



Vendor: CrowdStrike

Exam Code: CCSA-205

Exam Name: CrowdStrike Certified SIEM Analyst

Version: DEMO

QUESTION 1

Which query language is used to search data in CrowdStrike Falcon Next-Gen SIEM?

- A. SPL (Search Processing Language)
- B. CQL (CrowdStrike Query Language)
- C. KQL (Kusto Query Language)
- D. SQL

Answer: B

Explanation:

Falcon Next-Gen SIEM is built on the LogScale engine and uses CrowdStrike Query Language (CQL). CQL is a pipeline-based language where each expression is separated by the pipe character and passes its results to the next stage.

QUESTION 2

In CQL, what does a bare search term such as failed match against?

- A. Only the field named "message"
- B. The @rawstring field of the event
- C. All indexed field names
- D. Nothing; every search must specify a field

Answer: B

Explanation:

A free-text term is a substring search against @rawstring, which holds the original event text. Because it does not use extracted fields, free-text search is convenient but generally slower and less precise than field-based filters.

QUESTION 3

Which CQL expression returns events where the field status is anything other than 200?

- A. status != 200
- B. status <> 200
- C. NOT status == 200
- D. status.exclude(200)

Answer: A

Explanation:

CQL uses != for negation of a field test, and the equivalent form !status=200 is also valid. Note that events which do not contain the field at all are also returned by !=.

QUESTION 4

How is a regular expression filter written in CQL?

- A. field ~ "pattern"
- B. field=/pattern/
- C. regex(field, "pattern")
- D. field LIKE 'pattern'

Answer: B

Explanation:

Regular expressions are enclosed in forward slashes, for example `url=/admin/`. Adding the `i` flag after the closing slash, such as `/admin/i`, makes the match case-insensitive.

QUESTION 5

Which special field in CQL contains the timestamp used for placing an event on the search timeline?

- A. `@ingesttimestamp`
- B. `@timestamp`
- C. `@collect_time`
- D. `@eventtime`

Answer: B

Explanation:

`@timestamp` is the event time parsed from the log itself and it determines where the event appears in the time range and on charts. `@ingesttimestamp` records when the platform received the event and is useful for detecting ingest delay.

QUESTION 6

An analyst wants to find the difference between when an event occurred and when it was received. Which calculation is correct?

- A. `delay := @ingesttimestamp - @timestamp`
- B. `delay := @timestamp - @ingesttimestamp`
- C. `delay := now() - @collecttime`
- D. `delay := @timestamp / @ingesttimestamp`

Answer: A

Explanation:

Both timestamps are stored in milliseconds since epoch, so subtracting event time from ingest time yields the ingest lag. Large positive values indicate delayed forwarding, buffering at the collector, or clock skew on the source.

QUESTION 7

What is the purpose of the `:=` operator in CQL?

- A. It compares two fields for equality
- B. It assigns a value to a new or existing field
- C. It defines a query parameter
- D. It creates a saved search

Answer: B

Explanation:

`:=` performs assignment, as in `total := bytes_in + bytes_out`, and is shorthand for using the `eval()` function. The single `=` sign is reserved for filtering and comparison.

QUESTION 8

Which function limits the result set to the first 20 events returned in a non-aggregated search?

- A. | limit(20)
- B. | head(20)
- C. | first(20)
- D. | top(20)

Answer: B

Explanation:

head() returns the oldest events within the search window, while tail() returns the newest. When no argument is given, both default to 200 events.

QUESTION 9

Which CQL function counts events grouped by a field?

- A. | stats count by field
- B. | groupBy(field)
- C. | aggregate(field, count)
- D. | summarize(field)

Answer: B

Explanation:

groupBy(field) aggregates events by the specified field and, when no function is given, defaults to count(as=_count). Multiple fields can be supplied as an array, for example groupBy([user, host]).

QUESTION 10

What is the default number of groups (series) returned by groupBy() before results are truncated?

- A. 200
- B. 1,000
- C. 20,000
- D. Unlimited

Answer: C

Explanation:

groupBy() returns up to 20,000 groups by default and will warn that results were truncated if the cardinality is higher. The limit parameter can raise this up to the configured maximum, but very high-cardinality grouping should be avoided for performance reasons.

QUESTION 11

Which query returns the ten source IP addresses generating the most events?

- A. | top(src_ip)
- B. | sort(src_ip)
- C. | head(10, src_ip)
- D. | count(src_ip, limit=10)

Answer: A

Explanation:

top() is shorthand for grouping by the field, counting, and sorting descending, and its default limit is 10. The limit can be changed with top(src_ip, limit=25).

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>



10% Discount Coupon Code: ASTR14