Topic 1 - Exam A

Question #1 *Topic 1*

Which of the following is a suspicious process behavior?

A. PowerShell running an execution policy of RemoteSigned

B. An Internet browser (eg., Internet Explorer) performing multiple DNS requests

C. PowerShell launching a PowerShell script

D. Non-network processes (e.g., notepad.exe) making an outbound network connection

Question #2 *Topic 1*

Which field should you reference in order to find the system time of a *FileWritten event?

A. ContextTimeStamp_decimal

B. FileTimeStamp_decimal

C. ProcessStartTime_decimal

D. timestamp

Question #3 *Topic 1*

What Search page would help a threat hunter differentiate testing, DevOPs, or general user activity from adversary behavior?

A. Hash Search

B. IP Search

C. Domain Search

D. User Search

Question #4 *Topic 1*

An analyst has sorted all recent detections in the Falcon platform to identify the oldest in an effort to determine the possible first victim host. What is this type of analysis called?

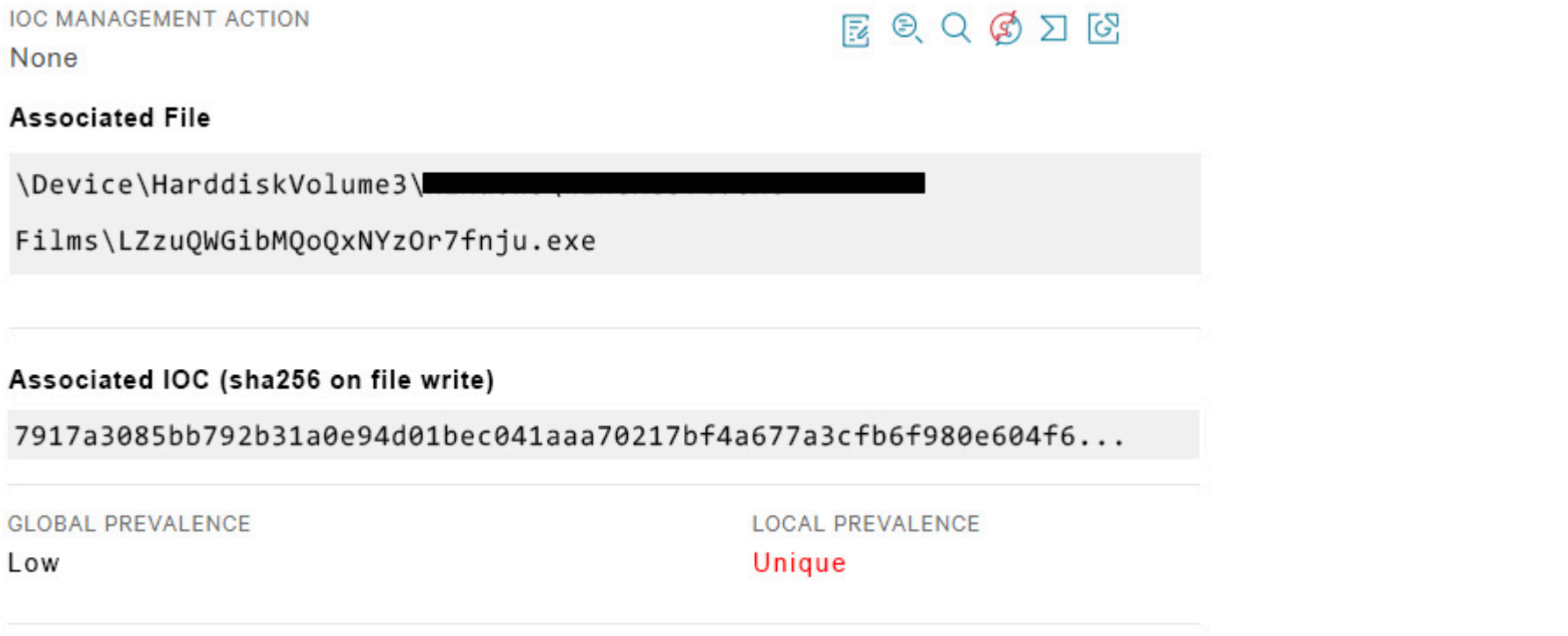
A. Visualization of hosts

B. Statistical analysis

C. Temporal analysis

D. Machine Learning

Question #5 *Topic 1*



Falcon detected the above file attempting to execute. At initial glance, what indicators can we use to provide an initial analysis of the file?

A. VirusTotal, Hybrid Analysis, and Google pivot indicator lights enabled

B. File name, path, Local and Global prevalence within the environment

C. File path, hard disk volume number, and IOC Management action

D. Local prevalence, IOC Management action, and Event Search

Question #6 *Topic 1*

A benefit of using a threat hunting framework is that it:

A. Automatically generates incident reports

B. Eliminates false positives

C. Provides high fidelity threat actor attribution

D. Provides actionable, repeatable steps to conduct threat hunting

Question #7 *Topic 1*

Which of the following is an example of a Falcon threat hunting lead?

A. A routine threat hunt query showing process executions of single letter filename (e.g., a.exe) from temporary directories

B. Security appliance logs showing potentially bad traffic to an unknown external IP address

C. A help desk ticket for a user clicking on a link in an email causing their machine to become unresponsive and have high CPU usage

D. An external report describing a unique 5 character file extension for ransomware encrypted files

Question #8 *Topic 1*

The Falcon Detections page will attempt to decode Encoded PowerShell Command line parameters when which PowerShell Command line parameter is present?

A. -Command

B. -Hidden

C. -e

D. -nop

Question #9 *Topic 1*

Which structured analytic technique contrasts different hypotheses to determine which is the best leading (prioritized) hypothesis?

A. Model hunting framework

B. Competitive analysis

C. Analysis of competing hypotheses

D. Key assumptions check

Question #10 *Topic 1*

Which SPL (Splunk) field name can be used to automatically convert Unix times (Epoch) to UTC readable time within the Falcon Event Search?

A. utc_time

B. conv_time

C. _time

D. time

Question #11 *Topic 1*

Which of the following would be the correct field name to find the name of an event?

A. Event_SimpleName

B. Event_Simple_Name

C. EVENT_SIMPLE_NAME

D. event_simpleName

Question #12 *Topic 1*

Event Search data is recorded with which time zone?

A. PST

B. GMT

C. EST

D. UTC

Question #13 *Topic 1*

Which of the following Event Search queries would only find the DNS lookups to the domain: www.randomdomain.com?

A. event_simpleName=DnsRequest DomainName=www.randomdomain.com

B. event_simpleName=DnsRequest DomainName=randomdomain.com ComputerName=localhost

C. Dns=randomdomain.com

D. ComputerName=localhost DnsRequest “randomdomain.com”

Question #14 *Topic 1*

How do you rename fields while using transforming commands such as table, chart, and stats?

A. By renaming the fields with the “rename” command after the transforming command. e.g. “stats count by ComputerName | rename count AS total_count”

B. You cannot rename fields as it would affect sub-queries and statistical analysis

C. By using the “renamed” keyword after the field name. e.g. “stats count renamed totalcount by ComputerName”

D. By specifying the desired name after the field name. e.g. “stats count totalcount by ComputerName”

Question #15 *Topic 1*

SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time. Which eval function is correct?

A. now

B. typeof

C. strftime

D. relative_time

Question #16 *Topic 1*

Which of the following queries will return the parent processes responsible for launching badprogram.exe?

A. [search (ParentProcess) where name=badprogram.exe] | table ParentProcessName _time

B. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename ParentProcessId_decimal AS TargetProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time

C. [search (ProcessList) where Name=badprogram.exe] | search ParentProcessName | table ParentProcessName _time

D. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename TargetProcessId_decimal AS ParentProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time

Question #17 *Topic 1*

You want to produce a list of all event occurrences along with selected fields such as the full path, time, username etc. Which command would be the appropriate choice?

A. fields

B. distinctcount

C. table

D. values

Question #18 *Topic 1*

When exporting the results of the following event search, what data is saved in the exported file (assuming Verbose Mode)?
event_simpleName=*Written | stats count by ComputerName

A. The text of the query

B. The results of the Statistics tab

C. No data. Results can only be exported when the “table” command is used

D. All events in the Events tab

Question #19 *Topic 1*

The help desk is reporting an increase in calls related to user accounts being locked out over the last few days. You suspect that this could be an attack by an adversary against your organization. Select the best hunting hypothesis from the following:

A. A zero-day vulnerability is being exploited on a Microsoft Exchange server

B. A publicly available web application has been hacked and is causing the lockouts

C. Users are locking their accounts out because they recently changed their passwords

D. A password guessing attack is being executed against remote access mechanisms such as VPN

Question #20 *Topic 1*

To find events that are outliers inside a network, _____is the best hunting method to use.

A. time-based

B. machine learning

C. searching

D. stacking

Question #21 *Topic 1*

Which of the following is a way to create event searches that run automatically and recur on a schedule that you set?

A. Workflows

B. Event Search

C. Scheduled Searches

D. Scheduled Reports

Question #22 *Topic 1*

Which of the following is a recommended technique to find unique outliers among a set of data in the Falcon Event Search?

A. Hunt-and-Peck Search Methodology

B. Stacking (Frequency Analysis)

C. Time-based Searching

D. Machine Learning

Question #23 *Topic 1*

Adversaries commonly execute discovery commands such as net.exe, ipconfig.exe, and whoami.exe. Rather than query for each of these commands individually, you would like to use a single query with all of them. What Splunk operator is needed to complete the following query? aid=my-aid event_simpleName=ProcessRollup2 (FileName=net.exe _____ FileName=ipconfig.exe _____ FileName=whoami.exe) | table ComputerName UserName FileName CommandLine

A. OR

B. IN

C. NOT

D. AND

Question #24 *Topic 1*

You would like to search for ANY process execution that used a file stored in the Recycle Bin on a Windows host. Select the option to complete the following EAM query. aid=my-aid ImageFileName=_____ event_simpleName=ProcessRollup2

A. *$Recycle.Bin^

B. *$Recycle.Bin*

C. ^$Recycle.Bin*

D. ^$Recycle.Bin%

Question #25 *Topic 1*

Which of the following is the proper method to quantify search results, enabling a hunter to quickly sort and identify outliers?

A. Using the “| stats count by” command at the end of a search string in Event Search

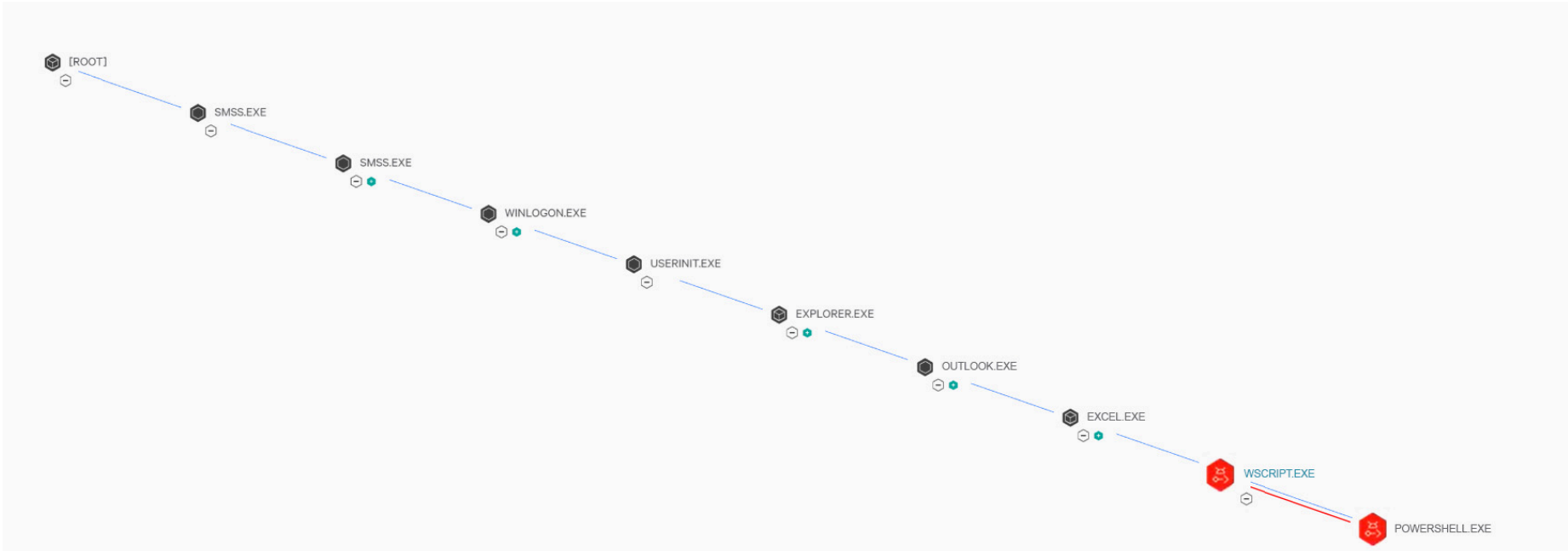
B. Using the “|stats count” command at the end of a search string in Event Search

C. Using the “|eval” command at the end of a search string in Event Search

D. Exporting Event Search results to a spreadsheet and aggregating the results

Question #26 *Topic 1*

What type of attack would this process tree indicate?



A. Brute Forcing Attack

B. Man-in-the-middle Attack

C. Phishing Attack

D. Web Application Attack

Question #27 *Topic 1*

Which pre-defined reports offer information surrounding activities that typically indicate suspicious activity occurring on a system?

A. Scheduled searches

B. Hunt reports

C. Sensor reports

D. Timeline reports

Question #28 *Topic 1*

Lateral movement through a victim environment is an example of which stage of the Cyber Kill Chain?

A. Command & Control

B. Actions on Objectives

C. Exploitation

D. Delivery

Question #29 *Topic 1*

Which tool allows a threat hunter to populate and colorize all known adversary techniques in a single view?

A. MISP

B. OWASP Threat Dragon

C. Open XDR

D. MITRE ATT&CK Navigator

Question #30 *Topic 1*

Which of the following is an example of actor actions during the RECONNAISSANCE phase of the Cyber Kill Chain?

A. Installing a backdoor on the victim endpoint

B. Discovering internet-facing servers

C. Emailing the intended victim with a malware attachment

D. Loading a malicious payload into a common DLL

Question #31 *Topic 1*

Which threat framework allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies?

A. MITRE ATT&CK

B. Lockheed Martin Cyber Kill Chain

C. Director of National Intelligence Cyber Threat Framework

D. NIST 800-171 Cyber Threat Framework

Question #32 *Topic 1*

In the MITRE ATT&CK Framework (version 11 - the newest version released in April 2022), which of the following pair of tactics is not in the Enterprise: Windows matrix?

A. Persistence and Execution

B. Impact and Collection

C. Privilege Escalation and Initial Access

D. Reconnaissance and Resource Development

Question #33 *Topic 1*

In which of the following stages of the Cyber Kill Chain does the actor not interact with the victim endpoint(s)?

A. Exploitation

B. Weaponization

C. Command & control

D. Installation

Question #34 *Topic 1*

What information is provided from the MITRE ATT&CK framework in a detection's Execution Details?

A. Grouping Tag

B. Command Line

C. Technique ID

D. Triggering Indicator

Question #35 *Topic 1*

You need details about key data fields and sensor events which you may expect to find from Hosts running the Falcon sensor. Which documentation should you access?

A. Events Data Dictionary

B. Streaming API Event Dictionary

C. Hunting and Investigation

D. Event stream APIs

Question #36 *Topic 1*

The Events Data Dictionary found in the Falcon documentation is useful for writing hunting queries because:

A. It provides pre-defined queries you can customize to meet your specific threat hunting needs

B. It provides a list of all the detect names and descriptions found in the Falcon Cloud

C. It provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console

D. It provides a list of compatible splunk commands used to query event data

Question #37 *Topic 1*

Which Falcon documentation guide should you reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts?

A. Hunting and Investigation

B. Customizable Dashboards

C. MITRE-Based-Falcon Detections Framework

D. Events Data Dictionary

Question #38 *Topic 1*

What topics are presented in the Hunting and Investigation Guide?

A. Detailed tutorial on writing advanced queries such as sub-searches and joins

B. Detailed summary of event names, descriptions, and some key data fields for hunting and investigation

C. Sample hunting queries, select walkthroughs and best practices for hunting with Falcon

D. Recommended platform configurations and prevention settings to ensure detections are generated for hunting leads

Question #39 *Topic 1*

Which of the following does the Hunting and Investigation Guide contain?

A. A list of all event types and their syntax

B. A list of all event types specifically used for hunting and their syntax

C. Example Event Search queries useful for threat hunting

D. Example Event Search queries useful for Falcon platform configuration

Question #40 *Topic 1*

Which document provides information on best practices for writing Splunk-based hunting queries, predefined queries which may be customized to hunt for suspicious network connections, and predefined queries which may be customized to hunt for suspicious processes?

A. Real Time Response and Network Containment

B. Hunting and Investigation

C. Events Data Dictionary

D. Incident and Detection Monitoring

Question #41 *Topic 1*

What is the main purpose of the Mac Sensor report?

A. To identify endpoints that are in Reduced Functionality Mode

B. To provide a summary view of selected activities on Mac hosts

C. To provide vulnerability assessment for Mac Operating Systems

D. To provide a dashboard for Mac related detections

Question #42 *Topic 1*

Where would an analyst find information about shells spawned by root, Kernel Module loads, and wget/curl usage?

A. Sensor Health report

B. Linux Sensor report

C. Sensor Policy Daily report

D. Mac Sensor report

Question #43 *Topic 1*

Which of the following best describes the purpose of the Mac Sensor report?

A. The Mac Sensor report displays a listing of all Mac hosts without a Falcon sensor installed

B. The Mac Sensor report provides a detection focused view of known malicious activities occurring on Mac hosts, including machine-learning and indicator-based detections

C. The Mac Sensor report displays a listing of all Mac hosts with a Falcon sensor installed

D. The Mac Sensor report provides a comprehensive view of activities occurring on Mac hosts, including items of interest that may be hunting or investigation leads

Question #44 *Topic 1*

In the Powershell Hunt report, what does the “score” signify?

A. Number of hosts that ran the PowerShell script

B. How recently the PowerShell script executed

C. Maliciousness score determined by NGAV

D. A cumulative score of the various potential command line switches

Question #45 *Topic 1*

In the Powershell Hunt report, what does the filtering condition of CommandLine!="*badstring*" do?

A. Prevents command lines containing “badstring” from being displayed

B. Displays only the command lines containing “badstring”

C. Highlights “badstring” in all command lines in the output

D. Highlights only the command lines containing “badstring”

Question #46 *Topic 1*

What Investigate tool would you use to allow an analyst to view all events for a specific host?

A. Bulk Timeline

B. Host Search

C. Host Timeline

D. Process Timeline

Question #47 *Topic 1*

What do you click to jump to a Process Timeline from many pages in Falcon, such as a Hash Search?

A. PID

B. Process ID or Parent Process ID

C. CID

D. Process Timeline Link

Question #48 *Topic 1*

What elements are required to properly execute a Process Timeline?

A. Agent ID (AID) and Target Process ID

B. Agent ID (AID) only

C. Hostname and Local Process ID

D. Target Process ID only

Question #49 *Topic 1*

What is the difference between a Host Search and a Host Timeline?

A. Host Search is used for detection investigation and Host Timeline is used for proactive hunting

B. A Host Search organizes the data in useful event categories like process executions and network connections; a Host Timeline provides an uncategorized view of recorded events in chronological order

C. You access a Host Search from a detection to show you every recorded process event related to the detection and you can only populate the Host Timeline fields manually

D. There is no difference. You just get to them different ways

Question #50 *Topic 1*

The Process Timeline Events Details table will populate the Parent Process ID and the Parent File columns when the cloudable Event data contains which event field?

A. ContextProcessId_decimal

B. RawProcessId_decimal

C. ParentProcessId_decimal

D. RpcProcessId_decimal

Question #51 *Topic 1*

While you're reviewing Unresolved Detections in the Host Search page, you notice the User Name column contains “hostname$.” What does this User Name indicate?

A. The User Name is a System User

B. The User Name is not relevant for the dashboard

C. There is no User Name associated with the event

D. The Falcon sensor could not determine the User Name

Question #52 *Topic 1*

Which of the following is TRUE about a Hash Search?

A. Wildcard searches are not permitted with the Hash Search

B. The Hash Search provides Process Execution History

C. The Hash Search is available on Linux

D. Module Load History is not presented in a Hash Search

Question #53 *Topic 1*

With Custom Alerts you are able to configure email alerts using predefined templates so you're notified about specific activity in your environment. Which of the following outlines the steps required to properly create a custom alert rule?

A. Choose the template you would like to configure, setup how often you would like the alert to run, and then schedule the alert

B. Choose the template you would like to configure, preview the search results, and then schedule the alert

C. Create the query for the alert, setup the email template for the alert, and then set the schedule for the alert

D. Create a new custom template, configure the email template, and then create the custom query for the alert

Question #54 *Topic 1*

What information is provided when using IP Search to look up an IP address?

A. Both internal and external IPs

B. Suspicious IP addresses

C. External IPs only

D. Internal IPs only

Question #55 *Topic 1*

What kind of activity does a User Search help you investigate?

A. A history of Falcon UI logon activity

B. A list of process activity executed by the specified user account

C. A count of failed user logon activity

D. A list of DNS queries by the specified user account

Question #56 *Topic 1*

To view Files Written to Removable Media within a specified timeframe on a host within the Host Search page, expand and refer to the _____ dashboard panel.

A. Command Line and Admin Tools

B. Processes and Services

C. Registry, Tasks, and Firewall

D. Suspicious File Activity

Question #57 *Topic 1*

When performing a raw event search via the Events search page, what are Event Actions?

A. Event Actions contains an audit information log of actions an analyst took in regards to a specific detection.

B. Event Actions contains the summary of actions taken by the Falcon sensor such as quarantining a file, prevent a process from executing or taking no actions and creating a detection only.

C. Event Actions are pivotable workflows including connecting to a host, pre-made event searches and pivots to other investigatory pages such as host search.

D. Event Actions is the field name that contains the event name defined in the Events Data Dictionary such as ProcessRollup, SyntheticProcessRollup, DNS request, etc.

Question #58 *Topic 1*

What information is shown in Host Search?

A. Quarantined Files

B. Prevention Policies

C. Intel Reports

D. Processes and Services

Question #59 *Topic 1*

You are reviewing a list of domains recently banned by your organization's acceptable use policy. In particular, you are looking for the number of hosts that have visited each domain. Which tool should you use in Falcon?

A. Create a custom alert for each domain

B. Allowed Domain Summary Report

C. Bulk Domain Search

D. IP Addresses Search

Question #60 *Topic 1*

Which field in a DNS Request event points to the responsible process?

A. ContextProcessId_readable

B. TargetProcessId_decimal

C. ContextProcessId_decimal

D. ParentProcessId_decimal