IBM

Exam M2150-662

Security Systems Sales Mastery Test v2

Version: 7.1

[Total Questions: 72]

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

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 to provide Layer 7 application-layer visibility into virtual network traffic, helping you understand and respond to activities in your network. This combined solution gives you greater visibility into network activity to better detect threats, meet policy and regulatory compliance requirements, and minimize risks to mission-critical services, data and assets.

* The QRadar QFlow Collector solution, paired with QRadar flow processors, provides this application layer (Layer 7) visibility, as well as classification of stateful applications and protocols such as voice over IP (VoIP), multimedia, enterprise resource planning (ERP), database, and hundreds of other protocols and applications. Application-aware flow data is obtained from a deep examination and inspection of every packet, which also allows for advanced threat detection through analysis of packet payload content. Correlating this flow information with network and security events, vulnerabilities, identity information and threat intelligence is the optimal way to obtain a complete and accurate view of an organization’s security posture.

Reference; IBM Security QRadar QFlow Collector appliances for security intelligence

Question No : 6

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

Explanation: IBM Endpoint Manager for Security and Compliance helps support endpoint security throughout your organization. Built on IBM Bigfix®technology, this software can help you protect endpoints and assure regulators that you are meeting security compliance standards. Now you can reduce the cost and complexity of IT management while enhancing business agility, speed to remediation and accuracy.

Question No : 7

What is the key to the significant time and money efficiencies that Tivoli Identity Manager (TIM) is able to afford customers?

A. Quick install and time to operation.
B. Support for a large number of target environments.
C. Assignment of users to roles and provisioning policies based on roles rather than individual users.
D. Graphical user interface that is far superior to the competition.

Answer: C

Explanation: Tivoli Identity Manager addresses provisioning of enterprise services and components in the following areas:

* Account access management
* Workflow and life cycle automation
* Provisioning policies
* Role-based access control
* Separation of duty capabilities
* Self-regulating user administration
* Customization

Reference: Tivoli Identity Manager, Version 5.1, Provisioning features

Question No : 8

With Tivoli Federated Identity Manager, which of the following customer scenarios is to be addressed?

A. The provisioning of identities to more than one domain or company.
B. Strict management of privileged users' identities to absolutely ensure there is no unauthorized sharing of their identities.
C. Cross-domain single sign-on, whether the requester is an external user or an internal employee.
D. Strong authentication requirements for any configuration.

Answer: C

Explanation: IBM Tivoli Access Manager for e-business

Key features include:

Provide a base for the federation of user identities. For standardized cross-domain authentication (federation), Tivoli Access Manager for e-business customers can upgrade to Tivoli Federated Identity Manager - a modular access control solution for cross-domain single sign-on.

Reference: IBM Tivoli Identity and Access Manager V1.0 and IBM Tivoli Unified Single Sign-On V1.0

Question No : 9

Which of the following IBM Security solutions offers the quickest approaches in terms of demoing, estimating ROI and quick implementation?

A. Tivoli Identity Manager.
B. Tivoli zSecure suite.
C. Tivoli Key Lifecycle Manager.
D. Tivoli Access Manager for Single Sign-On.

Answer: B

Explanation: Reference; Empowering Security and Compliance Management for the z/OS RACF Environment, Using IBM Tivoli Security Management for z/OS

Question No : 10

Your clients have expressed an interest in identity and access management, including comprehensive single sign-on, and have also indicated an interest in ensuring that the solution includes a capability where they are able to measure how they will do when they face future PCI-DSS audits. What IBM security solution is the best match for these clients?

A. Tivoli Identity and Access Assurance.
B. Tivoli Identity and Access Manager.
C. Tivoli Data and Application Security.
D. Tivoli Security Information and Access Manager.

Answer: B

Explanation: An example of what can be handled through Enterprise Single Sign-On Design Guide Using IBM Security Access Manager is:

* Facilitate the management and demonstration of the overall compliance posture with data privacy laws and industry regulations, such as HIPAA and PCI-DSS (Payment Card Industry Data Security Standard).

Reference; Enterprise Single Sign-On Design Guide Using IBM Security Access Manager for Enterprise Single Sign-On 8.2 (page 97, business requirements, 3rd bullet)

Question No : 11

Which of the following is a key benefit & feature of data protection add-on?

A. Out-of-the-box compliance templates to detect credit card numbers, social security numbers, among other sensitive data.
B. Continuous compliance to detect loss of credit card numbers, social security numbers, among other sensitive data.
C. Patch Management to reduce the risk of data loss due to open vulnerabilities.
D. All of the above.

Answer: B

Explanation: * IBM Endpoint Manager for Core Protection Data Protection Add-on
The optional IBM Endpoint Manager for Core Protection Data Protection Add-on can be deployed and managed through the IBM Tivoli Endpoint Manager infrastructure. The module also helps improve data protection capabilities while helping to control operational costs.
IBM Endpoint Manager for Core Protection Data Protection Add-on offers a robust data loss prevention and device control solution that integrates into the anti-virus and anti-malware capabilities provided by the Core Protection solution and can:

/ Secure data (sensitive or not) on devices that leave the business premises
/ Enforce security policies such that users can access sensitive data for their jobs, but not misuse or lose that data
/ Comply with the growing number of data privacy laws that affect the industry or company

Reference: IBM Endpoint Manager for Core Protection Data Protection Add-on

Question No : 12

Which one of the following best describes the business reason why customers purchase Key Lifecycle Manager?

A. They want to simplify management of keys, address regulations and avoid data loss and mismanagement.

B. They want to expire keys so frequently that manual management of the lifecycle of the keys is impractical.
C. They want to increase performance.
D. They want to minimize the number of keys that are used across the enterprise.

Answer: A

Explanation: * IBM Tivoli Key Lifecycle Manager V2.0 provides an automated solution to centralize and strengthen the encryption and key management process throughout the enterprise, helping minimize the risk of data exposure and reduce operational costs.

* IBM Tivoli Key Lifecycle Manager V2.0 helps you:
/ Manage your information risk by providing the capability to manage encryption keys used to secure information, address information integrity, implement encryption key retention policies, and ease data recovery.
/ Manage encryption keys for a wide variety of encryption implementations.
/ Provide a key management facility for transparent encryption, supporting IBM tape drives, IBM storage, and encryption end points, which support the Key Management Interoperability Protocol (KMIP) V1.0 standard.

Reference; IBM Tivoli Key Lifecycle Manager V2.0 delivers new pricing metric

Question No : 13

In a potential TAMeb sale, the client is a large customer and has large numbers of applications and servers involved in their SSO/Web authorization plans. Oracle Access Manager is the main competitor. What might you emphasize as you try to move the customer in your direction?

A. TAMeb scales well, and is much easier to manage, given a relatively small number of TAMeb servers involved, versus many OAM plug-ins to manage.
B. TAMeb scales well and can do software distribution to any and all clients involved in the scope of the SSO engagement.
C. TAMeb both scales well and performs well.
D. TAMeb is on a par with OAM from a scalability point of view but it has a wider number of applications that it supports out of the box.

Answer: A

Explanation: Note: