NSE8_812 Q&As

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

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

https://www.passapply.com/nse8_812.html

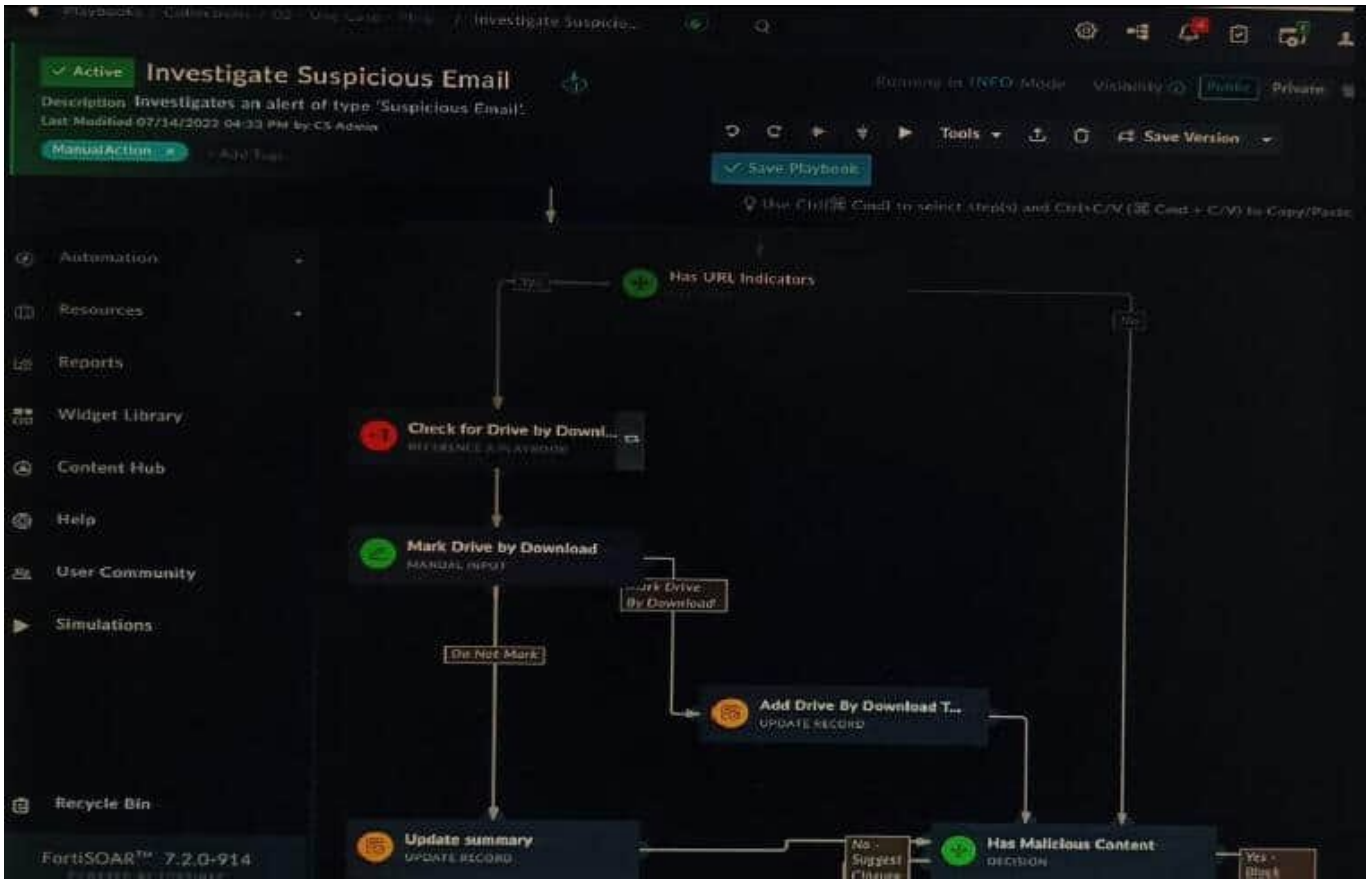
100% Passing Guarantee
100% Money Back Assurance

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 showing a FortiSOAR playbook.



You are investigating a suspicious e-mail alert on FortiSOAR, and after reviewing the executed playbook, you can see that it requires intervention.

What should be your next step?

A. Go to the Incident Response tasks dashboard and run the pending actions

B. Click on the notification icon on FortiSOAR GUI and run the pending input action

C. Run the Mark Drive by Download playbook action

D. Reply to the e-mail with the requested Playbook action

Correct Answer: A

Explanation: The exhibited playbook requires intervention, which means that the playbook has reached a point where it needs a human operator to take action. The next step should be to go to the Incident Response tasks dashboard and run

the pending actions. This will allow you to see the pending actions that need to be taken and to take those actions. The other options are not correct. Option B will only show you the notification icon, but it will not allow you to run the pending

input action. Option C will run the Mark Drive by Download playbook action, but this is not the correct action to take in this case. Option D is not a valid option.

Here are some additional details about pending actions in FortiSOAR:

Pending actions are actions that need to be taken by a human operator. Pending actions are displayed in the Incident Response tasks dashboard. Pending actions can be run by clicking on the action in the dashboard.

QUESTION 2

You are responsible for recommending an adapter type for NICs on a FortiGate VM that will run on an ESXi Hypervisor. Your recommendation must consider performance as the main concern, cost is not a factor. Which adapter type for the NICs will you recommend?

A. Native ESXi Networking with E1000

B. Virtual Function (VF) PCI Passthrough

C. Native ESXi Networking with VMXNET3

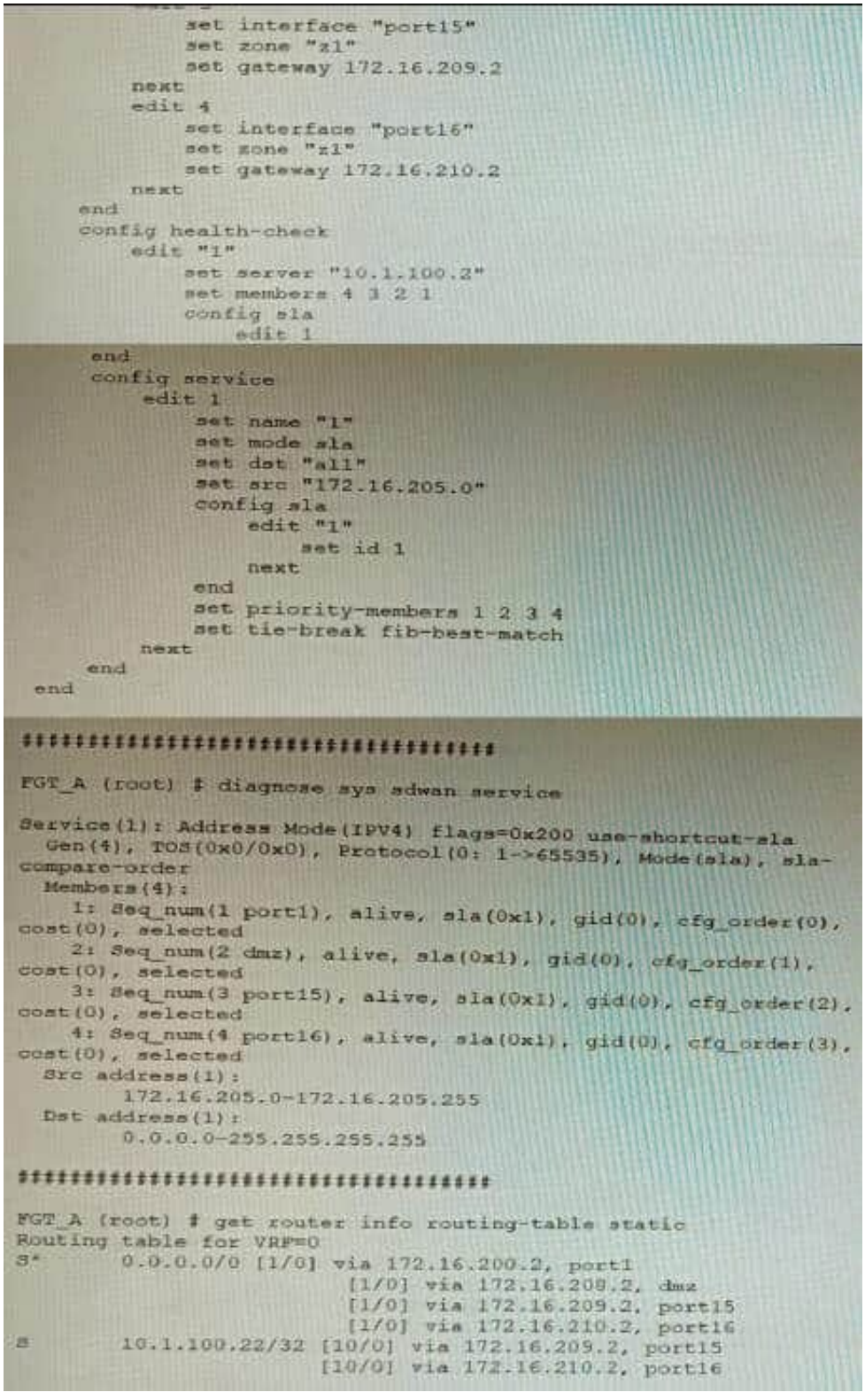
D. Physical Function (PF) PCI Passthrough

Correct Answer: C

Explanation: The FortiGate VM is a virtual firewall appliance that can run on various hypervisors, such as ESXi, Hyper-V, KVM, etc. The adapter type for NICs on a FortiGate VM determines the performance and compatibility of the network interface cards with the hypervisor and the physical network. There are different adapter types available for NICs on a FortiGate VM, such as E1000, VMXNET3, SR-IOV, etc. If performance is the main concern and cost is not a factor, one option is to use native ESXi networking with VMXNET3 adapter type for NICs on a FortiGate VM that will run on an ESXi hypervisor. VMXNET3 is a paravirtualized network interface card that is optimized for performance in virtual machines and supports features such as multiqueue support, Receive Side Scaling (RSS), Large Receive Offload (LRO), IPv6 offloads, and MSI/MSI-X interrupt delivery. Native ESXi networking means that the FortiGate VM uses the standard virtual switch (vSwitch) or distributed virtual switch (dvSwitch) provided by the ESXi hypervisor to connect to the physical network. This option can provide high performance and compatibility for NICs on a FortiGate VM without requiring additional hardware or software components. References: https://docs.fortinet.com/document/fortigate/7.0.0/vm-installation- for-vmware-esxi/19662/installing-fortigate-vm-on-vmware- esxihttps://docs.fortinet.com/document/fortigate/7.0.0/vm-installationfor-vmware- esxi/19662/networking

QUESTION 3

Refer to the exhibit showing an SD-WAN configuration. According to the exhibit, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, which outgoing interfaces will be used?



```
            set interface "port15"
            set zone "z1"
            set gateway 172.16.209.2
        next
        edit 4
            set interface "port16"
            set zone "z1"
            set gateway 172.16.210.2
        next
    end
    config health-check
        edit "1"
            set server "10.1.100.2"
            set members 4 3 2 1
            config sla
                edit 1
    end
    config service
        edit 1
            set name "1"
            set mode sla
            set dst "all"
            set src "172.16.205.0"
            config sla
                edit "1"
                    set id 1
                next
            end
            set priority-members 1 2 3 4
            set tie-break fib-best-match
        next
    end
end

####################################

FGT_A (root) # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-
compare-order
  Members(4):
    1: Seq_num(1 port1), alive, sla(0x1), gid(0), cfg_order(0),
cost(0), selected
    2: Seq_num(2 dmz), alive, sla(0x1), gid(0), cfg_order(1),
cost(0), selected
    3: Seq_num(3 port15), alive, sla(0x1), gid(0), cfg_order(2),
cost(0), selected
    4: Seq_num(4 port16), alive, sla(0x1), gid(0), cfg_order(3),
cost(0), selected
  Src address(1):
        172.16.205.0-172.16.205.255
  Dst address(1):
        0.0.0.0-255.255.255.255

####################################

FGT_A (root) # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 172.16.200.2, port1
                        [1/0] via 172.16.208.2, dmz
                        [1/0] via 172.16.209.2, port15
                        [1/0] via 172.16.210.2, port16
S       10.1.100.22/32 [10/0] via 172.16.209.2, port15
                       [10/0] via 172.16.210.2, port16
```

A. port16 and port1

B. port1 and port1

C. port16 and port15

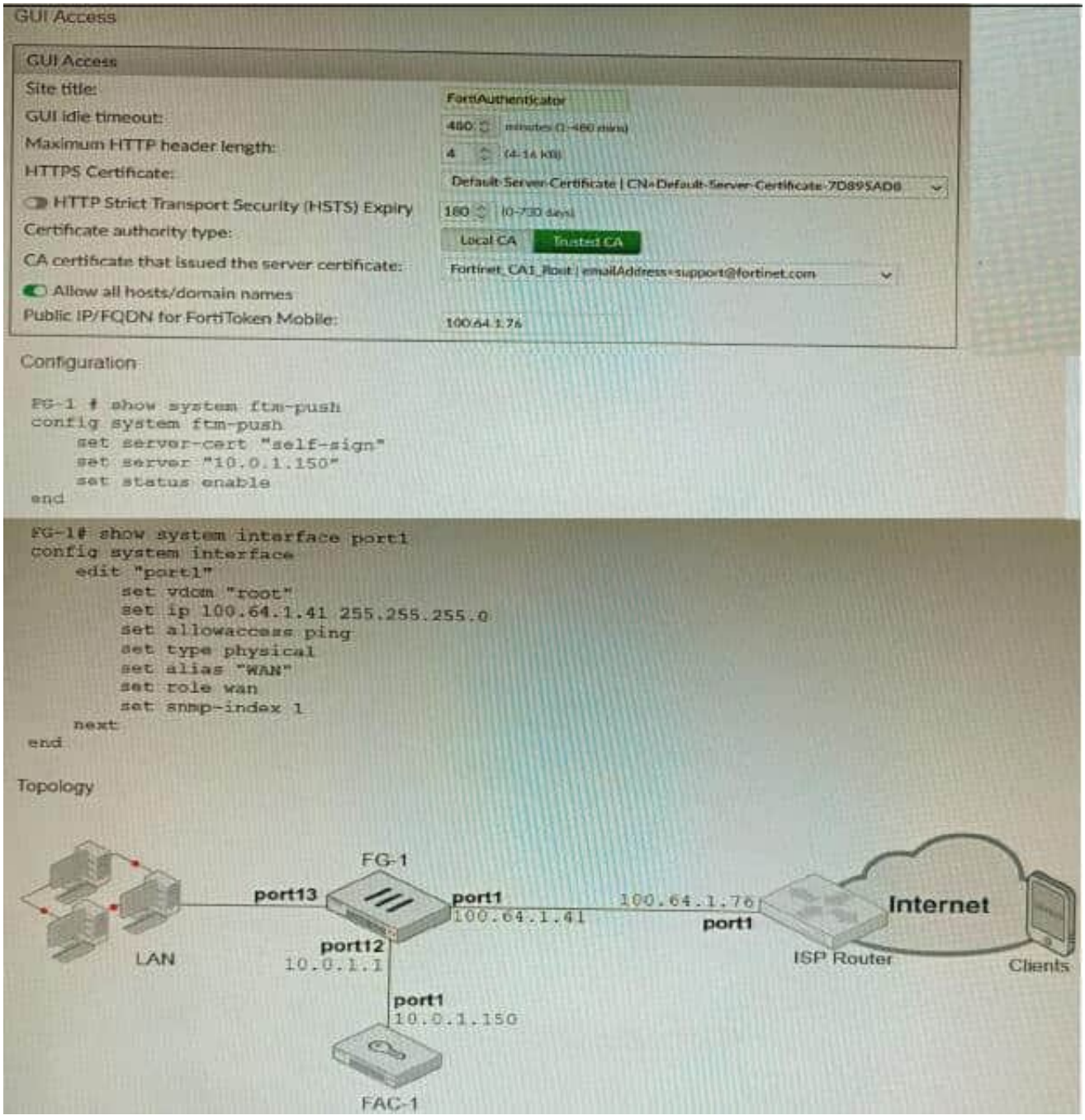
D. port1 and port15

Correct Answer: A

Explanation: According to the exhibit, the SD-WAN configuration has two rules: one for traffic to 10.1.100.0/24 subnet, and one for traffic to 10.1.100.16/28 subnet. The first rule uses the best quality strategy, which selects the SD-WAN member with the best measured quality based on performance SLA metrics. The second rule uses the manual strategy, which specifies port1 as the SD-WAN member to select. Therefore, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, the outgoing interfaces will be port16 and port1 respectively, assuming that port16 has the best quality among the SD- WAN members.
References:https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/218559/configurin g-the-sd-wan-interface

QUESTION 4

Refer to the exhibits.



An administrator has configured a FortiGate and Forti Authenticator for two-factor authentication with FortiToken push notifications for their SSL VPN login. Upon initial review of the setup, the administrator has discovered that the customers can manually type in their two-factor code and authenticate but push notifications do not work

Based on the information given in the exhibits, what must be done to fix this?

A. On FG-1 port1, the ftm access protocol must be enabled.

B. FAC-1 must have an internet routable IP address for push notifications.

C. On FG-1 CLI, the ftm-push server setting must point to 100.64.141.

D. On FAC-1, the FortiToken public IP setting must point to 100.64.1 41

Correct Answer: B

Explanation: FortiToken push notifications require that the FortiAuthenticator has an internet routable IP address. This is because the FortiAuthenticator uses this IP address to send push notifications to the FortiGate.

The other options are not correct. Enabling the ftm access protocol on FG-1 port1 is not necessary for push notifications to work. The ftm-push server setting on FG-1 CLI should already point to the FortiAuthenticator\\'s IP address. The

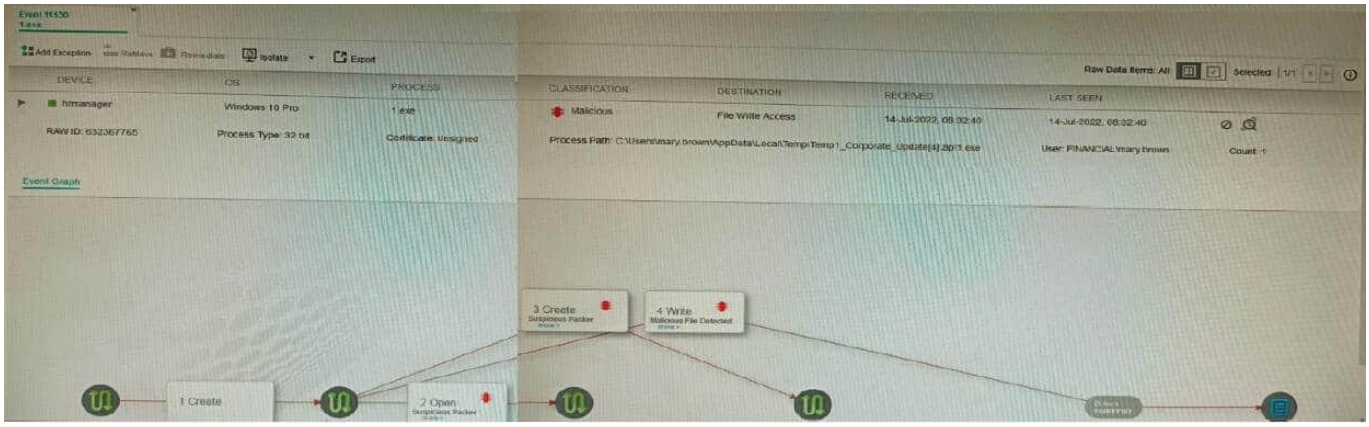
FortiToken public IP setting on FAC-1 is not relevant to push notifications.

Here is a table that summarizes the different options:

Option	Description
Enable the ftm access protocol on FG-1 port1	Not necessary for push notifications to work.
Set the ftm-push server setting on FG-1 CLI to the FortiAuthenticator's IP address	Already done.
Set the FortiToken public IP setting on FAC-1 to 100.64.141	Not relevant to push notifications.
Set the FortiAuthenticator's IP address to an internet routable IP address	Necessary for push notifications to work.

QUESTION 5

Refer to the exhibit.



The exhibit shows the forensics analysis of an event detected by the FortiEDR core

In this scenario, which statement is correct regarding the threat?

A. This is an exfiltration attack and has been stopped by FortiEDR.

B. This is an exfiltration attack and has not been stopped by FortiEDR

C. This is a ransomware attack and has not been stopped by FortiEDR.

D. This is a ransomware attack and has been stopped by FortiEDR

Correct Answer: B

Explanation: The exhibit shows that the FortiEDR core has detected an exfiltration attack. The attack is attempting to copy files from the device to an external location. The FortiEDR core has blocked the attack, and the files have not been

exfiltrated. The exhibit also shows that the attack is using the Cobalt Strike beacon. Cobalt Strike is a penetration testing tool that can be used for both legitimate and malicious purposes. In this case, the Cobalt Strike beacon is being used to

exfiltrate files from the device. The other options are incorrect. Option A is incorrect because the attack has not been stopped. Option C is incorrect because the attack is not a ransomware attack. Option D is incorrect because the FortiEDR

core has not stopped the attack.

References:

FortiEDR Forensics:

https://docs.fortinet.com/document/fortiedr/6.0.0/administration- guide/733983/forensics

Cobalt Strike: https://www.cobaltstrike.com/