Quiz Fortinet - Newest FCP_FSM_AN-7.2 - FCP - FortiSIEM 7.2 Analyst Exam Quiz

BONUS!!! Download part of TestKingIT FCP_FSM_AN-7.2 dumps for free: https://drive.google.com/open?id=12f3rU6DT31OHjh6d4H7clGaNH4KeHv0i

Many customers may be doubtful about our price. The truth is our price is relatively cheap among our peer. The inevitable trend is that knowledge is becoming worthy, and it explains why good FCP_FSM_AN-7.2 resources, services and data worth a good price. We always put our customers in the first place. Thus we offer discounts from time to time, and you can get 50% discount at the second time you buy our FCP_FSM_AN-7.2 question dumps after a year. Lower price with higher quality, that’s the reason why you should choose our FCP_FSM_AN-7.2 prep guide.

If you prefer to practice FCP_FSM_AN-7.2 questions and answers on paper, then our FCP_FSM_AN-7.2 exam dumps are your best choice. FCP_FSM_AN-7.2 PDF version is printable, and you can print them into a hard one and take notes on them, and you can take them with you. FCP_FSM_AN-7.2 exam bootcamp offers you free demo for you to have a try before buying, so that you can have a better understanding of what you are going to buy. FCP_FSM_AN-7.2 Exam Materials contain both questions and answers, and you can have a convenient check after practicing.

>> FCP_FSM_AN-7.2 Exam Quiz <<

FCP_FSM_AN-7.2 Exam | FCP_FSM_AN-7.2 Free Dump Download

This document of FCP_FSM_AN-7.2 exam questions is very convenient. Furthermore, the Fortinet FCP_FSM_AN-7.2 PDF questions collection is printable which enables you to study without any smart device. This can be helpful since many applicants prefer off-screen study. All these features of Fortinet FCP_FSM_AN-7.2 Pdf Format are just to facilitate your preparation for the FCP_FSM_AN-7.2 examination.

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

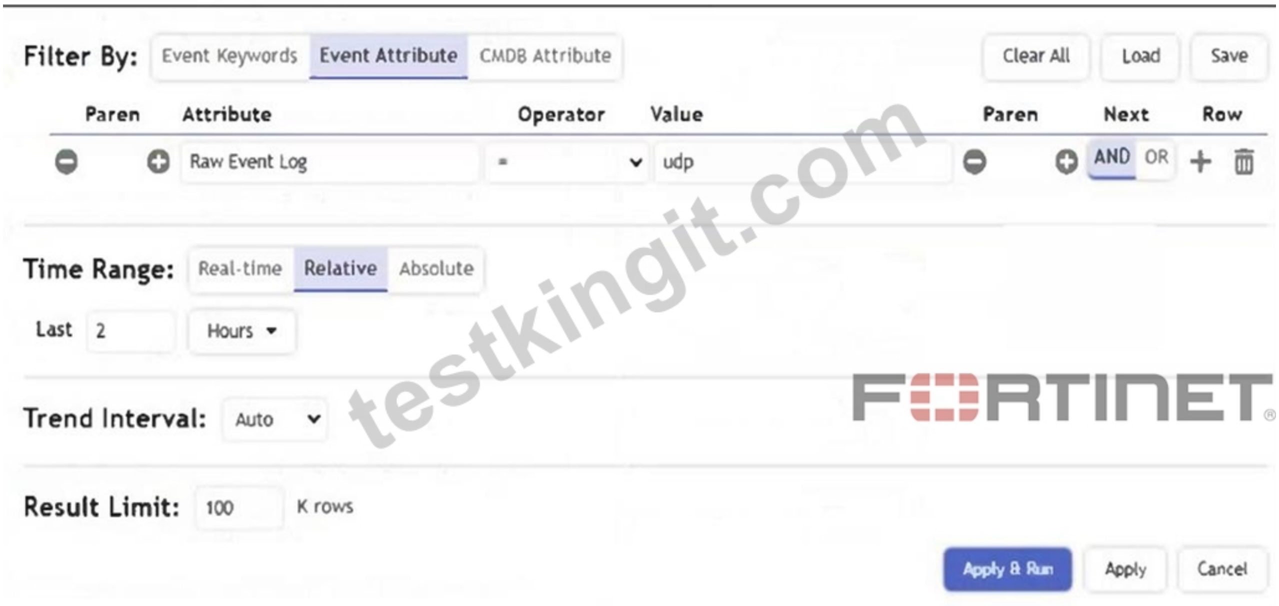
Topic	Details

Topic 1	- Rules and subpatterns: This section of the exam measures the skills of SOC Engineers and focuses on the construction and implementation of analytics rules. It involves identifying the different components that make up a rule, utilizing advanced features like subpatterns and aggregation, and practically configuring these rules within the FortiSIEM platform to detect security events.
Topic 2	- Machine learning, UEBA, and ZTNA: This section of the exam measures the skills of Advanced Security Architects and covers the integration of modern security technologies. It involves performing configuration tasks for machine learning models, incorporating UEBA (User and Entity Behavior Analytics) data into rules and dashboards for enhanced threat detection, and understanding how to integrate ZTNA (Zero Trust Network Access) principles into security operations.
Topic 3	- Analytics: This section of the exam measures the skills of Security Analysts and covers the foundational techniques for building and refining queries. It focuses on creating searches from events, applying grouping and aggregation methods, and performing various lookup operations, including CMDB and nested queries to effectively analyze and correlate data.
Topic 4	- Incidents, notifications, and remediation: This section of the exam measures the skills of Incident Responders and encompasses the entire incident management lifecycle. This includes the skills required to manage and prioritize security incidents, configure policies for alert notifications, and set up automated remediation actions to contain and resolve threats.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q18-Q23):

NEW QUESTION # 18
Refer to the exhibit.

Event Attribute



Filter By: Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
	Raw Event Log	=	udp		AND	

Time Range: Relative

Last 2 Hours

Trend Interval: Auto

Result Limit: 100 K rows

A FortiSIEM device is receiving syslog events from a FortiGate firewall. The FortiSIEM analyst is trying to search the raw event logs for the last two hours that contain the keyword "udp". However, they are getting no results from the search, which they know should be available. Based on the filter shown in the exhibit, why are there no search results?

- A. The keyword is case sensitive. Instead of typing udp in the Value field, the analyst should type UDP.
- B. The Time Range value should be set to Real-Time.
- C. The analyst selected AND in the Next column. This is the wrong Boolean operator.
- D. The analyst selected = in the Operator column. That is the wrong operator.

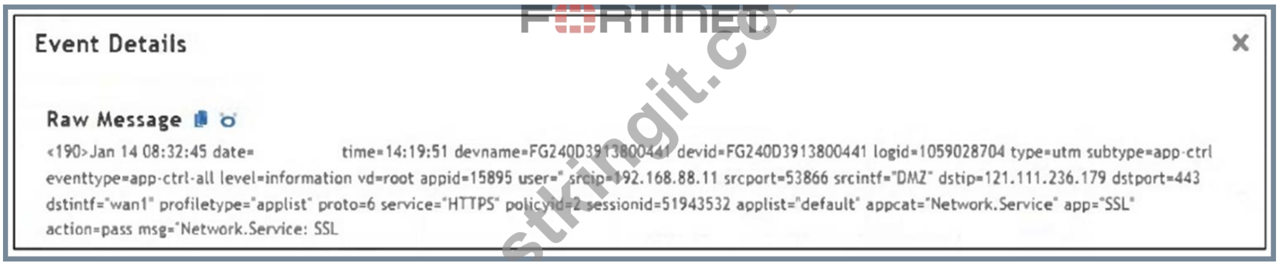
Answer: D

Explanation:
The operator is set to "=", which performs an exact match on the entire raw event log, not a substring search. To find logs that

contain the keyword "udp", the analyst should use the CONTAIN operator instead. This will return all logs where "udp" appears anywhere in the raw log message.

NEW QUESTION # 19

Refer to the exhibit.



```
<190>Jan 14 08:32:45 date=          time=14:19:51 devname=FG240D3913800441 devid=FG240D3913800441 logid=1059028704 type=utm subtype=app-ctrl
eventtype=app-ctrl-all level=information vd=root appid=15895 user=" srcip=192.168.88.11 srcport=53866 srcintf="DMZ" dstip=121.111.236.179 dstport=443
dstintf="wan1" profiletype="applist" proto=6 service="HTTPS" policyid=2 sessionid=51943532 applist="default" appcat="Network.Service" app="SSL"
action=pass msg="Network.Service: SSL
```

Which value would you expect the FortiSIEM parser to use to populate the Application Name field?

- A. SSL
- B. wan1
- C. applist
- D. Network.Service

Answer: A

Explanation:

The Application Name field in FortiSIEM is typically populated using the value of the app field in the raw log. In this event, app="SSL", so "SSL" is the expected application name parsed by FortiSIEM.

NEW QUESTION # 20

What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?

- A. SNMP
- B. FortiSIEM agent
- C. FortiSIEM worker
- D. SSH

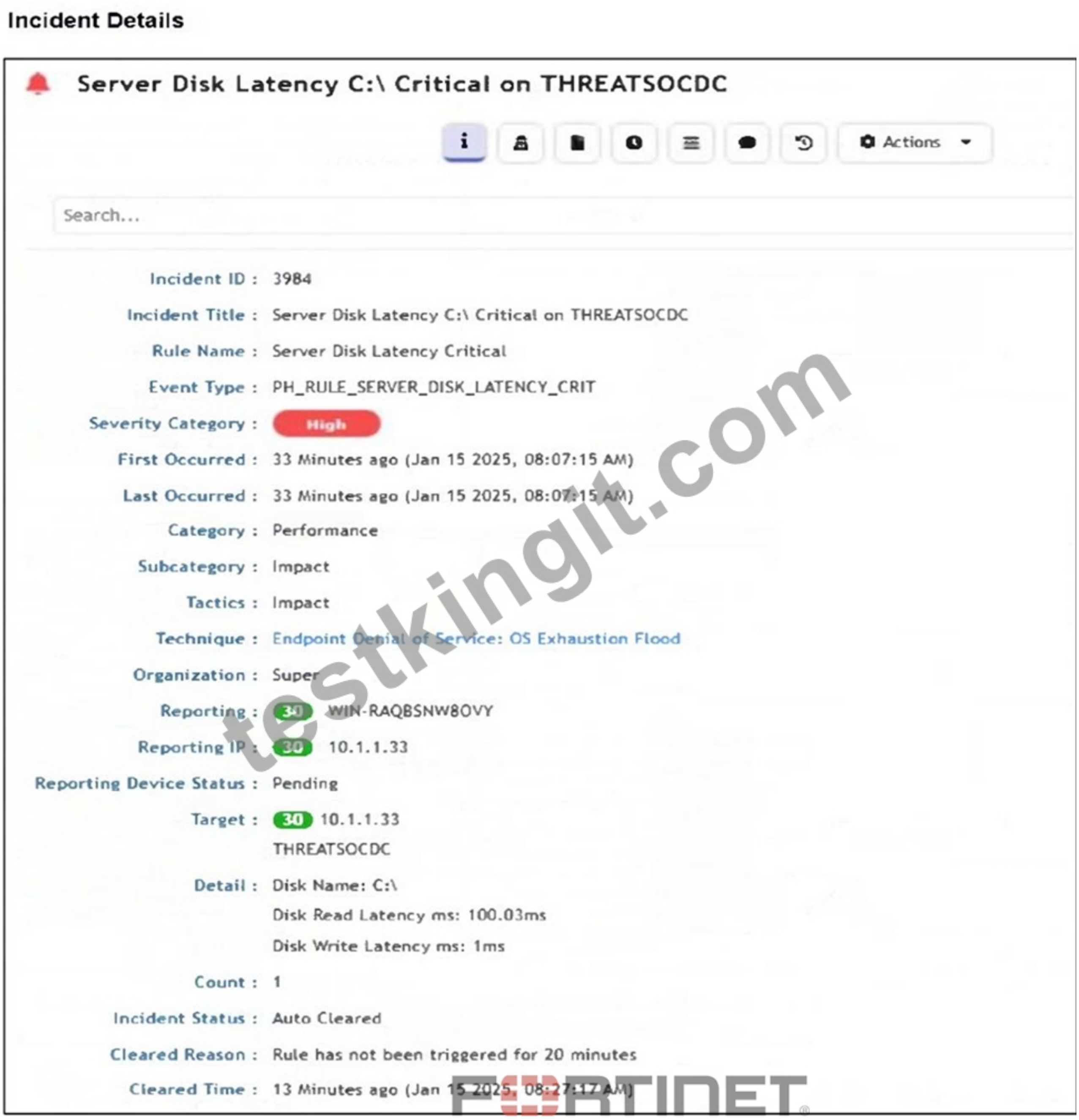
Answer: B

Explanation:

The FortiSIEM agent can be used to send detailed endpoint data such as user activity and process behavior to FortiSIEM, which is essential for performing User and Entity Behavior Analytics (UEBA).

NEW QUESTION # 21

Refer to the exhibit.



Incident Details

Server Disk Latency C:\ Critical on THREATSOCDC

Incident ID : 3984

Incident Title : Server Disk Latency C:\ Critical on THREATSOCDC

Rule Name : Server Disk Latency Critical

Event Type : PH_RULE_SERVER_DISK_LATENCY_CRIT

Severity Category : High

First Occurred : 33 Minutes ago (Jan 15 2025, 08:07:15 AM)

Last Occurred : 33 Minutes ago (Jan 15 2025, 08:07:15 AM)

Category : Performance

Subcategory : Impact

Tactics : Impact

Technique : Endpoint Denial of Service: OS Exhaustion Flood

Organization : Super

Reporting : 30 WIN-RAQBSNW8OVY

Reporting IP : 30 10.1.1.33

Reporting Device Status : Pending

Target : 30 10.1.1.33
THREATSOCDC

Detail : Disk Name: C:\
Disk Read Latency ms: 100.03ms
Disk Write Latency ms: 1ms

Count : 1

Incident Status : Auto Cleared

Cleared Reason : Rule has not been triggered for 20 minutes

Cleared Time : 13 Minutes ago (Jan 15 2025, 08:27:17 AM)

How was this incident cleared?

- A. The endpoint was rebooted and sent an all-clear signal to FortiSIEM.
- B. The analyst manually cleared the incident from the incident table.
- C. FortiSIEM cleared the incident automatically after 24 hours.
- D. The incident was cleared automatically by the rule.

Answer: D

Explanation:
The Incident Status shows "Auto Cleared", and the Cleared Reason states: "Rule has not been triggered for 20 minutes." This indicates that the incident was automatically cleared by the rule logic after a defined period of inactivity.

NEW QUESTION # 22
Which two settings must you configure to allow FortiSIEM to apply tags to devices in FortiClient EMS? (Choose two.)

- A. ZTNA tags defined on FortiSIEM
- B. FortiEMS API credentials defined on FortiSIEM
- C. Remediation script configured

- D. FortiSIEM API credentials defined on FortiEMS\

Answer: B,D

Explanation:
To allow FortiSIEM to apply tags to devices in FortiClient EMS, FortiEMS API credentials must be defined on FortiSIEM to enable communication with EMS, and FortiSIEM API credentials must be defined on FortiEMS to allow EMS to accept tagging instructions from FortiSIEM. This bidirectional API trust is essential for tag application.

NEW QUESTION # 23
......

There are three different versions of our FCP_FSM_AN-7.2 preparation prep including PDF, App and PC version. Each version has the suitable place and device for customers to learn anytime, anywhere. In order to give you a basic understanding of our various versions on our FCP_FSM_AN-7.2 Exam Questions, each version offers a free trial. So there are three free demos of our FCP_FSM_AN-7.2 exam materials. And you can easily download the demos on our website.

FCP_FSM_AN-7.2 Exam: https://www.testkingit.com/Fortinet/latest-FCP_FSM_AN-7.2-exam-dumps.html

- The Best FCP_FSM_AN-7.2 Exam Quiz and First-Grade FCP_FSM_AN-7.2 Exam - Trusted FCP - FortiSIEM 7.2 Analyst Free Dump Download □ Immediately open 【 www.examcollectionpass.com 】 and search for ▸ FCP_FSM_AN-7.2 ◂ to obtain a free download □Examcollection FCP_FSM_AN-7.2 Vce
- Exam FCP_FSM_AN-7.2 Pass Guide □ Dumps FCP_FSM_AN-7.2 Guide □ Exam FCP_FSM_AN-7.2 Pass Guide □ Easily obtain ✔ FCP_FSM_AN-7.2 □✔□ for free download through □ www.pdfvce.com □ □FCP_FSM_AN-7.2 Lab Questions
- Beneficial Fortinet FCP_FSM_AN-7.2 Dumps to Achieve Your Activity [2026] □ Immediately open ➥ www.exam4labs.com □ and search for ➤ FCP_FSM_AN-7.2 □ to obtain a free download □Exam FCP_FSM_AN-7.2 Pass Guide
- Beneficial Fortinet FCP_FSM_AN-7.2 Dumps to Achieve Your Activity [2026] □ Immediately open ➽ www.pdfvce.com □ and search for 「 FCP_FSM_AN-7.2 」 to obtain a free download □FCP_FSM_AN-7.2 Valid Study Materials
- Quiz Authoritative Fortinet - FCP_FSM_AN-7.2 Exam Quiz □ Easily obtain free download of 【 FCP_FSM_AN-7.2 】 by searching on 「 www.exam4labs.com 」 □Cert FCP_FSM_AN-7.2 Exam
- FCP_FSM_AN-7.2 Flexible Learning Mode □ FCP_FSM_AN-7.2 Flexible Learning Mode □ Test FCP_FSM_AN-7.2 Tutorials □ Copy URL ▹ www.pdfvce.com ◃ open and search for □ FCP_FSM_AN-7.2 □ to download for free □ □Exam FCP_FSM_AN-7.2 Price
- FCP_FSM_AN-7.2 Test Quiz □ FCP_FSM_AN-7.2 New Exam Camp ✌ FCP_FSM_AN-7.2 Lab Questions □ Open website ➽ www.practicevce.com □ and search for 《 FCP_FSM_AN-7.2 》 for free download □Exam FCP_FSM_AN-7.2 Tutorials
- Passing FCP_FSM_AN-7.2 Score Feedback □ FCP_FSM_AN-7.2 Lab Questions □ Exam FCP_FSM_AN-7.2 Price □ ✔ www.pdfvce.com □✔□ is best website to obtain ➽ FCP_FSM_AN-7.2 □ for free download □ □FCP_FSM_AN-7.2 Valid Study Materials
- Exam FCP_FSM_AN-7.2 Price □ Pass Leader FCP_FSM_AN-7.2 Dumps □ FCP_FSM_AN-7.2 Exam Course □ Search for ➥ FCP_FSM_AN-7.2 □ and obtain a free download on [www.easy4engine.com] □FCP_FSM_AN-7.2 Valid Study Materials
- Pass Guaranteed Quiz 2026 FCP_FSM_AN-7.2: Unparalleled FCP - FortiSIEM 7.2 Analyst Exam Quiz □ The page for free download of ➡ FCP_FSM_AN-7.2 □□□ on □ www.pdfvce.com □ will open immediately □Examcollection FCP_FSM_AN-7.2 Vce
- Exam FCP_FSM_AN-7.2 Tutorials ✍ Exam FCP_FSM_AN-7.2 Pass Guide □ Exam FCP_FSM_AN-7.2 Vce Format □ Search for { FCP_FSM_AN-7.2 } and download it for free on ▹ www.troytecdumps.com ◃ website □ □FCP_FSM_AN-7.2 Certification Exam
- motionenergy.com.tw, sincerequranicinstitute.com, onlyfans.com, www.stes.tyc.edu.tw, naatiwiththushara.com, www.stes.tyc.edu.tw, daotao.wisebusiness.edu.vn, www.stes.tyc.edu.tw, 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, dist-edu.acharya-iit.ac.in, Disposable vapes

2025 Latest TestKingIT FCP_FSM_AN-7.2 PDF Dumps and FCP_FSM_AN-7.2 Exam Engine Free Share: https://drive.google.com/open?id=12f3rU6DT31OHjh6d4H7clGaNH4KeHv0i