



Vendor: IBM

Exam Code: M2150-662

Exam Name: Security Systems Sales Mastery Test v2

Version: DEMO

QUESTION 1

What key feature can QRadar Log Manager do that the competition cannot?

- A. Detection and monitoring of Layer 7 (Application) traffic using a QFlow appliance.
- B. Upgrade to the full SIEM product through the use of a licence key update.
- C. Correlation of both Flow data and Event logs to alert on threats that others would miss.
- D. Search through event log data similar to "Google Search".

Answer: A

QUESTION 2

A client has IBM Security Desktop across their desktop clients, but not on the corporate endpoints. What is the best solution to propose if they are looking to consolidate vendors on the endpoint?

- A. IBM Security VSP, which will allow for virtualized protection, is the logical next technology.
- B. IBM Tivoli Endpoint Manager will be the natural evolution to extend the life of IBM Security Desktop.
- C. SELM service will enable the client to have appropriate logging without using on-site technology.
- D. Next Generation IPS is the best solution for long-term protection.

Answer: B

QUESTION 3

What lists of key words tell you a prospect is looking to buy a SIEM or Log Manager Product?

- A. Single Sign On (SSO), Application Scanning, Mobile Device Management.
- B. RSA , ArcSight, Splunk, Nitro, Log Logic.
- C. Data encryption, Virus Protection, Private data protection.
- D. Stop hackers, Block Denial Of Service (DOS) attacks, Scan for Vulnerabilities.

Answer: D

QUESTION 4

Why does the integration of network flow capture with behavioral analysis and anomaly detection provide greater security intelligence?

- A. Traffic profiling adds protection from zero-day threats.
- B. Correlation of threat data, flow data and system and application vulnerabilities enhances incident analysis.
- C. Network anomaly detection profiles user and system behavior and improves advanced threat protection.
- D. All of the above.

Answer: D

Explanation:

<http://www.slideshare.net/IBMDK/2012-q3-advanced-threat-protection-and-security-intelligence-ibm-smarter-business-copenhagen>
(slide 15, see 3rd bullet and sub-bullets)

QUESTION 5

You're involved in a highly competitive Enterprise Single Sign-On sale and the main competition is Oracle (with v-GO underpinning their solution). They have spread the word that TAM E-SSO requires a server and that they have a superior design because their solution is all client code. How would you respond?

- A. v-GO doesn't work very well, with a lot of customer complaints about it.
- B. v-GO is an appliance and therefore is not very flexible, in terms of meeting customers' specific needs.
- C. As a client-server solution, TAM E-SSO scales better than v-GO, v-GO requires an Active Directory (AD) Schema extension and they load down the AD infrastructure.
- D. V-GO hasn't been certified by DARPA and TAM E-SSO has.

Answer: C

QUESTION 6

Why does the X-Force research team analyze every vulnerability, providing valuable input into IBM's services and technologies?

- A. To prove it has the best global R&D Security organization.
- B. To monitor the threat landscape, determining new attack vectors, and offering a higher level of protection.
- C. To understand the evolving threats and publishing the X-Force updates.
- D. To provide a subscription service to keep clients abreast of new threats.

Answer: B

Explanation:

ftp://public.dhe.ibm.com/software/uk/itsolutions/soa-connectivity/Securing_the_Enterprise.pdf
(slide 8, second bulleted point)

Thank You for Trying Our Product

Lead2pass 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.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives®

10% Discount Coupon Code: ASTR14