الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

تقرير حول أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني

لعام 2024م

إشارة المشاركة: أبيض

تصنيف الوثيقة: عام

بالتعاون مع:

BCG IDC

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل أو خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

المحتويات

الملخص التنفيذي 1

مقدمة 2

كلمة شركاء إعداد التقرير 3

أبرز النتائج 5

1 المنهجية 7

1.1 تصنيف المنتجات والحلول والخدمات في قطاع الأمن السيبراني 7

2.1 جمع البيانات 8

3.1 ضمان الجودة 8

4.1 تحليل البيانات 9

5.1 تطوير المخرجات 9

2 أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني 10

1.2 سوق الأمن السيبراني 10

1.1.2 حجم السوق 10

2.1.2 الإنفاق حسب حجم الجهات في المملكة 10

3.1.2 حجم السوق حسب تصنيف منتجات وحلول وخدمات الأمن السيبراني 11

4.1.2 التوزيع الجغرافي لجانب الطلب 11

5.1.2 التوزيع الجغرافي لجانب العرض 12

6.1.2 تصنيف مقدمي منتجات وحلول وخدمات الأمن السيبراني 12

2.2 إسهام قطاع الأمن السيبراني في الناتج المحلي الإجمالي 13

ملحق (أ) 15

تصنيف المنتجات والحلول والخدمات في قطاع الأمن السيبراني

الملخص التنفيذي

تُعد الهيئة الوطنية للأمن السيبراني وفق تنظيمها الصادر بالأمر الملكي رقم (6801) في 1439/2/11هـ هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه. وتهدف إلى تعزيزه، حماية للمصالح الحيوية للدولة وأمنها الوطني، والبنى التحتية الحساسة، والقطاعات ذات الأولوية، والخدمات والأنشطة الحكومية. كما تضمنت اختصاصات الهيئة ومهماتها الواردة في تنظيمها، تحفيز نمو قطاع الأمن السيبراني في المملكة، وتشجيع الابتكار والاستثمار فيه، وإجراء الدراسات والبحوث والتطوير وعمليات التصنيع، ونقل التقنية وتطويرها، في الأمن السيبراني وما يرتبط به من مجالات.

وفي ضوء ما تقدم ولتعزيز فهم قطاع الأمن السيبراني من المنظور الاقتصادي؛ تم إعداد هذا التقرير والذي ينقسم إلى بابين رئيسيين، وفقًا للآتي: 1) المنهجية، حيث جرى في هذا الباب تصنيف سوق الأمن السيبراني لمنتجات وحلول وخدمات، ومن ثم تحديد الفئات المستهدفة وآلية جمع البيانات وتحليلها والتحقق من دقة المخرجات. 2) أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني، ويستعرض هذا الباب حجم السوق، وإنفاق الجهات العاملة في المملكة بمختلف أنشطتها وأحجامها، بالإضافة إلى التوزيع الجغرافي لجانبي العرض والطلب، وحصر مقدمي منتجات وحلول وخدمات الأمن السيبراني في المملكة، وتصنيفهم من حيث الحجم، وكذلك المساهمة الاقتصادية لقطاع الأمن السيبراني في الناتج المحلي الإجمالي.

مقدمـــة

يشهد قطاع الأمن السيبراني تطورًا حيويًا ومتسارعًا منذ تأسيسه في المملكة، حيث ابتدأت أعمال تأسيس هذا القطاع بشقيه الاقتصادي والأمني وبمختلف أبعاده المحلية والدولية، حتى أصبح النموذج السعودي في الأمن السيبراني أنموذجاً ناجحاً ورائداً في العالم يُحتذى به دوليّاً في هذا المجال.

ويتميز النموذج السعودي في الأمن السيبراني بالشمولية في تناول مجالات الأمن السيبراني سواءً التشريعية، أو الأمنية، أو الاقتصادية والتنموية. ويرتكز النموذج السعودي للأمن السيبراني على اللامركزية في التشغيل الذي يقع تحت مسؤولية الجهات الوطنية، والمركزية في حوكمة الأمن السيبراني على المستوى الوطني من خلال مركزية التنظيم، ومركزية العمليات وتحديدًا مركزية أعمال تقييم الأمن السيبراني، وأعمال الاستجابة للحوادث السيبرانية، وأعمال بناء القدرات وتأهيل الكفاءات على المستوى الوطني ويسهم النموذج السعودي للأمن السيبراني في تعزيز فهم المشهد السيبراني الوطني بأكمله بما يعظم مكاسب المملكة ومكانتها دوليًا، وتمكين الجهات الوطنية في الوقت نفسه من القيام بمهماتها واختصاصاتها ورفع جاهزيتها التشغيلية.

وللبناء على ما تحقق من مكتسبات، فقد تم إجراء دراسة لأبرز المؤشرات الاقتصادية المتعلقة بقطاع الأمن السيبراني في المملكة العربية السعودية على مدار العامين 2023م و 2024م، وتم فيها اتباع أفضل الممارسات المستخدمة؛ بما يسهم في تعزيز تنمية قطاع الأمن السيبراني في المملكة، ودعم رواد الأعمال، والمستثمرين. ويوضح هذا التقرير أبرز نتائج الدراسة.

كلمة شركاء إعداد التقرير

في ظل التطور المتسارع الذي يشهده قطاع الأمن السيبراني في المملكة، أصبح من المهم فهم سوق الأمن السيبراني الحالي ومتغيراته بشكلٍ مفصل؛ من خلال دراسة وتحليل حجم الإنفاق على حلول ومنتجات وخدمات الأمن السيبراني من قبل الجهات الحكومية ومنشآت القطاع الخاص ذات البنى التحتية الحساسة وبقية منشآت القطاع الخاص، لإعطاء نظرة مفصلة عن القوى المؤثرة في قطاع الأمن السيبراني في المملكة، وفهم توجهات العرض والطلب. كما تضمنت الدراسة تحليلًا عن كوادر الأمن السيبراني العاملة في قطاع الأمن السيبراني في المملكة، والتي تعد من المكونات الرئيسة لتنمية قطاع الأمن السيبراني، ومن مدخلات بناء إستراتيجيات تعزيز حماية الفضاء السيبراني.

وقد نتج عن التعاون المشترك بين مجموعة بوسطن الاستشارية (BCG)، وشركة البيانات الدولية (IDC)، والهيئة الوطنية للأمن السيبراني إعداد دراسة يحتذى بها عند النظر إلى أسواق الأمن السيبراني عالميًا. وقد أسهمت الخبرات العالمية والمتخصصة في المجال، والقدرات التحليلية، والفهم الواسع لقطاع الأمن السيبراني في المملكة؛ في تحليل واستخلاص أبرز المؤشرات الاقتصادية حول هذا القطاع الحيوي والواعد في المملكة. إذ تم تصنيف جميع منتجات وحلول وخدمات الأمن السيبراني، والعمل وفق منهجية دقيقة للحصول على نظرة تفصيلية حول سوق الأمن السيبراني ومتغيراته باستخدام النماذج الإحصائية والاقتصادية المتقدمة لاستخلاص استنتاجات ذات قيمة نوعية.

تنفرد هذه الدراسة في أساليب جمع البيانات وتحليلها على نحوٍ شاملٍ ومتكامل، حيث تم جمع بيانات العامين 2022م و2023م من عدة مصادر متنوعة تمثل كافة مكونات قطاع الأمن السيبراني؛ مما أسهم في رفع دقة نتائج هذه الدراسة والإحصائيات المستخرجة منها. وقد حققت عملية جمع البيانات، واستخدام أفضل الممارسات العالمية في تحليل ونمذجة تلك البيانات، مستوى ثقة إحصائي عند نسبة 98%، وبهامش خطأ 4%، لضمان جودة مخرجات الدراسة.

وقد تم تعزيز هذه الدراسة من خلال المشاركة الواسعة لأصحاب المصلحة، والتي اشتملت على جلسات النقاش مع الخبراء في المجال، بالإضافة إلى مدخلات الجهات الحكومية، ومنشآت القطاع الخاص ذات البنى التحتية الحساسة، وباقي منشآت القطاع الخاص، ومقدمي منتجات وحلول وخدمات الأمن السيبراني، والمؤسسات التعليمية في المملكة. حيث أضافت تلك المصادر رؤى متعددة لسوق الأمن السيبراني مما أسهم في دقة منهجية الدراسة إحصائيًا، وأن تكون ذات صلة بالسياق في المملكة.

وتسلط مخرجات هذه الدراسة الضوء على مختلف محاور سوق الأمن السيبراني في المملكة، لتكون أداة إستراتيجية لصناع القرار، والقادة، وأصحاب المصلحة في قطاع الأمن السيبراني في المملكة؛ بما توفره من فهم شاملٍ يمكن من توجيه التطورات والتوجهات المستقبلية في القطاع نحو دعم النمو الاقتصادي والاجتماعي في المملكة

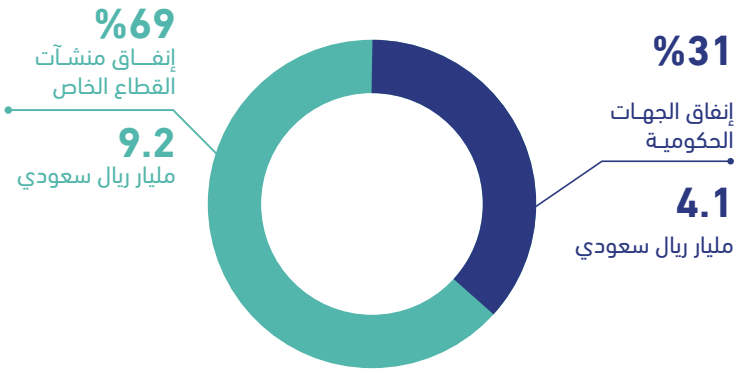
شركاء إعداد التقرير:

BCG IDC

أبــرز النتائــج

حجم سوق الأمن السيبراني في المملكة

13.3
مليار ريال سعودي



حجم المساهمة في الناتج المحلي الإجمالي بالأسعار الجارية

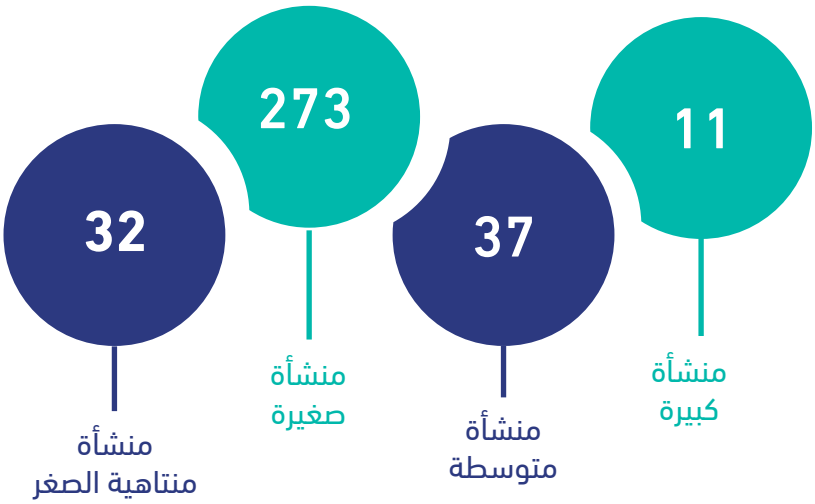
15.6
مليار ريال سعودي

%0.39
مساهمة القطاع في الناتج المحلي الإجمالي

%0.81
مساهمـة القطاع في الناتج المحلي الإجمالي غير النفطي

إشارة المشاركة: أبيض | تصنيف الوثيقة: عام

عدد مقدمي منتجات وحلول وخدمات الأمن السيبراني المسجلين لدى الهيئة



353
مقدم منتجات وحلول وخدمات أمن سيبراني

أبرز منتجات وحلول وخدمات الأمن السيبراني في المملكة


أمن الشبكات


تكامل أنظمة الأمن السيبراني


أمن الأجهزة الطرفية وإدارتها


إدارة مركز عمليات الأمن السيبراني


أمن الحوسبة السحابية

كوادر الأمن السيبراني في المملكة

19.6 ألف
مختص بالأمن السيبراني

%32
نسبة مشاركة المرأة

1 المنهجية

1.1 تصنيف المنتجات والحلول والخدمات في قطاع الأمن السيبراني

جرى العمل في هذه الخطوة، مع عدد من بيوت الخبرة لإنشاء تصنيف شامل لمنتجات وحلول وخدمات الأمن السيبراني (ملحق أ)، ومن ثم تقييمه مع عدد من الشركات العالمية، ومقدمي منتجات وحلول وخدمات الأمن السيبراني، ليصبح شاملًا ومفصلًا ومرنًا؛ ليغطي تفاصيل قطاع الأمن السيبراني. وقد جرى تصنيف المنتجات والحلول والخدمات في قطاع الأمن السيبراني لأكثر من (100) صنف، موزعة على (3) مستويات.

المستوى الأول

يوضح المستوى الأول التصنيف الأساسي لأنشطة قطاع الأمن السيبراني كمنتجات وحلول، أو خدمات بحسب نماذج تقديمها.

المستوى الثاني

يقسم كل فئة من فئات المستوى الأول إلى مجموعة من الأنشطة التفصيلية.

المستوى الثالث

يحدد منتجات وحلول وخدمات الأمن السيبراني في كل نشاط من أنشطة المستوى الثاني.

2.1 جمع البيانات

تضمنت هذه الخطوة تحديد الفئات المستهدفة، والبيانات التي سيتم جمعها، وآلية جمع البيانات، والعينة الإحصائية لكل فئة. واشتملت آلية جمع البيانات على استبانات، ومجموعات عمل، بالإضافة إلى إجراء مقابلات شخصية مع الخبراء في مجال الأمن السيبراني؛ لأخذ مدخلاتهم. وقد جرى تحديد جانب الطلب في السوق، ليشمل الجهات الحكومية، ومنشآت القطاع الخاص ذات البنى التحتية الحساسة، وبقية منشآت القطاع الخاص على مختلف أنشطتها وأحجامها. أما جانب العرض في السوق؛ فقد قامت الهيئة بجمع البيانات من مقدمي منتجات وحلول وخدمات الأمن السيبراني في المملكة. وعليه؛ فيمكن تحديد مستوى الثقة إحصائيًا لنتائج الدراسة عند (98%) وبهامش خطأ (4%). وقد جرى جمع بيانات الدراسة في الربع الأول من عامي 2023م و2024م.

3.1 ضمان الجودة

اشتملت هذه الخطوة على آلية للتحقق من صحة البيانات في مختلف مراحل الدراسة؛ لضمان دقة الإحصاءات والنتائج، بحسب أفضل المعايير للدراسات المشابهة، والمقترحة من الجهات الدولية، كالأمم المتحدة وغيرها. وشملت تطبيق معايير تقنية، لاستبعاد البيانات التي تعد خارج نطاق الدراسة والبيانات غير الدقيقة.

%98

مستوى الثقة

إحصائيًا لنتائج الدراسة

4.1 تحليل البيانات

جرى تطوير نماذج إحصائية واقتصادية مترابطة؛ لاستخلاص مرئيات نوعية على مستوى قطاع الأمن السيبراني في المملكة، بناءً على النمذجة الإحصائية لتحليل إيرادات مقدمي منتجات وحلول وخدمات الأمن السيبراني وإنفاق الجهات الحكومية ومنشآت القطاع الخاص ذات البنى التحتية الحساسة وبقية منشآت القطاع الخاص، والنمذجة الاقتصادية لتقدير حجم إسهام القطاع في الناتج المحلي الإجمالي.

وقد جرى الاستفادة من مدخلات الخبراء، والمختصين المحليين والدوليين، في هذا المجال، واستخدام الأدلة السياقية، والمقارنات المعيارية الدولية، والسجلات الإدارية الحكومية، لتأكيد مخرجات النماذج، بما في ذلك مجموعات البيانات من وزارة الموارد البشرية والتنمية الاجتماعية، والهيئة العامة للإحصاء، وهيئة الزكاة والضريبة والجمارك.

كما جرى تقدير إسهام قطاع الأمن السيبراني في الناتج المحلي الإجمالي بالمواءمة مع منهجية الهيئة العامة للإحصاء، والتي تضمنت تقدير إيرادات مقدمي منتجات وحلول وخدمات الأمن السيبراني في المملكة بناءً على مخرجات ونتائج الدراسة، وضرائب الشركات، والدعم المقدم لها، وتم استخدام جداول المدخلات والمخرجات الاقتصادية؛ لتقدير الآثار المباشرة وغير المباشرة للأعمال في قطاع الأمن السيبراني في المملكة.

5.1 تطوير المخرجات

استنادًا على نتائج النماذج الإحصائية والاقتصادية، جرى استخراج مرئيات نوعية عن سوق الأمن السيبراني في المملكة، ومساهمته الاقتصادية.

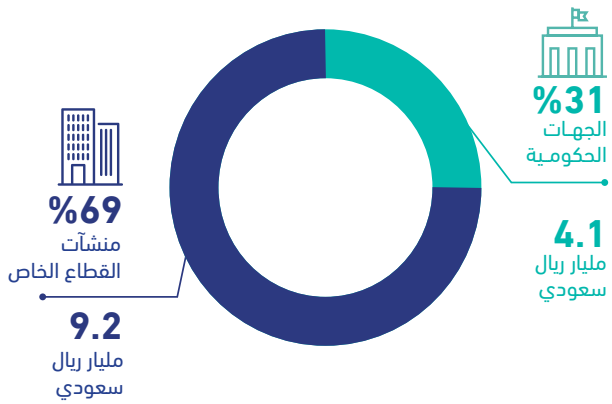
2 أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني

1.2 سوق الأمن السيبراني

1.1.2 حجم السوق

يمثل مجموع ما أنفقته الجهات العاملة في المملكة على منتجات وحلول وخدمات الأمن السيبراني (13.3) مليار ريال سعودي. ويتوزع الإنفاق في السوق على القطاعين العام والخاص؛ إذ بلغ مجموع إنفاق الجهات الحكومية (4.1) مليار ريال سعودي يشكل (31%) من حجم السوق، وأنفقت منشآت القطاع الخاص ما يقارب (9.2) مليار ريال سعودي، والتي يشكل (69%) من حجم السوق، منها (2.8) مليار ريال سعودي أنفقتها منشآت القطاع الخاص ذات البنى التحتية الحساسة.

13.3
مليار ريال سعودي



2.1.2 الإنفاق حسب حجم الجهات في المملكة

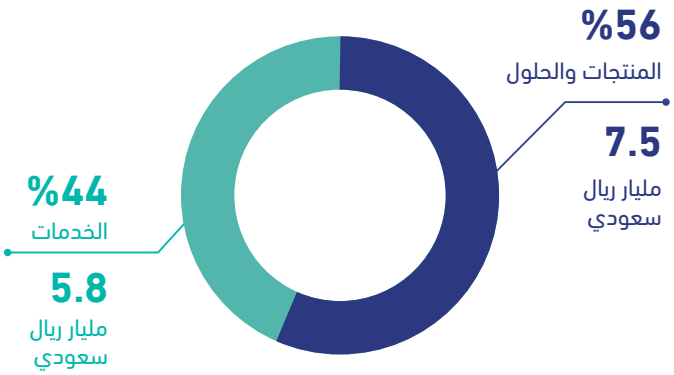
عند النظر إلى إنفاق الجهات في المملكة على منتجات وحلول وخدمات الأمن السيبراني في المملكة، فإن معظم إنفاق الجهات الحكومية ومنشآت القطاع الخاص ذات البنى التحتية الحساسة يتم في الجهات الكبيرة والكبيرة جدًا؛ وذلك لكونها جهات تشرف على جهات أخرى تابعة لها.

وبالنظر إلى بقية منشآت القطاع الخاص فإن المنشآت المتوسطة هي الأكثر إنفاقًا؛ حيث تمثل العدد الأكبر من منشآت القطاع الخاص التي تتطلب منتجات وحلول وخدمات الأمن السيبراني.

		كبيرة جدًا	كبيرة	متوسطة	صغيرة	متناهية الصغر
الجهات الحكومية	4.1 مليار ريال سعودي	%38	%50	%11	%1	-
منشآت القطاع الخاص ذات البنى التحتية الحساسة	2.8 مليار ريال سعودي	%33	%62	%4	%1	-
بقية منشآت القطاع الخاص	6.4 مليار ريال سعودي	%14	%26	%41	%16	%3

3.1.2 حجم السوق حسب تصنيف منتجات وحلول وخدمات الأمن السيبراني

ينقسم سوق الأمن السيبراني في المملكة حسب التصنيف إلى منتجات وحلول الأمن السيبراني، وخدمات الأمن السيبراني. حيث بلغت نسبة المنتجات والحلول (56%) من إجمالي حجم السوق بقيمة (7.5) مليار ريال سعودي، وتمثل خدمات الأمن السيبراني (44%) من إجمالي حجم السوق بقيمة (5.8) مليار ريال سعودي.



أبرز منتجات وحلول وخدمات الأمن السيبراني

- أمن الشبكات
- تكامل أنظمة الأمن السيبراني
- أمن الأجهزة الطرفية وإدارتها
- إدارة مراكز عمليات الأمن السيبراني
- أمن الحوسبة السحابية

4.1.2 التوزيع الجغرافي لجانب الطلب

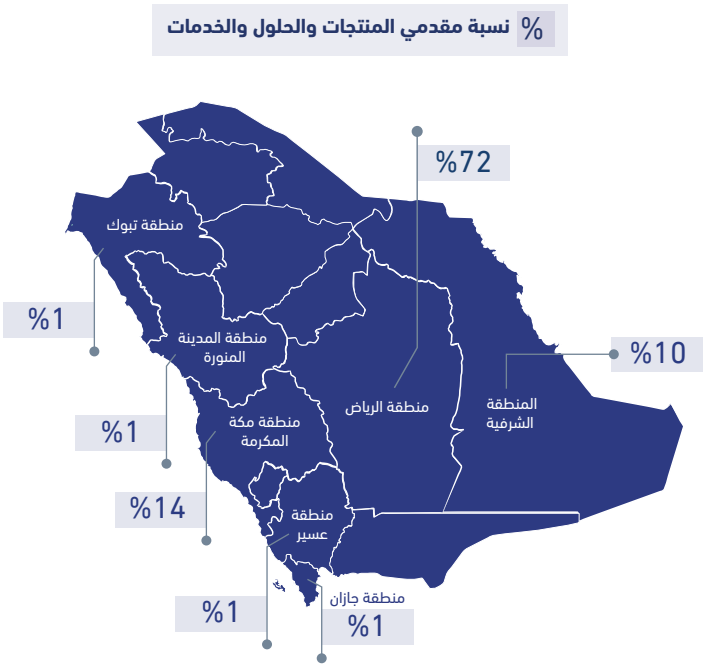
يعتمد التوزيع الجغرافي على المناطق الإدارية للمقرات الرئيسة للجهات العاملة في المملكة في جانب الطلب، حيث تتركز (83%) من هذه الجهات في منطقة الرياض، ومكة المكرمة، والمنطقة الشرقية بالتناسب مع التقارير الصادرة من الهيئة العامة للمنشآت الصغيرة والمتوسطة.

%83

من الجهات تتركز في منطقة الرياض، ومكة المكرمة، والمنطقة الشرقية

5.1.2 التوزيع الجغرافي لجانب العرض

يعتمد التوزيع الجغرافي لمقدمي منتجات وحلول وخدمات الأمن السيبراني على المناطق الإدارية للمقرات الرئيسة لها في المملكة. وتتصدر منطقة الرياض القائمة بنسبة (72%) من مقدمي المنتجات والحلول والخدمات، تليها منطقة مكة المكرمة بنسبة (14%)، والمنطقة الشرقية بنسبة (10%). ويتسق هذا التوزيع مع المناطق ذات التركيز الاقتصادي الأعلى في المملكة، بينما يتوزع (4%) من مقدمي منتجات وحلول وخدمات الأمن السيبراني على بقية المناطق الإدارية.



6.1.2 تصنيف مقدمي منتجات وحلول وخدمات الأمن السيبراني

جرى تصنيف حجم المنشآت التي تقدم منتجات وحلول وخدمات الأمن السيبراني في المملكة بناءً على تعريف الهيئة العامة للمنشآت الصغيرة والمتوسطة. ونظرًا لتقارب خصائص فئات المنشآت في قطاع الأمن السيبراني في المملكة، ولاستخلاص الاستنتاجات، بشكلٍ أوضح في هذه الدراسة؛ فقد تم دمج الفئتين الخاصة بمقدمي المنتجات والحلول والخدمات المتوسطة والكبيرة في فئة واحدة وتسميتها (الفئة الكبرى)، ودمج الفئتين الخاصة بمقدمي المنتجات والحلول والخدمات الصغيرة ومتناهية الصغر تحت مسمى (الفئة الصغرى).

تصنيف الهيئة العامة للمنشآت الصغيرة والمتوسطة	عدد مقدمي منتجات وحلول وخدمات الأمن السيبراني	النسبة من الإجمالي
كبيرة	11	%3
متوسطة	37	%11
صغيرة	273	%77
متناهية الصغر	32	%9
الإجمالي	**353**	**%100**

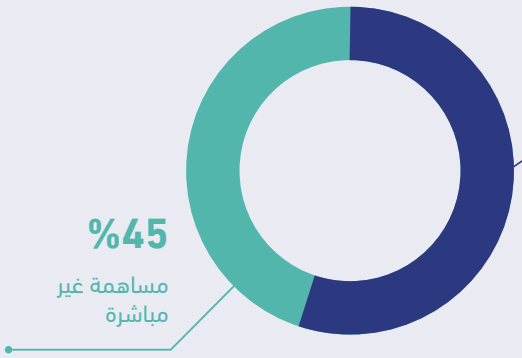
2.2 إسهام قطاع الأمن السيبراني في الناتج المحلي الإجمالي

بناءً على مخرجات دراسة سوق الأمن السيبراني في المملكة، والأرقام الصادرة من الهيئة العامة للإحصاء للعام 2023م؛ فإن إسهام قطاع الأمن السيبراني في الناتج المحلي الإجمالي بالأسعار الجارية يقدّر بحوالي (15.6) مليار ريال سعودي، منها (8.6) مليار ريال سعودي مساهمة مباشرة، و(7) مليار ريال سعودي مساهمة غير مباشرة.

ويمثل إسهام قطاع الأمن السيبراني في المملكة (0.39%) من الناتج المحلي الإجمالي، و(0.81%) من الناتج المحلي الإجمالي غير النفطي.

حجم المساهمة في الناتج المحلي الإجمالي بالأسعار الجارية

15.6
مليار ريال سعودي

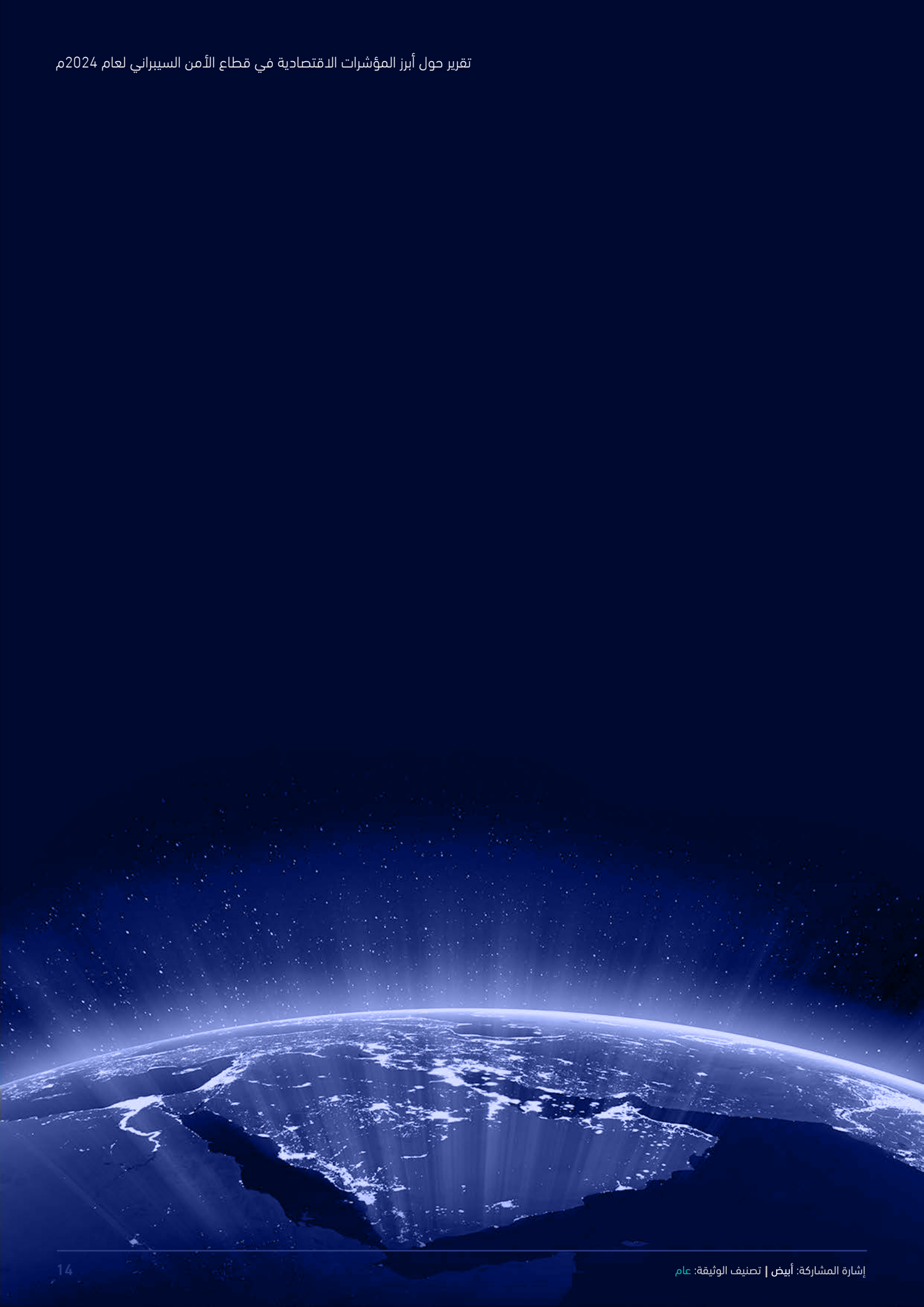


55%
مساهمة مباشرة
8.6
مليار ريال سعودي

45%
مساهمة غير مباشرة
7
مليار ريال سعودي

0.39%
مساهمة القطاع في الناتج المحلي الإجمالي

0.81%
مساهمة القطاع في الناتج المحلي الإجمالي غير النفطي



ملحق (أ)

تصنيف المنتجات والحلول والخدمات في قطاع الأمن السيبراني

المستوى الأول

يوضح المستوى الأول التصنيف الأساسي لأنشطة سوق الأمن السيبراني كمنتجات وحلول، أو خدمات بحسب نماذج تقديمها.

1	2	3	4	5
منتجات وحلول الأمن السيبراني	خدمات الأمن السيبراني المهنية	خدمات التنفيذ التقني للأمن السيبراني	الخدمات المدارة للأمن السيبراني	خدمات التدريب وبناء القدرات في الأمن السيبراني

المستوى الثاني

يقسم كل فئة من فئات المستوى الأول إلى مجموعة من الأنشطة التفصيلية.

1	منتجات وحلول الأمن السيبراني
1-1	أمن الأجهزة الطرفية وإدارتها
1-2	أمن الشبكات
1-3	أمن البيانات
1-4	أمن التطبيقات
1-5	إدارة هويات الدخول والصلاحيات
1-6	الحوكمة والمخاطر والالتزام
1-7	الأمن المادي
1-8	حلول عمليات الأمن السيبراني
1-9	أمن الحوسبة السحابية
1-10	أمن الأنظمة الحساسة

2	**خدمات الأمن السيبراني المهنية**
1-2	الاستشارات الإدارية في الأمن السيبراني
2-2	تقييم الالتزام بالضوابط السيبرانية
3-1	تقييم المخاطر السيبرانية
4-1	التقييمات الفنية في الأمن السيبراني
5-1	الاستشارات التقنية في الأمن السيبراني
6-1	الاستجابة والتحقيق في الحوادث السيبرانية
3	**خدمات التنفيذ التقني للأمن السيبراني**
1-3	تطوير منتجات وحلول الأمن السيبراني
2-3	تكامل أنظمة الأمن السيبراني
4	**الخدمات المدارة للأمن السيبراني**
1-4	إدارة مركز عمليات الأمن السيبراني
2-4	حلول الأمن السيبراني كخدمة
3-4	الإسناد الخارجي للقوى العاملة في الأمن السيبراني
5	**خدمات التدريب وبناء القدرات في الأمن السيبراني**
1-5	التدريب في مجال الأمن السيبراني
2-5	التوعية في مجال الأمن السيبراني
3-5	اختبارات وشهادات الأمن السيبراني
4-5	الفعاليات والمسابقات في الأمن السيبراني

المستوى الثالث

يحدد المنتجات والحلول أو الخدمات في كل نشاط من أنشطة المستوى الثاني.

1	**منتجات وحلول الأمن السيبراني**	
1-1	**أمن الأجهزة الطرفية وإدارتها**	
حلول الأمن السيبراني لحماية الأجهزة الطرفية، بما يشمل الخوادم والأجهزة المكتبية والأجهزة المحمولة.		
1-1-1	حلول أمن المتصفح	حلول أمن الأجهزة الطرفية لتأمين متصفحات الويب، والمتصفحات المحلية الآمنة، ووظائف المتصفحات الإضافية
2-1-1	حلول أمن الأجهزة الطرفية	حلول أمن الأجهزة الطرفية لتأمين الأجهزة الشخصية والخوادم وغيرها، من خلال الكشف عن البرامج الضارة والفيروسات وبرمجيات حصان طروادة وبرمجيات الابتزاز وما إلى ذلك والوقاية منها
3-1-1	حلول الرصد والاستجابة لدى الأجهزة الطرفية (EDR)	حلول أمن الأجهزة الطرفية لإجراء تحليلات مباشرة للتهديدات والاحتواء والتحقيق والاستجابة
4-1-1	حلول حماية الأجهزة المحمولة	حلول أمن الأجهزة الطرفية والتطبيقات التي تحمي الأجهزة المحمولة وتطبيقاتها/بياناتها
5-1-1	حلول إدارة الأجهزة المحمولة (MDM)	حلول أمن الأجهزة الطرفية لإدارة وتطبيق السياسات المرتبطة بالأجهزة المملوكة للجهات وأجهزة الموظفين
6-1-1	حلول جدار الحماية للأجهزة	حلول أمن الأجهزة الطرفية التي تنشئ برمجيات جدار الحماية لحماية الأجهزة الطرفية من الاتصالات الخبيثة
7-1-1	حلول إدارة الإعدادات الأمنية	حلول أمن الأجهزة الطرفية لإدارة الإعدادات الأمنية للأجهزة الطرفية للجهات ومراقبتها
8-1-1	حلول إدارة الأصول	حلول أمن الأجهزة الطرفية المستخدمة في إدارة كافة الأصول على مستوى الجهة، بما يشمل اكتشاف الأصول وقاعدة بيانات إعدادات الأصول
9-1-1	حلول إدارة وإعداد حزم التحديثات والإصلاحات	حلول أمن الأجهزة الطرفية لتحديد الإصلاحات وترتيبها حسب الأولوية واختبارها وتطبيقها على مستوى الجهة
2-1	**أمن الشبكات**	
حلول الأمن السيبراني لحماية البنية التحتية الشبكات بدءًا من محيط الشبكة إلى الأجهزة الطرفية.		
1-2-1	أنظمة اكتشاف ومنع التسلل (IDPS)	حلول أمن الشبكات التي تفحص الحركة في الشبكة وتكشف المحتوى الضار و ترسل التنبيهات (للكشف فقط) واتخاذ الإجراءات مثل الحظر (الكشف والوقاية)
2-2-1	حلول التحكم بدخول الشبكات	حلول أمن الشبكات التي تتيح للجهات الوصول إلى شبكات الجهة عن طريق المصادقة والإعدادات وإذن الدخول حسب الدور والسياسات الأخرى
3-2-1	حلول جدار حماية الشبكات	حلول أمن الشبكات التي تستخدم القواعد لمراقبة الحركة الصادرة والواردة الضارة في الشبكة وحظرها، بما يشمل جدار الحماية الجيل القادم التي تتمتّع بخصائص متقدّمة مثل الفحص العميق للحزم
4-2-1	حلول بوابة الويب الآمنة (SWG)	حلول أمن الشبكات التي تعمل على تصفية حركة المستخدمين وتحظر المحتوى الضار أو غير المرغوب (مثل: المحتويات ضد سياسات الجهة)
5-2-1	حلول العزل والحماية من التهديدات المتقدمة المستمرة	حلول أمن الشبكات، المؤتمتة أو اليدوية، التي تسمح بتحليل المحتوى المريب في بيئةٍ معزولة

6-2-1	حلول الخوادم الوكيلة (Proxy)	حلول أمن الشبكات التي تكون بمثابة وسيط بين المستخدم وشبكة الإنترنت، بما يزيد الكفاءة والأمن والخصوصية
7-2-1	حلول مصائد الهجمات (Honeynets/honeypots)	حلول أمن الشبكات التي تُطرح بمثابة فخ لخداع المهاجمين للابتعاد عن الأصول القيّمة وإعطاء فرق الأمن الفرصة للتحقيق في الهجمات والتعامل معها
8-2-1	الحلول الموحدة لإدارة التهديدات (UTM)	حلول أمن الشبكات للمؤسسات الصغيرة والمتوسطة التي تضم عدة أقسام وظيفية، مثل جدار الحماية وتصفية المحتوى ومضاد الفيروسات وغير ذلك
9-2-1	حلول الحماية من هجمات حجب الخدمة الموزعة (DDoS)	حلول أمن الشبكات للكشف عن الهجمات الموزعة لحجب الخدمة التي تحاول إغراق شبكة الجهة والحد من توافرها لتلبية الطلبات الحقيقية، والحماية منها
3-1	**أمن البيانات**	
حلول الأمن السيبراني التي تتيح حماية البيانات والتي تغطي البيانات الثابتة والمتنقلة.		
1-3-1	حلول اكتشاف البيانات وتصنيفها	حلول أمن البيانات التي تحدد البيانات الحساسة وتصنفها حسب التصنيف الملائم
2-3-1	حلول منع فقدان البيانات (DLP)	حلول أمن البيانات المتاحة للأجهزة الطرفية والشبكات لمنع فقدان البيانات الحساسة أو تسريبها
3-3-1	حلول إخفاء البيانات وترميزها	حلول أمن البيانات التي تُسهّل حماية المعلومات الحساسة ضمن البيانات، إما باستبدالها برمز (الترميز) أو حجب أو إزالة البيانات الحساسة (الحجب)
4-3-1	حلول تشفير الأجهزة الطرفية وأنظمة إدارة المفاتيح (KMS)	حلول أمن البيانات التي تحمي البيانات الثابتة (مثل الملفات والمجلدات وغير ذلك) باستخدام التشفير لمنع الوصول غير المصرح به، وتتضمن أيضًا الأنظمة التي تدير مفاتيح التشفير (مثل الإنشاء والتوزيع والإتلاف وغيرها)
5-3-1	حلول تشفير الشبكات	حلول أمن البيانات التي تحمي البيانات المتنقلة، وتؤمن البروتوكولات الآمنة (SSL/TLS)
6-3-1	حلول أمن قواعد البيانات والتخزين	حلول أمن البيانات التي تحمي قواعد البيانات وحاويات التخزين الأخرى، بما يشمل المراقبة والتحكم في الوصول والتشفير والتدقيق وغير ذلك
7-3-1	حلول النقل الآمن للملفات	حلول أمن البيانات لمشاركة البيانات بشكلٍ آمن
8-3-1	بوابة البريد الإلكتروني الآمنة (SEG)	حلول أمن البيانات التي تفحص البريد الإلكتروني الوارد العشوائي والضار وتحجبه (للحماية من التهديدات المستمرة المتقدمة للبريد الإلكتروني)
9-3-1	حلول تقنيات تعزيز الخصوصية (PET)	حلول أمن البيانات لإدارة البيانات الشخصية وحمايتها على مدار دورة حياتها بما يشمل الالتزام والقبول والتحكم والتدقيق وغير ذلك
10-3-1	حلول إدارة الحقوق الرقمية (DRM)	حلول أمن البيانات المستخدمة في تقييد الوصول إلى المحتوى المحمي وإدارته
11-3-1	حلول الحماية من برمجيات الفدية	حلول أمن البيانات المُصممة والمُحزمة خصيصًا لمنع تهديدات برمجيات الابتزاز والكشف عنها والاستجابة لها

4-1	أمن التطبيقات	
حلول الأمن السيبراني التي تتيح الحماية على مستوى التطبيقات.		
1-4-1	حلول اختبار أمن التطبيقات (AST)	حلول أمن التطبيقات لتحليل التطبيقات واختبارها لتحديد الثغرات الأمنية بما يشمل اختبار أمن التطبيقات الثابتة (SAST)، واختبار أمن التطبيقات الديناميكية (DAST)، واختبار أمن التطبيقات التفاعلية (IAST)، وكشف الهجمات في الوقت الفعلي للتطبيقات (RASP)
2-4-1	حلول جدار حماية تطبيقات الويب (WAF)	حلول أمن التطبيقات التي تحمي تطبيقات الويب بفرز طلبات HTTP/S ومراقبتها للكشف عن الأنشطة الضارة
3-4-1	حلول التحكم في التطبيقات	حلول أمن التطبيقات لتحديد قائمة التطبيقات المعتمدة لاستخدامها في المنظمة وتقييد تنفيذ التطبيقات غير المعتمدة (بما يشمل القائمة البيضاء والقائمة السوداء للتطبيقات)
4-4-1	حلول أمن واجهة برمجة تطبيقات الويب (Web API)	حلول أمن التطبيقات لحماية واجهات برمجة تطبيقات الويب (Web API)، بهدف تأمين نقل البيانات عن طريق واجهات برمجة التطبيقات ومنع الهجمات الضارة على واجهات تطبيقات الويب أو إساءة استخدامها
5-1	**إدارة هويات الدخول والصلاحيات**	
حلول الأمن السيبراني التي تتيح حوكمة وإدارة الهويات الرقمية للتطبيقات ضمن بيئة تقنية المعلومات.		
1-5-1	حلول إدارة كلمات المرور	حلول أمن الهوية وإدارتها المستخدمة في تخزين بيانات اعتماد المستخدمين وإدارتها بشكلٍ آمن
2-5-1	حلول حوكمة الهويات	حلول أمن الهوية وإدارتها لإدارة هويات المستخدمين على مستوى المنظمة أو المنظومة، بما يشمل الهوية الرقمية الموحدة
3-5-1	حلول إدارة صلاحيات الدخول	حلول أمن الهوية وإدارتها والتي تتيح التحكم بالوصول عن طريق المصادقة المركزية وتسجيل الدخول لمرة واحدة (SSO) والدخول عن بعد وإدارة الجلسات وغير ذلك
4-5-1	حلول إدارة صلاحيات الدخول المميز (PAM)	حلول أمن الهوية وإدارتها لتأمين الوصول المتقدّم إلى الأصول الحساسة وإدارتها
5-5-1	حلول التحقق	حلول أمن الهوية وإدارتها والتي تتحقق من الهوية الرقمية للأفراد وتتيح الوصول إلى الحلول
6-5-1	حلول إدارة الشهادات الرقمية	حلول أمن الهوية وإدارتها لتخزين الشهادات الرقمية التي تصّدق هويات الأطراف الموثوقة، وتوقيعها وإصدارها
7-5-1	حلول الحوسبة عالية الثقة	حلول أمن الهوية وإدارتها التي تمكّن مستويات أعلى من الثقة، مثل: الحوسبة الموثوقة (TC)، الأمن المتعدد المجالات (CDS)، والحلول الأمنية المتعددة المستويات
8-5-1	حلول التحقق متعدد العناصر	حلول أمن الهويّة وإدارتها والتي تتيح عناصر مصادقة إضافية مثل الرموز المشفرة والخصائص الحيوية وغير ذلك

6-1	الحوكمة والمخاطر والالتزام	
حلول الأمن السيبراني التي تتيح تخطيط الحوكمة وإدارة المخاطر وإدارة الالتزام لبيئة تقنية المعلومات.		
1-6-1	حلول الحوكمة والمخاطر والالتزام (GRC)	حلول الحوكمة والمخاطر والالتزام لمتابعة المخاطر السيبرانية للمؤسسة وبرامج الالتزام ومسؤولياته، وإدارتها
2-6-1	حلول إدارة مخاطر الأطراف الخارجية (TPRM)	حلول الحوكمة والمخاطر والالتزام التي تحمي ضد مخاطر سلسلة الإمداد، بما يشمل تقييم مخاطر الموردين وحلول أمن إدارة الموردين
7-1	الأمن المادي	
حلول الأمن السيبراني التي تتيح الوصول الفعلي الآمن والأمن البيئي.		
1-7-1	حلول مصادقة الدخول المادي وإدارة الوصول	حلول الأمن المادي مثل البوابات الدوارة وقارئات الشارة والأقفال المادية لتقييد الوصول إلى المواقع الفعلية
2-7-1	حلول المراقبة البيئية والمادية	حلول الأمن المادي المستخدمة في مراقبة البيئات الفعلية بما يتضمن كاميرات المراقبة وأجهزة الاستشعار للمياه/الدخان/الحركة وغير ذلك
8-1	حلول عمليات الأمن السيبراني	
حلول الأمن السيبراني المستخدمة لتنفيذ أنشطة ومهام الأمن السيبراني اليومية.		
1-8-1	حلول الاكتشاف والاستجابة للشبكات (NDR)	حلول عمليات الأمن السيبراني باستخدام التحليلات الأمنية للكشف عن أي تهديدات للشبكة من جهات معروفة أو غير معروفة وتقليل مخاطرها
2-8-1	حلول تصيد التهديدات السيبرانية	حلول عمليات الأمن السيبراني التي تدعم الكشف الاستباقي للتهديدات النشطة والجهات التخريبية غير المعروفة مسبقًا
3-8-1	حلول التحقيق الجنائي الرقمي	حلول عمليات الأمن السيبراني لتحديد الأدلة الإلكترونية والحصول عليها وتحليلها واستكمال التحقيقات بالاستعانة بالحاسوب
4-8-1	حلول تحليل السلوكيات واكتشاف الحالات الشاذة	حلول عمليات الأمن السيبراني المستخدمة في الكشف عن الإجراءات المريبة استنادًا إلى السلوكيات المعيارية، بما يشمل الكشف عن الاحتيال والوقاية منه
5-8-1	حلول المسح وتقييم الثغرات	حلول عمليات الأمن السيبراني التي من شأنها تحديد الثغرات الأمنية وتصنيفها وإدارتها
6-8-1	حلول اختبار الاختراقات	حلول عمليات الأمن السيبراني للكشف عن نقاط الضعف التي يمكن استغلالها في الوضع الأمني، واختبارها وتصنيفها، مثل: رفع الامتيازات
7-8-1	حلول إدارة الحوادث والتنسيق الأمني والأتمتة والاستجابة (SOAR)	حلول عمليات الأمن السيبراني التي من شأنها تنسيق الاستجابة إلى الأحداث الأمنية وأتمتتها وإدارتها
8-8-1	حلول إدارة المعلومات والأحداث الأمنية (SIEM)	حلول عمليات الأمن السيبراني لجمع الأحداث وإدارة السجلات وتصحيح السجلات
9-8-1	حلول المعلومات الاستباقية عن التهديدات السيبرانية	حلول عمليات الأمن السيبراني لاستيعاب النوايا والأهداف وتقنيات الهجوم للجهات التخريبية، وتحليلها وفحصها، بما يشمل الاستخبارات القابلة للقراءة آليًا وبالعين مثل مؤشرات الاختراق (IoC)
10-8-1	أدوات التوعية والتدريب في مجال الأمن السيبراني	حلول عمليات الأمن السيبراني لصقل مهارات المستخدمين ومختصي الأمن السيبراني، مثل الحملات المضادة للتصيد الاحتيالي والنطاقات السيبرانية وغير ذلك

9-1	**أمن الحوسبة السحابية**	
حلول الأمن السيبراني التي تتيح حماية التطبيقات القائمة على الحوسبة السحابية.		
1-9-1	حلول وسطاء الأمان للوصول إلى السحابة (CASB)	حلول أمن الحوسبة السحابية لإضافة الضوابط الأمنية إلى خدمات الحوسبة السحابية وضمان التزام المستخدمين بسياسات استخدام الحوسبة السحابية
2-9-1	أمن الجهد السحابي	حلول أمن الحوسبة السحابية، التي تحمي الجهد أثناء التنقل بين بيئات الحوسبة السحابية المختلفة
10-1	**أمن الأنظمة الحساسة**	
حلول الأمن السيبراني التي تتيح حماية الأنظمة الحساسة والأنظمة الخاصة مثل التقنية التشغيلية (OT).		
1-10-1	حلول الأمن الصناعي	حلول أمن الأنظمة الحساسة لحماية أنظمة التحكّم الصناعية (ICS) والتقنية التشغيلية (OT)، بما يشمل واجهة المستخدم والآلة (HMI)، والتحكم الإشرافي وتحصيل البيانات (SCADA)، والبيانات والأمن السيبراني لأنظمة التحكم الموزعة (DCS)
2-10-1	حلول أمن إنترنت الأشياء والأجهزة المدمجة	حلول أمن الأنظمة الحساسة التي تحمي الأجهزة غير التقليدية والأحادية الغرض والمتصلة بالإنترنت ضد التهديدات
2	**خدمات الأمن السيبراني المهنية**	
1-2	**الاستشارات الإدارية في الأمن السيبراني**	
الخدمات المهنية في الأمن السيبراني لتحديد مجالات التحسين الاستراتيجية وتقديم التوصيات.		
1-1-2	تطوير استراتيجية الأمن السيبراني وخارطة الطريق	الخدمات الاستشارية في الأمن السيبراني لوضع استراتيجية الأمن السيبراني (مثل الرؤية والرسالة وغيرهما) وخارطة طريق التنفيذ
2-1-2	تطوير سياسات وعمليات وإجراءات الأمن السيبراني	الخدمات الاستشارية في الأمن السيبراني لوضع السياسات والعمليات والإجراءات وأطر العمل في الأمن السيبراني بما يتماشى مع استراتيجية الأمن السيبراني والمعايير الداخلية والخارجية للمنظمة
3-1-2	تطوير نموذج قدرات الأمن السيبراني	الخدمات الاستشارية في الأمن السيبراني لتطوير قدرات الأمن السيبراني في المنظمة بما يشمل الهيكل التنظيمي والأدوار والمسؤوليات والحوكمة وما إلى ذلك
4-1-2	اعتماد وشهادات الأمن السيبراني للمنظمات	الخدمات الاستشارية في الأمن السيبراني لاعتماد الجهة وفقاً لمعيار الاعتماد المعترف به خارجيًا وبناءً على تقييم الأمن السيبراني
5-1-2	إدارة المشاريع وإدارة التغيير في مجال الأمن السيبراني	الخدمات الاستشارية في الأمن السيبراني التي تقدم إدارة التغيير وإدارة المشاريع في الأمن السيبراني باعتبارها جزء من تنفيذ المنتج/الحل وتحديثه وجزء من التحوّل في الأمن السيبراني
2-2	**تقييم الالتزام بالضوابط السيبرانية**	
الخدمات المهنية في الأمن السيبراني لإجراء تقييمات الأمن السيبراني على مستوى حوكمة الجهة.		
1-2-2	تقييم سياسات وعمليات وإجراءات الأمن السيبراني	خدمات تقييم الأمن السيبراني لتحليل سياسات الجهة وعملياتها وإجراءاتها وأطر عملها في الأمن السيبراني وتحديد نقاط الضعف وفرص التحسين
2-2-2	تقييم نموذج قدرات الأمن السيبراني	خدمات تقييم الأمن السيبراني لتقييم قدرات الأمن السيبراني في الجهة بما يشمل الهيكل التنظيمي والأدوار والمسؤوليات والحوكمة وما إلى ذلك
3-2-2	تقييم نضج الأمن السيبراني	خدمات تقييم الأمن السيبراني لتقييم مدى نضج الأمن السيبراني في الجهة وفقاً لمعيار محدد وباستخدام نموذج تقييم النضج، مثل: تقييم مدى نضج الامتثال للضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني
4-2-2	تدقيق/تقييم الالتزام بضوابط الأمن السيبراني	خدمات تقييم الأمن السيبراني للتحقق من الامتثال للأنظمة أو المعايير الوطنية والعالمية الأخرى

3-2	تقييم المخاطر السيبرانية	
الخدمات المهنية في تقييم المخاطر التي يتم إجراؤها لتحديد مخاطر الأمن السيبراني وتحديد إجراءات معالجة التهديدات وعوامل تهديد الأمن.		
1-3-2	تمرين تقييم المخاطر السيبرانية	خدمات تقييم المخاطر لتحديد مخاطر الأمن السيبراني في الجهة وتقييمها وترتيبها حسب الأولوية
2-3-2	تطوير سجل مخاطر الأمن السيبراني	خدمات تقييم المخاطر لتوثيق المخاطر السيبرانية وإجراءات إدارة المخاطر في مستودع إدارة المخاطر
4-2	التقييمات الفنية في الأمن السيبراني	
الخدمات المهنية في الأمن السيبراني التي تُقيّم النواحي التقنية للبيئة.		
1-4-2	تقييم الثغرات	الخدمات التقنية في الأمن السيبراني لتحديد الثغرات وتصنيفها وترتيبها حسب الأولوية في حل أو منظومة محددة
2-4-2	اختبار الاختراقات	الخدمات التقنية في الأمن السيبراني للعثور على الثغرات القابلة للاستغلال في حل أو منظومة محددة وإظهارها بشكلٍ استباقي
3-4-2	مراجعة معمارية الأمن السيبراني	الخدمات الفنية في الأمن السيبراني لتقييم مدى اكتمال الحلول وبنية الأمن السيبراني
4-4-2	خدمات تصيد التهديدات السيبرانية وتقييم الاختراق	الخدمات الفنية في الأمن السيبراني لتحديد التهديدات غير المكتشفة إما بشكلٍ استباقي (تصيد التهديدات) أو تفاعلي (تقييم الاختراق) استجابةً إلى العثور على مؤشرات الاختراق (IoCs)
5-4-2	تمرين الفريق الأحمر (Red teaming)	الخدمات الفنية في الأمن السيبراني المستخدمة في هجمات المخترقون الأخلاقيون (الفريق الأحمر) على أنظمة الجهة، فيما يحاول مدافعو الجهة (الفريق الأزرق) الدفاع عن الشبكة
6-4-2	تقييم أمن التطبيقات	الخدمات الفنية في الأمن السيبراني لتحديد العيوب والثغرات الأمنية في التطبيقات، مثل مراجعة شفرة المصدر واختبار أمن التطبيقات وما إلى ذلك
7-4-2	خدمات برامج مكافأة اكتشاف الثغرات (bug bounty)	الخدمات التقنية للأمن السيبراني لتشغيل برنامج يحفّز المخترقين الأخلاقيين لإجراء تقييمات مستقلة والإفصاح المسؤول
8-4-2	مراجعة إعدادات الأمن السيبراني	الخدمات الفنية في الأمن السيبراني لمراجعة التكوين الأمني للأجهزة وتحديد التكوينات الخاطئة وفرص تعزيزها
9-4-2	التقييم السيبراني والاعتماد للحلول	الخدمات الفنية في الأمن السيبراني لتقييم الحل واعتماده وفقاً لمعايير اعتماد مُعترَف بها خارجياً
5-2	الاستشارات التقنية في الأمن السيبراني	
الخدمات المهنية في الأمن السيبراني لتقديم التوصيات التقنية والأنشطة الاستشارية التقنية.		
1-5-2	تصميم معمارية الأمن السيبراني	الخدمات الفنية في الأمن السيبراني لتصميم البنية الأمنية للجهة باستخدام أفضل الممارسات ومبادئ التصميم الآمن
2-5-2	تطوير المعايير الفنية للأمن السيبراني	الخدمات الفنية للأمن السيبراني لوضع معايير قابلة للتنفيذ ومخصصة في الأمن السيبراني تتوافق مع معايير القطاع، بما يشمل وضع الحد الأدنى من المعايير الأمنية الأساسية (MBSS)
3-5-2	تطوير الخطة الفنية للأمن السيبراني	الخدمات الفنية في الأمن السيبراني لإعداد الخطط والعمليات التفصيلية، مثل استرداد البيانات الهامة وخطة استمرارية الأعمال وخطة التخفيف من المخاطر والثغرات وخطة الاستجابة للأحداث وغير ذلك
4-5-2	خدمات المعلومات الاستباقية عن التهديدات السيبرانية	الخدمات الفنية في الأمن السيبراني لتقديم المعلومات والتقارير لاستيعاب النوايا والأهداف وتقنيات الهجوم للجهات التخريبية وعوامل التهديدات (بما يشمل (Dark Web) والعلامة التجارية ومراقبة التهديدات الإلكترونية)، وتحليلها وفحصها

6-2	**الاستجابة والتحقيق في الحوادث السيبرانية**	
الخدمات المهنية في الأمن السيبراني لتحليل ومعالجة الحوادث والاختراقات في الأمن السيبراني.		
1-6-2	الاستجابة للحوادث السيبرانية	خدمات الاستجابة لحوادث الأمن السيبراني لمساعدة الجهات في إدارة حوادث الأمن السيبراني وتحليلها واحتوائها ومعالجتها والتعلّم منها
2-6-2	التحليل الجنائي في الأمن السيبراني	خدمات التحقيق الجنائي في حوادث الأمن السيبراني للحفاظ على الأدلة وتحليل تقنيات الجهات التخريبية وعوامل التهديدات (مثل: تحليل البرامج الضارة)
3	**خدمات التنفيذ التقني للأمن السيبراني**	
1-3	**تطوير منتجات وحلول الأمن السيبراني**	
خدمات الأمن السيبراني لتطوير منتجات الأمن السيبراني وحلوله.		
1-1-3	تطوير منتجات وحلول الأمن السيبراني	الخدمات الفنية للأمن السيبراني لتطوير منتجات وحلول مخصصة للأمن السيبراني لموردي الخدمات التقنية (مثل: منتجات العلامة البيضاء) والحكومات وغيرها من المستخدمين المتقدمين
2-3	**تكامل أنظمة الأمن السيبراني**	
خدمات الأمن السيبراني المقدمة من مورّدي الأمن السيبراني ومورّدي تقنية المعلومات وشركات تكامل الأنظمة لتنفيذ حل الأمن السيبراني أو إعداده.		
1-2-3	متطلبات الأمن السيبراني لتنفيذ الحلول	الخدمات الفنية للأمن السيبراني لتحديد متطلبات الأمن السيبراني لمنتجات أو حلول الأمن السيبراني الجديدة ولتنفيذ منتج أو حل الأمن السيبراني
2-2-3	معمارية وتصميم حلول الأمن السيبراني	الخدمات الفنية في الأمن السيبراني لتصميم بنية الأمن السيبراني للحل قبل تنفيذه باستخدام أفضل الممارسات ومبادئ التصميم الآمن (بما يشمل التصميم العام والتفصيلي)
3-2-3	تنفيذ وإعداد وتكامل حلول الأمن السيبراني	الخدمات الفنية في الأمن السيبراني لتنفيذ حلول الأمن السيبراني وإعدادها ودمجها ضمن بيئة الجهة بما يشمل عقود الصيانة والدعم للمنتج أو الحل

4	الخدمات المدارة للأمن السيبراني	
1-4	**إدارة مركز عمليات الأمن السيبراني**	
مراقبة الأمن السيبراني وتحديد التهديدات وتصعيد الحوادث.		
1-1-4	مراقبة الأمن السيبراني	إدارة خدمات مركز العمليات الأمنية المُدارة التي تُركّز على مراقبة تنبيهات الأمن السيبراني عن بعد من حلول الأمن السيبراني
2-1-4	خدمات الرصد والاستجابة المُدارة (MDR)	خدمات مركز العمليات الأمنية المُدارة للكشف عن أحداث الأمن السيبراني وفرزها والتحقيق فيها حال حدوثها وكذلك الاستجابة إلى الحوادث البسيطة والحد منها
2-4	**حلول الأمن السيبراني كخدمة**	
خدمات الأمن السيبراني المتصلة بالإسناد الخارجي لحلول الأمن السيبراني، بما يشمل إدارة الحلول والعمليات.		
1-2-4	حلول الأمن السيبراني كخدمة	خدمات الإسناد الخارجي في الأمن السيبراني التي تتيح التحكم في العمليات اليومية وتنفيذ حلول الأمن السيبراني بما في ذلك إدارة الحلول والعمليات، باستثناء مركز العمليات الأمنية المُدارة، والاستجابة إلى الحوادث
3-4	**الإسناد الخارجي للقوى العاملة في الأمن السيبراني**	
خدمات الأمن السيبراني المتصلة بإسناد القوى العاملة في الأمن السيبراني إلى الجهات.		
1-3-4	الإسناد الخارجي للقوى العاملة في الأمن السيبراني	خدمات الإسناد الخارجي في الأمن السيبراني التي تقدم المتعاقدين لسد النقص في موظفين الأمن السيبراني في الجهة، باستثناء أنشطة الاستجابة إلى الحوادث

5	**خدمات التدريب وبناء القدرات في الأمن السيبراني**	
1-5	**التدريب في مجال الأمن السيبراني**	
تقديم دورات تدريبية وورش عمل في الأمن السيبراني لموظفي الأمن السيبراني وغيرهم.		
1-1-5	التدريب الأكاديمي في الأمن السيبراني	خدمات التدريب في الأمن السيبراني التي تُركّز على المفاهيم والنظرية والإدارة في الأمن السيبراني
2-1-5	التدريب الفني في الأمن السيبراني	خدمات التدريب في الأمن السيبراني التي تركّز على الخبرات العملية في الأمن السيبراني بالأدوات والتقنيات التطبيقية
3-1-5	تمارين وعمليات المحاكاة في الأمن السيبراني	خدمات التدريب في الأمن السيبراني التي تُركّز على التدريب على نهج الكشف عن حوادث الأمن السيبراني والاستجابة لها ومعالجتها
2-5	**التوعية في مجال الأمن السيبراني**	
تقديم الدورات التوعوية وورش عمل لموظفي الأمن السيبراني وغيرهم.		
1-2-5	تطوير محتوى التوعية في مجال الأمن السيبراني	خدمات التوعية بالأمن السيبراني التي تُركّز على إنشاء المحتويات المخصصة لتحسين مستوى الوعي والفهم لدى الموظفين والعملاء وغيرهم في موضوع الأمن السيبراني
2-2-5	الدورات التدريبية وورش العمل للتوعية في مجال الأمن السيبراني	خدمات التوعية بالأمن السيبراني التي تُركّز على تقديم الدورات التوعوية المباشرة أو عن بعد في الأمن السيبراني للموظفين والعملاء وغيرهم
3-5	**اختبارات وشهادات الأمن السيبراني**	
إجراء الاختبارات وتقديم الشهادات في الأمن السيبراني للأفراد.		
1-3-5	اختبارات الأمن السيبراني للأفراد	خدمات إجراء الاختبارات في الأمن السيبراني لاختبار معارف الطلاب والمتخصصين في الأمن السيبراني ومهاراتهم وكفاءاتهم
2-3-5	الشهادات الاحترافية في الأمن السيبراني للأفراد	خدمات الاعتماد في الأمن السيبراني للتحقق من التدريب أو الخبرات واعتماد الأفراد من خلال تقديم شهادات معترف بها في الأمن السيبراني (بما يشمل الشهادات المعادلة)
4-5	**الفعاليات والمسابقات في الأمن السيبراني**	
إقامة الفعاليات والمسابقات في الأمن السيبراني للجهات.		
1-4-5	الفعاليات في الأمن السيبراني	خدمات الأمن السيبراني لتخطيط الفعاليات والمؤتمرات والمنتديات في الأمن السيبراني وتنظيمها وتنفيذها
2-4-5	المسابقات والتحديات في مجال الأمن السيبراني	خدمات الأمن السيبراني التي من شأنها التخطيط لمسابقات الأمن السيبراني وتنظيمها وإجراءها مثل الهاكاثونات ومسابقات الأمن السيبراني (CTF)

إخلاء المسؤولية

عملت الهيئة الوطنية للأمن السيبراني ومجموعة بوسطن الاستشارية (BCG) ومؤسسة البيانات الدولية (IDC)، على تطوير نموذج مخصص لتحليل ودراسة سوق الأمن السيبراني في المملكة واختباره والتحقق من صحة نتائجه. وإن جميع المعلومات المشمولة في هذا التقرير - المُعد وفقاً للنموذج المشار إليه أعلاه - هي معلومات عامة ولأغراض إرشادية فقط. وتحرص الهيئة الوطنية للأمن السيبراني ومجموعة بوسطن الاستشارية (BCG) ومؤسسة البيانات الدولية (IDC) على التأكد من دقة وصحة محتوى التقرير، إلا أنها لا تقدم أي إقرارات أو تعهدات من أي نوع كان سواء بشكل صريح أو ضمني، فيما يتعلق باكتمال، أو دقة، أو موثوقية، أو ملاءمة محتوى التقرير سواء كانت في هيئة نصوص أو تحليلات أو رسومات أو غير ذلك ولأي غرض كان. إن أي اعتماد على محتوى التقرير يكون بشكل تام على مسؤولية الجهة المتعاملة به -أياً كانت- ولا تتحمل الهيئة الوطنية للأمن السيبراني ومجموعة بوسطن الاستشارية (BCG) ومؤسسة البيانات الدولية (IDC) أي التزام أو مسؤولية من أي نوع عن أي أخطاء أو سهو في محتوى التقرير، كما أنها غير مسؤوله عن أي نوع من العواقب ذات صلة بمحتواه والذي يعد عرضة للتغيير في أي وقت ودون إشعار مسبق.

حقوق الملكية

الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority