# VMware.250-614.v2026-11-16.q45

| | |
|---|---|
| **Exam Code:** | 250-614 |
| **Exam Name:** | Symantec Endpoint Security Complete Admin R4 Technical Specialist |
| **Certification Provider:** | VMware |
| **Free Question Number:** | 45 |
| **Version:** | v2026-11-16 |
| **# of views:** | 113 |
| **# of Questions views:** | 450 |
| https://www.dumpsdb.com/dumps/VMware/250-614/VMware.250-614.v2026-11-16.q45 | |

**NEW QUESTION: 1**
What information is most commonly displayed on the ICDm Home view?
**A.** Policy inheritance hierarchy
**B.** Current threat posture and alerts
**C.** Device enrollment status
**D.** Endpoint OS patch levels
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 2**
What is the primary role of the Symantec Endpoint Security Complete cloud console?
**A.** Centrally manage policies, devices, and security posture
**B.** Act as a network firewall
**C.** Replace on-premises directory services
**D.** Perform local malware scanning on endpoints
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 3**
Why is context important during EDR investigations?
**A.** It automates remediation
**B.** It helps distinguish benign from malicious activity
**C.** It reduces storage needs

**D.** It limits alert visibility
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 4**
After isolating an endpoint, what should be done to ensure full remediation?
**A.** Investigate and remove persistence mechanisms
**B.** Disable alerts
**C.** Delete all logs
**D.** Reboot the endpoint only
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 5**
Which SES Complete controls help prevent threat execution?
(Select all that apply)
**A.** Application Control
**B.** Machine Learning
**C.** Device Grouping
**D.** File Reputation
**Answer: A,B,D (LEAVE A REPLY)**

**NEW QUESTION: 6**
How does Host Integrity support security posture?
**A.** By isolating endpoints
**B.** By managing content updates
**C.** By enforcing endpoint encryption
**D.** By detecting configuration drift
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 7**
Which MITRE ATT&CK tactic involves maintaining access over time?
**A.** Impact
**B.** Initial Access
**C.** Persistence
**D.** Discovery
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 8**
Which method allows administrators to onboard endpoints without manual installer distribution?
**A.** Manual local deployment
**B.** Email-based enrollment

**C.** Offline package installation
**D.** Script-based removal
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 9**
What is the recommended first step for an administrator to perform when beginning a discover and deploy campaign?
**A.** Configure the registry
**B.** Configure the SES policies and Groups
**C.** Disable the Windows firewall
**D.** Install the first SES agent in the subnet
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 10**
What advantage do Custom Application Behavior rules provide over general application blocking?
**A.** Granular control over specific actions
**B.** Automated policy inheritance
**C.** Broader application visibility
**D.** Reduced cloud dependency
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 11**
Which SES Complete capability helps prevent unauthorized device discovery activities?
**A.** Policy versioning
**B.** Host-based firewall controls
**C.** Device enrollment
**D.** ICDm reports
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 12**
What does Host Integrity primarily monitor?
**A.** Network bandwidth usage
**B.** Endpoint configuration and compliance status
**C.** User login activity
**D.** Cloud console availability
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 13**
Why is alert configuration important in ICDm?
**A.** To enable device enrollment

**B.** To control policy inheritance
**C.** To reduce endpoint storage usage
**D.** To ensure timely notification of significant threats
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 14**
Which criteria can be used to organize devices into groups?
(Select all that apply)
**A.** Organizational function
**B.** Threat severity level
**C.** Operating system type
**D.** Business unit requirements
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 15**
Why is the MITRE ATT&CK framework relevant to SES Complete?
**A.** It replaces antivirus signatures
**B.** It provides a model for mapping attacker techniques
**C.** It defines cloud licensing tiers
**D.** It controls endpoint enrollment
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 16**
An endpoint attempts to send sensitive data to an unknown external server. Which SES Complete feature helps block this behavior?
**A.** Adaptive Protection
**B.** Network Threat Protection
**C.** Policy Versioning
**D.** Host Integrity
**Answer: B (LEAVE A REPLY)**

**Valid 250-614 Dumps** shared by TrainingQuiz.com for Helping Passing 250-614 Exam! TrainingQuiz.com now offer the **newest 250-614 exam dumps**, the TrainingQuiz.com 250-614 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 250-614 dumps with Test Engine here: https://www.trainingquiz.com/250-614-practice-quiz.html (**132** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

**NEW QUESTION: 17**

What is the primary benefit of using ICDm reports?
**A.** Providing summarized threat and activity insights
**B.** Configuring security policies
**C.** Automating endpoint enrollment
**D.** Enforcing application restrictions
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 18**
Which data elements are commonly reviewed during EDR investigations?
(Select all that apply)
**A.** Process execution history
**B.** File activity
**C.** Policy assignment history
**D.** Network connections
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 19**
Which actions can be taken as part of threat mitigation?
(Select all that apply)
**A.** Change Active Directory schema
**B.** Quarantine malicious files
**C.** Kill a malicious process
**D.** Isolate an endpoint
**Answer: B,C,D (LEAVE A REPLY)**

**NEW QUESTION: 20**
What is a key benefit of integrated EDR workflows?
**A.** Limited investigation capability
**B.** Increased manual effort
**C.** Reduced endpoint visibility
**D.** Faster detection and response
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 21**
Security teams are overwhelmed by low-severity alerts. What ICDm feature should be adjusted first?
**A.** Endpoint enrollment method
**B.** Device group structure
**C.** Content update frequency
**D.** Alert severity thresholds
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 22**
What is the primary purpose of security policies in SES Complete?
**A.** To manage endpoint licensing
**B.** To define how endpoints are protected and monitored
**C.** To control cloud access permissions
**D.** To configure user authentication
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 23**
Which statement best describes SES Complete device management?
**A.** It provides inventory, status, and control of endpoints
**B.** It focuses only on threat alerts
**C.** It replaces network security tools
**D.** It manages only mobile devices
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 24**
An unknown executable is detected attempting to run on an endpoint. Which control helps restrict its execution without disrupting known applications?
**A.** Content Updates
**B.** Host Integrity
**C.** Adaptive Protection
**D.** Firewall Policy
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 25**
Which policy should an administrator edit to utilize the Symantec LiveUpdate server for pre-release content?
**A.** The System Schedule Policy
**B.** The System Policy
**C.** The LiveUpdate Policy
**D.** The Firewall Policy
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 26**
Which capability helps prevent malicious attempts to delete or encrypt critical data?
**A.** Content Updates
**B.** Application Control
**C.** Cloud Console Alerts
**D.** Device Group Management

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 27**
Which control is most effective against zero-day threats?
**A.** Machine Learning
**B.** Signature-based detection
**C.** Manual analysis
**D.** Policy versioning
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 28**
Which classification does Adaptive Protection use to evaluate applications?
**A.** Trusted, untrusted, expired
**B.** Internal, external, hybrid
**C.** Known good, unknown, malicious
**D.** Critical, high, low
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 29**
Multiple failed authentication attempts followed by a successful login are detected. What does this most likely indicate?
**A.** Brute-force or credential-stuffing attack
**B.** Policy version mismatch
**C.** Endpoint enrollment issue
**D.** Normal user behavior
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 30**
Why is rapid threat response important?
**A.** To increase alert volume
**B.** To reduce licensing costs
**C.** To minimize business impact
**D.** To automate policy creation
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 31**
Which activities might indicate malicious behavior detected by EDR?
(Select all that apply)
**A.** Policy updates
**B.** Unauthorized privilege escalation
**C.** Suspicious network connections

**D.** Process injection
**Answer: B,C,D (LEAVE A REPLY)**

**Valid 250-614 Dumps** shared by TrainingQuiz.com for Helping Passing 250-614 Exam! TrainingQuiz.com now offer the **newest 250-614 exam dumps**, the TrainingQuiz.com 250-614 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 250-614 dumps with Test Engine here: https://www.trainingquiz.com/250-614-practice-quiz.html (**132** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

**NEW QUESTION: 32**
Which report format is supported in Symantec Endpoint Security?
**A.** Text
**B.** XML
**C.** PDF
**D.** HTML
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 33**
What is a key characteristic of SES Complete in a hybrid environment?
**A.** Endpoint policies cannot be shared
**B.** On-premises and cloud endpoints are managed together
**C.** Only cloud endpoints are protected
**D.** Separate consoles are required
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 34**
An analyst needs to identify all endpoints that communicated with a suspicious IP address. Which ICDm capability should be used?
**A.** Alert Configuration
**B.** Policy Versioning
**C.** Event Search
**D.** Device Grouping
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 35**
What role does network protection play in SES Complete?
**A.** It configures device groups
**B.** It manages endpoint enrollment

**C.** It updates security policies
**D.** It blocks malicious inbound and outbound connections
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 36**
Which SES Complete features directly contribute to reducing attack surface?
(Select all that apply)
**A.** Host Integrity
**B.** Adaptive Protection
**C.** ICDm Reporting
**D.** Application Control
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 37**
Which components contribute to a layered defense strategy in SES Complete?
(Select all that apply)
**A.** Detection
**B.** Device enrollment
**C.** Response
**D.** Prevention
**Answer: A,C,D (LEAVE A REPLY)**

**NEW QUESTION: 38**
Which attack goal is most commonly associated with compromising Active Directory?
**A.** Reducing alert volume
**B.** Achieving lateral movement and privilege escalation
**C.** Improving policy management
**D.** Increasing endpoint performance
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 39**
Which capability enables EDR to identify suspicious endpoint activity?
**A.** Behavior analytics
**B.** Content updates
**C.** Policy inheritance
**D.** Device grouping
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 40**
After a surge in ransomware activity, which control should be reviewed to reduce data destruction risks?

**A.** ICDm Search
**B.** Policy Version History
**C.** Device Group Naming
**D.** Application Control
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 41**
Why is Active Directory (AD) a high-value target for attackers?
**A.** It replaces endpoint security agents
**B.** It stores endpoint antivirus signatures
**C.** It controls authentication and authorization across the enterprise
**D.** It manages endpoint content updates
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 42**
Which ICDm capability enables administrators to take direct action on detected events?
**A.** Response actions
**B.** Policy versioning
**C.** Reporting dashboard
**D.** Device grouping
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 43**
What is the primary purpose of ICDm in Symantec Endpoint Security Complete?
**A.** Policy creation and versioning
**B.** Content update distribution
**C.** Endpoint agent deployment
**D.** Centralized investigation and response management
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 44**
Which antimalware engine detects a malicious file created with a custom packet?
**A.** Emulator
**B.** Sapient
**C.** Core3
**D.** SONAR
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 45**
Which MITRE ATT&CK framework step includes destroying data and rendering an endpoint inoperable?

**A.** Kill Chain
**B.** Impact
**C.** Exfiltration
**D.** Rampage
**Answer: B (LEAVE A REPLY)**

**Valid 250-614 Dumps** shared by TrainingQuiz.com for Helping Passing 250-614 Exam! TrainingQuiz.com now offer the **newest 250-614 exam dumps**, the TrainingQuiz.com 250-614 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com 250-614 dumps with Test Engine here: https://www.trainingquiz.com/250-614-practice-quiz.html (**132** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)