

Exam : FCSS_SOC_AN-7.4

**Title : FCSS - Security Operations
7.4 Analyst**

Version : DEMO

1.Which connector on FortiAnalyzer is responsible for looking up indicators to get threat intelligence?

- A. The FortiGuard connector
- B. The FortiOS connector
- C. The FortiClient EMS connector
- D. The local connector

Answer: A

2.In the context of SOC operations, mapping adversary behaviors to MITRE ATT&CK techniques primarily helps in:

- A. Speeding up system recovery
- B. Predicting future attacks
- C. Understanding the attack lifecycle
- D. Facilitating regulatory compliance

Answer: C

3.You are managing 10 FortiAnalyzer devices in a FortiAnalyzer Fabric. In this scenario, what is a benefit of configuring a Fabric group?

- A. You can apply separate data storage policies per group.
- B. You can aggregate and compress logging data for the devices in the group.
- C. You can filter log search results based on the group.
- D. You can configure separate logging rates per group.

Answer: C

4.In managing events and incidents, which factors should a SOC analyst focus on to improve response times?

(Choose Three)

- A. Speed of alert generation
- B. Accuracy of event correlation
- C. Time spent in meetings
- D. Clarity of communication channels
- E. Efficiency of data entry processes

Answer: ABD

5.When designing a FortiAnalyzer Fabric deployment, what is a critical consideration for ensuring high availability?

- A. Configuring single sign-on
- B. Designing redundant network paths
- C. Regular firmware updates
- D. Implementing a minimalistic user interface

Answer: B