IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **250-580**

Title : Endpoint Security Complete - R2 Technical Specialist

Version : DEMO

1.What EDR function minimizes the risk of an endpoint infecting other resources in the environment?
A. Quarantine
B. Block
C. Deny List
D. Firewall
Answer: A
Explanation:
The function of "Quarantine" in Endpoint Detection and Response (EDR) minimizes the risk of an infected endpoint spreading malware or malicious activities to other systems within the network environment. This is accomplished by isolating or restricting access of the infected endpoint to contain any threat within that specific machine. Here's how Quarantine functions as a protective measure:
Detection and Isolation: When EDR detects potential malicious behavior or files on an endpoint, it can automatically place the infected file or process in a "quarantine" area. This means the threat is separated from the rest of the system, restricting its ability to execute or interact with other resources.
Minimizing Spread: By isolating compromised files or applications, Quarantine ensures that malware or suspicious activities do not propagate to other endpoints, reducing the risk of a widespread infection.
Administrative Review: After an item is quarantined, administrators can review it to determine if it should be deleted or restored based on a false positive evaluation. This controlled environment allows for further analysis without risking network security.
Endpoint-Specific Control: Quarantine is designed to act at the endpoint level, applying restrictions that affect only the infected system without disrupting other network resources.
Using Quarantine as an EDR response mechanism aligns with best practices outlined in endpoint security documentation, such as Symantec Endpoint Protection, which emphasizes containment as a critical first response to threats. This approach supports the proactive defense strategy of limiting lateral movement of malware across a network, thus preserving the security and stability of the entire system.

2.What priority would an incident that may have an impact on business be considered?
A. Low
B. Critical
C. High
D. Medium
Answer: C
Explanation:
An incident that may have an impact on business is typically classified with a High priority in cybersecurity frameworks and incident response protocols. Here's a detailed rationale for this classification:
Potential Business Disruption: An incident that affects or threatens to affect business operations, even if indirectly, is assigned a high priority to ensure swift response. This classification prioritizes incidents that may not be immediately critical but could escalate if not addressed promptly.
Risk of Escalation: High-priority incidents are situations that, while not catastrophic, have the potential to impact critical systems or compromise sensitive data, thus needing attention before they lead to severe business repercussions.
Rapid Response Requirement: Incidents labeled as high priority are flagged for immediate investigation

and containment measures to prevent further business impact or operational downtime.
In this context, while Critical incidents involve urgent threats with immediate, severe effects (such as active data breaches), a High priority applies to incidents with significant risk or potential for business impact. This prioritization is essential for effective incident management, enabling resources to focus on potential risks to business continuity.

3.Which antimalware intensity level is defined by the following: "Blocks files that are most certainly bad or potentially bad files results in a comparable number of false positives and false negatives."
A. Level 6
B. Level 5
C. Level 2
D. Level 1
Answer: B
Explanation:
In antimalware solutions, Level 5 intensity is defined as a setting where the software blocks files that are considered either most certainly malicious or potentially malicious. This level aims to balance security with usability by erring on the side of caution; however, it acknowledges that some level of both false positives (legitimate files mistakenly flagged as threats) and false negatives (malicious files mistakenly deemed safe) may still occur.
This level is typically used in environments where security tolerance is high but with an understanding that some legitimate files might occasionally be flagged. It provides robust protection without the extreme strictness of the highest levels, thus reducing, but not eliminating, the possibility of false alerts while maintaining an aggressive security posture.

4.The SES Intrusion Prevention System has blocked an intruder's attempt to establish an IRC connection inside the firewall.
Which Advanced Firewall Protection setting should an administrator enable to prevent the intruder's system from communicating with the network after the IPS detection?
A. Enable port scan detection
B. Automatically block an attacker's IP address
C. Block all traffic until the firewall starts and after the firewall stops
D. Enable denial of service detection
Answer: B
Explanation:
To enhance security and prevent further attempts from the intruder after the Intrusion Prevention System (IPS) has detected and blocked an attack, the administrator should enable the setting to Automatically block an attacker's IP address.
Here’s why this setting is critical:
Immediate Action Against Threats: By automatically blocking the IP address of the detected attacker, the firewall can prevent any further communication attempts from that address. This helps to mitigate the risk of subsequent attacks or reconnections.
Proactive Defense Mechanism: Enabling this feature serves as a proactive defense strategy, minimizing the chances of successful future intrusions by making it harder for the attacker to re-establish a connection to the network.

Reduction of Administrative Overhead: Automating this response allows the security team to focus on investigating and remediating the incident rather than manually tracking and blocking malicious IP addresses, thus optimizing incident response workflows.
Layered Security Approach: This setting complements other security measures, such as intrusion detection and port scan detection, creating a layered security approach that enhances overall network security.
Enabling automatic blocking of an attacker's IP address directly addresses the immediate risk posed by the detected intrusion and reinforces the organization's defense posture against future threats.

5.After several failed logon attempts, the Symantec Endpoint Protection Manager (SEPM) has locked the default admin account. An administrator needs to make system changes as soon as possible to address an outbreak, but the admin account is the only account.
Which action should the administrator take to correct the problem with minimal impact on the existing environment?
A. Wait 15 minutes and attempt to log on again
B. Restore the SEPM from a backup
C. Run the Management Server and Configuration Wizard to reconfigure the server
D. Reinstall the SEPM
Answer: A
Explanation:
In the situation where the default admin account of the Symantec Endpoint Protection Manager (SEPM) is locked after several failed login attempts, the best course of action for the administrator is to wait 15 minutes and attempt to log on again.
Here's why this approach is advisable:
Account Lockout Policy: Most systems, including SEPM, are designed with account lockout policies that temporarily disable accounts after a number of failed login attempts. Typically, these policies include a reset time (often around 15 minutes), after which the account becomes active again.
Minimal Disruption: Waiting for the account to automatically unlock minimizes disruption to the existing environment. This avoids potentially complex recovery processes or the need to restore from a backup, which could introduce additional complications or data loss.
Avoiding System Changes: Taking actions such as restoring the SEPM from a backup, reconfiguring the server, or reinstalling could lead to significant changes in the configuration and might cause further complications, especially if immediate action is needed to address an outbreak. Prioritizing Response to Threats: While it's important to respond to security incidents quickly, maintaining the integrity of the SEPM configuration and ensuring a smooth recovery is also crucial. Waiting for the lockout period respects the system's security protocols and allows the administrator to regain access with minimal risk.
In summary, waiting for the lockout to expire is the most straightforward and least disruptive solution, allowing the administrator to resume critical functions without unnecessary risk to the SEPM environment.