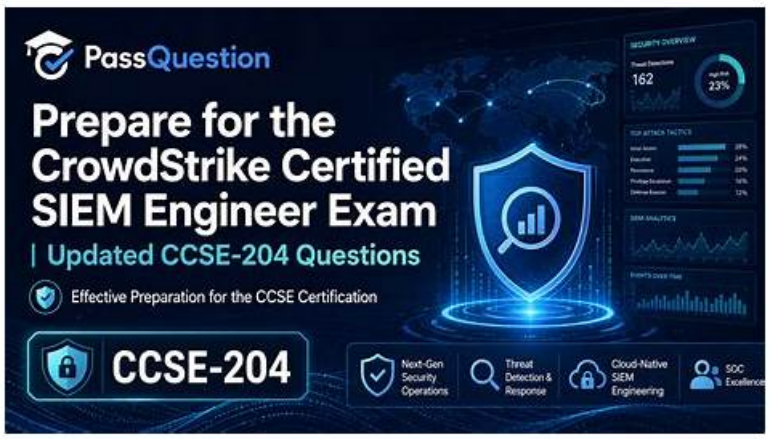
CrowdStrike CCSE-204 Valid Test Objectives & Latest CCSE-204 Test Preparation



Practice materials are typically seen as the tools of reviving, practicing and remembering necessary exam questions for the exam, spending much time on them you may improve the chance of winning. However, our CCSE-204 training materials can offer better condition than traditional practice materials and can be used effectively. We treat it as our major responsibility to offer help so our CCSE-204 Practice Guide can provide so much help, the most typical one is the efficiency of our CCSE-204 exam questions, which can help you pass the CCSE-204 exam only after studying for 20 to 30 hours.

CrowdStrike CCSE-204 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Administration and Maintenance	25%	- Access Control • 1. Authentication methods • 2. Role-based access - System Health Monitoring • 1. Storage management • 2. Performance tuning
Topic 2: Dashboards and Reporting	20%	- Visualization Techniques • 1. Report scheduling • 2. Dashboard creation
Topic 3: Search and Investigation	30%	- Incident Investigation • 1. Timeline analysis • 2. Evidence gathering - Search Processing Language (SPL) • 1. Basic search commands • 2. Statistical functions

Topic 4: Log Management and Data Collection	25%	- Data Sources and Connectors • 1. Third-party integrations • 2. Cloud-native log sources - Data Normalization • 1. Parsing rules • 2. Common Information Model (CIM)

>> CrowdStrike CCSE-204 Valid Test Objectives <<

Choosing CCSE-204 Valid Test Objectives - Say Goodbye to CrowdStrike Certified SIEM Engineer

There are a number of distinctions of our CCSE-204 Exam Questions that make it superior to those offered in the market. Firstly, you will find that there are three different vesions of our CCSE-204 learning guide: the PDF, Software and APP online. Though the content is the same, but the displays are all different. And you can study in all kind of conditions if you have three of them. Secondly, the prices of every version are favourable. And you can buy the Value Pack with discounted price.

CrowdStrike Certified SIEM Engineer Sample Questions (Q44-Q49):

NEW QUESTION # 44
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 --status
- D. logscale-collector check

Answer: B

Explanation:
The logscale-collector monitor command provides a real-time view of the Log Collector's operation, showing the status of sources and sinks to help ensure data is being ingested and processed correctly.

NEW QUESTION # 45
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 write permissions only
- C. NGSIEM with both read and write permissions
- D. NGSIEM with read permissions only

Answer: C

Explanation:
The correct answer is C. NGSIEM with both read and write permissions .
CrowdStrike integration guidance for querying Next-Gen SIEM event data states that the API client needs the NGSIEM scope with both Read and Write permissions . The documentation explains why: Write is required to create the search/query job, and Read is required to retrieve the query results.
Why the other options are incorrect:
A is incorrect because the documented requirement is Read + Write ; there is no documented "execute" permission in the cited guidance. B is incorrect because read-only access would let you read results but not create the query job. D is incorrect because write-only access would let you submit the job but not read the results back.

NEW QUESTION # 46
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. Edit in Search view
- B. Styling options
- C. Interactions options

Answer: B

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.

NEW QUESTION # 47
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. Custom role
- B. NG SIEM Analyst
- C. Falcon Security Lead
- D. NG SIEM Security Lead

Answer: A

Explanation:
The best answer is D. Custom role .
CrowdStrike documentation for Store app integrations states that the Falcon Administrator role is required to enable apps and plugins in the CrowdStrike Store, which is the administrative side of connector configuration. That shows connector configuration is a privileged task.
At the same time, Falcon Fusion SOAR is the workflow automation capability used to create SOAR automations in the Falcon platform. CrowdStrike describes Fusion SOAR as the workflow engine used to build and run workflows and automate actions across security processes.
Because the question specifically asks for the role that allows both actions while maintaining least privilege
, the most appropriate choice is a custom role that grants only the required permissions instead of assigning a broader built-in administrative role. This is an inference from the documented permission model: connector
/plugin setup requires elevated permissions, and SOAR workflow creation is a separate capability, so a narrowly scoped custom role is the least-privilege answer among the options.
Why the other options are not the best answer:
NG SIEM Analyst is intended for analyst activity, not configuration and automation administration. Falcon Security Lead is broader and not the most precise least-privilege answer. NG SIEM Security Lead may have wide SIEM access, but the question asks for the option that best maintains least privilege across both connector configuration and SOAR automation creation; that is better satisfied by a custom role . This conclusion is based on the documented need for elevated permissions for plugin configuration and the separate SOAR workflow capability.

NEW QUESTION # 48
An event has the following fields:

```
#event_simpleName: ProcessRollup2
CommandLine: "C:\Windows\System32\OpenSSH\ssh.exe" -R :12121 -N user1@8.8.8.8 -p 443
ComputerName: Workstation123
FileName: ssh.exe
ImageFileName: C:\Windows\System32\OpenSSH\ssh.exe
UserName: bsmith
```

Which CQL query will output the frequency of a unique set of ComputerName, UserName, CommandLine?

- A. #event_simpleName = ProcessRollup2
  | FileName = ssh.exe
  | CommandLine = /\s-R\s.+\s-p/

| groupBy([ComputerName, UserName, CommandLine], function=count())

- B. #event_simpleName = ProcessRollup2
  | FileName = ssh.exe
  | CommandLine = /\s-R\s.+\s-p/
  | table([ComputerName, UserName, CommandLine], function=count())
- C. #event_simpleName = ProcessRollup2 FileName = ssh.exe CommandLine = /\s-R\s.+\s-p/ | groupBy ([ComputerName, UserName, CommandLine])
- D. #event_simpleName = ProcessRollup2 FileName = ssh.exe CommandLine = /\s-R\s.+\s-p/ | table ([ComputerName, UserName, CommandLine]) | count()

Answer: A

Explanation:
CrowdStrike LogScale documentation states that groupBy() is used to group events by one or more specified fields, similar to SQL GROUP BY. The documentation also says the function parameter accepts aggregate functions, and its default is count(as=_count). That means the query that explicitly groups by ComputerName, UserName, and CommandLine and applies function=count() is the correct way to output the frequency of each unique combination of those three fields.
Why the other options are incorrect:
A is incorrect because table() formats output rows but does not aggregate unique combinations into frequencies the way groupBy() does. Adding count() after table() does not produce grouped counts for each unique triplet. B is incorrect because table() is not the aggregation function documented for grouped frequency counting; groupBy() is. D is close, but it relies on the default count behavior rather than explicitly specifying function=count(). Since the question asks which query will output the frequency of a unique set, C is the most correct and explicit choice.

NEW QUESTION # 49
.....

CCSE-204 □ and download it for free immediately on ▸ www.pdfvce.com ◂ □CCSE-204 Official Study Guide

- Exam Dumps CCSE-204 Pdf □ Valid CCSE-204 Exam Question □ New CCSE-204 Braindumps Questions □ Search for ➤ CCSE-204 □ and obtain a free download on 【 www.verifieddumps.com 】 □Latest Braindumps CCSE-204 Ebook
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes