DUMPSARENA

CrowdStrike Engineer

CrowdStrike CCSE-204

Version Demo

Total Demo Questions: 7

Total Premium Questions: 76

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Falcon Platform	3
Topic 2, Falcon LogScale	68
Topic 3, Falcon Fusion SOAR	4
Topic 4, Mix Questions	1
Total	76

QUESTION NO: 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

ANSWER: D

Explanation:

First-party detections are those native to the platform, while third-party detections are generated from data sources external to the platform. In Falcon Next-Gen SIEM, first-party detections are generated from CrowdStrike Falcon's own telemetry and detection capabilities, such as detections associated with endpoint activity collected by the Falcon sensor. They are therefore natively produced and enriched within the Falcon platform. Third-party detections, in contrast, result from security-relevant data ingested into Falcon Next-Gen SIEM from external technologies and services. These can include data from identity providers, firewalls, cloud platforms, network tools, email security products, and other supported log sources. Falcon normalizes, stores, correlates, and makes this external data available for investigation alongside CrowdStrike-native telemetry. The distinction describes the source and origin of the detection data, not the detection's severity, the team that authored a rule, or which users may view it. Understanding this source distinction helps analysts interpret available context and use Falcon's unified investigation workflows effectively across both CrowdStrike and non-CrowdStrike security data. CrowdStrike describes Falcon Next-Gen SIEM as bringing together first-party Falcon data with third-party data to support unified security operations. See CrowdStrike Falcon Next-Gen SIEM and CrowdStrike Falcon LogScale.

QUESTION NO: 2

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

ANSWER: A

Explanation:

NG SIEM Security Lead is the appropriate least-privilege role for a user who must configure connectors and create SOAR automations within Next-Gen SIEM. This role is intended for personnel who administer and tune SIEM operational capabilities rather than only investigate alerts and events. Its elevated Next-Gen SIEM permissions support configuration-oriented work, including managing data integrations/connectors and building the automation that operationalizes detection, enrichment, and response processes.

Using the purpose-built Next-Gen SIEM security-lead role follows least-privilege practice because access is scoped to SIEM leadership and configuration responsibilities instead of granting broad, tenant-wide Falcon administration. It enables the colleague to perform the requested operational tasks while preserving separation between SIEM administration and unrelated platform administration functions. CrowdStrike positions Next-Gen SIEM as a platform for unifying security data and automating investigation and response, and Falcon Fusion SOAR provides the workflow automation foundation used for

those automated processes. See CrowdStrike's Next-Gen SIEM overview and Falcon Fusion SOAR overview for the relevant product capabilities.

QUESTION NO: 3

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

ANSWER: C

Explanation:

NG SIEM Analyst is the appropriate least-privilege role for this requirement. It is intended for operational analysts who investigate security activity and work within incident-response workflows. The required access pattern combines visibility into case information with the ability to contribute operational XDR data, allowing the user to perform active investigation and response work rather than merely view information. At the same time, the role does not include the elevated case-template authoring capability requested to be denied. This distinction is important because case templates are reusable workflow and process-definition artifacts; controlling their modification helps preserve consistent case-management practices while allowing analysts to work on the cases and XDR records assigned to them. Assigning the purpose-built analyst role therefore grants the capabilities needed for day-to-day detection, investigation, and response activity without extending access into broader case-workflow administration. CrowdStrike describes Falcon Next-Gen SIEM as bringing together security data, investigation, and response workflows, while Falcon's role-based access control model supports assigning only the permissions needed for a user's function. See CrowdStrike Falcon Next-Gen SIEM and the Falcon documentation portal for role and permission configuration guidance.

QUESTION NO: 4

An automation account must submit a Next-Gen SIEM query job and then poll the job until it can retrieve the results. The account must not receive permissions unrelated to this workflow.

Which API-client permission configuration is required?

A. NGSIEM with read permissions only

B. NGSIEM with write permissions only

C. NGSIEM with both read and write permissions

D. Event Streams with read permissions only

ANSWER: C

Explanation:

The API client requires the **NGSIEM** scope with both **Read** and **Write** permissions. Submitting a query job requires write capability, while retrieving job status and results requires read capability.

Read-only access cannot create the query job, and write-only access cannot retrieve its output. Permissions for other Falcon API collections do not authorize the required Next-Gen SIEM query-job operations.

QUESTION NO: 5

A dashboard widget already returns the correct grouped results from its query. An engineer needs to replace the current table with a chart without changing the query, filters, or time range.

Which widget area should the engineer use?

A. Interactions options

B. Search view

C. Styling options

D. Data source selection

ANSWER: C

Explanation:

The engineer should use the Styling options. Visualization selection is a presentation setting for the widget, so changing it through Styling preserves the existing query and the data returned by that query.

Editing the query in Search view can change the result set, while Interactions options control dashboard behavior rather than the chart or display format.

QUESTION NO: 6

Which field is compliant with CrowdStrike Parsing Standard (CPS)?

A. Parser.type

B. #event.dataset

C. #event.trigger

D. Parser.name

ANSWER: B

Explanation:

#event.dataset is compliant with the CrowdStrike Parsing Standard (CPS). CPS defines normalized event fields and parser metadata conventions so that data from varied sources can be consistently categorized, searched, and used by shared content within Falcon LogScale. The **#event.dataset** field identifies the logical dataset to which an event belongs, such as a source-specific event stream or event category. Supplying this normalized value allows detections, dashboards, searches, and other content to distinguish related telemetry reliably without depending on vendor-specific raw-field names.

In CPS-aligned parsing, event metadata fields are prefixed with **#** and are populated as part of the parser's normalization process. **#event.dataset** is specifically part of the CPS event-field model and is used alongside other standardized event metadata, including fields such as **#event.kind** and **#ecs.version**, where applicable. Using the standard field consistently improves interoperability between parsers and makes downstream analysis more predictable. CrowdStrike's Falcon LogScale documentation describes parser development and normalized field practices in its Parsers documentation and provides broader implementation guidance in the Falcon LogScale documentation library.

QUESTION NO: 7

A parser needs to preserve the original third-party field name and also map it to an ECS-compatible field.

What is the best approach?

A. Delete the original field after mapping

B. Rename the original field to the ECS field

C. Keep the original Vendor field and assign its value to a new ECS field

D. Store both values only in @rawstring

ANSWER: C

Explanation:

Keep the original Vendor field and assign its value to a new ECS field is the appropriate parser design because it satisfies both source fidelity and normalization requirements. The vendor-specific field retains the exact semantic context and naming supplied by the third-party data source. This is valuable for troubleshooting ingestion, validating parser behavior, supporting source-specific investigations, and retaining access to details that may not be fully represented by a common schema.

At the same time, copying or assigning the parsed value to the applicable ECS-compatible field makes the event useful for consistent searches, dashboards, correlations, and detections that operate across multiple data sources. ECS is designed to provide a common field model so that equivalent concepts can be queried consistently regardless of their original source format. Preserving the source field alongside the normalized field therefore supports both operational transparency and cross-source analytics without sacrificing either capability.

This approach aligns with the general ECS principle of mapping source data into standardized fields while retaining relevant source-specific context. See the Elastic Common Schema reference and the CrowdStrike Falcon LogScale documentation library for schema and parser guidance.