Question #1 *Topic 1*

Which of the following is a reason to utilize ES risk framework as a part of detection building?

A. Create a feedback loop into threat intelligence to identify potential insider threats.

B. Help accelerate the run time of detections, allowing a faster mean time to detection.

C. Simplify SOAR automation and remediation, lowering the mean time to recover.

D. Help prioritize security findings based on their potential business impact.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

When creating a case in Splunk SOAR, which action should be taken to correlate various findings (risk notables) to ensure all are actioned?

A. Search Splunk Enterprise Security for similar or duplicate events based on the threat_object field in a risk notable.

B. Search Splunk Enterprise Security for all related events based on key fields in a notable and select how to process the results to decide which events to merge into the current investigation.

C. Search Splunk Enterprise Security for similar or duplicate events based on the risk_object field in a risk notable.

D. Search Splunk Enterprise Security for all related events based on key fields in a risk notable and select how to process the results to decide which events to merge into the current investigation.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Consider the following series of events:4:00 GMT Detection runs for interval 3:30-4:004:30 GMT Detection runs for interval 4:00-4:304:35 GMT Event 1 occurs on an endpoint4:45 GMT Event 1 is indexed5:00 GMT Detection runs for interval 4:30-5:005:05 GMT Event 1 finding is added to ES with timestamp 4:355:24 GMT Event 2 occurs on an endpoint5:30 GMT Detection runs for interval 5:00-5:305:35 GMT Event 2 is indexed6:00 GMT Detection runs for interval 5:30-6:00What is the problem with the detection schedule chosen and how can it be solved?

A. The time window for the detection is too large, causing duplicate alerts.

B. The logs are delayed so the detection time window needs to be increased.

C. The time window for the detection is too small, causing duplicate alerts.

D. The logs are delayed so the detection time window needs to be decreased.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

An effective method for building automation workflows is to follow the OODA (Observe, Orient, Decide, Act) loop stages. When transitioning between the Decide and Act stages, what additional work should be included before automating the Act stage?

A. Create a new response template.

B. Validate if the asset, identity, or service has an exemption.

C. Validate response data paths from Decide stage.

D. Create a new automation playbook.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

What is the best method to operationalize the results of a threat hunt for daily use by SOC analysts?

A. Communicate findings based on the hunt.

B. Create monthly reports based on the documented findings.

C. Create detections based on the documented findings.

D. Communicate gaps to the architecture team.

Suggested Answer: *C*

Community vote distribution

C (100%)

bolinhtinh Most Recent 2 months ago

Selected Answer: C

Threat hunting is a proactive, hypothesis-driven exercise designed to find malicious activity that has successfully bypassed existing security controls. However, a threat hunt is typically a one-time or periodic manual effort. To "operationalize" it means turning those manual discoveries into a repeatable, automated asset that protects the environment moving forward. Why C is correct: By converting the specific indicators of compromise (IOCs), behaviors, or tactics discovered during the hunt into permanent alerting detections (such as a Splunk correlation search), you hand that intelligence over to the Security Operations Center (SOC). This ensures that if that specific malicious behavior ever occurs again, an alert is automatically generated for daily triage by SOC analysts.

upvoted 1 times

Question #6 *Topic 1*

How can an engineer verify if results will return for a potential detection based on historical events within the organization?

A. Run the detection in Splunk Attack Range against the latest Atomic Red Team™ injections.

B. Run the detection with the added constraints of earliest=now latest=+24h.

C. Run the detection against production data within the same Splunk instance.

D. Run the detection with the added constraints of earliest=0 latest=l.

Suggested Answer: *C*

Community vote distribution

C (100%)

bolinhtinh Most Recent 2 months ago

Selected Answer: C

C is correct: Running the search against your actual production data (historical logs) is the only way to see if the detection logic matches real-world data patterns unique to your organization. This helps you validate if the logic works and check for potential false positives before turning the rule live.

upvoted 1 times

Question #7 *Topic 1*

Which of the following is not a type of metadata that can be returned by the metadata command?

A. sourcetypes

B. hosts

C. sources

D. assets

Suggested Answer: *D*

Community vote distribution

D (100%)

bolinhtinh Most Recent 2 months ago

Selected Answer: D

Why D is correct: assets is not a valid argument type for the metadata command. Splunk core doesn't track "assets" out of the box at the raw index metadata level; asset tracking is typically handled within the Asset and Identity framework inside Splunk Enterprise Security (ES) using lookup tables and KV stores.

upvoted 1 times

Question #8 *Topic 1*

MITRE D3FEND™ is designed to compliment MITRE's list of adversarial tactics, techniques, and common knowledge (ATT&CK®). Which tactics are associated with MITRE D3FEND™ in order to detect, deny, and disrupt adversarial efforts?

A. Harden, Detect, Exclude, Deceive, Eradicate

B. Harden, Detect, Isolate, Disrupt, Evict

C. Harden, Detect, Exclude, Define, Eradicate

D. Harden, Detect, Isolate, Deceive, Evict

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Below is an example of a sysmon process create log. Which EventCode would be associated to this log entry?

```
UtcTime: 2024-04-28 22:08:22.025
ProcessGuid: {a51eaell-bd69-1883-0000-0010e9d95e00}
ProcessId: 6228
Image: C:\Windows\System32\WindowsPowerShell\vl.0\powershell.exe
CommandLine: "C:\Windows\System32\WindowsPowerShell\vl.0\powershell.exe"
CurrentDirectory: C:\windows\temp\
User: LAB\rsmith
LogonGuid: {a23eae89-b357-5903-0000-002005eb0700}
LogonId: 0x7EB05
TerminalSessionId: 1
IntegrityLevel:
MediumHashes: SHA256=6055A20CF7EC81843310AD37700FF67B2CF8CDE3DCE68D54BA42934177C10B57
ParentProcessGuid: {a23eae89-bd28-5903-0000-00102f345d00)
ParentProcessId: 13220
Parentlinage: C:\Windows\System32\WindowsPowerShell\vl.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\vl.0\powershell.exe"
```

A. EventCode=4

B. EventCode=2

C. EventCode=1

D. EventCode=3

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Based on a recent red team exercise, an organization is highly concerned about pass the hash attacks especially including tools like Empire. Which EventCode associated to PowerShell Script Block Logging would be used to detect this activity?

A. EventCode=4126

B. EventCode=4168

C. EventCode=4624

D. EventCode=4104

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

When developing security metrics, why would a Key Performance Indicator (KPI) that focuses on total perimeter firewall blocks be an ineffective metric?

A. This a Key Result Indicator, not a KPI. It is a metric that is measuring the results of the perimeter firewall's actions, not the performance of the firewall.

B. Perimeter firewalls are exposed on the internet directly and thus subject to automated scanners and attack tools.

C. The metric is too high level, it should be broken down by the type of block. For example, blocks of remote systems that have repeated failed connections to services that do not exist.

D. Perimeter firewalls should be measured on both the number of connections that they permit as well as the number they block.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Which stash event field created by an adaptive response action allows for troubleshooting the correlation search that created the notable event?

A. search_sid

B. search_rid

C. orig_sid

D. orig_rid

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

An engineer needs to create a new report capturing the vendors and products that detect a particular CVE in their environment. How can they ensure that their search associated with the report only includes accelerated data?

A. Search for the vendor_product within the Vulnerabilities data model, using the | tstats command.

B. Search for the cve within the Vulnerabilities data model, using | tstats grouped by vendor_product with summariesonly=true.

C. Search for the vendor_product within the Updates data model, using the | tstats command.

D. Search for the vendor_product within the Updates data model, using | tstats grouped by eve with summariesonly=true.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

What field is used by default to direct data into CIM data model datasets?

A. sourcetype

B. tag

C. dataset

D. source

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

An engineer receives a report that the "Traffic over time by action" dashboard is not populating. It has been confirmed that the relevant logs are being ingested properly and they are CIM compliant.What other configuration may be missing?

A. The Performance data model is missing the network dataset.

B. The Network Traffic data model should be accelerated.

C. The Network Sessions data model has been deleted.

D. The Network Sessions data model should be accelerated.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

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

Suggested Answer: *B*

celace Most Recent 2 months, 3 weeks ago

B. Global field mappings

upvoted 1 times

Question #20 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

D (100%)

fordhamej Most Recent 4 months, 3 weeks ago

Selected Answer: D

D is the correct answer.

upvoted 2 times

51fccff 7 months, 1 week ago

Selected Answer: D

D. Splunk Security Essentials Data Inventory That is the tool designed to baseline and assess which data sources exist in a Splunk environment. The others focus on content, detections, or updates, not inventory.

upvoted 2 times

Question #21 *Topic 1*

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"

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

51fccff Most Recent 7 months, 1 week ago

Selected Answer: B

HTTP 403 means forbidden. Authentication succeeded, authorization failed. Wrong credentials usually give 401, a missing endpoint gives 404, and token versus basic auth is a configuration mismatch, not specifically a 403.

upvoted 2 times

Question #23 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

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.

Suggested Answer: *B*

celace Most Recent 2 months, 3 weeks ago

B. Response templates are assigned to specific incident types.

upvoted 1 times

Question #25 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

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.

Suggested Answer: *B*

celace Most Recent 2 months, 3 weeks ago

C. Leverage an index time configuration within the detection.

upvoted 1 times

Question #30 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

Which fields are used to determine asset priority, when priority is assigned through an asset and identity lookup?

A. dest, src, or dvc

B. dest_user or src_user

C. user or src_user

D. dest, src, or tag

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

What framework in Enterprise Security allows engineers to build detections using known malicious IOCs comparing them to event logs to find suspicious behavior?

A. Incident Management Framework

B. Asset & Intelligence Framework

C. Threat Intelligence Framework

D. OSINT Framework

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

Which of the following can process data from configured containers using an automated sequence of actions?

A. Workbooks

B. Cases

C. Playbooks

D. Containers

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

A Detection Engineer works closely with SOC leads to define expected analyst workflows, often documented as a Standard Operating Procedure (SOP). Which capability can be used to document expected analyst actions in an investigation?

A. Investigation notes

B. Adaptive response actions

C. Response templates

D. Correlation Search Editor

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

What document can be helpful in understanding the prioritization of risk when comparing entities in an organization?

A. A hierarchical organization chart

B. Infrastructure architecture diagrams

C. Application architecture diagrams

D. Business Continuity or Disaster Recovery plan

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

Which of the following cURL commands would allow an engineer to effectively disable the REST API endpoint they've been utilizing for testing a detection named TestSearchDevelopment?

A. curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/ -X DELETE

B. Splunk endpoints cannot be disabled.

C. curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable -X POST

D. curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable -X PUT

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

An engineer wants to track and report on all authentication to corporate assets, and wants to prioritize critical assets without significantly increasing the number of findings (notable events) generated. What process could be used to accomplish this goal?

A. Determine a general risk rule for all access attempts to all assets, and then increase the Risk Factor for critical assets.

B. Decrease the risk score of non-critical assets in all existing detections.

C. Add all access attempts to the Risk Index, and increase the Criticality of the critical assets.

D. Add the critical assets to the risk data model.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

In the context of Splunk's Common Information Model (CIM), which constraint ensures that events from different data sources appear in the applicable data model?

A. hosts

B. field names

C. sources

D. tags

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Which tool can help identify known tactics, techniques, and procedures that a threat group is most likely to use when targeting a financial organization?

A. The Lockheed Martin Cyber Kill Chain® Posture panel within Enterprise Security's Incident Review page

B. The MITRE ATT&CK® Posture panel within Mission Control's Incident Review page

C. The MITRE ATT&CK® matrix's industry heatmap in Splunk Security Essentials

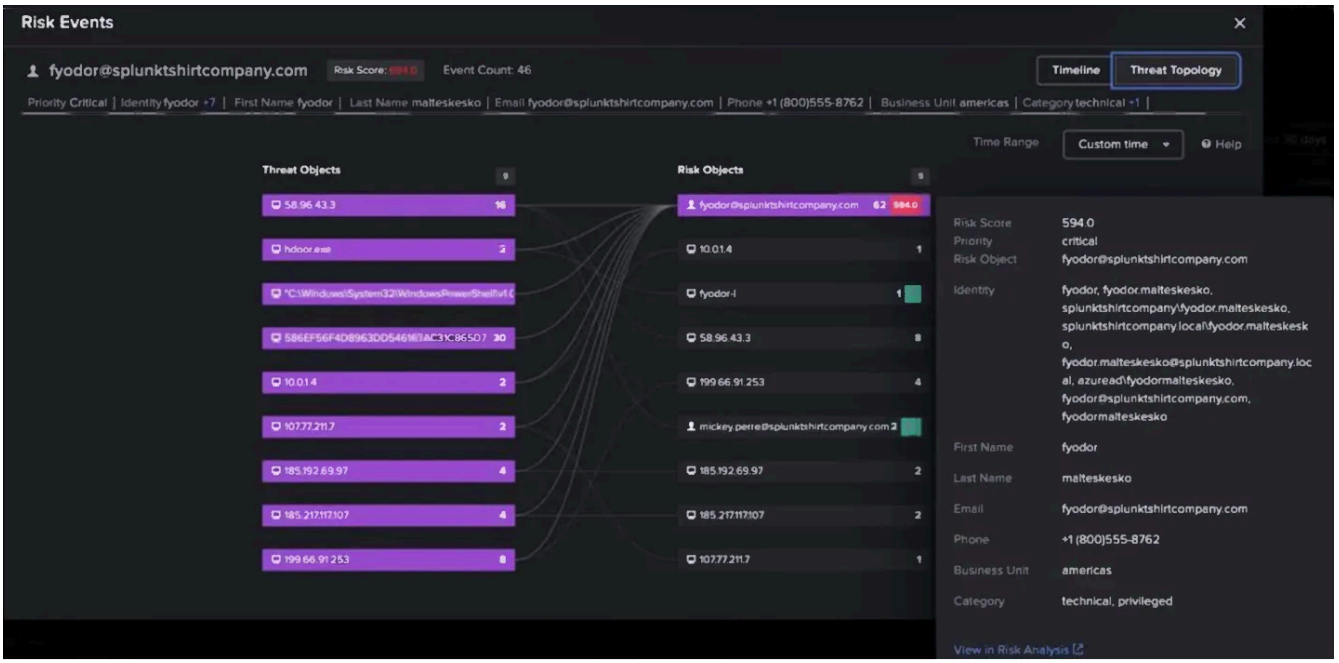
D. Splunk Threat Intelligence Management

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

Based on the provided screenshot, it's discovered that different machines or accounts have been associated with the shown threat objects. Enterprise Security has identified that these machines and accounts all point back to one owner - Fyodor.Which two frameworks in ES are responsible for programmatically associating this information together?



A. Threat Intelligence, Assets & Identities

B. Risk, Incident Review

C. Risk, Assets & Identities

D. Threat Intelligence, Risk

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

An engineer notices that a detection is creating multiple findings (notables) for the same potential incident. Which setting can be adjusted to reduce the number of generated findings (notables)?

A. Correlation search priority

B. Adaptive response actions

C. Adaptive risk modifier

D. Correlation search throttling

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

Which of the following should an engineer do as they evaluate their Threat Detection and Incident Response lifecycle?

A. Evaluate the threat process lifecycle based on contextual business and industry knowledge.

B. Use the MITRE ATT&CK® framework to evaluate the organization's risk appetite.

C. Focus efforts on the least impactful threat vectors.

D. Evaluate the threat process lifecycle based on profit margins and MTTR.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

Which of the following is the most efficient search to return a list of all visible indexes and the sourcetypes contained within them?

A. index=* | stats count by sourcetype, index

B. index=* sourcetype=* | stats values(sourcetype) by index

C. | tstats values(sourcetype) where index=true

D. | tstats values(sourcetype) where index=* by index

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

When creating a detection that searches user activity across CIM-compliant data, which CIM field should be reviewed to ensure that data is aggregated appropriately?

A. userid

B. identity

C. srcUser

D. user

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

The SOC Manager requested a better method to standardize the list of tasks that analysts follow when they evaluate events or cases. Which Splunk SOAR feature allows the creation of SOPs based on criteria like the type of event or attack vector?

A. Workbooks

B. Events

C. Cases

D. Incidents

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

In which threat intelligence KV store would a list of malicious domains (FQDNs) be stored?

A. certificate_intel

B. service_intel

C. http_intel

D. ip_intel

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

When building a metrics dashboard for the SOC manager, which metric would represent how long it takes to fully complete an investigation?

A. MTTR

B. MTTA

C. MTBF

D. MTTD

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

During a ransomware attack, an adversary might add a default user and password in registry, modify the wallpaper, and create bulk ransomware notes across multiple machines. What is Splunk's method for grouping these types of detections together?

A. Analytic Stories

B. Data models

C. Threat Intelligence

D. Assets & Identities framework

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

Which of the following identifies elements of the Detection Development Lifecyle (DDLC)?

A. Research, Develop, Document, Test, Deploy

B. Research, Design, Deploy, Validate

C. Design, Develop, Deploy, Monitor, Maintain

D. Design, Develop, Test, Deploy

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

The SOC notices over the course of an investigation there are numerous logs like the following:14-Apr-2024 20:16:49.083 client 15.111.116.918*18345 UDP: query: reallybad.c2.com IN A response: SERVFAIL +EWhat detection should be created to alert on this behavior for the future?

A. Excessive Endpoint Failures

B. Excessive Network Failures

C. Excessive Authentication Failures

D. Excessive DNS Failures

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!