Fortinet

Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2

NEW QUESTION 1
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 time period for the report.
C. The administrator selected the wrong devices in the Devices section.
D. The administrator selected the wrong hcache table for the report.

Answer: BC

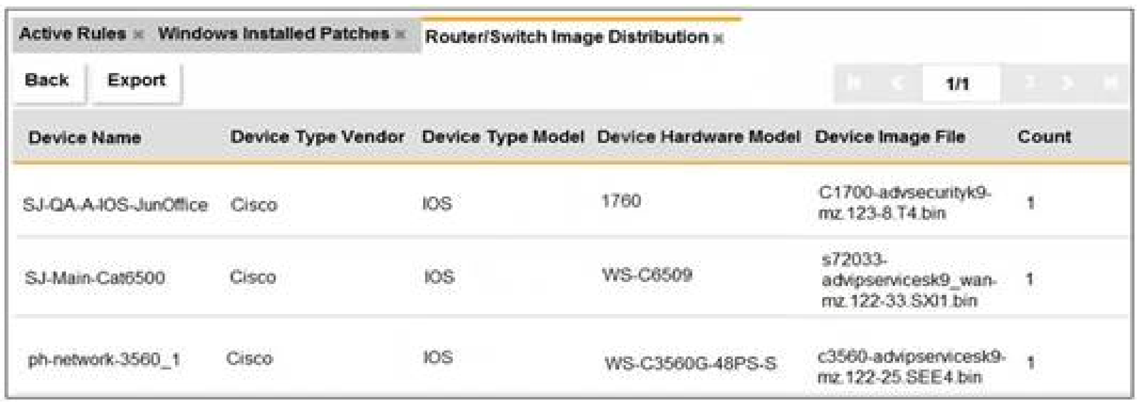
Explanation:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/32cb817d-a307- 11eb-b70b-00505692583a/FortiAnalyzer-7.0.0-Administration_Guide.pdf

NEW QUESTION 2
When device profiling rules are enabled, which devices connected on the network are evaluated by the device profiling rules?

A. Known trusted devices, each time they change location
B. All connected devices, each time they connect
C. Rogue devices, only when they connect for the first time
D. Rogue devices, each time they connect

Answer: C

NEW QUESTION 3
Refer to the exhibit.


Active Rules ×
Windows Installed Patches ×
Router/Switch Image Distribution ×
Back
Export
1/1

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 4
How can you achieve remote access and internel availability in an OT network?

A. Create a back-end backup network as a redundancy measure.
B. Implement SD-WAN to manage traffic on each ISP link.
C. Add additional internal firewalls to access OT devices.
D. Create more access policies to prevent unauthorized access.

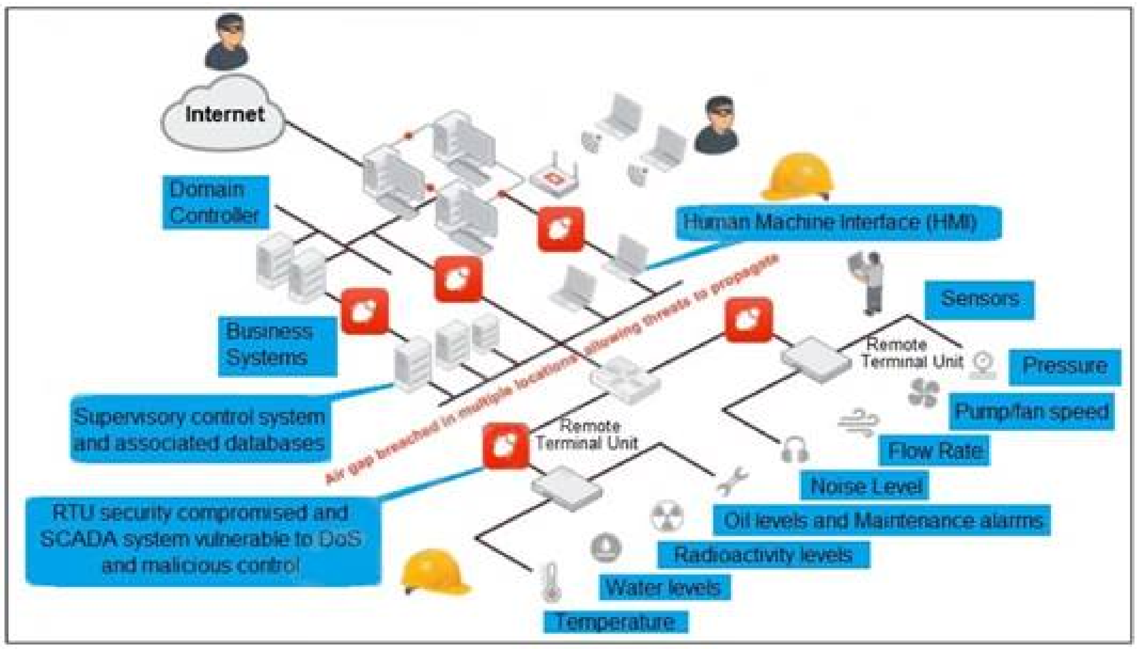
Answer: B

NEW QUESTION 5
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 6
Refer to the exhibit, which shows a non-protected OT environment.


Internet
Domain Controller
Business Systems
Supervisory control system and associated databases
RTU security compromised and SCADA system vulnerable to DoS and malicious control
Air gap breached in multiple locations allowing threats to propagate
Human Machine Interface (HMI)
Sensors
Remote Terminal Unit
Pressure
Pump/fan speed
Flow Rate
Remote Terminal Unit
Noise Level
Oil levels and Maintenance alarms
Radioactivity levels
Water levels
Temperature

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 7
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 8
What can be assigned using network access control policies?

A. Layer 3 polling intervals
B. FortiNAC device polling methods
C. Logical networks
D. Profiling rules

Answer: C

NEW QUESTION 9
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 10
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 10
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 14
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: C

NEW QUESTION 19
An OT administrator has configured FSSO and local firewall authentication. A user who is part of a user group is not prompted from credentials during authentication.
What is a possible reason?

A. FortiGate determined the user by passive authentication
B. The user was determined by Security Fabric
C. Two-factor authentication is not configured with RADIUS authentication method
D. FortiNAC determined the user by DHCP fingerprint method

Answer: A

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 25
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 28
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 31

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 35
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 40
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 45
......