



Vendor: HP

Exam Code: HP0-A100

Exam Name: HP ArcSight Security Solutions

Version: DEMO

QUESTION 1

Which statement is correct?

- A. SmartConnectors cannot execute commands.
- B. Smart Connect or installers are operating system independent
- C. SmartConnectors use the Event Category Model to describe normalized events
- D. SmartConnectors correlate events from raw data.

Answer: C

Explanation:

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

QUESTION 2

In the Workflow phase, what are Annotations?

- A. Annotations are a field in the ESM event schema that enables you to flag events for followup
- 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

Answer: C

QUESTION 3

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 lineage multiple SmartConnectors in a single device
- D. An appliance combining ESM functionality with an easy-to-deploy security monitoring and response system

Answer: C

Explanation:

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

QUESTION 4

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. SmartConnector
- B. Connector Appliance
- C. Logger
- D. Enterprise Security Manager

Answer: D

Explanation:

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

QUESTION 5

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 SmartConnector configuration
- D. To manage multiple retention policies

Answer: B

Explanation:

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

QUESTION 6

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

Answer: B

QUESTION 7

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

- A. SRL authenticationsupport
- B. Connector management
- C. First I tool Wizard
- D. Support forFIPS
- E. Connector appliancefunctionality

Answer: BD

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives[®]

10% Discount Coupon Code: BDNT2014