CrowdStrike Certified Falcon Administrator (CCFA) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **What type of host group allows the use of filters to define its members?**

   A. Static host group

   B. Dynamic host group

   C. Manual host group

   D. Default host group

2. **What is one method to uninstall the Falcon sensor on Windows?**

   A. Control Panel or the command line

   B. Task Manager or settings app

   C. PowerShell only

   D. System Preferences or command line

3. **Hunting Reports in CrowdStrike mainly provide information regarding?**

   A. Network performance metrics and bandwidth usage

   B. Potentially suspicious activity like executables running from certain directories

   C. Updates on software patches and vulnerabilities

   D. User account permission changes and audit logs

4. **How can you view the current sensor grouping tags on a Mac?**

   A. falconctl current-tags

   B. sudo falconctl grouping-tags get

   C. view falcon tags

   D. check falconctl tags

5. **The Prevention Policy Audit Trail details changes made to which of the following?**

   A. Sensor monitoring settings

   B. User access levels

   C. Prevention policies

   D. File inclusion settings

6. Which parameter is used to ensure the Falcon sensor installation occurs without immediate launch?

A. NO_START=1

B. DISABLE_LAUNCH=TRUE

C. FORCE_INSTALL=FALSE

D. PREVENT_START=YES

7. What role does the Falcon Security Lead have regarding user password management?

A. Can assign new user roles

B. Can reset passwords and 2FA tokens

C. Can manage all user accounts

D. Can modify system permissions

8. How long do tags persist if all associated hosts are inactive?

A. 30 days

B. 45 days

C. 60 days

D. 90 days

9. Which of the following best describes the function of Linux sensors in RFM?

A. They extensively monitor system events.

B. They send heartbeats but have no detections.

C. They operate with full detection capabilities.

D. They remove the need for manual updates.

10. Which of the following statements is true about the On-Cloud Machine Learning?

A. It operates only when connected to the internet

B. It interferes with existing Anti-Virus tools

C. It avoids storing bad hashes on the host

D. It functions independently of file attributes

Answers

1. **B**
2. **A**
3. **B**
4. **B**
5. **C**
6. **A**
7. **B**
8. **B**
9. **B**
10. **C**

Explanations

1. What type of host group allows the use of filters to define its members?

A. Static host group

B. Dynamic host group

C. Manual host group

D. Default host group

A dynamic host group is designed to automatically include members based on specified filters or criteria. This means that the members of a dynamic host group can change over time as the data that meets the filter criteria changes. For instance, if the filter is set to include all hosts running a certain operating system version, any new hosts that meet this criterion will automatically be added to the group. This feature ensures that the group is always up-to-date without manual intervention, making it highly efficient for environment management. In contrast, static host groups consist of a pre-defined set of hosts that do not change unless manually updated. Manual host groups also require individual management and do not utilize filters for dynamic membership. Default host groups typically serve as a foundational grouping but lack the filtering capability that is characteristic of dynamic host groups. Thus, dynamic host groups provide flexibility and ease of management through the use of filters, making them a preferred option in many scenarios.

2. What is one method to uninstall the Falcon sensor on Windows?

A. Control Panel or the command line

B. Task Manager or settings app

C. PowerShell only

D. System Preferences or command line

The correct response identifies that one method to uninstall the Falcon sensor on Windows is through the Control Panel or the command line. This approach aligns with standard Windows practices for managing installed software, where users can access the Control Panel to find and remove programs from their system. The command line also offers a powerful alternative for users who prefer or require automated script functionalities. Using the Control Panel is straightforward and familiar to most Windows users, comprising a graphic user interface that allows easy navigation to installed applications and their uninstallation. On the other hand, utilizing the command line offers flexibility and the ability to streamline the uninstallation process, especially in larger environments or remote management scenarios. Other options, such as using Task Manager or the settings app, do not provide standard methods for uninstallation of the Falcon sensor, though they may facilitate task management or general settings adjustments within the operating system. Similarly, PowerShell, despite its advanced capabilities for managing system configurations, is not the sole option for uninstallation, and System Preferences is not applicable to Windows, as it pertains to macOS.

3. Hunting Reports in CrowdStrike mainly provide information regarding?

A. Network performance metrics and bandwidth usage

B. Potentially suspicious activity like executables running from certain directories

C. Updates on software patches and vulnerabilities

D. User account permission changes and audit logs

Hunting Reports in CrowdStrike are primarily focused on identifying potentially suspicious activities within an environment, which can include things like executables running from unusual directories or patterns that deviate from normal behavior. This function is crucial for threat detection and response, as it allows security analysts to proactively investigate and mitigate risks posed by malicious actors. By highlighting these anomalies, the reports enable organizations to take swift action before any real harm occurs. The other options, while they do relate to aspects of security and IT management, fall outside the main focus of Hunting Reports. For instance, network performance metrics relate to the operational health of a network rather than security threats, software patches pertain to system maintenance rather than real-time detection of threats, and audit logs regarding user account changes are more about compliance and tracking rather than actively hunting for threats. Therefore, the emphasis of the Hunting Reports on potentially suspicious activity is what makes that choice the most relevant and correct answer in this context.

4. How can you view the current sensor grouping tags on a Mac?

A. falconctl current-tags

B. sudo falconctl grouping-tags get

C. view falcon tags

D. check falconctl tags

To view the current sensor grouping tags on a Mac, the command "sudo falconctl grouping-tags get" is used. This command directly retrieves and displays the grouping tags applied to the Falcon sensor on the macOS system. The use of "sudo" indicates that the command is run with superuser privileges, which is often necessary for interactions with system-level components like the Falcon sensor. The syntax of this command specifies that you're querying the current tags related to grouping, making it clear and specific for the purpose of inspection. It's important to utilize the correct command structure to ensure that the information retrieved is accurate and pertains specifically to the sensor's current configuration. This command is essential for administrators needing to manage or troubleshoot sensor deployments effectively.

5. The Prevention Policy Audit Trail details changes made to which of the following?

A. Sensor monitoring settings

B. User access levels

C. Prevention policies

D. File inclusion settings

The Prevention Policy Audit Trail is specifically designed to capture and record changes made to prevention policies within the CrowdStrike Falcon platform. This component of the system ensures that any adjustments or modifications to how threats are managed and mitigated are accurately tracked. By monitoring these changes, administrators can maintain oversight of their security configurations, allowing for greater accountability and traceability in security operations. Understanding the context of this feature highlights its importance in ensuring that any alterations to prevention policies are logged, enabling the organization to assess the impact of these changes over time. This capability is essential for security compliance and governance, as it allows teams to review past actions and understand the configuration landscape at any given moment, ultimately bolstering the organization's defense posture. In contrast, details such as sensor monitoring settings, user access levels, and file inclusion settings pertain to different aspects of configuration and management within the CrowdStrike platform, but are not covered under the Prevention Policy Audit Trail. Each of these areas has its own distinct tracking and management processes, underscoring the focused nature of the Prevention Policy Audit Trail on prevention policies specifically.

6. Which parameter is used to ensure the Falcon sensor installation occurs without immediate launch?

A. NO_START=1

B. DISABLE_LAUNCH=TRUE

C. FORCE_INSTALL=FALSE

D. PREVENT_START=YES

The parameter that is used to ensure the Falcon sensor installation occurs without immediate launch is designated as NO_START=1. This specific parameter indicates that the installation process should complete without initiating the sensor right away. In scenarios where you need to install the sensor but want to control when it goes active, setting this parameter allows the installation to finish without starting the sensor immediately. This is useful in environments where an administrator needs to conduct additional configurations or checks before allowing the sensor to start monitoring. In contrast, the other options either promote starting the sensor or don't provide the specific functionality required. For instance, DISABLE_LAUNCH=TRUE would imply that the sensor is to be disabled entirely, which is not the intended behavior of just delaying the launch. Similarly, FORCE_INSTALL=FALSE does not pertain to controlling the launch timing but rather concerns how the installation behaves regarding forced installation scenarios. PREVENT_START=YES suggests a prohibition on starting the sensor but is not a recognized parameter used in the installation context for delay. Thus, NO_START=1 is the explicit and correct choice for halting immediate sensor activation post-installation.

7. What role does the Falcon Security Lead have regarding user password management?

A. Can assign new user roles

B. Can reset passwords and 2FA tokens

C. Can manage all user accounts

D. Can modify system permissions

The Falcon Security Lead is positioned to oversee critical aspects of user account management, including the responsibility for resetting passwords and two-factor authentication (2FA) tokens. In an organization utilizing CrowdStrike's Falcon platform, the Security Lead plays a vital role in ensuring that access control measures are upheld and that users can regain access to their accounts when needed. Resetting passwords and 2FA tokens is crucial for maintaining the security integrity of user accounts, especially in the event of a compromised password or an inability to access a 2FA method. This role helps facilitate secure access while minimizing any potential downtime for users who may be locked out of their accounts. The other roles mentioned in the other choices revolve around user roles, account management, and system permissions but do not specifically address the critical function of overseeing password and authentication management that the Falcon Security Lead is empowered to perform.

8. How long do tags persist if all associated hosts are inactive?

A. 30 days

B. 45 days

C. 60 days

D. 90 days

Tags in the CrowdStrike environment are used to organize and manage the various hosts you are monitoring. When all associated hosts are inactive, their tags will persist for a set period. In this case, the correct duration for tags to remain in the system after the last associated host has gone inactive is 45 days. This timeframe allows administrators ample opportunity to reactivate those hosts or assess their status before the tags are permanently removed from the system. The persistence of 45 days balances operational efficiency with the need for administrators to maintain an accurate overview of their environment. During this time, any historical insights related to the tags can still be utilized effectively, which aids in security management and decision-making. After 45 days without any active hosts, tags are considered obsolete and are then removed to keep the tagging system relevant and uncluttered. This ensures that administrators are not overwhelmed by outdated tags that no longer serve a purpose.

9. Which of the following best describes the function of Linux sensors in RFM?

A. They extensively monitor system events.

B. They send heartbeats but have no detections.

C. They operate with full detection capabilities.

D. They remove the need for manual updates.

The function of Linux sensors in the context of RFM (Real-time File Monitoring) primarily involves monitoring and sending periodic status updates rather than directly identifying and responding to threats. In this capacity, the sensors act like support mechanisms, ensuring that the system is responsive by sending heartbeats, indicating that they are active and functioning. These sensors are designed to provide foundational visibility and operational awareness, but they do not engage in direct detection processes like their counterparts in other operating systems that might have fuller capabilities. Therefore, the emphasis on sending heartbeats signifies an important role in maintaining system communication and integrity, while the lack of detection suggests a limit to their direct engagement with threat mitigation. Understanding this function is crucial for administrators when configuring and managing Linux sensors within Falcon. Knowing their limitations allows for appropriate expectations and better strategic planning for security measures in their environments.

10. Which of the following statements is true about the On-Cloud Machine Learning?

A. It operates only when connected to the internet

B. It interferes with existing Anti-Virus tools

C. It avoids storing bad hashes on the host

D. It functions independently of file attributes

The assertion that On-Cloud Machine Learning avoids storing bad hashes on the host is accurate. This approach leverages the cloud's capabilities to utilize vast amounts of data and advanced algorithms for analysis and detection, which allows it to minimize the use of local resources and avoid the risks associated with malicious hash storage on the endpoint itself. By operating primarily in the cloud, it ensures that potentially harmful signatures or indicators of compromise (IOCs) aren't retained locally, thus enhancing security and reducing the attack surface. The cloud-based nature of the machine learning model means it can continuously learn and adapt without the need for persistent local storage of potentially harmful data. This makes it more efficient and responsive to emerging threats, as it can rely on centralized processing power and updated intelligence without compromising the security of the endpoint. In contrast, the other statements do not accurately reflect the functionality of On-Cloud Machine Learning. For instance, its reliance on internet connectivity is not a limitation but a fundamental characteristic of cloud solutions. Similarly, it does not inherently interfere with existing Anti-Virus tools; rather, it complements them by enhancing detection capabilities. Lastly, while it does analyze file attributes for classification and threat detection purposes, it does not function entirely independently of them, as file characteristics can play a role