

# PremiumVCEdump

PremiumVCEdump

> Contact Us

Login / Register

Search...



HOME

ALL VENDORS

GUARANTEE

FAQ

TESTIMONIALS

CART (0)

## Pass Your Next Certification Exam Fast!

Everything you need to prepare, learn & pass your certification exam easily.

365 days free updates. First attempt guaranteed success.

Try **Desktop Test Engine** before you buy

### Instant Download

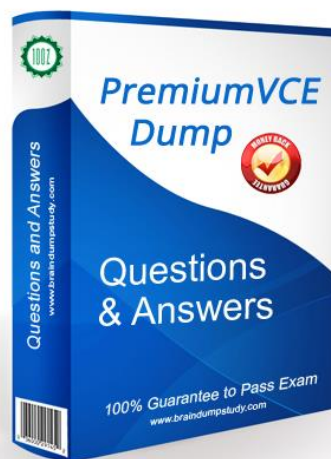


After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

### 365 Days Free Updates



Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.



### Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.



### Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

<http://www.premiumvcedump.com/>

High-Quality Certification Exam Premium VCE Braindumps materials

**Exam :** 2B0-101

**Title :** Enterasys Security Systems  
Engineer (ESSE) Recertification

**Vendors :** Enterasys Networks

**Version :** DEMO

NO.1 If a packet matched the rules for two virtual sensors it will be evaluated by?

- A. Both sensors
- B. The first sensor it matches
- C. The default sensor
- D. Overlapping rules are not permitted

Answer: B

This document was created with Win2PDF available at <http://www.win2pdf.com>.

The unregistered version of Win2PDF is for evaluation or non-commercial use only.

This page will not be added after purchasing Win2PDF.

NO.2 Agents can be deployed on?

- A. Only the Enterprise Management Server (EMS)
- B. Any managed node with a networked sensor deployed
- C. Any managed node with host sensor deployed
- D. Any managed node

Answer: D

NO.3 Which of the following Dragon Agents is used for detecting changes to host files?

- A. Real Time Console
- B. MD5 Sum
- C. Alarm Tool
- D. Database

Answer: B

NO.4 The attack category is for events that

- A. Attempt to discover weaknesses
- B. Map the structure of the network
- C. Have the potential to compromise the integrity of an end system.
- D. Deny access to resources

Answer: C

NO.5 Which alarm type is best described as: collects information for x period of time, then send event

notifications

- A. Real Time
- B. Summary
- C. Dynamic
- D. Interval

Answer: B

NO.6 Virtual sensor names?

- A. Are included in events they generate
- B. Must match the sensor key
- C. Must include the device name
- D. Require separate keys

Answer: A

NO.7 Agent status will show as Not Available until?

- A. The agent is committed
- B. The agent is deployed
- C. The agent is selected
- D. The remote node is deployed

Answer: B

NO.8 Agents can be deployed?

- A. Only on non-forwarding Event Flow Processor (EFPs)
- B. Only on forwarding Event Flow Processor (EFPs)
- C. Only on the Enterprise Management Server (EMS) station
- D. On any Event Flow Processor (EFP)

Answer: D

NO.9 In a standalone deployment the system will have?

- A. A net-config-client.xml file
- B. A net-config-server.xml file
- C. A net-config-server.xml and a net-config-client.xml file
- D. A net-config-server.xml, a net-config-client.xml and a net-config-reports.xml file

Answer: C

NO.10 Virtual Sensors can segregate traffic by?

- A. IP Address, VLAN, Port
- B. IP Address, VLAN, Port, Protocol
- C. IP Address, VLAN, Port, Protocol, Application
- D. IP Address, VLAN, Port, Application

Answer: B

NO.11 In an Event Flow Processor (EFP) a consumer can be?

- A. A Sensor or an Event Channel

- B. An Event channel only
- C. An Event channel or an Agent
- D. An Agent only

Answer: C

NO.12 MD5 checksums are

- A. Stored in a protected directory on the host
- B. Appended to the protected file
- C. Passed up the event channel to the MD5 Agent
- D. Stored in the /usr/dragon/bin directory on the Enterprise Management Server (EMS)

Answer: C

NO.13 The master Alarm Tool Default policy

- A. Is write locked
- B. Is writable
- C. Cannot be copied
- D. Cannot be associated with an Agent

Answer: A

NO.14 Which of the following best describes the commit operation?

- A. It uses the configuration channel to push a configuration to a device
- B. It uses the event channel to push a configuration to a device
- C. It writes a configuration change to the Enterprise Management Server (EMS) database
- D. It writes a configuration change to the management clients database

Answer: C

NO.15 Traffic direction refers to traffic flows in relation to the

- A. Server
- B. Protected network
- C. Client
- D. DMZ

Answer: B

NO.16 Before the host Sensor can be deployed

- A. It must be associated with a virtual sensor
- B. It must be associated with a host policy
- C. Its key must be added to the /usr/dragon/bin directory
- D. Its address must be added to /etc/hosts

Answer: B

NO.17 Signature OS

- A. Applies signature to network traffic originating from the specified OS
- B. Is used for writing Host signatures
- C. Is optional on Network signatures
- D. Is required on all signatures

Answer: B

NO.18 Dragonctl is used to?

- A. Start, stop and monitor the dragon processes on the remote node
- B. Write log files
- C. Monitor the Ring Buffer
- D. Maintain configuration channel connections

Answer: A

NO.19 The host policy MD5 detection module

- A. Detects any changes in the contents of protected file
- B. Detects file size increases
- C. Detects file truncations
- D. Detects ownership changes

Answer: A

NO.20 Which of the following Dragon Agents sends notifications when the sensors detect an event that match a rule?

- A. Real Time Console
- B. MD5 Sum
- C. Alarm Tool
- D. Database

Answer: C