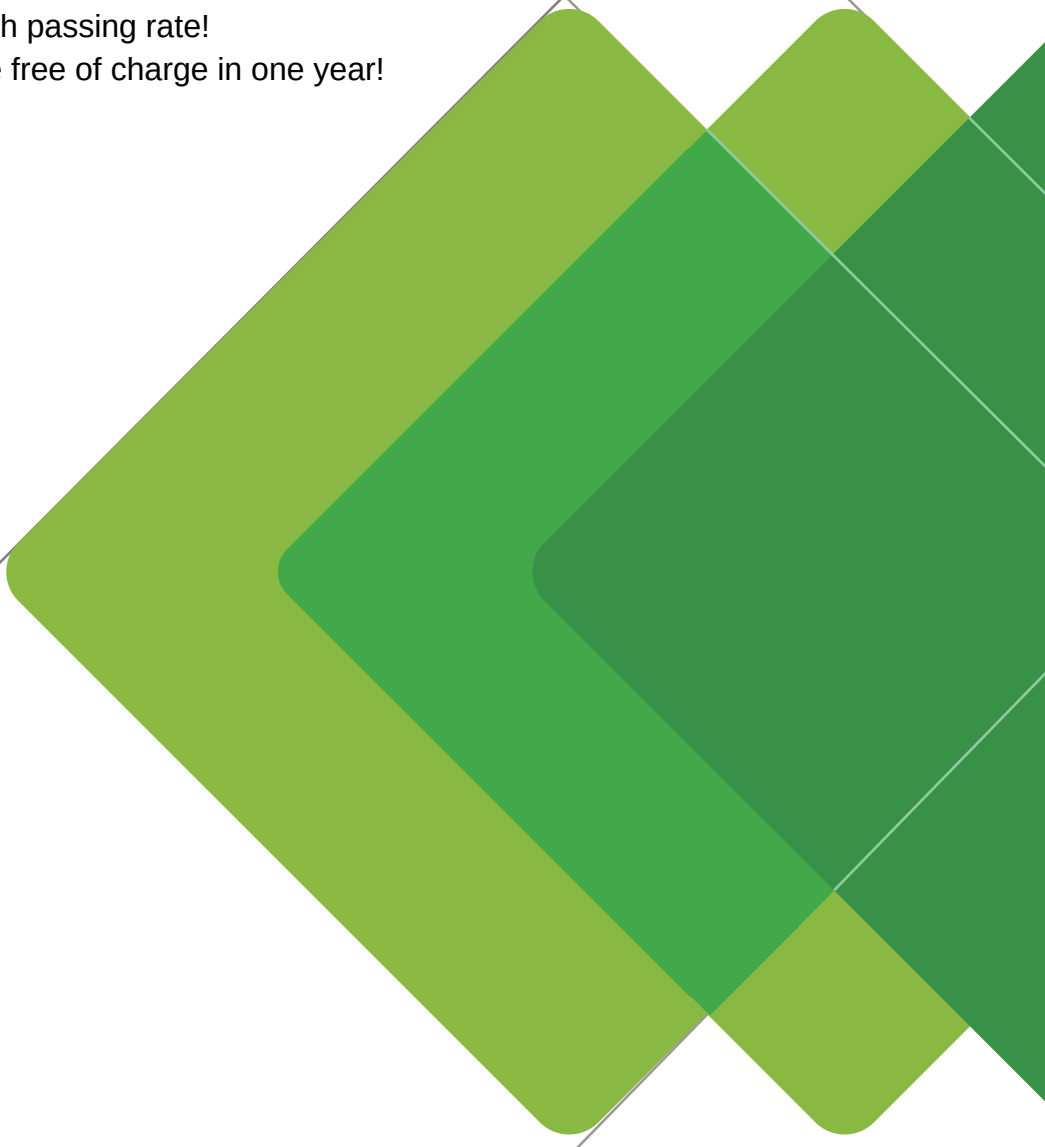
IT-DUMPS Q&A

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



Exam : **2B0-023**

Title : ES Advanced Dragon IDS

Version : DEMO

1. What are three primary common goals of a corporate/network security policy?

A. Authentication, Authorization and Accounting (AAA)

B. Security, Productivity and Adaptability (SPA)

C. Confidentiality, Integrity and Availability (CIA)

D. Authentication, Encryption and Compression (AEC)
Answer: C

2. Which of the following must an IDS administrator consider when deploying Dragon in accordance with a corporate security policy?

A. Must understand the purpose and scope of each aspect of the overall security policy

B. Must understand the security goals of each product in the organization (i.e., operating systems, routers, firewalls, NIDS, HIDS, VPN gateways)

C. Must understand the detailed configurations on each router within the security domain

D. Must understand how the security policy impacts the I.T. budget
Answer: AB

3. What functions can Dragon accomplish as related to a corporate/network security policy?

A. Dragon agents can gather information about network security compromises and automatically produce corporate/network security policy documents

B. Dragon agents can detect and log security policy deviations

C. Dragon agents can assist with security policy enforcement via Active Responses

D. Dragon can evaluate a corporate/network policy to determine if it is complete and effective
Answer: BC

4. Which vulnerability scanner and report format is required for use with the Dragon VCT?

A. MySQL; .msq formatted output

B. Nessis; .nfr formatted output

C. Nessus; .nes formatted output

D. Nessus; .nsr formatted output

E. NMAP; .nmp formatted output
Answer: D

5. Which of the following is NOT a recommended means of vulnerability response using Dragon?

A. Use the Dragon NMAP PERL scripts to tune the dragon.net file

B. Deploy Dragon Deceptive Services (Honeypot)

C. Deploy Dragon Vulnerability Correlation Tool

D. Enable SSL and AES on the Network Sensor to DPM communication channel

E. Correlate Dragon forensics reports with vulnerability scanner output, and create new signatures as necessary
Answer: D

6. Which of the following best describes the function of CVE?

A. A database of known attacks that can be loaded into an IDS or similar system

B. A database of numerically cross-referenced IDS events that can help any IDS to correlate detected attacks

C. A dictionary of standardized names for vulnerabilities and other information security exposures

D. All of the above
Answer: C

7. Which of the following is NOT a function of a network vulnerability scanner?

A. Monitors health of software applications

B. Output is critical in helping an IDS administrator know the state of the network

C. Catalogs vulnerabilities

D. Shuts down vulnerable TCP/UPD ports to prevent intrusion
Answer: D

8. Which of the following CONSUME event data from the Dragon Ring Buffer?

A. Alarmtool agent

B. Replication agent

C. Connection Manager

D. Consumer Agent
Answer: AB

9. Which of the following best describes the Host Sensor Event Detection Engine (EDE)?

A. Scrutinizes events, either altering the contents of the event or discarding it

B. Generates alerts or guarantees delivery of events to destinations C. Analyzes events and produces categorized event forensics reports

D. Detects an event and forwards it to the Host Sensor framework for processing
Answer: D

10. Which of the following best describe some scalability features of the Dragon Event Flow Processor (EFP)?

A. Consolidates events from multiple Dragon Policy Managers into one stream

B. Aggregated events from an EFP can be forwarded to other EFPs in a hierarchy

C. An EFP cannot simultaneously support Dragon Realtime Console, Forensics Console and Alarmtool

D. EFPs can be secured by a firewall and configured to initiate Sensor connections from inside the firewall
Answer: BD