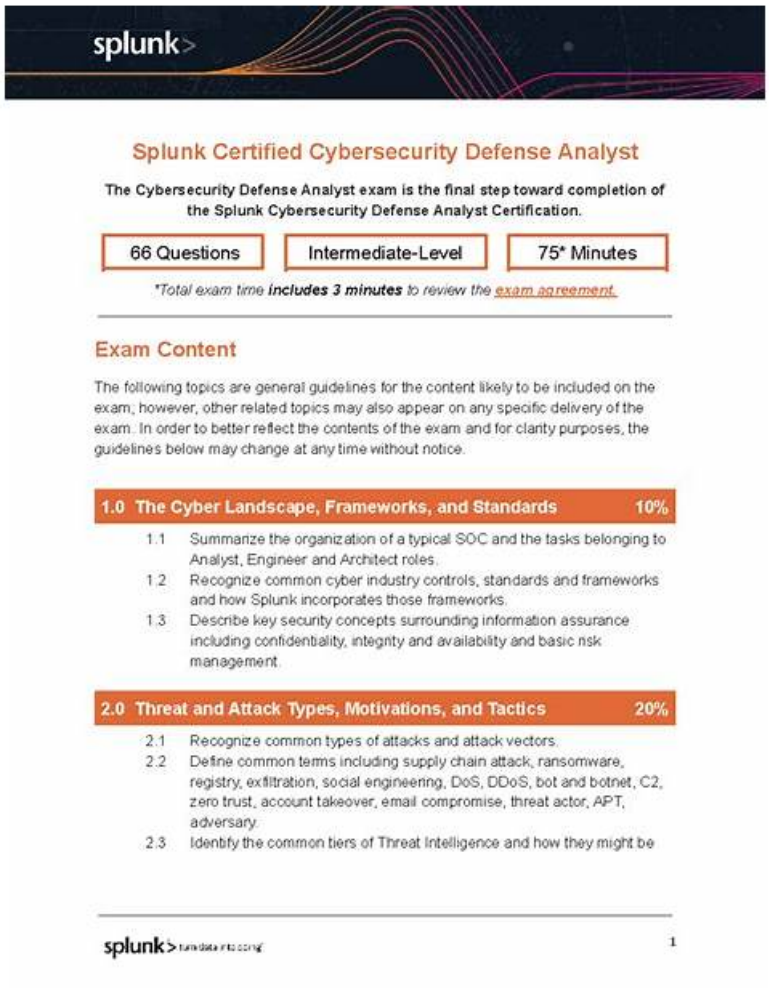
High Effective Splunk Certified Cybersecurity Defense Engineer Test Braindumps Make the Most of Your Free Time



splunk>

Splunk Certified Cybersecurity Defense Analyst

The Cybersecurity Defense Analyst exam is the final step toward completion of the Splunk Cybersecurity Defense Analyst Certification.

66 Questions | Intermediate-Level | 75* Minutes

*Total exam time **includes 3 minutes** to review the exam agreement.

Exam Content

The following topics are general guidelines for the content likely to be included on the exam, however, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0 The Cyber Landscape, Frameworks, and Standards 10%

1.1 Summarize the organization of a typical SOC and the tasks belonging to Analyst, Engineer and Architect roles.
1.2 Recognize common cyber industry controls, standards and frameworks and how Splunk incorporates those frameworks.
1.3 Describe key security concepts surrounding information assurance including confidentiality, integrity and availability and basic risk management.

2.0 Threat and Attack Types, Motivations, and Tactics 20%

2.1 Recognize common types of attacks and attack vectors.
2.2 Define common terms including supply chain attack, ransomware, registry, exfiltration, social engineering, DoS, DDoS, bot and botnet, C2, zero trust, account takeover, email compromise, threat actor, APT, adversary.
2.3 Identify the common tiers of Threat Intelligence and how they might be

splunk> turn data into doing

1

BONUS!!! Download part of Dumpleader SPLK-5002 dumps for free: https://drive.google.com/open?id=1yaPQQr4RpO0pcx5N5sUZdvupDOS3djg9

The Splunk SPLK-5002 practice test questions prep material has actual Splunk SPLK-5002 exam questions for our customers so they don't face any hurdles while preparing for Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) certification exam. The study material is made by professionals while thinking about our users. We have made the product user-friendly so it will be an easy-to-use learning material. We even guarantee our users that if they couldn't pass the Splunk SPLK-5002 Certification Exam on the first try with their efforts, they can claim a full refund of their payment from us (terms and conditions apply).

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details
Topic 1	• Detection Engineering: This section evaluates the expertise of Threat Hunters and SOC Engineers in developing and refining security detections. Topics include creating and tuning correlation searches, integrating contextual data into detections, applying risk-based modifiers, generating actionable Notable Events, and managing the lifecycle of detection rules to adapt to evolving threats.

Topic 2	• Automation and Efficiency: This section assesses Automation Engineers and SOAR Specialists in streamlining security operations. It covers developing automation for SOPs, optimizing case management workflows, utilizing REST APIs, designing SOAR playbooks for response automation, and evaluating integrations between Splunk Enterprise Security and SOAR tools.
Topic 3	• Auditing and Reporting on Security Programs: This section tests Auditors and Security Architects on validating and communicating program effectiveness. It includes designing security metrics, generating compliance reports, and building dashboards to visualize program performance and vulnerabilities for stakeholders.
Topic 4	• Building Effective Security Processes and Programs: This section targets Security Program Managers and Compliance Officers, focusing on operationalizing security workflows. It involves researching and integrating threat intelligence, applying risk and detection prioritization methodologies, and developing documentation or standard operating procedures (SOPs) to maintain robust security practices.
Topic 5	• Data Engineering: This section of the exam measures the skills of Security Analysts and Cybersecurity Engineers and covers foundational data management tasks. It includes performing data review and analysis, creating and maintaining efficient data indexing, and applying Splunk methods for data normalization to ensure structured and usable datasets for security operations.

Training SPLK-5002 Pdf, New SPLK-5002 Study Materials

As we all know, time for preparing a exam is quite tight. Once you have signed up for the exam, you need to prepare. Therefore improving the efficiency is quite necessary. Our SPLK-5002 training materials include the main knowledge point of the exam, which will help you to know the main knowledge. Besides the professionals check the SPLK-5002 at time, it can ensure the accuracy of the answers. Therefore, please make it easy to use the SPLK-5002 training materials freely.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q26-Q31):

NEW QUESTION # 26
An engineer is examining a correlation search as a part of a detection review, and sees that it is configured in the following fashion:

Which of the following is true about this configuration?

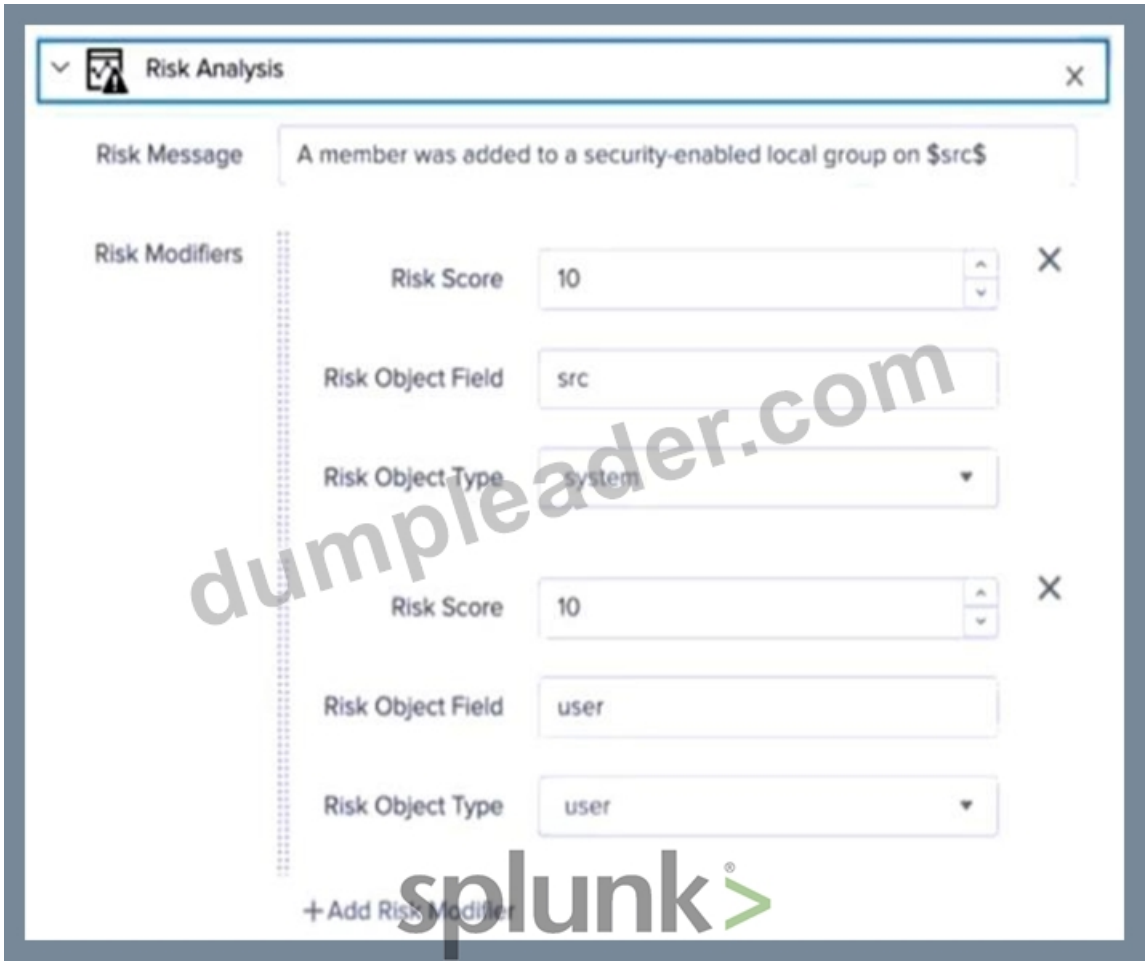
- A. The risk modifiers should be adjusted for an hour of data.
- B. The search will run as prescribed without issue every 30 minutes.
- C. There could be missing data as the search schedule is not ingesting data properly.
- D. There could be missing findings as the search frequency and time range are improperly configured.

Answer: D

Explanation:
The correlation search is scheduled to run every 2 minutes (*/2 * * * *) but is querying a 60-minute window (earliest = -60m@m). This large mismatch between the time range and the execution frequency is considered an improper configuration for ES correlation

searches.
Such a configuration can lead to inconsistent detection behavior, including missed or duplicate findings, because the search continually reprocesses a very large window using a very short execution interval.

NEW QUESTION # 27
Based on this example image, if it is detected that a member has been added to a security- enabled local group, how many risk events will be created?



- A. 0
- B. 1
- C. 2
- D. 3

Answer: A

Explanation:
In the example, there are two risk modifiers configured: one for the system (src) and one for the user. Each modifier creates a separate risk event with a score of 10. Therefore, the detection will generate 2 risk events in total.

NEW QUESTION # 28
A cyber defense engineer plays a role in maintaining a secure SOAR Cloud configuration. Which network security statement is correct about SOAR Cloud?

- A. The Automation Broker initiates an outbound SSL connection to Splunk Cloud, and also initiates an outbound connection to the managed endpoints.
- B. The Automation Broker initiates an outbound SSL connection to Splunk Cloud, and the managed endpoint initiates an outbound connection to the Automation Broker.
- C. Splunk Cloud initiates an outbound SSL connection to both the Automation Broker and managed endpoints.

- D. The Automation Broker initiates an inbound SSL connection to Splunk Cloud, and also initiates an outbound connection to the managed endpoints.

Answer: A

Explanation:
In Splunk SOAR Cloud, the Automation Broker is responsible for maintaining connectivity. It initiates an outbound SSL connection to Splunk Cloud (so no inbound firewall rules are needed) and also makes outbound connections to the managed endpoints to execute playbook actions securely.

NEW QUESTION # 29
Which of the following cURL commands would allow an engineer to effectively disable the REST API endpoint they've been utilizing for testing a detection named TestSearchDevelopment?

- A. curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable -X PUT
- B. Splunk endpoints cannot be disabled.
- C. curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable -X POST
- D. curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/ -X DELETE

Answer: C

Explanation:
To disable a saved search (detection) via the Splunk REST API, the correct syntax is a POST request to the .../disable endpoint. Thus, the proper cURL command is curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable -X POST

NEW QUESTION # 30
When should a detection be reviewed or retuned after deployment?

- A. As defined by the established detection lifecycle.
- B. Only if it has generated a large amount of false positives.
- C. Every 30 days.
- D. Only if it hasn't generated a finding after several weeks.

Answer: A

Explanation:
A detection should be reviewed or retuned as defined by the established detection lifecycle (DDLC). This ensures detections are consistently evaluated for accuracy, effectiveness, and alignment with evolving threats, rather than only reacting to false positives or inactivity.

NEW QUESTION # 31
.....

SPLK-5002 Braindumps

- Reliable SPLK-5002 Exam Braindumps - Free PDF Quiz 2026 First-grade Splunk Training SPLK-5002 Pdf □ Immediately open ⇛ www.pdfvce.com ⇚ and search for 「 SPLK-5002 」 to obtain a free download □Valid Test SPLK-5002 Fee
- Free PDF Splunk SPLK-5002 - Marvelous Reliable Splunk Certified Cybersecurity Defense Engineer Exam Braindumps □ □ Search for ➽ SPLK-5002 □ and easily obtain a free download on ➡ www.prep4away.com □□□ □SPLK-5002 Valuable Feedback
- Valid SPLK-5002 Dumps Demo □ SPLK-5002 Free Sample Questions □ SPLK-5002 Practice Guide □ Search for { SPLK-5002 } on （ www.pdfvce.com ） immediately to obtain a free download □Valid Dumps SPLK-5002 Files
- Free PDF Quiz 2026 Splunk SPLK-5002: Professional Reliable Splunk Certified Cybersecurity Defense Engineer Exam Braindumps □ Search for ➠ SPLK-5002 □ and download exam materials for free through 【 www.prep4away.com 】 □Reliable SPLK-5002 Braindumps
- SPLK-5002 Free Sample Questions □ SPLK-5002 Valid Test Vce Free □ SPLK-5002 Reliable Study Guide □ Download ▹ SPLK-5002 ◃ for free by simply searching on ▹ www.pdfvce.com ◃ □Reliable SPLK-5002 Exam Sample
- Valid Dumps SPLK-5002 Files □ Exam SPLK-5002 Guide □ SPLK-5002 Latest Exam Discount □ Go to website { www.dumpsmaterials.com } open and search for ➤ SPLK-5002 □ to download for free □Valid Dumps SPLK-5002 Files
- Reliable SPLK-5002 Exam Braindumps - Free PDF Quiz 2026 First-grade Splunk Training SPLK-5002 Pdf □ Search for ➥ SPLK-5002 □ and download it for free on ✔ www.pdfvce.com □✔□ website □SPLK-5002 Practice Guide
- Valid Dumps SPLK-5002 Files □ Braindumps SPLK-5002 Torrent □ Valid SPLK-5002 Dumps Demo □ Search for ➥ SPLK-5002 □ and download exam materials for free through ➡ www.dumpsmaterials.com □□□ □SPLK-5002 Reliable Test Dumps
- SPLK-5002 Practice Exams (Web-Based and Desktop) Software □ Search for □ SPLK-5002 □ and easily obtain a free download on ▹ www.pdfvce.com ◃ □Reliable SPLK-5002 Braindumps
- Reliable SPLK-5002 Exam Braindumps - Free PDF Quiz 2026 First-grade Splunk Training SPLK-5002 Pdf □ Search for 【 SPLK-5002 】 and download it for free immediately on ✔ www.testkingpass.com □✔□ □SPLK-5002 Latest Exam Discount
- amieuals552035.blazingblog.com, learning.d6driveresponsibly.it, bookmarkboom.com, roryoair466977.bloggosite.com, esmeedbaf307835.blogdeazar.com, laraptmn038088.fare-blog.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, aliviaudfw373994.blogars.com, adsbookmark.com, apollobookmarks.com, Disposable vapes

What's more, part of that Dumpleader SPLK-5002 dumps now are free: https://drive.google.com/open?id=1yaPQQr4RpO0pcx5N5sUZdvupDOS3djg9