IBM

Exam M2150-768

IBM Security Sales Mastery Test v4

Version: 7.0

[Total Questions: 62]

Question No : 1

A single appliance to collect events and flow data, perform data correlation and rule matching, report alerts and provide admin capability is called:

A. Flow processor.
B. QFlow Collector.
C. A Combined Flow/Event Appliance.
D. An All-in-One.

Answer: D
Reference: ftp://public.dhe.ibm.com/software/ch/pdf/qradar/Vormittag_slides.pdf (slide 23)

Question No : 2

Which statement best explains the business value of IBM Endpoint manger (BigFix) to your customer? (The elevator pitch).

A. IBM Endpoint Manager (BigFix) provides real-time visibility and control to help IT find and fix problems in minutes, across all endpoints. on and off the corporate network, compressing patch/inventory cycles to minutes/hours and ensuring continuous compliance.
B. IBM Endpoint Manager (BigFix) provides real-time visibility and control to help IT find and fix problems fast using a single agent, console and server to manage over 150k endpoints. BigFix helps clients streamline processes, reduce infrastructure costs and ensure continuous compliance.
C. IBM Endpoint Manager (BigFix) secures mobile devices and endpoints.

Answer: B

Question No : 3

IBM SAM for Mobile provides strong protection. When talking to clients about it, what might you want to work into the discussion?

A. SAM for Mobile can save money for clients with DataPower appliances.
B. SAM for Mobile appliances provide superior performance, TTV and TCO.
C. SAM for Mobile integrates other key IBM security controls (e. g., Trusteer. WorkLight

and MaaS360) to enforce more informed policy-driven access.
D. SAM for Mobile provides risk-/context-based access support that's critical for mobile endpoints outside the client's intranet.

Answer: D

Question No : 4

Your client uses IBM DataPower (DP) appliances in their DMZ for detecting and mitigating XML-based threats. They're currently unhappy with their (non-IBM) web and mobile security solution(s). What should you do?

A. Talk to them about Tivoli Security Policy Manager as a policy authoring tool and decision engine in support of the DP policy enforcement points.
B. Talk to them about IBM SAM for DataPower. They can leverage their DataPower investment, adding web and enhanced mobile security to their DP appliances.
C. Talk to them about IBM SAM for Mobile's ability to integrate with DataPower.
D. Propose a replacement of their current Web and Mobile controls in their DMZ with IBM SAM for Web and Mobile appliances, with a SAM for Mobile policy server supporting the SAM and DP appliances in the DMZ.

Answer: A

Question No : 5

What is a common z/OS security vulnerability?

A. Storage is not properly encrypted
B. Network access points are not properly protected
C. Too many users with the ability to circumvent controls
D. System z does not have certifications for Common Critera or FIPS 140

Answer: C
Reference: https://www-950.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/The%20Changing%20System%20z%20Threat%20Landscape%20Clement%2009-17-2014%20AJN%20v2/$file/The%20Changing%20System%20z%20Threat%20Landscape%20Clement%2009-17-2014%20AJN%20v2.pdf (page 7, see common security vulnerabilities)

Question No : 6

Trusteer Apex can block malicious communications from an endpoint infected with data-stealing malware. When doing so, which function does it perform?

A. Prevent the exploitation of known and zero-day vulnerabilities and stop drive-by downloads
B. Detect and remove known advanced malware from mobile devices
C. Prevent malware from compromising other processes and opening external communication channels
D. Prevent leakage of sensitive information via email and USB drives

Answer: A
Reference: http://www.ibm.com/developerworks/library/se-trusteer/

Question No : 7

The XGS Product Family consists of a number of different models. The XGS 7100 can protect up to which "inspected throughput" value?

A. 800 Mbps
B. 1.5Gbps
C. 7Gbps
D. 20Gbps

Answer: C
Reference: http://www.draware.dk/fileadmin/IBM/NetxGen_XGS/IBMInfrastructureSec_Oct2014__NetxGen_.pdf (slide 21)

Question No : 8

The organizations that receive the highest value from our endpoint management (BigFix) solution display which characteristic?

A. Organizations with multiple locations, large quantity of remote or mobile computers or distributed servers.
B. Multi-platform environments -desktops, laptops, servers, point-of-sale/embedded: Windows, UNIX, Linux, Mac, iOS. Android.
C. Compliance requirements -need to prove compliance with specific government regulations (e. D. HIPAA. PCI) and IT standards and policies: security compliance: license compliance, audits.
D. All of the above

Answer: C

Question No : 9

What key advantages does the QRadar Security Intelligence Platform offer over the competition?

A. Provides a single UI, workflow, reporting and correlation platform for all QRadar products, now and into the future.
B. Virtually every component of the QRadar platform is exposed via a robust set of APIs, allowing customers and partners to easily develop their own Security Intelligence applications.
C. The QRadar platform runs on most major operating systems, easing deployment and reducing overall costs.
D. QRadar itself is highly secure, and because its architecture is open, it has been certified by NIST and OASIS.

Answer: A

Question No : 10

Which Guardium solution provides dynamic data masking capabilities?

A. Guardium Data Encryption
B. Guardium Database Activity Monitoring
C. Guardium Vulnerability Assessment
D. Guardium for Applications