Splunk

Exam Questions SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

NEW QUESTION 1
What goal of an Advanced Persistent Threat (APT) group aims to disrupt or damage on behalf of a cause?

A. Hacktivism
B. Cyber espionage
C. Financial gain
D. Prestige

Answer: A

Explanation:
Hacktivismrefers to the use of hacking techniques by an Advanced Persistent Threat (APT) group to promote a political agenda or social cause. Unlike other motivations such as financial gain or espionage, the primary goal of hacktivism is to disrupt, damage, or deface systems to draw attention to a cause or to protest against something the group opposes.
? Hacktivism:
? Incorrect Options:
? Cybersecurity Literature:Books and articles on APT motivations often highlight hacktivism as a distinct category with a focus on ideological or political goals.

NEW QUESTION 2
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 3
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.

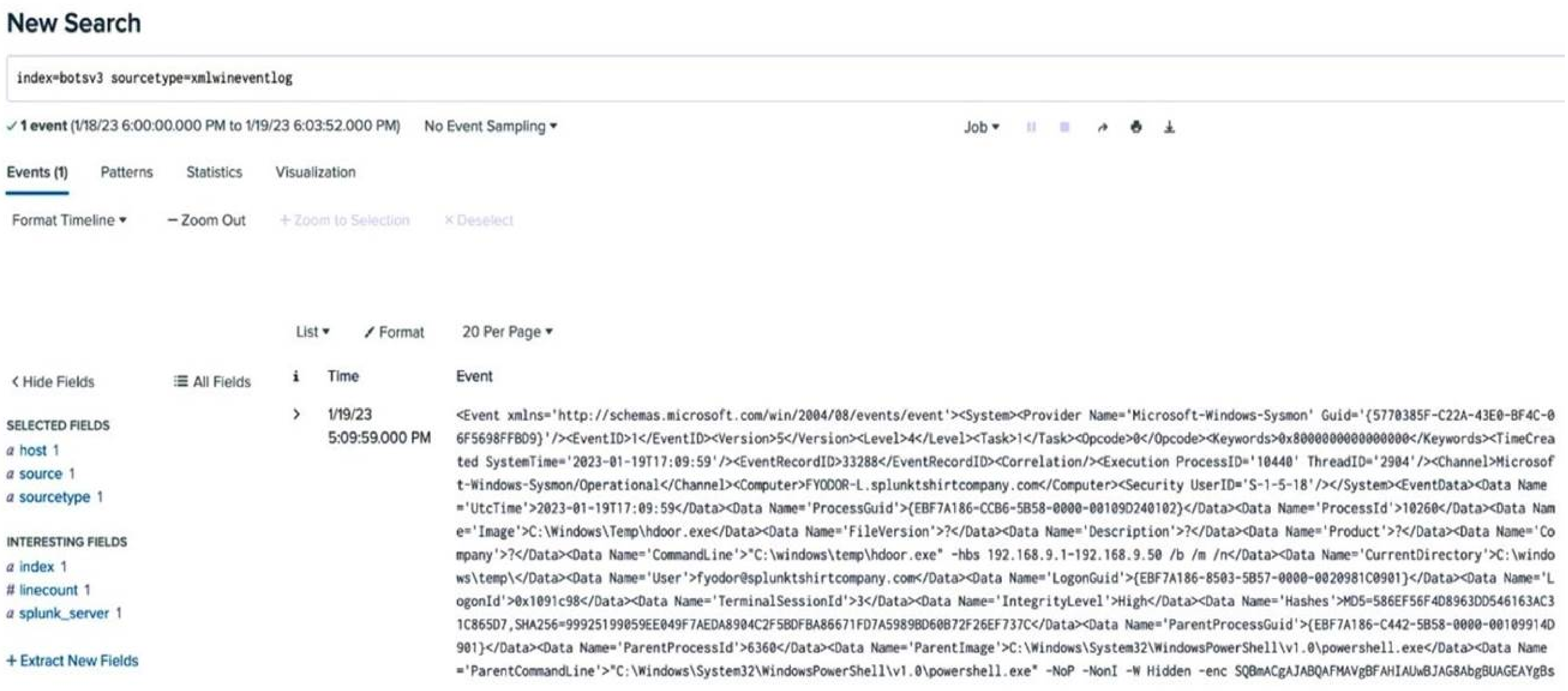
NEW QUESTION 4
An analyst is investigating how an attacker successfully performs a brute-force attack to gain a foothold into an organizations systems. In the course of the investigation the analyst determines that the reason no alerts were generated is because the detection searches were configured 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 5
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?



```
index=botsv3 sourcetype=xmlwineventlog
```

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-0
6F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCrea
ted SystemTime='2023-01-19T17:09:59'/><EventRecordID>33288</EventRecordID><Correlation/><Execution ProcessID='10440' ThreadID='2904'/><Channel>Microsof
t-Windows-Sysmon/Operational</Channel><Computer>FYODOR-L.splunktshirtcompany.com</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name
='UtcTime'>2023-01-19T17:09:59</Data><Data Name='ProcessGuid'>{EBF7A186-CCB6-5B58-0000-00109D240102}</Data><Data Name='ProcessId'>10260</Data><Data Nam
e='Image'>C:\Windows\Temp\hdoor.exe</Data><Data Name='FileVersion'>?</Data><Data Name='Description'>?</Data><Data Name='Product'>?</Data><Data Name='Co
mpany'>?</Data><Data Name='CommandLine'>"C:\windows\temp\hdoor.exe" -hbs 192.168.9.1-192.168.9.50 /b /m /n</Data><Data Name='CurrentDirectory'>C:\windo
ws\temp\</Data><Data Name='User'>fyodor@splunktshirtcompany.com</Data><Data Name='LogonGuid'>{EBF7A186-8503-5B57-0000-0020981C0901}</Data><Data Name='L
ogonId'>0x1091c98</Data><Data Name='TerminalSessionId'>3</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=586EF56F4D8963DD546163AC3
1C865D7,SHA256=99925199059EE049F7AEDA8904C2F5BDFBA86671FD7A5989BD60B72F26EF737C</Data><Data Name='ParentProcessGuid'>{EBF7A186-C442-5B58-0000-00109914D
901}</Data><Data Name='ParentProcessId'>6360</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name
='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc SQBmACgAJABQAFMAVgBFAHIAUwBJAG8AbgBUAGEAYgBs
```

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 6
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

Answer: C

Explanation:
? Continuous Monitoring Cycle:This cycle is part of a broader security strategy that involves constantly assessing and managing the security state of an organization's information systems. The phases generally include defining metrics, collecting data, analyzing it, reporting findings, and implementing improvements.
? Analyze and Report Phase:
? Purpose of Recommendations:The goal of this phase is to ensure that the organization??s security measures are continuously improved based on the latest data and threat landscape. It is a critical step in maintaining an effective security program that adapts to new challenges.
? NIST SP 800-137:This publication provides guidelines on continuous monitoring of information systems, detailing the processes involved, including the Analyze and Report phase.
? Security Operations Center (SOC) Best Practices:Many SOC frameworks emphasize the importance of the Analyze and Report phase in

NEW QUESTION 7
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

Answer: B

Explanation:
In Splunk, to filter users with over a thousand occurrences, the pipeline| stats count by user | where count > 1000 | sort - countis most effective. Thestats count by usercommand generates a count of occurrences for each user. Thewhereclause then filters out only those users who have more than 1000 occurrences. Finally,sort - countsorts the results in descending order by count. This approach is efficient for identifying outliers, such as users with a high number of events.

NEW QUESTION 8
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

Answer: A

Explanation:
To investigate which process initiated a network connection, an analyst would use theEndpointdata model in Splunk Enterprise Security. The Endpoint data model contains fields related to processes, file activity, and host-level data, which are essential for tracing back the source of suspicious network activity to the specific process or application that initiated it. This is crucial for understanding the scope of an attack and determining the origin of malicious network traffic.
Top of Form Bottom of Form

NEW QUESTION 9
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
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 10
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 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

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 14
An analyst is looking at Web Server logs, and sees the following entry as the last web request that a server processed before unexpectedly shutting down:
147.186.119.107 - - [28/Jul/2006:10:27:10 -0300] "POST /cgi-bin/shutdown/ HTTP/1.0" 200 3333
What kind of attack is most likely occurring?

A. Distributed denial of service attack.
B. Denial of service attack.
C. Database injection attack.
D. Cross-Site scripting attack.

Answer: B

Explanation:
The log entry indicates aPOST /cgi-bin/shutdown/request, which suggests that a command was sent to shut down the server via a CGI script. This kind of activity is indicative of aDenial of Service (DoS) attackbecause it involves sending a specific command that causes the server to stop functioning or shut down. This is different from a Distributed Denial of Service (DDoS) attack, which typically involves overwhelming the server with traffic rather than exploiting a specific command.

NEW QUESTION 15
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:
In Splunk, field extractions are essential for transforming raw log data into structured fields that are easier to work with during analysis. When the question refers to an analyst identifying helpful information in the raw logs that assists them in determining suspicious activity, the most effective way to streamline this process is throughfield extraction. This allows the Splunk system to automatically parse and tag the necessary data, making it more accessible for searches, dashboards, and alerts.
Let??s break down whyoption A: Create a field extraction for this informationis the best approach:
? Field Extraction Overview:
? Why Field Extraction?
? Comparison to Other Options:
? Cybersecurity Defense Analyst Best Practices:
References:
? Splunk Documentation: Field Extraction in Splunk
? Cybersecurity defense techniques emphasize the importance of making log data actionable, which aligns with common practices in Incident Detection & Response (IDR) environments. Structured data is key to this effort, and field extraction is a critical part of transforming raw logs into useful intelligence

NEW QUESTION 19
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

Answer: B

Explanation:
A briefing delivered by a Cyber Threat Intelligence (CTI) team to a Chief Information Security Officer (CISO) detailing the overall threat landscape is an example ofStrategicThreat Intelligence. Strategic intelligence focuses on high-level analysis of broader trends, threat actors, and potential risks to the organization over time. It is designed to inform senior leadership and influence long-term security strategies and policies. This contrasts withTacticalintelligence, which deals with immediate threats and actionable information, andOperationalintelligence, which is more focused on the details of specific threat actors or campaigns.

NEW QUESTION 23
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

Answer: C

Explanation:
Thestatscommand is used to generate statistics, such as counts, over specific fields. In this case, the commandindex=security_logs eventtype=failed_login | stats count as failed_attempts by src_ip | sort -failed_attemptscreates a temporary table that counts the number of failed login attempts (failed_attempts) for each source IP (src_ip). Thesort -failed_attemptsensures the results are ordered by the number of failed attempts in descending order, making it easier for an analyst to identify problematic IPs.

NEW QUESTION 26
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 30
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 Security Operations Center (SOC) manager is interested in creating a new dashboard for typosquatting after a successful campaign against a group of senior executives. Which existing ES dashboard could be used as a starting point to create a custom dashboard?

A. IAM Activity
B. Malware Center
C. Access Anomalies
D. New Domain Analysis

Answer: D

Explanation:
For creating a custom dashboard focused on typosquatting, theNew Domain Analysisdashboard in Splunk Enterprise Security (ES) would be a relevant starting point. Typosquatting typically involves the registration of domains similar to legitimate domains to deceive users, which is closely related to the analysis of newly registered or observed domains. This dashboard already includes tools and visualizations for monitoring and analyzing domain name activity, which can be adapted for the specific needs of monitoring for typosquatting.

NEW QUESTION 36
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 40
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 42
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

Answer: A

Explanation:
The log entry showing the same request repeated millions of times indicates aDenial of Service (DoS) Attack, where the server is overwhelmed by a flood of requests to a specific resource, in this case, the/login/page. This type of attack is aimed at making the server unavailable to legitimate users by exhausting its resources.
? Denial of Service Attack:
? Incorrect Options:
? Web Server Security:Understanding DoS attacks is critical for securing web servers and mitigating these types of disruptions.

NEW QUESTION 46
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 47

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.

Answer: D

Explanation:

In Splunk Enterprise Security, theRisk Event Timelineprovides a chronological view of risk events associated with a particular Risk Object, such as a user or device. This timeline helps analysts visualize and understand the sequence and nature of risk events over time, aiding in the investigation of security incidents.
? Risk Event Timeline:
? Incorrect Options:
? Splunk Documentation:Risk Event Timeline in Splunk Enterprise Security provides step-by-step details on how to access and interpret the timeline.

NEW QUESTION 49

......

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

100% Actual & Verified — Instant Download, Please Click
Order The SPLK-5001 Practice Test Here