

IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

Exam : **642-567**

Title : Advanced Security for Field
Engineers

Version : Demo

1. Regarding MARS Appliance rules, which three statements are correct? (Choose three.)
- A. There are three types of rules: System Inspection Rules, User Inspection Rules, and Drop 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.

Answer: ADF

2. Which action enables the MARS Appliance to ignore false positive events by either dropping the events completely, or by just logging them to the database?
- A. Creating System Inspection Rules using the Drop operation
 - B. Creating Drop Rules
 - C. Inactivating the Rules
 - D. Inactivating events
 - E. Deleting the false positive events from the Incidents > False Positives screen
 - F. Deleting the false positive events from the Management > Event Management screen

Answer: B

3. Which of the following is a supported mitigation feature on the MARS Appliance?
- A. Generating and pushing configuration commands to Layer 3 devices
 - B. Generating and pushing configuration commands to Layer 2 devices
 - C. Automatically dropping all suspected traffic at the nearest firewall
 - D. Automatically dropping all suspected traffic at the nearest IPS appliance

Answer: B

4. Which browser plug-in is required to view the charts and graphs on the MARS Appliance?
- A. Macromedia Flash Player
 - B. Sun Microsystems Java
 - C. Microsoft PowerPoint
 - D. Adobe SVG Viewer

Answer: D

5. A MARS Appliance cannot access certain devices through the default gateway. Troubleshooting has determined that this is a MARS configuration issue. Which additional MARS configuration will be required to correct this issue?
- A. Use the MARS GUI to enable a dynamic routing protocol.
 - B. Use the MARS GUI to add a static route.

- C. Use the MARS GUI to configure multiple default gateways.
- D. Use the MARS CLI to enable a dynamic routing protocol.
- E. Use the MARS CLI to add a static route.
- F. Use the MARS CLI to configure multiple default gateways.

Answer: E

6. When adding a device to the MARS Appliance, what is the reporting IP address of the device?

- A. the source IP address that sends syslog information to the MARS Appliance
- B. the IP address MARS uses to access the device via SNMP
- C. the IP address MARS uses to access the device via Telnet or SSH
- D. the pre-NAT IP address of the device
- E. the highest loopback IP address configured on the Cisco reporting device

Answer: A

7. What enables the MARS Appliance to profile network usage and detect statistically significant anomalous behavior from a computed baseline?

- A. MARS Global Controller
- B. VMS
- C. Netflow
- D. CiscoWorks
- E. MARS custom parser

Answer: C

8. Which is a benefit of using the dollar variable (like \$TARGET01) when creating queries in MARS?

- A. The dollar variable enables multiple queries to reference the same common 5-tuples information using a variable.
- B. The dollar variable ensures that the probes and attacks that are reported are happening to the same host.
- C. The dollar variable allows matching of any unknown reporting device.
- D. The dollar variable allows matching of any event type groups.
- E. The dollar variable enables the same query to be applied to different reports.

Answer: B

9. What will happen if you try to run a MARS query that will take a long time to complete?

- A. After submitting the query, the MARS GUI screen will be locked up until the query completes.
- B. The query will be automatically saved as a rule.
- C. The query will be automatically saved as a report.
- D. You will be prompted to "Submit Batch" to run the query in batch mode.

E. You will be prompted to "Submit Inline" to run the query immediately.

Answer: D

10. The MARS Appliance (running release 3.4.1) supports which protocol for data archiving and restoring?

A. NFS

B. TFTP

C. FTP

D. secured FTP

Answer: A