

CrowdStrike CCIS

CrowdStrike Identity Specialist

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/ccis>

Latest Version: 6.0

Question: 1

A Fusion SOAR condition block evaluates a defined parameter and routes the workflow only if the condition evaluates to ____.

- A. high
- B. true
- C. integer
- D. null

Answer: B

Question: 2

In Falcon Identity Protection, a _____ account is one created to serve as a trap, triggering alerts if it is accessed or queried.

- A. stale
- B. federated
- C. honeypot
- D. external

Answer: C

Question: 3

How does Falcon Identity Protection differentiate between “Identity Threat Detection” (ITD) and “Identity Threat Protection” (ITP)?

- A. ITD is focused on email filtering, while ITP blocks USB access
- B. ITD provides detection only, whereas ITP includes active policy enforcement
- C. ITD manages MFA settings, ITP handles only cloud connectors
- D. ITD is limited to cloud identities, ITP handles on-premises accounts

Answer: B

Question: 4

How are honeytoken accounts typically used in Falcon Identity Protection?

- A. To store backup configurations
- B. To reset user passwords automatically
- C. To sync account settings across domains
- D. To serve as decoys for detecting identity-based attacks

Answer: D

Question: 5

What advantage does GraphQL offer over traditional REST APIs for identity queries in Falcon?

- A. It provides encrypted DNS tunneling
- B. It allows clients to retrieve only the exact data fields required
- C. It requires fewer user permissions
- D. It automatically corrects syntax errors

Answer: B

Question: 6

What two insights can be gained from adjusting the “Goals” in the Domain Security overview?
(Choose two)

- A. Customization of risk prioritization for business context
- B. Alert threshold tuning for antivirus
- C. Visual benchmarks against security maturity objectives
- D. Determining daily login hours per user

Answer: A,C

Question: 7

What is a key architectural advantage of Falcon Identity Protection over traditional endpoint detection and response (EDR) solutions?

- A. It only monitors Windows endpoints in isolation
- B. It relies entirely on signature-based detection
- C. It requires no configuration for policy enforcement
- D. It observes domain controller traffic for identity signals

Answer: D

Question: 8

Which two authentication control methods are supported for third-party integrations in Falcon Identity Protection?

(Choose two)

- A. Conditional risk-based MFA
- B. Static port blocking
- C. RADIUS-based enforcement
- D. Biometric hardware filtering

Answer: A,C

Question: 9

Which permission must be enabled on an API key to query privileged user risk data in Falcon Identity Protection?

- A. "Detection Write"
- B. "Identity Protection Read"
- C. "Sensor Control"
- D. "Report Generation Only"

Answer: B

Question: 10

Where can you access the configuration settings for MFA and IDaaS connectors in Falcon Identity Protection?

- A. Under the "Monitor" tab
- B. In the "Explore" menu
- C. Within the "Configure" section of the platform
- D. Through Falcon's external API only

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>