Fortinet

Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2

NEW QUESTION 1
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. IEC104

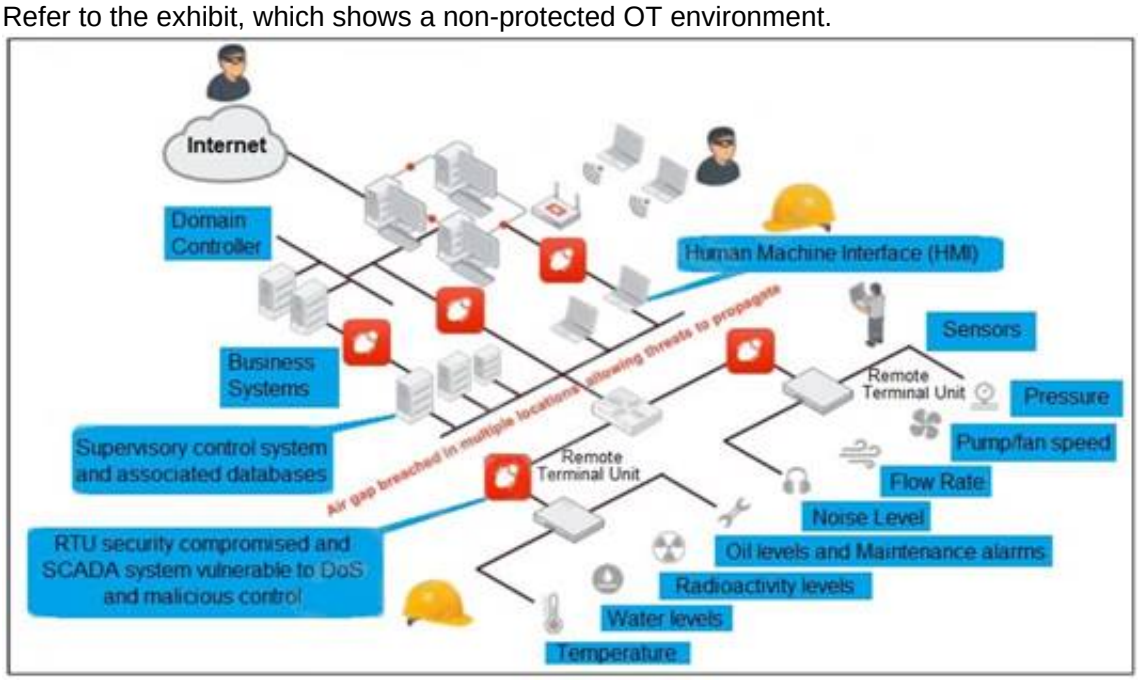
Answer: CD

NEW QUESTION 2
You are investigating a series of incidents that occurred in the OT network over past 24 hours in FortiSIEM.
Which three FortiSIEM options can you use to investigate these incidents? (Choose three.)

A. Security
B. IPS
C. List
D. Risk
E. Overview

Answer: CDE

NEW QUESTION 3
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. Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.
B. Deploy a FortiGate device within each ICS network.
C. Configure firewall policies with web filter to protect the different ICS networks.
D. Configure firewall policies with industrial protocol sensors
E. Use segmentation

Answer: ACD

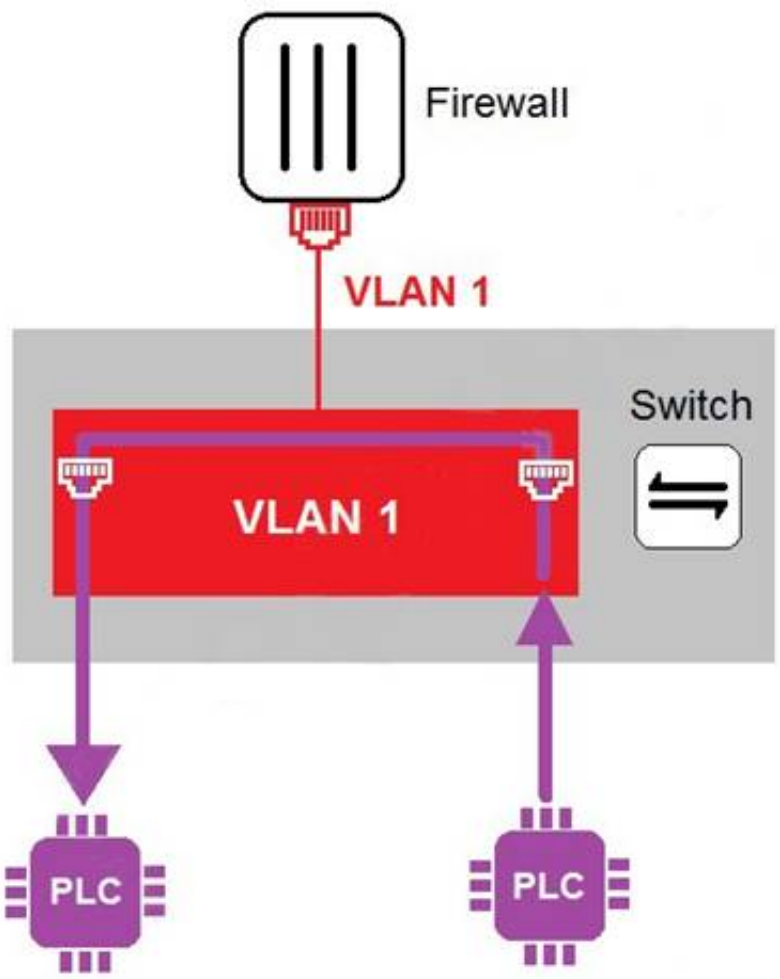
NEW QUESTION 4
An OT administrator is defining an incident notification policy using FortiSIEM and would like to configure the system with a notification policy. If an incident occurs, the administrator would like to be able to intervene and block an IP address or disable a user in Active Directory from FortiSIEM.
Which step must the administrator take to achieve this task?

A. Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.
B. Create a notification policy and define a script/remediation on FortiSIEM.
C. Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.
D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.

Answer: B

Explanation:
https://fusecommunity.fortinet.com/blogs/silviu/2022/04/12/fortisiempublishingscript

NEW QUESTION 5
Refer to the exhibit



In the topology shown in the exhibit, both PLCs can communicate directly with each other, without going through the firewall.
Which statement about the topology is true?

A. PLCs use IEEE802.1Q protocol to communicate each other.
B. An administrator can create firewall policies in the switch to secure between PLCs.
C. This integration solution expands VLAN capabilities from Layer 2 to Layer 3.
D. There is no micro-segmentation in this topology.

Answer: D

NEW QUESTION 6
An OT network architect must deploy a solution to protect fuel pumps in an industrial remote network. All the fuel pumps must be closely monitored from the corporate network for any temperature fluctuations.
How can the OT network architect achieve this goal?

A. Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature security rule on the corporate network.
B. Configure a fuel server on the corporate network, and deploy a FortiSIEM with a single pattern temperature performance rule on the remote network.
C. Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature performance rule on the corporate network.
D. Configure both fuel server and FortiSIEM with a single-pattern temperature performance rule on the corporate network.

Answer: C

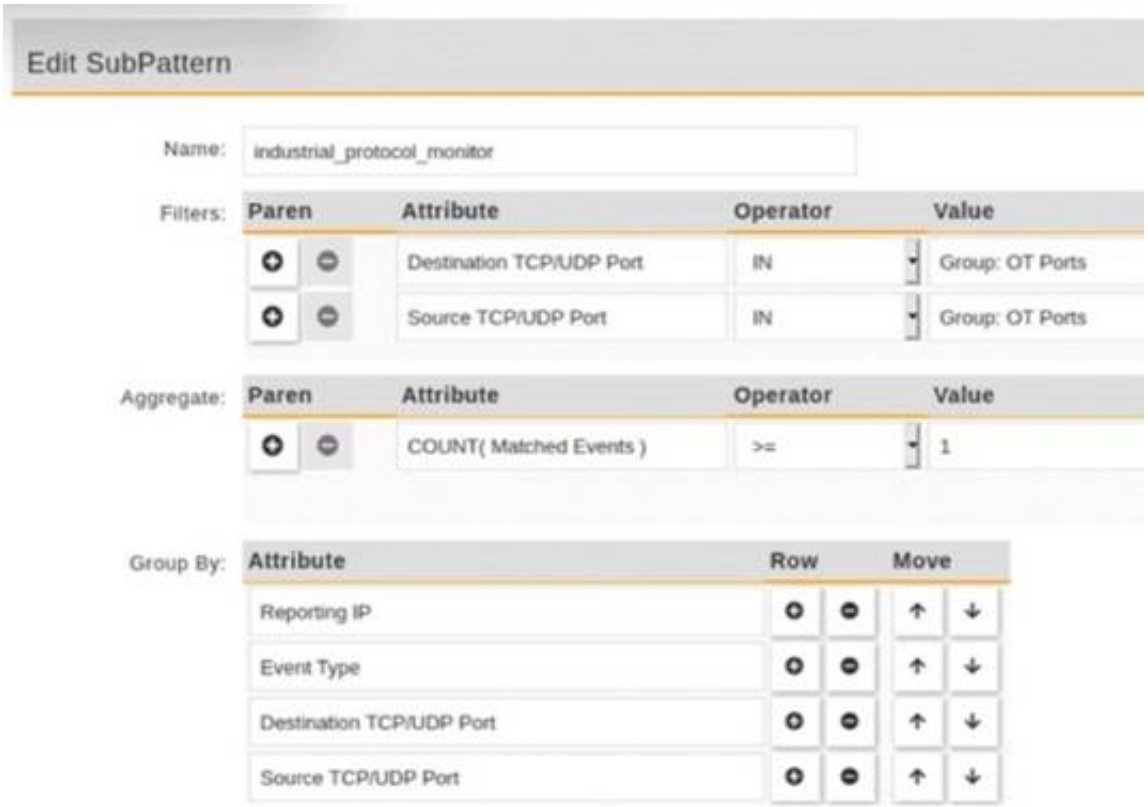
Explanation:
This way, FortiSIEM can discover and monitor everything attached to the remote network and provide security visibility to the corporate network

NEW QUESTION 7
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: AD

NEW QUESTION 8
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. 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: B

NEW QUESTION 9
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: BC

NEW QUESTION 10
What triggers Layer 2 polling of infrastructure devices connected in the network?

A. A failed Layer 3 poll
B. A matched security policy
C. A matched profiling rule
D. A linkup or linkdown trap

Answer: D

NEW QUESTION 10
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 exploits that affect PLCs.
Which security sensor must implement to detect these types of industrial exploits?

A. Intrusion prevention system (IPS)
B. Deep packet inspection (DPI)
C. Antivirus inspection
D. Application control

Answer: B

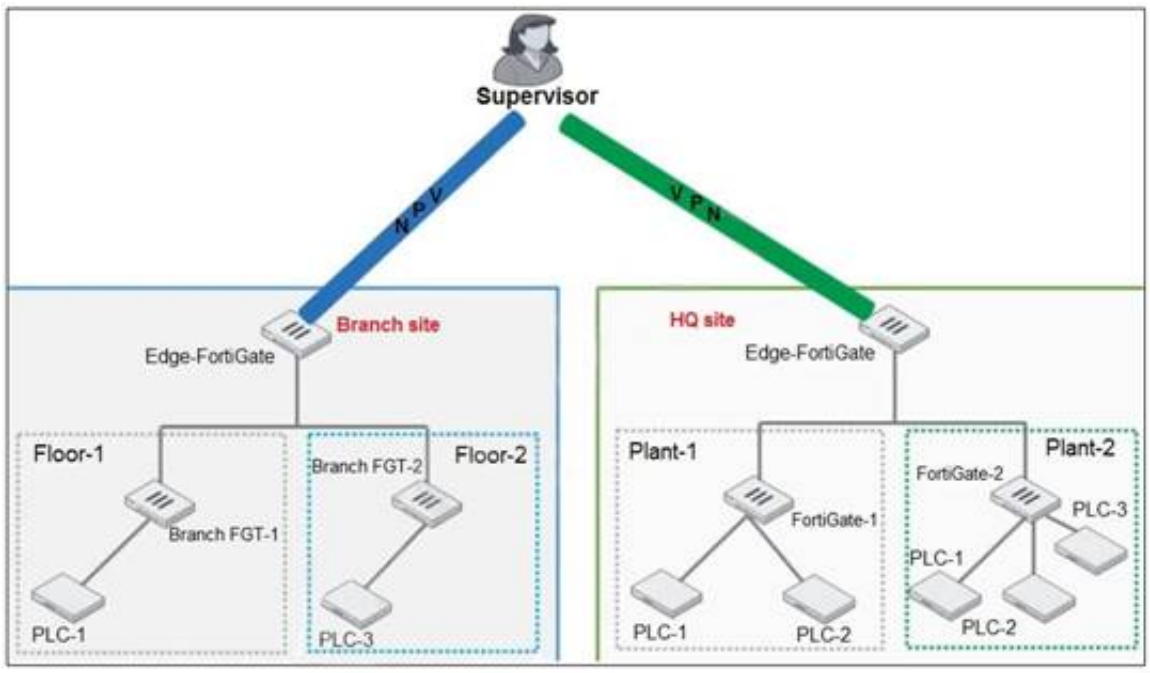
NEW QUESTION 13
Which three Fortinet products can be used for device identification in an OT industrial control system (ICS)? (Choose three.)

A. FortiNAC
B. FortiManager
C. FortiAnalyzer
D. FortiSIEM
E. FortiGate

Answer: ADE

Explanation:
A. FortiNAC - FortiNAC is a network access control solution that provides visibility and control over network devices. It can identify devices, enforce access policies, and automate threat response.
* D. FortiSIEM - FortiSIEM is a security information and event management solution that can collect and analyze data from multiple sources, including network devices and servers. It can help identify potential security threats, as well as monitor compliance with security policies and regulations.
* E. FortiAnalyzer - FortiAnalyzer is a central logging and reporting solution that collects and analyzes data from multiple sources, including FortiNAC and FortiSIEM. It can provide insights into network activity and help identify anomalies or security threats.
Reference:
Fortinet NSE 7 - OT Security 6.4 Study Guide, Chapter 4: OT Security Devices, page 4-20.

NEW QUESTION 17
Refer to the exhibit.



You need to configure VPN user access for supervisors at the breach and HQ sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.
What must you do to achieve this objective?

A. You must use a FortiAuthenticator.
B. You must register the same FortiToken on more than one FortiGate.
C. You must use the user self-registration server.
D. You must use a third-party RADIUS OTP server.

Answer: A

NEW QUESTION 20
When you create a user or host profile, which three criteria can you use? (Choose three.)

A. Host or user group memberships
B. Administrative group membership
C. An existing access control policy
D. Location
E. Host or user attributes

Answer: ADE

Explanation:
https://docs.fortinet.com/document/fortinac/9.2.0/administration-guide/15797/user-host-profiles

NEW QUESTION 23
Which three common breach points can be found in a typical OT environment? (Choose three.)

A. Global hat
B. Hard hat
C. VLAN exploits
D. Black hat
E. RTU exploits

Answer: BDE

NEW QUESTION 26
An administrator wants to use FortiSoC and SOAR features on a FortiAnalyzer device to detect and block any unauthorized access to FortiGate devices in an OT network.
Which two statements about FortiSoC and SOAR features on FortiAnalyzer are true? (Choose two.)

A. You must set correct operator in event handler to trigger an event.
B. You can automate SOC tasks through playbooks.
C. Each playbook can include multiple triggers.
D. You cannot use Windows and Linux hosts security events with FortiSoC.

Answer: AB

Explanation:
Ref: https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/268882/fortisoc

NEW QUESTION 27
What two advantages does FortiNAC provide in the OT network? (Choose two.)

A. It can be used for IoT device detection.
B. It can be used for industrial intrusion detection and prevention.
C. It can be used for network micro-segmentation.
D. It can be used for device profiling.

Answer: AD

Explanation:
Typically, in a microsegmented network, NGFWs are used in conjunction with VLANs to implement security policies and to inspect and filter network communications. Fortinet FortiSwitch and FortiGate NGFW offer an integrated approach to microsegmentation.

NEW QUESTION 31
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: BC

NEW QUESTION 32
An OT administrator deployed many devices to secure the OT network. However, the SOC team is reporting that there are too many alerts, and that many of the alerts are false positive. The OT administrator would like to find a solution that eliminates repetitive tasks, improves efficiency, saves time, and saves resources.
Which products should the administrator deploy to address these issues and automate most of the manual tasks done by the SOC team?

A. FortiSIEM and FortiManager
B. FortiSandbox and FortiSIEM
C. FortiSOAR and FortiSIEM
D. A syslog server and FortiSIEM

Answer: C

NEW QUESTION 33
In a wireless network integration, how does FortiNAC obtain connecting MAC address information?

A. RADIUS
B. Link traps
C. End station traffic monitoring
D. MAC notification traps

Answer: A

Explanation:
FortiNAC can integrate with RADIUS servers to obtain MAC address information for wireless clients that authenticate through the RADIUS server. Reference: Fortinet NSE 7 - OT Security 6.4 Study Guide, Chapter 4: OT Security Devices, page 4-28.

NEW QUESTION 35
Refer to the exhibits.

Which statement is true about the traffic passing through to PLC-2?

A. IPS must be enabled to inspect application signatures.
B. The application filter overrides the default action of some IEC 104 signatures.
C. IEC 104 signatures are all allowed except the C.BO.NA 1 signature.
D. SSL Inspection must be set to deep-inspection to correctly apply application control.

Answer: B

NEW QUESTION 39
An OT supervisor has configured LDAP and FSSO for the authentication. The goal is that all the users be authenticated against passive authentication first and, if passive authentication is not successful, then users should be challenged with active authentication.
What should the OT supervisor do to achieve this on FortiGate?

A. Configure a firewall policy with LDAP users and place it on the top of list of firewall policies.
B. Enable two-factor authentication with FSSO.
C. Configure a firewall policy with FSSO users and place it on the top of list of firewall policies.
D. Under config user settings configure set auth-on-demand implicit.

Answer: C

Explanation:
The OT supervisor should configure a firewall policy with FSSO users and place it on the top of list of firewall policies in order to achieve the goal of authenticating users against passive authentication first and, if passive authentication is not successful, then challenging them with active authentication.

NEW QUESTION 40
Refer to the exhibit.

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		●	●

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?

A. In the PCI logging dashboard and there are one or more high-severity security incidents for the FortiGate device.

B. In the summary 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 business service dashboard and there are one or more high-severity security incidents for the FortiGate device.

Answer: B

NEW QUESTION 42
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE7_OTS-7.2 Practice Exam Features:

* NSE7_OTS-7.2 Questions and Answers Updated Frequently

* NSE7_OTS-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_OTS-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_OTS-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year