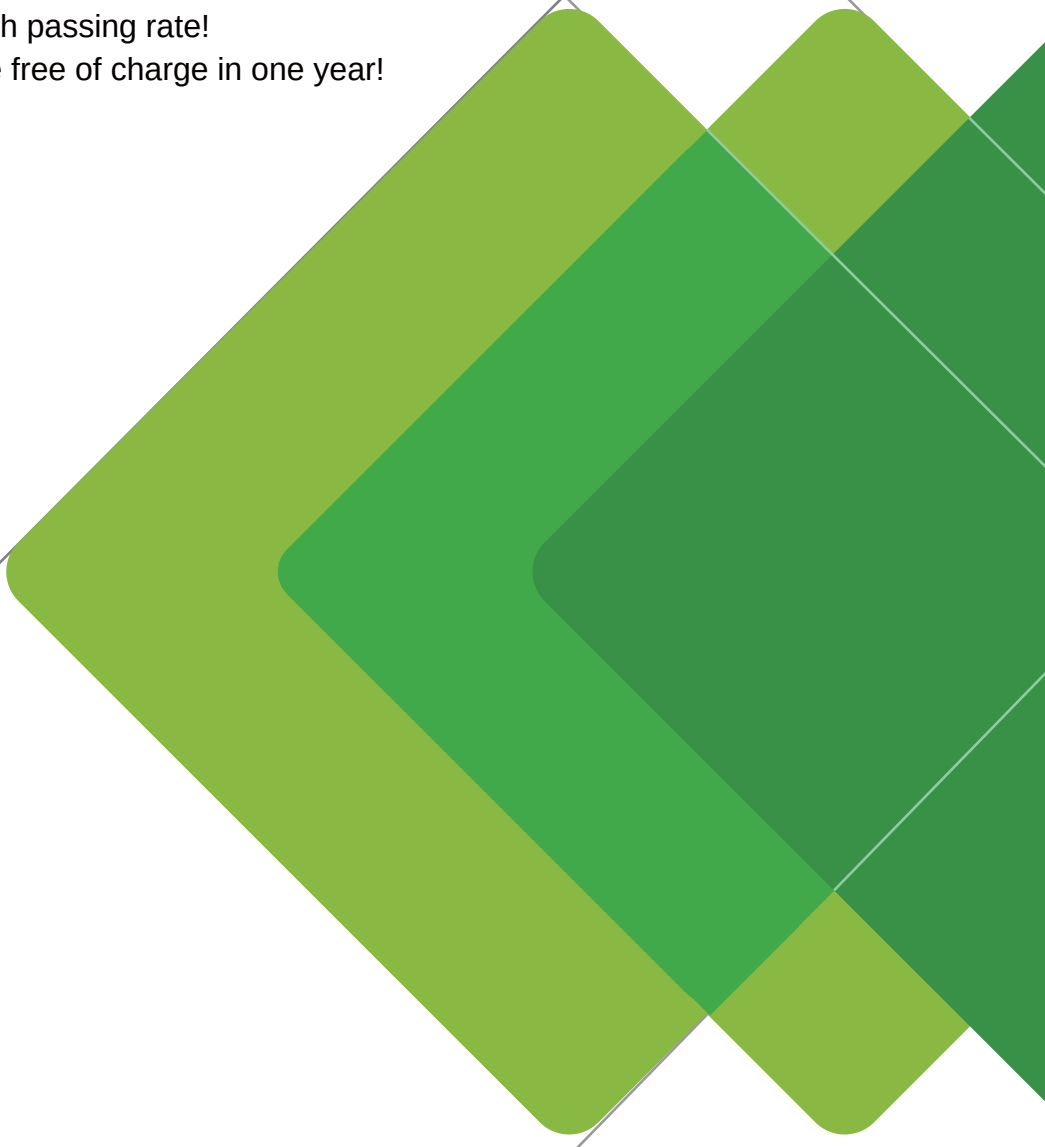
IT-DUMPS Q&A

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



Exam : **642-545**

Title : Implementing Cisco Security Monitoring, Analysis and Response System

Version : Demo

1. Which attack can be detected by Cisco Security MARS using NetFlow data?

A. man-in-the middle attack

B. day-zero attack

C. spoof attack

D. Land attack

E. buffer overflow attack

Answer: B

2. What is used to publish events to Cisco Security MARS about Cisco IPS signatures that have fired?

A. SNMP

B. SSL

C. HTTPS

D. SDEE

E. syslog

F. Secure FTP

Answer: D

3. 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.

Answer: B

4. Which statement is true about the case management feature of Cisco Security MARS?

A. Cases are created on a global controller, but they can be viewed and modified on a local controller.

B. The global controller has a Case bar and all cases are selected from the Query/Reports > Cases page.

C. Cases are created on a local controller, but they can be viewed and modified on a global controller.

D. The Cases page on a local controller has an additional drop-down filter to display cases per a global controller.

Answer: C

5. At what level of operation does the Cisco Security MARS appliance perform NAT and PAT resolution?

A. Local (Level 0)

B. Basic (Level 1)

C. Intermediate (Level 2)

D. Advanced (Level 3)

E. Global (Level 4)

Answer: C