# Symantec.250-561.v2023-07-06.q23

| | |
|---|---|
| **Exam Code:** | 250-561 |
| **Exam Name:** | Endpoint Security Complete - Administration R1 |
| **Certification Provider:** | Symantec |
| **Free Question Number:** | 23 |
| **Version:** | v2023-07-06 |
| **# of views:** | 102 |
| **# of Questions views:** | 234 |
| https://www.freecram.net/torrent/Symantec.250-561.v2023-07-06.q23.html | |

**NEW QUESTION: 1**
An administrator must create a custom role in ICDm.
Which area of the management console is able to have access restricted or granted?
**A.** Agent deployment
**B.** Policy Management
**C.** Custom Dashboard Creation
**D.** Hybrid device management
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 2**
What is the frequency of feature updates with SES and the Integrated Cyber Defense Manager (ICDm)
**A.** Weekly
**B.** Bi-monthly
**C.** Quarterly
**D.** Monthly
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 3**
Which report template includes a summary of risk distribution by devices, users, and groups?
**A.** Device Integrity
**B.** Comprehensive
**C.** Threat Distribution
**D.** Weekly
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 4**

A user downloads and opens a PDF file with Adobe Acrobat. Unknown to the user, a hidden script in the file begins downloading a RAT.
Which Anti-malware engine recognizes that this behavior is inconsistent with normal Acrobat functionality, blocks the behavior and kills Acrobat?
**A.** Emulator
**B.** IPS
**C.** Sapient
**D.** SONAR
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 5**
Which Symantec component is required to enable two factor authentication with VIP on the Integrated Cyber Defense manager (ICDm)?
**A.** A physical token or a secure USB key
**B.** A software token and an active directory account
**C.** A physical token or a software token
**D.** A software token and a VIP server
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 6**
The ICDm has generated a blacklist task due to malicious traffic detection. Which SES component was utilized to make that detection?
**A.** Antimalware
**B.** IPS
**C.** Firewall
**D.** Reputation
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 7**
Which two (2) steps should an administrator take to guard against re-occurring threats? (Select two)
**A.** Confirm that daily active and weekly full scans take place on all endpoints
**B.** Quarantine affected endpoints
**C.** Use Power Eraser to clean endpoint Windows registries
**D.** Add endpoints to a high security group and assign a restrictive Antimalware policy to the group
**E.** Verify that all endpoints receive scheduled Live-Update content
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 8**
Which alert rule category includes events that are generated about the cloud console?
**A.** System

**B.** Diagnostic
**C.** Application Activity
**D.** Security
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 9**
What are two (2) benefits of a fully cloud managed endpoint protection solution? (Select two)
**A.** Increased content update frequency
**B.** Reduced 3rd party licensing cost
**C.** Reduced database usage
**D.** Reduced network usage
**E.** Increased visibility
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 10**
Which statement best defines Machine Learning?
**A.** A program that needs user input to perform a task.
**B.** A program that teams from observing other programs.
**C.** A program that learns from experience to optimize the output of a task.
**D.** A program that require data to perform a task.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 11**
Which two (2) Discovery and Deploy features could an administrator use to enroll MAC endpoints? (Select two)
**A.** Invite User
**B.** A custom Direct installation package
**C.** Push Enroll
**D.** A custom Installation package creator pact
**E.** A default Direct Installation package
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 12**
What are the Exploit Mitigation security control's mitigation techniques designed to prevent?
**A.** Misbehaving applications
**B.** Packed file execution
**C.** Rootkit downloads
**D.** File-less attacks
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 13**

What characterizes an emerging threat in comparison to traditional threat?
**A.** Emerging threats use new techniques and 0-day vulnerability to propagate.
**B.** Emerging threats requires artificial intelligence to be detected.
**C.** Emerging threats are undetectable by signature based engines.
**D.** Emerging threats are more sophisticated than traditional threats.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 14**
Which Anti-malware technology should an administrator utilize to expose the malicious nature of a file created with a custom packet?
**A.** Sandbox
**B.** SONAR
**C.** Reputation
**D.** Emulator
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 15**
Which option should an administrator utilize to temporarily or permanently block a file?
**A.** Encrypt
**B.** Delete
**C.** Blacklist
**D.** Hide
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 16**
In which phase of MITRE framework would attackers exploit faults in software to directly tamper with system memory?
**A.** Defense Evasion
**B.** Discovery
**C.** Execution
**D.** Exfiltration
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 17**
An administrator learns of a potentially malicious file and wants to proactively prevent the file from ever being executed.
What should the administrator do?
**A.** Add the filename and SHA-256 hash to a Blacklist policy
**B.** Adjust the Antimalware policy age and prevalence settings
**C.** Add the file SHA1 to a blacklist policy
**D.** Increase the Antimalware policy Intensity to Level 5
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 18**
Which file property does SES utilize to search the VirusTotal website for suspicious file information?
**A.** File size
**B.** File hash
**C.** File name
**D.** File reputation
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 19**
Which default role has the most limited permission in the Integrated Cyber Defense Manager?
**A.** Limited Administrator
**B.** Endpoint Console Domain Administrator
**C.** Server Administrator
**D.** Restricted Administrator
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 20**
What version number is assigned to a duplicated policy?
**A.** One
**B.** Zero
**C.** The original policy's number plus one
**D.** The original policy's version numb
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 21**
Which security control is complementary to IPS, providing a second layer of protection against network attacks?

**A.** Antimalware
**B.** Firewall
**C.** Host Integrity
**D.** Network Protection
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 22**
Which policy should an administrator edit to utilize the Symantec LiveUpdate server for pre-release content?
**A.** The LiveUpdate Policy
**B.** The Firewall Policy
**C.** The System Policy
**D.** The System Schedule Policy
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 23**
Which Endpoint > Setting should an administrator utilize to locate unmanaged endpoints on a network subnet?
**A.** Discover and Deploy
**B.** Endpoint Enrollment
**C.** Discover Endpoints
**D.** Device Discovery
**Answer: (SHOW ANSWER)**