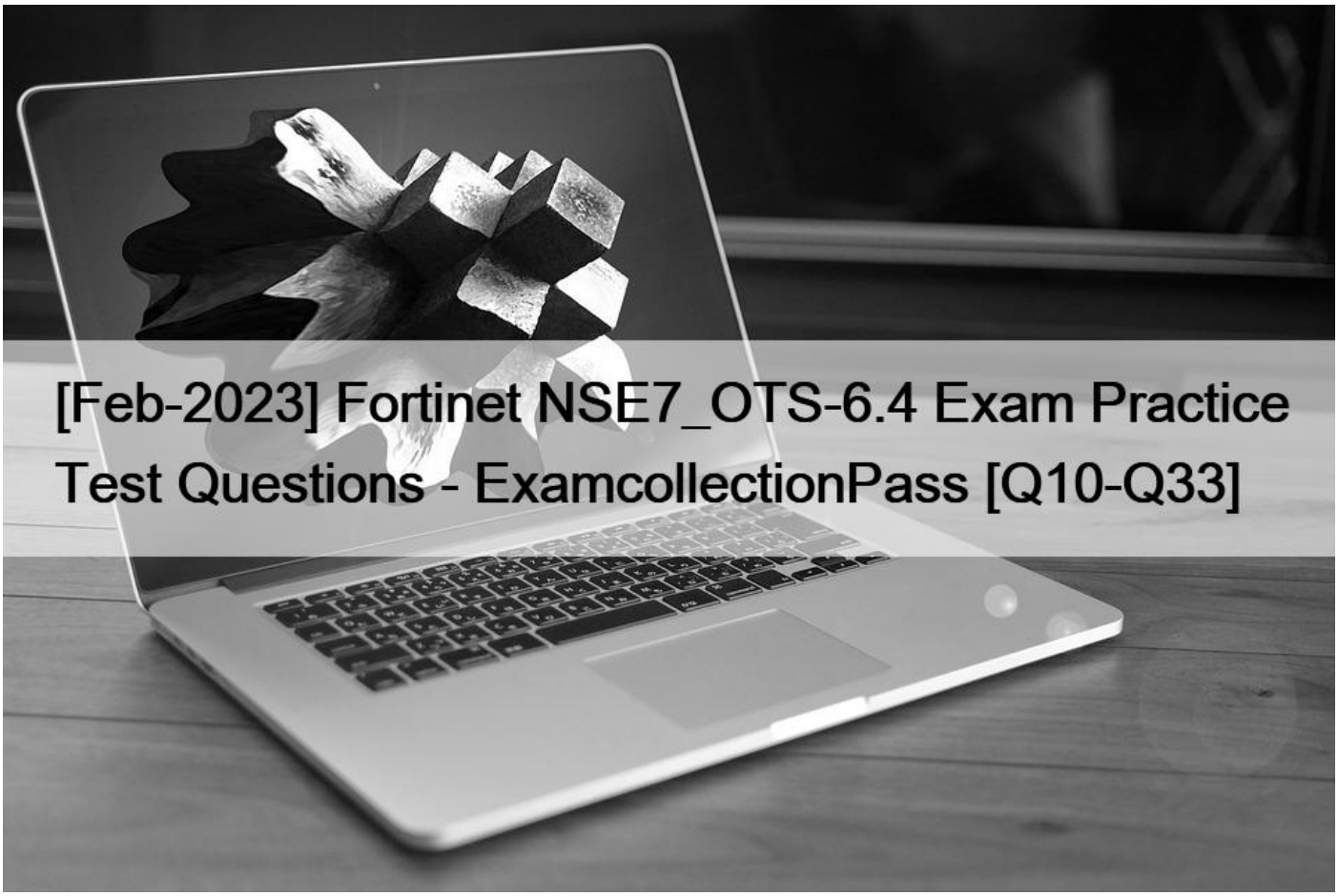
[Feb-2023 Fortinet NSE7_OTS-6.4 Exam Practice Test Questions - ExamcollectionPass [Q10-Q33



[Feb-2023] Fortinet NSE7_OTS-6.4 Exam Practice Test Questions - ExamcollectionPass
Updated Certification Exam NSE7_OTS-6.4 Dumps - Practice Test Questions

Following is the info about the Passing Score, Duration & Questions for the Fortinet NSE7_OTS-6.4 Exam

The passing score: Not foundLanguages: EnglishNumber of Questions: 35 questionsTime Duration: 60 minutes

What is the exam cost of Fortinet NSE7_OTS-6.4 Exam Certification

The exam cost of Fortinet NSE7_OTS-6.4 Certification Exam is $400 USD.

Q10. 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?

* FortiSIEM and FortiManager

* FortiSandbox and FortiSIEM
* FortiSOAR and FortiSIEM
* A syslog server and FortiSIEM

Q11. What triggers Layer 2 polling of infrastructure devices connected in the network?
* A failed Layer 3 poll
* A matched security policy
* A matched profiling rule
* A linkup or linkdown trap

Q12. 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 FortiSIEM CMDB report
* A FortiAnalyzer device report
* A FortiSIEM incident report
* A FortiSIEM analytics report

Q13. 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?
* It uses OSI Layer 2 and the primary device sends data based on request from secondary device.
* It uses OSI Layer 2 and both the primary/secondary devices always send data during the communication.
* It uses OSI Layer 2 and both the primary/secondary devices send data based on a matching token ring.
* It uses OSI Layer 2 and the secondary device sends data based on request from primary device.

Q14. What can be assigned using network access control policies?
* Layer 3 polling intervals
* FortiNAC device polling methods
* Logical networks

* Profiling rules

Q15. 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.)
* Security
* IPS
* List
* Risk
* Overview

Q16. 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?
* Configure a firewall policy with LDAP users and place it on the top of list of firewall policies.
* Enable two-factor authentication with FSSO.
* Configure a firewall policy with FSSO users and place it on the top of list of firewall policies.
* Under config user settings configure set auth-on-demand implicit.

Q17. Which three criteria can a FortiGate device use to look for a matching firewall policy to process traffic? (Choose three.)
* Services defined in the firewall policy.
* Source defined as internet services in the firewall policy
* Lowest to highest policy ID number
* Destination defined as internet services in the firewall policy
* Highest to lowest priority defined in the firewall policy

Q18. Which three common breach points can be found in a typical OT environment? (Choose three.)
* Global hat
* Hard hat
* VLAN exploits
* Black hat
* RTU exploits

Q19. 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.)
* You must set correct operator in event handler to trigger an event.
* You can automate SOC tasks through playbooks.
* Each playbook can include multiple triggers.
* You cannot use Windows and Linux hosts security events with FortiSoC.

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

Q20. Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)
* SNMP
* ICMP
* API
* RADIUS

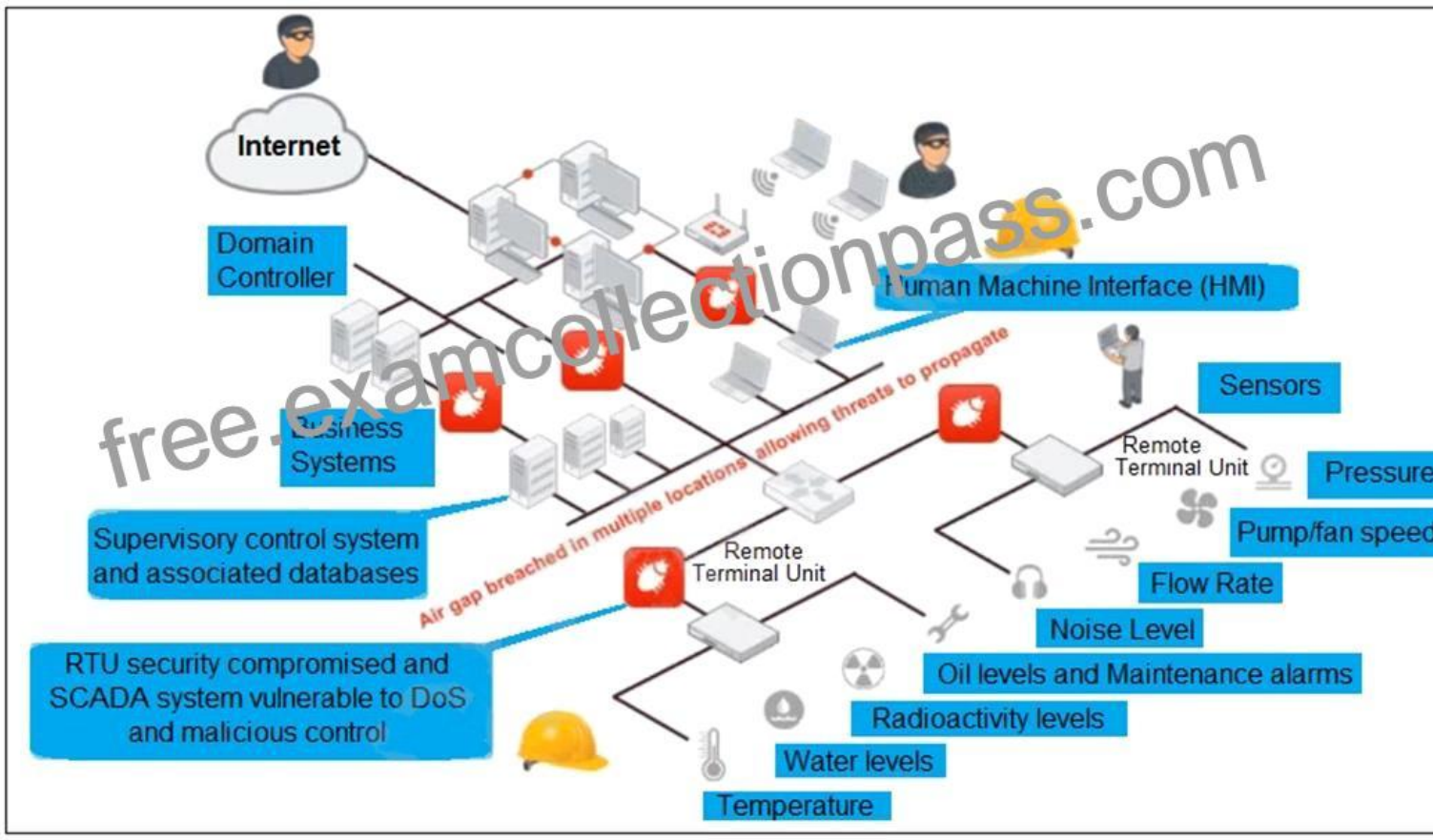
* TACACS

Q21. 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?
* Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.
* Create a notification policy and define a script/remediation on FortiSIEM.
* Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.
* Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.

Q22. Which three Fortinet products can be used for device identification in an OT industrial control system (ICS)? (Choose three.)
* FortiNAC
* FortiManager
* FortiAnalyzer
* FortiSIEM
* FortiGate

Q23. 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.)
* Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.
* Deploy a FortiGate device within each ICS network.
* Configure firewall policies with web filter to protect the different ICS networks.
* Configure firewall policies with industrial protocol sensors
* Use segmentation