الاسم: _____ التاريخ: _____ الدرجة: _____

حماية البيانات وتخزين المؤسسات دليل الأمان

إخفاء البيانات، والترميز (tokenization)، والتشفير أثناء السكون مقابل أثناء النقل، والنسخ الاحتياطية دون اتصال

نظرة تعليمية عامة على حماية البيانات

مرحبًا! ترشدك حزمة الأنشطة هذه عبر معايير وضوابط حماية البيانات. ستستكشف تشفير القرص الكامل وضوابط الوصول الآمن والنسخ الاحتياطية للأجهزة ووضع الأمان السحابي وتقنيات إخفاء البيانات.

نقاط التحقق في ورقة العمل

- [ ] **الجزء 1-4: أتقن الأمن السيبراني ومنع التهديدات.**
- [ ] **الجزء 5-7: حل الكلمات المتقاطعة وألغاز البحث عن الكلمات.**
- [ ] **الجزء 8-9: حل دراسات الحالة وتحدي الشيفرة.**
- [ ] **الجزء 10: راجع صفحات الأسئلة الشائعة الأساسية والمتقدمة.**
- [ ] **الجزء 11: استكشف 10 حقائق مثيرة من الواقع.**
- [ ] **إضافي: تحدّي فكّر بسرعة**

مؤمَّن
تشفير البيانات
معيار AES بطول 256 بت

متوافق
المعايير العالمية
أطر GDPR وCCPA

انعدام الثقة
سياسة الوصول
المصادقة متعددة العوامل

افتح دليل VPN.com للأمن السيبراني

URL: https://www.vpn.com/cybersecurity/data-protection/

خارطة طريقك لتعلّم استراتيجية حماية البيانات

- ميّز بين تقنيتي إخفاء البيانات والترميز (tokenization).
- طبّق التشفير أثناء التخزين لمحركات التخزين والتشفير أثناء النقل باستخدام TLS.
- صمّم أنظمة نسخ احتياطي معزولة عن الشبكة وغير متصلة للحماية من برمجيات الفدية.

تعليمات دليل حماية البيانات

أجب عن أسئلة الاختيار من متعدد وأسئلة صحيح/خطأ، وأكمل الجمل الناقصة باستخدام بنك الكلمات، وطابق التعريفات، وحُلّ الكلمات المتقاطعة وبحث الكلمات. طبّق معرفتك على حماية البيانات. واختم بالنشاط الإضافي «فكّر بسرعة».

حماية البيانات وأمان تخزين المؤسسات (مقدمة)

تحمي حماية البيانات أصول بيانات الشركة عبر الإخفاء والترميز (tokenization) وتشفير قواعد البيانات أثناء السكون وبروتوكولات النقل الآمنة. ويساعد تصميم نسخ احتياطية معزولة عن الشبكة على ضمان إمكانية استعادة قواعد البيانات الرئيسية عند وقوع اختراق نشط.

اقرأ كل نقطة تحقق بعناية، ثم اختر الإجابة الصحيحة أو اكتبها.

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما الغرض الرئيسي من إخفاء البيانات؟
   - A. استبدال المعرّفات الحساسة بأحرف وهمية لكنها واقعية لحماية الخصوصية
   - B. ضغط ملفات قواعد البيانات الكبيرة لتوفير مساحة التخزين على الخادم الفعلي
   - C. حذف رسائل البريد الإلكتروني القديمة لجهات اتصال العملاء من أنظمة النسخ الاحتياطي الأرشيفية
   - D. إخفاء عنوان IP العام لخادم قاعدة البيانات عن عمليات المسح عبر الإنترنت

2. ما الآلية التي تشفّر الملفات المخزنة على القرص الصلب لخادم قاعدة البيانات؟
   - A. تشفير القرص الكامل أثناء التخزين
   - B. بروتوكولات مصافحة جلسة TLS أثناء النقل
   - C. قواعد إعادة توجيه خادم الأسماء الديناميكي DNS
   - D. المصادقة متعددة العوامل باستخدام مفاتيح عتادية

3. ما الذي يمثل البيانات أثناء النقل؟
   - A. حزم البيانات المتنقلة عبر موجّهات الشبكة ومحوّلاتها
   - B. سجلات معاملات قواعد البيانات المخزّنة على قرص احتياطي بارد
   - C. ملفات مستخدمين مؤرشفة محفوظة في خزنة سحابية معزولة
   - D. ملفات تهيئة النظام الثابتة على تخزين سطح مكتب محلي

4. لماذا تُعد النسخة الاحتياطية المنتظمة غير المتصلة حاسمة للحماية من برمجيات الفدية؟
   - A. يوفر نسخة نظيفة غير متصلة لاستعادة الملفات دون دفع فدية
   - B. يمنع المخترقين من فحص إعدادات المنافذ المفتوحة
   - C. يزيد سرعات نطاق إرسال الشبكة المحلية
   - D. يؤتمت سجلات الموافقة الاختيارية على ملفات تعريف الارتباط في المتصفحات

5. ماذا تفعل ترميز البيانات (Tokenization)؟
   - A. يستبدل أرقام البطاقات الحساسة برموز عشوائية غير حساسة
   - B. يوجّه حركة الويب عبر عدة عقد onion آمنة
   - C. يفحص أدلة النظام بحثًا عن البرمجيات الخبيثة المعتمدة على التوقيعات
   - D. يدقق أوقات جلسات تسجيل دخول مسؤولي قاعدة البيانات

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. يغيّر إخفاء البيانات سجلات قاعدة البيانات بشكل دائم في بيئات الإنتاج.

صحيح خطأ

7 سؤال 7

7. يجب عزل النسخ الاحتياطية خارج الموقع عن شبكة الشركة الرئيسية لمنع انتشار برامج الفدية.

صحيح خطأ

8 سؤال 8

8. تؤمّن شهادات SSL/TLS قواعد البيانات بتشفير البيانات المخزنة أثناء السكون على الوسائط المادية.

صحيح خطأ

9 سؤال 9

9. يتحقق الوصول إلى الشبكة بانعدام الثقة (ZTNA) من هوية كل مستخدم قبل منحه الوصول إلى قاعدة البيانات.

صحيح خطأ

10 سؤال 10

10. يخزن الترميز المعتمد على الخزنة (Vault-based tokenization) قيم البطاقة الأصلية في خزنة رموز مركزية آمنة.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

اقرأ كل جملة أدناه وأكمل الفراغ بالمصطلح الصحيح من بنك الكلمات.

1. يسمى استبدال الأسماء الشخصية بعناصر نائبة واقعية _____ البيانات.
2. يحمي تشفير كتل التخزين المادية أصول قاعدة البيانات _____ .
3. تشفر بروتوكولات TLS حزم البيانات النشطة أثناء _____ .
4. تحد الأذونات القائمة على الأدوار من المستخدمين الذين يمكنهم الحصول على _____ لقاعدة البيانات.
5. تتطلب استعادة ملفات الشركة السليمة بعد حدوث اختراق _____ آمنة غير متصلة.
6. يقيّم تدقيق إعدادات السحابة _____ الأمني للمؤسسة.

بنك كلمات المفردات

أثناء السكون | إخفاء | الاحتياطي | التشفير | النقل | الوضع | حق الوصول | نسخة احتياطية

اكتب إجاباتك هنا:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

نقطة التحقق 4: مطابقة مفاهيم الأمان

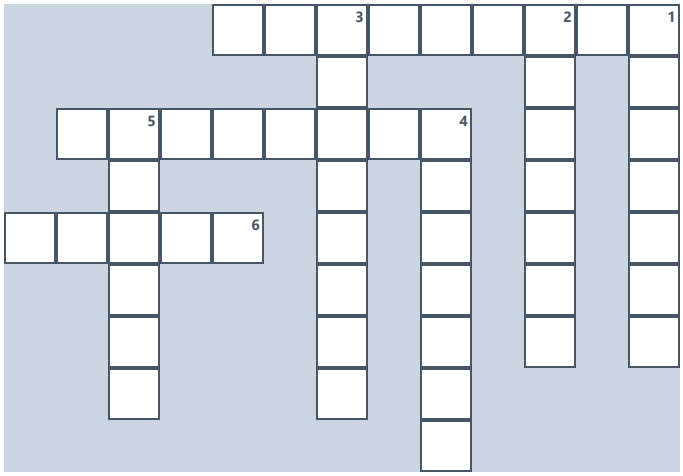
مطابقة التعريفات

طابق كل مصطلح مفردات على اليمين مع تعريفه الصحيح على اليسار بكتابة الحرف المقابل (A-H) في مربع الإدخال القابل للتعبئة.

1. التشفير	A	إنشاء نسخ آمنة خارج الموقع من البيانات لاستعادتها عند أعطال النظام.
2. نسخة احتياطية	B	تحويل النص الصريح إلى نص مشفر غير مقروء بحيث تبقى البيانات المعترضة خاصة.
3. التقليل	C	الحالة الأمنية الجماعية وجاهزية الدفاع للسحابة الخاصة بالمؤسسة.
4. الوصول	D	الامتثال للمعايير التنظيمية مثل GDPR أو CCPA لإدارة معلومات المستخدمين الخاصة.
5. الوضع الأمني	E	حادث أمني يُوصل فيه إلى بيانات محمية أو تُكشف دون تفويض.
6. الاختراق	F	تقييد أذونات القراءة والكتابة في قاعدة البيانات على أدوار المستخدمين الموثّقين.
7. الامتثال	G	استبدال الأحرف الحساسة في حقول قاعدة البيانات لحماية الهويات الشخصية.
8. الإخفاء	H	الحد من جمع البيانات الشخصية إلى أدنى قدر مطلق يلزم للعمليات.

نقطة التحقق 5: لغز الكلمات المتقاطعة

حلّ الكلمات المتقاطعة بكتابة الحروف في المربعات البيضاء النشطة. تتوافق الأرقام مع الدلائل أدناه.



أفقي

1. إنشاء نسخ آمنة خارج الموقع لاستعادة البيانات عند أعطال النظام (9)

4. استيفاء معايير تنظيمية مثل GDPR أو CCPA لإدارة معلومات المستخدمين الخاصة (8)

6. الحالة الأمنية الجماعية وجاهزية الدفاع لسحابة المؤسسة (5)

عمودي

1. استبدال أحرف حساسة في حقول قاعدة البيانات لحماية الهويات الشخصية (7)

2. حصر جمع البيانات الشخصية في الحد الأدنى اللازم للعمليات (7)

3. حادث أمني يُنفذ فيه إلى بيانات محمية أو تُكشف دون تصريح (8)

4. تحويل النص الصريح إلى نص مشفر غير مقروء ليبقى ما يُعترض من بيانات خاصاً (7)

5. حصر أذونات القراءة والكتابة في قاعدة البيانات بأدوار المستخدمين الموثقين (6)

نقطة التحقق 5 – نشاط بديل: أدلة الكلمات المتقاطعة الميسَّرة

يمكن لمستخدمي قارئ الشاشة ولوحة المفاتيح كتابة إجابات الكلمات المتقاطعة مباشرة في حقول النص أدناه.

أفقي

1 أفقي: إنشاء نسخ آمنة خارج الموقع لاستعادة البيانات عند أعطال النظام (9 حروف):

4 أفقي: استيفاء معايير تنظيمية مثل GDPR أو CCPA لإدارة معلومات المستخدمين الخاصة (8 حروف):

6 أفقي: الحالة الأمنية الجماعية وجاهزية الدفاع لسحابة المؤسسة (5 حروف):

عمودي

1 عمودي: استبدال أحرف حساسة في حقول قاعدة البيانات لحماية الهويات الشخصية (7 حروف):

2 عمودي: حصر جمع البيانات الشخصية في الحد الأدنى اللازم للعمليات (7 حروف):

3 عمودي: حادث أمني يُنفذ فيه إلى بيانات محمية أو تُكشف دون تصريح (8 حروف):

4 عمودي: تحويل النص الصريح إلى نص مشفر غير مقروء ليبقى ما يُعترض من بيانات خاصاً (7 حروف):

5 عمودي: حصر أذونات القراءة والكتابة في قاعدة البيانات بأدوار المستخدمين الموثقين (6 حروف):

نقطة التحقق 6: البحث عن الكلمة المخفية

ابحث عن 8 مصطلحات مفردات رئيسية مخبأة في الشبكة أدناه. يمكن أن تكون الكلمات أفقية أو رأسية أو قطرية.

ا	ل	و	ض	ع	ت	ك	خ	ط	ص	ث	ص	خ	ه	ص
ج	ل	ع	ش	ج	س	ف	ف	ا	ص	ل	ك	ر	ع	ع
ل	م	ن	ه	ه	ر	ت	ن	ل	ل	ق	ز	ن	ب	ض
ج	ل	ل	ي	ل	ق	ت	ل	ا	ن	ت	ء	ي	ت	ء
ل	و	ض	د	ص	ا	ز	ء	ج	ف	ج	ش	ل	خ	ك
ا	ص	ت	و	ب	ل	ا	ا	ء	ف	ج	ص	ف	ا	ج
ث	و	ق	ج	د	ا	ز	س	ل	ج	م	ل	ع	ي	ح
ت	ل	س	م	ء	ح	ن	د	ل	ا	ي	د	ا	ا	ر
م	ا	ل	ق	ف	ت	ك	ه	خ	ل	خ	ل	ص	م	و
ا	ن	ج	ف	ث	ي	ب	د	ن	ا	خ	ت	ض	ش	ا
ل	م	ء	ث	ث	ا	ط	ر	س	خ	ع	م	ر	ش	ع
ا	ط	ه	ق	ز	ط	ل	ل	ز	ف	ء	ا	ق	ا	ي
ر	و	ب	ث	م	ي	ث	ب	ز	ا	ط	ء	ر	ش	ق
ق	ك	ف	ض	ت	ع	ء	ث	ر	ء	ث	ق	ض	و	ص
ي	ك	ب	ف	ي	ه	ع	ر	ي	ج	ث	و	ص	م	ب

قائمة كلمات المفردات

التشفير الاحتياطي التقليل الوصول الوضع الاختراق الامتثال الاخفاء

نقطة التحقق 6 – نشاط بديل: مطابقة المفردات الميسَّرة

طابق كل مصطلح من المصطلحات الـ 8 في البحث عن الكلمات مع تعريفه الصحيح بكتابة الحرف (A-H) في الفراغ.

مصطلحات المفردات
A. التشفير
B. الاحتياطي
C. التقليل
D. الوصول
E. الوضع
F. الاختراق
G. الامتثال
H. الاخفاء

التعريفات وحقول المطابقة
1. حادث أمني يُنفذ فيه إلى بيانات محمية أو تُكشف دون تصريح.
2. استبدال أحرف حساسة في حقول قاعدة البيانات لحماية الهويات الشخصية.
3. حصر أذونات القراءة والكتابة في قاعدة البيانات بأدوار المستخدمين الموثقين.
4. الحالة الأمنية الجماعية وجاهزية الدفاع لسحابة المؤسسة.
5. استيفاء معايير تنظيمية مثل GDPR أو CCPA لإدارة معلومات المستخدمين الخاصة.
6. حصر جمع البيانات الشخصية في الحد الأدنى اللازم للعمليات.
7. تحويل النص الصريح إلى نص مشفر غير مقروء ليبقى ما يُعترض من بيانات خاصاً.
8. إنشاء نسخ آمنة خارج الموقع لاستعادة البيانات عند أعطال النظام.

نقطة التحقق 7: تحدي الكلمات المبعثرة

أعد ترتيب الحروف أدناه للكشف عن المفاهيم والمصطلحات الأساسية في الأمن السيبراني. اكتب إجاباتك في مربعات الإدخال المخصصة.

1. ش ي ا ف ر ت ل _____
2. ا ت ل ي ل ق ل _____
3. و ا ع ض ل _____
4. م ا ل ث ت ا ل ا _____
5. ا ت ل ي ي ح ا ط ا _____
6. و ص ا و ل ل _____
7. ا ق ت ر ا ل خ ا _____
8. ل خ ء ا ا ف ا _____

نشاط إضافي: فكّر بسرعة

اكتب 3 إجابات لكل فئة. يفوز أول من يكمل القائمة.

1	أشياء تحتفظ بنسخة احتياطية منها		
2	كلمات متعلقة بالأمن السيبراني		
3	أشخاص مسموح لهم برؤية البيانات الحساسة		
4	طرق لحذف البيانات بأمان		
5	أماكن تُخزَّن فيها البيانات		
6	أشياء ينبغي تشفيرها		
7	بيانات يجب على المستشفى حمايتها		
8	أنواع النسخ الاحتياطي		
9	معلومات لا ينبغي أن تشاركها أبدًا		
10	علامات تحذيرية في البريد الإلكتروني		
11	عادات آمنة يمكنك البدء بها اليوم		
12	أشخاص يمكنك طلب مساعدة تقنية منهم		
13	أجهزة يمكن اختراقها		
14	طرق لحماية البيانات		
15	أشياء قد تتلف البيانات		

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: ترقية تشفير قواعد بيانات المؤسسات أثناء التخزين

🔒

السيناريو: يخزّن متجر تجزئة عبر الإنترنت قواعد بيانات المعاملات على تخزين سحابي دون تشفير القرص بالكامل. أشار تدقيق امتثال حديث إلى أن هذا يمثل خطرًا جسيمًا على أمن البيانات بموجب CCPA. صمّم بنية للتعافي.

سؤال للنقاش: حلّل مخاطر الامتثال لـ CCPA، واقترح استراتيجية تشفير للبيانات المخزنة.

دراسة الحالة 2: احتواء برمجيات الفدية واستعادة البيانات

🔒

السيناريو: يشفّر هجوم برنامج فدية نشط محركات الشبكة في شبكة محلية مؤسسية. اكتشف المدير الإصابة مبكرًا. خطّط لخطوات الاحتواء والتعافي.

سؤال للنقاش: فصّل إجراءات الاحتواء الفورية، وخطّط لعملية استعادة آمنة.

نقطة التحقق 9: فك الشيفرة

يحمي متخصص الأمن السيبراني أصول الشبكة من الجهات التهديدية عبر الإنترنت. استخدم مفتاح الحرف إلى الرقم أدناه لفك تشفير الرسالة بكتابة الحروف المطابقة في الفراغات.

مفتاح التشفير من الحرف إلى الرقم

ا=1 ب=2 ت=3 ث=4 ج=5 ح=6 خ=7 د=8 ذ=9 ر=10 ز=11

س=12 ش=13 ص=14 ض=15 ط=16 ظ=17 ع=18 غ=19 ف=20 ق=21 ك=22

ل=23 م=24 ن=25 هـ=26 و=27 ي=28 ة=29 ى=30 ء=31 ؤ=32 ئ=33

29	14	1	7	23	1		22	3	1	25	1	28	2		24	6	1

29	25	24	1		16	2	1	27	15	2

الرسالة بعد فك التشفير:

نصيحة: يمثل كل رقم حرفًا عربيًا واحدًا من المفتاح أعلاه.

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول الأمن السيبراني (الجزء A)

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q1: ما حماية البيانات؟

هي عملية تأمين البيانات الشخصية وبيانات الأعمال من الوصول غير المصرّح به أو الفقدان أو التلف عبر ضوابط تقنية.

Q2: لماذا يُعد تشفير القرص بالكامل مهمًا؟

يؤمّن كتل البيانات المخزنة على الأقراص المادية، فيمنع أي شخص من قراءة البيانات إذا سرق القرص الصلب فعليًا.

Q3: ما الفرق بين التشفير أثناء التخزين والتشفير أثناء النقل؟

يؤمّن التشفير أثناء السكون الملفات المخزنة على الأقراص، بينما يؤمّن التشفير أثناء النقل الحزم النشطة المتنقلة عبر الموجّهات.

Q4: ما إخفاء البيانات (data masking)؟

يستبدل التفاصيل الحساسة (مثل أرقام بطاقات الائتمان) ببيانات خيالية لكنها واقعية للاختبار دون كشف السجلات الحقيقية.

Q5: لماذا تُعد النسخة الاحتياطية غير المتصلة بالإنترنت مهمة؟

يحتفظ بنسخة نظيفة من ملفاتك معزولة عن الشبكة، ما يساعد على حماية نسخك الاحتياطية من التشفير بواسطة برمجيات الفدية.

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول الأمن السيبراني (الجزء B)

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: ما خزنة ترميز البيانات (data tokenization vault)؟

قاعدة بيانات آمنة ومعزولة تربط الرموز العشوائية بقيمها الحساسة الأصلية (مثل أرقام بطاقات الائتمان الأساسية).

Q7: ماذا يعني الوصول إلى قواعد البيانات بنموذج الثقة المعدومة؟

يعني التحقق من هوية كل مستخدم وحالة جهازه عند كل تسجيل دخول، بدلًا من الثقة بأي شخص داخل الشبكة.

Q8: كيف يحمي TLS البيانات أثناء النقل؟

يشفّر TLS حمولة جلسة TCP، مما يمنع الجهات الخبيثة على الشبكات العامة من التنصت على الحزم أثناء النقل أو تعديلها.

Q9: ما تدقيق الوصول إلى قواعد البيانات؟

التسجيل المستمر لاستعلامات قواعد البيانات وعمليات تسجيل الدخول لكشف أنماط الوصول غير المصرح به أو الشذوذات الأمنية.

Q10: ما تدقيق الوضع الأمني السحابي؟

عملية تحلل تهيئات السحابة لتحديد المنافذ المفتوحة وقواعد الوصول الخاطئة التهيئة وثغرات الامتثال الأمني.

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول الأمان (الجزء C)

استكشف الجوانب التقنية المتقدمة لأطر الأمان وتحليل البرمجيات الخبيثة والامتثال للبيانات.

Q1: كيف يعمل تشفير المغلف؟

يشفّر البيانات بمفتاح بيانات، ثم يشفّر مفتاح البيانات هذا بمفتاح رئيسي، ما يبسّط تخزين المفاتيح وتدويرها.

Q2: ما التشفير المتجانس (homomorphic)؟

طريقة تشفير متقدمة تتيح إجراء العمليات مباشرة على البيانات المشفّرة دون فك تشفيرها أولًا.

Q3: لماذا يُستخدم تشفير أعمدة قواعد البيانات؟

يشفّر أعمدة حساسة محددة (مثل أرقام الضمان الاجتماعي) كلًّا على حدة، فيحميها حتى لو حصل المسؤولون على إذن قراءة عام للجدول.

Q4: ما منع فقدان البيانات (DLP)؟

برنامج يراقب نقاط خروج الشبكة لاكتشاف عمليات النقل الصادرة غير المصرح بها للملفات الحساسة وحظرها.

Q5: كيف تحمي النسخ الاحتياطية بنظام الكتابة مرة واحدة والقراءة مرات عديدة (WORM) من برامج الفدية؟

تمنع نسخ WORM الاحتياطية حذف الملفات أو تعديلها لمدة محددة، مما يمنع برمجيات الفدية من تشفير النسخ الاحتياطية الموجودة.

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول الأمان (الجزء D)

استكشف الجوانب التقنية المتقدمة لأطر الأمان وتحليل البرمجيات الخبيثة والامتثال للبيانات.

Q6: ما خطر إعادة استخدام المفاتيح؟

إعادة استخدام مفتاح التشفير نفسه عبر قواعد بيانات مختلفة تعني أن اختراق مفتاح واحد يكشف جميع قواعد البيانات.

Q7: كيف يحسّن ترميز قواعد البيانات الامتثال لقانون CCPA؟

تعمل الرموز المميزة على ترميز السجلات بأسماء مستعارة في الأنظمة غير الإنتاجية وتحد من التعرض للاختراق، لكن البيانات المرمّزة قد تظل معلومات شخصية.

Q8: لماذا يُعد تصنيف البيانات أمرًا بالغ الأهمية؟

يصنّف الملفات بحسب مستوى الحساسية، ما يساعد المؤسسات على تطبيق أقوى ضوابط التشفير والوصول على البيانات عالية الخطورة.

Q9: ما دور تدوير المفاتيح؟

يحد تحديث مفاتيح التشفير بانتظام من حجم البيانات التاريخية المكشوفة إذا جرى كسر مفتاح واحد في النهاية.

Q10: كيف تحمي البيئات الآمنة المعزولة استعلامات قواعد البيانات في الذاكرة؟

تعزل المناطق الآمنة (secure enclaves) عمليات الاستعلام في كتل ذاكرة محمية بالمعالج، مما يمنع مسؤولي المضيف من الاطلاع على النص الصريح في الذاكرة العشوائية.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

دخلت لوائح GDPR حيز التنفيذ في مايو 2018، فغيّرت طريقة إدارة المواقع العالمية لموافقات ملفات تعريف الارتباط وسجلات البيانات الشخصية.

2. نظرة على الأمن

قد تصل غرامة انتهاك GDPR إلى 20 مليون يورو أو 4% من الإيرادات العالمية، ما يمثل تعرضًا قانونيًا كبيرًا. [4]

3. نظرة على الأمن

دخل قانون CCPA حيز التنفيذ في يناير 2020، وأرسى حقوقًا رائدة للمستهلكين في مجال الخصوصية الرقمية في الولايات المتحدة.

4. نظرة على الأمن

يقلل تقليل البيانات من حجم تخزين قاعدة البيانات، فيخفض تكاليف تشغيل الخوادم ويقلل نطاق أثر الاختراق.

5. نظرة على الأمن

يحل التمزيق التشفيري تحدي حذف النسخ الاحتياطية عبر إتلاف المفاتيح بدلًا من تعديل ملفات شرائط النسخ الاحتياطي التاريخية.

6. نظرة على الأمن

سنّت معظم دول العالم الآن قوانين لحماية البيانات الشخصية لصون حقوق خصوصية المستهلك.

7. رؤية حول الأمان

تُحظر نماذج الموافقة بالاشتراك المسبق ذات المربعات المحددة مسبقًا صراحةً بموجب التعريفات التنظيمية الأوروبية لخصوصية البيانات.

8. رؤية حول الأمان

يشترط GDPR الإبلاغ عن خروقات البيانات الشخصية إلى السلطة الرقابية خلال 72 ساعة من العلم بها، متى كان ذلك ممكنًا. [3]

9. رؤية حول الأمان

يجعل تجزئة كلمات المرور بخوارزميات بطيئة مثل bcrypt أو Argon2 كسر التجزئات المسروقة دون اتصال أصعب بكثير. [6]

10. نظرة على الأمن

تمثل البيانات الساكنة ملفات قواعد البيانات المحفوظة، بينما تشمل البيانات أثناء النقل الحزم المتحركة فعليًا عبر موجّهات الشبكة.

المراجع والمصادر التقنية

أُعد دليل الدراسة والألغاز التفاعلية استنادًا إلى معايير NIST وOWASP العالمية ومعايير الامتثال لخصوصية البيانات.

المراجع الأكاديمية والصناعية

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 السؤال 1 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما الغرض الرئيسي من إخفاء البيانات؟ → استبدال المعرّفات الحساسة بأحرف وهمية لكنها واقعية لحماية الخصوصية

2 السؤال 2 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما الآلية التي تشفّر الملفات المخزنة على القرص الصلب لخادم قاعدة البيانات؟ → تشفير القرص الكامل أثناء التخزين

3 السؤال 3 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما الذي يمثل البيانات أثناء النقل؟ → حزم البيانات المتنقلة عبر موجّهات الشبكة ومحوّلاتها

4 السؤال 4 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

لماذا تُعد النسخة الاحتياطية المنتظمة غير المتصلة حاسمة للحماية من برمجيات الفدية؟ → يوفر نسخة نظيفة غير متصلة لاستعادة الملفات دون دفع فدية

5 السؤال 5 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ماذا تفعل ترميز البيانات (Tokenization)؟ → يستبدل أرقام البطاقات الحساسة برموز عشوائية غير حساسة

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

يغيّر الإخفاء (Masking) نسخ الاختبار أو يخفي القيم وقت الاستعلام؛ بينما تبقى سجلات الإنتاج دون تغيير.

7 السؤال 7

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يجب عزل النسخ الاحتياطية خارج الموقع عن شبكة الشركة الرئيسية لمنع انتشار برامج الفدية.

8 السؤال 8

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

تحمي شهادات TLS البيانات أثناء النقل؛ أما البيانات الساكنة فتحتاج إلى تشفير القرص أو الملف أو قاعدة البيانات.

9 السؤال 9

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يتحقق الوصول إلى الشبكة بانعدام الثقة (ZTNA) من هوية كل مستخدم قبل منحه الوصول إلى قاعدة البيانات.

10 السؤال 10

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يحتفظ الترميز المعتمد على الخزنة بالقيم الأصلية في خزنة رموز آمنة تربط كل رمز بعودته إلى بياناته.

مفاتيح المفردات ومعيار التقييم

معيار التصحيح للمعلم: امنح 1 نقطة لكل مطابقة صحيحة (المجموع 8 نقطة) ولكل مصطلح سياق (المجموع 6 نقطة).

نقطة التحقق 4: مفتاح الإجابة – مطابقة المفاهيم

B 1. التشفير	A 2. نسخة احتياطية	H 3. التقليل	F 4. الوصول
C 5. الوضع الأمني	E 6. الاختراق	D 7. الامتثال	G 8. الإخفاء

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 إخفاء	2 أثناء السكون	3 النقل	4 حق الوصول
5 نسخة احتياطية	6 الوضع		

نقطة التحقق 6 – نشاط بديل: مفتاح الإجابة – مطابقة المفردات

1 F – الاختراق	2 H – الاخفاء	3 D – الوصول	4 E – الوضع
5 G – الامتثال	6 C – التقليل	7 A – التشفير	8 B – الاحتياطي

ملاحظات النقاش للمعلمين

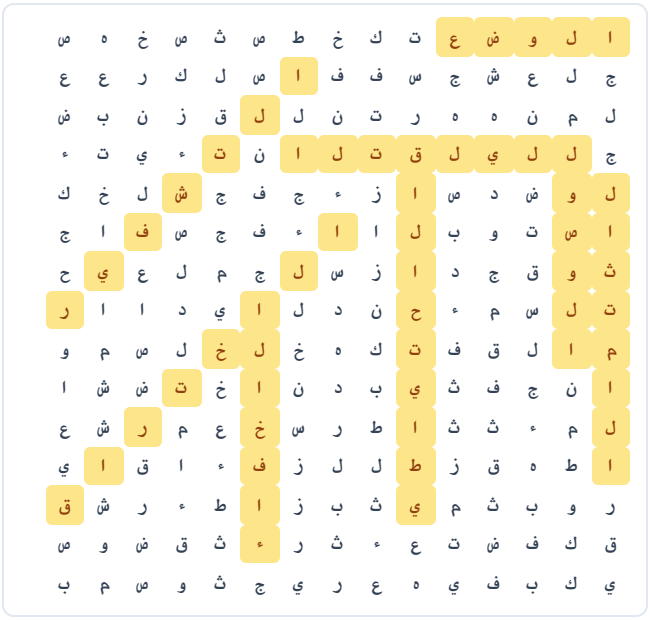
المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح التشفير ونسخة احتياطية والتقليل بكلماتهم الخاصة وإعطاء مثال على كل منها.

دراسات الحالة:
اطلب من الطلاب أن يدعموا توصياتهم بحقائق من ورقة العمل لا بآرائهم.

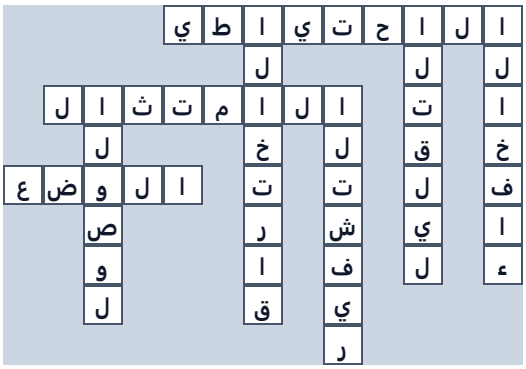
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات



حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

1 أفقي: الاحتياطي إنشاء نسخ آمنة خارج الموقع لاستعادة البيانات عند أعطال النظام (9 حروف)

4 أفقي: الامتثال استيفاء معايير تنظيمية مثل GDPR أو CCPA لإدارة معلومات المستخدمين الخاصة (8 حروف)

6 أفقي: الوضع الحالة الأمنية الجماعية وجاهزية الدفاع لسحابة المؤسسة (5 حروف)

عمودي

1 عمودي: الاخفاء استبدال أحرف حساسة في حقول قاعدة البيانات لحماية الهويات الشخصية (7 حروف)

2 عمودي: التقليل حصر جمع البيانات الشخصية في الحد الأدنى اللازم للعمليات (7 حروف)

3 عمودي: الاختراق حادث أمني يُنفذ فيه إلى بيانات محمية أو تُكشف دون تصريح (8 حروف)

4 عمودي: التشفير تحويل النص الصريح إلى نص مشفر غير مقروء ليبقى ما يُعترض من بيانات خاصاً (7 حروف)

5 عمودي: الوصول حصر أذونات القراءة والكتابة في قاعدة البيانات بأدوار المستخدمين الموثقين (6 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. شيافرتل — **التشفير**
2. اتليلقل — **التقليل**
3. واعضل — **الوضع**
4. مالثتالا — **الامتثال**
5. اتلييحاطا — **الاحتياطي**
6. وصاوللا — **الوصول**
7. اقترالخا — **الاختراق**
8. لخءاافا — **الاخفاء**

مفتاح تحدي الشيفرة السرية

"احم بياناتك الخاصة بضوابط آمنة"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: ترقية تشفير قواعد بيانات المؤسسات أثناء التخزين

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يخزّن متجر إلكتروني قواعد بيانات المعاملات على التخزين السحابي دون تشفير كامل للقرص. وقد صنّف تدقيق امتثال حديث ذلك على أنه خطر جسيم على أمن البيانات بموجب CCPA. صمّم بنية للاسترداد.
- الاستراتيجية والحل الموصى بهما: تنفيذ تشفير القرص الكامل AES-256 أثناء السكون على جميع أنظمة الملفات. واستخدام خدمة مركزية لإدارة المفاتيح (KMS) مع تدوير تلقائي، وفرض سياسات IAM صارمة للتحكم في الوصول لفك التشفير.

B دراسة الحالة 2: احتواء برمجيات الفدية واستعادة البيانات

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يشفّر هجوم فدية نشط محركات الأقراص الشبكية على شبكة محلية لشركة. وقد اكتشف المسؤول الإصابة مبكرًا. خطط لخطوات الاحتواء والاسترداد.
- الاستراتيجية والحل الموصى بهما: اعزل الجزء المخترق فورًا. وأعد تهيئة نقاط النهاية المتأثرة واستعدها من أحدث نسخة احتياطية غير متصلة بالشبكة من نوع الكتابة مرة واحدة والقراءة المتعددة (WORM). تحقق من سلامة النسخة الاحتياطية قبل إعادة توصيل الأنظمة.