Splunk

Exam Questions SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

NEW QUESTION 1
Which of the following is considered Personal Data under GDPR?

A. The birth date of an unidentified user.
B. An individual's address including their first and last name.
C. The name of a deceased individual.
D. A company's registration number.

Answer: B

Explanation:
Under the General Data Protection Regulation (GDPR), Personal Data is any information relating to an identified or identifiable natural person. An individual's address, combined with their first and last name, clearly identifies a person, making it Personal Data under GDPR. The other options provided do not meet the GDPR criteria for Personal Data: the birth date of an unidentified user does not identify a person, the name of a deceased individual is not covered under GDPR, and a company??s registration number pertains to an entity rather than a natural person.
Top of Form Bottom of Form

NEW QUESTION 2
While testing the dynamic removal of credit card numbers, an analyst lands on using therexcommand. 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 aboverexcommand is correctly written.

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

Answer: A

Explanation:
Therexcommand in Splunk can be used to extract or replace data using regular expressions. To dynamically replace values with a specific pattern, such as replacing credit card numbers with "X", the mode needs to be set tosed. Thesedmode allows for string replacement within a field using regular expressions, enabling the substitution of matching patterns with a specified string.

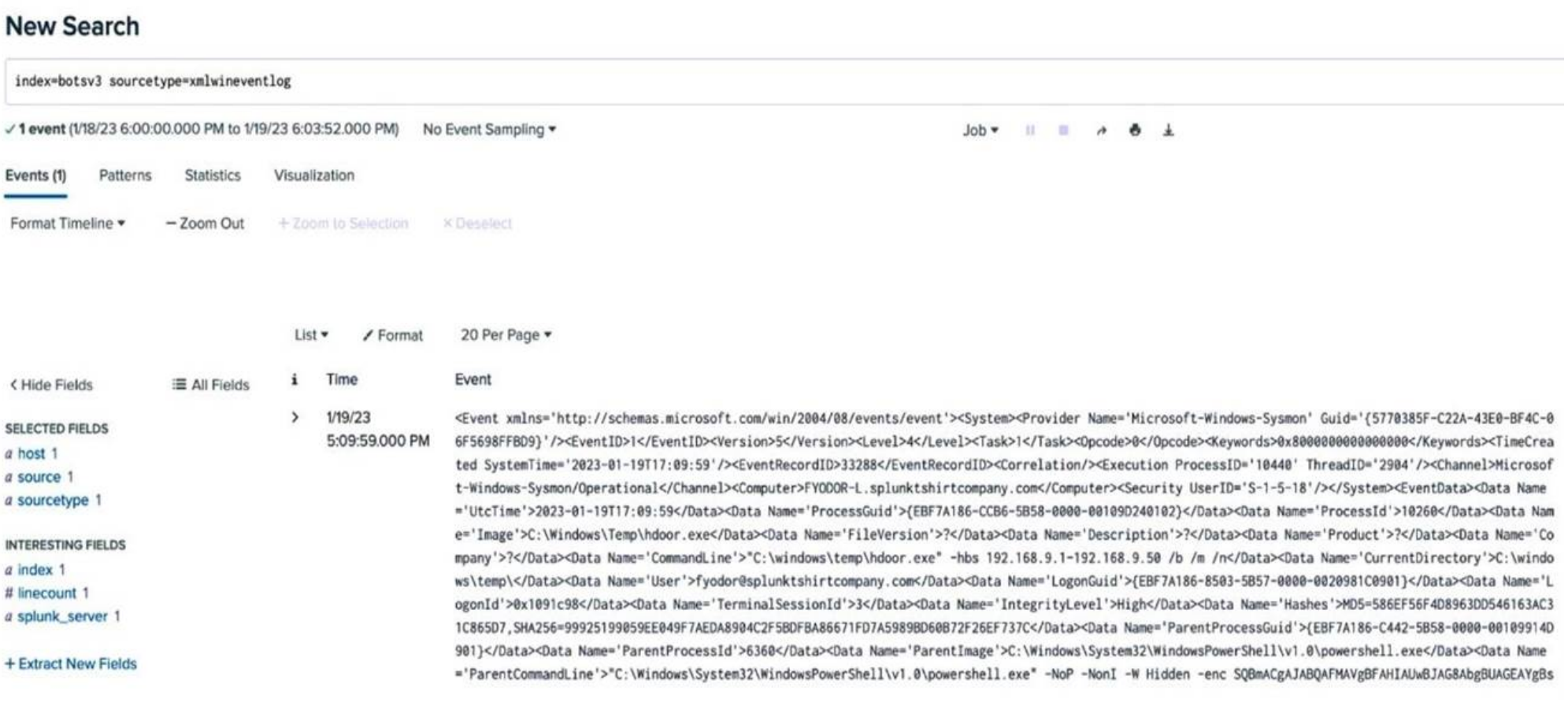
NEW QUESTION 3
An analyst is investigating how an attacker successfully performs a brute-force attack to gain a foothold into an organizations systems. In the course of the investigation the analyst determines that the reason no alerts were generated is because the detection searches were configured to run against Windows data only and excluding any Linux data.
This is an example of what?

A. A True Positive.
B. A True Negative.
C. A False Negative.
D. A False Positive.

Answer: C

Explanation:
This scenario is an example of aFalse Negativebecause the detection mechanisms failed to generate alerts for a brute-force attack due to a misconfiguration—specifically, the exclusion of Linux data from the detection searches. A False Negative occurs when a security control fails to detect an actual malicious activity that it is supposed to catch, leading to undetected attacks and potential breaches.

NEW QUESTION 4
An analyst is building a search to examine Windows XML Event Logs, but the initial search is not returning any extracted fields. Based on the above image, what is themost likelycause?



A. The analyst does not have the proper role to search this data.
B. The analyst is searching newly indexed data that was improperly parsed.
C. The analyst did not add the excract command to their search pipeline.
D. The analyst is not in the Drooer Search Mode and should switch to Smart or Verbose.

Answer: D

Explanation:
In Splunk, when an analyst is building a search and finds that extracted fields are not appearing, it often relates to the search mode being used.Smart ModeorVerbose Modeare better suitedfor field extraction as they allow Splunk to automatically extract and display fields based on the data being searched.
? Search Modes in Splunk:
? Incorrect Options:
? Splunk Documentation:Search modes and their impact on field extraction.

NEW QUESTION 5
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:
In Splunk,streaming commandsprocess each event individually as it is passed through the search pipeline and should be placed beforeaggregating commands, which operate on the entire set of results at once. This best practice ensures efficient processing and minimizes resource usage, as streaming commands reduce the amount of data before aggregation occurs. This approach leads to faster and more efficient searches. In contrast, the other options, such as using wildcards excessively or searching over all time, can lead to performance issues and excessive data processing.

NEW QUESTION 6
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:
AnIntrusion Detection System (IDS)typically sits at the network perimeter and is designed to detect suspicious traffic, including command and control (C2) traffic and other potentially malicious activities.
? Intrusion Detection Systems:
? Incorrect Options:
? Network Security Practices:IDS implementation is a standard practice for perimeter security to detect early signs of network intrusion.

NEW QUESTION 7
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

Answer: D

Explanation:
The MITRE ATT&CK framework categorizes Tactics, Techniques, and Procedures (TTPs) used by attackers. It is a globally accessible knowledge base of adversarial tactics and techniques based on real-world observations, and it is widely used by cybersecurity professionals to understand and defend against various cyber threats.
? Tactics, Techniques, and Procedures (TTPs):
? MITRE ATT&CK Framework:MITRE ATT&CK organizes these TTPs into a matrix that reflects different stages of an attack lifecycle, from initial access to exfiltration. The framework helps security teams by:
? Why MITRE ATT&CK:Unlike compliance-focused frameworks like NIST 800-53 or ISO 27000, which provide security controls and best practices, MITRE ATT&CK is specifically focused on the behavior of adversaries. This focus makes it an invaluable resource for understanding how attacks unfold and how to counteract them.
? MITRE ATT&CK Website:The official site provides detailed information on each tactic and technique, along with examples of how they have been used in real-world attacks.
? Threat Intelligence Platforms:Many platforms integrate with MITRE ATT&CK, providing enhanced detection and response capabilities by mapping security events to the framework.
? Security Research Papers:Numerous papers and reports analyze specific attacks using the ATT&CK framework, offering insights into its practical applications in cybersecurity defense.
References:MITRE ATT&CK is a foundational tool in modern cybersecurity, providing a detailed and actionable understanding of adversary behaviors that can be directly applied to enhance an organization's defensive posture.

NEW QUESTION 8
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

Answer: C

Explanation:
In Splunk Enterprise Security, when assets are properly defined and enabled, the fieldsrc_categoryis automatically added to search results. This field categorizes the source IP addresses according to their asset classification, which helps in analyzing and filtering search results based on the type of assets involved in an event. Proper asset and identity management within Splunk ES enhances the ability to contextualize and prioritize security incidents.

NEW QUESTION 9
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:
In an organization, theSecurity Architectis typically responsible for designing new processes or selecting the tools necessary to protect assets that are identified as being at risk. The Security Architect has the expertise to design a comprehensive security solution that addresses the specific needs of the organization, considering various factors like existing infrastructure, threatlandscape, and compliance requirements. They work closely with other roles, such as Security Engineers, to implement these solutions.

NEW QUESTION 10
What is the main difference between a DDoS and a DoS attack?

A. A DDoS attack is a type of physical attack, while a DoS attack is a type of cyberattack.
B. A DDoS attack uses a single source to target a single system, while a DoS attack uses multiple sources to target multiple systems.
C. A DDoS attack uses multiple sources to target a single system, while a DoS attack usesa single source to target a single or multiple systems.
D. A DDoS attack uses a single source to target multiple systems, while a DoS attack uses multiple sources to target a single system.

Answer: C

Explanation:
The primary difference between a Distributed Denial of Service (DDoS) attack and a Denial of Service (DoS) attack is in the source of the attack. ADDoSattack involves multiple compromised systems (often part of a botnet) attacking a single target, overwhelming it with traffic or requests. In contrast, aDoSattack typically involves a single source attacking the target. The goal of both attacks is to make a service unavailable, but DDoS attacks are usually more difficult to defend against because of their distributed nature.

NEW QUESTION 10
When searching in Splunk, which of the following SPL commands can be used to run a subsearch across every field in a wildcard field list?

A. foreach
B. rex
C. makeresults
D. transaction

Answer: A

Explanation:
Theforeachcommand in Splunk is used to iterate over a list of fields that match a wildcard expression and apply a subsearch or function to each of them. This is particularly useful when you need to perform an operation across multiple fields dynamically identified by a wildcard pattern. None of the other options (rex,makeresults, ortransaction) are designed for this specific purpose. Theforeachcommand allows for flexible and efficient processing of multiple fields without having to explicitly name them all.

NEW QUESTION 12
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

Answer: B

Explanation:
Splunk Security Essentials is a powerful tool that an analyst can use to analyze the data types available and understand their potential security uses. It provides a framework for exploring how different data sources can be leveraged within Splunk to enhance security monitoring and detection capabilities.
? Splunk Security Essentials:This app is designed to help users maximize the value
of their data by providing examples of security use cases, detection searches, and best practices tailored to the available data sources. It offers a comprehensive overview of how various types of data can be used within Splunk, making it easier for analysts to identify gaps in data utilization.
? Data Source Analysis:Through Splunk Security Essentials, an analyst can:
? Why Security Essentials:This tool is particularly useful for organizations looking to ensure that they are fully utilizing their available data within Splunk Enterprise Security. It provides actionable insights and examples that can help analysts fine- tune their security operations and improve threat detection.
? Splunk Security Essentials Documentation:The official documentation provides detailed instructions on how to use the app to analyze data sources and implement best practices for security monitoring.
? User Community Discussions:Many Splunk users share their experiences and strategies for using Security Essentials to optimize their security posture in forums and blogs.

NEW QUESTION 17
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.

Answer: D

Explanation:
An executable running from theC:\Windows\Tempdirectory is a significant red flag because temporary directories are often world writable, meaning any user or process can write files to them. This characteristic makes these directories an attractive
target for attackers who want to drop, stage, and execute malware without worrying about restrictive file permissions.
? Temp Directories Characteristics:
? Security Risks:
? Investigation Importance:The fact that an executable is running fromC:\Windows\Tempwarrants further investigation to determine whether it is malicious. Analysts should check:
? Windows Security Best Practices:Documentation on how to secure temp directories and monitor for suspicious activity is available from both Microsoft and various security communities.
? Incident Response Playbooks:Many playbooks include steps for investigating suspicious activity in temp directories as part of broader malware detection and response strategies.
? MITRE ATT&CK Framework:Techniques involving the use of temporary directories are well-documented in the framework, offering insights into how adversaries leverage these locations during an attack.

NEW QUESTION 21
A threat hunter generates a report containing the list of users who have logged in to a particular database during the last 6 months, along with the number of times they have each authenticated. They sort this list and remove any user names who have logged in more than 6 times. The remaining names represent the users who rarely log in, as their activity is more suspicious. The hunter examines each of these rare logins in detail.
This is an example of what type of threat-hunting technique?

A. Least Frequency of Occurrence Analysis
B. Co-Occurrence Analysis
C. Time Series Analysis
D. Outlier Frequency Analysis

Answer: A

Explanation:
The scenario described is an example ofLeast Frequency of Occurrence Analysis. This threat-hunting technique focuses on identifying events or behaviors that occur infrequently, under the assumption that rare activities could indicate abnormal or suspicious behavior. By filtering out users who log in frequently and focusing on those with rare login attempts, the threat hunter aims to identify potentially suspicious activity that warrants further investigation. This technique is particularly effective in detecting stealthy attacks that might evade more common detection methods.
Top of Form Bottom of Form

NEW QUESTION 26
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

Answer: C

Explanation:
According to Splunk CIM (Common Information Model) documentation, thesrc_userfield in the Authentication Data Model represents the user who initiated an action, including privilege escalation. This field is used to track the source user responsible for generating an authentication event, which is critical in understanding and responding to potential security incidents involving privilege escalation. The other fields likedest_userorusernamehave different roles, focusing on the target of the action or the general username involved.
Top of Form Bottom of Form

NEW QUESTION 27
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

Answer: D

Explanation:
The scenario describes an attack where thousands of failed login attempts are made using various usernames and passwords, which is indicative of aCredential Stuffingattack. This type of attack involves using lists of stolen credentials (usernames and passwords) obtained from previous data breaches to attempt to gain unauthorized access to user accounts. Attackers take advantage of the fact that many users reuse passwords across multiple sites. UnlikePassword Spraying(which tries a few common passwords against many accounts) orPassword Cracking(which tries to guess or decrypt passwords), credential stuffing leverages large datasets of valid credentials obtained from other breaches.
Top of Form Bottom of Form

NEW QUESTION 28
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.

Answer: D

Explanation:
In this scenario, the analyst cannot conclude whether the Notable Event is a true positive or a false positive due to the absence of necessary logs and artifacts. The appropriate eventdisposition in this case is "Other," as it indicates that further action is required, such as ingesting the missing logs. The involvement of a security engineer to ensure the necessary data is available for proper investigation is implied, making "Other" the most suitable option.

NEW QUESTION 32
A Risk Notable Event has been triggered in Splunk Enterprise Security, an analyst investigates the alert, and determines it is a false positive. What metric would be used to define the time between alert creation and close of the event?

A. MTTR (Mean Time to Respond)
B. MTBF (Mean Time Between Failures)
C. MTTA (Mean Time to Acknowledge)
D. MTTD (Mean Time to Detect)

Answer: A

Explanation:
In incident response and cybersecurity operations, Mean Time to Respond (MTTR) is a key metric. It measures the average time it takes from when an alert is created to when it is resolved or closed. In the scenario, an analyst identifies a Risk Notable Event as a false positive and closes it; the time taken from the alert's creation to its closure is what MTTR measures. This metric is crucial in understanding how efficiently a security team responds to alerts and incidents, thus contributing to overall security posture improvement.

NEW QUESTION 33
The Lockheed Martin Cyber Kill Chain® breaks an attack lifecycle into several stages. A threat actor modified the registry on a compromised Windows system to ensure that their malware would automatically run at boot time. Into which phase of the Kill Chain would this fall?

A. Act on Objectives
B. Exploitation
C. Delivery

D. Installation

Answer: D

Explanation:
The Lockheed Martin Cyber Kill Chain® is a widely recognized framework that breaks down the stages of a cyber attack. The stages are: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives. The scenario described—modifying the registry on a compromised Windows system to ensure malware runs at boot time—fits into theInstallationphase. This phase involves placing a persistent backdoor or other malicious software on the victim's system, ensuring it can be executed again, even after a system reboot. By modifying the registry, the attacker is achieving persistence, a classic example of the Installation phase.

NEW QUESTION 35
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-5001 Practice Exam Features:

* SPLK-5001 Questions and Answers Updated Frequently

* SPLK-5001 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-5001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-5001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year