



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



CERTIFICATION TEST

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

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

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **StewartJ** 5 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

🗳️ 👤 **alanalanalan** 7 months, 1 week ago

Selected Answer: D

Support answer is D

upvoted 2 times

🗳️ 👤 **silva222222** 7 months, 3 weeks ago

Selected Answer: D

Correct answer and LETTER (D)

This is the most suspicious behavior because programs like notepad.exe typically don't need internet access. It could indicate malware attempting to communicate with a remote server.

upvoted 2 times

🗳️ 👤 **dylann** 8 months, 2 weeks ago

C. PowerShell launching a PowerShell script

This behavior can be suspicious because it indicates the use of PowerShell to execute scripts, which is commonly exploited by attackers to run malicious code on a system. It's often a sign of potential compromise or unauthorized activity.

upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (100%)

examtopics3000 **Highly Voted** 1 year, 11 months ago

Selected Answer: A

ContextTimeStamp: System time of event creation.

upvoted 7 times

dpari **Most Recent** 7 months, 1 week ago

events-data-Dictionary: ContextTimeStamp_decimal: The time the event occurred on the system, as seen by the sensor.

upvoted 1 times

alanalanalan 1 year ago

Selected Answer: A

the question is asking "system time of xxx". the "*FileWritten event" is the event, the focus is the system time, so the answer is A

Document : Falcon Documentation > Event Investigation > Events > Events Full Reference (Events Data Dictionary)

ContextTimeStamp_decimal

The time at which an event occurred on the system, as seen by the sensor (in decimal, non-hex format). Not to be confused with timestamp which is the time the event was received by the cloud.

upvoted 3 times

silva222222 1 year, 1 month ago

Selected Answer: A

(A) ContextTimeStamp_decimal: This field specifically refers to the time the event was captured by the security system, which is what you're interested in for a FileWritten event.

upvoted 2 times

gr23 1 year, 5 months ago

ContextTimeStamp. FileTimeStamp only records time of file modification, not creation.

upvoted 1 times

Joe_Kwok 1 year, 11 months ago

Selected Answer: A

System time should be ContextTimeStamp_decimal

upvoted 4 times

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

Suggested Answer: D

Community vote distribution

D (100%)

  **pokewww** Highly Voted 1 year, 10 months ago

Selected Answer: D

User Search is a search page that allows a threat hunter to search for user activity across endpoints and correlate it with other events. This can help differentiate testing, DevOPs, or general user activity from adversary behavior by identifying anomalous or suspicious user actions, such as logging into multiple systems, running unusual commands, or accessing sensitive files.

Reference: <https://www.crowdstrike.com/blog/tech-center/user-search-in-crowdstrike-falcon/>
upvoted 5 times

  **alanalanalan** Most Recent 1 year ago

Selected Answer: D

The question is asking "user activity", so the answer is D. User Search
upvoted 1 times

  **silva222222** 1 year, 1 month ago

Selected Answer: D

D. User Search
upvoted 1 times

  **examtopics3000** 1 year, 10 months ago

In addition, there is no "domain search" menu as such. There is "bulk domains".
upvoted 1 times

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

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: C

C. Temporal analysis
upvoted 1 times

IOC MANAGEMENT ACTION

None

**Associated File**

```
\Device\HarddiskVolume3\
Films\LZzuQWGibMQoQxNYzOr7fnju.exe
```

Associated IOC (sha256 on file write)

```
7917a3085bb792b31a0e94d01bec041aaa70217bf4a677a3cfb6f980e604f6...
```

GLOBAL PREVALENCE

Low

LOCAL PREVALENCE

Unique

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

Suggested Answer: B

Community vote distribution

B (100%)

alanalanalan 1 year ago**Selected Answer: B**

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

The all information was shown on the photo
upvoted 1 times

silva222222 1 year, 1 month ago**Selected Answer: B**

The most informative indicators for initial file analysis after a Falcon detection are:

B. File name, path, Local and Global prevalence within the environment
upvoted 1 times

Chiquitabandita 1 year, 9 months ago**Selected Answer: B**

the initial analysis typically starts with the file's name, path, and prevalence within your environment.
upvoted 1 times

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

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **alanalanalan** 1 year ago

Selected Answer: D

D. Provides actionable, repeatable steps to conduct threat hunting
upvoted 1 times

🗳️ 👤 **silva222222** 1 year, 1 month ago

Selected Answer: D

The biggest benefit of using a threat hunting framework is that it:

D. Provides actionable, repeatable steps to conduct threat hunting
upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: A

Selected Answer: A

upvoted 1 times

🗨️ 👤 **silva222222** 1 year, 1 month ago

Selected Answer: A

The best example of a Falcon threat hunting lead in the context of CrowdStrike is:

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

upvoted 1 times

🗨️ 👤 **Tech_Amit** 1 year, 2 months ago

I think , it should be B

upvoted 1 times

🗨️ 👤 **Tech_Amit** 1 year, 2 months ago

I think , it should be A

upvoted 1 times

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

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: C

Answer C ("-e"). Powershell "-e" indicates that the following command fragment is "encoded"
upvoted 1 times

🗳️ 👤 **silva222222** 1 year, 1 month ago

Selected Answer: C

The Falcon Detections page will attempt to decode encoded PowerShell command line parameters when the parameter present is:

C. -e
upvoted 1 times

🗳️ 👤 **Jimmy390** 1 year, 9 months ago

Selected Answer: C

Answer C ("-e"). Powershell "-e" indicates that the following command fragment is "encoded"
upvoted 3 times

🗳️ 👤 **examtopics3000** 1 year, 11 months ago

Selected Answer: C

Answer C ("-e"). Powershell "-e" indicates that the following command fragment is "encoded".
upvoted 4 times

🗳️ 👤 **examtopics3000** 1 year, 11 months ago

Isn't the correct answer "-e"?
upvoted 4 times

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

Suggested Answer: C

Community vote distribution

C (100%)

 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: C

C. Analysis of competing hypotheses

upvoted 1 times

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

Suggested Answer: *C*

Community vote distribution

C (100%)

🗨️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: C

C. _time

upvoted 1 times

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

Suggested Answer: D

Community vote distribution

D (100%)

  **nestorian** Highly Voted 1 year, 11 months ago

D event_simpleName
upvoted 7 times

  **examtopics3000** 1 year, 11 months ago



Is this test/questions good, is it reliable?
upvoted 1 times

  **Pipo12345** 1 year, 6 months ago



Quite a lot/If not all the questions you see here will show up in the exam. Some answers in here are wrong but the questions are real. Always check the comments.
upvoted 1 times

  **alanalanalan** Most Recent 11 months, 3 weeks ago

Selected Answer: D
D. event_simpleName
upvoted 1 times

  **five55** 1 year, 3 months ago

100 PERCENT D
upvoted 1 times

  **gr23** 1 year, 5 months ago

D. event_simpleName. When you see the other questions with sample queries provided, this is how this field name is written.
upvoted 1 times

  **Chiquitabandita** 1 year, 9 months ago

Selected Answer: D
<https://community.splunk.com/t5/Splunk-Search/Splunk-Subsearch-Join-Combine-event-query-assistance/m-p/457160>
upvoted 3 times

Event Search data is recorded with which time zone?

- A. PST
- B. GMT
- C. EST
- D. UTC

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: D

D. UTC

upvoted 2 times

🗳️ 👤 **Chiquitabandita** 1 year, 9 months ago

Selected Answer: D

Event Search data is typically recorded with the UTC (Coordinated Universal Time) time zone. So, the correct option is D. UTC. This is a common practice in cybersecurity and log management to maintain consistency and accuracy across different systems and time zones.

upvoted 4 times

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"

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **alanalanalan** 11 months, 3 weeks ago

Selected Answer: A

A. event_simpleName=DnsRequest DomainName=www.randomdomain.com
upvoted 1 times

🗨️ **five55** 1 year, 3 months ago

Selected Answer: A

I think it a because we do not need to put the Computer Name as Host. We only interested in the domain address
upvoted 1 times

🗨️ **kangaru** 1 year, 5 months ago

Selected Answer: A

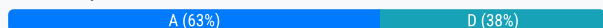
B: This would not match www.randomdomain.com without using *
C: Same as B
D. This one work, but not written in the best practice format. The use of 'ComputerName' diverts the success criteria of question.
upvoted 1 times

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"

Suggested Answer: A

Community vote distribution



🗳️ **examtopics3000** Highly Voted 1 year, 11 months ago

For me, the correct answer is A. "By renaming the fields with the "rename" command after the transforming command. e.g. "stats count by ComputerName | rename count AS total_count"

upvoted 6 times

🗳️ **NastyNutsu** Most Recent 5 months, 4 weeks ago

Selected Answer: A

What is Splunk questions doing here in CCFH-202?

upvoted 1 times

🗳️ **alanalanalan** 11 months, 3 weeks ago

Selected Answer: A

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

good reference : <https://gist.github.com/ag-michael/4fc4e4ae7a8226dcb679261f18a3500d>

upvoted 1 times

🗳️ **silva222222** 1 year, 1 month ago

Selected Answer: A

The correct answer is A. By renaming the fields with the "rename" command after the transforming command. For example, "stats count by ComputerName | rename count AS total_count". This allows you to rename fields after performing transforming commands like table, chart, or stats, enabling you to customize the field names as needed for clarity or consistency in your analysis.

upvoted 1 times

🗳️ **kangaru** 1 year, 5 months ago

Selected Answer: A

D may be correct, but the example 'stats count (as) totalcount by ComputerName' works only on 'stats' and 'chart'. 'Table' however, does not support using 'as' to rename field on the fly. However, with '| rename input as output' works for all table, chart and stats, which sufficiently satisfy the success criteria of the question.

upvoted 1 times

🗳️ **gr23** 1 year, 5 months ago

A, You rename after the transform command. The results of the transform command are "renamed" to what you specify, This doesn't affect sub-queries and stat analysis

upvoted 1 times

🗳️ **joal23** 1 year, 8 months ago

Letter A, because letter D is wrong. See this example: event_platform=win event_simpleName=ProcessRollup2 FileName=PowerShell.exe | stats count(aid) as psExecutionCount by FileName

You can see on this url: https://www.reddit.com/r/crowdstrike/comments/ns4k9q/20210604_cool_query_friday_stats/

upvoted 4 times

🗳️ **Jimmy390** 1 year, 9 months ago

Selected Answer: D

Because you are using transforming commands, definitely D, check the example queries here:

https://www.reddit.com/r/crowdstrike/comments/tz5obg/20220408_cool_query_friday_scoring_user_logon/

upvoted 1 times

  **Chiquitabandita** 1 year, 9 months ago

Selected Answer: A

I change my answer to A

<https://docs.splunk.com/Documentation/Splunk/8.2.3/SearchReference/Rename>

upvoted 2 times

  **Chiquitabandita** 1 year, 9 months ago

Selected Answer: D

specify the desired name after the field name

upvoted 2 times

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

Suggested Answer: C

Community vote distribution


C (100%)

  **alanalanalan** 11 months, 3 weeks ago

Selected Answer: C

C. strftime

upvoted 1 times

  **kangaru** 1 year, 5 months ago

| eval starttime=strftime(StartTimestamp,"%Y-%m-%dT%H:%M:%S.%Q")

upvoted 1 times

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

Suggested Answer: B

Community vote distribution

B (78%)

D (22%)

🗳️ **alanalanalan** 11 months, 3 weeks ago

Selected Answer: B

Selected Answer: B

upvoted 1 times

🗳️ **five55** 1 year, 3 months ago

Selected Answer: B

You need to combine the field the only way we can do with subsearch

upvoted 1 times

🗳️ **gr23** 1 year, 5 months ago

B. To find "parent" you rename ParentProcessID_decimal to TargetProcessID_decimal

upvoted 1 times

🗳️ **Pipo12345** 1 year, 6 months ago

Selected Answer: B

B is correct.

upvoted 1 times

🗳️ **joal23** 1 year, 8 months ago

Is Letter B. The Parent Process is when rename ParentProcessId_decimal as TargetProcessId_decimal.

upvoted 2 times

🗳️ **Chiquitabandita** 1 year, 9 months ago

Selected Answer: D

This query will return the parent processes responsible for launching badprogram.exe by using a subsearch to find the processrollup2 events where FileName is badprogram.exe, then renaming the TargetProcessId_decimal field to ParentProcessId_decimal and using it as a filter for the main search, then using stats to count the occurrences of each FileName by _time.

upvoted 2 times

🗳️ **kangaru** 1 year, 5 months ago

By renaming TargetProcessId_decimal field to ParentProcessId_decimal, you pivot the targetprocess of badprogram.exe as the child and search for all child process launched by badprogram.exe instead, not the process that spawned badprogram.exe.

upvoted 1 times

🗳️ **Chiquitabandita** 1 year, 9 months ago

Selected Answer: B

query filters for "badprogram.exe" and renames the ParentProcessId_decimal to TargetProcessId_decimal to find the parent processes associated with it. The "stats count by FileName _time" part of the query helps present the results effectively.

upvoted 1 times

🗳️ **examtopics3000** 1 year, 11 months ago

Selected Answer: B

Sorry, correct answer is B

upvoted 3 times

  **examtopics3000** 1 year, 11 months ago

For me, correct answer is D

upvoted 1 times

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

Suggested Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **NastyNutsu** 5 months, 4 weeks ago

Selected Answer: C

...|TABLE fullpath _time username

* field is used to include or exclude specified fields in the search results

* distinctcount is used to count the distinct values of a field.

* values is used to list the unique values of a field but doesn't create a table format for mutiple fields
upvoted 2 times

🗲️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: C

C. table

upvoted 1 times

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

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **NastyNutsu** 5 months, 4 weeks ago

Selected Answer: B

B. When you run an event search like event_simpleName=*Written | stats count by ComputerName in Splunk and choose to export the results, the data saved in the exported file will be the results shown in the Statistics tab.

upvoted 1 times

🗳️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: B

B. The results of the Statistics tab

the keyword is "stats"

upvoted 1 times

🗳️ 👤 **kangaru** 1 year, 5 months ago

Selected Answer: B

Verified B

upvoted 1 times

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

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **NastyNutsu** 5 months, 4 weeks ago

Selected Answer: D

- A. does not explain the increase in account lockouts
 - B. same as A
 - C. unlikely that multiple people change their password at the same period
 - D. this indicate that a brute force attack, which results in multiple account get lockouts (best answer).
- upvoted 1 times

🗨️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: D

Selected Answer: D
upvoted 1 times

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

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ **alanalanalan** 11 months, 3 weeks ago

Selected Answer: D

D. stacking

upvoted 1 times

🗨️ **kangaru** 1 year, 5 months ago

<https://proinf.com/threat-hunting-techniques-checklist-examples-process-exection-metrics#:~:text=Stacking%20One%20of%20the%20methods,or%20outliers%20of%20those%20results.>

upvoted 1 times

🗨️ **Jimmy390** 1 year, 9 months ago

Selected Answer: D

stacking

upvoted 1 times

🗨️ **Joe_Kwok** 1 year, 10 months ago

Selected Answer: D

stacking is always for outliers finding.

example:

<https://www.crowdstrike.com/blog/mo-shells-mo-problems-file-list-stacking/>

upvoted 3 times

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

Suggested Answer: C

Community vote distribution

C (100%)

🗉 👤 **Infosec703** 10 months, 3 weeks ago

Selected Answer: C

CrowdStrike has Scheduled Search functionality, vendor demo at link at:

<https://www.youtube.com/watch?v=jIN2AhLyMjl>

upvoted 1 times

🗉 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: C

C. Scheduled Searches

reference : CrowdStrike Scheduled Search Add-on for Splunk

upvoted 1 times

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

Suggested Answer: B

Community vote distribution

B (100%)

  **alanalanalan** 11 months, 3 weeks ago

Selected Answer: B

B. Stacking (Frequency Analysis)

upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **nestorian** Highly Voted 👍 1 year, 11 months ago

Answer is A. OR

upvoted 5 times

🗲️ 👤 **alanalanalan** Most Recent ⌚ 11 months, 3 weeks ago

Selected Answer: A

Answer is A. OR

upvoted 1 times

🗲️ 👤 **gr23** 1 year, 5 months ago

Answer is A. AND is implied and not needed in most queries.

upvoted 1 times

🗲️ 👤 **Jimmy390** 1 year, 9 months ago

Selected Answer: A

Answer is A. OR

upvoted 2 times

🗲️ 👤 **examtopics3000** 1 year, 11 months ago

Selected Answer: A

Answer is A. OR

upvoted 4 times

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%

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: B

B. *\$Recycle.Bin*

Regex, use the *

upvoted 3 times

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

Suggested Answer: A

Community vote distribution

A (100%)

alanalanalan 11 months, 3 weeks ago

Selected Answer: A

Answer : A

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

keyword : stats count by

Reference : Investigating and Querying Event Data with Falcon EDR

upvoted 1 times

five55 1 year, 3 months ago

Selected Answer: A

100 percent A

upvoted 1 times

five55 1 year, 3 months ago

Selected Answer: A

I think B is wrong because stats count "by" has to be there

upvoted 1 times

gr23 1 year, 5 months ago

Answer is A. stats count BY. Look at any of the sample queries CS gives you on their blogs and they all have stats count BY.

upvoted 1 times

Chiquitabandita 1 year, 9 months ago

I think this is a bad question though, you could use stats count or stats count by, it depends on what the desired outcome is and it is not specified in the question clearly.

upvoted 1 times

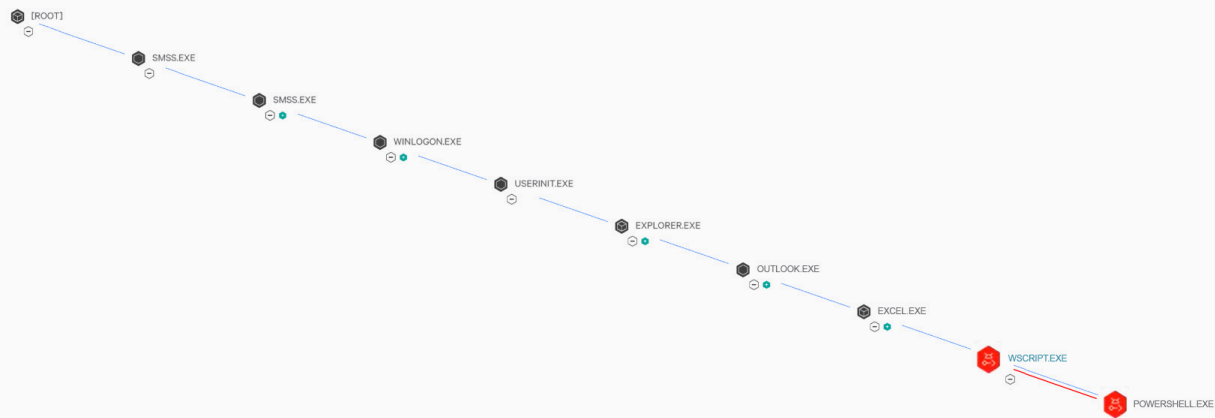
Chiquitabandita 1 year, 9 months ago

Selected Answer: A

The "| stats count by" command allows you to aggregate and count results based on specific fields, which is useful for quantifying and summarizing search results and identifying outliers based on different criteria.

upvoted 2 times

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

Suggested Answer: C

Community vote distribution

C (100%)

NastyNutsu 5 months, 3 weeks ago

Phishing attacks typically involve tricking users into opening malicious attachments or links in email applications like Outlook, which then execute scripts (WScript) and potentially malicious commands (PowerShell).

upvoted 1 times

alanalanalan 11 months, 3 weeks ago

Selected Answer: C

C. Phishing Attack

A, B, D are incorrect

upvoted 1 times

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

Suggested Answer: B

Community vote distribution

B (100%)

  **alanalanalan** 11 months, 3 weeks ago

Selected Answer: B

B. Hunt reports

upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: A

A. Command & Control
upvoted 1 times

🗳️ 👤 **gr23** 1 year, 5 months ago

Answer is A. Command and Control. Lateral movement is a method of control/eluding detection.
upvoted 1 times

🗳️ 👤 **Jimmy390** 1 year, 9 months ago

Selected Answer: A

<https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/>
upvoted 4 times

🗳️ 👤 **Chiquitabandita** 1 year, 9 months ago

Selected Answer: A

<https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/>
upvoted 1 times

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

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **NastyNutsu** 5 months, 3 weeks ago

Selected Answer: D

D, where CK in ATT&CK is stand for Common Knowledge.

upvoted 1 times

🗳️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: D

D. MITRE ATT&CK Navigator

upvoted 1 times

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

Suggested Answer: *B*

Community vote distribution

B (100%)

 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: B

B. Discovering internet-facing servers

upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: A

A. MITRE ATT&CK

upvoted 2 times

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

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **alananalan** 11 months, 3 weeks ago

Selected Answer: D

D. Reconnaissance and Resource Development

The question is asking "not"
upvoted 1 times

🗳️ 👤 **gr23** 1 year, 5 months ago

D. These two tactics are a part of the PRE-ATT&CK matrix and not ATT&CK
upvoted 3 times

🗳️ 👤 **Jonnelson** 1 year, 9 months ago

Selected Answer: D

D according to MITRE ATT&CK website
upvoted 1 times

🗳️ 👤 **Jimmy390** 1 year, 9 months ago

Selected Answer: D

<https://attack.mitre.org/matrices/enterprise/windows/>
upvoted 1 times

🗳️ 👤 **Chiquitabandita** 1 year, 9 months ago

Selected Answer: D

<https://attack.mitre.org/matrices/enterprise/windows/>
upvoted 1 times



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

Suggested Answer: B

Community vote distribution

B (100%)

  **NastyNutsu** 5 months, 3 weeks ago

Selected Answer: B

The interaction with the victim's endpoint begins at the Exploitation stage. The Weaponization stage involves preparation without direct interaction with the victim.

upvoted 1 times

  **alanalanalan** 11 months, 3 weeks ago

Selected Answer: B

B. Weaponization

the question is asking "not"

upvoted 1 times

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

Suggested Answer: C

Community vote distribution

C (100%)

 **alanalanalan** 11 months, 3 weeks ago

Selected Answer: C

C. Technique ID

upvoted 2 times

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

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **alanalanalan** 11 months, 2 weeks ago

Selected Answer: A

A. Events Data Dictionary

Document : Falcon Documentation > Event Investigation > Events > Events Full Reference (Events Data Dictionary)

This reference contains all sensor and non-sensor events and their available documentation in one location.

upvoted 2 times

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

Suggested Answer: C

Community vote distribution

C (100%)

 **alanalanalan** 11 months, 2 weeks ago

Selected Answer: C

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

Document : Falcon Documentation > Event Investigation > Events > Events Full Reference (Events Data Dictionary)

The Events Data Dictionary provides reference information about the events found in these locations:

Event Search helps you get complete visibility into all hosts running the Falcon sensor.

This guide contains:

- A summary of events by platform
- Names and descriptions of each event
- Some key data fields for the most common events
- Copy-and-paste sample queries for the most common events

upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (100%)

 **alanalanalan** 11 months, 2 weeks ago

Selected Answer: A

A. Hunting and Investigation

The question keyword "hunt".

Document : Falcon Documentation > Event Investigation > Hunting and Investigation (Legacy)
upvoted 1 times

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

Suggested Answer: C

Community vote distribution

C (100%)

 **alanalanalan** 11 months, 2 weeks ago

Selected Answer: C

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

The Hunting Guide for Windows teaches you how to hunt for adversaries, suspicious activities, suspicious processes, and vulnerabilities on the Windows platform using Falcon.

This guide contains information about how to hunt using Falcon and is tailored specifically towards users running the Falcon sensor on Windows devices. However, a lot of the ideas and concepts also apply to users running the Falcon sensor on Mac or Linux. Depending on the sensor platform, however, the names and descriptions of certain events as well as custom query syntax will vary

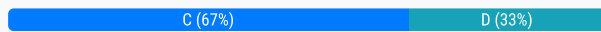
upvoted 2 times

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

Suggested Answer: C

Community vote distribution



alanalanalan 11 months, 2 weeks ago

Selected Answer: C

C. Example Event Search queries useful for threat hunting

I think the question (and the user guide) is focus on " threat hunting", and the answer D keyword is "Falcon platform configuration". The question and guide is more on threat hunting , NOT the configuration.

So I think C is better answer.

upvoted 1 times

five55 1 year, 3 months ago

Selected Answer: C

I think C is the correct answer

upvoted 1 times

gr23 1 year, 5 months ago

D is not suitable here. The question is about Threat Hunting and not platform administration.

upvoted 1 times

VasiOnCacao 1 year, 6 months ago

Selected Answer: D

I think D is more suitable here.

upvoted 1 times

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

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **alanalanalan** 11 months, 2 weeks ago

Selected Answer: B

B. Hunting and Investigation

question keyword "hunt"

upvoted 1 times

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

Suggested Answer: B

Community vote distribution

B (100%)

 **alanalanalan** 11 months, 1 week ago

Selected Answer: B

Answer B

B. To provide a summary view of selected activities on Mac hosts
upvoted 1 times

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

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **NastyNutsu** 5 months, 3 weeks ago

Selected Answer: B

"...by root..." gave this away...

upvoted 1 times

🗨️ 👤 **alanalanalan** 11 months, 1 week ago

Selected Answer: B

B. Linux Sensor report

upvoted 1 times

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

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **alanalanalan** 11 months, 1 week ago

Selected Answer: D

Answer D

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
upvoted 1 times

🗳️ 👤 **gr23** 1 year, 5 months ago

D, What they said.
upvoted 1 times

🗳️ 👤 **Jonnelson** 1 year, 9 months ago

Selected Answer: D

D Is the correct answer
upvoted 2 times

🗳️ 👤 **Chiquitabandita** 1 year, 9 months ago

Selected Answer: 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.
upvoted 2 times