



# Symantec

## ST0-085 Exam

### **Symantec Security Information Manager 4.7 Technical Assessment Exam**

**Thank you for Downloading ST0-085 exam PDF Demo**

**You can Buy Latest ST0-085 Full Version Download**

<https://www.certkillers.net/Exam/ST0-085>

<https://www.certkillers.net>

---

**Question: 1.**

---

Which tab on the Information Manager Console allows you to view threat and vulnerability information?

- A. Rules
- B. Dashboard
- C. Reports
- D. Intelligence

---

**Answer: D**

---

---

**Question: 2.**

---

Which component escalates security events into incidents?

- A. rules
- B. events
- C. incidents
- D. tickets

---

**Answer: A**

---

---

**Question: 3.**

---

What does the Correlation Engine analyze events against once all rules are properly defined?

- A. the rule criteria, create triggers, and correlate conclusions into incidents
- B. false positives, create conclusions, and correlate conclusions into incidents
- C. the rule criteria, create conclusions, and correlate conclusions into incidents
- D. the rule criteria, create conclusions, and send conclusions to the database

---

**Answer: C**

---

---

**Question: 4.**

---

What is the purpose of the critical business assets management feature?

- A. It enables automatic identification and prioritization of security threats that impact business-critical applications.
- B. It obtains an overview of business assets.
- C. It makes it possible to change collectors' configurations to meet business assets needs.
- D. It provides a visual picture of where critical business assets are located.

---

**Answer: D**

---

---

**Question: 5.**

---

Which of the following vendor hardware is recommended to use with Symantec Security Information Manager (SSIM)?

- A. IBM
- B. NEC
- C. Dell
- D. Hitachi

---

**Answer: C**

---

---

**Question: 6.**

---

What are the hard drive specifications for the hardware?

- A. 6 drives (2 mirrored and 4 in RAID 5)
- B. 6 drives (2 mirrored and 4 in RAID 10)
- C. 6 drives (RAID 5)
- D. 2 drives (mirrored)

---

**Answer: A**

---

---

**Question: 7.**

---

Which third-party software components support LDAP for users, roles, and configurations?

- A. IBM Directory Server
- B. Microsoft Active Directory Server
- C. IBM DB2 8.1
- D. IBM DB2 8.2

---

**Answer: A**

---

---

**Question: 8.**

---

Which OS listed does hardware used for the Symantec Security Information Manager (SSIM) image support?

- A. SUSE
- B. Centos
- C. Redhat
- D. SE Linux

---

**Answer: C**

---

---

**Question: 9.**

---

Symantec Security Information Manager Series Appliance installs which operating system by default?

- A. Solaris
- B. Windows
- C. SUSE
- D. Red Hat

---

**Answer: D**

---

---

**Question: 10.**

---

Which database houses incidents and summary data?

- A. Oracle
- B. MySQL
- C. MSSQL
- D. IBM DB2

---

**Answer: C**

---

---

**Question: 11.**

---

Which component sends events to the Event Service for processing?

- A. the Symantec Security Information Manager (SSIM) collector
- B. the Symantec Security Information Manager (SSIM) on-box collector
- C. the Symantec Security Information Manager (SSIM) off-box collector
- D. the Symantec Security Information Manager (SSIM) agent

---

**Answer: D**

---

---

**Question: 12.**

---

What is the difference between Symantec Security Information Manager (SSIM) on-box and off-box collectors?

- A. Off-box collectors are installed on the SSIM products and on-box collectors are installed on the appliance.
- B. On-box collectors are installed prior to SSIM software installation and off-box collectors are installed separately.
- C. On-box collectors are automatically installed with the SSIM software and off-box collectors are installed separately.
- D. Off-box collectors are installed on the appliance and on-box collectors are installed on assets.

---

**Answer: C**

---

---

**Question: 13.**

---

Which Symantec Security Information Manager component retrieves security content in near-realtime from Symantec?

- A. LiveUpdate
- B. LiveUpdate and licensed DeepSight Integration Module simultaneously
- C. Licensed DeepSight Integration Module
- D. Security content retrieval is automatic.

---

**Answer: C**

---

---

**Question: 14.**

---

Which of the following are all on-box collectors?

- A. PIX, UNIX Syslog and Data Leakage Prevention
- B. Checkpoint, Snort and PIX
- C. PIX, Snort and Symantec Web Gateway
- D. Checkpoint, UNIX Syslog and Control Compliance Suite

---

**Answer: B**

---

---

**Question: 15.**

---

On which two operating systems can the Symantec Security Information Manager Agent be installed? (Select two.)

- A. Solaris 9
- B. Windows 2000
- C. Centos
- D. IBM AIX 5
- E. HP-UX 11

---

**Answer: AB**

---

---

**Question: 16.**

---

Where do Symantec Security Information Manager collectors send events?

- A. Event Disposition
- B. Event Archive
- C. Event Reporting

D. Event Logger

---

**Answer: D**

---

---

**Question: 17.**

---

What is Device-level aggregation?

- A. parsing data with data sensors
- B. grouping data to reduce traffic and database size
- C. forwarding event data to the appliance
- D. event and log sensing

---

**Answer: B**

---

---

**Question: 18.**

---

What information must be obtained prior to product deployment and configuration of the Symantec Security Information Manager appliance?

- A. which on-box collectors are appropriate for installation
- B. the number of nodes found in the customer's infrastructure
- C. the number of security events per day the appliance will handle
- D. the air-conditioning and power requirements

---

**Answer: C**

---

---

**Question: 19.**

---

What information is necessary to properly size a deployment?

- A. hard drive space, events per second and geographic locations
- B. events per second, collector types and incident-to-event ratio
- C. hard drive space, incidents per second and collector types
- D. events per second, geographic locations and event-to-incident ratio

---

**Answer: D**

---

---

**Question: 20.**

---

What are the specified minimum hardware requirements for installing and running the Symantec Security Information Manager Console?

- A. 1 GB RAM and 1 GB disk space
- B. 1 GB RAM and 512 MB disk space
- C. 512 MB RAM and 1 GB disk space

D. 512 MB RAM and 103 MB disk space

---

**Answer: D**

---

CertKillers.net

## Thank You for trying ST0-085 PDF Demo

To Buy Latest ST0-085 Full Version Download visit link below

<https://www.certkillers.net/Exam/ST0-085>

## Start Your ST0-085 Preparation

**[Limited Time Offer]** Use Coupon “CKNET” for Further discount on your purchase. Test your ST0-085 preparation with actual exam questions.

<https://www.certkillers.net>