

2B0-023 braindumps

Enterasys Networks Enterasys Networks Certification

2B0-023: ES Advanced Dragon IDS

Practice Exam: 2B0-023 Exams

Exam Number/Code: 2B0-023

Exam Name: ES Advanced Dragon IDS

Questions and Answers: 50 Q&As

([Enterasys Networks Certification](#))



Exam : [2B0-023](#)

"ES Advanced Dragon IDS", also known as 2B0-023 exam, is a Enterasys Networks certification. With the complete collection of exam questions, Just4Study has assembled to take you through 50 Q&As to your 2B0-023 exam preparation. In the 2B0-023 exam resources, you will cover every field and category in Enterasys Networks Certification helping to ready you for your successful Enterasys Networks Certification.

The exam questions cover the latest real test and with all the correct answer. we promise the Q&A for Enterasys Networks Enterasys Networks Certification 2B0-023 (ES Advanced Dragon IDS) examination of original title complete coverage. 2B0-023 exam questions help you pass the exam.

Just4Study 2B0-023 Feature:

* High quality - High quality and valued for the 2B0-023 Exam: 100% Guarantee to Pass Your 2B0-023 exam and get your Enterasys Networks Certification certification.

* Authoritative - Authoritative braindumps with complete details about 2B0-023 exam.

* Cheaper - Our Just4Study products are cheaper than any other website. With our completed Enterasys Networks Certification resources, you will minimize your **Enterasys Networks Enterasys Networks Certification** cost and be ready to pass your 2B0-023 exam on Your First Try, 100% Money Back Guarantee included!

* Free - Try free Enterasys Networks Certification demo before you decide to buy it in <http://www.Just4Study.com>.

Just4Study Guarantee:

Just4Study 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 2B0-023 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!

Free 2B0-023 Demo Download

Just4Study offers free demo for Enterasys Networks Certification 2B0-023 exam (ES Advanced Dragon IDS). You can check out the interface, question quality and usability of our practice exams before you decide to buy it. We are the only one site can offer demo for almost all products.

The Questions & Answers cover the latest real test and with all the correct answer. we promise the Q&A for **Enterasys Networks Enterasys Networks Certification 2B0-023** examination of original title complete coverage. 2B0-023 Questions & Answers help you pass the exam. Otherwise, we will give you a full refund.

VUE/Prometric Code: 2B0-023

Exam Name: ES Advanced Dragon IDS(Enterasys Networks Certification)

Questions and Answers: 50 Q&A

[Enterasys Networks 2B0-023](#) Test belongs to one of the Enterasys Networks Certification certified test, if needs to obtain the Enterasys Networks Certification certificate, you also need to participate in other related test, the details you may visit the [Enterasys Networks Certification](#) certified topic, in there, you will see all related Enterasys Networks Certification certified subject of examination.

Just4Study professional provide Enterasys Networks Certification 2B0-023 the newest Q&A, completely covers 2B0-023 test original topic. With our complete Enterasys Networks Certification resources, you will minimize your Enterasys Networks Certification cost and be ready to pass your 2B0-023 tests on Your First Try, 100% Money Back Guarantee included!

Just4Study Help You Pass Any IT Exam

[Just4Study.com](#) offers incredible career enhancing opportunities. We are a team of IT professionals that focus on providing our customers with the most up to date material for any IT certification exam. This material is so effective that we Guarantee you will pass the exam or your money back.

Exam : Enterasys Networks 2B0-023

Title : ES Advanced Dragon IDS

1. 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

2. 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

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 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

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 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

7. 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

8. 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

9. 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

10. 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

[2B0-023 Braindumps](#)

Related 2B0-023 Exams

[2B0-012](#) *ES Switching Edition 4.0*

[2B0-021](#) *ES XSR Configuration*

[2B0-015](#) *ES Wireless*

[2B0-100](#) *Enterasys Systems Engineer (ESE) Recertification*

[2B0-019](#) *ES Policy Enabled Networking*

[2B0-102](#) *Enterasys Security Systems Engineer-Defense*

[2B0-104](#) *Enterasys Certified Internetworking Engineer(ECIE)*

2B0-024 *ES Secure Networks*

2B0-101 *Enterasys Security Systems Engineer (ESSE) Recertification*

2B0-011 *ES Router Configuration*

2B0-022 *ES XSR Security*

2B0-103 *Enterasys Security Systems Engineer-NAC*

2B0-018 *ES Dragon IDS*

2B0-023 *ES Advanced Dragon IDS*

2B0-020 *ES NetSight Atlas*

Other Enterasys Networks Exams

2B0-020

2B0-024

2B0-022

2B0-102

2B0-023

2B0-012

2B0-104

2B0-019

2B0-011

2B0-021

2B0-100

2B0-018

2B0-103

2B0-015

2B0-101