



**Vendor:** Symantec

**Exam Code:** 250-604

**Exam Name:** Symantec Endpoint Security Complete Admin  
R3 Technical Specialist

**Version:** DEMO

**QUESTION 1**

What feature in ICDm allows administrators to generate summaries of threat activity for compliance or audits?

- A. Threat Activity Recorder
- B. Administrative Reports
- C. Audit Log Viewer
- D. Network Trace Analysis

**Answer: B**

**QUESTION 2**

Which monitoring techniques are used by Threat Defense for Active Directory to identify potentially malicious behaviors in AD environments? (Choose two)

- A. Tracking PowerShell command logs and matching them against whitelisted scripts
- B. Monitoring failed login attempts and abnormal authentication requests
- C. Analyzing Group Policy inheritance across domain trees
- D. Observing abnormal access to administrative shares and sensitive AD objects

**Answer: BD**

**QUESTION 3**

Which two advantages does using a hybrid SES Complete architecture offer for enterprise environments? (Choose two)

- A. Enables rapid deployment without client reinstalls
- B. Supports policy inheritance directly from Active Directory
- C. Provides flexibility in managing cloud and on-premise assets
- D. Requires fewer endpoints for cloud registration

**Answer: AC**

**QUESTION 4**

How can EDR assist security administrators in distinguishing between suspicious and confirmed malicious activity?

- A. By auto-deploying new agents across endpoints
- B. By comparing behaviors against predefined threat intelligence baselines
- C. By modifying user roles and access rights
- D. By issuing licensing alerts for underused devices

**Answer: B**

**QUESTION 5**

Scenario: A tech startup with 200 employees is rapidly scaling its workforce, many of whom are remote. The company is deploying SES Complete but has limited time for hands-on IT support and limited internal infrastructure.

What strategies help maximize SES Complete's benefits for a fast-scaling startup with limited IT

operations? (Choose three)

- A. Use ICDm for real-time monitoring and control
- B. Deploy agents with pre-configured policies via GPO or automated scripts
- C. Set up local policy servers in each location
- D. Implement weekly agent audits by IT staff
- E. Rely on cloud-native auto-update features for threat intelligence

**Answer:** ABE

#### QUESTION 6

What benefit does behavioral tuning offer in the context of App Control and reducing the endpoint attack surface?

- A. It ensures antivirus signatures are updated every 2 hours.
- B. It enables the creation of USB device whitelists.
- C. It fine-tunes detection rules to reduce false positives and improve user experience.
- D. It provides remote desktop access to endpoints during threats.

**Answer:** C

#### QUESTION 7

How does ICDm determine the severity of an incident in the dashboard view?

- A. Based on real-time bandwidth usage
- B. Through threat classification models and policy mapping
- C. By calculating alert count per endpoint
- D. By comparing CPU usage across devices

**Answer:** B

#### QUESTION 8

Which prerequisite is necessary before deploying Threat Defense for Active Directory (TDAD) in SES Complete?

- A. Configuration of LiveUpdate Administrator
- B. Integration of ICDm with Microsoft Intune
- C. Installation of the TDAD sensor on a domain controller
- D. Activation of Network Integrity policies

**Answer:** C

#### QUESTION 9

Which feature in EDR supports submitting executable files for further sandbox-based malware analysis?

- A. Policy Reversion Tool
- B. File Submission
- C. Endpoint Status View

D. Network Integrity Monitor

**Answer: B**

**QUESTION 10**

Which antimalware engine detects a malicious file created with a custom packet?

- A. Emulator
- B. Sapient
- C. Core3
- D. SONAR

**Answer: A**

**QUESTION 11**

Which policy should an administrator edit to utilize the Symantec LiveUpdate server for pre-release content?

- A. The System Policy
- B. The LiveUpdate Policy
- C. The System Schedule Policy
- D. The Firewall Policy

**Answer: A**

**QUESTION 12**

What benefit does deploying Threat Defense for Active Directory offer in hybrid environments with both on-premises and cloud identity providers?

- A. It disables all cloud sync operations while protecting AD.
- B. It supports identity federation between AD and cloud services like Azure AD.
- C. It ensures consistent threat visibility across both on-prem and cloud AD infrastructures.
- D. It allows AD policies to be overridden by cloud-native endpoint policies.

**Answer: C**

**QUESTION 13**

Which two types of policy adaptations are possible using SES Complete behavior-based policy tuning? (Choose two)

- A. Whitelisting internal tools that show abnormal behavior
- B. Automatically uninstalling legacy applications
- C. Blocking applications that do not match expected behavior
- D. Changing device group names based on alert severity

**Answer: AC**

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives

**10% Discount Coupon Code: ASTR14**