IDP유효한덤프자료최신버전덤프공부자료

요즘같이 시간인즉 금이라는 시대에 시간도 절약하고 빠른 시일 내에 학습할 수 있는 DumpTOP의 덤프를 추천합니다. 귀중한 시간절약은 물론이고 한번에CrowdStrike IDP인증시험을 패스함으로 여러분의 발전공간을 넓혀줍니다.

CrowdStrike IDP 시험요강:

주제	소개
주제 1	• 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.
주제 2	• Falcon Fusion SOAR for Identity Protection: Explores SOAR workflow automation including triggers, conditions, actions, creating custom • templated • scheduled workflows, branching logic, and loops.
주제 3	• Risk Management with Policy Rules: Covers creating and managing policy rules and groups, triggers, conditions, enabling • disabling rules, applying changes, and required Falcon roles.

주제 4	• Domain Security Assessment: Focuses on domain risk scores, trends, matrices, severity • likelihood • consequence factors, risk prioritization, score reduction, and configuring security goals and scopes.
주제 5	• 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.
주제 6	• Multifactor Authentication (MFA) and Identity-as-a-service (IDaaS) Configuration Basics: Focuses on accessing and configuring MFA and IDaaS connectors, configuration fields, and enabling third-party MFA integration.
주제 7	• Risk Assessment: Covers entity risk categorization, risk and event analysis dashboards, filtering, user risk reduction, custom insights versus reports, and export scheduling.
주제 8	• Configuration and Connectors: Addresses domain controller monitoring, subnet management, risk settings, MFA and IDaaS connectors, authentication traffic inspection, and country-based lists.
주제 9	• 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.
주제 10	• GraphQL API: Covers Identity API documentation, creating API keys, permission levels, pivoting from Threat Hunter to GraphQL, and building queries.

최신 CrowdStrike CCIS IDP 무료샘플문제 (Q23-Q28):

질문 # 23
Which option can be selected from the Threat Hunter menu to open the current Threat Hunter query in a new window as Graph API format?

- A. Open Query in API Builder
- B. Save as Custom Query
- C. Save as Custom Report
- D. Export to API Builder

정답：A

설명：
Falcon Threat Hunter provides a direct integration with theAPI Builderto support advanced investigation workflows and automation. According to the CCIS curriculum, analysts can take an existing Threat Hunter query and convert it into aGraphQL-compatible formatby selectingOpen Query in API Builderfrom the Threat Hunter menu.
This option opens the current query in a new window within API Builder, automatically translating the query structure into GraphQL syntax where applicable. This enables security teams to reuse validated hunting logic for automation, reporting, or external integrations without rewriting queries from scratch.
The other menu options serve different purposes:
* Export to API Builderis not a valid menu action.
* Save as Custom Querystores the query for reuse inside Threat Hunter.
* Save as Custom Reportgenerates a reporting artifact, not an API query.

BecauseOpen Query in API Builderis the only option that opens the query in GraphQL format in a new window,Option Dis the correct and verified answer.

질문 # 24
Considering the following example, what MITRE ATT&CK tactic would you use to complete the workflow?

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

정답：C

설명:
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.

질문 # 25
How many days will an identity-based incident be suppressed if new events related to the same incident occur?

- A. 7 days
- B. 30 days
- C. 5 days
- D. 14 days

정답：C

설명:
Falcon Identity Protection usesincident suppression windowsto prevent alert fatigue while still maintaining accurate incident tracking. According to the CCIS documentation, whennew events related to an existing identity-based incident occur, the incident issuppressed for 5 days.
This suppression means that Falcon does not generate a new incident for the same activity during this window. Instead, additional detections areadded to the existing incident, allowing analysts to view the full progression of the threat in a single investigative context.
The 5-day suppression window ensures that ongoing identity attacks-such as repeated authentication abuse or lateral movement-are consolidated rather than fragmented across multiple incidents. This improves investigation efficiency and aligns with Falcon's incident lifecycle management approach.
Because the suppression period is fixed at5 days,Option Dis the correct and verified answer.

질문 # 26
Under which CrowdStrike documentation category could you find Identity Protection API information?

- A. Falcon Management
- B. CrowdStrike Store
- C. CrowdStrike APIs
- D. Tools and Reference

정답：C

설명：
Identity Protection API documentation is part of CrowdStrike's centralized API documentation structure.
According to the CCIS curriculum,Identity Protection API information is located under the
"CrowdStrike APIs" documentation category.
This category includes:
* API authentication and scopes
* Identity Protection GraphQL schemas
* Query examples for detections, incidents, users, and risk
* Usage guidance and limitations
CrowdStrike consolidates all API-related documentation in one location to ensure consistent access and maintenance across Falcon modules. Identity Protection APIs are not documented under Falcon Management, Store, or general reference sections.
Because all product APIs-including Identity Protection-are documented underCrowdStrike APIs,Option Dis the correct and verified answer.

질문 # 27
What trigger will cause a Falcon Fusion Workflow to activate from Falcon Identity Protection?

- A. Alert > Identity detection
- B. New endpoint detection
- C. New incident
- D. Spotlight user action > Host

정답：A

설명：
Falcon Fusion workflows integrate directly with Falcon Identity Protection throughidentity-based triggers, allowing automated responses to identity threats. The correct trigger that activates a Falcon Fusion workflow from Identity Protection isAlert > Identity detection.
Identity detections are generated when Falcon observes suspicious or malicious identity behavior, such as credential abuse, abnormal authentication patterns, lateral movement attempts, or policy violations related to identity risk. These detections are distinct from endpoint-only detections or incidents and are specifically designed to representidentity-based attack activity.
WhileNew incidentandNew endpoint detectionare valid Falcon Fusion triggers in other Falcon modules, they are not the primary triggers for identity-focused automation. Similarly,Spotlight user action > Host relates to vulnerability management workflows rather than identity analytics.
The CCIS curriculum emphasizes that Falcon Fusion enablesautomated identity response, such as notifying security teams, disabling accounts, enforcing MFA, or triggering SOAR actions, based onidentity detections.
Therefore, workflows tied toAlert > Identity detectionallow organizations to respond quickly and consistently to identity threats, makingOption Cthe correct answer.

질문 # 28
.....

- 시험패스 가능한 IDP유효한 덤프자료 공부문제 □ ➤ www.passtip.net □웹사이트에서➤ IDP □를 열고 검색하여 무료 다운로드IDP덤프공부문제
- 적중율 높은 IDP유효한 덤프자료 인증덤프자료 □ ➡ www.itdumpskr.com □□□은▷ IDP ◁무료 다운로드를 받을 수 있는 최고의 사이트입니다IDP최신 시험 예상문제모음
- IDP최신버전덤프 □ IDP최신버전덤프 □ IDP완벽한 시험공부자료 □ 검색만 하면□ www.dumptop.com □에서⇛ IDP ⇚무료 다운로드IDP시험대비 덤프공부문제
- 최신버전 IDP유효한 덤프자료 시험공부자료 □ □ www.itdumpskr.com □에서 검색만 하면➽ IDP □를 무료로 다운로드할 수 있습니다IDP적중율 높은 시험덤프공부
- 높은 통과율 IDP유효한 덤프자료 시험패스의 강력한 무기 □ 무료로 다운로드하려면⇛ www.exampassdump.com⇚로 이동하여（ IDP ）를 검색하십시오IDP최신버전 공부문제
- IDP유효한 덤프자료 덤프는 CrowdStrike Certified Identity Specialist(CCIS) Exam 시험문제의 모든 범위가 포함 □ □《 www.itdumpskr.com 》에서 검색만 하면➽ IDP □를 무료로 다운로드할 수 있습니다IDP인증시험 인기 덤프자료
- IDP자격증공부 □ IDP높은 통과율 공부자료 □ IDP높은 통과율 공부자료 □ ➠ www.pass4test.net □웹사이트에서[IDP]를 열고 검색하여 무료 다운로드IDP인기자격증 시험 덤프자료
- bbs.t-firefly.com, myportal.utt.edu.tt, www.stes.tyc.edu.tw, creativespacemastery.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, www.stes.tyc.edu.tw, 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, Disposable vapes