معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

JAZAN UNIVERSITY

دبلوم امن المعلومات

الفصل 4: تصميم الأنظمة المقاومة للهجمات

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

دبلوم امن المعلومات

- **اسم المـقرر:** مبادئ التصميم في الأمن السبراني
- **رمز المـــقرر:** ISE125
- **الموضـــوع:** الفصل 4: تصميم الأنظمة المقاومة للهجمات

أهداف الفصل

- **يطبق** مبادئ تقليل سطح الهجوم والتحصين وافتراض الاختراق على معمارية معطاة.
- **يصمم** حواجز أمنية وتقنيات عزل لخفض نصف قطر الانفجار.
- **يميز** التوافر عن الموثوقية ويقترح آليات مناسبة لكل منهما.
- **يحلل** مسار حركة جانبية محتمل ويقترح حاجزاً يكسره.
- **يقارن** الدفاع الشبكي التقليدي بمنهج الثقة الصفرية على مستوى المبدأ.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

خريطة الفصل

يعالج الفصل ستة محاور مترابطة.

CHAPTER MAP · SIX AXES

ستة محاور مترابطة في الفصل

01
مقاومة الهجمات
وافتراض الاختراق

02
تقليل سطح الهجوم
والحواجز الأمنية

03
التجزئة والعزل
خفض نصف قطر الانفجار

04
التوافر والموثوقية
والتعافي

05
الثقة الصفرية
والمراقبة المستمرة

06
تطبيق قرارات التصميم
على مستندات تعليمية للشركة

يبدأ الفصل بافتراض الاختراق وينتهي بتطبيق قرارات التصميم على مستندات الشركة.

خطة الوحدات الزمنية ومسار البدء

- ابدأ بالوحدة الأولى، ثم أكمل الوحدات بالترتيب.
- تتضمن كل وحدة تمهيداً وأهدافاً خاصة ومحتوى موجهاً ونشاط معالجة معرفة وتقويماً أو مخرجاً محدداً وملخصاً.
- يبلغ زمن كل وحدة 60 دقيقة.
- يوزع الفصل 180 دقيقة لدراسة المحتوى، و90 دقيقة للأنشطة، و60 دقيقة للتقييمات، و30 دقيقة لمرحلة المشروع التراكمي.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

خطة الوحدات الزمنية ومسار البدء (تابع)

الوحدة	خطوات التعلم الإلزامية	الزمن
1	تمهيد وأهداف ودراسة المقاومة 30، نشاط تحليل سطح الهجوم 15، تقويم ذاتي للوحدة 15	60 دقيقة
2	تمهيد وأهداف ودراسة الحواجز والمناطق 30، نشاط قراءة A1 15، الجزء الأول من الواجب 15	60 دقيقة
3	تمهيد وأهداف ودراسة العزل والحركة الجانبية 30، نشاط تحليل A3 15، الجزء الثاني من الواجب 15	60 دقيقة
4	تمهيد وأهداف ودراسة التوافر والتعافي 30، نشاط قرار الفشل الآمن 15، الجزء الثالث من الواجب 15	60 دقيقة

خطة الوحدات الزمنية ومسار البدء (تابع)

الوحدة	خطوات التعلم الإلزامية	الزمن
5	تمهيد وأهداف ودراسة الثقة الصفرية والمراقبة 30، نشاط مقارنة المنهجين 15، المرحلة الأولى من المشروع 15	60 دقيقة
6	تمهيد وأهداف وتحليل A2 و A4 30، نشاط تصميم الحواجز 15، المرحلة الثانية من المشروع 15	60 دقيقة
الإجمالي	دراسة المحتوى 180، الأنشطة 90، التقييمات 60، المشروع التراكمي 30	360 دقيقة

- تعليمات البدء: دوّن إجابة كل نشاط في ملف تعلمك، ثم قارنها بالإجابة النموذجية التالية مباشرة.
- نفذ الاختبار القصير بعد إكمال وحدات الفصل، وأنجز أجزاء الواجب الثلاثة في الوحدات الثانية والثالثة والرابعة.
- استخدم منتدى المقرر للأسئلة العلمية، وقيّم وضوح الوحدة في أداة التغذية الراجعة في المنصة بعد إكمالها.

مقاومة الهجمات

مقاومة الهجمات هي تصميم النظام لحماية العمليات والأصول أمام التهديدات، وتقليل الضرر، ودعم الاستمرار أو الاستعادة.

لا تقتصر المقاومة على منع نقطة الدخول الأولى. في الشركة، ينبغي أن يحافظ التصميم على حماية بيانات العملاء حتى عند تعطل مكوّن أو تأثر خدمة، عبر حدود ثقة وضوابط واستجابة وتعافٍ مترابطة.

افتراض الاختراق (Assume Breach)

افتراض الاختراق هو أن يتعامل المصمم مع احتمال تأثر أصل أو حساب أو نقطة دخول.

لذلك لا يمنح الثقة لمستخدم أو جهاز بسبب موقعه الشبكي فقط. في تقرير الحادثة التعليمي، استخدمت بيانات اعتماد صحيحة من جهاز غير معتمد، لكن التحقق من الجهاز والجدار الناري الداخلي حدّا من الوصول اللاحق.

تقليل سطح الهجوم

تقليل سطح الهجوم (Attack Surface Reduction) يعني حصر الوظائف والخدمات والواجهات والاتصالات اللازمة للغرض التشغيلي.

كل خدمة غير لازمة أو اتصال غير مبرر يضيف فرصة تعرض محتملة. في نموذج المناطق، لا تستقبل منطقة التطبيقات اتصالات مباشرة من الإنترنت أو شبكة الزوار، لأن وصولها يمر عبر مسار محدد ومبرر.

التحصين

التحصين (Hardening) يقوي المكونات ويقلل الخدمات غير الضرورية ويضبط التهيئة ويحافظ على أمنها.

لكنه لا يعوض غياب تصميم معماري آمن. في حالة خدمة معالجة المرفقات، لا يكفي تقوية الخادم وحده، بل يجب عزله عن منطقة البيانات وتشغيله بحساب منخفض الصلاحيات لتقليل الأثر المحتمل.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

نشاط الوحدة الأولى: تقليل سطح خدمة المرفقات

- خصص 15 دقيقة لتحليل خدمة معالجة المرفقات.
- اكتب ثلاث وظائف أو اتصالات ينبغي أن تبقى ضرورية لتلقي الملف وفحصه وتمرير الملف السليم.
- ثم اكتب وظيفتين أو اتصالين لا يحتاجهما المسار، مثل الوصول المباشر إلى منطقة البيانات.
- اختر إجراء تحصين واحداً، واربطه بسبب تقليل فرصة التعرض أو الحد من الأثر.

إجابة نشاط الوحدة الأولى

- يبقي التصميم استقبال الملف في البوابة، وفحصه في بيئة رملية، وتمرير الملف السليم إلى خدمة التطبيق.
- ويحظر اتصال خدمة المعالجة المباشر بمنطقة البيانات أو منحها صلاحية إدارية.
- يكون التحصين بتشغيل الخدمة بحساب منخفض الصلاحيات.
- يحقق القرار تقليل سطح الهجوم، ويحد أثر خدمة معالجة متأثرة قبل وصولها إلى بيانات العملاء.

الحواجز الأمنية (Security Barriers)

الحواجز الأمنية ضوابط تفصل بين أصل أو منطقة أو مستوى ثقة وآخر، وتقيّد الوصول أو تدفق البيانات.

ترتبط قيمة الحاجز بالتهديد أو المسار الذي يعالجه، لا بوجوده الشكلي. في سجل المخاطر، يعالج فحص المرفقات المعزول الخطر R-17، ويكمله منع اتصال خدمة المعالجة المباشر بمنطقة البيانات.

الجدار الناري (Firewall)

- الجدار الناري حاجز أمني يقيّد تدفقات اتصال محددة بين المناطق أو الأصول.
- وظيفته فرض حدود الاتصال التي يبررها التصميم، ولا يمثل ضماناً منفرداً للأمن.
- **الوظيفة:** تقييد تدفقات الاتصال بين مستويات الثقة.
- **المسؤوليات:** تعريف التدفقات المسموحة، رفض المسارات غير المبررة، فصل المناطق، دعم تقليل الحركة الجانبية، مراجعة الاستثناءات.
- القواعد والمعايير: NIST SP 800-53 Rev.
- 5, NIST CSF 2.0, NIST SP 800-207.
- **الأجهزة أو الأدوات:** جدار ناري، بوابة وصول، نقطة تحكم في الوصول، آلية هوية وتفويض.
- **المخرج:** جدول تدفقات مسموحة ومحظورة ومبرراتها.
- **مثال:** يرفض الجدار الناري الداخلي اتصال بوابة الويب أو منطقة الإدارة مباشرة بمنطقة البيانات، ويتيح لخدمات التطبيقات المحددة فقط العمليات المبررة.

الجدار الناري (Firewall) (الشكل)

FIREWALL · TRUST BOUNDARY

الجدار الناري

المرسل
بوابة الويب / الإدارة

رفض مباشر

الجدار الناري
Firewall
حاجز بين مستويات الثقة

خدمات مبررة

المستقبل
منطقة البيانات

الأجهزة

- جدار ناري
  Firewall
- بوابة وصول
- نقطة تحكم في الوصول
- آلية هوية وتفويض

بين المناطق أو الأصول

البروتوكولات والمعايير

- NIST SP 800-53 Rev. 5
- NIST CSF 2.0
- NIST SP 800-207

فرض حدود يبررها التصميم
وليس ضماناً منفرداً للأمن

الوظائف الرئيسية

- تقييد تدفقات الاتصال
- تعريف التدفقات المسموحة
- رفض المسارات غير المبررة
- فصل المناطق
- تقليل الحركة الجانبية
- مراجعة الاستثناءات
- جدول تدفقات ومبررات

يرفض الاتصال المباشر بمنطقة البيانات ويتيح فقط خدمات التطبيقات المبررة.

الكشف الشبكي (Network Detection)

- الكشف الشبكي يدعم معرفة النشاط أو الحدث الذي يحتاج إلى تحليل واستجابة، ولا يساوي المنع.
- يربط المصمم التنبيه بسياق الأصل والمسار حتى تتحول المراقبة إلى قرار استجابة قابل للمراجعة.
- **الوظيفة:** إظهار الأحداث التي تستوجب التحليل والاستجابة.
- **المسؤوليات:** جمع الأدلة التشغيلية، رصد النشاط غير المعتاد، ربط الحدث بالأصل، حفظ السجلات، دعم التحسين.
- القواعد والمعايير: NIST CSF 2.0, NIST SP 1299, NIST SP 800-53 Rev 5.
- **الأجهزة أو الأدوات:** مصادر مراقبة، سجلات تدقيق، بوابات وصول، نقاط إنفاذ سياسة.
- **المخرج:** تنبيه موثق ومسار حدث وأدلة للتحليل.
- **مثال:** صدر تنبيه التقرير INC-2026-0417 من المراقبة المستمرة في منطقة الإدارة، ثم حفظت السجلات لتحديد المسار المرصود.

الكشف الشبكي (Network Detection) (الشكل)

NETWORK DETECTION

الكشف الشبكي (Network Detection)

الأجهزة

- مصادر مراقبة
- سجلات تدقيق
- بوابات وصول
- نقاط إنفاذ سياسة

البروتوكولات والمعايير

- NIST CSF 2.0
- NIST SP 1299
- NIST SP 800-53 Rev. 5

الوظائف الرئيسية

- إظهار أحداث التحليل
- جمع الأدلة التشغيلية
- رصد النشاط غير المعتاد
- ربط الحدث بالأصل
- حفظ السجلات
- دعم التحسين

الكشف يدعم معرفة الحدث ولا يساوي المنع؛ التنبيه يُربط بسياق الأصل والمسار ليصبح قرار استجابة قابلاً للمراجعة.

المنع الشبكي (Network Prevention)

- المنع الشبكي يوقف أو يقيّد نشاطاً غير مسموح وفق سياسة وضابط مناسبين.
- يوازن المصمم بين منع المسار الضار واستمرار الخدمة واحتمال الحجب الخاطئ، ثم يحدد إجراءً مكملاً عند الحاجة.
- **الوظيفة:** تقييد النشاط غير المسموح قبل انتقال أثره.
- **المسؤوليات:** تطبيق سياسة المنع، تحديد المسارات المحظورة، تقييد المحاولات المتكررة، تسجيل القرار، مراجعة الأثر التشغيلي.
- القواعد والمعايير: NIST SP 800-53 Rev 5, NIST CSF 2.0, NIST SP 1299.
- **الأجهزة أو الأدوات:** جدار ناري، بوابة وصول، نقاط تحكم في الوصول، مصادر مراقبة.
- **المخرج:** قرار منع موثق وتنبيه وإجراء استمرارية.
- **مثال:** في R-20 يقيّد تحديد معدل الطلبات محاولات التخمين، ويكمله قفل مؤقت متدرج وتنبيه العميل.

(الشكل) المنع الشبكي (Network Prevention)

NETWORK PREVENTION

المنع الشبكي

الأجهزة

- جدار ناري
- بوابة وصول
- نقاط تحكم في الوصول
- مصادر مراقبة
- قفل مؤقت متدرج

البروتوكولات والمعايير

- NIST SP 800-53 Rev. 5
- NIST CSF 2.0
- NIST SP 1299
- سياسة وضابط مناسبان
- قرار منع موثق

الوظائف الرئيسية

- تقييد النشاط غير المسموح
- تطبيق سياسة المنع
- تحديد المسارات المحظورة
- تقييد المحاولات المتكررة
- تسجيل القرار
- مراجعة الأثر التشغيلي
- تنبيه وإجراء استمرارية

يوازن المصمم بين منع المسار الضار واستمرار الخدمة واحتمال الحجب الخاطئ.
في R-20 يقيّد تحديد معدل الطلبات محاولات التخمين ويكمله تنبيه العميل.

التجزئة الشبكية (Network Segmentation)

- التجزئة الشبكية تنظيم للبيئة في مناطق موارد ذات مستويات ثقة وضوابط اتصال محددة.
- وظيفتها تقليل الانتشار المحتمل للحادث وفرض نقاط تحكم واضحة.
- **الوظيفة:** تقليل نطاق الضرر المحتمل.
- **المسؤوليات:** تصنيف الأصول حسب حساسيتها، تحديد حدود الثقة، تعريف التدفقات المبررة، منع الوصول الجانبي غير اللازم، مراجعة الاستثناءات الموثقة.
- **البروتوكولات والمعايير:** NIST CSF 2.0، NIST SP 800-207، NIST SP 800-53 Rev. 5.
- **الأجهزة:** جدران نارية، بوابات وصول، نقاط تحكم في الوصول، آليات الهوية والتفويض.
- **المخرج:** مخطط مناطق ثقة وجدول تدفقات مسموحة.
- **مثال:** تفصل الشركة منطقة معالجة المرفقات عن منطقة البيانات ولا تسمح لها باتصال مباشر.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

التجزئة الشبكية (Network Segmentation) (الشكل)

NETWORK SEGMENTATION

التجزئة الشبكية

الوظائف الرئيسية

- تقليل نطاق الضرر
- تصنيف الأصول
- تحديد حدود الثقة
- تعريف التدفقات المبررة
- منع الوصول الجانبي
- مراجعة الاستثناءات

البروتوكولات والمعايير

- NIST SP 800-53 Rev. 5
- NIST SP 800-207
- NIST CSF 2.0

مخطط مناطق وجدول تدفقات

الأجهزة

- جدران نارية
- بوابات وصول
- نقاط تحكم في الوصول
- آليات الهوية والتفويض

مناطق موارد بمستويات ثقة وضوابط اتصال محددة تقلّل انتشار الحادث.

المناطق الأمنية (Security Zones)

المنطقة الأمنية مجموعة أصول أو تدفقات لها مستوى ثقة ومتطلبات حماية متقاربة، وتفصلها نقاط تحكم واضحة.

في الشركة، تضم المنطقة العامة الإنترنت وشبكة الزوار، بينما تضم منطقة البيانات قواعد بيانات العملاء وسجلات المعاملات. هذا الفصل يساعد المصمم على تبرير كل اتصال بدلاً من افتراض أن كل الأصول الداخلية متساوية الثقة.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

المنطقة المنزوعة السلاح (DMZ)

المنطقة المنزوعة السلاح (DMZ) منطقة وسيطة لخدمات تتطلب اتصالاً من بيئات أقل ثقة، مع تجنب منحها وصولاً مباشراً وغير مقيد للأصول الداخلية الحساسة.

في نموذج الشركة، تستضيف هذه المنطقة بوابة الويب العامة وواجهة استقبال الطلبات. تمر الطلبات عبر حاجز تطبيقات ويب قبل وصولها إلى خدمة التطبيق.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

نشاط الوحدة الثانية: قراءة مسارات المناطق

- خصص 15 دقيقة لقراءة A1. دوّن مساراً مسموحاً ضرورياً يبدأ بالعميل وينتهي بعملية محددة على قاعدة البيانات.
- ثم دوّن مسارين محظورين صراحة، وحدد في كل منهما المنطقة الأقل ثقة والأصل الحساس الذي تحميه قاعدة الحظر.
- اختم بذكر حاجز أو نقطة تحقق تبرر قرارك.

إجابة نشاط الوحدة الثانية

- المسار الضروري هو العميل إلى بوابة الويب في المنطقة المنزوعة السلاح، ثم الطلبات الموثقة إلى خدمات التطبيقات، ثم عمليات محددة على قاعدة البيانات.
- يحظر اتصال شبكة الزوار مباشرة بمنطقة البيانات، ويحظر اتصال بوابة الويب مباشرة بمنطقة الإدارة أو البيانات.
- يحمي الحظر الأصول الحساسة من تدفقات لا تحتاجها، ويجعل خدمة التطبيق الوسيط المصرح به.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

العزل الشبكي (Network Isolation)

العزل الشبكي يقيد الاتصال بين الشبكات أو المناطق أو التدفقات، ويقلل إمكان انتقال الأثر من أصل متأثر إلى أصل آخر.

في الشركة، يحظر افتراضياً اتصال شبكة الزوار أو بوابة الويب بمنطقة البيانات أو الإدارة. العزل لا يغني عن المصادقة والتفويض، لكنه يضيف حداً معمارياً يقلل الحركة غير الضرورية بين الموارد.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

العزل على مستوى المضيف

عزل المضيف (Host Isolation) يقيد ما يستطيع نظام أو حساب أو عملية الوصول إليه داخل البيئة الحاسوبية نفسها.

يكمل العزل الشبكي عندما لا تكون الشبكة وحدها حداً كافياً للحماية. في الخطر R-19، يحد تشغيل خدمات التطبيقات بحسابات خدمة منفصلة ومحدودة الصلاحيات من قدرتها على قراءة سجلات لا تحتاج إليها أو تعديلها.

العزل بالحاويات

العزل بالحاويات (Container Isolation) قرار لتقليل تداخل أعباء العمل ومكوّنات التطبيق.

لا تعد الحاوية حداً أمنياً مضموناً وحدها، بل تحتاج إلى هوية وصلاحيات وتهيئة ومراقبة مناسبة. في خدمة معالجة المرفقات، يمكن حصر المهمة في بيئة عمل مقيدة ومنفصلة عن قاعدة البيانات، مع منع الاتصالات غير اللازمة إلى المناطق الداخلية.

البيئة الرملية (Sandbox)

البيئة الرملية (Sandbox) بيئة مقيدة لتشغيل أو فحص مكوّن مع تقليل قدرته على الوصول إلى الموارد الحساسة.

وظيفتها تقليل أثر المحتوى غير الموثوق، لا ضمان سلامة المحتوى بصورة مطلقة. في الشركة، تفحص منطقة معالجة المرفقات الملفات الواردة قبل تمرير الملفات السليمة إلى خدمة التطبيق، دون اتصال مباشر بقاعدة البيانات.

نصف قطر الانفجار (Blast Radius)

نصف قطر الانفجار هو نطاق الأصول أو البيانات أو الوظائف التي قد تتأثر عند اختراق مكوّن أو حساب.

يخفضه المصمم بالعزل وأقل الامتيازات وفصل المناطق. في حالة خادم ويب متأثر، يمنع فصل طبقة الويب عن منطقة البيانات تحول الحادث إلى وصول مباشر لسجلات العملاء أو النسخ التشغيلية.

الحركة الجانبية (Lateral Movement)

الحركة الجانبية انتقال الخصم بعد نقطة دخول أولية إلى أصول أو حسابات أو خدمات أخرى.

يركز تحليلها على ما يستطيع الأصل المتأثر الوصول إليه لاحقاً. في التقرير INC-2026-0417، انتقل المسار المرصود من جهاز غير موثوق إلى حساب موظف ثم لوحة الدعم، قبل أن يرفض الجدار الناري الداخلي محاولة الوصول إلى منطقة البيانات.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

نشاط الوحدة الثالثة: كسر الحركة الجانبية

- خصص 15 دقيقة لتحليل تقرير INC-2026-0417. اكتب المسار المرصود بترتيبه، ثم حدد الحاجز الذي رفض الجلسة الإدارية والحاجز الذي رفض الوصول إلى منطقة البيانات.
- اشرح في جملتين كيف خفض كل حاجز نصف قطر الانفجار.
- لا تضف سبباً للحصول على بيانات الاعتماد، لأن التقرير لا يثبت طريقة الحصول عليها.

إجابة نشاط الوحدة الثالثة

- المسار هو جهاز غير موثوق، ثم حساب الموظف، ثم لوحة الدعم الداخلية، ثم محاولة الوصول إلى خدمة في منطقة البيانات.
- رفض التحقق من حالة الجهاز الجلسة الإدارية لعدم تحقق متطلبات الثقة.
- ورفض الجدار الناري الداخلي الاتصال من منطقة الإدارة إلى منطقة البيانات.
- حدّ الحاجزان من انتقال الأثر، ولم يظهر دليل على الوصول إلى سجلات العملاء أو تعديلها.

التوافر (Availability)

التوافر هو قدرة المستخدم أو العملية المصرح لها على الوصول إلى خدمة أو مورد عند الحاجة.

لا يعني التوافر فتح الوصول عند تعطل ضابط أمني. في نموذج الشركة، عند تعطل خدمة المصادقة ترفض المنصة الوصول إلى وظائف العملاء والإدارة، مع الإبقاء على المحتوى العام للقراءة فقط حيثما أمكن، حفاظاً على أمن الخدمة.

الموثوقية (Reliability)

الموثوقية هي قدرة النظام على أداء وظيفته المتوقعة باستمرار ضمن شروط محددة.

ترتبط بتحمل الأعطال والتعافي، لكنها ليست مرادفاً للتوافر. قد تكون الخدمة متاحة مؤقتاً، لكنها لا تؤدي وظيفتها بصورة صحيحة أو متسقة. لذلك يحدد المصمم الخدمات الحرجة وتبعياتها وسلوكها عند الفشل، ثم يختبر الاستعادة والتحسين.

التكرار (Redundancy)

التكرار هو وجود مكوّنات أو مسارات بديلة مخطط لها لتقليل أثر فشل مكوّن واحد.

لا يكفي تكرار الخدمة إذا كانت البدائل غير محمية أو غير خاضعة للهوية والتدقيق. في بوابة دفع تعليمية، يحدد المصمم البديل ومسار الخدمة والتبعيات، ثم يراجع أن الانتقال إلى البديل لا يمنح صلاحيات أوسع أو يضعف تكامل المعاملة.

التجاوز عند الفشل (Failover)

التجاوز عند الفشل (Failover) انتقال الخدمة أو الحمل إلى مكوّن أو مسار بديل عند فشل المكوّن الأساسي.

يحدد التصميم متى يحدث الانتقال، وما الذي يظل متاحاً، وما الذي يجب أن يفشل بأمان. في الخدمة الحساسة، لا يجب أن يؤدي انتقال الحمل إلى تجاوز التحقق من الهوية أو منح وصول تلقائي للوظائف الخاصة.

النسخ الاحتياطي الآمن

النسخ الاحتياطي الآمن يدعم القدرة على الاستعادة، مع حماية النسخ ووسائطها وصلاحيات الوصول إليها والتحقق من قابليتها للاستعادة.

في الخطر R-21، قد يؤدي اختراق حساب إداري إلى حذف النسخ أو تشفيرها. لذلك تستخدم الشركة نسخاً معزولة غير قابلة للتعديل لفترة احتفاظ محددة، وتفصل صلاحيات تشغيل النسخ عن إدارة المنصة.

التعافي من الكوارث (Disaster Recovery)

التعافي من الكوارث ينظم العودة المخططة للخدمات أو البيانات بعد تعطل جسيم أو حادث مؤثر.

يرتبط بوظيفة التعافي (Recover) في إطار NIST CSF 2.0، وبأولويات الخدمات والنسخ الاحتياطي وخطط الاستعادة. لا يكفي وجود نسخة احتياطية، بل يجب أن تحدد الخطة ما يستعاد أولاً وكيف يتحقق الفريق من سلامة الخدمة المستعادة.

الفشل الآمن (Fail-Safe)

الفشل الآمن يعني ألا يؤدي تعطل خدمة أو فقدان ضابط مساند إلى توسيع الوصول أو تجاوز التحقق أو كشف بيانات حساسة.

في الشركة، إذا تعطلت المصادقة، ترفض المنصة الوظائف الخاصة ولا تمنح صلاحيات تلقائية. القرار يوازن بين استمرار المحتوى العام وحماية العمليات التي تحتاج إلى تحقق من هوية المستخدم وتفويضه.

نشاط الوحدة الرابعة: قرار توافر آمن

- خصص 15 دقيقة لمقارنة بديلين عند تعطل خدمة المصادقة المركزية.
- البديل الأول يتيح وظائف العملاء والإدارة تلقائياً.
- البديل الثاني يرفض الوظائف الخاصة ويبقي المحتوى العام للقراءة فقط حيثما أمكن.
- اختر البديل الأنسب، ثم اذكر أثره في السرية والتوافر، واذكر آلية واحدة تدعم الاستعادة دون توسيع الصلاحيات.

إجابة نشاط الوحدة الرابعة

- البديل الأنسب هو رفض الوظائف الخاصة وإبقاء المحتوى العام للقراءة فقط حيثما أمكن.
- يحمي القرار السرية لأنه لا يمنح وصولاً غير موثق، ويحقق توافراً محدوداً للمحتوى العام.
- يمكن أن يدعم التكرار أو التجاوز عند الفشل الاستمرارية، بشرط استمرار التحقق من الهوية والتدقيق في المسار البديل.
- هذا سلوك فشل آمن لا فشل مفتوح.

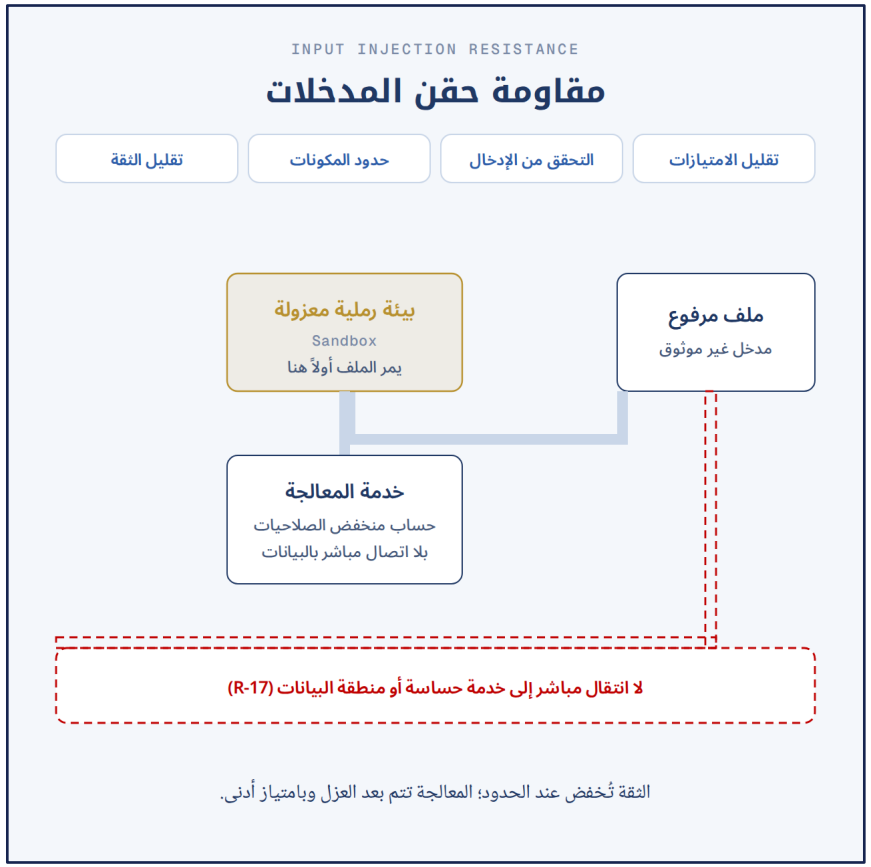
معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مقاومة القوة الغاشمة

- **مقاومة القوة الغاشمة (Brute-Force Resistance)** تعالج محاولات التخمين المتكرر ضمن تصميم الهوية والوصول.
- تستخدم ضوابط حماية ومراقبة مناسبة، مع تجنب رسائل واجهة تكشف معلومات تساعد التخمين.
- في الخطر R-20 المبين في سجل المخاطر اللاحق، يجمع التصميم بين تحديد معدل الطلبات، والتحقق الإضافي عند زيادة المحاولات، والقفل المؤقت المتدرج، والرفض الآمن عند تعطل المصادقة.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مقاومة حقن المدخلات



- **مقاومة حقن المدخلات (Input Injection Resistance)** تعالج تقليل الثقة بالمدخلات وضبط حدود المكونات والتحقق من الإدخال وتقليل الامتيازات.
- في الخطر R-17 المبين في سجل المخاطر اللاحق، لا ينتقل الملف المرفوع مباشرة إلى خدمة حساسة.
- يمر أولاً ببيئة رملية معزولة، ثم تعمل خدمة المعالجة بحساب منخفض الصلاحيات ومن دون اتصال مباشر بمنطقة البيانات.

الثقة الصفرية (Zero Trust)

- الثقة الصفرية نموذج يركز على حماية المستخدمين والأصول والموارد، ولا يمنح ثقة ضمنية بسبب الموقع أو ملكية الأصل.
- ينفذ التحقق قبل إنشاء جلسة المورد، ويكمل حدود الشبكة ولا يلغي قيمتها.
- **الوظيفة:** حماية الموارد قبل إنشاء الجلسة.
- **المسؤوليات:** توثيق الموارد، تحديد الأصل المطلوب حمايته، التحقق من هوية المستخدم، التحقق من حالة الجهاز، تفويض وصول مناسب، مراقبة الأحداث ومراجعة الضوابط.
- الأطر والمعايير: NIST SP 800-207, NIST CSF 2.0, NIST SP 1299.
- **الأجهزة أو الأدوات:** نقاط إنفاذ سياسة، ضوابط هوية ووصول، مصادر مراقبة، بوابات وصول.
- **المخرج:** خريطة موارد وسياسة وصول ونقاط تحقق.
- **مثال:** لا يسمح لحساب موظف بالدخول إلى الإدارة من جهاز جديد قبل التحقق من هويته وحالة جهازه.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

الثقة الصفرية (Zero Trust) (الشكل)

ZERO TRUST · NIST SP 800-207

الثقة الصفرية (Zero Trust)

لا ثقة ضمنية للموقع أو ملكية الأصل · التحقق قبل إنشاء الجلسة

الأجهزة

- نقاط إنفاذ سياسة
- ضوابط هوية ووصول
- مصادر مراقبة
- بوابات وصول

البروتوكولات والمعايير

- NIST SP 800-207
- NIST CSF 2.0
- NIST SP 1299

المخرج: خريطة موارد
وسياسة وصول ونقاط تحقق

الوظائف الرئيسية

- حماية الموارد قبل الجلسة
- توثيق الموارد
- تحديد الأصل المطلوب حمايته
- التحقق من هوية المستخدم
- التحقق من حالة الجهاز
- تفويض وصول مناسب
- مراقبة الأحداث ومراجعة الضوابط

يكمل حدود الشبكة ولا يلغي قيمتها، ولا يمنح ثقة ضمنية بسبب الموقع.

الفرق بين الدفاع المحيطي والثقة الصفرية

- يركز الدفاع الشبكي التقليدي على حماية حدود الشبكة والمناطق، ولذلك يمثل الجدار الناري وحدود الثقة عناصر مهمة فيه.
- **أما الثقة الصفرية (Zero Trust)** فتركز على حماية المورد نفسه، ولا تمنح الثقة لمستخدم أو جهاز بسبب موقعه فقط.
- يبقى التقسيم مفيداً، لكن الوصول إلى مورد حساس يحتاج تحققاً من هوية المستخدم وحالة الجهاز وتفويضاً مناسباً قبل الجلسة.

جانب المقارنة	الدفاع المحيطي التقليدي	الثقة الصفرية
مركز الحماية	حدود الشبكة والمناطق	المستخدمون والأصول والموارد
أساس الثقة	الموقع قد يؤثر في قرار الثقة	لا ثقة ضمنية بسبب الموقع
قرار الوصول	ضوابط عند الحدود	تحقق وتفويض قبل جلسة المورد

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

نشاط الوحدة الخامسة: مقارنة قرار الوصول

- خصص 15 دقيقة لمقارنة طلب وصول إلى لوحة الدعم من جهاز جديد.
- اكتب كيف يتعامل دفاع محيطي تقليدي مع موقع الجهاز وحدود المنطقة، ثم اكتب ما الذي تضيفه الثقة الصفرية قبل جلسة المورد.
- اختم بقرار وصول من سطرين يذكر هوية المستخدم وحالة الجهاز والتفويض المطلوب.

إجابة نشاط الوحدة الخامسة

- يحمي الدفاع المحيطي لوحة الدعم بفصل منطقة الإدارة وحدودها، لكنه لا يجعل الموقع سبباً كافياً لقبول الطلب.
- تضيف الثقة الصفرية التحقق من هوية المستخدم وحالة الجهاز والتفويض الملائم قبل الجلسة.
- في حالة جهاز جديد، لا يمنح الوصول إلى لوحة الدعم حتى تحقق المتطلبات.
- يبقى الجدار الناري الداخلي حاجزاً إضافياً يمنع انتقال الجلسة إلى منطقة البيانات.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

المراقبة المستمرة (Continuous Monitoring)

المراقبة المستمرة تدعم الكشف والتحليل والاستجابة والتحسين، ولا تقتصر على جمع السجلات دون غرض أو حماية.

تربط الأدلة التشغيلية بقرارات المخاطر والضوابط. في التقرير INC-2026-0417، أسهمت المراقبة في اكتشاف نشاط من جهاز غير معتمد، ثم حفظ السجلات وتعليق الجلسة وإعادة التحقق من هوية المستخدم.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مستند تطبيقي: مخطط المناطق الأمنية

النموذج: نموذج اعتماد المناطق الأمنية والتجزئة

شركة الحلول التقنية والخدمات الرقمية
تطوير وإدارة المنصات الرقمية والخدمات السحابية
جازان، المملكة العربية السعودية
الرقم الضريبي: 300000000000003 · السجل التجاري: 1010000000
هاتف: 0500000000

نموذج اعتماد المناطق الأمنية والتجزئة

تاريخ المراجعة: 2026-03-12

النطاق التشغيلي: منصة رقمية تقدم خدمات سحابية لعملاء من منشآت سعودية، مع بوابة ويب عامة ولوحة إدارة داخلية وخدمة لمعالجة المرفقات.

المنطقة العامة: الإنترنت وشبكة الزوار. لا تحتوي على بيانات عملاء أو حسابات إدارية، ولا يسمح منها بالوصول المباشر إلى أي خادم داخلي.

المنطقة المنزوعة السلاح: تستضيف بوابة الويب العامة وواجهة استقبال الطلبات. تمر جميع الطلبات عبر حاجز تطبيقات ويب قبل وصولها إلى خدمة التطبيق.

منطقة التطبيقات: تستضيف خدمات المنصة وواجهات البرمجة التي تعالج الطلبات المصرح بها فقط. لا تستقبل اتصالات مباشرة من شبكة الزوار أو الإنترنت.

منطقة البيانات: تحتوي على قواعد بيانات العملاء وسجلات المعاملات والنسخ التشغيلية. يسمح بالوصول إليها من خدمات التطبيقات المحددة فقط وبحسابات خدمة محدودة الصلاحية.

منطقة الإدارة: تحتوي على محطات فريق الدعم وأدوات المراقبة الإدارية. يتطلب الدخول إليها مصادقة متعددة العوامل وجهازاً إدارياً معتمداً.

منطقة معالجة المرفقات: بيئة رملية معزولة لفحص الملفات الواردة من العملاء قبل تمرير الملفات السليمة إلى خدمة التطبيق. لا تملك اتصالاً مباشراً بقاعدة البيانات.

مسار مسموح ضروري: العميل يصل إلى بوابة الويب في المنطقة المنزوعة السلاح، ثم تمر الطلبات الموثقة إلى خدمات التطبيقات، ثم تنفذ خدمات التطبيقات عمليات محددة على قاعدة البيانات.

مسار محظور صراحة: أي اتصال من شبكة الزوار أو بوابة الويب مباشرة إلى منطقة البيانات أو منطقة الإدارة محظور افتراضياً.

الحالة الآمنة عند تعطل خدمة المصادقة: رفض الوصول إلى الوظائف الخاصة بالعملاء والإدارة، مع الإبقاء على المحتوى العام للقراءة فقط حيثما أمكن.

يعتمد النموذج مبدأ افتراض الاختراق: وجود جهاز أو خدمة داخل منطقة ما لا يمنحها ثقة تلقائية للوصول إلى المناطق الأعلى حساسية.

مقدم الطلب	المسؤول	الاعتماد
----------	----------	----------

مستند تعليمي افتراضي. الأسماء والأرقام غير حقيقية.

- اقرأ المخطط بوصفه قراراً لتحديد مناطق الثقة.
- تبدأ رحلة العميل من المنطقة العامة إلى بوابة الويب في المنطقة المنزوعة السلاح، ثم إلى خدمات التطبيقات المصرح بها.
- لاحظ أن منطقة البيانات تستقبل عمليات محددة من خدمات التطبيقات فقط.
- بعد القراءة، حدد مسارين محظورين ولماذا يخفض كل منهما خطر الوصول غير المصرح به.

جدول الحواجز الأمنية وفئات الهجوم

الحاجز الأمني	فئة الخطر المستهدفة	ما يحد منه	الإجراء المكمل
بيئة رملية معزولة	رفع ملف ضار	انتقال الملف إلى البيئة الداخلية	حساب منخفض الصلاحيات
مصادقة متعددة العوامل	استخدام حساب من جهاز غير موثوق	الاعتماد على كلمة المرور وحدها	التحقق من حالة الجهاز
جدار ناري داخلي	وصول جانبي إلى البيانات	اتصال غير مبرر بين المناطق	فصل حسابات الخدمات
نسخ معزولة	حذف النسخ أو تشفيرها	فقدان قدرة الاستعادة	اختبار الاستعادة دورياً

يربط الجدول كل حاجز بمسار خطر محدد وإجراء مكمل.
لا يعالج الحاجز الواحد جميع آثار الخطر، لذلك يختار المصمم ضوابط متكاملة مرتبطة بالأصل والتهديد ونقطة الدخول.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مستند تطبيقي: سجل المخاطر والحواجز

المستند: سجل مخاطر وحواجز أمنية لمنصة الخدمات السحابية

شركة الحلول التقنية والخدمات الرقمية

تطوير وإدارة المنصات الرقمية والخدمات السحابية
جازان، المملكة العربية السعودية
الرقم الضريبي: 300000000000003 · السجل التجاري: 1010000000
هاتف: 0500000000

سجل مخاطر وحواجز أمنية لمنصة الخدمات السحابية

مراجعة معمارية بتاريخ 12-03-2026، شركة الحلول التقنية والخدمات الرقمية

رمز الخطر	الأصل أو المنطقة	التهديد المحتمل	نقطة الدخول أو المسار	الأثر المتوقع	الحاجز الأساسي	الإجراء المكمل
R-17	بوابة الويب في المنطقة المنزوعة السلاح	رفع ملف ضار يستغل خدمة معالجة المرفقات	العميل يرفع مرفقاً عبر البوابة العامة	تنفيذ غير مصرح به على خادم البوابة ومحاولة الانتقال إلى خدمات التطبيق	فحص المرفقات في بيئة رملية معزولة قبل المعالجة	تشغيل خدمة معالجة الملفات بحساب منخفض الصلاحيات ومنع اتصالها المباشر بمنطقة البيانات
R-18	محطة عمل موظف في منطقة الإدارة	سرقة بيانات اعتماد موظف عبر رسالة احتيالية	استخدام حساب موظف من جهاز غير موثوق ثم محاولة الوصول إلى أدوات الإدارة	تعديل إعدادات المنصة أو الاطلاع على سجلات تشغيلية حساسة	مصادقة متعددة العوامل والتحقق من حالة الجهاز قبل منح الوصول	تجزئة منطقة الإدارة وتسجيل الجلسات الإدارية ومراجعة التنبيهات بصورة مستمرة
R-19	خدمات التطبيقات	استغلال خدمة تطبيق للوصول الجانبي إلى قاعدة البيانات	خدمة تطبيق مخترقة تحاول استخدام صلاحية أوسع من المطلوب	قراءة أو تعديل سجلات عملاء خارج نطاق الخدمة المتضررة	جدار ناري داخلي يسمح فقط باتصالات خدمة التطبيق المحددة نحو قاعدة البيانات	فصل حسابات الخدمات وتطبيق أقل الامتيازات ومراقبة الاستعلامات غير المعتادة
R-20	واجهة الدخول للعملاء	محاولات متكررة لتخمين كلمات المرور	طلبات دخول متتابعة من مصادر متعددة إلى واجهة المصادقة	تعطيل الخدمة أو الاستيلاء على حسابات ضعيفة الحماية	تحديد معدل الطلبات وفرض تحقق إضافي عند زيادة المحاولات الفاشلة	قفل مؤقت متدرج للحسابات مع تنبيه العميل وعدم السماح بالدخول عند تعطل المصادقة
R-21	النسخ الاحتياطية للبيانات	حذف أو تشفير النسخ الاحتياطية بعد اختراق حساب إداري	محاولة استخدام صلاحيات الإدارة للوصول إلى مخزن النسخ	إطالة زمن التعافي وفقدان القدرة على استعادة البيانات السليمة	نسخ احتياطي معزول غير قابل للتعديل لفترة احتفاظ محددة	اختبار الاستعادة دورياً وفصل صلاحيات تشغيل النسخ عن صلاحيات إدارة المنصة

الضوابط الواردة أمثلة تعليمية معمارية، وليست إعدادات تشغيلية أو قواعد تفصيلية للنشر.

مستند تعليمي افتراضي، الأسماء والأرقام غير حقيقية

- اقرأ سجل المخاطر من رمز الخطر إلى الإجراء المكمل.
- يبين الصف R-19 أن خدمة التطبيقات قد تحاول الوصول إلى قاعدة البيانات بصلاحيات واسعة.
- الحاجز الأساسي هو الجدار الناري الداخلي، لكن الحماية تكتمل بفصل حسابات الخدمات وأقل الامتيازات ومراقبة الاستعلامات غير المعتادة.
- استخدم هذا النمط لتحليل بقية الصفوف.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مستند تطبيقي: تقرير حادثة أولي

النموذج: تقرير حادثة أمنية أولي

شركة الحلول التقنية والخدمات الرقمية

تطوير وإدارة المنصات الرقمية والخدمات السحابية
جازان، المملكة العربية السعودية
الرقم الضريبي: 300000000000003 · السجل التجاري: 1010000000
هاتف: 0500000000

تقرير حادثة أمنية أولي

رقم التقرير: INC-2026-0417

تاريخ الاكتشاف: 2026-04-17

وقت الاكتشاف: 10:26

مصدر التنبيه: نظام المراقبة المستمرة في منطقة الإدارة.

الأصل المتأثر مبدئياً: محطة عمل موظف ضمن منطقة الإدارة، تستخدم للوصول إلى لوحة الدعم الداخلية.

وصف الواقعة: رصد النظام محاولة دخول ناجحة إلى حساب موظف من جهاز لم يسبق اعتماده، تلتها محاولات اتصال إلى خدمة إدارية ثم إلى منطقة البيانات.

المسار المرصود: جهاز غير موثوق إلى حساب الموظف، ثم إلى لوحة الدعم الداخلية، ثم محاولة الوصول إلى خدمة في منطقة البيانات.

ما الذي أوقف المسار: تم رفض الجلسة الإدارية لأن الجهاز لم يحقق متطلبات الثقة، كما رفض الجدار الناري الداخلي طلب الاتصال من منطقة الإدارة إلى منطقة البيانات.

الأثر المؤكد عند إصدار التقرير: لا يوجد دليل على الوصول إلى سجلات العملاء أو تعديلها. جرى تعليق جلسة الحساب مؤقتاً وحفظ السجلات للتحليل.

الإجراء الفوري: إلغاء الجلسات النشطة للحساب، طلب إعادة التحقق من هوية المستخدم، وعزل محطة العمل عن منطقة الإدارة إلى حين الفحص.

السبب المحتمل قيد التحقق: استخدام بيانات اعتماد صحيحة من جهاز غير معتمد. لا تزال طريقة الحصول على بيانات الاعتماد غير مؤكدة.

التوصية المعمارية: الإبقاء على الفصل بين منطقة الإدارة ومنطقة البيانات، وتعزيز التحقق المستمر من الجهاز والهوية وتقليل صلاحيات حسابات الدعم إلى المهام الضرورية فقط.

التقرير أولي ويعرض حقائق الرصد المتاحة في تاريخ الإصدار، ولا ينسب الحادث إلى شخص أو جهة.

مقدم الطلب	المسؤول	الاعتماد
----------	----------	----------

مستند تعليمي افتراضي. الأسماء والأرقام غير حقيقية.

- ابدأ من وقت الاكتشاف 10:26 في 2026-04-17، ثم تتبع المسار المرصود في التقرير INC-2026-0417. انتقل النشاط من جهاز غير موثوق إلى حساب موظف ثم لوحة الدعم الداخلية.
- أوقفت متطلبات الثقة للجهاز الجلسة الإدارية، ورفض الجدار الناري الداخلي محاولة الاتصال بمنطقة البيانات.
- استخرج قرارين معماريين أبقيا الأثر محدوداً.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مستند تطبيقي: جدول تقدير المخاطر

الجدول: مصفوفة أولوية معالجة المخاطر

شركة الحلول التقنية والخدمات الرقمية
تطوير وإدارة المنصات الرقمية والخدمات السحابية
جازان، المملكة العربية السعودية
الرقم الضريبي: 300000000000003 · السجل التجاري: 1010000000
هاتف: 0500000000

مصفوفة أولوية معالجة المخاطر

مستخرجة من سجل المخاطر المعماري بتاريخ 20-04-2026

رمز الخطر	سيناريو الخطر	الاحتمال من 1 إلى 5	الأثر من 1 إلى 5	درجة الخطر	أولوية المعالجة
R-17	ملف ضار يصل إلى بوابة الويب ويحاول تجاوز معالجة المرفقات	4	5	20	عاجلة
R-18	بيانات اعتماد موظف تستخدم من جهاز غير موثوق للوصول إلى الإدارة	3	5	15	عاجلة
R-19	خدمة تطبيق متضررة تحاول الوصول إلى قاعدة البيانات بصلاحيات واسعة	3	5	15	عاجلة
R-20	محاولات متكررة لتخمين كلمات مرور حسابات العملاء	5	3	15	مرتفعة
R-21	محاولة حذف النسخ الاحتياطية أو تشفيرها عبر صلاحيات إدارية	2	5	10	مرتفعة
متوسط درجة الخطر					**15**
أعلى درجة خطر					**20**

الدرجة أداة لترتيب الأولويات التعليمية ولا تغني عن تحليل سياق العمل ومتطلبات التوافر والموثوقية.

مستند تعليمي افتراضي، الأسماء والأرقام غير حقيقية

- يعرض الجدول خمسة مسارات خطر ويحسب درجة كل مسار من الاحتمال والأثر.
- درجة R-17 تساوي 20.0 من احتمال 4 وأثر 5، وهي أعلى درجة في الجدول.
- بينما يبلغ متوسط درجات المخاطر 15.0. استخدم الترتيب لتحديد أولوية المعالجة، ثم اربط كل معالجة بحاجز وإجراء مكمل بدلاً من الاكتفاء بدرجة الخطر.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مثال محلول على النموذج: تحليل أولويات الحواجز الأمنية

الجدول: مصفوفة أولوية معالجة المخاطر

شركة الحلول التقنية والخدمات الرقمية
تطوير وإدارة المنصات الرقمية والخدمات السحابية
جازان، المملكة العربية السعودية
الرقم الضريبي: 300000000000003 · السجل التجاري: 1010000000
هاتف: 0500000000

مصفوفة أولوية معالجة المخاطر

مستخرجة من سجل المخاطر المعماري بتاريخ 20-04-2026

رمز الخطر	سيناريو الخطر	الاحتمال من 1 إلى 5	الأثر من 1 إلى 5	درجة الخطر	أولوية المعالجة

الدرجة أداة لترتيب الأولويات التعليمية ولا تغني عن تحليل سياق العمل ومتطلبات التوافر والموثوقية.

مستند تعليمي افتراضي، الأسماء والأرقام غير حقيقية

- **المعطيات:** يتضمن النموذج خمسة مخاطر هي R-17 وR-18 وR-19 وR-20 وR-21. يحتوي كل صف على سيناريو الخطر والاحتمال من 1 إلى 5 والأثر من 1 إلى 5 وأولوية المعالجة.
- المطلوب حساب درجة الخطر لكل صف، ثم تحديد أعلى درجة ومتوسط الدرجات قبل ربط النتائج بقرارات الحواجز والعزل.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

الخطوة 1 من 3: إدخال معطيات الاحتمال والأثر

الجدول: مصفوفة أولوية معالجة المخاطر

شركة الحلول التقنية والخدمات الرقمية
تطوير وإدارة المنصات الرقمية والخدمات السحابية
جازان، المملكة العربية السعودية
الرقم الضريبي: 300000000000003 · السجل التجاري: 1010000000
هاتف: 0500000000

مصفوفة أولوية معالجة المخاطر

مستخرجة من سجل المخاطر المعماري بتاريخ 20-04-2026

رمز الخطر	سيناريو الخطر	الاحتمال من 1 إلى 5	الأثر من 1 إلى 5	درجة الخطر	أولوية المعالجة
R-17	ملف ضار يصل إلى بوابة الويب ويحاول تجاوز معالجة المرفقات	4	5		عاجلة
R-18	بيانات اعتماد موظف تستخدم من جهاز غير موثوق للوصول إلى الإدارة	3	5		عاجلة
R-19	خدمة تطبيق متضررة تحاول الوصول إلى قاعدة البيانات بصلاحيات واسعة	3	5		عاجلة
R-20	محاولات متكررة لتخمين كلمات مرور حسابات العملاء	5	3		مرتفعة
R-21	محاولة حذف النسخ الاحتياطية أو تشفيرها عبر صلاحيات إدارية	2	5		مرتفعة

الدرجة أداة لترتيب الأولويات التعليمية ولا تغني عن تحليل سياق العمل ومتطلبات التوافر والموثوقية.

مستند تعليمي افتراضي، الأسماء والأرقام غير حقيقية

- تسجل المعطيات كما وردت في المستند.
- للخطر R-17 الاحتمال 4 والأثر 5، وللخطر R-18 الاحتمال 3 والأثر 5. يسجل R-20 احتمالاً مقداره 5 وأثراً مقداره 3. لا تحدد الأولوية من الانطباع عن السيناريو، بل من حساب الدرجة أولاً ثم قراءة مستوى الأثر والضوابط المطلوبة.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

الخطوة 2 من 3: حساب درجة الخطر

شركة الحلول التقنية والخدمات الرقمية
تطوير وإدارة المنصات الرقمية والخدمات السحابية
جازان، المملكة العربية السعودية
الرقم الضريبي: 300000000000003 · السجل التجاري: 1010000000
هاتف: 0500000000

الجدول: مصفوفة أولوية معالجة المخاطر

مصفوفة أولوية معالجة المخاطر

مستخرجة من سجل المخاطر المعماري بتاريخ 20-04-2026

رمز الخطر	سيناريو الخطر	الاحتمال من 1 إلى 5	الأثر من 1 إلى 5	درجة الخطر	أولوية المعالجة
R-17	ملف ضار يصل إلى بوابة الويب ويحاول تجاوز معالجة المرفقات	4	5	20	عاجلة
R-18	بيانات اعتماد موظف تستخدم من جهاز غير موثوق للوصول إلى الإدارة	3	5	15	عاجلة
R-19	خدمة تطبيق متضررة تحاول الوصول إلى قاعدة البيانات بصلاحيات واسعة	3	5	15	عاجلة
R-20	محاولات متكررة لتخمين كلمات مرور حسابات العملاء	5	3	15	مرتفعة
R-21	محاولة حذف النسخ الاحتياطية أو تشفيرها عبر صلاحيات إدارية	2	5	10	مرتفعة

الدرجة أداة لترتيب الأولويات التعليمية ولا تغني عن تحليل سياق العمل ومتطلبات التوافر والموثوقية.

مستند تعليمي افتراضي. الأسماء والأرقام غير حقيقية

- تحسب درجة الخطر بضرب الاحتمال في الأثر.
- لذلك تكون درجة R-17 هي 4 × 5 = 20.0.
- وتكون درجتا R-18 وR-19 كل منهما 3 × 5 = 15.0.
- أما R-20 فتبلغ درجته 5 × 3 = 15.0، ويبلغ R-21 2 × 5 = 10.0.
- يساعد الحساب على ترتيب المعالجة بصورة منظمة.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

الخطوة 3 من 3: قراءة الناتج وترتيب القرار

الجدول: مصفوفة أولوية معالجة المخاطر

شركة الحلول التقنية والخدمات الرقمية
تطوير وإدارة المنصات الرقمية والخدمات السحابية
جازان، المملكة العربية السعودية
الرقم الضريبي: 300000000000003 · السجل التجاري: 1010000000
هاتف: 0500000000

مصفوفة أولوية معالجة المخاطر

مستخرجة من سجل المخاطر المعماري بتاريخ 20-04-2026

رمز الخطر	سيناريو الخطر	الاحتمال من 1 إلى 5	الأثر من 1 إلى 5	درجة الخطر	أولوية المعالجة
R-17	ملف ضار يصل إلى بوابة الويب ويحاول تجاوز معالجة المرفقات	4	5	20	عاجلة
R-18	بيانات اعتماد موظف تستخدم من جهاز غير موثوق للوصول إلى الإدارة	3	5	15	عاجلة
R-19	خدمة تطبيق متضررة تحاول الوصول إلى قاعدة البيانات بصلاحيات واسعة	3	5	15	عاجلة
R-20	محاولات متكررة لتخمين كلمات مرور حسابات العملاء	5	3	15	مرتفعة
R-21	محاولة حذف النسخ الاحتياطية أو تشفيرها عبر صلاحيات إدارية	2	5	10	مرتفعة
متوسط درجة الخطر					15
أعلى درجة خطر					20

الدرجة أداة لترتيب الأولويات التعليمية ولا تغني عن تحليل سياق العمل ومتطلبات التوافر والموثوقية.

مستند تعليمي افتراضي، الأسماء والأرقام غير حقيقية

- **الناتج:** أعلى درجة خطر هي 20.0 للخطر R-17، ومتوسط الدرجات هو 15.0. تبدأ الشركة بمعالجة R-17 عبر فحص المرفقات في بيئة رملية وعزلها عن منطقة البيانات.
- تظل الدرجة مؤشراً لترتيب القرار، ولا تعفي المصمم من تحليل الأصل المتأثر والحواجز الحالية والإجراءات المكملة والمخاطر المتبقية.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

نشاط تطبيقي: اختيار الحاجز المناسب

ورقة العمل: ورقة عمل: المسار والضابط والحالة الآمنة

شركة الحلول التقنية والخدمات الرقمية

تطوير وإدارة المنصات الرقمية والخدمات السحابية
جازان، المملكة العربية السعودية
الرقم الضريبي: 300000000000003 · السجل التجاري: 1010000000
هاتف: 0500000000

ورقة عمل: المسار والضابط والحالة الآمنة

#	السيناريو	التهديد أو القرار المطلوب	الضابط والمبرر
1	ترفع جهة عميلة ملفاً مرفقاً إلى البوابة العامة، ولا يمكن الوثوق بمحتوى الملف قبل فحصه.	التهديد هو تنفيذ محتوى ضار أو انتقاله من البوابة إلى البيئة الداخلية.	تُعالج المرفقات في بيئة رملية معزولة، ثم يمر فقط الملف الذي اجتاز الفحص إلى خدمة التطبيق. العزل يقلل نصف قطر الانفجار إذا احتوى الملف على محتوى ضار.
2	تحتاج خدمة التطبيق إلى قراءة بيانات معاملة محددة، لكنها لا تحتاج إلى إدارة قاعدة البيانات أو قراءة جميع السجلات.	القرار المطلوب هو تقليل الصلاحيات التي يمكن أن تستغلها خدمة تطبيق متضررة.	يستخدم حساب خدمة محدود الصلاحيات مع قواعد جدار ناري داخلي تسمح بالاتصالات الضرورية فقط. يطبق ذلك مبدأ أقل الامتيازات ويكسر مسار الحركة الجانبية.
3	تعطلت خدمة المصادقة المركزية مؤقتاً أثناء ضغط مرتفع على واجهة الدخول.	القرار المطلوب هو تحديد سلوك النظام عند فقدان القدرة على التحقق من هوية المستخدم.	يرفض النظام الوصول إلى الوظائف الخاصة بالعملاء والإدارة ولا يمنح صلاحيات تلقائية، مع إتاحة المحتوى العام للقراءة فقط عند الإمكان. هذا فشل آمن يحافظ على الأمن دون فتح مسار غير موثق.
4	تمت محاولة استخدام حساب موظف صحيح من جهاز جديد خارج بيئة العمل المعتادة.	التهديد هو الاعتماد على كلمة المرور وحدها ومنح ثقة ضمنية للحساب بعد دخوله الشبكة.	يتطلب الوصول مصادقة متعددة العوامل والتحقق من حالة الجهاز ومراقبة الجلسة. هذا يطبق الثقة الصفرية لأن كل طلب حساس يعاد التحقق منه.
5	خادم ويب في المنطقة المنزوعة السلاح يحاول الاتصال مباشرة بقاعدة بيانات العملاء.	التهديد هو توسع أثر اختراق خادم ويب إلى بيانات العملاء الحساسة.	يرفض الجدار الناري الداخلي الاتصال المباشر، وتكون خدمة التطبيق الوسيط الوحيد المصرح به بطلبات محددة. يؤدي فصل الطبقات إلى حصر الضرر في المنطقة المنزوعة السلاح.

تستخدم السيناريوهات بيانات الوثائق التعليمية السابقة نفسها لبناء تسلسل: مخطط مناطق ثم تحليل خطر ثم تقرير حادثة ثم قرار معماري.

مستند تعليمي افتراضي، الأسماء والأرقام غير حقيقية

- اقرأ السيناريو الخامس في ورقة العمل.
- يحاول خادم ويب في المنطقة المنزوعة السلاح الاتصال مباشرة بقاعدة بيانات العملاء.
- حدد التهديد، ثم اختر ضابطاً معمارياً واحداً وإجراءً مكملاً.
- اكتب تبريراً من سطرين يربط قرارك بتقليل نصف قطر الانفجار ومنع الحركة الجانبية.
- أكمل النشاط قبل كشف الإجابة النموذجية.

إجابة النشاط، منع اتصال خادم الويب بمنطقة البيانات

- التهديد هو توسع أثر اختراق خادم الويب إلى بيانات العملاء الحساسة.
- الضابط المناسب هو رفض الجدار الناري الداخلي الاتصال المباشر من المنطقة المنزوعة السلاح إلى منطقة البيانات.
- الإجراء المكمل هو أن تكون خدمة التطبيق الوسيط الوحيد المصرح به لتنفيذ طلبات محددة.
- يقلل فصل الطبقات نصف قطر الانفجار ويحصر الضرر المحتمل في المنطقة الأقل ثقة.

جدول مقارنة أنماط العزل

نمط العزل	موضع التطبيق	الهدف الرئيس	قرار التصميم المناسب
العزل الشبكي	بين المناطق والتدفقات	تقييد الاتصالات	فصل الزوار عن البيانات
عزل المضيف	داخل النظام أو الحساب	تقييد الامتيازات	حساب خدمة محدود
العزل بالحاويات	بين أعباء العمل	تقليل تداخل المكونات	خدمة معالجة منفصلة
البيئة الرملية	تشغيل مكوّن غير موثوق	تقليل أثر المحتوى	فحص المرفقات الواردة

يختار المصمم نمط العزل وفق الأصل ودرجة الحساسية والتدفقات الضرورية.
ويمكن الجمع بين الأنماط عندما لا يكفي حد واحد لتقليل أثر الاختراق.

جدول قرارات التوافر والموثوقية

الآلية	الهدف التشغيلي	الخطر الأمني المحتمل	الضابط المكمل
التكرار	تقليل أثر فشل مكوّن	بديل غير محمي	ضبط الهوية والتدقيق
التجاوز عند الفشل	استمرار الخدمة عبر بديل	تجاوز التحقق	سلوك فشل آمن
النسخ الاحتياطي	دعم الاستعادة	حذف النسخ أو تشفيرها	عزل النسخ واختبارها
المحتوى العام للقراءة	استمرار محدود للخدمة	كشف محتوى خاص	حظر الوظائف الخاصة

يوازن التصميم بين التوافر والسرية وتكامل البيانات.
استمرار الخدمة لا يبرر توسيع الوصول عند فقدان القدرة على التحقق من الهوية أو التفويض.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مثال محلول، خفض نصف قطر الانفجار لخدمة المرفقات

- **المعطيات:** الخطر R-17 يتعلق بملف ضار يصل إلى بوابة الويب ويحاول تجاوز معالجة المرفقات.
- تبلغ درجة الخطر 20.0، وهي الأعلى في جدول المخاطر.
- **الخطوات:**
- **الناتج:** ينحصر الأثر المحتمل في بيئة معالجة مقيدة بدلاً من انتقاله إلى بيانات العملاء.

١ نحدد بوابة الويب نقطة دخول للملف غير الموثوق.

٢ نعزل فحص الملف في بيئة رملية قبل المعالجة.

٣ نشغل خدمة المعالجة بحساب منخفض الصلاحيات.

٤ نمنع اتصال خدمة المعالجة المباشر بمنطقة البيانات.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مثال محلول، قرار توافر آمن عند تعطل المصادقة

- **المعطيات:** تعطلت خدمة المصادقة المركزية، وتحتاج المنصة إلى تحديد ما يبقى متاحاً للعملاء والإدارة.
- **الخطوات:**
- **الناتج:** تستمر خدمة محدودة دون منح وصول غير موثق أو توسيع الصلاحيات عند الفشل.

١ نميز المحتوى العام عن الوظائف الخاصة.

٢ نرفض الوصول إلى وظائف العملاء والإدارة لغياب التحقق.

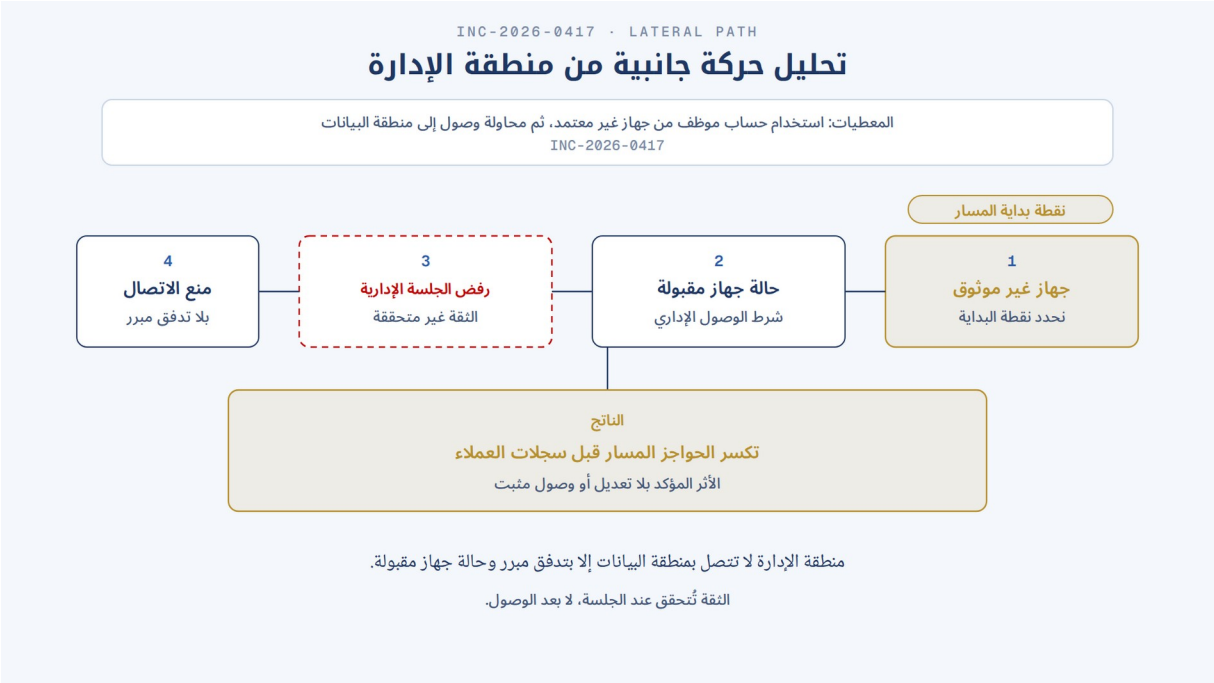
٣ نسمح بقراءة المحتوى العام حيثما أمكن.

٤ نوثق القرار ونراجع أثره على التوافر والسرية.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مثال محلول، تحليل حركة جانبية من منطقة الإدارة

- **المعطيات:** يرصد التقرير INC-2026-0417 استخدام حساب موظف من جهاز غير معتمد، ثم محاولة وصول إلى منطقة البيانات.
- **الخطوات:**
- **الناتج:** تكسر الحواجز المسار قبل وصوله إلى سجلات العملاء، ويظل الأثر المؤكد بلا تعديل أو وصول مثبت.



١ نحدد الجهاز غير الموثوق نقطة بداية المسار.

٢ نتحقق من أن الوصول الإداري يحتاج حالة جهاز مقبولة.

٣ نرفض الجلسة الإدارية عند عدم تحقق متطلبات الثقة.

٤ نمنع اتصال منطقة الإدارة بمنطقة البيانات دون تدفق مبرر.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

نشاط الوحدة السادسة: تصميم حواجز مترابطة

- خصص 15 دقيقة لاختيار خطرين من R-17 إلى R-21. أنشئ لكل خطر صفاً يتضمن الأصل، والمسار أو نقطة الدخول، والحاجز الأساسي، والإجراء المكمل، والأثر الذي يخفضه القرار.
- استخدم أرقام الاحتمال والأثر كما وردت في A4، ثم اشرح لماذا لا تكفي درجة الخطر وحدها لاتخاذ قرار التصميم.

إجابة نشاط الوحدة السادسة

- يمكن تحليل R-17 بربط بوابة الويب بملف ضار، وفحص المرفقات في بيئة رملية، وتشغيل خدمة المعالجة بحساب منخفض الصلاحيات ومنع اتصالها بمنطقة البيانات.
- ويمكن تحليل R-19 بربط خدمات التطبيقات بمحاولة وصول جانبي، وجدار ناري داخلي، وفصل حسابات الخدمات وأقل الامتيازات.
- ترتب الدرجة الأولوية، لكن الأصل والمسار والحواجز والمخاطر المتبقية تحدد القرار.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مرحلة المشروع التراكمي الرابعة

- عنوان المرحلة: تصميم الحواجز الأمنية والعزل وخطة التوافر والموثوقية.
- اختر النظام الرقمي الذي اعتمدتموه في المشروع، ثم أعدوا جدولاً يحدد المناطق الأمنية والأصول والتدفقات المسموحة والحواجز.
- أضيفوا قرارين للعزل، وسيناريو فشل آمن، وخطة مبدئية للتوافر أو التعافي.
- يجب أن يوضح كل قرار التهديد الذي يعالجه والأثر الذي يحد منه.
- مخرج التسليم: ملحق من صفحتين إلى ثلاث صفحات يضاف إلى ملف المشروع التراكمي.

خلاصة الفصل

- **طبقت** هدف الفصل الأول عند ربط تقليل سطح الهجوم والتحصين وافتراض الاختراق بالمعمارية.
- **حققت** الهدف الثاني عند اختيار الحواجز والعزل لتقليل نصف قطر الانفجار.
- **ميزت** بين التوافر والموثوقية، وربطت التكرار والتجاوز بالفشل الآمن.
- **حللت** الحركة الجانبية في التقرير INC-2026-0417 وحددت الحواجز التي أوقفتها.
- **قارنت** الدفاع المحيطي بالثقة الصفرية من حيث مركز الحماية ومنح الثقة والتحقق قبل الجلسة.

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

مراجع الفصل

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.
2. Joint Task Force. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). National Institute of Standards and Technology.
3. Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology.
4. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). National Institute of Standards and Technology.
5. National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0: Resource & Overview Guide (NIST SP 1299).

معهد البحوث والخدمات الاستشارية
Institute of Research and Consulting Services

شكراً لكم

معهد البحوث والخدمات الاستشارية – جامعة جازان