Fortinet

Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2

NEW QUESTION 1
Refer to the exhibit.

Device Name	Device Type Vendor	Device Type Model	Device Hardware Model	Device Image File	Count
SJ-QA-A-IOS-JunOffice	Cisco	IOS	1760	C1700-advsecurityk9-mz.123-8.T4.bin	1
SJ-Main-Cat6500	Cisco	IOS	WS-C6509	s72033-advipservicesk9_wan-mz.122-33.SXI1.bin	1
ph-network-3560_1	Cisco	IOS	WS-C3560G-48PS-S	c3560-advipservicesk9-mz.122-25.SEE4.bin	1

An OT administrator ran a report to identify device inventory in an OT network. Based on the report results, which report was run?

A. A FortiSIEM CMDB report
B. A FortiAnalyzer device report
C. A FortiSIEM incident report
D. A FortiSIEM analytics report

Answer: A

NEW QUESTION 2
To increase security protection in an OT network, how does application control on ForliGate detect industrial traffic?

A. By inspecting software and software-based vulnerabilities
B. By inspecting applications only on nonprotected traffic
C. By inspecting applications with more granularity by inspecting subapplication traffic
D. By inspecting protocols used in the application traffic

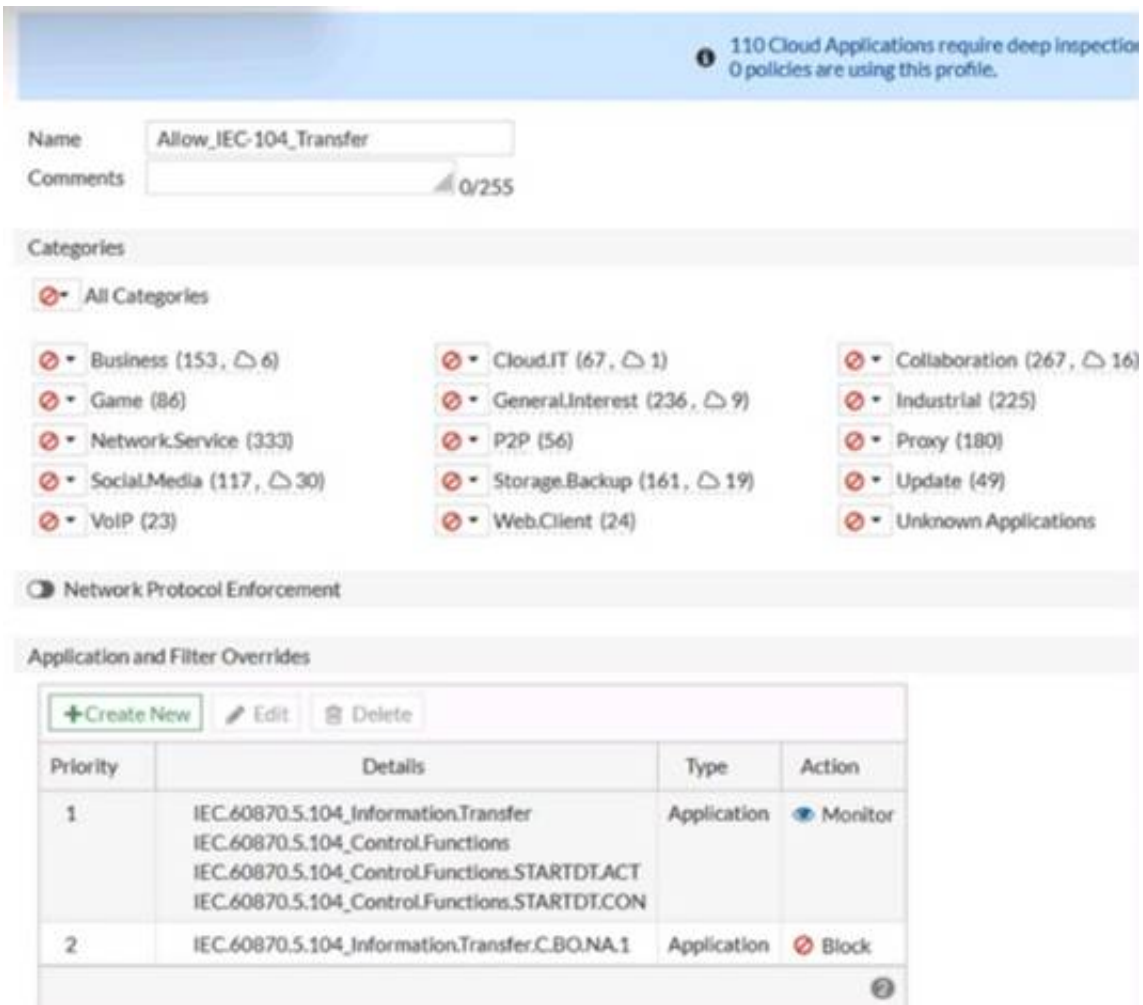
Answer: B

NEW QUESTION 3
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 4
Refer to the exhibit.



An OT network security audit concluded that the application sensor requires changes to ensure the correct security action is committed against the overrides filters.

Which change must the OT network administrator make?

A. Set all application categories to apply default actions.
B. Change the security action of the industrial category to monitor.
C. Set the priority of the C.BO.NA.1 signature override to 1.
D. Remove IEC.60870.5.104 Information.Transfer from the first filter override.

Answer: C

Explanation:
According to the Fortinet NSE 7 - OT Security 6.4 exam guide1, the application sensor settings allow you to configure the security action for each application category andnetwork protocol override. The security action determines how the FortiGate unit handles traffic that matches the application category or network protocol override. The security action can be one of the following:
? Allow: The FortiGate unit allows the traffic without any further inspection.
? Monitor: The FortiGate unit allows the traffic and logs it for monitoring purposes.
? Block: The FortiGate unit blocks the traffic and logs it as an attack.
The priority of the network protocol override determines the order in which the FortiGate unit applies the security action to the traffic. The lower the priority number, the higher the priority. For example, a priority of 1 is higher than a priority of 10.
In the exhibit, the application sensor has the following settings:
? The industrial category has a security action of allow, which means that the FortiGate unit will not inspect or log any traffic that belongs to this category.
? The IEC.60870.5.104 Information.Transfer network protocol override has a
security action of block, which means that the FortiGate unit will block and log any traffic that matches this protocol.
? The IEC.60870.5.104 Control.Functions network protocol override has a security
action of monitor, which means that the FortiGate unit will allow and log any traffic that matches this protocol.
? The IEC.60870.5.104 Start/Stop network protocol override has a security action of
allow, which means that the FortiGate unit will not inspect or log any traffic that matches this protocol.
? The IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override has a
security action of block, which means that the FortiGate unit will block and log any traffic that matches this protocol.
The problem with these settings is that the IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override has a lower priority than the IEC.60870.5.104 Information.Transfer network protocol override. This means that if the traffic matches both protocols, the FortiGate unit will apply the security action of the higher priority override, which is block. However, the IEC.60870.5.104 Transfer.C.BO.NA.1 protocol is used to transfer binary outputs, which are essential for controlling OT devices. Therefore, blocking this protocol could have negative consequences for the OT network.
To fix this issue, the OT network administrator must set the priority of the IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override to 1, which is higher than the priority of the IEC.60870.5.104 Information.Transfer network protocol override. This way, the FortiGate unit will apply the security action of the lower priority override, which is allow, to the traffic that matches both protocols. This will ensure that the FortiGate unit does not block the traffic that is used to transfer binary outputs, while still blocking the traffic that is used to transfer information.
1: NSE 7 Network Security Architect - Fortinet

NEW QUESTION 5
Which two statements about the Modbus protocol are true? (Choose two.)

A. Modbus uses UDP frames to transport MBAP and function codes.
B. Most of the PLC brands come with a built-in Modbus module.
C. You can implement Modbus networking settings on internetworking devices.
D. Modbus is used to establish communication between intelligent devices.

Answer: BC

NEW QUESTION 6
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 7
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 8
An OT architect has deployed a Layer 2 switch in the OT network at Level 1 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.
What 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: C

Explanation:
The statement that is true about the traffic between PLC1 and PLC2 is that PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.

NEW QUESTION 9
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 10
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The NSE7_OTS-7.2 Practice Test Here