

Exam : Enterasys Networks 2B0-023

Title : ES Advanced Dragon IDS

Version : Demo

Important Note, Please Read Carefully

Other examsoon products

[All examsoon IT Exam Products](#)

Our products of Offline Testing Engine

Use the offline Testing engine product to practice the questions in an exam environment.

Build a foundation of knowledge which will be useful also after passing the exam.

[examsoon Testing Engine](#)

Guarantee

Examsoon provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!.

Features

1. Comprehensive questions with complete details
2. Instant Downloadable in PDF form.
3. Verified Answers Researched by Industry Experts
4. Questions accompanied by exhibits
5. Drag and Drop questions as experienced in the Actual Exams.
6. These questions and answers are backed by our GUARANTEE.
7. Questions updated on regular basis.
8. Like actual certification exams our product is in multiple-choice questions (MCQs).

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

Examsoon.com was founded in 2006. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially [Adobe](#), [Apple](#), [Citrix](#), [Comptia](#), [EMC](#), [HP](#), [Juniper](#), [LPI](#), [Nortel](#), [Oracle](#), [SUN](#), [Vmware](#) and so on. And help you pass any IT Certification exams at the first try.

we guarantee your success at the first attempt with only our Certification Question&Answers, if you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

You can reach us at any of the email addresses listed below.

E-MAIL: [examsoon\(at\)hotmail.Com](mailto:examsoon(at)hotmail.Com)