EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

What does the following Icon indicate about the user?



A. Never logged in

B. Stale

C. Not connected

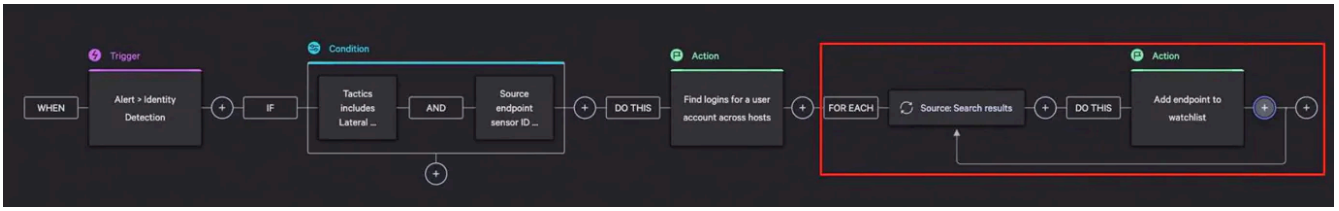
D. Disabled

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

What is happening in the outlined section within this Fusion Workflow?



A. Conditional Loop

B. Sequential Loop

C. Parallel Action

D. Parallel Loop

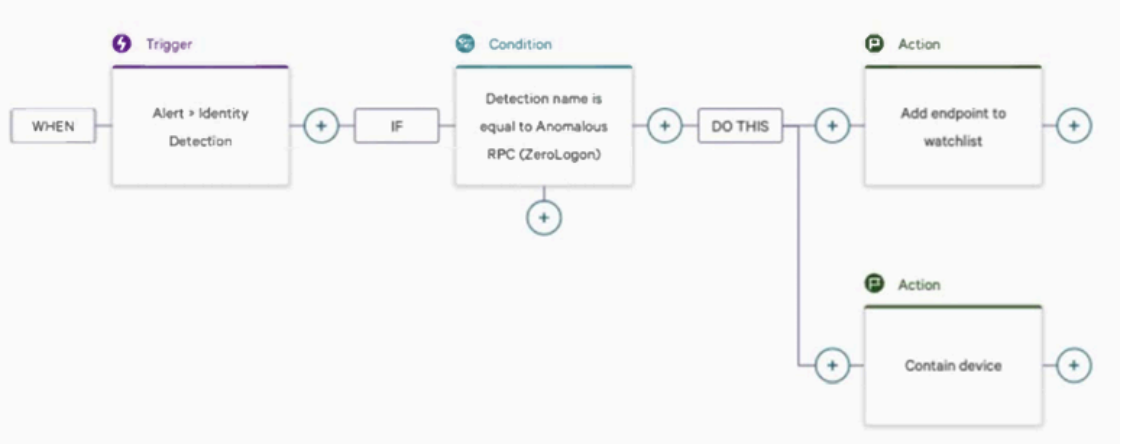
Suggested Answer: *A*

The workflow repeats actions for each search result in a conditional loop.

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Given the Falcon Fusion workflow in the figure above, which of the following correctly explains this workflow?



A. For Anomalous RPC detections of any kind, the source endpoint will be network contained

B. For Anomalous RPC detections of any kind, the source endpoint will be added to a watchlist and network contained

C. Any Identity Protection detections for Anomalous RPC (ZeroLogon) will result in the source endpoint being added to the watchlist and network contained

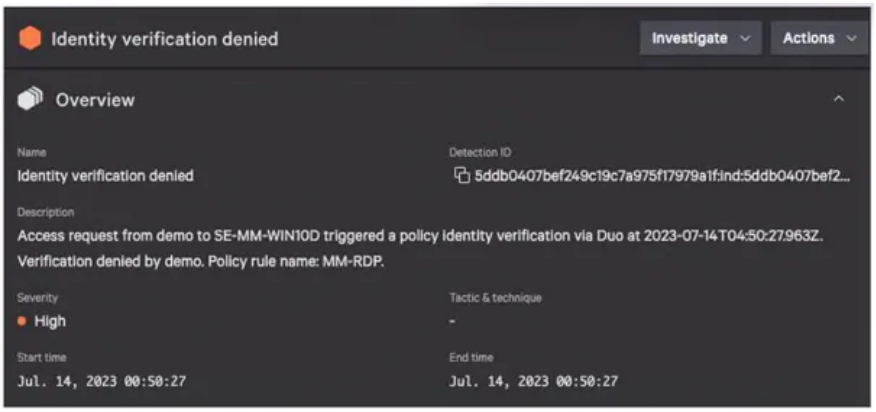
D. Any Identity Protection detections for Anomalous RPC (ZeroLogon) will result in the source user being added to the watchlist and restricted from future logons

Suggested Answer: *C*
Trigger and condition specify Identity Detection and Anomalous RPC (ZeroLogon); actions target endpoint.

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Using the provided example detection, which of the following statements is TRUE in relation to Falcon detections and the MITRE ATT&CK Framework TTPs?



A. CrowdStrike is able to identify TTPs that don't map directory to the MITRE Framework

B. CrowdStrike is able to make updates to MITRE ATT&CK Framework TTPs with detection artifacts

C. All Falcon detections have at least one TTP from the MITRE ATT&CK Framework

D. CrowdStrike is able to combine TTPs from the MITRE ATT&CK Framework, the Cyber Kill Chain, as well as internal Falcon intelligence

Suggested Answer: *D*
The example shows no mapped tactic or technique, consistent with combined frameworks and internal intelligence.

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

The meaning of the icons shown are watched, inactive, privileged and _____?



A. Unlocked

B. Programmatic Account

C. Compromised Password

D. Stale

Suggested Answer: *C*

The four icons represent watched, inactive, privileged, and compromised password.

Community vote distribution

C (100%)

fafd232_ Most Recent 4 months, 1 week ago

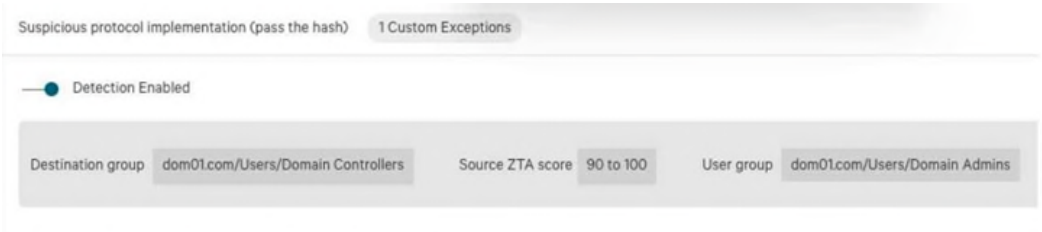
Selected Answer: C

This is the right answer, but the order of the images are wrong for some reason. The unlocked icon the compromised password icon

upvoted 1 times

Question #6 *Topic 1*

Given the detection exclusion shown above, which answer CORRECTLY describes how this would work regarding the “Suspicious protocol implementation (pass the hash)” detection?



A. It WILL trigger when Domain Admins attempt this activity against domain controllers, as long as the source host has a Zero Trust Assessment score of 90+

B. It will NOT trigger when Domain Admins attempt this activity against domain controllers as long as the source host has a Zero Trust Assessment score of 90+

C. It will NOT trigger when Domain Admins attempt this activity against domain controllers, as long as the domain controllers have a Zero Trust Assessment score of 90+

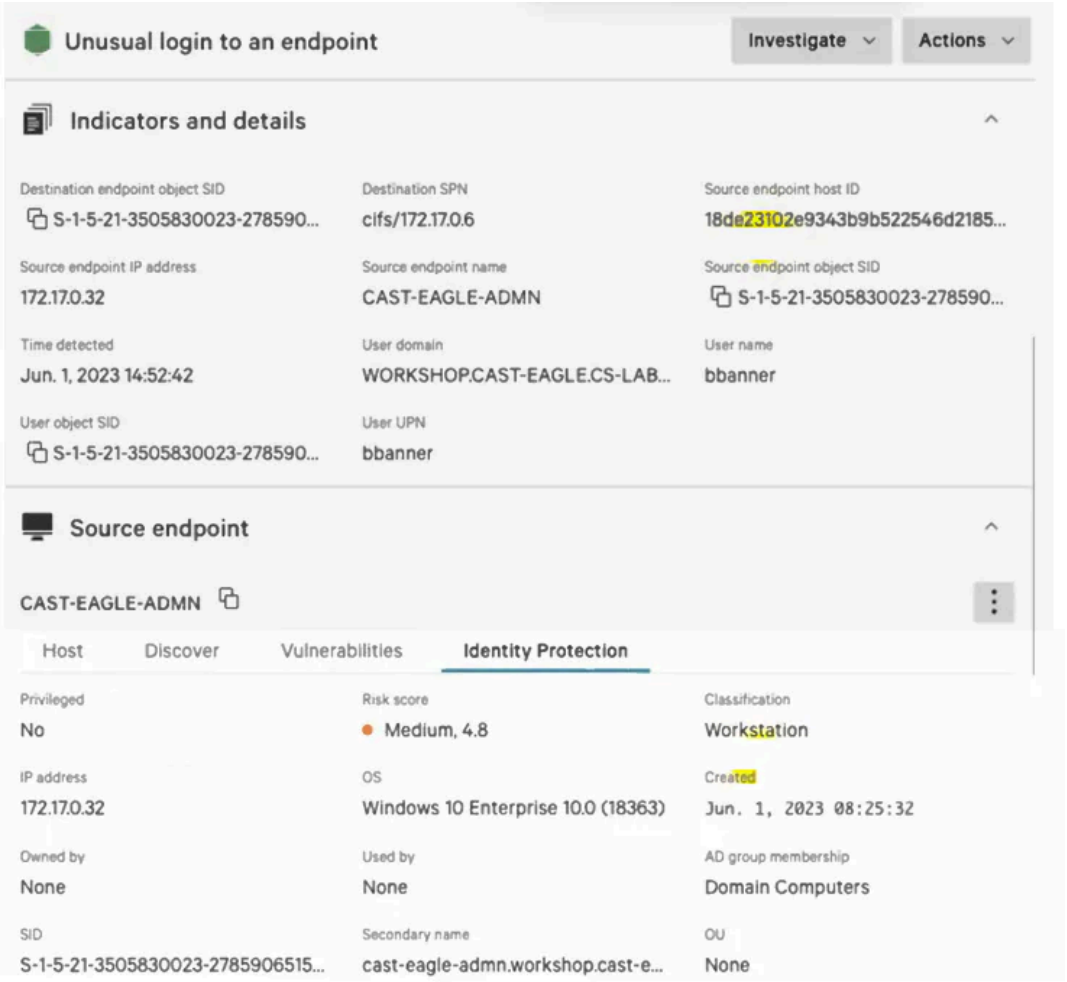
D. It will NOT trigger when any privileged user attempts this activity against domain controllers, as long as the source host has a Zero Trust Assessment score of 90+

Suggested Answer: *B*
Exclusion applies to Domain Admins targeting domain controllers when source ZTA score is 90–100.

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

Given information from the Falcon Identity Protection detection shown in the figure above, which of the following responses is TRUE?



A. User bbanner typically uses computer CAST-EAGLE-ADMN, but is seen logging into another computer

B. User bbanner does not typically use CAST-EAGLE-ADMN, but is seen logging into this computer

C. User bbanner logged into privileged computer CAST-EAGLE-ADMN, which should not be allowed

D. User CAST-EAGLE-ADMN logged into computer bbanner, which is unusual

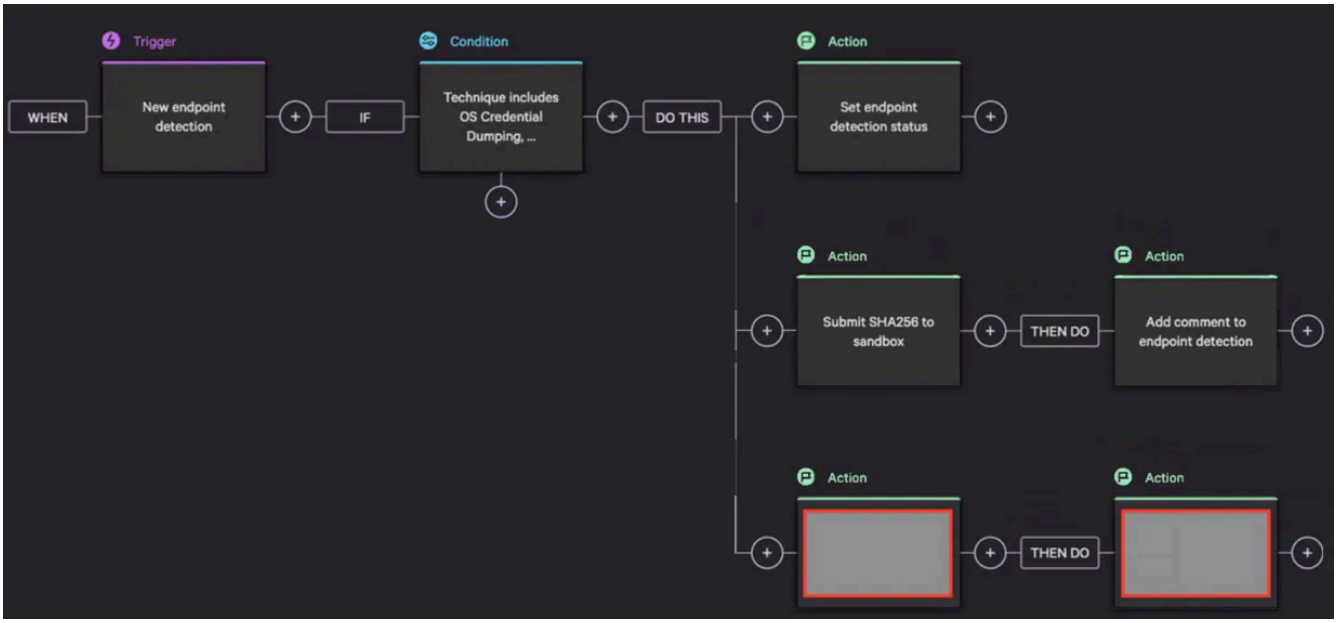
Suggested Answer: *B*

The detection describes an unusual login to CAST-EAGLE-ADMN by user bbanner.

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

What needs to be added to the following Fusion Workflow in order to monitor entities related to these particular endpoint detections?



A. Add user and endpoint to marked list

B. Network contain user and endpoint

C. Add user and endpoint to watchlist

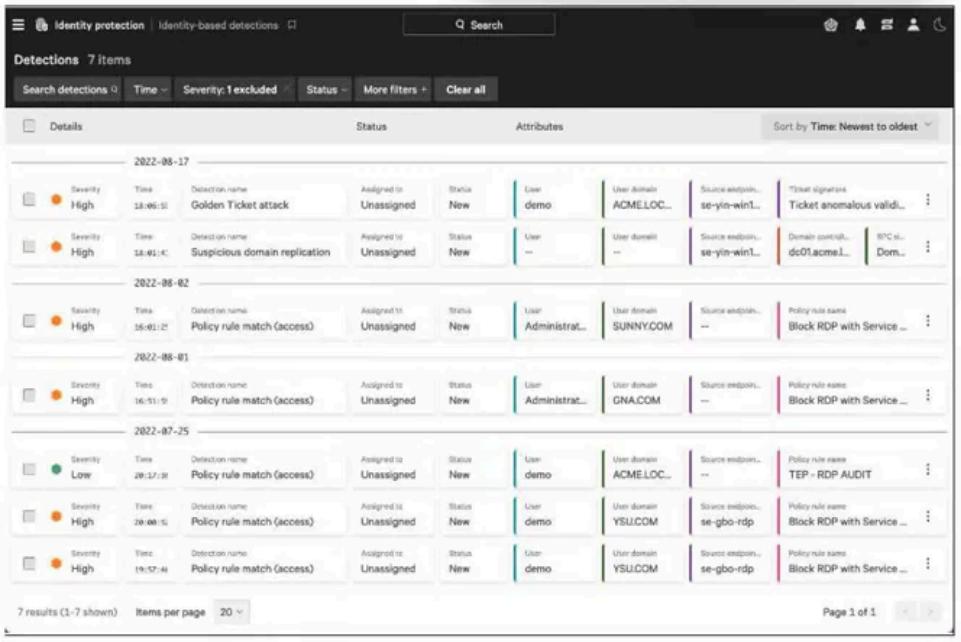
D. Get device details and add endpoint to host group

Suggested Answer: *C*
The workflow needs additional actions to watchlist both related entities.

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Which of the following are not included within the three-dot menu on Identity-based Detections?



A. Edit status

B. Add comment

C. Add exclusion

D. Add to Watchlist

Suggested Answer: *C*

The three-dot menu includes common detection actions; Add exclusion is not listed there.

Community vote distribution

D (100%)

3de0689 Most Recent 4 months, 2 weeks ago

Selected Answer: D

Add To Watchlist is NOT an option, but Add Exclusion is. Just checked

upvoted 1 times

Question #10 *Topic 1*

The Risk Matrix shows the risks rated by two parameters, what are they?



A. Likelihood and Consequences

B. Rarity and Visibility

C. Exposure and Severity

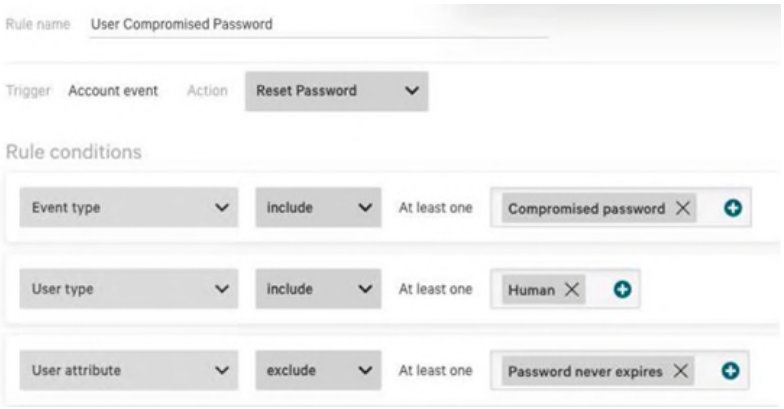
D. Complexity and Quantity

Suggested Answer: *A*
The risk matrix axes are likelihood and consequence.

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Which answer properly describes the impact of the policy shown above?



A. For each new user event of a compromised password: if the user account is Human and does NOT have a never expiring password, this account will be set to change password at next login

B. For each user with a compromised password: if the user account is Human and HAS a never expiring password, this account will be set to change password at next login

C. For each new user event of a compromised password: if the user account is Human and HAS a never expiring password, this account will be set to change password at next login

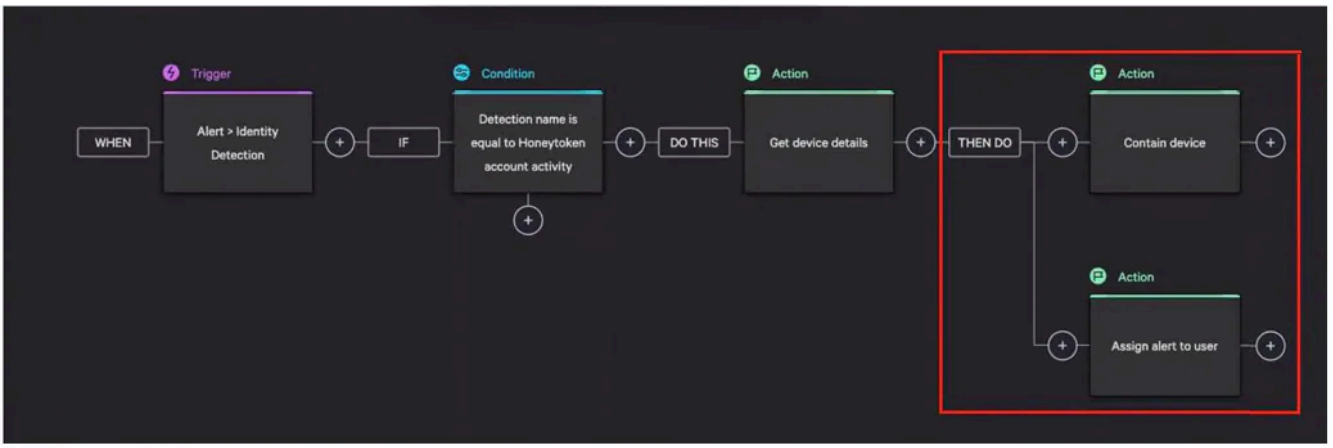
D. For each user with a compromised password: if the user account is Human and does NOT have a never expiring password, this account will be set to change password at next login

Suggested Answer: *C*
The rule matches compromised-password events for Human users with password never expires excluded.

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

What is the outlined section of this Fusion Workflow called?



A. Parallel Loop

B. Sequential Actions

C. Parallel Condition

D. Parallel Actions

Suggested Answer: *D*

The outlined section contains multiple actions branching in parallel.

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

What is the best way to create a Honeytoken account?

A. Creating a Honeytoken user account, using the name of a fake employee in the Finance department, with the account inside the IT Department OU

B. Creating a low-interaction Honeytoken computer account that is configured to mimic an AD FS server

C. Creating a Honeytoken user account named MSSQL_Admin, with a fake password in the Description attribute

D. Creating a high-interaction Honeytoken computer account that is configured to mimic a MySQL server

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

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

A. Tools and Reference

B. Falcon Management

C. CrowdStrike APIs

D. CrowdStrike Store

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

In the Domain security overview, there are 4 different goals that can be addressed, each characterized by the specific risks. Which of the following is NOT one of those goals?

A. Reduce Attack Surface

B. Pen Testing

C. AD Hygiene

D. Privileged Groups Management

Suggested Answer: *B*

fafd232_ Most Recent 4 months, 1 week ago

Selected Answer: D

Its D.

This may be confusing. But if you double check, the 'Privileged Groups Management' goal doesn't exist, but 'Privileged User Management' does!

upvoted 1 times

Drikhj 7 months, 2 weeks ago

Selected Answer: D

Creo que la clave de respuestas puede ser incorrecta. En la «Descripción general de la seguridad de dominios» actual, los cuatro objetivos que se muestran son: «Higiene de AD», «Pruebas de penetración», «Gestión de usuarios con privilegios» y «Reducción de la superficie de ataque». Dado que las «Pruebas de penetración» figuran explícitamente como un objetivo válido, la opción B no debería ser la respuesta correcta. La opción que NO es uno de los objetivos enumerados es la D, «Gestión de grupos con privilegios», ya que el producto utiliza «Gestión de usuarios con privilegios».

upvoted 2 times

Question #16 *Topic 1*

Which of the following is the best use case for Honeytoken accounts?

A. Luring attackers that may be in the organization

B. Alerting on unauthorized access to Domain Controllers

C. Notifying the use of a 'Break Glass' account

D. Collecting passwords from failed logon attempts

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

What basic configuration fields are typically required for cloud Multi-Factor Authentication connectors?

A. Service account user name and password

B. Connector application identifier & secret keys

C. Domain controller host name and IP address

D. Domain Administrator user name and password

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Due to a ransomware incident, the previous administrator disabled the Identity Protection detection for Suspicious lateral movement. Which answer describes the potential risk of this configuration?

A. This will prevent legitimate lateral movement from occurring

B. Any potentially malicious lateral movement activity will not have detections within Identity Protection

C. This configuration is acceptable, as long as the source user is added to the watch list

D. This configuration is acceptable, as long as an Identity-based policy is configured to prevent all ransomware lateral movement

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

The Monitor section of Identity Protection can be used to:

A. Configure domains, appliances, subnets, connectors, risk configuration, and settings

B. Modify predefined reports and review a list of saved & custom reports

C. Search through raw events, detect and identify security events, or further investigate security events reported by the system

D. View the overall AD hygiene, risk level and the priorities facing the domain from the security posture perspective

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Which of the following demonstrates a detection is enabled?

A. The toggle next to the Detection Enabled is marked in gray

B. The toggle next to the Detection Enabled is marked in green

C. The detection has a Disabled tag next to it

D. The detection has an Enabled tag next to it

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

What is the recommended action for the "Guest Account Enabled" risk?

A. Disable the endpoint in Active Directory

B. Disable Guest accounts on all endpoints

C. Apply a policy rule with an "Access" trigger and "Block" action on the Guest account

D. Add related endpoints to a watchlist

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Subnets can be setup as one of the following types: Internal, _____, WIFI, or NAT.

A. LAN

B. VPN

C. External

D. Firewall

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

How does CrowdStrike Falcon Identity Protection help customers identify different types of accounts in their domain?

A. Analyzes authentication traffic and automatically classifies programmatic and human accounts

B. Implements advanced encryption algorithms for account metadata

C. Assigns a human authorizer to each programmatic account for approval

D. Conducts regular vulnerability assessments on programmatic accounts

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Which of the following API permissions are required in order to add/remove an entity to a watchlist?

A. Identity Protection Entities: Write

B. Identity Protection GraphQL: Write

C. Identity Protection Assessment Write & Identity Protection GraphQL: Write

D. Identity Protection Entities Write & Identity Protection GraphQL: Write

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Which of the following best describes how Policy Group and Policy Rule precedence works?

A. There is no precedence with Policy Groups or Policy Rules, they enact policy if the conditions match

B. Policy Groups only group Policy Rules together. Precedence is dictated by the Rules

C. Policy Groups are evaluated in the order in which the groups appear on the page. The Policy Rules within those groups are evaluated in the order in which they appear in the group

D. Policy Groups are evaluated in the order in which the groups appear on the page; however, Policy Rules within those groups have no precedence

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

What factors contribute to the domain Risk Score on the Domain Security Overview Page?

A. The Average Assessment Score under the Zero Trust Assessment page

B. The number of Privileged Users

C. The number of domains protected by Falcon Identity Protection

D. The issues that are listed below the Risk Score

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Which of the following is TRUE regarding the risk stale user accounts pose to an organization?

A. Stale accounts are susceptible to social engineering attacks, such as phishing

B. Stale accounts do not pose a threat

C. Stale accounts are typically not monitored for unusual activity

D. Stale accounts usually have a phone number that is no longer valid for MFA requests

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

While investigating an ongoing identity incident, you notice a stale user account logged in for the first time. What is a stale account defined as?

A. An account that has been dormant or inactive for more than twelve months

B. An account that has been dormant or inactive for more than one month

C. An account that has been dormant or inactive for more than six months

D. An account that has been dormant or inactive for more than three months

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Which entity tab will show an administrator how to lower the account's risk score?

A. Activity

B. Risk

C. Timeline

D. Asset

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

What role does the Falcon sensor play in Falcon Identity Protection?

A. Enables secure access management for domain controllers

B. Provides visibility, threat detection, and enforcement to Microsoft Active Directory

C. Enhances network performance and reduces latency

D. Performs regular vulnerability assessments on domain controllers

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

How does Identity Protection extend the capabilities of existing multi-factor authentication (MFA)?

A. Identity Protection is not going to detect risky user behavior

B. Identity Protection will replace third party MFA and trigger as it detects risky or abnormal behaviors

C. Identity Protection does not support on-premises MFA connectors

D. Implementation of a second layer security control using policy rules as it detects risky or abnormal behaviors

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

The _____ events are excluded by default while Low, Medium, & High detections are visible.

A. Internal

B. Informational

C. Inferior

D. Indiscrete

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

Which section within the Falcon documentation would you be able to find supported versions of Active Directory Federation Services (AD FS)?

A. Identity Protection Integration

B. Identity Monitoring

C. Investigation

D. Identity Protection Configuration

Suggested Answer: *D*

Drikhj Most Recent 7 months, 2 weeks ago

Selected Answer: A

The correct answer is A. Identity Protection Integration.

This can be verified directly in the Falcon console documentation. When searching for "AD FS" under Support and Resources > Documentation, the result is found under:

Identity Protection and MFA → Identity Protection Integration → "Integrating Identity Protection with AD FS"

This section lists the supported versions and requirements:

• AD FS v4.0

• Windows Server 2016

• .NET Framework 4.5.2 or later

Note: Falcon Identity Protection supports applications that integrate with AD FS through SAML.

The other options are incorrect because:

- Identity Monitoring focuses on activity monitoring, not integration requirements

- Investigation is for incident response workflows

- Identity Protection Configuration covers post-deployment settings, not supported versions

upvoted 2 times

Question #34 *Topic 1*

What is the purpose behind creating Policy Rules?

A. Policy Rules determine how the console tracks and learns behavior for users in the environment

B. Policy Rules determine the scope in which the sensor collects information on the environment

C. Policy Rules determine what actions to take in response to certain triggers/conditions observed within the environment

D. Policy Rules determine what actions an admin in the console can take before making adjustments

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

What does the NIST SP800-207 framework define?

A. Principles of Least Privilege and Identity Segmentation

B. Implementation of inherent trust zones for Government Agencies specifically dealing in classified information

C. CrowdStrike Identity Protection implementation and configuration

D. Zero Trust and Zero Trust Architecture tenets, guiding principles, implementation strategies, use cases, and more

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Which of the following MFA providers are NOT supported by Falcon Identity?

A. DUO

B. Azure (Entra) MFA

C. Firebase

D. Symantec VIP

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

Within identity-based detections, the recommended actions will include how to Investigate & _____ the suspicious security events.

A. Recover

B. Resolute

C. Remediate

D. Recon

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

When creating a Falcon Fusion Workflow with Identity Protection, which operator would you use to filter on a pattern?

A. Is equal to

B. Matches

C. Includes

D. Does not match

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Describe the difference between a Human account and a Programmatic account?

A. A human account is an Administrator

B. A human account is often used interactively

C. A Programmatic account is only used interactively

D. A Programmatic account is never authorized for multi-factor authentication

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Which page will have to be visited in order to setup a new MFA provider?

A. Configure -> Settings

B. Enforce -> Policy Rules

C. Configure -> Connectors

D. Monitor -> Domain Security Overview

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

How long does it typically take Falcon Identity to develop a baseline of a user?

A. Three months

B. One week

C. One month

D. Two weeks

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 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

Suggested Answer: *B*

Percy73729 Most Recent 2 months, 1 week ago

Selected Answer: C

Answer is C - On;y the Membership by Severity displays a bar graph

upvoted 1 times

Question #43 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

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

A. Endpoint Manager

B. Workflow Author

C. Device Control Manager

D. Falcon Analyst

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

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

Suggested Answer: *C*

fafd232_ Most Recent 4 months, 1 week ago

Selected Answer: D

Can confirm its D. Policy rules, analytics, and settings are under Enforce (back in the older UI, which this exam seems to be based off)

upvoted 1 times

Question #48 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!