NSE7_ADA-6.3 Q&As

Fortinet NSE 7 - Advanced Analytics 6.3

Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse7_ada-6-3.html

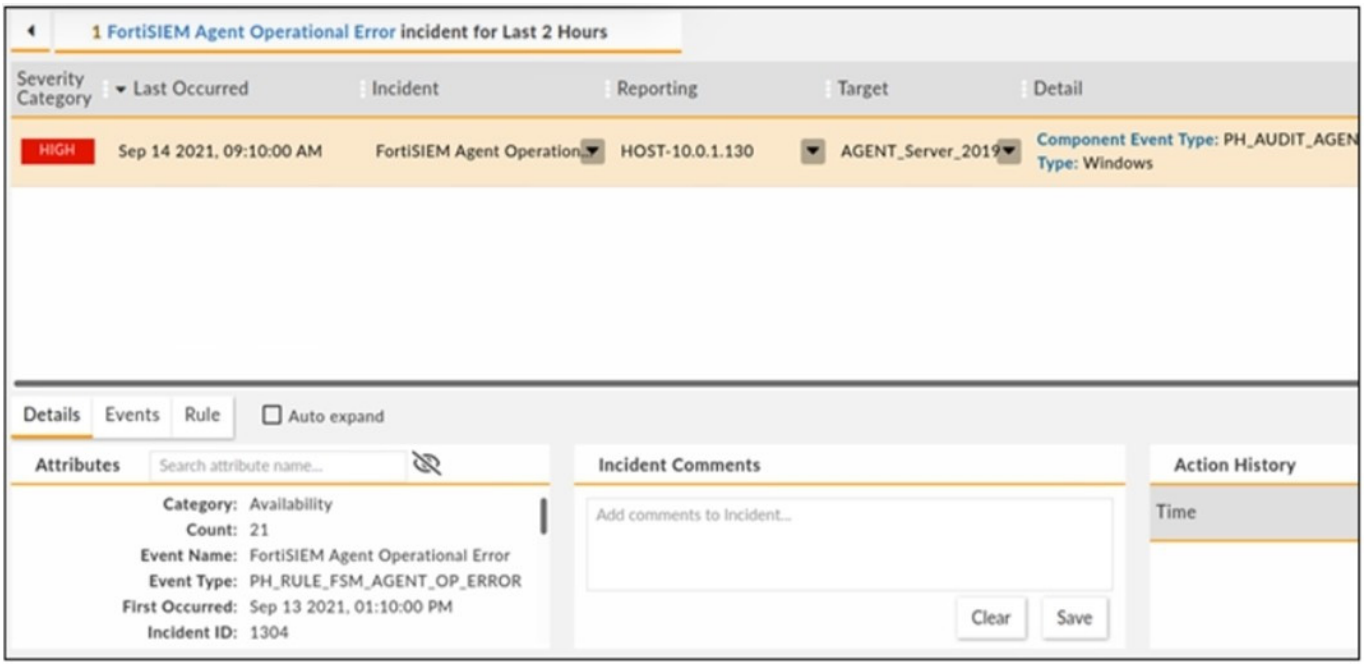
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit.



How long has the UEBA agent been operationally down?

A. 21 Hours

B. 9 Hours

C. 20 Hours

D. 2 Hours

Correct Answer: A

Explanation: The UEBA agent status shows that it has been operationally down for one day and three hours ago (1d3h). This means that it has been down for 24 hours plus three hours, which is equal to 21 hours.

QUESTION 2

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 FortiOS.

C. Run the block IP FortiOS 5.4

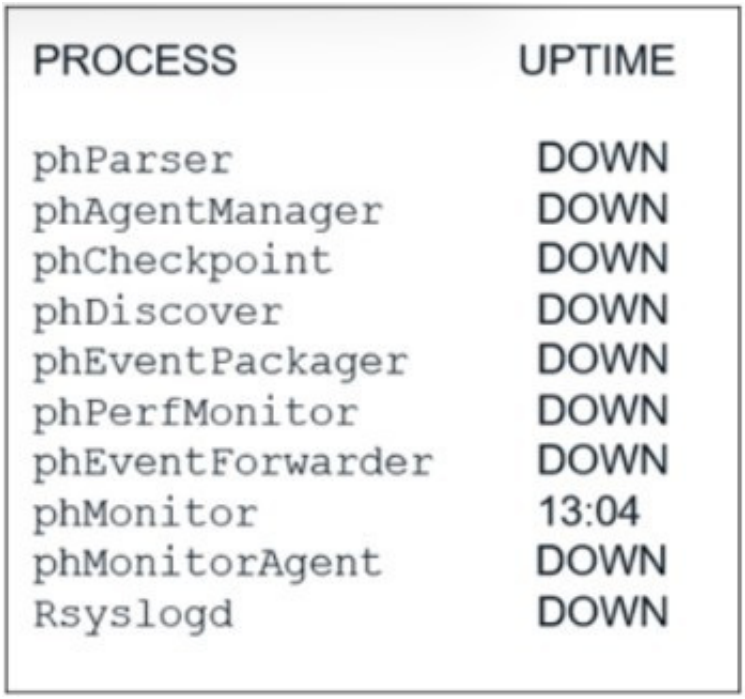
D. Run the block domain Windows DNS

Correct Answer: C

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 3

Refer to the exhibit.



PROCESS	UPTIME
phParser	DOWN
phAgentManager	DOWN
phCheckpoint	DOWN
phDiscover	DOWN
phEventPackager	DOWN
phPerfMonitor	DOWN
phEventForwarder	DOWN
phMonitor	13:04
phMonitorAgent	DOWN
Rsyslogd	DOWN

An administrator deploys a new collector for the first time, and notices that all the processes except the phMonitor are down. How can the administrator bring the processes up?

A. The administrator needs to run the command phtools --start all on the collector.

B. Rebooting the collector will bring up the processes.

C. The processes will come up after the collector is registered to the supervisor.

D. The collector was not deployed properly and must be redeployed.

Correct Answer: C

Explanation: The collector processes are dependent on the registration with the supervisor. The phMonitor process is responsible for registering the collector to the supervisor and monitoring the health of other processes. After the registration is successful, the phMonitor will start the other processes on the collector.

QUESTION 4

Refer to the exhibit.

Event Receive Time	Event Type	Source IP	Destination IP	Reporting IP	User	Raw Event Log
08:49:01 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:49:24 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02…
08:50:45 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:55:09 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.5	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Sarah	<189>date=2018-02-02…
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02…

An administrator runs an analytic search for all FortiGate SSL VPN logon failures. The results are grouped by source IP, reporting IP, and user. The administrator wants to restrict the results to only those rows where the COUNT >= 3. Which user would meet that condition?

A. Sarah

B. Jan

C. Tom

D. Admin

Correct Answer: C

Explanation: The user who would meet that condition is Tom. Tom has four rows in the results where the COUNT is greater than or equal to three, meaning he had at least three SSL VPN logon failures from the same source IP and reporting IP. The other users have either less than three rows or less than three COUNT in each row.

QUESTION 5

Which syntax will register a collector to the supervisor?

A. phProvisionCollector --add

B. phProvisionCollector --add

C. phProvisionCollector --add

D. phProvisionCollector --add

Correct Answer: B

Explanation: The syntax that will register a collector to the supervisor is phProvisionCollector --add . This command will initiate the registration process between the collector and the supervisor, and exchange certificates and configuration information. The parameter is the IP address of the supervisor node.

Questions