الاسم: _____ التاريخ: _____ الدرجة: _____

أساسيات الأمن السيبراني والتهديدات عبر الإنترنت الوقاية

تهديدات الأمن السيبراني، وجدران حماية الشبكات، والمصادقة متعددة العوامل، وأطر الأمان

نظرة تعليمية عامة على أساسيات الأمن السيبراني

مرحبًا! ترشدك حزمة الأنشطة هذه عبر المبادئ الأساسية للأمن السيبراني والوقاية من التهديدات عبر الإنترنت. ستستكشف تهديدات البرمجيات الخبيثة والمصادقة متعددة العوامل وجدران حماية الشبكات وأطر الاستجابة للحوادث.

مؤمَّن
تشفير البيانات
معيار AES بطول 256 بت

متوافق
المعايير العالمية
أطر GDPR وCCPA

انعدام الثقة
سياسة الوصول
المصادقة متعددة العوامل

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**

افتح دليل VPN.com للأمن السيبراني

URL: https://www.vpn.com/cybersecurity/

خارطة طريقك لتعلّم أساسيات الأمن السيبراني

- تعرّف على النواقل الشائعة للبرمجيات الخبيثة والتصيّد الاحتيالي واختراق شبكات الشركات.
- طبّق ضوابط الأمن السيبراني القياسية، ومنها MFA وجدران الحماية والدفاع عن نقاط النهاية.
- قيّم إجراءات الاستجابة للحوادث للحد من آثار اختراق البيانات.
- حلّل عوامل المخاطر المؤسسية والمواءمة الأمنية وفق إرشادات NIST.
- هيّئ ممارسات النظافة الأمنية للتخفيف من حشو بيانات الاعتماد الآلي.

تعليمات دليل الأمن السيبراني

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 منع التهديدات. واختم بالنشاط الإضافي «فكّر بسرعة».

أساسيات الأمن السيبراني والوقاية من التهديدات (مقدمة)

يحمي الأمن السيبراني الشبكات والأنظمة والبيانات من الهجمات الرقمية غير المصرح بها. ويُعد تطوير عادات أمنية قوية وتهيئة جدران الحماية واشتراط المصادقة متعددة العوامل وتدريب الموظفين على التعرف على التهديدات مكونات أساسية للدفاع عن شبكة الشركة.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. 1. ما الهدف الرئيسي من هجوم التصيّد الاحتيالي؟
   - A. سرقة بيانات الاعتماد وبيانات المستخدم الحساسة
   - B. تحسين ظهور الموقع في محركات البحث
   - C. زيادة سعة عرض نطاق الشبكة
   - D. إدارة تكرار مركز البيانات الاحتياطي

2. 2. ما الآلية التي توفر أقوى حماية للحساب؟
   - A. المصادقة متعددة العوامل باستخدام مفاتيح عتادية
   - B. كلمات مرور معقدة تُحدَّث كل ثلاثين يومًا
   - C. تقييد تسجيل الدخول إلى الحساب بساعات العمل
   - D. إخفاء اسم مستخدم الحساب عن الأدلة العامة

3. 3. ما الذي يحدد حمولة الإصابة ببرمجيات الفدية؟
   - A. تشفير ملفات النظام والمطالبة بدفع مبلغ
   - B. تسجيل ضغطات المفاتيح بصمت وإرسالها إلى خوادم بعيدة
   - C. حقن إعلانات غير مصرح بها في المتصفحات
   - D. استخدام موارد المعالج المحلي لتعدين العملات المشفرة

4. 4. كيف يؤثر استغلال اليوم الصفري على الدفاعات الأمنية؟
   - A. يستهدف الثغرات المجهولة غير المصحَّحة
   - B. يعطّل جدار حماية الشركة تلقائيًا
   - C. يجبر النظام على إعادة تشغيل كاملة
   - D. لا يتطلب أي ميزانية للمعالجة

5. 5. ما الإطار الذي يحكم ضوابط أمان الشركات؟
   - A. إرشادات إطار NIST للأمن السيبراني
   - B. مواصفات مخطط مستندات W3C HTML5
   - C. أدلة تثبيت برامج تشغيل الطابعات
   - D. تعريفات بروتوكولات التوجيه الصادرة عن IETF

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6 tf

6. تستهدف هجمات التصيّد الاحتيالي حسابات البريد الإلكتروني الشخصية فقط.

صحيح ○ خطأ ○

7 سؤال 7 tf

7. تساعد المصادقة متعددة العوامل (MFA) في حظر هجمات حشو بيانات الاعتماد.

صحيح ○ خطأ ○

8 سؤال 8 tf

8. تفحص جدران الحماية حركة الشبكة لحجب الوصول غير المصرّح به إلى المنافذ.

صحيح ○ خطأ ○

9 سؤال 9 tf

9. تتطلب معالجة استغلالات اليوم الصفري تحديثات تعريفات مكافحة الفيروسات القياسية.

صحيح ○ خطأ ○

10 سؤال 10 tf

10. الطُعم (honeypot) خادم خدّاع يُستخدم لاستدراج مجرمي الإنترنت.

صحيح ○ خطأ ○

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. يثبت مسؤولو الشبكات _____ لتصفية الحركة الواردة.
2. يستخدم المهاجم _____ ثغرة اليوم الصفري لتجاوز تصحيحات النظام.
3. يرسل المهاجمون رسائل بريد مزورة لتنفيذ حملات _____ ضد الموظفين.
4. برمجيات الفدية شكل مدمر من _____ يقفل بيانات المستخدم.
5. يخفف تطبيق قواعد _____ القوية لكلمات المرور مخاطر سرقة بيانات الاعتماد.
6. لحماية الاتصالات الحساسة، يطبق المستخدمون بروتوكولات _____ .

بنك كلمات المفردات

استغلال | البرمجيات الخبيثة | التشفير | التصيد الاحتيالي | العوامل | الفدية | النظافة الأمنية | جدار حماية

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الأمان

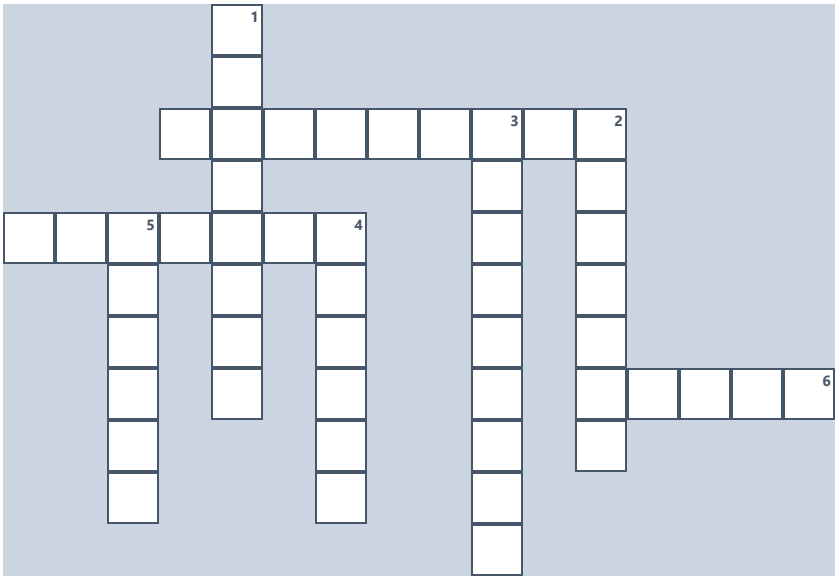
مطابقة التعريفات

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

1. تهديد برمجيات الفدية	A	إرشادات منظمة مثل NIST تُستخدم لإدارة المخاطر السيبرانية.
2. المصادقة متعددة العوامل	B	خطة منظمة للتعامل مع الاختراقات الأمنية والحد منها.
3. استغلال ثغرة يوم الصفر	C	حاجز شبكي يرشّح حركة المرور بناءً على قواعد الأمان.
4. مصيدة الخداع	D	برمجية خبيثة تشفّر البيانات وتطلب دفع مبلغ مالي مقابل فك التشفير.
5. جدار حماية الاختراق	E	استغلال ثغرة قبل إصدار الشركة المطورة تصحيحًا لها.
6. الاستجابة للحوادث	F	أفضل الممارسات لإدارة بيانات الاعتماد ومفاتيح المصادقة.
7. نظافة كلمات المرور	G	تحقق أمني يتطلب عاملين أو أكثر من عوامل المصادقة.
8. إطار الأمان	H	نظام خادع يُعدّ لاستدراج الجهات الخبيثة وتحليلها.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

2. استغلال ثغرة يُستهدف قبل إصدار الشركة المصنعة تصحيحاً لها (9)

4. أفضل الممارسات لإدارة بيانات الاعتماد ومفاتيح المصادقة (7)

6. نظام خداعي يُنصب لاستدراج الجهات الخبيثة وتحليلها (5)

عمودي

1. حاجز شبكي يرشح الحركة بحسب قواعد الأمان (8)

2. تحقق أمني يتطلب عاملين أو أكثر من عوامل المصادقة (7)

3. خطة منظمة للتعامل مع الاختراقات الأمنية والحد من آثارها (9)

4. برمجية خبيثة تشفر البيانات وتطلب دفعاً مالياً مقابل فك التشفير (6)

5. إرشادات منظمة مثل NIST تُستخدم لإدارة المخاطر السيبرانية (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

2 أفقي: استغلال ثغرة يُستهدف قبل إصدار الشركة المصنعة تصحيحاً لها (9 حروف):

4 أفقي: أفضل الممارسات لإدارة بيانات الاعتماد ومفاتيح المصادقة (7 حروف):

6 أفقي: نظام خداعي يُنصب لاستدراج الجهات الخبيثة وتحليلها (5 حروف):

عمودي

1 عمودي: حاجز شبكي يرشح الحركة بحسب قواعد الأمان (8 حروف):

2 عمودي: تحقق أمني يتطلب عاملين أو أكثر من عوامل المصادقة (7 حروف):

3 عمودي: خطة منظمة للتعامل مع الاختراقات الأمنية والحد من آثارها (9 حروف):

4 عمودي: برمجية خبيثة تشفر البيانات وتطلب دفعاً مالياً مقابل فك التشفير (6 حروف):

5 عمودي: إرشادات منظمة مثل NIST تُستخدم لإدارة المخاطر السيبرانية (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.

ش	ة	ع	غ	ك	ة	د	ا	ة	ك	ط	ت	م	س	د
ف	ل	م	ط	ك	ة	ك	ل	ف	ف	ا	ت	ه	م	ن
ح	ص	ع	ش	ب	ا	ب	ف	ا	ت	ل	ق	ة	ص	ش
ة	غ	ط	ص	ة	ه	ص	د	ظ	ج	ا	ل	ع	ش	ج
ب	س	ل	ع	ع	ا	ص	ي	ن	ك	ط	ق	ر	ج	ع
ا	ع	ا	ك	ل	ل	م	ة	ل	ه	ا	ن	ر	د	ت
ج	م	ك	ف	ز	ا	م	ب	ا	ي	ر	ج	ن	ا	ظ
ت	و	ت	ظ	ي	س	د	ص	ل	ز	ظ	ج	ع	ر	ج
س	ل	ة	ق	ت	ت	ه	ب	ع	ا	ظ	ف	ج	ن	ص
ا	ا	ج	ف	ج	غ	د	ر	و	س	ج	ل	ك	ا	ع
ل	ح	س	م	ظ	ل	ن	د	ا	ل	و	ح	ا	ر	ا
ا	ل	ق	ع	ك	ا	ه	ة	م	ك	ش	م	ه	ي	م
ت	ع	غ	ب	د	ل	م	ة	ل	ي	س	ا	ل	ظ	غ
غ	ص	ر	س	ع	ل	ش	ط	ط	ن	ق	ر	ك	ل	ر
ظ	ا	ف	و	د	و	ب	غ	م	غ	ب	ر	ط	ظ	ر

قائمة كلمات المفردات

الفدية العوامل الاستغلال الطعم جدارناري الاستجابة النظافة الاطار

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. الفدية
B. العوامل
C. الاستغلال
D. الطعم
E. جدارناري
F. الاستجابة
G. النظافة
H. الاطار

التعريفات وحقول المطابقة
1. حاجز شبكي يرشح الحركة بحسب قواعد الأمان.
2. خطة منظمة للتعامل مع الاختراقات الأمنية والحد من آثارها.
3. برمجية خبيثة تشفر البيانات وتطلب دفعاً مالياً مقابل فك التشفير.
4. تحقق أمني يتطلب عاملين أو أكثر من عوامل المصادقة.
5. أفضل الممارسات لإدارة بيانات الاعتماد ومفاتيح المصادقة.
6. إرشادات منظمة مثل NIST تُستخدم لإدارة المخاطر السيبرانية.
7. استغلال ثغرة يُستهدف قبل إصدار الشركة المصنعة تصحيحاً لها.
8. نظام خداعي يُنصب لاستدراج الجهات الخبيثة وتحليلها.

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. ف ا د ي ة ل
2. ل ا ا س ل غ ل ت ا
3. ر د ج ن ا ي ر ا
4. ة ل ا ظ ف ا ن
5. ا ل و ع ا م ل
6. ع ا ط م ل
7. ج ا ب ة ا س ل ت ا
8. ا ر ا ا ط ل

نشاط إضافي: فكّر بسرعة

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

1	وظائف في الأمن السيبراني		
2	أسباب لتحديث البرامج		
3	أشياء يستطيع جدار الحماية حظرها		
4	علامات تحذيرية في البريد الإلكتروني		
5	أشياء تحتفظ بنسخة احتياطية منها		
6	أنواع شهيرة من الهجمات السيبرانية		
7	أشياء يمكن أن يستدرجها فخ المخترقين (honeypot)		
8	معلومات لا ينبغي أن تشاركها أبدًا		
9	علامات إصابة الحاسوب		
10	أفلام أو مسلسلات عن المخترقين		
11	طبقات أمنية يمكنك بناؤها		
12	أشياء تتدرب عليها في تمرين أمني		
13	أدوات أمنية تعرفها		
14	أشخاص يمكنك طلب مساعدة تقنية منهم		
15	كلمات تبدأ بـ "سيبراني"		

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: استراتيجية التعافي من برمجيات الفدية



السيناريو: أصيبت شبكة مؤسسية ببرنامج فدية أقفل قواعد بيانات حيوية. يطالب المهاجمون بدفع 100,000 دولار بعملة مشفرة. لدى الشركة نسخ احتياطية غير متصلة بالإنترنت عمرها 24 ساعة.

سؤال للنقاش: حلّل مخاطر الدفع، وقيّم استراتيجية التعافي.

دراسة الحالة 2: الدفاعات ضد حشو بيانات الاعتماد



السيناريو: تتعرض خدمة عبر الإنترنت لهجوم حشو بيانات الاعتماد، حيث يختبر المخترقون ملايين أزواج اسم المستخدم وكلمة المرور المسروقة من مواقع أخرى.

سؤال للنقاش: اشرح آلية هذا الهجوم، ولخّص نظامين دفاعيين.

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	21	8	1	14	24	23	1	2
22	24	1	17	25		25	24	1

23	24	1	27	18	23	1
29	8	8	18	3	24	

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 الهدف الرئيسي من الأمن السيبراني؟

الهدف الرئيسي هو حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به والهجمات والأضرار العرضية.

Q2: كيف يختلف التصيّد الاحتيالي عن التصيّد الموجّه؟

التصيّد الاحتيالي حملة بريد إلكتروني واسعة تستهدف مستخدمين عشوائيين، بينما يستهدف التصيّد الموجّه أفرادًا محددين باستخدام بيانات شخصية.

Q3: ما جدار حماية الشبكة؟

جدار الحماية نظام أمان للشبكة يراقب حركة المرور الواردة والصادرة ويرشّحها استنادًا إلى قواعد أمان محددة مسبقًا.

Q4: لماذا تُعد المصادقة متعددة العوامل (MFA) ضرورية؟

تضيف المصادقة متعددة العوامل (MFA) طبقة دفاع بالغة الأهمية، فتمنع الوصول حتى لو سرق المهاجمون بيانات اعتماد كلمة المرور الأساسية أو كسروها.

Q5: ما الذي يعرّف فيروس الحاسوب؟

الفيروس برمجية خبيثة ذاتية النسخ تلتصق بالملفات السليمة وتنتشر عبر الأنظمة بمجرد تنفيذها.

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

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: كيف تقفل برامج الفدية البيانات المحلية؟

تستخدم برامج الفدية خوارزميات تشفيرية لتشفير ملفات المستخدم، فتجعلها غير قابلة للقراءة إلى أن يُطبَّق مفتاح فك التشفير.

Q7: ما الثغرة من نوع اليوم الصفري (zero-day)؟

ثغرة اليوم الصفري (zero-day) خلل أمني في البرمجيات لا يعرفه المورّد، فلا يتبقى وقت لتطوير تصحيح قبل الاستغلال.

Q8: ما دور إطار NIST؟

يوفر إطار NIST إرشادات ومعايير طوعية لمساعدة المؤسسات على إدارة مخاطر الأمن السيبراني والحد منها.

Q9: ما خطة الاستجابة للحوادث الأمنية؟

هو مجموعة موثقة من الإجراءات لاكتشاف الاختراقات الأمنية وتعرض الشبكة للخطر واحتوائها والتعافي منها.

Q10: كيف تستغل الهندسة الاجتماعية المستخدمين؟

تستخدم الهندسة الاجتماعية التلاعب النفسي لخداع الموظفين لكشف كلمات المرور أو تنزيل ملفات خبيثة.

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

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

Q1: كيف يُغرق هجوم DDoS خوادم الويب؟

يُنسّق هجوم DDoS ملايين أجهزة شبكات الروبوت المخترقة لإغراق خادم بحركة المرور، فيستنزف حدود النطاق الترددي والمعالج.

Q2: ما الفرق بين التشفير المتماثل وغير المتماثل؟

يستخدم التشفير المتماثل مفتاحًا واحدًا للتشفير وفك التشفير، بينما يستخدم التشفير غير المتماثل زوج مفاتيح عامًا وخاصًا.

Q3: كيف ينفّذ المخترقون هجمات حقن SQL؟

يدخل المهاجمون أوامر SQL خبيثة في حقول النماذج لخداع قاعدة البيانات الخلفية وحملها على إفشاء سجلات مستخدمين غير مصرّح بها.

Q4: ما الحركة الجانبية (lateral movement) في اختراقات الشبكات؟

هي التقنية التي يستغل فيها المهاجمون الوصول الأولي إلى الخادم لاختراق أنظمة مترابطة أخرى على الشبكة الداخلية.

Q5: كيف يعيد انتحال DNS توجيه حركة الويب؟

يغيّر انتحال DNS سجلات ذاكرة خادم الأسماء المؤقتة، فيوجّه المستخدمين الشرعيين إلى مواقع خبيثة مشابهة بدلًا من النطاقات المقصودة.

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

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

Q6: ما رمز الأمان المادي؟

هو جهاز مادي (مثل YubiKey) يولّد براهين مصادقة تشفيرية، ويوفر أقصى دفاع ضد التصيّد الاحتيالي عن بُعد.

Q7: كيف تستخدم فرق الأمن أنظمة الإغراء (honeypots) الخادعة؟

تنشر الفرق خوادم خداعية غير إنتاجية لاكتشاف عمليات الاختراق مبكرًا وتحليل أنماط هجوم الجهات غير المصرح لها.

Q8: ما مبدأ الامتيازات الأدنى؟

هو معيار أمني يقضي بتقييد حقوق وصول المستخدم إلى الحد الأدنى المطلق اللازم لأداء أدوارهم الوظيفية.

Q9: كيف يستغل هجوم الوسيط (Man-in-the-Middle) الاتصالات؟

يعترض مهاجم الاتصالات بين جهازين على شبكات غير مشفّرة ويعدّلها، فيسرق رموز الجلسات وبيانات الاعتماد.

Q10: ما مؤشرات الاختراق (IOCs)؟

مؤشرات الاختراق (IOCs) أدلة جنائية رقمية، مثل تعديلات غير معتادة في السجل أو حركة IP مشبوهة، تدل على اختراق النظام.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

يفحص المهاجمون الإنترنت باستمرار بحثًا عن خوادم ضعيفة ويرسلون رسائل تصيّد احتيالي إلى صناديق بريد الموظفين.

2. نظرة على الأمن

الخطأ البشري، مثل النقر على روابط التصيّد الاحتيالي، عامل شائع في اختراقات البيانات، ولهذا يهم التدريب.

3. نظرة على الأمن

تشمل تكاليف اختراق البيانات الغرامات القانونية وفقدان العملاء والتحقيق والإصلاح، وقد تصل إلى ملايين الدولارات.

4. نظرة على الأمن

المصادقة متعددة العوامل المقاومة للتصيّد، مثل مفاتيح الأمان المادية، هي أقوى أنواع MFA والمعيار الذي تحث عليه CISA. [2]

5. نظرة على الأمن

لا تزال برامج الفدية تشكّل تهديدًا كبيرًا لشبكات المؤسسات، وتحث CISA على اعتماد نسخ احتياطية مشفرة وغير متصلة بالإنترنت كدفاع رئيسي. [4]

6. نظرة على الأمن

يتضمن إطار NIST للأمن السيبراني 2.0 (2024) ست وظائف أساسية: الحوكمة، التعريف، الحماية، الكشف، الاستجابة، التعافي. [1]

7. رؤية حول الأمان

تختبر روبوتات حشو بيانات الاعتماد أزواج أسماء المستخدمين وكلمات المرور المسرّبة على نطاق واسع مقابل بوابات تسجيل الدخول المصرفية والتجارة الإلكترونية.

8. رؤية حول الأمان

توجد أسواق لاستغلالات اليوم الصفري في أنحاء العالم، حيث قد تُباع الثغرات عالية الخطورة بمبالغ كبيرة قبل إصلاحها.

9. رؤية حول الأمان

يبلّغ نظام الطُعم (honeypot) عن تنبيهات التسلل فورًا لأن المستخدمين الشرعيين ليس لديهم سبب للوصول إليه.

10. نظرة على الأمن

يشفّر بروتوكول Transport Layer Security (TLS) جلسات المتصفح، مما يمنع التقاط الحزم على شبكات Wi-Fi العامة.

المراجع والمصادر التقنية

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

المراجع الأكاديمية والصناعية

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

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

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 **هجمات التصيّد الاحتيالي** التصيّد الاحتيالي — الإجابة الصحيحة: A

ملاحظة للمعلم

تحاول حملات التصيّد الاحتيالي سرقة بيانات الاعتماد وبيانات المستخدمين الحساسة باستخدام رسائل بريد إلكتروني منتحلة. المرجع: OWASP Secure Configuration.

2 **حماية الحساب** مفتاح MFA — الإجابة الصحيحة: A

ملاحظة للمعلم

توفر المصادقة متعددة العوامل (MFA) باستخدام رموز عتادية أقوى دفاع للوصول إلى الحساب. المصدر: NIST Digital Identity.

3 **تهديد برامج الفدية** برامج الفدية — الإجابة الصحيحة: A

ملاحظة للمعلم

تشفّر برامج الفدية الأنظمة والبيانات الحيوية وتطالب بدفع عملة مشفرة مقابل مفاتيح فك التشفير. المصدر: Center for Internet Security (CIS).

4 **ثغرة اليوم الصفري** اليوم الصفري — الإجابة الصحيحة: A

ملاحظة للمعلم

تستغل تهديدات اليوم الصفري ثغرات أمنية غير مُصلّحة وغير معروفة قبل أن يتوفر إصلاح من المورّد. الاستشهاد: OWASP Secure Configuration.

5 **أطر الأمان** الأطر — الإجابة الصحيحة: A

ملاحظة للمعلم

توفر أطر مثل NIST إرشادات منظمة تساعد المؤسسات على إدارة المخاطر السيبرانية والحد منها. المصدر: NIST Digital Identity.

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 **التصيّد الاحتيالي الموجّه** التصيّد الاحتيالي

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

تستهدف هجمات التصيّد الاحتيالي الشبكات المؤسسية والحسابات الشخصية معًا لتوسيع ناقلات الاستغلال. المرجع: OWASP Secure Configuration.

7 **السؤال 7**

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تتطلب MFA عاملًا ثانيًا، لذا فإن كلمة مرور مسروقة وحدها لا تكفي عادةً لتسجيل الدخول.

8 **جدار حماية حركة المرور** جدار الحماية

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تفحص جدران الحماية حركة البيانات على منافذ شبكة محددة وتحجبها لتصفية الاتصالات غير المصرّح بها. المصدر: Center for Internet Security (CIS).

9 **الاستجابة لهجمات اليوم الصفري** اليوم الصفري

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

تتطلب معالجة ثغرات اليوم الصفري ترقيعات برمجية وترشيح WAF لأن التوقيعات غير موجودة بعد. المصدر: OWASP Secure Configuration.

10 **مصائد العسل الخادعة** مصيدة العسل

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

مصائد العسل خوادم خادعة يستخدمها فرق الأمان لاستدراج الجهات الخبيثة والتنبيه إليها ودراستها. المصدر: Center for Internet Security (CIS).

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

D 1. تهديد برمجيات الفدية	G 2. المصادقة متعددة العوامل	E 3. استغلال ثغرة يوم الصفر	H 4. مصيدة الخداع
C 5. جدار حماية الاختراق	B 6. الاستجابة للحوادث	F 7. نظافة كلمات المرور	A 8. إطار الأمان

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 جدار حماية	2 استغلال	3 التصيد الاحتيالي	4 البرمجيات الخبيثة
5 النظافة الأمنية	6 التشفير		

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

1 E – جدارناري	2 F – الاستجابة	3 A – الفدية	4 B – العوامل
5 G – النظافة	6 H – الاطار	7 C – الاستغلال	8 D – الطعم

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح تهديد برمجيات الفدية والمصادقة متعددة العوامل واستغلال ثغرة يوم الصفر بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

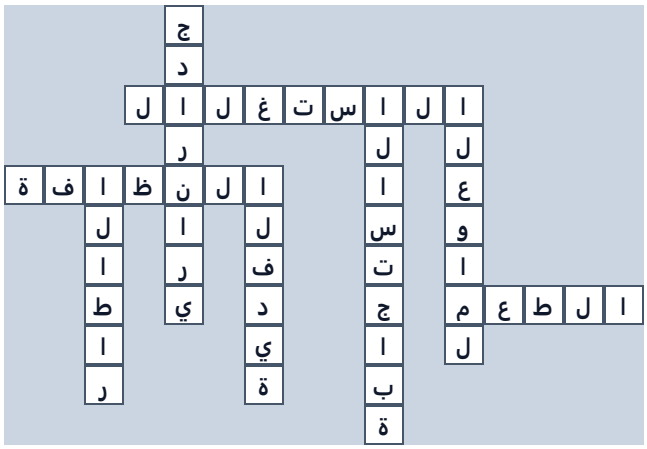
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

ش	ة	ع	غ	ك	ة	د	ا	ة	ك	ط	ت	م	س	د
ف	ل	م	ط	ك	ة	ك	ل	ف	ف	ا	ت	ه	م	ن
ح	س	ع	ش	ب	ا	ب	ف	ا	ت	ل	ق	ة	ص	ش
ة	غ	ط	ص	ه	ة	ص	د	ظ	ج	ا	ل	ع	ش	ج
ب	س	ل	ع	ع	ا	ص	ي	ن	ك	ط	ق	ر	ج	ع
ا	ع	ا	ك	ل	ل	م	ة	ل	ه	ا	ن	ر	د	ت
ج	م	ك	ف	ز	ا	م	ب	ا	ي	ر	ج	ن	ا	ظ
ت	و	ت	ظ	ي	س	د	ص	ل	ز	ظ	ج	ع	ر	ج
س	ل	ة	ق	ت	ت	ه	ب	ع	ا	ظ	ف	ج	ن	ص
ا	ا	ج	ف	ج	غ	د	ر	و	س	ج	ل	ك	ا	ع
ل	ح	س	م	ظ	ل	ن	د	ا	ل	و	ح	ا	ر	ا
ا	ل	ق	ع	ك	ا	ه	ة	م	ش	ك	م	ه	ي	م
ت	ع	غ	ب	د	ل	م	ة	ل	ي	س	ا	ظ	ل	غ
غ	ص	ر	س	ع	ل	ش	ط	ط	ن	ق	ر	ك	ل	ر
ظ	ا	ف	و	د	و	ب	غ	م	غ	ب	ر	ط	ظ	ر

حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

2 أفقي: الاستغلال استغلال ثغرة يُستهدف قبل إصدار الشركة المصنعة تصحيحاً لها (9 حروف)

4 أفقي: النظافة أفضل الممارسات لإدارة بيانات الاعتماد ومفاتيح المصادقة (7 حروف)

6 أفقي: الطعم نظام خداعي يُنصب لاستدراج الجهات الخبيثة وتحليلها (5 حروف)

عمودي

1 عمودي: جدارناري حاجز شبكي يرشح الحركة بحسب قواعد الأمان (8 حروف)

2 عمودي: العوامل تحقق أمني يتطلب عاملين أو أكثر من عوامل المصادقة (7 حروف)

3 عمودي: الاستجابة خطة منظمة للتعامل مع الاختراقات الأمنية والحد من آثارها (9 حروف)

4 عمودي: الفدية برمجية خبيثة تشفر البيانات وتطلب دفعاً مالياً مقابل فك التشفير (6 حروف)

5 عمودي: الاطار إرشادات منظمة مثل NIST تُستخدم لإدارة المخاطر السيبرانية (6 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. فاديةل → **الفدية**
2. لااسلغلتا → **الاستغلال**
3. ردجنايرا → **جدارناري**
4. ةلاظفان → **النظافة**
5. الوعامل → **العوامل**
6. عاطمل → **الطعم**
7. جابةاسلتا → **الاستجابة**
8. اراطل → **الاطار**

مفتاح تحدي الشيفرة السرية

"أمن نظامك بالمصادقة متعددة العوامل"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: استراتيجية التعافي من برمجيات الفدية

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: أصيبت شبكة شركة ببرمجية فدية قفلت قواعد بيانات حيوية. يطالب المهاجمون بدفع 100,000 دولار بعملة مشفرة. لدى الشركة نسخ احتياطية غير متصلة بالشبكة عمرها 24 ساعة.
- الاستراتيجية والحل الموصى بهما: مخاطر الدفع: الدفع لا يضمن فك تشفير الملفات، ويصنّف الشركة هدفًا يدفع، ويموّل النشاط الإجرامي. استراتيجية الاسترداد: ينبغي للفريق عزل المضيفات المصابة، ومسح الخوادم المخترقة، واستعادة البيانات من النسخ الاحتياطية غير المتصلة. ويجب عليه ترقيع ناقل الوصول الأولي (التصيّد الاحتيالي أو الثغرة) لمنع إعادة الإصابة فورًا.

B دراسة الحالة 2: الدفاعات ضد حشو بيانات الاعتماد

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: تتعرض خدمة إلكترونية لهجوم حشو بيانات الاعتماد، حيث يختبر المخترقون ملايين أزواج اسم المستخدم/كلمة المرور المسروقة من مواقع أخرى.
- الاستراتيجية والحل الموصى بهما: الآلية: يستغل المهاجمون إعادة استخدام كلمات المرور عبر المواقع باستخدام روبوتات آلية لتسجيل الدخول إلى حسابات المستخدمين. وسائل الدفاع: 1. تحظر المصادقة متعددة العوامل (MFA) محاولات تسجيل الدخول حتى لو كانت كلمة المرور صحيحة. 2. يحظر تطبيق تحديد المعدل واختبارات CAPTCHA حركة الروبوتات الآلية من إغراق نقاط تسجيل الدخول.