Cisco 642-545

642-545 Implementing Cisco Security Monitoring, Analysis and Response System

Practice Test

Version 1.1

QUESTION NO: 1

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) is an appliance-based, all-inclusive solution that provides unmatched insight and control of your existing security deployment. Which three items are correct with regard to Cisco Security MARS rules? (Choose three.)

A. There are three types of rules.
B. Rules can be deleted.
C. Rules can be created using a query.
D. Rules trigger incidents.

Answer: A,C,D

QUESTION NO: 2

Which three benefits are of deploying Cisco Security MARS appliances by use of the global and local controller architecture? (Choose three.)

A. A global controller can provide a summary of all local controllers information (network topologies, incidents, queries, and reports results).
B. A global controller can provide a central point for creating rules and queries, which are applied simultaneously to multiple local controllers.
C. A global controller can correlate events from multiple local controllers to perform global sessionizations.
D. Users can seamlessly navigate to any local controller from the global controller GUI.

Answer: A,B,D

QUESTION NO: 3

Which item is the best practice to follow while restoring archived data to a Cisco Security MARS appliance?

A. Use Secure FTP to protect the data transfer.
B. Use "mode 5" restore from the Cisco Security MARS CLI to provide enhanced security during the data transfer.
C. Choose Admin > System Maintenance > Data Archiving on the Cisco Security MARS GUI to perform the restore operations on line.
D. To avoid problems, restore only to an identical or higher-end Cisco Security MARS appliance.

Answer: D

QUESTION NO: 4

A Cisco Security MARS appliance can't access certain devices through the default gateway. Troubleshooting has determined that this is a Cisco Security MARS configuration issue. Which additional Cisco Security MARS configuration will be required to correct this issue?

A. Use the Cisco Security MARS GUI to configure multiple default gateways
B. Use the Cisco Security MARS GUI or CLI to configure multiple default gateways
C. Use the Cisco Security MARS GUI or CLI to enable a dynamic routing protocol
D. Use the Cisco Security MARS CLI to add a static route

Answer: D

QUESTION NO: 5

Which two options are for handling false-positive events reported by the Cisco Security MARS appliance? (Choose two.)

A. mitigate at Layer 2
B. archive to NFS only
C. drop
D. log to the database only

Answer: C,D

QUESTION NO: 6

What is the reporting IP address of the device while adding a device to the Cisco Security MARS appliance?

A. The source IP address that sends syslog information to the Cisco Security MARS appliance
B. The pre-NAT IP address of the device
C. The IP address that Cisco Security MARS uses to access the device via SNMP
D. The IP address that Cisco Security MARS uses to access the device via Telnet or SSH

Answer: A

QUESTION NO: 7

Which statement best describes the case management feature of Cisco Security MARS?

A. It is used to conjunction with the Cisco Security MARS incident escalation feature for incident reporting
B. It is used to capture, combine and preserve user-selected Cisco Security MARS data within a specialized report
C. It is used to automatically collect and save information on incidents, sessions, queries and reports dynamically without user interventions
D. It is used to very quickly evaluate the state of the network

Answer: B

QUESTION NO: 8

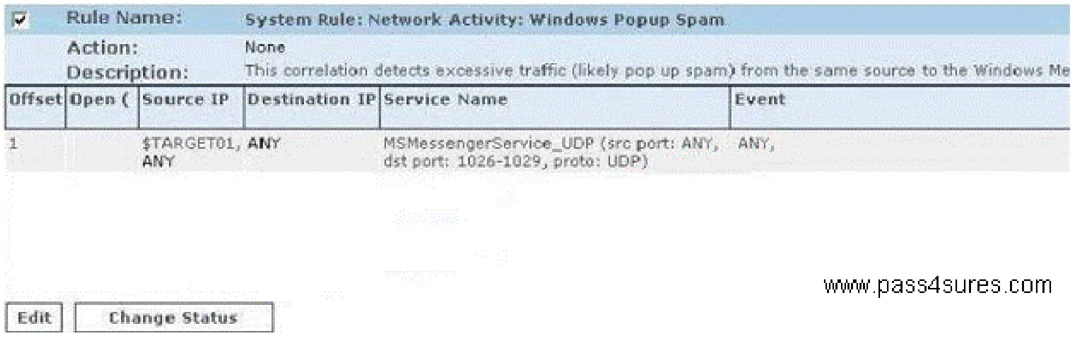
Which two configuration tasks are needed on the Cisco Security MARS for it to receive syslog messages relayed from a syslog relay server? (Choose two.)

A. Define the syslog relay collector.
B. Add the syslog relay server application to Cisco Security MARS as Generic Syslog Relay Any.
C. Define the syslog relay source list.
D. Add the reporting devices monitored by the syslog relay server to Cisco Security MARS.

Answer: B,D

QUESTION NO: 9

Here is a question that you need to answer. You can click on the Question button to the left to view the question and click on the MARS GUI Screen button to the left to capture the MARS GUI screen in order to answer the question. While viewing the GUI screen capture, you can view the complete screen by use of the left/right scroll bar on the bottom of the GUI screen. Choose the correct answer from among the options. What actions will you take to configure the MARS appliance to send out an alert when the system rule fires according to the MARS GUI screen shown?



☑ Rule Name: System Rule: Network Activity: Windows Popup Spam

Action: None

Description: This correlation detects excessive traffic (likely pop up spam) from the same source to the Windows Me

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET01, ANY	ANY	MSMessengerService_UDP (src port: ANY, dst port: 1026-1029, proto: UDP)	ANY,

A. Click "Edit" to edit the "Operation" field of the rule, select the appropriate alert option(s), then apply.
B. Click on "None" in the "Action" field, select the appropriate alerts, then apply.
C. Click "Edit" to edit the "Reported User" field of the rule, select the appropriate alert option(s),then apply.
D. Click on "Active" in the "Status" field, select the appropriate alerts, then apply.

Answer: B

QUESTION NO: 10

Which action enables the Cisco Security MARS appliance to ignore false-positive events by either dropping the events completely or by just logging them to the database?

A. Inactivating the rules
B. Creating system inspection rules using the drop operation
C. Deleting the false-positive events from the events management page
D. Creating drop rules

Answer: D

QUESTION NO: 11

In order to enable the Cisco Security MARS appliance to perform mitigation, which two configuration options are correct? (Choose two.)

A. SNMP RW community string
B. A NetFlow device added in the Cisco Security MARS database
C. Telnet or SSH access type with SNMP RO community
D. SSL communications with the network devices

Answer: A,C

QUESTION NO: 12

Which two alert actions can notify a user that a Cisco Security MARS rule has fired, and that an incident has been logged? (Choose two.)

A. syslog
B. Short Message Service
C. OPSEC-LEA (clear and encrypted)