الاسم: _____ التاريخ: _____ الدرجة: _____

برامج مضادات الفيروسات ونقاط النهاية دليل الحماية

كشف التوقيعات، والكشف الاستدلالي، ومراقبة السلوك، والعزل في بيئة معزولة، والتحديثات

نظرة تعليمية على برامج مكافحة الفيروسات

مؤمَّن
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 برامج مكافحة الفيروسات وحماية نقاط النهاية. ستستكشف قواعد بيانات التواقيع والماسحات الاستدلالية والمراقبة السلوكية وملفات العزل الافتراضية (sandbox) وتخفيف الإنذارات الكاذبة.

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/antivirus/

خارطة طريقك لتعلّم استراتيجية مكافحة الفيروسات

- ميّز بين اكتشاف البرمجيات الخبيثة القائم على التوقيعات والقائم على الاستدلال.
- افهم بروتوكولات مراقبة السلوك وعزل البيئة المعزولة.
- قيّم آثار الفحص الفوري على أداء النظام ونقاط النهاية.
- الحد من التصنيفات الإيجابية الخاطئة باستخدام التحقق من الشهادات الرقمية.
- إدارة توزيع تحديثات التعريفات اليومية عبر نقاط النهاية المؤسسية.

تعليمات دليل مكافحة الفيروسات

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 الأمان بمضاد الفيروسات لنقاط النهاية. واختم بالنشاط الإضافي «فكّر بسرعة».

الحماية من الفيروسات وفحص التوقيعات (مقدمة)

تحمي برامج مضادات الفيروسات نقاط النهاية بتحديد البرمجيات الخبيثة وعزلها وإزالتها. وتجمع الأنظمة الحديثة بين قواعد بيانات التواقيع (مطابقة تجزئات التهديدات المعروفة) والأساليب الاستدلالية (تحليل بنية الملف) ومراقبة السلوك لاكتشاف ثغرات اليوم الصفر.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما قيود الكشف المعتمد على التواقيع؟
   - A. لا يستطيع التعرف على البرمجيات الخبيثة المجهولة أو المعدّلة
   - B. يولّد معدلات مرتفعة من الإيجابيات الكاذبة
   - C. يتطلب قدرة معالجة عالية من وحدة المعالجة المركزية
   - D. يعمل فقط عند الاتصال بالإنترنت

2. كيف ترصد الماسحات الاستكشافية متغيرات البرمجيات الخبيثة الجديدة؟
   - A. بتحديد الأنماط وبنى الشيفرة المشبوهة
   - B. بمطابقة تجزئات الملفات مع قاعدة بيانات للتهديدات
   - C. بحذف جميع الملفات التنفيذية غير الموقّعة تلقائيًا
   - D. برفع كل ملف إلى مجلد سحابي عام

3. ما الغرض من تنفيذ برنامج مكافحة الفيروسات في بيئة معزولة؟
   - A. عزل الملفات وتحليلها في خزنة افتراضية آمنة
   - B. تسريع نقل النسخ الاحتياطي لنظام الملفات المحلي
   - C. تحديث تصحيحات الأمان لنظام التشغيل المحلي
   - D. ضغط ملفات المستندات الكبيرة لتوفير مساحة التخزين

4. ما طريقة الكشف التي تحدد سلوك التهديد في الوقت الفعلي؟
   - A. تحليل سلوكي يراقب إجراءات البرمجيات
   - B. فحص السجلات التاريخية يُجرى خلال الليل
   - C. تدخل يدوي من المستخدم للإبلاغ عن التطبيقات البطيئة
   - D. مراجعات يدوية أسبوعية للبرامج المثبتة

5. لماذا تُعد تحديثات التعريفات المنتظمة حاسمة للماسحات؟
   - A. لتغذية محركات التوقيعات بمعرّفات التهديدات في قاعدة البيانات
   - B. لزيادة سرعات ساعة المعالج المركزي أثناء العمليات
   - C. لتعديل أزمنة التخزين المؤقت العالمية لخوادم أسماء DNS
   - D. لتفويض إعدادات ملفات تعريف الارتباط في متصفح الويب

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6 tf

6. يطابق كشف التوقيعات تجزئات الملفات التشفيرية مع قوائم قواعد البيانات.

صحيح خطأ

7 سؤال 7 tf

7. قد تُطلق الماسحات الاستكشافية تنبيهات إيجابية كاذبة على ملفات آمنة.

صحيح خطأ

8 سؤال 8 tf

8. تتيح بيئة الاختبار المعزولة للبرمجيات الخبيثة الوصول إلى ملفات الشبكة بلا حدود.

صحيح خطأ

9 سؤال 9 tf

9. يحظر الفحص السلوكي الملفات عندما تُظهر إجراءات خبيثة.

صحيح خطأ

10 سؤال 10 tf

10. برامج مضادات الفيروسات القياسية توقف جميع هجمات اليوم صفر بالكامل.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. يعتمد الماسح التقليدي على مطابقة _____ لتحديد البرمجيات الخبيثة المعروفة.
2. يسمى تحليل أنماط شيفرة الملفات فحص _____ .
3. تعزل برامج مكافحة الفيروسات الملفات المشبوهة في بيئة _____ .
4. تراقب المراقبة الفورية _____ البرامج بحثاً عن الأنشطة المشبوهة.
5. تنزّل الماسحات _____ قاعدة البيانات يومياً للتعرف على التهديدات الجديدة.
6. تؤدي البرامج الآمنة المصنفة كبرمجيات خبيثة إلى تنبيهات إيجابية _____ .

بنك كلمات المفردات

الاستدلال | التوقيع | الحماية | الصندوق الرملي | العزل | تحديثات | سلوك | كاذبة

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الأمان

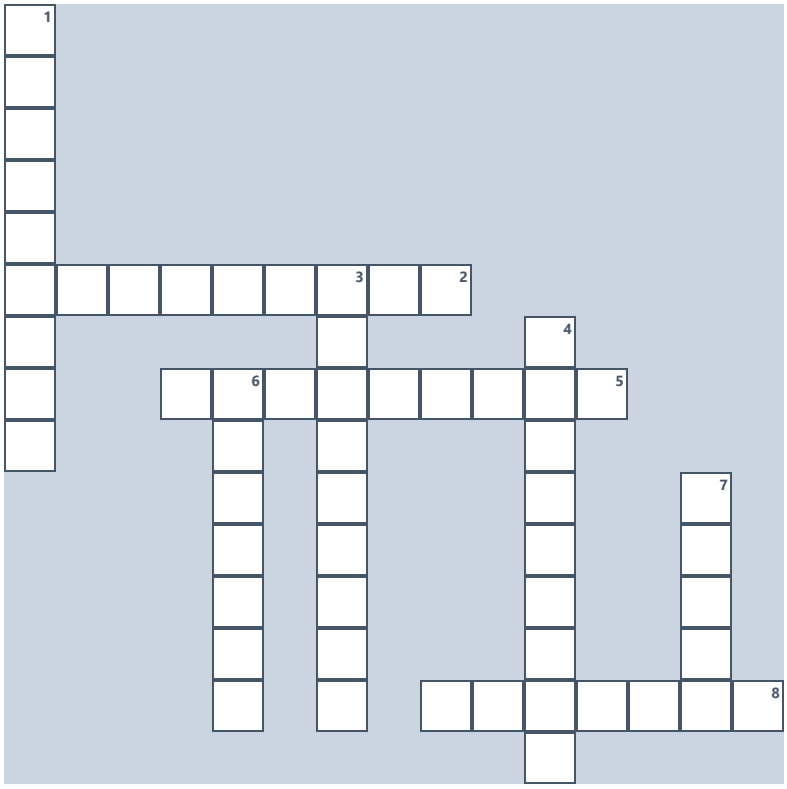
مطابقة التعريفات

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

1. توقيع التجزئة	A	حصر الملفات المشبوهة لمنع تعرض النظام المحلي.
2. الاستدلال على الشفرة	B	مجموعة برمجيات تفحص نقاط النهاية وتحميها من الثغرات.
3. بيئة عزل الملفات	C	مراقبة أفعال البرمجيات قيد التشغيل بحثًا عن أنماط تشغيل خبيثة.
4. فحص السلوك	D	بصمة فريدة في قاعدة بيانات تشفيرية تُستخدم لتحديد التهديدات المعروفة.
5. تحديثات يومية	E	بيئة اختبار افتراضية آمنة تشغّل شيفرة غير موثوقة بأمان.
6. إيجابي كاذب	F	تنزيلات منتظمة للتعريفات تغذي قاعدة بيانات التهديدات.
7. عزل التهديدات	G	تحليل قائم على القواعد يضع علامة على الملفات ذات تخطيطات الشيفرة المشبوهة.
8. أداة مكافحة الفيروسات	H	تنبيه أمني يصنّف خطأً برنامجًا آمنًا على أنه برمجية خبيثة.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

2. مراقبة أفعال البرامج قيد التشغيل بحثاً عن أنماط تشغيل خبيثة (9)

5. تحليل قائم على القواعد يضع علامة على الملفات ذات تركيب الشيفرة المشبوه (9)

8. مجموعة برمجيات تفحص الأجهزة الطرفية وتحميها من الثغرات (7)

عمودي

1. تنبيه أمني يصنف خطأً برنامجاً آمناً على أنه برمجية خبيثة (9)

3. بيئة اختبار افتراضية آمنة تشغّل الشيفرة غير الموثوقة بأمان (9)

4. تنزيلات منتظمة للتعريفات تغذي قاعدة بيانات التهديدات (9)

6. بصمة تشفيرية فريدة في قاعدة البيانات تُستخدم لتحديد التهديدات المعروفة (7)

7. حصر الملفات المشبوهة لمنع تعريض النظام المحلي للخطر (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. الدلائل الأفقية الدلائل الرأسية

أفقي

2 أفقي: مراقبة أفعال البرامج قيد التشغيل بحثاً عن أنماط تشغيل خبيثة (9 حروف):

5 أفقي: تحليل قائم على القواعد يضع علامة على الملفات ذات تركيب الشيفرة المشبوه (9 حروف):

8 أفقي: مجموعة برمجيات تفحص الأجهزة الطرفية وتحميها من الثغرات (7 حروف):

عمودي

1 عمودي: تنبيه أمني يصنف خطأً برنامجاً آمناً على أنه برمجية خبيثة (9 حروف):

3 عمودي: بيئة اختبار افتراضية آمنة تشغّل الشيفرة غير الموثوقة بأمان (9 حروف):

4 عمودي: تنزيلات منتظمة للتعريفات تغذي قاعدة بيانات التهديدات (9 حروف):

6 عمودي: بصمة تشفيرية فريدة في قاعدة البيانات تُستخدم لتحديد التهديدات المعروفة (7 حروف):

7 عمودي: حصر الملفات المشبوهة لمنع تعريض النظام المحلي للخطر (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.

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

قائمة كلمات المفردات

التوقيع الاستدلال صندوقرملي فحصالسلوك التحديثات انذاركاذب العزل الحماية

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. التوقيع
B. الاستدلال
C. صندوقرملي
D. فحصالسلوك
E. التحديثات
F. انذاركاذب
G. العزل
H. الحماية

التعريفات وحقول المطابقة
1. مراقبة أفعال البرامج قيد التشغيل بحثاً عن أنماط تشغيل خبيثة.
2. مجموعة برمجيات تفحص الأجهزة الطرفية وتحميها من الثغرات.
3. تنزيلات منتظمة للتعريفات تغذي قاعدة بيانات التهديدات.
4. تحليل قائم على القواعد يضع علامة على الملفات ذات تركيب الشيفرة المشبوه.
5. حصر الملفات المشبوهة لمنع تعريض النظام المحلي للخطر.
6. بصمة تشفيرية فريدة في قاعدة البيانات تُستخدم لتحديد التهديدات المعروفة.
7. بيئة اختبار افتراضية آمنة تشغّل الشيفرة غير الموثوقة بأمان.
8. تنبيه أمني يصنف خطأً برنامجاً آمناً على أنه برمجية خبيثة.

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

نشاط إضافي: فكّر بسرعة

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

1	أسباب لتحديث البرامج		
2	أشخاص يمكنك طلب مساعدة تقنية منهم		
3	أشياء تفعلها عندما يعثر برنامج مكافحة الفيروسات على تهديد		
4	علامات إصابة الحاسوب بفيروس		
5	أشياء توضع في الحجر الصحي		
6	أماكن تختبئ فيها الفيروسات		
7	معلومات لا ينبغي أن تشاركها أبدًا		
8	أنواع البرمجيات الخبيثة		
9	أدوات أمنية تعرفها		
10	أشياء يفحصها برنامج مكافحة الفيروسات		
11	أشياء تحتفظ بنسخة احتياطية منها		
12	أجهزة يمكن اختراقها		
13	برامج مكافحة الفيروسات التي تعرفها		
14	أسباب الإنذارات الكاذبة		
15	عادات آمنة يمكنك البدء بها اليوم		

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: الفحص بالتوقيعات مقابل الفحص الاستدلالي



السيناريو: ينزّل موظف أداة مخصصة طوّرها فريق آخر داخليًا. يجتازها الماسح القائم على التواقيع، لكن الماسح الاستدلالي يضعها علامة بوصفها مشبوهة.

سؤال للنقاش: اشرح سبب حدوث ذلك، وكيف يمكن التحقق مما إذا كان الملف آمنًا.

دراسة الحالة 2: التعامل مع الإيجابيات الكاذبة



السيناريو: يترجم مطوّر برمجيات تطبيقه. يضع برنامج مكافحة الفيروسات في النظام علامة على الملف التنفيذي الجديد بوصفه برمجية خبيثة ويعزله في الحجر الصحي.

سؤال للنقاش: لخّص مخاطر إدراج الملف في القائمة البيضاء، وصف مسار الحل الصحيح.

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

3	1	28	5	24	10	2	23	1		20	13	22	1

29	8	28	8	5	23	1		29	4	28	2	7	23	1

23	1	23	8	3	12	1	23	1	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: كيف تحدد برامج مكافحة الفيروسات البرمجيات الخبيثة؟

يحدد البرمجيات الخبيثة باستخدام مطابقة تواقيع قاعدة البيانات وتحليل بنية الشيفرة الاستكشافي والمراقبة السلوكية الفورية.

Q2: ما الكشف المعتمد على التواقيع؟

هي طريقة فحص تطابق تجزئات الملفات التشفيرية مع قوائم قواعد البيانات للتهديدات المعروفة من البرمجيات الخبيثة.

Q3: ما الماسح الاستدلالي (heuristic scanner)؟

يحلل الاستدلال الاستكشافي بنية الملف وتعليمات الشيفرة، ويرصد الأنماط المشبوهة الشائعة في متغيرات البرمجيات الخبيثة.

Q4: ماذا يعني عزل ملف في الحجر الصحي (quarantine)؟

ينقل مضاد الفيروسات الملف إلى مجلد آمن معزول، ويمنع تنفيذه لحماية نظام التشغيل.

Q5: ما الإيجابية الكاذبة في برامج مكافحة الفيروسات؟

هو خطأ يُوسّم فيه برنامج شرعي وآمن خطأً كبرمجية خبيثة بواسطة خوارزميات الفحص.

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

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: كيف تحمي مراقبة السلوك الأنظمة؟

يراقب البرمجيات قيد التشغيل في الوقت الفعلي، ويحجب العمليات التي تحاول إجراء تغييرات مشبوهة مثل حقن الشيفرة.

Q7: لماذا يُعد اختبار البيئة المعزولة (sandbox) مهمًا؟

يشغّل العزل في صندوق الرمل الملفات غير الموثوقة في آلة افتراضية معزولة، ويراقب الإجراءات بأمان دون تعريض النظام للخطر.

Q8: كم مرة ينبغي تحديث تعريفات برامج مكافحة الفيروسات؟

ينبغي أن تحدّث الماسحات التعريفات يوميًا أو كل ساعة للتعرف على سلالات البرمجيات الخبيثة المكتشفة حديثًا.

Q9: ما الفرق بين برنامج مكافحة الفيروسات وEDR؟

يركّز مضاد الفيروسات على فحص الملفات، بينما يوفّر الكشف والاستجابة لنقاط النهاية (EDR) تتبّعًا للتهديدات واحتواءً لها على مستوى الشبكة بأكملها.

Q10: هل يمكنني تشغيل برنامجين لمكافحة الفيروسات معًا؟

لا. فتشغيل ماسحين نشطين يتسبب في تعارضات في النظام ويبطئ الأداء وقد يعطل كل منهما عمليات الآخر.

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

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

Q1: كيف تقلل القواعد الاستدلالية تجاوز التهديدات؟

يحلل الاستدلال الاستكشافي أنماط التهديد العامة بدلًا من التواقيع المحددة، فيرصد المتغيرات المعدَّلة من عائلات البرمجيات الخبيثة المعروفة.

Q2: ما الفيروس متعدد الأشكال؟

هي برمجية خبيثة تغيّر بنية ملفها وروتين فك التشفير مع كل تنفيذ، ما يجعل فحوص التواقيع غير فعالة.

Q3: كيف تكتشف بيئات العزل (sandboxes) التهرب من الأجهزة الافتراضية؟

تحاكي بيئات العزل الحديثة نقرات الفأرة ومدة تشغيل النظام، فتخدع البرمجيات الخبيثة المصممة للاختباء عند تشغيلها في الأجهزة الافتراضية.

Q4: ما صيغ تنزيل تحديثات التوقيعات؟

عادةً ما تكون التحديثات ملفات فروق ثنائية تزايدية خفيفة، مما يقلل استهلاك عرض النطاق الترددي لشبكة العميل.

Q5: كيف تدير وكلاء نقاط النهاية عمليات الفحص المحلية؟

تجري برمجيات الوكيل فحوصات خلفية خفيفة، وتُحيل عمليات البحث العميقة عن التجزئات التشفيرية إلى قواعد بيانات التهديدات السحابية.

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

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

Q6: ما فحص اكتشاف الجذور الخفية (rootkit)؟

يفحص جداول الذاكرة على مستوى النواة، متجاوزًا واجهات API لنظام التشغيل التي تعترضها الجذور الخفية (rootkits) لإخفاء خيوطها النشطة.

Q7: كيف يحظر فحص السلوك برامج الفدية؟

يكتشف حلقات التشفير الجماعي الآلي للملفات، فينهي عملية المضيف قبل قفل قواعد بيانات النظام.

Q8: ما التحقق من شهادة توقيع الشيفرة؟

تفحص الماسحات التوقيعات الرقمية للشيفرة مقابل جهات إصدار الشهادات الجذرية الموثوقة، للتحقق من هوية مطور البرنامج.

Q9: كيف تؤثر أدوات التعبئة (packers) في محركات الفحص؟

تضغط أدوات التغليف حمولات البرمجيات الخبيثة أو تشفّرها. ويجب على الماسحات فك الملف في الذاكرة قبل إجراء مطابقة التواقيع.

Q10: كيف تؤتمت أدوات EDR العزل؟

تعزل وكلاء EDR نقاط النهاية المخترقة على مستوى الشبكة، فيحجبون الحركة الجانبية مع السماح بوصول المحللين.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

تخزّن قواعد بيانات التوقيعات تجزئات البرمجيات الخبيثة المعروفة، لذا لا تُكتشف الملفات الجديدة كليًا أو المعدّلة إلى أن تتحدث التعريفات.

2. نظرة على الأمن

يمكن لمحركات الاستدلال الاستكشافي رصد بعض متغيرات البرمجيات الخبيثة الجديدة قبل وجود التواقيع، على حساب مزيد من الإنذارات الكاذبة.

3. نظرة على الأمن

تكلّف التنبيهات الإيجابية الكاذبة فرق تقنية المعلومات وقتًا في التحقق من الملفات التي عُزلت خطأً واستعادتها.

4. نظرة على الأمن

تغيّر البرمجيات الخبيثة متعددة الأشكال شيفرتها مع كل نسخة، لذا يجمع المدافعون بين التواقيع والفحوص الاستدلالية والسلوكية.

5. نظرة على الأمن

تفحص محركات مكافحة الفيروسات السحابية تجزئات الملفات المشبوهة مقابل قواعد بيانات تهديدات كبيرة عبر الإنترنت في وقت شبه فوري.

6. نظرة على الأمن

يكتب مؤلفو البرمجيات الخبيثة أكوادًا مخصصة مصممة لفحص بيئات العزل، وتؤخر التنفيذ لتجاوز المؤقتات.

7. رؤية حول الأمان

يدفع الموردون تحديثات التعريفات إلى نقاط النهاية بانتظام ليتمكن الماسحات من التعرف على التهديدات المؤكدة حديثًا.

8. رؤية حول الأمان

تستهدف أدوات مراقبة السلوك الخاصة ببرامج الفدية استدعاءات Win32 API المحددة المرتبطة بتشفير الملفات وحذف النسخ الظلية.

9. رؤية حول الأمان

قد تقلل توقيعات الشيفرة الصالحة خطر الإيجابيات الكاذبة، لكن الملفات الموقعة تُفحص أيضًا، لأن البرمجيات الخبيثة يمكن توقيعها أيضًا.

10. نظرة على الأمن

تعدّل برمجيات Rootkit بنى نواة النظام، مما يتطلب ماسحات متخصصة تعمل أثناء الإقلاع للكشف عنها وتنظيفها.

المراجع والمصادر التقنية

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

المراجع الأكاديمية والصناعية

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.
https://csrc.nist.gov/pubs/sp/800/83/r1/final

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

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

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

[5] 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

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 السؤال 1 التوقيعات — الإجابة الصحيحة: A

ملاحظة للمعلم

يعتمد الفحص بالتوقيعات على تجزئات قاعدة بيانات معروفة، فيفشل في اكتشاف البرمجيات الخبيثة المجهولة أو المعدّلة. المصدر: OWASP Secure Configuration.

2 السؤال 2 الاستدلال الاستكشافي — الإجابة الصحيحة: A

ملاحظة للمعلم

تحلل الاستدلالات تخطيط الشيفرة وأوامرها لتحديد السمات المشبوهة في المتغيرات الجديدة للتهديدات. المصدر: Center for Internet Security (CIS).

3 السؤال 3 العزل في صندوق الرمل — الإجابة الصحيحة: A

ملاحظة للمعلم

تشغّل بيئة العزل الملفات المشبوهة في جهاز افتراضي معزول لمراقبة سلوك التنفيذ بأمان. المصدر: NIST Digital Identity.

4 السؤال 4 السلوكي — الإجابة الصحيحة: A

ملاحظة للمعلم

يراقب فحص السلوك البرامج قيد التشغيل في الوقت الفعلي لحظر التغييرات غير المصرح بها في النظام. المصدر: Center for Internet Security (CIS).

5 السؤال 5 التحديثات — الإجابة الصحيحة: A

ملاحظة للمعلم

تنزّل الماسحات تحديثات التعريفات التراكمية اليومية لتبقى متزامنة مع مشهد التهديدات. المصدر: OWASP Secure Configuration.

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6 التوقيعات — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تحسب أدوات التوقيعات تجزئات تشفيرية وتطابقها مع قاعدة بيانات تجزئات تهديدات معروفة. المصدر: OWASP Secure Configuration.

7 السؤال 7 الاستدلال الاستكشافي — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تشغّل المحركات الاستدلالية تخطيطات قائمة على القواعد قد تصنّف ملفات سليمة وآمنة على أنها مشبوهة. المصدر: Center for Internet Security (CIS).

8 السؤال 8 العزل في صندوق الرمل — الإجابة الصحيحة: خطأ

ملاحظة للمعلم

تشغّل بيئة العزل الشيفرة في حاوية افتراضية، وتحظر بصرامة الوصول إلى المشاركات الشبكية. المصدر: NIST Digital Identity.

9 السؤال 9 السلوكي — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تنبّه المراقبة في الوقت الفعلي إلى العمليات قيد التشغيل التي تحاول كتابة غير مشروعة أو قفل ملفات. المصدر: Center for Internet Security (CIS).

10 السؤال 10 — الإجابة الصحيحة: خطأ

ملاحظة للمعلم

لا يوقف أي برنامج مكافحة فيروسات كل هجمات اليوم الصفر؛ إذ يمكن للتهديدات المجهولة أن تتفادى التواقيع والاستدلال.

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. توقيع التجزئة	G 2. الاستدلال على الشفرة	E 3. بيئة عزل الملفات	C 4. فحص السلوك
F 5. تحديثات يومية	H 6. إيجابي كاذب	A 7. عزل التهديدات	B 8. أداة مكافحة الفيروسات

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 التوقيع	2 الاستدلال	3 الصندوق الرملي	4 سلوك
5 تحديثات	6 كاذبة		

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

1 D – فحصالسلوك	2 H – الحماية	3 E – التحديثات	4 B – الاستدلال
5 G – العزل	6 A – التوقيع	7 C – صندوقرملي	8 F – انذاركاذب

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح توقيع التجزئة والاستدلال على الشفرة وبيئة عزل الملفات بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

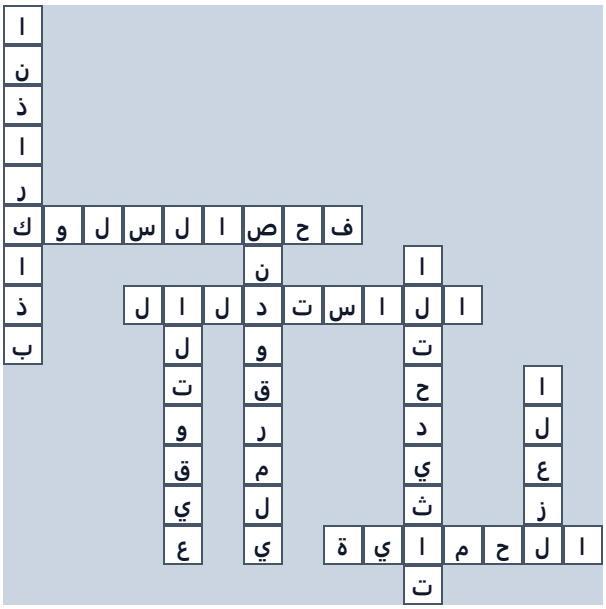
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

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

حل الكلمات المتقاطعة



أفقي

2 أفقي: فحصالسلوك مراقبة أفعال البرامج قيد التشغيل بحثاً عن أنماط تشغيل خبيثة (9 حروف)

5 أفقي: الاستدلال تحليل قائم على القواعد يضع علامة على الملفات ذات تركيب الشيفرة المشبوه (9 حروف)

8 أفقي: الحماية مجموعة برمجيات تفحص الأجهزة الطرفية وتحميها من الثغرات (7 حروف)

عمودي

1 عمودي: انذاركاذب تنبيه أمني يصنف خطأً برنامجاً آمناً على أنه برمجية خبيثة (9 حروف)

3 عمودي: صندوقرملي بيئة اختبار افتراضية آمنة تشغّل الشيفرة غير الموثوقة بأمان (9 حروف)

4 عمودي: التحديثات تنزيلات منتظمة للتعريفات تغذي قاعدة بيانات التهديدات (9 حروف)

6 عمودي: التوقيع بصمة تشفيرية فريدة في قاعدة البيانات تُستخدم لتحديد التهديدات المعروفة (7 حروف)

7 عمودي: العزل حصر الملفات المشبوهة لمنع تعريض النظام المحلي للخطر (5 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. وياقعتل — **التوقيع**
2. يصلونرمقد — **صندوقرملي**
3. ايدلثتحات — **التحديثات**
4. علزال — **العزل**
5. لتللدساا — **الاستدلال**
6. واحلسفلكص — **فحصالسلوك**
7. كاذباانرذ — **انذاركاذب**
8. لمةاياح — **الحماية**

مفتاح تحدي الشيفرة السرية

"اكشف البرمجيات الخبيثة الجديدة بالاستدلال"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: الفحص بالتوقيعات مقابل الفحص الاستدلالي

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: ينزّل موظف أداة مخصصة بُنيت داخليًا بواسطة فريق آخر. يجتازها ماسح التوقيعات، لكن الماسح الاستدلالي يصنّفها على أنها مشبوهة.
- الاستراتيجية والحل الموصى بهما: لماذا حدث ذلك: يفحص فحص التوقيعات تجزئات الملفات؛ ولأن الملف مخصص، فهو غير موجود في قاعدة بيانات التهديدات. أما الاستدلال (Heuristics) فيحلل البنية ويرصد الإجراءات المشبوهة (مثل الكتابة في السجل). التحقق: شغّل الملف في بيئة معزولة (sandbox) لمراقبة إجراءاته، وافحص التوقيعات الرقمية، وأرسل التجزئة إلى بوابات استخبارات التهديدات.

B دراسة الحالة 2: التعامل مع الإيجابيات الكاذبة

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يترجم مطور برمجيات تطبيقه. يصنّف برنامج مكافحة الفيروسات في النظام الملف التنفيذي الجديد على أنه برمجية خبيثة ويعزله في الحجر.
- الاستراتيجية والحل الموصى بهما: مخاطر القائمة البيضاء: قد يتيح تجاوز الماسحات تشغيل شيفرة حقيقية مصابة. مسار الحل: أرسل الملف إلى مورّد برنامج مكافحة الفيروسات للتحليل، ووقّع الشيفرة رقميًا باستخدام جهات إصدار الشهادات، واضبط مؤقتًا استثناءات لمجلدات محددة بدلًا من إيقاف برنامج مكافحة الفيروسات.