# CrowdStrike Falcon Platform Practice Test (Sample)

## Study Guide


**Everything you need from our exam experts!**

# Questions

1. **What type of actions can users perform if they are assigned the Real Time Responder - Read Only Analyst Role?**
   - A. Execute remediation commands
   - B. Manage user permissions
   - C. Run read-only response commands
   - D. Create new alert rules

2. **How does CrowdStrike Falcon contribute to incident recovery?**
   - A. By permanently deleting all breach-related data
   - B. By providing tools and insights for system restoration
   - C. By performing automatic backups and recovery
   - D. By notifying users about the incident

3. **Which of the following best describes exploit prevention?**
   - A. A method used solely for network traffic management
   - B. A proactive security feature against malware attacks on known vulnerabilities
   - C. A technique focused on improving user productivity
   - D. A tool for managing user permissions

4. **Which feature enhances the analysis of potential security incidents?**
   - A. Real-time data logging
   - B. Machine learning algorithms
   - C. Static code analysis
   - D. Manual threat assessments

5. **What does "malware containment" help accomplish in the Falcon Platform?**
   - A. Updating software regularly
   - B. Isolating compromised endpoints
   - C. Scoring applications for security
   - D. Implementing user training

**6. How can organizations ensure compliance with regulations using the Falcon Platform?**

- **A. By utilizing social media integration features**
- **B. By using the reporting features and data logging capabilities**
- **C. By employing manual monitoring of user activities**
- **D. By offering employee training sessions only**

**7. What happens when an active host is deleted within the CrowdStrike Falcon dashboard?**

- **A. The host is permanently removed**
- **B. The host is moved to Trash but continues sending events**
- **C. The host is quarantined**
- **D. The host is disabled**

**8. What is “behavioral-based detection”?**

- **A. A method depending solely on user behavior**
- **B. A detection method focusing on unusual behavior patterns**
- **C. A signature-based detection technique**
- **D. A manual review of logs**

**9. What is the significance of the Falcon Dashboard?**

- **A. It displays user permissions**
- **B. It provides an overview of security status and threats**
- **C. It serves as a backup solution**
- **D. It hosts live training sessions**

**10. What feature in CrowdStrike Falcon allows users to define and enforce policies for detecting malicious activities?**

- **A. Threat Intelligence Manager**
- **B. Falcon Policy Manager**
- **C. Response Command Center**
- **D. Secure Endpoint Manager**

# Answers

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

# Explanations

## 1. What type of actions can users perform if they are assigned the Real Time Responder - Read Only Analyst Role?

**A. Execute remediation commands**

**B. Manage user permissions**

**C. Run read-only response commands**

**D. Create new alert rules**

**The role of a Real Time Responder - Read Only Analyst is specifically designed to allow users to observe and analyze data without the ability to execute commands that could alter the environment or system state. Therefore, users assigned this role can run read-only response commands, which are vital for assessment and analysis. This means they can access and review live data and telemetry, assess threat events, and gather intelligence through the platform's interfaces without making changes or impacting ongoing operations. This role is primarily focused on providing insights, allowing analysts to effectively monitor security incidents, visualize live system states, and gather information required for decision-making, all while maintaining system integrity by restricting the ability to carry out remediation or operational commands. Hence, it serves a critical purpose in incident response by enabling thorough investigation and oversight without the complications of execution permissions.**

## 2. How does CrowdStrike Falcon contribute to incident recovery?

**A. By permanently deleting all breach-related data**

**B. By providing tools and insights for system restoration**

**C. By performing automatic backups and recovery**

**D. By notifying users about the incident**

**CrowdStrike Falcon contributes to incident recovery primarily through the provision of tools and insights for system restoration. After a security incident, organizations need to understand what aspects of their systems were affected, the nature of the attack, and a clear path forward to restore operations. CrowdStrike Falcon's approach includes detailed forensics and visibility into the incident, which helps teams to identify compromised endpoints and rectify vulnerabilities. The platform offers features such as threat intelligence, attack surface reduction, and post-incident analysis, which are essential for understanding how to effectively restore systems to a secure state. This allows organizations to not only recover from the incident but also improve their security posture to prevent future occurrences. Having detailed information about the nature of the attack and affected systems empowers incident response teams to make informed decisions about recovery strategies, ensuring that they can effectively restore operations while minimizing risk. In comparison, options that involve automatically deleting data or performing backups focus on reactive measures rather than the proactive insights and tools needed for comprehensive incident recovery. Notifying users about an incident does not encapsulate the broader role that Falcon plays in aiding organizations through the recovery process, which emphasizes the need for analysis and restoration capability.**

## 3. Which of the following best describes exploit prevention?

**A. A method used solely for network traffic management**

**B. A proactive security feature against malware attacks on known vulnerabilities**

**C. A technique focused on improving user productivity**

**D. A tool for managing user permissions**

**Exploit prevention is best described as a proactive security feature designed specifically to guard against malware attacks that target known vulnerabilities in software and systems. This approach is critical in cybersecurity because it aims to stop the exploitation of vulnerabilities before they can be successfully leveraged by attackers to compromise a system. It involves the use of various techniques, including intrusion prevention systems, behavioral analysis, and signature-based threat detection, to identify and thwart malicious activities. The focus of exploit prevention is on anticipating potential threats and blocking them in real-time, thereby enhancing the overall security posture of an organization. This differs significantly from other options, such as solely managing network traffic, improving user productivity, or managing user permissions, which do not directly address the risks associated with exploitation of vulnerabilities by malware.**

## 4. Which feature enhances the analysis of potential security incidents?

**A. Real-time data logging**

**B. Machine learning algorithms**

**C. Static code analysis**

**D. Manual threat assessments**

**Machine learning algorithms significantly enhance the analysis of potential security incidents by enabling automated detection and response capabilities. These algorithms process and analyze vast amounts of data to identify patterns, anomalies, and potential threats that may not be immediately apparent to human analysts. By leveraging historical data and continuously learning from new threats and incidents, machine learning algorithms can improve the accuracy and efficiency of threat detection and incident analysis. This capability allows organizations to respond more swiftly to emerging threats, as these algorithms can often recognize and react to indicators of compromise in real-time. Additionally, the predictive nature of machine learning can help anticipate future threats by analyzing trends and behaviors associated with past incidents, further enhancing an organization's overall security posture. Other options, while they each have their advantages, do not offer the same level of adaptability and efficiency that machine learning provides in the context of analyzing security incidents. Real-time data logging offers visibility but lacks analysis capabilities on its own. Static code analysis helps identify vulnerabilities in the software development phase but does not address live incident analysis. Manual threat assessments rely on human expertise, which can be time-consuming and may miss quick-moving threats.**

## 5. What does "malware containment" help accomplish in the Falcon Platform?

**A. Updating software regularly**

**B. Isolating compromised endpoints**

**C. Scoring applications for security**

**D. Implementing user training**

**Malware containment within the CrowdStrike Falcon Platform is designed to isolate compromised endpoints. This crucial feature allows organizations to effectively reduce the risk of further infection or data exfiltration once a potential malware incident has been detected on a system. By isolating an endpoint, the Falcon Platform prevents malicious activity from spreading across the network, allowing for a more controlled investigation and remediation process. When an endpoint is isolated, it is cut off from the rest of the network while still maintaining essential management and monitoring capabilities. This ensures that security teams can respond swiftly to the threat without impacting the entire network's functionality. Additionally, containment helps in preserving forensic data that can be critical for understanding the nature and extent of the compromise. Other options, while they may be important elements of a complete security strategy, do not directly relate to the specific function of containment that the Falcon Platform provides in dealing with malware incidents. For instance, updating software regularly is more about preventative maintenance rather than active response to a compromise, scoring applications for security deals with evaluating risks, and user training focuses on human factors in security.**

## 6. How can organizations ensure compliance with regulations using the Falcon Platform?

**A. By utilizing social media integration features**

**B. By using the reporting features and data logging capabilities**

**C. By employing manual monitoring of user activities**

**D. By offering employee training sessions only**

**Organizations can ensure compliance with regulations by leveraging the reporting features and data logging capabilities available on the Falcon Platform. These features enable organizations to collect and analyze data related to their security posture, which is vital for regulatory compliance. Effective reporting capabilities allow organizations to generate detailed logs and reports that document security events and incidents, ensuring that they have the necessary evidence to demonstrate compliance during audits. Additionally, data logging capabilities provide a record of user activities, system changes, and security measures implemented, which can be critical for meeting various regulatory requirements. Regulatory compliance often mandates specific record-keeping and reporting standards; thus, having a robust system that can accurately track and report on relevant data significantly helps organizations meet these obligations. This not only prepares them for compliance checks but also enhances their overall security by keeping a transparent account of their security measures and incidents.**

## 7. What happens when an active host is deleted within the CrowdStrike Falcon dashboard?

**A. The host is permanently removed**

**B. The host is moved to Trash but continues sending events**

**C. The host is quarantined**

**D. The host is disabled**

**When an active host is deleted within the CrowdStrike Falcon dashboard, the correct outcome is that the host is moved to Trash but continues sending events. This process allows for a temporary removal of the host from the active list without losing the historical data or event information associated with it. Moving the host to Trash means that while it is no longer considered an active or monitored host within the dashboard, it still retains its connection and can send events back to the Falcon platform. This feature is particularly beneficial for maintaining a view of past activities and for potential future investigations or compliance audits, as the data can still be analyzed even though the host itself is not actively managed. In contrast to other options, where a host would either be permanently removed, quarantined, or disabled, the ability to continue receiving events while in Trash allows for ongoing monitoring of the host's activities even after its deletion from the main dashboard interface. This reflects a nuanced approach to host management, prioritizing data integrity and continued oversight.**

## 8. What is “behavioral-based detection”?

**A. A method depending solely on user behavior**

**B. A detection method focusing on unusual behavior patterns**

**C. A signature-based detection technique**

**D. A manual review of logs**

**Behavioral-based detection refers to a method of identifying potential threats by monitoring and analyzing patterns of activity within a system or network. This approach focuses on recognizing unusual or suspicious behavior that deviates from established norms. By looking for anomalies, such as unexpected file movements, abnormal network traffic, or unusual login attempts, behavioral-based detection can identify malicious actions that might not be recognized through traditional methods, which often rely on known signatures of malware or specific patterns of activity. This technique is particularly valuable in cybersecurity, as it can detect never-before-seen attacks or zero-day exploits that do not match any known signatures. It leverages machine learning and artificial intelligence to continuously learn and adapt to new behaviors, improving the accuracy and efficacy of threat detection over time.**

## 9. What is the significance of the Falcon Dashboard?

**A. It displays user permissions**

**B. It provides an overview of security status and threats**

**C. It serves as a backup solution**

**D. It hosts live training sessions**

**The Falcon Dashboard is significant because it provides an overview of the security status and threats facing an organization. This central hub is critical for security professionals, as it aggregates and presents real-time data on endpoint activity, detection of threats, and overall security posture. By visualizing security metrics and trends, users can quickly identify vulnerabilities, understand the current threat landscape, and make informed decisions about security measures and incident response. The dashboard includes information such as alerts for detected threats, statistics on active endpoints, and other key performance indicators that help organizations monitor their security health. This insight is essential in prioritizing response actions and ensuring that the security team effectively addresses any potential risks to the organization.**

## 10. What feature in CrowdStrike Falcon allows users to define and enforce policies for detecting malicious activities?

**A. Threat Intelligence Manager**

**B. Falcon Policy Manager**

**C. Response Command Center**

**D. Secure Endpoint Manager**

**The Falcon Policy Manager is a key feature in CrowdStrike Falcon that empowers users to define and enforce policies tailored for detecting malicious activities. This tool enables security teams to establish rules and parameters that dictate how the Falcon platform identifies potential threats, thus ensuring a proactive approach to cyber threat management. By utilizing the Falcon Policy Manager, organizations can customize their detection strategies to align with their specific operational environment, compliance requirements, and risk levels. This includes configuring settings for various detection capabilities such as antivirus, firewall, and behavior-based detection. Ultimately, the effective use of the Falcon Policy Manager enhances the overall security posture by fostering a more structured and organized approach to threat detection and management.**