Question #1 *Topic 1*

A Falcon Log Collector has been configured with 4 sinks of type memory, each having a queue size of 2GB.
What is the minimum memory requirement produced by this configuration?

A. 9 GB

B. 12 GB

C. 10 GB

D. 8 GB

Suggested Answer: *C*

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

Question #2 *Topic 1*

Which default role will maintain least privilege and allow for creation and management of parsers?

A. NG SIEM Analyst

B. NG SIEM Security Lead

C. NG SIEM Administrator

D. NG SIEM Analyst – Read Only

Suggested Answer: *B*

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

Question #3 *Topic 1*

What are the two types of connectors used to integrate data between third-party systems and Falcon?

A. Internal and External

B. Push and Pull

C. On-Prem and Cloud

D. Syslog and Application Programming Interface (API)

Suggested Answer: *B*

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

Question #4 *Topic 1*

What is the first consideration when determining the necessary sizing requirements for log collector clients in a Next-Gen SIEM deployment?

A. The expected daily log volume from each data source

B. The available network bandwidth between the log collectors and the Next-Gen SIEM platform

C. The number of concurrent users accessing the Next-Gen SIEM console

D. The processing power and memory of the log collector host systems

Suggested Answer: *A*

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

Question #5 *Topic 1*

What is the purpose of labels in Fleet Management?

A. Set passwords for collector instances

B. Categorize collectors for group configurations

C. Monitor network traffic

D. Assign IP addresses to collectors

Suggested Answer: *B*

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

Question #6 *Topic 1*

As a Next-Gen SIEM Engineer, you are responsible for managing and tuning correlation rules to improve the detection of potential security incidents. One of your correlation rules is designed to detect multiple failed login attempts that are followed by a successful login within a short time frame.
Which step would you take to tune this correlation rule to reduce false positives while maintaining its effectiveness?

A. Increase the time window for detecting multiple failed login attempts to capture more data

B. Add a condition to exclude known trusted IP addresses from triggering the rule

C. Decrease the threshold for the number of failed login attempts required to trigger the rule

D. Remove the condition for a successful login to simplify the rule

Suggested Answer: *B*

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

Question #7 *Topic 1*

Which statement is accurate about how data ingest is measured and represented in Next-Gen SIEM?

A. Average GB/day for all sources (pre-parsing)

B. Average GB/month for first and third-party sources (pre-parsing)

C. Average GB/month for all sources (post-parsing)

D. Average GB/day for third-party sources only (pre-parsing)

Suggested Answer: *A*

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

Question #8 *Topic 1*

Following the principle of least privilege, which is the appropriate role to grant a Falcon Next-Gen SIEM user the permissions to read case data and write XDR data while denying the permission to write case templates?

A. NG SIEM Security Lead

B. NG SIEM Analyst – Read Only

C. NG SIEM Analyst

D. NGSIEM Administrator

Suggested Answer: *C*

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

Question #9 *Topic 1*

You need to ingest data from a custom internal application hosted on-prem. The application writes logs to a file on a syslog server.
Which data connector would you use?

A. Google Cloud Pub / Sub Data Connector

B. HTTP Event Connector

C. Amazon S3 Data Connector

D. Azure Virtual Machines Data Connector

Suggested Answer: *B*

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

Question #10 *Topic 1*

You find a Falcon Log Collector instance on a Linux system that is not connected to Fleet Management.
What command would you use to enroll the Falcon Log Collector?

A. "C:\Program Files (x86)\CrowdStrike\Humio Log Collector\humio-log-collector.exe" enroll <TOKEN>

B. sudo logscale-collector enroll <TOKEN>

C. sudo humio-log-collector enroll <TOKEN>

D. sudo humio-log-collector --token <TOKEN> enroll

Suggested Answer: *C*

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

Question #11

Topic 1

What is the time format for the @timestamp field when data is parsed using the CrowdStrike Parsing Standard (CPS)?

A. ISO 8601

B. Unix Time in microseconds

C. Human-readable

D. Unix Time in milliseconds

Suggested Answer: *A*

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

Question #12 *Topic 1*

Which CQL statement below includes correct placement of the AND statements and the pipe symbol?

A. #sourcefile="jobfilename" AND stdout=/\[[\+]\]/ | groupBy([hostname], function=collect([hostname,stdout])) AND stdout != "" AND stdout != "* No artifacts *" | select([hostname,stdout])

B. #sourcefile="jobfilename" | stdout=/\[[\+]\]/ | groupBy([hostname], function=collect([hostname,stdout])) | stdout != "" AND stdout != "* No artifacts *" AND select([hostname,stdout])

C. #sourcefile="jobfilename" AND stdout=/\[[\+]\]/ | groupBy([hostname], function=collect([hostname,stdout])) | stdout != "" AND stdout != "* No artifacts *" | select([hostname,stdout])

D. #sourcefile="jobfilename" | stdout=/\[[\+]\]/ AND groupBy([hostname], function=collect([hostname,stdout])) AND stdout ! = "" | stdout != "* No artifacts *" | select([hostname,stdout])

Suggested Answer: *C*

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

Question #13 *Topic 1*

A correlation rule is generating a high volume of detections. You have been asked to temporarily deactivate it so your team can investigate.
What will happen to previously generated detections while the rule is in a deactivated state?

A. They will not be impacted and will remain within the console

B. Their status will change to closed and tagged as true positives in the console

C. Their status will change to closed and tagged as false positives in the console

D. They will be immediately deleted from the console

Suggested Answer: *A*

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

Question #14 *Topic 1*

What is the recommended order of the three required activities to build an efficient CQL query?

A. Filter > Format > Aggregate

B. Filter > Aggregate > Format

C. Format > Filter > Aggregate

D. Aggregate > Filter > Format

Suggested Answer: *B*

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

Question #15 *Topic 1*

You have been tasked with parsing the following space delimited log:

```
2025-06-03 12:13:07 johndoe 192.168.5.15 login
```

The log source data is guaranteed to always be in the same order.

Which function can parse this log?

A. parseCEF()

B. parseJson()

C. parseCsv()

D. parseFixedWidth()

Suggested Answer: *C*

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

Question #16

Topic 1

You are reviewing a lookup file to determine whether an event was successfully parsed during ingestion.
Which metadata field indicates the event’s parsing status?

A. @ingesttimestamp

B. @rawstring

C. @error_msg

D. @event_parsed

Suggested Answer: *D*

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

Question #17 *Topic 1*

Review the log event below:

```
{"ts": "2018/11/01 14:31:10", "server": "webOl", "message": "Out of memory"}
```

Which parsing function is correct to add a missing timezone field?

A. parseJson() | parseTimestamp("dd/MMM/yyyy:HH:mm:ss Z", timezone="Europe/Paris", field=ts)

B. kvParse() | findTimestamp(field=ts, timezone="Europe/London")

C. kvParse() | findTimestamp(timezone="America/New_York")

D. parseJson() | parseTimestamp("yyyy/MM/dd HH:mm:ss", timezone="Europe/Paris", field=ts)

Suggested Answer: *D*

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

Question #18 *Topic 1*

What is true about first-party data from the Falcon platform and its integration into Next-Gen SIEM?

A. First-party data requires a log collector installation

B. It is quickly ingested to Next-Gen SIEM via a third-party integration

C. It is instantly accessible within Next-Gen SIEM

Suggested Answer: *C*

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

Question #19 *Topic 1*

What is the correct mode to enroll LogCollector into Fleet Management with configuration of the log sources stored and managed centrally in Next-Gen SIEM?

A. Full

B. Complete

C. Central

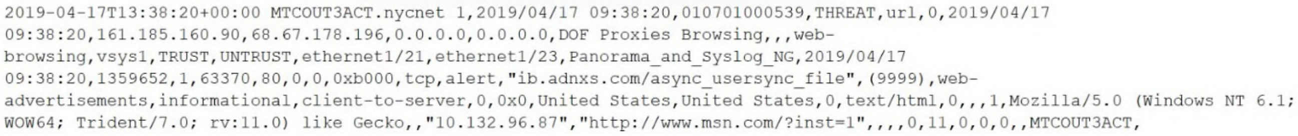
D. localConfig

Suggested Answer: *C*

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

Question #20 Topic 1

Review the log sample below:



```
2019-04-17T13:38:20+00:00 MTCOUT3ACT.nycnet 1,2019/04/17 09:38:20,010701000539,THREAT,url,0,2019/04/17
09:38:20,161.185.160.90,68.67.178.196,0.0.0.0,0.0.0.0,DOF Proxies Browsing,,,web-
browsing,vsys1,TRUST,UNTRUST,ethernet1/21,ethernet1/23,Panorama_and_Syslog_NG,2019/04/17
09:38:20,1359652,1,63370,80,0,0,0xb000,tcp,alert,"ib.adnxs.com/async_usersync_file",(9999),web-
advertisements,informational,client-to-server,0,0x0,United States,United States,0,text/html,0,,,1,Mozilla/5.0 (Windows NT 6.1;
WOW64; Trident/7.0; rv:11.0) like Gecko,,"10.132.96.87","http://www.msn.com/?inst=1",,,,0,11,0,0,0,,MTCOUT3ACT,
```

What type of parser should be used to extract fields and values from this log?

A. XML

B. CSV

C. JSON

D. Key-Value

Suggested Answer: *B*

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

Question #21 *Topic 1*

Which command helps visualize in real time whether sources and sinks are working properly in the Log Collector?

A. journalctl -u logscale-collector

B. logscale-collector monitor

C. logscale-collector check

D. logscale-collector --status

Suggested Answer: *B*

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

Question #22 *Topic 1*

When deploying the Falcon Log Collector using the commands in the CrowdStrike Fleet Management interface, what is the correct service name?

A. flc-api

B. humio-collector

C. logscale-collector

D. flc-collector

Suggested Answer: *C*

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

Question #23 *Topic 1*

You need to provide a colleague the appropriate role to allow for configuration of connectors and creation of SOAR automations in Next-Gen SIEM. Which role will provide these permissions while also maintaining least privilege?

A. NG SIEM Security Lead

B. NG SIEM Analyst

C. Falcon Security Lead

D. Custom role

Suggested Answer: *A*

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

Question #24 *Topic 1*

You notice that the format of incoming logs suddenly changes from JSON format to key-value pairs during log collection.
What action would you take to parse the data correctly?

A. Use a multi-source configuration with different parsers per source

B. Switch to fleet mode and monitor the logs

C. Restart the log collector in debug mode

D. Disable parsing entirely

Suggested Answer: *A*

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

Question #25 *Topic 1*

You notice a larger than expected ingest delay from one of your high-volume streaming log collectors.
Which setting should you increase on the log collector to improve performance?

A. Amount of available disk space

B. Available source throughput

C. Number of concurrent requests a sink is using

D. Default memory queue size

Suggested Answer: *D*

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

Question #26 *Topic 1*

You are configuring third-party data for ingestion. Once a connection is established, you see the HTTP response code 413 as received by your data shipper.
What does this response code indicate?

A. Bad request. Might indicate invalid data format or no data.

B. Bad request. Connection is accessing non-existent endpoints.

C. This transient error might occur in rare cases. Wait and retry the request.

D. Bad request. The payload size exceeds the allowed limit.

Suggested Answer: *D*

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

Question #27 *Topic 1*

Which are valid parse functions in CQL?

A. parseCEF()
parseIETF()
parseJson()

B. parseCEF()
parseJson()
parseXml()

C. parseCEF()
parseIETF()
parseXml()

D. parseIETF()
parseJson()
parseXml()

Suggested Answer: *B*

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

Question #28 *Topic 1*

How does a first-party detection differ from a third-party detection?

A. First-party detections are those native to the platform, while third-party detections are those created by the customer’s security team

B. First-party detections can be seen by all users, while third-party detections require special roles and permissions to be viewed

C. First-party detections are a higher severity than third-party detections and should be triaged first

D. First-party detections are those native to the platform, while third-party detections are generated from data sources external to the platform

Suggested Answer: *D*

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

Question #29 *Topic 1*

What is the maximum number of active correlation rules in a CID?

A. 1000

B. 250

C. 750

D. 500

Suggested Answer: *D*

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

Question #30 *Topic 1*

Which three System alerts are enabled by default in Next-Gen SIEM for third-party connectors?

A. Alert if connector receives no data in 24 hours
Alert if connector is disconnected
Resolve alerts within 30 days

B. Alert if daily data ingestion limit exceeded
Alert if monthly data ingestion limit is exceeded
Resolve alerts within 30 days

C. Alert if connector is disconnected
Alert if daily data ingestion limit exceeded
Alert if monthly data ingestion limit is exceeded

D. Alert if connector receives no data in 24 hours
Alert if daily data ingestion limit exceeded
Alert if monthly data ingestion limit is exceeded

Suggested Answer: *D*

Community vote distribution

A (100%)

2bc8d14 21 hours, 6 minutes ago

Selected Answer: A

Note: The Automatically resolve alerts within 30 days, Alert if connector is disconnected, and Alert if connector receives no data in 24 hours settings are enabled by default. If you disable these alerts settings, it may take up to 1 minute for alerts to appear when you enable them again.

upvoted 1 times