Exam Questions SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

https://www.2passeasy.com/dumps/SPLK-5001/

NEW QUESTION 1
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.

Answer: D

Explanation:
Indicators of Compromise (IOCs) are artifacts that are used to identify potential malicious activity within a network or system. Common IOCs include domains, IP addresses, and file hashes that are associated with malicious activity. However, a specific password, while potentially sensitive, is not typically considered an IOC because it is more of a credential than an artifact indicating a compromise. IOCs are used to detect and respond to threats, while compromised credentials are a result of those threats.

NEW QUESTION 2
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.

Answer: C

Explanation:
When creating performant searches in Splunk, it is a best practice to utilize specific fields to return only the data that is required. This approach minimizes the amount of data processed and speeds up search performance. By explicitly specifying the fields of interest using commands likefields, you reduce the overhead on Splunk??s processing engine, leading to faster and more efficient queries. In contrast, using wildcards or overly broad searches can lead to slower performance due to the increased data volume being processed.
Top of Form Bottom of Form

NEW QUESTION 3
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

Answer: B

Explanation:
TheEnterprise Security Content Update (ESCU)app is a pre-packaged app that delivers security content and detections on a regular, ongoing basis for Splunk Enterprise Security (ES) and Splunk SOAR. ESCU provides regular updates with new correlation searches, dashboards, and other content that help organizations stay up-to-date with the latest threats and detection techniques. This app is specifically designed to enhance the capabilities of Splunk ES by providing out-of-the-box security content that can be customized and used immediately.

NEW QUESTION 4
An analyst is investigating a network alert for suspected lateral movement from one Windows host to another Windows host. According to Splunk CIM documentation, the IP address of the host from which the attacker is moving would be in which field?

A. host
B. dest
C. src_nt_host
D. src_ip

Answer: D

Explanation:
According to Splunk??s Common Information Model (CIM) documentation, when investigating network alerts, the IP address of the host from which an attacker is moving (source) is typically stored in thesrc_ipfield. Thehostfield generally refers to the name of the host that logged the event,destrefers to the destination IP, andsrc_nt_hostrefers to the NetBIOS name of the source host. Thesrc_ipfield is specifically used to denote the source IP address in the context of network communication, which is critical for tracing lateral movement.

NEW QUESTION 5
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 6
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 7
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

Answer: B

Explanation:
TheRisk Frameworkin Splunk Enterprise Security is designed to raise the threat profile of individuals or assets based on their activities. It allows security teams to assign risk scores to users or devices that engage in suspicious or anomalous behaviors, making it easier to identify entities that may require further investigation.
? Risk Framework:
? Incorrect Options:
? Splunk Documentation:Detailed information on the Risk Framework and how it integrates with other security features in Splunk ES.

NEW QUESTION 8
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 9
Which of the following is a tactic used by attackers, rather than a technique?

A. Gathering information about a target.
B. Establishing persistence with a scheduled task.
C. Using a phishing email to gain initial access.
D. Escalatingprivileges via UAC bypass.

Answer: A

Explanation:
Tacticsare the overarching objectives or strategies attackers use during their operations, whiletechniquesare the specific methods used to achieve these tactics. In this case,gathering information about a target(often referred to as Reconnaissance) is atacticbecause it represents a high-level objective of understanding the target. The other options provided (persistence, phishing, privilege escalation) are specifictechniquesused to achieve the broader goals or tactics.

NEW QUESTION 10
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

Answer: A

Explanation:
The examples provided correspond to Tactics, Techniques, and Procedures (TTPs) in the following order:
? Lateral movement– This is aTactic. Tactics represent the goals or objectives of an adversary, such as moving laterally within a network to gain broader access.
? Exploiting a remote service– This is aTechnique. Techniques are specific methods used to achieve a tactic, such as exploiting a service to move laterally.
? Use EternalBlue to exploit a remote SMB server– This is aProcedure. Procedures are the detailed steps or specific implementations of a technique, such as using the EternalBlue exploit to target SMB vulnerabilities.
Thus, the correct order isTactic, Technique, Procedure.

NEW QUESTION 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:
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 15
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

Answer: B

Explanation:
NetFlow data is a powerful data source for monitoring and analyzing network traffic patterns within an organization. It provides detailed information about the flow of data between devices on a network, including source and destination IP addresses, ports, and protocols. By analyzing NetFlow data, security analysts can detect unusual communication patterns that may indicate malicious activity, such as lateral movement, data exfiltration, or communication with command and control servers. Other options like EDS (Endpoint Detection Systems), Email, and IAM (Identity and Access Management) are also valuable, but NetFlow is specifically designed for network traffic analysis.
Top of Form Bottom of Form

NEW QUESTION 18
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

Answer: D

Explanation:
? Pyramid of Pain Overview:The Pyramid of Pain categorizes indicators based on how difficult they are for attackers to alter:
? Why Hash Values Are Least Effective:
? David Bianco's Pyramid of Pain Blog Post:Bianco??s original post and related materials provide a deep dive into why hash values are the least effective and why focusing on higher-level indicators is more impactful for security operations.
? Threat Intelligence Reports:Many reports emphasize the importance of focusing on TTPs over simpler indicators like hash values to build a more resilient detection and response strategy.

NEW QUESTION 23
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 25
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)

Answer: A

Explanation:
Thecoalescefunction in Splunk is used to return the first non-null value from a list of fields. The SPL| eval src = coalesce(src,machine_name)allows the analyst to dynamically populate thesrcfield with the value frommachine_nameifsrcis empty. This is a useful technique when dealing with inconsistent data sources or during field extraction issues, ensuring that the analyst can continue their investigation without missing critical events.

NEW QUESTION 28
Which stage of continuous monitoring involves adding data, creating detections, and building drilldowns?

A. Implement and Collect
B. Establish and Architect
C. Respond and Review
D. Analyze and Report

Answer: A

Explanation:
In the context of continuous monitoring, theImplement and Collectstage involves adding data sources, creating detections, and building drilldowns. This stage is focused on the practical setup and configuration necessary to ensure that monitoring systems are properly gathering the necessary data and that the relevant detection mechanisms are in place to identify potential threats. Other stages, such asAnalyze and Report, are more focused on the interpretation and presentation of this data after collection.

NEW QUESTION 29
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 32
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

Answer: D

Explanation:

TheevalSPL expression in Splunk supports several categories of functions, includingJSON functions(e.g.,spath),Text functions(e.g.,substr,trim), andComparison and Conditional functions(e.g.,if,case). However,Threat functionsis not a valid category within theevalcommand. Theevalcommand is primarily used for transforming and manipulating data in various ways, but it does not include a category specifically for threat-related functions.

NEW QUESTION 35

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-5001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-5001 Product From:

https://www.2passeasy.com/dumps/SPLK-5001/

Money Back Guarantee

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