PassQueen
a.k.a dumpsqueen.com

CrowdStrike Certified Falcon Responder

CrowdStrike CCFR-201b

Version Demo

Total Demo Questions: 22

Total Premium Questions: 229

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

What do IOA exclusions help you achieve?

A. Reduce false positives based on Next-Gen Antivirus settings in the Prevention Policy

B. Reduce false positives of behavioral detections from IOA based detections only

C. Reduce false positives of behavioral detections from IOA based detections based on a file hash

D. Reduce false positives of behavioral detections from Custom IOA and OverWatch detections only

ANSWER: B

Explanation:

Reduce false positives of behavioral detections from IOA based detections only is correct because an Indicator of Attack (IOA) exclusion is designed to suppress a specific behavioral detection when the observed activity is known to be legitimate in a particular environment. Falcon IOAs identify suspicious behavior patterns—such as process execution, command-line activity, or other attack-like techniques—rather than relying solely on a known malicious file. When approved software, administrative tooling, or a business workflow predictably triggers an IOA, an exclusion can prevent repeat detections for that legitimate behavior while allowing the relevant IOA protection to remain active for other activity. This lets responders tune behavioral detection outcomes and reduce operational noise without broadly disabling prevention capabilities. Exclusions should be narrowly scoped and validated carefully, since behavioral telemetry and IOA detections are an important layer for identifying adversary techniques that may not have a known malicious hash or signature. CrowdStrike describes IOAs as behavior-based indicators that help identify attacks in progress; see CrowdStrike's IOA overview. Additional context on Falcon's behavioral approach is available in the CrowdStrike Falcon Prevent overview.

QUESTION NO: 2

While investigating a detection, you pivot to the Advanced Event Search.

Which field would you filter by to return events executing from a specific directory on the host?

A. TreeId

B. @source

C. ParentBaseFileName

D. FilePath

ANSWER: D

Explanation:

FilePath is the appropriate field because it records the full filesystem path associated with the executing image or file in relevant Falcon endpoint event data. Filtering this field lets a responder constrain results to activity launched from a particular directory, such as a user-writable location, a temporary folder, a downloads path, or another suspected staging directory. For example, a search can match values beginning with a directory path to locate processes whose executable files were run from that location. This is particularly useful during detection triage because execution path is a strong investigative pivot: it helps establish where a process originated and identify additional executions from the same directory across the affected host or broader environment. The field is therefore directly aligned with a request to return events based on the directory from which activity executed. CrowdStrike's event documentation describes endpoint event fields and their use in searching, while the LogScale search documentation explains field-based filtering and matching patterns used in Advanced Event Search. See the CrowdStrike Event Data Dictionary and CrowdStrike LogScale search documentation.

QUESTION NO: 3

What happens when you create a Sensor Visibility Exclusion for a trusted file path?

A. It excludes host information from Detections and Incidents generated within that file path location

B. It prevents file uploads to the CrowdStrike cloud from that file path

C. It excludes sensor monitoring and event collection for the trusted file path

D. It disables detection generation from that path, however the sensor can still perform prevention actions

ANSWER: C

Explanation:

Creating a Sensor Visibility Exclusion for a trusted file path excludes that path from Falcon sensor visibility: the sensor does not monitor activity or collect telemetry events associated with the excluded path. This capability is intended for narrowly scoped situations in which known, trusted software generates a high volume of non-actionable activity or where collecting visibility data from a particular location is not desired. Because the exclusion affects the sensor's collection of visibility data, analysts will have less or no endpoint telemetry for activity occurring under that trusted path. Use these exclusions carefully and limit their scope as much as possible, since endpoint telemetry is fundamental to threat hunting, investigation, and detection context. CrowdStrike documentation describes Sensor Visibility Exclusions as a mechanism for excluding specified activity from sensor visibility and emphasizes configuring exclusions only for understood and trusted activity. For general guidance on managing Falcon prevention and exclusion policies, see the CrowdStrike Falcon Prevent overview and CrowdStrike's endpoint security best-practices guide.

QUESTION NO: 4

A responder has identified a suspicious PowerShell script executing on a domain controller. To perform a deep-dive forensic analysis of every action taken by that specific processâ€"including network connections and file modificationsâ€"the analyst needs to pivot to a Process Timeline. What is the absolute minimum telemetry data required to generate this auto-filled view?

A. Agent ID (AID) and Local IP Address

B. Agent ID (AID) and Target Process ID (TargetProcessId_decimal)

C. Hostname and MAC Address

D. User SID and SHA256 Hash

ANSWER: B

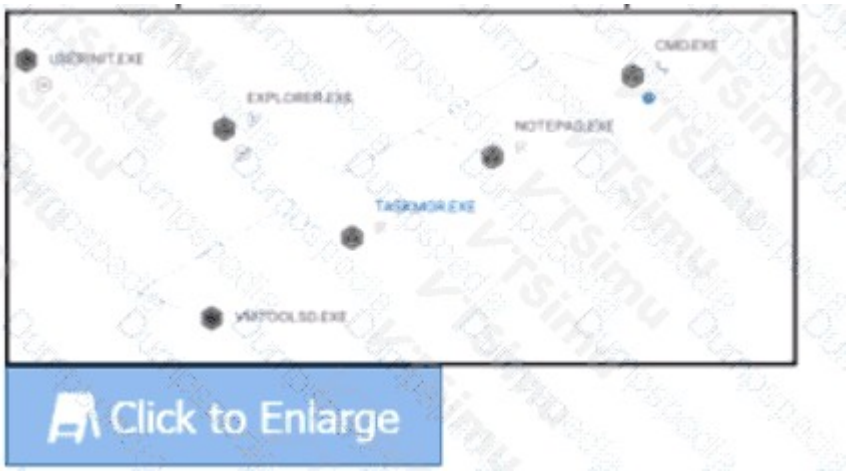
Explanation:

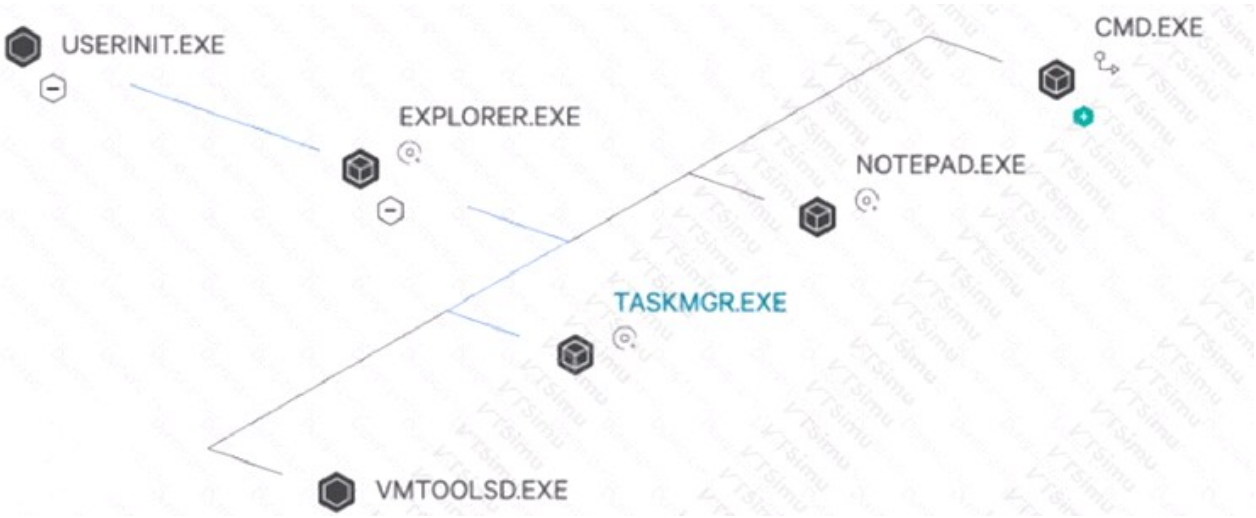
Agent ID (AID) and Target Process ID (TargetProcessId_decimal) is the minimum information needed to open an auto-filled Process Timeline for the specific PowerShell process. The Agent ID uniquely identifies the Falcon sensor/endpoint that generated the telemetry, ensuring the investigation is scoped to the correct domain controller. `TargetProcessId_decimal` identifies the particular process instance on that endpoint. Together, these values provide the endpoint-and-process context Falcon requires to retrieve and organize the related process activity chronologically.

Process Timeline is intended to help responders investigate the full behavioral record associated with one process, including process execution details, file-system activity, registry activity where available, and network events. Supplying the target process identifier rather than only a host identifier is essential because a single host can run many PowerShell processes, potentially with reused names or similar command lines. The decimal process-ID field is the event value used for this pivot and enables Falcon to load the corresponding process-focused view directly. This workflow supports rapid investigation and containment decisions using endpoint detection and response telemetry. See CrowdStrike's Endpoint Detection and Response overview and the CrowdStrike Falcon documentation portal for product documentation and event-investigation guidance.

QUESTION NO: 5

How are processes on the same plane ordered (bottom ' VMTOOLSD.EXE ' to top CMD.EXE ')?





A. Process ID (Descending, highest on bottom)

B. Time started (Descending, most recent on bottom)

C. Time started (Ascending, most recent on top)

D. Process ID (Ascending, highest on top)

ANSWER: B

Explanation:

Time started (Descending, most recent on bottom) is correct. In the Falcon process visualization, processes that occupy the same plane are positioned according to their process-start timestamps. The ordering runs from newer process starts at the bottom toward older process starts at the top. Therefore, when reading vertically within one plane, VMTOOLSD.EXE at the bottom represents a more recently started process than CMD.EXE at the top. This consistent time-based layout helps a responder interpret process relationships and event sequence without treating process identifiers as a timeline. Process IDs are operating-system-assigned values and do not reliably express the order in which processes began, whereas the start-time field directly represents chronology. Using the visual ordering together with the process tree, command line, user context, and related events enables investigators to reconstruct execution activity and identify where a process fits into the endpoint's observed activity. Falcon Insight provides the endpoint telemetry and investigation context used for this type of process analysis. See CrowdStrike's overview of Falcon Insight XDR and its explanation of endpoint detection and response.

QUESTION NO: 6

When performing a ' Hash Search ' , which of the following is NOT a filter available for use?

A. SHA256

B. MD5

C. File Type

D. Filename

ANSWER: C

Explanation:

File Type is the correct selection because Falcon Hash Search is designed to locate file instances by their hash identifiers and associated file-name metadata, rather than by a file-type classification. A hash search begins with a known file fingerprint, such as a cryptographic hash, and Falcon uses that value to identify matching files observed by the platform. Filename metadata can also be used to refine the search when analysts need to distinguish files that share naming characteristics or investigate a known artifact.

File type is a separate attribute derived from a file's format or content and is not one of the available Hash Search filters. This distinction matters during incident response: hashes are deterministic identifiers for a specific file's contents, while file-type labels are broader descriptive properties and do not provide the same precise matching behavior. Analysts should therefore use Hash Search for hash- and filename-based pivots, then use other Falcon investigation views or event-search workflows when they need to scope results using file-format-related context. For background on why hashes serve as unique file identifiers, see CrowdStrike's file hash overview. CrowdStrike's developer documentation also describes the platform's searchable file and indicator data model.

QUESTION NO: 7

Multiple detections with the process schtasks.exe begin to alert in the UI. The process executes the following command line on several unique hosts:

schtasks.exe /Query /TN " Qljsscdqr "

What is the most efficient way to identify which hosts are executing this scheduled task?

A. Filter detections by command line and sort by ' Host:A to Z '

B. Filter detections by command line and group by triggering file

C. Filter detections by the triggering file and sort by ' Host:A to Z '

D. Filter detections by command line and group by host

ANSWER: D

Explanation:

Filter detections by command line and group by host is the most efficient approach because the full command line contains the specific scheduled-task name, `Qljsscdqr`. Filtering on that distinctive value narrows the detection set to the activity relevant to this investigation, rather than including all benign and unrelated uses of the legitimate Windows `schtasks.exe` utility. Grouping the resulting detections by host then immediately consolidates repeated detections from each endpoint and presents the affected systems as the primary investigation scope. This lets a responder quickly determine where the task query occurred, prioritize endpoints for review, and pivot into the associated detection details or process activity for each host.

Scheduled tasks are a common persistence and execution mechanism, and adversaries may use the Windows Task Scheduler command-line utility to enumerate, create, modify, or run tasks. A task name that is unusual and repeated across multiple endpoints is therefore a valuable indicator for focused scoping. CrowdStrike describes how endpoint detection and response supports investigation and response across endpoint activity, while its scheduled-task guidance provides context for why task-related command lines merit investigation. See CrowdStrike's EDR overview and CrowdStrike's scheduled tasks guide.

QUESTION NO: 8

When viewing the main ' Quarantine ' dashboard to manage blocked files, which of the following pieces of information CANNOT be seen by default?

A. Filename

B. Host Name

C. Hash

D. Date Quarantined

ANSWER: C

Explanation:

Hash is the information that cannot be seen by default in the main Falcon Quarantine dashboard. The dashboard is designed first as an operational queue for responders to identify a quarantined item, understand where it originated, and determine when the quarantine event occurred. Its default view therefore emphasizes immediately actionable, human-readable context such as the file name, the affected host, and quarantine timing. A cryptographic file hash is valuable for threat hunting, indicator correlation, malware analysis, and searching across security tools, but it is not part of the default high-level Quarantine table presentation. Responders can obtain additional file metadata through the relevant file, detection, event, or investigation details when deeper analysis is needed. This distinction helps keep the primary Quarantine view focused on managing quarantined artifacts while preserving more technical identifiers for drill-down workflows and integrations. CrowdStrike describes Falcon's prevention and response capabilities, including investigation context, in its Falcon endpoint protection overview. For product-specific console behavior and available workflow details, authorized customers should consult the current CrowdStrike Falcon documentation portal, since displayed fields can vary with console releases and feature entitlements.

QUESTION NO: 9

What is the difference between Managed and Unmanaged Neighbors in the Falcon console?

A. A managed neighbor is currently network contained and an unmanaged neighbor is uncontained

B. A managed neighbor has an installed and provisioned sensor

C. An unmanaged neighbor is in a segmented area of the network

D. A managed sensor has an active prevention policy

ANSWER: B

Explanation:

A managed neighbor has an installed and provisioned sensor. In Falcon's network-visibility and asset-discovery context, a neighbor is an endpoint identified through its network relationship with a Falcon-sensored host. "Managed" denotes that CrowdStrike Falcon recognizes the neighbor as a host enrolled in the customer's Falcon environment: the Falcon sensor is installed and has successfully provisioned, enabling the console to associate the observed device with a managed endpoint record. This distinction helps responders understand which discovered systems can be directly investigated and acted on through Falcon versus systems that have only been observed communicating on the network. The classification is based on Falcon sensor deployment and provisioning status, rather than containment state, network segmentation, or a particular prevention-policy assignment. Managed endpoint status is central to Falcon's ability to provide endpoint telemetry and response capabilities. For additional platform and sensor information, see CrowdStrike's Falcon Prevent overview and the CrowdStrike Falcon documentation portal.

QUESTION NO: 10

When a responder is looking at the ' Full Detection Details ' page, they can toggle between several views. Which of the following is NOT a layout option available for viewing these details?

A. Graph View

B. Tree View

C. Process Timeline

D. List View

ANSWER: C

Explanation:

Process Timeline is the correct selection because it is not one of the selectable layout modes in Falcon's Full Detection Details experience. That page provides distinct ways to visualize and inspect the activity associated with a detection, including a graphical relationship-oriented presentation, a hierarchical process-oriented presentation, and a list-oriented presentation. These layouts help a responder pivot between understanding relationships among processes and events, following parent-child execution context, and reviewing event records in a structured format. A timeline can be a useful investigative concept, but it is not the named layout toggle provided on the Full Detection Details page. Responders should use the available layouts to establish execution context, identify related activity, and investigate the detection efficiently before taking response actions. CrowdStrike describes Falcon Insight XDR as providing correlated endpoint visibility and investigation capabilities, which is the broader product context for working detections: CrowdStrike Falcon Insight XDR. Additional official CrowdStrike resources for Falcon documentation are available through the CrowdStrike Falcon documentation portal.

QUESTION NO: 11

An attacker attaches cmd.exe as a debugger to osk.exe through a registry key.

What tactic and technique describe this activity?

A. Persistence via Image File Execution Options Injection

B. Post-Exploit via Malicious Tool Execution

C. Persistence via External Remote Services

D. Privilege Escalation via Bypass User Account Control

ANSWER: A

Explanation:

Persistence via Image File Execution Options Injection is correct because the Image File Execution Options registry mechanism can define a debugger for a specified executable. When the configured target, such as osk.exe, is launched, Windows starts the program specified in the Debugger value instead. Configuring cmd.exe in this way gives an attacker a reliable execution path tied to the launch of a legitimate Windows accessibility executable. This behavior is mapped by MITRE ATT&CK to Image File Execution Options Injection (T1546.012), a sub-technique of Event Triggered Execution. It can support persistence because the registry configuration remains in place and can repeatedly trigger attacker-controlled execution whenever the target executable is invoked. Depending on the target binary and system context, this technique can also contribute to privilege escalation or defense evasion, but persistence accurately describes the tactic requested here. Incident responders should inspect Image File Execution Options registry locations for unexpected Debugger values, particularly under `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options`. MITRE documents the technique and its relevant registry artifacts at MITRE ATT&CK: Image File Execution Options Injection. Microsoft also documents the Image File Execution Options debugger setting at Configuring Image File Execution Options.

QUESTION NO: 12

In the " Full Detection Details " , which view will provide an exportable text listing of events like DNS requests. Registry Operations, and Network Operations?

A. Thedata is unable to be exported

B. View as Process Tree

C. View as Process Timeline

D. View as Process Activity

ANSWER: D

Explanation:

View as Process Activity is the correct view because it presents the endpoint telemetry associated with the relevant process as an event-oriented activity listing. This format is intended for reviewing the discrete actions recorded during process execution, including DNS activity, Registry operations, and Network operations. It gives responders a detailed, text-based record that can be exported for offline analysis, case documentation, evidence handling, or sharing with other investigation teams. The activity-focused presentation is especially useful when an analyst needs to move beyond the high-level detection summary and examine the sequence and attributes of individual events generated on the host. Exporting this event listing helps preserve the investigative context and supports correlation with logs from other security tools. This capability aligns with Falcon's endpoint detection and response workflow, which provides rich endpoint visibility and investigation data to help responders analyze suspicious behavior. See CrowdStrike's overview of its Endpoint Detection and Response platform and its EDR learning resource for additional context on endpoint telemetry and investigation capabilities.

QUESTION NO: 13

When an organization needs to detect a specific behavior that is unique to their environment, they can create a Custom IOA. Which of the following is NOT required when configuring a custom IOA from scratch?

A. Selecting a Rule Type (e.g., Process Creation).

B. Specifying the Severity level of the resulting detection.

C. Assigning a specific host group to the IOA rule at the time of creation.

D. Providing a unique name for the rule.

ANSWER: C

Explanation:

Assigning a specific host group to the IOA rule at the time of creation is not required. A Custom IOA is first defined as a behavioral rule: the administrator chooses the applicable rule type and configures the criteria that identify the targeted activity, along with rule metadata such as its name and detection severity. This creates a reusable rule definition that can be organized and managed independently of endpoint targeting.

Deployment scope is handled separately through Custom IOA rule groups and Falcon prevention policies. Administrators can add the rule to a rule group and then enable or apply that group through the relevant policy configuration. Because Falcon policies can be assigned to host groups, this model lets an organization control where the Custom IOA is enforced without making a host-group assignment an intrinsic requirement of the rule-creation workflow. It also supports testing and phased rollout: a rule can be authored and reviewed before it is enabled for a selected population of endpoints. CrowdStrike describes Custom IOAs as configurable behavioral detections within Falcon's endpoint protection capabilities; see the CrowdStrike Falcon Prevent overview and the CrowdStrike documentation portal for product documentation and configuration guidance.

QUESTION NO: 14

During an advanced hunting session, a responder is writing a custom query in the Event Search tool to track the lineage of a suspicious process. They notice a field labeled TargetProcessId_decimal. Which of the following sentences accurately describes the technical significance of this value within the CrowdStrike telemetry ecosystem?

A. It is the standard Process ID (PID) assigned by the Windows Task Manager.

B. It is a sensor-assigned, environment-wide unique decimal identifier for that specific process instance.

C. It represents the memory offset where the process ' s primary thread began.

D. It is a count of the total number of child processes spawned by that executable.

ANSWER: B

Explanation:

It is a sensor-assigned, environment-wide unique decimal identifier for that specific process instance. Falcon telemetry uses sensor-generated process identifiers to associate activity with the precise process instance that performed it. The `TargetProcessId_decimal` field is the decimal representation of the target process identifier, making it practical to use in Event Search filters, joins, correlations, and lineage investigations. In particular, a responder can use this identifier with related process-ID fields to pivot between events involving a process and reconstruct parent/child or source/target relationships. This distinction is important during investigations because operating-system process IDs can be reused after a process exits; Falcon's process-instance tracking provides the telemetry context needed to reliably distinguish activity associated with one observed process instance from later activity that may use the same operating-system PID. The field's `_decimal` suffix describes its numeric representation for searching and comparison; it does not change the identity being tracked. This supports the core EDR investigative workflow of correlating endpoint events into an actionable process story. See CrowdStrike's overview of endpoint detection and response investigations and the Falcon platform's endpoint telemetry and investigation capabilities.

QUESTION NO: 15

Which of the following is an example of a MITRE ATT AND CK tactic?

A. Eternal Blue

B. Defense Evasion

C. Emotet

D. Phishing

ANSWER: B

Explanation:

Defense Evasion is a MITRE ATT&CK tactic. In the ATT&CK Enterprise matrix, tactics represent an adversary's high-level tactical objective—the "why" behind a set of activities during an intrusion. Defense Evasion encompasses the objective of avoiding detection or otherwise bypassing defensive controls while carrying out malicious activity. MITRE maps a number of techniques to this tactic, such as Impair Defenses, Masquerading, Modify Registry, and Obfuscated Files or Information. Analysts use tactic-level classifications to understand where observed behavior fits in an attack lifecycle and to organize investigations, detections, and response actions around adversary goals. For example, if a Falcon detection is associated with Defense Evasion, a responder should assess whether the adversary attempted to disable security tooling, hide artifacts, alter system configuration, or otherwise reduce visibility before proceeding with later objectives. MITRE's Enterprise ATT&CK tactics page identifies Defense Evasion as one of its defined tactics, and its tactic detail page provides the associated techniques and current mappings. See the MITRE ATT&CK Enterprise tactics matrix and the Defense Evasion tactic page.

QUESTION NO: 16

The User Search results are organized into several categories. Which of the following is NOT a sub-heading in the User Search?

A. User Logons

B. Unique Executables Written

C. Admin tool usage

D. Network Connections

ANSWER: B

Explanation:

Unique Executables Written is not a User Search results sub-heading. Falcon User Search is designed to pivot from a user identity to activity attributed to that user, presenting the activity in investigation-oriented groupings such as logons, administrative-tool activity, and network activity. These groupings help responders quickly establish where and when an account authenticated, identify potentially significant administrative actions, and review communication activity associated with the account. The wording “Unique Executables Written” instead describes a distinct metric or aggregation of file-write activity. While executable creation or writing can be valuable evidence during an investigation, that phrasing is not one of the categories used to organize the User Search results view. This distinction matters because User Search is focused on user-centric behavioral pivots rather than acting as a generic inventory of unique files written by endpoints. CrowdStrike describes Falcon’s investigation capabilities and its use of endpoint telemetry for threat hunting and response in its Falcon Insight overview and discusses responder investigation workflows in the Falcon Investigate announcement.

QUESTION NO: 17

A security analyst is triaging a high-severity alert on a critical production server. To understand the adversary ' s intent and technical execution within the framework of industry standards, the analyst refers to the console ' s categorization. Which specific methodology does CrowdStrike utilize within the Falcon platform to classify detections based on technical behavior?

A. MITRE ATT&CK framework

B. NIST Incident Response Lifecycle

C. Falcon Adversary Attribution Matrix

D. Cyber Kill Chain Classification

ANSWER: A

Explanation:

MITRE ATT&CK framework is correct because Falcon uses the industry-standard MITRE ATT&CK knowledge base to contextualize detection behavior in terms of adversary tactics and techniques. This mapping helps an analyst move beyond a single alert name and understand both the likely objective of the activity, such as credential access or persistence, and the technical method used to pursue that objective. In Falcon, this ATT&CK context supports triage by providing a consistent vocabulary for investigating related behaviors, assessing potential adversary progression, searching for similar activity, and communicating findings across incident-response teams. ATT&CK is specifically designed as a behavior-focused framework based on observed adversary tradecraft, making it appropriate for classifying detections by technical behavior. CrowdStrike describes how its platform incorporates MITRE ATT&CK to provide adversary and behavioral context, while MITRE maintains the authoritative catalog of tactics, techniques, and procedures. See CrowdStrike’s MITRE ATT&CK overview and the MITRE ATT&CK knowledge base.

QUESTION NO: 18

What actions are available for domain name-based Indicators of Compromise (IOCs) in Falcon?

A. Detect onlyAllow

B. BlockDetect onlyAllow

C. BlockAllowNo action

D. Detect onlyNo action

ANSWER: D

Explanation:

Detect only
No action is correct because Falcon treats domain name indicators as network-oriented observables rather than executable objects that the endpoint sensor can directly permit or prevent based on content. Selecting **Detect only** instructs Falcon to generate detection visibility when the sensor observes activity matching the domain indicator. This is useful to identify hosts, users, processes, and network activity associated with known suspicious infrastructure while supporting investigation and response workflows.

No action is the non-enforcement setting for a domain indicator. It permits the indicator to remain defined without creating an enforcement response from that IOC configuration. This supports situations in which a responder needs to retain, stage, validate, or document an indicator before using it for active detection. Domain IOC handling should therefore be understood as an observability and detection capability in Falcon IOC Management, not as a domain allowlisting or endpoint-blocking control. Responders needing immediate network containment should use the appropriate Falcon response and policy capabilities in addition to IOC-based visibility. CrowdStrike provides background on the role of indicators in detection and investigation in its Indicators of Compromise technical hub and explains Falcon's endpoint detection and response approach in its Falcon Insight overview.

QUESTION NO: 19

A responder is analyzing a process tree where a suspicious executable is listed as a direct child of services.exe. In this scenario, which source is most likely responsible for the execution?

A. An interactive user login via RDP.

B. A Windows Service or a process launched by the Service Control Manager.

C. A web browser download initiated by the end user.

D. A script executed directly from a removable USB drive.

ANSWER: B

Explanation:

A Windows Service or a process launched by the Service Control Manager. is correct because `services.exe` is the Windows Service Control Manager (SCM) process. Its role is to manage installed services, including starting service executables during boot or on demand and controlling their lifecycle. Therefore, when an executable appears as a direct child of `services.exe` in a Falcon process tree, the execution is most consistent with the SCM launching a service process. This lineage is an important investigative signal: responders should examine the service's name, binary path, start mode, account context, command-line arguments, creation or modification history, and associated registry configuration. On Windows, service configuration is stored under `HKLM\SYSTEM\CurrentControlSet\Services`, and service-installed binaries can execute with highly privileged identities such as LocalSystem. Microsoft documents that the SCM is responsible for starting and managing services, and its service-management architecture provides the context needed to validate this process relationship. See Microsoft: About the Service Control Manager and Microsoft: Services.

QUESTION NO: 20

Refer to the image.

You receive the detection displayed in the image above on a host in your environment.

Assuming you have the correct permissions, where would you navigate to remotely connect to the host and investigate further?

A. Investigate > Connect to host

B. View Incident > Connect to host

C. Actions > Connect to host

ANSWER: C

Explanation:

Actions > Connect to host is the correct navigation path because the detection view provides responder actions in its Actions menu, including the ability to initiate a remote session with the affected endpoint. Selecting Connect to host launches a Real Time Response session in the context of that specific host, enabling an authorized responder to conduct live investigation without first navigating away from the detection. This supports common incident-response tasks such as collecting relevant files and system information, reviewing running processes or persistence evidence, executing approved RTR commands, and taking response actions where organizational policy permits.

Availability of this action depends on both the responder's Falcon role permissions and the host's assigned Real Time Response policy. The user must have the applicable RTR access level, and the endpoint must be able to communicate with the Falcon cloud. Starting from the detection also preserves the operational workflow: the responder can review the alert details, identify the affected device, and immediately open a host connection for deeper validation and containment-oriented investigation. CrowdStrike describes Real Time Response as its capability for remotely accessing endpoints and performing live investigative actions; see the CrowdStrike Real Time Response overview and the Falcon Insight product overview.

QUESTION NO: 21

You receive an email from a third-party vendor that one of their services is compromised,thevendor names a specific IP address that the compromised service was using. Where would you input this indicator to find any activity related to this IP address?

A. IP Addresses

B. Remote or Network Logon Activity

C. Remote Access Graph

D. Hash Executions

ANSWER: A

Explanation:

IP Addresses is the appropriate place to enter the vendor-provided IP indicator when investigating whether it has appeared in the environment. An IP address is a network-based indicator of compromise, and the IP-address investigation view is designed to pivot from that value into the relevant Falcon telemetry. This lets a responder identify associated endpoint

activity, review connections involving the address, determine which hosts communicated with it, and establish the time frame and scope of possible exposure. Starting with the indicator itself also supports a focused triage workflow: validate whether the IP is present, assess the related processes and devices, and use those findings to decide whether containment or deeper investigation is needed. CrowdStrike describes indicators of compromise as observable artifacts that can be used to identify potentially malicious activity; IP addresses are one of the common indicator types used in threat hunting and incident response. See CrowdStrike's overview of indicators of compromise and its guidance on threat hunting.

QUESTION NO: 22

Which of the following is NOT a filter available on the Detections page?

A. Severity

B. CrowdScore

C. Time

D. Triggering File

ANSWER: B

Explanation:

CrowdScore is the correct selection because it is not a standard filter field on the Falcon Detections page. The Detections page is designed for responders to locate, triage, and investigate individual endpoint detections using detection-centric attributes, including values such as severity, time range, and details associated with the event that triggered the detection. These filters help narrow operational detection queues according to when activity occurred, its assessed severity, and relevant event or file context.

CrowdScore is instead associated with CrowdStrike's assessment and risk-scoring capabilities, where an organization's security posture or exposure is represented through a score. That type of aggregate posture metric is conceptually separate from the fields used to search and refine individual detection records during incident response. A responder investigating detections would therefore use the Detections workflow and its event-focused filters rather than a CrowdScore value. CrowdStrike's documentation portal provides the product documentation for Falcon investigation workflows, while the CrowdStrike Tech Hub provides supporting material on detection and response operations: CrowdStrike Falcon Documentation and CrowdStrike Tech Hub.