KillTest

質量更高　服務更好



練習題

https://www.killtest.net

一年免費更新服務

Exam : **NSE7_ADA-6.3**

Title : Fortinet NSE 7 - Advanced Analytics 6.3

Version : DEMO

1.How can you invoke an integration policy on FortiSIEM rules?
A. Through Notification Policy settings
B. Through Incident Notification settings
C. Through remediation scripts
D. Through External Authentication settings
Answer: A
Explanation:
You can invoke an integration policy on FortiSIEM rules by configuring the Notification Policy settings. You can select an integration policy from the drop-down list and specify the conditions for triggering it. For example, you can invoke an integration policy when an incident is created, updated, or closed.
Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 9

2.How do customers connect to a shared multi-tenant instance on FortiSOAR?
A. The MSSP must provide secure network connectivity between the FortiSOAR manager node and the customer devices.
B. The MSSP must install a Secure Message Exchange node to connect to the customer's shared multi-tenant instance.
C. The customer must install a tenant node to connect to the MSSP shared multi-tenant instance.
D. The MSSP must install an agent node on the customer's network to connect to the customer's shared multi-tenant instance.
Answer: C
Explanation:
To connect to a shared multi-tenant instance on FortiSOAR, the MSSP must install an agent node on the customer’s network. The agent node acts as a proxy between the customer’s devices and the FortiSOAR manager node. The agent node also performs data collection, enrichment, and normalization for the customer’s data sources.
Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 11

3.In the event of a WAN link failure between the collector and the supervisor, by default, what is the maximum number of event files stored on the collector?
A. 30.000
B. 10.000
C. 40.000
D. 20.000
Answer: B
Explanation:
By default, the maximum number of event files stored on the collector in the event of a WAN link failure between the collector and the supervisor is 10.000. This value can be changed in the collector.properties file by modifying the parameter max_event_files_to_store.
Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 13

4.What is the disadvantage of automatic remediation?
A. It can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network.

B. It is equivalent to running an IPS in monitor-only mode — watches but does not block.
C. External threats or attacks detected by FortiSIEM will need user interaction to take action on an already overworked SOC team.
D. Threat behaviors occurring during the night could take hours to respond to.
Answer: A
Explanation:
The disadvantage of automatic remediation is that it can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network. Automatic remediation can have unintended consequences if not carefully planned and tested. Therefore, it is recommended to use manual or semi-automatic remediation for sensitive or critical systems.
Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 15

5.What are the modes of Data Ingestion on FortiSOAR? (Choose three.)
A. Rule based
B. Notification based
C. App Push
D. Policy based
E. Schedule based
Answer: ABE
Explanation:
The modes of Data Ingestion on FortiSOAR are notification based, app push, and schedule based. Notification based mode allows FortiSOAR to receive data from external sources via webhooks or email notifications. App push mode allows FortiSOAR to receive data from external sources via API calls or scripts. Schedule based mode allows FortiSOAR to pull data from external sources at regular intervals using connectors.
Reference: Fortinet NSE 7 - Advanced Analytics 6.3 Exam Description, page 17