Vendor: Splunk

Exam Code: SPLK-5002

Exam Name: Splunk Certified Cybersecurity Defense Engineer

Version: DEMO

QUESTION 1
Which Splunk Enterprise Security add-on facilitates the ingestion of Threat Intelligence data?

A. TA-ThreatIntel
B. SA-ESSIntel
C. ESS-Intel
D. SA-ThreatIntelligence

Answer: D
Explanation:
The SA-ThreatIntelligence add-on in Splunk Enterprise Security is responsible for ingesting and normalizing threat intelligence data. It manages threat feeds and ensures they are available for correlation searches and risk analysis within ES.

QUESTION 2
In a Risk-Based Alerting implementation with Splunk Enterprise Security, which of the following best describes a risk factor?

A. A SOAR action that is drawn from annotations.
B. A multiplier of risk that depends on the characteristics of the specific user or asset.
C. A tool to enable risk data model acceleration.
D. An event that modifies risk based on the characteristics of the specific user or asset.

Answer: B
Explanation:
In Risk-Based Alerting (RBA), a risk factor is a multiplier of risk applied based on the characteristics of a user or asset, such as criticality or sensitivity. This allows higher-risk entities to accumulate risk more quickly and ensures prioritization aligns with business impact.

QUESTION 3
In a contextualization playbook, a URL is transmitted to a sandbox for examination and disposition recommendation. What underlying HTTP method is used to transmit this data to the sandbox?

A. PUT
B. POST
C. GET
D. STOR

Answer: B
Explanation:
In a contextualization playbook, when transmitting a URL or file to a sandbox for analysis, the data is sent using the HTTP POST method. POST is used because it allows submitting data in the request body, unlike GET which only appends parameters to the URL.

QUESTION 4
What provides consistency for data mapping applied to data model and saved search exports between Splunk Enterprise Security and Splunk SOAR?

A. Global field aliases
B. Global field mappings

C. Field labels
D. Field aliases

Answer: B
Explanation:
Global field mappings provide consistency for how data is mapped when exporting from Splunk Enterprise Security to Splunk SOAR. They ensure that fields align correctly across both platforms, allowing seamless integration and accurate automation or reporting.

QUESTION 5
Which tool can help provide a baseline of the data sources in a given Splunk environment?

A. Enterprise Security Content Update
B. Enterprise Security Data Library
C. Splunk Security Essentials Analytic Stories
D. Splunk Security Essentials Data Inventory

Answer: B
Explanation:
The Enterprise Security Data Library (ESDL) provides a baseline of the data sources available in a Splunk environment. It helps identify which data sources are present, how they map to security use cases, and whether they align with Enterprise Security requirements.

QUESTION 6
An engineer is writing a correlation search and wants to use T1027 from MITRE ATT&CK® as a field in Incident Review. Assuming they are writing a correlation search that does not use the Risk data model, what example statement should be appended at the end of their correlation search?

A. | eval annotations.mitre_attack.mitre_technique_id="T1027"
B. | set annotations.mitre_attack.mitre_technique_id="T1027"
C. | set field.mitre_attack.mitre_technique_id="T1027"
D. | eval field.mitre_attack.mitre_technique_id="T1027"

Answer: A
Explanation:
To associate a MITRE ATT&CK® technique with a correlation search that does not use the Risk data model, the correct approach is to append an eval statement that sets the annotation field. The correct syntax is | eval annotations.mitre_attack.mitre_technique_id="T1027".

QUESTION 7
An automation engineer for the Wonderland SOC, has configured a new asset and is getting an HTTP 403 response code. Which of the following is the possible cause of this error code?

A. The asset endpoint requires a token not username and password.
B. Asset credentials don't have adequate permissions.
C. The endpoint that the asset is configured for does not exist.
D. Either asset username or password are incorrect.

Answer: B
Explanation:
An HTTP 403 (Forbidden) response indicates that authentication may be successful, but the

credentials do not have sufficient permissions to access the requested resource. In Splunk SOAR asset configuration, this typically means the account used is valid but lacks the required authorization.

QUESTION 8
Which of the following is a methodology to help prevent malicious lateral movement?

A. MITRE ATT&CK
B. Zero Trust
C. Lockheed Martin Cyber Kill Chain®
D. Breakglass

Answer: B
Explanation:
Zero Trust is a security methodology that helps prevent malicious lateral movement by enforcing the principle of “never trust, always verify.” It restricts access based on continuous verification, least privilege, and microsegmentation, making it harder for attackers to move laterally within the network.

QUESTION 9
How does Mission Control decipher which response template to assign to findings?

A. This is determined when creating a detection in ES, which gets carried over to Mission Control.
B. Response templates are assigned to specific incident types.
C. The only way to configure this is with SOAR.
D. Mission Control uses AI to decipher which response templates are assigned.

Answer: B
Explanation:
In Mission Control, response templates are assigned to specific incident types. When a finding is generated and categorized under an incident type, the corresponding response template is automatically applied, ensuring consistency in investigation and response actions.

QUESTION 10
For detections that leverage a CIM data model, which aspect of the configuration is responsible for determining which indexes are being searched?

A. The data model's eval expression.
B. The data model's dataset hierarchy.
C. The data model's index list.
D. The data model's constraint macro.

Answer: D
Explanation:
For detections using a CIM data model, the data model’s constraint macro defines which indexes are searched. This macro ensures that only relevant indexed data is pulled into the data model, controlling the search scope for detections.

QUESTION 11
The threat-hunting team has identified suspicious activity. An analyst manually creates a notable

event using an event action to track the activity. How should a detection engineer ensure this activity automatically produces findings in the future?

A. Create a SOAR playbook to assign risk modifiers for events matching the activity.
B. Create a correlation search to produce notable events for the activity.
C. Create a risk modifier for events matching the activity.
D. Create a SOAR playbook to identify events matching the activity and assign an urgency.

Answer: B
Explanation:
To ensure that suspicious activity consistently generates findings in the future, the detection engineer should create a correlation search for the identified activity. This automates detection by continuously monitoring for the same pattern and producing notable events when it occurs again.

QUESTION 12
A detection engineer is using a threat defense informed strategy to define use cases. Which Splunk app would best facilitate their use case development process by cross referencing detections with the MITRE ATT&CK® Framework?

A. Supporting add-on for MITRE ATT&CK®
B. Splunk Security Essentials App
C. Enterprise Security
D. Enterprise Security Content Update App

Answer: B
Explanation:
The Splunk Security Essentials App is the best tool for developing use cases with a threat defense informed strategy. It allows engineers to cross-reference detections with the MITRE ATT&CK® Framework, providing guided analytic stories and mapping detections to adversary tactics and techniques.

QUESTION 13
What can an engineer use to capture contextual values from a dashboard and create a drilldown to link to a new search?

A. Tokens
B. JSON
C. Aliases
D. Environment variables

Answer: A
Explanation:
In Splunk dashboards, tokens are used to capture contextual values such as field selections or time ranges. These tokens can then be passed into a drilldown to dynamically link to and populate a new search with the selected context.

QUESTION 14
A corporate laptop was disconnected from the internet Friday at 5PM local time. While offline, the user unknowingly opened a malicious file. The laptop came back online the following Monday morning, 9AM local time. The current detection has a 15 minute lookback period. How can the detection be tuned to account for this scenario?

A. Increase the info_min_time to account for the weekend.
B. Leverage an event time configuration within the detection.
C. Leverage an index time configuration within the detection.
D. Increase the info_max_time to account for the weekend.

Answer: B
Explanation:
To catch events that occurred while the laptop was offline and only indexed later, the detection should leverage event time rather than index time. Event time ensures detections are based on when the activity actually happened, not when the logs were ingested, preventing missed findings after delayed ingestion.

QUESTION 15
Which of the following detections would use a high count of events with Windows Event Code 4740 grouped by a user to determine suspicious behavior?

A. Detect Excessive User Logins
B. Detect Excessive AWS Security Scanning
C. Detect Excessive Network Connections
D. Detect Excessive User Account Lockouts

Answer: D
Explanation:
Windows Event Code 4740 indicates that a user account has been locked out. A high count of these events grouped by user would therefore map to the detection "Detect Excessive User Account Lockouts", signaling possible brute-force or malicious login attempts.

QUESTION 16
A SOC's Incident Response Standard Operating Procedure (SOP) calls for any phishing emails containing files to be detonated in Splunk Attack Analyzer for evaluation. Which of the following can an engineer implement to gain efficiency through automation?

A. Automatically send all findings containing the tag "phishing" to create an email notification for the SOC.
B. Use a SOAR playbook to submit the email to PhishTank, which will automatically handle the Splunk Attack Analyzer submission, and make this information available to an assigned analyst.
C. Automatically assign findings containing the tag "phishing" to analysts to speed up the start of data collection steps and reduce the time to disposition for the finding.
D. Use a SOAR playbook to handle the Splunk Attack Analyzer submission and data collection steps, and make this information available to an assigned analyst.

Answer: D
Explanation:
The most efficient approach is to use a SOAR playbook to automatically handle the Splunk Attack Analyzer submission and data collection steps, then present the results to the assigned analyst. This reduces manual effort, accelerates phishing investigation workflows, and aligns directly with the SOC's SOP.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**