Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2

https://www.2passeasy.com/dumps/NSE7_OTS-7.2/

NEW QUESTION 1
Refer to the exhibit.

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
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
The OT network analyst runs different level of reports to quickly explore threats that exploit the network. Such reports can be run on all routers, switches, and firewalls. Which FortiSIEM reporting method helps to identify these type of exploits of image firmware files?

A. CMDB reports
B. Threat hunting reports
C. Compliance reports
D. OT/IoT reports

Answer: B

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.
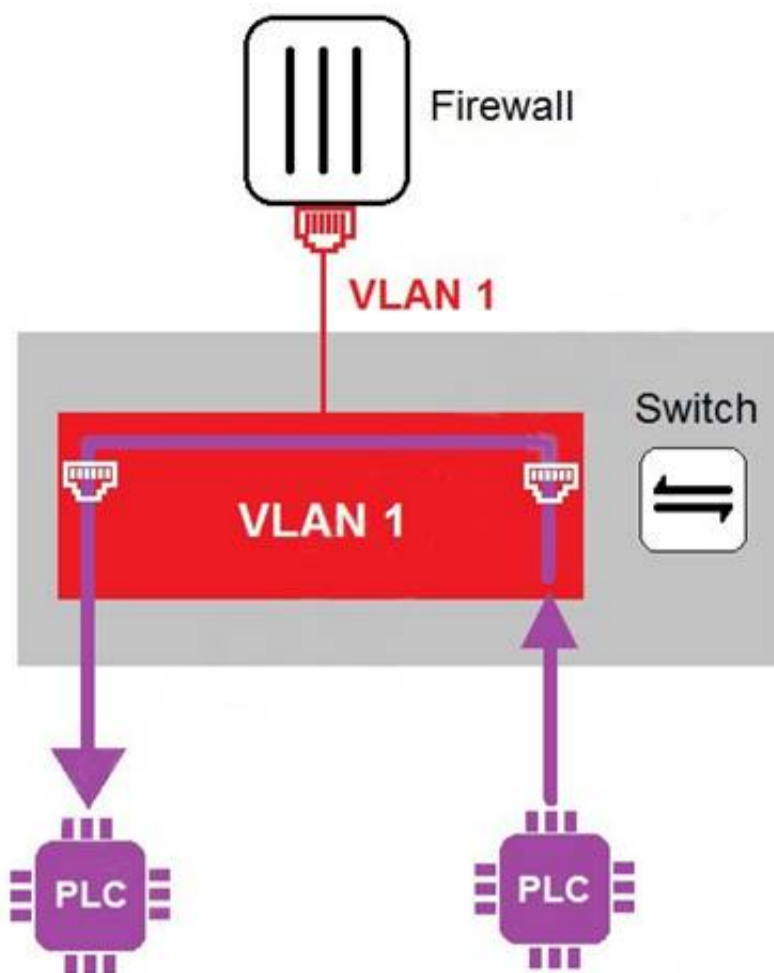D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.

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 consists of multiple FortiGate devices. The edge FortiGate device is deployed as the secure gateway and is only allowing remote operators to access the ICS networks on site.
Management hires a third-party company to conduct health and safety on site. The third-party company must have outbound access to external resources.
As the OT network administrator, what is the best scenario to provide external access to the third-party company while continuing to secure the ICS networks?

A. Configure outbound security policies with limited active authentication users of the third-party company.
B. Create VPN tunnels between downstream FortiGate devices and the edge FortiGate to protect ICS network traffic.
C. Split the edge FortiGate device into multiple logical devices to allocate an independent VDOM for the third-party company.
D. Implement an additional firewall using an additional upstream link to the internet.

Answer: C

NEW QUESTION 7

An OT network architect needs to secure control area zones with a single network access policy to provision devices to any number of different networks.
On which device can this be accomplished?

A. FortiGate
B. FortiEDR
C. FortiSwitch
D. FortiNAC

Answer: A

Explanation:
An OT network architect can accomplish the goal of securing control area zones with a single network access policy to provision devices to any number of different networks on a FortiGate device.

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 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. A supervisor must purchase an industrial signature database and import it to the FortiGate.
B. An administrator must create their own database using custom signatures.
C. By default, the industrial database is enabled.
D. A supervisor can enable it through the FortiGate CLI.

Answer: D

NEW QUESTION 10

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

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?

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 security 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 15
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_OTS-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_OTS-7.2 Product From:

https://www.2passeasy.com/dumps/NSE7_OTS-7.2/

Money Back Guarantee

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