HP

Exam HP0-A100

HP ArcSight Security Solutions

Version: 6.0

[Total Questions: 60]

Question No : 1

Which statement is correct?

A. ArcSight Logger event schema is different from the ESM event schema
B. ArcSight Logger receives events from Connectors rather than from raw events
C. ArcSight Logger cannot compress data.
D. ArcSight Logger must be used together with an ArcSight ESM

Answer: B

Question No : 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
Reference: http://www.flashcardmachine.com/arcsight-esm.html

Question No : 3

Whatis the main purpose of the ArcSight ESM?

A. To archive raw event data
B. To correlate events and provide real-time threat detection
C. To centrally manage SmartConnector configuration
D. To manage multiple retention policies

Answer: B
Reference:http://www8.hp.com/us/en/software-solutions/arcsight-esm-enterprise-security-management/index.html

Question No : 4

What isthe main purpose of using IdentityView within an ESM environment?

A. To correlate identity information maintained by the Identity Management System with events generated m the network
B. To model network architecture within the ESM environment to performadvanced correlation on Asset and User events
C. To extract user and asset information from events in a logger environment to perform correlation analysis on them
D. To forward LDAP and active directory events to ESM Server

Answer: B
Reference:http://h10120.www1.hp.com/expertone/datacard/Course/00924200

Question No : 5

Which statementis true about ArcSight IdentityView?

A. It uses the Arc Sight Actor ModelImport Connector to populateandmaintain themodelin sync with your identityManagement System (IDMS)
B. It is one core component ofArcSightESM system without separate licensing.
C. It uses theArcSightNetworkModel Import Connector to populate and maintain the model in syncwith yourIdentity Management System (IDMS)
D. It uses the Arc Sight Asset Model importConnector to populate and maintain the model in sync with your Identity Management System (IDMS)

Answer: D

Question No : 6

Which eventsschema group describesthe sensor that sends eventsthe SmartConnector?

A. Source

B. Agent
C. Device
D. Root

Answer: C

Question No : 7

Which schemagroup contains the timestamp of the event and name of the event?

A. Source Event Schema
B. Category Event Schema
C. Agent Event Schema
D. Root Event Schema

Answer: A

Question No : 8

What is the purpose of the ArcSight ESM?

A. Enables a security bus that allows devices to communicate
B. Enables situational awarenessand visibility of the security risks across an organization
C. Enables security device management using a common browser-based Management Console
D. Enables security integration between disparate devices

Answer: B

Question No : 9

ArcSightIdentityView is utilized by which product?

A. ArcSight Connectors
B. ArcSight Logger
C. ArcSight Connector Appliance
D. ArcSight ESM