BRANDEFENSE COUNTRY REPORT · SAUDI ARABIA 2026

Brandefense: تقرير مشهد التهديدات السيبرانية في السعودية 2026

ادعاءات بيانات العملاء وطلب الهويات وسرد متكرر للتعطيل في اقتصاد خدمات واسع الاتصال

Odin by Brandefense

فترة البحث: 1 يناير–22 نوفمبر 2026

الإصدار 1.0 · 22 · TLP:CLEAR · Public Research Edition نوفمبر 2026

4	96 من 249	220	30
قرارات قيادية مرتبطة بإجراءات لها مسؤولون	نطاقًا مقيمًا ارتبطت ببيانات اعتماد معروضة للبيع وقت الفحص	منشور منتدى موسوم بالسعودية في الفترة	إدراجًا موسومًا بالسعودية في فترة التقرير

المحتويات

المحتويات

Translated with AI

ترجمت هذه النسخة بمساعدة الذكاء الاصطناعي من النسخة الإنجليزية الأصلية، وتعد النسخة الإنجليزية هي المرجع.

01	الملخص التنفيذي	05
	خريطة التقرير	08
02	السياق الرقمي وسياق التهديدات في السعودية	09
03	الانكشاف الوطني: قائمة مختارة من 250 نطاقًا	12
04	ملاحظات الويب المظلم وأدلة الحالات	19
05	أمثلة على الاستهداف بحسب القطاع	40
06	نشاط ناشطي القرصنة وادعاءات التعطيل وحالة الخدمة	44
07	الجهات الفاعلة والادعاءات وإدراجات الفدية	51
08	اقتصاد الاحتيال الظاهر في الأدلة	59
09	نظرة معمّقة على المصارف والخدمات المالية	63
10	الاستجابة التنظيمية والوطنية	67
11	التوقعات	71
12	خطة العمل	75
A	الملحق A. النطاق والمصادر والثقة	81
B	الملحق B. سجل بطاقات الأدلة العامة	84
C	الملحق C. المصادر	85
D	الملحق D. مسرد المصطلحات	87
E	الملحق E. موضوعات ادعاء إضافية خضعت للمراجعة	88
	عن هذا التقرير	91

القيادة التنفيذية	12 → 11 → 3 → 1
مركز العمليات والهوية	12 → 7 → 6 → 4
مكافحة الاحتيال والدعم	12 → 9 → 8
مالكو البيانات والمورّدين	12 → 10 → 5 → 4
الشؤون القانونية والامتثال	12 → 10 → 1

عن هذه النسخة

بحث وتحليل وصياغة بمساعدة الذكاء الاصطناعي من Odin by Brandefense. تشترك النسخة الإنجليزية والنسخة العربية في حدود الأدلة نفسها. تاريخ التحقق من المصادر: 22–23 نوفمبر 2026. ملخص المنهجية في الملحق A.

ترجمة بالذكاء الاصطناعي. عند أي اختلاف بين النسختين، تكون النسخة الإنجليزية هي المرجع.

المحتويات ومسارات القراءة

الفصل	السؤال
1. الملخص التنفيذي	ما القرارات الأهم أولًا؟
2. السياق الرقمي	أين تلتقي الهوية والثقة في الخدمات؟
3. الانكشاف الوطني	ما الذي تثبته القائمة المختارة؟
4. أدلة الويب المظلم	ما الذي عُرض أو طُلب أو ادُّعي؟
5. أمثلة القطاعات	أي مسؤول ينبغي أن يتصرف أولًا؟
6. نشاط ناشطي القرصنة والتعطيل	كيف تقارن الادعاءات بأدلة الخدمة؟
7. الجهات الفاعلة والفدية	ما الذي تثبته هويات النشر والإدراجات؟
8. اقتصاد الاحتيال	أين قد تلتقي عروض الحسابات والبيانات بمخاطر الدفع؟
9. الخدمات المالية	كيف تعمل الهوية والدعم ومكافحة الاحتيال معًا؟
10. الاستجابة التنظيمية	ما شروط الإبلاغ ومسؤولوه؟
11. التوقعات	ما الأدلة الجديدة التي تغيّر الاستجابة؟
12. خطة العمل	ما الذي يجب اختباره خلال 30/60/90 يومًا؟
الملاحق A–E	النطاق وبطاقات الأدلة والمصادر والمسرد

مسار القيادة هو الفصول 1 و3 و10 و11 و12. ومسار مركز العمليات هو الفصول 4 و6 و7 و12. ومسار البيانات والتطبيقات والمورّدين هو الفصول 4 و5 و8 و9 و10.

تحكم التقرير ثلاثة أوصاف للأدلة. **مرصود** يعني وجود منشور أو إدراج أو ملاحظة عامة محفوظة. **مدعى** يعني أن ناشرًا يزعم نتيجة. **مبلّغ عنه أو مؤكد** يسمّي المصدر والمعلومة المحددة التي يسندها. ولا يثبت أي وصف كل ما يقوله المصدر.

01

الفصل 01

الملخص التنفيذي

يجيب هذا الفصل عن

ما أولويات المؤسسات السعودية، وما قوة الأدلة؟

4

قرارات قيادية مرتبطة بإجراءات لها مسؤولون

أربعة قرارات للقادة 07

الدراسة بالأرقام 07

الفصل 01

الملخص التنفيذي

باختصار

تحتاج حادثة تطبيق مُفصح عنها وإعلانات بيانات عملاء وادعاءات تعطيل متكررة إلى مسارات استجابة مختلفة. ويسجل Ransompedia عدد 30 إدراجًا موسومًا بالسعودية. وعُرضت بيانات اعتماد مرتبطة بعدد 96 من 249 نطاقًا مقيمًا للبيع؛ وتبلغ القيمة الوطنية الرئيسية لـ Atlas مقدار 52/100. ولا تثبت الملاحظات وصولًا حاليًا أو انتشارًا وطنيًا. تحقّق من الهويات وعلاقات البيانات، واختبر التعافي، وأنشئ مسارًا موحدًا للإبلاغ وحماية العميل.

يغطي التقرير المنشورات والإصدارات من 1 يناير إلى 22 نوفمبر 2026. وتغطي الأنشطة الحديثة 8–22 نوفمبر. وكان يوم القطع ما زال جاريًا أثناء البحث. وتمثل ملاحظاتنا والتقارير العامة مجموعات أدلة منفصلة. ولا يعني تاريخ المنشور تلقائيًا تاريخ الدخول. [S2][S1]

1. يفصل حادث التطبيق المُفصح عنه السرية عن الاستمرارية. أكد بيان بدجت السعودية في 9 يونيو وصولًا غير مصرح به إلى جزء محدود من بيانات بعض عملاء التطبيق. وقالت الشركة إن البيانات المالية والمصرفية لم تتأثر وإن العمليات استمرت. وتبقى حدود الأثر رواية الشركة. ولم يقدّم الإفصاح عدد عملاء متأثرين أو سببًا جذريًا (4.5§ ، الحالة A). [S28][S18][S17]

2. تصف الإعلانات خدمات حساسة وموّردين، مع نتائج غير متحقق منها. تغطي عشرة ملفات منتديات شيفرة جهة عامة وبيانات صحية وطلب حسابات وسجلات استثمار وأرشيف مقاولين وCRM عافية وبيانات سائقين وطرود. وتوثّق إعلانات أو طلبًا، لا دخولًا مؤكدًا. وتبدأ الاستجابة بتطابق داخلي مصرح به أو مع موّرد (4.6§). [S1]

3. يتكرر سرد التعطيل من مارس إلى أكتوبر. تضم مادة Team 313 المحفوظة 17 منشورًا ضمن تسع سلاسل ادعاء من مارس إلى أكتوبر. وتظهر خدمات مالية وعامة وتعليمية وتطبيق موظفين واتصالات. ومدد الهجوم المدعاة ليست وقت انقطاع مقيسًا (6.3§). [S1]

4. تبرر إدراجات الفدية الجاهزية من دون إثبات انتشار الحوادث. يضم المصدر 30 إدراجًا موسومًا بالسعودية، مقابل 84 للإمارات و9 لقطر و7 للكويت و9 لعُمان. وتقع ثلاثة إدراجات سعودية في الفترة الحديثة. وتبقى تواريخها وتسمياتها ملاحظات مصدر، من دون تأكيد رسمي للجهات المعنية مثبت هنا (7§). [S2]

اختيرت دول المقارنة كأمثلة لتوفير السياق فقط؛ ولا ينطوي اختيارها على أي ترتيب أو تقييم سياسي.

5. تمنح الإدراجات الحالية التحقق من الهوية نطاقًا محددًا. عُرضت بيانات اعتماد مرتبطة بعدد 96 من 249 نطاقًا مقيمًا للبيع. وتبلغ القيمة الوطنية الرئيسية لـ Atlas للقائمة المقيمة 52/100. وتبقى نتيجة نطاق واحد من 250 مختارًا مجهولة. وتحد الملكية وتداخل المجموعات الاستدلال على الكيانات؛ ويبقى انتشار ضوابط البريد وDNS والويب غير مقيم (3§). [S4][S3]

أربعة قرارات للقادة

1. **أنشئ مسارًا لفرز تنبيهات الهوية الآن.** يتولى مسؤول الهوية مسار إشارات الإدراجات وطلب الحسابات وارتباطات الأجهزة. افحص التنبيهات سريعًا واحتوِ فورًا عند وجود دليل على مادة مصادقة مسروقة قابلة للاستخدام أو نشاط غير مصرح به. واحفظ نتيجة الفرز وقرار التعافي (A01–A03، §12.1).
2. **تحقّق من علاقات بيانات العملاء والمورّدين.** يحدّد مسؤولو التطبيقات ومخاطر المورّدين الوصول إلى البيانات الحساسة والتخزين المشترك. اختبر الفصل بين حسابات التطبيق وأكّد مسارات تصعيد المورّدين الحرجين. وصعّد الادعاء عند وجود مادة مطابقة موثوقة أو تأكيد مورّد (A04، A09، §12.1).
3. **أثبت التعافي والتقييم المستقل لحالة الخدمة.** على مسؤولي الاستمرارية والعمليات استعادة خدمة حرجة والتدرّب على إدارة ادعاء تعطيل. ودليل الإنجاز نتيجة استعادة ورواية للوظائف المتأثرة تسندها بيانات الخدمة (A05، A10، §12.1).
4. **اربط مسؤولي الاحتيال والخصوصية والإبلاغ.** اختبر رحلة آمنة لاستعادة حساب وتغيير دفع. ووثّق من يقيّم شروط الإشعار ومن يعتمد الرسائل ومن يحمي المعاملة. وتتقدم الاستجابة للحادث على جدول البرنامج (A08، A11، A12، §12.1).

الدراسة بالأرقام

748,946
منشورات موسومة بارتباط بالسعودية خلال الفترة

ما ليس هو
ليس هجمات أو أشخاصًا متأثرين أو استهدافًا سعوديًا متحققًا منه

220
منشور منتدى محفوظ موسوم بالسعودية عبر الفترة

ما ليس هو
ليس حوادث فريدة أو كل محتوى المنتديات السعودي

9 / 17
منشورات / سلاسل ادعاء من هوية النشر Team 313

ما ليس هو
ليس انقطاعات مقيسة أو مشغّلين مستقلين

30
إدراجات Ransompedia موسومة بالسعودية

ما ليس هو
ليس دخولًا مؤكدًا أو تشفيرًا أو تقدير خسائر

3
إدراجات موسومة بالسعودية بتاريخ 8–22 نوفمبر

ما ليس هو
ليس ثلاث حوادث مؤكدة جديدة

250
نطاقًا مرشّحًا في عشر خلايا مدمجة

ما ليس هو
ليس عينة ممثلة أو ترتيب كيانات متحققًا منه

52/100
القيمة الوطنية الرئيسية لـ Atlas لعدد 249 نطاقًا مقيمًا

ما ليس هو
ليست نسبة اختراق أو تقدير انتشار وطني

16
ملف حالة مفصلًا يشمل حملات أبلغت عنها المصادر

ما ليس هو
ليس مجموعًا وطنيًا للحوادث

19
بطاقة منشور عامة مرتبطة بسجل مصدر خاص

ما ليس هو
ليس كل المنشورات المرصودة أو ادعاءات مؤكدة مستقلًا

خريطة التقرير

تتبّع القرار من النتيجة التنفيذية إلى دليله ومسؤوله واختبار إغلاقه. وتحدّد إحالات الفصول موضع تقييم العبارة.

القيادة التنفيذية	ما أولويات الاهتمام والتمويل؟	1 → 3 → 11 → 12
مركز العمليات والهوية	هل تتعلق الإشارة بوصول قابل للاستخدام أو أثر في الخدمة؟	4 → 6 → 7 → 12
مكافحة الاحتيال والدعم	هل يرتبط حدث عميل بتغيير حساب أو دفع؟	8 → 9 → 12
مالكو البيانات والمورّدين	ما السجلات أو الصلاحيات المشتركة ذات الصلة؟	4 → 5 → 10 → 12
الشؤون القانونية والامتثال	ما الشروط والمواعيد التي تحتاج قرارًا؟	1 → 10 → 12

سؤال الدليل	اقرأ	سؤال الإنجاز
هل السجل طلب أو إعلان أو إفصاح مؤكد؟	4 والملحق B	ما المعلومة التي ثبتت فعلًا؟
هل ترتبط ملاحظتان؟	7	هل توجد صلة ملموسة أم نموذج تحليلي فقط؟
هل تأثرت الخدمة؟	6	ماذا تظهر السجلات التشغيلية المستقلة؟
هل تنطبق قاعدة على الجهة؟	10	من وثّق الانطباق وقرار الإبلاغ؟

الخلاصات الرئيسية

01
ابدأ بالهوية وبيانات العملاء والاستمرارية وقرارات الإبلاغ ذات المسؤولين.

02
افصل الادعاءات المرصودة عن الوصول المتحقق منه وأثر الخدمة.

03
قيّم التقدم بأدلة الإنجاز في خطة العمل.

الفصل 02

السياق الرقمي وسياق التهديدات في السعودية

يجيب هذا الفصل عن

ما السمات التي تحدد أولويات الدفاع في الاقتصاد الرقمي؟

99.6%

استخدام الإنترنت لدى الأفراد بعمر 15–74 سنة في المسح الرسمي لعام 2026

2.1 الاتصال يجعل هوية الخدمة حدًا أمنيًا 10

2.2 الطاقة والنقل والمورّدون يحتاجون إلى خطط استجابة مختلفة 10

2.3 الحملات الإقليمية سياق له أدلة سعودية محدودة 10

2.4 اقرأ التحذيرات الرسمية بوصفها مهام تشغيلية 11

الفصل 02

السياق الرقمي وسياق التهديدات في السعودية

باختصار

تعمل الخدمات السعودية في بيئة واسعة الاتصال. ويبيّن المسح الرسمي للأسر انتشار استخدام الإنترنت والخدمات الحكومية الرقمية. ويصف باحثون أمنيون حملات تصيّد مؤسسية ورش كلمات مرور استهدفت جهات سعودية. وتتناول هذه المصادر مجموعات مختلفة. وهي تدعم الاهتمام بالهوية وتطبيقات الهاتف والعلامات الموثوقة، من دون أن تثبت معدلًا وطنيًا للهجمات. حدّد الحسابات والمورّدين القادرين على تغيير دفعة أو كشف بيانات عملاء، ثم اختبر ضوابطهم.

2.1 الاتصال يجعل هوية الخدمة حدًا أمنيًا

أفاد الإصدار الإحصائي الرسمي في 1 نوفمبر بأن 99.6% من الأفراد بعمر 15–74 سنة يستخدمون الإنترنت. وبلغ استخدام الخدمات الحكومية الرقمية 98.4% في هذه الفئة. وهذه نتائج مسح، وليست مقياسًا للأمن ولا وصفًا للسكان بكل أعمارهم. [S16]

السؤال العملي للمدافعين هو أين يضع الناس ثقتهم. فقد ينتقل العميل بين رسالة وتطبيق ومكالمة دعم وموافقة على دفع ضمن معاملة واحدة. ولا تكفي قوة الضابط في مرحلة لإثبات هوية كل المشاركين في المراحل الأخرى. ويحتاج مسؤول الضابط إلى رؤية المعاملة كاملة.

لذلك يربط هذا التقرير بين هوية المؤسسة والاحتيال الموجّه إلى المستهلك. وهذا الربط نموذج تحليلي لمسارات إساءة استخدام محتملة. ولا يثبت وجود مشغّل واحد يجمع حملة تصيّد مؤسسية وبائع حسابات منفصلًا.

2.2 الطاقة والنقل والمورّدون يحتاجون إلى خطط استجابة مختلفة

تشمل القائمة المختارة خدمات عامة وطاقة ومالًا ونقلًا وصناعة وتعليمًا وصحة وخدمات تجارية. وهدفها دعم القرارات عبر الاعتماد المتبادل بين الجهات. وهي ليست ترتيبًا اقتصاديًا ولا مسحًا يمثل المؤسسات السعودية كلها. [S3]

يحتاج المشغّل الصناعي إلى حماية وصول المهندسين والتعافي الآمن. ويحتاج مزوّد النقل إلى حماية الحجوزات وبيانات العملاء والواجهات التشغيلية. وتحتاج الجامعة إلى تمييز حسابات الموظفين عن حسابات الطلاب والخريجين. وقد تحجب الاستجابة الموحدة لكل ارتباط بنطاق هذه الفروق.

وقد يحتفظ المورّد بنسخ من بيانات مهمة تشغيليًا حتى عندما لا يتأثر نظام الجهة الرئيسية. ولذلك يستدعي ادعاء يسمّي مقاولًا مراجعة مشاركة البيانات. لكنه لا يثبت الوصول إلى كل شركاء المشروع.

2.3 الحملات الإقليمية سياق له أدلة سعودية محدودة

أفادت Unit 42 في موجزها الإقليمي (النسخة المحدّثة في 17 أبريل) بتصيّد لبيانات اعتماد مؤسسية واحتيال مالي موجّهين إلى مؤسسات سعودية. وأفادت Check Point باستهداف سعودي محدود ضمن حملة أوسع لرش كلمات المرور على Microsoft 365. ولم يقدّم أي المصدرين مجموعًا وطنيًا للحوادث السعودية. [S11][S12]

وتختلف النتائج الدفاعية. فصفحة دخول مؤسسية مقنعة تستدعي مصادقة تراعي أصل الطلب وقناة لإبلاغ المستخدم. ورش كلمات المرور يستدعي تحليل المصادقة على مستوى بيئة المؤسسة. ولا تثبت أي من الملاحظتين أيّ حساب سعودي استُخدم بنجاح، إن وُجد.

لا ترد أوصاف سياسية إلا عند الحاجة إلى فهم إسناد المصدر في بحثه. ويقيّم التقرير النشاط السيبراني الموصوف. ولا يقدّم تقييمًا للحكومات أو الأسرة المالكة أو العلاقات الإقليمية أو الدين أو قرارات السياسة العامة.

2.4 اقرأ التحذيرات الرسمية بوصفها مهام تشغيلية

توفّر الضوابط الأساسية الحالية للهيئة الوطنية للأمن السيبراني أساسًا للجهات المشمولة بنطاقها. وينشر Saudi CERT تحذيرات أمنية للمنتجات. وتثبت التحذيرات وجود توصية بفحص المنتجات المتأثرة، ولا تثبت مهاجمة شبكات سعودية عبر تلك المنتجات. [S13][S6]

والانضباط المطلوب هو إغلاق دورة العمل. حدّد مسؤول الخدمة، وتحقّق من انطباق التنبيه، واتخذ الإجراء، واحتفظ بدليل النتيجة. وإغلاق تذكرة لأن التحديث نُزّل لا يثبت تحديث كل النسخ المتأثرة.

الخلاصات الرئيسية

01
افصل مؤشرات الاتصال في المسوح عن قياسات الهجمات.

02
احمِ رحلة الهوية والدفع كاملة، بما فيها المورّدون.

03
حوّل كل تحذير منطبق إلى مهمة لها مسؤول ودليل إغلاق.

الفصل 03

الانكشاف الوطني: قائمة مختارة من 250 نطاقًا

يجيب هذا الفصل عن

ما الإشارات المرصودة التي تحتاج مسؤولًا للتحقق؟

96 من 249

نطاقًا مقيمًا ارتبطت ببيانات اعتماد معروضة للبيع وقت الفحص

3.1 بطاقة المجموعة المدروسة 13

3.2 القيمة الوطنية الرئيسية لـ Atlas وإشارات القطاعات 14

3.3 تحتاج الأجهزة وسجلات الاعتماد إلى مسؤولين مختلفين 15

3.4 الذكر والأسماء الشبيهة سياق 17

3.5 ملاحظات ضوابط النطاقات الخارجية 17

3.6 اجعل الاستجابة متناسبة 18

الفصل 03

الانكشاف الوطني: قائمة مختارة من 250 نطاقًا

باختصار

عُرضت بيانات اعتماد مرتبطة بعدد 96 من 249 نطاقًا مقيمًا للبيع وقت الفحص. وتضم القائمة المختارة 250 نطاقًا مرشحًا لمؤسسات؛ يفتقر أحدها إلى نتيجة انكشاف مكتملة. وتبلغ القيمة الوطنية الرئيسية لـ Atlas للقائمة المقيمة 52/100. وتصف ارتباطات الأجهزة والاعتماد ملاحظات خارجية، لا دخولًا مؤكدًا أو انتشارًا وطنيًا. وتبقى الملكية وتداخل المجموعات من حدود الأدلة. تحقّق من الحسابات الحالية وارتباطات أجهزة الموظفين وعلاقات الخدمات مع المسؤولين عنها.

3.1 بطاقة المجموعة المدروسة

البند	التعريف
الاختيار	250 نطاقًا مرشحًا لمؤسسات في عشر خلايا قطاعية تضم كل منها 25، اختيرت لأدوارها العامة أو عملياتها السعودية المهمة
الوحدة	نطاق رئيسي مختار لكل جهة مرشحة؛ قد تتداخل الكيانات القانونية المرتبطة والمجموعات المشتركة
حالة الهوية	لم تُثبت ملكية كل نطاق وحالته التشغيلية واستقلال كيانه
لقطة الانكشاف	22 نوفمبر 2026؛ عدد التقييمات المكتملة للنطاقات 249، مع نتيجة واحدة مجهولة في الخدمات الرقمية والاتصالات
تواريخ السجلات	ملاحظات الأجهزة والاعتماد والوثائق والإدراجات المحفوظة عند اللقطة؛ لا تقتصر على مادة التُقطت أول مرة خلال 2026
سياق الذكر	19 نوفمبر 2025–18 نوفمبر 2026؛ منفصل عن فترة نشر المنشورات في التقرير
الأسماء الشبيهة	فترة ملاحظات منفصلة من 30 يومًا؛ تحتاج العلاقات المرشحة إلى تحقق
التعميم	نتائج وصفية للنطاقات المختارة فقط؛ لا تقدير لانتشار وطني ولا تعداد لكيانات مستقلة

القائمة أداة للتحقيق، وليست قائمة ضحايا. ولا يعني الإدراج وقوع حادث أو أن كل سجل مرتبط يخص موظفًا. وتبقى نتيجة النطاق الغائب مجهولة، ويُستبعد من مقامات الانكشاف. [S3]

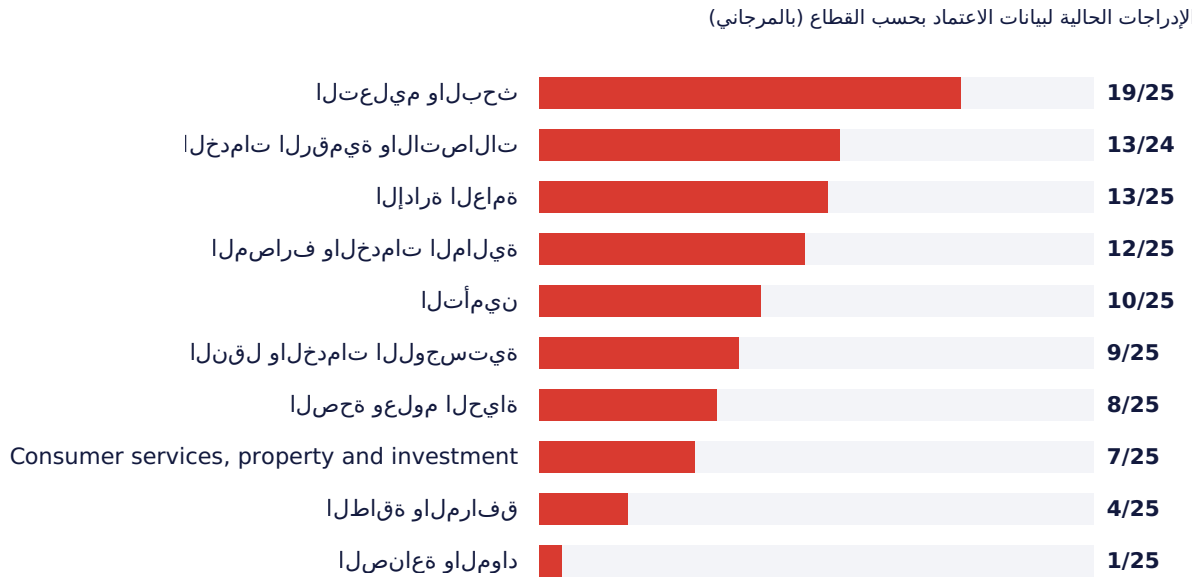
3.2 القيمة الوطنية الرئيسية لـ Atlas وإشارات القطاعات

عُرضت بيانات اعتماد مرتبطة بعدد 96 من 249 نطاقًا مقيمًا للبيع. يثبت الإدراج وجود إعلان وقت الفحص، لكنه لا يثبت صلاحية الاعتماد أو نشاط الحساب أو إتمام البيع أو الدخول. تحقّق من الخدمة والهوية المعنيتين قبل إجراء معطّل. [S3]

تبلغ القيمة الوطنية الرئيسية لـ Atlas للقائمة المقيمة ذات 249 نطاقًا 52/100. وتشير القيم الأعلى إلى انكشاف مرصود أكبر على مقياس 0–100. وليست النتيجة نسبة اختراق أو احتمال حادث أو تقييمًا لكل المؤسسات السعودية. وهي تستبعد النطاق الذي يفتقر إلى نتيجة مكتملة.

لا يُنشر سوى التقييم الوطني. وتعرض صفوف القطاعات الإشارات المقيسة ومقاماتها. وفي الشكل والجدول أدناه، يحصي عمود «المدرجة حاليًا» النطاقات المقيمة التي ارتبطت ببيانات اعتماد معروضة للبيع وقت الفحص، لا مؤسسات معروضة للبيع. ولا يعني تساوي أعداد النطاقات المختارة تساوي الحجم الاقتصادي أو استقلال الملكية أو الخطر الأمني.

الإدراجات الحالية لبيانات الاعتماد عبر مجموعات القطاعات المقيمة



النطاقات المدرجة / النطاقات المقيمة؛ استُبعدت النتيجة المجهولة. لا يثبت الإدراج وصولًا قابلًا للاستخدام. المصدر: Brandefense Atlas وارتباطات النطاقات في Blackhole، 22 نوفمبر 2026 [S3]. 250 نطاقًا مختارًا، 249 مقيمًا؛ قد تتداخل السجلات وتشمل ملاحظات أقدم.

القطاع	المختارة	المقيمة	المدرجة حاليًا	الوثائق
الإدارة العامة	25	25	13	220
المصارف والخدمات المالية	25	25	12	70
التأمين	25	25	10	10
الطاقة والمرافق	25	25	4	133
الصناعة والمواد	25	25	1	44

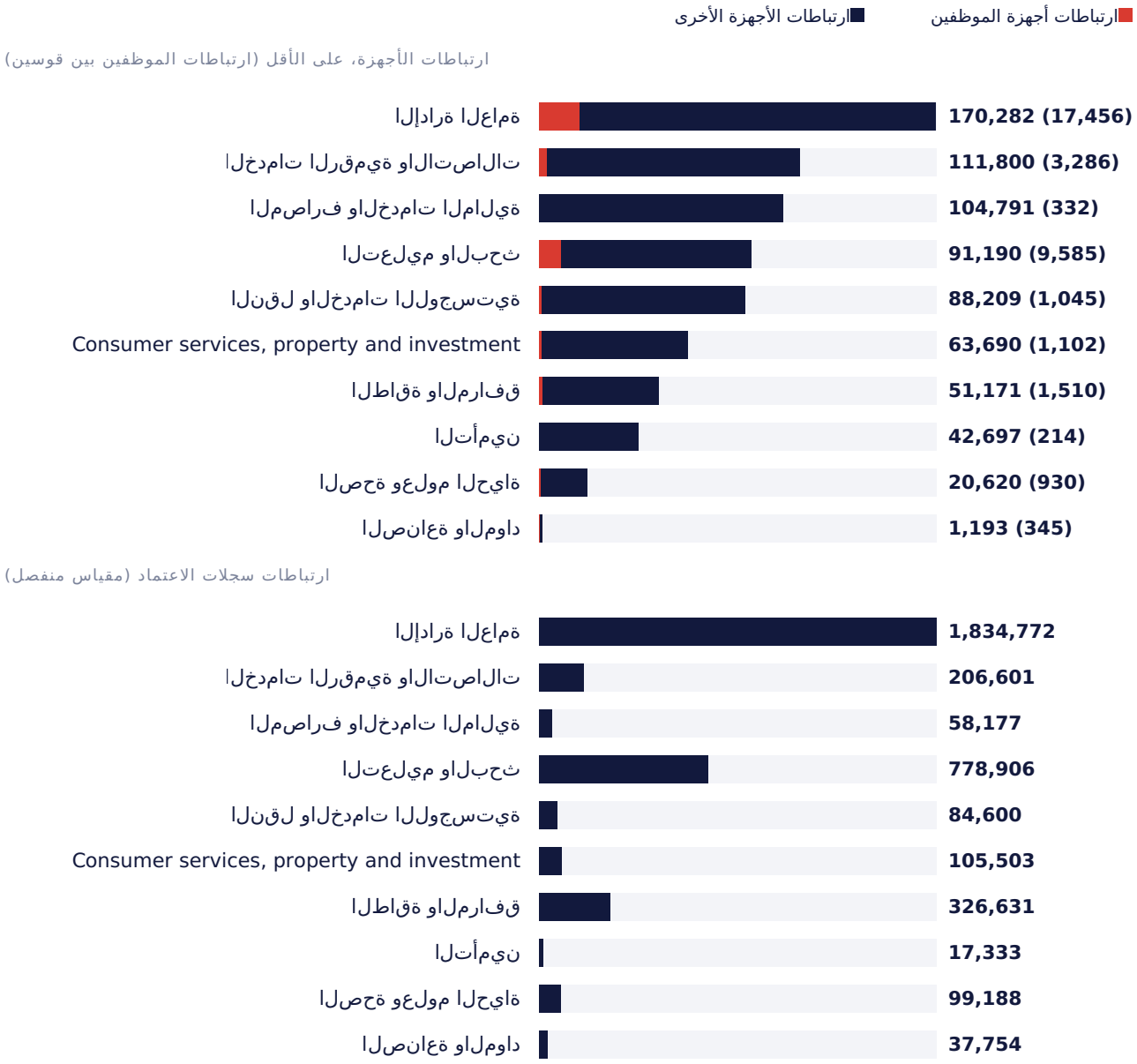
القطاع	المختارة	المقيمة	المدرجة حاليًا	الوثائق
النقل والخدمات اللوجستية	25	25	9	86
الخدمات الرقمية والاتصالات	25	24	13	110
الصحة وعلوم الحياة	25	25	8	88
التعليم والبحث	25	25	19	269
خدمات المستهلك والعقارات والاستثمار	25	25	7	98
المجموع	250	249	96	1,128

يضم عمود الوثائق 1,128 ارتباطًا بوثائق عبر 156 نطاقًا مقيمًا. ولا تثبت هذه الملاحظات السرية أو الاستحواذ غير المشروع أو وصول خصم. وقد تفسرها وثائق عامة أو مادة متكررة.

3.3 تحتاج الأجهزة وسجلات الاعتماد إلى مسؤولين مختلفين

تضم القائمة المقيمة ما لا يقل عن 745,643 ارتباطًا بأجهزة، منها 35,805 ارتباطًا بأجهزة موظفين. وتضم كذلك 3,549,465 ارتباطًا بسجلات اعتماد. وقد تتداخل هذه المجموعات عبر النطاقات؛ وليست أشخاصًا متمايزين أو عددًا وطنيًا للأجهزة. [S3]

ارتباطات الأجهزة وسجلات الاعتماد مجموعتان مختلفتان



المصدر: Brandefense Atlas وارتباطات النطاقات في Blackhole، 22 نوفمبر 2026 [S3]. 250 نطاقًا مختارًا، 249 مقيمًا؛ قد تتداخل السجلات وتشمل ملاحظات أقدم.

القطاع	المقيمة	الأجهزة، على الأقل	أجهزة الموظفين	سجلات الاعتماد
الإدارة العامة	25	170,282	17,456	1,834,772
المصارف والخدمات المالية	25	104,791	332	58,177
التأمين	25	42,697	214	17,333
الطاقة والمرافق	25	51,171	1,510	326,631
الصناعة والمواد	25	1,193	345	37,754

القطاع	المقيمة	الأجهزة، على الأقل	أجهزة الموظفين	سجلات الاعتماد
النقل والخدمات اللوجستية	25	88,209	1,045	84,600
الخدمات الرقمية والاتصالات	24	111,800	3,286	206,601
الصحة وعلوم الحياة	25	20,620	930	99,188
التعليم والبحث	25	91,190	9,585	778,906
خدمات المستهلك والعقارات والاستثمار	25	63,690	1,102	105,503
المجموع	249	745,643	35,805	3,549,465

تُعرض ارتباطات أجهزة الموظفين ضمن رؤية الأجهزة ولا تُضاف إليها. وقد تخص الارتباطات الأخرى عملاء أو مستخدمين آخرين للخدمات. ولا يثبت ارتباط نطاق مصرفي وحده الوصول إلى بنية المصرف.

تسهم الإدارة العامة بعدد 1,834,772 ارتباطًا بسجلات اعتماد، ويسهم التعليم والبحث بعدد 778,906. وتدعم الأعداد تحققًا موجهًا مع مسؤولي الهوية والخدمات. ولا ترتب معدلات الدخول الحالي ولا تثبت زمن انكشاف حساب.

قد تبقى السجلات التاريخية ظاهرة بعد المعالجة. تحقّق من وجود الهوية وتغيير مادة المصادقة ذات الصلة وما إذا تبعها نشاط مريب. وعند تأييد وصول موظف، راجع الجلسات وطرق الاسترداد والصلاحيات المفوضة إلى جانب كلمات المرور.

3.4 الذكر والأسماء الشبيهة سياق

تضم رؤية الذكر السنوية إشارات محادثة لعدد 56 من النطاقات المختارة وإشارات ويب لعدد 27. وقد تشمل المجموعتان المتداخلتان الأخبار والروابط المشروعة ونقاشات العملاء والإعلانات. ولا يثبت الذكر وحده نشاطًا عدائيًا. [S3]

تظهر أسماء شبيهة مرشحة لعدد 182 من 249 نطاقًا مقيمًا. ولا يثبت التشابه وحده الانتحال أو التصيد. تحقّق من الملكية والتفويض وسلوك الخدمة قبل تصعيد اشتباه بإساءة العلامة.

الإدراج الحالي وسجل الاعتماد التاريخي وارتباط الوثيقة والاسم الشبيه المرشح إشارات منفصلة. ولا تُجمع لإنتاج عدد أشخاص متأثرين. أحل كل معلومة موثوقة إلى مسؤول الهوية أو الأجهزة أو الاحتيال أو البيانات أو العلامة المعني.

3.5 ملاحظات ضوابط النطاقات الخارجية

لا تتوفر نتائج مكتملة لضوابط النطاقات الخارجية. لذلك لا ينشر التقرير انتشار DMARC أو SPF أو DKIM أو DNSSEC أو TLS أو ترويسات الويب، ولا مؤشرًا قطاعيًا لسلامة الإعدادات. وليس عدد النطاقات المختارة مقامًا لضوابط مقيمة. [S4]

تصف ملاحظات DNS والمواقع العامة الخدمات في تاريخ فحصها. ولا تقيس فاعلية البرنامج الأمني للمؤسسة كلها. ولا تثبت شهادة صالحة ضبط الوصول في التطبيق، كما أن غياب الملاحظة لا يعني فشل الضابط.

يجب تقييم مصادقة البريد عبر منظومة الإرسال الفعلية. فقد لا تصف سياسة النطاق المختار كل شركة تابعة أو نطاق فرعي أو مرسل خارجي. حدّد تدفقات البريد المشروعة واختبر أثر التغيير في العمل قبل تغيير الإنفاذ.

3.6 اجعل الاستجابة متناسبة

الملاحظة	التحقق الأول	القرار المتناسب
إعلان بيانات اعتماد	الهوية وإمكان الاستخدام والحداثة والمعالجة السابقة	التحقيق؛ والاحتواء عند وجود دليل على وصول مسروق قابل للاستخدام أو إساءة استخدام
ارتباط جهاز	الملكية والسياق والحسابات المعنية	الإحالة إلى مسار أمن الجهاز أو العميل المناسب
سجل اعتماد تاريخي	ما إذا تغير الوصول المعني	الإغلاق بدليل أو التحقيق في الانكشاف غير المحسوم
اسم شبيه مرشح	استخدام العلامة وسلوك الخدمة والتفويض	المراجعة واستخدام مسار حماية العلامة المناسب
مشكلة في سياسة البريد أو الخدمة	إعداد الإرسال أو الخدمة الفعلي	التصحيح مع مسؤول الخدمة

الخلاصات الرئيسية

01

تغطي القيمة الوطنية الرئيسية لـ Atlas عدد 249 نطاقًا مقيمًا ضمن القائمة المختارة.

02

تتداخل مجموعات الأجهزة والاعتماد والإدراجات والوثائق ولا تُجمع بوصفها ضحايا.

03

تحقّق من الهوية والمالك والخدمة قبل اختيار استجابة معطلة.

الفصل 04

ملاحظات الويب المظلم وأدلة الحالات

يجيب هذا الفصل عن

ما الذي تثبته المادة المحفوظة عن ادعاءات البيانات والحسابات والوصول؟

220

منشور منتدى موسوم بالسعودية في الفترة

4.1 بطاقة نطاق البيانات 20

4.2 الحجم الشهري وحدوده 20

4.3 فئات الأدلة المتكررة 22

4.4 التوقيت والتكرار والحداثة 22

4.5 حالات من تقارير عامة 23

4.6 ملفات حالات المنتديات 26

4.7 النشاط الحديث: 8–22 نوفمبر 36

4.8 ما الذي تسنده الحالات وما الذي لا تسنده 38

الفصل 04

ملاحظات الويب المظلم وأدلة الحالات

باختصار

تتضمن مادة المنتديات إعلانات بيانات عملاء ووثائق وطلب حسابات وعروض وصول بعيد. ويتركز الوسم الأوسع في أول شهرين، مع حدود صريحة لرؤية المحتوى. وتحفظ عشرة ملفات منتديات الفرق بين المنشور وادعاء البيانات والوصول المتحقق منه. وتضيف التقارير العامة إفصاح تطبيق مؤكدًا وحملات مبلّغًا عنها. تحقّق من الصلة عبر سجلات داخلية وقنوات مورّدين معتمدة قبل وصف الأثر.

4.1 بطاقة نطاق البيانات

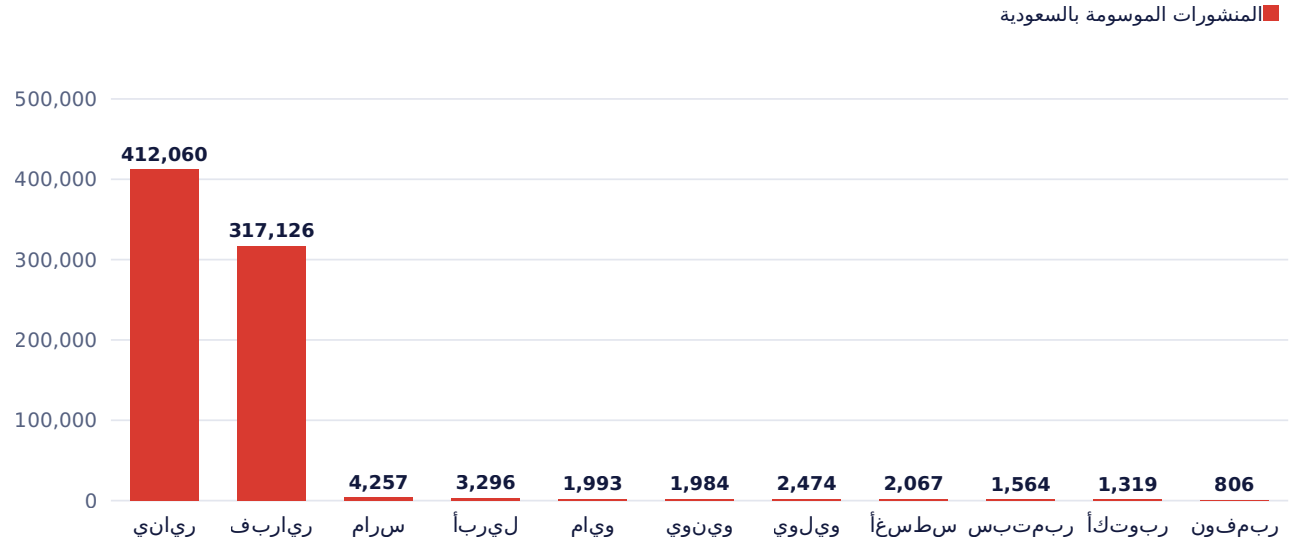
البند	النطاق
الفترة	1 يناير–22 نوفمبر 2026 بحسب وقت المنشور
حجم الوسم الجغرافي	748,946 منشورًا مرتبطًا بالسعودية؛ لا يثبت الوسم الاستهداف
مادة المنتديات الموسومة	220 منشورًا محفوظًا في الفترة
المادة المرتبطة بالعربية	5,043 منشورًا محفوظًا يحمل ارتباطًا بالعربية
المادة المجمعة المحفوظة	33,458 منشورًا متمايزًا عبر رؤى المحتوى
التفسير	المنشورات والحسابات والإعلانات والبيانات المدعاة والحوادث وحدات مختلفة
دليل النتيجة	الادعاءات لا تتحقق من جهة الهدف؛ ولم يُختبر وصول معروض

يصف النطاق المادة الملحوظة. وقد تكرر منشورات منتجًا أو تذكر دولًا عدة أو تناقش حدثًا أقدم. ولذلك لا يتحول الارتباط ببلد إلى عدد ضحايا. [S1]

4.2 الحجم الشهري وحدوده

يعرض الشكل حجم المنشورات الموسومة بالسعودية. ويشكل يناير وفبراير 97.4% من هذا الحجم. ولا يفسر التقرير التوزيع بوصفه تغيرًا في وتيرة الهجمات. [S1]

يهيمن أول شهرين على حجم المنشورات الموسومة بالسعودية



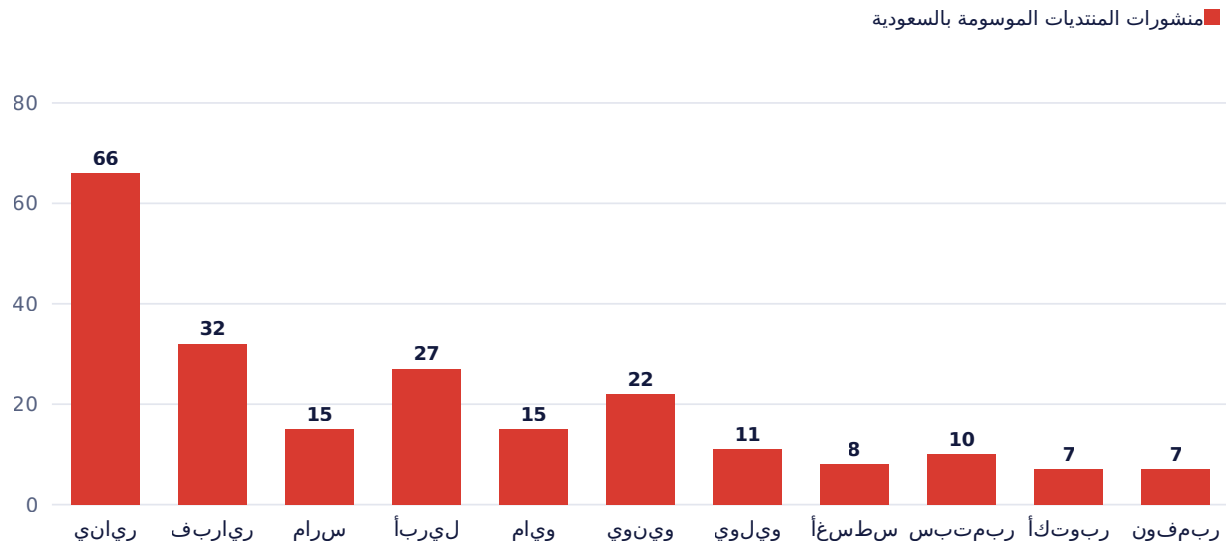
المصدر: Brandefense Blackhole، المنشورات الموسومة بالسعودية، 1 يناير-22 نوفمبر 2026؛ نوفمبر جزئي [S1]. حجم المنشورات لا يقيس الهجمات.

الشهر	المنشورات الموسومة بالسعودية
2026-01	412,060
2026-02	317,126
2026-03	4,257
2026-04	3,296
2026-05	1,993
2026-06	1,984
2026-07	2,474
2026-08	2,067
2026-09	1,564
2026-10	1,319
2026-11	806
المجموع	748,946

تهيمن قوائم إعلانات خدمات على مادة يناير وفبراير، وغالبًا ما تذكر السعودية عنصرًا ضمن عرض متعدد الدول. ويحد ذلك من قيمتها دليلًا على تهديد خاص بالسعودية. وتتفاوت التغطية بحسب الشهر والمصدر. ولا تثبت هذه الملاحظات انتشارًا وطنيًا أو تغيّرًا في وتيرة الهجمات.

وتفيد رؤية المنتديات سؤالًا مختلفًا: ما العروض والنقاشات الظاهرة في مجموعة المصدر؟ وهي تضم 66 منشورًا في يناير، وكل شهر لاحق أقل من يناير. وهذه تغطية لملاحظات منتديات، وليست منحنى حوادث وطنيًا.

تسجّل رؤية المنتديات الموسومة بالسعودية أكبر حجم لها في يناير



المصدر: Brandefense Blackhole، المنشورات الموسومة بالسعودية، 1 يناير-22 نوفمبر 2026؛ نوفمبر جزئي [S1]. حجم المنشورات لا يقيس الهجمات.

4.3 فئات الأدلة المتكررة

الفئة	أمثلة محفوظة	ما يمكن إثباته	ما لا يمكن استنتاجه
إعلانات بيانات	أوصاف استثمار وصحة وعافية وسائقين وطرود	عرض وحقوله أو كمياته المعلنة	الأصالة أو الوصول الحالي أو الأشخاص المتأثرون
حزم وثائق وشيفرة	أرشيف جهة عامة ومقاولين	وصف وتسلسل تداول	التصنيف أو وصول الإنتاج أو أثر في كل الشركاء
طلب حسابات	طلبات حسابات مرتبطة بالسعودية	اهتمام شراء معلن	العرض المتاح أو الصفقة أو الوصول الصالح
إعلان وصول بعيد	عرض وصول لمنشأة طبية	ادعاء قدرة من بائع	مصادقة ناجحة أو تحكم تشغيلي
ادعاءات تعطيل	منشورات أهداف خدمية وتحديثات متكررة	سرد نشر	انقطاع مقيس أو سبب أو وصول إلى بيانات
إعلانات خدمات احتيال	توفير أصحاب حسابات وطلب حساب استقبال	عرض خدمة أو طلب	غسل أموال مكتمل أو نجاح احتيال أو وصول إلى أنظمة بنك

تتداخل موضوعات هذه الفئات. وليست أحكام حوادث متنافية، ولا تُجمع لإنتاج مجموع وطني. وتحفظ ملفات الحالات المعلومة المحددة التي يسندها كل مصدر.

4.4 التوقيت والتكرار والحداثة

قد تجدد إعادة النشر الاهتمام من دون إثبات دخول جديد. ففي الحالة E يصف الناشر إعادة النشر صراحة. وفي الحالة H تضيف المتابعة عينة في اليوم نفسه. وفي الحالة L تصف سجلات عدة موضوع أرشيف واحدًا. [S1]

ويوضح عرض بيانات موظفين في مارس حداثة غير محسومة. سأل رد عما إذا كانت المادة من 2021، بينما أكد الناشر أنها حديثة. ولا يحسم الحوار عمر السجلات. وهو يدعم مراجعة الحوادث والمعالجة السابقة قبل اختيار استجابة معطلة جديدة. [S1]

وينطبق التمييز على روايات الدخول التقنية. فقد يدعي بائع خداع موظف أو استمرار وصول من دون تقديم دليل على نجاح المسار. ويحفظ التقرير ذلك كادعاء، ولا يتبناه سلسلة هجوم ثابتة.

ووصف نقل في 10 سبتمبر وثائق للقطاع العام أيضًا. ولم تثبت علاقته بأرشيف يونيو. ولا يثبت تشابه الأوصاف تطابق الملفات أو تاريخ اقتناء جديدًا. [S1]

4.5 حالات من تقارير عامة

تفصل الحالات التالية إفصاح جهة تحكم عن ادعاء إجرامي منقول وحملات رصدها باحثون. وتشير تواريخها إلى النشر ما لم يحدّد المصدر تاريخ حدث صراحة. وهي ليست أربعة اختراقات مؤكدة إضافية.

الحالة A

A

إفصاح عن بيانات عملاء تطبيق هاتف

النقل والخدمات اللوجستية

إفصاح الشركة

الادعاء والمصدر	في 9 يونيو، أفصحت بدجت السعودية عن وصول غير مصرح به إلى جزء محدود من بيانات بعض العملاء عبر تطبيقها. ونشرت وسائل أخبار مالية بيان الشركة الرسمي أيضًا. [S28][S18][S17]
التسلسل الزمني	قالت الشركة إنها فعّلت إجراءات الاحتواء بعد الاكتشاف، وواصلت التقييم الفني بالتنسيق مع الجهات المعنية. ولم يذكر الإفصاح تاريخ الدخول أو عدد العملاء المتأثرين.
ما يمكن إثباته	أكدت الشركة علنًا حادث وصول إلى بيانات عملاء. وقالت إن المعلومات المالية والمصرفية لم تتأثر وإن الخدمات استمرت من دون انقطاع. وتبقى هذه الحدود للنطاق والأثر تصريحات الشركة.
البدائل والحدود	لا يحدّد الإفصاح جهة فاعلة أو ثغرة أو الحقول المتأثرة أو صلة ببرامج الفدية. ولا يحسم استمرار الخدمة أثر الحادث في سرية البيانات.
الاستجابة	ينبغي لمسؤولي التطبيقات تحديد الوصول إلى بيانات العملاء واختبار الفصل بين حساباتهم وحفظ تسلسل القرار. وعلى فرق الخصوصية تقييم شروط الإشعار وفق نطاق بيانات متحقق منه.

الخلاصة

تحقق من النطاق عبر إدارة الحادث؛ فالاستمرارية والسرية أمران منفصلان.

توضح الحالة ضرورة تقييم استمرارية العمل وسرية البيانات كلًا على حدة. ولا تسند استنتاجًا عن أمن تطبيقات أخرى أو قطاع النقل كله.

الحالة B

B ادعاء غير متحقق منه لبيانات قطاع الإنشاءات

الإنشاءات

ادعاء منقول - غير متحقق منه

الادعاء والمصدر	نقلت The National رواية جهة رصد عن ادعاء WallStreet يخص شركة إنشاءات. وتعلقت المزاعم بمجموعة ملفات كبيرة ومعلومات موظفين. وتبقى كمياتها المعلنة غير متحقق منها. [S19]
التسلسل الزمني	نُشرت المقالة في 6 أكتوبر وربطت المزاعم بيوم 3 أكتوبر. وتاريخ الحدث المدعى ليس وقت دخول متحققًا منه. وكرر نقل في 21 أكتوبر مزاعم مشابهة، من دون تأكيد مستقل أو حدث جديد ثابت. [S1]
ما يمكن إثباته	نشرت الصحيفة الادعاء وطلبت تعليقًا. ولم تقدّم تأكيدًا رسميًا لسرقة بيانات. ولم تتضمن الرواية المقروءة ردًا جوهريًا من الشركة أو تأكيدًا من جهة مختصة.
البدائل والحدود	قد تضم المادة سجلات لدى مورّد أو بيانات معاد تداولها أو نطاقًا مبالغًا فيه. ولا يثبت الإعلان أو ذكر مشروع دخولًا إلى شبكة الجهة الرئيسية. ولا يحدّد التقرير أيّ هذه البدائل صحيح.
الاستجابة	ينبغي لمالكي البيانات المعنية مراجعة المشاركة التعاقدية وطلب بيان محدد النطاق من المورّدين عبر القنوات المعتمدة. صعّد عند ربط سجلات موثوقة أو تأكيد مورّد الادعاء ببيانات محمية.

الخلاصة

تحقق من علاقة البيانات قبل وصف الأثر في الشركاء.

يبرر ادعاء يخص مورّدًا تحديد علاقة البيانات. ولا يبرر إعلان دخول إلى أنظمة كل شريك. ويحجب المرجع العام رابط المقالة لحماية الشركة غير المسماة.

الحالة C

C حملة مبلّغ عنها لرش كلمات مرور سحابية

الهوية عبر القطاعات

حملة رصدها باحثون

الادعاء والمصدر	أفادت Check Point بثلاث موجات في 3 و13 و23 مارس. ووصف بحثها استهدافًا سعوديًا محدودًا ضمن حملة تركزت في دول أخرى. [S12]
التسلسل الزمني	نُشر التقرير في 31 مارس. وهو يصف محاولات عبر حسابات كثيرة، ولا يصف إفصاحًا سعوديًا واحدًا. ولا يقدّم عددًا سعوديًا للجلسات الناجحة.
ما يمكن إثباته	رصد المصدر نشاط الحملة ضد بعض الأهداف السعودية. وقدّرت Check Point بثقة متوسطة أن منشأ الجهة الفاعلة هو إيران. وينقل هذا التقرير الإسناد بوصفه تقييم المصدر فقط.

البدائل والحدود	لا يجوز تحويل وصف الوصول إلى البريد على مستوى الحملة إلى إثبات وصول لدى كل هدف سعودي. ولا تثبت التقنية المشتركة أن جهة مسماة في تقرير آخر شغّلت هذه الحملة.
الاستجابة	ينبغي لفرق الهوية فحص إخفاقات المصادقة عبر الحسابات وربطها بالجلسات الناجحة والنشاط اللاحق. واحفظ التفسيرات البديلة، مثل تغييرات مشروعة في خدمة الهوية.

الخلاصة

افحص الحسابات والجلسات من دون تعميم نتائج الحملة.

الوحدة العملية هي الحساب والجلسة. ولا يغيّر الإسناد إلى بلد ضرورة التحقق من تسلسل المصادقة الملحوظ قبل اختيار الاحتواء.

الحالة D

D انتحال مبلّغ عنه للدخول المؤسسي والدفع

الاحتيال عبر القطاعات

حملة رصدها باحثون

الادعاء والمصدر	وصفت Unit 42 تصيّدًا مؤسسيًا موجّهًا إلى السعودية ينتحل علامات أنظمة ERP، إلى جانب طُعوم فواتير واستثمار ومصارف. والموجز رواية حملة، وليس إحصاءً وطنيًا للضحايا. [S11]
التسلسل الزمني	حُدّثت النسخة المستشهد بها في 17 أبريل 2026. وتخص ملاحظاته الإقليمية الأوسع دولًا مختلفة، فلا تُنسب كلها إلى السعودية.
ما يمكن إثباته	أفاد المصدر بتصيّد واحتيال مالي موجّهين إلى السعودية. ولم ينشر مجموع خسائر سعوديًا أو قائمة ضحايا مكتملة أو عدد عمليات وصول ناجحة للحسابات في هذه الملاحظات.
البدائل والحدود	قد تُستخدم علامة في طُعم من دون الوصول إلى أنظمتها. ولا تثبت قوالب صفحات أو خدمات استضافة مشتركة وجود مشغّل واحد. ولا نضيف إسنادًا إلى دولة لهذا الوصف السعودي للاحتيال.
الاستجابة	اختبر الإبلاغ عن طُعوم الدخول المؤسسي والتحقق الموثوق من تعليمات الدفع. واربط حالات دعم العملاء والاحتيال عندما تتعلق بالمعاملة أو عملية الاستعادة نفسها.

الخلاصة

احمِ مسارات الدخول والتحقق الموثوق من الدفع.

تتجاوز الثقة في العلامة حدود المؤسسة. ولذلك تحتاج الاستجابة إلى أدلة تقنية ومسار آمن يتحقق عبره العميل من التعليمات. ولا يثبت تنبيه رصد العلامة وحده من خسر مالًا.

4.6 ملفات حالات المنتديات

تصف الملفات التالية إعلانات مرصودة وطلب شراء واحدًا. ولا يثبت أي منها دخولًا مؤكدًا رسميًا. وتبقى إعادة النشر والردود ضمن الملف الأصلي. ويسجّل سجل البطاقات تاريخ المنشور، لا تاريخ السرقة. [S1]

الحالة E

E

ادعاء شيفرة وبيانات اعتماد لجهة عامة

بطاقة الدليل B01 | 17 يناير 2026 | منتدى | الإدارة العامة

ادعاء غير متحقق منه

الادعاء	أعلن ناشر شيفرة مصدرية وبيانات اعتماد لقواعد بيانات نُسبت إلى جهة عامة. وقدّم شكوى حقوق نشر مزعومة بوصفها تأكيدًا للمادة.
التسلسل الزمني	يبدأ النقاش المحفوظ في 17 يناير، مع سجلات مرتبطة في 18 و24 يناير. وصرّح الناشر بأنه يعيد النشر. وتثبت هذه التواريخ التداول، لا الحصول الأول على المادة.
ما يمكن إثباته	نحتفظ بإعلان المنتدى ورواية إعادة النشر. ولا يتحقق التقرير من الشيفرة المعروضة أو أي بيانات اعتماد.
البدائل والحدود	لا تثبت الشكوى الأصالة. وقد تكون المادة تاريخية أو منسوخة أو إعداد اختبار. ولا تجعل إعادة الإعلان الوصول المدعى حاليًا.
الاستجابة	على مسؤولي المستودعات والهوية مقارنة الادعاء بسجلات داخلية مصرح بها. وإذا طابق سر مكشوف حقيقي استخدامًا حاليًا، فاحتوِ الانكشاف عبر إدارة الحادث. لا تختبر الوصول المعروض.

الخلاصة

افحص مصدر الشيفرة والأسرار الحالية عبر سجلات داخلية مصرح بها.

بطاقة الدليل B01 — 17 يناير 2026

zer0sintt منتدى Forum الإنجليزية

النص الأصلي

so I am reposting it

الترجمة

أعيد نشره

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته
إعلان شيفرة مصدرية وبيانات اعتماد، مع تصريح بإعادة النشر. [S1]

ما لم يثبت
لا تثبت شكوى حقوق نشر أو قطعة شيفرة أو منشورات متكررة دخولًا أو وصولًا حاليًا صالحًا. وقد تكون القطعة قديمة أو منسوخة أو إعداد اختبار أو غير قابلة للاستخدام.

الحالة F

F

عرض بيانات خدمة صحية

بطاقة الدليل B02 · 30 يناير 2026 · منتدى · الرعاية الصحية

ادعاء غير متحقق منه

الادعاء	عرض منشور في 30 يناير بيانات نُسبت إلى خدمة بيانات صحية ووصفها بأنها حديثة. وجمعت أوصاف الحقول معلومات هوية واتصال وصحة.
التسلسل الزمني	تاريخ المنشور هو التوقيت الوحيد المثبت للعرض. ولا يثبت وقت نشوء السجلات أو وقت الوصول المدعى.
ما يمكن إثباته	أعلن الناشر مجموعة بيانات تتضمن فئات حقول حساسة. ووصف الحداثة يعود إلى الناشر.
البدائل والحدود	لا تثبت قائمة حقول مصدرًا من نظام إنتاج أو اكتمالًا. وقد تشبه بيانات عامة أو اصطناعية أو لدى مورّد أو قديمة مخططًا داخليًا. ولا يحسم التقرير التفسير المنطبق.
الاستجابة	على مالكي البيانات التحقق من علاقات الحقول مقابل مخازن مصرح بها وتقييم الحساسية. وعند وجود قرائن، تحدّد فرق الخصوصية والحوادث نطاق الوصول والإبلاغ. ولا يحسم وصف عينة وحده القرار.

الخلاصة

طابق الحقول بتدفقات بيانات مضبوطة قبل تحديد استجابة الخصوصية.

بطاقة الدليل B02 — 30 يناير 2026

alwayslearning منتدى Forum الإنجليزية

النص الأصلي

Data is fresh. Data is highly valuable.

الترجمة

البيانات حديثة. البيانات عالية القيمة.

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته
عرض بيانات صحية يصف حقول هوية واتصال وصحة. [S1]

ما لم يثبت
لا يثبت الارتباط ببلد وأوصاف المخطط المصدر أو الاكتمال أو الحداثة أو الوصول إلى الإنتاج. والعينة المقدمة غير متحقق منها.

الحالة G

G طلب حسابات هوية رقمية وبنية تحتية

بطاقة الدليل B03 · 2 فبراير 2026 · منتدى · الهوية عبر القطاعات

طلب مرصود

الادعاء	في 2 فبراير، طلب مشترٍ حسابات مرتبطة بالسعودية ووصفها بأنها جاهزة ومفحوصة. وشمل الطلب خدمات هوية وبنية تحتية نصفها هنا بصورة عامة.
التسلسل الزمني	نحتفظ بمنشور طلب واحد لهذا الملف. ولم يُثبت رد بائع أو صفقة أو نجاح مصادقة لاحق.
ما يمكن إثباته	يبيّن المنشور رغبة معلنة في الشراء. ولا يثبت وجود حساب متاح أو خدمة ضعيفة.
البدائل والحدود	قد يعلن مشترٍ طلبه من دون أن يحصل على شيء. ولا يثبت الطلب سعرًا أو عرضًا متاحًا أو صلاحية حساب أو علاقة صاحبه بالخدمة المطلوبة.
الاستجابة	ينبغي لفرق الهوية مراجعة مسارات الاستعادة عالية المخاطر ووصول المقاولين. يوجّه الطلب مراجعة ضوابط؛ أما الإجراءات المعطلة للحسابات فتحتاج صلة أقوى بهوية فعلية أو إساءة استخدام.

الخلاصة

راجع ضوابط الاستعادة؛ لا يحدد طلب المشتري حسابًا مكشوفًا.

بطاقة الدليل B03 — 2 فبراير 2026

l0rd0f · منتدى · Forum · الإنجليزية

النص الأصلي

Looking to buy any saudi-arabia related accounts

الترجمة

أرغب بشراء أي حسابات مرتبطة بالسعودية

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته
طلب واحد لحسابات هوية وبنية تحتية مرتبطة بالسعودية. [S1]

ما لم يثبت
يثبت الطلب الاهتمام فقط. ولا يبيّن بائعًا أو صفقة أو صلاحية حساب أو مصادقة ناجحة أو دخولًا إلى أنظمة الجهة المعنية.

الحالة H

H

عرض بيانات عملاء منصة استثمار

بطاقة الدليل B04 · 13 فبراير 2026 · منتدى · الخدمات المالية

ادعاء غير متحقق منه

الادعاء	أعلن بائع نحو 7,000 سجل مستثمر نُسبت إلى منصة استثمار. وشمل الوصف حقول هوية وتسجيل وإشارات إلى حسابات مالية.
التسلسل الزمني	نشر البائع في 13 فبراير وأضاف مادة عينة لاحقًا في اليوم نفسه. وهما سجلان في ملف واحد.
ما يمكن إثباته	الإعلان والمتابعة محفوظان. ويدعم السياق المتطابق استمرار العرض، لا وقوع حادثين.
البدائل والحدود	لم يُتحقق من عدد السجلات أو الأرصدة أو مصدر البيانات. ولا تثبت حقول المحفظة أو الحساب الوصول إلى أموال أو خسارتها.
الاستجابة	على مالكي البيانات ومكافحة الاحتيال تقييم تطابق الحقول مع واجهات مصرح بها. وافحص نشاط الحساب المرتبط عند وجود قرائن. وافصل تقييم الإفصاح عن تقييم خسارة الدفع.

الخلاصة

افصل إفصاح بيانات العملاء عن سلامة المحافظ والخسارة المالية.

بطاقة الدليل B04 — 13 فبراير 2026

agent7001 · منتدى · Forum · الإنجليزية

النص الأصلي

around 7k of investors data.

الترجمة

بيانات لنحو 7k مستثمرين.

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته
عرض سجلات استثمار ومتابعة في اليوم نفسه. [S1]

ما لم يثبت
المنشوران ملف واحد، لا حادثان. وأعداد السجلات وحقول الحساب والمحفظة ادعاءات بائع؛ لا تثبت صحة رصيد أو خسارة أو وصولًا حاليًا.

الحالة ا

حزمة مقاولين مع وثائق مشاريع

بطاقة الدليل B05 · 23 فبراير 2026 · منتدى · الإنشاءات والهندسة

ادعاء غير متحقق منه

الادعاء	أعلن بائع حزمة مقاولين بسعر 40,000 USD. وشمل الوصف ملفات موظفين وخرائط مشاريع وعقودًا، وزعم اتفاقًا أثّر في إدراج إحدى الشركات.
التسلسل الزمني	يحمل سجلان متشابهان بدرجة كبيرة الوقت نفسه في 23 فبراير. وهما يوثّقان إعادة إعلان، لا تأكيدًا مستقلًا.
ما يمكن إثباته	العرض والحجم والسعر المطلوب محفوظة بوصفها تصريحات البائع. ولم يُثبت بيع مكتمل أو اتفاق.
البدائل والحدود	قد تخص وثائق المورّد جهة رئيسية من دون أن تثبت الوصول إلى أنظمتها. ولم يُتحقق من المحتوى أو حساسيته التقنية أو صلته بالتشغيل.
الاستجابة	على المشتريات وأمن الهندسة تحديد الاعتماد على الوثائق المشتركة. تحقّق من الصلة عبر المالكين المصرح لهم، ثم راجع صلاحيات المورّد وواجبات الإبلاغ عند وجود تطابق.

الخلاصة

تحقق من مشاركة بيانات المقاولين من دون نسبة أثر إلى الجهات الرئيسية.

بطاقة الدليل B05 — 23 فبراير 2026

ryhem · منتدى · Forum · الإنجليزية

النص الأصلي

Data volume: [quantity removed] Price: $40,000

الترجمة

حجم البيانات: [حُذفت الكمية] السعر: 40,000$

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته
إعلانان متشابهان بدرجة كبيرة لحزمة مقاولين. [S1]

ما لم يثبت
تدعم النسخ المتشابهة إعادة النشر، لا التأكيد المستقل. والاتفاق المدعى والمحتويات ومعلومات الأنظمة الصناعية ومدى الوصول غير متحقق منها.

الحالة J

ادعاء بيانات CRM لخدمة عافية

بطاقة الدليل B06 · 27 فبراير 2026 · منتدى · الصحة والخدمات الاستهلاكية

ادعاء غير متحقق منه

الادعاء	ادعى إعلان في 27 فبراير وجود سجلات عملاء نُسبت إلى خدمة عافية، بسعر مطلوب 150 USD. وزعم الناشر خداع موظف لتمكين الوصول إلى CRM.
التسلسل الزمني	يثبت المنشور المحفوظ وقت ظهور العرض. ولا يثبت وقت تواصل الموظف المزعوم أو استخراج البيانات.
ما يمكن إثباته	وصف البائع مجموعة بيانات وسعرًا ورواية دخول. وهذه ادعاءات داخل إعلان واحد.
البدائل والحدود	لا يثبت مخطط ملصق رواية الهندسة الاجتماعية أو استمرار الوصول إلى CRM. ويبقى عدد السجلات وادعاء وثائق الهوية غير متحقق منهما.
الاستجابة	عند تطابق الوصف مع بيانات داخلية، راجع صلاحيات CRM والوصول بمساعدة الدعم وعمليات التصدير غير المعتادة. واحفظ أدلة الجلسات والتغييرات الإدارية قبل تحديد نطاق الاحتواء.

الخلاصة

راجع صلاحيات CRM والتصدير عند وجود تطابق داخلي.

بطاقة الدليل B06 — 27 فبراير 2026

sexyskin منتدى Forum الإنجليزية

النص الأصلي

tricked employee to get me inside the CRM panel

الترجمة

خدعت موظفًا ليُدخلني إلى لوحة CRM

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته
عرض CRM لخدمة عافية وسعر مطلوب ورواية مدعاة لخداع موظف. [S1]

ما لم يثبت
لم تُثبت طريقة الدخول أو عدد السجلات أو ادعاءات وثائق الهوية مستقلًا. ولا يثبت مخطط وعينة ملصقان استمرار الوصول أو أثرًا وطنيًا.

الحالة K

K

عرض بيانات سائقين وتصاريح

بطاقة الدليل B07 · 19 أبريل 2026 · منتدى · النقل والخدمات العامة

ادعاء غير متحقق منه

الادعاء	وصف عرض في أبريل سجلات تتضمن حقول سائقين وهوية واتصال وتراخيص ومركبات. ويشير الوصف العام إلى خدمة بيانات نقل بدل تحديد نظام بعينه.
التسلسل الزمني	تظهر سجلات مرتبطة في 19 و20 أبريل. وتكرر النسخ والردود موضوع البيانات المعروضة نفسه.
ما يمكن إثباته	نحتفظ بأوصاف الحقول والعدد المعلن بوصفها ادعاء. ولا تقدّم البطاقة المعروضة اقتباسًا يسند تلك الحقول. ولا تثبت منشورات متعددة حوادث مصدر متعددة.
البدائل والحدود	قد تعكس البيانات جمعًا أقدم أو تصدير مورّد أو مصادر مختلطة. ولا يثبت عنوان المنتدى وصولًا حديثًا أو أشخاصًا متمايزين.
الاستجابة	على مالكي بيانات النقل مقارنة العلاقات الموصوفة بسجلات مصرح بها. وافحص الاستعلام أو التصدير الجماعي ذي الصلة عند وجود تطابق. ولا تنسب المصدر اعتمادًا على أسماء حقول مألوفة.

الخلاصة

تحقق من علاقات بيانات السائقين قبل نسبة نظام أو عدّ أشخاص.

بطاقة الدليل B07 — 19 أبريل 2026

ناشر غير مسمى · منتدى · Forum · الإنجليزية

النص الأصلي

K. لا يُعرض مقتطف عام؛ لُخصت فئات الحقول في الحالة

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته
عرض وردود تصف حقول سائقين وتراخيص ومركبات. ولا يُعرض اقتباس يسند تلك الحقول. [S1]

ما لم يثبت
الكلمات المكررة تصف مجموعة بيانات معلنة واحدة. ولا يثبت عنوان المنتدى حادثًا حديثًا أو تفرّد السجلات أو الوصول إلى نظام الهدف أو مصدر البيانات.

الحالة L

L

تداول حزمة وثائق للقطاع العام

بطاقة الدليل B08 · 8 يونيو 2026 · منتدى · الإدارة العامة

ادعاء غير متحقق منه

الادعاء	وصف نقاش في يونيو أرشيفًا يضم وثائق وإشعارات وصورًا ومراسلات نُسبت إلى القطاع العام. وادعى الوصف الأصلي أيضًا حساسية المادة.
التسلسل الزمني	ظهرت منشورات مرتبطة في 8 و9 يونيو. وتشير صيغ التوقيت المختلفة إلى فترة التداول نفسها، ولا تثبت سرقات منفصلة.
ما يمكن إثباته	تداولت سجلات المنتديات وصف الأرشيف. ولا يثبت الوصف التصنيف المدعى أو الأصالة.
البدائل والحدود	قد تكرر النسخ مادة تاريخية أو مختلطة. ولا يثبت حجم الأرشيف أو مظهر الوثيقة الوصول إلى نظام إنتاج أو حادثًا جديدًا.
الاستجابة	على مسؤولي السجلات والأمن تقييم الأصالة والحساسية الحالية عبر قنوات مصرح بها. وراجع ضوابط مشاركة الوثائق المعنية عند وجود قرائن. ولا تنزّل أرشيفًا متداولًا لمجرد تكرار الادعاء.

الخلاصة

قيّم الأصالة والحساسية؛ الأرشيفات المتكررة ليست دخولًا جديدًا.

بطاقة الدليل B08 — 8 يونيو 2026

ناشر غير مسمى · منتدى · Forum · الإنجليزية

النص الأصلي

Photos of docs + whatsapp chats

الترجمة

صور وثائق ومحادثات واتساب

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته
وصف أرشيف وثائق متداول عبر سجلات منتديات. [S1]

ما لم يثبت
لا يثبت وصف أرشيف الأصالة أو التصنيف أو الوصول إلى الإنتاج أو دخولًا جديدًا. والنسخ والردود ليست حوادث مستقلة.

الحالة M

M

ادعاء نشر بيانات طرود

بطاقة الدليل B09 · 15 سبتمبر 2026 · منتدى · النقل والخدمات اللوجستية

ادعاء غير متحقق منه

الادعاء	زعم ناشر في سبتمبر وجود مجموعة كبيرة من بيانات الطرود بوحدة الأسطر، وأعلن جزءًا أصغر منها. وذكر الوصف فئات حقول المرسل والمستلم.
التسلسل الزمني	يعود المنشور المحفوظ إلى 15 سبتمبر. ولا يثبت زعمه وقوع حدث في 2026 تاريخ حادث بصورة مستقلة.
ما يمكن إثباته	الإعلان وكمياته محفوظان. وتصف الكميات ما ادعاه الناشر، لا مجموعة مقيسة من الأشخاص المتأثرين.
البدائل والحدود	الأسطر والسجلات والشحنات والأشخاص وحدات مختلفة. ولا يمكن ضرب طرفين لكل سطر لإنتاج مجموع أشخاص متمايزين. ولم يُتحقق من الاستخراج أو الحداثة أو أي بيع مكتمل.
الاستجابة	على مالكي خدمات التوصيل التحقق من المصدر مقابل سجلات معاملات مصرح بها. وقيّم مخاطر انتحال دعم العملاء والوصول غير المعتاد عند وجود قرائن. ولا تنشر معرّفات شحن أو بيانات اتصال أثناء التحقق.

الخلاصة

عامل أسطر الشحنات والسجلات والأشخاص كوحدات مختلفة.

بطاقة الدليل B09 — 15 سبتمبر 2026

ناشر غير مسمى | منتدى | Forum | الإنجليزية

النص الأصلي

affecting both domestic and international shipments.

الترجمة

تشمل الشحنات المحلية والدولية

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته

إعلان بيانات طرود يدعي أعداد أسطر وحقول مرسلين ومستلمين. [S1]

ما لم يثبت

الأسطر والسجلات والأشخاص وحدات مختلفة. ولا يثبت وجود حقلين أو طرفين في السطر ضعف عدد الأشخاص المتمايزين. ولا نحتفظ باستخراج متحقق منه أو سبب جذري أو رد رسمي أو بيع مكتمل.

الحالة N

N

ادعاء أرشيف شيفرة ووثائق لمقاول

بطاقة الدليل B10 | 28 سبتمبر 2026 | منتدى | الإنشاءات والهندسة

ادعاء غير متحقق منه

الادعاء	وصف منشور في 28 سبتمبر أرشيف مقاول يضم شيفرة ووثائق مشاريع وعقودًا وصور وثائق هوية. ووصف حجمين للأرشيف قبل فك الضغط وبعده، وحُذفا هنا.
التسلسل الزمني	أعلن المنشور التداول وضم ادعاءً منفصلًا باستمرار الوصول. ولم يقدّم دليلًا من جهة الهدف يثبت بداية الوصول أو نهايته.
ما يمكن إثباته	نحتفظ بالوصف والأحجام وادعاء الاستمرارية بوصفها تصريحات الناشر. ولا تتحقق بها محتويات الأرشيف.
البدائل والحدود	قد تُنسخ شيفرة من دون إثبات وصول إلى الإنتاج. وقد تأتي الوثائق من تخزين مشترك أو حادث أقدم. ولم يُثبت أثر في الأنظمة الصناعية.
الاستجابة	على أمن المقاول التحقق من الملكية ومراجعة صلاحيات المستودعات والوثائق. وافحص الاستمرارية عبر بيانات داخلية عند وجود قرائن. ولا يبرر ادعاء علني اختبار أي مسار وصول معروض.

الخلاصة

تحقق من نطاق المستودع والوثائق قبل فحص الاستمرارية المدعاة.

بطاقة الدليل B10 — 28 سبتمبر 2026

ناشر غير مسمى · منتدى · Forum · الإنجليزية

النص الأصلي

Free full leak includes:

الترجمة

يتضمن التسريب الكامل المجاني:

ملاحظة. إعلان أو طلب فقط؛ التاريخ تاريخ المنشور. [S1]

ما يمكن إثباته
وصف أرشيف شيفرة ووثائق لمقاول، مع ادعاء استمرار وصول غير متحقق منه. [S1]

ما لم يثبت
يزعم الناشر أيضًا استمرار الوصول، وهو غير متحقق منه. ولا تثبت أحجام الأرشيف وقائمة المحتويات دخولًا ناجحًا أو وصولًا حاليًا أو أثرًا في الأنظمة الصناعية.

ينتهي كل ملف عند حدود أدلته. وقد يغيّر تطابق داخلي موثوق الاستجابة، لكنه لا يصحّح بأثر رجعي كل تفاصيل رواية البائع.

4.7 النشاط الحديث: 8–22 نوفمبر

يجمع النشاط الحديث أنواع أدلة مختلفة. ولا يحوّلها الجدول إلى مجموع حوادث. فقد يصف إصدار نوفمبر تحذيرًا أو إعلانًا أو مادة أقدم، بدل دخول جديد.

يصف عدد المنشورات الخمسة أدناه والمخطط الشهري للمنتديات المادة الموسومة بالسعودية. وتصف الحالة P أربعة منشورات ضمن المادة المحفوظة الأوسع. ولم يُثبت هنا تداخلها مع المجموعة الموسومة؛ فلا تجمع هذه الأعداد. [S1]

التاريخ	الدليل	التقييم	القرار الفوري
8–22 نوفمبر	5 منشورات منتدى موسومة بالسعودية	تشمل مجموعة بوسم بلد ملتبس ومنشورات خدمات وبرامج غير مرتبطة؛ لم يُثبت حادث سعودي مؤكد جديد	افحص الموضوع والعمر قبل فتح حادث جديد [S1]
9–10 نوفمبر	عرض جلسة مقاول عبر أربعة منشورات منتدى	ملف عرض وصول واحد غير متحقق منه، منفصل عن ادعاء أرشيف أكتوبر	تحقق من الهويات ومسؤوليات بيانات المورّد ذات الصلة [S1]
9 نوفمبر	إدراج N0n لهدف مصنّف تعليميًا	ادعاء إجرامي في Ransompedia	تحقّق من أي علاقة خدمة أو مورّد ذات صلة [S2]
11 نوفمبر	إدراج Thegentlemen لهدف مصنّف صحيًا	ادعاء إجرامي في Ransompedia	قيّم صلة البيانات الحساسة والاستمرارية من دون افتراض التأكيد [S2]
16 نوفمبر	إدراج Aoqin	ادعاء إجرامي؛ يختلف تصنيف الصناعة عن نقل علني	تحقّق من علاقة العمل والبلد [S2]

التاريخ	الدليل	التقييم	القرار الفوري
11–12 نوفمبر	تنبيها CERT لمنتجات Microsoft وGoogle	نصائح تحديث رسمية، لا دليل استغلال سعودي	حدّد مسؤولي الأصول المشمولة واحفظ دليل التحديث [S26] [S27]
20 نوفمبر	تنبيهان حرجان لمنتجات Veeam وGitLab	إدراجات تحذير رسمية	تحقّق من تفاصيل المورّد وانطباق المنتج [S13]
21 نوفمبر	تنبيهان حرجان لمنتجات Palo Alto Networks وCisco	إدراجات تحذير رسمية	راجع أصول الحافة والشبكة المشمولة [S13]

الحالة P

P عرض جلسة لمقاول في نوفمبر

بطاقة الدليل B19 | 9 نوفمبر 2026 | منتدى | الإنشاءات والهندسة

عرض وهمي غير متحقق منه

الادعاء	أعلن بائع جلسة نشطة مرتبطة بمقاول إنشاءات، ووصف مواد عطاءات ومالية وهندسية. ويعود ادعاء حداثة المادة إلى البائع. [S1]
التسلسل الزمني	ظهرت أربعة منشورات منتدى محفوظة في 9 و10 نوفمبر. وتشكل ملف عرض واحدًا، لا أربعة حوادث ثابتة.
ما يمكن إثباته	نحتفظ بالإعلانات وأوصاف نطاقها المتكررة. وادعى البائع قدرة وصول تتجاوز عرض بيانات ثابتة عاديًا.
البدائل والحدود	لم تُختبر جلسة أو بيانات اعتماد أو مادة معروضة. وتبقى قابلية الاستخدام والأصالة والحداثة وأثر الهدف غير متحقق منها. ولا يثبت موضوع الإنشاءات صلة بادعاء أرشيف أكتوبر المنفصل.
الاستجابة	على مسؤولي الهوية والمورّدين المعنيين تقييم نطاق الحساب والجلسات المصرح بها ومسؤوليات مشاركة البيانات عبر سجلات داخلية. وإذا ثبتت مادة مسروقة قابلة للاستخدام أو نشاط غير مصرح به، فاحتوِه فورًا واحفظ قرار الإبلاغ.

الخلاصة

تحقق من الهوية وعلاقة المورّد المعنيتين، من دون اختبار جلسات معروضة.

بطاقة الدليل B19 | 9 نوفمبر 2026

بائع غير مسمى | منتدى | Forum | الإنجليزية

النص الأصلي

including closed technical and financial tender proposals

الترجمة

بما فيها عروض عطاءات فنية ومالية مغلقة

ملاحظة. لم تُختبر الجلسة المدعاة. وهذا منفصل عن ادعاء أرشيف الإنشاءات في أكتوبر.

ما يمكن إثباته

تعلن أربعة منشورات عرض وصول واحدًا لجلسة مقاول، وتصف مواد عطاءات ومالية وهندسية. [S1]

ما لم يثبت

وصول جلسة قابل للاستخدام أو صحة بيانات أو حداثة أو سجلات متمايزة أو تسليم مكتمل أو أثر لدى الهدف.

يأتي مثال الإصدارات التالي من تنبيه PAN-OS الصادر عن المورّد في 11 نوفمبر. ولا ننسبه إلى حادث سعودي. وفُحص سجل NVD وقُرئت الإصدارات المتأثرة والمصلحة في جدول المورّد. [S15][S14]

الثغرة	الفرع المتأثر	الإصدار المصلح	التفسير
CVE-2026-0326	PAN-OS 12.2 قبل 12.2.4-h2	12.2.4-h2 أو أحدث	مشكلة مشروطة في معالجة الخدمات
CVE نفسها	PAN-OS 12.1 قبل 12.1.10-h4	12.1.10-h4 أو أحدث	افحص شروط الإعداد عند المورّد
CVE نفسها	PAN-OS 11.2 قبل 11.2.16-h2	11.2.16-h2 أو أحدث	أكّد الفرع المثبت
CVE نفسها	PAN-OS 11.1 قبل 11.1.16-h5	11.1.16-h5 أو أحدث	تتطلب الإصدارات الأقدم غير المدعومة إصدارًا مدعومًا مصلحًا

يصف المورّد تعطيل معالجة خدمة أو فساد ذاكرة في إعدادات محددة. ويقول التنبيه المقروء إنه لا يعلم باستغلال خبيث. ويذكر أن Panorama وPrisma Access غير متأثرين. ويتبع عملاء Cloud NGFW تعليمات صيانة المورّد. [S14]

قد يبرر تنبيه تحديث إجراءً من دون إثبات هجوم سعودي. أغلق المهمة بأدلة الأصل والإعداد والإصدار المثبت فعليًا. ولا يقدّم التقرير استغلالًا أو قاعدة كشف.

4.8 ما الذي تسنده الحالات وما الذي لا تسنده

تدعم الحالات معًا مسارات تحقيق عملية للبيانات الحساسة والحسابات والمورّدين والخدمات. ولا تثبت قائمة ضحايا وطنية مكتملة أو مشغّلين إجراميين متمايزين أو مجموع خسائر مالية.

قد تبقى الحالة ادعاء غير متحقق منه مع تبرير مراجعة ضابط متناسبة. وينبغي أن يسجّل القرار دليله وحدّه. وعندما يغيّر تطابق داخلي الثقة، احفظ الدليل الجديد بوصفه عبارة منفصلة.

الخلاصات الرئيسية

01

يثبت المنشور التداول قبل أن يثبت أثرًا لدى الهدف.

02

الإدراجات والتحذيرات والإفصاحات الحديثة مجموعات منفصلة.

03

تحقّق من الحساب أو علاقة البيانات أو الخدمة قبل قرار الاحتواء والإبلاغ.

الفصل 05

أمثلة على الاستهداف بحسب القطاع

يجيب هذا الفصل عن

ما الأدلة المهمة لكل مسؤول خدمة، وما أول إجراء؟

10

خلايا قطاعية في القائمة؛ الأمثلة تصف الأدلة ولا تمنح تقييمات خطر قطاعية

5.1 وجّه الأدلة إلى مسؤول الخدمة 41

5.2 الوصول البعيد الطبي عبارة منفصلة 42

5.3 قد تعبر البيانات القطاعات من دون إثبات حادث مشترك 42

5.4 استخدم معيار إغلاق يناسب الادعاء 43

الفصل 05

أمثلة على الاستهداف بحسب القطاع

باختصار

تساعد أسماء القطاعات على توجيه النتيجة إلى مسؤول. ولا تثبت الانتشار ولا تبرر تقييمًا. وتتعلق أبرز الأمثلة بادعاءات شيفرة ووثائق عامة وعروض صحية وبيانات مستثمرين وأرشيف مقاولين وسجلات نقل. وفي هذه الملفات، لا يحمل إفصاحًا رسميًا إلا حادث التطبيق المسمى. طابق الملاحظة ذات الصلة بالبيانات أو الخدمة الفعلية، ثم اتخذ أول إجراء يسنده التطابق.

5.1 وجّه الأدلة إلى مسؤول الخدمة

يعرض الجدول أمثلة والاستجابة الأولى. ولا يعني غياب نتيجة حادث لقطاع أنه لم يتأثر. [S1][S2][S17]

القطاع	المثال الملحوظ	حالة الدليل	الاستجابة الأولى
الإدارة العامة	أوصاف شيفرة واعتماد ووثائق وادعاءات تعطيل	إعلانات وادعاءات من دون تحقق لدى الهدف	التحقق من مصدر الشيفرة أو الوثيقة وحالة الخدمة
المصارف والخدمات المالية	عرض بيانات مستثمرين وطلب حسابات وحملات اعتماد	تصريحات بائعين وتقارير باحثين	ربط الهوية والاستعادة والتحقيق في الدفع
التأمين	عرض خدمة بيانات صحية قد يتصل بسير عمل مترابط	فئات بيانات مدعاة؛ لا أثر عام في شركات التأمين	فحص علاقات مشاركة البيانات قبل تعيين الملكية
الطاقة والمرافق	عروض وثائق مقاولين ونقل ادعاء بيانات طاقة	ادعاءات مورّدين وكمية منقولة	فصل نطاق بيانات الجهة الرئيسية والمورّد
الصناعة والمواد	أوصاف أرشيف مشاريع ومقاولين	الأصالة والأثر التشغيلي غير متحقق منهما	مراجعة صلاحيات الوثائق الهندسية والمستودعات المصرح بها
النقل والخدمات اللوجستية	إفصاح تطبيق مؤكد وعروض بيانات طرود وسائقين	إفصاح شركة واحد وعروض منفصلة غير متحقق منها	تقييم وصول بيانات العملاء ونسخ المورّدين والانتحال
الخدمات الرقمية والاتصالات	طلب حسابات وادعاء تعطيل اتصالات	طلب أو ادعاء؛ لا وصول مؤكد إلى خدمة	التحقق من مسارات الحساب وقياس الإتاحة مستقلًا
الصحة وعلوم الحياة	عروض بيانات صحة وCRM عافية ووصول بعيد طبي	ادعاءات بيانات أو وصول؛ لا بيع مكتمل مثبت	التحقق من نطاق البيانات الحساسة ومراجعة الوصول المميز
التعليم والبحث	ادعاءات تعطيل خدمة تعليمية وإدراجات المصدر	سلاسل ادعاء وملاحظات إدراج	فصل إتاحة الموقع العام عن الوصول إلى بيانات الطلاب والموظفين
الخدمات الاستهلاكية والعقارات والاستثمار	انتحال خدمات وعروض بيانات عملاء	بيانات احتيال رسمية وادعاءات بائعين	ربط بلاغات الدعم بالتحقق الموثوق من الدفع والاستعادة

5.2 الوصول البعيد الطبي عبارة منفصلة

عرض إعلان منتدى في 3 مايو وصولًا بعيدًا نُسب إلى منشأة طبية سعودية. ولم يُتحقق من وصف البائع للحجم والوصول. وهو منفصل عن عرض البيانات الصحية في الحالة F. [S1]

بطاقة الدليل B15 — 3 مايو 2026

ناشر غير مسمى · منتدى · Forum · الإنجليزية

النص الأصلي

Huge medical facility

الترجمة

منشأة طبية كبيرة

ملاحظة. إعلان أو طلب أو نقل فقط.

ما يمكن إثباته
أعلن بائع وصولًا بعيدًا منسوبًا إلى منشأة طبية؛ لم يُتحقق من وصول حالي أو صفقة. [S1]

ما لم يثبت
القدرة أو التسليم أو الصفقات المكتملة أو الوصول الحالي أو الأثر لدى الجهة المعنية.

والفرق مهم. فادعاء البيانات يستدعي تقييم المصدر والإفصاح. ويستدعي إعلان الوصول أيضًا فحص الهوية والخدمة البعيدة عند وجود تطابق موثوق. ولا يثبت أي منهما وحده حدثًا يخص سلامة المرضى أو تعطيلًا تشغيليًا.

5.3 قد تعبر البيانات القطاعات من دون إثبات حادث مشترك

قد يضم أرشيف مقاول وثائق تخص الطاقة أو النقل. وقد تصل خدمة بيانات عملاء بين جهة صحية ومسار مالي. ولا يثبت ورود أسماء قطاعات متعددة الوصول إلى نظام كل مؤسسة.

ينبغي أن يقود مسؤول العقد أو تدفق البيانات فحص النطاق الأول. وبعده تحدد فرق الأمن الأنظمة والصلاحيات والسجلات التي تحتاج تحقيقًا. ويمنع ذلك نسبة حادث واسع إلى كل علامة يذكرها إعلان.

5.4 استخدم معيار إغلاق يناسب الادعاء

النتيجة	دليل الإغلاق	ما لا يغلقها
بيانات قديمة يعاد إعلانها	عمر متحقق منه ونطاق متأثر ومعالجة سابقة	قول البائع إنها حديثة
وصف شيفرة أو بيانات اعتماد	تقييم داخلي للمصدر وقرار الانكشاف	سمعة المنتدى أو شكوى مزعومة
حزمة وثائق مورّد	نطاق مشاركة مؤكد ورد المورّد	استمرار خدمة الجهة الرئيسية العامة
عرض وصول بعيد	تقييم الهوية والخدمة ومراجعة السجلات المعنية	غياب بيان اختراق علني مطابق
ادعاء تعطيل	حالة خدمة مقيسة مستقلًا ووظائف متأثرة	قول الناشر إن الهجوم انتهى

هذه نتائج تحقيق، وليست طلبًا لاختبار وصول خارجي أو شراء مادة معروضة. ويمكن تقييم كل حالة عبر سجلات داخلية مشروعة وقنوات مورّدين معتمدة.

الخلاصات الرئيسية

01
وجّه كل ملاحظة إلى مسؤول بيانات أو خدمة أو مورّد.

02
لا يثبت إعلان متعدد القطاعات دخولًا متعدد القطاعات.

03
احسم التقييم بدليل مناسب، لا بتأكيد البائع.

الفصل 06

نشاط ناشطي القرصنة وادعاءات التعطيل وحالة الخدمة

يجيب هذا الفصل عن

كيف يستجيب المدافع عندما تسبق الادعاءات العلنية الأثر المتحقق منه؟

17

منشورًا محفوظًا ضمن تسع سلاسل ادعاء من هوية نشر واحدة

6.1 تسلسل زمني يفصل أنواع الأدلة 45

6.2 تحتاج ادعاءات DDoS المنقولة إلى رواية خدمة مستقلة 46

6.3 سلاسل ادعاء متكررة في المنشورات المحفوظة 46

6.4 الادعاء مقابل الرواية المتحقق منها 49

6.5 ينبغي أن تتشارك العمليات والاتصال سجل حقائق واحدًا 49

6.6 جهّز بيانًا أوليًا قابلًا للاستخدام 49

الفصل 06

نشاط ناشطي القرصنة وادعاءات التعطيل وحالة الخدمة

باختصار

قد تخلق ادعاءات التعطيل ضغطًا قبل إثبات الأثر لدى المؤسسة. ونقلت Unit 42 مثالين سعوديين يخصان موقع خدمة مالية وخدمة حكومية. ولا تقدّم رواية المصدر مدة انقطاع مقيسة بصورة مستقلة لهذين المثالين. اعتبر الادعاء إشارة للتحقق من الإتاحة والمصادقة والوصول إلى البيانات كلًا على حدة. جهّز اتصالات التخفيف لدى المزوّد ومسارًا للرسائل الوقائعية، ثم اختبرهما مع العمليات.

6.1 تسلسل زمني يفصل أنواع الأدلة

يفصل التسلسل البحث المنشور والبيانات الرسمية وملاحظات الإدراج من بياناتنا. وليس تسلسلًا لاختراقات مؤكدة. والتواريخ تواريخ نشر أو إدراج، إلا عندما يصرّح البند بغير ذلك.

31 مارس 2026	**Check Point Research**	يفيد بثلاث موجات رش كلمات مرور في مارس مع استهداف سعودي محدود [S12]
16 أبريل 2026	**بيان شرطة**	يفيد بإجراء بشأن إعلانات خدمات وهمية، من دون ادعاء دخول إلى أنظمة [S20]
9 يونيو 2026	**إفصاح الشركة**	يؤكد وصولًا محدودًا إلى بيانات عملاء التطبيق؛ وحدود الأثر تصريحات الشركة [S17]
6 أكتوبر 2026	**The National**	تنقل ادعاء بيانات غير متحقق منه في قطاع الإنشاءات [S19]
9 نوفمبر 2026	**ملاحظة Ransompedia**	يظهر إدراج تعليمي موسوم بالسعودية؛ لم يُثبت تأكيد رسمي [S2]
11 نوفمبر 2026	**ملاحظة Ransompedia**	يظهر إدراج صحي موسوم بالسعودية؛ لم يُثبت تأكيد رسمي [S2]
12 نوفمبر 2026	**Saudi CERT**	ينشر تنبيه تحديث أمني لمنتجات Google [S27]
16 نوفمبر 2026	**ملاحظة Ransompedia**	يظهر ثالث إدراج حديث موسوم بالسعودية؛ يحتاج تصنيف القطاع إلى حذر [S2]
20 نوفمبر 2026	**Saudi CERT**	يدرج تنبيهين حرجين لمنتجات Veeam وGitLab [S13]
21 نوفمبر 2026	**Saudi CERT**	يدرج تنبيهين حرجين لمنتجات Palo Alto Networks وCisco [S13]

6.2 تحتاج ادعاءات DDoS المنقولة إلى رواية خدمة مستقلة

نقل موجز Unit 42 الإقليمي ادعاء Sylhet Gang بشأن أنظمة حكومية، وادعاء DieNet بشأن موقع بنك سعودي. ونستخدم فئات أهداف عامة لأن التأكيد الرسمي لهذين الادعاءين لم يُثبت. [S11]

هذه ادعاءات تخص أهدافًا، وليست دليلًا على نشاط ناجح. وفي مثال مطار منفصل في الموجز تناقض جغرافي، لذلك لا نستخدمه دليلًا سعوديًا. ولا نستخلص منه استنتاجًا جغرافيًا أو سياسيًا.

قد تساعد صورة شاشة أو ملاحظة إتاحة عن بُعد المحلل على تحديد موضع التحقيق. لكنها لا تثبت تجربة المستخدم أو سبب الانقطاع أو الوصول إلى بيانات محمية. فقد يتاح الموقع من شبكة ويتعذر من أخرى. ويجب أن تحدد العمليات الوظائف المتأثرة من بياناتها.

6.3 سلاسل ادعاء متكررة في المنشورات المحفوظة

تتضمن المادة المحفوظة 17 منشورًا من هوية النشر Team 313، ضمن تسع سلاسل ادعاء. وتخص خدمات عامة وخدمات مالية وتعليمًا وتطبيقًا للموظفين وخدمة اتصالات. وهذه سلاسل ادعاء، وليست تسعة انقطاعات مؤكدة. [S1]

تواريخ المنشورات	الهدف العام	نوع العبارة الملحوظة	حد الأثر
24 مارس	خدمة عامة للجمهور	ادعاء تعطيل ومدة مقصودة	المدة غير مقيسة
25 مارس	خدمات للقطاع العام	منشورا قوائم أهداف	لا تثبت القوائم الأثر
6–8 أغسطس	تطبيقات عامة للجمهور	ادعاء ومنشورات متابعة	الوصول الداخلي غير متحقق منه
11–12 سبتمبر	خدمات عامة للجمهور	ادعاء تعطيل خوادم داخلية	لا نحتفظ بتأكيد من الجهة المعنية
13 سبتمبر	خدمة مالية	ادعاء ومتابعة	أثر العملاء غير مقيس
14 سبتمبر	خدمة مالية أخرى	ادعاء ومتابعة	أثر العملاء غير مقيس
18 سبتمبر	خدمة تعليمية	ادعاء وتحديثات	أثر الخدمة والبيانات غير متحقق منه
19 سبتمبر	تطبيق للموظفين	إعلان تعطيل ومدة مقصودة	لا انقطاع متحقق منه لخدمة الموظفين
2 أكتوبر	خدمة اتصالات	إعلان تعطيل ومدة مقصودة	لا أثر متحقق منه على الشبكة كلها

لغة المتابعة جزء من سجل الادعاء. ولا تمثل إعادة زعم التأثير في أنظمة داخلية دليلًا مستقلًا على الوصول إليها. ولا يجوز جمع المدد المقصودة للهجوم بوصفها مجموع وقت انقطاع.

بطاقة الدليل B11 — 24 مارس 2026

Team 313 قناة مراسلة Telegram الإنجليزية

النص الأصلي

The attack will last for two hours.

الترجمة

سيستمر الهجوم ساعتين.

ملاحظة. المدة المدعاة ليست وقت انقطاع مقيسًا.

ما يمكن إثباته
منشور ادعاء أو تحديث من هوية النشر نفسها. [S1]

ما لم يثبت
مدة انقطاع فعلية أو وصول داخلي أو سرقة بيانات.

بطاقة الدليل B12 — 6 أغسطس 2026

Team 313 قناة مراسلة Telegram العربية

النص الأصلي

سيستمر الهجوم لمدة 6 ساعات.

ملاحظة. المدة المدعاة ليست وقت انقطاع مقيسًا.

ما يمكن إثباته
منشور ادعاء أو تحديث من هوية النشر نفسها. [S1]

ما لم يثبت
مدة انقطاع فعلية أو وصول داخلي أو سرقة بيانات.

بطاقة الدليل B13 — 11 سبتمبر 2026

Team 313 قناة مراسلة Telegram الإنجليزية

النص الأصلي

The attack resulted in the disruption of internal servers

الترجمة

أدى الهجوم إلى تعطيل خوادم داخلية.

ملاحظة. المدة المدعاة ليست وقت انقطاع مقيسًا.

ما يمكن إثباته
منشور ادعاء أو تحديث من هوية النشر نفسها. [S1]

ما لم يثبت
مدة انقطاع فعلية أو وصول داخلي أو سرقة بيانات.

بطاقة الدليل B14 — 2 أكتوبر 2026

Team 313 قناة مراسلة Telegram العربية

النص الأصلي

سيستمر الهجوم لمدة 24 ساعة.

ملاحظة. المدة المدعاة ليست وقت انقطاع مقيسًا.

ما يمكن إثباته
منشور ادعاء أو تحديث من هوية النشر نفسها. [S1]

ما لم يثبت
مدة انقطاع فعلية أو وصول داخلي أو سرقة بيانات.

الحالة O

O

سرد متكرر لحملة تعطيل (B11, B12, B13, B14)

خدمات عامة وتجارية

سلاسل ادعاء - أثر غير متحقق منه

الادعاء

كررت هوية النشر Team 313 ادعاءات تعطيل خدمات ووصفت مددًا مخططًا لها. وزعمت إحدى السلاسل أثرًا في خوادم داخلية من دون دليل من بيئة الهدف.

التسلسل الزمني

تمتد السلاسل المحفوظة من مارس إلى أكتوبر. والتحديثات داخل السلسلة متابعات لسياق الادعاء نفسه، وليست تأكيدات مستقلة من الجهة المعنية.

ما يمكن إثباته	نلاحظ المنشورات واستمرار هوية النشر. وهي تثبت سرد ادعاءات علنيًا متكررًا عبر فئات خدمات عدة.
البدائل والحدود	قد تتعذر صفحة عامة من دون وصول إلى أنظمة داخلية. وقد تؤثر الصيانة أو التصفية أو الحركة المشروعة في الرؤية. ولا يحسم التقرير ما إذا سبب أي ادعاء انقطاعًا متحققًا منه.
الاستجابة	اربط بيانات مزوّد الحافة والخدمة والمصادقة. وأكّد الوظيفة المتأثرة والمدة بصورة مستقلة. وإذا تعلقت الأدلة ببيانات أو حسابات محمية، فافحص تلك المسألة منفصلة عن الإتاحة.

الخلاصة

افصل مدة الهجوم التي يذكرها الناشر عن أثر الخدمة المقيس بصورة مستقلة.

وينطبق الفصل نفسه على نقل DieNet في مطلع مارس وادعاء خدمة دفع نُسب إلى Keymous Plus في التقارير المحفوظة. وهما يثبتان تداول الادعاءات، لا مشغّلًا مشتركًا ولا أثر عملاء متحققًا منه. [S1]

سردت منشورات باسم ServerKillers في 12 سبتمبر وباسم DARKSTORM في 26 أكتوبر أهداف مواقع عامة أيضًا. ولا نحتفظ بأثر مقيس مستقلًا لهذين المثالين. ولا تثبت مواقع عدة في قائمة انقطاعات متحققة متعددة. [S1]

ونسب نقل عربي منفصل إلى Handala ادعاء بيانات في قطاع الطاقة. وهذا ادعاء منقول. ولا تثبت أصالة البيانات أو التشفير أو أثرًا في التقنية التشغيلية أو تأكيد الجهة المعنية. [S1]

بطاقة الدليل B18 — 4 مارس 2026

ناشر غير مسمى | قناة مراسلة | Telegram | العربية

النص الأصلي

حوالي [quantity removed]

ملاحظة. إعلان أو طلب أو نقل فقط.

ما يمكن إثباته

نقل إخباري عربي لادعاء Handala بشأن بيانات طاقة. [S1]

ما لم يثبت

القدرة أو التسليم أو الصفقات المكتملة أو الوصول الحالي أو الأثر لدى الجهة المعنية.

6.4 الادعاء مقابل الرواية المتحقق منها

النقطة	الادعاء أو التقرير	الرواية الرسمية المتاحة	الحد المستقل
تعطيل خدمة حكومية	ادعاء نقلته Unit 42	لا نحتفظ بتأكيد حادث لهذا المثال	لا استنتاج عن أثر خدمة مقيس [S11]
تعطيل موقع مالي	ادعاء DieNet نقلته Unit 42	لا نحتفظ بتأكيد حادث لهذا المثال	لا استنتاج عن مدة انقطاع أو أثر معاملات [S11]
بيانات الإنشاءات	مزاعم WallStreet نقلتها الصحيفة عن جهة رصد	لا تأكيد جوهري في الرواية المقروءة	تبقى الكميات المدعاة غير متحقق منها [S19]
بيانات عملاء التطبيق	أفصحت الشركة عن وصول غير مصرح به	أكدت الشركة حادث بيانات عملاء محدودًا	حدود البيانات المالية والاستمرارية تصريحات الشركة [S18][S17]

تجيب الأعمدة عن أسئلة مختلفة. ولا يثبت غياب تأكيد متاح أن الادعاء كاذب. ولا يثبت بيان رسمي عن استمرار الخدمة وحده عدم تأثر السرية.

6.5 ينبغي أن تتشارك العمليات والاتصال سجل حقائق واحدًا

يحتاج فريق الحادث إلى سجل حالة خدمة يضم الوقت والوظيفة المتأثرة والبيانات الداعمة وما لم يُحسم. ويجب أن يستخدم الاتصال المؤسسي هذا السجل. ولا ينبغي تقدير حجم بيانات مسروقة من عنوان الجهة المدعية، أو استنتاج خسائر العملاء من حجم الحركة.

عند التحقق من حدث إتاحة، فعّل التواصل مع مزوّد التخفيف ومسؤول الخدمة. واحفظ خط الأساس الطبيعي ليظل ارتفاع الطلب المشروع أو الصيانة تفسيرًا بديلًا قابلًا للاختبار. ولا تؤخر التعافي أثناء تحديد كاتب المنشور.

وعندما تشير الأدلة إلى وصول إلى بيانات، افتح تحقيقًا منفصلًا. فنجاح تخفيف DDoS لا يغلق حادث سرية. وبالمثل، لا يثبت ادعاء بيع بيانات ضرورة إعلان انقطاع.

6.6 جهّز بيانًا أوليًا قابلًا للاستخدام

ينبغي أن يحدّد البيان الخدمة قيد التقييم بلغة يفهمها العملاء، ويصف الأثر المتحقق منه، ويحدّد موعد التحديث التالي. ويجب تجنّب الإسناد حتى تسنده أدلة ويُعتمد. وتظل متطلبات التنسيق القطاعية منطبقة (§10).

ويمكن لتمرين اختبار ما إذا كان الدعم والأمن والعمليات والاتصال ينتجون رواية واحدة. ومعيار الإنجاز بيان متسق تسنده بيانات الخدمة ومسار تصعيد قابل للتنفيذ. وليس الاتفاق على السرد السياسي للجهة المدعية.

الخلاصات الرئيسية

01

تعامل مع منشورات التعطيل كادعاءات حتى تثبت بيانات الخدمة الأثر.

02

تحتاج الإتاحة والوصول إلى البيانات والإسناد إلى نتائج منفصلة.

03

اختبر اتصالات التخفيف والرسائل الوقائعية مع العمليات.

الفصل 07

الجهات الفاعلة والادعاءات وإدراجات الفدية

يجيب هذا الفصل عن

ما الهويات التي تظهر في الأدلة، وما العلاقات التي يمكن إسنادها؟

30

إدراجًا موسومًا بالسعودية في فترة التقرير

7.1 افصل الهوية عن المشغّل 52

7.2 أبحاث حملات بإسناد إلى المصدر 53

7.3 هويات النشر وادعاءات ناشطي القرصنة 54

7.4 المقارنة الإقليمية للفدية 56

7.5 هويات الإدراج وتركّزها 56

7.6 استخدم أدلة الابتزاز لقرارات الاستمرارية 58

الفصل 07

الجهات الفاعلة والادعاءات وإدراجات الفدية

باختصار

يسجل Ransompedia عدد 30 إدراجًا موسومًا بالسعودية خلال الفترة. وللمقارنة، لدى الإمارات 84 وقطر 9 والكويت 7 وعُمان 9. وهذه ملاحظات لادعاءات إجرامية في المصدر، وليست معدلات حوادث مؤكدة. وتعرّف أسماء الجهات هويات نشر أو إدراج، ولا تحدد المشغّلين وحدها. أبقِ إسناد الباحث مرتبطًا بمصدره، واستخدم كل إدراج لاختبار خطط الاستمرارية والاستجابة للهوية ذات الصلة.

اختيرت دول المقارنة كأمثلة لتوفير السياق فقط؛ ولا ينطوي اختيارها على أي ترتيب أو تقييم سياسي.

7.1 افصل الهوية عن المشغّل

حساب المنتدى واسم موقع تسريب الفدية واسم الحملة كيانات من أنواع مختلفة. ويدعم تكرار اسم مستعار ارتباطًا في النشر. لكنه لا يثبت أن الشخص نفسه يدير كل حساب أو أن بائعًا شغّل حملة دخول وصفها باحثون.

تسمّي خريطة العلاقات التالية صلات المصادر وروابط التخطيط. وتعرض الخريطة علاقات المصادر. وروابط التخطيط التي يناقشها النص نموذج تحليلي، من دون ادعاء مشغّلين مشتركين.



تمثل صلة Ransompedia بملاحظات الإدراج بيانات Brandefense الخاصة. وليست تأكيدًا علنيًا مستقلًا لكل حادث. وتمثل صلة الناشر البحثي بالحملة تقرير ذلك الناشر. [S1][S2][S11][S12]

7.2 أبحاث حملات بإسناد إلى المصدر

حملة غير مسماة لرش كلمات مرور سحابية

يتبع وصف الحملة رواية المصدر

حملة اعتماد أبلغ عنها باحثون | قدّرت Check Point منشأها بإيران بثقة متوسطة

في السعودية، 2026

3, 13, 23 مارس
موجات الحملة؛ استهداف سعودي محدود

31 مارس
نشر البحث

الأهداف المُدّعاة

أهداف سعودية محدودة؛ لا عدد سعودي لعمليات ناجحة

في التقارير العامة

Check Point [S12]: ثلاث موجات واستهداف سعودي محدود وتقدير منشأ بثقة متوسطة

تقييمنا

يثبت المصدر نشاط حملة ضد بعض الأهداف السعودية. ولا يثبت وصولًا ناجحًا لدى كل هدف.

درجة الثقة
استهداف رصده الباحث؛ النتائج السعودية غير محسومة

قدّرت Check Point بثقة متوسطة أن منشأ جهة رش كلمات المرور على Microsoft 365 هو إيران. وهذا الإسناد يخص Check Point. وتصف روايتها استهدافًا سعوديًا محدودًا، ولا تثبت مجموعًا سعوديًا لعمليات وصول ناجحة. [S12]

يضع تقرير Microsoft Digital Defense Report لعام 2026 السعودية عند 2% من إشعارات الأنشطة المرتبطة بإيران بين يوليو 2025 ويونيو 2026. ويشير التقرير أيضًا إلى أن الجهات المرتبطة بدول تجمع بين التجسس طويل الأمد والتموضع المسبق واحتمال التعطيل. وتعكس حصة 2% إشعارات المورّد لعملاء Microsoft لا معدل هجمات وطنيًا، وتبقى منفصلة عن ادعاءات ناشطي القرصنة في الفصل 6. [S33]

ومطابقة التقنية نموذج تحليلي للسلوك الذي وصفه المصدر. ولا تحدّد جهة فاعلة ولا تثبت نجاح كل خطوة لدى مؤسسة سعودية.

التقنيات المذكورة في أبحاث الشركات الأمنية، بحسب التكتيك

الوصول إلى بيانات الاعتماد
T1110.003 رش كلمات المرور: سلوك وصفه المصدر، نموذج تحليلي

نموذج تحليلي من Odin by Brandefense لسلوك وصفته Check Point [S12]، راجعناه مقابل MITRE ATT&CK [S30] في 22 نوفمبر 2026؛ وليس إسنادًا أو سلسلة دخول كاملة مؤكدة. [S12]

التكتيك	التقنية	الدليل	السؤال الدفاعي
الوصول إلى بيانات الاعتماد	T1110.003، رش كلمات المرور	تصف Check Point محاولات عبر حسابات كثيرة بكلمات مرور ضعيفة؛ وتعرّف MITRE التقنية	أي الحسابات المستهدفة تُظهر جلسات ناجحة مريبة أو نشاطًا لاحقًا؟

يسند وصف MITRE ورواية المصدر هذه المطابقة السلوكية. ولا يضيف التقرير سلسلة دخول مكتملة أو قاعدة كشف قابلة للنشر مباشرة. [S30][S12]

7.3 هويات النشر وادعاءات ناشطي القرصنة

Team 313

هوية نشر فقط

جهة تدعي التعطيل | لا يستنتج التقرير ارتباطًا بدولة

في السعودية، 2026

مارس
سلاسل ادعاء تخص خدمات عامة

أغسطس
ادعاءات تطبيقات وتحديثات

سبتمبر
ادعاءات لخدمات عامة ومالية وتعليمية وتطبيق موظفين

أكتوبر
ادعاء يخص خدمة اتصالات

الأهداف المُدّعاة

فئات واسعة لخدمات عامة وتجارية

بكلماتهم

“سيستمر الهجوم لمدة 6 ساعات.” B12

في التقارير العامة

17 منشورًا محفوظًا في تسع سلاسل ادعاء؛ الأثر غير متحقق منه [S1]

تقييمنا

تدعم الادعاءات والتحديثات المتكررة ارتباط نشر. ولا تثبت انقطاعًا مقيسًا أو وصولًا داخليًا أو تحكمًا مشتركًا مع هويات أخرى.

درجة الثقة
مرتفعة في رصد النشر؛ أثر الجهة المعنية غير متحقق منه

بائعون ومشترون منفصلون في المنتديات

نموذج تحليلي لفئات الأدلة

إعلانات وطلبات مستقلة | لا تثبت مؤسسة أو مشغّل مشترك

في السعودية، 2026

يناير–سبتمبر
إعلانات بيانات ووثائق وحسابات

فبراير
طلب حسابات وعروض بيانات عملاء

الأهداف المُدّعاة

الإدارة العامة والصحة والمال والنقل والمورّدون

بكلماتهم

“Looking to buy any saudi-arabia related accounts” B03

في التقارير العامة

إعلانات منتديات محفوظة؛ لا صفقة أو تأكيد من الجهة المعنية [S1]

تقييمنا

هذه هويات نشر وأوصاف منتجات منفصلة. وينظم الجمع مهام المدافع ولا يصف مؤسسة إجرامية واحدة.

درجة الثقة
مرتفعة في رصد العروض والطلب؛ القدرات المعلنة غير متحقق منها

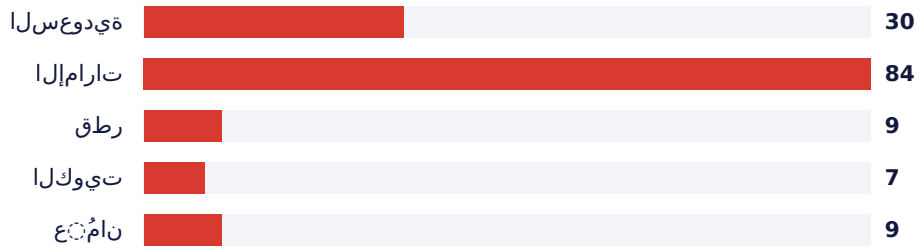
تساعد هويات النشر المحللين على التعرف إلى إعادة الادعاءات والعروض اللاحقة. ولا ينبغي أن تصبح سببًا لتبنّي ادعاءات الأثر أو الانتماء السياسي. ويختبر الفصل 6 ادعاءات التعطيل مقابل سؤال مستقل عن حالة الخدمة.

لا تربط أدلة بنية تحتية أو تشغيلية ملموسة هنا بائعي المنتديات وحملة رش كلمات المرور وهويات الفدية. ولا يقدّمها التقرير بوصفها مؤسسة واحدة.

7.4 المقارنة الإقليمية للفدية

تستخدم المقارنة المصدر نفسه والفترة الزمنية نفسها للدول الخمس. وتقارن ملاحظات إدراج. ولا تعدّل بحسب السكان أو عدد المؤسسات أو ممارسات الإفصاح أو مدى رؤية المصدر. [S2]

تقع الإدراجات الموسومة بالسعودية دون الإمارات وفوق دول الخليج الثلاث الأخرى للمقارنة



إدراجات المصدر نفسه والفترة نفسها؛ دون تعديل بحسب السكان أو ظهور الحالات في المصدر، وليست ترتيبًا للخطر الوطني. المصدر: Brandefense Ransompedia، 1 يناير-22 نوفمبر 2026؛ نوفمبر جزئي [S2]. الإدراجات ملاحظات مصدر وليست حوادث مؤكدة.

الدولة	الإدراجات	التفسير
السعودية	30	إدراجات موسومة بالسعودية
الإمارات العربية المتحدة	84	المصدر والفترة نفسيهما
قطر	9	المصدر والفترة نفسيهما
الكويت	7	المصدر والفترة نفسيهما
عُمان	9	المصدر والفترة نفسيهما

توفّر الدول الأربع سياقًا تشغيليًا إقليميًا. وتشمل الطاقة والمال والنقل والخدمات الرقمية، مع مجموعات مؤسسات مختلفة. ولا يثبت العدد الأعلى احتمالًا أعلى للهجوم.

7.5 هويات الإدراج وتركّزها

تستخدم الإدراجات السعودية المحفوظة 18 اسم مجموعة مختلفًا. وأكثرها Thegentlemen بعدد 8 من 30 إدراجًا (26.7%). ولدى N0n عدد 3؛ ولدى كل من Hyflock وAPT73 وINC Ransom عدد 2. وتظهر بقية الأسماء مرة واحدة. وهذه تكرارات أسماء، لا أعداد مشغّلين مستقلين. [S2]

عرض إدراجات Ransompedia

هويات منفصلة لمواقع تسريب

ملاحظات إدراج من بياناتنا | لا يستنتج مشغّل مشترك

في السعودية، 2026

يناير–نوفمبر
30 إدراجًا موسومًا بالسعودية

8–22 نوفمبر
3 إدراجات حديثة

الأهداف المُدّعاة

قطاعات كما يسميها المصدر؛ يتطلب البلد وهوية الكيان حذرًا

في التقارير العامة

30 إدراجًا، منها 8 باسم Thegentlemen [S2]؛ وهي ادعاءات إجرامية

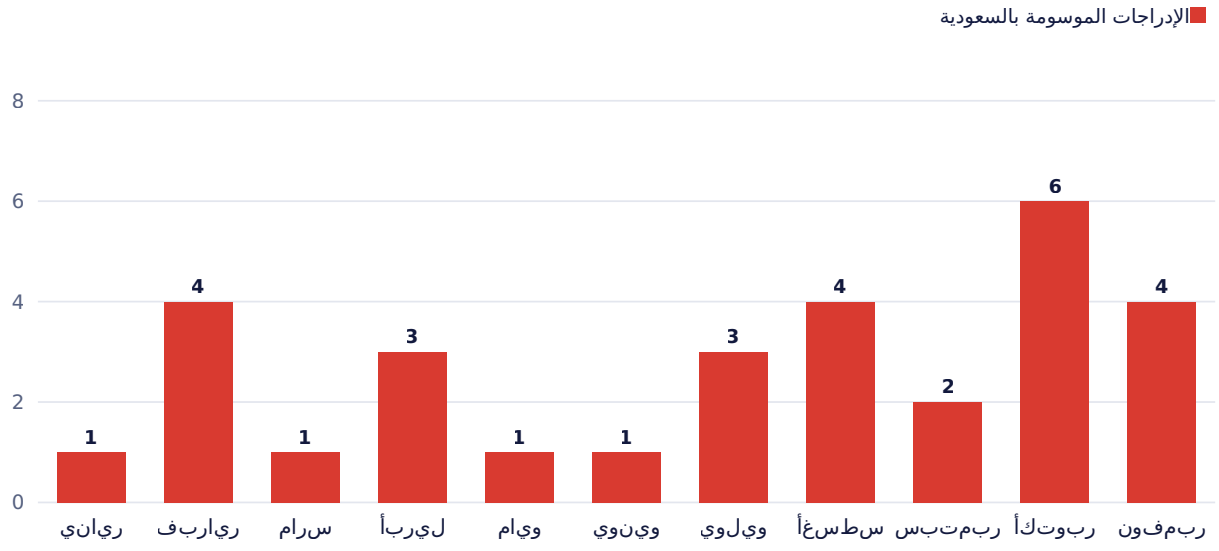
تقييمنا

يدعم تكرار الإدراج مراجعة استمرارية محددة النطاق. ولا يثبت دخولًا أو تشفيرًا أو خسارة مالية أو أعداد مشغّلين مستقلين.

درجة الثقة
مرتفعة في السجلات المحفوظة؛ نتائج الجهة المعنية غير متحقق منها

يتضمن التوزيع الزمني 6 إدراجات في أكتوبر و4 في نوفمبر حتى القطع. وتقع ثلاثة من إدراجات نوفمبر ضمن 8–22 نوفمبر. ولا يستنتج التقرير معدل نمو من شهر جارٍ غير مكتمل.

تظهر إدراجات عبر الفترة، مع ستة في أكتوبر



المصدر: Brandefense Ransompedia، 1 يناير–22 نوفمبر 2026؛ نوفمبر جزئي [S2]. الإدراجات ملاحظات مصدر وليست حوادث مؤكدة.

حقول القطاعات في المصدر تسميات وصفية مرفقة بالإدراجات. ويحتاج بعضها إلى تحقق، خصوصًا عندما تُصنّف شركة تجارة أو خدمات في صناعة أخرى. ويحتاج اسم النطاق أيضًا إلى تحقق جغرافي قبل تحويله إلى ادعاء عن كيان قانوني سعودي.

وتحمل الإدراجات 29 اسم هدف مختلفًا. وهذا ليس عددًا متحققًا منه لمؤسسات سعودية مستقلة. فقد تؤثر العلامات المرتبطة والضحايا المتكررون والمورّدون وأخطاء البلد في التفسير. ولذلك يبقي التقرير الإدراج وحدة أساسية.

7.6 استخدم أدلة الابتزاز لقرارات الاستمرارية

ينبغي أن يطلق الإدراج ذو الصلة تقييمًا محدد النطاق: هل تتصل فئات البيانات أو الخدمات بالمؤسسة، وهل توجد قرائن داخلية أو لدى مورّد؟ وعلى العمليات التحقق من حالة الخدمة. وتفحص فرق الهوية مواد المصادقة القابلة للاستخدام عند وجود مؤشر. وتقيّم الخصوصية نطاق البيانات الشخصية.

وتستحق النسخ الاحتياطية اختبار جاهزية منفصلًا. فلا يثبت عرض بيانات تشفير الأنظمة، ولا تثبت استعادة ناجحة عدم الإفصاح عن بيانات. ويحفظ سجل حادث مفيد هذين الاستنتاجين منفصلين.

الخلاصات الرئيسية

01

لا تحدد أسماء النشر والإدراج مشغّلين مستقلين.

02

تقيس المقارنة الخليجية إدراجات المصدر، مع مجموعات دول مختلفة.

03

تحقّق من العلاقة المتأثرة واختبر التعافي من دون اعتبار الادعاء أثرًا مؤكدًا.

الفصل 08

اقتصاد الاحتيال الظاهر في الأدلة

يجيب هذا الفصل عن

ماذا تعني طلبات الحسابات وعروض بيانات العملاء وبيانات الاحتيال الرسمية للمدافع؟

2

مثالان لسعر مطلوب، من دون دليل على بيع مكتمل

8.1 يظهر الطلب قبل إثبات العرض المتاح 60

8.2 قد تدعم بيانات العملاء فرضية احتيال 61

8.3 بيانات البطاقات في المنشورات: رؤية ضيقة 61

8.4 لا تقيس الأسعار المطلوبة قيمة السوق 61

8.5 تصف البيانات الرسمية مسار احتيال موسمي 62

8.6 أبقِ سلسلة الاحتيال نموذج تخطيط 62

الفصل 08

اقتصاد الاحتيال الظاهر في الأدلة

باختصار

تظهر الأدلة طلبًا لحسابات مرتبطة بالسعودية وإعلانات لبيانات عملاء واستثمار ونقل وموّردين. وتشمل أيضًا بيانات رسمية عن خدمات موسمية وهمية. وهذه ملاحظات منفصلة تختلف صلتها بالضرر المالي. فالسعر مطلوب، والطلب رغبة شراء، ووصف البيانات ادعاء. اربط الدعم ومكافحة الاحتيال والهوية حول رحلة العميل، وتحقّق من أي حساب أو معاملة متأثرة.

8.1 يظهر الطلب قبل إثبات العرض المتاح

طلب المشتري في الحالة G حسابات جاهزة ومفحوصة لخدمات سعودية. وهذا يثبت طلب قدرة حساب. ولا يثبت توفرها أو صاحب الحساب أو صفقة مكتملة. [S1]

ويؤثر التمييز في الاستجابة. فقد يبرر منشور الطلب مراجعة الاستعادة ووصول الموّردين، لكنه لا يحدد حسابًا لتعطيله. وتحتاج الفرق تطابقًا بهوية فعلية أو نشاط إساءة موثوقًا قبل احتواء موجّه.

وقد تجمع أوصاف البائعين منتجات عدة: وصولًا إلى حسابات ومعلومات هوية وقوائم اتصال وأرشيف وثائق. ولا يعامل التقرير كل عنصر بوصفه وصولًا صالحًا للاستخدام. فالحدث الملحوظ هو العرض نفسه.

يكمل طلب الحالة G إعلان خدمة بالروسية يعرض توفير حسابات وسيطة في السعودية وأسواق أخرى. وطلب منشور عربي أيضًا حسابًا لاستقبال مدفوعات واقترح عمولة. ولا يثبت أيهما صفقة مكتملة أو وصولًا إلى نظام بنك. [S1]

بطاقة الدليل B16 — 18 يوليو 2026

FandyUAE · منتدى · Forum · الروسية

النص الأصلي

Есть много дропов по ОАЭ, Сауди и другим арабским странам.

الترجمة

يتوفر كثير من الحسابات الوسيطة (drops) في الإمارات والسعودية ودول عربية أخرى.

ملاحظة. إعلان أو طلب أو نقل فقط.

ما يمكن إثباته
إعلان خدمة متعدد الدول يعرض توفير حسابات وسيطة. [S1]

ما لم يثبت
القدرة أو التسليم أو الصفقات المكتملة أو الوصول الحالي أو الأثر لدى الجهة المعنية.

بطاقة الدليل B17 — 3 أبريل 2026

ناشر غير مسمى · قناة مراسلة · Telegram · العربية

النص الأصلي

رجاء يكون شخص مستقبل و عنده توثيق و سمعة

ملاحظة. إعلان أو طلب أو نقل فقط.

ما يمكن إثباته
طلب حساب لاستقبال مدفوعات؛ لم يُثبت التنفيذ. [S1]

ما لم يثبت
القدرة أو التسليم أو الصفقات المكتملة أو الوصول الحالي أو الأثر لدى الجهة المعنية.

8.2 قد تدعم بيانات العملاء فرضية احتيال

تصف ملفات الاستثمار والعافية والطرود فئات حقول مختلفة. وإذا كانت المادة أصلية وحديثة، فقد تساعد محتالًا على تخصيص رسالة أو انتحال خدمة. وهذا نموذج تحليلي مشروط، وليس دليلًا على أن الإعلانات سببت خسارة احتيال بعينها. [S1]

وقد يحتفظ فريق الدعم بأول دليل مفيد. فقد يصف العميل مكالمة استعادة أو طلب دفع غير متوقع أو تغيير بيانات اتصال. وينبغي أن يحفظ سجل الدعم الرسالة بأمان ويرتبط بحالة الهوية أو الاحتيال عند الحاجة.

لا تطلب من العملاء إرسال بيانات اعتماد أو تفاصيل بطاقات عبر رسائل دعم عادية. وفّر مسار خدمة موثوقًا واستخدم مراجع معاملات داخلية. وتحذف بطاقات الأدلة العامة البيانات الشخصية ومعرّفات الشحن عمدًا.

8.3 بيانات البطاقات في المنشورات: رؤية ضيقة

نطاق أرقام البطاقات

لا تثبت ملاحظات بطاقات الدفع المحدودة هذه صلاحية حالية أو احتيالًا مكتملًا أو اختراق أنظمة الجهات المصدرة أو خسائر احتيال وطنية.

يضم المحتوى المحفوظ من 1 يناير إلى 22 نوفمبر 2026 عدد 337 سجل بطاقة دفع متمايزًا مرتبطًا بالسعودية عبر 386 منشورًا. ويعني السجل المتمايز رقم بطاقة دفع فريدًا مرتبطًا ببادئة جهة إصدار سعودية؛ وقد يتكرر السجل الواحد في منشورات عدة، كما قد يضم المنشور الواحد سجلات متعددة. ولا تسند هذه الملاحظات ترتيبًا لأمن الجهات المصدرة، ولا تثبت صلاحية حالية أو معاملة احتيال. [S5]

8.4 لا تقيس الأسعار المطلوبة قيمة السوق

المثالان التاليان تصريحات بائعين. ولا يثبتان دفع مشترٍ أو تسليم المادة أو صحة الكميات. [S1]

الملف	الكمية المعلنة	السعر المطلوب	الحد المثبت
حزمة المقاولين، الحالة I	حزمة وثائق مقاولين	USD 40,000	إعلان متكرر؛ الاتفاق والبيع غير متحقق منهما
CRM لخدمة عافية، الحالة J	سجلات عملاء مدعاة	USD 150	العدد ورواية الدخول غير متحقق منهما

لا يمكن مقارنة السعرين بوصفهما تكلفة موثوقة للوحدة. فالمنتجات وفئات البيانات والحساسية المدعاة والمصداقية مختلفة. ولا يثبت السعر المنخفض أو المرتفع الأصالة.

ويجب أن تتبع الميزانية الدفاعية أهمية العمل والانكشاف المتحقق منه. فقسمة سعر مطلوب على عدد سجلات مدعى تضيف دقة ظاهرية، من دون إثبات جودة المادة أو نطاقها أو أثرها المالي.

8.5 تصف البيانات الرسمية مسار احتيال موسمي

وصفت بيانات شرطة رسمية في 16 و23 أبريل و3 و19 مايو إعلانات خدمات وهمية على وسائل التواصل. ووصف بيان 10 مايو خدمات وهمية وأساور مزيفة، ولم يحدّد الإعلان على وسائل التواصل صراحة. [S20][S21][S22][S23][S24]

تصف هذه البيانات اعتقالات وإحالات، لا إدانات أو دخولًا مؤكدًا إلى أنظمة. وصلتها الأمنية هي المسار من موضوع خدمة موثوقة إلى طلب دفع أو هوية. ولا يلزم استنتاج عن سياسة الخدمة العامة نفسها.

وعلى مالكي الخدمات تسهيل التحقق من قنوات الشراء والدعم المشروعة. وينبغي أن يسمّي تحذير العميل السلوك غير الآمن، مثل تنفيذ طلب دفع غير مطلوب، وأن يوجّه إلى قناة معروفة. ولا ينبغي أن يعيد نشر رابط إجرامي نشط.

8.6 أبقِ سلسلة الاحتيال نموذج تخطيط

المرحلة المحتملة	الملاحظة الداعمة	ما لم يُثبت	المسؤول الدفاعي
جمع سياق الهوية	إعلانات بيانات عملاء ووثائق	الأصالة والنطاق الحالي ووجود مشترٍ	البيانات والخصوصية
الحصول على قدرة حساب	طلب شراء وروايات وصول	صفقة مكتملة أو وصول صالح	الهوية
انتحال خدمة	أبحاث أمنية وبيانات احتيال رسمية	صلة بملف بائع محدد	المخاطر الرقمية والدعم
طلب دفع أو تحويل مساره	طُعوم فواتير واستثمار في البحث	خسارة وطنية أو معدل نجاح	عمليات مكافحة الاحتيال
إعادة استخدام المادة	إعادة نشر وردود في المجموعة	تطابق الملفات أو المشغّلون المشتركون	استخبارات التهديدات

هذا نموذج تحليلي لمهام التحقيق. وليس عملية إجرامية كاملة مرصودة. ويلزم تطابق ملموس في حساب أو معاملة أو مورّد لربط الحالات تشغيليًا.

الخلاصات الرئيسية

01 الطلب المعلن والبيانات المعروضة والاحتيال المكتمل نتائج مختلفة.

02 رؤية البطاقات ضيقة ولا تقيس خسارة الاحتيال.

03 اربط أدلة الدعم والهوية والاحتيال حول أحداث عملاء متحقق منها.

الفصل 09

نظرة معمّقة على المصارف والخدمات المالية

يجيب هذا الفصل عن

كيف تربط المؤسسة المالية إشارات الهوية وادعاءات بيانات العملاء وضوابط الدفع؟

25

نطاقًا مقيمًا لخدمات مالية ضمن القائمة المختارة

9.1 افصل المجموعات المالية 64

9.2 انكشاف النطاقات المالية 64

9.3 قد تغيّر استعادة الحساب قرار الدفع 65

9.4 أهمية انطباق متطلبات البنك المركزي في 2026 65

9.5 يجب أن يحفظ التحقيق المالي سلسلة الأحداث 66

9.6 أسئلة لمسؤول أمن المعلومات المالي 66

الفصل 09

نظرة معمّقة على المصارف والخدمات المالية

باختصار

تضم الخلية المالية بنوكًا وخدمات مالية أخرى. وتتوفر نتائج انكشاف مكتملة لنطاقاتها البالغ عددها 25، لكنها لا تصلح مقامًا خاصًا بالبنوك. والأدلة المفيدة أكثر تحديدًا: عرض بيانات مستثمرين وطلب حسابات وهجمات اعتماد مبلّغ عنها ومتطلبات البنك المركزي. اختبر تفاعل الاستعادة والوصول الجديد وتعليمات الدفع. وصعّد عندما يوفّر حساب أو معاملة فعلية قرائن، واحفظ قرار الإبلاغ.

9.1 افصل المجموعات المالية

المجموعة	النتيجة المتاحة	ما لا تثبته
النطاقات المالية المختارة	25 نطاقًا مقيمًا؛ ارتبط 12 منها بإدراجات اعتماد حالية	عدد بنوك مستقلة أو معدل انتشار وطني
إعلان بيانات استثمار	نحو 7,000 سجل مدعى في ملف واحد	مستثمرين متحققًا منهم أو أرصدة أو خسارة مالية
طلب المشتري لحسابات	منشور طلب يخص خدمات سعودية	توفر العرض أو الصلاحية أو بيع حساب مكتمل
ملاحظات بطاقات الدفع	ملاحظات محدودة موصوفة في §8.3	أمن الجهة المصدرة أو خسارة احتيال بطاقات وطنية
حملات بيانات الاعتماد	تقارير باحثين عن نشاط موجّه إلى السعودية	معدل نجاح وصول للحسابات على مستوى السعودية

يتعلق ادعاء بيانات الاستثمار بسياق خدمة مالية. ولا يثبت حادثًا في نظام مصرفي. وبالمثل، لا يثبت استخدام علامة بنك في طُعم تصيّد الوصول إلى أنظمة البنك نفسه. [S1][S11][S12]

لا ننشر ترتيبًا للجهات المصدرة هنا. ولا تثبت الملاحظات أعداد العملاء المتأثرين أو أمن الجهات المصدرة. وتتطلب قرارات الاحتيال والدعم أدلة تخص عميلًا أو معاملة فعلية.

9.2 انكشاف النطاقات المالية

تضم النطاقات المالية المقيمة البالغ عددها 25 ما لا يقل عن 104,791 ارتباطًا بأجهزة، منها 332 ارتباطًا بأجهزة موظفين، وعدد 58,177 ارتباطًا بسجلات اعتماد. وتخص إدراجات الاعتماد الحالية 12 نطاقًا. ولا تثبت الملاحظات دخولًا لأنظمة البنوك أو حسابات مسروقة نشطة أو أعداد عملاء متأثرين. [S3]

تظل ملاحظات بطاقات الدفع خاضعة للحدود في §8.3. ولا تثبت صلاحية حالية أو احتيالًا أو وصولًا إلى نظام الجهة المصدرة أو مسؤوليتها عن إصابة جهاز. [S5]

يجب على المسؤول المالي فصل التحقق من أجهزة الموظفين عن حماية حسابات العملاء. والخطوة التالية إثبات صلة الحساب وحداثة المادة ضمن السجلات المصرح بها. وتحتاج فرق الاحتيال والدعم إلى أدلة معاملات وعملاء قبل تقرير وقوع حدث مالي.

9.3 قد تغيّر استعادة الحساب قرار الدفع

تبدأ مراجعة داخلية مفيدة برحلة عميل اصطناعية. اختبر طلب استعادة مشروعًا وتغيير بيانات اتصال وجهازًا جديدًا ووجهة دفع جديدة. وحدّد الفريق الذي يرى كل حدث وما إذا كانت الأدلة تنتقل مع الحالة بين الفرق.

يجب أن يكون الاختبار مصرحًا به وألا يستخدم بيانات عملاء حقيقية. ونتيجته دليل عن الرحلة المختبرة، ولا تثبت منع كل صور الانتحال.

المصادقة متعددة العوامل جزء من التقييم. وعلى الفرق فحص الجلسات الحالية ومسارات الاستعادة وتفويض تعليمات الدفع أيضًا. ولا ينبغي أن يغلق وجودها وحده تحقيقًا في مواد مصادقة مسروقة قابلة للاستخدام أو اشتباه إساءة استخدام جلسة.

9.4 أهمية انطباق متطلبات البنك المركزي في 2026

أصبحت المتطلبات الأساسية لمكافحة الاحتيال سارية في 13 أبريل 2026. ويشمل نطاقها شركات التمويل ومزوّدي خدمات الدفع وفق أحكام الجهات والخدمات المحددة. ولا ينبغي وصف إطار مكافحة الاحتيال المصرفي المنفصل بأنه أُنشئ حديثًا في ذلك التاريخ. [S9]

تدعو متطلبات الوقاية إلى مصادقة بحسب المخاطر، تشمل MFA للإجراءات الأعلى خطرًا، مثل التسجيل والدفع وإعادة تعيين بيانات الاعتماد وتعليمات صرف التمويل. وتتناول أيضًا التحقق من هوية العميل ومخاطر الأطراف الثالثة. [S10]

ومهمة الجهة العضو ربط القواعد المنطبقة بخدماتها. ولا يُستنتج النطاق القانوني لمجرد وجود نطاق في الخلية المالية للتقرير. وعلى مسؤول التواصل التنظيمي تأكيد إشعار الانطباق الوارد من البنك المركزي وتعليمات الإبلاغ والاتصال ذات الصلة (§10).

9.5 يجب أن يحفظ التحقيق المالي سلسلة الأحداث

الإشارة	الفحص الأول	محفّز التصعيد	السجل المحفوظ
عرض بيانات مستثمرين	الحقول ذات الصلة وعلاقات المشاركة المشروعة	تطابق موثوق بسجلات محمية	النطاق وتقييم المصدر وقرار الخصوصية
استعادة مريبة	تفويض العميل وإجراءات الدعم	تغيير غير معتمد أو مادة مسروقة قابلة للاستخدام أو جلسة مسيئة	تسلسل الاستعادة والمصادقة
تعليمات دفع جديدة	التحقق الموثوق وتغييرات الحساب المرتبطة	فشل التحقق أو دليل احتيال موثوق	قرار الدفع والتواصل مع العميل
مؤشر حملة اعتماد	الحسابات والمحاولات والجلسات الناجحة	وصول مريب تؤيده قرائن أو نشاط لاحق	أدلة الهوية والتطبيق
إدراج ابتزاز ذو صلة	علاقة العمل والمورّد	تأكيد داخلي أو من مورّد أو مادة مطابقة موثوقة	تقييم الاستمرارية والسرية والإشعار

يصف الجدول منطق استجابة مقترحًا. ولا يدّعي وقوع كل إشارة لدى بنك خلال فترة التقرير.

9.6 أسئلة لمسؤول أمن المعلومات المالي

اسأل هل تستطيع المؤسسة ربط تفاعل دعم بأحداث الحساب والدفع اللاحقة. وهل يستطيع محلل المناوبة الليلية الوصول إلى صاحب قرار قادر على احتواء الوصول وحماية المعاملة. وهل يعمل مسار الإبلاغ قبل اكتمال الاستنتاج الفني.

يجب أن يتضمن دليل الإنجاز حالة مختبرة والمسؤولين وسجل القرار المحفوظ. ولا تغني لوحة تعرض تنبيهات أكثر عن هذا الدليل.

الخلاصات الرئيسية

01
النطاقات المالية وعملاء البنوك وملاحظات البطاقات مجموعات مختلفة.

02
اختبر الاستعادة وتغييرات الدفع عالية المخاطر رحلة عميل واحدة.

03
أكّد انطباق قواعد البنك المركزي واحفظ دليل كل تصعيد وقرار إبلاغ.

الفصل 10

10 الاستجابة التنظيمية والوطنية

يجيب هذا الفصل عن

ما الالتزامات التي يجب إدراجها في خطة الحوادث، ومن يملك قرار كل منها؟

72 ساعة

الحد الأقصى لإشعار الجهة المختصة بحوادث البيانات الشخصية المستوفية للشروط، من وقت العلم

10.1 تحديد الانطباق يسبق حساب المهلة 68

10.2 افصل مسارات الإشعار 68

10.3 يجب أن تتبع الأدلة مسؤول الضابط 69

10.4 الإنفاذ والتحذيرات يحملان معاني مختلفة 69

10.5 حوّل الامتثال إلى استجابة مجرّبة 70

الفصل 10

الاستجابة التنظيمية والوطنية

باختصار

قد تنطبق واجبات إبلاغ متعددة على الحدث نفسه. تتناول ضوابط الهيئة الوطنية الحوادث السيبرانية، وللبنك المركزي متطلبات تخص القطاع. وتربط لائحة حماية البيانات مهلة إشعار الجهة المختصة باحتمال الضرر أو المساس بالحقوق والمصالح. وتختلف النطاقات والمحفّزات والجهات المتلقية. ولا يعني تحذير احتيال وحده وقوع تسرب واجب الإبلاغ. عيّن المسؤولين القانونيين والتشغيليين، ووثّق وقت العلم، واختبر مسارات الإبلاغ المنطبقة قبل الحادث.

10.1 تحديد الانطباق يسبق حساب المهلة

الجدول التالي دليل عملي لتوزيع المسؤوليات. ولا يحل محل المشورة بشأن الوضع القانوني للجهة. وقد يسبق التزام المورّد التعاقدي واجب الإبلاغ التنظيمي الخاص به.

الجهة	الأداة ذات الصلة	الفحص الأول	المسؤول
جهة حكومية أو جهة بنية تحتية حرجة مشمولة	الضوابط الأساسية للهيئة الوطنية للأمن السيبراني	تأكيد النطاق وتصنيف الحادث وتعليمات الجهة التنظيمية	مسؤول أمن المعلومات والامتثال
بنك خاضع لإطار البنك المركزي	إطار الأمن السيبراني والقواعد المصرفية ذات الصلة	تأكيد التصنيف الحالي ومسار الإبلاغ	مسؤول أمن المعلومات ومسؤول التواصل التنظيمي
شركة تمويل أو مزوّد دفع	المتطلبات الأساسية لمكافحة الاحتيال والقواعد السيبرانية المنطبقة	تأكيد الترخيص والخدمة وإشعار الانطباق الصادر عن البنك المركزي والضوابط الإضافية	مسؤول مكافحة الاحتيال والامتثال
جهة تحكم في بيانات شخصية	نظام حماية البيانات الشخصية ولائحته التنفيذية	تقييم الضرر المحتمل والحقوق أو المصالح المتأثرة	مسؤول الخصوصية والمستشار القانوني
مزوّد خدمة خارجية	الأنظمة المنطبقة وعقود العملاء	تحديد العملاء المتأثرين ومهل العقود وترابط واجبات الإبلاغ	مسؤول الخدمة والشؤون القانونية

تشمل الضوابط الأساسية الجهات الحكومية والجهات التابعة لها، وكذلك الجهات الخاصة التي تملك بنى تحتية وطنية حرجة أو تشغّلها أو تستضيفها. وتشجّع الجهات الأخرى على استخدامها. ويجب توثيق الانطباق بدل استنتاجه من اسم القطاع. [S6]

تكمل وثيقة الهيئة CSCC 2:2026 الضوابط الأساسية ECC-2:2024 للأنظمة الحساسة. ويشمل نطاقها الجهات الوطنية المالكة أو المشغّلة لأنظمة تستوفي معايير الوثيقة، ومنها جهات عامة وخاصة. حدّد الانطباق على مستوى النظام إلى جانب الأساس؛ ولا نستنتج هنا تاريخ نفاذ جديدًا. [S31]

والجدول ليس جردًا نظاميًا كاملًا. وتظل الأدوات القطاعية والسحابية والتشغيلية وغيرها بحاجة إلى مراجعة تخص الجهة.

10.2 افصل مسارات الإشعار

يبيّن الجدول الأحكام الأساسية التي قُرئت لهذا التقرير. ولا نستنتج مهلة موحدة لكل الأحداث السيبرانية.

الأداة	الحكم المتحقق منه	المهمة العملية	الحد
ECC-2:2024	خطط الاستجابة وتصنيف الحوادث وإبلاغ الهيئة الوطنية	تضمين مسار تصعيد للهيئة في خطة الحوادث	لا يضع هذا الحكم مهلة عامة قدرها 72 ساعة
إطار البنك المركزي للأمن السيبراني، 3.3.15	الإبلاغ الفوري لإشراف مخاطر تقنية المعلومات عند وقوع حادث متوسط أو مرتفع وتحديده؛ وطلب عدم الممانعة قبل التفاعل الإعلامي المرتبط	ربط التصنيف بالتواصل التنظيمي والإعلامي	تأكيد التعليمات الحالية المنطبقة على الجهة العضو
اللائحة التنفيذية لحماية البيانات، المادة 24	إشعار الجهة المختصة خلال 72 ساعة من العلم عند تحقق شرط الضرر المحتمل أو المساس بالحقوق والمصالح	تسجيل العلم والنطاق والمخاطر والاحتواء وقرار الإشعار	استكمال المعلومات غير المتاحة بأسرع وقت ممكن مع مبررات التأخير
المادة 24، الأفراد المتأثرون	إشعار صاحب البيانات دون تأخير غير مبرر عند تحقق شرط الضرر الخاص بهذا الحكم	إعداد إشعارات واضحة وقنوات اتصال آمنة	لا تغني مهلة إشعار الجهة المختصة عن هذا الواجب المنفصل
المتطلبات الأساسية لمكافحة الاحتيال	سارية من 13 أبريل 2026 وفق نطاق الجهات والخدمات المحدد	ربط المنتجات والتراخيص بالضوابط المطلوبة	لا توصف بأنها إطار جديد لكل البنوك

تستند هذه الأحكام إلى النصوص الرسمية. ويسبق إطار البنك المركزي المصرفي عام 2026. وقد صدرت المتطلبات الأساسية في 2025 وأصبحت سارية في 2026. ولا يجوز تبادل تاريخ الإصدار وتاريخ النفاذ. [S6][S7][S8][S9]

10.3 يجب أن تتبع الأدلة مسؤول الضابط

يحتاج قرار الإبلاغ إلى أساس وقائعي يمكن الدفاع عنه. سجّل ما كان معلومًا، ومتى عُرف، والبيانات المعنية، والضرر المحتمل، وصاحب القرار. وحدّث التقييم مع تغيّر الأدلة. وقد يكون الادعاء العلني إشارة البداية من دون أن يثبت بعد وصولًا غير مصرّح به.

في الخصوصية، لا تنتظر التقرير الجنائي الرقمي النهائي قبل تقييم شرط الإشعار. وفي تعطل الخدمة، افصل أثر العملاء عن إتاحة صفحة عامة. وفي الاحتيال، احفظ تسلسل المعاملة ورحلة الموافقة منفصلين عن الرسالة التسويقية.

ينبغي أن يعدّ المستشار القانوني سجل قرار موجزًا مع مسؤول أمن المعلومات ومسؤول مكافحة الاحتيال. يوضح الأدوات المنطبقة والمسارات المختارة ومبرر أي قرار بعدم الإشعار. ولا يدّعي التقرير إرسال إشعار في أي حالة يصفها.

10.4 الإنفاذ والتحذيرات يحملان معاني مختلفة

في 16 يناير، أفادت وكالة الأنباء الرسمية بأن لجان سدايا أصدرت 48 قرارًا خلال العام السابق. وتناول البيان معالجة البيانات الشخصية وتدابير الحماية والتسويق. وهذه قرارات إدارية تخص العام السابق، وليست مجموعًا للحوادث السيبرانية في 2026. [S25]

تناولت بيانات شرطة رسمية في أبريل ومايو خدمات وهمية ومخططات تتعلق بالتصاريح. وذكرت أربعة منها إعلانات وسائل التواصل. ووصف بيان 10 مايو خدمات وهمية وأساور مزيفة. وهي دليل على بيانات إنفاذ تخص الاحتيال. ولا تثبت دخولًا إلى أنظمة الجهات التي انتحلت الإعلانات صفتها. [S20][S21][S22][S23][S24]

الدرس العملي هو وصل خدمة العملاء بالأمن. فينبغي أن يصل بلاغ العميل عن إعلان خدمة وهمي إلى فريق يحفظ الرسالة ويقيّم انكشاف الدفع ويوجّه العميل بأمان. ولا يعلّق التقرير على سياسة الخدمة العامة نفسها.

10.5 حوّل الامتثال إلى استجابة مجرّبة

الاختبار	المسؤول	دليل الإنجاز
وصول ادعاء خارج ساعات العمل	قائد الاستجابة	تأكيد استلام مسجّل بالوقت وقرار تصنيف مسجّل
احتمال الوصول إلى بيانات عملاء	مسؤول الخصوصية	وقت العلم وتقييم الضرر وقرار مسار الإبلاغ
تغيّر دفعة بعد تواصل مع الدعم	مسؤول مكافحة الاحتيال	سجل حالة مرتبط ومراجعة المعاملة
إبلاغ مورّد عن انكشاف	مسؤول مخاطر الأطراف الثالثة	نطاق مشاركة البيانات وترابط إشعارات العملاء
الحاجة إلى بيان علني	الاتصال المؤسسي ومسؤول التواصل التنظيمي	بيان وقائعي معتمد والتنسيق التنظيمي المطلوب

الخلاصات الرئيسية

01
تختلف النطاقات وشروط الإشعار بين الهيئة الوطنية والبنك المركزي ومتطلبات الخصوصية.

02
احفظ وقت العلم وما لم يُحسم، من دون انتظار كل الإجابات الفنية.

03
اختبر مسارات الإبلاغ والاتصال مع مسؤولين محددين.

الفصل 11

التوقعات

يجيب هذا الفصل عن

ما الأحكام التي تسندها الأدلة، وما الإشارات التي تغيّر الاستجابة؟

3

سيناريوهات تخطيط مشروطة، من دون تقديرات احتمالية

11.1 الأحكام الرئيسية 72

11.2 الإشارات التي قد تغيّر التقييم 73

11.3 سيناريوهات مشروطة 73

11.4 ما الذي ينبغي أن تقيسه القيادة لاحقًا 74

الفصل 11

التوقعات

باختصار

تحتاج إساءة استخدام الهوية والاحتيال على العملاء وادعاءات الابتزاز إلى أدلة ومسارات استجابة مختلفة. وتدعم التقارير الحالية الاستعداد لكل منها، لكنها لا تثبت وتيرتها الوطنية ولا تتنبأ بالخسائر. وأقوى الأحكام يتعلق بالإجراء: تحقّق من الحساب أو الخدمة أو مجموعة البيانات قبل وصف الأثر. تعامل مع السيناريوهات التالية بوصفها افتراضات تخطيط. وعيّن مسؤولًا وإشارة تبدأ كل استجابة أو تغيّرها أو توقفها.

11.1 الأحكام الرئيسية

تخص الثقة المعلومة المحددة. وليست تقييمًا لبائع أو بلد أو مؤسسة.

الحكم	الثقة	الأساس	الحد
تحتاج هجمات بيانات الاعتماد إلى مسار تحقيق دائم	مرتفعة في ضرورة التحقيق	تقارير فريقين بحثيين عن تصيّد ورش كلمات مرور يستهدفان السعودية	لا يقدّم أي منهما معدل نجاح سعوديًا وطنيًا
تبرر ادعاءات الابتزاز العلنية الاستعداد للاستمرارية	مرتفعة في صلتها بالتخطيط	إدراجات Ransompedia خلال الفترة	لا يثبت الإدراج دخولًا أو تشفيرًا أو خسارة
قد تستدعي ادعاءات بيانات المورّد مراجعة لبيانات العملاء	متوسطة بوصفها خطرًا مشروطًا	ادعاءات بيانات الإنشاءات والأعمال الأخرى	قد تبقى أصالة الملفات وملكيتها ومسار الوصول غير معروفة
يتطلب انتحال الخدمات تنسيق مكافحة الاحتيال والدعم	مرتفعة في صلته بالتشغيل	تقارير باحثين وبيانات احتيال رسمية	لا تقيس البيانات انتشار الاحتيال وطنيًا
لا تدعم القائمة المختارة تقديرًا وطنيًا للانكشاف	مرتفعة	نطاقات مختارة اختيارًا هادفًا وعدد 249 تقييم انكشاف مكتملًا	لا استدلال إحصائي خارج الملاحظات المحددة

لا يتطلب الحكم الأول دليلًا على هجوم مكتمل لدى كل مؤسسة. بل يتطلب مسارًا موثوقًا من الإشارة إلى القرار. ويجب أن يحدّد المسؤول وجود الحساب وإمكان استخدام الوصول وما إذا تبعه نشاط مريب. [S11][S12]

ويتعلق الحكم الثاني بالجاهزية، ولا يتنبأ بتعطل مؤسسة مدرجة. فقد تبرر أهمية العمل اختبار استعادة، من دون تبنّي رواية مجموعة إجرامية عن الحدث. [S2]

11.2 الإشارات التي قد تغيّر التقييم

الدليل الجديد	ما الذي يتغيّر	الإجراء الأول للمسؤول
ظهور حساب نشط مطابق وجلسة مريبة	ينتقل الإدراج من ملاحظة سوقية إلى مؤشر حادث داخلي	يحفظ فريق الهوية السجلات ويقيّم الاحتواء
تأكيد جهة التحكم أو الجهة التنظيمية الوصول إلى بيانات	يصبح الادعاء إفصاحًا مؤكدًا ضمن نطاقه المعلن	يحدّث مسؤول الخصوصية المخاطر وقرارات الإبلاغ
تطابق حقول عينة مع سجلات داخلية مصرح بفحصها	يقوى تقييم أصالة تلك السجلات	يفحص مالك البيانات المصدر من دون تنزيل المادة المعروضة
إظهار بيانات الخدمة تعطلًا أثناء الادعاء	يصبح قياس أثر الإتاحة مستقلًا ممكنًا	تسجّل العمليات المدة والوظائف المتأثرة
إثبات معالجة مجموعة بيانات قديمة	قد لا تستدعي إعادة الإعلان الاستجابة المعطلة نفسها	يربط فريق الحوادث الادعاء بدليل الإغلاق السابق
تأكيد المورّد نطاقًا أضيق	يمكن تضييق تقييم انكشاف الشركاء	يحدّث مسؤول الأطراف الثالثة جرد مشاركة البيانات

لا تحدد إشارة واحدة المشغّل. ولا تثبت إعادة استخدام اسم أو تطابق عنوان أو مشاركة منصة وجود تحكم مشترك. وعندما تبقى العلاقات افتراضية، يسمّيها التقرير نموذجًا تحليليًا.

11.3 سيناريوهات مشروطة

السيناريو A: ما زال حساب معروض قابلًا للاستخدام

ينطبق افتراض التخطيط هذا عند ظهور إشارة تخص الهوية أو الوصول البعيد. والمحفّز دليل داخلي على مواد مصادقة مسروقة قابلة للاستخدام أو نشاط غير مصرح به. ويجب أن يحتوي فريق الهوية الوصول المعني ويحفظ الأدلة فورًا. ولا يثبت سجل تاريخي وحده تحقق هذا المحفّز. أغلق التحقيق الموجّه عندما تسند أدلة الحساب والجلسات القرار وتُتحقق أي معالجة لازمة.

السيناريو B: يتزامن ادعاء علني مع ضغط على الخدمة

المحفّز دليل مستقل على أثر في العملاء أو حركة غير معتادة أو تغيير غير مصرح به. وعلى العمليات تفعيل مسار التخفيف والتعافي المتفق عليه. وينبغي أن ينشر الاتصال المؤسسي الحقائق المعتمدة عبر إدارة الحادث فقط. ولا تثبت صورة ادعاء وحدها تعطلًا. أنهِ استجابة الإتاحة المشددة عندما تستوفي وظائف الخدمة المقيسة معايير التعافي المتفق عليها. وأبقِ تحقيقات البيانات أو الهوية غير المحسومة مفتوحة.

السيناريو C: تظهر بيانات يحتفظ بها مورّد في عرض

المحفّز صلة موثوقة ببيانات المؤسسة أو عقدها. وعلى فريقَي مخاطر المورّدين والخصوصية تحديد السجلات التي شُوركت والعملاء المحتمل تأثرهم. ولا يثبت اسم مشروع في إعلان الوصول إلى شبكة الجهة الرئيسية. أغلق مسار المورّد عندما يحدد مالكو البيانات النطاق ويتحققون من المعالجة اللازمة، أو يوثقون سبب عدم التطابق. وإلا فاحتفظ بقرار غير محسوم.

11.4 ما الذي ينبغي أن تقيسه القيادة لاحقًا

قِس القرارات المكتملة بدل حجم التنبيهات. ومن النتائج المفيدة زمن البت في الإدراج، وزمن احتواء الوصول القابل للاستخدام، ودليل الاستعادة، وحصة المورّدين الحرجين ذوي مسارات الإشعار المختبرة. وهذه مقاييس إدارية مقترحة، وليست وصفًا للأداء السعودي الحالي.

يشير تحسن هذه المقاييس إلى استجابة أكثر موثوقية. لكنه لا يثبت وحده تراجع محاولات الهجوم. وينطبق التمييز نفسه عندما يظهر عدد أقل من المنشورات في فترة لاحقة.

الخلاصات الرئيسية

01
تخص الثقة عبارة محددة يسندها مصدر واضح.

02
تحتاج السيناريوهات المشروطة إلى محفّزات قابلة للرصد وشرط للتوقف.

03
قِس الوصول المتحقق منه وأثر العملاء وقرارات الاستجابة المكتملة.

12

الفصل 12

خطة العمل

يجيب هذا الفصل عن

ما الذي يبدأ الآن، وما الأدلة التي تنتظرها القيادة خلال 30 و60 و90 يومًا؟

15

إجراءً له مسؤول ودليل إنجاز صريح

12.1 المحفّزات الفورية وبرنامج 30/60/90 يومًا 76

12.2 بحسب الدور 78

12.3 مسارات التحقق لمركز العمليات الأمنية 78

12.4 كيف يمكن أن تساعد Brandefense 79

الفصل 12

خطة العمل

باختصار

ابدأ بفرز إشارات الهوية والاستجابة لبيانات العملاء والاستمرارية. وتسندها حملات بيانات الاعتماد المبلّغ عنها وإفصاح تطبيق الهاتف المؤكد وإدراجات الابتزاز العلنية. يبني الجدول قدرة دائمة. ولا يؤخر الاحتواء أو حماية العميل أو الإبلاغ الواجب عند ظهور حادث موثوق. حدّد لكل إجراء مسؤولًا واحدًا وسجلًا يبيّن ما اختُبر. وراجع الأدلة غير المحسومة مع القيادة بدل إغلاق التذكرة بناءً على افتراض.

12.1 المحفّزات الفورية وبرنامج 30/60/90 يومًا

يبدأ البرنامج عندما تعتمده المؤسسة. وأي دليل موثوق على وصول مسروق قابل للاستخدام أو نشاط غير مصرح به أو ضرر للعملاء يفعّل إدارة الحادث فورًا. والفترات التالية أهداف تنفيذ يقترحها التقرير، وليست مهلًا قانونية.

30–01

A01: أنشئ مسارًا لتنبيهات الأسواق وارتباطات الأجهزة، واختبر تنبيهًا اصطناعيًا مصرحًا به وتحقّق من الإشارات الواردة

المسؤول
مسؤول الهوية

دليل الإنجاز
نطاق رصد محدد وتسليم مناوبة مختبر وقرارات بشأن التنبيهات الواردة

A02: عند العثور على مواد مصادقة مسروقة قابلة للاستخدام أو وصول مريب، احتوِ الوصول المعني فورًا

المسؤول
قائد الاستجابة

دليل الإنجاز
إجراءات الجلسات والحسابات والسجلات المحفوظة وقرار تعافٍ موثق

A03: راجع الدخول المؤسسي واستعادة الحساب في ضوء أدلة التصيّد ورش كلمات المرور

المسؤول
هندسة الهوية

دليل الإنجاز
مسارات مصادقة مختبرة وسجل استثناءات وأحداث دخول خاضعة للرصد

A04: ارسم تدفقات بيانات العملاء في التطبيق واختبر الفصل بين صلاحيات الحسابات باستخدام حسابات اختبار مصرح بها

المسؤول
مسؤول التطبيق

دليل الإنجاز
خريطة بيانات معتمدة ونتائج موثقة لاختبار التحكم في الوصول

A05: اختبر استعادة خدمة حرجة وحدّد الانطباق النظامي الأولي وشجرة قرار الإبلاغ

المسؤول
مسؤول الاستمرارية

دليل الإنجاز
دليل استعادة وخريطة معتمدة من الشؤون القانونية أو الامتثال تربط الجهة والأداة والجهة المتلقية والمحفّز، وسجل وقت العلم وجهات إبلاغ محدثة

60–312

A06: أنشئ رصدًا مستمرًا لانتحال الخدمات والمورّدين

المسؤول
مسؤول المخاطر الرقمية

دليل الإنجاز
نطاق رصد ومسار تصعيد وحالة نموذجية أُغلقت عبر المسار

A07: قيّم مصادقة البريد من دون اعتبار غياب الملاحظة غيابًا للضابط

المسؤول
مسؤول البريد

دليل الإنجاز
سياسات متحقق منها لنطاقات الإرسال واستثناءات موثقة

A08: اربط حالات الدعم والهوية واحتيال الدفع عندما تخص المعاملة نفسها

المسؤول
مسؤول مكافحة الاحتيال

دليل الإنجاز
إجراء لربط الحالات واختبار اصطناعي كامل لاستعادة الحساب

A09: راجع مشاركة البيانات مع المورّدين الحرجين وترابط واجبات الإشعار

المسؤول
مسؤول مخاطر الأطراف الثالثة

دليل الإنجاز
فئات بيانات ومسؤوليات وصول ومسار تصعيد مختبر لكل مورّد حرج

A10: تدرّب على التحقق المستقل من حالة الخدمة أثناء ادعاء ابتزاز أو DDoS

المسؤول
مسؤول العمليات

دليل الإنجاز
حالة تسندها بيانات الخدمة واتصال للتخفيف ورسائل وقائعية معتمدة

90–613

A11: دقّق خريطة الانطباق الأولية للهيئة الوطنية والبنك المركزي وحماية البيانات التي أُعدّت ضمن A05

المسؤول
مسؤول الامتثال

دليل الإنجاز
خريطة معتمدة تربط الأدوات بالجهات ومسؤولون للمعالجة

A12: اختبر تغييرات الدفع واستعادة الحساب عالية المخاطر بسيناريوهات اصطناعية آمنة

المسؤول
هندسة مكافحة الاحتيال

دليل الإنجاز
نتائج كشف ودليل وقف التغييرات غير المصرح بها أو تصعيدها

A13: أزل وصول المورّد غير اللازم وقلّل الاعتماد على صلاحيات إدارية مشتركة

المسؤول
مسؤول البنية التحتية

دليل الإنجاز
صلاحيات خضعت للمراجعة واستثناءات موثقة واختبار تعافٍ

A14: أغلق عينة من تذاكر التحذيرات بناءً على أدلة الأصول والإصدارات الفعلية

المسؤول
مسؤول إدارة الثغرات

دليل الإنجاز
أصول مشمولة وتأكيد معالجة واستثناءات مقبولة

A15: راجع الادعاءات غير المحسومة ومعالجة الحوادث السابقة مع القيادة

المسؤول	دليل الإنجاز
مسؤول أمن المعلومات	سجل قرارات ومسؤولون متأخرون ودروس مدمجة في خطط الاستجابة

يختلف A01 عن A02. فالرصد يوفّر الرؤية، والاحتواء يستجيب لخطر متحقق منه. ولا ينبغي اعتبار سجل اعتماد قديم أو ارتباط بنطاق عميل أو عنوان عرض دليلًا على حساب موظف صالح حاليًا.

ويعالج A04 وA08 حدّين مختلفين أيضًا. يتحكم مسؤول التطبيق في الوصول إلى البيانات المخزنة. وتقيّم مكافحة الاحتيال الشخص والجهاز ورحلة الدفع. ولا يثبت نجاح اختبار التطبيق سلامة استعادة الحساب عبر الدعم أو إضافة مستفيد جديد.

12.2 بحسب الدور

الدور	القرار الأول	اطلب	تجنّب
مجلس الإدارة والقيادة التنفيذية	تمويل الاستجابة وفق أهمية العمل	دليل A05 والسجل غير المحسوم في A15	اعتبار عدد التنبيهات تقديرًا للخسائر
مسؤول أمن المعلومات	إنشاء قيادة حادث موحدة للفرق التقنية والتجارية	مسؤولي A01–A03 ودليل التصعيد	إعلان حسم ادعاء علني من دون تقييم وقائعي
مركز العمليات الأمنية	فصل محاولات المصادقة عن الجلسات الناجحة والنشاط اللاحق	بيانات دخول المؤسسة والبريد والوصول البعيد والخدمة	حجب كل خدمة مشتركة لمجرد ورودها في بحث
فريق الهوية	تحديد إمكان استخدام الحساب ومواد المصادقة المشار إليها	نطاق الحساب ودليل الجلسات والمعالجة السابقة	افتراض أن حالة MFA تحسم التحقيق
مكافحة الاحتيال وخدمة العملاء	حماية المعاملات المعنية وتوفير قناة استجابة آمنة	تسلسل مرتبط ودليل التفويض وتغيير الدفع	إعادة العميل إلى الرسالة المشبوهة
الخصوصية والشؤون القانونية	تحديد شروط الإشعار وحفظ تسلسل القرار	سجلات A05 وA11	انتظار يقين تقني كامل قبل تقييم الواجبات
المشتريات والمورّدون	تأكيد البيانات والوصول المشتركين ذوي الصلة	أدلة A09 وA13	اعتبار ادعاء مقاول دليلًا على الوصول إلى كل شريك

12.3 مسارات التحقق لمركز العمليات الأمنية

هذه أسئلة تحقيق وليست قواعد كشف قابلة للنشر مباشرة. وتتطلب بيانات محلية مصرحًا بها وضبطًا يناسب البيئة.

الإشارة	تحقّق أولًا	صعّد عندما	سجل الإغلاق
فشل المصادقة لدى حسابات كثيرة	تغييرات خدمة الهوية المشروعة ونطاق الحسابات وتوزيع الوقت	تتوافق المحاولات مع وصول ناجح مريب أو قرائن أخرى	الحسابات والجلسات المفحوصة والتفسير البديل
بلاغ عن صفحة دخول مؤسسية مزيفة	مصدر الرسالة وتفاعل المستخدم الفعلي	قُدمت مواد مصادقة أو وُجدت جلسة غير معتمدة أو فُتح محتوى خبيث	الاحتواء وفحص الجهاز والتواصل مع المستخدم
ادعاء بيع بيانات يسمّي مورّدًا	العقد المعني ونطاق مشاركة البيانات	تطابق مادة موثوقة سجلات محمية أو يصل تأكيد المورّد	تقييم مالك البيانات وقرار الإبلاغ
تداول ادعاء تعطيل	بيانات الإتاحة والمعاملات المستقلة	يُتحقق من أثر في الخدمة أو إعداد غير مصرح به	المدة والوظائف والتخفيف والتعافي
إضافة وجهة دفع بعد استعادة الحساب	دليل الاستعادة وتفويض العميل	يفشل التحقق الموثوق من التغيير أو تُكشف إساءة استخدام	قرار الدفع والتواصل مع العميل وحالة الحادث المرتبطة

لا يبرر محفّز التصعيد تجاهل الأدلة الأخرى. وعلى الفرق حفظ النتائج المتعارضة وإعادة تقييم النطاق. وقد يبقى ادعاء علني غير متحقق منه تحت المتابعة بينما يُحتوى حدث داخلي مؤكد منفصل.

12.4 كيف يمكن أن تساعد Brandefense

تجمع Brandefense استخبارات التهديدات السيبرانية والحماية من المخاطر الرقمية وإدارة سطح الهجوم الخارجي. وتشمل الأعمال المرتبطة بقرارات التقرير رصد إدراجات بيانات الاعتماد والانتحال ومتابعة ادعاءات الابتزاز وترتيب أولويات الانكشاف الخارجي. وتظل ملاحظات المنتج بحاجة إلى تحقق في بيئة العميل.

ابدأ بنطاق محدد يضم النطاقات والعلامات والخدمات الحرجة والمورّدين المهمين للمؤسسة. واتفق على متلقي النتائج والأدلة التي تبدأ التحقيق وكيفية توثيق الإغلاق. والقيمة هي مسار قرار قابل للاستخدام، لا عدد أكبر من التنبيهات.

اطلب عرضًا توضيحيًا

الخلاصات الرئيسية

01
ابدأ البرنامج الآن واستجب فورًا لدليل حادث موثوق.

02
لكل إجراء مسؤول واحد ودليل إغلاق قابل للملاحظة.

03
افصل قرارات الرصد والتحقق والاحتواء والإبلاغ القانوني.

A–E

الملاحق

الملاحق

يجيب هذا الفصل عن

ما الذي تقيسه الملاحظات، وأين تبدأ حدودها؟

1 يناير–22 نوفمبر 2026

فترة المجموعة الرئيسية بحسب وقت المنشور

الملحق A. النطاق والمصادر والثقة 81

الملحق B. سجل بطاقات الأدلة العامة 84

الملحق C. المصادر 85

الملحق D. مسرد المصطلحات 87

الملحق E. موضوعات ادعاء إضافية خضعت للمراجعة 88

الملحق A. النطاق والمصادر والثقة

اختيرت دول المقارنة كأمثلة لتوفير السياق فقط؛ ولا ينطوي اختيارها على أي ترتيب أو تقييم سياسي.

A.1 الوقت ومجموعات الأدلة

الفترة الرئيسية للتقرير من 1 يناير إلى 22 نوفمبر 2026 بحسب وقت المنشور. ويغطي القسم الحديث 8–22 نوفمبر. وجرت الأبحاث بينما كان يوم القطع جاريًا. وقد يصف المنشور مادة أقدم، ولا يثبت وقت النشر وقت الدخول.

تبقى مجموعات الأدلة منفصلة: منشورات مرتبطة ببلد ومحتوى محفوظ وسجلات منتديات وإعلانات وملفات ادعاء وهويات نشر ونطاقات مختارة وملاحظات بطاقات وإدراجات فدية. ولا تُجمع لإنتاج عدد هجمات وطني.

A.2 ملاحظات الويب المظلم

يستخدم Odin by Brandefense ملاحظات Brandefense Blackhole للمنشورات، ومنها المنتديات والمراسلة. ويبلغ الحجم المرتبط بالسعودية 748,946 منشورًا. وتضم رؤية المحتوى 33,458 منشورًا متمايزًا عبر المجموعات المحفوظة، منها 220 منشور منتدى موسومًا بالسعودية و5,043 منشورًا مرتبطًا بالعربية. [S1]

تتفاوت التغطية بحسب الشهر والمصدر. ولا تمثل المادة كل منصة أو كل نقاش مرتبط بالسعودية. ولا تثبت هذه الملاحظات انتشارًا وطنيًا أو تغيّرًا في وتيرة الهجمات.

وقد تشمل الملاحظات إعلانات متعددة الدول وأسماء غير مرتبطة ومادة تاريخية. ولا يثبت الارتباط ببلد وجود استهداف.

ترتبط كل بطاقة منشور معروضة بسجل مصدر خاص محفوظ. وتحفظ الاقتباسات جزءًا سرديًا أصيلًا قصيرًا. وتحذف البطاقات العامة سجلات الأفراد وبيانات الاعتماد والاتصال ومعرّفات الضحايا والروابط الإجرامية النشطة. وتُفصل الترجمة عن المقتطف الأصلي.

A.3 قائمة المؤسسات والانكشاف

تضم القائمة 250 نطاقًا رئيسيًا مرشّحًا في عشر خلايا قطاعية مدمجة، في كل منها 25. ويعكس الاختيار أدوارًا عامة وعمليات سعودية مهمة. وليست ترتيبًا منشورًا لأكبر 250 مؤسسة، ولا تعداد كيانات مستقلة، ولا عينة ممثلة إحصائيًا. وتبقى الملكية والحالة التشغيلية وتداخل المجموعات حدودًا. [S3]

تضم لقطة الانكشاف في 22 نوفمبر 2026 نتائج مكتملة لعدد 249 من 250 نطاقًا مختارًا. وتبلغ القيمة الوطنية الرئيسية لـ Atlas لهذه المجموعة المقيمة 52/100. ولا يُنشر سوى التقييم الوطني. وتبقى نتيجة النطاق المتبقي مجهولة ويُستبعد من مقامات الانكشاف.

تصف أعداد الأجهزة والاعتماد والوثائق والإدراجات الملاحظات المحفوظة عند اللقطة، ومنها سجلات أقدم. ويغطي الذكر السنوي 19 نوفمبر 2025–18 نوفمبر 2026؛ وتغطي الأسماء الشبيهة المرشحة فترة منفصلة من 30 يومًا. والإدراج إعلان، ولا يثبت الارتباط بنطاق دخولًا مؤكدًا. [S3]

A.4 ملاحظات ضوابط النطاقات الخارجية

لا تتوفر للنشر نتائج مكتملة لضوابط النطاقات الخارجية. ولا يُستنتج انتشار ضوابط أو نتيجة مؤشر سلامة. ويجب أن تبقى الملاحظة الغائبة غير معروفة بدل تحويلها إلى ضابط فاشل. [S4]

تصف ملاحظات ضوابط النطاقات الخارجية خدمة في وقت فحصها. ولا تصادق على أمن المؤسسة كلها ولا تثبت ملكية النطاق. وتتطلب نتائج سياسة البريد وحالة الشهادات وترويسات الويب مقامات مقيمة منفصلة.

A.5 بيانات البطاقات

لا تثبت ملاحظات بطاقات الدفع المحدودة هذه صلاحية حالية أو احتيالًا مكتملًا أو اختراق أنظمة الجهات المصدرة أو خسائر احتيال وطنية. ولا تسند ترتيبًا لأمن الجهات المصدرة. ويعني سجل البطاقة المتمايز رقم بطاقة دفع فريدًا مرتبطًا ببادئة جهة إصدار سعودية خلال فترة التقرير الرئيسية؛ وقد تكرر المنشورات سجلًا واحدًا أو تدرج سجلات عدة. [S5]

تنطبق هذه الحدود أينما ذُكرت ملاحظات البطاقات، بما فيها فصل الخدمات المالية. ولا ننشر اتجاهًا شهريًا أو ترتيبًا للجهات المصدرة.

A.6 إدراجات الفدية والابتزاز

يوفّر Ransompedia عدد 30 إدراجًا موسومًا بالسعودية في الفترة. وتستخدم المقارنة الفترة نفسها للإمارات وقطر والكويت وعُمان. ولا يجوز اعتبار تواريخ الإدراج تواريخ دخول إلى الأنظمة. [S2]

الإدراج ادعاء إجرامي. ولا يثبت الإدراج تأكيدًا رسميًا أو تشفيرًا أو تعطيلًا تشغيليًا أو خسارة مالية. وقد تحتاج تسميات البلد والصناعة والأهداف إلى تحقق. وليست أسماء الأهداف كيانات قانونية مستقلة بالضرورة.

A.7 التقارير الخارجية والنصوص النظامية

تُنسَب المعلومات الخارجية إلى مصادرها. وتثبت بيانات جهات التحكم صدور إفصاح، وتسند المعلومات التي أكدتها الجهة. ويثبت نقل صحفي ادعاءات منشورة ضمن حدوده. ويسند البحث الأمني سلوك الحملة الذي يصفه.

قُرئت النصوص النظامية والضوابط للأحكام المحددة المستشهد بها. ولا يحل التقرير محل مشورة خاصة بالجهة أو تعليمات تنظيمية حالية. ونفصل تواريخ النشر والنفاذ والحادث.

الثغرة الوحيدة التي يناقشها التقرير هي CVE-2026-0326. وفُحص سجل NVD وتنبيه المورّد في 22 نوفمبر 2026. ويتبع جدول الإصدارات المصلحة المورّد. ولا نستنتج استغلالًا سعوديًا من سجل الثغرة. [S15][S14]

A.8 تغطية الحوادث

تشمل تغطية الحوادث مادة منتديات محفوظة وتقارير عامة وبيانات رسمية. وتسند هذه الملاحظات المعلومات المحددة المنسوبة إلى كل مصدر.

لم تتوفر بعض الأرشيفات الرسمية للفترة كاملة. ولذلك لا تثبت الأدلة المتاحة تعدادًا وطنيًا شاملًا. ولا يعني نقص التغطية عدم وقوع حدث.

تفيد صفحة منجزات الهيئة الوطنية لعام 2025 برصد أكثر من 2,000 حادثة سيبرانية والاستجابة لها. ويقيس هذا الرقم الرسمي مجموعة مختلفة عن ملاحظات الويب المظلم ومواقع التسريب لعام 2026 في هذا التقرير، ولم يُثبت هنا مجموع مماثل للهيئة لعام 2026 يتيح مقارنة متكافئة. [S34]

ويمكن لمشغّل منفرد نشر سلسلة سنوية متسقة وفق تعريفاته الخاصة. وعلى سبيل المثال، تسجّل مؤشرات الحوكمة والاستدامة لعام 2025 لدى مجموعة stc عدد 8,405 محاولات هجوم و15 هجومًا فعليًا لدى stc السعودية في 2024، مقابل 10,313 محاولة و16 هجومًا فعليًا في 2025. وتوضح هذه السلسلة مقارنة محدودة بمشغّل واحد، لا معدل حوادث وطنيًا. [S35]

تثبت المصادر العامة المقروءة إفصاح جهة تحكم مسماة واحدة بين الملفات المفصلة. وتبقى الحالات الأخرى حملات أبلغت عنها مصادر أو إعلانات أو طلبًا أو ادعاءات غير متحقق منها. ولا يدّعي التقرير أنها كل الحوادث التي أثرت في السعودية.

A.9 الثقة وحدود القرار

الوصف	المعنى	المثال
ثقة مرتفعة في الملاحظة	يسند سجل محفوظ العبارة مباشرة	نشر بائع عرضًا
مبلّغ عنه من مصدر	يصف ناشر مسمى السلوك أو الرواية	رش كلمات مرور رصده باحثون
إفصاح رسمي	تؤكد مؤسسة أو جهة مختصة المعلومة المحددة	إفصاح بيانات عملاء التطبيق
نتيجة غير متحقق منها	يفتقر أثر الهدف المدعى إلى دعم مستقل هنا	وصول أو سرقة أو مدة أو بيع يدعيه ناشر
نموذج تحليلي	تفسير مسمى للتخطيط	علاقة محتملة بين سياق الهوية واحتيال الدفع

يبقى التفسير البديل المعقول ظاهرًا بجوار كل حالة. وقد يضيّق تأكيد جهة تحكم عدم اليقين من دون إثبات كل ادعاء محيط. ونحذف الاستنتاج غير المدعوم بدل تعويضه بوصف ثقة.

الخلاصات الرئيسية

01
لكل مجموعة وحدتها ووقتها وحدود تغطيتها.

02
الادعاء المحفوظ ونتيجة الهدف المؤكدة عبارتان مختلفتان.

03
استخدم حد الدليل لاختيار خطوة تحقق تالية متناسبة.

الملحق B. سجل بطاقات الأدلة العامة

تظهر البطاقات بجوار مناقشتها. وتواريخها تواريخ منشورات، لا تواريخ حوادث ثابتة. وتدعم خريطة الأدلة الخاصة تتبّع المصدر من دون نشر روابطه أو معرّفات الضحايا.

البطاقة	تاريخ المنشور	المنصة	الاسم	اللغة	الفصل
B01	2026-01-17	منتدى	zer0sintt	الإنجليزية	4
B02	2026-01-30	منتدى	alwayslearning	الإنجليزية	4
B03	2026-02-02	منتدى	l0rd0f	الإنجليزية	4
B04	2026-02-13	منتدى	agent7001	الإنجليزية	4
B05	2026-02-23	منتدى	ryhem	الإنجليزية	4
B06	2026-02-27	منتدى	sexyskin	الإنجليزية	4
B07	2026-04-19	منتدى	ناشر غير مسمى	الإنجليزية	4
B08	2026-06-08	منتدى	ناشر غير مسمى	الإنجليزية	4
B09	2026-09-15	منتدى	ناشر غير مسمى	الإنجليزية	4
B10	2026-09-28	منتدى	ناشر غير مسمى	الإنجليزية	4
B11	2026-03-24	قناة مراسلة	Team 313	الإنجليزية	6
B12	2026-08-06	قناة مراسلة	Team 313	العربية	6
B13	2026-09-11	قناة مراسلة	Team 313	الإنجليزية	6
B14	2026-10-02	قناة مراسلة	Team 313	العربية	6
B15	2026-05-03	منتدى	ناشر غير مسمى	الإنجليزية	5
B16	2026-07-18	منتدى	FandyUAE	الروسية	8
B17	2026-04-03	قناة مراسلة	ناشر غير مسمى	العربية	8
B18	2026-03-04	قناة مراسلة	ناشر غير مسمى	العربية	6
B19	2026-11-09	منتدى	بائع غير مسمى	الإنجليزية	4

الملحق C. المصادر

أرقام المصادر التي لا تظهر سُحبت أثناء المراجعة ولا يُستشهد بها. وتعرّف بنود بياناتنا المجموعة المحفوظة؛ ولا نقدّم روابط عامة للمادة الخاصة. وتسجل البنود الخارجية التاريخ وحالة قراءة النص الداعم. ويحمي مرجع أصل الموقع الموسوم «حُجب رابط المقالة» الهدف غير المسمى.

S1: Odin by Brandefense: Saudi dark-web observations. مجموعة ملاحظات خاصة؛ حُجبت المصادر الخاصة. تم التحقق في: 2026-11-22. حالة القراءة: own data.

S2: Ransompedia: Saudi Arabia and Gulf comparison. مجموعة ملاحظات خاصة؛ حُجبت المصادر الخاصة. تم التحقق في: 2026-11-22. حالة القراءة: own data.

S3: Atlas exposure ratings and Blackhole domain associations. مجموعة ملاحظات خاصة؛ حُجبت المصادر الخاصة. تم التحقق في: 2026-11-22. حالة القراءة: own data.

S4: Odin by Brandefense: external domain-control observations. مجموعة ملاحظات خاصة؛ حُجبت المصادر الخاصة. تم التحقق في: 22-11-2026. حالة القراءة: own data.

S5: Odin by Brandefense: payment-card observations. مجموعة ملاحظات خاصة؛ حُجبت المصادر الخاصة. تم التحقق في: 2026-11-22. حالة القراءة: own data.

S6: NCA: Essential Cybersecurity Controls ECC-2:2024. https://cdn.nca.gov.sa/api/files/public/upload/86e09090-44e4-481f-bc28-355673607654_ECC--2024-EN.pdf تم التحقق في: 22-11-2026. حالة القراءة: web PDF read.

S7: SDAIA: Implementing Regulation of the Personal Data Protection Law. https://dgp.sdaia.gov.sa/wps/wcm/connect/2a9a4744-a2ae-444f-bad2-6dacde843637/The%2Bimpelementing%2Bregulation%2Bof%2Bthe%2Bpersonal%2Bdata%2Bprotection%2Blaw.pdf?CACHEID=ROOTWORKSPACE-2a9a4744-a2ae-444f-bad2-6dacde843637-pcruNj.&CONVERT_TO=url&MOD=AJPERES تم التحقق في: 2026-11-22. حالة القراءة: web PDF read.

S8: SAMA: Cyber Security Framework. https://rulebook.sama.gov.sa/en/cyber-security-framework-2 تم التحقق في: 2026-11-22. حالة القراءة: web text read.

S9: SAMA: Counter-Fraud Fundamental Requirements. https://rulebook.sama.gov.sa/en/counter-fraud-fundamental-requirements تم التحقق في: 22-11-2026. حالة القراءة: web text read.

S10: SAMA: Fraud Prevention section 3.2. https://rulebook.sama.gov.sa/en/32-fraud-prevention تم التحقق في: 2026-11-22. حالة القراءة: web text read.

S11: Unit 42: regional cyber-risk brief, updated 17 April 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/ تم التحقق في: 22-11-2026. حالة القراءة: web text read.

S12: Check Point Research: Microsoft 365 password-spray campaign. https://blog.checkpoint.com/research/iran-nexus-password-spray-campaign-targeting-cloud-environments-with-a-focus-on-the-middle-east/ تم التحقق في: 2026-11-22. حالة القراءة: web text read.

S13: Saudi CERT security alerts index. https://nca.gov.sa/en/cert/ تم التحقق في: 22-11-2026. حالة القراءة: web text read.

S14: Palo Alto Networks: CVE-2026-0326 advisory. https://security.paloaltonetworks.com/CVE-2026-0326 تم التحقق في: 2026-11-22. حالة القراءة: web text read.

S15: NVD: CVE-2026-0326. https://nvd.nist.gov/vuln/detail/CVE-2026-0326 تم التحقق في: 22-11-2026. حالة القراءة: NVD record read.

S16: Saudi Press Agency: GASTAT household ICT use in 2026. https://spa.gov.sa/en/N2715791 تم التحقق في: 2026-11-22. حالة القراءة: official statement text read.

S17: Saudi Exchange: issuer disclosure of limited mobile-app customer-data access. https://www.saudiexchange.sa/wps/portal/saudiexchange/newsandreports/issuer-news/issuer-announcements/issuer-announcements-details/?anCat=1&anId=95974&cs=4260&locale=en تم التحقق في: 22-11-2026. حالة القراءة: official statement text read.

S18: Mubasher: issuer statement on customer-data incident. https://english-old.mubasher.info/news/4624554/The-United-International-Transportation-Company-Budget-Saudi-Announces-a-Limited-Cyber-security-Incident-Involving-a-Portion-of-the-Data-of-Certain-Customers-of-the-Budget-Saudi-Mobile-Application- تم التحقق في: 22-11-2026. حالة القراءة: Live body read.

S19: The National: relayed construction-sector data claim. https://www.thenationalnews.com/ (حُجب رابط المقالة) تم التحقق في: 22-11-2026. حالة القراءة: Article body read; article URL withheld.

S20: SPA: police notice on fraudulent service advertisements, 16 April. https://www.spa.gov.sa/en/N2563378 تم التحقق في: 22-11-2026. حالة القراءة: official statement text read.

S21: SPA: police notice on fraudulent service advertisements, 23 April. https://www.spa.gov.sa/en/N2569817 تم التحقق في: 22-11-2026. حالة القراءة: official statement text read.

S22: SPA: police notice on fraudulent service advertisements, 3 May. https://www.spa.gov.sa/en/N2576669 تم التحقق في: 2026-11-22. حالة القراءة: official statement text read.

S23: SPA: police notice on fraudulent services and counterfeit wristbands, 10 May. https://www.spa.gov.sa/en/N2582285 تم التحقق في: 22-11-2026. حالة القراءة: official statement text read.

S24: SPA: police notice on fraudulent service advertisements, 19 May. https://spa.gov.sa/en/N2590305 تم التحقق في: 2026-11-22. حالة القراءة: official statement text read.

S25: SPA: SDAIA prior-year privacy enforcement decisions. https://spa.gov.sa/en/N2489505 تم التحقق في: 22-11-2026. حالة القراءة: official statement text read.

S26: Saudi CERT: Microsoft alert 2026-8020. https://nca.gov.sa/en/cert/8145/ تم التحقق في: 22-11-2026. حالة القراءة: Original live alert body read.

S27: Saudi CERT: Google alert 2026-8026. https://nca.gov.sa/en/cert/8153/ تم التحقق في: 22-11-2026. حالة القراءة: Original live alert body read.

S28: ArabicTrader: reporting of official mobile-app incident disclosure. https://www.arabictrader.com/en/news/stock-market/219537/saudi-budget-reveals-stock-market-of-a-limited-hack-through-its-electronic-application تم التحقق في: 22-11-2026. حالة القراءة: Live body read.

S29: Brandefense: capabilities and demo. https://brandefense.io/request-a-demo/ تم التحقق في: 22-11-2026. حالة القراءة: Live body read.

S30: MITRE ATT&CK: Password Spraying T1110.003. https://attack.mitre.org/techniques/T1110/003/ تم التحقق في: 2026-11-22. حالة القراءة: Live body read.

S31: NCA: Critical Systems Cybersecurity Controls CSCC 2:2026. https://cdn.nca.gov.sa/api/public/cms/files/14828b9c-c1d5-4c6c-9b06-b6564f3ed17a_CSCC---2-2026-AR-.pdf تم التحقق في: 22-11-2026. حالة القراءة: Official Arabic PDF read; version, introduction and scope.

S32: Dataminr: regional football-data advertisement. https://www.dataminr.com/ (حُجب رابط المقالة) تم التحقق في: 2026-11-22. حالة القراءة: Article body read; article URL withheld.

S33: Microsoft: Microsoft Digital Defense Report 2026، الصادر في 1 أكتوبر 2026. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/2026-Microsoft-Digital-Defense-Report.pdf تم التحقق في 23 نوفمبر 2026 (23-11-2026). حالة القراءة: web PDF read.

S34: الهيئة الوطنية للأمن السيبراني (NCA): أبرز المنجزات (محطات 2025). https://nca.gov.sa/en/nca-achievements/ تم التحقق في 23 نوفمبر 2026 (23-11-2026). حالة القراءة: web text read.

S35: مجموعة stc: تقرير الاستدامة لعام 2025، مؤشرات الحوكمة والاستدامة، الصادر في 26 يونيو 2026. https://www.stc.com/content/dam/groupsites/stc-sustainability-report-2025/esg-metrics/ تم التحقق في 23 نوفمبر 2026 (23-11-2026). حالة القراءة: web text read.

الملحق D. مسرد المصطلحات

المصطلح	معناه في التقرير
Atlas	تقييم الانكشاف الخارجي المستخدم للقائمة المقيمة في هذا التقرير
القيمة الوطنية الرئيسية	قيمة Atlas واحدة للقائمة المقيمة كلها؛ لا يُنشر تقييم لمؤسسة أو قطاع
ارتباط جهاز	سجل خارجي يربط جهازًا بنطاق خدمة؛ تتطلب الملكية والوصول الحالي تحققًا
إعلان	عرض بائع منشور، من دون صفقة متحقق منها
طلب حساب	طلب مشترٍ، من دون إثبات العرض المتاح أو الوصول الصالح
سجل اعتماد	سجل مرتبط بالمصادقة؛ تتطلب الصلاحية الحالية تقييمًا
إدراج حالي	مادة مصادقة معلنة وقت الملاحظة؛ لا دليل على حساب قابل للاستخدام
ادعاء مجموعة بيانات	زعم يخص سجلات أو ملفات قد يبقى مصدرها وعددها غير متحقق منهما
جهة التحكم	الطرف الذي يحدد غرض معالجة البيانات الشخصية وكيفيتها
صاحب البيانات	الشخص الذي تتعلق به البيانات الشخصية
رش كلمات المرور	تجربة مجموعة صغيرة من كلمات المرور عبر حسابات كثيرة
MFA	مصادقة تتطلب أكثر من عامل مستقل
ERP	تخطيط موارد المؤسسة، فئة من أنظمة إدارة الأعمال
CRM	إدارة علاقات العملاء، ومنها أنظمة تحفظ تفاعلاتهم وسجلاتهم
DDoS	حجب خدمة موزع، أي محاولة لتعطيل إتاحة خدمة
DMARC	سياسة نطاق وآلية تقارير لمصادقة البريد
SPF / DKIM	آليتا تفويض مرسل وتوقيع رسالة في مصادقة البريد
DNSSEC	مصادقة بيانات DNS عبر سلسلة ثقة موقّعة
TLS	تشفير الاتصالات الشبكية ومصادقتها
إدراج فدية	ادعاء موقع تسريب؛ لا يثبت تشفيرًا أو دخولًا مؤكدًا
نموذج تحليلي	تفسير تخطيط مفصول صراحة عن الروابط التشغيلية الثابتة

الملحق E. موضوعات ادعاء إضافية خضعت للمراجعة

توسّع هذه البنود الحالات المفصلة. وهي إعلانات أو طلبات أو نقل أو مؤشرات غير محسومة، وليست دخولًا مؤكدًا إضافيًا. وقد تتداخل مع بعضها أو مع حالة أو إدراج. وتشير التواريخ إلى منشورات المصادر، إلا عندما يوضح البند أنه تاريخ نشر بحث. ولا نستنتج مجموع حوادث وطنيًا. [S1]

المعرّف / التاريخ	الموضوع العام	حد الدليل	القرار الأول للمسؤول
T01 · 2026-03-01	سلسلة استهداف وحالة خدمة مصرفية	رسائل متكررة ولغة انتهاء مهلة؛ لا انقطاع مقيس مستقلًا	مسؤول الخدمة المالية: تحقق من الإتاحة
T02 · 2026-03-03	ادعاء موقع اتصالات	صيغة أهداف وروابط فحص؛ لا دليل وصول إلى الشبكة	العمليات: حدّد الوظائف المتأثرة
T03 · 2026-03-06	قائمة أهداف مواقع عامة	أهداف عدة في رسالة؛ ليست حوادث مؤكدة	مسؤولو الخدمات: تحققوا من الحالة مستقلًا
T04 · 2026-04-04 / 2026-04-05	ادعاءات اعتماد وبيانات لجهات عامة	سلسلة باسم ذاتي تعد بنشر بيانات؛ الوصول غير متحقق منه	الهوية والبيانات: قيّما التطابقات الداخلية
T05 · 2026-07-06	نقل عرض بيانات صحية	إعلان منقول؛ المصدر والحداثة غير محسومين	الخصوصية: تحقق من علاقة البيانات
T06 · 2026-08-03	ادعاء شبكة جهة عامة صناعية	لا تثبت مزاعم الإعداد والثغرات الوصول	البنية التحتية: قيّم السجلات المصرح بها
T07 · 2026-07-21	مؤشر ابتزاز صحي غير محسوم البلد	النطاق السعودي غير مثبت؛ مستبعد من ادعاءات الحوادث السعودية	لا تنسب ضحية إلى السعودية
T08 · 2026-03-22	طلب بيانات اعتماد	طلب مشترٍ؛ لا اقتناء أو وصول صالح مثبت	الهوية: راجع الاستعادة والرصد
T09 · 2026-04-03 / 2026-07-26	عروض حسابات ولاء	بائعون منفصلون؛ لا وصول إلى أنظمة الطيران أو تنفيذ مثبت	مكافحة الاحتيال: قيّم نشاط العملاء المعني
T10 · 2026-06-24 / 2026-07-06	إعلانات خدمات اختبارات ترخيص	ادعاء قدرة متعدد الدول؛ لا دخول مثبت إلى جهة اختبار	نزاهة الخدمة: تحقق من البلاغات ذات الصلة
T11 · 2026-01-04	ادعاء مورّد أمن سيبراني إقليمي	لا تثبت مزاعم مواد عملاء سعوديين الوصول إلى كل عميل	مخاطر المورّدين: حدّد نطاق البيانات المشتركة
T12 · 2026-01-14	إعلان وصول إلى جدار ناري	لم يُختبر وصول؛ المؤسسة والقدرة غير متحقق منهما	الهوية والبنية: تحققا من الإشارات المعنية
T13 · 2026-01-16 / 2026-01-20	نقاش أرشيف مورّد صحي	تداخل محتمل مع إدراج؛ لا يؤكد الأرشيف المحجوب والردود الادعاء	مسؤول المورّد: حدّد العلاقة قبل عدّ حادث
T14 · 2026-01-22 / 2026-01-26	عروض بيانات اتصالات	عروض متكررة وأسعار مختلفة؛ العمر والتفرّد غير محسومين	مالك البيانات: قيّم المصدر والمعالجة السابقة

المعرّف / التاريخ	الموضوع العام	حد الدليل	القرار الأول للمسؤول
T15 · 2026-02-14 / 2026-02-15	ادعاء بيانات أرقام هاتف	يصف البائع المادة صراحة بأنها غير متحقق منها؛ السجلات ليست أشخاصًا متحققًا منهم	الخصوصية: اطلب دليل مصدر أقوى
T16 · 2026-02-28	عرض بيانات عضوية ترفيه ولياقة	صلة محتملة بالحالة ا؛ لا حدث جديد متحقق منه مستقلًا	مسؤول بيانات العملاء: قارن النطاق
T17 · 2026-03-13	ادعاء شيفرة وتدمير لتطبيق نقل	مزاعم شيفرة وحذف وتعطيل؛ لا تأكيد من الجهة المعنية	التطبيق والعمليات: قيّما كل معلومة منفصلة
T18 · 2026-03-17	ادعاء بيانات جهة صحية خاصة	حقول اتصال وبيانات ديموغرافية؛ الحجم وتاريخ الاقتناء غير مسندين	مالك البيانات: تحقق من الحقول المعنية
T19 · 2026-03-26	ادعاء بيانات خدمة عضوية أعمال	أوصاف اتصال وعضوية وسجلات؛ الحداثة والوصول غير متحقق منهما	مسؤول الخدمة: قيّم التصدير والصلاحيات
T20 · 2026-03-13 / 2026-04-10	ادعاءات بيانات SQL لتطبيق	إعادة نشر محتملة؛ لا يثبت عنوان بسنة جارية وصولًا حاليًا	مسؤول التطبيق: حدّد المصدر
T21 · 2026-04-12 / 2026-04-13	تداول بيانات اتصال وعملاء	نسخ عدة لموضوع واحد؛ الحداثة والتفرّد غير متحقق منهما	الخصوصية: قيّم البيانات المطابقة بدل حجم النشر
T22 · 2026-04-13	بيانات عملاء بعناوين متعارضة	تبقى الكميات المتعارضة غير محسومة؛ لا نختار رقمًا بوصفه حقيقة	مالك البيانات: احسم المصدر قبل النطاق
T23 · 2026-04-12	عنوان بيانات مقتضب مرتبط بالسعودية	سرد غير كافٍ للمصدر أو الحداثة أو حدث متمايز	أبقِه ادعاء غير محسوم
T24 · 2026-03-17	ادعاء تعطيل خدمة رقمية	اسم ذاتي وروابط فحص؛ لا انقطاع مقيس	العمليات: تحقق من وظائف العملاء
T25 · 2026-05-05 / 2026-05-07	إدراج عالمي لسير ووثائق	جزء بوسم بلد؛ ليس حادث مؤسسة سعودية أو أشخاصًا متحققًا منهم	مالك البيانات: قيّم تطابقًا ذا صلة فقط
T26 · 2026-01-14 / 2026-05-01	بيانات عملاء محتملين عالمية أقدم	ردود لاحقة تعيد مادة عالمية؛ لا مجموع سعودي فقط أو دخول جديد	اربط بالنطاق السابق بدل حدث جديد
T27 · 2026-02-24	نقل طاقة وهندسة مختلط الدول	يتداخل مع إدراج محفوظ؛ ليست المادة المدعاة سعودية فقط بالضرورة	مسؤول المورّد: حدّد السجلات المنطبقة
T28 · 2026-02-23	نقل وثائق مقاولين	يتداخل مع الحالة ا؛ لا تثبت وثائق صناعية الوصول إلى أنظمة التحكم	أمن الهندسة: تحقق من البيانات والصلاحيات
T29 · 2026-09-12	قائمة أهداف مواقع عامة باسم ServerKillers	ادعاء باسم ذاتي؛ لا أثر مقيس مستقلًا	العمليات: تحقق من كل خدمة ذات صلة
T30 · 2026-10-26	قائمة أهداف مواقع عامة باسم DARKSTORM	ليست القائمة دليل انقطاعات متعددة أو وصول داخلي	مسؤولو الخدمات: حدّدوا الحالة والنطاق

المعرّف / التاريخ	الموضوع العام	حد الدليل	القرار الأول للمسؤول
T31 · 2026-09-10	نقل وثائق للقطاع العام	صلة محتملة بأرشيف أقدم؛ تطابق الملفات غير مثبت	مسؤول السجلات: قيّم المصدر والمعالجة السابقة
T32 · 2026-10-21	نقل ادعاء بيانات إنشاءات	يتداخل مع الحالة B؛ لا تأكيد مستقل أو حدث جديد مثبت	مخاطر المورّدين: حافظ على التحقيق المحدد القائم
T33 · 2026-09-28	تطبيق صحي يتعامل مع معلومات متبرعين	ادعاء بيانات؛ الأصالة والعمر والتفرّد والوصول الحالي غير متحقق منها	الخصوصية ومسؤول التطبيق: قيّما تطابق بيانات ذا صلة
T34 · 2026-11-09 / 2026-11-10	إعلان جلسة لمقاول	أربعة منشورات متكررة تشكل الحالة P؛ لم تُختبر جلسة أو مادة معروضة	الهوية ومسؤول المورّد: تحققا من النطاق واحفظا الأدلة
T35 · 2026-10-14	ادعاء خدمة إقليمية لمعالجة المدفوعات	مزاعم بيانات تجار ومعاملات ومسار دخول تقني؛ لا تأكيد أو خسارة مثبتة	الدفع والبيانات: قيّما السجلات المعنية من دون اختبار وصول
T36 · 2026-04-27، تاريخ نشر البحث	إعلان بيانات إقليمية لكرة القدم	وصف باحث مجموعة ملفات تضم مواد مرتبطة بالسعودية؛ لا وصول مؤكد إلى نظام سعودي أو مجموع للأشخاص المتأثرين	مسؤولو بيانات الأفراد والمورّدين: تحققوا من علاقات الوثائق المعنية

وصف تقرير بحثي منفصل إعلان بيانات إقليمية لكرة القدم. ولا تثبت المواد المرتبطة بالسعودية وصولًا إلى مؤسسة سعودية أو عددًا خاصًا بالسعودية للأشخاص المتأثرين. ولا يتبنى التقرير تأطيرًا سياسيًا أو انتماءً لفاعل. [S32]

عن هذا التقرير

هذه نسخة السعودية من سلسلة Brandefense Country Report 2026، أعدّها Odin by Brandefense. وهي موجهة لقيادات الأمن ومراكز العمليات ومسؤولي الخدمات ومكافحة الاحتيال والشؤون القانونية والامتثال.

تجمع Brandefense استخبارات التهديدات السيبرانية والحماية من المخاطر الرقمية وإدارة سطح الهجوم الخارجي. وتبقى ملاحظات المنتج أدلة للتحقيق وترتيب الأولويات. ولا تحل محل سجلات الهوية والخدمة والحوادث الخاصة بالمؤسسة. [S29]

تترجم النسخة العربية الإنجليزية وتحفظ حدود أرقامها ومصادرها وادعاءاتها. وعند الاختلاف، تكون النسخة الإنجليزية هي المرجع.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO