الاسم: _____ التاريخ: _____ الدرجة: _____

هجمات برامج الفدية والأعمال التعافي

تنفيذ الحمولة، وتشفير الملفات، والنسخ الاحتياطية دون اتصال، وإجراءات الاحتواء، والتعافي من الكوارث.

نظرة تعليمية عامة على هجمات برامج الفدية

مؤمّن
تشفير البيانات
معيار AES بطول 256 بت

متوافق
المعايير العالمية
أطر GDPR وCCPA

انعدام الثقة
سياسة الوصول
المصادقة متعددة العوامل

مرحبًا! ترشدك حزمة الأنشطة هذه عبر هجمات برامج الفدية والتعافي في الأعمال. ستستكشف تنفيذ الحمولة وتشفير الملفات والنسخ الاحتياطية غير المتصلة واحتواء التهديد ومدفوعات العملات المشفّرة وخطط التعافي من الكوارث.

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/ransomware-attack/

خارطة طريقك لتعلّم التعافي من برامج الفدية

- ميّز بين أحصنة طروادة وبرمجيات الفدية وبرمجيات التجسس.
- حلّل الملفات الخبيثة داخل بيئات معزولة آمنة.
- صياغة إجراءات سريعة لعزل الشبكة واحتواء الحادث.

تعليمات دليل هجمات برامج الفدية

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 التعافي من برامج الفدية. واختم بالنشاط الإضافي «فكّر بسرعة».

هجمات برامج الفدية والتعافي من الكوارث (مقدمة)

تقفل حمولات برامج الفدية تخزين النظام تشفيريًا وتطالب بدفعات بعملات مشفرة مقابل مفاتيح فك التشفير. ويشمل الحد من هذا التهديد قواعد عزل الشبكة، وتحليل البرمجيات الخبيثة في بيئات معزولة، ونسخًا احتياطية باردة قوية معزولة عن الشبكة.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. 1. ما الآلية الرئيسية لهجوم برمجيات الفدية؟
   - A. تشفير تشفيري لملفات المستخدم لحرمانه من الوصول إلى النظام
   - B. حقن أوامر SQL خبيثة في حقول النماذج
   - C. التقاط حزم الشبكة على اتصال Wi-Fi عام
   - D. تزوير ترويسات البريد الإلكتروني لتجاوز التحقق من SPF

2. 2. ما هي النسخة الاحتياطية غير المتصلة (الباردة)؟
   - A. نسخة تخزين مفصولة عن الشبكة لحمايتها من انتشار البرمجيات الخبيثة
   - B. نسخة احتياطية مخزّنة على القرص الصلب لخادم الويب الرئيسي
   - C. ذاكرة مؤقتة لسجلات سجل النظام
   - D. أداة إدارية تُستخدم لإعادة تعيين كلمات مرور المستخدمين

3. 3. كيف ينبغي لفرق الأمان عزل الأنظمة المصابة أثناء هجوم فدية؟
   - A. فصل كابلات الشبكة وتعطيل الواجهات اللاسلكية فورًا
   - B. ترقية قاعدة بيانات تواقيع مضاد الفيروسات
   - C. إيقاف خادم DNS الأساسي
   - D. إعادة تسمية امتدادات الملفات المخترقة

4. 4. لماذا تنصح الجهات الأمنية بعدم دفع فدية برمجيات الفدية؟
   - A. دفع الأموال يشجع المهاجمين ولا يضمن تسليم مفتاح فك التشفير
   - B. يبطل جميع وثائق تأمين الشركة تلقائيًا
   - C. يخطر كل عميل بالبريد الإلكتروني تلقائيًا
   - D. يُتلف ملفات النسخ الاحتياطي المتبقية للنظام

5. 5. ما هي خطة التعافي من الكوارث (DRP)؟
   - A. عملية منظمة لاستعادة العمليات والبيانات بعد اختراق النظام
   - B. إعداد جدار حماية يربط منافذ الشبكة الواردة
   - C. مخطط قاعدة بيانات يسرد صلاحيات المستخدمين الإدارية
   - D. بروتوكول مصادقة البريد الإلكتروني يرفض النطاقات المنتحلة

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. يمكن أن تنتشر حمولات برامج الفدية بسهولة إلى النسخ الاحتياطية المتصلة بالشبكة.

صحيح ○ خطأ ○

7 سؤال 7

7. دفع فدية العملات المشفرة يضمن نجاح فك تشفير الملفات.

صحيح ○ خطأ ○

8 سؤال 8

8. يساعد فصل الأنظمة المصابة عن الشبكة في إيقاف انتشار برنامج الفدية إلى الأنظمة المجاورة.

صحيح ○ خطأ ○

9 سؤال 9

9. لا تستخدم برمجيات الفدية التشفير المتماثل أبدًا لتشفير تخزين النظام.

صحيح ○ خطأ ○

10 سؤال 10

10. يُعد اختبار إجراءات استعادة البيانات بانتظام جزءًا أساسيًا من التعافي من الكوارث.

صحيح ○ خطأ ○

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. يعتمد حجب الوصول إلى الملفات المحلية على عملية _____ التي تستخدم خوارزميات تشفيرية.
2. الشفرة الخبيثة النشطة المنفذة على النظام هي _____ .
3. تمثل نسخ التخزين المنفصلة خارج الموقع نسخا احتياطية _____ آمنة.
4. يتطلب إيقاف انتشار البرمجيات الخبيثة _____ لنقاط نهاية الشبكة.
5. الدفعة بالعملة المشفرة التي يطلبها المجرمون الإلكترونيون هي _____ .
6. تمثل استعادة ملفات البيانات التشغيلية _____ من الكوارث.

بنك كلمات المفردات

التشفير التعافي الحمولة العزل الفدية الكوارث باردة طروادة

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الأمان

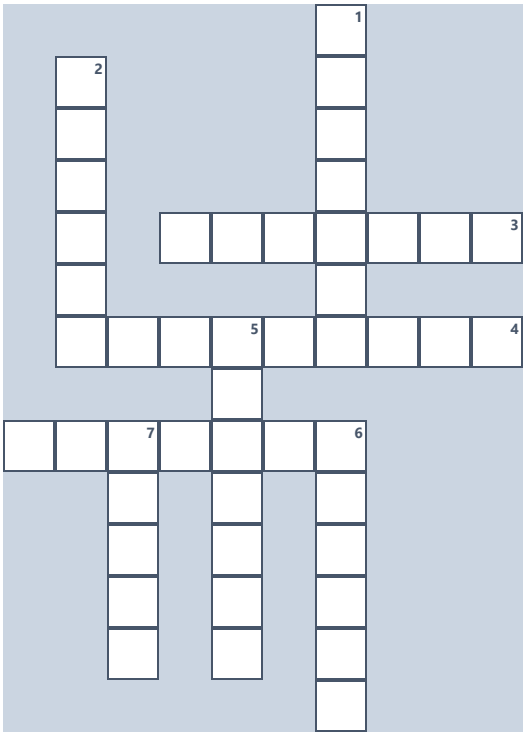
مطابقة التعريفات

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

1. التشفير		A	فصل أنظمة الشبكة المصابة.
2. الحمولة		B	ملف خبيث متنكر في هيئة ملف سليم.
3. نسخة احتياطية غير متصلة		C	قفل الملفات تشفيريًا.
4. العزل		D	حدث تعطل كبير في النظام.
5. فدية		E	تشغيل برمجيات خبيثة.
6. التعافي		F	نسخة غير متصلة ومفصولة.
7. الكارثة		G	استعادة قاعدة البيانات من النسخة الاحتياطية.
8. حصان طروادة		H	طلب صرف مفتاح تشفيري.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

3. حدث تعطل كبير في النظام (7)

4. نسخة غير متصلة بالشبكة (9)

6. استعادة قاعدة البيانات من النسخة الاحتياطية (7)

عمودي

1. تنفيذ برمجية خبيثة (7)

2. ملف خبيث متنكر في هيئة ملف سليم (6)

5. قفل الملفات تشفيريا (7)

6. طلب دفع مقابل المفتاح التشفيري (6)

7. فصل أنظمة الشبكة المصابة (5)

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

3 أفقي: حدث تعطل كبير في النظام (7 حروف):

4 أفقي: نسخة غير متصلة بالشبكة (9 حروف):

6 أفقي: استعادة قاعدة البيانات من النسخة الاحتياطية (7 حروف):

عمودي

1 عمودي: تنفيذ برمجية خبيثة (7 حروف):

2 عمودي: ملف خبيث متنكر في هيئة ملف سليم (6 حروف):

5 عمودي: قفل الملفات تشفيريا (7 حروف):

6 عمودي: طلب دفع مقابل المفتاح التشفيري (6 حروف):

7 عمودي: فصل أنظمة الشبكة المصابة (5 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.

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

قائمة كلمات المفردات

التشفير الحمولة نسخةباردة العزل الفدية التعافي الكوارث طروادة

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. الحمولة
C. نسخةباردة
D. العزل
E. الفدية
F. التعافي
G. الكوارث
H. طروادة

التعريفات وحقول المطابقة
1. نسخة غير متصلة بالشبكة.
2. ملف خبيث متنكر في هيئة ملف سليم.
3. قفل الملفات تشفيريا.
4. طلب دفع مقابل المفتاح التشفيري.
5. فصل أنظمة الشبكة المصابة.
6. حدث تعطل كبير في النظام.
7. تنفيذ برمجية خبيثة.
8. استعادة قاعدة البيانات من النسخة الاحتياطية.

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. ة ن د ة س ا ر ب خ
3. ا ف د ة ي ل
4. ث ل ا و ر ا ك
5. و ة م ح ا ل ل
6. ز ا ع ل ل
7. ا ف ا ي ل ع ت
8. و ة ط د ا ر

نشاط إضافي: فكّر بسرعة

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

1. معلومات لا ينبغي أن تشاركها أبدًا
2. أجهزة يمكن اختراقها
3. أسباب عدم دفع الفدية
4. عادات آمنة يمكنك البدء بها اليوم
5. أدوات أمنية تعرفها
6. طرق لحماية حساباتك
7. علامات إصابة الحاسوب
8. أماكن لحفظ نسخة احتياطية
9. ملفات لا تريد فقدانها أبدًا
10. طرق انتشار برامج الفدية
11. أشياء تفعلها في الساعة الأولى من الهجوم
12. أشخاص تتواصل معهم أثناء الهجوم
13. أشياء يمكن أن يقفلها برنامج الفدية
14. كلمات متعلقة بالأمن السيبراني
15. جهات كثيرًا ما تُستهدف

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: احتواء حمولة برمجيات الفدية في المؤسسات



السيناريو: تعرضت الشبكة المحلية لشركة لاختراق من برمجية فدية نشطة. بدأت خوادم الملفات الرئيسية بعرض امتدادات ملفات بصيغة .locked.

سؤال للنقاش: فصّل خطوات الاحتواء، ولخّص بروتوكول استعادة البيانات.

دراسة الحالة 2: تقييم بنى النسخ الاحتياطي دون اتصال



السيناريو: تريد مؤسسة تصميم استراتيجية للنسخ الاحتياطي للبيانات تقلل خطر اختراق النسخ الاحتياطية، حتى لو اختُطفت الشبكة المحلية الأساسية بالكامل بواسطة برنامج فدية.

سؤال للنقاش: صمّم نظام خزنة تخزين نسخ احتياطية آمنة غير متصلة.

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

10	20	13	24	23	1		24	1	17	25	23	1		8	18	3	12	1

29	8	10	1	2		29	7	12	25		25	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 برمجيات الفدية؟

برامج الفدية هي برمجيات خبيثة مصممة لحجب الوصول إلى أنظمة الحاسوب أو ملفاته إلى أن يُدفع مبلغ فدية.

Q2: كيف تنتشر برمجيات الفدية؟

عبر مرفقات رسائل التصيّد الاحتيالي، وثغرات البرمجيات غير المُرقَّعة، وأنظمة الوصول عن بُعد المخترقة. [1]

Q3: لماذا يُطلب الدفع بالعملات المشفرة؟

توفر العملات المشفرة مثل Bitcoin إخفاءً نسبيًا للهوية، مما يصعّب على جهات إنفاذ القانون تتبع الأموال.

Q4: هل يحظر برنامج مكافحة الفيروسات برامج الفدية؟

نعم، لكن مكافح الفيروسات المعتمد على التواقيع قد يفشل أمام حمولات برمجيات الفدية الجديدة من نوع يوم الصفر.

Q5: ما النسخة الاحتياطية المعزولة عن الشبكة (air-gapped)؟

نسخة احتياطية لا ترتبط فعليًا أو منطقيًا بالشبكة الرئيسية، مما يحميها من الانتشار.

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

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: ما الابتزاز المزدوج؟

عندما لا يكتفي المهاجمون بتشفير الملفات بل يسرقون أيضًا بيانات حساسة للتهديد بتسريبها علنًا إذا لم يُدفع المقابل.

Q7: ما أداة فك التشفير (decryptor)؟

أداة برمجية تحتوي على المفتاح التشفيري اللازم لاستعادة الملفات المقفلة إلى نص صريح.

Q8: كيف تكتشف برامج الفدية مبكرًا؟

بمراقبة أنظمة الملفات بحثًا عن نشاط تعديل وإعادة تسمية مفاجئ وواسع النطاق للملفات.

Q9: ما دور التأمين؟

يمكن أن يساعد التأمين السيبراني في تغطية تكاليف التعافي، لكن شروط التغطية وقواعد دفع الفدية تختلف بحسب الوثيقة.

Q10: هل يجب أن أعيد تشغيل نظام مصاب؟

لا، فقد تؤدي إعادة التشغيل إلى إتلاف أدلة الذاكرة المتطايرة؛ اعزل الجهاز عن الشبكة بدلًا من ذلك. [1]

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

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

Q1: كيف تستخدم برمجيات الفدية التشفير غير المتماثل؟

يستخدم مفتاحًا عامًا مضمّنًا في البرمجية الخبيثة لتشفير الملفات، ويتطلب المفتاح الخاص للمهاجم لفك تشفيرها.

Q2: لماذا يُستخدم التشفير المتماثل أيضًا؟

التشفير المتماثل (مثل AES) سريع ويمكنه قفل قواعد بيانات ضخمة في دقائق، بينما تؤمّن المفاتيح غير المتماثلة مفتاح AES.

Q3: ما التجزئة المنطقية؟

تقسيم الشبكات إلى مناطق معزولة، ما يمنع البرمجيات الخبيثة من الانتشار جانبيًا من عقد محطات العمل إلى الخوادم الأساسية.

Q4: ما التخزين WORM؟

وسائط الكتابة مرة واحدة والقراءة المتعددة، التي تمنع حمولات برمجيات الفدية من تعديل بيانات النسخ الاحتياطي أو الكتابة فوقها أو حذفها.

Q5: ما النسخ الاحتياطية الظلية (shadow copies)؟

لقطات نسخ احتياطي محلية ينشئها Windows؛ وغالبًا ما تحذفها برمجيات الفدية أولًا باستخدام أدوات إدارية.

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

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

Q6: كيف تمكّن سرقة بيانات الاعتماد هجمات برامج الفدية؟

يشتري المهاجمون بيانات دخول إدارية مسرّبة لتسجيل الدخول عبر أسطح المكتب البعيدة وتنفيذ برامج الفدية يدويًا عبر الشبكة.

Q7: ما اختبار الاستعادة التجريبي (dry-run restoration)؟

استعادة قواعد البيانات الاحتياطية بانتظام في بيئات اختبار معزولة للتحقق من أن سرعة الاستعادة وسلامة البيانات تستوفيان مقاييس التعافي من الكوارث.

Q8: كيف يوقف الكشف والاستجابة عند نقاط النهاية (EDR) برامج الفدية؟

بتحليل سلوك العمليات (مثل التشفير السريع) وتعليق التطبيق المارق بسرعة.

Q9: ما نموذج برامج الفدية كخدمة (RaaS)؟

نموذج امتياز تجاري يؤجّر فيه مطورو البرمجيات الخبيثة أدوات بناء برمجيات الفدية للشركاء مقابل نسبة من العوائد.

Q10: كيف يتسبب RDP غير المحدّث في هجوم الفدية؟

تتيح بوابات بروتوكول سطح المكتب البعيد المكشوفة وغير المحدّثة للمهاجمين تخمين عمليات تسجيل الدخول بالقوة الغاشمة وتشغيل البرمجيات الخبيثة يدويًا.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

غالبًا ما يستخدم مشغّلو برامج الفدية أدوات مثل vssadmin.exe لحذف النسخ الظلية في Windows ومنع الاستعادة المحلية. [1]

2. نظرة على الأمن

تُستخدم مفاتيح AES-256 المتماثلة عادةً لتشفير حمولات الملفات، ثم تُقفل بمفاتيح RSA العامة.

3. نظرة على الأمن

قد يستغرق التعافي من هجوم ناجح بالفدية أسابيع، ولهذا تهم النسخ الاحتياطية غير المتصلة التي جرى اختبارها.

4. نظرة على الأمن

لا يؤيد مكتب FBI دفع الفدية ويحذر من أن الدفع لا يضمن استعادة أي بيانات. [2]

5. نظرة على الأمن

ينبغي أن تحدد خطط التعافي من الكوارث (DRP) هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO).

6. نظرة على الأمن

يوصي مكتب FBI بنسخ احتياطية مشفرة وغير قابلة للتغيير، أي لا يمكن تعديلها أو حذفها. [3]

7. رؤية حول الأمان

يستخدم مطورو برامج الفدية تقنيات تعتيم متقدمة لتجاوز ماسحات مكافحة الفيروسات التقليدية القائمة على التوقيعات.

8. رؤية حول الأمان

يقيّد تقسيم الشبكة الحركة الجانبية، مما يساعد على منع انتشار برمجيات الفدية إلى ما بعد المضيف الأول المصاب. [3]

9. رؤية حول الأمان

تُعد الخدمات البعيدة المكشوفة وضعيفة التأمين، مثل بروتوكول سطح المكتب البعيد (RDP)، نقطة دخول شائعة لبرمجيات الفدية. [1]

10. نظرة على الأمن

توصي CISA بالاحتفاظ بنسخ احتياطية مشفرة دون اتصال، لأن كثيرًا من أنواع برمجيات الفدية تبحث عن النسخ الاحتياطية التي يمكن الوصول إليها وتحذفها. [1]

المراجع والمصادر التقنية

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

المراجع الأكاديمية والصناعية

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

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

[5] 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

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 **السؤال 1** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما الآلية الرئيسية لهجوم برمجيات الفدية؟ → تشفير تشفيري لملفات المستخدم لحرمانه من الوصول إلى النظام

2 **السؤال 2** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما هي النسخة الاحتياطية غير المتصلة (الباردة)؟ → نسخة تخزين مفصولة عن الشبكة لحمايتها من انتشار البرمجيات الخبيثة

3 **السؤال 3** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

كيف ينبغي لفرق الأمان عزل الأنظمة المصابة أثناء هجوم فدية؟ → فصل كابلات الشبكة وتعطيل الواجهات اللاسلكية فورًا

4 **السؤال 4** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

لماذا تنصح الجهات الأمنية بعدم دفع فدية برمجيات الفدية؟ → دفع الأموال يشجع المهاجمين ولا يضمن تسليم مفتاح فك التشفير

5 **السؤال 5** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما هي خطة التعافي من الكوارث (DRP)؟ → عملية منظمة لاستعادة العمليات والبيانات بعد اختراق النظام

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يمكن أن تنتشر حمولات برامج الفدية بسهولة إلى النسخ الاحتياطية المتصلة بالشبكة.

7 السؤال 7

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: يحذر مكتب FBI من أن الدفع لا يضمن استعادة أي بيانات.

8 السؤال 8

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

صحيح: تنصح CISA بفصل المضيفين المصابين أو إخراج الشبكة من الخدمة لاحتواء الانتشار.

9 السؤال 9

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: يشفّر برنامج الفدية الملفات عادةً بشيفرات متماثلة سريعة مثل AES.

10 السؤال 10

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يُعد اختبار إجراءات استعادة البيانات بانتظام جزءًا أساسيًا من التعافي من الكوارث.

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

C 1. التشفير	E 2. الحمولة	F 3. نسخة احتياطية غير متصلة	A 4. العزل
H 5. فدية	G 6. التعافي	D 7. الكارثة	B 8. حصان طروادة

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 التشفير	2 الحمولة	3 باردة	4 العزل
5 الفدية	6 التعافي		

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

1 C – نسخةباردة	2 H – طروادة	3 A – التشفير	4 E – الفدية
5 D – العزل	6 G – الكوارث	7 B – الحمولة	8 F – التعافي

ملاحظات النقاش للمعلمين

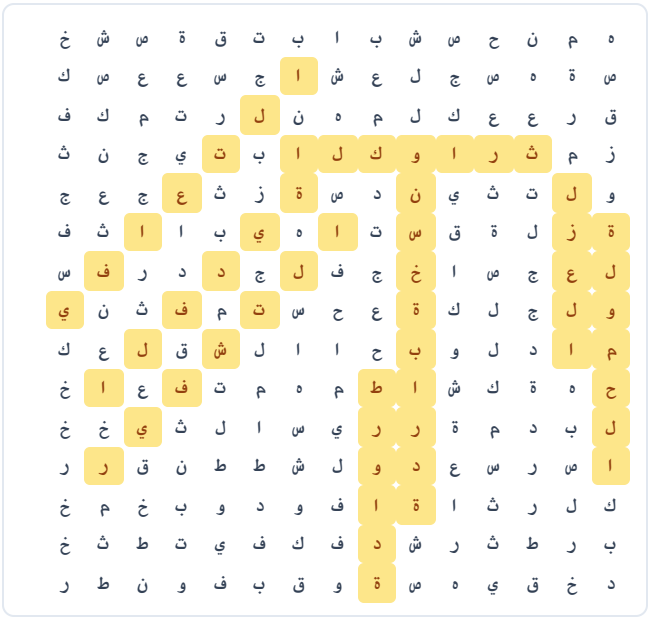
المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح التشفير والحمولة ونسخة احتياطية غير متصلة بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

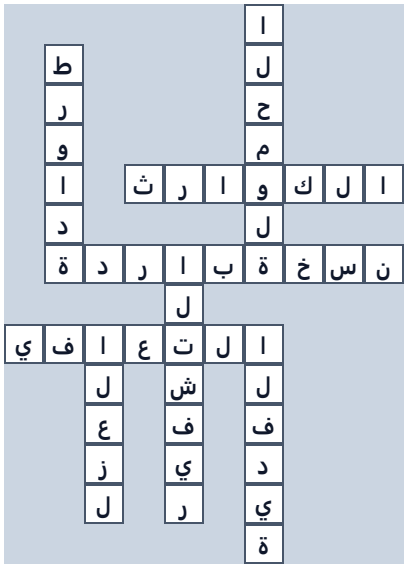
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات



حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

3 أفقي: الكوارث حدث تعطل كبير في النظام (7 حروف)

4 أفقي: نسخةباردة نسخة غير متصلة بالشبكة (9 حروف)

6 أفقي: التعافي استعادة قاعدة البيانات من النسخة الاحتياطية (7 حروف)

عمودي

1 عمودي: الحمولة تنفيذ برمجية خبيثة (7 حروف)

2 عمودي: طروادة ملف خبيث متنكر في هيئة ملف سليم (6 حروف)

5 عمودي: التشفير قفل الملفات تشفيريا (7 حروف)

6 عمودي: الفدية طلب دفع مقابل المفتاح التشفيري (6 حروف)

7 عمودي: العزل فصل أنظمة الشبكة المصابة (5 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. شيافرتل ← **التشفير**
2. ةندةساربخ ← **نسخةباردة**
3. افدةيل ← **الفدية**
4. ثلاوراك ← **الكوارث**
5. وةمحالل ← **الحمولة**
6. زاعلل ← **العزل**
7. افايلعت ← **التعافي**
8. وةطدار ← **طروادة**

مفتاح تحدي الشيفرة السرية

"استعد النظام المشفر من نسخة باردة"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: احتواء حمولة برمجيات الفدية في المؤسسات

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: اخترقت برمجية فدية نشطة الشبكة المحلية لشركة. بدأت خوادم الملفات الرئيسة تعرض امتدادات ملفات بالصيغة .locked.
- الاستراتيجية والحل الموصى بهما: افصل جميع الخوادم المتأثرة عن الشبكة المحلية. أنهِ جلسات الإدارة النشطة. استعد الملفات غير المخترقة من نظام نسخ احتياطي آمن غير متصل ومقفل ضد الكتابة.

B دراسة الحالة 2: تقييم بنى النسخ الاحتياطي دون اتصال

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: تريد مؤسسة تصميم استراتيجية للنسخ الاحتياطي تقلل من خطر اختراق النسخ الاحتياطية حتى لو سيطرت برمجية الفدية سيطرة كاملة على الشبكة المحلية الرئيسية.
- الاستراتيجية والحل الموصى بهما: تنفيذ تخزين الكتابة مرة واحدة والقراءة المتعددة (WORM). وإنشاء عزل منطقي بفصل نظام النسخ الاحتياطي عن جميع الشبكات، وفرض تدوير يومي للوسائط المادية.