Vendor: IBM

Exam Code: M2150-662

Exam Name: IBM Security Systems Sales Mastery Test v2

Version: Demo

Question No : 1

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

A. SingleSign 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 ActiveDirectory (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 automateaccess 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 vulnerabilityin 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 visibilityinto 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 thisapplication 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 significanttime 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 onroles 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 - amodular 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 ComplianceManagement 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 aninterest 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 DesignGuide 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 lossdue 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

Whichone 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 frequentlythat 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 yourinformation 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 encryptionimplementations.
/ 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 themain 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:

* Tivoli Access Manager for E-Business (TAMeb)
* Tivoli Access Manager for e-business provides robust, policy-based security to a corporate Web environment. TAMeb provides authentication of users, control of access privileges, auditing, single sign-on, high availability, and logging.
* Tivoli Access Manager for e-business includes support to help large numbers of users participate in convenient, available, and personalized transactions. IBM works with the leading application providers through the 'Ready for Tivoli' program to build out-of-the-box integrations.

Question No : 14

A customer indicates a desire to cover their Web Single Sign-on requirement comprehensively. Your response to them is that withTivoli Access Manager for e-business, we can address _____

A. Web transactions involving access requests coming from the Internet and targeted to the internal network.
B. Web transactions within the internal network.
C. Web transactions involvingInternet-to-internal-network flows and transactions within the internal network.
D. Web transactions, client-server transactions, email transactions and secure FTP transactions.

Answer: A

Explanation: Note:
* Web transactions are not controlled by the organizationproviding the transaction, and they may be initiated in unknown numbers from unknown locations.
Reference; RedBooks Paper, IBM Tivoli Access Manager for e-business

Question No : 15

What are QRadar's key differentiators?

A. There are 2 Differentiators -Ease of use, High Availability.

B. There are 4 Differentiators - Single Sign On, Object oriented database, Application scanning, Identity and access management.
C. There are 3 Differentiators - Most Automation, Most Integration, Most Intelligent.
D. Thereare 5 Differentiators - Data loss prevention, Risk management , High Availability , Deep Packet Inspection, Block attackers.

Answer: C

Explanation: * Automated failover:

QRadar HA supports seamless failover between the primary and the high availability appliance in the event of primary appliance or network failures, and tests for connectivity to all appliances within its distributed deployment, including network devices such as switches and routers to determine when (or if) a failover occurs.

* Fully supported and integrated with all QRadar appliances:

QRadar HA is fully integrated into all QRadar appliances, including all-in-one systems and distributed appliances.

Reference: QRadar SIEM

Question No : 16

Which of the following statements is true about Continuous Compliance?

A. Policy compliance is continuously monitored and enforced at the endpoint; changes are reported immediately.
B. The security team can instantly check on the current state of security and compliance anytime.
C. No high-risk periods, lowertotal cost, continuous improvement.
D. All of the above.

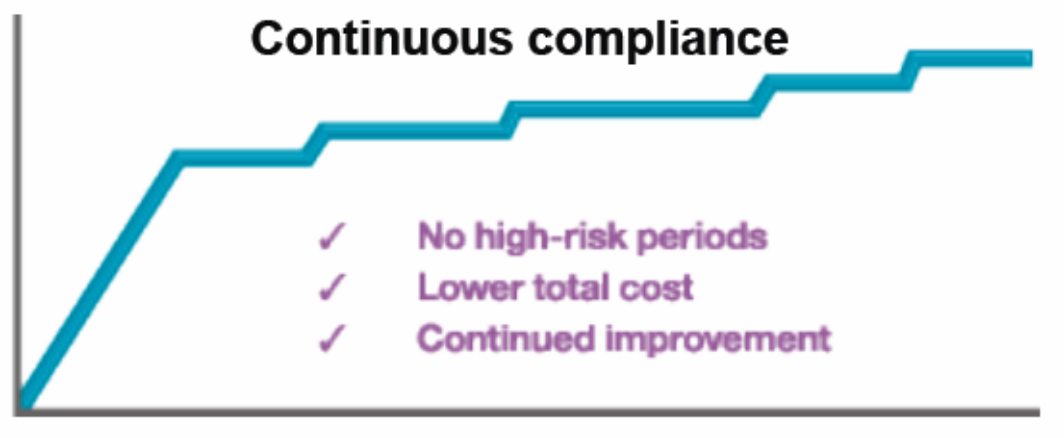
Answer: D

Explanation: IBM Endpoint Manager and “Continuous Compliance”

1. Security and operations work together to formulate policies and service-level agreements (SLAs)
2. Operations implements the baseline(patch, configuration, anti-virus, etc.) across all

endpoints in the organization
3. (A) Policy compliance is continuously monitored and enforced at the endpoint; changes are reported immediately
4. (B) The security team can instantly check on the currentstate of security and compliance anytime
5. Security and operations teams work together to continually strengthen security and adjust to evolving requirements

C:



Reference: IBM Endpoint Manager

Question No : 17

Which of the following statements bestdistinguishes between why customers purchase Access Manager for e-business or Security Policy Manager?

A. Access Manager is for customers who don't need the overhead of security policy; Security Policy Manager is for customers who need to set policy and then measure against that policy for GRC purposes.
B. Access Manager is for small and medium customers and Security Policy Manager addresses large, high-scale implementations.
C. Access Manager is operational ("access") and Security Policy Manager is administrative ("policy").
D. Access Manager addresses coarse-grained access control and Security Policy Manager addresses fine-grained access control.

Answer: D

Explanation: IBM Security Policy Manager can be used in the following ways:
Fine-Grained AuthorizationControl as opposed to coarse grained SAMeB (IBM Security Access Manager for e-Business) group to J2EE Role Mapping (Sample: Policy to restrict a money transfer that exceeds $500 in a single transaction)
Note: * (not C)Tivoli Access Manager for e-business(TAMeb) provides robust, policy-based security to a corporate Web environment. TAMeb provides authentication of users, control of access privileges, auditing, single sign-on, high availability, and logging.

* Tivoli Security Policy Manager
Strengthen access control, facilitate compliance and support operational governance across the enterprise

Centralize security policy management and fine-grained data access control
IBM Tivoli Security Policy Manager centralizes security policy management and fine-grained data access control for applications, databases, portals and services.

/ Automate, manage and enforce data-level access for applications and services
Manage data entitlement and fine-grained access for applications, databases, portals and services
/ Change and control security policies centrally to quickly, consistently and efficiently address compliance requirements
/ Manage security policies and entitlements throughout the policy life cycle, from authoring and publishing to enforcing and updating
/ Enforce policies at run time, strengthening your organization's security posture
/ Use federated policy management to help bridge the gap between business and IT approaches to security policy
/ Supports a broad set of platforms, including IBM AIX, Red Hat Enterprise Linux, Microsoft Windows, and Solaris environments

Reference: Focus on IBM Security: IBM Security Policy Manager and IBM Security Access Manager for e-Business

Question No : 18

Which environments does IBM's full set of single sign-on solutions?

A. Key management, XACML access control rules and patch management.
B. Web, federated and enterprise.
C. Identities, access control, z/OS security administration and data security.
D. Identity and Access Assurance, Security Management for z/OS and Dataand Application Security

Answer: B

Explanation: * IBM Tivoli Federated Identity Manager provides web and federated single sign-on (SSO) to users throughout multiple applications.

* IBM Security Access Manager for Enterprise Single Sign-On allows users to access alltheir applications with a single password. This award-winning solution supports Microsoft Windows, web, Java, Telnet, mainframe, and in-house applications.

Question No : 19

A client has deployed SourceFire IPS appliances but finds it challenging to keep up with the constant flood of signatures. What is the best IBM Security technology differentiator?

A. Protocol Analysis Module in IBM Security host, endpoint, and network solutions.
B. Content Analyzer function in IBM Security IPS appliances.
C. The decryptions function in IBM Security Server Sensor.
D. IBM Security SecurityFusion Module function in IBM Security SiteProtector.

Answer: A

Explanation: The core of the preemptive technology is the protocol analysis module or PAM (Protocol Analysis Module). PAM is byfar the best security differentiator that our threat management products have. PAM offers its significant benefits throughout our threat mitigation solutions . . . it is implemented the same for endpoints, for servers and for gateways. The way PAM is architected, there is the possibility of adding new components as needed so when hacking technology evolves, we can evolve and extend the threat protection capability One of the core differentiators within PAM is that it depends on vulnerability knowledgeand heuristics (proactive/preemptive) . . .

Reference; IBM Proventia Management SiteProtector, SecurityFusion Module Guide

Question No : 20

Which of the following statements is true for Tivoli Endpoint Manager for Security and Compliance?

A. Discover10% - 30% less assets than previously reported.
B. Library of less than 5,000 compliance settings, including support for FDCC SCAP, DISA STIG.
C. Manually and periodically enforce policy at the end point.
D. Achieve 95%+ first-pass success rates within hours of policy or patch deployment.

Answer: D
Reference: Ibm security overview bp enablement 22 feb-2012 v harper

URL: http://www.slideshare.net/ArrowECSMarketing/ibm-security-overview-bp-enablement-22-feb2012-v-harper (slide 23)

Question No : 21

Which of the following solutions is the core solution for addressing customer requirements for simplified administration for z/OS?

A. zSecure Audit.
B. zSecure Admin.
C. zSecure Alert
D. zSecure Command Verifier.

Answer: B
Explanation: zSecure Admin is designed tohelp manage the security administration of RACF with less system resources and administrator time than conventional RACF administration requires. To provide some of these benefits, zSecure Admin enables you to automate recurring and time consuming securitytasks, such as:

Adding or deleting user IDs and groups
Granting access to users and user groups

Setting passwords and resetting revoked user IDs
Determining access of user IDs or groups
Providing both periodic and one-off reports

Reference; IBMz/OS Mainframe Security and Audit Management Using the IBM Security zSecure Suite

Question No : 22

A large industrial client is currently evaluating IPS technology. The important issues are network up time and false positives disrupting the client's business partner connections. What is the most appropriate IBM Security technology for this client?

A. Centralized command and control of IPS through IBM Security SiteProtector.
B. IBM Security MX0804 with the IPS agent actively configured.
C. IBM SecurityGX appliance where simulation mode can be leveraged.
D. IBM Security Server.

Answer: A

Explanation: IBM Security SiteProtector System:
Easily deploy and manage other types of IBM intrusion prevention solutions, including network and host intrusion prevention systems(IPS) and protection for virtual servers.

Reference: IBM Security SiteProtector System:

Question No : 23

You are in a competitive user management/identity management/ user provisioning sale, and the decision seems to hinge on who has the superior role management capabilities. How do you handle this?

A. Expand the discussion to include access management and pull TAMeb into the sale.
B. Expand the discussion to include enterprise audit management and compliance and pull TSIEM into the sale.

C. Bring Tivoli Provisioning Role Manager into the picture.
D. Tout TIM's significant role management capabilities and emphasize the fact that TIM comes with Role and Policy Modeling in the package, whereas competitors charge extra for it.

Answer: D

Explanation:
Note:
* IBM TivoliIdentity Manager V5.1 helps you simplify and reduce cost of administration:
/ Role modeling and mining helps facilitate the quick building of an effective role and access structure from a business centric approach.

* Tivoli Identity Manager also provides:
A dynamic policy management engine that automates user provisioning and aids in compliance efforts.

* IBM Tivoli Identity Manager V5.1 is an automated and policy-based solution that manages user access across IT environments.

* IBM Tivoli Identity Manager, also known as TIM, is an Identity Management System product from IBM.
TIM provides centralized identity lifecycle management. It can automatically create, manage, and delete user access to various system resources such as files, servers, applications, and more based on job roles or requests.

Question No : 24

Pick the TRUE statement.

A. QRadar can detect threats that other systems miss.
B. QRadar can detect insider fraud.
C. QRadar can consolidate big data.
D. All of the above.

Answer: D

Explanation: IBMSecurity Intelligence with Big Data provides exceptional threat and risk detection, combining deep security expertise with analytical insights on a massive scale. For forward-leaning organizations seeking advanced insight into security risks, the IBM

solution – including IBM QRadar Security Intelligence Platform and IBM Big Data Platform – provides a comprehensive, integrated approach that combines real-time correlation for continuous insight, custom analytics across massive structured and unstructured data, and forensic capabilities for irrefutable evidence. The combination can help you address advanced persistent threats, fraud and insider threats.

Question No : 25

For which of the following platforms is advanced management supported for Tivoli EndpointManager for Mobile Device Manager?

A. Android via native BigFix agent.
B. iOS via Apple's MDM APIs.
C. Symbian via native BigFix agent.
D. Both A and B.

Answer: D

Explanation: IBM Endpoint Manager for Mobile Devices allows organizations to manage phones and tablets(both employee-owned and corporate-owned) using the same BigFix platform and infrastructure that manages desktops, laptops, and servers.

Devices can be managed using agent functionality on the device that give a wide-range of management and security functionality. For Android/Windows Mobile, the agent is a BigFix Agent variant (A). For Apple iOS, management is done using Apple's MDM APIs that are natively supported by Apple (B).

Reference: Tivoli Endpoint Manager >Mobile Device Management >Mobile Devices Overview

Question No : 26

When trying to prevent data breaches, which of the following controls must be implemented?

A. Monitor transactions without requiring changes to databases or applications.
B. Compare all transactions to policy and block violations in real-time.
C. Automate and centralize controls to streamline compliance validation.
D. All of the above.

Answer: D

Question No : 27

Which current Analyst report on Database Activity Monitoring places Guardium as the leader?

A. Gartner MagicQuadrant.
B. IDC Curve.
C. ForesterWave.
D. Reuters Report.

Answer: C

Explanation: IBM, Imperva, and Sentrigo lead the pack. These vendors offer strong support for most database auditing features and functionality to meet any enterprise auditing requirements.
IBMInfoSphere Guardium offers support for almost any of the features that one might find in an auditing and real-time protection solution. InfoSphere Guardium offers strong support for database-access auditing, application auditing, policy management, auditing repository, and real-time protection.

Reference: The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011

Question No : 28

Which of the following is a component of Tivoli Endpoint Manager for Core Protection?

A. Patch Management.
B. Web, file, email reputation services.
C. Managed endpoint software inventory.
D. All of the above.

Answer: B

Explanation: * IBM Endpoint Manager for Core Protection:
Works at multiple levels of threat protection including helping to stop threats before they arrive.It checks files, URLs and emails for malicious potential in near real time.

* Protects with methods including le and web reputation, behavior monitoring, personal rewall, data loss prevention and device control

Reference: Data Sheet, IBM Endpoint Manager for Core Protection

Question No : 29

Which attack vector is primarily identified by web application security scanning solutions?

A. Denial of Service (DoS).
B. Pattern-based attacks.
C. SQL Injection
D. Privileged user violations.

Answer: C

Explanation: * TheIBM Security AppScan portfolio includes solutions specifically designed for non-security experts to execute automated test scripts configured by the security team to identify common vulnerabilities, such as SQL injection and cross-site scripting (XSS)

* Aweb application security scanner facilitates the automated review of a web application with the expressed purpose of discovering security vulnerabilities, and are required to comply with various regulatory requirements. Web application scanners can look for a wide variety of vulnerabilities, including:
/ Input/Output validation: (Cross-site scripting, SQL Injection, etc.)
/ Specific application problems
/ Server configuration mistakes/errors/version

* In a copyrighted report published in March 2012 by security vendor Cenzic, the most common application vulnerabilities in recently tested applications include:
Cross Site Scripting, 37%
SQL Injection, 16%
Path Disclosure, 5%

Denial of Service, 5%
Code Execution, 4%
Memory Corruption, 4%
Cross Site RequestForgery, 4%
Information Disclosure, 3%
Arbitrary File, 3%
Local File Include, 2%
Remote File Include, 1%
Overflow 1%
Other, 15%

Reference; IBM Security AppScan, Application security and risk management

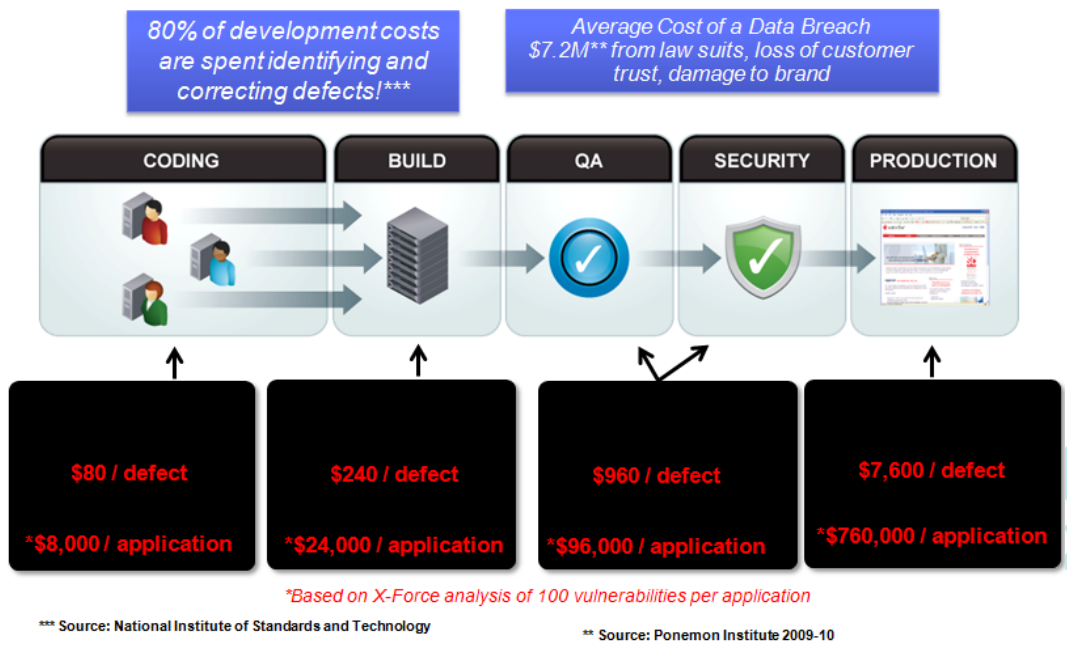
Question No : 30

What is the cost to customers ofremediating a typical number application vulnerabilities if they are identified during application build?

A. $8,000
B. $24,000
C. $96,000
D. $760,000

Answer: B

Explanation:



Reference; Selling the IBM Security, part 2 of 3

Question No : 31

A client with a TippingPoint deployment is concerned about the solution's long-term viability. What products should the sales representative prepare to discuss?

A. IBM Security SiteProtector and IBM Security Network IPS.
B. IBM Security SiteProtector and IBM Security Next Generation IPS.
C. IBM Security SiteProtector and IBM Security Virtual Server Protection.
D. Both A and B.

Answer: B