Vendor:HP

Exam Code:HP0-A100

Exam Name:HP ArcSight Security Solutions

Version: Demo

QUESTION 1

Which type of ESM resources is able to create correlation events?

A. Rules and correlation data monitors

B. Reports

C. Trend tables

D. Active and session lists

Correct Answer: B

QUESTION 2

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

A. Flex

B. Threat

C. Attacker

D. Root

Correct Answer: B

QUESTION 3

Which events schema group describes the sensor that sends events the Smart Connector?

A. Source

B. Agent

C. Device

D. Root

Correct Answer: C

QUESTION 4

Which component performs event aggregation?

A. ESM Database

B. ESM Manager

C. CORR-Engine

D. Smart Connectors

Correct Answer: D

QUESTION 5

What is a function of a Connector Appliance?

A. To provide a Smart Connector management facility in logger-only environments

B. To provide a secure web-based console to ESM

C. To profile common attack patterns on the network

D. To perform advanced correlation evaluation

Correct Answer: B

QUESTION 6

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

Correct Answer: D

QUESTION 7

Which feature of Arc Sight Smart Connectors reduces the quantity of events sent to the ESM Manager?

A. Normalization

B. Host name lookup

C. Categorization

D. Aggregation

Correct Answer: D

QUESTION 8

What is a major benefit of using ArcSight ESM?

A. Collecting row data and archive

B. Real time threat detection

C. Detecting software ending flaws

D. Encrypting raw event data

Correct Answer: B

QUESTION 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.

Correct Answer: A

QUESTION 10

What is the major benefit of using ArcSight Connector Appliance?

A. Ability to detect common patterns on your network

B. Ability to configure, monitors, tune, and update Smart Connectors

C. Ability to perform correlation on raw data

D. Long-term storage of data

Correct Answer: C

QUESTION 11

Which task is performed by the manager during the Priority Evaluation and Network Model Lookup phase?

A. Batching

B. Parsing

C. Asset model lookup

D. Raw events processing

Correct Answer: D

QUESTION 12

Which schema group 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

Correct Answer: A