Fortinet.NSE6_OTS_AR-7.6.v2026-05-16.q53

Exam Code:	NSE6_OTS_AR-7.6
Exam Name:	Fortinet NSE 6 - OT Security 7.6 Architect
Certification Provider:	Fortinet
Free Question Number:	53
Version:	v2026-05-16
# of views:	161
# of Questions views:	530
https://www.freepdfdumps.com/Fortinet.NSE6_OTS_AR-7.6.v2026-05-16.q53.html	

NEW QUESTION: 1
What are two critical tasks the OT network auditors must perform during OT network risk assessment and management? (Choose two.)
A. Planning a threat hunting strategy
B. Implementing strategies to automatically bring PLCs offline
C. Creating disaster recovery plans to switch operations to a backup plant
D. Evaluating what can go wrong before it happens
Answer: A,D (LEAVE A REPLY)
Planning a threat hunting strategy is essential for proactively searching for threats and vulnerabilities in the OT environment before they manifest into attacks.
Evaluating what can go wrong before it happens is a core part of risk assessment, involving the identification and analysis of potential risks and their impacts on OT systems.
Implementing strategies to automatically bring PLCs offline is generally not a responsible or safe approach in OT environments because it could disrupt critical industrial processes.
Creating disaster recovery plans is important for overall business continuity but is not primarily a task of auditors during risk assessment-it is more of a broader business continuity or incident response responsibility.

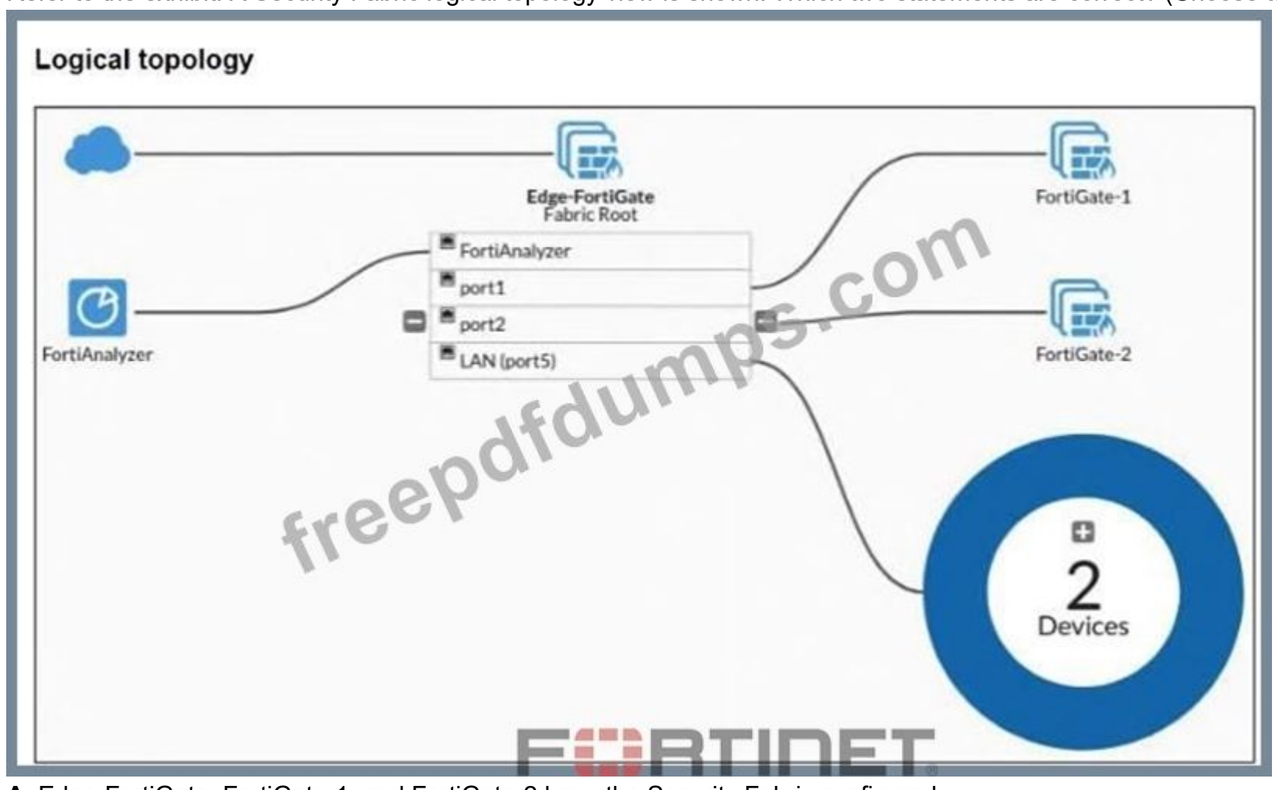
NEW QUESTION: 2
What is the main difference between real-time logs and historical logs on FortiAnalyzer?
A. Real-time logs are indexed in the SQL database, but historical logs are not.
B. Real-time logs are indexed while historical logs are compressed in the SQL database.
C. Historical logs are compressed and real-time logs are indexed in the SQL database.
D. Historical logs are indexed in the SQL database, but real-time logs are not.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
You want to monitor the performance of your specific OT sensors. Where must you fine-tune the event handling for these sensors on FortiSIEM?
A. In the Risk Summary section on the Dashboard tab
B. In the rule on the Resources tab
C. In the Investigation section on the Analytics tab
D. In the business services group on the CMDB tab

Answer: B (LEAVE A REPLY)
Fine-tuning event handling for specific sensors in FortiSIEM is done within the rule configuration, where conditions, thresholds, and logic are adjusted to control how events are generated and processed.

NEW QUESTION: 4
In an operation technology (OT) network. FortiAnalyzer is used to receive and process logs from responsible FortiGate devices.
Which statement about why FortiAnalyzer is receiving and processing multiple log messages from a given programmable logic controller (PLC) or remote terminal unit (RTU) is true?
A. To track external threats and prevent them attacking the OT network.
B. To isolate PLCs or RTUs in the event of external attacks
C. To help OT administrators troubleshoot and diagnose the OT network
D. To determine which type of messages from the PLC or RTU causes issues in the plant.
Answer: C (LEAVE A REPLY)
FortiAnalyzer is designed to collect and process logs from devices in the OT network, such as PLCs and RTUs, to provide actionable insights. By receiving and analyzing these log messages, FortiAnalyzer helps OT administrators troubleshoot and diagnose issues in the network. This includes identifying abnormal behavior, performance issues, or security threats, which are critical for maintaining the operational integrity and reliability of the OT environment.

NEW QUESTION: 5
Refer to the exhibit. A Security Fabric logical topology view is shown. Which two statements are correct? (Choose two.)



A. Edge-FortiGate, FortiGate-1, and FortiGate-2 have the Security Fabric configured.
B. Device detection is enabled on port5 of the Edge-FortiGate device.
C. FortiAnalyzer is connected only to Edge-FortiGate.

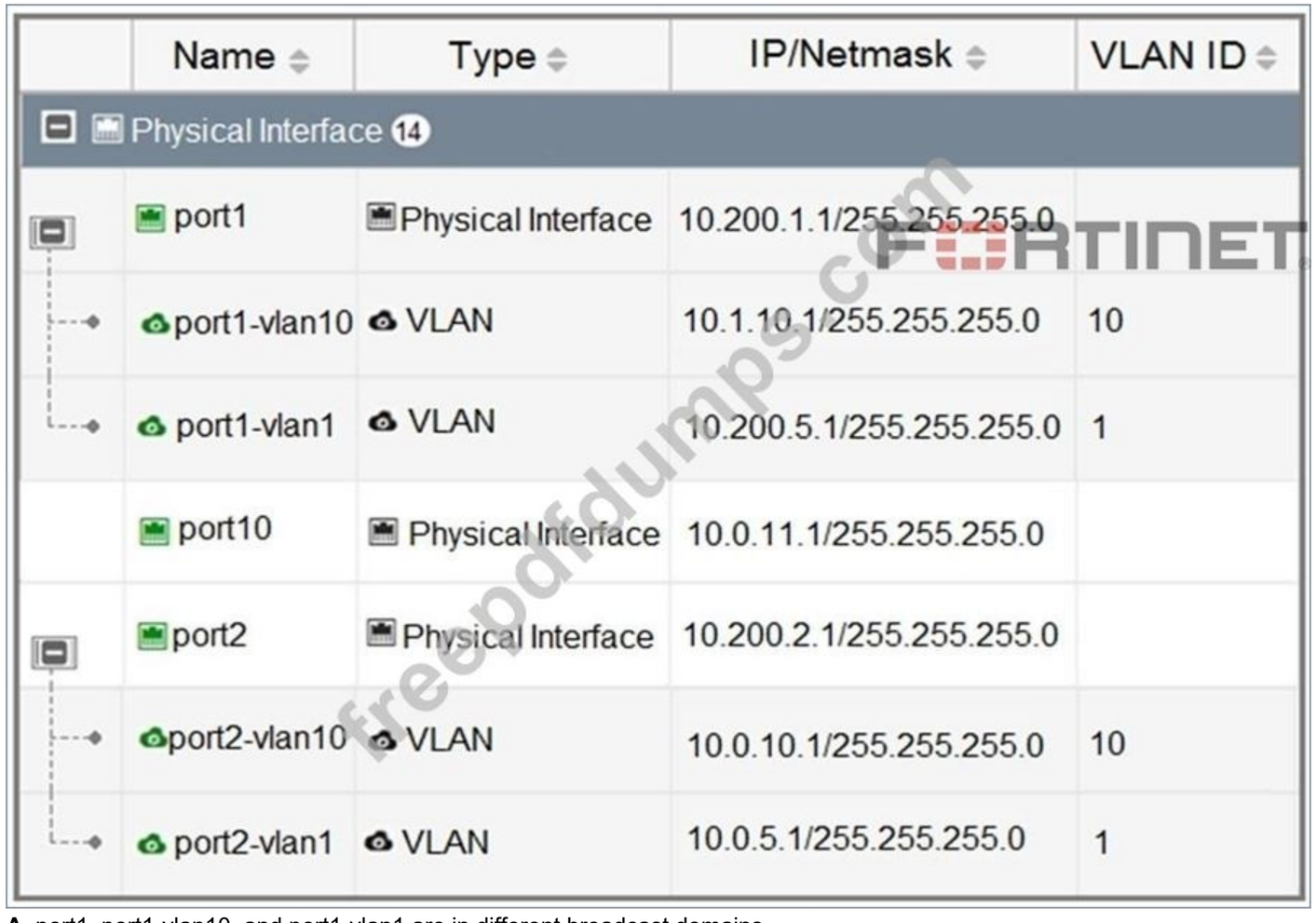
D. FortiAnalyzer has the Security Fabric configured.

Answer: B,C (LEAVE A REPLY)

The topology shows two detected devices grouped behind LAN (port5), which indicates device detection is enabled on port5 of the Edge-FortiGate. It also shows FortiAnalyzer linked directly only to the Edge-FortiGate, not as a separate Security Fabric member connected to the downstream FortiGates.

NEW QUESTION: 6

Refer to the exhibit. Which statement about the interfaces shown in the exhibit is true?



A. port1, port1-vlan10, and port1-vlan1 are in different broadcast domains

B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain

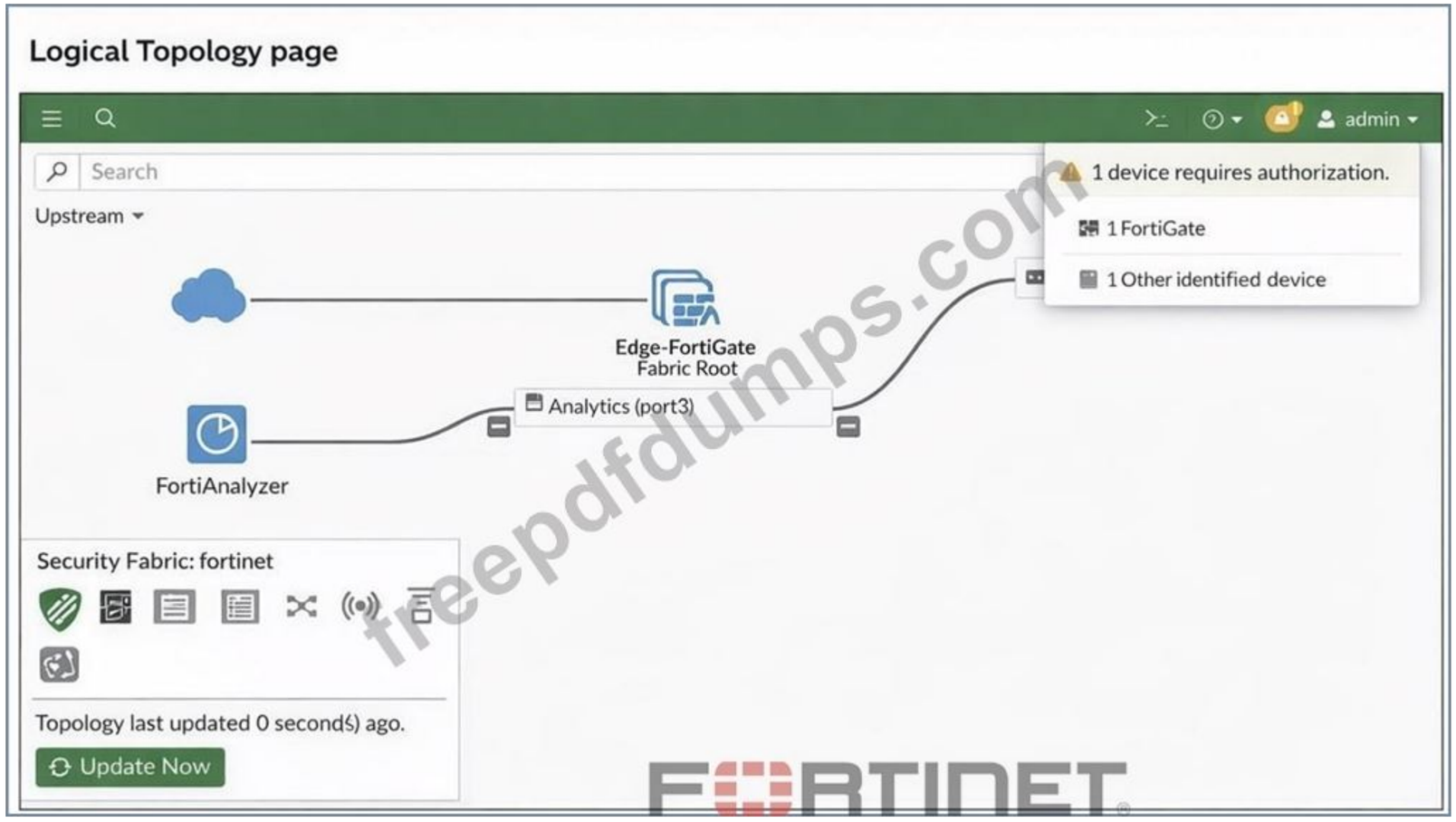
C. The VLAN ID of port1-vlan1 can be changed to the VLAN ID 10.

D. port2, port2-vlan10, and port2-vlan1 are part of the software switch interface.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 7

Refer to the exhibit. A Logical Topology page of a FortiGate device is shown.



Your OT company wants to gain visibility into the network. You decide to implement device detection with the Security Fabric.

Based on the exhibit, which statement is correct? (Choose one answer)

A. Device Detection is enabled on port3.

B. Device Detection is enabled on the other identified device.

C. The other identified device must be authorized on FortiAnalyzer.

D. The other identified device must be authorized on the root FortiGate.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 8

Which three Fortinet products can you use for device identification in an OT industrial control system (ICS)? (Choose three.)

A. FortiSIEM

B. FortiManager

C. FortiAnalyzer

D. FortiGate

E. FortiNAC

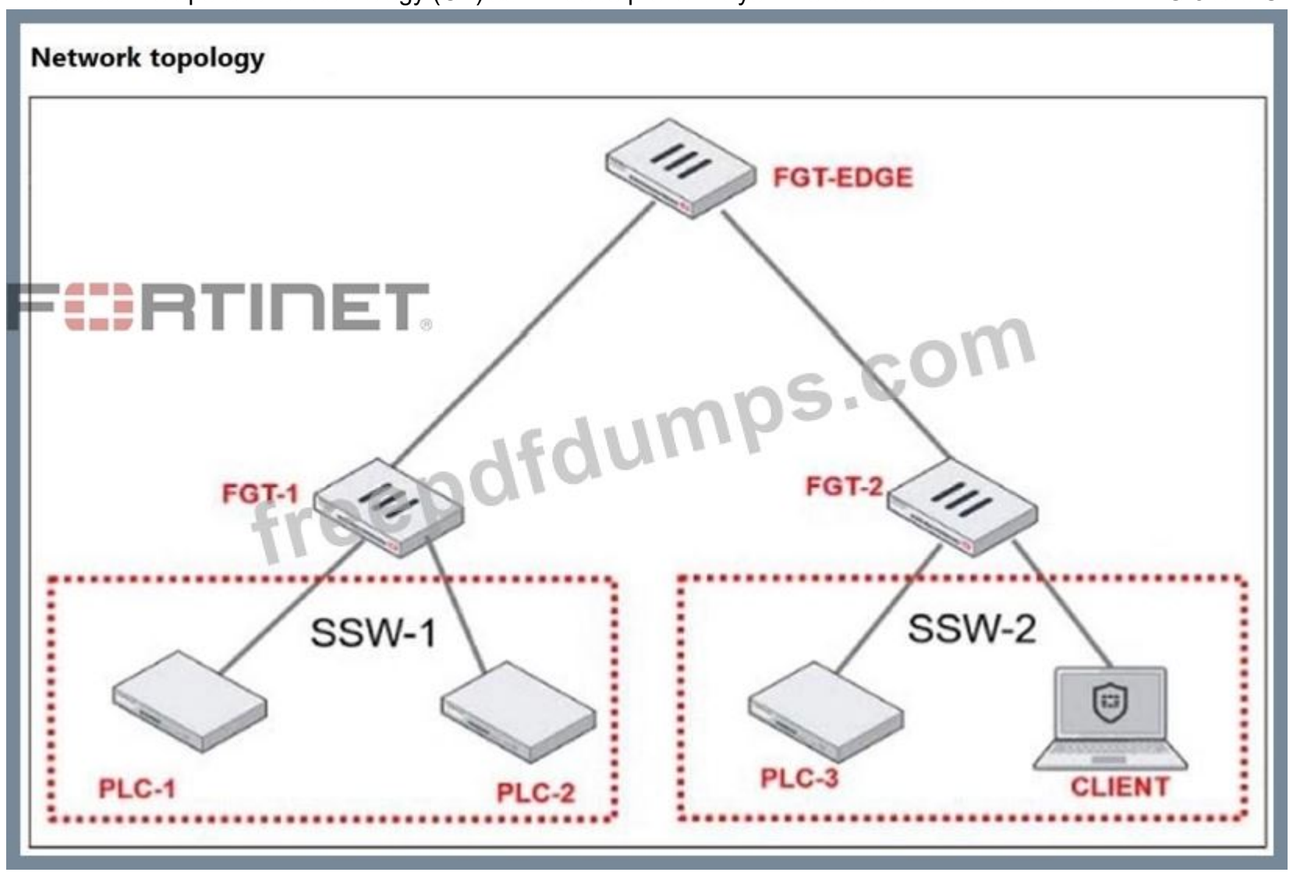
Answer: A,D,E (LEAVE A REPLY)

FortiNAC continuously collects identity records, profiles, and classifies devices in OT networks using a variety of methods including active and passive scanning.

FortiGate contributes by providing session and flow data that helps in device identification and classification.
FortiSIEM aggregates security and operational data from various sources including FortiGate and FortiNAC to provide comprehensive visibility and identification.

NEW QUESTION: 9
Which two of the following features do most industrial protocols lack? (Choose two.)
A. Real-time data exchange
B. Deterministic timing
C. TLS encryption
D. Authentication
Answer: (SHOW ANSWER)
Most legacy OT/industrial protocols were built for speed and determinism, not security, so they typically omit built-in TLS encryption and authentication mechanisms.

NEW QUESTION: 10
Refer to the exhibit. PLC-3 and CLIENT can send traffic to PLC-1 and PLC-2. FGT-2 has only one software switch (SSW-2) connecting both PLC-3 and CLIENT. PLC-3 and CLIENT can send traffic to each other at the layer 2 level.
What must the operational technology (OT) admin do to prevent layer 2-level communication between PLC-3 and CLIENT?

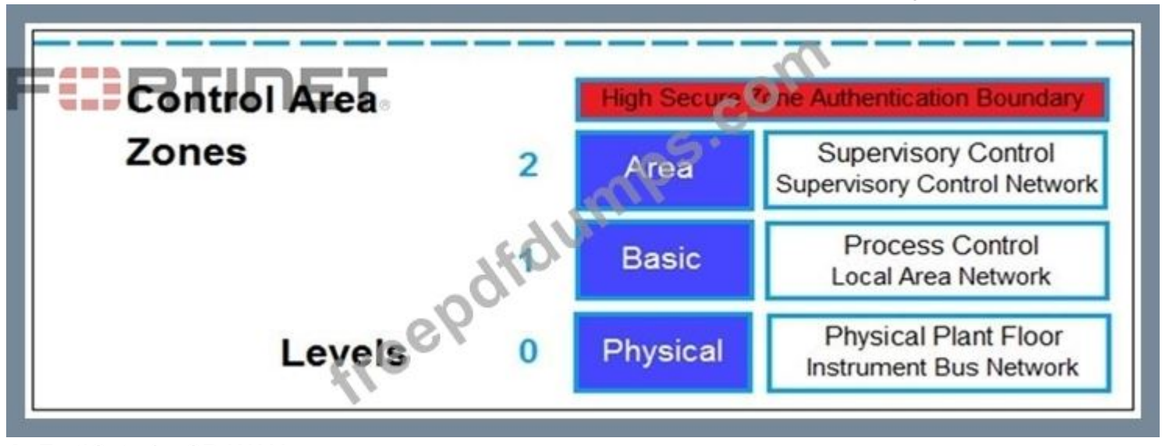


A. Set a unique forward domain for each interface of the software switch.
B. Create a VLAN for each device and replace the current FGT-2 software switch members.

C. Enable explicit intra-switch policy to require firewall policies on FGT-2.
D. Implement policy routes on FGT-2 to control traffic between devices.
Answer: (SHOW ANSWER)
Set the software switch to explicit intra-switch policy so traffic between its member ports must pass through FortiGate policies instead of being bridged at Layer 2. This stops PLC-3 and CLIENT from communicating directly at L2.

NEW QUESTION: 11
A supervisor is configuring a software switch on a FortiGate device. What must the supervisor configure on FortiGate to control the traffic between member interfaces on the software switch, using firewall policies?
A. The supervisor must add different VLAN interfaces to the software switch.
B. The supervisor must configure a separate forward domain for the software switch.
C. The supervisor must configure the software switch with at least one wireless interface and one VLAN interface.
D. The supervisor must configure intra-switch-policy to explicit.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Refer to the exhibit. Based on the Purdue model, which three measures can be implemented in the control area zone using the Fortinet Security Fabric? (Choose three.)



A. FortiGate for SD-WAN
B. FortiGate for application control and intrusion prevention system (IPS)
C. FortiNAC for network access control
D. FortiSIEM for security incident and event management
E. FortiEDR for endpoint detection
Answer: B,C,E (LEAVE A REPLY)
FortiGate for application control and intrusion prevention system (IPS): In the control area zones, FortiGate can provide critical security measures such as application control and intrusion prevention. This helps detect and prevent unauthorized activities and threats targeting the OT network.
FortiNAC for network access control: FortiNAC can be used to enforce network access policies, ensuring that only authorized devices and users can access specific zones within the control area, thereby reducing the risk of unauthorized access or breaches.
FortiSIEM for security incident and event management: FortiSIEM provides centralized monitoring and analysis of security incidents and events across the OT environment. It helps to identify potential threats, improve visibility, and ensure quick responses to security incidents.

NEW QUESTION: 13
Refer to the exhibit. An operational technology (OT) network security audit concluded that the application sensor does not block the IEC.60870.5.104_Information.Trasfer.C.BO.NA.1 signature.
Which change must the OT network administrator make?

Application control

New Application Sensor

110 Cloud Applications require deep inspection.
0 policies are using this profile.

Name: Allow_IEC-104_Transfer

Comments: 0/255

Categories

All Categories

Business (153, 6)	Cloud.IT (67, 1)	Collaboration (267, 16)	Email (77, 12)
Game (86)	General.Interest (236, 9)	Industrial (225)	Mobile (3)
Network.Service (333)	P2P (56)	Proxy (180)	Remote.Access (97)
Social.Media (117, 30)	Storage.Backup (161, 19)	Update (49)	Video/Audio (153, 17)
VoIP (23)	Web.Client (24)	Unknown Applications	

Network Protocol Enforcement

Application and Filter Overrides

+Create New | Edit | Delete

Priority	Details	Type	Action
1	IEC.60870.5.104_Information.Transfer IEC.60870.5.104_Control.Functions IEC.60870.5.104_Control.Functions.STARTDT.ACT IEC.60870.5.104_Control.Functions.STARTDT.CON	Application	Monitor
2	IEC.60870.5.104_Information.Transfer.C_BO_NA_1	Application	Block

FORTINET

A. Set all application categories to apply default actions.
B. Change the security action of the industrial category to monitor.
C. Update the priority of the C.BO.NA.1 signature override to 1.
D. Remove IEC.60870.5.104_Information.Transfer.C.BO.NA.1 from the first filter override.
Answer: C (LEAVE A REPLY)
The current configuration assigns priority 2 to the
IEC.60870.5.104_Information.Transfer.C.BO.NA.1 application signature and sets it to Block.
Priority 1 contains broader IEC.60870.5.104_Information.Transfer entries set to Monitor, which overrides the block action due to higher priority. To ensure that the C.BO.NA.1 signature is blocked, it must have higher priority than the general monitoring rule.

NEW QUESTION: 14
Which three device profiling methods of FortiNAC are considered non-direct? (Choose three.)
A. TCP
B. SSH
C. Network traffic
D. IP range
E. Location
Answer: (SHOW ANSWER)

NEW QUESTION: 15
An OT administrator configured and ran a default application risk and control report in FortiAnalyzer to learn more about the key application crossing the network. However, the report output is empty despite the fact that some related real-time and historical logs are visible in the FortiAnalyzer.
What are two possible reasons why the report output was empty? (Choose two.)
A. The administrator selected the wrong logs to be indexed in FortiAnalyzer.
B. The administrator selected the wrong hcache table for the report.
C. The administrator selected the wrong time period for the report.
D. The administrator selected the wrong devices in the Devices section.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 16
Refer to the exhibit. You are creating a new operational technology (OT) rule to monitor Modbus protocol traffic on FortiSIEM.
Which action must you take to ensure that all Modbus messages on the network match the rule?

A new OT rule

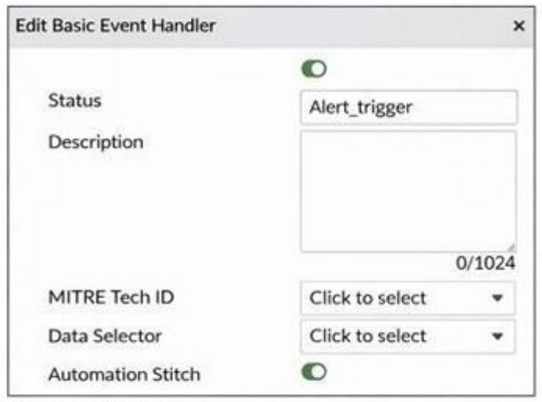
A. The condition on the SubPattern filter must use the AND logical operator.
B. Add a new condition to filter Modbus traffic based on the source TCP/UDP port.
C. In the Group By section, remove all attributes that are not configured in the Filter section.
D. In the Aggregate section, set the attribute value to equal to or greater than 0.
Answer: D (LEAVE A REPLY)
The current Aggregate condition is set to COUNT(Matched Events) >= 1, which only triggers the rule after at least one event. To ensure all Modbus messages (including the first one) match the rule, the condition must be >= 0, so every event is considered, including the very first occurrence.

NEW QUESTION: 17
As an OT network administrator, you are managing three FortiGate devices that each protect different levels on the Purdue model. To increase traffic visibility, you are required to implement additional security measures to detect protocols from PLCs.
Which security sensor must you implement to detect protocols on the OT network?

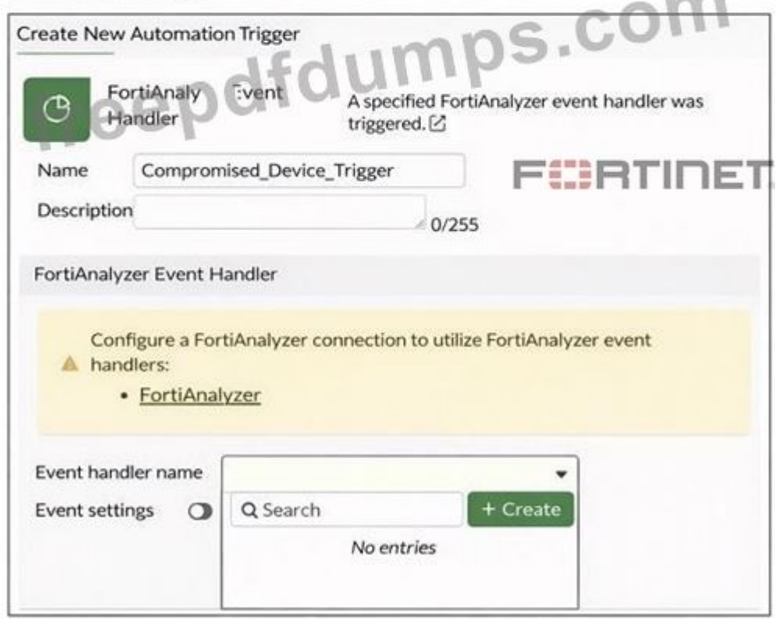
A. Intrusion prevention system (IPS)
B. Deep packet inspection (DPI)
C. Antivirus inspection
D. Application control (AC)
Answer: A (LEAVE A REPLY)
The FortiGuard Operational Technology (OT) Security Service for FortiGate combines IPS and application control signatures tailored to OT environments, enabling detection and protection of OT-specific protocols and threats.
IPS is essential for detecting network-level threats and protocols associated with OT devices including PLCs.
Deep packet inspection (DPI) is part of the traffic analysis process but the primary sensor for detecting specific OT protocols is IPS.
Antivirus and application control are generally less focused on protocol detection for OT networks compared to IPS.

NEW QUESTION: 18
Refer to the exhibits. A partial Basic Event Handler page on FortiAnalyzer and the creation of a trigger in a FortiGate device are shown.

Partial Basic Event Handler page



Creation of a trigger



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 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 configure the FortiAnalyzer setting on the FortiGate device.

B. You must configure the trigger on the root FortiGate.

C. You must authorize the FortiGate device on FortiAnalyzer

D. You must click + Create in the Event handler name field.

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 19

The OT network analyst run different level of reports to quickly explore failures that could put the network at risk. Such reports can be about device performance.

Which FortiSIEM reporting method helps to identify device failures?
A. Business service reports
B. Device inventory reports
C. CMDB operational reports
D. Active dependent rules reports
Answer: C (LEAVE A REPLY)
The CMDB (Configuration Management Database) operational reports in FortiSIEM allow you to monitor device performance, health, and status.
Through CMDB, you can check device monitoring status, detect if FortiSIEM is falling behind on data collection, and identify any monitoring errors or failures.
This reporting helps quickly explore issues related to device performance that could put the network at risk.

NEW QUESTION: 20
To improve the protection of your OT network, you want to automate on FortiGate the handling of compromised devices notified by FortiAnalyzer. What must you configure?
A. An event handler with the parameter Automation Stitch enabled on FortiAnalyzer
B. An Automation with a LOCAL_HOST connector on FortiAnalyzer
C. The Security Fabric settings on FortiGate
D. A FortiOS Event Log trigger on FortiGate
Answer: A (LEAVE A REPLY)
Automation between FortiAnalyzer and FortiGate relies on event handlers configured on FortiAnalyzer with Automation Stitch enabled, which allows FortiAnalyzer to trigger automated actions on FortiGate when specific events, such as compromised devices, are detected.

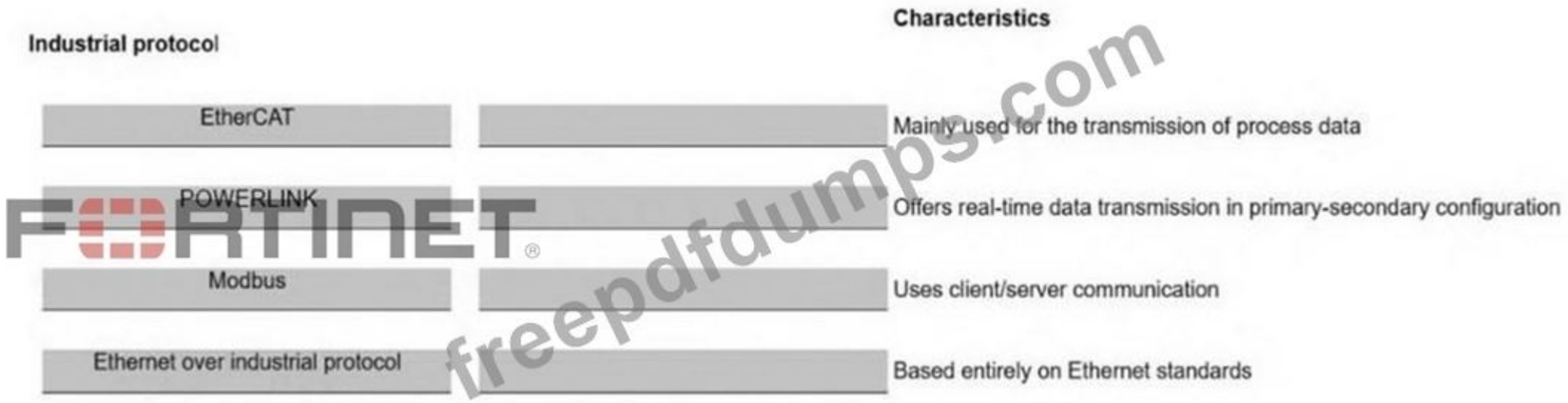
NEW QUESTION: 21
Refer to the exhibit. Given the configurations on the FortiGate, which statement is true?

```
config system interface
     edit VLAN101_dmz
          set forward-domain 101
next
     edit VLAN101_internal
          set forward-domain 101
end
```

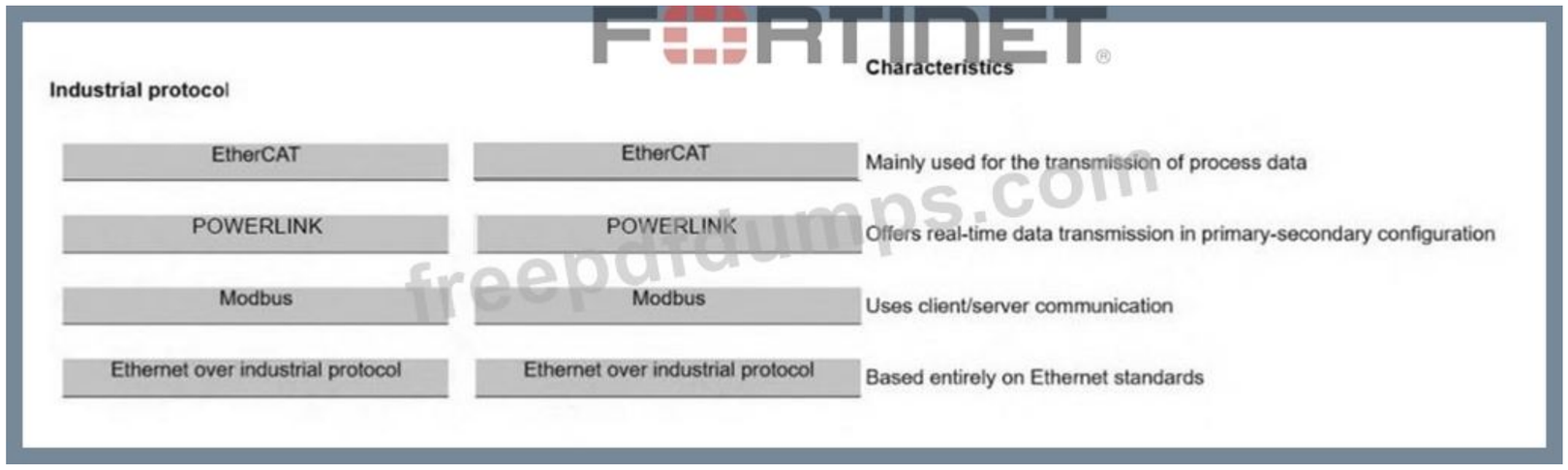

A. FortiGate is configured with forward-domains to forward only domain controller traffic.
B. FortiGate is configured with forward-domains to reduce unnecessary traffic.
C. FortiGate is configured with forward-domains to forward only company domain website traffic.
D. FortiGate is configured with forward-domains to filter and drop non-domain controller traffic.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
Drag and Drop Question
Match each industrial protocol to its corresponding characteristics.

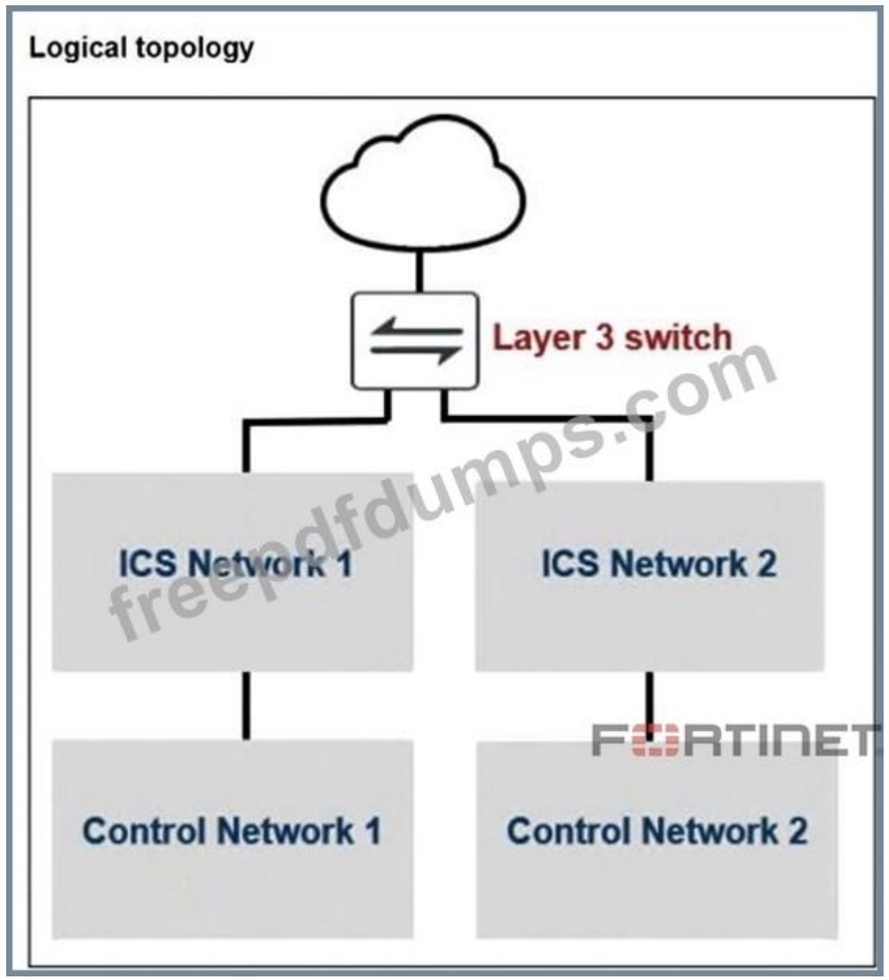
Select each OT industrial protocol in the column on the left and drag and drop it into the blank space next to its corresponding characteristics in the column on the right. After matching a device type to its characteristics, you can move it again if you want to change your answer by clicking the industrial protocol name. You must match all four industrial protocols to their characteristics in the work area.



Answer:



NEW QUESTION: 23
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 the network 2.

How can you achieve the segmentation?

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)

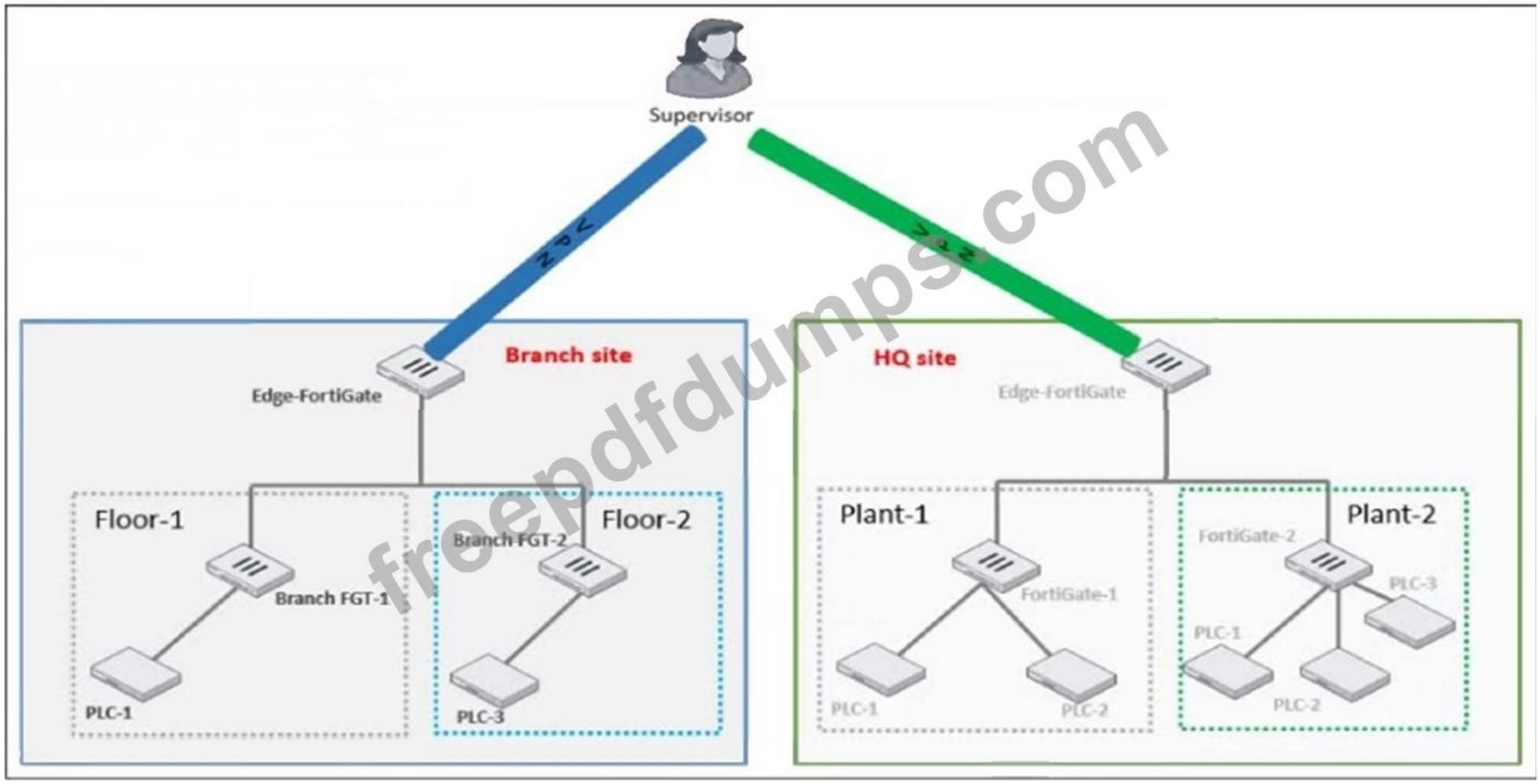
Forward domain IDs allow segmentation of traffic within the same Layer 3 infrastructure by assigning separate domains to different networks, effectively isolating Network 1 and Network 2 while still using the same physical device.

NEW QUESTION: 24

Refer to the exhibit. You need to configure VPN user access for supervisors at the branch and HQ sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.

What must you do to achieve this objective?

Network topology



A. Direct users to the self-registration server portal.

B. Import the FortiToken on each FortiGate.

C. Deploy FortiAuthenticator.

D. Use a RADIUS OTP server.

Answer: C (LEAVE A REPLY)

A single soft FortiToken can be validated by multiple FortiGate VPN gateways only when token authentication is centralized. FortiAuthenticator provides that central OTP/RADIUS service, so both FortiGates query the same token record for the supervisors.

NEW QUESTION: 25

The operational technology (OT) network analyst runs different levels of reports to investigate threats that exploit the network. The analyst can run these reports on all routers, switches, and firewalls.
Which FortiSIEM reporting method can analysts use to identify threats that exploit image firmware files?

A. CMDB reports
B. Threat hunting reports
C. Compliance reports
D. OT/IoT reports
Answer: (SHOW ANSWER)
Threat hunting reports let analysts query events and indicators (like anomalous firmware image access/use) across routers, switches, and firewalls, revealing exploits targeting firmware files.

NEW QUESTION: 26
Refer to the exhibit. You are navigating through FortiSIEM in an OT network. How do you view information presented in the exhibit and what does the FortiGate device security status tell you?

Maint	Device	Type	Organization	Avail Status	Perf Status	Security Status
●	FG240D3913800441	Fortinet FortiOS	Super	●	●	⊗
●	SJ-QA-F-Lnx-CHK	Checkpoint FireWall	Super	●	●	⚠
●	FAPS321C-default	Fortinet FortiAP	Super	●	●	

A. In the summary dashboard and there are one or more high-severity security incidents for the FortiGate device.
B. In the business service dashboard and there are one or more high-severity security incidents for the FortiGate device.
C. In the widget dashboard and there are one or more high-severity incidents for the FortiGate device.
D. In the PCI logging dashboard and there are one or more high-severity security incidents for the FortiGate device.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
An OT supervisor needs to protect their network by implementing security with an industrial signature database on the FortiGate device.
Which statement about the industrial signature database on FortiGate is true?
A. By default, the industrial database is enabled.
B. An administrator must create their own database using custom signatures.
C. A supervisor can enable it through the FortiGate CLI.
D. A supervisor must purchase an industrial signature database and import it to the FortiGate.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
You want to improve the security of your OT network and therefore deploy a FortiGate device with the OT signatures database. Which two statements about this database are true? (Choose two.)
A. You must install a valid OT security service license.

B. You must import the OT signatures database manually.
C. The OT signatures database is enabled by default.
D. You must set exclude-signatures to none in the console line interface.
Answer: A,C (LEAVE A REPLY)
The OT signatures database is part of the Fortinet OT security service and requires a valid license to be available. Once licensed, the OT signatures database is enabled by default on supported FortiGate devices.

NEW QUESTION: 29
Refer to the exhibit.

Firewall Policy page

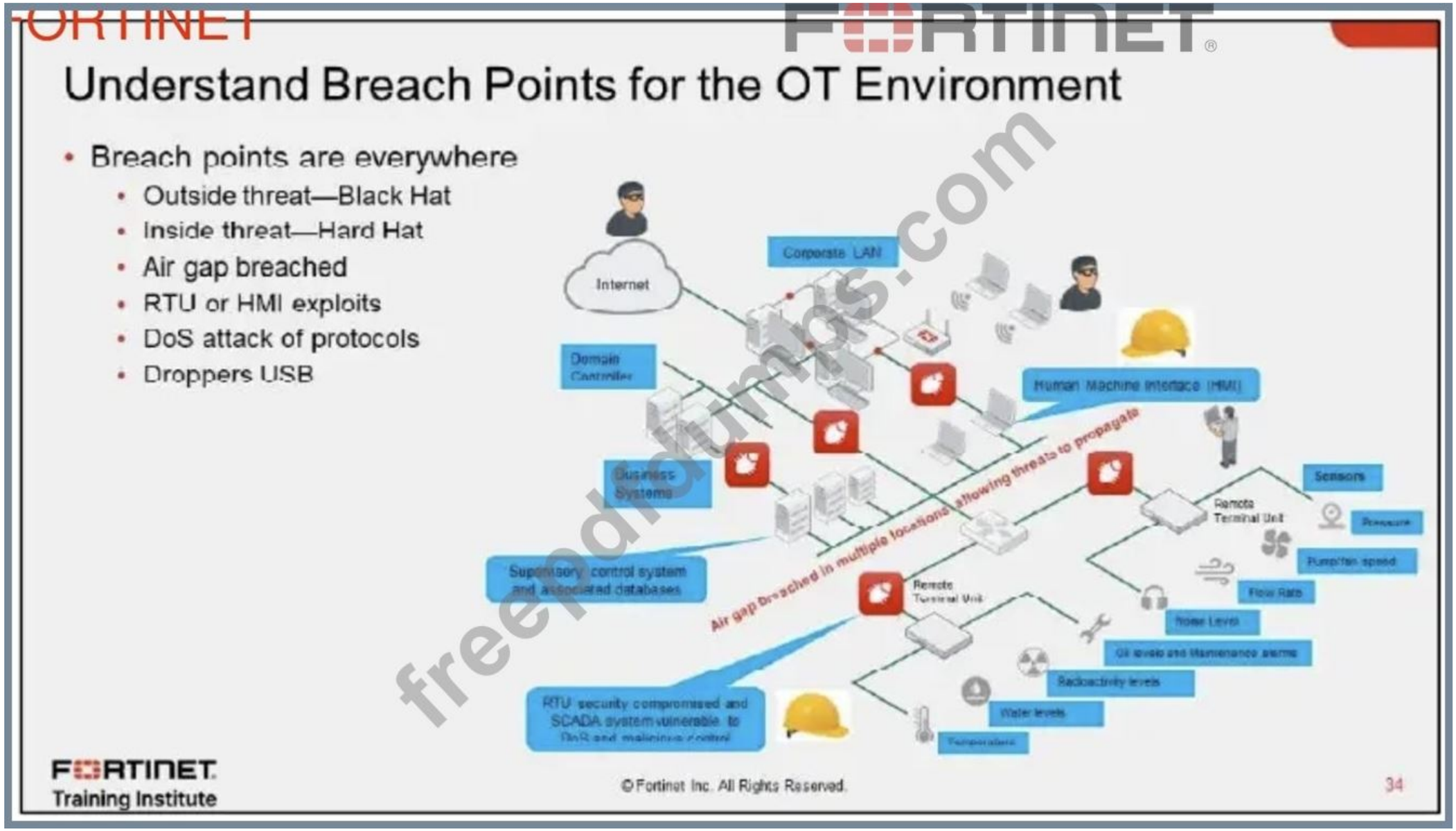
	Policy	ID	Source	Destination	Schedule	Service	Action	Type	Security Profiles
	LAN (port5) → port2 3								
	PLC1_access (8)	8	all Supervisor	PLC-1	always	ALL	✓ ACCEPT	Standard	no-inspection
	Supervisor_access (9)	9	all Supervisor	PLC-1	always	ALL_ICMP	✓ ACCEPT	Standard	no-inspection
	Floor-2_Access (7)	7	all Management	all	always	ALL_ICMP	✓ ACCEPT	Standard	no-inspection

A firewall policy page is shown.
To improve the security of your OT network, you have configured a Supervisor profile in the firewall policies, as shown in the exhibit. However, a supervisor is reporting that he cannot ping PLC-1.
What are the two reasons? (Choose two.)
A. The supervisor must first authenticate using a protocol such as HTTPS or Telnet.
B. The Supervisor profile is not configured in the remote server.
C. The firewall policy ID 8 is not enabled.
D. The CLI parameter auth-on-demand is set to always.
Answer: A,D (LEAVE A REPLY)
When identity-based policies are used, the user must first authenticate through a supported method such as HTTPS or Telnet before traffic like ICMP is permitted. Additionally, when auth- on-demand is set to always, authentication is required before any traffic is allowed, which prevents the ping until the user is authenticated.

NEW QUESTION: 30
In your OT environment, you want to detect the devices passively. Which two methods must you implement? (Choose two.)
A. SSH
B. SNMP
C. Vendor OUI
D. Network traffic

Answer: C,D (LEAVE A REPLY)
Passive device detection relies on observing existing network data without actively querying devices. Vendor OUI enables identification based on MAC address prefixes, and analyzing network traffic allows discovery and profiling of devices through their communication patterns.

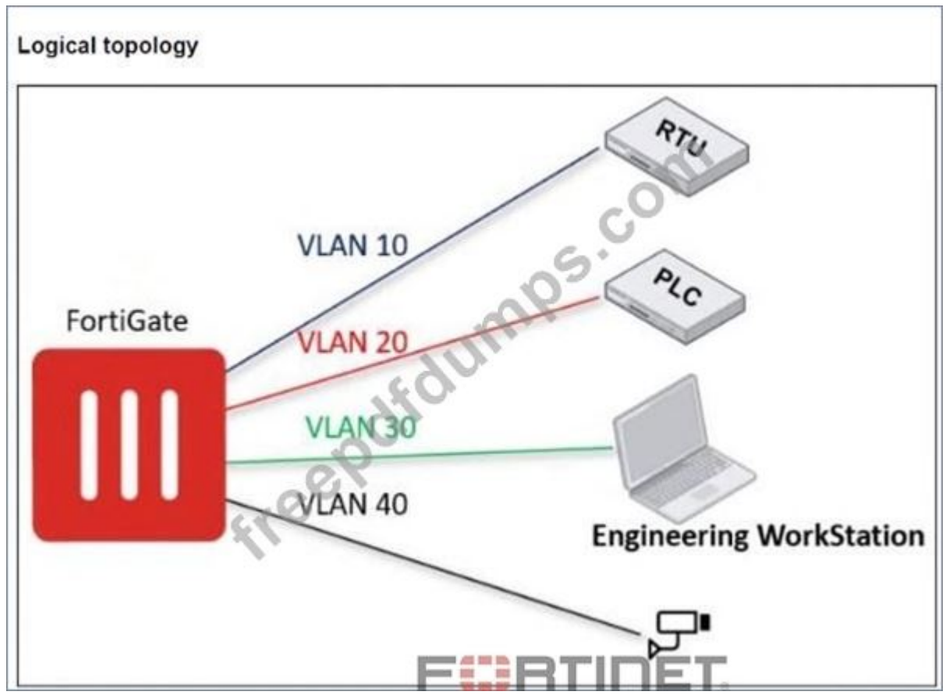
NEW QUESTION: 31
Which three common breach points can you find in a typical OT environment? (Choose three.)
A. Global hat
B. Hard hat
C. VLAN exploits
D. Black hat
E. RTU exploits
Answer: (SHOW ANSWER)



NEW QUESTION: 32
Which two frameworks are common to secure ICS industrial processes, including SCADA and DCS? (Choose two.)

A. Modbus
B. NIST Cybersecurity
C. IEC 62443
D. IEC 104
Answer: B,C (LEAVE A REPLY)
NIST Cybersecurity Framework
This framework provides a comprehensive approach to managing cybersecurity risk across an organization, including industrial control systems. It offers a structured methodology for identifying, assessing, prioritizing, and responding to cyber threats.
IEC 62443
This standard specifically addresses cybersecurity for industrial automation and control systems (IACS). It provides detailed guidance on securing various aspects of ICS, from network segmentation to secure communication protocols.

NEW QUESTION: 33
Refer to the exhibit.



A partial OT network is shown.
You want to enforce access control from Engineering Workstation to PLC.
How can you achieve this on FortiGate?
A. You must create forward domain IDs.
B. You must set the software switch to implicit.
C. You must add authentication in the corresponding firewall policy.
D. You must create VDOMs.
Answer: (SHOW ANSWER)

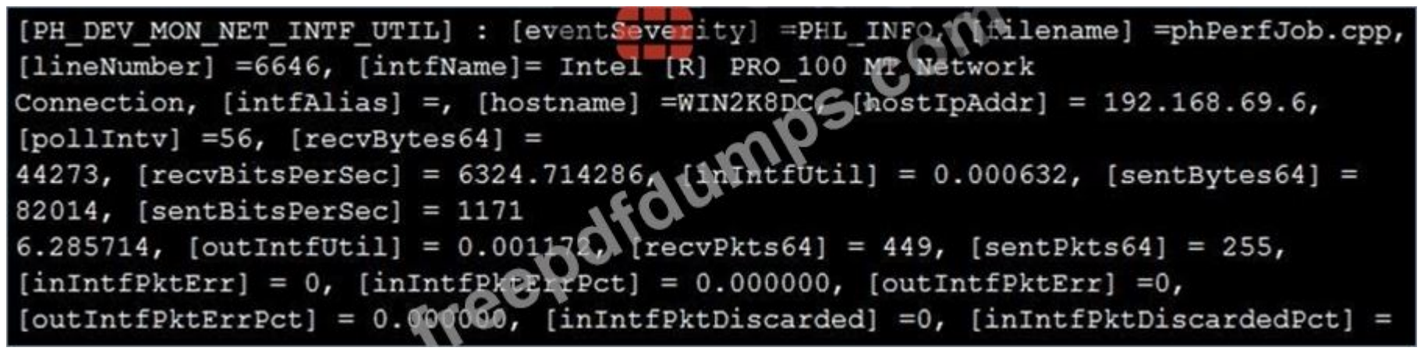
Access control from the Engineering Workstation to the PLC is enforced by applying authentication in the firewall policy that governs traffic between their VLANs. This ensures only authenticated users or devices are allowed to reach the PLC.

NEW QUESTION: 34
Operational technology (OT) network analysts run different levels of reports to identify failures that could put the network at risk. Some of these reports may be related to device performance.
Which FortiSIEM reporting method helps identify device failures?
A. Configuration management database (CMDB) operational reports
B. Business service reports
C. Device inventory reports
D. Payment card industry (PCI) logging reports
Answer: A (LEAVE A REPLY)
The Configuration Management Database (CMDB) operational reports in FortiSIEM are used to monitor and analyze the operational status of devices. These reports can help identify device failures by providing detailed insights into device configurations, statuses, and performance metrics. CMDB operational reports are particularly useful for troubleshooting and maintaining the health of devices in an OT network, ensuring that any potential failures or risks to the network are promptly addressed.

NEW QUESTION: 35
You want to improve access control for your large OT network using passive authentication. What must you configure on FortiGate?
A. Local users
B. Two-factor authentication
C. Fortinet Single-Sign On (FSSO)
D. A FortiAuthenticator device as a remote server
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
A FortiGate device is newly deployed as the edge gateway of an OT network security fabric. The downstream FortiGate devices are also newly deployed as Security Fabric leafs to protect the control area zone.
With no additional essential networking devices, and to implement micro-segmentation on this OT network, what configuration must the OT network architect apply to control intra-VLAN traffic?
A. Enable transparent mode on the edge FortiGate device.
B. Enable security profiles on all interfaces connected in the control area zone.
C. Set up VPN tunnels between downstream and edge FortiGate devices.
D. Create a software switch on each downstream FortiGate device.
Answer: D (LEAVE A REPLY)
A software switch groups multiple interfaces at Layer 2.
However, for micro-segmentation, you usually separate interfaces per subnet/device group and apply inter-interface policies on the FortiGate.
By doing this, the FortiGate can control intra-VLAN (or intra-subnet) traffic without additional networking hardware.

NEW QUESTION: 37
Refer to the exhibit. From your analysis of the output, which statement about the output is true?



A. This is a sample of a FortiAnalyzer system interface event log.

B. This is a sample of an SNMP temperature control event log.

C. This is a sample of a PAM event type.

D. This is a sample of FortiGate interface statistics.

Answer: C (LEAVE A REPLY)

ph_dev_mon is a PAM event. Hostname is WIN2K8DC (a win server) not Fortigate.

NEW QUESTION: 38

Which two statements are true when you deploy FortiGate as an offline IDS? (Choose two.)

A. FortiGate receives traffic from configured port mirroring.

B. Network traffic goes through FortiGate.

C. FortiGate acts as network sensor.

D. Network attacks can be detected and blocked.

Answer: A,C (LEAVE A REPLY)

FortiGate receives traffic from configured port mirroring

In an offline IDS configuration, a FortiGate is typically set up to receive a copy of network traffic from specific ports or VLANs through port mirroring, allowing it to analyze the data without impacting the normal network flow.

FortiGate acts as a network sensor

Since it is passively monitoring the traffic, FortiGate can detect malicious activity based on its pre- defined intrusion detection signatures without blocking the traffic.

NEW QUESTION: 39

Refer to the exhibit. The Core Network Security Connectors page of the FortiGate-2 device is shown.

Which statement is correct? (Choose one answer)

A. You must configure the FortiAnalyzer settings on FortiGate-2.

B. You must enable Security Fabric Connection on the FortiGate-2 interface.

C. FortiGate-2 is not authorized on the root FortiGate.

D. FortiGate-2 serves as Fabric Root.

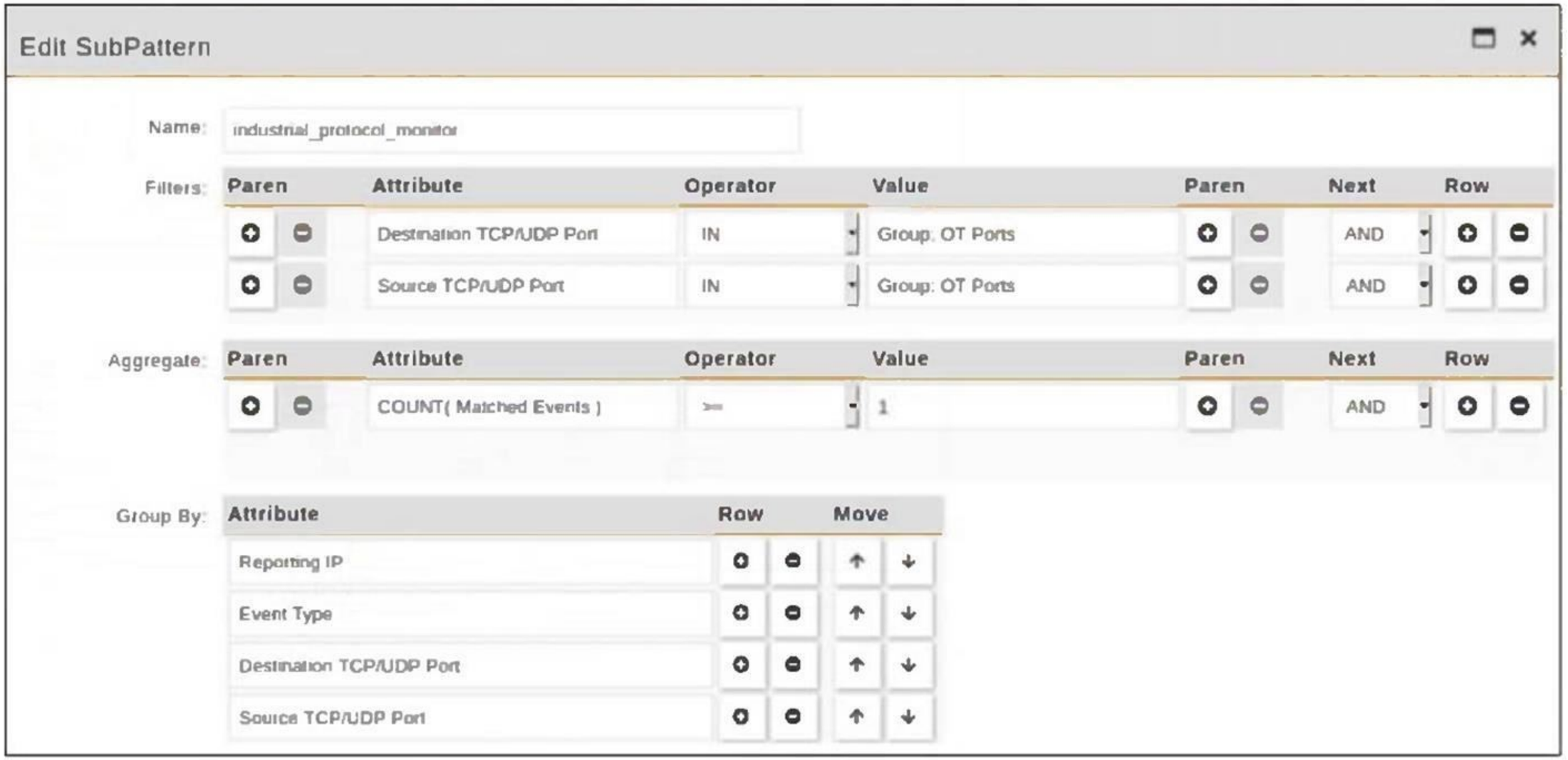
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40

Refer to the exhibit. An operational technology rule is created and successfully activated to monitor the Modbus protocol on FortiSIEM. However, the rule does not trigger incidents despite Modbus traffic and application logs being received correctly by FortiSIEM.

Which statement correctly describes the issue on the rule configuration?

A new OT rule



A. The first condition on the SubPattern filter must use the OR logical operator.
B. The attributes in the Group By section must match the ones in Fitters section.
C. The Aggregate attribute COUNT expression is incompatible with the filters.
D. The SubPattern is missing the filter to match the Modbus protocol.
Answer: D (LEAVE A REPLY)
The subpattern only filters on TCP/UDP ports (group "OT Ports"); it never specifies Modbus.
Without a protocol (or specific Modbus port) filter, FortiSIEM won't match Modbus events, so no incidents are triggered.

NEW QUESTION: 41
What are two benefits of a Nozomi integration with FortiNAC? (Choose two.)

A. Enhanced point of connection details
B. Direct VLAN assignment
C. Adapter consolidation for multi-adapter hosts
D. Importation and classification of hosts
Answer: C,D (LEAVE A REPLY)
Devices known to Nozomi can be imported and registered or classified automatically. The imported devices will be profiled based on information retrieved from the Nozomi product.
Devices with multiple network adapters will have the devices consolidated under the single device in the FortiNAC.

NEW QUESTION: 42
In the Purdue model, at which level are physical assets like the Industrial Internet of Things (IIoT) placed?
A. At Level 5 only
B. At Level 1 only
C. Above Level 4
D. Below Level 3.5
Answer: (SHOW ANSWER)
In the Purdue model, Level 1 represents basic control and physical processes, where sensors, actuators, and IIoT devices interact directly with the physical environment.

NEW QUESTION: 43
As an OT administrator, it is important to understand how industrial protocols work in an OT network. Which communication method is used by the Modbus protocol?
A. It uses OSI Layer 2 and the primary device sends data based on request from secondary device.
B. It uses OSI Layer 2 and both the primary/secondary devices always send data during the communication.
C. It uses OSI Layer 2 and both the primary/secondary devices send data based on a matching token ring.
D. It uses OSI Layer 2 and the secondary device sends data based on request from primary device.
Answer: D (LEAVE A REPLY)
Modbus is master/slave: the master (primary) polls; a slave (secondary) replies only when requested. That fits "secondary sends data based on request from primary device."

NEW QUESTION: 44
An OT network administrator is trying to implement active authentication.
Which two methods should the administrator use to achieve this? (Choose two.)
A. Two-factor authentication on FortiAuthenticator
B. Role-based authentication on FortiNAC
C. FSSO authentication on FortiGate
D. Local authentication on FortiGate
Answer: A,D (LEAVE A REPLY)
Local authentication on a FortiGate and two-factor authentication via FortiAuthenticator both require the user to actively present credentials (and an OTP), which is the essence of active authentication.

NEW QUESTION: 45
Refer to the exhibit. The OT devices behind the ruggedized FortiGate have vulnerabilities and you want to apply a virtual patching profile in the firewall policy.

Why is Virtual Patching not available in the Security Profiles section? (Choose one answer)

A. You must have a valid OT security service license.

B. You must have a ruggedized FortiGate allowing the virtual patching feature.

C. You must enable OT signatures.

D. You must enable Virtual Patching in the Feature Visibility section.

Answer: (SHOW ANSWER)

NEW QUESTION: 46

As an OT network administrator, you are required to generate reports that primarily use the same type of data sent to FortiSIEM. These reports are based on the preloaded analytic searches.

Which two actions can you take on FortiSIEM to enhance running reports for future use? (Choose two.)

A. Create custom reports to process additional analytic searches.

B. Export the preloaded analytics searches to an external syslog server

C. Save the analytic searches and turn them into report definitions.

D. Automate running these reports upon receiving new logs

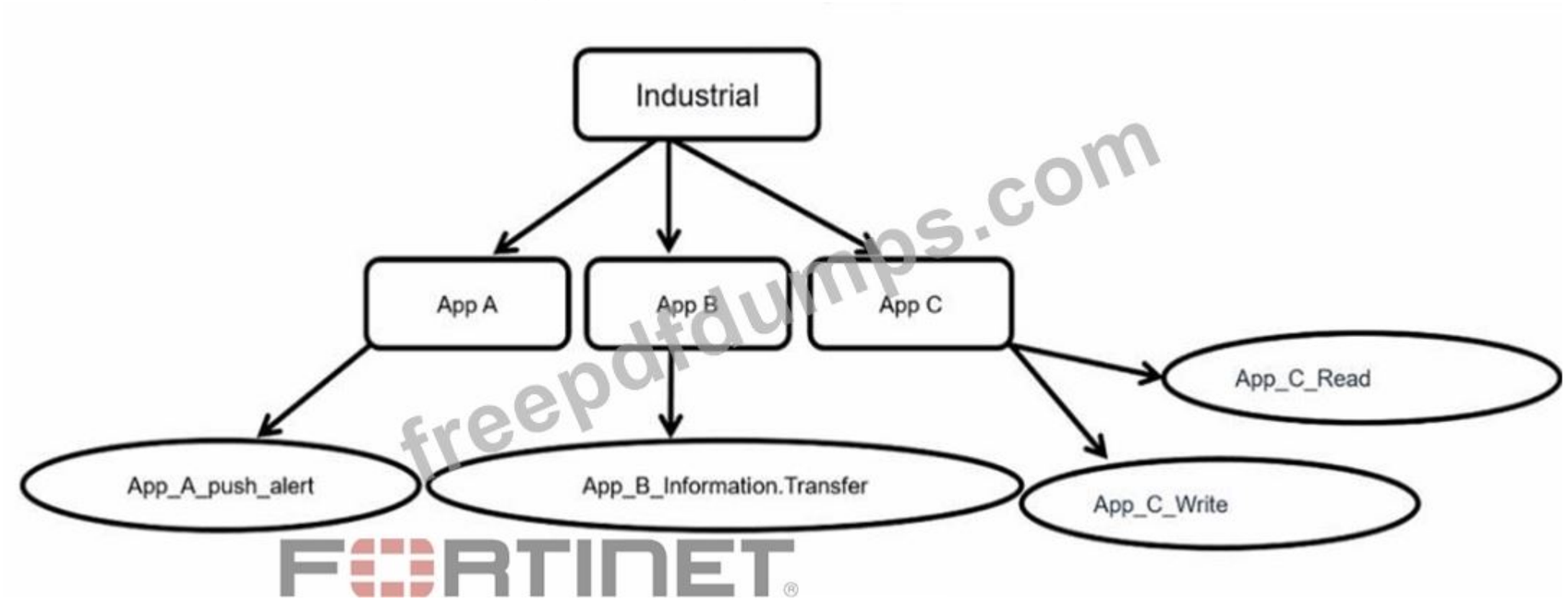
Answer: A,C (LEAVE A REPLY)

Create custom reports to process additional analytic searches: FortiSIEM allows you to create custom reports tailored to specific requirements. This is useful if the preloaded analytic searches do not completely fulfill your reporting needs or if additional data processing is required.

Save the analytic searches and turn them into report definitions: FortiSIEM enables you to save analytic searches and convert them into reusable report definitions. These report definitions can then be used to generate consistent reports based on the same criteria in the future.

NEW QUESTION: 47
An OT architect has deployed a Layer 2 switch in the OT network at Level 1 in the Purdue model- process control. The purpose of the Layer 2 switch is to segment traffic between PLC1 and PLC2 with two VLANs.
All the traffic between PLC1 and PLC2 must first flow through the Layer 2 switch and then through the FortiGate device in the Level 2 supervisory control network.
Which statement about the traffic between PLC1 and PLC2 is true?
A. The Layer 2 switch rewrites VLAN tags before sending traffic to the FortiGate device.
B. The Layer 2 switches routes any traffic to the FortiGate device through an Ethernet link.
C. PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.
D. In order to communicate, PLC1 must be in the same VLAN as PLC2.
Answer: (SHOW ANSWER)
Since PLC1 and PLC2 are segmented into two VLANs on a Layer 2 switch, traffic between them requires inter-VLAN routing.
The Layer 2 switch handles VLAN segmentation but does not route traffic between VLANs.
For communication between VLANs, traffic must be sent to a router or Layer 3 device-in this case, the FortiGate device in the Layer 2 supervisory control network.
The traffic flows from PLCs to the Layer 2 switch and then over a trunk link (carrying VLAN tags) to the FortiGate, which performs inter-VLAN routing.
The trunk link allows multiple VLAN-tagged traffic to be carried between the Layer 2 switch and the FortiGate for routing.
Options regarding VLAN tags rewriting or requiring PLCs to be in the same VLAN are incorrect because VLAN tagging remains consistent on trunk links and PLCs are intentionally segmented.

NEW QUESTION: 48
Refer to the exhibit. Which statement is true about application control inspection?



A. The industrial application control inspection process is unique among application categories.

B. Security actions cannot be applied on the lowest level of the hierarchy.
C. You can control security actions only on the parent-level application signature
D. The parent signature takes precedence over the child application signature.
Answer: D (LEAVE A REPLY)
Application control inspection in Fortinet firewalls utilizes a hierarchical structure where applications are categorized and classified. A parent signature encompasses a group of related child applications. If a security action is defined on the parent signature, it will apply to all child applications within that group. Therefore, the parent signature takes precedence over the child application signature, meaning if a child application is allowed access based on its own signature but the parent signature has a blocking rule, the child application will still be blocked.

NEW QUESTION: 49
Which statemenl about the IEC 104 protocol is true?
A. IEC 104 is used for telecontrol SCADA in electrical engineering applications.
B. IEC 104 is IEC 101 compliant in old SCADA systems.
C. IEC 104 protects data transmission between OT devices and services.
D. IEC 104 uses non-TCP/IP standards.
Answer: A (LEAVE A REPLY)
IEC 104 is a widely used protocol in the field of Supervisory Control and Data Acquisition (SCADA) for electrical engineering applications, specifically telecontrol. It's designed to facilitate communication between control stations and substations in power grids.

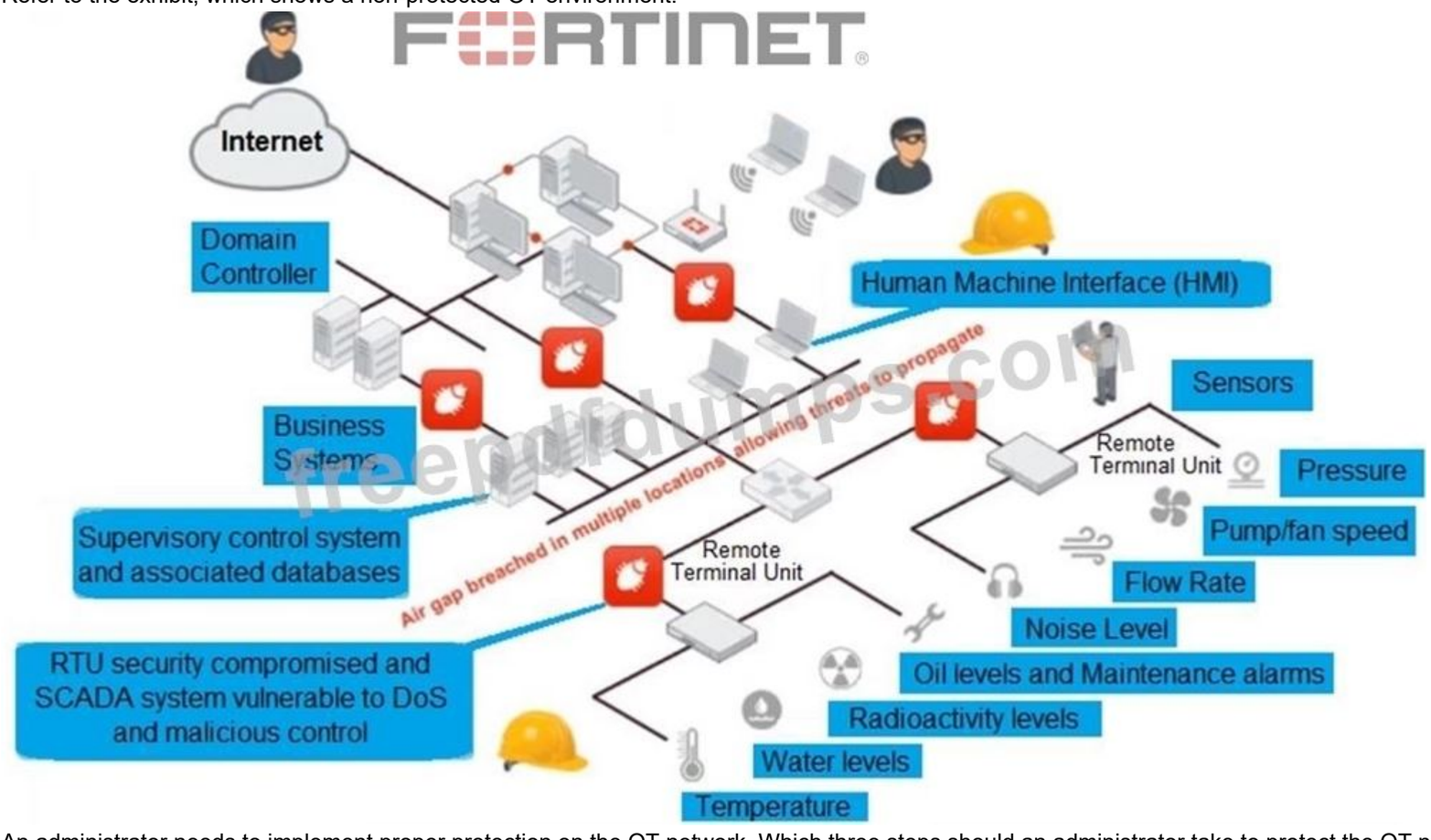
NEW QUESTION: 50
Which type of attack posed by skilled and malicious users of security level 4 (SL 4) of IEC 62443 is designed to defend against intentional attacks?
A. Users with access to moderate resources
B. Users with low access to resources
C. Users with unintentional operator error
D. Users with substantial resources
Answer: D (LEAVE A REPLY)
SL 1 → Protects against unintentional operator error or casual mistakes.
SL 2 → Protects against intentional misuse by attackers with low resources.
SL 3 → Protects against skilled and malicious attackers with moderate resources.
SL 4 → Protects against highly skilled attackers with substantial resources (e.g., nation-state level).

NEW QUESTION: 51
With the limit of using one firewall device, the administrator enables multi-VDOM on FortiGate to provide independent multiple security domains to each ICS network.
Which statement ensures security protection is in place for all ICS networks?
A. Each traffic VDOM must have a direct connection to FortiGuard services to receive the required security updates.
B. The management VDOM must have access to all global security services.
C. Each VDOM must have an independent security license.
D. Traffic between VDOMs must pass through the physical interfaces of FortiGate to check for security incidents.
Answer: B (LEAVE A REPLY)
In a multi-VDOM setup, one VDOM typically acts as the management VDOM (often called "root") which manages global settings and security services like FortiGuard updates.
This management VDOM handles access to global security services that benefit all traffic VDOMs.
Individual traffic VDOMs process their own traffic and enforce security policies but rely on the management VDOM for centralized access to global security services.

Each VDOM does not need an independent security license; the license is for the device as a whole.
Traffic between VDOMs does not need to pass through physical interfaces to be inspected; inter- VDOM links and policies handle traffic inspection.
Each VDOM does not require direct FortiGuard connections; this can be centralized in the management VDOM.

NEW QUESTION: 52
How are rogue devices evaluated in FortiNAC?
A. Through queries to FortiGuard servers
B. Through device profiling rules
C. Through the import of the devices list
D. Through the local device database (CIDB)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
Refer to the exhibit, which shows a non-protected OT environment.



An administrator needs to implement proper protection on the OT network. Which three steps should an administrator take to protect the OT network? (Choose three.)
A. Configure firewall policies with web filter to protect the different ICS networks.
B. Use segmentation

C. Deploy a FortiGate device within each ICS network.
D. Configure firewall policies with industrial protocol sensors
E. Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.
Answer: B,C,D (LEAVE A REPLY)