ISLEVER

M2150-662

IBM Security Systems Sales Mastery Test v2

DEMO

https://www.islever.com/m2150-662.html
https://www.islever.com/ibm.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

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
Explanation: * IBM Security QRadar Log Manager is a high-performance system for collecting, analyzing, archiving and storing large volumes of network and security event logs. It analyzes data from network and security devices, servers and operating systems, applications, endpoints and more to provide near real-time visibility into developing threats. IBM Security QRadar Log Manager can also help you meet compliance monitoring and reporting requirements.

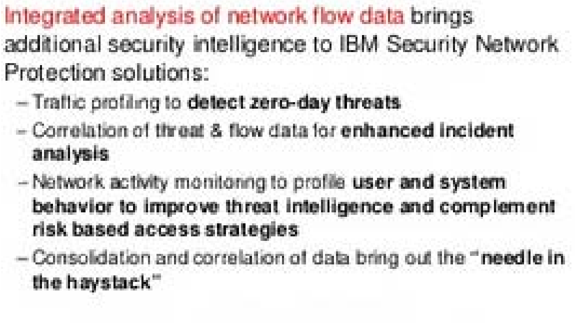
Incorrect:
Not A: not related to signing on.
Not B, not C: not related to data encryption.

QUESTION NO: 2

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:



Integrated analysis of network flow data brings additional security intelligence to IBM Security Network Protection solutions:

- Traffic profiling to **detect zero-day threats**
- Correlation of threat & flow data for **enhanced incident analysis**
- Network activity monitoring to profile **user and system behavior to improve threat intelligence and complement risk based access strategies**
- Consolidation and correlation of data bring out the "**needle in the haystack**"

Reference: 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 NO: 3

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
Explanation:

Note:
* The IBM Tivoli Access Manager for Enterprise Single Sign-On (TAM E-SSO) empowers enterprises to automate access to corporate information, strengthen security, and enforce compliance at the enterprise endpoints. With TAM E-SSO, enterprises can efficiently manage business risks, achieve regulatory compliance, decrease IT costs, and increase user efficiency.

* V-Go SSO works with many directories, including Novell's eDirectory, Sun's Java System Directory, LDAPv2- or LDAPv3-compliant servers, and many databases, including IBM DB2,

Microsoft SQL Server and Oracle.

QUESTION NO: 4

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: Additional to its own research, X-Force reviews each published vulnerability in order to monitor the threat landscape, determining new attack vectors, and
offering a higher level of protection.

Reference; Securing the Enterprise Achieving Security and business compliance with IBM

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

QUESTION NO: 5

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

Explanation: * IBM Security QRadar VFlow Collector: Combines with IBM Security QRadar SIEM