Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

SPLK-3001 Dumps
SPLK-3001 Braindumps
SPLK-3001 Real Questions
SPLK-3001 Practice Test
SPLK-3001 Actual Questions

PASS

Splunk

SPLK-3001

Splunk Enterprise Security Certified Admin

Question: 59

The Add-On Builder creates Splunk Apps that start with what?
A . DA
B . SA
C . TA
D . App-

Answer: C

Explanation:

Reference: https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/

Question: 60

When investigating, what is the best way to store a newly-found IOC?
A . Paste it into Notepad.
B . Click the “Add IOC” button.
C . Click the “Add Artifact” button.
D . Add it in a text note to the investigation.

Answer: B

Question: 61

What feature of Enterprise Security downloads threat intelligence data from a web server?
A . Threat Service Manager
B . Threat Download Manager
C . Threat Intelligence Parser
D . Threat Intelligence Enforcement

Answer: B

Question: 62

Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?
A . VIP
B . Priority
C . Importance
D . Criticality

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

Question: 63

Which argument to the | tstats command restricts the search to summarized data only?
A . summaries=t
B . summaries=all
C . summariesonly=t
D . summariesonly=all

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

Question: 64

Which setting is used in indexes.confto specify alternate locations for accelerated storage?
A . thawedPath
B . tstatsHomePath
C . summaryHomePath
D . warmToColdScript

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

Question: 65

Which of the following are examples of sources for events in the endpoint security domain dashboards?
A . REST API invocations.
B . Investigation final results status.
C . Workstations, notebooks, and point-of-sale systems.

D . Lifecycle auditing of incidents, from assignment to resolution.

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

Question: 66

Which of the following is a way to test for a property normalized data model?
A . Use Audit -> Normalization Audit and check the Errors panel.
B . Run a | datamodelsearch, compare results to the CIM documentation for the datamodel.
C . Run a | loadjobsearch, look at tag values and compare them to known tags based on the encoding.
D . Run a | datamodelsearch and compare the results to the list of data models in the ES normalization guide.

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/ UsetheCIMtonormalizedataatsearchtime

Question: 67

In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?
A . Save the settings.
B . Apply the correct tags.
C . Run the correct search.
D . Visit the CIM dashboard.

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSECdata

Question: 68

What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?
A . ess_user
B . ess_admin
C . ess_analyst
D . ess_reviewer

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Triagenotableevents

Question: 69

When creating custom correlation searches, what format is used to embed field values in the title, description, and drill-down fields of a notable event?
A . $fieldname$
B . “fieldname”
C . %fieldname%
D . _fieldname_

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

Question: 70

What does the risk framework add to an object (user, server or other type) to indicate increased risk?
A . An urgency.
B . A risk profile.
C . An aggregation.
D . A numeric score.

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskScoring

Question: 71

DRAG DROP

You are implementing Dynamics 365 Customer Service for your company.

The company is deciding whether to use an on-premises or online implementation. One of the biggest concerns is about disaster recovery processes.

You need to explain how each system would be recovered with minimal effort and loss of data in case of a disaster.

Which recovery method should you use? To answer, drag the appropriate recovery methods to the correct location. Each recovery method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.

Answer Area

Recovery methods	Location	Recovery method
Back up databases to Microsoft Azure daily and then restore to new servers.	On-premises	
Promote Sandbox to production.	Online	
Use an included feature.		
Replicate the environment weekly to backup servers.		

Answer:

Answer Area

Recovery methods	Location	Recovery method
Back up databases to Microsoft Azure daily and then restore to new servers.	On-premises	Back up databases to Microsoft Azure daily and then restore to new servers.
Promote Sandbox to production.	Online	Use an included feature.
Use an included feature.		
Replicate the environment weekly to backup servers.		

Explanation:

Reference:

https://docs.microsoft.com/en-gb/power-platform/admin/backup-restore-environments

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*