Exam Code: 642-545

Exam Name: Implementing Cisco Security Monitoring, Analysis and Response System

Vendor: CISCO

Version: DEMO

Part: A

1: Which three statements are true about Cisco Security MARS rules? (Choose three.)

A.There are three types of rules.

B.Rules can be saved as reports.

C.Rules can be deleted.

D.Rules trigger incidents.

E.Rules can be defined using a seed file.

F.Rules can be created using a query.

Correct Answers: A D F

2: Which of the following alert actions can be transmitted to a user as notification that a Cisco Security MARS rule has fired, and that an incident has been logged? (Choose two.)

A.Distributed Threat Mitigation

B.Short Message Service

C.SNMP trap

D.XML notification

E.syslog

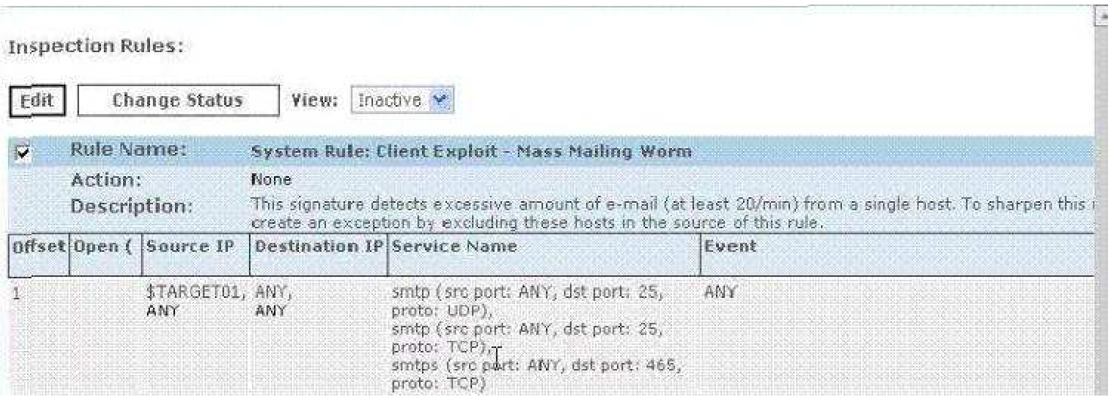
F.OPSEC-LEA (clear and encrypted)

Correct Answers: B D

3: This item contains one question that you must answer.You can view the question by clicking on the Question button to the left.In order to answer the question,you will need to refer to the MARS GUI screen capture by clicking on the MARS GUI Screen button to the left.When viewing the GUI screen capture,use the left/right scroll bar on the bottom of the GUI screen to view the complete screen.

View the question by clicking on the Question button to the left.Then,choose the correct answer from among the options.

MARS GUI Screen



☑ Rule Name: System Rule: Client Exploit - Mass Mailing Worm

Action: None

Description: This signature detects excessive amount of e-mail (at least 20/min) from a single host. To sharpen this
create an exception by excluding these hosts in the source of this rule.

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET01, ANY	ANY, ANY	smtp (src port: ANY, dst port: 25, proto: UDP), smtp (src port: ANY, dst port: 25, proto: TCP), smtps (src port: ANY, dst port: 465, proto: TCP)	ANY

Referning to the System Inspection Rule shown on the MARS GUI screen,which one of the following statements is correct?

A.Click on "Add" to activate the rule.

B.Click on "Activate" to activate the rule.

C.Click on "Change Status" to activate the rule.

D.Click on "Edit." then you can apply and activate the rule.

E.Click on "Duplicate" to archive the rule to a remote NAS.

Correct Answers: C

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

A.It is used to automatically collect and save information on incidents, sessions, queries, and reports dynamically without user interventions.

B.It is used to capture, combine, and preserve user-selected Cisco Security MARS data within a specialized report.

C.It is used to very quickly evaluate the state of the network.

D.It is used in conjunction with the Cisco Security MARS incident escalation feature for incident reporting.

Correct Answers: B

5: Which two of the following statements are correct regarding the Cisco Security MARS rules? (Choose two)

A.User-defined rules are treated as global rules. When an incident is fired by a user-defined rule on the Cisco Security MARS local controller, the rule propagates to the Cisco Security MARS global controller.

B.Predefined system rules are treated as global rules. When an incident is fired by a system rule on the Cisco Security MARS local controller, the system rule propagates to the Cisco Security MARS global controller.

C.Drop rules are treated as global rules so it will automatically propagate to the Cisco Security MARS global controller.

D.Rules can be created on both the Cisco Security MARS global controller and the Cisco Security MARS local controllers. Rules on the Cisco Security MARS global controller will propagate down to the Cisco Security MARS local controllers.

E.It is not possible to edit the global rules created on the Cisco Security MARS global controller from the Cisco Security MARS local controller.

Correct Answers: B D

6: Which three statements are correct about the Cisco Security MARS global and local controller architecture? (Choose three.)

A.The global controller can correlate events from different local controllers into a common session.

B.One global controller can support multiple local controllers.

C.Each zone can have one local controller.

D.All local controllers events are propagated to the global controller for correlations.

E.The global controller and the local controllers can be running different Cisco Security MARS OS versions.

F.Incidents can be viewed on the global controller based on a selected local controller.

Correct Answers: B C F

7: What are three benefits in deploying Cisco Security MARS appliances using 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.The architecture provides redundancy in case one of the Cisco Security MARS local controllers fails within a zone.

D.Users can seamlessly navigate to any local controller from the global controller GUI.

E.A global controller can correlate events from multiple local controllers to perform global sessionizations.

F.Rules that apply to multiple local controllers cannot be created on the global controller and pushed down to them from a central location.

Correct Answers: A B D

8: When restoring archived data to a Cisco Security MARS appliance, what is the best practice to follow?

A.Use HTTPS to protect the data transfer.

B.Use Secure FTP to protect the data transfer.

C.Use "mode 5" restore from the Cisco Security MARS CLI to provide enhanced security during the data transfer.

D.Choose Admin > System Maintenance > Data Archiving on the Cisco Security MARS GUI to perform the restore operations on line.

E.To avoid problems, restore only to an identical or higher-end Cisco Security MARS appliance.

Correct Answers: E

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

A.archive to NFS only

B.save as a false-positive report

C.drop

D.mitigate at Layer 2

E.log to the database only

F.escalate to the Cisco Security MARS administrator

Correct Answers: C E

10: When adding a device to the Cisco Security MARS appliance, what is the reporting IP address of the device?

A.the source IP address that sends syslog information to the Cisco Security MARS appliance

B.the IP address that Cisco Security MARS uses to access the device via SNMP

C.the IP address that Cisco Security MARS uses to access the device via Telnet or SSH

D.the pre-NAT IP address of the device

Correct Answers: A