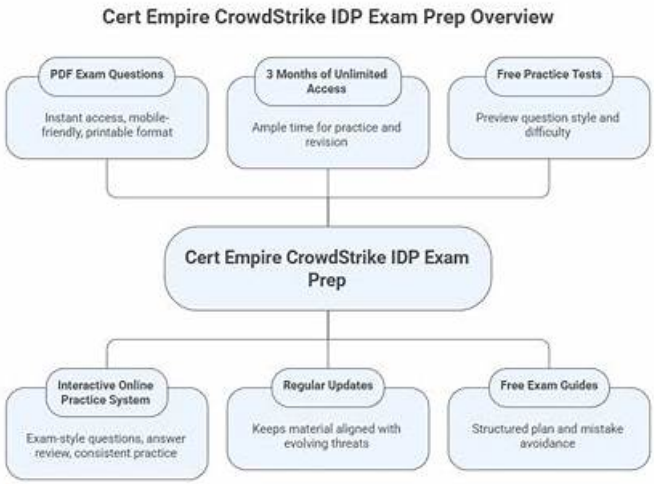
CrowdStrike IDP Questions - Reduce your Chances of Failure in Exam



BONUS!!! Download part of Fast2test IDP dumps for free: https://drive.google.com/open?id=1DIfJBTKrmStvbVAsE1HcdJUsTFC8879f

If you choose the test IDP certification and then buy our IDP study materials you will get the panacea to both get the useful certificate and spend little time. Passing the test certification can help you stand out in your colleagues and have a bright future in your career. If you buy our IDP Study Materials you odds to pass the test will definitely increase greatly.

CrowdStrike IDP Exam Syllabus Topics:

Topic	Details
Topic 1	• GraphQL API: Covers Identity API documentation, creating API keys, permission levels, pivoting from Threat Hunter to GraphQL, and building queries.
Topic 2	• Configuration and Connectors: Addresses domain controller monitoring, subnet management, risk settings, MFA and IDaaS connectors, authentication traffic inspection, and country-based lists.
Topic 3	• Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.
Topic 4	• Risk Management with Policy Rules: Covers creating and managing policy rules and groups, triggers, conditions, enabling • disabling rules, applying changes, and required Falcon roles.
Topic 5	• Zero Trust Architecture: Covers NIST SP 800-207 framework, Zero Trust principles, Falcon's implementation, differences from traditional security models, use cases, and Zero Trust Assessment score calculation.
Topic 6	• User Assessment: Examines user attributes, differences between users • endpoints • entities, risk baselining, risky account types, elevated privileges, watchlists, and honeytoken accounts.
Topic 7	• Identity Protection Tenets: Examines Falcon Identity Protection's architecture, domain traffic inspection, EDR complementation, human vulnerability protection, log-free detections, and identity-based attack mitigation.

Topic 8	• Threat Hunting and Investigation: Focuses on identity-based detections and incidents, investigation pivots, incident trees, detection evolution, filtering, managing exclusions and exceptions, and risk types.
Topic 9	• Falcon Identity Protection Fundamentals: Introduces the four menu categories (monitor, enforce, explore, configure), subscription differences between ITD and ITP, user roles, permissions, and threat mitigation capabilities.

IDP Exam Guide & IDP Customized Lab Simulation

You must want to receive our IDP practice questions at the first time after payment. Don’t worry. As long as you finish your payment, our online workers will handle your orders of the IDP study materials quickly. The whole payment process lasts a few seconds. And if you haven't received our IDP Exam Braindumps in time or there are some trouble in opening or downloading the file, you can contact us right away, and our technicals will help you solve it in the first time.

CrowdStrike Certified Identity Specialist(CCIS) Exam Sample Questions (Q24-Q29):

NEW QUESTION # 24
What is the recommended action for the"Guest Account Enabled"risk?

- A. Disable the endpoint in Active Directory
- B. Apply a policy rule with an "Access" trigger and "Block" action on the Guest account
- C. Disable Guest accounts on all endpoints
- D. Add related endpoints to a watchlist

Answer: C

Explanation:
In Falcon Identity Protection, the"Guest Account Enabled"risk highlights the presence of local or domain guest accounts that remain active across endpoints. Guest accounts are inherently high-risk because they typically lack strong authentication controls, are rarely monitored, and are frequently abused by attackers for lateral movement and persistence.
The CCIS curriculum explicitly recommendsdisabling Guest accounts on all endpointsas the primary remediation action. This is because guest accounts often bypass standard identity governance processes and violate the principles ofleast privilegeandZero Trust, both of which are foundational to Falcon Identity Protection's security model. Disabling these accounts removes an unnecessary and dangerous authentication path from the environment.
Other options are incorrect because:
* Adding endpoints to a watchlist does not remediate the risk.
* Blocking access via a policy rule is less effective than eliminating the account entirely.
* Disabling endpoints in Active Directory does not directly address the guest account exposure.
Falcon Identity Protection prioritizeselimination of weak identity configurations, and disabling guest accounts is a direct, effective action that immediately lowers identity risk scores and reduces attack surface.
Therefore,Option Cis the correct and verified answer.

NEW QUESTION # 25
Which of the following statements isNOTtrue as it relates to Identity Events, Detections, and Incidents?

- A. Not all events are security events that become elements of detections
- B. An event can become an element of a detection that preceded it in time
- C. A detection can become an element of an incident that preceded it in time
- D. Events related to an incident that occur after the incident is marked In Progress will create a new incident

Answer: D

Explanation:

Falcon Identity Protection follows acorrelation and enrichment modelwhere events, detections, and incidents are dynamically linked over time. According to the CCIS curriculum,events that occur after an incident is marked In Progress do not automatically create a new incident. Instead, related events and detections are typicallyadded to the existing incident, provided they fall within the incident's correlation and suppression window.
This behavior allows Falcon to present asingle evolving incident, showing the full progression of an identity attack rather than fragmenting activity into multiple incidents. Therefore, statementA is not true.
The other statements are correct:
* Detections can be retroactively associated with incidents that occurred earlier if correlation logic determines relevance.
* Events can be linked to detections even if the detection is created after the event occurred.
* Not all events are security-relevant; many remain informational and never become detections.
This adaptive correlation model is a core concept in CCIS training and supports efficient investigation and incident lifecycle management. Hence,Option Ais the correct answer.

NEW QUESTION # 26
Where in the Identity Protection module can one view the monitoring status of domain controllers?

- A. System Notifications
- B. Domains
- C. Connectors
- D. Settings

Answer: B

Explanation:
In Falcon Identity Protection, theDomainspage is where administrators can view themonitoring and health status of domain controllers. The CCIS curriculum explains that this page provides visibility into which domain controllers are actively reporting authentication traffic, their inspection status, and whether Authentication Traffic Inspection (ATI) is enabled.
This view is essential for validating coverage and ensuring that Falcon Identity Protection has sufficient visibility into domain authentication activity. Administrators can quickly identify gaps, such as domain controllers that are not reporting or are misconfigured, and take corrective action.
The other options serve different purposes:
* Settingsmanage general configuration.
* System Notificationsdisplay alerts and messages.
* Connectorsmanage integrations such as MFA and IDaaS.
Because domain controller visibility and monitoring health are managed at the domain level,Option C (Domains)is the correct and verified answer.

NEW QUESTION # 27
When creating an API key, which scope should be selected to retrieve Identity Protection detection and incident information?

- A. Identity Protection Incidents
- B. Identity Protection Assessment
- C. Identity Protection Data
- D. Identity Protection Detections

Answer: D

Explanation:
To retrieve identity-based detections and incident-related data using the CrowdStrike APIs, the API key must include the correctpermission scope. According to the CCIS curriculum, theIdentity Protection Detections scope is required to access identity-based detection and incident information through GraphQL.
This scope allows API queries to retrieve:
* Identity-based detections
* Associated incident metadata
* Detection attributes such as severity, status, and related entities
Incident data in Falcon Identity Protection isderived from detections, making the Detections scope the authoritative permission set for this information. Without this scope, GraphQL queries related to identity detections and incidents will fail authorization.
The other scopes are either too narrow or unrelated to detection retrieval. Therefore,Option Ais the correct and verified answer.

NEW QUESTION # 28

Considering the following example, what MITRE ATT&CK tactic would you use to complete the workflow?

- A. Lateral Movement
- B. Credential Access
- C. Privilege Escalation
- D. Initial Access

Answer: A

Explanation:
The provided Falcon Fusion SOAR workflow example shows a trigger based on anIdentity Detection, followed by conditions and actions that search for recently logged-in users and related entities across endpoints. According to the CCIS curriculum, this type of workflow aligns with theLateral Movementtactic in the MITRE ATT&CK framework.
Lateral Movement involves an attacker moving from one system or account to another after initial access has been achieved. The workflow's logic-correlating identity detections with additional users and endpoints- supports identifying and responding to movement across the environment using compromised or abused credentials.
The other tactics do not best fit this scenario:
* Initial Access occurs earlier in the attack chain.
* Credential Access focuses on obtaining credentials.
* Privilege Escalation centers on increasing access rights.
Because the workflow is designed to detect and respond tomovement between systems and identities, Option C (Lateral Movement)is the correct and verified answer.

NEW QUESTION # 29
.....

Comfortable life will demoralize and paralyze you one day. So you must involve yourself in meaningful experience to motivate yourself. For example, our IDP study materials perhaps can become your new attempt. In fact, learning our IDP learning quiz is a good way to inspire your spirits. Not only that you can pass the exam and gain the according IDP certification but also you can learn a lot of knowledge and skills on the subjest.

enter □ IDP □ and obtain a free download □IDP Valid Study Materials

- 100% Pass Quiz 2026 IDP: CrowdStrike Certified Identity Specialist(CCIS) Exam – High Pass-Rate Latest Dumps Sheet □ □ Copy URL ▸ www.prepawaypdf.com ◂ open and search for □ IDP □ to download for free □IDP Download Demo
- 2026 Realistic IDP Latest Dumps Sheet - CrowdStrike Certified Identity Specialist(CCIS) Exam Exam Guide Free PDF □ （ www.pdfvce.com ） is best website to obtain ▸ IDP ◂ for free download □IDP Braindumps Torrent
- IDP Reliable Exam Pdf □ IDP Latest Dumps Files □ IDP Valid Study Materials □ Simply search for （ IDP ） for free download on { www.testkingpass.com } □Exam IDP Quizzes
- Realistic IDP Latest Dumps Sheet Help You to Get Acquainted with Real IDP Exam Simulation □ The page for free download of ➽ IDP □ on ➥ www.pdfvce.com □ will open immediately □Valid IDP Exam Discount
- IDP Valid Study Materials □ Exam IDP Quizzes □ IDP Exam Consultant □ Easily obtain □ IDP □ for free download through ▹ www.troytecdumps.com ◃ □IDP Reliable Test Questions
- Get Trustable IDP Latest Dumps Sheet and Best Accurate IDP Exam Guide □ Open ✔ www.pdfvce.com □✔□ and search for □ IDP □ to download exam materials for free □Reliable IDP Test Blueprint
- Exam IDP Quizzes □ IDP Reliable Exam Pdf □ IDP Braindumps Torrent ❣ Open ▹ www.vce4dumps.com ◃ enter [IDP] and obtain a free download □Trustworthy IDP Practice
- tiffanyhkjb275375.blogofchange.com, donnawauc265988.wikigiogio.com, hyperbookmarks.com, alyssahkhg811476.blogrenanda.com, pr8bookmarks.com, sairagtef893484.life3dblog.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, jobs.electronicsweekly.com, stevexnpv676204.plpwiki.com, e-bookmarks.com, Disposable vapes

DOWNLOAD the newest Fast2test IDP PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1DIfJBTKrmStvbVAsE1HcdJUsTFC8879f