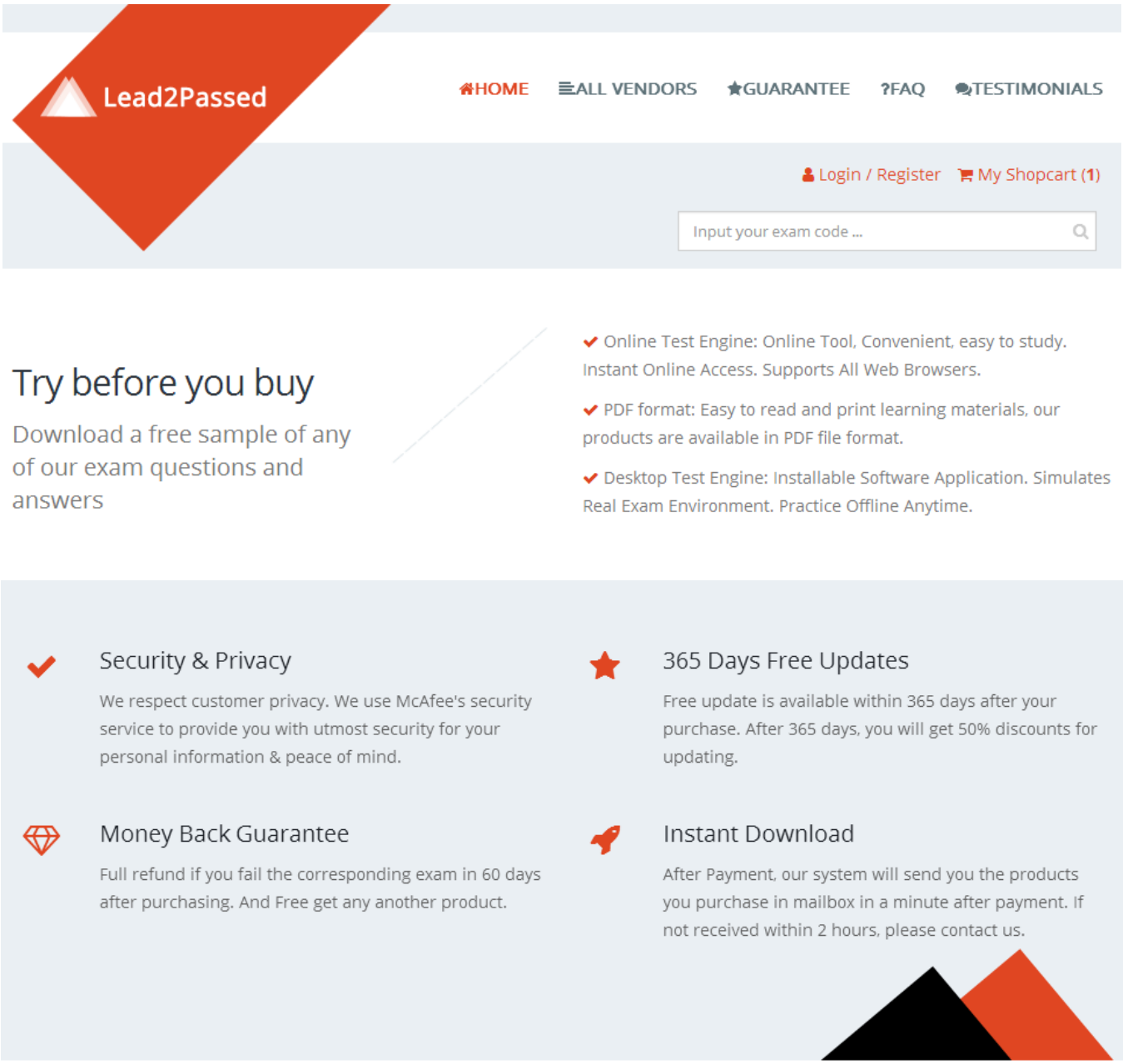
Lead2Passed



http://www.lead2passed.com

Valid Certification Exam Dumps Materials and Study Guide - Lead2Passed

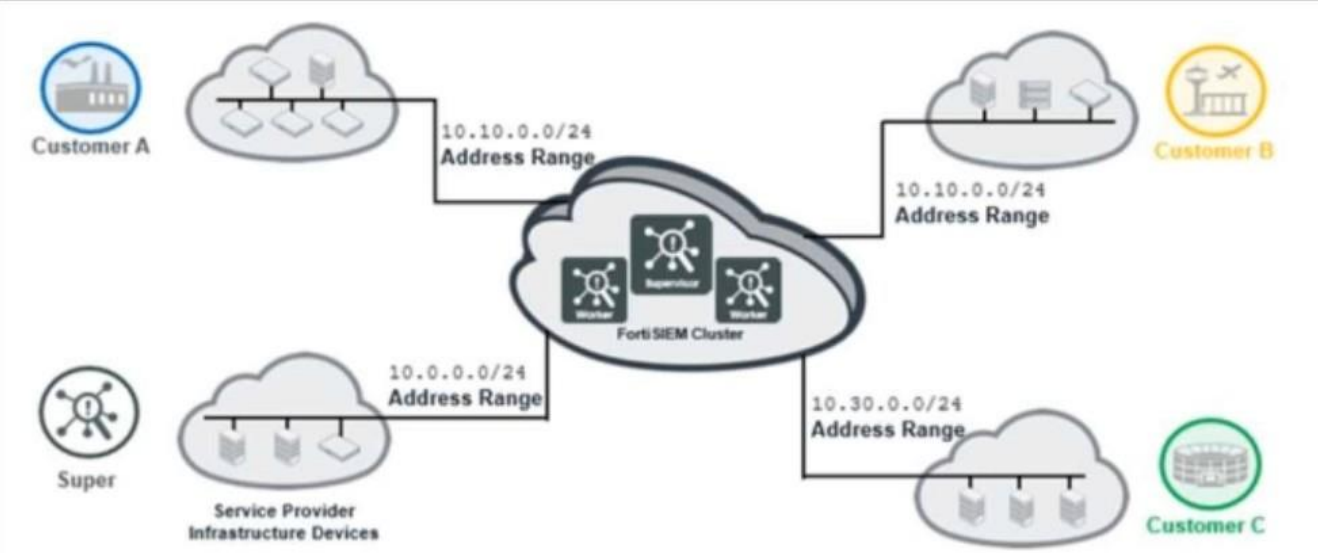
Exam : **FCSS_ADA_AR-6.7**

Title : FCSS—Advanced Analytics 6.7 Architect

Vendor : Fortinet

Version : DEMO

NO.1 Refer to the exhibit.



The service provider deployed FortiSIEM without a collector and added three customers on the supervisor.
What mistake did the administrator make?

A. The number of workers on the FortiSIEM cluster must match the number of customers added

B. Collectors must be deployed on all customer premises before they are added to organization on the supervisor.

C. At least one collector must be deployed to collect logs from service provider infrastructure devices.

D. Customer A and customer B have overlapping IP addresses.

Answer: C

Explanation:
The administrator deployed FortiSIEM without a collector, meaning there is no dedicated system collecting logs from service provider infrastructure devices. Without a collector, the FortiSIEM supervisor and workers must directly ingest logs, which is not ideal for a multi-tenant service provider setup. A collector is necessary to efficiently gather logs before forwarding them to the FortiSIEM cluster.

NO.2 Which three processes are collector processes? (Choose three.)

A. phParser

B. phAgentManager

C. phMonitorAgent

D. phReportMaster

E. phRuleMaster

Answer: A,B,C

Explanation:
These three processes are essential for a FortiSIEM collector, as they handle event parsing, agent communication, and system monitoring.
*phParser is responsible for parsing and processing collected logs before forwarding them.
*phAgentManager manages agent communication, ensuring logs are received and forwarded correctly.

*phMonitorAgent monitors the health of the collector itself, reporting system status to the FortiSIEM supervisor.
phReportMaster and phRuleMaster do not run on collectors. They are supervisor/worker processes handling reporting and rule evaluation, respectively.

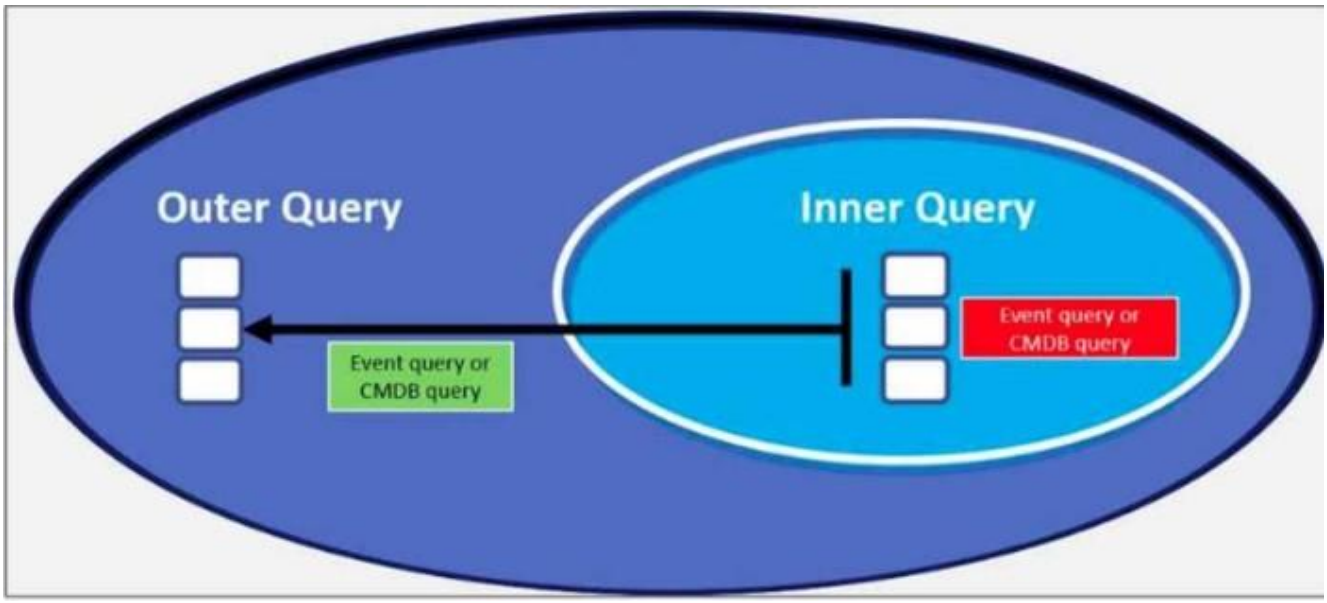
NO.3 Which organization do agents belong to after registration? (Choose two.)
A. The windows agents belong to the super organization.
B. The agents belong to the organization specified in the agent installation setup wizard for Windows platforms.
C. The Linux agents belong to the super local organization.
D. The agents belong to the organization specified in the command line parameters for Linux platforms.
Answer: B,D
Explanation:
When registering agents in FortiSIEM, the organization to which they belong depends on how they are installed:
*Windows Agents
*During installation, the setup wizard prompts the user to specify the organization.
*This ensures the agent is correctly assigned to the organization defined during setup.
*Linux Agents
*Installation on Linux requires command-line parameters, including the organization name.
*This means that the organization is explicitly defined during the installation process.

NO.4 In a customer network that includes a collector, which device performs device discoveries?
A. Agent
B. Supervisor
C. Worker
D. Collector
Answer: B
Explanation:
In a FortiSIEM deployment, device discovery is handled by the Supervisor, even when a Collector is present.
*The Supervisor initiates active scans using protocols such as SNMP, WMI, SSH, and API queries to discover devices in the network.
*Collectors do not perform discovery; they primarily collect and forward logs from designated devices to the Supervisor.
*Workers handle event processing, not discovery.

NO.5 What are the modes of Data Ingestion on FortiSOAR? (Choose three.)
A. Policy based
B. Rule based
C. App Push
D. Schedule based
E. Notification based

Answer: B,C,D
Explanation:
FortiSOAR supports multiple data ingestion modes to allow efficient data collection and automation. The three primary modes are:
1. Rule-Based
2. App Push
3. Schedule-Based

NO.6 Refer to the exhibit.



Which scenario is not a supported nested query scenario?
A. The outer query is the event query, and the inner query is the event query.
B. The outer query is the event query, and the inner query is the CMDB query.
C. The outer query is the CMDB query, and the inner query is the event query.
D. The outer query is the CMDB query, and the inner query is the CMDB query.
Answer: D
Explanation:
FortiSIEM does not allow CMDB queries to be nested within other CMDB queries. CMDB data is static information, and nesting would not add value or function properly in query execution.