Exam Code: 000-530

Exam Name: IBM Internet Security Systems Technical Test

Vendor: IBM

Version: DEMO

Part: A

1: A client requests a GX5108CF demonstration. After receiving the GX5108CF and BYP-2T-2S-0L-P bypass unit, the client calls the SE and explains that the four segments in the network are copper running at 1GBPS. How should the SE respond?

A.Arrange for 2x (DUAL-TVR-KIT-TX-ROHS) transceiver kits and 1x (BYP-4T-0S-0L-P) bypass units.

B.Arrange for a Gx5108SFP with 4x (DUAL-TVR-KIT-LX-ROHS) transceiver kits.

C.Arrange for 4x (DUAL-TVR-KIT-TX-ROHS) transceiver kits (2 kits for NIPS and 2 kits for the bypass unit).

D.Arrange for 4x (DUAL-TVR-KIT-TX-ROHS) transceiver kits and 1x (BYP-4T-0S-0L-P) bypass units.

Correct Answers: A

2: A client needs to make a decision regarding HIPS. He is very busy and relying on the SEs security expertise. He has requested a quick proposal with minimal options. Considering the clients requirements, which of the following is most important to determine?

A.The type of operating system and hardware specifications on each server

B.The type of operating system, kernel, exact OS versions, and hardware specifications on each server

C.The operating systems used by the majority of the servers

D.The clients budget and whether Server Sensor or Proventia Server best meets the clients needs

Correct Answers: B

3: A client requests a Proventia MFS demonstration. How should the SE respond?

A.Request a discussion to understand the clients requirements, verify the MFS is the best fit, and arrange the demonstration.

B.Describe the different MFS models and recommend the MX1004 for the demonstration.

C.Arrange a demonstration to feature high availability.

D.Review the clients network topology and recommend an appropriate MX appliance in transparent mode.

Correct Answers: A

4: After an initial meeting and follow-up phone discussions, the client has requested a test of the Proventia GX5008, along with a short demonstration. What should be the SEs next step?

A.Since the correct model is established, there is no reason to further query the client. Arrange a date to deliver the box and perform a demonstration.

B.Ask the client for a list of operating systems with kernel and exact OS versions, and hardware specifications of the servers on their network.

C.Find an activity away from the normal office environment that the client enjoys (for example, golf) and discuss the demonstration requirements.

D.Send the client a checklist with specific items to have ready, such as power, management IP, types of interfaces on switch and link speeds, monitor, and keyboard for console access.

Correct Answers: D

5: What steps should an SE take to prepare for a GX3002 evaluation?

A.1. Obtain a Proventia Network IPS appliance, license, and Quick Start Guide.

2. Immediately send the items to the client.

3. Ensure the client can log in to support and submit inquiries.

B.1. Schedule the evaluation at a time when there is a dedicated client resource.

2. Help the client create a list of evaluation items.

3. Call the client regularly during the evaluation to check progress and offer assistance.

C.1. Schedule a time to go onsite for the evaluation.

2. Obtain a Proventia Network IPS appliance and license.

3. Conduct the evaluation and send a report to the client summarizing findings.

D.1. Offer the client a one month license to evaluate.

2. Arrange for a project manager and delivery team to be onsite during the evaluation.

3. Follow up with the client to ensure all the features are being demonstrated.

Correct Answers: B

6: A client has requested a demonstration of high availability. How can an SE help ensure a smooth demonstration?

A.Conduct a technical meeting to determine whether the clients traffic is symmetric or asymmetric and how the network is designed for redundancy.

B.Explain to the client that high availability cannot be demonstrated and refer to the IBM ISS technical whitepaper for further information.

C.Ensure there are at least two bypass units available during the demonstration.

D.Use the GX6116 for the demonstration because it meets the client requirements for high availability, power supply, 16 ports, and port failover.

Correct Answers: A

7: A client has requested a Proventia Network IPS demonstration that focuses on protection against attacks and ease of use. Which tasks best demonstrate these features?

A.Enable X-Force recommended signatures and switch from simulation mode to inline protection mode.

B.Log in to MSS Portal, use the portal, and use OOB when the management port link is unavailable.

C.Define Open Signatures and start a Go to Assist session.

D.Send email alerts and SNMP traps and integrate Proventia Network IPS with Tivoli.

Correct Answers: A

8: After an SE performs a successful HIPS demonstration, the client requests a two week evaluation period.   While waiting for the clients decision, what should the SE do?

A.Wait for the evaluation period to end, and then ask the client for feedback.

B.Make regular calls during the two weeks to check on the clients progress and ascertain if they need help. Sync up with the sales person and keep him updated.

C.Keep calling the client, but keep in mind that this may lead him to make more queries and find issues with our product, especially if the client is not proficient in the product.

D.Since the demonstration was successful, dedicate time to other projects. This ensures that pipelines are healthy.

Correct Answers: B

9: After a successful demonstration the client requests a license in order to further evaluate the product. What action should the SE take?

A.Give the client the license, and offer him as much time as necessary since this is only an evaluation.

B.Ask the client about his expectations regarding the evaluation, and explain the minimum time and resources he will need during the evaluation period.

C.Agree to give the client the license, and inform him of the thirty-day policy.

D.Explain to the client that as part of the demonstration agreement, he is obligated to make a decision.

Correct Answers: B

10: An SE is accompanying the sales team to a sales presentation. The sales team asks the SE to discuss commercial and open-source vulnerability scanning solutions. What content should the SE include?

A.Vulnerability scanning tools must be based on high-quality vulnerability research to be most effective.

B.Commercial tools always check for more vulnerabilities than open source tools.

C.Open source tools might cause a denial of service during a scan, but commercial products never cause this problem.

D.Commercial vulnerability scanning tools are faster than open source tools.

Correct Answers: A

11: Which of the following is true regarding how SiteProtector can be deployed?

A.It can only be deployed as a stand-alone server or as an appliance.

B.It can be deployed in a stand-alone or distributed architecture.

C.It must be deployed by IBM ISS Professional Services.

D.It must be deployed with all Network IPS appliances.

Correct Answers: B

12: Which component commits IDS events to the SiteProtector Database?

A.IDS Appliance

B.Agent Manager

C.Event Collector

D.Secure Sync

Correct Answers: C

13: An SE is working with the sales team to prepare a response to an RFP for penetration testing services and vulnerability management tools. The RFP asks for detailed information regarding vulnerabilities found by the vendor at other client sites in the same industry. How should the SE handle this request?

A.Refer to the standard contractual confidentiality clause.

B.Provide the information but do not provide names.

C.Provide the requested information with names.

D.Refer the request to the sales team.

Correct Answers: D

14: Which statement best describes the ports on the Proventia GX6116?

A.The device has 16 network segments with 5Gbps of processing ability per segment and a built-in Layer-1 bypass unit.

B.The device has 16 network segments for protection of Ethernet circuits, a built-in Layer-1 bypass unit and 6Gbps of aggregate throughput across the appliance.

C.The device has 16 traffic ports which can be used in pairs to provide protection for 8 Ethernet segments and has a processing engine which can sustain 5Gbps of traffic with no internal Layer-1 bypass units.

D.The device has 6Gbps of traffic processing ability with 11 port pairs for protection of Ethernet segments, 6 of which have internal bypass units built into the appliance.

Correct Answers: C

15: Which policy contains signature exceptions for specific VLANs?

A.Firewall

B.User Defined Events

C.Protection Domains

D.Connection Events

Correct Answers: C

16: An SE is helping the sales team identify an integrated security solution to support 2,000 users in a head office. Comprehensive protection, cost-effectiveness, and simplicity are all important criteria for the client. What solution should the SE suggest?

A.Enterprise Scanner, Proventia Network IPS appliances, and SiteProtector

B.Proventia Desktop, SiteProtector, and Proventia Network IPS appliances

C.Proventia MX1004 appliance

D.Proventia MX5008 appliance

Correct Answers: B

17: A client had a security incident involving the misuse of an administrator login which resulted in the loss of a large amount of confidential data. The client has started a security project to avoid similar incidents in the future. What should the SE propose to the client?

A.RealSecure Server Sensor deployment to detect and alert on suspicious administrator account activity

B.Data Management and Administration review workshop to implement a comprehensive solution and avoid future incidents

C.Tivoli Identity Management solution and an ISS Data Loss Prevention solution to address the primary technical issues

D.A solution that encompasses many IBM ISS products and offerings to address the broader

security issues, not just the misuse of one login

Correct Answers: D

18: When copying XPU update files to the Proventia MFS device for a manual update, what is the required protocol, username, and folder?

A.SCP, root, and /var/spool/updates

B.SCP, admin, and /usr/iss/xpu

C.SFTP, ISSDaemon, and /var/run/updater

D.SFTP, root, and /var/updates

Correct Answers: A

19: An SE is working with the clients network administrator to design a network IPS deployment. The network administrator asks to deploy high availability under the current discount with no additional costs. The SE has the pricing and discount guide onsite. What should the SE do?

A.Calculate the clients exact discount rate for high availability.

B.Tell the client that high availability is sold only at full price.

C.Refer the question to the Account Executive.

D.Estimate the clients discount rate.

Correct Answers: C

20: An SE is meeting with a client to discuss an upcoming Proventia Network IPS deployment. The sales team wants to close the deal as soon as possible. Before placing the order, the client wants an agreement to have a 4-hour replacement service for failed hardware. What should the SE propose?

A.A cold spare

B.Premium Support

C.An evaluation unit in case the hardware fails

D.Active/Passive High Availability

Correct Answers: A