

NSE5_EDR-5.0^{Q&As}

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse5_edr-5-0.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



https://www.pass2lead.com/nse5_edr-5-0.html

2024 Latest pass2lead NSE5_EDR-5.0 PDF and VCE dumps Download

QUESTION 1

| Which connectors car | you use for the FortiED | R automated incident res | sponse? (Choose two.) |
|----------------------|-------------------------|--------------------------|-----------------------|
|----------------------|-------------------------|--------------------------|-----------------------|

- A. FortiNAC
- B. FortiGate
- C. FortiSiem
- D. FortiSandbox

Correct Answer: AB

QUESTION 2

Which statement is true about the flow analyzer view in forensics?

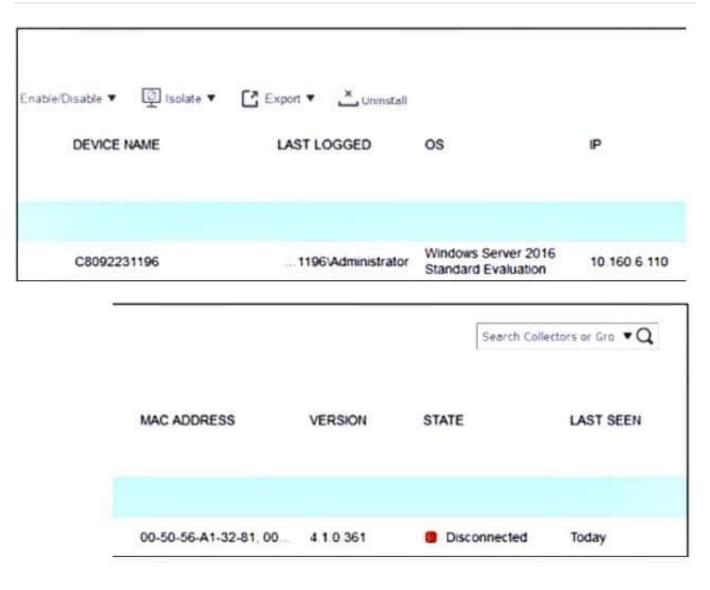
- A. It displays a graphic flow diagram.
- B. Two events can be compared side-by-side.
- C. It shows details about processes and sub processes.
- D. The stack memory of a specific device can be retrieved

Correct Answer: A

QUESTION 3

Refer to the exhibits.





| Admini | strator: Command Prompt | | |
|----------|-------------------------|-------------------|-------------|
| C:\Users | \Administrator>netsta | t -an | |
| Active C | onnections | | |
| Proto | Local Address | Foreign Address | State |
| TCP | 0.0.0.0:135 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:445 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:5985 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:49692 | 0.0.0.0:0 | LISTENING |
| TCP | 10.160.6.110:139 | 0.0.0.0:0 | LISTENING |
| TCP | 10.160.6.110:50853 | 10.160.6.100:8080 | SYN_SENT |
| TCP | 172.16.9.19:139 | 0.0.0.0:0 | LISTENING |
| TCP | 172.16.9.19:49687 | 52.177.165.30:443 | ESTABLISHED |
| | | | |

The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address 10.160.6.100 using default port. Based on the netstat command output what must you do to resolve the connectivity issue?



https://www.pass2lead.com/nse5_edr-5-0.html

2024 Latest pass2lead NSE5_EDR-5.0 PDF and VCE dumps Download

- A. Reinstall collector agent and use port 443
- B. Reinstall collector agent and use port 8081
- C. Reinstall collector agent and use port 555
- D. Reinstall collector agent and use port 6514

Correct Answer: B

QUESTION 4

A FortiEDR security event is causing a performance issue with a third-parry application. What must you do first about the event?

- A. Contact Fortinet support
- B. Terminate the process and uninstall the third-party application
- C. Immediately create an exception
- D. Investigate the event to verify whether or not the application is safe

Correct Answer: D

QUESTION 5

What is the role of a collector in the communication control policy?

- A. A collector blocks unsafe applications from running
- B. A collector is used to change the reputation score of any application that collector runs
- C. A collector records applications that communicate externally
- D. A collector can quarantine unsafe applications from communicating

Correct Answer: C

NSE5 EDR-5.0 Practice
Test

NSE5 EDR-5.0 Study
Guide

NSE5_EDR-5.0 Braindumps