# SPLK-5002퍼펙트인증공부 - SPLK-5002퍼펙트덤프최신버전

Dumps BASE
New SPLK-5002 Dumps – The Latest Learning
Resources for Splunk Certified Cybersecurity
Defense Engineer Exam Preparation
DATA

2025 Itexamdump 최신 SPLK-5002 PDF 버전 시험 문제집과 SPLK-5002 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=1-uaynQqW31ye9ScraJYRNa9THLcIkr0x

Splunk인증 SPLK-5002시험은 멋진 IT전문가로 거듭나는 길에서 반드시 넘어야할 높은 산입니다. Splunk인증 SPLK-5002시험문제패스가 어렵다한들Itexamdump덤프만 있으면 패스도 간단한 일로 변경됩니다. Itexamdump의 Splunk인증 SPLK-5002덤프는 100%시험패스율을 보장합니다. Splunk인증 SPLK-5002시험문제가 업데이트되면 Splunk인증 SPLK-5002덤프도 바로 업데이트하여 무료 업데이트서비스를 제공해드리기에 덤프유효기간을 연장해는것으로 됩니다.

## Splunk SPLK-5002 시험요강:

| 주제 | 소개 |
|---|---|
| 주제 1 | • Data Engineering: This section of the exam measures the skills of Security Analysts and Cybersecurity Engineers and covers foundational data management tasks. It includes performing data review and analysis, creating and maintaining efficient data indexing, and applying Splunk methods for data normalization to ensure structured and usable datasets for security operations. |
| 주제 2 | • Auditing and Reporting on Security Programs: This section tests Auditors and Security Architects on validating and communicating program effectiveness. It includes designing security metrics, generating compliance reports, and building dashboards to visualize program performance and vulnerabilities for stakeholders. |
| 주제 3 | • Automation and Efficiency: This section assesses Automation Engineers and SOAR Specialists in streamlining security operations. It covers developing automation for SOPs, optimizing case management workflows, utilizing REST APIs, designing SOAR playbooks for response automation, and evaluating integrations between Splunk Enterprise Security and SOAR tools. |
| 주제 4 | • Building Effective Security Processes and Programs: This section targets Security Program Managers and Compliance Officers, focusing on operationalizing security workflows. It involves researching and integrating threat intelligence, applying risk and detection prioritization methodologies, and developing documentation or standard operating procedures (SOPs) to maintain robust security practices. |
| 주제 5 | • Detection Engineering: This section evaluates the expertise of Threat Hunters and SOC Engineers in developing and refining security detections. Topics include creating and tuning correlation searches, integrating contextual data into detections, applying risk-based modifiers, generating actionable Notable Events, and managing the lifecycle of detection rules to adapt to evolving threats. |

# SPLK-5002 덤프공부, SPLK-5002시험자료

SPLK-5002덤프를 퍼펙트하게 공부하시면 보다 쉽게 시험에서 패스할수 있습니다. 다년간 IT업계에 종사하신 전문가들이 SPLK-5002인증시험을 부단히 연구하고 분석한 성과가 SPLK-5002덤프에 고스란히 담겨져 있어 시험합격율이 100%에 달한다고 해도 과언이 아닌것 같습니다.SPLK-5002덤프 구매의향이 있으신 분은 구매페이지에서 덤프 데모문제를 다운받아 보시고 구매결정을 하시면 됩니다.Itexamdump는 모든 분들이 시험에서 합격하시길 항상 기원하고 있습니다.

# 최신 Cybersecurity Defense Analyst SPLK-5002 무료샘플문제 (Q79-Q84):

### 질문 # 79

How can you incorporate additional context into notable events generated by correlation searches?

- A. By optimizing the search head memory
- B. By using the dedup command in SPL
- C. By configuring additional indexers
- D. By adding enriched fields during search execution

### 정답：D

### 설명：

In Splunk Enterprise Security (ES), notable events are generated by correlation searches, which are predefined searches designed to detect security incidents by analyzing logs and alerts from multiple data sources. Adding additional context to these notable events enhances their value for analysts and improves the efficiency of incident response.
To incorporate additional context, you can:
Use lookup tables to enrich data with information such as asset details, threat intelligence, and user identity.
Leverage KV Store or external enrichment sources like CMDB (Configuration Management Database) and identity management solutions.
Apply Splunk macros orevalcommands to transform and enhance event data dynamically.
Use Adaptive Response Actions in Splunk ES to pull additional information into a notable event.
The correct answer is A. By adding enriched fields during search execution, because enrichment occurs dynamically during search execution, ensuring that additional fields (such as geolocation, asset owner, and risk score) are included in the notable event.
References:
Splunk ES Documentation on Notable Event Enrichment
Correlation Search Best Practices
Using Lookups for Data Enrichment

### 질문 # 80

A company wants to implement risk-based detection for privileged account activities.
Whatshould they configure first?

- A. Asset and identity information for privileged accounts
- B. Correlation searches with low thresholds
- C. Automated dashboards for all accounts
- D. Event sampling for raw data

### 정답：A

### 설명：

Why Configure Asset & Identity Information for Privileged Accounts First?
Risk-based detection focuses on identifying and prioritizing threats based on the severity of their impact. For privileged accounts (admins, domain controllers, finance users), understanding who they are, what they access, and how they behave is critical.
#Key Steps for Risk-Based Detection in Splunk ES:1##Define Privileged Accounts & Groups - Identify high- risk users (Admin, HR, Finance, CISO).2##Assign Risk Scores - Apply higher scores to actions involving privileged users.3##Enable Identity & Asset Correlation - Link users to assets for better detection.
4##Monitor for Anomalies - Detect abnormal login patterns, excessive file access, or unusual privilege escalation.
#Example in Splunk ES:

A domain admin logs in from an unusual location # Trigger high-risk alert A finance director downloads sensitive payroll data at midnight # Escalate for investigation Why Not the Other Options?

#B. Correlation searches with low thresholds - May generate excessive false positives, overwhelming the SOC.#C. Event sampling for raw data - Doesn't provide context for risk-based detection.#D. Automated dashboards for all accounts - Useful for visibility, but not the first step for risk-based security.

References & Learning Resources

#Splunk ES Risk-Based Alerting (RBA): https://www.splunk.com/en_us/blog/security/risk-based-alerting.html#Privileged Account Monitoring in Splunk: https://docs.splunk.com/Documentation/ES/latest/User/RiskBasedAlerting#Implementing Privileged Access Security (PAM) with Splunk: https://splunkbase.splunk.com

### 질문 # 81

How can you ensure that a specific sourcetype is assigned during data ingestion?

- A. Use props.conf to specify the sourcetype.
- B. Define the sourcetype in the search head.
- C. Use REST API calls to tag sourcetypes dynamically.
- D. Configure the sourcetype in the deployment server.

**정답： A**

**설명：**

Why Useprops.confto Assign Sourcetypes?

In Splunk, sourcetypes define the format and structure of incoming data. Assigning the correct sourcetype ensures that logs are parsed, indexed, and searchable correctly.

#How Doesprops.confHelp?

props.confallows manual sourcetype assignment based on source or host.

Ensures that logs are indexed with the correct parsing rules (timestamps, fields, etc.).

#Example Configuration inprops.conf:

ini

CopyEdit

```
[source::/var/log/auth.log]
sourcetype = auth_logs
```

#This forces all logs from/var/log/auth.logto be assigned sourcetype=auth_logs.

Why Not the Other Options?

#B. Define the sourcetype in the search head - Sourcetypes are assigned at ingestion time, not at search time.

#C. Configure the sourcetype in the deployment server - The deployment server manages configurations, butprops.confis what actually assigns sourcetypes.#D. Use REST API calls to tag sourcetypes dynamically - REST APIs help modify configurations, but they don't assign sourcetypes directly during ingestion.

References & Learning Resources

#Splunkprops.confDocumentation:https://docs.splunk.com/Documentation/Splunk/latest/Admin/Propsconf#Best Practices for Sourcetype Management: https://www.splunk.com/en_us/blog/tips-and- tricks#Splunk Data Parsing Guide: https://splunkbase.splunk.com

### 질문 # 82

What is the purpose of using data models in building dashboards?

- A. To compress indexed data
- B. To provide a consistent structure for dashboard queries
- C. To reduce storage usage on Splunk instances
- D. To store raw data for compliance purposes

**정답： B**

**설명：**

Why Use Data Models in Dashboards?

SplunkData Modelsallow dashboards toretrieve structured, normalized data quickly, improving search performance and accuracy.

#How Data Models Help in Dashboards?(AnswerB)#Standardized Field Naming- Ensures that queries always useconsistent field names(e.g.,src_ipinstead ofsource_ip).#Faster Searches- Data models allow dashboards torun structured searches instead of raw

log queries.#Example:ASOC dashboard for user activity monitoringuses a CIM-compliantAuthentication Data Model, ensuring that querieswork across different log sources.
Why Not the Other Options?
#A. To store raw data for compliance purposes- Raw data is stored in indexes,not data models.#C. To compress indexed data- Data modelsstructuredata but donot perform compression.#D. To reduce storage usage on Splunk instances- Data modelshelp with search performance, not storage reduction.
References & Learning Resources
#Splunk Data Models for Dashboard Optimization: https://docs.splunk.com/Documentation/Splunk/latest /Knowledge/Aboutdatamodels#Building Efficient Dashboards Using Data Models: https://splunkbase.splunk. com#Using CIM-Compliant Data Models for Security Analytics: https://www.splunk.com/en_us/blog/tips- and-tricks

### 질문 # 83

Which report type is most suitable for monitoring the success of a phishing campaign detection program?

- A. Weekly incident trend reports
- B. Risk score-based summary reports
- C. SLA compliance reports
- D. Real-time notable event dashboards

**정답： D**

**설명：**
Why Use Real-Time Notable Event Dashboards for Phishing Detection?
Phishing campaigns require real-time monitoring to detect threats as they emerge and respond quickly.
#Why "Real-Time Notable Event Dashboards" is the Best Choice? (Answer B)#Shows live security alerts for phishing detections.#Enables SOC analysts to take immediate action (e.g., blocking malicious domains, disabling compromised accounts).#Uses correlation searches in Splunk Enterprise Security (ES) to detect phishing indicators.
#Example in Splunk:#Scenario: A company runs a phishing awareness campaign.#Real-time dashboards track:
How many employees clicked on phishing links.
How many users reported phishing emails.
Any suspicious activity (e.g., account takeovers).
Why Not the Other Options?
#A. Weekly incident trend reports - Helpful for analysis but not fast enough for phishing detection.#C. Risk score-based summary reports - Risk scores are useful but not designed for real-time phishing detection.#D.
SLA compliance reports - SLA reports measure performance but don't help actively detect phishing attacks.
References & Learning Resources
#Splunk ES Notable Events & Phishing Detection: https://docs.splunk.com/Documentation/ES#Real-Time Security Monitoring with Splunk: https://splunkbase.splunk.com#SOC Dashboards for Phishing Campaigns:
https://www.splunk.com/en_us/blog/tips-and-tricks

### 질문 # 84

......

- 시험패스 가능한 SPLK-5002퍼펙트 인증공부 최신버전 덤프데모문제 다운로드 □ 무료로 쉽게 다운로드하려면⤜ www.dumptop.com □에서【 SPLK-5002 】를 검색하세요SPLK-5002시험대비 인증공부자료
- SPLK-5002퍼펙트 인증공부 최신 시험 최신 덤프 □ 오픈 웹 사이트☀ www.itdumpskr.com □☀□검색▹ SPLK-5002 ◃무료 다운로드SPLK-5002시험대비 덤프공부자료
- SPLK-5002퍼펙트 인증공부 완벽한 덤프 최신버전 자료 □ 무료 다운로드를 위해 지금“ www.dumptop.com ”에서□ SPLK-5002 □검색SPLK-5002완벽한 인증자료
- SPLK-5002최신 업데이트 시험덤프 □ SPLK-5002최고품질 덤프샘플문제 □ SPLK-5002시험대비 덤프자료 □ □ www.itdumpskr.com □을(를) 열고□ SPLK-5002 □를 입력하고 무료 다운로드를 받으십시오SPLK-5002완벽한 인증자료
- SPLK-5002인증시험대비자료 □ SPLK-5002최고덤프 □ SPLK-5002높은 통과율 인기 시험자료 □ ⇒ kr.fast2test.com⇐을(를) 열고（ SPLK-5002 ）를 검색하여 시험 자료를 무료로 다운로드하십시오SPLK-5002 Dumps
- SPLK-5002최고품질 덤프샘플문제 □ SPLK-5002인증시험대비자료 □ SPLK-5002인증시험대비자료 □（ www.itdumpskr.com ）을(를) 열고⇛ SPLK-5002 ⇚를 검색하여 시험 자료를 무료로 다운로드하십시오SPLK-5002시험대비 인증공부자료
- SPLK-5002퍼펙트 인증공부 100% 합격 보장 가능한 최신버전 공부자료 □ 시험 자료를 무료로 다운로드하려면➠ www.exampassdump.com □을 통해✔ SPLK-5002 □✔□를 검색하십시오SPLK-5002퍼펙트 덤프 최신 데모문제
- pct.edu.pk, www.stes.tyc.edu.tw, www.61921.com, cocoasr18.blogspot.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lms.ait.edu.za, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, my.ishen021.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

BONUS!!! Itexamdump SPLK-5002 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1-uaynQqW31ye9ScraJYRNa9THLcIkr0x