Chapter 7

1. **A user is proposing the purchase of a patch management solution for a company. The user wants to give reasons why the company should spend money on a solution. What benefits does patch management provide? (Choose three.)**

   - Administrators can approve or deny patches.
   - Updates can be forced on systems immediately.
   - Updates cannot be circumvented

يقترح أحد المستخدمين شراء حل لإدارة التصحيح لشركة. يريد المستخدم إبداء الأسباب التي تجعل الشركة تنفق الأموال على الحل. ما الفوائد التي توفرها إدارة التصحيح؟ (اختر ثلاثة.)

- يمكن للمسؤولين الموافقة على التصحيحات أو رفضها.
- يمكن فرض التحديثات على الأنظمة على الفور.
- لا يمكن التحايل على التحديثات

2. **A user calls the help desk complaining that an application was installed on the computer and the application cannot connect to the Internet. There are no antivirus warnings and the user can browse the Internet. What is the most likely cause of the problem?**

   - computer firewall

يتصل أحد المستخدمين بمكتب المساعدة ويشتكي من تثبيت أحد التطبيقات على الكمبيوتر ولا يمكن للتطبيق الاتصال بالإنترنت. لا توجد تحذيرات لمكافحة الفيروسات ويمكن للمستخدم تصفح الإنترنت. ما هو السبب الأكثر احتمالا لهذه المشكلة؟ جدار حماية الكمبيوتر

3. **Companies may have different operation centers that handle different issues with the IT operations. If an issue is related to network infrastructure, what operation center would be responsible?**

   - NOC
   - SOC
   - HVAC
   - HR

- قد يكون لدى الشركات مراكز تشغيل مختلفة تتعامل مع مشكلات مختلفة في عمليات تكنولوجيا المعلومات. إذا كانت هناك مشكلة تتعلق بالبنية التحتية للشبكة ، فما هو مركز العمليات الذي سيكون مسؤولاً؟

4. **Why is WPA2 better than WPA?**

   - mandatory use of AES algorithms

5. **A company wants to implement biometric access to its data center. The company is concerned with people being able to circumvent the system by being falsely accepted as legitimate users. What type of error is false acceptance?**

شركة تريد تنفيذ الوصول البيومتري إلى مركز البيانات الخاص بها. تهتم الشركة بقدرة الأشخاص على التحايل على النظام من خلال قبولهم خطأً كمستخدمين شرعيين. ما هو نوع الخطأ القبول الزائف؟ Type II

6. **An administrator of a small data center wants a flexible, secure method of remotely connecting to servers.Which protocol would be best to use؟**

يريد مسؤول مركز بيانات صغير طريقة مرنة وآمنة للاتصال بالخوادم عن بُعد. ما هو البروتوكول الأفضل للاستخدام؟ Secure Shell

- **Which service will resolve a specific web address into an IP address of the destination web server? DNS**

- ما الخدمة التي ستحل عنوان ويب محددًا إلى عنوان IP لخادم الويب الوجهة؟

7. **Which three items are malware? (Choose three.)**

- virus
- Trojan horse
- keylogger

ما العناصر الثلاثة التي تعتبر برامج ضارة؟ (اختر ثلاثة.) فايروس • حصان طروادة • كلوغر

8. **The CIO wants to secure data on company laptops by implementing file encryption. The technician determines the best method is to encrypt each hard drive using Windows BitLocker. Which two things are needed to implement this solution? (Choose two.)**

- at least two volumes
- TPM

- يريد رئيس قسم المعلومات تأمين البيانات على أجهزة الكمبيوتر المحمولة الخاصة بالشركة من خلال تطبيق تشفير الملفات. يحدد الفني أن أفضل طريقة هي تشفير كل محرك أقراص ثابت باستخدام Windows BitLocker. أي شيئين مطلوبين لتنفيذ هذا الحل؟ (إختر إثنين.)

9. **A user makes a request to implement a patch management service for a company. As part of the requisition the user needs to provide justification for the request. What three reasons can the user use to justify the request? (Choose three.)**

- no opportunities for users to circumvent updates
- the ability to obtain reports on systems
- the ability to control when updates occur

يقوم أحد المستخدمين بتقديم طلب لتنفيذ خدمة إدارة التصحيح لإحدى الشركات. كجزء من الطلب ، يحتاج المستخدم إلى تقديم مبرر للطلب. ما هي الأسباب الثلاثة التي يمكن للمستخدم استخدامها لتبرير الطلب؟ (اختر ثلاثة.)

- لا توجد فرص للمستخدمين للتحايل على التحديثات
- الحصول على تقارير عن الأنظمة
- القدرة على التحكم في وقت حدوث التحديثات

10. **The manager of desktop support wants to minimize downtime for workstations that crash or have other software-related issues. What are three advantages of using disk cloning? (Choose three.)**

- can provide a full system backup
- easier to deploy new computers within the organization
- ensures a clean imaged machine
-

- يريد مدير دعم سطح المكتب تقليل وقت التوقف عن العمل لمحطات العمل التي تتعطل أو بها مشكلات أخرى متعلقة بالبرمجيات. ما هي المزايا الثلاث لاستخدام استنساخ القرص؟ (اختر ثلاثة.)

- يمكن أن توفر نسخة احتياطية كاملة للنظام
- سهولة نشر أجهزة كمبيوتر جديدة داخل المنظمة
- يضمن وجود آلة مصورة نظيفة

11. **A user is asked to analyze the current state of a computer operating system. What should the user compare the current operating system against to identify potential vulnerabilities?**

- a baseline

يطلب من المستخدم تحليل الحالة الحالية لنظام تشغيل الكمبيوتر. ما الذي يجب على المستخدم مقارنة نظام التشغيل الحالي به لتحديد نقاط الضعف المحتملة؟ خط الأساس

12. **What is the difference between an HIDS and a firewall?**

- An HIDS monitors operating systems on host computers and processes file system activity. Firewalls allow or deny traffic between the computer and other systems.

-
- ما هو الفرق بين HIDS وجدار الحماية؟
- يقوم HIDS بمراقبة أنظمة التشغيل على أجهزة الكمبيوتر المضيفة وعمليات نشاط نظام الملفات. تسمح جدران الحماية بحركة المرور بين الكمبيوتر والأنظمة الأخرى أو ترفضها.

13. **What are three types of power issues that a technician should be concerned about? (Choose three.)**

- blackout
- brownout
- spike

- ما هي الأنواع الثلاثة من مشكلات الطاقة التي يجب أن يهتم بها الفني؟ (اختر ثلاثة.)

- انقطع الكهرباء - براون آوت - تصاعد

14. **A new PC is taken out of the box, started up and connected to the Internet. Patches were downloaded and installed. Antivirus was updated. In order to further harden the operating system what can be done?**

- Remove unnecessary programs and services.

- يتم إخراج جهاز كمبيوتر جديد من العلبة وتشغيله وتوصيله بالإنترنت. تم تنزيل التصحيحات وتثبيتها. تم تحديث برنامج مكافحة الفيروسات. من أجل تقوية نظام التشغيل بشكل أكبر ، ما الذي يمكن فعله؟
- إزالة البرامج والخدمات غير الضرورية.

15. **The company has many users who telecommute. A solution needs to be found so a secure communication channel can be established between the remote location of users and the company. What is a good solution for this situation?**

- VPN

- لدى الشركة العديد من المستخدمين الذين يعملون عن بعد. يجب إيجاد حل حتى يمكن إنشاء قناة اتصال آمنة بين الموقع البعيد للمستخدمين والشركة. ما هو الحل الجيد لهذا الموقف؟

16. **Why should WEP not be used in wireless networks today?**

- easily crackable

لماذا لا يجب استخدام WEP في الشبكات اللاسلكية اليوم؟ قابل للتصدع بسهولة

17. **A user calls the help desk complaining that the password to access the wireless network has changed without warning. The user is allowed to change the password, but an hour later, the same thing occurs. What might be happening in this situation?**

- rogue access point

يتصل أحد المستخدمين بمكتب المساعدة ويشتكي من تغيير كلمة المرور الخاصة بالوصول إلى الشبكة اللاسلكية دون سابق إنذار. يُسمح للمستخدم بتغيير كلمة المرور ، ولكن بعد ساعة يحدث نفس الشيء. ماذا يمكن أن يحدث في هذه الحالة؟ نقطة وصول خادعة

18. **An intern has started working in the support group. One duty is to set local policy for passwords on the workstations. What tool would be best to use?**

- secpol.msc

- بدأ المتدرب العمل في مجموعة الدعم. واجب واحد هو وضع سياسة محلية لكلمات المرور على محطات العمل. ما هي الأداة الأفضل للاستخدام؟

19. **The manager of a department suspects someone is trying to break into computers at night. You are asked to find out if this is the case. What logging would you enable?**

- audit

- مدير قسم يشتبه في أن شخصا ما يحاول اقتحام أجهزة الكمبيوتر ليلا. يُطلب منك معرفة ما إذا كان هذا هو الحال. ما التسجيل الذي يمكنك تمكينه؟

20. **After a security audit for an organization, multiple accounts were found to have privileged access to systems and devices. Which three best practices for securing privileged accounts should be included in the audit report? (Choose three.)**

- Enforce the principle of least privilege.
- Secure password storage.
- Reduce the number of privileged accounts.

بعد إجراء تدقيق أمني لإحدى المؤسسات ، تم العثور على حسابات متعددة تتمتع بامتيازات الوصول إلى الأنظمة والأجهزة. ما هي أفضل ثلاث ممارسات لتأمين الحسابات المميزة التي يجب تضمينها في تقرير التدقيق؟ (اختر ثلاثة.) فرض مبدأ الامتياز الأقل. - • تخزين آمن لكلمات المرور. - • تقليل عدد الحسابات المميزة.

Chapter 8

1. **An auditor is asked to assess the LAN of a company for potential threats. What are three potential threats the auditor may point out? (Choose three.)**

   - a misconfigured firewall
   - unauthorized port scanning and network probing
   - unlocked access to network equipment

- يُطلب من المدقق تقييم الشبكة المحلية للشركة بحثًا عن التهديدات المحتملة. ما هي التهديدات المحتملة الثلاثة التي قد يشير إليها المدقق؟ (اختر ثلاثة.)
- جدار حماية تم تكوينه بشكل خاطئ
- فحص المنافذ غير المصرح به والتحقق من الشبكة
- وصول غير مقفل إلى معدات الشبكة

2. **As part of HR policy in a company, an individual may opt-out of having information shared with any third party other than the employer. Which law protects the privacy of personal shared information?**

   - GLBA

- كجزء من سياسة الموارد البشرية في الشركة ، يجوز للفرد إلغاء الاشتراك في مشاركة المعلومات مع أي طرف ثالث بخلاف صاحب العمل. أي قانون يحمي خصوصية المعلومات الشخصية المشتركة؟
- GLBA

3. **As a security professional, there is a possibility to have access to sensitive data and assets. What is one item a security professional should understand in order to make informed ethical decisions?**

   - laws governing the data

- كمحترف أمني ، هناك إمكانية للوصول إلى البيانات والأصول الحساسة. ما هو العنصر الوحيد الذي يجب أن يفهمه متخصص الأمن من أجل اتخاذ قرارات أخلاقية مستنيرة؟
- القوانين التي تحكم البيانات

4. **A security professional is asked to perform an analysis of the current state of a company network. What tool would the security professional use to scan the network only for security risks?**

   - vulnerability scanner

يُطلب من أخصائي الأمن إجراء تحليل للحالة الحالية لشبكة الشركة. ما الأداة التي سيستخدمها متخصص الأمن لفحص الشبكة فقط بحثًا عن مخاطر الأمان؟

الماسح الضوئي

5. **A consultant is hired to make recommendations on managing device threats in a company. What are three general recommendations that can be made? (Choose three.)**

- Disable administrative rights for users.
- Enable automated antivirus scans.
- Enable screen lockout.

- يتم تعيين مستشار لتقديم توصيات بشأن إدارة تهديدات الجهاز في الشركة. ما هي ثلاث توصيات عامة يمكن تقديمها؟ (اختر ثلاثة.) تعطيل الحقوق الإدارية للمستخدمين.
- تمكين عمليات الفحص الآلي لمكافحة الفيروسات. - تفعيل قفل الشاشة.

6. **What three services does CERT provide? (Choose three.)**

- develop tools, products, and methods to analyze vulnerabilities
- develop tools, products, and methods to conduct forensic examinations
- resolve software vulnerabilities

ما هي الخدمات الثلاث التي تقدمها CERT؟ (اختر ثلاثة.)
تطوير أدوات ومنتجات وأساليب لتحليل نقاط الضعف
تطوير أدوات ومنتجات وطرق لإجراء فحوصات الطب الشرعي
حل نقاط الضعف في البرامج

7. **What are two items that can be found on the Internet Storm Center website? (Choose two.)**

- InfoSec reports
- InfoSec job postings

- ما هما العنصران اللذان يمكن العثور عليهما على موقع Internet Storm Center؟ (إختر إثنين.)
- تقارير InfoSec - إعلانات الوظائف InfoSec

8. **What can be used to rate threats by an impact score to emphasize important vulnerabilities?**

- NVD

ما الذي يمكن استخدامه لتقييم التهديدات حسب درجة التأثير للتأكيد على نقاط الضعف المهمة؟

NVD

9. **A breach occurs in a company that processes credit card information. Which industry specific law governs credit card data protection?**

- PCI DSS

- يحدث خرق في شركة تعالج معلومات بطاقة الائتمان. ما هو القانون الخاص بالصناعة الذي يحكم حماية بيانات بطاقة الائتمان؟ PCI DSS

10. **Why is Kali Linux a popular choice in testing the network security of an organization?**

- It is an open source Linux security distribution and contains over 300 tools

- لماذا يعتبر Kali Linux خيارًا شائعًا في اختبار أمان شبكة مؤسسة ما؟

إنه توزيع أمان Linux مفتوح المصدر ويحتوي على أكثر من ٣٠٠ أداة

11. **A company is attempting to lower the cost in deploying commercial software and is considering a cloud based service. Which cloud based service would be best to host the software?**

- SaaS

- تحاول إحدى الشركات خفض تكلفة نشر البرامج التجارية وتفكر في تقديم خدمة قائمة على السحابة. ما الخدمة المستندة إلى السحابة الأفضل لاستضافة البرنامج؟ SaaS

12. **An organization has implemented a private cloud infrastructure. The security administrator is asked to secure the infrastructure from potential threats. What three tactics can be implemented to protect the private cloud? (Choose three.)**

- Update devices with security fixes and patches.
- Test inbound and outbound traffic.
- Disable ping, probing, and port scanning.

- قامت إحدى المؤسسات بتنفيذ بنية أساسية خاصة بالسحابة الإلكترونية. يُطلب من مسؤول الأمان تأمين البنية التحتية من التهديدات المحتملة. ما هي الأساليب الثلاثة التي يمكن تنفيذها لحماية السحابة الخاصة؟ (اختر ثلاثة.) تحديث الأجهزة مع تصحيحات وتصحيحات الأمان.
- اختبر حركة المرور الواردة والصادرة.
- تعطيل فحص الاتصال والتحقق والمنافذ.

13. **A school administrator is concerned with the disclosure of student information due to a breach. Under which act is student information protected?**

- FERPA

- يهتم مسؤول المدرسة بالإفصاح عن معلومات الطالب بسبب حدوث خرق. بموجب أي قانون يتم حماية معلومات الطالب؟

- فيربا

14. **What are the three broad categories for information security positions? (Choose three.)**

- definers
- monitors
- builders

- ما هي الفئات الثلاث العامة لشغل وظائف أمن المعلومات؟ (اختر ثلاثة.)

محددات - • الشاشات - • بناة

15. **What are two potential threats to applications? (Choose two.)**

- data loss
- unauthorized access

- ما هما التهديدان المحتملان للتطبيقات؟ (إختر إثنين.)
- فقدان البيانات
- دخول غير مرخص

16. **If a person knowingly accesses a government computer without permission, what federal act laws would the person be subject to?**

- CFAA

- إذا قام شخص ما عن عمد بالوصول إلى جهاز كمبيوتر حكومي دون إذن ، فما هي قوانين القانون الفيدرالية التي سيخضع لها الشخص؟ CFAA

17. **A company has had several incidents involving users downloading unauthorized software, using unauthorized websites, and using personal USB devices. The CIO wants to put in place a scheme to manage the user threats. What three things might be put in place to manage the threats? (Choose three.)**

- Disable CD and USB access.
- Provide security awareness training.
- Use content filtering.

تعرضت إحدى الشركات للعديد من الحوادث التي تنطوي على قيام المستخدمين بتنزيل برامج غير مصرح بها ، واستخدام مواقع ويب غير مصرح بها ، واستخدام أجهزة USB شخصية. يريد رئيس قسم المعلومات وضع مخطط لإدارة تهديدات المستخدم. ما الأشياء الثلاثة التي يمكن وضعها لإدارة التهديدات؟ (اختر ثلاثة.)

- تعطيل الوصول إلى القرص المضغوط و USB.
- تقديم تدريب للتوعية الأمنية. - استخدم تصفية المحتوى.

18. **What are three disclosure exemptions that pertain to the FOIA? (Choose three.)**

- confidential business information
- national security and foreign policy information
- law enforcement records that implicate one of a set of enumerated concern

- ما هي استثناءات الإفصاح الثلاثة التي تتعلق بقانون حرية المعلومات؟ (اختر ثلاثة.)
- معلومات تجارية سرية - معلومات الأمن القومي والسياسة الخارجية
- سجلات إنفاذ القانون التي تشير إلى مجموعة من المخاوف التي تم تعدادها

19. **Unauthorized visitors have entered a company office and are walking around the building. What two measures can be implemented to prevent unauthorized visitor access to the building? (Choose two.)**

- Establish policies and procedures for guests visiting the building.
- Conduct security awareness training regularly.

دخل الزوار غير المصرح لهم إلى مكتب الشركة ويتجولون في المبنى. ما الإجراءان اللذان يمكن تنفيذهما لمنع دخول الزوار غير المصرح لهم إلى المبنى؟ (إختر إثنين.)

وضع السياسات والإجراءات للضيوف الذين يزورون المبنى.

إجراء تدريب للتوعية الأمنية بانتظام.