CrowdStrike
CCSE-204
CrowdStrike SIEM Engineer

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

Which troubleshooting step is most effective when a parser intermittently fails to extract values from certain log lines?

A. Delete and re-add the data connector
B. Increase collector CPU and memory allocation
C. Re-clone the parser to reset all settings
D. Review the parser's regex expressions for optional fields

Answer: D

Question: 2

A SOC engineer is asked to create a custom dashboard panel that highlights failed login attempts correlated with geolocation dat
a. Which additional component is required?
A. A lookup file mapping IP ranges to locations
B. A parsing rule to remove all IP fields
C. Falcon Data Replicator for exporting logs
D. A new user role with admin rights

Answer: A

Question: 3

Which Python SDK is officially supported for interacting with CrowdStrike APIs in automation workflows?

A. PyFalcon
B. Boto3
C. FalconPy
D. Requests

Answer: C

Question: 4

A security engineer is tasked with creating a new custom role that allows access to ingestion dashboards but prevents modification of correlation rules. Which step must they take first?

A. Assign the Investigator role and disable write access
B. Clone the default role most similar to the intended permissions
C. Create a new role from scratch with no base permissions
D. Enable the Administrator role and manually deselect correlation permissions

Answer: B

Question: 5

While reviewing SIEM access logs, an admin notices repeated failed login attempts from a user account belonging to a former employee. What should be the immediate action?

A. Reset the user's password and notify them
B. Assign the account to a generic "Inactive Users" role
C. Leave it as is since the employee is no longer active
D. Disable or remove the user account from Falcon SIEM immediately

Answer: D

Question: 6

A SOC engineer is tasked with testing a new parser. Which is the best practice for validating it?

A. Deploy the parser directly into production and monitor results
B. Create parser test cases with sample log events before production use
C. Bypass parser validation since logs can be fixed later in queries
D. Only test parsing by reviewing ingestion dashboards

Answer: B

Question: 7

An organization wants to assign the minimum necessary privileges to a SOC analyst who only needs to view dashboards and investigate alerts in Falcon SIEM. Which predefined role should be assigned?

A. Administrator
B. Investigator
C. Detection Analyst
D. Content Creator

Answer: C

Question: 8

A custom parser was deployed successfully, but users report that dashboards show “Unknown Field” in place of expected values. What is the most probable reason?

A. The parser was cloned instead of built from scratch
B. The field was not properly mapped to the Falcon schema
C. The ingestion rate exceeded the collector’s EPS capacity
D. A default parser was accidentally left active

Answer: B

Question: 9

Which Falcon feature enables SOC teams to build automated workflows for common incident response actions like isolating hosts or blocking IPs?

A. Falcon Fusion SOAR
B. Falcon Data Replicator
C. Lookup File Manager
D. CQL Queries

Answer: A

Question: 10

An engineer wants to design a CQL query that filters failed logins and groups them by source IP. Which function is most appropriate?

A. join
B. lookup
C. group by
D. parse_json

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/