Vendor: CrowdStrike

Exam Code: CCIS

Exam Name: CrowdStrike Certified Identity Specialist

Version: DEMO

QUESTION 1
On the Risk Analysis dashboard, _____ displays a bar graph showing the distribution of risk scores by OU or department with each bar color-coded to show the count of users by risk score.

A. Membership by Impact
B. Membership by OU
C. Membership by Severity
D. Outliers

Answer: B
Explanation:
Membership by OU presents a bar graph that shows how risk scores are distributed across organizational units or departments, with color-coding to represent the number of users at each risk level.

QUESTION 2
When configuring on-premises Azure (Entra) MFA using the NPS extension, what ports are required for Authentication by default?

A. 53 & 68
B. 80 & 443
C. 53 & 66
D. 1812 & 1813

Answer: D
Explanation:
On-premises Azure (Entra) MFA using the NPS extension relies on RADIUS for authentication, which by default uses UDP ports 1812 for authentication and 1813 for accounting.

QUESTION 3
In order to lower a domain risk score, you will need to:

A. Enable the risk in the Risk Management section under the Risk Configuration page
B. Resolve the detection by changing its status from New to Close: Resolve
C. Delete the domain from Falcon Identity Protection
D. Perform the Recommended Actions for each risk on the related entities

Answer: D
Explanation:
Lowering the domain risk score requires addressing and remediating the underlying issues contributing to risk by performing the recommended actions on the affected entities, which reduces or eliminates the associated risks.

QUESTION 4
What Zero Trust principal is associated with always verifying access all the time, for all resources?

A. Limiting the blast radius
B. Continuous verification

C. Deploying rapid and scalable policy models
D. Automating context collection and response

Answer: B
Explanation:
Continuous verification is the Zero Trust principle that requires access to be constantly evaluated and reverified for every request and resource, rather than relying on implicit trust.

QUESTION 5
Which role can create a Falcon Fusion workflow for Identity Detections?

A. Endpoint Manager
B. Workflow Author
C. Device Control Manager
D. Falcon Analyst

Answer: B
Explanation:
Creating Falcon Fusion workflows requires the Workflow Author role, which grants permission to build, edit, and manage automated workflows, including those triggered by Identity Protection detections.

QUESTION 6
Which section of the Falcon Identity Protection module do you use to manage your Policy Rule groups?

A. Reports
B. System Notifications
C. Configure
D. Enforce

Answer: D
Explanation:
Policy Rule groups are managed within the Enforce section, which is where Identity Protection policies, rules, and enforcement logic are created, organized, and maintained.

QUESTION 7
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 Report
C. Export to API Builder
D. Save as Custom Query

Answer: A
Explanation:
This option opens the active Threat Hunter query in a new window formatted for the Graph API, allowing it to be reviewed, tested, or reused directly within the API Builder.

QUESTION 8
The configuration of the Azure AD (Entra ID) Identity-as-a-Service connector requires what three pieces of information?

A. Tenant Domain, Client Secret User Identifier
B. Tenant Domain, Application ID, Scope
C. Tenant Domain, Application ID, Application Secret
D. Tenant Domain, Token Configuration File

Answer: C
Explanation:
Configuring the Azure AD (Entra ID) Identity-as-a-Service connector requires the tenant domain to identify the directory, the application ID to identify the registered app, and the application secret to authenticate the connector securely.

QUESTION 9
Where can the entities related to a specific risk be inspected?

A. Monitor > Domain Security Overview > Click on a Risk > Show Related Entities
B. Monitor > Users > Click on a User > Similar Entities
C. Monitor > Risk Analysis > Membership By Seventy > Click on a Risk
D. Configure > Risk Configuration > Search the relevant risk > Show Related Entities

Answer: A
Explanation:
Entities associated with a specific risk are accessed from the Domain Security Overview by selecting the risk and using the option to show related entities, which provides visibility into the users, computers, or other objects contributing to that risk.

QUESTION 10
Detection-based risks trigger on internal logic to identify suspicious network traffic. Analysis-based risks trigger on account _____ or new vulnerabilities.

A. misconfigurations
B. group
C. locations
D. priorities

Answer: A
Explanation:
Analysis-based risks are generated by evaluating account misconfigurations or the presence of newly identified vulnerabilities, rather than real-time detection of suspicious activity.

QUESTION 11
Which of the following API permissions are required, at a minimum, in order to search identity timeline data?

A. Identity Protection Timeline: Write & Identity Protection GraphQL: Read
B. Identity Protection Timeline: Read & Identity Protection GraphQL: Read
C. Identity Protection Timeline: Write & Identity Protection GraphQL: Write

D. Identity Protection Timeline: Read & Identity Protection GraphQL: Write

Answer:
Explanation:
Searching identity timeline data requires read access to the timeline dataset and read access to query it through the GraphQL interface, so both Timeline read and GraphQL read permissions are required at a minimum.

QUESTION 12
Which of the following represents a legitimate use-case for disabling a detection-based risk?

A. Organization has a manual process for changing local administrator passwords for new endpoints, so they disabled detections for Duplicated Local Administrator
B. Organization uses a 3rd-party software for domain password management which does not leverage Active Directory Password Policies, so they disabled the detection-based risk for "Inadequate Password Policy"
C. User disabled detections for NTLMv2 Compatibility due to the presence of legacy operating systems in their environment
D. User disabled detections for GPO Exposed Password to prevent other Identity Protection administrators from seeing unintended information

Answer: B
Explanation:
Disabling a detection-based risk can be legitimate when an organization intentionally manages the related control through an alternative mechanism. In this case, a third-party domain password management solution that does not rely on Active Directory password policies makes the associated detection noisy or irrelevant, justifying its disablement.

QUESTION 13
Which of the following is NOT an event that is monitored for a Honeytoken account?

A. Email address was changed on a Honeytoken account
B. A Honeytoken account was created
C. Logon Activity from a Honeytoken account
D. Password reset on a Honeytoken account

Answer: B
Explanation:
Honeytoken monitoring focuses on post-creation activity that indicates potential misuse or attacker interaction, such as logons, password resets, or attribute changes. The creation of the Honeytoken account itself is not a monitored event for alerting purposes.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html