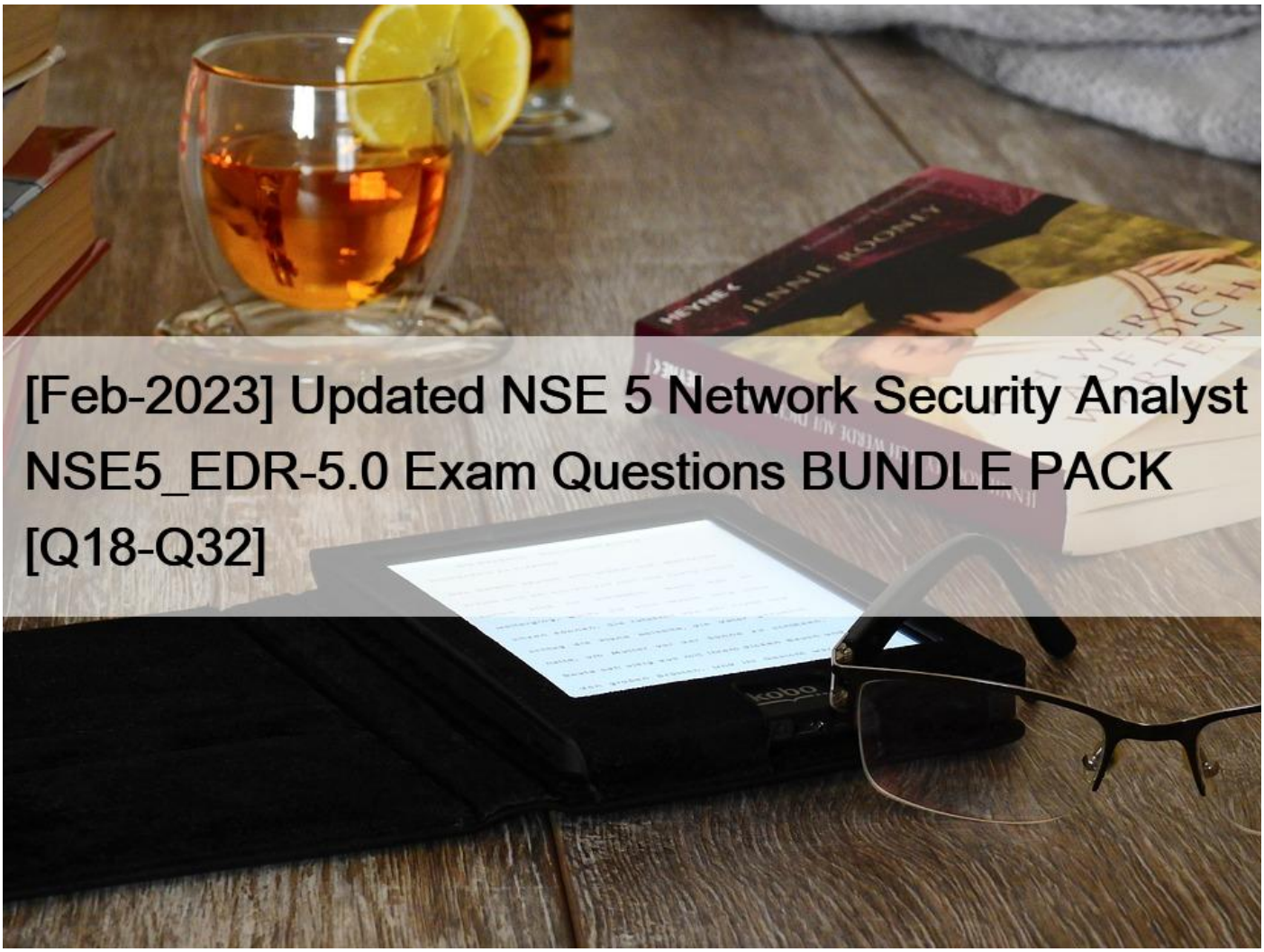
[Feb-2023 Updated NSE 5 Network Security Analyst NSE5_EDR-5.0 Exam Questions BUNDLE PACK [Q18-Q32



[Feb-2023 Updated NSE 5 Network Security Analyst NSE5_EDR-5.0 Exam Questions BUNDLE PACK Master The Fortinet Content NSE5_EDR-5.0 EXAM DUMPS WITH GUARANTEED SUCCESS!

Fortinet NSE5_EDR-5.0 Exam Syllabus Topics:

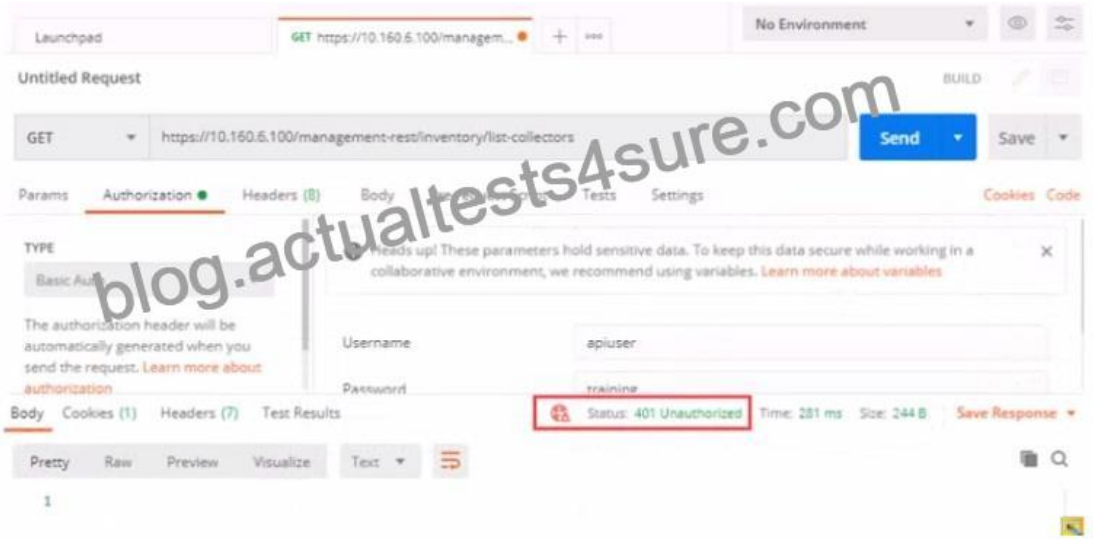
TopicDetailsTopic 1- Configure threat hunting profiles and scheduled queries- Perform FortiEDR inventory and use system tools
Topic 2- Analyze threat hunting data- FortiEDR troubleshooting, Configure playbooks, Deploy FortiXDRTopic 3- Configure security policies- Perform installation processTopic 4- Events, forensics, and threat hunting- Analyze security events and alertsTopic 5- Perform alert analysis on FortiEDR security events and logs- Explain FortiEDR architecture and technical positioningTopic 6- Use API to carry out FortiEDR management functions- FortiEDR security settings and policies

NEW QUESTION 18

What is the benefit of using file hash along with the file name in a threat hunting repository search?
* It helps to make sure the hash is really a malware
* It helps to check the malware even if the malware variant uses a different file name
* It helps to find if some instances of the hash are actually associated with a different file
* It helps locate a file as threat hunting only allows hash search

NEW QUESTION 19

Refer to the exhibit.



Based on the postman output shown in the exhibit why is the user getting an unauthorized error?
* The user has been assigned Admin and Rest API roles
* FortiEDR requires a password reset the first time a user logs in
* Postman cannot reach the central manager
* API access is disabled on the central manager

NEW QUESTION 20

A company requires a global communication policy for a FortiEDR multi-tenant environment.

How can the administrator achieve this?
* An administrator creates a new communication control policy and shares it with other organizations
* A local administrator creates new a communication control policy and shares it with other organizations
* A local administrator creates a new communication control policy and assigns it globally to all organizations
* An administrator creates a new communication control policy for each organization

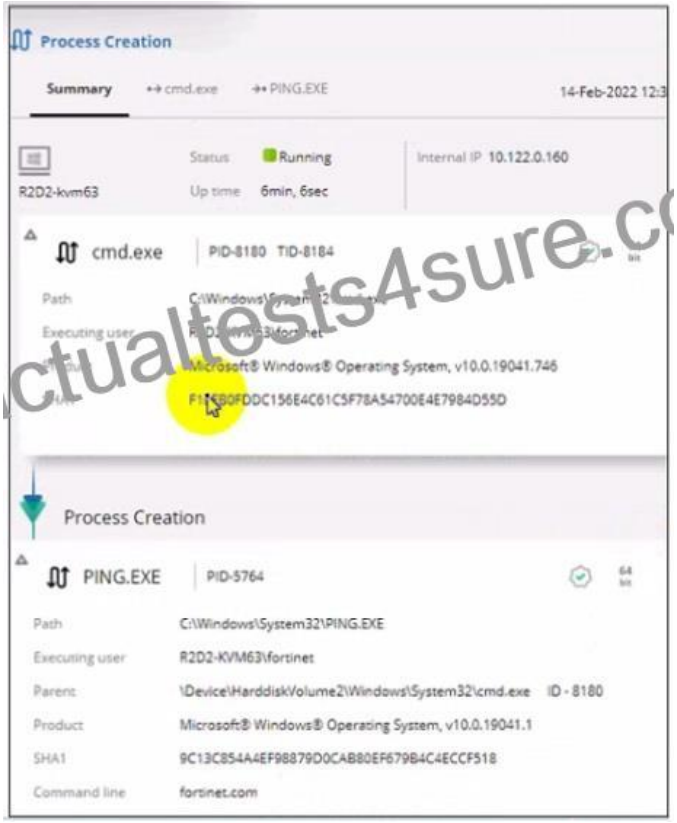
NEW QUESTION 21

Which threat hunting profile is the most resource intensive?
* Comprehensive
* Inventory
* Default

* Standard Collection

NEW QUESTION 22

Refer to the exhibit.



Based on the threat hunting event details shown in the exhibit, which two statements about the event are true?

(Choose two.)
* The PING EXE process was blocked
* The user fortinet has executed a ping command
* The activity event is associated with the file action
* There are no MITRE details available for this event

NEW QUESTION 23

Which two types of remote authentication does the FortiEDR management console support? (Choose two.)
* Radius
* SAML
* TACACS
* LDAP

NEW QUESTION 24

Refer to the exhibit.

Based on the threat hunting query shown in the exhibit which of the following is true?
* RDP connections will be blocked and classified as suspicious
* A security event will be triggered when the device attempts a RDP connection
* This query is included in other organizations
* The query will only check for network category

NEW QUESTION 25

An administrator needs to restrict access to the ADMINISTRATION tab inthe central manager for a specific account.

What role should the administrator assign to this account?
* Admin
* User
* Local Admin
* REST API

NEW QUESTION 26

What is the role of a collector in the communication control policy?
* A collector blocks unsafe applications from running
* A collector is used to change the reputation score of any application that collector runs
* A collector records applications that communicate externally
* A collector can quarantine unsafe applications from communicating

NEW QUESTION 27

How does FortiEDR implement post-infection protection?
* By preventing data exfiltration or encryption even after a breach occurs
* By using methods used by traditional EDR

* By insurance against ransomware
* By real-time filtering to prevent malware from executing

NEW QUESTION 28

Which connectors can you use for the FortiEDR automated incident response? (Choose two.)
* FortiNAC
* FortiGate
* FortiSiem
* FortiSandbox

NEW QUESTION 29

Refer to the exhibit.

Based on the event shown in the exhibit, which two statements about the event are true? (Choose two.)
* The NGAV policy has blocked TestApplication exe
* TestApplication exe is sophisticated malware
* The user was able to launch TestApplication exe
* FCS classified the event as malicious