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.passapply.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

QUESTION 1

Which three steps does FortiXDR perform to find and prevent cyberattacks? (Choose three.)

A. Extended analysis

B. Extended detection

C. Extended discovery

D. Extended investigation

E. Extended response

Correct Answer: BDE

QUESTION 2

Which two types of traffic are allowed while the device is in isolation mode? (Choose two.)

A. Outgoing SSH connections

B. HTTP sessions

C. ICMP sessions D. Incoming RDP connections

Correct Answer: CD

QUESTION 3

How does FortiEDR implement post-infection protection?

A. By preventing data exfiltration or encryption even after a breach occurs

B. By using methods used by traditional EDR

C. By insurance against ransomware

D. By real-time filtering to prevent malware from executing

Correct Answer: A

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf

QUESTION 4

Refer to the exhibit.

The exhibit shows an event viewer.

▼ All	ID	DEVICE	PROCESS
Payroll Manager.exe (3 events)			
☐ ▶	9715	⬛ cwinserv-32 🖥	Payroll Manager.exe
▷ ⬢⬛ User: CWINSERV-32\Administrator		Certificate: Unsigned	Process path: .
☐ ▶	9695	⬛ cwinserv-32 🖥	Payroll Manager.exe
☐ ▶	8878	⬛ cwinserv-32 🖥	Payroll Manager.exe
CryptoLocker2.exe (1 event)			

CLASSIFICATION ▲	DESTINATIONS	RECEIVED ▼	LAST UPDATED	
⊕ Suspicious		25-Nov-2020, 06:09:07		
⊕ Suspicious	74.125.235.20	25-Nov-2020, 06:09:07	25-Nov-2020, 06:09:07	⊘
..inistrator\Downloads\Resources\TestFiles\Fake Malware\Payroll Manager.exe Raw data items: 1				
⊕ Suspicious	74.125.235.20	25-Nov-2020, 06:07:43	25-Nov-2020, 06:07:43	⊘
⊕ Suspicious	74.125.235.20	21-Sep-2020, 06:45:53	21-Sep-2020, 11:21:11	⊘
⊕ Malicious		28-Sep-2020, 05:46:35		

What is true about the Payroll Manager.exe event?

A. An event has not been handled by a console admin

B. An event has been deleted

C. A rule assigned action is set to block but the policy is in simulation mode

D. An event has been handled by the communication control policy

Correct Answer: C

QUESTION 5

Which FortiEDR component must have JumpBox functionality to connect with FortiAnalyzer?

A. Collector

B. Core

C. Central manager

D. Aggregator

Correct Answer: B

You need an on premise CORE , with jump box functionality and valid API access, to Gate, Analyzer, NAC and or Sandbox.

Latest NSE5_EDR-5.0 Dumps   NSE5_EDR-5.0 Practice Test   NSE5_EDR-5.0 Braindumps