Splunk

Exam Questions SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Which of the following is a correct Splunk search that will return results in the most performant way?

A. index=foo host=i-478619733 | stats range(_time) as duration by src_ip | bin duration span=5min | stats count by duration, host
B. | stats range(_time) as duration by src_ip | index=foo host=i-478619733 | bin duration span=5min | stats count by duration, host
C. index=foo host=i-478619733 | transaction src_ip |stats count by host
D. index=foo | transaction src_ip |stats count by host | search host=i-478619733

Answer: A

Explanation:
The correct Splunk search that returns results in the most performant way is index=foo host=i-478619733 | stats range(_time) as duration by src_ip | bin duration span=5min | stats count by duration, host. This search is optimized by:
? Starting with the most specific search criteria (index and host) to reduce the data set.
? Applying aggregation functions (stats) early, which helps minimize the amount of data processed in subsequent commands.
? Usingbinto group data efficiently before performing further statistical calculations.
? Search Optimization:
? Performance Considerations:
? Splunk Search Documentation:The official Splunk documentation provides guidelines on how to construct efficient searches, including the best practices for usingstats,bin, and indexing.
? Splunk Performance Tuning Guides:These guides offer in-depth advice on optimizing searches for speed and efficiency, with examples of common pitfalls and how to avoid them.

NEW QUESTION 2
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:
TheTERM()search command in Splunk allows an analyst to match a specific term exactly as it appears, even if it contains characters that are usually considered minor breakers, such as periods or underscores. By usingTERM(), the search engine treats everything inside the parentheses as a single term, which is especially useful for searching log data where certain values (like IP addresses or filenames) should be matched exactly as they appear in the logs.

NEW QUESTION 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 15
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 20
There are many resources for assisting with SPL and configuration questions. Which of the following resources feature community-sourced answers?

A. Splunk Answers
B. Splunk Lantern
C. Splunk Guidebook
D. Splunk Documentation

Answer: A

Explanation:
Splunk Answersis a community-driven Q&A platform where users can ask questions and share knowledge about Splunk. It is known for providing community-sourced answers to a wide rangeof questions, including SPL (Search Processing Language) queries, configuration issues, and general best practices. Users can contribute by answering questions based on their own experiences, making it a valuable resource for troubleshooting and learning.
? B. Splunk Lantern:This is a resource for best practices, how-tos, and use case guides, but it??s not a community-sourced Q&A platform.
? C. Splunk Guidebook:This is not a known resource in the context of community- sourced answers.
? D. Splunk Documentation:While highly detailed and official, it is not community- sourced but rather maintained by Splunk's own teams.
? Splunk Answers Platform:Splunk Answers
Incorrect Options:References:

NEW QUESTION 25

The field file_acl contains access controls associated with files affected by an event. In which data model would an analyst find this field?

A. Malware
B. Alerts
C. Vulnerabilities
D. Endpoint

Answer: D

Explanation:
Thefile_aclfield, which contains access controls associated with files affected by an event, is part of theEndpointdata model in Splunk. The Endpoint data model is designed to include information related to file access, process activity, and user activity on endpoints. Fields likefile_aclare critical for understanding permissions and potential security risks associated with file access and manipulation, which are key aspects of endpoint security monitoring.

NEW QUESTION 26
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

Answer: C

Explanation:
In most organizations, the Security Engineer is typically responsible for implementing new processes or solutions that have been selected to protect assets. This role involves the practical application of security tools, technologies, and practices to safeguard the organization??s infrastructure and data.
? Role of Security Engineer:
? Contrast with Other Roles:
? Job Descriptions and Industry Standards:Detailed descriptions of Security Engineer roles in job postings and industry standards highlight their responsibilities in implementing security solutions.
? Security Operations Best Practices:These documents and guidelines often outline the division of responsibilities in a security team, confirming that Security Engineers are the primary implementers.

NEW QUESTION 31
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 36
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.

Answer: D

Explanation:
A threat hunt is an iterative process where a hypothesis is developed and tested against data in an environment to detect the presence of threats or adversarial

tactics, techniques, and procedures (TTPs).
? Understanding the Hypothesis:
? Search and Analysis:
? Evaluation of the Hypothesis:
? Successful Threat Hunt:
? MITRE ATT&CK Framework:Understanding how threat actors utilize tactics like Cobalt Strike for C2 can be aligned with TTPs in the framework, helping to build effective hypotheses.
? Threat Hunting Resources:Books like "The Threat Hunter's Handbook" often describe scenarios where proving a negative (i.e., the absence of a threat) is a valid and successful outcome of a hunt.
Outcome of the Threat Hunt:References:

NEW QUESTION 41
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 44
While the top command is utilized to find the most common values contained within a field, a Cyber Defense Analyst hunts for anomalies. Which of the following Splunk commands returns the least common values?

A. least
B. uncommon
C. rare
D. base

Answer: C

Explanation:
In Splunk, therarecommand is used to return the least common values in a field. This command is particularly useful for anomaly detection, as it helps identify unusual or infrequent occurrences in a dataset, which may indicate potential security issues.
? rare Command:
? Incorrect Options:
? Splunk Command Documentation:rare command usage for identifying uncommon values.

NEW QUESTION 47
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

Answer: A

Explanation:
Splunk Enterprise Security (ES) provides various features to enhance security monitoring, analysis, and incident response. One of the powerful features in Splunk ES isAnnotations. This feature allows security analysts to map and categorize correlation search results according to well-known industry frameworks such as the CIS Critical Security Controls, MITRE ATT&CK, and the Lockheed Martin Cyber Kill Chain®.
? Purpose of Annotations:
? How Annotations Work:
? Integration with Frameworks:
Annotations in Splunk ES:Practical Example:Consider a correlation search that detects unusual behavior indicating potential lateral movement within a network. If this alert is annotated with a reference to the MITRE ATT&CK framework, it might map to techniques like "T1021 - Remote Services," which is associated with the lateral movement tactic. This mapping not only categorizes the event but also helps in planning the next steps for containment and investigation.
? Efficiency in Response:By aligning alerts with industry frameworks, annotations
help in quickly identifying the nature and potential impact of a threat.
? Consistency in Analysis:Provides a standardized method for categorizing and responding to alerts, ensuring that all analysts interpret and react to threats in a consistent manner.
? Improved Reporting:Allows for better visualization and reporting of threats according to established frameworks, making it easier to communicate risks and actions to stakeholders.
? Splunk Documentation:Annotations in Splunk ES
? MITRE ATT&CK Framework:MITRE ATT&CK®
? Lockheed Martin Cyber Kill Chain®:Cyber Kill Chain
? CIS Critical Security Controls:CIS Controls
Why Annotations Are Important:References:

NEW QUESTION 50
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 55
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

Answer: A

Explanation:
? Unusual Traffic Patterns:
? Possible Threat Activities:
Scenario Analysis:Conclusion:Given the evidence of large data transfers to a single external system without corresponding inbound traffic,data exfiltrationis the most likely scenario. This suggests that an adversary has compromised the server and is extracting valuable or sensitive data from the organization.
? Data Exfiltration Techniques:Techniques such as those documented in the MITRE
ATT&CK framework (e.g.,T1041 - Exfiltration Over C2 Channel) detail how attackers move data out of a network.
? Incident Response Playbooks:Many incident response frameworks emphasize monitoring for unusual outbound traffic as a primary indicator of data exfiltration.

NEW QUESTION 59
An organization is using Risk-Based Alerting (RBA). During the past few days, a user account generated multiple risk observations. Splunk refers to this account as what type of entity?

A. Risk Factor
B. Risk Index
C. Risk Analysis
D. Risk Object

Answer: D

Explanation:
In Splunk??s Risk-Based Alerting (RBA) framework, aRisk Objectrefers to the specific entity (such as a user account, IP address, or host) that is associated with risk observations. When auser account generates multiple risk observations, it is labeled as a Risk Object, allowing security teams to track and manage risk more effectively.
? Risk Object:
? Incorrect Options:
? Splunk RBA Documentation:Detailed descriptions of how Risk Objects function within the Risk-Based Alerting framework.

NEW QUESTION 64
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 69
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 74
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 78
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:
Themakeresultscommand in Splunk is used to generate a single-row result that can be used to create test data within a search pipeline. This command is particularly useful for testing and experimenting with SPL commands on a small set of synthetic data without relying on existing logs or events in the Splunk index. It is commonly used by analysts who want to test commands or SPL syntax before applying them to real data.

NEW QUESTION 80
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 83
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 85
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 90
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 93
An analyst needs to create a new field at search time. Which Splunk command will dynamically extract additional fields as part of a Search pipeline?

A. rex
B. fields
C. regex
D. eval

Answer: A

Explanation:
In Splunk, therexcommand is used to extract fields from raw event data using regular expressions. This command allows analysts to dynamically extract additional fields as part of a search pipeline, which is crucial for creating new fields during search time based on specific patterns found in the log data. Therexcommand is highly flexible and powerful, making it essential for refining and manipulating data in a Splunk environment. The other options (fields,regex,eval) have their uses, butrexis specifically designed for dynamic field extraction.

NEW QUESTION 98
.....

Relate Links

100% Pass Your SPLK-5001 Exam with Exambible Prep Materials

https://www.exambible.com/SPLK-5001-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/