Splunk.SPLK-3001.v2022-08-25.q95

□□□□:	SPLK-3001
□□□□:	Splunk Enterprise Security Certified Admin Exam
□□□:	Splunk
□□ □□ □□□:	95
□□:	v2022-08-25
# □□ □:	1875
# □□ □□□:	950
https://www.krdump.com/Splunk.SPLK-3001.v2022-08-25.q95.html	

NEW QUESTION: 1
□□ □□ ID □□□ □□ □□ □□□ □□□ □□□□ □□□□□ □□□□ □□□□ □□□□□?
A. VIP
B. □□□□
C. □□□
D. □□□
Answer: B (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION: 2
□□ □□ □□□ □□□□ Splunk_TA_ForIndexers □□□□ □□□ □ □□□ □ □□ □ □□ □□□ □□ □□□?
A. indexes.conf, props.conf, transforms.conf
B. input.conf, props.conf, transforms.conf
C. eventtypes.conf, indexes.conf, tags.conf
D. web.conf, props.conf, transforms.conf
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
□□ □ Web Intelligence □□□□□ □□□□□?
A. □□□□□ □□
B. □□□□ □□
C. □□□ :http □□□□ □□□□
D. HTTP □□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 4
□□ □ ES □□ □□□□□ □□□□□ □□ □□□ □□□□□?
A. □□□.
B. KV □□□.
C. □□ □□□□□.
D. □□ □□□.
Answer: C (LEAVE A REPLY)
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecuritySHC

NEW QUESTION: 5
□□□□□ CIM □ □ CIM □□ □□ □□□□□ □□□ □□□□□ □□ □□ □□ □□□ □□□□. □□ □□□□□□□ □□ □□□□□□□. □□□ □□□ □□□□ □□□□□ □□□□ □□□ ES □□□ □□ □□. ES□ □□□□ □□ □□ □□□ □□□□□?
A. □ □□ □□□ □□□□ □□□ ES□ □□□□□.
B. □□ □□ □□□ ES□ □□□□□.
C. □□ □□□ CPU □□ □□□ □□ □□□ ES□ □□□□□□.
D. □□ □□□□ CIM □□□ □□ □□□ □□ ES□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6
□□□ □□ □□ □□□ □□ □□□□ □□□□□?
A. cim_modactions
B. module_history
C. cim_adaptiveactions
D. module_action_history
Answer: A (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

NEW QUESTION: 7
□□ □□ □□□ □□□ □□□□□?
A. □□□□□ □□□□ □□ □□.
B. KV □□□ □□□□□ □□□ □□□□□.
C. □□ □□ □□ □□.
D. Threat_activity □□□□ □□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
ES □□□ □□□ □□□□□ □□ □□ □□□ □□□□□?
A. 1□
B. 15□

C. 1□□
D. 5□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
□□□□□ □□□ □□□□ □□□ □□□□□?
A. □□ □□ □□□ □□ □□□ □□ □□□.
B. □□ □□ □□ ID□ □□□ □□ □□ □ □□ □□ □□□ □□ □□□ □□□□□□.
C. □□ □□□□ □ □□ □□□.
D. □□ □□ □□□□ □□ □□ □□ □□ □□ □ □□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
Enterprise Security□ □□ □□□ □ □□□□ □□ □□□□□ □□□□ □□□□□□□?
A. □□ □□□ □□□
B. □□ □□□□ □□□
C. □□ □□□□□ □□
D. Therat □□ □□□
Answer: B (LEAVE A REPLY)
□□
"Threat Intelligence Framework□ □□□□□ □□ □ □□□□ □□□□□□ □ □□□□□ □□□ □□□ □ □□□ □□□□ □□□ □□(□□ □□□□□ □□□□)□ □□□□□. □ □□□ □□□ □□□□□□ Inputs.conf □□□ " □□ □□".

NEW QUESTION: 11
□□ □□ □□□□□ □□□□□ □□□ □□□□ □ □□ □□□□ □□□ □□□□□?
A. □□ -> □□□ □□ -> □□: □□ □□ □□
B. □□ -> □□□□ □□ -> □□□□ □□ □□ -> □□□ □□
C. □□ -> □□□□ □□ -> □□□□ □□ □□ -> □□□ □□
D. □□ -> □□□□ □□ -> □□ □□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
□□ □□ | tstats □□□ □□□ □□□ □□□□□ □□□□□?
A. □□=t
B. □□□=□□
C. □□□=t
D. □□=□□
Answer: (SHOW ANSWER)

NEW QUESTION: 13

□□□ □ □□ □□□ IOC□ □□□□ □□ □□ □□□ □□□□□?
A. "□□□□ □□" □□□ □□□□□.
B. □□□ □□□ □□□ □□□□□.
C. □□□□ □□□□□□.
D. "IOC □□" □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
□□□□□ □□□ □□□□ □□□ □□□□□?
A. □□ □□□□ □ □□ □□□.
B. □□ □□ □□□ □□ □□□ □□ □□□.
C. □□ □□ □□□□ □□ □□ □□ □□ □□ □ □□□.
D. □□ □□ □□ ID□ □□□ □□ □□ □ □□ □□ □□□ □□ □□□ □□□□□□.
Answer: D (LEAVE A REPLY)
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION: 15
□□ □ ES□□ □□□□ □□□ □□□ □□□□□? (□□ □□ □□ □□)
A. □
B. □□
C. □□
D. □□□□ □□□
Answer: (SHOW ANSWER)
□□:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

NEW QUESTION: 16
□□□□ ES □□□□ □□□□ □□□ □□ □□□□ □□□ □□□ □□□. □ □□ □□□ □□□□ □□ □ □□□□□?
A. □□□ □□□.
B. □□□ □□□ □□.
C. □□□ □□.
D. □□□ □□ □□.
Answer: B (LEAVE A REPLY)
□□:
https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-.html

SPLK-3001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-3001 □□! DumpTop □ □□ **SPLK-3001** □□ □□□ □□□□□□, DumpTop SPLK-3001 □□ □□□ □□□□□□□□ □

□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-3001 □□□ □□□□□.
https://www.dumptop.com/Splunk/SPLK-3001-dump.html (**101** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 17
□□ □□ □□□□□□ □□□□□ □□□ □□□□ □□ □ □□ □ □□□□□ □□ □□□ □□□□ □ □□?
A. ess_user
B. ess_reviewer
C. ess_analyst
D. ess_admin
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
□□ □□□□ □□□□ □□ □□□□ □□□□ □□□□□ □□□□ □□ Enterprise Security□ □□ □□ □□ □ □□ □□□□ □□ □□□□ □□□□ □□□□□ □□□□□?
A. □□□□ □□
B. □□□ □□□□□
C. □□ □□□□□
D. □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
□□ □□ □□□□□□ □□□□□ □□□ □□□□ □□ □ □□ □ □□□□□ □□ □□□ □□□□ □ □□?
A. ess_reviewer
B. ess_user
C. ess_analyst
D. ess_admin
Answer: C (LEAVE A REPLY)

NEW QUESTION: 20
□□□ □□ □□□ eventtype□ □□□□ □□ □□□ □□□ □□□ □ □□ □□□ □□□□□?
A. □□□ □□□□□.
B. □□□ □□□ □□□□□.
C. □□□ □□□ □□□□□.
D. CIM □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSEC □□□

NEW QUESTION: 21
□□ □ □ ES □□□ □□ □□ □□ □□ □□□ □□□ □□□□□?
A. □□ □□ □□□ □□□□□.
B. □□ □□ □□□ □□□□□.
C. □□□□ □□ □□□ □□□□ □□□□ □□□□.
D. □□□□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
□□□ □□ □□ □□□ □□□ □□□□□?
A. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments
B. KV □□□
C. □□□□□ □□□
D. □□ □□.csv □□
Answer: (SHOW ANSWER)

NEW QUESTION: 23
□□ □□□□ □□ □□□□ □□□, □□ □□ □□ □ □□ □□ □ □□ □□ □□□ □ □□□□?
A. □□ □□.
B. □□□ □□□□□□.
C. □□ □□□.
D. □□□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable

NEW QUESTION: 24
ES □□ □□ □□□ □□□□□ □□□ □□□ □□□□□?
A. □□ □□ □□
B. □□□ □□
C. □□ □□
D. □□ □□ □□□□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
□□□ □□ □□ □□ □□□ □□□ □ □□□□□ □□□□ □□, □□ □ □□□□ □□□ □□ □□ □□ □□ □ □□□□ □□□ □□□□□?
A. $□□□$
B. "□□□"
C. %□□□%
D. _□□□_
Answer: (SHOW ANSWER)

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

NEW QUESTION: 26
□□□□□ □□□□ □□□□ □□□□ □□ □□□ □ □□□ □□□□□?
A. □□ □□ □ □□.
B. □□□ □ □□□.
C. □□ □□ □ □□□.
D. □□ □□ □ □□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
□□ □□ ID □□□ □□ □□ □□□ □□□ □□□□ □□□□□ □□□□ □□□□ □□□□□?
A. VIP
B. □□□□
C. □□□
D. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
□□ □□ □□□□□ □□□□□ □□□ □□□□ □ □□ □□□□ □□□ □□□□□?
A. □□ -> □□□ □□ -> □□: □□ □□ □□
B. □□ -> □□□□ □□ -> □□□□ □□ □□ -> □□□ □□
C. □□ -> □□□□ □□ -> □□□□ □□ □□ -> □□□ □□
D. □□ -> □□□□ □□ -> □□ □□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
ES □□□□ □□□□ □□□□ .spl□ □□ □□□□ □□□□□. ES □□□□ □□□□□ □□□□ □□ □ □ □□ □□ □□□ □□□□□?
A. □ □ □□□ □□□□□ □□ □□ □□□□ □ □□□□ □□ □□□□□.
B. □□ □ □□□□□ □□ □□ □ □ □□□□ □□□□□.
C. □□□□ □□□ □□□ □ .spl □□□□ □□□□ □□□□.
D. □□□□ □□□ □□□ □□□ □ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30
□□ □□ □□□□□ □□□□□ □□□ □□□□ □ □□ □□□□ □□□ □□□□□?
A. □□ -> □□□□ □□ -> □□ □□□ □□
B. □□ -> □□□ □□ -> □□: □□ □□ □□
C. □□ -> □□□□ □□ -> □□□□ □□ □□ -> □□□ □□

D. □□ -> □□□□ □□ -> □□□□ □□ □□ -> □□□ □□
Answer: C (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables

NEW QUESTION: 31
□□ □□□□ □□□□ □□ □□□□ □□□□ □□□□□ □□□□ □□ Enterprise Security□ □□ □□ □□ □ □□ □□□□ □□ □□□□ □□□□ □□□□□ □□□□□?
A. □□ □□
B. □□□□ □□
C. □□□ □□□□□
D. □□ □□□□□
□□: (□□)
□□
Answer: A (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards

SPLK-3001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-3001 □□! DumpTop □ □□ **SPLK-3001** □□ □□□ □□□□□□, DumpTop SPLK-3001 □□ □□□ □□□□□□□□ □ □□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-3001 □□□ □□□□□.
https://www.dumptop.com/Splunk/SPLK-3001-dump.html (**101** Q&As Dumps, **30%OFF Special Discount:** **KrDump**)

NEW QUESTION: 32
□□ □□□ □□ □□ □□□ □□□□ □□□ □□□□□?
A. props, conf□□ tstatsHomePath □□ □□
B. □□□, conf□□ tstatsHomePath □□ □□
C. □□□□ □ □□ □□ □□□□, conf
D. □□□□ □□ □□□□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 33
CIM □□□ □□□ □□ □□□□□ □□ □□□□ □□□□□?
A. □□□□□ □□
B. □□ □ □□□□□
C. _□□ □ □□
D. □□ □□□
Answer: D (LEAVE A REPLY)

□□:
https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

NEW QUESTION: 34
□□ □□□ □□□ □ □□□?
A. ess_admin □□□□ □□.
B. □□ □□□□.
C. □□ □□□ □ ess-admin□□□.
D. □□□ □□□□ □□□.
Answer: A (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

NEW QUESTION: 35
ES □□□ □□ □□ □□□□ □□□□ □□□ □□□□□?
A. □□ -> □□ □□
B. □□ -> □□ -> □□
C. □□ -> □□□ □□□□□ -> □□ -> "□□□□□□ □□" □□
D. □□ -> □□□ □□□□□ -> □□ □□ -> SplunkEnterpriseSecuritySuite □□ □□ "□□□" □□
Answer: (SHOW ANSWER)
□□/□□:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizemenubar#Restore_the_default_navigation

NEW QUESTION: 36
□ □□□□ □□□□ □ □□ □□ □□□ □□□□ □□□□ □□□ □□□□□?
A. □□ □□
B. □□□
C. □□
D. □□
Answer: (SHOW ANSWER)
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

NEW QUESTION: 37
□□□□□ □□□□ □□ □□ ID□ □□□□ □□□ □□□ □□□□?
A. □□ □□□.
B. □□□ □□□□□.
C. □□ □□.
D. □□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38

Enterprise Security□ □□ □□□ □ □□□□ □□ □□□□□ □□□□ □□□□□□□?
A. □□ □□□□□ □□
B. Therat □□ □□□
C. □□ □□□ □□□
D. □□ □□□□ □□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
□□□□□ □□□□ □□ □□ ID□ □□□□ □□□ □□□ □□□□?
A. □□ □□.
B. □□□ □□□□□.
C. □□ □□□.
D. □□.
Answer: (SHOW ANSWER)
□□
https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

NEW QUESTION: 40
□□ □□□□□ □□ □□□ □□□□ □□ indexes.conf□□ □□ □□□ □□□□□?
A. tstatsHomePath
B. □□□ □□
C. □□ □□
D. □ToColdScript
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
□□□ □□ □□□□ □□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□□ □□□□. □□□ □□ □ □□ □□□ □□□ □□ □□ □□□ □□□ □□□□ □□□?
A. □□
B. □
C. □□
D. □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
□□ □ Splunk Enterprise Security□ □□□□ □□ □□□□ □□ □□ □□□ □□□□□?
A. SplunkWeb(8068), Splunk Management(8089), KV Store(8000)
B. SplunkWeb(8390), Splunk Management(8323), KV Store(8672)
C. SplunkWeb(8000), Splunk Management(8089), KV Store(8191)
D. SplunkWeb(8043), Splunk Management(8088), KV Store(8191)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
□□□ □□□ ID □□□ 'identity' □□ □□□□ □□ □□ □□□□ □□□□ □□ □□□□□?
A. □, □□□ □□.
B. □□
C. IP □□.
D. □□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
□□□□□ □□□ □□□ □□□□ □ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□□ □□□□.
B. □ □□.
C. □ □□ □□.
D. □□ □.
Answer: C (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

NEW QUESTION: 45
□□□ □□ □□□□ □□ □□ □□□ □□□ □□ □□ □□ □□□□ □□□□ □□□□. □□□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□□ □□□?
A. □
B. □□
C. □□
D. □□
Answer: (SHOW ANSWER)
□□:
https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches.html

NEW QUESTION: 46
ES □□□ □□□ □ □□ □□ □□ □ □□ □□□□□?
A. ES□ □□□□□.
B. □□□ □□□ □□□ □□□□□.
C. □□□ □□□□□ □□□□□.
D. □□ □□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
□□/□□:

SPLK-3001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-3001 □□! DumpTop □ □□ **SPLK-3001** □□ □□□ □□□□□□, DumpTop SPLK-3001 □□ □□□ □□□□□□□□ □ □□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-3001 □□□ □□□□□.
https://www.dumptop.com/Splunk/SPLK-3001-dump.html (**101** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 47
Enterprise Security□ □□□ □ □□ □□ □□ □□□ □□□□ □□□□ □□□ □□ □□ □ □□□□?
A. Splunk_DS_ForIndexers.spl
B. Splunk_ES_ForIndexers.spl
C. Splunk_SA_ForIndexers.spl
D. Splunk_TA_ForIndexers.spl
Answer: D (LEAVE A REPLY)
□□
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

NEW QUESTION: 48
□□ □ ES□ □□□□ □□ □□□ □□□ □□□□□?
A. □□ KV □□□.
B. □□ □□ □□□ □□□□□□□.
C. □□□□ □□□□□.
D. □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 49
□□□ □□ □□□□ □□ □□ □□□ □□□ □□ □□ □□ □□□□ □□□□ □□□□. □□□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□□ □□□?
A. □
B. □□
C. □□
D. □□
Answer: (SHOW ANSWER)

NEW QUESTION: 50
□□□□ □□□□ □□ □□ □□□□□□ □□□ □ □□□□□ □□□□ □□ □□□□ □□ □□□ □□ □□ □□□□□ "Nslookup" □□□ □□ □□□ □□□□□ □□□ □□□□.
□□□□ □ □□□ □□□□ □□ □□ □□□ □□□□ □□□?
A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup
B. □□ -> □□□ □□ -> □□: □□ □□ □□ -> □□□□□ -> □□ □□ -> Nslookup
C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup

D. Configure -> Type: Correlation Search -> Notable -> □□ □□ -> Nslookup
Answer: (SHOW ANSWER)

NEW QUESTION: 51
ES □□ □□ □□□ □□□□□ □□□ □□□ □□□□□?
A. □□ □□
B. □□ □□ □□□□□
C. □□ □□
D. □□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
□□ □□ □□□□□ □□□□□ □□□ □□□□ □ □□ □□□□ □□□ □□□□□?
A. □□ -> □□□□ □□ -> □□ □□□ □□
B. □□ -> □□□ □□ -> □□: □□ □□ □□
C. □□ -> □□□□ □□ -> □□□□ □□ □□ -> □□□ □□
D. □□ -> □□□□ □□ -> □□□□ □□ □□ -> □□□ □□
Answer: C (LEAVE A REPLY)
□□
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables

NEW QUESTION: 53
□ □□□ □□ □□ □□□ □□ □□ □□□□□□?

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

A. □□ □□□□□.
B. □□ □□□□□.
C. □□□ □□ □□□□□.
D. IP □□ □□.
Answer: (SHOW ANSWER)
□□/□□: https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector

NEW QUESTION: 54
□□ □□□ □□ □□ □□□ □□□□ □□ indexes.conf□□ □□ □□□ □□□□□?
A. □□ □□

B. tstatsHomePath
C. □□□ □□
D. warmToColdScript
Answer: (SHOW ANSWER)
□□/□□: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

NEW QUESTION: 55
□□ □□ □□□□□ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□ □□□ □□□□ □□□ □□□□ □□ □□.
B. □□ □□□□ □□□□ □□□□□ □□□ □□□.
C. □□□ □□.
D. □□ □□□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 56
□□ □ □□ □□□□ □□□□□ □□□□ □□ □□□ □□□□ □□ □□□□ ES □□□ □□□□□?
A. □□ □□ □□□.
B. □□ □□ □□.
C. □□ □□□□ □□□□.
D. □□□□ □□□□□ □□□□.
Answer: (SHOW ANSWER)
□□:
https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html

NEW QUESTION: 57
□□□□ ES□ □□□□ □□ □□□ □□ □□□ □□□□□□□ □□□□. □□ □□□□ OS, CPU □ RAM□ □□ □□ □□ □□ □□□ □□□□□?
A. OS: 32□□, RAM: 16MB, CPU: 12□□
B. OS: 64□□, RAM: 32MB, CPU: 12□□
C. OS: 64□□, RAM: 12MB, CPU: 16□□
D. OS: 64□□, RAM: 32MB, CPU: 16□□
Answer: C (LEAVE A REPLY)
□□/□□: https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware

NEW QUESTION: 58
□□□□□ □□□□ □□ □□ ID□ □□□□ □□□ □□□ □□□□?
A. □□ □□.
B. □□□ □□□□□.
C. □□ □□□.
D. □□.
Answer: B (LEAVE A REPLY)

□□/□□: https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

NEW QUESTION: 59
□□ □□□ □□ □□□□ ES□□ □□□□ □□□ □ □□□□?
A. □□□ □□□□
B. □□ -> □□□ □□
C. □□□□ □□□ □□□□
D. □□ □□ -> ES -> □□□□
Answer: B (LEAVE A REPLY)
□□
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export

NEW QUESTION: 60
□□ □ Splunk Enterprise Security□ □□□□ □□ □□□□ □□ □□ □□□ □□□□□?
A. SplunkWeb(8000), Splunk Management(8089), KV Store(8191)
B. SplunkWeb(8088), Splunk Management(8089), KV Store(8000)
C. SplunkWeb(8043), Splunk Management(8088), KV Store(8191)
D. SplunkWeb(8386), Splunk Management(8926), KV Store(8106)
Answer: A (LEAVE A REPLY)
□□/□□: https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

NEW QUESTION: 61
□□ □ Splunk Enterprise Security□ □□ □□□ □□□□ □□□ □ □□ □□ □□□□□?
A. .spl□ □□□
B. CIM_□ □□□
C. Splunk_TA_□ □□□
D. TECH_□ □□□
Answer: C (LEAVE A REPLY)

SPLK-3001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-3001 □□! DumpTop □ □□ **SPLK-3001** □□ □□□ □□□□□□, DumpTop SPLK-3001 □□ □□□ □□□□□□□□ □ □□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-3001 □□□ □□□□□.
https://www.dumptop.com/Splunk/SPLK-3001-dump.html (**101** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 62
□□ □ □□□□□ □□ □□□ □□□□□ □□□ □□ □□ □□□□□?
A. REST API □□.
B. □□ □□ □□ □□.

C. □□□□□□, □□□ □ POS □□□.
D. □□□□ □□□□ □□□□□ □□ □□ □□.
Answer: D (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

NEW QUESTION: 63
□□□ □□ □□□ eventtype□ □□□□ □□ □□□ □□□ □□□ □ □□ □□□ □□□□□?
A. CIM □□□□□ □□□□□.
B. □□□ □□□ □□□□□.
C. □□□ □□□ □□□□□.
D. □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
□□ □ ES□ □□□□□ □ □□ □□ □□□□□ □□□ □□□□□? (□□ □□ □□ □□)
A. □□□
B. SplunkEnterpriseThreatGenerator
C. VulnScanSPL
D. □□□/□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 65
□□□□ ES□ □□□□ □□ □□□ □□ □□□ □□□□□□□ □□□□. □□ □□□□ OS, CPU □ RAM□ □□ □□ □□ □□ □□□ □□□□□?
A. OS: 32□□, RAM: 16MB, CPU: 12□□
B. OS: 64□□, RAM: 32MB, CPU: 12□□
C. OS: 64□□, RAM: 12MB, CPU: 16□□
D. OS: 64□□, RAM: 32MB, CPU: 16□□
Answer: (SHOW ANSWER)
□□:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware

NEW QUESTION: 66
□□ □□ □□□□□ □□□ □□□□□?
A. □□ □□ □□□ □ □□.
B. □□□□□ □□□ □□ □□ □□□ □□□□□.
C. SOC□□ □□ □□ □□ □□.
D. □□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)

Security Posture □□□□□ SOC(Security Operations Center)□ □□□□□ □□□ □□□ □□ □□□□ □ □□□□□ □□□□ □□ □□ □□□ □□□□ □□□□□ □□□□□□□. □ □□□□□ □□ 24□□ □□□ □□ □□□□ □□ 24□□ □□□ □□□ □□ □□□□ □□□ □□□ □□ □ □□□□□ □□□ □□.
□□: https://docs.splunk.com/Documentation/ES/6.1.0/User/SecurityPosturedashboard

NEW QUESTION: 67
Enterprise Security□ □□□□□ □□ □□ □□□ □□ □□□□ □□□□ □□□□□?
A. Tstats
B. □□□ □□
C. KV □□□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Enterprise Security□ □□ □□ □□ □ □□□ □□□ IP □□□ □□ □□□ □□□ □□ □□□□□?
A. □□ □□□□□.
B. □□□.
C. □□.
D. □□ □□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
□□ □ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□ □□□□ □□□□□.
B. □□ □□ □□ □□□□□□□.
C. □□ □□□ □□ Python □□□□ □□□□□.
D. MongoDB.com□□ □□ □□□ KV Store□ □□□□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70
Enterprise Security□ □□□□□ □□ □□ □□□ □□ □□□□ □□□□ □□□□□?
A. Tstats
B. KV □□□
C. □□□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
□□:
https://docs.splunk.com/Splexicon:Knowledgeobject

NEW QUESTION: 71

□ □□□□ □□□□ □ □□ □□ □□□ □□□□ □□□□ □□□ □□□□□?
A. □□ □□
B. □□□
C. □□
D. □□
Answer: (SHOW ANSWER)

NEW QUESTION: 72
□□□□ □□□□ □□ □□ □□□□□□ □□□ □ □□□□□ □□□□ □□ □□□□ □□ □□□ □□ □□ □□□□□ "Nslookup" □□□ □□ □□□ □□□□□ □□□ □□□□. □□□□ □ □□□ □□□□ □□ □□ □□□ □□□□ □□□?
A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup
B. Configure -> Type: Correlation Search -> Notable -> □□ □□ -> Nslookup
C. □□ -> □□□ □□ -> □□: □□ □□ □□ -> □□ □□ -> □□ □□
-> □□
D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup
Answer: C (LEAVE A REPLY)

NEW QUESTION: 73
ES□ □□□ □ □□□□ ss_usor □□□ Leers□ □□□□□ □□□□ □□ □□□ □□□□□□. □□□ □ □□□ □□□□ □□□ □□ □□□□ □□□ □□□□□ □□□ □ □□□ □□□ □□□□□?
A. Splunk □□□ □□□□ ess_user □□□ □□□□ edit_notabie_events □□□ □□□□□.
B. Enterprise Security□□ ess_user □□□ □□□ □□□□□ □□□ □□□ □□□□□.
C. □□ □□ □□□ □□ □□□ □□□□□. □□□ □□□ □□ □□ □□□□ ess_user□ □□□□□.
D. □□ □□ □□□ □□□ □□□ □□□□□. □□ □□□ □□ □□ □□□□ ess_user□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 74
"□□ □□"□ "□□□ □□ □□"□ □□ □□□ □□□ □□□□□. □□□ □□□□?
A. □□ □□□ □□□□□ □□□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□ □□□□□.
B. □□ □□□ □□□□□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□□□.
C. □□ □□□ □□ □□□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□□□.
D. □□ □□□ □□□□□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
□□/□□: https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

NEW QUESTION: 75
□□ □□ ID □□□ □□ □□ □□□ □□□ □□□□ □□□□□ □□□□ □□□□ □□□□□?
A. VIP
B. □□□□

C. □□□
D. □□□
Answer: B (LEAVE A REPLY)
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION: 76
□□ □□□□ □□ □□□□ □□□, □□ □□ □□ □ □□ □□ □ □□ □□ □□□ □ □□□□?
A. □□ □□.
B. □□□ □□□□□□.
C. □□ □□□.
D. □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable

SPLK-3001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-3001 □□! DumpTop □ □□ **SPLK-3001** □□ □□□ □□□□□□, DumpTop SPLK-3001 □□ □□□ □□□□□□□□ □ □□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-3001 □□□ □□□□□.
https://www.dumptop.com/Splunk/SPLK-3001-dump.html (**101** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 77
□□ □ □□ □□□ ES□ □□□□ □□ □□□ □□□□□?
A. □□ □□ □□□□.
B. □□□ □□ □□ □.
C. TA-*□ □□□ □□ □□ □□□□□□□.
D. □□ □□ □ CIM □□ □□.
Answer: A (LEAVE A REPLY)
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecurity

NEW QUESTION: 78
ES □□□□ □□□□ □□□□ .spl□ □□ □□□□ □□□□□. ES □□□□ □□□□□ □□□□ □□ □ □ □□ □□ □□□ □□□□□?
A. □□□□ □□□ □□□ □□□ □ □□□ □□□□□.
B. □□□□ □□□ □□□ □ .spl □□□□ □□□□ □□□□.
C. □ □ □□□ □□□□□ □□ □□ □□□□ □ □□□□ □□ □□□□□.
D. □□ □ □□□□□ □□ □□ □ □ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)

□□ □□□ □ □□□ □□□□□(□□□□ □□□ □ □□) □□□ □□□ □□ □□ □□□(□□ □ □□) □ □□□□ □□□.

NEW QUESTION: 79
□□ □□□□□□ □□ □□□ □□□□ □□ □□(□□□, □□ □□ □□ □□)□ □□□ □□□□□?
A. □□□□□.
B. □□ □□□.
C. □□□□□.
D. □□ □□□□□.
Answer: C (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskScoring

NEW QUESTION: 80
□□ □□ □□□□□ □□□ □□ □□□ □□□ □□□□□?
A. □□□ □□
B. □□ □□□□□
C. □□
D. □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 81
□□□□□ □□□□ □□□□ □□□□ □□ □□□ □ □□□ □□□□□?
A. □□ □□ □ □□□.
B. □□□□ □ □□□.
C. □□□ □ □□□.
D. □□ □□ □ □□.
Answer: A (LEAVE A REPLY)
□□/□□: https://docs.splunk.com/Documentation/ES/6.4.1/User/Howurgencyisassigned

NEW QUESTION: 82
□□ □□□ □□□ □□ □□□□□?
A. □□ □□ □□□□□ □□ □□ □□ □ □□□□.
B. □□ □□ □□□□□ □□□ □□ □□□ □ □□□□.
C. □□ □□ □□□□□ □□ □□ □ □□□□.
D. □□ □□ □□ □ □□□ □□ □□ □□ □□□ □□.
Answer: (SHOW ANSWER)

NEW QUESTION: 83
□□ □ ES □□ □□□□□ □□□□□ □□ □□□ □□□□□?
A. □□ □□□.

B. □□□□□□.
C. KV □□□.
D. □□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
□□ □ ES□ □□□□□ □ □□ □□ □□□□□ □□□ □□□□□? (□□ □□ □□ □□)
A. □□□
B. □□□/□□
C. VulnScanSPL
D. SplunkEnterpriseThreatGenerator
Answer: (SHOW ANSWER)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Downloadthreatfeed

NEW QUESTION: 85
□□□ □□□ □□□□ □□□ □ □□□□?
A. GitHub
B. SplunkBase
C. www.splunk.com
D. ES □□ □□□
Answer: B (LEAVE A REPLY)
□□/□□: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

NEW QUESTION: 86
□ □□□ □□ □□ □□□ □□ □□ □□□□□□?

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

Killdump.com

A. □□ □□□□□.
B. □□□ □□ □□□□□.
C. IP □□ □□.
D. □□ □□□□□.
Answer: A (LEAVE A REPLY)

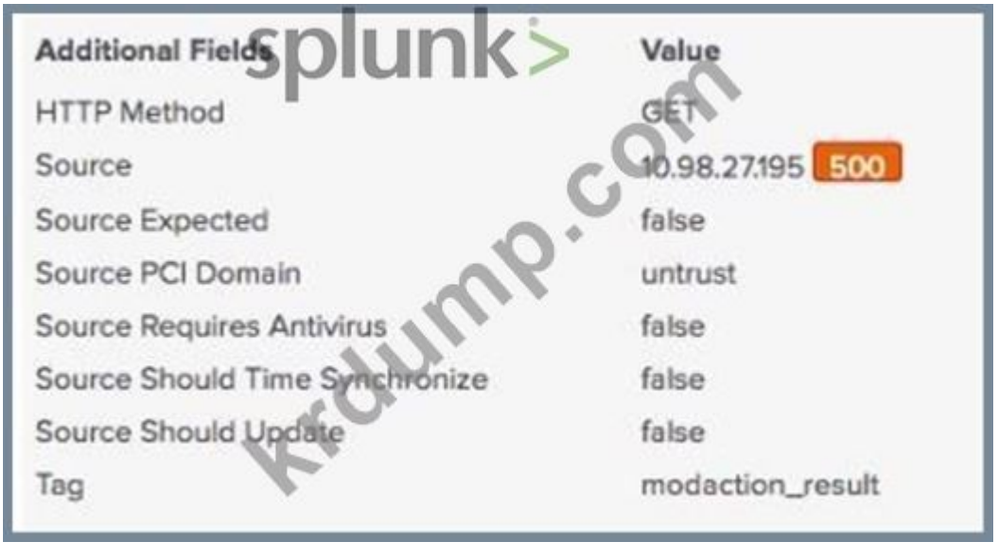
NEW QUESTION: 87
ES□ □□ □ □□ □□□□ □□□ □ □□□ □□ □□ □□□ □□□ □□□ □□□?
A. □ □ □□□ □□□ □□□ □□ -> □□ □□□□ □□□□□.
B. ES□ □□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □ □□ □□□□ □□□□□.
C. □□ □ □ □□□ □□□ □□□ □□ □□ □□ □□□□□.
D. ES□ SMTP □ HTTP □□□□ □□ □□□ □ □ □□□□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 88
□□ □□□□ ES □□ □□ □□ □□□□ □□□□ □□□ □□□□□?
A. □□ -> □□ □□ □□ -> "□□□□" □□ □□
B. □□ -> □□, □□□ □ □□ -> "□□□□" □□□□ □□□
C. □□ -> □□□ □□ -> "□□□□" □□ □ "□□□□" □□ □□
D. □□ -> □□, □□□ □ □□ -> "SplunkEnterpriseSecuritySuite" □ □□ □ "- □□"□□ □□□
Answer: A (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Listcorrelationsearches

NEW QUESTION: 89
ES □□□ □□ □□ □□□□ □□□□ □□□ □□□□□?
A. □□ -> □□ □□
B. □□ -> □□ -> □□
C. □□ -> □□□ □□□□□ -> □□ -> "□□□□□□ □□" □□
D. □□ -> □□□ □□□□□ -> □□ □□ -> SplunkEnterpriseSecuritySuite □□ □□ "□□□" □□
Answer: B (LEAVE A REPLY)
□□:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizemenubar#Restore_the_default_navigation

NEW QUESTION: 90
□□ configLradon □□□ □□□□ spiunk_TA_Forindexers □□□□ □□□ □ vrfilch 3□□ □□□ □□□ □ □□□□?
A. eventtypes.conf, indexes.conf, tags.conf
B. input.conf, props.conf, transforms.conf
C. web.conf, props.conf, transforms.conf
D. indexes.conf, props.conf, transforms.conf
Answer: (SHOW ANSWER)

NEW QUESTION: 91
□ □□□ □□ □□ □□□ □□ □□ □□□□□□?



A. IP □□ □□.
B. □□ □□□□□.
C. □□□ □□ □□□□□.
D. □□ □□□□□.
Answer: B (LEAVE A REPLY)

SPLK-3001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-3001 □□! DumpTop □ □□ **SPLK-3001** □□ □□□ □□□□□□, DumpTop SPLK-3001 □□ □□□ □□□□□□□□ □ □□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-3001 □□□ □□□□□.
https://www.dumptop.com/Splunk/SPLK-3001-dump.html (**101** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 92
□□ □□□□ □□ □□□□ □□□, □□ □□ □□ □ □□ □□ □ □□ □□ □□□ □ □□□□?
A. □□□□ □□□ □□□□□.
B. □□□ □□□□□.
C. □□ □□□.
D. □□□ □□□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 93
□□□□ □□□ □ □□ □□□□ □□□ □□□ □□ □□□□□ ES□□ □□□ □ □□□ □□ □□ □□ □□□ □□ □□□ □□□□□□?
A. □□□ □□□□□.
B. □□ □□□ □□ □□□.
C. □□ □□.
D. Splunk □□ □□ □□□ □□ □□□.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
□□ □□□□ ES □□ □□ □□ □□□□ □□□□ □□□ □□□□□?
A. □□ -> □□ □□ □□ -> "□□□□" □□ □□
B. □□ -> □□, □□□ □ □□ -> "□□□□" □□□□ □□□
C. □□ -> □□□ □□ -> "□□□□" □□ □ "□□□□" □□ □□
D. □□ -> □□, □□□ □ □□ -> "SplunkEnterpriseSecuritySuite" □ □□ □ "- □□"□□ □□□
Answer: A (LEAVE A REPLY)
□□
□□/□□: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Listcorrelationsearches

NEW QUESTION: 95
summariesonly=trueoption□ □□ □□ □□□ □□ □□□ □□□?
A. □□ □□□□ □□□□□.
B. □□ □□□□ □□□ □□□□ □□□□□.
C. □□ □□ □□ □□□ □□□□□.
D. □□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
□□/□□: https://community.splunk.com/t5/Splunk-Enterprise-Security/Why-do-correlation-searches-in-Enterprise-Security-not-use-quot/mp/262622

SPLK-3001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-3001 □□! DumpTop □ □□ **SPLK-3001** □□ □□□ □□□□□□, DumpTop SPLK-3001 □□ □□□ □□□□□□□□ □ □□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-3001 □□□ □□□□□.
https://www.dumptop.com/Splunk/SPLK-3001-dump.html (**101** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)