PassQueen
a.k.a dumpsqueen.com

Splunk Certified Cybersecurity Defense Analyst

Splunk SPLK-5001

Version Demo

Total Demo Questions: 11

Total Premium Questions: 115

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security Operations and the Cybersecurity Defense Analyst	13
Topic 2, Understanding Cyber Attacks	17
Topic 3, Threat and Vulnerability Management	4
Topic 4, Security Monitoring	57
Topic 5, Incident Response	7
Topic 6, Investigations	16
Topic 7, Mix Questions	1
Total	115

QUESTION NO: 1

Why is tstats more efficient than stats for large datasets?

A. tstats is faster since it operates at the beginning of the search pipeline.

B. tstats is faster since it only looks at indexed metadata, not raw data.

C. tstats is faster due to its SQL-like syntax.

D. tstats is faster since it searches raw logs for extracted fields.

ANSWER: B

Explanation:

tstats is faster since it only looks at indexed metadata, not raw data. The `tstats` command performs statistical aggregation over indexed fields and data-model acceleration summaries, rather than retrieving and processing the full raw text of every matching event. This substantially reduces the data that Splunk must read and evaluate, lowering disk I/O, CPU work, and search-time field-extraction overhead. For large data volumes, that distinction can make a query complete much more quickly than an equivalent search that uses `stats` after processing matching events.

In particular, `tstats` can query index-time fields such as host, source, sourcetype, and index, and it can use accelerated data models for datasets represented in a data model. Its efficiency depends on the needed fields being available in indexed data or acceleration summaries and on writing the query within `tstats` capabilities. This makes it especially valuable for security analytics and high-volume reporting, where repeated aggregations over large time ranges are common. Splunk documents that `tstats` is faster than `stats` because it searches only indexed fields and does not search raw event data. See Splunk tstats command reference and Splunk data model acceleration documentation.

QUESTION NO: 2

An analysis of an organization's security posture determined that a particular asset is at risk and a new process or solution should be implemented to protect it. Typically, who would be in charge of designing the new process and selecting the required tools to implement it?

A. SOC Manager

B. Security Engineer

C. Security Architect

D. Security Analyst

ANSWER: C

Explanation:

Security Architect is the correct role because this role translates identified business and security risks into an overall security design. After an asset has been identified as at risk, the Security Architect evaluates the organization's environment, applicable threats, architectural constraints, security requirements, and governance obligations to define an appropriate protective process or technical solution. This includes selecting security technologies and specifying how controls should fit together within the broader enterprise architecture. The architect's output commonly includes security patterns, control requirements, technology standards, and implementation designs that can be used by engineering teams to deploy and operate the selected solution. This responsibility is broader than simply administering a security tool: it requires aligning the proposed control with risk treatment objectives and the organization's existing systems. In Splunk-centered security operations, this architecture work can include determining how telemetry should be collected, which data sources and controls are needed, and how the resulting security capabilities support detection and response objectives. Splunk describes its security solutions as bringing together security data and workflows for threat detection, investigation, and response, which depend on deliberate design of data and security capabilities. See Splunk Security Solutions and the NIST guidance on integrating security into enterprise architecture in NIST SP 800-160, Volume 1.

QUESTION NO: 3

An analyst is investigating email events in which the field `url` contains multiple extracted values for each message. The analyst needs to compare every individual URL against a threat-intelligence lookup and return one result row for each URL.

Which SPL command should be used before the lookup?

A. `| makemv delim="," url`

B. `| mvcombine url`

C. `| mvexpand url`

D. `| spath input=url`

ANSWER: C

Explanation:

`mvexpand url` is correct because it expands a multivalue field into separate result rows, one for each value of `url`. The lookup can then evaluate each URL individually. `mvcombine` performs the opposite operation by combining values, while `makemv` creates multivalue fields from a single field and is unnecessary when the field is already multivalue.

QUESTION NO: 4

Which of the following is a best practice for searching in Splunk?

A. Streaming commands run before aggregating commands in the Search pipeline.

B. Raw word searches should contain multiple wildcards to ensure all edge cases are covered.

C. Limit fields returned from the search utilizing the cable command.

D. Searching over All Time ensures that all relevant data is returned.

ANSWER: A

Explanation:

Streaming commands run before aggregating commands in the Search pipeline. is a Splunk search-performance best practice because streaming commands can process events individually as they flow through the pipeline. Commands such as `search`, `where`, `eval`, and `fields` can filter, modify, or remove data early, reducing the number of events and the amount of field data that later commands must handle. Aggregating or transforming commands, such as `stats`, typically need to evaluate the complete result set before producing their final output. Placing event-level filtering and field-reduction operations before aggregation therefore reduces the workload required for those more resource-intensive stages. This ordering helps searches finish faster, use fewer search resources, and scale more effectively when working with large data volumes. Splunk's search optimization guidance emphasizes filtering data as early as possible and understanding command types so that searches can be structured efficiently. For further details, see the Splunk documentation on command types and the Search command reference.

QUESTION NO: 5

Which of the following data sources would be most useful to determine if a user visited a recently identified malicious website?

A. Active Directory Logs

B. Web Proxy Logs

C. Intrusion Detection Logs

D. Web Server Logs

ANSWER: B

Explanation:

Web Proxy Logs are the most useful source because a web proxy intermediates outbound HTTP and HTTPS connections made by users and systems. Its records commonly capture the requested URL or domain, destination address, timestamp, authenticated user or source device, HTTP method, response status, and policy action. An analyst can search those fields for the newly identified malicious domain, URL, or IP address, then correlate matching events to a user and endpoint to establish whether access was attempted or successful. Proxy telemetry also supplies useful context for incident scoping, such as the number of visits, bytes transferred, user-agent values, and whether the proxy blocked or allowed the request. In Splunk Enterprise Security, proxy data is a key network data source and is commonly normalized into the Web data model, enabling consistent searches, investigations, and correlation across proxy products. Splunk's Common Information Model identifies web-related fields such as `url`, `dest`, `user`, and `action`, which support this type of threat-intelligence matching and attribution. See Splunk's Web data model documentation and the Splunk CIM Web data model reference.

QUESTION NO: 6

Which search command allows an analyst to match whatever is inside the parentheses as a single term in the index, even if it contains characters that are usually recognized as minor breakers such as periods or underscores?

A. CASE()

B. LIKE()

C. FORMAT ()

D. TERM ()

ANSWER: D

Explanation:

`TERM ()` is correct because the `TERM` search modifier instructs Splunk to treat the content in its parentheses as one indexed term. This is particularly important when searching for values that include characters Splunk ordinarily recognizes as minor breakers, including periods and underscores. For example, a value such as `foo.bar` can be searched with `TERM(foo.bar)` so that Splunk matches the complete indexed term rather than handling the period as a delimiter during search processing. This behavior helps analysts make precise searches for technical indicators and structured values found in events, such as hostnames, file names, process names, identifiers, and dotted strings. The value supplied to `TERM` must correspond to an indexed term, because the modifier works at the index-term level rather than reconstructing arbitrary text at search time. Splunk documents `TERM` under search term modifiers and notes that it is designed to match terms containing minor breakers. See the Splunk Search Reference and the guidance on using CASE and TERM to match phrases.

QUESTION NO: 7

According to Splunk CIM documentation, which field in the Authentication Data Model represents the user who initiated a privilege escalation?

A. dest_user

B. src_user_id

C. src_user

D. username

ANSWER: C

Explanation:

`src_user` is the CIM Authentication data-model field for the user who originated an authentication-related action. In a privilege-escalation event, this is the account that initiates the escalation request or action, making `src_user` the appropriate normalized field for the initiating identity. CIM normalization is designed to retain a consistent semantic distinction between the originating side of an event and other identities or entities involved. This distinction lets analysts write portable searches, correlation rules, and detections that work across data sources with different native field names.

For example, an event showing an administrator invoking a command or workflow that elevates privileges should map the administrator or initiating account into `src_user`. This preserves the identity needed to investigate who initiated the activity, support attribution, and correlate authentication behavior across normalized CIM data. Splunk's Authentication data model documents `src_user` as the source user associated with an authentication event and identifies its relevance to privilege-escalation scenarios. See the Splunk CIM Authentication data model documentation and the Splunk Common Information Model overview.

QUESTION NO: 8

A Risk Rule generates events on Suspicious Cloud Share Activity and regularly contributes to confirmed incidents from Risk Notables. An analyst realizes the raw logs these events are generated from contain information which helps them determine what might be malicious.

What should they ask their engineer for to make their analysis easier?

A. Create a field extraction for this information.

B. Add this information to the risk message.

C. Create another detection for this information.

D. Allowlist more events based on this information.

ANSWER: A

Explanation:

Create a field extraction for this information. A field extraction parses a meaningful value from the raw event data and makes it available as a named field at search time. This lets the analyst search, filter, group, and correlate the cloud-share attributes that help establish whether activity is malicious, rather than repeatedly inspecting unstructured raw text. For example, extracted values can be used in ad hoc investigations, pivots, statistics, dashboard panels, and follow-on SPL searches involving the risk events and their source telemetry.

Field extractions also provide a reusable and consistent interpretation of the data for all analysts. Once the engineer defines the extraction with an appropriate regular expression, delimiter, or other extraction method, the relevant context is accessible throughout Splunk security workflows wherever the underlying events are searched. This directly improves triage efficiency while preserving the original event data and enabling more reliable investigation of the suspicious cloud-share behavior. Splunk describes fields as searchable name-and-value pairs and documents how field extractions make data in events available for search: Splunk field extraction documentation. Further details on using extracted fields in searches are available in the Splunk Search Reference.

QUESTION NO: 9

An analyst would like to test how certain Splunk SPL commands work against a small set of data. What command should start the search pipeline if they wanted to create their own data instead of utilizing data contained within Splunk?

A. makeresults

B. rename

C. eval

D. stats

ANSWER: A

Explanation:

The correct command is `makeresults`. This generating command creates one or more synthetic result events, allowing an analyst to begin an SPL pipeline without searching indexed data. It is particularly useful for testing SPL syntax, validating transformations, building examples, and experimenting with commands against a controlled, small dataset. By default, `makeresults` produces a single result with a `_time` field; options such as `count` can produce multiple results. Analysts can then use subsequent pipeline commands to create fields and values—for example, with `eval`—and apply reporting or transformation commands to observe their behavior. Because it generates the initial events itself, `makeresults` must be placed at the start of the search pipeline. Splunk classifies it as a generating command, meaning it creates a result set rather than operating on events returned by an earlier search command. See the Splunk Search Reference for makeresults and Splunk's documentation on search command types.

QUESTION NO: 10

What device typically sits at a network perimeter to detect command and control and other potentially suspicious traffic?

A. Host-based firewall

B. Web proxy

C. Endpoint Detection and Response

D. Intrusion Detection System

ANSWER: D

Explanation:

Intrusion Detection System is correct because a network-based IDS is commonly positioned at high-value network locations, including the perimeter, where it can inspect traffic entering and leaving the organization. Its purpose is to monitor packets and network activity for indicators of compromise, policy violations, known attack signatures, anomalous behavior, and communications associated with command-and-control infrastructure. Visibility at this boundary makes it especially useful for identifying suspicious outbound connections from compromised internal hosts as well as malicious inbound activity.

NIST describes network-based intrusion detection systems as technologies that monitor network traffic and analyze it for signs of possible incidents. Alerts and event records generated by these sensors can then be sent to a SIEM such as Splunk for correlation with endpoint, authentication, DNS, proxy, and threat-intelligence data. This combined analysis helps defenders validate whether a suspected command-and-control connection represents a real compromise and prioritize response activity. See NIST's Guide to Intrusion Detection and Prevention Systems and Splunk's Splunk Enterprise Security data prerequisites documentation.

QUESTION NO: 11

A Cyber Threat Intelligence (CTI) team produces a report detailing a specific threat actor's typical behaviors and intent. This would be an example of what type of intelligence?

A. Operational

B. Executive

C. Tactical

D. Strategic

ANSWER: A

Explanation:

Operational is correct because the report centers on a particular threat actor and describes that actor's behavior and intent. Operational cyber threat intelligence provides context that helps defenders understand an adversary's motivations, objectives, targeting, capabilities, and patterns of activity. This intelligence is commonly used to support security operations by connecting observed activity to a known actor or campaign and informing decisions about likely threats, prioritization, and defensive posture.

The key distinction is that the report is actor-focused and contextual: it characterizes how a specific adversary tends to act and what that adversary is trying to achieve. That context supports an operational understanding of the threat environment, rather than merely listing isolated technical artifacts. The information can help analysts assess whether activity observed in their environment aligns with the actor's known profile and anticipate what the actor may attempt next. NIST describes cyber threat information sharing and the value of contextual information for improving organizations' cybersecurity decisions in NIST SP 800-150. Splunk also discusses threat intelligence as contextual information that enables organizations to understand and respond to threats in its overview of threat intelligence.