Vendor: Fortinet

Exam Code: NSE6_EDR_AD-7.0

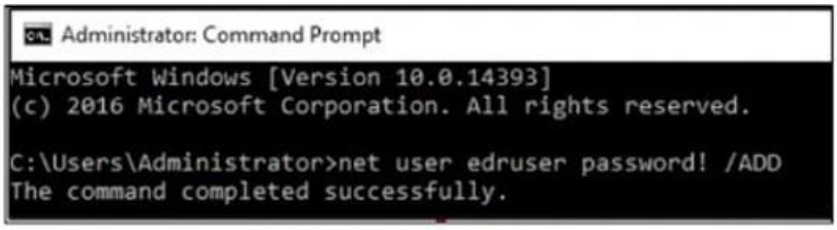
Exam Name: Fortinet NSE 6 - FortiEDR 7.0 Administrator

Version: DEMO

QUESTION 1
Refer to the exhibits. What happens when the `net user` command runs on an endpoint?

Query configuration

CLI output

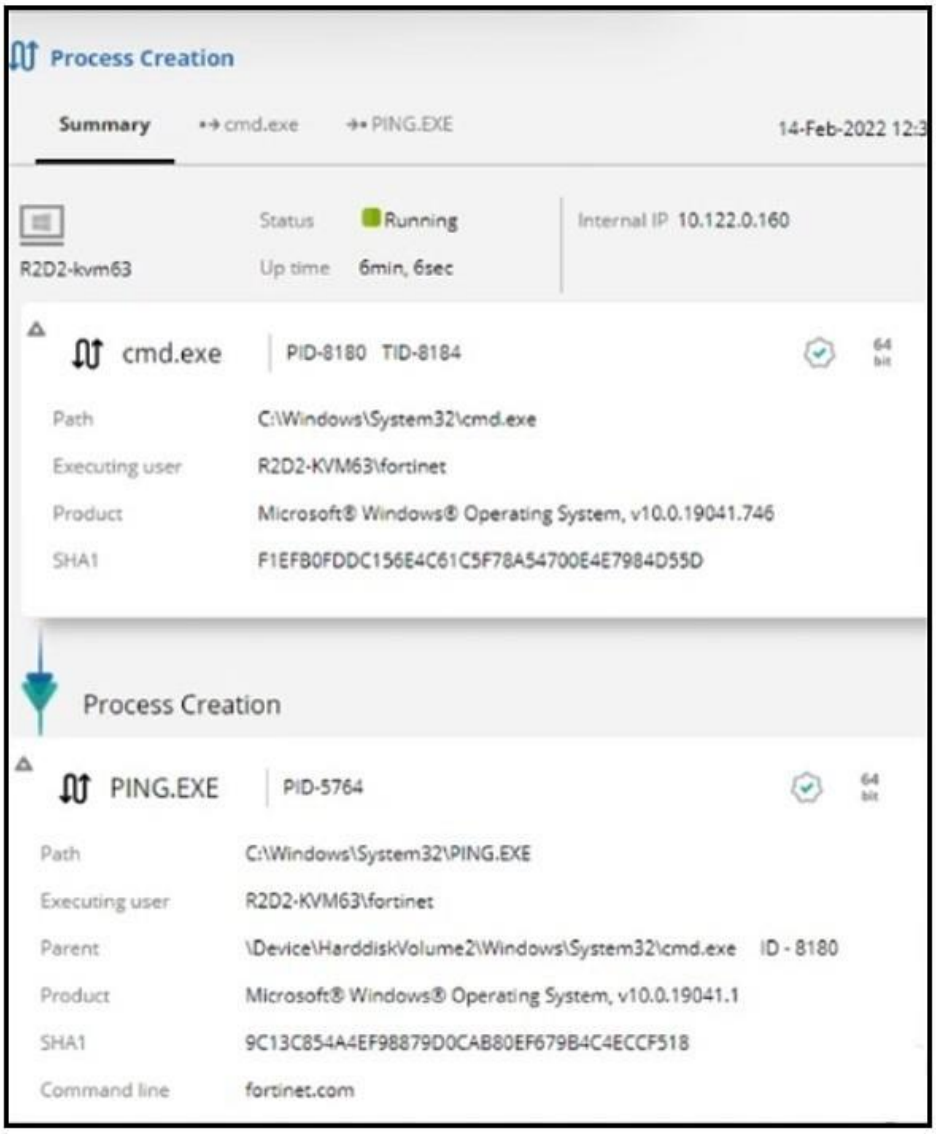


A. It triggers FortiEDR rules because the activity is not suspicious.
B. It triggers CLI commands by default.
C. It triggers an incident when the query matches the target process (net.exe).
D. It triggers an immediate endpoint alert.

Answer: C
Explanation:
The query is configured to detect executions of the process net.exe and is scheduled to run periodically with a suspicious classification. When the command runs on an endpoint, the query matches the target process and FortiEDR generates an incident based on the defined hunting rule.

QUESTION 2
Refer to the exhibit. Based on the threat hunting event details shown in the exhibit, which two statements about the event are true? (Choose two.)

Threat hunting event details



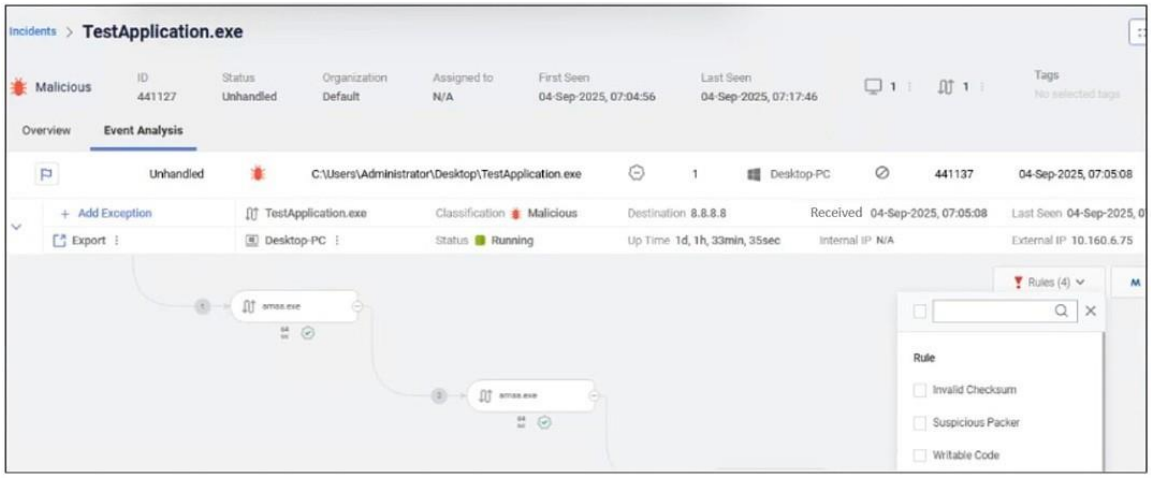
A. The user Fortinet has executed a ping command.
B. The activity event is associated with the file action.
C. There are no MITRE details available for this event.
D. The PING.EXE process was blocked.

Answer: AC
Explanation:
The event shows that cmd.exe launched PING.EXE with the command line parameter fortinet.com and lists the executing user as fortinet, indicating that this user executed the ping command. The event view does not display any MITRE ATT&CK technique mapping or related details, indicating that MITRE information is not available for this event.

QUESTION 3

Refer to the exhibit. Based on the event shown in the exhibit, which two statements about the event are true? (Choose two.)

Event



A. The user was able to launch TestApplication.exe.
B. The event is marked as Handled.
C. FCS classified the event as malicious.
D. TestApplication.exe is sophisticated malware.

Answer: AC
Explanation:
The event view shows the process TestApplication.exe with status Running, indicating the application was successfully launched on the endpoint. The classification label indicates the event is marked as malicious and the classification source is FortinetCloudServices, confirming that FCS performed the malicious classification.

QUESTION 4
You are asked to create a playbook to isolate a device with a collector. Which action category does isolating a device with a collector fall under?

A. Investigation
B. Custom
C. Notifications
D. Remediation

Answer: D
Explanation:
Isolating a device is an automated response action used to contain a threat by restricting the endpoint's network communication. In FortiEDR playbooks, containment and corrective actions such as isolating a device are categorized under remediation because they actively mitigate or stop malicious activity on the endpoint.

QUESTION 5
A collector attempts to access a known malicious website. FortiEDR is configured for eXtended detection with FortiAnalyzer. What two roles does Fortinet Cloud Services (FCS) perform in this

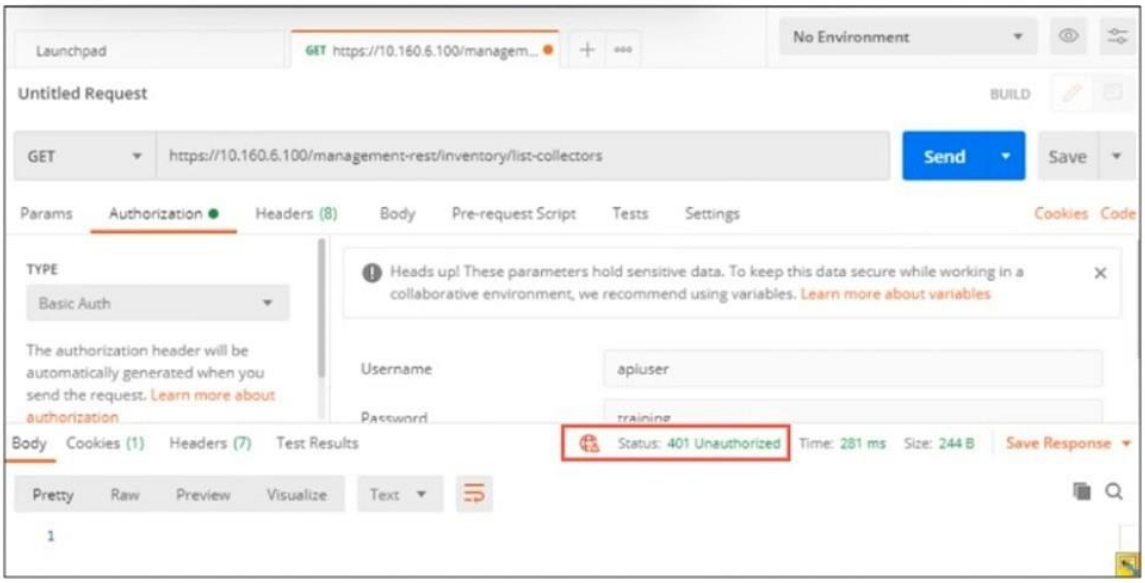
process? (Choose two.)

A. FCS sends a log record to FortiAnalyzer.
B. FCS sends OS metadata to the FortiEDR manager.
C. FCS identifies if a malicious event has taken place and reports the detection incident.
D. FCS correlates and analyzes the collected logs.

Answer: CD
Explanation:
Fortinet Cloud Services performs advanced cloud-based analysis of events collected from endpoints and integrated systems. It correlates and analyzes the collected logs and telemetry to determine malicious activity. After identifying that a malicious event has occurred, it classifies the event and reports the detection incident back to the FortiEDR system.

QUESTION 6
Refer to the exhibit. Based on the postman output shown in the exhibit, why is the user receiving an unauthorized error?

Postman output



A. The central manager is rejecting the request because of an unsupported HTTP method.
B. API access is disabled on the central manager.
C. The user account does not have the REST API role assigned.
D. FortiEDR requires a password reset the first time a user logs in.

Answer: C
Explanation:
A 401 Unauthorized response indicates that the request reached the FortiEDR central manager but the user credentials do not have permission to access the REST API. In FortiEDR, API requests require the user account to have the REST API role assigned; otherwise the system rejects the request even if the username and password are correct.

QUESTION 7

You discovered that a newly installed collector does not display on the Inventory tab in the central manager. Which two troubleshooting steps must you perform? (Choose two.)

A. Check whether the FortiEDR services are running on the collector device.
B. Verify that the central manager can resolve the collector hostname through DNS.
C. Export and review the collector logs from the Central Manager for connection errors.
D. Verify that TCP ports 8081 and 555 are open between the collector and the central manager.

Answer: AD
Explanation:
The collector must have FortiEDR services running to establish communication with the central manager. If the services are not running, the collector cannot register or appear in the Inventory tab. Communication between the collector and the central manager also requires specific ports to be open, including TCP ports 8081 and 555, which are used for management and communication between the components.

QUESTION 8
Refer to the exhibit. Based on the FortiEDR status output shown in the exhibit, what are two reasons for the degraded state? (Choose two.)

```
Microsoft Windows [Version 10.0.19043.1526]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>"C:\Program Files\Fortinet\FortiEDR\FortiEDRCollectorService.exe" --status
FortiEDR Service: Up
FortiEDR Driver: Up
FortiEDR Status: Degraded (no configuration)
```

A. The endpoint cannot reach the central manager.
B. The collector is installed with an incorrect registration password.
C. The endpoint has windows firewall enabled.
D. The collector is installed with an incorrect port number.

Answer: AB
Explanation:
The status shows that the FortiEDR service and driver are running, but the collector state is degraded with the message “no configuration.” This condition occurs when the collector cannot retrieve its configuration from the central manager. This typically happens if the endpoint cannot communicate with the central manager or if the collector was installed using an incorrect registration password, preventing proper registration and configuration retrieval.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**