www.atmicnetworks.com

ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

www.atmicnetworks.com

Question: 1

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:

Quarantine or isolate a hostin response to malware detection.

Trigger a full disk scan when suspicious activity is detected.

Notify relevant stakeholders through ticketing systems or direct communication tools.

Update firewall rules to block traffic from a suspicious IP address.

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.

Question: 2

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:

Annotations help analysts understand and categorize security events by aligning them with recognized security frameworks. This alignment provides context, making it easier to understand the nature of threats and how they fit within broader threat models or attack strategies.

How Annotations Work:

When a correlation search in Splunk ES triggers an alert, Annotations can automatically tag the alert with relevant tactics, techniques, and procedures (TTPs) from frameworks like MITRE ATT&CK. This helps in categorizing the event within the context of known attack patterns, offering insights into potential next steps by an attacker and recommended defensive actions.

Annotations can be manually added or configured to be applied automatically based on the nature of the search results.

Integration with Frameworks:

MITRE ATT&CK: Annotations can map alerts to specific techniques and tactics in the MITRE ATT&CK framework, which provides a detailed knowledge base of adversary behaviors, tactics, and techniques.

CIS Critical Security Controls: These controls can also be mapped through annotations, allowing the organization to measure and improve its security posture against these controls.

Lockheed Martin Cyber Kill Chain®: This model focuses on the stages of a cyberattack, and annotations can help identify where in the kill chain a particular alert fits, providing a clearer understanding of the attack's progression.

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

Question: 3

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.
C. It improves the performance of search queries on raw data.
D. It enables the use of advanced machine learning algorithms.
E. 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:

Search and Reporting: Creating efficient and standardized searches that apply across multiple data sources.

Dashboards and Visualizations: Building dashboards that pull in data from various sources in a consistent manner.

Correlation Searches: Developing correlation searches that detect patterns or anomalies across different types of data, enhancing threat detection.

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.

Question: 4

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):

Tactics: The high-level goals that attackers aim to achieve during an attack. For example, gaining initial access to a network.

Techniques: The specific methods used to achieve these tactics, such as phishing or exploiting a vulnerability.

Procedures: The detailed steps and tools that attackers use to implement a technique.

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:

Mapping Detection and Defense: Organizations can map their existing detection capabilities against the ATT&CK matrix to identify gaps.

Threat Hunting: Security teams use the framework to guide their threat-hunting activities, focusing on specific techniques associated with known adversaries.

Incident Response: During incident response, analysts can use the ATT&CK framework to understand the behaviors exhibited by an attacker, which helps in creating effective containment and eradication strategies.

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.

Reference: 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.

Question: 5

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:

The hypothesis here is that a threat actor might userundll32 for proxy execution of malicious code and leverage Cobalt Strike for command and control (C2).

The hunt would involve looking for indicators of these specific activities in logs and artifacts like Sysmon logs, netflow, IDS alerts, and EDR data.

Search and Analysis:

The threat hunter performed an extensive search across multiple log sources and found no evidence of Cobalt Strike or the specific malicious activities hypothesized.

Evaluation of the Hypothesis:

If the hypothesis were proven true,the presence of Cobalt Strike or related artifacts would be detected.

However, the hypothesis was not proven; instead, the hunt provided strong evidence that Cobalt Strike and the hypothesized malicious activities are not present.

Successful Threat Hunt:

The goal of threat hunting is not always to find a threat but to gain confidence in the security posture of the environment.

Outcome of the Threat Hunt:
Outcome D correctly identifies that the hunt was successful because it provided strong evidence supporting the absence of the hypothesized threat, thus improving confidence in the organization's security.

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.

Question: 6

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

www.atmicnetworks.com

Explanation:

Unusual Traffic Patterns:

The key observation here is that one of the servers is sending out a significantly large amount of data to a single external system, with no corresponding increase in incoming traffic.

Possible Threat Activities:

A. Data Exfiltration:

This scenario typically aligns with data exfiltration, where an attacker has successfully compromised a system and is sending out large volumes of stolen data to an external server.

Data exfiltration often involves consistent or large data transfers over time to an external IP address, which matches the description provided.

C. Network Reconnaissance:

While reconnaissance involves scanning and probing, it generally does not produce large outbound data flows but rather small, frequent connection attempts or queries.

C. Data Infiltration:

Infiltration would involve incoming data to the compromised server, which contradicts the scenario as there is no observed increase in incoming traffic.

D. Lateral Movement:

Lateral movement would involve traffic between internal systems rather than large amounts of data being sent to an external system.

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.

Question: 7

In which phase of the Continuous Monitoring cycle are suggestions and improvements typically made?

A. Define and Predict
D. Establish and Architect
E. Analyze and Report
F. Implement and Collect

www.atmicnetworks.com

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:

Data Evaluation: In this phase, the data collected from various monitoring tools and sensors is thoroughly analyzed. Security analysts look for trends, anomalies, and indications of potential threats or vulnerabilities.

Reporting: After the analysis, a report is generated that highlights the findings, including any detected issues, their potential impact, and the current effectiveness of security measures.

Recommendations: Based on the analysis, the report usually includes suggestions for improvements, such as additional security controls, configuration changes, or policy updates. These recommendations are aimed at enhancing the organization's security posture and addressing any identified gaps or weaknesses.

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

Question: 8

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:

Explore Use Cases: Discover how specific data sources can be used to detect different types of security threats.

Assess Data Completeness: Evaluate whether all relevant data sources are being ingested and utilized within Splunk.

Optimize Security Monitoring: Identify new opportunities for enhancing security monitoring by integrating additional data sources or improving the use of existing ones.

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.

Question: 9

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\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:

World Writable: Temporary directories like C:\Windows\Tempare typically writable by all users, which reduces the complexity for an attacker to place and execute malicious files.

Lack of Permissions Control: Since these directories do not have strict permission controls, attackers can easily exploit them to execute malicious payloads without being hindered by file access restrictions.

Security Risks:

Malware Staging: Attackers often use temp directories to stage malware because they can avoid detection by traditional security controls that monitor more critical directories like system folders.

Persistence Mechanisms: Some malware will persist in these directories and execute from them each time the system starts or when a particular trigger is activated.

Privilege Escalation: In some cases, malicious files placed in temp directories can be executed by more privileged processes, leading to privilege escalation.

Investigation Importance: The fact that an executable is running from C:\Windows\Tempwarrants further investigation to determine whether it is malicious. Analysts should check:

File Origin: How the file got there, which user or process created it.

Behavior: What the executable is doing, such as establishing network connections, modifying system settings, or interacting with other sensitive files.

Integrity: Whether the executable is a legitimate system file or a potential piece of malware.

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.

Question: 10

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, the Risk 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:

The Risk Event Timeline is accessible by clicking the risk event count associated with a Risk Object in the Incident Review dashboard. This action opens up the timeline view, which provides a detailed chronological

perspective on how risk events have unfolded.

This feature is particularly useful for tracking the progression of threats and understanding the context of incidents.

Incorrect Options:

A. Running the Risk Analysis Adaptive Response action within the Notable Event: This option pertains to running a response action rather than visualizing risk events over time.

B. Via a workflow action for the Risk Investigation dashboard: Although workflow actions can lead to various dashboards, the specific visualization described is accessed via the Risk Event Timeline.

C. Via the Risk Analysis dashboard under the Security Intelligence tab in Enterprise Security: While this dashboard provides valuable insights into risk data, the specific chronological visualization is found in the Risk Event Timeline.

Splunk Documentation: Risk Event Timeline in Splunk Enterprise Security provides step-by-step details on how to access and interpret the timeline.

Question: 11

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 through field 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 why option A: Create a field extraction for this information is the best approach:

Field Extraction Overview:

Field extraction is a process within Splunk that takes unstructured log data and converts it into structured fields. This makes it possible to directly query and display these fields, allowing analysts to quickly find and use relevant data in their investigations.

For example, if the logs contain IP addresses, user IDs, file names, or activity types, extracting these fields enables the analyst to filter and correlate data much more effectively without manually scanning the raw logs.

Why Field Extraction?

In this case, the question suggests that the raw logs contain information that helps determine whether activity is malicious. By creating field extractions for the relevant data points, analysts can use those structured fields to build queries and visualizations, drastically speeding up analysis time.

Analysts can write custom Splunk queries to isolate events that meet specific conditions, such as matching specific cloud sharing activities associated with risk notables.

Field extraction improves not only real-time analysis but also supports retrospective analysis and incident correlation across multiple events.

Comparison to Other Options:

Option B: Add this information to the risk message– While adding more context to a risk message could be useful for reviewing individual alerts, it doesn't improve the efficiency of log analysis. The analyst still would need to go back and manually inspect raw logs for more detailed data.

Option C: Create another detection for this information– Creating additional detections adds more rules,

but doesn't solve the fundamental issue of having raw logs that aren't easily searchable. You can only build effective detections when you have structured data available.

Option D: Allowlist more events based on this information– Allowlisting is generally used to reduce noise or irrelevant logs, but it doesn't help extract the necessary details for analysis. It may reduce unnecessary alerts, but won't help analyze the suspicious events that do arise.

Cybersecurity Defense Analyst Best Practices:

Field extractions should be created for any important log source or data point, especially when handling complex or multi-part log entries (e.g., cloud sharing logs). This ensures logs are searchable and actionable, allowing for faster identification of anomalies and malicious activity.

Analysts should collaborate with engineers to ensure these extractions are tuned and validated. The extraction should be tailored to isolate the fields most relevant for identifying suspicious activity.

Once fields are extracted, analysts can create dashboards, real-time alerts, or retrospective searches based on the structured data for more effective incident response.

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

Question: 12

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:

IDS are deployed at strategic points within the network, often at the perimeter, to monitor incoming and outgoing traffic for signs of malicious activity.

These systems are configured to detect various types of threats, including C2 traffic, which is a key indicator of compromised systems communicating with an attacker-controlled server.

Incorrect Options:

A. Host-based firewall: This is more focused on controlling traffic at the endpoint level, not at the network perimeter.

B. Web proxy: Primarily used for controlling and filtering web traffic, but not specifically designed to detect C2 traffic.

C. Endpoint Detection and Response (EDR):Focuses on endpoint protection rather than monitoring network perimeter traffic.

Network Security Practices: IDS implementation is a standard practice for perimeter security to detect early signs of network intrusion.

Question: 13

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: B

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:

A DoS attack involves a single attacker (or sometimes a small number of sources) sending a massive number of requests to a target server, overwhelming its ability to handle legitimate traffic.

The repetitive log entries reflect the server's inability to process legitimate requests due to the overwhelming number of identical requests.

Incorrect Options:

B. Distributed Denial of Service Attack: This involves multiple sources attacking simultaneously. The log provided does not indicate multiple sources, which would be characteristic of a DDoS attack.

C. Cross-Site Scripting Attack: This attack involves injecting malicious scripts into webpages viewed by other users, not overwhelming a server with traffic.

D. Database Injection Attack: This is an attack against a database via SQL injection or similar techniques, not overwhelming a server with traffic.

Web Server Security: Understanding DoS attacks is critical for securing web servers and mitigating these types of disruptions.

Question: 14

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:

David Bianco's Pyramid of Pain is a framework used to understand the effectiveness of different types of indicators in detecting and responding to cyber threats. The Pyramid of Pain categorizes indicators based on how difficult they are for an attacker to change and thus how painful it would be for them if these indicators were used for detection or prevention.

Hash values: These are the easiest indicators for attackers to change. Hash values correspond to specific files or artifacts. If a hash value is detected and blocked, attackers can easily modify the file slightly to change the hash and bypass detection. Therefore, using hash values for continuous monitoring is least effective, as attackers can quickly adapt.

Domain names: While more challenging to change than hash values, domain names can still be modified relatively easily by attackers (e.g., by registering new domains).

Network artifacts: These refer to network behaviors and patterns that are indicative of malicious activity. While not as easily changed as domain names or hash values, attackers can still modify their network behavior or use different protocols to avoid detection.

Tactics, Techniques, and Procedures (TTPs): These are the hardest for attackers to change. TTPs describe the methods and strategies that attackers use to achieve their objectives. Changing TTPs requires significant effort and often indicates a fundamental change in the attacker's methodology. Therefore, TTPs are the most valuable indicators for continuous monitoring.

Hash values are the least effective indicator type for continuous monitoring in the Pyramid of Pain framework because attackers can easily alter files to produce different hash values, making it an ineffective means of detection over time. This contrasts with TTPs, which are more fundamental to the attacker's strategy and harder to change, providing a more reliable means of detection.

Question: 15

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:

Implementation: Security Engineers are tasked with the hands-on deployment and configuration of security systems, including firewalls, intrusion detection systems (IDS),and endpoint protection solutions. When a risk is identified, they are the ones who implement the necessary technological controls or processes to mitigate that risk.

Technical Expertise: Security Engineers possess the technical skills required to integrate new solutions into the existing environment, ensuring that they operate effectively without disrupting other systems.

Collaboration: While Security Architects design the overall security architecture and the SOC Manager oversees operations, the Security Engineer works on the ground, implementing the detailed aspects of the solutions.

Contrast with Other Roles:

Security Architect: Designs the security framework and architecture but does not usually perform the actual implementation.

SOC Manager: Oversees the security operations and might coordinate the response but does not directly implement new solutions.

Security Analyst: Monitors and analyzes security data, but typically does not implement new security systems.

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.

Question: 16

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 isindex=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:

Efficient Indexing: By specifyingindex=fooandhost=i-478619733at the start, the search limits the scope of data that needs to be processed, which significantly improves performance.

Early Aggregation: The stats command is used early in the search to aggregate data bysrc_ip, which reduces the volume of data passed to the next stages of the pipeline.

Use of bin: Grouping durations with bin before performing a second stats aggregation reduces the number of unique values, making the final stats calculation more efficient.

Performance Considerations:

Order of Operations: Splunk processes search commands from left to right. Starting with a broad data retrieval and then narrowing down with stats and bin commands ensures that the least amount of data is processed in the final stages.

Avoiding Suboptimal Patterns:T he other options either apply operations in a less efficient order or involve unnecessary steps that increase processing time and resource usage.

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.

Question: 17

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 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.

Incorrect Options:

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.

Question: 18

A successful Continuous Monitoring initiative involves the entire organization. When an analyst discovers the need for more context or additional information, perhaps from additional data sources or altered correlation rules, to what role would this request generally escalate?

A. SOC Manager
B. Security Analyst
C. Security Engineer

D. Security Architect

Answer: C Explanation:

In a successful Continuous Monitoring initiative, when an analyst identifies the need for more context or additional information, the request typically escalates to a Security Engineer. Security Engineers are responsible for the integration and configuration of additional data sources, and they can alter correlation rules or enhance data ingestion pipelines to provide the necessary context for analysts.

Security Engineer:

Manages and optimizes security tools and systems, including SIEM (like Splunk), and ensures that the necessary data sources are integrated into the monitoring environment.

Responsible for creating and tuning correlation rules and maintaining the infrastructure required for continuous monitoring.

Incorrect Options:

A. SOC Manager: Oversees the overall operations of the SOC but does not typically handle the technical integration of data sources.

B. Security Analyst: Primarily focuses on monitoring, detecting, and responding to security incidents, rather than configuring systems.

D. Security Architect: Focuses on the overall design of the security infrastructure, not on the day-to-day integration of data sources.

Continuous Monitoring Best Practices: Industry standards emphasize the role of Security Engineers in maintaining and enhancing security monitoring systems.

Question: 19

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:

The Risk Framework in 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:

This framework aggregates risk events and calculates risk scores that help in prioritizing alerts and focusing on high-risk entities within the organization.

By identifying and raising the profile of entities involved in suspicious activities, it enables proactive threat detection and response.

Incorrect Options:

A. Threat Intelligence Framework: Integrates threat intelligence feeds but does not directly handle risk scoring of assets.

C. Notable Event Framework: Manages notable events but is not focused on risk profiling.

D. Asset and Identity Framework: Manages asset and identity data, linking them with events, but does not perform risk scoring.

Splunk Documentation: Detailed information on the Risk Framework and how it integrates with other security features in Splunk ES.

Question: 20

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, the rare command 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:

This command works by identifying values that appear infrequently within a specified field. Ita€™s a powerful tool for Cyber Defense Analysts who are looking for anomalies that could signify malicious activities.

Incorrect Options:

A. least: This is not a valid Splunk command.

B. uncommon: This is not a valid Splunk command.

D. base: This is not a relevant command for finding the least common values.

Splunk Command Documentation: rare command usage for identifying uncommon values.

Question: 21

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

A. Act on Objectives
B. Exploitation
C. Delivery

D. Installation

Answer: D

Explanation:

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

Question: 22

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.

Question: 23

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

www.atmicnetworks.com

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.

Question: 24

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.

Question: 25

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:

APT groups motivated by hacktivism typically target organizations or entities that they see as adversaries to their cause. The attacks can range from defacing websites to launching Distributed Denial of Service (DDoS) attacks to disrupt services.

This form of cyber activity is intended to create awareness or send a message, often aligning with the group's

ideological beliefs.

Incorrect Options:

B. Cyber espionage: Focuses on gathering intelligence and sensitive information, often for national or corporate advantage, not necessarily for disruption.

C. Financial gain: Involves attacks aimed at monetary theft, not ideologically driven disruption.

D. Prestige: While some attacks are motivated by the desire for recognition, hacktivism specifically refers to ideological causes.

Cybersecurity Literature: Books and articles on APT motivations often highlight hacktivism as a distinct category with a focus on ideological or political goals.

Question: 26

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: D

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:

Focuses on the specific, detailed activities of threat actors, such as the Tactics, Techniques, and Procedures (TTPs) they employ.

This intelligence helps in creating defensive strategies, such as refining detection rules, improving incident response plans, and enhancing threat hunting efforts.

Incorrect Options:

A. Operational: Operational intelligence involves real-time information and insights that support ongoing operations, often within a narrow timeframe.

B. Executive: Executive intelligence is high-level and strategic, intended for decision-makers and typically involves summaries rather than detailed technical information.

D. Strategic: Strategic intelligence is long-term and broad in scope, focusing on overall trends and the geopolitical context, rather than specific TTPs.

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

Question: 27

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: B

Explanation:

In Splunk's Risk-Based Alerting (RBA) framework, a Risk Object refers to the specific entity (such as a user account, IP address, or host) that is associated with risk observations. When a user account generates multiple risk observations, it is labeled as a Risk Object, allowing security teams to track and manage risk more effectively.

Risk Object:

The Risk Object is central to Splunk's RBA approach, which aggregates and evaluates risk across entities within an environment. This allows for a focused response to high-risk entities based on the accumulation of risk events.

Incorrect Options:

A. Risk Factor: This might refer to specific criteria or conditions that contribute to risk but does not denote the entity itself.

B. Risk Index: Could refer to a collection of risk-related data, not the specific entity.

C. Risk Analysis: Refers to the process of analyzing risk, not the entity under observation.

Splunk RBA Documentation: Detailed descriptions of how Risk Objects function within the Risk-Based Alerting framework.

Question: 28

When searching in Splunk, which of the following SPL commands can be used to run a sub search across every field in a wildcard field list?

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

Answer: A

Explanation:

The foreach command in Splunk is used to iterate over a list of fields that match a wildcard expression

www.atmicnetworks.com

and apply a sub search 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, or transaction) are designed for this specific purpose. The for each command allows for flexible and efficient processing of multiple fields without having to explicitly name them all.

Question: 29

How are Notable Events configured in Splunk Enterprise Security?

A. During an investigation.
B. As part of an audit.
C. Via an Adaptive Response Action in a regular search.
D. Via an Adaptive Response Action in a correlation search.

Answer: D

Explanation:

Notable Events in Splunk Enterprise Security are configured as part of a correlation search, where an Adaptive Response Action can be set to create a Notable Event when certain conditions are met. These correlation searches are pre-defined or custom searches that look for specific patterns of interest, such as security incidents or anomalies. The use of Adaptive Response Actions within these searches allows for the automated creation of Notable Events, which can then be investigated by security analysts. This configuration is a crucial part of Splunk's security operations capabilities.

Question: 30

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. The host field generally refers to the name of the host that logged the event, dest refers 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.

Question: 31

Which of the following data sources can be used to discover unusual communication within an organization’s network?

A. EDS
C. 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.

Question: 32

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 – count is most effective. The stats count by user command generates a count of occurrences for each user. The where clause then filters out only those users who have more than 1000 occurrences. Finally, sort – count sorts the results in descending order by count. This approach is efficient for identifying outliers, such as users with a high number of events.

Question: 33

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 called Framework 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.

Question: 34

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 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.

Question: 35

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:

The file_aclfield, which contains access controls associated with files affected by an event, is part of the Endpointdata 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.

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 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.

Question: 37

What is the main difference between hypothesis-driven and data-driven Threat Hunting?

A. Data-driven hunts always require more data to search through than hypothesis-driven hunts.
B. Data-driven hunting tries to uncover activity within an existing data set, hypothesis-driven hunting begins with a potential activity that the hunter thinks may be happening.
C. Hypothesis-driven hunts are typically executed on newly ingested data sources, while data-driven hunts are not.
D. Hypothesis-driven hunting tries to uncover activity within an existing data set, data-driven hunting begins with an activity that the hunter thinks may be happening.

Answer: B

Explanation:

The main difference between hypothesis-driven and data-driven threat hunting lies in the approach. In hypothesis-driven hunting, the hunter starts with a theory or hypothesis about what kind of malicious activity might be occurring and then searches the data to confirm or refute that hypothesis. On the other hand, data-driven hunting involves sifting through existing datasets to uncover patterns, anomalies, or activities that were not initially suspected. Hypothesis-driven approaches are more focused and often guided by threat intelligence or knowledge of attacker behaviors, while data-driven approaches rely on broad data analysis to identify unexpected threats.

Question: 38

The Security Operations Center (SOC) manager is interested in creating a new dashboard for

Typo squatting 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 typo squatting, the New Domain Analysisdashboard in Splunk Enterprise Security (ES) would be a relevant starting point. Typo squatting 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 typo squatting.

Question: 39

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 uses a 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. A DDoS attack involves multiple compromised systems (often part of a botnet) attacking a single target, overwhelming it with traffic or requests. In contrast, a DoS attack 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.

Question: 40

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.

Question: 41

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

www.atmicnetworks.com

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 a Credential Stuffing attack. 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. Unlike Password Spraying(which tries a few common passwords against many accounts) or Password Cracking(which tries to guess or decrypt passwords), credential stuffing leverages large datasets of valid credentials obtained from other breaches.

Question: 42

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 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:

Implementation: Security Engineers are tasked with the hands-on deployment and configuration of security systems, including firewalls, intrusion detection systems (IDS),and endpoint protection solutions. When a risk is identified, they are the ones who implement the necessary technological controls or processes to mitigate that risk.

Technical Expertise: Security Engineers possess the technical skills required to integrate new solutions into the existing environment, ensuring that they operate effectively without disrupting other systems.

Collaboration: While Security Architects design the overall security architecture and the SOC Manager oversees operations, the Security Engineer works on the ground, implementing the detailed aspects of the solutions.

Contrast with Other Roles:

Security Architect: Designs the security framework and architecture but does not usually perform the actual implementation.

SOC Manager: Oversees the security operations and might coordinate the response but does not directly implement new solutions.

Security Analyst: Monitors and analyzes security data, but typically does not implement new security systems.

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.

Question: 43

After discovering some events that were missed in an initial investigation, an analyst determines this is because some events have an empty src field. Instead, the required data is often captured in another field called machine_name.
What SPL could they use to find all relevant events across either field until the field extraction is fixed?

A. | eval src = coalesce(src,machine_name)
B. | eval src = src + machine_name
C. | eval src = src . machine_name
D. | eval src = tostring(machine_name)

Answer: A

Explanation:

The coalesce function in Splunk is used to return the first non-null value from a list of fields. The SPL| eval src = coalesce(src,machine_name)allows the analyst to dynamically populate the srcfield with the value from machine_nameifsrcis empty. This is a useful technique when dealing with inconsistent data sources or during field extraction issues, ensuring that the analyst can continue their

investigation without missing critical events.

Question: 44

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
8. rename
C. eval
D. stats

Answer: A

Explanation:

The make results 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.

Question: 45

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 a Technique as 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.

Question: 46

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 like fields, 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.

Question: 47

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:

The Enterprise 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.

Question: 48

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 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.

Question: 49

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.

Question: 50

www.atmicnetworks.com

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

Question: 51

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 architecturesare 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.

Question: 52

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:

Thee valSPL 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 is 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.

Question: 53

Which of the following is a tactic used by attackers, rather than a technique?

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

Answer: A

Explanation:

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

Question: 54

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.

Question: 55

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 a False Negative because 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.

Question: 56

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 the Endpoint data 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.

Question: 57

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: C
Explanation:

In Splunk, streaming commands process each event individually as it is passed through the search pipeline and should be placed before aggregating 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.

Question: 58

While testing the dynamic removal of credit card numbers, an analyst lands on using the rex command. 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 above rex command is correctly written.

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

Answer: A

Explanation:

The rex command 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 to sed. The sed mode allows for string replacement within a field using regular expressions, enabling the substitution of matching patterns with a specified string.

Question: 59

Which of the following use cases is best suited to be a Splunk SOAR Playbook? A Forming hypothesis for Threat Hunting
B. Visualizing complex datasets.
C. Creating persistent field extractions.
D. Taking containment action on a compromised host

Answer: D

Explanation:

Splunk SOAR (Security Orchestration, Automation, and Response) playbooks are designed to automate security tasks, making taking containment action on a compromised host the best-suited use case. A SOAR playbook can automate the response actions such as isolating a host, blocking IPs, or disabling accounts, based on predefined criteria. This reduces response time and minimizes the impact of security incidents. The other options, like forming hypotheses for threat hunting or visualizing datasets, are more manual processes and less suited for automation via a playbook.

Question: 60

Which of the following is not considered an Indicator of Compromise (IOC)?

A. A specific domain that is utilized for phishing.
B. A specific IP address used in a cyberattack.
C. A specific file hash of a malicious executable.
D. A specific password for a compromised account.

Answer: D

Explanation:

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

www.atmicnetworks.com

Question: 61

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, the src_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 like dest_user or username have different roles, focusing on the target of the action or the general username involved.

Question: 62

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 a Tactic. 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 a Technique. Techniques are specific methods used to achieve a tactic, such as exploiting a service to move laterally.

Use Eternal Blue to exploit a remote SMB server– This is a Procedure. Procedures are the detailed steps or specific implementations of a technique, such as using the Eternal Blue exploit to target SMB vulnerabilities.

Thus, the correct order is Tactic, Technique, Procedure.

Question: 63

An analyst is attempting to investigate a Notable Event within Enterprise Security. Through the course of their investigation they determined that the logs and artifacts needed to investigate the alert are not available. What event disposition should the analyst assign to the Notable Event?

A. Benign Positive, since there was no evidence that the event actually occurred. B. False Negative, since there are no logs to prove the activity actually occurred. C. True Positive, since there are no logs to prove that the event did not occur.
D. Other, since a security engineer needs to ingest the required logs.

Answer: D

Explanation:

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

Question: 64

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.

Question: 65

Which of the Enterprise Security frameworks provides additional automatic context and correlation to fields that exist within raw data?

A. Asset and Identity
B. Threat Intelligence
C. Adaptive Response
D. Risk

Answer: A **Explanation:**

www.atmicnetworks.com

The Asset and Identity framework within Splunk Enterprise Security provides additional automatic context and correlation to fields that exist within raw data. By associating IP addresses, usernames, and other identifiers with known assets and identities within the organization, this framework enhances the context of security events and facilitates moreaccurate and meaningful analysis. This allows analysts to

better understand the impact of security incidents and to prioritize their responses based on the criticality of the assets involved.

Question: 66

In Splunk Enterprise Security, what is the purpose of annotations?

A. To correct erroneous data
B. To document the source of data
C. To provide context to data points
D. To visualize data trends

Answer: C

Explanation:

Annotations within Splunk Enterprise Security are used to provide additional context to data points, aiding in the analysis and understanding of security events.

Question: 67

An analyst needs to find events where the username is "admin" and the action taken was "failed login". Which SPL command is most suitable for this query?

A. EVAL
B. REX
C. SEARCH
D. TABLE

Answer: C

Explanation:

The SEARCH command in SPL is most suitable for finding specific events, such as those with "admin" as the username and "failed login" as the action, by directly specifying these criteria in the search.

Question: 68

In a scenario where a SOC analyst identifies an anomaly in HTTP traffic, which Splunk Enterprise Security feature should be used to investigate further?

A. Traffic Analysis Dashboard
B. Identity Resolver
C. Protocol Intelligence
D. Asset Investigator

Answer: A

Explanation:

The Traffic Analysis Dashboard in Splunk Enterprise Security would be the appropriate feature to use for further investigation into anomalies in HTTP traffic, providing detailed insights into network traffic patterns.

Question: 69

A Splunk analyst wants to prioritize incidents based on asset criticality. Which feature within Splunk Enterprise

Security supports this functionality?

A. Risk Scoring
B. Threat Intelligence
C. Notable Events
D. Asset Lists

Answer: A

Explanation:

Risk Scoring within Splunk Enterprise Security allows for the prioritization of incidents based on various factors, including asset criticality, enabling a more targeted response to threats.

Question: 70

You're analyzing traffic logs and notice a high volume of requests over a short period targeting a single server. What type of attack does this pattern suggest?

A. DDoS
C. Phishing
D. SQL Injection
E. Man-in-the-Middle

Answer: A

Explanation:

A high volume of requests over a short period targeting a single server suggests a DDoS (Distributed Denial of Service) attack, aiming to overwhelm the server and disrupt its normal operations.

Question: 71

A security analyst is investigating a notable event related to a potential insider threat. Which Splunk feature should be utilized to track the user's activity across various systems?

A. Identity Resolver
B. Timeline
C. User Behavior Analytics (UBA)
D. Asset Investigator

Answer: C

Explanation:

User Behavior Analytics (UBA) in Splunk is the ideal feature to utilize when investigating potential insider threats, as it can help in tracking and analyzing a user's activity across various systems to identify anomalous behavior.

Question: 72

An organization is evaluating its cybersecurity posture against the MITRE ATT&CK framework. How can Splunk assist in this evaluation?

A. By enforcing compliance with ATT&CK standards
B. By generating ATT&CK tactics and techniques
C. By directly preventing ATT&CK tactics
D. By mapping security events to ATT&CK tactics and techniques

www.atmicnetworks.com

Answer: D

Explanation:

Splunk can assist in evaluating an organization's cybersecurity posture against the MITRE ATT&CK framework by mapping detected security events to specific ATT&CK tactics and techniques, helping to identify potential attack vectors and strategies.

Question: 73

Which of the following scenarios is best suited for utilizing SOAR playbooks in Splunk Enterprise Security?

A. Detailed forensic analysis
B. Scheduling regular system backups
C. Automating response to common threats
D. Orchestrating responses across multiple tools
E. Manual threat hunting

Answer: C, D

Explanation:

SOAR playbooks are best utilized for automating response to common threats and orchestrating responses across multiple tools, streamlining the response process and improving efficiency.

Question: 74

What is the main purpose of implementing a zero trust architecture within an organization's cybersecurity strategy?

A. To eliminate the need for firewalls and antivirus software
B. To solely rely on external threat intelligence for security
C. To reduce the complexity of the network infrastructure
D. To ensure that all users, whether inside or outside the organization's network, are authenticated and authorized before accessing resources

Answer: D

Explanation:

The main purpose of implementing a zero trust architecture is to ensure that all users and devices are authenticated and authorized before being granted access to resources, regardless of their location relative to the organization's network.

Question: 75

An engineer is setting up Splunk to monitor cloud-based applications. Which sourcetype is essential for analyzing AWS CloudTrail logs?

A. aws:cloudwatch
B. aws:s3
C. aws:cloudtrail
D. aws:ec2

Answer: C

Explanation:

The aws:cloudtrail sourcetype is essential for analyzing AWS CloudTrail logs in Splunk, as it is specifically designed to handle and parse logs generated by AWS CloudTrail.

Question: 76

In the context of cyber defense, what does the term "C2" refer to?

A. Cybersecurity Compliance
B. Command and Control
C. Category 2 threat level
D. Cloud to Cloud integration

Answer: B

Explanation:

C2 stands for Command and Control, which refers to the infrastructure attackers use to maintain communication with and control over compromised systems or networks.

Question: 77

An organization implements a new framework aligning with Splunk. Which framework aims at improving risk management processes?

A. COSO
B. ISO/IEC 27001
C. COBIT
D. ITIL

Answer: B

Explanation:

ISO/IEC 27001 is focused on information security management systems (ISMS) and is commonly aligned with Splunk to enhance cybersecurity and risk management processes.

Question: 78

Which of the following best describes the concept of "zero trust"?

A. A system that trusts all internal devices B. A network with no security measures
C. Trusting no external systems
D. A security model that requires verification for every access attempt, regardless of location

Answer: D

Explanation:

The "zero trust" model is a security concept that requires strict identity verification for every person and device trying to access resources, regardless of whether they are inside or outside the network perimeter.

Question: 79

Which of the following best describes the concept of "dwell time" in cybersecurity?

A. Time to respond to an incident
B. Time a threat actor remains undetected within a network

C. Time to detect a breach
D. Time from detection to eradication

Answer: B

Explanation:

Dwell time refers to the amount of time a threat actor remains undetected within a network, indicating the effectiveness of an organization's detection capabilities.

Question: 80

When configuring a dashboard in Splunk Enterprise Security, which information is essential for tracking brute force login attempts?

A. Geolocation of access attempts
B. Failed login attempts
C. Successful login attempts
D. Usernames used in login attempts
E. Timestamps of login attempts

Answer: A, B, D, E

Explanation:

For tracking brute force login attempts, monitoring failed login attempts, geolocation, timestamps, and usernames used provides comprehensive insight into potential security incidents.

Question: 81

During a security audit, an analyst uses Splunk to identify unauthorized data access. Which data model in Splunk is most appropriate for this analysis?

A. Intrusion Detection
B. Web
C. Change
D. Authentication

Answer: D

Explanation:

The Authentication data model is most appropriate for analyzing unauthorized data access, as it provides insights into user login activities and access patterns.

Question: 82

In the context of Splunk, what does a high number of Notable Events in a short period likely indicate?

A. An ongoing cyber attack
B. Scheduled maintenance
C. A misconfigured device
D. A successful system update

Answer: A

Explanation:

A high number of Notable Events in a short period in Splunk typically indicates an ongoing cyber attack or a significant security incident requiring immediate attention.

Question: 83

A Splunk analyst needs to monitor for an increase in failed login attempts across multiple systems. Which SPL command is most suitable for identifying this trend?

A. dbinspect
B. top
C. timechart
D. stats

Answer: C

Explanation:

The "timechart" command in SPL is most suitable for monitoring trends over time, such as an increase in failed login attempts across multiple systems, by allowing the analyst to visualize changes in login attempt patterns.

Question: 84

After deploying a new detection rule, an analyst observes a surge in false positives. What action should be taken to refine the detection accuracy?

A. Increase the rule's threshold
B. Review and adjust the rule's logic
C. Disable the rule temporarily
D. Ignore the false positives

Answer: B

Explanation:

Reviewing and adjusting the rule's logic is the appropriate action to refine detection accuracy and reduce false positives, ensuring that the rule more accurately identifies true threats.

Question: 85

What does a "Notable Event" in Splunk Enterprise Security signify?

A. An event that requires immediate action
B. A false positive
C. An event tagged for future review
D. A routine system log

Answer: A

Explanation:

A "Notable Event" in Splunk Enterprise Security signifies an incident or anomaly that requires attention or investigation, often indicative of a potential security threat.

Question: 86

Which of the following is NOT a common data source for threat analysis in cyber defense?

A. Social media feeds
B. Network traffic logs
C. Encrypted data packets
D. Antivirus software alerts

www.atmicnetworks.com

Answer: C
Explanation:

While network traffic logs, antivirus alerts, and social media can be valuable for threat analysis, encrypted data packets are not directly usable as a data source without decryption.

Question: 87

A SOC team is using Splunk to integrate threat intelligence feeds. Which tier of Threat Intelligence involves strategic, high-level information?

A. Strategic
B. Tactical
C. Technical
D. Operational

Answer: A
Explanation:

Strategic Threat Intelligence provides high-level information aimed at decision-makers, focusing on broad cybersecurity trends and policies.

Question: 88

In an effort to improve incident response times, a SOC implements automated playbooks in Splunk. Which phase of incident response does this primarily enhance?

A. Preparation
B. Containment, Eradication, and Recovery
C. Post-Incident Activity
D. Detection and Analysis

Answer: B
Explanation:

Implementing automated playbooks in Splunk primarily enhances the Containment, Eradication, and Recovery phase of incident response by enabling quicker and more efficient responses to identified threats.

Question: 89

For compliance with HIPAA, what Splunk capability ensures that access to sensitive patient data is logged and auditable?

A. Access Control Lists
B. Audit Logs
C. Data Models
D. Indexer Clustering

Answer: B
Explanation:

Audit Logs in Splunk ensure that access to sensitive patient data is logged and auditable, meeting HIPAA requirements for tracking access to protected health information.

Question: 90

Which of the following best describes the use of "tstats" in SPL?

A. To translate search results into statistical data
B. To generate time-based statistics from indexed data
C. To track the statistical trends of search queries
D. To apply statistical functions to transaction data

Answer: B

Explanation:

tstats in SPL is used to generate time-based statistics from indexed data, allowing for efficient aggregation and analysis of large datasets over time.

Question: 91

In a phishing incident response scenario, which type of adaptive response action is most effective in Splunk Enterprise Security?

A. Updating antivirus signatures
B. Scanning emails for malicious attachments
C. Disabling compromised user accounts
D. Blocking IP addresses at the firewall

Answer: C

Explanation:

Disabling compromised user accounts is an effective adaptive response action in the case of a phishing incident, as it immediately prevents further unauthorized access using the affected credentials.

Question: 92

When configuring Splunk to alert on data exfiltration attempts, which of the following indicators should be monitored?

A. Usage of common file transfer tools
B. Multiple failed login attempts
C. Encryption of bulk data within a short time frame
D. Access to sensitive data outside of business hours
E. Unusual outbound traffic volume

Answer: A, C, D, E **Explanation:**

Monitoring for unusual outbound traffic volume, usage of common file transfer tools, access to sensitive data outside of business hours, and encryption of bulk data within a short time frame are crucial indicators of potential data exfiltration attempts.

Question: 93

A SOC analyst notices unusual outbound traffic patterns during off-hours. Which type of attack could this indicate?

A. SQL Injection
B. DDoS
C. Phishing
D. Data Exfiltration

Answer: D

Explanation:

Unusual outbound traffic patterns during off-hours could indicate Data Exfiltration, where sensitive data is being unauthorizedly transmitted outside the organization.

Question: 94

How can Splunk's Enterprise Security Asset and Identity framework enhance incident investigation?

A. By correlating events with known asset and identity information
B. By automatically blocking malicious IP addresses
C. By encrypting sensitive data in transit
D. By anonymizing user identity in logs

Answer: A

Explanation:

Splunk's Enterprise Security Asset and Identity framework can enhance incident investigation by correlating events with known asset and identity information, providing context and aiding in the analysis of security events.

Question: 95

When a new malware signature is identified, which Splunk functionality allows for the retrospective analysis of historical data to identify past occurrences?

A. Adaptive Response
B. Correlation Search
C. Archive Search
D. Data Model Acceleration

Answer: B

Explanation:

Correlation Search in Splunk allows for the retrospective analysis of historical data to identify past occurrences of newly identified malware signatures by correlating current threat intelligence with past events.

Question: 96

To enhance threat hunting capabilities, a SOC analyst plans to use Splunk to focus on behavioral analytics. Which aspect should be prioritized?

A. Real-time event monitoring
B. User and entity behavior analytics (UEBA)
C. Historical log analysis
D. Static rule-based detection

Answer: B

Explanation:

User and Entity Behavior Analytics (UEBA) should be prioritized to focus on behavioral analytics in Splunk, as it uses advanced analytics to identify anomalies in user and entity behavior that may indicate a threat.

www.atmicnetworks.com

Question: 97

In the event of a detected email compromise, which of the following adaptive response actions should be prioritized?

A. Review email server logs for anomalies
B. Isolate compromised systems

C. Scan emails for additional threats
D. Update firewall rules
E. Reset passwords of affected accounts

Answer: A, B, C, E

Explanation:

In the event of an email compromise, scanning emails for additional threats, resetting passwords of affected accounts, isolating compromised systems, and reviewing email server logs for anomalies should be prioritized to contain the threat and prevent further damage.

Question: 98

Which SPL command is best used for grouping events by a common field?

A. JOIN STATS REX EVAL
B. **Answer: B**
C. **Explanation:**
D.

The STATS command in SPL is best used for aggregating data, such as summing values or counting events, and can group results based on a common field.

Question: 99

A Splunk search reveals multiple instances of a rare process being executed across several endpoints. What type of analysis does this suggest?

A. Statistical analysis B. Behavioral analysis C. Geographic analysis D. Temporal analysis **Answer: B**

Explanation:

The discovery of multiple instances of a rare process being executed across several endpoints suggests Behavioral analysis, as it involves examining unusual behaviors or patterns that deviate from the norm, potentially indicating malicious activity.

Question: 100

What is the purpose of a supply chain attack?

A. To exploit vulnerabilities in software development processes
B. To increase the cost of goods
C. To create a shortage of essential supplies
D. To disrupt the physical delivery of goods

Answer: A

Explanation:

A supply chain attack aims to exploit vulnerabilities in the software development or distribution process, allowing attackers to compromise products or systems downstream.

Question: 101

During a threat hunting exercise, an analyst uses Splunk to search for anomalies in system registry settings. This is indicative of what kind of attack?

A. Ransomware
B. Cross-Site Scripting
C. Man-in-the-Middle
D. SQL Injection

Answer: A

Explanation:

Ransomware attacks often involve changes to system registry settings to execute malicious scripts, making this a focus area during threat hunting exercises.

Question: 102

An organization's firewall logs show repeated attempts to access a port that should not be publicly accessible. What is the first step in investigating this using Splunk?

A. Implement a SIEM solution to automate the analysis
B. Use the search feature in Splunk to analyze access attempts
C. Modify firewall rules to block the suspicious IP addresses
D. Notify the network team to physically inspect the firewall **Answer: B**

Explanation:

Using the search feature in Splunk to analyze the access attempts is the first step in investigating repeated unauthorized access attempts, allowing for a detailed analysis of the events before taking further action.

Question: 103

What Splunk feature helps in visualizing the geographic distribution of threat origins?

A. Lookup tables
B. Statistical charts
C. Correlation searches
D. Geo-mapping dashboards

Answer: D

Explanation:

Geo-mapping dashboards in Splunk help in visualizing the geographic distribution of threat origins, enabling analysts to see where attacks are originating from on a map.

Question: 104

During a review, an analyst identifies a Risk Notable Event with a low score. What does this indicate in terms of priority?

A. False positive
B. High priority
C. Medium priority
D. Low priority

Answer: D **Explanation:**

A Risk Notable Event with a low score in Splunk indicates it is of low priority, suggesting it may pose a minimal risk compared to events with higher scores.

Question: 105

In the context of cybersecurity, what does the principle of "least privilege" entail?

A. Installing antivirus software on all devices
B. Encrypting all data, regardless of sensitivity
C. Conducting regular penetration tests
D. Granting users the minimum level of access necessary for their role

Answer: D

Explanation:

The principle of "least privilege" entails granting users the minimum level of access necessary for their role, minimizing the potential impact of a compromised account.

Question: 106

What role does the Asset and Identity framework play in Splunk Enterprise Security?

A. Encrypting sensitive data
B. Managing user permissions
C. Correlating events with assets and identities
D. Defining network architecture

Answer: C

Explanation:

The Asset and Identity framework in Splunk Enterprise Security helps in correlating events with specific assets and identities, enhancing the context and relevance of security events.

Question: 107

A SOC analyst observes a spike in SQL injection attempts. Which Splunk functionality should be used to analyze the source and pattern of these attempts?

A. Threat intelligence correlation
B. Sourcetype analysis
C. Transaction search
D. Geospatial lookup

Answer: A

Explanation:

Threat intelligence correlation in Splunk can be used to analyze the source and pattern of SQL injection attempts by comparing the observed activities with known threat intelligence data.

Question: 108

Which of the following frameworks is commonly integrated with Splunk for cybersecurity purposes?

A. Agile

B. PRINCE2
C. ISO 9001
D. NIST Cybersecurity Framework
Answer: D
Explanation:

The NIST Cybersecurity Framework is commonly integrated with Splunk for enhancing cybersecurity measures and compliance, unlike ISO 9001, PRINCE2, or Agile, which serve different purposes.

Question: 109

In Splunk, what is the primary use of the "LOOKUP" command in SPL?

A. To generate alerts based on specific conditions B. To correlate events with external data sources C. To visualize data in charts and graphs D. To search for specific patterns within data **Answer: B**
Explanation:

The "LOOKUP" command in SPL is used to enrich your data by correlating events with external data sources, allowing for more detailed analysis.

Question: 110

In Splunk, what is the significance of using the "rex" command in SPL?

A. To rename existing fields
B. To exclude results from a search
C. To perform statistical calculations
D. To extract fields from unstructured data
Answer: D
Explanation:

The "rex" command in SPL is used to extract fields from unstructured data, enabling more detailed analysis and segmentation of data based on specific patterns or criteria.

Question: 111

What does the "EVAL" command in SPL primarily accomplish?

A. Evaluates conditions to filter events
B. Performs statistical calculations on fields
C. Extracts fields from event data
D. Creates or modifies fields based on existing values
Answer: D
Explanation:

The "EVAL" command in SPL is used to create or modify fields based on existing values in your event data, allowing for data manipulation and calculation.

Question: 112

Which of the following best describes the primary role of an Analyst in a SOC?

A. Designing security architectures
B. Developing security policies
C. Monitoring and analyzing security events
D. Implementing security solutions

Answer: C

Explanation:

An Analyst in a SOC primarily focuses on monitoring and analyzing security events to detect potential threats. The other roles are generally associated with Engineers, Architects, or Policy Makers.

Question: 113

What is the primary purpose of Risk Based Alerting in Splunk Enterprise Security?

A. To correlate events and assign risk scores
B. To generate alerts based on predefined thresholds
C. To prioritize alerts based on asset value
D. To automate response actions

Answer: A

Explanation:

Risk Based Alerting in Splunk Enterprise Security aims to correlate events and assign risk scores to prioritize and focus on the most critical threats.

Question: 114

Which of the following is a best practice for SIEM operation in Splunk Enterprise Security?

A. Use only real-time searches
B. Restrict the use of dashboards
C. Leverage the Common Information Model (CIM)
D. Avoid data normalization

Answer: C

Explanation:

Leveraging the Common Information Model (CIM) is a best practice in SIEM operation for Splunk Enterprise Security as it helps in normalizing data for analysis, reporting, and alerting.

Question: 115

Which of the following techniques is used in threat hunting to identify deviations from the norm?

A. Keyword searching
B. User behavior analytics
C. Outlier detection
D. Long tail analysis

Answer: B, C, D **Explanation:**

Long tail analysis and outlier detection are techniques used in threat hunting to identify unusual patterns or deviations from normal behavior, which might indicate a security threat.

Question: 116

In a phishing simulation, employees receive an email asking to update their passwords. This exercise aims to test awareness regarding what type of attack?

A. Ransomware
B. DDoS
C. Supply Chain Attack
D. Social Engineering

Answer: D

Explanation:

This exercise simulates a Social Engineering attack, specifically phishing, where attackers deceive individuals into revealing sensitive information, like passwords.

Question: 117

An organization wants to enhance its incident response with automation. Which Splunk feature should be utilized for defining automated actions in response to specific threats?

A. Asset and Identity Management
B. Correlation Searches
C. Data Models
D. Adaptive Response Actions

Answer: D

Explanation:

Adaptive Response Actions in Splunk allow for the definition of automated actions in response to specific threats, enhancing the incident response process.

Question: 118

Which of the following is a characteristic of a botnet?

A. A single powerful computer
B. A network of compromised devices
C. A cybersecurity framework
D. A type of malware

Answer: B

Explanation:

A botnet is a network of compromised devices, often infected with malware, that can be controlled remotely by an attacker, typically used for launching attacks like DDoS.

Question: 119

When configuring Splunk for efficient threat hunting, why is it important to customize sourcetypes?

A. To ensure data encryption
B. To reduce license usage by filtering out unnecessary data
C. To increase the speed of real-time searches
D. To facilitate data normalization and parsing

Answer: D

Explanation:

Customizing sourcetypes in Splunk is important for threat hunting as it facilitates data normalization and parsing, making it easier to analyze and correlate data from various sources.

Question: 120

A security analyst is using SPL to track an advanced persistent threat (APT). Which command can be used to identify patterns over time, such as login failures?

A. CHART
B. STATS
C. TIMECHART
D. TREND

Answer: C

Explanation:

The TIMECHART command in SPL is best suited for identifying patterns over time, such as tracking login failures, by allowing analysts to create time-series visualizations of data.

Question: 121

A cybersecurity analyst is assessing different data sources in Splunk. Which data source is most critical for identifying lateral movement within a network?

A. Antivirus alerts
B. Firewall logs
C. Authentication logs
D. DNS query logs

Answer: C

Explanation:

Authentication logs are crucial for identifying lateral movement within a network as they track user logins and resource access, which can indicate unauthorized access or movement.

Question: 122

What is the primary benefit of using the Common Information Model (CIM) in Splunk for cybersecurity analysis?

A. Speeds up search queries
B. Automates data encryption
C. Enables data normalization across different data sources
D. Reduces data storage requirements

Answer: C

Explanation:

The primary benefit of using the Common Information Model (CIM) in Splunk is to enable data normalization across different data sources, making it easier to analyze and correlate data from disparate systems.

Question: 123

What type of cyber defense system is primarily used to detect and prevent unauthorized access to networks?

A. Intrusion Detection System
B. Firewall
C. Data Loss Prevention
D. Antivirus

Answer: B

Explanation:

A Firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules, aiming to block unauthorized access.

Question: 124

For a SOC analyst focusing on cloud security, which Splunk sourcetype would be most relevant for analyzing Azure AD sign-in logs?

A. azure:audit
B. aws:cloudtrail
C. ms:o365:management
D. google:gcp:pubsub

Answer: A

Explanation:

For analyzing Azure AD sign-in logs, the "azure:audit" sourcetype would be most relevant, as it is specifically designed to handle and interpret Azure-related log data.

Question: 125

An analyst uses SPL to correlate events from multiple data sources. Which command is best suited for combining data based on a common field?

A. JOIN
B. SORT
C. TABLE
D. DEDUP

Answer: A

Explanation:

The JOIN command in SPL is used to combine data from multiple sources based on a common field, allowing for correlation and more comprehensive analysis.

Question: 126

Which of the following is a primary function of the Threat Intelligence framework in Splunk?

A. Automatically patching vulnerable systems
B. Blocking detected threats in real time
C. Correlating events with external threat data
D. Encrypting sensitive data at rest

Answer: C

Explanation:

The primary function of the Threat Intelligence framework in Splunk is to correlate events with external threat data, enabling analysts to identify and respond to potential threats based on known indicators of compromise.

www.atmicnetworks.com

Question: 127

A Splunk dashboard is configured to monitor for an increase in traffic from known malicious IP addresses. Which type of cyber defense mechanism does this represent?

A. Corrective Deterrent Detective Preventive
B. **Answer: C**
C. **Explanation:**
D.

Monitoring for an increase in traffic from known malicious IP addresses is a Detective control, as it aims to detect and identify potential security threats.

Question: 128

How does Splunk assist in identifying phishing emails through log analysis?

A. By analyzing email content for malicious links
B. By tracking the volume of emails sent from unknown domains
C. By correlating login failures with email receipt times
D. By detecting anomalies in email header data

Answer: A

Explanation:

Splunk assists in identifying phishing emails by analyzing email content for malicious links, using log data to highlight emails that may contain phishing attempts.

Question: 129

In a multi-cloud environment, which Splunk feature is vital for centralizing log management across different cloud platforms?

A. HTTP Event Collector
B. Cloud Gateway
C. Distributed Search
D. Federated Search

Answer: D

Explanation:

Federated Search in Splunk is vital for centralizing log management across different cloud platforms, allowing searches across multiple Splunk deployments, including those in various cloud environments.

Question: 130

A company wants to monitor its network for potential command and control (C2) traffic. Which type of

Splunk search would be most effective for this purpose?

A. Ad hoc search
B. Real-time search
C. Historical search

D. Scheduled search

Answer: B Explanation:

A real-time search in Splunk would be most effective for monitoring potential command and control (C2) traffic, as it allows for the immediate detection and response to such activities as they occur.

Question: 131

During an investigation, what is the first stage according to Splunk's five stages of investigation?

A. Eradication
B. Identification
C. Containment
D. Preparation

Answer: D Explanation:

According to Splunk's five stages of investigation, the first stage is Preparation, where analysts prepare tools, processes, and mindsets for effective investigation.

Question: 132

How does Splunk's Custom Alert Actions feature contribute to automated incident response?

A. By creating detailed incident reports
B. By encrypting alert data for secure transmission
C. By reducing the frequency of alert notifications
D. By initiating predefined response actions to specific security alerts

Answer: D

Explanation:

Splunk's Custom Alert Actions feature contributes to automated incident response by initiating predefined response actions to specific security alerts, streamlining the SOC's response process.

Question: 133

What is the main function of Splunk's Asset Investigator in a cybersecurity context?

A. To automate asset inventory updates
B. To track the movement of physical assets
C. To manage digital certificates
D. To provide detailed investigations into assets related to security incidents

Answer: D

Explanation:

Splunk's Asset Investigator provides detailed investigations into assets related to security incidents, offering insights into the scope and impact of the incident on organizational assets.

Question: 134

What advantage does integrating Splunk with Network Behavior Analysis (NBA) tools offer?

A. Comprehensive analysis of network traffic for suspicious behavior
B. Bandwidth optimization based on analysis findings
C. Real-time network encryption
D. Automated network device configuration

Answer: A

Explanation:

Integrating Splunk with Network Behavior Analysis (NBA) tools offers the advantage of comprehensive analysis of network traffic for suspicious behavior, enhancing the detection of advanced threats.

Question: 135

What functionality does the Splunk App for Enterprise Security add to standard Splunk deployments in a SOC environment?

A. Advanced threat detection rules and visualizations
B. Integration with physical security systems
C. Automatic data deletion for compliance
D. Enhanced data encryption

Answer: A

Explanation:

The Splunk App for Enterprise Security adds advanced threat detection rules and visualizations to standard Splunk deployments, enhancing the SOC's ability to identify and respond to threats.

Question: 136

What role does the "bloom filter" play in Splunk's indexing process?

A. It reduces disk space usage by compressing index files
B. It encrypts data at the point of indexing
C. It prevents duplicate data from being indexed
D. It enhances search speed by pre-filtering index searches

Answer: D

Explanation:

The "bloom filter" in Splunk's indexing process enhances search speed by pre-filtering index searches, allowing the system to quickly determine if a search term is not present in an index.

Question: 137

In what way does Splunk's support for custom Data Enrichment enhance threat intelligence?

A. By duplicating data across multiple indexes for redundancy
B. By adding contextual information to raw data for deeper analysis
C. By compressing data to save storage space
D. By encrypting data in transit

Answer: B

Explanation:

Splunk's support for custom Data Enrichment enhances threat intelligence by adding contextual information to raw data, providing deeper analysis and more accurate threat detection.

Question: 138

In reviewing Splunk dashboards, an analyst notices a large volume of traffic to a seldom-used application, mostly during off-peak hours. Which cybersecurity concern does this pattern most likely raise?

A. Unauthorized Access
B. Denial of Service (DoS) Attack
C. Application Layer Attack
D. Misconfiguration

Answer: A

Explanation:

The large volume of traffic to a seldom-used application mostly during off-peak hours, as noticed on Splunk dashboards, most likely raises a concern for Unauthorized Access, indicating potential exploitation or reconnaissance activities.

Question: 139

In a mobile security context, what unique data source can Splunk analyze for threat detection?

A. Battery usage patterns
B. GPS location data
C. Mobile application logs D. SMS message content **Answer: C**

Explanation:

Splunk can analyze mobile application logs as a unique data source for threat detection, providing insights into application behavior, potential security issues, and user interactions.

Question: 140

While reviewing network traffic logs in Splunk, an analyst observes a series of rapid, high-volume data requests to a server hosting sensitive data. Which type of cybersecurity threat does this scenario suggest?

A. Phishing Attack
B. Advanced Persistent Threat (APT)
C. Distributed Denial of Service (DDoS)
D. Insider Threat

Answer: C

Explanation:

This scenario suggests a Distributed Denial of Service (DDoS) attack, characterized by rapid, high- volume requests to overwhelm and incapacitate a server, potentially as a diversion for other malicious activities.

Question: 141

What is the purpose of Splunk's Data Lineage feature in cybersecurity investigations?

A. To automate the archival of old data

B. To encrypt data in transit between Splunk components
C. To provide real-time data visualization
D. To track the movement and transformation of data through various systems

Answer: D

Explanation:

Data Lineage in Splunk tracks the movement and transformation of data through various systems, providing critical insights during cybersecurity investigations by showing how data has been altered or transferred.

Question: 142

How do Splunk's machine learning capabilities enhance anomaly detection in cybersecurity?

A. By using pre-defined static rules for all users
B. By requiring user input for each detection
C. By manually setting thresholds for alerts
D. By learning normal behavior patterns to identify outliers

Answer: D

Explanation:

Splunk's machine learning capabilities enhance anomaly detection by learning normal behavior patterns and identifying outliers, providing a dynamic and adaptive approach to detecting potential threats.

Question: 143

How does Splunk assist in the management and analysis of Endpoint Detection and Response (EDR) data?

A. By encrypting endpoint data
B. By physically securing endpoints
C. By directly managing endpoint security settings
D. By consolidating EDR data from multiple endpoints for centralized analysis

Answer: D

Explanation:

Splunk consolidates Endpoint Detection and Response (EDR) data from multiple endpoints for centralized analysis, enhancing the organization's ability to detect and respond to endpoint-related security threats.

Question: 144

What is the significance of using the "sourcetype" attribute in Splunk for cybersecurity data analysis?

A. It determines the geographical location of data sources
B. It specifies the data encryption method
C. It categorizes data to facilitate parsing and analysis
D. It defines the data retention policy

Answer: C

Explanation:

The "sourcetype" attribute in Splunk categorizes data to facilitate parsing and analysis, allowing cybersecurity analysts to apply specific parsing rules and extract meaningful information more efficiently.

Question: 145

How does Splunk's Modular Input Framework enhance data collection from various sources?

A. By reducing the volume of incoming data
B. By standardizing data formats for easier analysis
C. By encrypting all incoming data
D. By allowing the development of custom data collectors

Answer: D

Explanation:

Splunk's Modular Input Framework enhances data collection by allowing the development of custom data collectors, enabling the integration of diverse data sources into Splunk for comprehensive analysis.

Question: 146

What feature does Splunk offer to track changes in critical system files for security purposes?

A. Configuration File Snapshot
B. Audit Trail Tracking
C. Change Management Dashboard
D. File Integrity Monitoring

Answer: D

Explanation:

File Integrity Monitoring in Splunk allows organizations to track changes in critical system files, helping to identify unauthorized modifications that could indicate a security breach.

Question: 147

In incident response, how can Splunk's Timeline feature assist analysts?

A. By visualizing the sequence of events leading up to an incident
B. By predicting the time of the next attack
C. By backdating security patches
D. By scheduling future security scans

Answer: A

Explanation:

Splunk's Timeline feature assists analysts in incident response by visualizing the sequence of events leading up to an incident, helping to identify the cause and scope of security breaches.

Question: 148

An organization notices irregular patterns in login attempts from geographically inconsistent locations using Splunk. What type of security compromise is most likely occurring?

A. Brute Force Attack
B. Man-in-the-Middle Attack
C. Credential Stuffing
D. Phishing

Answer: C

Explanation:

The irregular patterns in login attempts from geographically inconsistent locations likely indicate Credential Stuffing, where attackers use stolen account credentials to gain unauthorized access to user accounts.

Question: 149

After deploying a new set of correlation rules in Splunk, an analyst notices an uptick in alerts related to unusual outbound network traffic from several endpoints. What might be occurring on these endpoints?

A. Data Exfiltration Effort
B. DDoS Attack Origination
C. Policy Violation
D. Ransomware Activity

Answer: A

Explanation:

The uptick in alerts related to unusual outbound network traffic from several endpoints, after deploying new correlation rules in Splunk, might indicate a Data Exfiltration Effort, where sensitive data could be transmitted to unauthorized entities.

Question: 150

In what way does Splunk facilitate the analysis of multi-cloud environments?

A. By limiting data analysis to the primary cloud provider
B. By providing separate instances for each cloud provider
C. By encrypting data transferred between cloud providers
D. By consolidating data from various cloud providers into a single platform

Answer: D

Explanation:

Splunk facilitates the analysis of multi-cloud environments by consolidating data from various cloud providers into a single platform, enabling unified analysis and monitoring across diverse cloud infrastructures.

Question: 151

What role does Splunk's Knowledge Objects play in enhancing SOC operations?

A. Managing user permissions and access controls B. Automating the response to security incidents C. Encrypting sensitive data within Splunk
D. Facilitating data enrichment and search efficiency **Answer: D**

Explanation:

Splunk's Knowledge Objects facilitate data enrichment and search efficiency by allowing users to reuse and share search and analysis components, enhancing SOC operations.

Question: 152

A SOC team observes a pattern of failed login attempts followed by a successful login from an unfamiliar IP address in Splunk logs. What is this sequence of events most indicative of?

A. Service Interruption
B. Account Takeover
C. Insider Threat
D. Password Spraying

Answer: D Explanation:

This sequence of events, observed in Splunk logs, is most indicative of Password Spraying, where attackers attempt to access accounts by trying common passwords across many accounts until one succeeds.

Question: 153

How does Splunk's Predictive Modelling feature support cybersecurity forecasting?

A. By simulating potential cyber attacks
B. By analyzing past security incidents to predict future threats
C. By visualizing future security trends
D. By automatically adjusting security settings based on predictions

Answer: B

Explanation:

Splunk's Predictive Modelling supports cybersecurity forecasting by analyzing past security incidents to predict future threats, enabling proactive security measures and planning.

Question: 154

In the context of cloud security, how does Splunk's integration with Cloud Access Security Brokers (CASBs) enhance data protection?

A. By offering physical security for cloud data centers
B. By consolidating security policies across cloud platforms
C. By providing a VPN for cloud services
D. By monitoring cloud traffic for suspicious activities **Answer: D**

Explanation:

Splunk's integration with Cloud Access Security Brokers (CASBs) enhances data protection by monitoring cloud traffic for suspicious activities and enforcing security policies across cloud platforms.

Question: 155

In what way does Splunk's integration with third-party threat intelligence sources enhance security operations?

A. By reducing the volume of logs collected from intelligence sources
B. By encrypting data exchanged with threat intelligence sources
C. By automatically updating security policies based on intelligence data
D. By providing a centralized platform for threat intelligence management **Answer: D**

Explanation:

Splunk's integration with third-party threat intelligence sources enhances security operations by providing a centralized platform for threat intelligence management, enriching internal data with external insights.

Question: 156

How is Splunk's Dashboard Studio utilized in enhancing situational awareness in SOC operations?

A. By automatically updating dashboards with new threat data
B. By reducing the number of dashboards required
C. By creating customizable, interactive dashboards for real-time monitoring
D. By encrypting dashboard data

Answer: C

Explanation:

Splunk's Dashboard Studio is utilized in enhancing situational awareness in SOC operations by creating customizable, interactive dashboards for real-time monitoring of security posture and threats.

Question: 157

What is the main advantage of integrating Splunk with a ticketing system like ServiceNow for SOC operations?

A. Automatically closes all high-priority tickets
B. Facilitates streamlined incident management and response
C. Increases the speed of Splunk searches
D. Encrypts communication between Splunk and ServiceNow

Answer: B

Explanation:

Integrating Splunk with a ticketing system like ServiceNow facilitates streamlined incident management and response by automating the creation, tracking, and resolution of incidents.

Question: 158

What advantage does Splunk's Dynamic Data Active Archive offer for long-term data storage in cybersecurity?

A. It ensures data is stored in a tamper-proof format for forensic analysis
B. It encrypts archived data for enhanced security
C. It archives data in real-time for immediate retrieval
D. It compresses data to reduce storage costs

Answer: A

Explanation:

Splunk's Dynamic Data Active Archive ensures data is stored in a tamper-proof format, crucial for forensic analysis in cybersecurity, providing integrity and authenticity to archived data.

Question: 159

In what way does Splunk facilitate the monitoring of Software as a Service (SaaS) applications for security threats?

A. By aggregating and analyzing logs from SaaS applications
B. By encrypting data stored within SaaS applications
C. By directly managing SaaS application security settings
D. By reducing the bandwidth used by SaaS applications

www.atmicnetworks.com

Answer: A

Explanation:

Splunk facilitates the monitoring of SaaS applications for security threats by aggregating and analyzing logs from these applications, providing visibility into user activities and potential security incidents.

Question: 160

In the context of network security, how is Splunk used to monitor encrypted traffic for anomalies?

A. By analyzing metadata and traffic patterns
B. By blocking all encrypted traffic
C. By redirecting encrypted traffic to a honeypot
D. By decrypting all traffic in real-time

Answer: A

Explanation:

Splunk is used to monitor encrypted traffic for anomalies by analyzing metadata and traffic patterns, which can reveal suspicious activities without needing to decrypt the traffic.

Question: 161

How does the Splunk Common Information Model (CIM) aid in compliance reporting?

A. By encrypting report data
B. By limiting access to reports based on user roles
C. By normalizing data to fit standardized reporting formats
D. By automatically submitting reports to regulatory bodies

Answer: C

Explanation:

The Splunk CIM aids in compliance reporting by normalizing data to fit standardized reporting formats, making it easier to generate reports that meet regulatory requirements.

Question: 162

What role does Splunk's Data Enrichment play in incident analysis?

A. To provide additional context to incident data, aiding in a deeper understanding
B. To encrypt incident data for secure analysis
C. To increase the speed of data analysis
D. To reduce the volume of data analyzed during an incident

Answer: A

Explanation:

Data Enrichment in Splunk plays a crucial role in incident analysis by providing additional context to incident data, aiding in a deeper understanding of the nature and scope of the incident.

Question: 163

How does the integration of Splunk with Endpoint Protection Platforms (EPP) improve endpoint security?

A. By automatically deploying endpoint protection agents
B. By encrypting communication between endpoints and the Splunk platform
C. By centralizing endpoint security logs for analysis
D. By reducing the number of endpoint security alerts generated

Answer: C

Explanation:

The integration of Splunk with Endpoint Protection Platforms (EPP) improves endpoint security by centralizing endpoint security logs for analysis, enhancing the visibility and management of endpoint threats.

Question: 164

Which of the following is a key benefit of Splunk's built-in scripting capabilities for cybersecurity teams?

A. Executing custom alert actions based on specific triggers
B. Automating routine data cleaning tasks
C. Generating synthetic test data
D. Performing automatic system backups at regular intervals

Answer: A

Explanation:

A key benefit of Splunk's built-in scripting capabilities is executing custom alert actions based on specific triggers, allowing cybersecurity teams to automate responses to detected threats.

Question: 165

How does Splunk's Machine Learning Toolkit enhance cybersecurity defenses?

A. By encrypting all stored data
B. By predicting future attacks based on past data
C. By creating virtual environments for malware analysis
D. By automatically patching software vulnerabilities

Answer: B

Explanation:

Splunk's Machine Learning Toolkit enhances cybersecurity defenses by predicting future attacks based on past data, allowing organizations to proactively address potential threats.

Question: 166

How can the Splunk Machine Learning Toolkit (MLTK) be utilized in identifying phishing attempts?

A. By automatically responding to phishing emails
B. By predicting user responses to phishing emails
C. By visualizing the geographic origin of phishing emails
D. By analyzing email patterns and detecting anomalies

Answer: D

Explanation:

The Splunk MLTK can be utilized in identifying phishing attempts by analyzing email patterns and detecting anomalies that deviate from normal email behavior, aiding in the early detection of phishing campaigns.

Question: 167

How does Splunk's use of Data Models contribute to its efficiency in security analytics?

A. By compressing raw data to save storage
B. By organizing data into a hierarchical structure for faster querying
C. By duplicating data for redundancy and backup purposes
D. By encrypting sensitive data within the model

Answer: B

Explanation:

Data Models contribute to Splunk's efficiency in security analytics by organizing data into a hierarchical structure, enabling faster and more efficient querying of complex datasets.

Question: 168

How does Splunk's Anomaly Detection feature aid in proactive threat hunting?

A. By encrypting sensitive anomaly data
B. By visualizing network traffic patterns
C. By scheduling regular anomaly reports
D. By identifying unusual behavior based on historical data

Answer: D

Explanation:

Splunk's Anomaly Detection aids in proactive threat hunting by identifying unusual behavior based on historical data, allowing for the early detection of potential security incidents.

Question: 169

For GDPR compliance, how does Splunk assist in monitoring data access and movement?

A. By alerting on unauthorized data access attempts B. By creating audit trails for data access and changes C. By automatically redacting personal data from logs D. By visualizing data flow in real-time dashboards **Answer: B**

Explanation:

For GDPR compliance, Splunk assists by creating audit trails for data access and changes, ensuring that there is transparency and accountability for how personal data is handled.

Question: 170

Which aspect of Splunk architecture is crucial for scaling to meet high data volume needs of large enterprises?

A. Search Head Clustering
B. Modular Inputs
C. Forwarder Management
D. Index Replication

Answer: A

Explanation:

Search Head Clustering in Splunk architecture is crucial for scaling to meet high data volume needs of large enterprises by distributing the search load across multiple search heads.

Question: 171

How does Splunk facilitate the monitoring of privileged user activities to prevent insider threats?

A. By tracking and analyzing all privileged user actions within the system
B. By encrypting the actions of privileged users for secure monitoring
C. By reducing the number of privileged users in the system
D. By automatically elevating user privileges for monitoring

Answer: A

Explanation:

Splunk facilitates the monitoring of privileged user activities by tracking and analyzing all privileged user actions within the system, helping to detect and prevent potential insider threats.

Question: 172

What is the benefit of using Splunk's Lookup Tables in the context of threat correlation?

A. They allow for the correlation of external threat data with internal event data
B. They reduce the amount of data Splunk needs to index
C. They provide a method for dynamic data encryption
D. They automatically update firewall rules based on threat data

Answer: A

Explanation:

Lookup Tables in Splunk allow for the correlation of external threat data with internal event data, enhancing threat detection and response by providing additional context to security events.

Question: 173

How do Splunk Alerts contribute to an organization's incident response strategy?

A. By automating data backups
B. By encrypting sensitive incident data
C. By notifying teams of potential incidents based on predefined criteria
D. By scheduling security scans

Answer: C

Explanation:

Splunk Alerts notify teams of potential incidents based on predefined criteria, enabling a swift and coordinated response to security threats, which is a cornerstone of an effective incident response strategy.

Question: 174

When optimizing Splunk for high-volume data ingest, what configuration can help manage performance?

A. Reducing data retention periods
B. Throttling data input rates
C. Increasing the number of search heads

D. Indexer clustering and load balancing

Answer: D

Explanation:

Indexer clustering and load balancing can help manage performance when optimizing Splunk for high- volume data ingest, ensuring efficient data processing and availability.

Question: 175

Utilizing Splunk, a security team identifies irregular application behavior, including unexpected system calls and data requests. What does this behavior most likely suggest about the application?

A. It is experiencing a Denial of Service attack
B. It contains a Zero-Day Exploit
C. It has a misconfiguration issue
D. It is being used for Command and Control communications

Answer: B

Explanation:

Irregular application behavior, identified using Splunk, such as unexpected system calls and data requests, most likely suggests the presence of a Zero-Day Exploit within the application, potentially allowing attackers to exploit previously unknown vulnerabilities.

Question: 176

Why is it crucial to define granular roles and permissions in Splunk for a SOC team?

A. To simplify the onboarding process for new analysts
B. To minimize data breach risks by applying the principle of least privilege
C. To ensure all team members have admin privileges
D. To increase the data processing speed by spreading tasks

Answer: B

Explanation:

Defining granular roles and permissions in Splunk for a SOC team is crucial to minimize data breach risks by applying the principle of least privilege, ensuring users have access only to the data and functionalities necessary for their role.

Question: 177

During a routine check, a SOC analyst uses Splunk to identify an unexpected spike in database read operations after hours. What does this anomaly most likely indicate in terms of cybersecurity threats?

A. Cross-Site Scripting
B. Zero-Day Exploit
C. Data Exfiltration
D. SQL Injection

Answer: C **Explanation:**

An unexpected spike in database read operations after hours, as identified using Splunk, most likely indicates Data Exfiltration, where sensitive data is being unauthorizedly accessed and possibly extracted.

Question: 178

What advantage does Splunk offer for managing the complexities of IoT security?

A. Physically securing IoT devices
B. Aggregating and analyzing data from diverse IoT devices
C. Automating device firmware updates
D. Creating dedicated IoT networks

Answer: B

Explanation:

Splunk offers the advantage of aggregating and analyzing data from diverse IoT devices, helping to manage the complexities of IoT security by providing insights into device behavior and potential threats.

Question: 179

How can Splunk's Indexer Clustering improve data availability in a cybersecurity context?

A. By reducing the number of required search heads
B. By compressing data to save storage space
C. By encrypting all stored data
D. By duplicating data across multiple indexers to prevent data loss **Answer: D**

Explanation:

Indexer Clustering in Splunk duplicates data across multiple indexers, enhancing data availability and reliability, which is crucial for maintaining continuous cybersecurity monitoring and analysis.

Question: 180

How can a SOC use Splunk's real-time monitoring capabilities for proactive threat hunting?

A. By using real-time alerts to track live data feeds for unusual patterns
B. By setting up dashboards to display past security incidents
C. By manually reviewing logs at the end of each day
D. By scheduling daily reports to summarize potential threats

Answer: A

Explanation:

A SOC can use Splunk's real-time monitoring capabilities for proactive threat hunting by setting up realtime alerts to track live data feeds for unusual patterns, enabling immediate detection and response to potential threats.

Question: 181

What role does the Splunk HTTP Event Collector (HEC) play in securing web applications?

A. Encrypting web traffic
B. Automatically patching web application vulnerabilities
C. Blocking malicious web requests
D. Aggregating and analyzing web application logs in real time

www.atmicnetworks.com

Answer: D
Explanation:

The Splunk HTTP Event Collector (HEC) aggregates and analyzes web application logs in real time, providing insights into web application activities and potential security threats.

Question: 182

A healthcare organization uses Splunk to monitor for unusual access to patient records. A sudden increase in record access by a single user outside of normal working hours is detected. What kind of threat might this activity represent?

A. Credential Stuffing
B. Insider Threat
C. Phishing Scam
D. Malware Infection

Answer: B
Explanation:

A sudden increase in patient record access by a single user outside of normal working hours, as detected using Splunk, might represent an Insider Threat, suggesting unauthorized or malicious activity from within the organization.

Question: 183

How does Splunk's support for Scripted Alerts contribute to incident response?

A. By automating specific actions when predefined conditions are met
B. By duplicating alerts to multiple teams for redundancy
C. By reducing the number of false positive alerts
D. By encrypting all alert data

Answer: A
Explanation:

Splunk's support for Scripted Alerts contributes to incident response by automating specific actions when predefined conditions are met, enhancing the speed and efficiency of the response to security incidents.

Question: 184

How can the use of Splunk's Predictive Analytics improve threat detection?

A. By forecasting future security trends based on historical data
B. By creating detailed user profiles for marketing purposes
C. By automatically updating firewall rules
D. By generating compliance reports for regulatory bodies

Answer: A
Explanation:

Splunk's Predictive Analytics can forecast future security trends based on historical data, allowing organizations to anticipate and prepare for potential threats before they occur.

Question: 185

How can Splunk's Visualization capabilities be used in cybersecurity compliance reporting?

A. By creating real-time dashboards for network traffic
B. By visualizing encryption standards compliance
C. By displaying user access levels across the organization
D. By generating interactive charts and graphs for audit trails

Answer: D

Explanation:

Splunk's Visualization capabilities can be used in cybersecurity compliance reporting by generating interactive charts and graphs for audit trails, making it easier to demonstrate compliance to regulatory bodies.

Question: 186

An analyst uses Splunk to track file integrity monitoring alerts and observes repeated unauthorized changes to critical system files. What type of cyber attack could this indicate?

A. Malware Infection
B. Phishing Attack
C. Supply Chain Compromise
D. Privilege Escalation

Answer: A

Explanation:

Repeated unauthorized changes to critical system files, as tracked using Splunk's file integrity monitoring alerts, could indicate a Malware Infection, potentially compromising system integrity and security.

Question: 187

How can Splunk's Data Lifecycle Management assist in compliance with data retention policies?

A. By automatically encrypting all stored data
B. By duplicating data for offsite storage
C. By managing the storage, archiving, and deletion of data according to policy
D. By reducing the volume of data collected

Answer: C

Explanation:

Splunk's Data Lifecycle Management assists in compliance with data retention policies by managing the storage, archiving, and deletion of data according to specified policies, ensuring regulatory compliance.

Question: 188

In what way does the integration of Splunk with Network Packet Capture tools enhance network security monitoring?

A. By reducing the volume of traffic that needs to be analyzed

B. By enabling real-time decryption of network traffic
C. By providing a backup of all network traffic
D. By enriching network security data with detailed packet-level insights

Answer: D

Explanation:

Integrating Splunk with Network Packet Capture tools enriches network security data with detailed packet-level insights, offering deeper visibility into network activities and potential threats.

Question: 189

In what way does the integration of Splunk with Security Orchestration, Automation, and Response (SOAR) platforms benefit SOC operations?

A. By automating routine security tasks and workflows
B. By manually coordinating responses to security incidents
C. By encrypting data exchanged between Splunk and SOAR platforms
D. By reducing the data analysis capabilities of Splunk

Answer: A

Explanation:

The integration of Splunk with SOAR platforms benefits SOC operations by automating routine security tasks and workflows, enhancing efficiency and effectiveness in incident response.

Question: 190

How can Splunk's Glass Tables be utilized in cybersecurity operations?

A. For interactive dashboards visualizing complex correlations
B. To automate threat response workflows
C. To display real-time threat intelligence data
D. For dynamic asset mapping

Answer: A

Explanation:

Glass Tables in Splunk can be utilized for creating interactive dashboards that visualize complex correlations and metrics, helping cybersecurity operations to understand and communicate security posture.

Question: 191

How does the integration of Splunk with Identity and Access Management (IAM) systems enhance security operations?

A. By reducing the number of required Splunk user licenses
B. By encrypting communication between Splunk and IAM systems
C. By automatically provisioning user accounts in Splunk
D. By centralizing user authentication logs for analysis

Answer: D

Explanation:

Integrating Splunk with Identity and Access Management (IAM) systems centralizes user authentication logs for analysis, enhancing security operations by providing insights into user activities and potential unauthorized

access attempts.

Question: 192

In the context of Advanced Persistent Threats (APTs), how does Splunk's Long-Term Trend Analysis provide value?

A. By reducing the storage of historical data to save space
B. By identifying subtle, long-term patterns indicative of APT activity
C. By predicting the next APT attack
D. By encrypting historical data for analysis

Answer: B

Explanation:

Splunk's Long-Term Trend Analysis provides value in the context of APTs by identifying subtle, longterm patterns indicative of APT activity, aiding in the early detection and understanding of sophisticated threats.

Question: 193

In what way does Splunk's support for Geospatial Data enhance cybersecurity analysis?

A. By mapping the origin of cyber attacks on a geographic map
B. By optimizing the distribution of security resources
C. By tracking the physical location of network devices
D. By encrypting geospatial data for secure analysis

Answer: A

Explanation:

Splunk's support for Geospatial Data enhances cybersecurity analysis by mapping the origin of cyber attacks on a geographic map, providing visual context to threat origins and spread.

Question: 194

What is the purpose of Splunk's Real-Time Search in the context of security monitoring?

A. To throttle incoming data for optimized analysis
B. To encrypt data streams in real-time
C. To archive data in real-time
D. To analyze security data as it's ingested for immediate threat detection

Answer: D

Explanation:

Splunk's Real-Time Search enables the analysis of security data as it's ingested, allowing for immediate threat detection and rapid response to emerging threats.

Question: 195

What is the function of Splunk's Sourcetype Renaming in log management?

A. To encrypt log data for secure storage
B. To duplicate log data for redundancy

C. To reduce the volume of logs ingested
D. To change the sourcetype attribute of logs for consistent data categorization

Answer: D

Explanation:

Splunk's Sourcetype Renaming function allows changing the sourcetype attribute of logs for consistent data categorization, improving the organization and analysis of log data.

Question: 196

What advantage do Splunk Data Models offer in terms of data analysis?

A. They provide real-time data encryption
B. They reduce the amount of data stored, saving disk space
C. They allow for hierarchical organization of data for easier analysis
D. They automate the process of data deletion after analysis

Answer: C

Explanation:

Splunk Data Models offer the advantage of allowing for a hierarchical organization of data, making it easier to perform in-depth analysis by structuring data in a logical and accessible format.

Question: 197

In incident response, how does Splunk's Adaptive Response feature streamline SOC workflows?

A. By encrypting communication between Splunk components
B. By providing real-time alerts for all security events
C. By enabling automated actions in response to specific conditions
D. By facilitating automatic data backups

Answer: C

Explanation:

Splunk's Adaptive Response feature streamlines SOC workflows by enabling automated actions in response to specific conditions, reducing manual intervention and accelerating response times.

Question: 198

An increase in encrypted traffic to unknown external IP addresses is detected by Splunk. What should be the primary concern for cybersecurity teams?

A. Enhanced privacy measures
B. Network performance issues due to encryption overhead
C. Compliance with data protection regulations
D. Potential exfiltration of sensitive data

Answer: D

Explanation:

An increase in encrypted traffic to unknown external IP addresses, as detected by Splunk, should primarily concern cybersecurity teams with the Potential Exfiltration of Sensitive Data, indicating a security breach.

Question: 199

A series of alerts in Splunk show an exponential increase in the execution of a specific script across multiple endpoints. What cybersecurity concern is this most indicative of?

A. Scheduled task execution
B. A system-wide update process
C. An orchestrated worm propagation
D. Standard software deployment

Answer: C

Explanation:

An exponential increase in the execution of a specific script across multiple endpoints, indicated by Splunk alerts, is most indicative of An Orchestrated Worm Propagation, suggesting the spread of malicious software within the network.

Question: 200

Splunk reports an unexpected surge in the use of encrypted messaging apps on corporate devices. What might be the implication for corporate security?

A. Compliance with updated communication policies
B. Enhancement of employee privacy and data security
C. Adoption of better communication tools by employees
D. Evasion of corporate data leakage prevention measures

Answer: D

Explanation:

An unexpected surge in the use of encrypted messaging apps on corporate devices, as reported by Splunk, might imply Evasion of Corporate Data Leakage Prevention Measures, potentially circumventing security controls.

Question: 201

Splunk alerts show a spike in user privilege escalation requests. What could be the underlying reason for these alerts?

A. Potential abuse of privilege escalation mechanisms
B. System updates requiring temporary elevated privileges
C. A policy change increasing security levels
D. Routine administrative tasks

Answer: A

Explanation:

A spike in user privilege escalation requests, as shown by Splunk alerts, could indicate Potential Abuse of Privilege Escalation Mechanisms, suggesting an attempt to gain unauthorized access or control.

Question: 202

Through Splunk, an analyst discovers an unusual number of new devices connecting to the network, with many failing to adhere to security policies. What might this indicate?

A. An ongoing BYOD policy implementation
B. The presence of rogue devices on the network
C. Network scanning by an external attacker
D. A spike in guest network usage

Answer: B

Explanation:

Discovering an unusual number of new devices connecting to the network through Splunk, many of which fail to adhere to security policies, might indicate The Presence of Rogue Devices on the Network, posing a significant security risk.

Question: 203

After a system upgrade, Splunk detects numerous failed integrations with third-party services. What might be the primary cause of these failures?

A. Third-party services undergoing maintenance
B. Network outages affecting third-party services
C. Incompatibilities introduced by the system upgrade D. Credential rotation not updated in the system

Answer: C

Explanation:

Numerous failed integrations with third-party services detected by Splunk after a system upgrade might primarily be caused by Incompatibilities Introduced by the System Upgrade, affecting the seamless interaction between systems.

Question: 204

Splunk detects a pattern of repeated access to deprecated APIs from legacy systems. What might this activity suggest in terms of security?

A. Potential exploitation of known vulnerabilities
B. Regular maintenance activities on legacy systems
C. Testing of backward compatibility by developers
D. Ongoing modernization of legacy systems

Answer: A

Explanation:

A pattern of repeated access to deprecated APIs from legacy systems, as detected by Splunk, might suggest Potential Exploitation of Known Vulnerabilities, risking system integrity.

Question: 205

Splunk identifies repeated use of outdated protocols in data transmissions. What might be the immediate cybersecurity action required?

A. Upgrading network infrastructure
B. Isolating affected systems for further investigation
C. Enforcing updated protocol standards through policy
D. Conducting a security awareness training session **Answer: C**

Explanation:

Repeated use of outdated protocols in data transmissions, as identified by Splunk, might require the immediate cybersecurity action of Enforcing Updated Protocol Standards through Policy to mitigate vulnerabilities.

Question: 206

Splunk logs show repeated login failures followed by a system shutdown from a critical infrastructure system. What cybersecurity issue does this pattern most likely represent?

A. Hardware failure
B. Scheduled system maintenance
C. User error causing system instability
D. Brute force attack leading to a system crash

Answer: D

Explanation:

Repeated login failures followed by a system shutdown from a critical infrastructure system, as shown in Splunk logs, most likely represent a Brute Force Attack Leading to a System Crash, potentially as a denial-of-service tactic.

Question: 207

Splunk network traffic analysis reveals a consistent pattern of fragmented packets originating from the same IP range. What might this pattern suggest about network security?

A. Routine packet fragmentation due to large data transfers
B. Network congestion and packet fragmentation
C. Misconfigured network equipment
D. A fragmentation attack to evade IDS/IPS systems

Answer: D

Explanation:

Consistent pattern of fragmented packets from the same IP range, as revealed by Splunk, might suggest a Fragmentation Attack to Evade IDS/IPS Systems, potentially bypassing security measures.

Question: 208

Following a policy change, Splunk indicates a shift in data transfer volumes to cloud storage services. What might be the cause of this change?

A. Enhanced cloud backup procedures
B. Adoption of a new cloud storage policy
C. Transition to remote work practices
D. Unauthorized data exfiltration to cloud services

Answer: D

Explanation:

A shift in data transfer volumes to cloud storage services following a policy change, as indicated by Splunk, might be caused by Unauthorized Data Exfiltration to Cloud Services, raising concerns about data leakage.

www.atmicnetworks.com

Question: 209

Splunk's analysis of user activity logs shows a pattern of data access that aligns with the timing of competitive product launches. What might this suggest?

A. Benchmarking efforts for product development
B. Collaboration with industry partners
C. Competitive intelligence gathering by employees
D. Coincidental alignment with industry events

Answer: C

Explanation:

A pattern of data access aligning with the timing of competitive product launches, as shown in Splunk's analysis, might suggest Competitive Intelligence Gathering by Employees, potentially indicating corporate espionage.

Question: 210

A financial institution uses Splunk to monitor transactions and detects a pattern of small, irregular transactions across multiple accounts. What cybersecurity concern is this pattern indicative of?

A. Money Laundering B. Credit Card Fraud C. Insider Trading D. Account Takeover

Answer: A **Explanation:**

The pattern of small, irregular transactions across multiple accounts, detected using Splunk, is indicative of Money Laundering activities, where illicit funds are processed through seemingly normal transactions to obscure their origin.

Question: 211

A sudden increase in network traffic to unfamiliar foreign IP addresses is observed in Splunk after hours. What is the most likely explanation?

A. Engagement with new international clients
B. Misconfigured network routing
C. Malicious data exfiltration attempts
D. Automated software updates

Answer: C

Explanation:

A sudden increase in network traffic to unfamiliar foreign IP addresses after hours, as observed in Splunk, is most likely explained by Malicious Data Exfiltration Attempts, suggesting a security breach.

Question: 212

Following a security patch rollout, Splunk shows an unusual pattern of system reboots and service restarts across the network. What might this pattern indicate?

A. Normal behavior during system updates
B. An attacker exploiting the patching process

C. Successful patch deployment across the network
D. Incompatibility of the patch with certain systems

Answer: D

Explanation:

An unusual pattern of system reboots and service restarts across the network following a security patch rollout, as shown by Splunk, might indicate Incompatibility of the Patch with Certain Systems, potentially causing disruptions.

Question: 213

An organization's Splunk system reports a high number of internal port scans following a BYOD policy update. What might be occurring within the internal network?

A. Unauthorized network mapping by a rogue device
B. Integration of BYOD devices into the network
C. Compliance scanning by the security team
D. Performance testing of the internal network

Answer: A

Explanation:

A high number of internal port scans following a BYOD policy update, as reported by an organization's Splunk system, might indicate Unauthorized Network Mapping by a Rogue Device, posing a security risk.

Question: 214

After the rollout of a new software update, Splunk identifies an unusual pattern of system reboots across the network. What might this indicate?

A. Successful deployment of the update
B. Incompatibility issues causing system crashes
C. Activation of a dormant virus
D. Normal behavior for update installation

Answer: B

Explanation:

An unusual pattern of system reboots across the network identified by Splunk after a software update might indicate Incompatibility Issues Causing System Crashes, requiring immediate investigation.

Question: 215

Splunk's monitoring of system logs reveals unauthorized changes to firewall rules. What is the immediate implication of this discovery?

A. Testing of new security policies
B. Compromise of administrative credentials
C. Upcoming network infrastructure upgrade
D. Inadvertent changes by IT staff

Answer: B

Explanation:

Unauthorized changes to firewall rules, as revealed by Splunk's monitoring of system logs, imply a

Compromise of Administrative Credentials, posing a serious threat to network security.

Question: 216

Following a cybersecurity training session, Splunk logs an increase in reported phishing attempts. What might this increase indicate?

A. Malfunctioning email spam filters
B. An active phishing campaign targeting the organization
C. The effectiveness of the cybersecurity training
D. Increased vigilance leading to over-reporting

Answer: C

Explanation:

An increase in reported phishing attempts following a cybersecurity training session, as logged by Splunk, might indicate the Effectiveness of the Cybersecurity Training, showing heightened employee awareness.

Question: 217

Splunk alerts reveal a pattern of access to high-value assets during unusual hours without corresponding business need. What might this indicate?

A. System misconfiguration
B. Insider threat exploiting access privileges
C. Automated data archiving
D. Scheduled maintenance

Answer: B

Explanation:

A pattern of access to high-value assets during unusual hours without a corresponding business need, as revealed by Splunk alerts, might indicate an Insider Threat Exploiting Access Privileges, potentially leading to data breaches.

Question: 218

Splunk's network monitoring tools reveal intermittent but persistent connections to rare ports on external servers. What might this activity most likely represent in a cybersecurity context?

A. Covert exfiltration of data to external servers
B. Routine peer-to-peer file sharing by employees
C. Regular updates from external software vendors
D. Network performance testing by the IT department

Answer: A

Explanation:

Intermittent but persistent connections to rare ports on external servers, as revealed by Splunk, most likely represent Covert Exfiltration of Data to External Servers, suggesting unauthorized data transfer.

Question: 219

During a network segmentation project, Splunk begins to log an unusual amount of traffic between segments. What might this indicate about the project's impact on network security?

A. Improved traffic flow efficiency
B. Decreased network latency
C. Enhanced network performance
D. Potential misconfiguration exposing internal services

Answer: D

Explanation:

The unusual amount of traffic between segments logged by Splunk during a network segmentation project might indicate a Potential Misconfiguration Exposing Internal Services, possibly creating security vulnerabilities.

Question: 220

Splunk reveals an unusual pattern of system file modifications before the deployment of a critical update. What cybersecurity risk does this pattern present?

A. Supply chain attack inserting malicious code
B. Accidental file changes by IT staff
C. Normal update preparation activities
D. Pre-update testing anomalies

Answer: A

Explanation:

An unusual pattern of system file modifications before a critical update deployment, revealed by Splunk, presents a cybersecurity risk of a Supply Chain Attack Inserting Malicious Code, potentially compromising the update.

Question: 221

A series of alerts in Splunk indicate an abnormal increase in file deletion activities across multiple endpoints. What is the most likely cause of this activity?

A. Routine system maintenance
B. Implementation of a new data retention policy
C. Automated cleanup by endpoint protection
D. Malicious insider activity

Answer: D

Explanation:

An abnormal increase in file deletion activities across multiple endpoints, as indicated by Splunk alerts, is most likely caused by Malicious Insider Activity, suggesting intentional harm or theft of data.

Question: 222

Following a software update, Splunk detects an increase in error messages from several systems. What might this suggest about the update?

A. Unintended disruption due to compatibility issues
B. Enhanced system performance
C. Successful integration with existing systems
D. Activation of dormant malware

Answer: A

Explanation:

An increase in error messages from several systems following a software update, as detected by Splunk, might suggest Unintended Disruption due to compatibility issues with the existing system environment.

Question: 223

Anomalies in CPU usage patterns across several servers are detected by Splunk. What might this be symptomatic of in terms of cybersecurity?

A. Distributed Denial of Service (DDoS) attack absorption
B. Normal fluctuations in server load
C. Cryptojacking malware infection
D. Scheduled batch processing jobs

Answer: C

Explanation:

Anomalies in CPU usage patterns across several servers detected by Splunk might be symptomatic of a Cryptojacking Malware Infection, utilizing server resources for unauthorized cryptocurrency mining.

Question: 224

After a security policy update, Splunk detects an increase in the use of unauthorized cloud storage apps. What might this indicate about employee compliance?

A. A lack of awareness or misunderstanding of the policy
B. Resistance to the policy and potential data security risks
C. General awareness and adherence to the new policy
D. The need for additional training on security policies

Answer: B

Explanation:

An increase in the use of unauthorized cloud storage apps after a security policy update, as detected by Splunk, might indicate Resistance to the Policy and Potential Data Security Risks, showing noncompliance.

Question: 225

After implementing endpoint detection solutions, Splunk starts logging unusual binary executions across the network. What might this imply?

A. Regular system updates across the network
B. Execution of legitimate administrative scripts
C. Deployment of new enterprise software
D. Indications of a polymorphic malware outbreak

Answer: D

Explanation:

Unusual binary executions across the network, as logged by Splunk after implementing endpoint detection solutions, might imply Indications of a Polymorphic Malware Outbreak, suggesting advanced malware evasion techniques.

Question: 226

www.atmicnetworks.com

An analyst notes an increase in encrypted traffic bypassing standard monitoring tools. What might this suggest about network security?

A. Increased use of secure web applications
B. Implementation of stronger encryption protocols
C. Enhanced user privacy measures
D. Circumvention of network monitoring tools by malicious actors

Answer: D

Explanation:

An increase in encrypted traffic bypassing standard monitoring tools, as noted by an analyst, might suggest Circumvention of Network Monitoring Tools by Malicious Actors, potentially hiding malicious activities.

Question: 227

A company's Splunk monitoring reveals consistent access attempts to restricted areas of its network from an unauthorized source. What does this persistent behavior most likely indicate?

A. An external penetration testing exercise
B. A misconfigured network device
C. Routine automated network scanning
D. Persistent threat actor presence

Answer: D

Explanation:

Consistent access attempts to restricted network areas from an unauthorized source, as revealed by Splunk monitoring, most likely indicate the presence of a Persistent Threat Actor, attempting to gain or expand access within the network.

Question: 228

An analysis of proxy server logs in Splunk shows repeated attempts to access blocked URLs categorized as malicious. What might be the root cause of these attempts?

A. Accidental clicks on phishing links in emails
B. Malware attempting to communicate with command and control servers
C. Automated scripts testing network security controls
D. Employees trying to bypass internet usage policies

Answer: B

Explanation:

Repeated attempts to access blocked URLs categorized as malicious, as shown in proxy server logs in Splunk, might be due to Malware Attempting to Communicate with Command and Control Servers.

Question: 229

Splunk's SIEM tools report abnormal patterns of access to the source code repository, including nighttime pulls. What cybersecurity risk does this pose?

A. Intellectual property theft

B. Normal operations by a global development team
C. Scheduled synchronization of development environments
D. Overzealous security scanning tools

Answer: A

Explanation:

Abnormal patterns of access to the source code repository, including nighttime pulls as reported by Splunk's SIEM tools, pose a cybersecurity risk of Intellectual Property Theft, potentially leading to data breaches.

Question: 230

Splunk's analysis of login events shows a pattern of successive failed logins followed by account lockouts across multiple user accounts. What might this behavior suggest?

A. System-wide password reset
B. User error in password entry
C. Account lockout policy enforcement
D. Brute force attack attempting to gain access

Answer: D

Explanation:

A pattern of successive failed logins followed by account lockouts, as analyzed by Splunk, might suggest a Brute Force Attack Attempting to Gain Access, indicating a systematic attempt to compromise user credentials.

Question: 231

An analyst observes through Splunk a pattern of sequential port scanning activities originating from a single IP address. What is the most likely intent behind this activity?

A. Testing network performance and latency
B. Conducting a penetration test as part of a security audit
C. Mapping the network for potential vulnerabilities
D. Routine network maintenance by IT staff

Answer: C

Explanation:

A pattern of sequential port scanning activities originating from a single IP address, as observed through Splunk, is most likely intended for Mapping the Network for Potential Vulnerabilities, commonly performed by attackers during reconnaissance.

Question: 232

Splunk's logs show an abrupt increase in login attempts with administrative credentials from foreign locations. What does this activity likely signify?

A. International expansion of the IT team
B. Regular VPN connections by remote employees
C. Implementation of a new global access policy
D. Credential stuffing attack from compromised sources

www.atmicnetworks.com

Answer: D

Explanation:

An abrupt increase in login attempts with administrative credentials from foreign locations, as shown in Splunk's logs, likely signifies a Credential Stuffing Attack from Compromised Sources, indicating a security threat from stolen credentials.

Question: 233

Splunk alerts indicate a surge in traffic on unusual ports. What type of threat could this activity suggest?

A. Port forwarding setup by the network team
B. Network scanning by an external attacker
C. Misconfigured network devices
D. Legitimate use of alternative network protocols

Answer: B

Explanation:

A surge in traffic on unusual ports, as indicated by Splunk alerts, could suggest Network Scanning by an External Attacker, potentially looking for vulnerable entry points.

Question: 234

Splunk records a sudden spike in failed access attempts to secure storage areas during a holiday period. What might this anomaly indicate?

A. Scheduled security drills by the security team B. Employees working remotely during holidays C. System errors in access control mechanisms D. Potential physical security breach attempts **Answer: D**

Explanation:

A sudden spike in failed access attempts to secure storage areas during a holiday period, as recorded by Splunk, might indicate Potential Physical Security Breach Attempts, highlighting a security concern during off-hours.

Question: 235

Splunk detects irregular API call patterns to internal systems. What might this irregularity indicate?

A. Scheduled maintenance activities
B. Developer testing of new features
C. Integration of new software tools
D. Potential exploitation of API vulnerabilities

Answer: D

Explanation:

Irregular API call patterns to internal systems, as detected by Splunk, might indicate Potential Exploitation of API Vulnerabilities, potentially leading to unauthorized access or data breaches.

Question: 236

An analyst notices an unusual spike in database queries containing obfuscated SQL code through Splunk.

What might this signify in terms of cybersecurity threats?

A. Routine maintenance by database administrators
B. An ongoing SQL injection attack
C. Database optimization efforts
D. Implementation of new database reporting tools

Answer: B

Explanation:

An unusual spike in database queries containing obfuscated SQL code, as noticed by an analyst through Splunk, might signify an Ongoing SQL Injection Attack, aiming to exploit database vulnerabilities.

Question: 237

A security team uses Splunk to monitor access to a proprietary software repository and notices downloads from non-standard geographic locations. What might this suggest?

A. Network routing anomalies
B. Time zone synchronization issues
C. Potential intellectual property theft
D. Global expansion of the development team

Answer: C

Explanation:

Noticing downloads from non-standard geographic locations, as monitored by Splunk, might suggest Potential Intellectual Property Theft, indicating unauthorized access and potential exfiltration of proprietary software.

Question: 238

An organization's Splunk system flags an anomaly in DNS query volumes, with a sudden spike in requests for a single domain. What could this indicate?

A. Compromised credentials
B. The onset of a DDoS attack
C. Command and Control (C2) communication
D. A successful phishing attack

Answer: C

Explanation:

A sudden spike in DNS query volumes for a single domain, flagged by Splunk, could indicate Command and Control (C2) communication, where compromised systems are attempting to connect to an attacker's server for instructions.

Question: 239

A retail company uses Splunk to monitor point-of-sale (POS) systems and notices a pattern of transactions that are abnormally small and frequent. What kind of cybersecurity issue could this pattern suggest?

A. System malfunction
B. Credit card skimming
C. Employee theft
D. Promotional abuse

Answer: B

Explanation:

A pattern of abnormally small and frequent transactions on POS systems, as monitored by Splunk, could suggest Credit Card Skimming, where small amounts are charged to test and use stolen credit card information.

Question: 240

Following a VoIP system upgrade, Splunk detects an unusual pattern of calls to international numbers. What might be the concern here?

A. Unauthorized use of VoIP services for toll fraud
B. Normal operations by global sales teams
C. Testing of new international call features
D. Configuration errors leading to misrouted calls

Answer: A

Explanation:

An unusual pattern of calls to international numbers following a VoIP system upgrade, as detected by Splunk, might be a concern for Unauthorized Use of VoIP Services for Toll Fraud, indicating exploitation.

Question: 241

Splunk alerts to an abnormal increase in database transactions linked to a single user account outside business hours. What might this activity most likely indicate?

A. User account misconfiguration
B. Unauthorized database access and potential data leakage
C. Scheduled database maintenance tasks
D. Automated database backups

Answer: B

Explanation:

An abnormal increase in database transactions linked to a single user account outside business hours, as alerted by Splunk, most likely indicates Unauthorized Database Access and Potential Data Leakage, suggesting compromised credentials or insider misuse.

Question: 242

Splunk analysis reveals repetitive data transfers at high volumes from a server to an unknown external endpoint. What might this pattern most likely indicate?

A. Indicators of data exfiltration to an unauthorized entity
B. Legitimate data sharing with partners
C. Normal traffic due to cloud synchronization services
D. Scheduled data backups

Answer: A

Explanation:

Repetitive high-volume data transfers from a server to an unknown external endpoint, as revealed by Splunk analysis, might most likely indicate Indicators of Data Exfiltration to an Unauthorized Entity, raising serious data leakage concerns.

Question: 243

Splunk's forensic analysis tools uncover deleted logs and cleared event histories in several critical systems. What might this suggest?

A. Automated log rotation policies
B. Routine log management and maintenance
C. System errors leading to data loss
D. A cover-up attempt following unauthorized access

Answer: D

Explanation:

Deleted logs and cleared event histories in critical systems, as uncovered by Splunk, might suggest a Cover-up Attempt Following Unauthorized Access, indicating a possible security breach.

Question: 244

Following a security incident, Splunk indicates repeated access to backup storage locations. What might this activity indicate?

A. Routine backup verification processes
B. Implementation of a new backup solution
C. Preparation for data recovery
D. Potential tampering with backup data

Answer: D

Explanation:

Repeated access to backup storage locations following a security incident, as indicated by Splunk, might suggest Potential Tampering with Backup Data, endangering data integrity and recovery efforts.

Question: 245

After implementing new network controls, Splunk shows a decrease in detected malware traffic but an increase in blocked URLs. What does this suggest about the network controls?

A. Overly restrictive URL filtering
B. Effective malware detection and prevention
C. Proper implementation of whitelist policies
D. Inadequate malware signature updates

Answer: B

Explanation:

A decrease in detected malware traffic with an increase in blocked URLs, as shown by Splunk, suggests Effective Malware Detection and Prevention, indicating the new network controls are successfully identifying and blocking threats.

Question: 246

Splunk highlights unusual activity in the use of administrative tools on workstations. What might this suggest?

A. IT department conducting system audits
B. Unauthorized use of administrative tools by non-IT personnel
C. Deployment of new IT management software
D. Regular maintenance activities by administrators

Answer: B

Explanation:

Unusual activity in the use of administrative tools on workstations, as highlighted by Splunk, might suggest Unauthorized Use of Administrative Tools by Non-IT Personnel, raising concerns about internal security threats.

Question: 247

A Splunk dashboard for a large retailer shows a significant increase in transactions processed just below the fraud detection threshold. What cybersecurity concern could this pattern indicate?

A. Transaction laundering
B. System optimization by finance
C. Bulk purchasing by resellers
D. Loyalty program exploitation

Answer: A

Explanation:

A significant increase in transactions processed just below the fraud detection threshold, as shown on a Splunk dashboard for a large retailer, could indicate Transaction Laundering, where illegitimate transactions are masked as legitimate.

Question: 248

An analyst observes an anomaly in the rate of file modifications on a server hosting critical applications. What might this signify?

A. Normal application updates
B. Indicators of a file integrity attack
C. Scheduled system backups
D. Misconfiguration of file synchronization services

Answer: B

Explanation:

An anomaly in the rate of file modifications on a critical application server, as observed by an analyst, might signify Indicators of a File Integrity Attack, potentially compromising application security.

Question: 249

Splunk identifies an unusual pattern of system shutdowns across multiple endpoints within a short timeframe. What cybersecurity concern might this raise?

A. Indications of a coordinated attack
B. An impending hardware failure
C. Accidental user-triggered shutdowns
D. Routine maintenance activities

Answer: A

Explanation:

An unusual pattern of system shutdowns identified by Splunk across multiple endpoints within a short timeframe might raise concerns about Indications of a Coordinated Attack, suggesting a potential attempt to disrupt operations or conceal other malicious activities.

Question: 250

Splunk alerts a financial organization to a series of small, high-frequency transactions from a dormant account. What does this suggest?

A. An error in the transaction processing system
B. Account reactivation by the legitimate owner
C. Testing of stolen financial credentials
D. Implementation of a new fintech application

Answer: C

Explanation:

A series of small, high-frequency transactions from a dormant account, as alerted by Splunk, suggests Testing of Stolen Financial Credentials, potentially indicating fraudulent activity.

Question: 251

Following the introduction of a new application, Splunk records an unexpected increase in inter-service communication errors. What could this increase indicate?

A. Network congestion issues
B. Enhanced security measures blocking certain communications
C. Successful integration of the new application
D. Incompatibilities between the new application and existing systems

Answer: D

Explanation:

An unexpected increase in inter-service communication errors following the introduction of a new application, as recorded by Splunk, could indicate Incompatibilities Between the New Application and Existing Systems, potentially affecting system stability.

Question: 252

Splunk's monitoring of firewall changes indicates unauthorized rule modifications allowing traffic from previously blocked IPs. What might this imply?

A. Accidental changes during routine maintenance B. Testing of new network segmentation strategies C. A policy update reflecting business needs
D. Compromise of firewall administrative credentials **Answer: D**

Explanation:

Unauthorized firewall rule modifications allowing traffic from previously blocked IPs, as indicated by Splunk, might imply a Compromise of Firewall Administrative Credentials, posing a significant security risk.

Question: 253

Splunk's analysis of email gateways reveals a significant rise in blocked email attachments. What could be the reason behind this trend?

A. Users sending large files against company policy
B. A widespread email-borne malware campaign
C. An increase in spam emails due to marketing activities
D. Enhanced email filtering rules recently applied

Answer: B

Explanation:

A significant rise in blocked email attachments, as revealed by Splunk's analysis of email gateways, could be due to A Widespread Email-borne Malware Campaign, leading to stricter attachment filtering to prevent malware spread.

Question: 254

During a routine analysis with Splunk, an analyst discovers that certain internal documents are being accessed repeatedly from an external IP address. What is the most likely explanation for this activity?

A. An insider sharing sensitive information
B. A breach in data security
C. A Distributed Denial of Service (DDoS) attack
D. A web crawler indexing site content

Answer: B

Explanation:

The repeated access of internal documents from an external IP address, as discovered during a routine Splunk analysis, most likely points to a Breach in Data Security, suggesting unauthorized access to sensitive information.

Question: 255

Following a phishing alert, Splunk tracks an increase in internal emails containing suspicious attachments. What might be happening within the organization?

A. A widespread phishing attack targeting employees
B. The introduction of a new email-based reporting tool
C. An internal awareness campaign using test phishing emails
D. Accidental forwarding of spam emails by employees **Answer: A**

Explanation:

An increase in internal emails containing suspicious attachments following a phishing alert, as tracked by Splunk, might indicate A Widespread Phishing Attack Targeting Employees, suggesting an internal security breach.

Question: 256

Splunk detects consistent traffic from several internal IPs to a single external IP at peak hours. What might this pattern suggest?

A. Potential command and control (C2) communication
B. User-initiated cloud storage synchronization
C. Regular data backup processes
D. Scheduled software updates

Answer: A

Explanation:

Consistent traffic from several internal IPs to a single external IP at peak hours, as detected by Splunk, might suggest Potential Command and Control (C2) Communication, indicating a compromised network.

Question: 257

Splunk alerts a manufacturing company to unusual activity in its Industrial Control Systems (ICS) network, such as unexpected commands sent to machinery. What type of threat does this signify?

A. Malware targeting the ICS network
B. Physical tampering with industrial machinery
C. A phishing campaign against company employees
D. An employee's accidental misuse of systems

Answer: A

Explanation:

Unusual activity in the ICS network, such as unexpected commands sent to machinery detected by Splunk, signifies a Malware threat targeting the ICS network, potentially aiming to disrupt operations or cause physical damage.

Question: 258

Splunk identifies unusual login attempts to administrative interfaces from geofenced regions during a public holiday. What does this scenario likely indicate?

A. Geofencing policy misconfigurations
B. Scheduled maintenance tasks requiring admin access
C. A targeted attack on administrative interfaces
D. Remote work by administrative staff

Answer: C

Explanation:

Unusual login attempts to administrative interfaces from geofenced regions during a public holiday, as identified by Splunk, likely indicate a Targeted Attack on Administrative Interfaces, suggesting a breach attempt.

Question: 259

Splunk alerts indicate a sudden and widespread change in file extensions across numerous endpoints. What could this widespread change most likely represent?

A. Batch renaming by user departments
B. A widespread ransomware infection

C. Implementation of new data archiving policies
D. Mass file corruption due to disk failure

Answer: B

Explanation:

Sudden and widespread changes in file extensions across numerous endpoints, as indicated by Splunk alerts, could most likely represent A Widespread Ransomware Infection, encrypting files for extortion.

Question: 260

After enabling new detection rules, Splunk starts generating alerts on unusual file access patterns during business hours. What might this indicate?

A. Insider threat accessing sensitive information
B. Routine file system indexing by search services
C. Implementation of a document management system
D. Deployment of an automated data archiving solution **Answer: A**

Explanation:

Unusual file access patterns during business hours, as detected by Splunk after enabling new rules, might indicate an Insider Threat Accessing Sensitive Information, suggesting unauthorized internal activities.

Question: 261

Splunk identifies a pattern of traffic redirection from a corporate website to unfamiliar external sites. What cybersecurity risk does this pattern present?

A. Possible DNS hijacking or website compromise
B. Updates to the corporate website's external links
C. The implementation of new marketing strategies
D. Routine redirection to external collaboration platforms

Answer: A

Explanation:

A pattern of traffic redirection from a corporate website to unfamiliar external sites, as identified by Splunk, presents a cybersecurity risk of Possible DNS Hijacking or Website Compromise, indicating potential tampering.

Question: 262

An anomaly in system performance metrics is detected by Splunk, with several systems showing high memory usage but low activity. What might this anomaly suggest?

A. A memory leak in a recently deployed application
B. The presence of stealthy malware residing in memory
C. Normal behavior due to memory-intensive scheduled tasks
D. An impending hardware failure requiring immediate attention

Answer: B

Explanation:

An anomaly in system performance metrics, with high memory usage but low activity as detected by Splunk,

might suggest The Presence of Stealthy Malware Residing in Memory, indicating a covert operation.

Question: 263

An organization's Splunk system reports an increase in encrypted traffic that bypasses established inspection tools. What could be the implication of this increase?

A. Upgrades to network encryption protocols
B. Malicious actors using encryption to evade detection
C. Increased use of VPNs by employees
D. Implementation of new privacy standards

Answer: B

Explanation:

An increase in encrypted traffic that bypasses established inspection tools, as reported by an organization's Splunk system, could imply that Malicious Actors are Using Encryption to Evade Detection, potentially concealing nefarious activities.

Question: 264

New Search

index*botsv3 source type«xml*i ineventlog

✓ 1 event (1/18/23 6:00:00 000 PM to 1/19/23 6 03 52 000 PM) No Event Sampling •

Events (1) Patterns Statistics Visualization

Format Timeline ’ — Zoom Out

List • / Format 20 Per Page »

< Hide Fields .= All Fields i Time Event

SELECTED FIELDS

0 host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

<1 index 1

linecount 1

a splunk server 1

> 1.19/23 5:09 59 000 PM

<Event xmlns*'http://schemas.Microsoft com/wi **6F5698FFB09)' /xEventIO>K/EventIDxVersion>!**

ted System!ime-' 2023 01 -19117:09:59'/xEventi t-w indOWS-Sy smon/Ope rati ona1</C hanne1><Compul •'Utclime' >2023-01 - 19117:09:59</Da taxOata N; e-' Image'>C:\Windo«s\Temp\hdoor .exe</DataxOi mpany' >?</DataxData Name-' Command!. i ne' >’C: \» ws\temp\</Data><Data Name’’User‘>fyodor^splur ogon!d>0xl091c98</DataxData Name=‘Terminal! 1C86507, SHA256=99925199059EEM9F7AEDM904C2F! 901)</0atax0ata Name’’ParentProcessId’>6360’

www.atmicnetworks.com

■' ParentCommandL ine' >“C: \Windo«\Sy stem32\Wi r

+ Extract New Fields

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?

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: C

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:

Fast Mode: Optimizes search performance by limiting field extractions to only those required by the search. If the analyst is in Fast Mode, non-required fields may not be extracted or displayed.

Smart Mode: Balances performance and field extraction, allowing fields to be automatically extracted and made available for analysis.

Verbose Mode: Extracts all fields and provides the most complete view of the data, though it may be slower.

Incorrect Options:

A. The analyst does not have the proper role to search this data: If this were the case, the analyst might not be able to search at all, rather than just missing extracted fields.

www.atmicnetworks.com

B. The analyst is searching newly indexed data that was improperly parsed: This would likely lead to no data being returned, rather than just missing fields.

C. The analyst did not add the extract command to their search pipeline: Field extraction in Splunk is usually automatic unless specific commands are used; the issue here is more likely related to search mode.

Splunk Documentation: Search modes and their impact on field extraction.