements are correct? (Choose two answers)

A. The attack uses the Modbus protocol.

B. The attack is mitigated.

C. The attack uses the IEC 104 protocol.

D. The event severity is high.

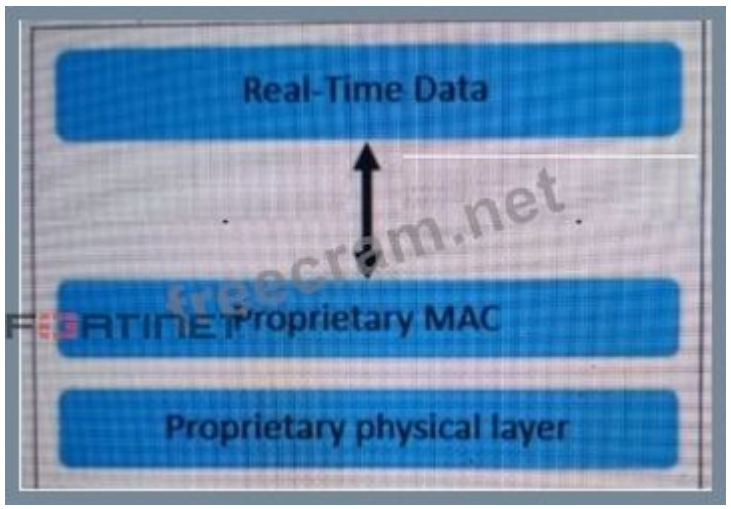
E. The target device IP address is 10.1.5.20.

Answer: (SHOW ANSWER)

Based on the technical data provided in the exhibits and the OT Security 7.6 Architect curriculum:

Industrial Protocol Identification (Statement A): The log details exhibit clearly shows that the Destination Port used in the attack is 502. According to the study guide's section on Industrial Protocol Protection, the standard port used by the Modbus TCP protocol is 502. Furthermore, the attack name identifies a "Triangle.Research.Nano-10.PLC," which are industrial controllers commonly utilizing Modbus for communications.
Attack Mitigation (Statement B): The log details specify that the Action taken by the FortiGate (Edge-FortiGate) was dropped. In cybersecurity and Fortinet fabric operations, dropping a packet associated with an IPS signature means the traffic was blocked from reaching its target, thereby mitigating the attack.
Target IP Address (Statement E): The log detail explicitly lists the Destination IP as 192.168.2.3. The Incident Analysis page also titles the incident with dstip:192.168.2.3. While the "Affected Endpoint" is shown as 10.1.5.20, in an "outgoing" attack direction (as shown in the log), this likely refers to the internal source/attacker IP, whereas the target is the destination IP (192.168.2.3). Thus, Statement E is incorrect.
Protocol Conflict (Statement C): The IEC 104 protocol typically utilizes port 2404. Since the log specifies port 502, Statement C is incorrect.
Severity Distinction (Statement D): While the Incident severity is marked as High, the question specifically asks about event severity. The "Events" table at the bottom of the Incident Analysis page shows a "User login/logout failed" event with a medium severity. Because there is a distinction in the management console between the severity of individual events and the aggregated incident, and Statement A and B are technically definitive based on port and action, A and B are the correct architectural choices.

NEW QUESTION: 17
Refer to the exhibit.



An industrial Ethernet protocol skipping layers 3 to 6 is shown. Which industrial Ethernet protocol is it? (Choose one answer)
A. POWERLINK
B. Ethernet over industrial protocol
C. Modbus
D. EtherCAT
Answer: (SHOW ANSWER)

The correct answer is D. EtherCAT. The study guide explicitly states under the Ethernet/IP and EtherCAT section that "EtherCAT is a protocol that offers real-time communication in a primary-secondary configuration" and "EtherCAT skips layers 3 to 6 to deliver real-time communication." It also adds that "the most important feature of this protocol is that secondary devices collect only the information they need from the data packets." This matches the exhibit exactly, where the diagram shows Real-Time Data above a Proprietary MAC and Proprietary physical layer, reflecting the protocol structure that bypasses the intermediate OSI layers.
The other options do not match this behavior. The guide says POWERLINK uses layer 2 and layer 7 of the OSI model, not that it skips layers 3 to 6. It also explains that Ethernet/IP is the industrial protocol based entirely on Ethernet standards and adapts to the OSI model. Modbus is described as an open client/server protocol and is not suitable for transmitting data in real time. Therefore, the protocol in the exhibit is clearly EtherCAT.