KillTest

質量更高　服務更好



練習題

https://www.killtest.net

一年免費更新服務

Exam : **HP0-A100**

Title : HP ArcSight Security Solutions

Version : DEMO

1.What is the major benefit of ArcSight Logger?
A. Correlation of raw events
B. Long-term storage of events
C. Storage of connectors
D. Real-time threat detection
Answer: D
Explanation:
http://www8.hp.com/us/en/software-solutions/siem-security-information-eventmanagement/(see key benefits and features)

2.What is CIP an acronym for?
A. Collector Intrusion Package
B. Compliance Insight Package
C. Correlation Incursion Package
D. Component Instruction Package
Answer: B
Explanation: http://www.flashcardmachine.com/arcsight-esm.html

3
What is the primary feature of Connector Appliance?
A. Aggregates events to reduce the quantity sent to the manager
B. Long-term storage of data
C. Used to develop the Network Model
D. Supports bulk operations on all SmartConnectors
Answer: D

4.The ArcSight ESM collects, normalizes, aggregates, and filters millions of what?
A. Intrusions
B. Transactions
C. Packets
D. Log events
Answer: D
Explanation:
http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-government/sbaGov_arcsightDguide.pdf

5.Which Arc Sight solution delivers Arc Sight content to add specific compliance or standard requirements such as PCI and Sarbanes-Oxley (SOX)?
A. Compliance Insight Package
B. ArcSightResource Collector
C. ArcSightUpdate Package
D. ArcSightPackage Bundle
Answer: A
Explanation:

http://www8.hp.com/us/en/softwaresolutions/software.html?compURI=1340221#.VLNR79LF_Ws