VMware.250-614.v2026-09-15.q42

Exam Code:	250-614
Exam Name:	Symantec Endpoint Security Complete Admin R4 Technical Specialist
Certification Provider:	VMware
Free Question Number:	42
Version:	v2026-09-15
# of views:	121
# of Questions views:	420
https://www.exam-tests.com/250-614-exam/VMware.250-614.v2026-09-15.q42.html	

NEW QUESTION: 1
How does EDR differ from traditional endpoint protection?
A. EDR provides visibility into post-execution activity
B. EDR manages endpoint licensing
C. EDR relies only on signatures
D. EDR eliminates prevention controls
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
Which control is most effective against zero-day threats?
A. Machine Learning
B. Policy versioning
C. Signature-based detection
D. Manual analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
Which classification does Adaptive Protection use to evaluate applications?
A. Internal, external, hybrid
B. Known good, unknown, malicious
C. Trusted, untrusted, expired
D. Critical, high, low
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
What is the primary purpose of device groups in SES Complete?
A. Control network segmentation
B. Configure user authentication
C. Assign endpoint licenses
D. Organize endpoints for policy assignment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
When an endpoint is compromised and quarantined, which online resource is available to remediate the infection?
A. Windows Update
B. LiveUpdate
C. SymDiag
D. Security Response
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
After a surge in ransomware activity, which control should be reviewed to reduce data destruction risks?
A. Application Control
B. Device Group Naming
C. ICDm Search
D. Policy Version History
Answer: A (LEAVE A REPLY)

NEW QUESTION: 7
Which activities might indicate malicious behavior detected by EDR?
(Select all that apply)
A. Unauthorized privilege escalation
B. Policy updates
C. Suspicious network connections
D. Process injection
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 8
What information is most commonly displayed on the ICDm Home view?
A. Current threat posture and alerts
B. Policy inheritance hierarchy
C. Endpoint OS patch levels
D. Device enrollment status

Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
An administrator wants different security policies for finance and engineering endpoints.
What SES Complete feature enables this separation?
A. Device groups
B. Content updates
C. Threat mitigation actions
D. ICDm alert filters
Answer: (SHOW ANSWER)

NEW QUESTION: 10
After isolating an endpoint, what should be done to ensure full remediation?
A. Disable alerts
B. Delete all logs
C. Investigate and remove persistence mechanisms
D. Reboot the endpoint only
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
Which indicator is most likely associated with C2 activity?
A. Repeated outbound connections to unknown IPs
B. Increased local disk usage
C. User login failures
D. Endpoint OS updates
Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
Which SES Complete controls rely on behavioral analysis?
(Select all that apply)
A. Adaptive Protection
B. Machine Learning
C. Behavior Monitoring
D. Policy Versioning
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 13
What is a primary advantage of managing hybrid endpoints through SES Complete?
A. Elimination of endpoint telemetry
B. Reduced endpoint visibility
C. Unified policy enforcement across environments

D. Increased reliance on manual processes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 14
Using the ICDm console, a SES administrator issues a device command. When will the command be executed on the endpoint?
A. Immediately
B. When the endpoint reboots
C. At the next heartbeat
D. When the user is idle
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
Which SES Complete capability helps prevent unauthorized device discovery activities?
A. Host-based firewall controls
B. Device enrollment
C. Policy versioning
D. ICDm reports
Answer: (SHOW ANSWER)

NEW QUESTION: 16
An endpoint is confirmed to be compromised. Which EDR action should be taken first to limit lateral movement?
A. Isolate the endpoint
B. Generate a report
C. Reassign device group
D. Update content definitions
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which indicator is most likely to trigger an EDR alert?
A. Regular OS updates

B. Suspicious process execution
C. Policy synchronization
D. User password changes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
Which statement best summarizes Threat Defense for Active Directory in SES Complete?
A. It replaces ICDm functionality
B. It manages endpoint device groups
C. It focuses solely on endpoint malware
D. It protects identities and detects AD-based threats
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which SES Complete controls help prevent threat execution?
(Select all that apply)
A. Device Grouping
B. Machine Learning
C. Application Control
D. File Reputation
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 20
Which statement best summarizes SES Complete security controls?
A. They rely only on signatures
B. They focus exclusively on detection
C. They eliminate the need for administrators
D. They provide layered protection across attack stages
Answer: D (LEAVE A REPLY)

NEW QUESTION: 21
Why is visibility into AD authentication activity critical?
Response:
A. It reduces system performance
B. It increases reporting complexity
C. It replaces endpoint telemetry
D. It helps detect compromised accounts early
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22

A trusted application begins performing suspicious actions. Which feature allows fine-grained control over this behavior?
A. Policy Versioning
B. Custom Application Behavior
C. Device Grouping
D. Adaptive Protection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
Which data sources are typically reviewed during an ICDm investigation?
(Select all that apply)
A. Endpoint telemetry
B. Policy assignment history
C. Network activity logs
D. Alert details
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 24
What is the purpose of Adaptive Protection's Monitor mode?
A. To gain visibility into the operational impact of unusual behavior
B. To view the results of Symantec's behavioral global intelligence data analytics
C. To create a list of risky application behaviors
D. To deny unusual application behavior
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
An endpoint exhibits unusual process spawning behavior without a known malware signature. Which EDR capability detects this?
A. Device management
B. Behavior-based detection
C. Policy versioning
D. Signature scanning
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
Which SES Policy protects against port scan detections?
A. Exploit Mitigation
B. Firewall
C. IPS
D. Device Control
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Why is context important during EDR investigations?
A. It automates remediation
B. It limits alert visibility
C. It reduces storage needs
D. It helps distinguish benign from malicious activity
Answer: (SHOW ANSWER)

NEW QUESTION: 28
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. Install the first SES agent in the subnet
D. Disable the Windows firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 29
How does SES Complete support scalability across large enterprises?
A. Through centralized cloud-based management
B. By requiring local management servers per site
C. By enforcing manual policy updates
D. By limiting device group sizes
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 31
A previously unseen executable attempts to run on an endpoint. Which Adaptive Protection action is most appropriate?
A. Restrict execution until reputation is established
B. Allow execution permanently
C. Uninstall the endpoint agent
D. Disable endpoint networking

Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
What is a key benefit of automatic content updates?
A. Elimination of endpoint agents
B. Reduced endpoint storage usage
C. Faster response to emerging threats
D. Manual administrator control
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
Which layer of protection focuses on stopping threats before execution?
A. Prevention
B. Response
C. Investigation
D. Detection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
Which control helps reduce the attack surface by limiting allowed applications?
A. Application Control
B. Device Grouping
C. Policy Versioning
D. Content Updates
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
Why is the MITRE ATT&CK framework relevant to SES Complete?
A. It controls endpoint enrollment
B. It replaces antivirus signatures
C. It provides a model for mapping attacker techniques
D. It defines cloud licensing tiers

Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
An endpoint fails compliance checks after a configuration change. Which SES Complete feature detects this issue?
A. Content Updates
B. Host Integrity
C. ICDm Search
D. Adaptive Protection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
Which capability enables EDR to identify suspicious endpoint activity?
A. Behavior analytics
B. Policy inheritance
C. Content updates
D. Device grouping
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
Which component is responsible for enforcing security policies on the endpoint?
A. Directory service
B. Cloud console
C. Endpoint agent
D. ICDm portal
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
What is the purpose of policy versioning?
A. Limit policy usage to one endpoint
B. Increase network throughput
C. Track changes and ensure correct policy deployment
D. Control alert thresholds
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40
Which attack goal is most commonly associated with compromising Active Directory?
A. Achieving lateral movement and privilege escalation
B. Improving policy management
C. Reducing alert volume
D. Increasing endpoint performance

Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
What is the name of the cloud-based Management Console that is used to configure and manage an SES Complete implementation?
A. The Integrated Security Protection Manager (ISPm)
B. Symantec Endpoint Security Manager (SESM)
C. The Symantec Console (SC)
D. The Integrated Cyber Defense Manager (ICDm)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 42
Why is endpoint telemetry important for EDR?
A. It automates policy creation
B. It replaces prevention controls
C. It provides visibility into endpoint behavior
D. It reduces storage usage
Answer: C (LEAVE A REPLY)