



Vendor: CrowdStrike

Exam Code: CCSE-204

Exam Name: CrowdStrike Certified SIEM Engineer

Version: DEMO

QUESTION 1

Which sequence correctly describes the process for duplicating a workflow in Fusion SOAR?

- A. Go to Fusion SOAR > Workflow Management > Select "All Workflows" tab > Right-click on the workflow to duplicate > Select "Clone Workflow" > Modify workflow parameters > Click "Validate" > Set workflow status > Click Apply Changes
- B. Go to Fusion SOAR > Fusion SOAR > Workflows > Select the checkbox next to the workflow you want to duplicate > Click "Actions" at the top of the page > Select "Create Copy" > Edit workflow name and description > Configure trigger conditions > Click Next > Review workflow canvas > Click Finish
- C. Go to Fusion SOAR > Fusion SOAR > Workflows > Click Open (three dots) menu for the workflow you want to duplicate > Click "Duplicate workflow" > Update and rename the duplicated workflow > Click Save and exit to save the updated workflow
- D. Go to Fusion SOAR > Fusion SOAR > Workflows > Find the workflow to duplicate > Click the workflow name > Select "Duplicate" from Actions menu > Edit the workflow configuration > Click "Create" to generate the new workflow > Set Status to On

Answer: C

Explanation:

In Fusion SOAR, duplicating a workflow is done through the workflow's options menu (three dots), selecting "Duplicate workflow," and then updating and saving the new workflow. This ensures the original workflow remains unchanged while creating an editable copy.

QUESTION 2

You want a consistent view of events from various data sources.

Which ECS field type should you normalize?

- A. Base Fields
- B. Extended Fields
- C. Detection Fields
- D. Core Fields

Answer: D

Explanation:

Normalizing events to Core Fields in the Elastic Common Schema (ECS) provides a consistent structure across different data sources, enabling reliable search, correlation, and detection in Next-Gen SIEM.

QUESTION 3

Which default parser would you use to parse the log event below?

```
Jan 15 14:22:07 host1 sshd[1234]: Failed login
```

- A. Key-value
- B. JSON
- C. Regex
- D. Syslog

Answer:

Explanation:

The log follows the standard syslog format (timestamp, hostname, process, message). The

default Syslog parser is designed to extract fields from such logs efficiently.

QUESTION 4

You clone a default parser and modify only the `parseTimestamp()` function to accommodate custom time format in your logs.

What is the impact on queries that search for this data?

- A. No changes are necessary because all fields will be the same in both parsers
- B. The `#Cps.version` field will need to be updated
- C. The `#type` field will need to be updated
- D. The `#` character needs to be removed from tagged fields as cloning the parser removes all tagged fields

Answer: A

Explanation:

Cloning a parser and modifying only the `parseTimestamp()` function does not change the field names or structure. Queries referencing existing fields will continue to work without modification.

QUESTION 5

You are onboarding a log source that includes a timestamp with a different timezone.

How should you address any time parsing errors that occur?

- A. Clone the parser and manually apply the timezone parameter
- B. Adjust the log source to reflect the correct timezone before sending logs
- C. Clone the parser and change the timestamp field name
- D. Clone the parser and drop the timestamp field, use `ingesttimestamp` instead

Answer: A

Explanation:

When logs have timestamps in a different timezone, cloning the parser and specifying the correct timezone parameter in the `parseTimestamp()` function ensures accurate time parsing without altering field names or losing data.

QUESTION 6

The `parseJson()` function would be used to parse which log message format from the list below?

- A. `level=debug msg="Disconnected" host=app01`
- B. `192.168.1.1 [192.168.1.1] - - [10/May/2024:14:23:11 +0000] "GET/index.html"`
- C. `{ "level": "info", "msg": "User login", "user": "john_doe" }`
- D. `2024-05-10T14:23:11Z INFO Service started`

Answer: C

Explanation:

The `parseJson()` function is used to parse logs that are in JSON format, allowing extraction of fields such as `level`, `msg`, and `user` into structured, searchable data.

QUESTION 7

You are creating a dashboard in Next-Gen SIEM and want to change the visualization used by a widget.

What must be selected to make this change?

- A. Interactions options
- B. Edit in Search view
- C. Styling options

Answer: C

Explanation:

In Next-Gen SIEM dashboards, Styling options allow you to change the visualization type of a widget, including charts, tables, and graphs, without modifying the underlying query.

QUESTION 8

Which combination of scope and permissions must be configured to create an API token that allows you to create and get the results of a query job in Next-Gen SIEM?

- A. NGSiem with both write and execute permissions
- B. NGSiem with read permissions only
- C. NGSiem with both read and write permissions
- D. NGSiem with write permissions only

Answer: C

Explanation:

Creating a query job requires write permission, while retrieving the results requires read permission. Therefore, an API token must have both read and write permissions scoped to NGSiem.

QUESTION 9

How can you enable internal logging for a specific Falcon Log Collector instance from the Fleet view?

- A. Reinstall the collector with logging enabled
- B. Edit the local configuration file
- C. Select "Manage Internal Logging" from the menu
- D. Restart the collector service with the flag "Manage Internal Logging"

Answer: C

Explanation:

In the Fleet view, internal logging for a specific Falcon Log Collector can be enabled directly by selecting "Manage Internal Logging", which allows configuration of logging levels and collection without modifying the installation or configuration files.

QUESTION 10

In the Next-Gen SIEM Connector Dashboard, what is the maximum retention period for which you can query third-party data ingestion metrics?

- A. 30 days
- B. 60 days
- C. 90 days

D. 180 days

Answer: C

Explanation:

The Next-Gen SIEM Connector Dashboard allows querying third-party data ingestion metrics for up to 90 days, providing visibility into trends and connector performance over this period.

QUESTION 11

You are creating a dashboard that will display inbound network connections. You want to give users the ability to filter the source IP address using a dashboard parameter, so they have the option to either type in the IP they want to filter on or select from a list of IPs found in the data.

What type of parameter would you use?

- A. File
- B. Query
- C. FreeText
- D. FixedList

Answer: B

Explanation:

A Query parameter dynamically retrieves values from the data, allowing users to either select from a list of existing IPs or type in a custom IP. This provides flexibility compared to a FixedList or FreeText parameter.

QUESTION 12

You are performing a search query using data from the Falcon Sensor and third-party data connectors.

Which Advanced Event Search data source should you choose?

- A. All
- B. Falcon
- C. Third-party
- D. Custom

Answer: A

Explanation:

Selecting All as the data source in Advanced Event Search allows you to query across both Falcon Sensor data and third-party data connectors, ensuring comprehensive search results from all available sources.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14