HP

Exam HP0-A100

HP ArcSight Security Solutions

Verson: Demo

[Total Questions: 10]

Question No : 1

Whichtype of ESM resources isable to create correlation events?

A. Rules and correlation data monitors
B. Reports
C. Trend tables
D. Active and session lists

Answer: B
Reference:http://www.ndm.net/siem/arcsight/arcsight-esm

Question No : 2

In which phase are functions from the ESM Console (such as NS lookup, Ping, Port info,Trace routeand who is) performed?

A. Workflow
B. Analysis
C. Trending
D. Correlation

Answer: B

Question No : 3

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
Reference:http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/(see key benefits and features)

Question No : 4

Howdoes the ArcSight ESM Manager display statistical views of the dataon your network?

A. Active channels
B. Rules
C. Cases
D. Dashboards

Answer: B
Reference:http://www.splunk.com/web_assets/pdfs/resources/Integrating_Splunk_with_Arcsight.pdf

Question No : 5

Which component performs event aggregation?

A. ESM Database
B. ESM Manager
C. CORR-Engine
D. Smart Connectors

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 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 : 8

In which ESM event schemagroup can the Priority field with a value from 0 to 10 (calculated using ArcSightproprietary Threat Level Formula) be found?

A. Flex
B. Threat
C. Attacker
D. Root

Answer: B

Question No : 9

What are the features that allow you to use Arc Sight Logger throughout your network?

A. Logger has pre-packaged content with forensics on-the-fly capability.
B. Logger allows you to deploy a single solution to manage all log data across your enterprise.
C. Logger uses a pattern matching and anomaly detection system to find very subtle and sophisticated threats.
D. Logger has two deployment options with a detached database.

Answer: A

Reference:https://www.scribd.com/doc/231540875/Arcsight-Complete-Overview

Question No : 10

How does a CIP help an organization? (Select two.)

A. Reduces deployment times of ArcSight components in the organization
B. Contributes to establishing a strong IT governance program and reducing costs
C. Shares, uploads, or downloads connectors within your ArcSight community
D. Helps to meet regulatory compliance requirements
E. Helps to define high availability scenarios for ArcSight components

Answer: B,D