



Splunk

Exam Questions SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

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.

? Using binto 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 using stats, 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:

The TERM() 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 using TERM(), 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:

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

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

Answer: D

Explanation:

Adaptive Response is a feature in Splunk's Enterprise Security (ES) framework that allows security teams to automate actions and responses based on alerts or notable events. This feature is pivotal for orchestrating automated incident response processes, reducing the time between detection and response, and integrating Splunk with external systems to trigger appropriate actions.

? Purpose: Adaptive Response enables the automation of specific tasks or workflows

based on security events detected by Splunk ES. For instance, it can trigger actions such as isolating a compromised host, blocking IP addresses, or enriching data by querying additional sources when a notable event occurs.

? Mechanism: When a notable event is identified within the Splunk platform, Adaptive

Response can execute a series of predefined actions. These actions can be configured within the Splunk interface, allowing them to run automatically or with manual approval depending on the organization's needs. This capability is essential for streamlining security operations, especially in environments where quick response is critical.

? Integration with External Applications:One of the key features of Adaptive

Response is its ability to integrate with third-party security tools and solutions. This integration extends the capabilities of Splunk by allowing it to interact with other systems like firewalls, intrusion prevention systems (IPS), endpoint detection and response (EDR) tools, and ticketing systems. This ensures a coordinated and comprehensive defense mechanism.

? Usage in Security Operations:Security analysts often rely on Adaptive Response

for managing and automating common security tasks, such as:

? Splunk Documentation:Splunk Enterprise Security has detailed guides and resources explaining how Adaptive Response functions within the platform and how to configure and use it effectively. You can access the official documentation for more in-depth technical instructions and examples.

? Splunk Education:Splunk offers training courses specifically for Splunk ES, where Adaptive Response is covered as a key topic. These resources provide practical insights and best practices from experienced Splunk users.

? Security Analyst Community Discussions:Forums and community discussions are excellent resources where analysts share their experiences and configurations using Adaptive Response, often with detailed examples and troubleshooting tips.

References:Adaptive Response is a powerful tool for any Security Operations Center (SOC) aiming to enhance their incident response capabilities, making it a critical feature within Splunk's Enterprise Security framework.

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

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 7

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

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

Answer: A

Explanation:

In the context of Intrusion Detection Systems (IDS), determining whether an event is a True Negative, True Positive, False Negative, or False Positive depends on the system's detection and the reality of the situation.

Let's break down the scenario: IDS Signature Explanation:

The IDS is set to detect and alert on logins to a server, but only if they happen during a specific time window, from 6:00 PM to 6:00 AM.

The question states that no alerts occur during this time frame, but the IDS signature is known to be correct.

Understanding Detection Terms:

True Positive: The IDS correctly detects an intrusion or suspicious activity that is actually happening.

True Negative: The IDS does not detect any activity because no suspicious or malicious activity is occurring, and this lack of detection is correct.

False Positive: The IDS detects an intrusion or activity, but it is a false alarm (i.e., there is no real threat).

False Negative: The IDS fails to detect a real intrusion or activity when it should have, missing a legitimate alert.

Applying the Scenario:

In this case, no IDS alerts occurred during the specified time frame. If there were no actual logins during this period and the signature was designed correctly, then the absence of alerts is expected and appropriate.

Since no suspicious logins occurred, and the IDS did not trigger any alerts, this situation represents a True Negative—the system correctly identified that there was no suspicious activity to alert on.

Why the Answer is "True Negative":

The IDS signature is working as expected.
The condition that would trigger an alert (logins during the specified time) did not happen, so the lack of alerts is a correct response.
Therefore, this is classified as a True Negative because no malicious activity took place, and the IDS correctly refrained from raising an alert.
Comparison to Other Options:
* B. True Positive – This would indicate that an alert occurred because of actual suspicious activity, but in this case, no alerts occurred.
* C. False Negative – This would mean that suspicious activity occurred, but the IDS failed to detect it. In this case, there was no activity to detect, so this option is not correct.
* D. False Positive – This would suggest the IDS raised an alert when no suspicious activity happened, but again, no alerts occurred, so this doesn't apply.
References:
Cybersecurity analysts working with IDS systems frequently use concepts like True Negative and False Positive in evaluating the effectiveness of their detection tools.
The correct handling of such detection cases is critical to minimizing unnecessary alerts (False Positives) and ensuring real threats are not missed (avoiding False Negatives).

NEW QUESTION 8

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 the most likely cause?

New Search

index=botsv3 sourcetype=xmlwineventlog

✓ 1 event (1/18/23 6:00:00.000 PM to 1/19/23 6:03:52.000 PM) No Event Sampling

Job

Events (1)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

Hide Fields

All Fields

Time

Event

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a index 1

linecount 1

a splunk_server 1

+ Extract New Fields

1/19/23

5:09:59.000 PM

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFB09}" /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2023-01-19T17:09:59"/><EventRecordID>33288</EventRecordID><Correlation/><Execution ProcessID="10440" ThreadID="2904" /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>FY0D0R-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 Name="Image">C:\Windows\Temp\hdoor.exe</Data><Data Name="FileVersion">?</Data><Data Name="Description">?</Data><Data Name="Product">?</Data><Data Name="Company">?</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:\windows\temp\</Data><Data Name="User">fyodor@splunktshirtcompany.com</Data><Data Name="LogonGuid">{EBF7A186-8503-5B57-0000-0020981C0901}</Data><Data Name="LogonId">0x1091c98</Data><Data Name="TerminalSessionId">3</Data><Data Name="IntegrityLevel">High</Data><Data Name="Hashes">MD5=586EF56F4D8963DD546163AC31C865D7,SHA256=99925199059EE049F7AEDA8904C2F58DFBA86671FD7A59898D60B72F26EF737C</Data><Data Name="ParentProcessGuid">{EBF7A186-C442-5B58-0000-00109914D901}</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</Data></EventData></Event>

- 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 exctract command to their search pipeline.
- D. The analyst is not in the Droouer 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 Mode or Verbose Mode are better suited for 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 9

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

Guaranteed success with Our exam guides

visit - <https://www.certshared.com>

NEW QUESTION 10

A Cyber Threat Intelligence (CTI) team produces a report detailing a specific threat actor's typical behaviors and intent. This would be an example of what type of intelligence?

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

Answer: C

Explanation:

Tactical intelligence provides insights into the specific behaviors, tools, and techniques used by threat actors. When a Cyber Threat Intelligence (CTI) team produces a report detailing a threat actor's typical behaviors and intent, they are delivering tactical intelligence. This type of intelligence is actionable and directly supports defenders in identifying, mitigating, and responding to threats in a timely manner.

? Tactical Intelligence:

? Incorrect Options:

? CTI Frameworks: Standards such as the MITRE ATT&CK framework, which classify tactical intelligence within the spectrum of threat intelligence.

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:

An Intrusion 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

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 Answers is 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 range of 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 is 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 20

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

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

Answer: A

Explanation:

The Common Information Model (CIM) in Splunk is a crucial component that allows for the normalization and standardization of data across various sources. By using CIM, disparate data sources can be mapped to a common schema, which makes it significantly easier to correlate and analyze data across different logs and systems.

? Purpose of CIM: CIM provides a standardized format for fields and event types

across various data sources in Splunk. This normalization allows analysts to use consistent field names and structures when performing searches, regardless of the original data source's format.

? Benefit of Easier Correlation: One of the primary challenges in security operations

is correlating data from different sources—like firewalls, intrusion detection systems (IDS), endpoint security solutions, and network logs—to identify potential security incidents. CIM facilitates this by ensuring that all relevant data adheres to a common schema, enabling seamless correlation and analysis. For example, CIM allows a security analyst to write a single query that can apply to data from multiple sources, simplifying the detection of complex threats.

? How it Works: CIM is implemented through data models in Splunk, which act as a

blueprint for mapping and transforming raw data into a structured format. These data models cover a wide range of security domains, such as authentication, network traffic, and malware, ensuring that data from different security tools can be

easily integrated and analyzed together.

? Use Cases:The primary use cases for CIM include:

? Splunk CIM Documentation:The official documentation provides comprehensive guides on how to implement and use CIM for various data sources, including detailed field mappings and examples.

? Splunk Security Essentials:This resource offers practical examples and pre-built use cases that utilize CIM for effective security operations.

? Community Blogs and Discussions:Many experienced Splunk users share best practices for using CIM in forums and blogs, where they discuss real-world applications and troubleshooting tips.

NEW QUESTION 21

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 26

The United States Department of Defense (DoD) requires all government contractors to provide adequate security safeguards referenced in National Institute of Standards and Technology (NIST) 800-171. All DoD contractors must continually reassess, monitor, and track compliance to be able to do business with the US government.

Which feature of Splunk Enterprise Security provides an analyst context for the correlation search mapping to the specific NIST guidelines?

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

Answer: D

Explanation:

Splunk Enterprise Security provides a feature calledFramework Mappingthat allows correlation searches to be mapped to specific cybersecurity frameworks, including NIST 800-171, which is crucial for DoD contractors. This mapping provides context to the analyst by showing how particular searches align with compliance requirements, aiding in continuous monitoring and reassessment as mandated by the DoD. This feature is integral for organizations that need to demonstrate compliance with NIST guidelines and other security frameworks.

NEW QUESTION 27

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 32

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 35

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 38

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 42

What is the following step-by-step description an example of?

- * 1. The attacker devises a non-default beacon profile with Cobalt Strike and embeds this within a document.
- * 2. The attacker creates a unique email with the malicious document based on extensive research about their target.
- * 3. When the victim opens this document, a C2 channel is established to the attacker??s temporary infrastructure on a compromised website.

- A. Tactic
- B. Policy
- C. Procedure
- D. Technique

Answer: D

Explanation:

The step-by-step description provided is an example of aTechniqueas defined in the MITRE ATT&CK framework. Techniques are the specific methods adversaries use to achieve their objectives during an attack, such as establishing command and control (C2) channels or delivering payloads via phishing emails. In this scenario, the attacker uses a non-default beacon profile in Cobalt Strike, sends a malicious document via email, and establishes a C2 channel once the victim interacts with the document, all of which are examples of adversary techniques.

NEW QUESTION 45

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 47

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 of Strategic Threat 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 with Tactical intelligence, which deals with immediate threats and actionable information, and Operational intelligence, which is more focused on the details of specific threat actors or campaigns.

NEW QUESTION 50

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, the Implement and Collect stage 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 as Analyze and Report, are more focused on the interpretation and presentation of this data after collection.

NEW QUESTION 53

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:

The stats command is used to generate statistics, such as counts, over specific fields. In this case, the command `index=security_logs eventtype=failed_login | stats count as failed_attempts by src_ip | sort -failed_attempts` creates a temporary table that counts the number of failed login attempts (failed_attempts) for each source IP (src_ip). The sort -failed_attempts ensures 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 55

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 57

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:

The `makeresults` command 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 59

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 the `C:\Windows\Temp` directory 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 from `C:\Windows\Temp` warrants 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 63

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 of Least 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 68

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:

The `eval` SPL expression in Splunk supports several categories of functions, including JSON functions (e.g., `spath`), Text functions (e.g., `substr`, `trim`), and Comparison and Conditional functions (e.g., `if`, `case`). However, Threat functions are not a valid category within the `eval` command. The `eval` command 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 69

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 a Denial 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 70

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 71

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

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

Answer: D

Explanation:

The Splunk Security Content library, which includes apps like ESCU (Enterprise Security Content Update) and SSE (Splunk Security Essentials), primarily consists of Dashboards, Reports, and Correlation Searches. Validated architectures are not a component of these content libraries. Instead, validated architectures refer to predefined, best-practice designs for deploying and configuring Splunk in a way that ensures optimal performance and scalability, which is separate from the content libraries focused on delivering security detections and visualizations.

Top of Form Bottom of Form

NEW QUESTION 72

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, the rex command 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. The rex command 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, but rex is specifically designed for dynamic field extraction.

NEW QUESTION 77

.....

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](#)