Cisco

642-545

Implementing Cisco Security Monitoring, Analysis and Response System

network and security devices. What is a supported mitigation feature on the Cisco Security MARS appliance?

A. Storing and identifying NetFlow data for attack mitigation
B. Generating and pushing configuration commands to Layer 2 devices
C. Generating and pushing configuration commands to Layer 3 devices
D. Automatically dropping all suspected traffic at the nearest IPS appliance

Answer: B

Question: 62
Cisco Security MARS combines network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification, and automated mitigation capabilities. Which action will you take to enable 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 drop rules
C. Deleting the false-positive events from the Incidents page
D. Deleting the false-positive events from the Event Management page

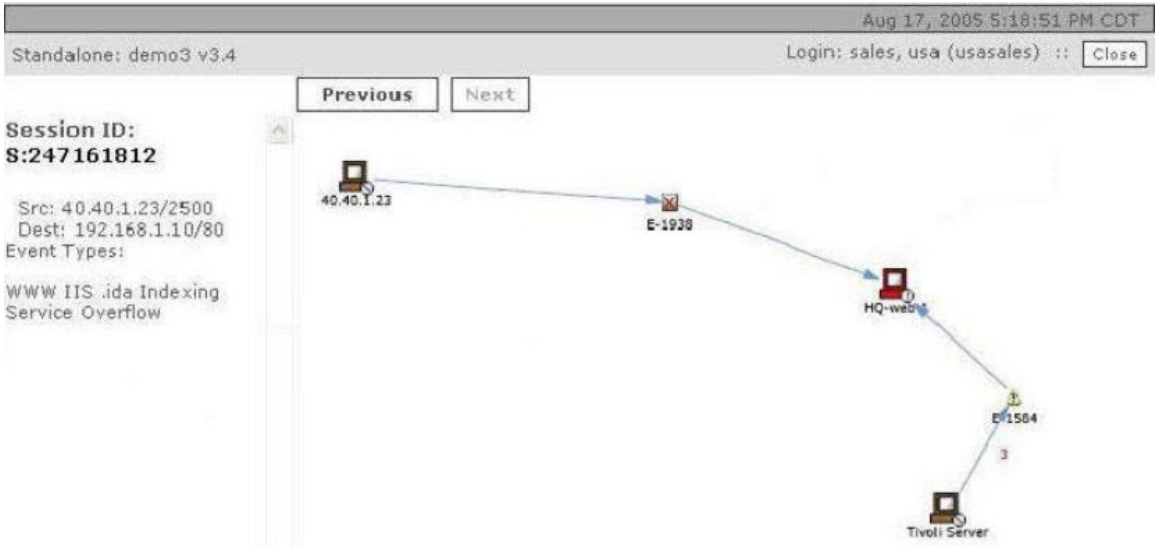
Answer: B

Question: 63
In which two ways could the Cisco Security MARS present the incident data to the user graphically from the Summary Dashboard? (Select two)

A. Compromised topology information
B. Event type group matrix
C. Path information
D. Incident vector information

Answer: C, D

Question: 64
Which three items are correct based on the Incident Vector Graph shown on the MARS GUI screen? (Choose three.)



A. The port being attacked is port 80.
B. This incident has two associated Event Types.
C. Click the Previous button to view any other Sessions related to this incident.
D. The device being attacked is the Tivoli Server.

Answer: A, B, D

Question: 65
Which two statements accurately describe the Cisco Security MARS rules? (Choose two)

A. Drop rules are treated as global rules so it will automatically propagate 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. It is not possible to edit the global rules created on the Cisco Security MARS global controller from the Cisco Security MARS local 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.

Answer: B, D

Question: 66
Which three options are true with regard to the Cisco Security MARS global and local controller architecture? (Choose three.)

A. All local controllers events are propagated to the global controller for correlations.
B. One global controller can support multiple local controllers.
C. Each zone can have one local controller.
D. Incidents can be viewed on the global controller based on a selected local controller.

Answer: B, C, D

Question: 67
Cisco Security MARS uses NetFlow data to perform which function?

A. Traffic profiling and statistical anomaly detection
B. Correlation across NAT boundary
C. Data reductions
D. Events normalization

Answer: A

Pass your exam at First Attempt....Guaranteed!