

## Testking.HP0-A100,60.Questions

Number: HP0-A100  
Passing Score: 800  
Time Limit: 120 min  
File Version: 13.05

TESTKING



HP0-A100

HP ArcSight Security Solutions

- ★ I have uploaded new file in which i have corrected all wrong answers .
- ★ I have updated the vce with new answers from forum and pdf.
- ★ This VCE is valid n awesome, I passed Today,971/1000
- ★ I have solved " Stream read error " problem in VCE player .
- ★ Modified few questions, fixed few spelling mistakes and typos.

**Exam A****QUESTION 1**

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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: [http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-government/sbaGov\\_arcsightDguide.pdf](http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-government/sbaGov_arcsightDguide.pdf) (See the page #04 line #05).

**QUESTION 2**

How many ESM event schema groups are there?

- A. 5
- B. 17
- C. 300
- D. 400

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 3**

Which ESM component does the Event Priority Evaluation and Asset Model look up?

- A. ESM console
- B. CORR engine
- C. Smart Connectors
- D. ESM manager

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 4**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 5**

What are three resources used in the Correlation phase of the event lifecycle?

- A. Rules, active channels, trends
- B. Dashboards, queries, filters
- C. Query viewers, active channels, data monitors
- D. Filters, rules, data monitors

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://www.triadsquare.com/training-programs/security-information-and-event-management-siem/arcsight/aesa-esm-security-analyst> (See the Learning Objectives Point #04).

#### **QUESTION 6**

Which event schema group describes the Smart Connector that reported the event to the manager?

- A. Root
- B. Agent
- C. Source
- D. Device

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-government/sbaGov\\_arcsightDguide.pdf](http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-government/sbaGov_arcsightDguide.pdf)

#### **QUESTION 7**

What is a purpose of Smart Connectors?

- A. To parse raw data
- B. To calculate priority value
- C. To generate reports
- D. To perform correlation

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 8**

How does the ArcSight ESM Manager display statistical views of the data on your network?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www.splunk.com/web\\_assets/pdfs/resources/Integrating\\_Splunk\\_with\\_Arcsight.pdf](http://www.splunk.com/web_assets/pdfs/resources/Integrating_Splunk_with_Arcsight.pdf)

**QUESTION 9**

Which database management system technology is utilized by the Arc Sight ESM 6.5c?

- A. DB2
- B. CORR-Engine
- C. SQL Server Express Edition
- D. Oracle 10g

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.linkedin.com/pub/roger-linnenburger/65/179/a3b>

**QUESTION 10**

What does Arc Sight Identity View integrate?

- A. Flex Connectors
- B. Out-of-the-box leading IAM technologies
- C. Industry Standard Database connectivity via JDBC
- D. Smart Connectors

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://www.ndm.net/siem/arc sight/arc sight-identityview>

**QUESTION 11**

What is an example of a CIP package used for compliance?

- A. DOD
- B. NSA
- C. PCI
- D. MOD

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

answer is valid.

#### **QUESTION 12**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www.metanetivs.com/wp-content/uploads/2013/03/METANET\\_BOOKLET\\_FOR\\_SCREEN.pdf](http://www.metanetivs.com/wp-content/uploads/2013/03/METANET_BOOKLET_FOR_SCREEN.pdf)

#### **QUESTION 13**

What is 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 Smart Connector configuration
- D. To manage multiple retention policies

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### **QUESTION 14**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 15**

Which security product features are offered in ArcSight Express? (Select two)

- A. SRL authentication support
- B. Connector management
- C. First I tool Wizard
- D. Support for FIPS
- E. Connector appliance functionality

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 16**

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

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 17**

The normalization process occurs at which event lifecycle phase?

- A. Reporting and incident analysis
- B. Monitoring and investigation
- C. Priority evaluation and network model lookup
- D. Data collection and event processing

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 18**

Which event lifecycle phase discovers the relationships between events, infers the significance of those relationships, prioritizes them, and provides a framework to take action?

- A. Correlation evaluation
- B. Priority evaluation and network model lookup
- C. Workflow
- D. Data collection and event processing

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 19**

Which statement describes a CIP?

- A. A collection of packages to interface ArcSight products with ticket management systems

- B. A suite of ArcSight resources focusing on system performance issues
- C. A product that scales easily to manage extreme machine data across IT
- D. A collection of ArcSight resources to monitor IT assets, based on regulatory requirements

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://www8.hp.com/h20195/v2/GetPDF.aspx%2F4AA4-4850ENW.pdf> (page 1, ease the compliance burden)

#### **QUESTION 20**

What is the output of the Data Collection and Event Processing phase?

- A. Correlation events
- B. Base events
- C. Filtered events
- D. Raw events

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 21**

Which appliance provides advanced event correlation, event analysis and investigation, options for remediation and even, storage?

- A. ArcSight Connector Appliance
- B. ArcSight Network Configuration Manager/Threat Response Manager
- C. ArcSight Logger Appliance
- D. ArcSight Express

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 22**

What is the purpose of the ArcSight ESM?

- A. Enables a security bus that allows devices to communicate
- B. Enables situational awareness and 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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 23**

Which resource used in the Workflow phase in the event lifecycle, .tracks either individual events or multiple related events?

- A. Reports
- B. Stages
- C. Query viewers
- D. Cases

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 24**

What is the extension used to deliver and install CIPs?

- A. aup
- B. cab
- C. cip
- D. arb

**Correct Answer:** A

**Section: (none)**  
**Explanation**

**Explanation/Reference:**

Reference: <http://www.virtuemartrewardpoints.com/documentation/virtuemart-reward-points-vm2-manual>

#### **QUESTION 25**

What is the main purpose of using Identity View within an ESM environment?

- A. To correlate identity information maintained by the Identity Management System with events generated in the network
- B. To model network architecture within the ESM environment to perform advanced 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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <http://h10120.www1.hp.com/expertone/datacard/Course/00924200>

#### **QUESTION 26**

What is the most important reason or benefit for customers to use ArcSight ESM?

- A. Events correlation
- B. Raw data storage
- C. Events aggregation
- D. Central management of connectors

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

answer is up to date.

#### **QUESTION 27**

What is the main purpose of the ArcSight ESM Query Viewer resource?

- A. To view both SQL queries and reports in a dashboard

- B. To view quick, high-level summaries of security events
- C. To get low-level detailed event activities
- D. To view and edit the underlying SQL queries

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference:

[http://www.hpenterprisesecurity.com/collateral/protect2012/HP\\_Protect\\_2012\\_Sessions.pdf](http://www.hpenterprisesecurity.com/collateral/protect2012/HP_Protect_2012_Sessions.pdf)

#### **QUESTION 28**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

REFERENCE:

[http://www.hp.com/hpinfo/newsroom/press\\_kits/2013/HPDiscover2013/Datasheet\\_ArcSight\\_Connectors.pdf](http://www.hp.com/hpinfo/newsroom/press_kits/2013/HPDiscover2013/Datasheet_ArcSight_Connectors.pdf)

#### **QUESTION 29**

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 Arc Sight community
- D. Helps to meet regulatory compliance requirements
- E. Helps to define high availability scenarios for ArcSight components

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 30**

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**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 31**

Which type of ESM resources are imported from an external Identity Management System by using IdentityView?

- A. Actors
- B. Asset Categories
- C. Users
- D. Customers

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://protect724.hp.com/docs/DOC-1803>

**QUESTION 32**

Which component performs event aggregation?

- A. ESM Database
- B. ESM Manager
- C. CORR-Engine

D. Smart Connectors

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 33**

ArcSight IdentityView is utilized by which product?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 35**

The ArcSight ESM uses which component to gather events?

- A. Nodes
- B. Smart Connectors
- C. Collectors
- D. Adapters

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://www8.hp.com/h20195/V2/getpdf.aspx/4AA4-5836ENW.pdf?ver=1.0>

### **QUESTION 36**

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

- A. Source
- B. Agent
- C. Device
- D. Root

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 37**

Which function is performed by the ArcSight ESM Manager?

- A. Aggregates events
- B. Normalizes event data into CEF fields
- C. Receives raw events from devices spread throughout the network
- D. Prioritizes events

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 38**

What is IAM an acronym for?

- A. Intrusion and Access Management
- B. Identity and Access Management
- C. Incident Account Management
- D. Identity Account Management

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www8.hp.com/us/en/software-solutions/software.html?compURI=1340156#.VLT0K9LF\\_Ws](http://www8.hp.com/us/en/software-solutions/software.html?compURI=1340156#.VLT0K9LF_Ws)

**QUESTION 39**

How are CIPs licensed?

- A. CIPs are included as standard in Logger
- B. CIPs are additional, paid for components.
- C. CIPs are included as standard in Connector Appliance
- D. CIPs are included as standard in ESM

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 40**

What is the name of the process that parses raw events and stores them into the corresponding data fields in the ESM event schema?

- A. Batching
- B. Aggregation
- C. Normalization
- D. Filtering

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 41**

What is an ArcSight Logger architecture component?

- A. Oracle Database
- B. Receivers
- C. Pattern Discovery
- D. Correlation Engine

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://www.experis.com/jobs/USA/USCampusPro/en/job/information-technology/guerneville/security-analyst-arcsight-2591314-20150106.html>

**QUESTION 42**

What are functions of a Smart Connector? (Select two)

- A. Collecting data from a source device
- B. Parking and normalizing events
- C. Long-term storage repository for events
- D. Performing correlation evaluation
- E. Discovering day-zero attacks

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://ijecs.in/issue/v3-i4/20%20ijecs.pdf> (See the Page #02).

**QUESTION 43**

What does the ArcSight ESM prioritize?

- A. Every event
- B. Correlated events only
- C. Forwarded events only
- D. Every event exclusive of audit and monitor events

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference:

file:///C:/Users/AbDullah/Downloads/bcs\_sb\_TechPartner\_HP\_ArcSight\_EN\_v1f.pdf

**QUESTION 44**

For its correlation and automated event analysis capabilities, which ESM component is considered the brain of the HP ArcSight SIEM platform?

- A. web server
- B. ESM manager
- C. ESM console
- D. CORR-E database

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 45**

Which component is customer-built?

- A. Nodes
- B. Adapters
- C. Flex Connectors
- D. Collectors

**Correct Answer:** C

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 46**

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

**Section:** (none)

**Explanation****Explanation/Reference:**

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

**QUESTION 47**

What is CIP an acronym for?

- A. Collector Intrusion Package
- B. Compliance Insight Package
- C. Correlation Incursion Package
- D. Component Instruction Package

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:**

Reference: <http://www.flashcardmachine.com/arcsight-esm.html>

**QUESTION 48**

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 Smart Connectors

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

corrected and modified.

#### **QUESTION 49**

The ArcSight ESM collects, normalizes, aggregates, and filters millions of what?

- A. Intrusions
- B. Transactions
- C. Packets
- D. Log events

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-government/sbaGov\\_arcsightDguide.pdf](http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-government/sbaGov_arcsightDguide.pdf)

#### **QUESTION 50**

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. Arc Sight Resource Collector
- C. Arc Sight Update Package
- D. Arc Sight Package Bundle

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www8.hp.com/us/en/software-solutions/software.html?compURI=1340221#.VLNR79LF\\_Ws](http://www8.hp.com/us/en/software-solutions/software.html?compURI=1340221#.VLNR79LF_Ws)

**QUESTION 51**

What is a reporting enhancement in ArcSight Express release 4.0?

- A. Ability to include more than one chart type in a report
- B. Ability to define non ESM users as recipients, and create a report once and distribute it to multiple recipients
- C. Ability to generate reports of list members
- D. Ability to generate reports of trend data

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www.computerlinks.com/fms/23622.hp\\_arcsight\\_express\\_4\\_0.pdf](http://www.computerlinks.com/fms/23622.hp_arcsight_express_4_0.pdf)

**QUESTION 52**

Which component performs the data collection and normalization?

- A. Data monitors
- B. FSM manager
- C. Smart Connectors
- D. Correlation engine

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference:

[http://www.splunk.com/web\\_assets/pdfs/resources/Integrating\\_Splunk\\_with\\_Arcsight.pdf](http://www.splunk.com/web_assets/pdfs/resources/Integrating_Splunk_with_Arcsight.pdf)

**QUESTION 53**

Which statement is true about Arc Sight Identity View?

- A. It uses the Arc Sight Actor Model Import Connector to populate and maintain the model in sync with your identity Management System (IDMS)
- B. It is one core component of ArcSight ESM system without separate licensing.
- C. It uses the Arc Sight Network Model Import Connector to populate and maintain the model in sync with your Identity Management System (IDMS)
- D. It uses the Arc Sight Asset Model import Connector to populate and maintain the model in sync with your Identity Management System (IDMS)

**Correct Answer:** D

**Section: (none)**  
**Explanation**

**Explanation/Reference:**

**QUESTION 54**

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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <http://www.ndm.net/siem/arcsight/arcsight-esm>

**QUESTION 55**

What is a major benefit of using ArcSight ESM?

- A. Collecting raw data and archive
- B. Real time threat detection
- C. Detecting software ending flaws
- D. Encrypting raw event data

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <http://www8.hp.com/us/en/software-solutions/arcsight-esm-enterprise-security-management/>

**QUESTION 56**

Which statement is correct?

- A. Smart Connectors cannot execute commands.

- B. Smart Connect or installers are operating system independent
- C. Smart Connectors use the Event Category Model to describe normalized events
- D. Smart Connectors correlate events from raw data.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://h20195.www2.hp.com/V2/getpdf.aspx/4AA5-1975ENW.pdf> (See the Overview 2nd and 3rd paragraph).

#### **QUESTION 57**

In the Workflow phase, what are Annotations?

- A. Annotations are a field in the ESM event schema that enables you to flag events for follow up
- B. Annotations are pointers to an internal or external web page where a user can find more information about vulnerable
- C. Annotations are a monitoring tool used by Security Operation Centers
- D. Annotations are an ESM resource to export event data to third-party products, such as BMC Remedy

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 58**

What is ArcSight Express?

- A. An appliance that builds and maintains a detailed understanding of your network's topology, enabling you to centrally manage your infrastructure
- B. An appliance used for long term log data retention and forensics, with very high throughput
- C. An appliance to host and inline multiple Smart Connectors in a single device
- D. An appliance combining ESM functionality with an easy-to-deploy security monitoring and response system

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/index.html>

**QUESTION 59**

Which HP Enterprise Security Product analyzes and correlates every event that occurs across the organization to deliver accurate prioritization of security risks and compliance violations?

- A. Smart Connector
- B. Connector Appliance
- C. Logger
- D. Enterprise Security Manager

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://www8.hp.com/us/en/software-solutions/asset/software-asset-viewer.html?module=1623263&asset=1356091>

**QUESTION 60**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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