الاسم: _____ التاريخ: _____ الدرجة: _____

بنية انعدام الثقة والأمان

التحقق المستمر، والتقسيم الدقيق للشبكة، وإدارة الهوية والوصول، وأقل الامتيازات، وفحوصات الوضع الأمني.

نظرة عامة تعليمية على أمان انعدام الثقة

مرحبًا! ترشدك حزمة الأنشطة هذه عبر بنية انعدام الثقة (Zero Trust) وأمانها. ستستكشف التحقق المستمر، وتجزئة الشبكة الدقيقة، وإدارة هوية الوصول (IAM)، والحد الأدنى من الامتيازات، ومراجعة الجلسات.

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/zero-trust-cyber-security/

خارطة طريقك لتعلّم استراتيجية انعدام الثقة

- افهم المبدأ الأساسي للتحقق المستمر.
- طبّق التجزئة الدقيقة للشبكة والوصول بأقل الامتيازات.
- هيّئ فحوصات الوضع الأمني للأجهزة وتدقيق الجلسات النشطة.

تعليمات دليل أمان انعدام الثقة

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 بنية Zero Trust. واختم بالنشاط الإضافي «فكّر بسرعة».

بنية انعدام الثقة والأمان (مقدمة)

يستبدل أمان انعدام الثقة نماذج محيط الشبكة القديمة بسياسة صارمة هي 'لا تثق أبدًا، تحقق دائمًا'. ويحظر تطبيق التقسيم الدقيق وإدارة الهوية والوصول (IAM) وحقوق أقل الامتيازات وفحوصات الوضع الأمني حركة التهديدات الجانبية.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما المبدأ الأساسي لأمان انعدام الثقة (Zero Trust)؟
   - A. لا تثق أبدًا، تحقق دائمًا من كل طلب وصول بغض النظر عن مصدره
   - B. افتراض أن كل حركة المرور داخل جدار حماية الشركة آمنة
   - C. تخزين ملفات قاعدة البيانات دون تشفير لتحسين السرعة
   - D. فرض مصادقة البريد الإلكتروني باستخدام سجلات SPF فقط

2. ما هو التقسيم الدقيق للشبكة؟
   - A. تقسيم الشبكات إلى مناطق صغيرة معزولة لاحتواء الحركة الجانبية
   - B. تشفير بطاقات الشبكة أثناء نقل البيانات
   - C. ربط جميع الخوادم المحلية بعنوان IP عام واحد
   - D. مراقبة ضغطات مفاتيح المستخدم في جلسات المتصفح

3. ما مبدأ الامتياز الأدنى؟
   - A. تقييد أذونات وصول المستخدم بما هو ضروري لعمله فقط
   - B. منح جميع صلاحيات النظام لكل مستخدم افتراضيًا
   - C. السماح بتسجيلات الدخول المجهولة إلى خوادم قواعد بيانات الشركة
   - D. تهيئة أجهزة توجيه Wi-Fi العامة دون كلمات مرور

4. ما إدارة الهوية والوصول (IAM)؟
   - A. أطر تدير الهويات الرقمية وتتحكم في امتيازات النظام
   - B. أدوات مضادات الفيروسات التي تفحص أدلة الملفات المحلية
   - C. نظام تخزين احتياطي يستخدم وسائط معزولة عن الشبكة
   - D. بروتوكول بوابة البريد الإلكتروني يرفض النطاقات المنتحلة

5. ماذا تعني المصادقة المستمرة؟
   - A. التحقق المتكرر من هوية المستخدم ووضع الجهاز أثناء جلسة نشطة
   - B. تغيير كلمة المرور الرئيسية كل 10 دقائق
   - C. تجزئة سجلات قواعد البيانات باستخدام خوارزميات متعددة
   - D. تشفير حزم نقل الشبكة باستخدام مفاتيح TLS

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. يفترض انعدام الثقة أن كل حركة البيانات داخل جدار الحماية المؤسسي آمنة.

○ صحيح ○ خطأ

7 سؤال 7

7. تحد التجزئة الدقيقة من قدرة المهاجمين على التحرك جانبيًا عبر الخوادم الداخلية.

○ صحيح ○ خطأ

8 سؤال 8

8. يمنح مبدأ أقل الامتيازات حق الوصول إلى جميع ملفات قاعدة البيانات افتراضيًا.

○ صحيح ○ خطأ

9 سؤال 9

9. يتحقق التحقق المستمر من سلامة الجهاز وبيانات الاعتماد طوال جلسة تسجيل الدخول.

○ صحيح ○ خطأ

10 سؤال 10

10. يقلل تطبيق نموذج انعدام الثقة من أثر اختراق بيانات تسجيل دخول الشركة.

○ صحيح ○ خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. يسمى طلب بيانات الاعتماد عند كل نقطة وصول _____ المستمر.
2. يسمى تقسيم شبكة الشركة إلى مناطق صغيرة جدا _____ الدقيقة.
3. تستخدم تهيئة الهويات الرقمية والتحكم بالوصول نظام _____ .
4. يقيد أذونات المستخدمين مبدأ أقل _____ .
5. يفحص تقييم سلامة الأجهزة المتصلة _____ الجهاز.
6. يعد تسجيل الجلسات النشطة ومراجعتها من أعمال _____ الأمني.

بنك كلمات المفردات

التجزئة | التحقق | التدقيق | الهوية | امتياز | جدار حماية | وضعية | IAM

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الأمان

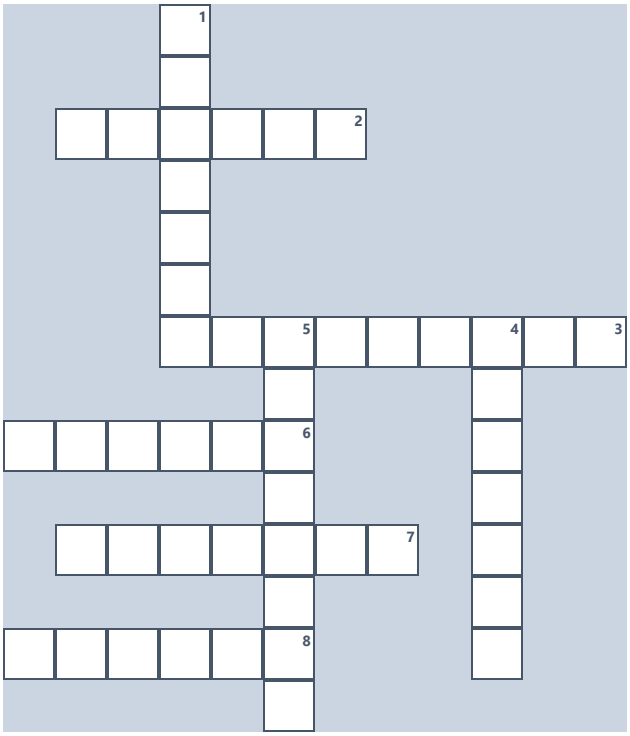
مطابقة التعريفات

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

1. التحقق	A	إدارة الوصول إلى بيانات اعتماد المستخدمين.
2. التجزئة	B	مبدأ أقل حقوق وصول.
3. IAM	C	توجيه حركة حزم الشبكة.
4. الامتياز	D	حماية الحاجز الخارجي للشبكة.
5. الوضع الأمني	E	مراجعة جلسات الوصول المسجلة.
6. التدقيق	F	تقسيم مناطق الشبكة الداخلية.
7. جدار الحماية	G	التحقق دائمًا من بيانات اعتماد المستخدم.
8. جهاز التوجيه	H	تقييم حالة سلامة الجهاز.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

2. إدارة وصول بيانات اعتماد المستخدمين (6)

3. حماية الحاجز الخارجي للشبكة (9)

6. فحص بيانات اعتماد المستخدم باستمرار (6)

7. مراجعة جلسات الوصول المسجلة (7)

8. توجيه حزم حركة الشبكة (6)

عمودي

1. تقييم حالة سلامة الجهاز (7)

4. تقسيم مناطق الشبكة الداخلية (7)

5. مبدأ أقل حقوق وصول ممكنة (8)

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: إدارة وصول بيانات اعتماد المستخدمين (6 حروف):

3 أفقي: حماية الحاجز الخارجي للشبكة (9 حروف):

6 أفقي: فحص بيانات اعتماد المستخدم باستمرار (6 حروف):

7 أفقي: مراجعة جلسات الوصول المسجلة (7 حروف):

8 أفقي: توجيه حزم حركة الشبكة (6 حروف):

عمودي

1 عمودي: تقييم حالة سلامة الجهاز (7 حروف):

4 عمودي: تقسيم مناطق الشبكة الداخلية (7 حروف):

5 عمودي: مبدأ أقل حقوق وصول ممكنة (8 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.

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

قائمة كلمات المفردات

التحقق التجزئة الهوية الامتياز الوضعية التدقيق جدارحماية الموجه

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. التحقق
B. التجزئة
C. الهوية
D. الامتياز
E. الوضعية
F. التدقيق
G. جدارحماية
H. الموجه

التعريفات وحقول المطابقة
1. حماية الحاجز الخارجي للشبكة.
2. مراجعة جلسات الوصول المسجلة.
3. مبدأ أقل حقوق وصول ممكنة.
4. تقسيم مناطق الشبكة الداخلية.
5. توجيه حزم حركة الشبكة.
6. تقييم حالة سلامة الجهاز.
7. إدارة وصول بيانات اعتماد المستخدمين.
8. فحص بيانات اعتماد المستخدم باستمرار.

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. ت ا ح ق ق ل
2. ة ا ه ي و ل
3. ض ا ع ة و ي ل
4. ح ة ي ر ا م ج د ا
5. ز ة ج ت ا ئ ل
6. ا ز م ي ا ت ل ا
7. ا ي ق ق ل د ت
8. م ه ا ج و ل

نشاط إضافي: فكّر بسرعة

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

1	معلومات لا ينبغي أن تشاركها أبدًا		
2	عادات آمنة يمكنك البدء بها اليوم		
3	أشياء يجري التحقق منها على الجهاز		
4	أشياء تُسجَّل في السجلات		
5	كلمات متعلقة بالأمن السيبراني		
6	أشياء تتحقق منها الثقة المعدومة (Zero Trust)		
7	أماكن تُبرز فيها هويتك في الحياة اليومية		
8	طرق لإثبات أنك أنت فعلًا		
9	أشياء تفعلها بعد تسرّب البيانات		
10	علامات إصابة الحاسوب		
11	أسباب لتحديث البرامج		
12	مستويات الوصول في الشركة		
13	أدوات أمنية تعرفها		
14	مناطق يمكن تقسيم الشبكة إليها		
15	أقوال مأثورة عن الثقة		

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: الانتقال إلى بنية شبكة انعدام الثقة



السيناريو: تستخدم مؤسسة كبيرة حاليًا شبكة داخلية مسطحة يستطيع فيها أي جهاز على الشبكة المحلية الوصول إلى جميع خوادم الشركة وقواعد بياناتها.

سؤال للنقاش: صمّم استراتيجية للتجزئة الدقيقة للشبكة للحد من الحركة الجانبية.

دراسة الحالة 2: نشر ضوابط الوصول بأقل الامتيازات



السيناريو: تكشف سجلات التدقيق أن مستخدمي قواعد البيانات المؤقتين والموظفين ذوي المستوى الأدنى يملكون أذونات قراءة وكتابة شاملة لقواعد بيانات المحاسبة الحرجة.

سؤال للنقاش: دقّق امتيازات IAM في قواعد البيانات وقيّدها لفرض مبدأ الحد الأدنى من الامتيازات.

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	28	25	2	2		1	24	33	1	8		21	21	6	3

29	25	24	1	23	1		29	21	4	23	1		24	1	8	18	25	1

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 Zero Trust؟

انعدام الثقة إطار أمني يفترض وجود التهديدات داخل حدود الشبكة وخارجها، ويتطلب التحقق من كل طلب. [1]

Q2: ما القاعدة الأساسية في Zero Trust؟

لا تثق أبدًا، وتحقق دائمًا.

Q3: ما التجزئة الدقيقة (micro-segmentation)؟

تقسيم الشبكة إلى أجزاء منطقية صغيرة وآمنة للتحكم في حركة المرور واحتواء الاختراقات.

Q4: ما مبدأ الامتيازات الأدنى؟

منح المستخدمين الحد الأدنى فقط من حقوق الوصول اللازمة لأداء مهامهم المحددة. [2]

Q5: ماذا يعني IAM؟

إدارة الهوية والوصول.

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

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: كيف يفيد فحص وضعية الجهاز؟

يتحقق من أن الجهاز محدَّث ويعمل عليه برنامج مكافحة فيروسات نشط وأنه آمن قبل السماح بالوصول.

Q7: ما الحركة الجانبية؟

العملية التي يستخدمها المهاجمون للتنقل عبر شبكة من عقدة مخترقة أولية إلى أنظمة أعلى قيمة.

Q8: هل تحل الثقة المعدومة محل جدران الحماية؟

لا، بل يعززها بإضافة فحوصات تتمحور حول الهوية وجدران حماية للتقسيم الداخلي.

Q9: ما المصادقة المستمرة؟

تحقق مستمر من هوية المستخدم طوال جلسة تسجيل الدخول النشطة، لا عند تسجيل الدخول الأولي فقط.

Q10: لماذا تُعد الشبكة المسطحة خطرة؟

في الشبكات المسطحة، تتيح عقدة واحدة مخترَقة للمهاجمين الوصول بسهولة إلى أي قاعدة بيانات على الشبكة.

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

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

Q1: كيف يعالج Zero Trust نموذج المحيط؟

يحل محل نموذج «القلعة والخندق» القديم، ناقلًا الدفاع من شبكات الحدود إلى هويات مستخدمين وموارد محددة.

Q2: ما نقطة قرار السياسة (PDP)؟

مكوّن النظام الذي يقيّم طلبات التفويض وفق القواعد الأمنية ليقرر ما إذا كان ينبغي منح الوصول.

Q3: ما نقطة تطبيق السياسات (PEP)؟

عقدة النظام (مثل بوابة أو وكيل) التي تسمح فعليًا بطلبات الاتصال أو تحظرها بناءً على قرار PDP.

Q4: كيف يدعم التحكم في الوصول القائم على الأدوار (RBAC) نموذج الثقة المعدومة؟

يجمّع RBAC الأذونات في أدوار محددة، مما يساعد على منع المستخدمين من وراثة امتيازات إدارية مفرطة.

Q5: ما التحكم في الوصول السياقي؟

تقييم طلبات تسجيل الدخول باستخدام أدلة ثانوية مثل الموقع الجغرافي ووضع الجهاز ووقت تسجيل الدخول لتقدير المخاطر.

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

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

Q6: بماذا تختلف التجزئة الدقيقة عن شبكات VLAN القياسية؟

تقسّم شبكات VLAN الشبكات إلى أجزاء منطقية واسعة على الطبقة 2، بينما تستخدم التجزئة الدقيقة سياسة برمجية لعزل أحمال العمل الفردية.

Q7: ما الوصول في الوقت المناسب (JIT)؟

منح أذونات إدارية مرتفعة مؤقتًا وإلغاؤها تلقائيًا بمجرد انتهاء المهمة.

Q8: كيف تؤمّن واجهات API في إطار الثقة المعدومة؟

باشتراط رموز OAuth موقّعة تشفيريًا وتدقيق تواقيع الطلبات عند كل بوابة API.

Q9: ما عميل الوصول إلى الشبكة بنموذج الثقة المعدومة (ZTNA)؟

وكيل برمجي ينشئ اتصالات صادرة آمنة ومشفّرة بتطبيقات محددة بدلًا من الشبكات الفرعية الخام.

Q10: كيف يساعد تدقيق السجلات في Zero Trust؟

يتيح التسجيل المستمر لأدوات التحليلات الأمنية الآلية اكتشاف الحالات الشاذة وتعليق عمليات تسجيل الدخول المارقة فورًا.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

تستبدل بنى انعدام الثقة نموذج القلعة والخندق القديم بقواعد تحقق تتمحور حول الهوية.

2. نظرة على الأمن

يقلص التقسيم الدقيق للشبكة المساحة التي تصل إليها البرمجيات الخبيثة بعزل أحمال العمل في مناطق صغيرة محمية.

3. نظرة على الأمن

يركّز انعدام الثقة على حماية الموارد مثل الأصول والخدمات والحسابات بدلًا من أجزاء الشبكة. [1]

4. نظرة على الأمن

تقلل سياسات الوصول بأقل الامتيازات من خطر تسرب البيانات من قواعد البيانات الأساسية على يد المطلعين من الداخل.

5. نظرة على الأمن

يتحقق التحقق من وضع الجهاز من مستويات تحديث نظام التشغيل وحالة برنامج مكافحة الفيروسات النشطة في الوقت الفعلي.

6. نظرة على الأمن

يمكن لوسطاء الوصول إلى الشبكة بانعدام الثقة (ZTNA) استبدال شبكات VPN المؤسسية أو استكمالها لتقييد نطاق وصول المستخدم.

7. رؤية حول الأمان

يقلل تفويض الامتيازات الإدارية في الوقت المناسب (JIT) خطر سرقة بيانات الاعتماد على وحدات تحكم النطاق.

8. رؤية حول الأمان

تسجل عمليات التحقق المستمر سلوك الجلسات وتدققه، وتعلّق المستخدمين الذين تظهر لديهم أنماط تنفيذ نصوص شاذة.

9. رؤية حول الأمان

تفشل الدفاعات المحيطية التقليدية في حظر الهجمات الجانبية بمجرد تسرب بيانات اعتماد إدارية.

10. نظرة على الأمن

يقدم المنشور الخاص NIST Special Publication 800-207 (2020) تعريفًا مجردًا لبنية انعدام الثقة (Zero Trust) مع نماذج النشر. [1]

المراجع والمصادر التقنية

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

المراجع الأكاديمية والصناعية

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

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

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

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

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 السؤال 1 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما المبدأ الأساسي لأمان انعدام الثقة (Zero Trust)؟ ← لا تثق أبدًا، تحقق دائمًا من كل طلب وصول بغض النظر عن مصدره

2 السؤال 2 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما هو التقسيم الدقيق للشبكة؟ ← تقسيم الشبكات إلى مناطق صغيرة معزولة لاحتواء الحركة الجانبية

3 السؤال 3 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما مبدأ الامتياز الأدنى؟ ← تقييد أذونات وصول المستخدم بما هو ضروري لعمله فقط

4 السؤال 4 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما إدارة الهوية والوصول (IAM)؟ ← أطر تدير الهويات الرقمية وتتحكم في امتيازات النظام

5 السؤال 5 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ماذا تعني المصادقة المستمرة؟ ← التحقق المتكرر من هوية المستخدم ووضع الجهاز أثناء جلسة نشطة

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: لا تمنح الثقة المعدومة (Zero Trust) أي ثقة ضمنية بناءً على موقع الشبكة، داخلها أو خارجها.

7 السؤال 7

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

صحيح: المناطق الصغيرة المعزولة تحد من مدى تحرك المتسلل بين الخوادم.

8 السؤال 8

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: يمنح مبدأ الحد الأدنى من الامتيازات الحد الأدنى من الوصول الذي يحتاجه كل دور فقط.

9 السؤال 9

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يتحقق التحقق المستمر من سلامة الجهاز وبيانات الاعتماد طوال جلسة تسجيل الدخول.

10 السؤال 10

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يقلل تطبيق نموذج انعدام الثقة من أثر اختراق بيانات تسجيل دخول الشركة.

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

G 1. التحقق	F 2. التجزئة	A 3. IAM	B 4. الامتياز
H 5. الوضع الأمني	E 6. التدقيق	D 7. جدار الحماية	C 8. جهاز التوجيه

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 التحقق	2 التجزئة	3 IAM	4 امتياز
5 وضعية	6 التدقيق		

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

1 G – جدارحماية	2 F – التدقيق	3 D – الامتياز	4 B – التجزئة
5 H – الموجه	6 E – الوضعية	7 C – الهوية	8 A – التحقق

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح التحقق والتجزئة وIAM بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

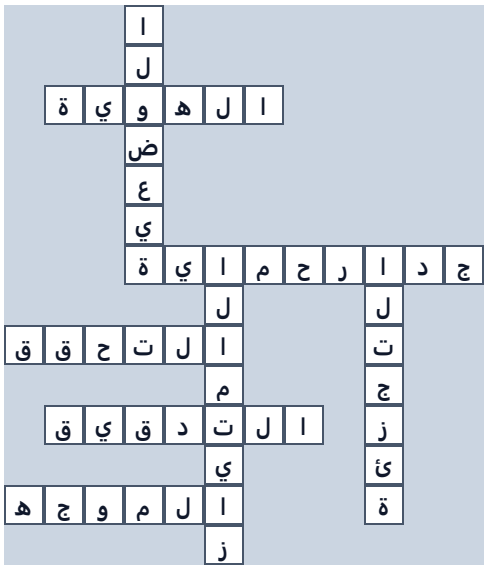
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

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

حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

2 أفقي: الهوية إدارة وصول بيانات اعتماد المستخدمين (6 حروف)

3 أفقي: جدارحماية حماية الحاجز الخارجي للشبكة (9 حروف)

6 أفقي: التحقق فحص بيانات اعتماد المستخدم باستمرار (6 حروف)

7 أفقي: التدقيق مراجعة جلسات الوصول المسجلة (7 حروف)

8 أفقي: الموجه توجيه حزم حركة الشبكة (6 حروف)

عمودي

1 عمودي: الوضعية تقييم حالة سلامة الجهاز (7 حروف)

4 عمودي: التجزئة تقسيم مناطق الشبكة الداخلية (7 حروف)

5 عمودي: الامتياز مبدأ أقل حقوق وصول ممكنة (8 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. تاحققل ← **التحقق**
2. ةاهيول ← **الهوية**
3. ضاعةويل ← **الوضعية**
4. حةيرامجدا ← **جدارحماية**
5. زةجتائل ← **التجزئة**
6. ازمياتلا ← **الامتياز**
7. ايققلدت ← **التدقيق**
8. مهاجول ← **الموجه**

مفتاح تحدي الشيفرة السرية

"تحقق دائما ببنية انعدام الثقة الآمنة"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: الانتقال إلى بنية شبكة انعدام الثقة

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: تستخدم مؤسسة كبيرة حاليًا شبكة داخلية مسطحة يمكن فيها لأي جهاز على الشبكة المحلية الوصول إلى جميع خوادم الشركة وقواعد بياناتها.
- الاستراتيجية والحل الموصى بهما: قسّم الشبكة المسطحة إلى مناطق أقسام معزولة. وركّب جدران حماية داخلية للتحكم في حركة البيانات بين المناطق، وفرض التحقق من رمز الاتصال لكل وصول.

B دراسة الحالة 2: نشر ضوابط الوصول بأقل الامتيازات

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: تكشف سجلات التدقيق أن مستخدمي قواعد بيانات مؤقتين وموظفين من المستوى الأدنى يملكون أذونات قراءة وكتابة شاملة على قواعد بيانات المحاسبة الحيوية.
- الاستراتيجية والحل الموصى بهما: إلغاء جميع الامتيازات الإدارية الشاملة. وتطبيق التحكم في الوصول القائم على الأدوار (RBAC) بما يطابق الأدوار الوظيفية بدقة، وإنشاء مراجعات أسبوعية آلية للأذونات.