Number: SPLK-5001
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: SPLK-5001

Exam Name: Splunk Certified Cybersecurity Defense Analyst

Exam A

QUESTION 1
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.

Correct Answer: C
Section:

QUESTION 2
While testing the dynamic removal of credit card numbers, an analyst lands on using the rex command. What mode needs to be set to in order to replace the defined values with X?
| makeresults
| eval ccnumber='511388720478619733'
| rex field=ccnumber mode=??? 's/(\d{4}-){3)/XXXX-XXXX-XXXX-/g'
Please assume that the above rex command is correctly written.

A. sed
B. replace
C. mask
D. substitute

Correct Answer: A
Section:

QUESTION 3
After discovering some events that were missed in an initial investigation, an analyst determines this is because some events have an empty src field. Instead, the required data is often captured in another field called machine_name.
What SPL could they use to find all relevant events across either field until the field extraction is fixed?

A. | eval src = coalesce(src,machine_name)
B. | eval src = src + machine_name
C. | eval src = src . machine_name
D. | eval src = tostring(machine_name)

Correct Answer: A
Section:

QUESTION 4
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

Correct Answer: A
Section:

QUESTION 5
An analyst is examining the logs for a web application's login form. They see thousands of failed logon attempts using various usernames and passwords. Internet research indicates that these credentials may have been compiled by combining account information from several recent data breaches.
Which type of attack would this be an example of?

A. Credential sniffing
B. Password cracking
C. Password spraying
D. Credential stuffing

Correct Answer: D
Section:

QUESTION 6
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

Correct Answer: C
Section:

QUESTION 7
Which of the following data sources can be used to discover unusual communication within an organization's network?

A. EDS
B. Net Flow
C. Email
D. IAM

Correct Answer: B
Section:

QUESTION 8
Which of the following is a best practice when creating performant searches within Splunk?

A. Utilize the transaction command to aggregate data for faster analysis.
B. Utilize Aggregating commands to ensure all data is available prior to Streaming commands.
C. Utilize specific fields to return only the data that is required.
D. Utilize multiple wildcards across fields to ensure returned data is complete and available.

Correct Answer: C
Section:

QUESTION 9
Which pre-packaged app delivers security content and detections on a regular, ongoing basis for Enterprise Security and SOAR?

A. SSE
B. ESCU
C. Threat Hunting
D. InfoSec

Correct Answer: B
Section:

QUESTION 10
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 ()

Correct Answer: D
Section:

QUESTION 11
Which field is automatically added to search results when assets are properly defined and enabled in Splunk Enterprise Security?

A. asset_category
B. src_ip
C. src_category
D. user

Correct Answer: C
Section:

QUESTION 12
An IDS signature is designed to detect and alert on logins to a certain server, but only if they occur from 6:00 PM - 6:00 AM. If no IDS alerts occur in this window, but the signature is known to be correct, this would be an example of what?

A. A True Negative.
B. A True Positive.

C. A False Negative.
D. A False Positive.

Correct Answer: A
Section:

QUESTION 13
Which of the following is not a component of the Splunk Security Content library (ESCU, SSE)?

A. Dashboards
B. Reports
C. Correlation searches
D. Validated architectures

Correct Answer: D
Section:

QUESTION 14
The eval SPL expression supports many types of functions. Which of these function categories is not valid with eval?

A. JSON functions
B. Text functions
C. Comparison and Conditional functions
D. Threat functions

Correct Answer: D
Section:

QUESTION 15
Which Enterprise Security framework provides a mechanism for running preconfigured actions within the Splunk platform or integrating with external applications?

A. Asset and Identity
B. Notable Event
C. Threat Intelligence
D. Adaptive Response

Correct Answer: D
Section:

QUESTION 16
Which of the following Splunk Enterprise Security features allows industry frameworks such as CIS Critical Security Controls, MITRE ATT&CK, and the Lockheed Martin Cyber Kill Chain to be mapped to Correlation Search results?

A. Annotations
B. Playbooks
C. Comments
D. Enrichments

Correct Answer: A
Section:

QUESTION 17
Which of the following is the primary benefit of using the CIM in Splunk?

A. It allows for easier correlation of data from different sources.
B. It improves the performance of search queries on raw data.
C. It enables the use of advanced machine learning algorithms.
D. It automatically detects and blocks cyber threats.

Correct Answer: A
Section:

QUESTION 18
Which of the following use cases is best suited to be a Splunk SOAR Playbook?

A. Forming hypothesis for Threat Hunting
B. Visualizing complex datasets.
C. Creating persistent field extractions.
D. Taking containment action on a compromised host

Correct Answer: D
Section:

QUESTION 19
Which of the following is not considered an Indicator of Compromise (IOC)?

A. A specific domain that is utilized for phishing.
B. A specific IP address used in a cyberattack.
C. A specific file hash of a malicious executable.
D. A specific password for a compromised account.

Correct Answer: D
Section:

QUESTION 20
According to Splunk CIM documentation, which field in the Authentication Data Model represents the user who initiated a privilege escalation?

A. username
B. src_user_id
C. src_user
D. dest_user

Correct Answer: C
Section:

QUESTION 21
The following list contains examples of Tactics, Techniques, and Procedures (TTPs):
1. Exploiting a remote service
2. Lateral movement
3. Use EternalBlue to exploit a remote SMB server
In which order are they listed below?

A. Tactic, Technique, Procedure
B. Procedure, Technique, Tactic
C. Technique, Tactic, Procedure
D. Tactic, Procedure, Technique

Correct Answer: A
Section:

QUESTION 22
An analyst is attempting to investigate a Notable Event within Enterprise Security. Through the course of their investigation they determined that the logs and artifacts needed to investigate the alert are not available.
What event disposition should the analyst assign to the Notable Event?

A. Benign Positive, since there was no evidence that the event actually occurred.
B. False Negative, since there are no logs to prove the activity actually occurred.
C. True Positive, since there are no logs to prove that the event did not occur.
D. Other, since a security engineer needs to ingest the required logs.

Correct Answer: D
Section:

QUESTION 23
Tactics, Techniques, and Procedures (TTPs) are methods or behaviors utilized by attackers. In which framework are these categorized?

A. NIST 800-53
B. ISO 27000
C. CIS18
D. MITRE ATT&CK

Correct Answer: D
Section:

QUESTION 24
A threat hunter executed a hunt based on the following hypothesis:
As an actor, I want to plant rundll32 for proxy execution of malicious code and leverage Cobalt Strike for Command and Control.
Relevant logs and artifacts such as Sysmon, netflow, IDS alerts, and EDR logs were searched, and the hunter is confident in the conclusion that Cobalt Strike is not present in the company's environment.
Which of the following best describes the outcome of this threat hunt?

A. The threat hunt was successful because the hypothesis was not proven.
B. The threat hunt failed because the hypothesis was not proven.
C. The threat hunt failed because no malicious activity was identified.

D. The threat hunt was successful in providing strong evidence that the tactic and tool is not present in the environment.

Correct Answer: D
Section:

QUESTION 25
An analyst notices that one of their servers is sending an unusually large amount of traffic, gigabytes more than normal, to a single system on the Internet. There doesn't seem to be any associated increase in incoming traffic. What type of threat actor activity might this represent?

A. Data exfiltration
B. Network reconnaissance
C. Data infiltration
D. Lateral movement

Correct Answer: A
Section:

QUESTION 26
In which phase of the Continuous Monitoring cycle are suggestions and improvements typically made?

A. Define and Predict
B. Establish and Architect
C. Analyze and Report
D. Implement and Collect

Correct Answer: C
Section:

QUESTION 27
An analyst is not sure that all of the potential data sources at her company are being correctly or completely utilized by Splunk and Enterprise Security. Which of the following might she suggest using, in order to perform an analysis of the data types available and some of their potential security uses?

A. Splunk ITSI
B. Security Essentials
C. SOAR
D. Splunk Intelligence Management

Correct Answer: B
Section:

QUESTION 28
During their shift, an analyst receives an alert about an executable being run from C:\Windows\Temp. Why should this be investigated further?

A. Temp directories aren't owned by any particular user, making it difficult to track the process owner when files are executed.
B. Temp directories are flagged as non-executable, meaning that no files stored within can be executed, and this executable was run from that directory.
C. Temp directories contain the system page file and the virtual memory file, meaning the attacker can use their malware to read the in memory values of running programs.
D. Temp directories are world writable thus allowing attackers a place to drop, stage, and execute malware on a system without needing to worry about file permissions.

Correct Answer: D
Section:

QUESTION 29
An analyst would like to visualize threat objects across their environment and chronological risk events for a Risk Object in Incident Review. Where would they find this?

A. Running the Risk Analysis Adaptive Response action within the Notable Event.
B. Via a workflow action for the Risk Investigation dashboard.
C. Via the Risk Analysis dashboard under the Security Intelligence tab in Enterprise Security.
D. Clicking the risk event count to open the Risk Event Timeline.

Correct Answer: D
Section:

QUESTION 30
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.

Correct Answer: A
Section:

QUESTION 31
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

Correct Answer: D
Section:

QUESTION 32
Upon investigating a report of a web server becoming unavailable, the security analyst finds that the web server's access log has the same log entry millions of times:
147.186.119.200 - - [28/Jul/2023:12:04:13 -0300] 'GET /login/ HTTP/1.0' 200 3733
What kind of attack is occurring?

A. Denial of Service Attack
B. Distributed Denial of Service Attack
C. Cross-Site Scripting Attack
D. Database Injection Attack

Correct Answer: B
Section:

QUESTION 33
According to David Bianco's Pyramid of Pain, which indicator type is least effective when used in continuous monitoring?

A. Domain names
B. TTPs
C. NetworM-lost artifacts
D. Hash values

Correct Answer: D
Section:

QUESTION 34
Splunk Enterprise Security has numerous frameworks to create correlations, integrate threat intelligence, and provide a workflow for investigations. Which framework raises the threat profile of individuals or assets to allow identification of people or devices that perform an unusual amount of suspicious activities?

A. Threat Intelligence Framework
B. Risk Framework
C. Notable Event Framework
D. Asset and Identity Framework

Correct Answer: B
Section:

QUESTION 35
A Cyber Threat Intelligence (CTI) team delivers a briefing to the CISO detailing their view of the threat landscape the organization faces. This is an example of what type of Threat Intelligence?

A. Tactical
B. Strategic
C. Operational
D. Executive

Correct Answer: B
Section:

QUESTION 36
An analyst investigates an IDS alert and confirms suspicious traffic to a known malicious IP. What Enterprise Security data model would they use to investigate which process initiated the network connection?

A. Endpoint
B. Authentication
C. Network traffic
D. Web

Correct Answer: A
Section:

QUESTION 37
When threat hunting for outliers in Splunk, which of the following SPL pipelines would filter for users with over a thousand occurrences?

A. | sort by user | where count > 1000
B. | stats count by user | where count > 1000 | sort - count
C. | top user
D. | stats count(user) | sort - count | where count > 1000

Correct Answer: B
Section:

QUESTION 38
The United States Department of Defense (DoD) requires all government contractors to provide adequate security safeguards referenced in National Institute of Standards and Technology (NIST) 800-171. All DoD contractors must continually reassess, monitor, and track compliance to be able to do business with the US government.
Which feature of Splunk Enterprise Security provides an analyst context for the correlation search mapping to the specific NIST guidelines?

A. Comments
B. Moles
C. Annotations
D. Framework mapping

Correct Answer: D
Section:

QUESTION 39
An analyst is investigating the number of failed login attempts by IP address. Which SPL command can be used to create a temporary table containing the number of failed login attempts by IP address over a specific time period?

A. index=security_logs eventtype=failed_login | eval count as failed_attempts by src_ip | sort -failed_attempts
B. index=security_logs eventtype=failed_login | transaction count as failed_attempts by src_ip | sort -failed_attempts
C. index=security_logs eventtype=failed_login | stats count as failed_attempts by src_ip | sort -failed_attempts
D. index=security_logs eventtype=failed_login | sum count as failed_attempts by src_ip | sort -failed_attempts

Correct Answer: C
Section:

QUESTION 40
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 implementing the new process or solution that was selected?

A. Security Architect
B. SOC Manager
C. Security Engineer
D. Security Analyst

Correct Answer: C
Section: