Fortinet

FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

Latest Version: 6.0

Question: 1

When narrowing down suspicious outbound traffic, which two filters are typically most helpful? (Choose two.)

A. Destination country
B. Action (blocked/allowed)
C. Firmware version
D. Disk usage

Answer: A,B

Question: 2

How does FortiAnalyzer standardize log fields coming from different Security Fabric devices so that threat data can be categorized consistently?

A. By enabling Threat Intelligence Manager
B. By relying on Automatic Taxonomy Mapping
C. By running the Fabric Ratings Engine
D. By using Fabric log normalization and the SIEM database (siemdb)

Answer: D

Question: 3

Which two types of log conditions can be used to trigger an event handler? (Choose two.)

A. Severity level
B. Traffic shaping policy
C. Subtype (e.g. virus, webfilter)
D. Interface duplex mode

Answer: A,C

Question: 4

In the Log Browser, which field indicates the device that generated the log?

A. devid
B. devname
C. vd
D. subtype

Answer: B

Question: 5

Which two fields are commonly added during log normalization on FortiAnalyzer?
(Choose two.)

A. Source country
B. FortiGuard rating
C. Normalized action
D. Normalized application name

Answer: C,D

Question: 6

Where can an analyst preview a report layout before generating it?

A. Dataset Editor
B. Chart Widget Library
C. Report Designer
D. FortiView

Answer: C

Question: 7

Which two log types are most useful when investigating malware infections reported by a FortiGate?
(Choose two.)

A. System event logs
B. Web Filter logs
C. Admin logs
D. Antivirus logs

Answer: B,D

Question: 8

What is the primary benefit of integrating FortiAnalyzer into the Security Fabric?

A. Automated licensing for all Fabric devices
B. Unified log analytics and incident correlation
C. Automatic deployment of FortiGate policies
D. Real-time HA failover across the entire Fabric

Answer: B

Question: 9

Which two log filters are best suited to investigate a suspected brute-force login attack?
(Choose two.)

A. Application = “HTTPS.BROWSER”
B. Source IP = suspected attacker IP
C. Log type = event, subtype = system
D. Time range = last 30 days

Answer: B,C

Question: 10

Where can analysts view detailed logs that contributed to a specific incident?

A. Incident → Logs tab
B. Report Browser
C. Playbook Center
D. Fabric View

Answer: A

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer