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.geekcert.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

QUESTION 1

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.

QUESTION 2

Which of the following are two Tactics in the MITRE ATTandCK framework? (Choose two.)

A. Root kit

B. Reconnaissance

C. Discovery

D. BITS Jobs

E. Phishing

Correct Answer: BC

Explanation: Reconnaissance and Discovery are two Tactics in the MITRE ATTandCK framework. Tactics are the high-level objectives of an adversary, such as initial access, persistence, lateral movement, etc. Reconnaissance is the tactic of gathering information about a target before launching an attack. Discovery is the tactic of exploring a compromised system or network to find information or assets of interest. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 21

QUESTION 3

What is Tactic in the MITRE ATTandCK framework?

A. Tactic is how an attacker plans to execute the attack

B. Tactic is what an attacker hopes to achieve

C. Tactic is the tool that the attacker uses to compromise a system

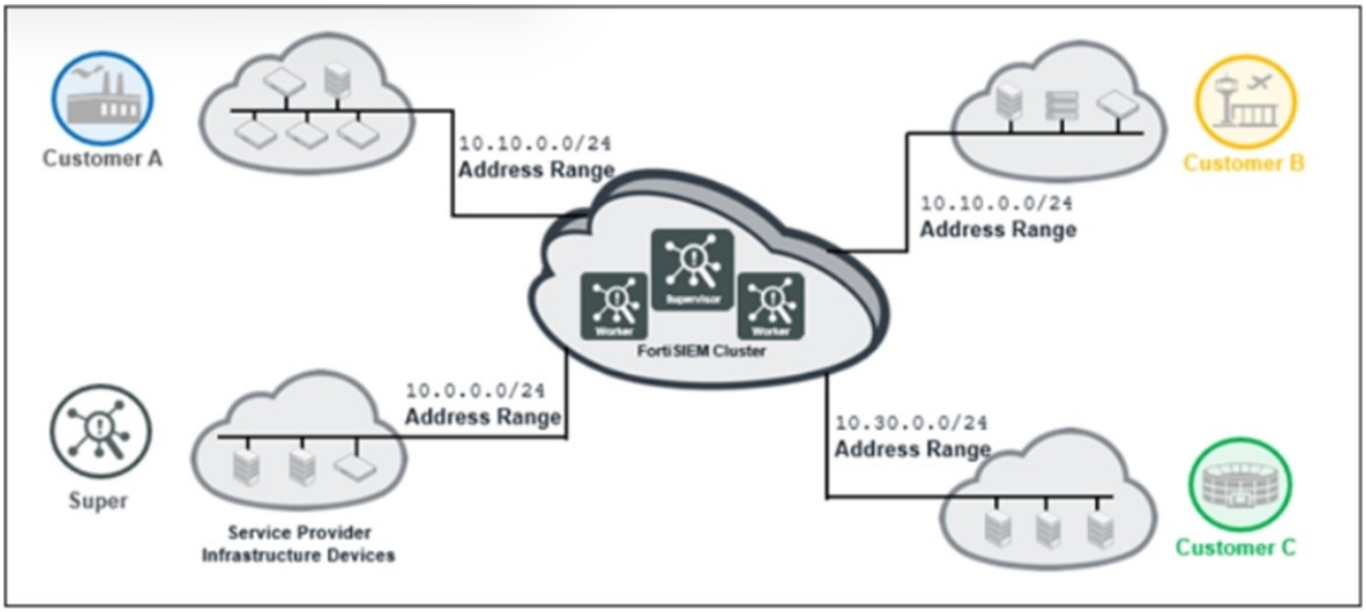
D. Tactic is a specific implementation of the technique

Correct Answer: B

Explanation: Tactic is what an attacker hopes to achieve in the MITRE ATTandCK framework. Tactic is a high-level category of adversary behavior that describes their objective or goal. For example, some tactics are Initial Access, Persistence, Lateral Movement, Exfiltration, etc. Each tactic consists of one or more techniques that describe how an attacker can accomplish that tactic.

QUESTION 4

Refer to the exhibit.



The service provider deployed FortiSIEM without a collector and added three customers on the supervisor. What mistake did the administrator make?

A. Customer A and customer B have overlapping IP addresses.

B. Collectors must be deployed on all customer premises before they are added to organizations on the supervisor.

C. The number of workers on the FortiSIEM cluster must match the number of customers added.

D. At least one collector must be deployed to collect logs from service provider infrastructure devices.

Correct Answer: A

Explanation: The mistake that the administrator made is that customer A and customer B have overlapping IP addresses. This will cause confusion and errors in event collection and correlation, as well as CMDB discovery and classification. To avoid this problem, each customer should have a unique IP address range or use NAT to translate their IP addresses.

QUESTION 5

What happens to UEBA events when a user is off-net?

A. The agent will upload the events to the Worker if it cannot upload them to a FortiSIEM collector

B. The agent will cache events locally if it cannot upload them to a FortiSIEM collector

C. The agent will upload the events to the Supervisor if it cannot upload them to a FortiSIEM collector

D. The agent will drop the events if it cannot upload them to a FortiSIEM collector

Correct Answer: B

Explanation: When a user is off-net, meaning they are not connected to a network where a FortiSIEM collector is reachable, then UEBA events will be cached locally by the agent if it cannot upload them to a FortiSIEM collector. The agent will store up to 100 MB of events in a local database file and try to upload them when it detects a network change or every five minutes.