Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

NSE7_ADA-6.3 Dumps
NSE7_ADA-6.3 Braindumps
NSE7_ADA-6.3 Real Questions
NSE7_ADA-6.3 Practice Test
NSE7_ADA-6.3 Actual Questions

Fortinet

NSE7_ADA-6.3

NSE 7 - Advanced Analytics 6.3

Question: 1

How can you invoke an integration policy on FortiSIEM rules?

A. Through Notification Policy settings
B. Through Incident Notification settings
C. Through remediation scripts
D. Through External Authentication settings

Answer: A

Explanation:

You can invoke an integration policy on FortiSIEM rules by configuring the Notification Policy settings. You can select an integration policy from the drop-down list and specify the conditions for triggering it. For example, you can invoke an integration policy when an incident is created, updated, or closed.

Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 9

Question: 2

How do customers connect to a shared multi-tenant instance on FortiSOAR?

A. The MSSP must provide secure network connectivity between the FortiSOAR manager node and the customer devices.
B. The MSSP must install a Secure Message Exchange node to connect to the customer's shared multi-tenant instance.
C. The customer must install a tenant node to connect to the MSSP shared multi-tenant instance.
D. The MSSP must install an agent node on the customer's network to connect to the customer's shared multi-tenant instance.

Answer: D

Explanation:

To connect to a shared multi-tenant instance on FortiSOAR, the MSSP must install an agent node on the customerâs network. The agent node acts as a proxy between the customerâs devices and the FortiSOAR manager node. The agent node also performs data collection, enrichment, and normalization for the customerâs data sources.

Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 11

Question: 3

In the event of a WAN link failure between the collector and the supervisor, by default, what is the maximum number of event files stored on the collector?

A. 30.000
B. 10.000
C. 40.000
D. 20.000

Answer: B

Explanation:

By default, the maximum number of event files stored on the collector in the event of a WAN link failure between the collector and the supervisor is 10.000. This value can be changed in the collector.properties file by modifying the parameter max_event_files_to_store.

Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 13

Question: 4

What is the disadvantage of automatic remediation?

A. It can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network.
B. It is equivalent to running an IPS in monitor-only mode â watches but does not block.
C. External threats or attacks detected by FortiSIEM will need user interaction to take action on an already overworked SOC team.
D. Threat behaviors occurring during the night could take hours to respond to.

Answer: A

Explanation:

The disadvantage of automatic remediation is that it can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network. Automatic remediation can have unintended consequences if not carefully planned and tested. Therefore, it is recommended to use manual or semi-automatic remediation for sensitive or critical systems.

Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 15

Question: 5

What are the modes of Data Ingestion on FortiSOAR? (Choose three.)

A. Rule based
B. Notification based
C. App Push
D. Policy based
E. Schedule based

Answer: A,B,C,E

Explanation:

The modes of Data Ingestion on FortiSOAR are notification based, app push, and schedule based. Notification based mode allows FortiSOAR to receive data from external sources via webhooks or email notifications. App push mode allows FortiSOAR to receive data from external sources via API calls or scripts. Schedule based mode allows

FortiSOAR to pull data from external sources at regular intervals using connectors.

Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 17

Question: 6

How can you empower SOC by deploying FortiSOAR? (Choose three.)

A. Aggregate logs from distributed systems
B. Collaborative knowledge sharing
C. Baseline user and traffic behavior
D. Reduce human error
E. Address analyst skills gap

Answer: A,B,D,E

Explanation:

You can empower SOC by deploying FortiSOAR in the following ways:

Collaborative knowledge sharing: FortiSOAR allows you to create and share playbooks, workflows, tasks, and notes among SOC analysts and teams. This enables faster and more consistent incident response and reduces duplication of efforts.

Reduce human error: FortiSOAR automates repetitive and tedious tasks, such as data collection, enrichment, analysis, and remediation. This reduces the risk of human error and improves efficiency and accuracy.

Address analyst skills gap: FortiSOAR provides a graphical user interface for creating and executing playbooks and workflows without requiring coding skills. This lowers the barrier for entry-level analysts and helps them learn from best practices and expert knowledge.

Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 19

Question: 7

Which of the following are two Tactics in the MITRE ATT&CK framework? (Choose two.)

A. Root kit
B. Reconnaissance
C. Discovery
D. BITS Jobs
E. Phishing

Answer: A,B,C

Explanation:

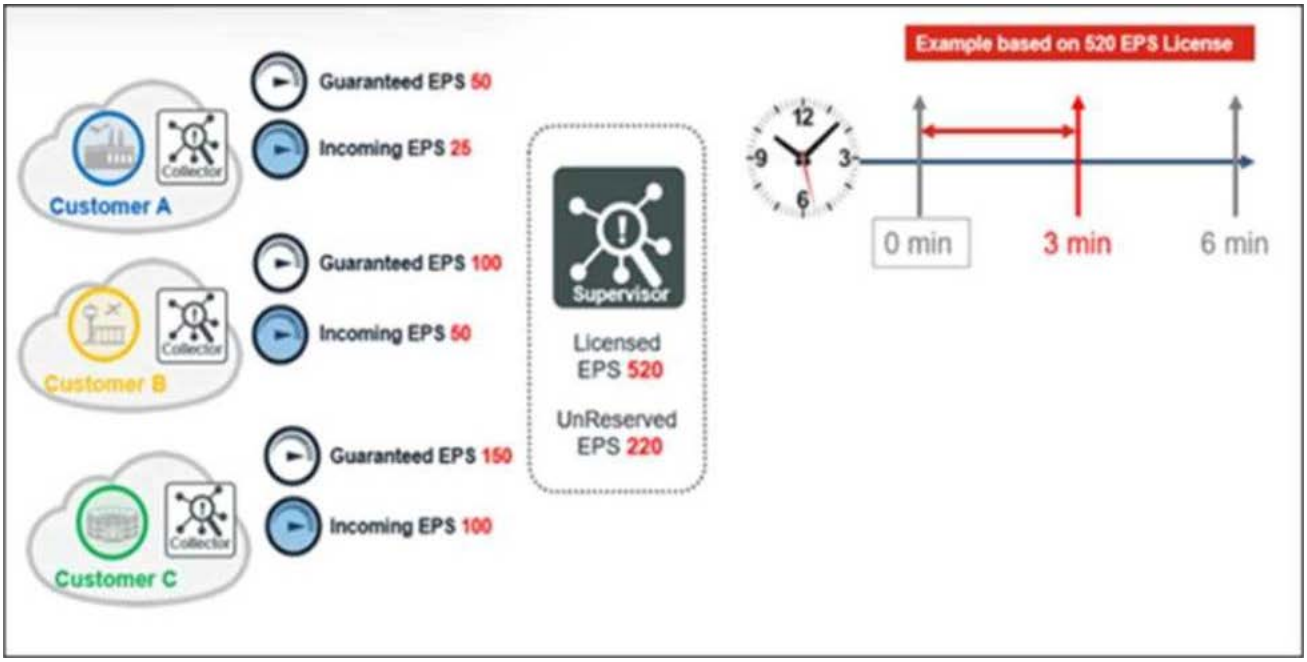
Reconnaissance and Discovery are two Tactics in the MITRE ATT&CK framework. Tactics are the high-level objectives of an adversary, such as initial access, persistence, lateral movement, etc. Reconnaissance is the tactic of gathering information about a target before launching an attack. Discovery is the tactic of exploring a compromised

system or network to find information or assets of interest.

Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 21

Question: 8

Refer to the exhibit. Click on the calculator button.



Based on the information provided in the exhibit, calculate the unused events for the next three minutes for a 520 EPS license.

A. 72460
B. 73460
C. 74460
D. 71460

Answer: B

Explanation:

The unused events for the next three minutes for a 520 EPS license can be calculated by multiplying the licensed EPS by the time interval and subtracting the total number of events received in that interval. In this case, the calculation is:

520 x 180 - 27000 = 73460

Question: 9

Refer to the exhibit.

```
<?xml version="1.0" encoding="UTF-8" ?>
<incident incidentId="723" ruleType="PH_RULE_VIRUS_BY_FIREWALL_NON_REMEDY" severity="9"
   repeatCount="1" organization="Aviation" status="0">
  <name>Malware found by firewall but not remediated</name>
  <remediation></remediation>
  <description>Detects that firewall content inspection devices found a virus but could not remediate it</description>
  <policyID></policyID>
  <displayTime>Thu Feb 06 13:56:00 EST 2020</displayTime>
  <incidentCategory>Security/Persistence</incidentCategory>
  <incidentSource>
  <entry attribute="srcIpAddr" name="Source IP">10.0.3.10
 (Win_Agent)</entry>
  </incidentSource>
  <incidentTarget>
  </incidentTarget>
  <incidentDetails>
  <entry attribute="virusName" name="Malware Name">EICAR_TEST_FILE</entry>

  </incidentDetails>
  <affectedBizSrvc>null</affectedBizSrvc>
  <identityLocation>
</identityLocation>  </incident>
```

An administrator wants to remediate the incident from FortiSIEM shown in the exhibit.

What option is available to the administrator?

A. Quarantine IP FortiClient
B. Run the block MAC FortiO
C. Run the block IP FortiOS 5.4
D. Run the block domain Windows DNS

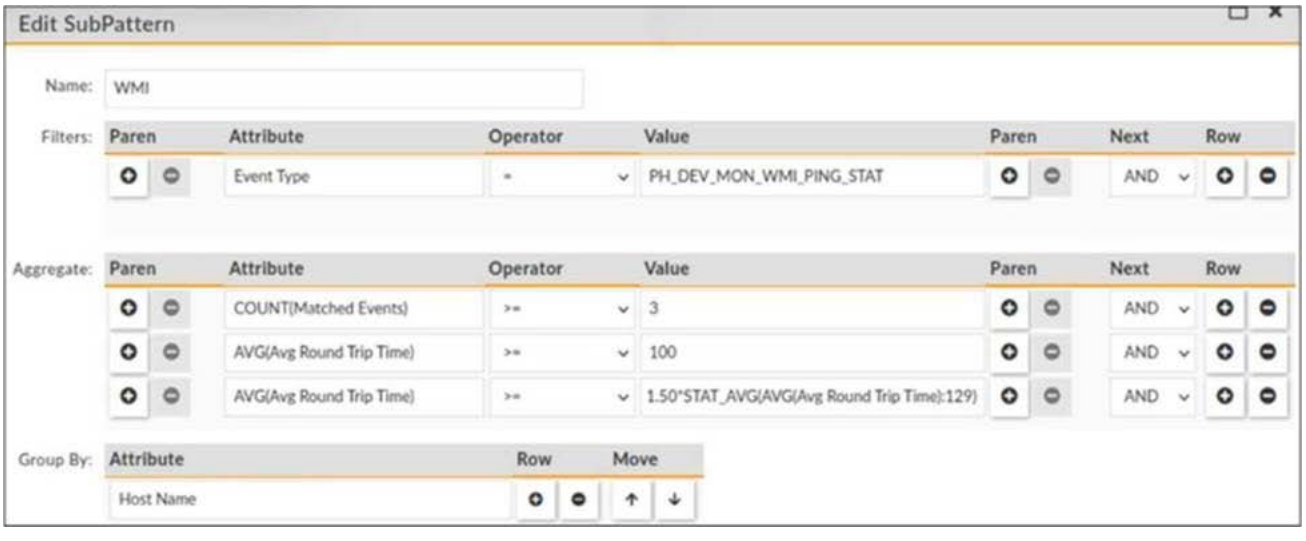
Answer: B

Explanation:

The incident from FortiSIEM shown in the exhibit is a brute force attack on a FortiGate device. The remediation option available to the administrator is to run the block IP FortiOS 5.4 action, which will block the source IP address of the attacker on the FortiGate device using a firewall policy.

Question: 10

Refer to the exhibit.



The window for this rule is 30 minutes.

What is this rule tracking?

A. A sudden 50% increase in WMI response times over a 30-minute time window
B. A sudden 1.50 times increase in WMI response times over a 30-minute time window
C. A sudden 75% increase in WMI response times over a 30-minute time window
D. A sudden 150% increase in WMI response times over a 30-minute time window

Answer: B

Explanation:

The rule is tracking the WMI response times from Windows devices using a baseline calculation. The rule will trigger an incident if the current WMI response time is greater than or equal to 1.50 times the average WMI response time in the last 30 minutes.

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*