

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

تقرير حول

أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني

لعام 2026م

إشارة المشاركة: أبيض

تصنيف الوثيقة: عام

بالتعاون مع:

BCG IDC

بسم الله الرحمن الرحيم

بروتوكول إشارة المشاركة (TLP):

يستخدم هذا البروتوكول 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 او خارج الجهة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

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

أخضر – مشاركة في نفس المجتمع

المستلم يمكنه مشاركة المعلومات مع آخرين في نفس الجهة أو جهة أخرى على علاقة معهم أو في نفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

المحتويات

الملخص التنفيذي 6

مقدمة 7

كلمة شركاء إعداد التقرير 8

1 المنهجية 10

1.1 تصنيف المنتجات والخدمات في قطاع الأمن السيبراني 10

2.1 جمع البيانات 12

3.1 ضمان الجودة 12

4.1 تحليل البيانات 12

5.1 إعداد المخرجات 13

أبرز النتائج 14

2 أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني 18

1.2 سوق الأمن السيبراني 18

1.1.2 حجم السوق 18

2.1.2 الإنفاق حسب حجم الجهات 19

3.1.2 حجم السوق حسب تصنيفات منتجات وخدمات الأمن السيبراني 20

4.1.2 التوزيع الجغرافي لجانبي الطلب والعرض 20

5.1.2 مقدمي منتجات وخدمات الأمن السيبراني 21

2.2 مساهمة قطاع الأمن السيبراني في الناتج المحلي الإجمالي 22

3 أبرز مؤشرات القوى العاملة في قطاع الأمن السيبراني 24

1.3 حجم كوادر الأمن السيبراني 24

2.3 مشاركة المرأة 25

3.3 التعليم في الأمن السيبراني 25

الخاتمة 26

ملحق (أ) 27

تصنيف المنتجات والخدمات في قطاع الأمن السيبراني

الملخص التنفيذي

تُعد الهيئة الوطنية للأمن السيبراني، وفق تنظيمها الصادر بالأمر الملكي رقم (6801) في 1439/2/11هـ الجهة المختصة في المملكة العربية السعودية بالأمن السيبراني والمرجع الوطني في شؤونه. وتهدف الهيئة إلى تعزيزه؛ حمايةً 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. وبهدف فهم الوضع الراهن لقطاع الأمن السيبراني في المملكة؛ أعدت الهيئة الوطنية للأمن السيبراني بالتعاون مع مجموعة بوسطن الاستشارية (BCG)، ومؤسسة البيانات الدولية (IDC) هذا التقرير السنوي الثالث، الذي يشمل نتائج دراسة البيانات وتحليلها التي جرى جمعها لعام 2025م، كما يقارن النتائج مع الإحصاءات الواردة في التقريرين السابقين. ويقدم التقرير تحليلًا مفصلًا عن قطاع الأمن السيبراني، ويحدد العوامل الأساسية في توجيه المبادرات، والبرامج المستقبلية، في سبيل تعزيز النمو، والمساعدة في الحفاظ على مكانة المملكة عالميًا في مجال الأمن السيبراني.

ينقسم التقرير إلى ثلاثة أقسام رئيسة:

1. المنهجية: يوضح هذا القسم تفاصيل إطار العمل المستخدم لدراسة السوق، وأساليب جمع البيانات، وإجراءات التأكد من مستوى دقة البيانات، والتحقق من صحتها، بالإضافة إلى الأدوات التحليلية المستخدمة لاستخلاص المخرجات.

2. أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني:
يستعرض هذا القسم نظرة اقتصادية عن قطاع الأمن السيبراني في المملكة، وتقييم حجم السوق الذي بلغ (16.3) مليار ريال سعودي، وتوزيع الإنفاق حسب القطاعات، إذ يشكل إنفاق منشآت القطاع الخاص (69%) من حجم السوق، في حين يشكل إنفاق الجهات الحكومية (31%). كما يستعرض التقرير التوزيع الجغرافي لجانبي العرض والطلب، ومقدمي منتجات وخدمات الأمن السيبراني المسجلين لدى الهيئة، البالغ (473) منشأة، بالإضافة إلى مساهمة قطاع الأمن السيبراني في الناتج المحلي الإجمالي بالأسعار الجارية والتي بلغت (20) مليار ريال سعودي؛ وهو ما يمثل (0.42%) من الناتج المحلي الإجمالي و(0.71%) من الناتج المحلي للأنشطة غير النفطية.

3. أبرز مؤشرات القوى العاملة في قطاع الأمن السيبراني:
يقدم هذا القسم حجم القوى العاملة في القطاع. وقد أظهرت الدراسة استمرار نمو عدد الكفاءات السيبرانية في المملكة؛حيث بلغ عدد مختصي الأمن السيبراني العاملين في القطاع أكثر من (22) ألف مختص، تشكل نسبة الإناث منهم (33%)، مما يعكس جهود المملكة في ترسيخ الشمولية نحو توسيع قاعدة الكفاءات العاملة في القطاع.

إشارة المشاركة: أبيض | تصنيف الوثيقة: عام



مقدمـــة

يشهد قطاع الأمن السيبراني في المملكة نموًا وتطورًا حيويًا ملحوظًا، وهو ما تؤكده المؤشرات الدولية؛ إذ حافظت المملكة على المرتبة الأولى عالميًا في مؤشر الأمن السيبراني للعام الثالث على التوالي، ضمن تقرير (الكتـــاب الســـنـــوي للتنافســـيـــة العالميـــة للعـــام 2026م) الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية بسويسرا (IMD)؛ وذلك استمرارًا لما تحقق في عامي 2024م و 2025م. ويأتي هذا الترتيب ترسيخًا لموقع المملكة الرائد والمتقدم في هذا القطاع الحيوي والواعد؛ إذ سبق وأن أكدته مؤشرات دولية أخرى، ومنها تصنيف المملكة أنموذجًا رائدًا في الفئة الأعلى (Role-Modelling) في المؤشر العالمي للأمن السيبراني 2024م، الصادر عن منظمة الأمم المتحدة عبر وكالتها المتخصصة بتكنولوجيا المعلومات والاتصالات (ITU).

ويبرز في ذلك النموذج السعودي في الأمن السيبراني بوصفه أنموذجًا معياريًا للتميز؛ بما نتج عنه من تحسينات اقتصادية وأمنية، فهو شمولي في تناوله لمجالات الأمن السيبراني التشريعية، والأمنية، والاقتصادية. ويرتكز هذا النموذج على المركزية في حوكمة الأمن السيبراني على المستوى الوطني؛ شاملة أعمال التقييم، والاستجابة وبناء القدرات الوطنية، واللامركزية في التشغيل والذي يعد من مسؤولية الجهات الوطنية.

ويسهم النموذج السعودي في فهم وإدارة المشهد السيبراني الوطني بأكمله؛ بما يعظم من مكاسب المملكة، ويرتقي بمكانتها الدولية، ويمكّن الجهات الوطنية في الوقت نفسه من القيام بمهماتها واختصاصاتها، ورفع جاهزيتها التشغيلية.

وبناءً على منهجية الدراسة السنوية التي تجريها الهيئة الوطنية للأمن السيبراني، تم تطبيق الإطار البحثي القائم على الأدلة؛ لإعداد التحليل الاقتصادي السنوي الرابع للقطاع في المملكة، بالتعاون مع مجموعة بوسطن الاستشارية (BCG)، ومؤسسة البيانات الدولية (IDC). وتتّبع الدراسة أفضل الممارسات العالمية في اختيار العينات والتحقق، والنمذجة الاقتصادية، وحققت مستوى ثقةٍ إحصائيًا يتجاوز (98%) وبهامش خطأ يبلغ حوالي (3.5%). وفي هذا السياق، تسلّط المرئيات المستخلصة الضوء على هيكلية السوق، والمساهمة في الناتج المحلي الإجمالي، ودور القوى العاملة في تنمية القطاع.

كلمة شركاء إعداد التقرير

رسّخت المملكة واحدةً من أكثر منظومات الأمن السيبراني تنظيمًا وأسرعها نضجًا عالميًا، مستندةً في ذلك إلى النموذج الذي تتبناه الهيئة الوطنية للأمن السيبراني في حوكمة الأمن السيبراني، وتنمية القدرات، وتمكين المنظومة. وهيأت المملكة المقومات اللازمة للنمو المستدام لقطاع الأمن السيبراني من خلال توفير ضوابط الأمن السيبراني، والأطر التنظيمية بهدف تعزيز قدرات الجهات الوطنية في مواجهة التهديدات السيبرانية.

وعلى مدى الأعوام الثلاثة الماضية، تعاونت الهيئة الوطنية للأمن السيبراني، مع مجموعة بوسطن الاستشارية (BCG)، ومؤسسة البيانات الدولية (IDC)، لتنفيذ دراسة سنوية لقطاع الأمن السيبراني في المملكة. وقد أسهم استمرار هذا التعاون في بناء سلسلة بيانات متسقة ومتجانسة، تُمكّن من تتبع التغيرات خلال سنوات الدراسة ورصد الاتجاهات طويلة المدى، مثل معدل النمو السنوي المركب (CAGR)، كما توفر هذه القاعدة المرجعية قياسًا دقيقًا للأثر الاقتصادي والتنموي للقطاع في المملكة، وتعزيز موثوقية التنبؤات المستقبلية، مما يدعم اتخاذ قرارات إستراتيجية مبنية على الأدلة والبيانات.

كما أسهم التعاون بين الهيئة الوطنية للأمن السيبراني والجهات الحكومية، والمؤسسات الأكاديمية، ومقدمي منتجات وخدمات الأمن السيبراني، والقطاع الخاص، في دعم التطور المستمر لمنظومة الأمن السيبراني في المملكة. وقد عززت هذه الجهود تنمية القوى العاملة، وشجعت الابتكار، ووسعت القدرات المحلية، ودعمت نمو صناعة وطنية واعدة للأمن السيبراني، تساهم في تحقيق المستهدفات الوطنية للتنوع الاقتصادي.

وفي ضوء هذه المعطيات، ومن خلال التحليل الاقتصادي الشامل ضمن أعمال الدراسة السنوية، يقدم هذا التقرير نظرة شاملة على قطاع الأمن السيبراني من خلال ثلاثة أبعاد مترابطة، تمثّل سوق الأمن السيبراني، ومساهمة القطاع في الناتج المحلي الإجمالي، والقوى العاملة فيه. ويهدف التقرير إلى تزويد متخذي القرار، والمستثمرين، وكافة الجهات الفاعلة والمختصين في منظومة الأمن السيبراني بقاعدة مشتركة من البيانات والحقائق، تدعم اتخاذ القرارات، وتعزز استدامة تطور قطاع الأمن السيبراني في المملكة.

ومن المتوقع أن يواصل قطاع الأمن السيبراني مساره التصاعدي بوصفه أولوية إستراتيجية وأحد روافد الأمن الوطني، مدفوعًا بتنامي المخاطر السيبرانية عالميًا، بالإضافة إلى الفرص الاقتصادية التي يوفرها كأحد القطاعات الاقتصادية الواعدة. وبذلك يساهم قطاع الأمن السيبراني بشكل مباشر في تحقيق رؤية السعودية 2030، من خلال بناء صناعة سيبرانية وطنية متكاملة، وتعزيز الابتكار وريادة الأعمال.

شركاء إعداد التقرير:

BCG IDC

إشارة المشاركة: أبيض | تصنيف الوثيقة: عام





1 المنهجية

استخدمت الهيئة الوطنية للأمن السيبراني الإطار البحثي، الذي أعدته سابقًا، لتقديم نظرة شاملة عن قطاع الأمن السيبراني في المملكة. وبدأت الدراسة من خلال ربط سلسلة القيمة بأكملها، بالتصنيف الذي أعدته الهيئة من ثلاثة مستويات، تمثل (5) فئات شاملة، و(25) مجموعة أنشطة، و(100) نوعًا من المنتجات والخدمات.

وباستخدام هذا التصنيف؛ عمل فريق الدراسة على إنشاء مجموعات بيانات أساسية عن قطاع الأمن السيبراني في المملكة، مستمدة من أصحاب المصلحة. وتشمل هذه المجموعات بيانات الأمن السيبراني للجهات الحكومية، ومنشآت القطاع الخاص ذات البنى التحتية الحساسة، وبقية منشآت القطاع الخاص على اختلاف أحجامها وأنشطتها، بالإضافة إلى مقدمي منتجات وخدمات الأمن السيبراني، والمؤسسات التعليمية، والمتخصصين في مجال الأمن السيبراني. وجرى استخدام ضوابط متعددة لجودة البيانات لتدقيق كل مدخل؛ بما فيها عمليات التحقق من العينات، واختبارات القيم الاستثنائية، والمطابقة مع الإحصاءات الرسمية. وهذه الإجراءات أدت إلى تحقيق مستوى ثقة إحصائي يزيد على (98%) بهامش خطأ (3.5%)، وهو أعلى من المعايير المعتادة لمثل هذه الدراسة.

وجرى تحليل البيانات المعالجة من خلال مجموعة نماذج تشغيلية واقتصادية، بالمواءمة مع منهجية الهيئة العامة للإحصاء وشركاء الأبحاث الرائدين عالميًا.

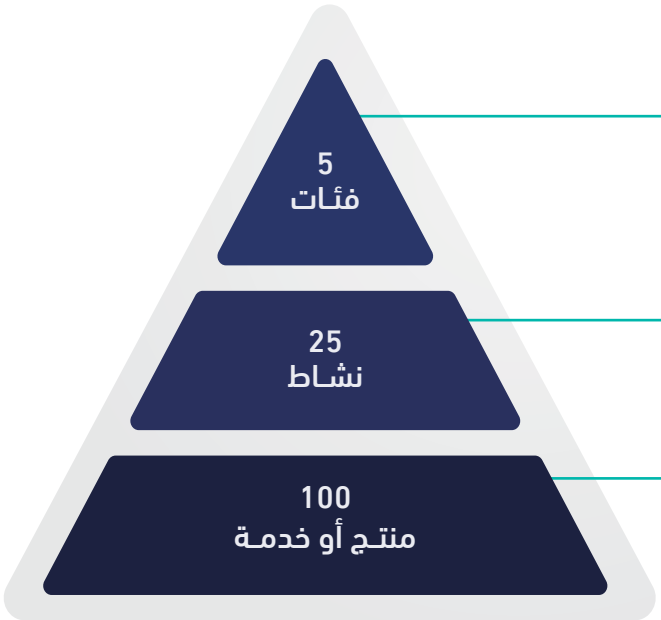
وقد استخلصت هذه النماذج (التي تقيس حجم الإيرادات، وحجم الطلب، وحجم القوى العاملة، والمساهمة في الناتج المحلي الإجمالي) أبرز المؤشرات الواردة في هذا التقرير، مما يضمن دقتها الإحصائية وإمكانية تتبعها ومقارنتها بشكل سنوي.

1.1 تصنيف المنتجات والخدمات في قطاع الأمن السيبراني

جرى تطوير تصنيف شامل للمنتجات والخدمات في قطاع الأمن السيبراني (الملحق أ)؛ بالتعاون مع العديد من المؤسسات البحثية، وشركات تحليل سوق الأمن السيبراني الرائدة. وتم تقييم العديد من الشركات العالمية ومقدمي منتجات وخدمات الأمن السيبراني، بغرض تغطية تفاصيل قطاع الأمن السيبراني على نحوٍ شامل ومرن؛ يجري تحديثه عند الحاجة؛ لعكس التطور في السوق وتقنياته. وقد اشتمل تصنيف المنتجات والخدمات في قطاع الأمن السيبراني، على (100) منتج وخدمة، جرى تقسيمها إلى ثلاثة مستويات، كما هو موضح في الشكل الآتي.



مستويات تصنيف منتجات وخدمات الأمن السيبراني



المستوى الأول

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

المستوى الثاني

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

المستوى الثالث

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



2.1 جمع البيانات

بدأت الدراسة بتحديد رؤية شاملة لمشهد الأمن السيبراني في المملكة؛ من خلال إشراك جميع فئات أصحاب المصلحة. وجرى جمع البيانات في الجهات الحكومية، ومنشآت القطاع الخاص التي تملك أو تشغّل أو تستضيف البنى التحتية الحساسة، والمنشآت الأخرى في القطاع الخاص بمختلف الأحجام، والأنشطة، ومقدمي منتجات وخدمات الأمن السيبراني، والمختصين العاملين في مجال الأمن السيبراني والمؤسسات التعليمية. وقد قام فريق الدراسة بنشر استبيان وطني مدعوم بجلسات مركّزة للنقاش، بالإضافة إلى المقابلات الشخصية.

وقد نتج عن ذلك إعداد مجموعة بيانات أساسية؛ تضم إفادات جرى التحقق منها، وتغطي الجهات المعنية بجانب الطلب، والمنشآت المعنية بجانب العرض المسجلة لدى الهيئة الوطنية للأمن السيبراني، والمؤسسات التعليمية، والمختصين في مجال الأمن السيبراني. وقد أفضى حجم المشاركة إلى تحقيق مستوى ثقة إحصائي يزيد على (98%) بهامش خطأ قدره (3.5%)، ليتجاوز معايير الدراسات المشابهة.

3.1 ضمان الجودة

اشتملت هذه الخطوة على تطبيق عدة معايير لتجويد البيانات تتسق مع المعايير الدولية، والضوابط والمواصفات الصادرة من مكتب إدارة البيانات الوطنية التابع للهيئة السعودية للبيانات والذكاء الاصطناعي؛ بدءًا من جمع البيانات ووصولًا إلى نمذجتها. وتضمنت تلك المعايير استخدام عمليات التحقق الآلي، والمراجعات اليدوية؛ للكشف عن القيم الاستثنائية، وغيرها من المعايير. كما تم عقد عدد من جلسات المتابعة، التي أجريت مع المشاركين في الاستبيان، والمقابلات مع الخبراء على مستوى قطاع الأمن السيبراني؛ للتحقق من صحة النتائج، واختبار المرئيات؛ بهدف ضمان دقة مخرجات الدراسة مما يمنح الثقة لصناع القرار، والمستثمرين، ورواد الأعمال.

%98
مستوى الثقة الإحصائي

%3.5
هامـــش الخطـــأ

ضمنت المنهجية مستوى ثقة إحصائي عالي، وهامش خطأ محدود؛ نتيجة ارتفاع حجم المشاركة في الدراسة

4.1 تحليل البيانات

استُخدمت البيانات المعالجة في تطوير النماذج الإحصائية والاقتصادية؛ لاستخلاص المؤشرات والمرئيات النوعية لقطاع الأمن السيبراني في المملكة. وجرى من خلال



هذه النماذج قياس حجم الإنفاق على منتجات وخدمات الأمن السيبراني من قبل الجهات الحكومية، ومنشآت القطاع الخاص ذات البنى التحتية الحساسة، وبقية منشآت القطاع الخاص بمختلف أحجامها وأنشطتها. كما جرى تحليل إيرادات مقدمي منتجات وخدمات الأمن السيبراني، والاستفادة من مدخلات الخبراء والمختصين المحليين والدوليين في هذا المجال، واستخدام الأدلة السياقية، والمقارنات المعيارية الدولية، ومجموعات البيانات الرسمية من وزارة الموارد البشرية والتنمية الاجتماعية، والهيئة العامة للإحصاء، والهيئة العامة للمنشآت الصغيرة والمتوسطة؛ وذلك لتأكيد مخرجات النماذج.

كما تم استخدام النمذجة الاقتصادية بالمواءمة مع منهجية الهيئة العامة للإحصاء؛ لتقدير مساهمة القطاع في الناتج المحلي الإجمالي، ومن ثم تحديد الأثر الاقتصادي للقطاع في المملكة، مع الأخذ في الحسبان إيرادات مقدمي المنتجات والخدمات، وضرائب الشركات، والدعم المقدم لها، ودخل العاملين في المجال. وتم استخدام جداول المدخلات والمخرجات الاقتصادية؛ لتقدير الآثار المباشرة وغير المباشرة للأعمال في قطاع الأمن السيبراني في المملكة.

ولهدف تحليل ومقارنة معدل التغيير على المؤشرات خلال الثلاث أعوام الماضية، تم احتساب معدل النمو السنوي المركب باستخدام بيانات عام 2023م كخط أساس.

5.1 إعداد المخرجات

تم استخراج مرئيات نوعية عن سوق الأمن السيبراني في المملكة، ومساهمته الاقتصادية، استنادًا إلى نتائج النماذج الإحصائية والاقتصادية. ومن أبرز هذه المرئيات حجم السوق، مساهمة القطاع بالناتج المحلي الإجمالي، وكوادر الأمن السيبراني في المملكة.



مساهمة قطاع الأمن السيبراني في الناتج المحلي الإجمالي



حجم سوق الأمن السيبراني



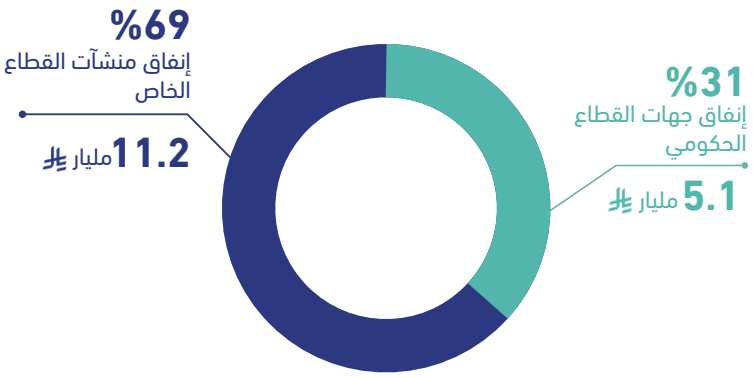
كوادر الأمن السيبراني

*قد لا تتطابق بعض المجاميع والنسب المئوية الواردة في هذا التقرير بشكل دقيق وذلك بسبب تقريب الأعداد.

أبــرز النتائــج

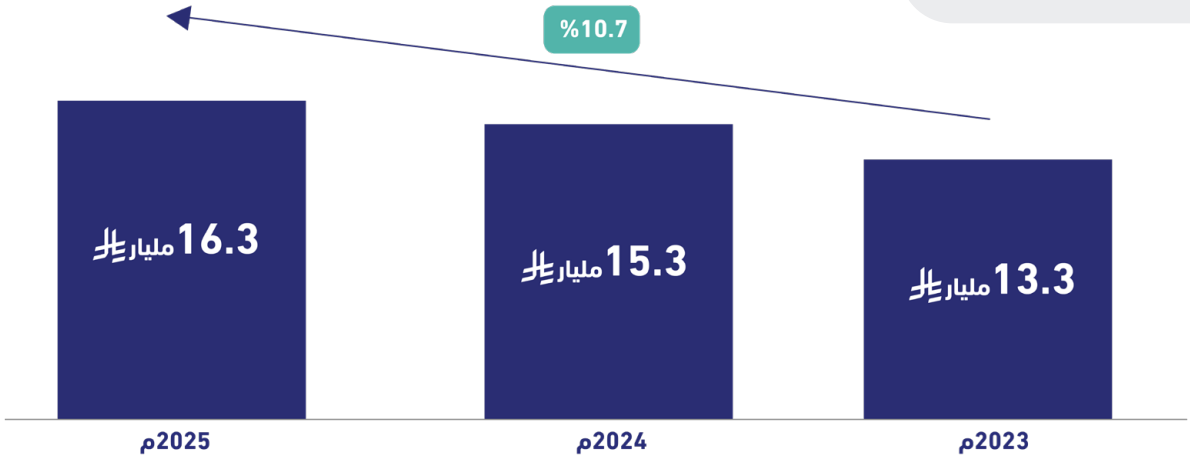
حجم سوق الأمن السيبراني في المملكة

16.3 مليار ﷼



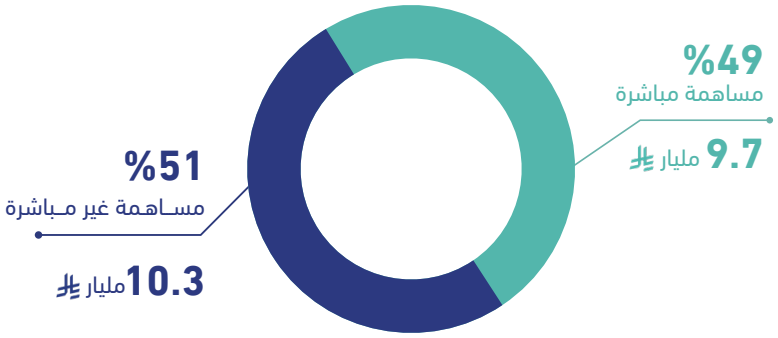
معدل النمو السنوي المركب لحجم السوق

%10.7



إشارة المشاركة: أبيض | تصنيف الوثيقة: عام

المساهمة في الناتج المحلي بالأسعار الجارية



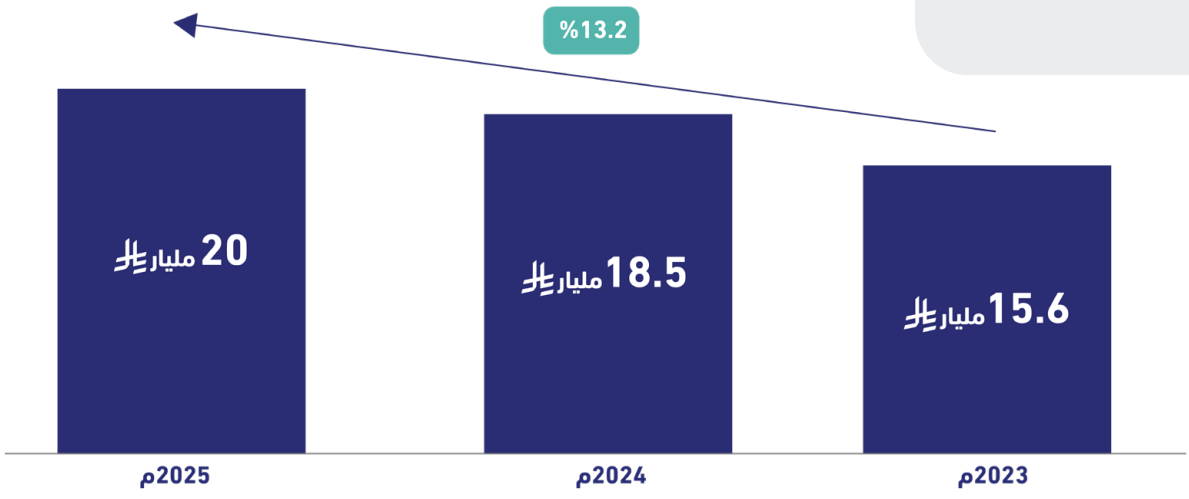
20 مليار ﷼

%0.42
مساهمة القطاع في الناتج المحلي الإجمالي

%0.71
مساهمة القطاع في الناتج المحلي للأنشطة غير النفطية

معدل النمو السنوي المركب لمساهمة القطاع في الناتج المحلي الإجمالي

%13.2



مقدمو منتجات وخدمات الأمن السيبراني المسجلين لدى الهيئة الوطنية للأمن السيبراني:

473
منشأة مسجلة

19	83	187	184
منشأة كبيرة	منشأة متوسطة	منشأة صغيرة	منشأة متناهية الصغر

توزيع الإيرادات حسب حجم منشآت مقدمي المنتجات والخدمات:

الفئة الصغرى		الفئة الكبرى	
المنشآت متناهية الصغر	المنشآت الصغيرة	المنشآت المتوسطة	المنشآت الكبيرة
%0.8	%12.5	%51.0	%35.7

أبرز منتجات وخدمات الأمن السيبراني في المملكة حسب حجم السوق

- أمن الأجهزة الطرفية وإدارتها
- أمن الشبكات
- حلول عمليات الأمن السيبراني
- تكامل أنظمة الأمن السيبراني
- أمن البيانات

إشارة المشاركة: أبيض | تصنيف الوثيقة: عام

كوادر الأمن السيبراني في المملكة

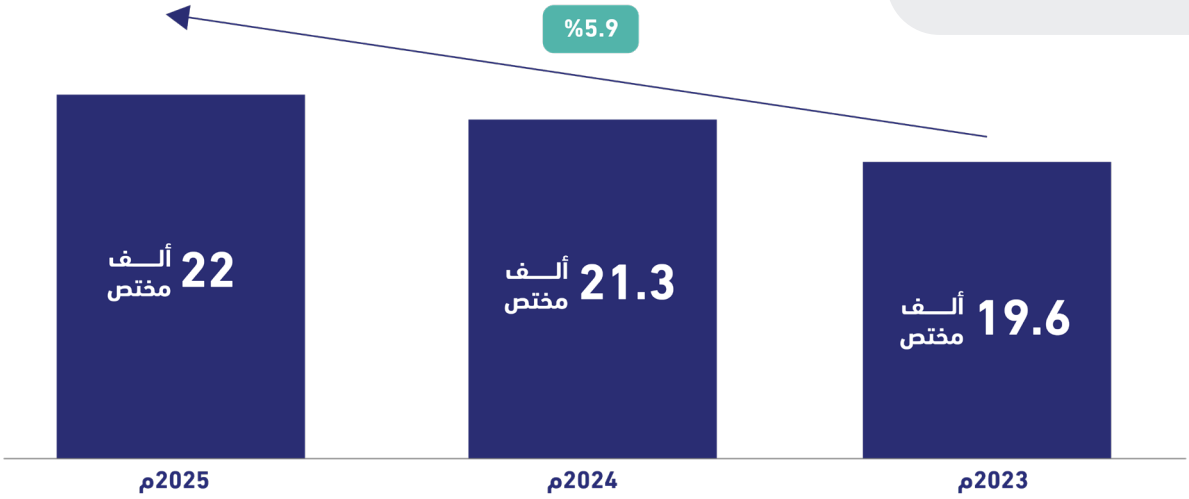
22 ألف
مختص في الأمن السيبراني

%33
مشـــاركـــة المـــرأة

6.7 ألف
خريج من برامج ومسارات الأمن السيبراني في المملكة

معدل النمو السنوي المركب للكوادر السيبرانية في المملكة

%5.9



2 أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني

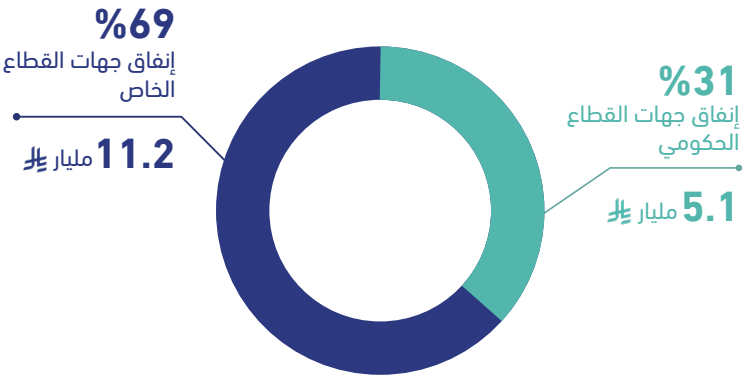
1.2 سوق الأمن السيبراني

1.1.2 حجم السوق

بلغ حجم سوق الأمن السيبراني في المملكة (16.3) مليار ريال سعودي خلال عام 2025م، وبنسبة معدل نمو سنوي مركب قدره (10.7%). وأسهم في هذا النمو، أعمال الهيئة الوطنية للأمن السيبراني الرامية لتعزيز الأمن السيبراني في المملكة؛ إلى جانب الجهود المتواصلة التي تبذلها الهيئة في تطوير الأطر التنظيمية، وتنمية القدرات، ورفع مستوى الوعي، وتمكين المنظومة. وبلغ مجموع إنفاق الجهات الحكومية (5.1) مليار ريال سعودي يشكل (31%) من حجم السوق. وفي المقابل، بلغ مجموع إنفاق منشآت القطاع الخاص نحو (11.2) مليار ريال سعودي، ليشكل (69%) تقريبًا من حجم السوق؛ منها (3.4) مليارات ريال سعودي أنفقتها منشآت القطاع الخاص ذات البنى التحتية الحساسة، لحماية العمليات التشغيلية التي تعد ركيزة أساسية للاقتصاد الوطني.

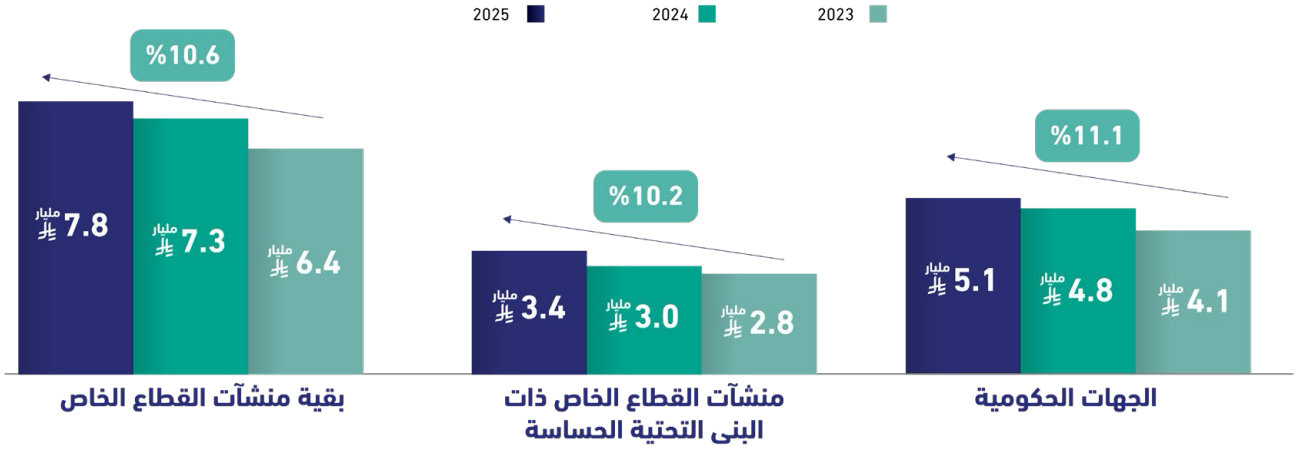
حجم السوق

16.3 مليار ﷼



وتشير معدلات النمو المتقاربة بين الجهات الحكومية، ومنشآت القطاع الخاص ذات البنى التحتية الحساسة، وبقية منشآت القطاع الخاص، إلى استمرار توسع الإنفاق على الأمن السيبراني عبر مختلف شرائح السوق والأنشطة الاقتصادية.

معدل النمو السنوي المركب لحجم السوق حسب فئة الجهات



2.1.2 الإنفاق حسب حجم الجهات

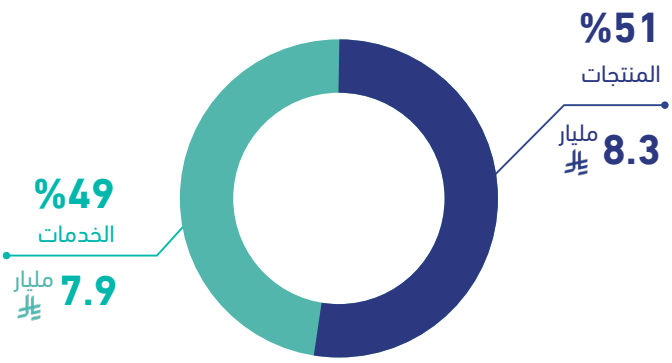
جرى تصنيف الجهات في المملكة حسب الحجم بناءً على تصنيف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت). وعند تحليل إنفاق الجهات على منتجات وخدمات الأمن السيبراني في المملكة؛ يتبين أن معظم الإنفاق لدى الجهات الحكومية ومنشآت القطاع الخاص ذات البنى التحتية الحساسة يتركز في الجهات الكبيرة. إذ بلغت نسبة الإنفاق للجهات الكبيرة في القطاع الحكومي (93.4%)، وللمنشآت الكبيرة في القطاع الخاص ذات البنى التحتية الحساسة (94%) ؛وذلك نظرًا لطبيعة أدوارها التنظيمية، ومتطلباتها التشغيلية، وحجم البنى التحتية التقنية لديها.

وفيما يتعلق ببقية منشآت القطاع الخاص فإن الإنفاق يتوزع على مختلف أحجامها بطريقة مختلفة. إذ استحوذت الجهات الصغيرة على (38.4%) من إجمالي الإنفاق، تليها الجهات المتوسطة (30.4%)،ثم الجهات الكبيرة (25.3%)، والجهات متناهية الصغر (5.9%). وفي حين تواصل الجهات الكبيرة استثماراتها بمعدلات أكبر في الأمن السيبراني على مستوى الجهة الواحدة؛ فإن إجمالي إنفاق الجهات الصغيرة والمتوسطة والمتناهية الصغر يعكس اتساع انتشارها في السوق السعودي. ويؤكد هذا التوزيع تنامي الاستثمار في الأمن السيبراني لدى كافة قطاعات الأعمال، وعدم اقتصاره على الكيانات الكبرى.

	مجموع الإنفاق (مليار ريال)	الجهات الكبيرة	الجهات المتوسطة	الجهات الصغيرة	الجهات متناهية الصغر
الجهات الحكومية	5.1	%93.4	%6.5	%0.1	-
منشآت القطاع الخاص ذات البنى التحتية الحساسة	3.4	%94	%5.9	%0.1	-
بقية منشآت القطاع الخاص	7.8	%25.3	%30.4	%38.4	%5.9

3.1.2 حجم السوق حسب تصنيف منتجات وخدمات الأمن السيبراني

ينقسم سوق الأمن السيبراني في المملكة حسب التصنيف، إلى منتجات وخدمات للأمن السيبراني. وقد بلغ الإنفاق على المنتجات (8.3) مليار ريال سعودي، ويشكل ذلك (51%) من حجم السوق، مسجلًا معدل نمو سنوي مركبًا قدره (5.2%)، في حين بلغ الإنفاق على الخدمات (7.9) مليار ريال سعودي، وهو ما يشكل (49%) من حجم السوق، مسجلًا معدل نمو سنوي مركبًا قدره (17.4%) خلال الفترة نفسها.



وعند النظر إلى أبرز المنتجات والخدمات حسب حجم الإنفاق لعام 2025م، يتبين بروز مجالات أمن الشبكات، وأمن الأجهزة الطرفية وإدارتها، وحلول عمليات الأمن السيبراني، وتكامل أنظمة الأمن السيبراني، وأمن البيانات، وهذا ما يؤكد استمرار الجهات بإعطاء الأولوية لمجالات الدفاع، والاستجابة للتهديدات السيبرانية.

أبرز منتجات وخدمات الأمن السيبراني في المملكة

- أمن الأجهزة الطرفية وإدارتها
- أمن الشبكات
- حلول عمليات الأمن السيبراني
- تكامل أنظمة الأمن السيبراني
- أمن البيانات

وخلال الفترة من عام 2023م إلى عام 2025م، نما سوق الأمن السيبراني بنحو (3.0) مليارات ريال. وأسهمت الخدمات بنحو (2.1) مليار ريال، أي ما يقارب (70%) من إجمالي هذه الزيادة، مقارنة بنحو (0.9) مليار ريال للمنتجات، مما أدى إلى تقلص الفرق بين الإنفاق على المنتجات والخدمات من (1.5) مليار ريال في عام 2023م إلى نحو (0.3) مليار ريال في عام 2025م.

وقد جاء هذا التحول مدفوعًا بزيادة حجم الإنفاق على الخدمات والقدرات التي تتطلب تشغيلًا مستمرًا، والحلول التي تتطلب جهودًا مكثفة لتنفيذها وتكاملها، وذلك بالتوازي مع استمرار الهيئة الوطنية للأمن السيبراني في تطوير الأطر التنظيمية ومتابعة الالتزام بها، كالإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدار (RFMSOC-1:2024). وفي المقابل، أدى طول دورات تحديث التقنيات واستبدالها إلى الحد من وتيرة النمو السنوي في بعض فئات سوق المنتجات.

4.1.2 التوزيع الجغرافي لجانبي الطلب والعرض

يستمر تركز التوزيع الجغرافي لجهات جانب الطلب؛ إذ تتخذ (91%) من الجهات منطقة الرياض، ومكة المكرمة، والمنطقة الشرقية مقرًا رئيسًا لها. وهو ما يعكس الثقل الاقتصادي لهذه المناطق، ويتسق مع التقارير الاقتصادية والتجارية.



%91

من جهات الطلب مقرها الرئيسي في منطقة الرياض، ومكة المكرمة، والمنطقة الشرقية.

إشارة المشاركة: أبيض | تصنيف الوثيقة: عام

كما يتسق التوزيع الجغرافي لجانب العرض مع جانب الطلب، إذ توجد (97%) من المراكز الرئيسية لمقدمي منتجات وخدمات الأمن السيبراني المسجلين لدى الهيئة الوطنية للأمن السيبراني في كل من منطقة الرياض، ومنطقة مكة المكرمة، والمنطقة الشرقية. وتضم منطقة الرياض (75%) من مقدمي المنتجات والخدمات، ومنطقة مكة المكرمة (10%)، والمنطقة الشرقية (12%). ويعكس هذا التوزيع استمرار قرب مقدمي المنتجات والخدمات من مراكز الطلب الرئيسة في المملكة، بما يمكّنهم من خدمة الشريحة الأكبر من عملاء الأمن السيبراني بكفاءة أعلى، ويدعم في الوقت ذاته مواصلة تطوير منظومات الأمن السيبراني على مستوى المناطق الأخرى.



%97

من مقدمي المنتجات والخدمات مراكزهم الرئيسية في منطقة الرياض، ومكة المكرمة، والمنطقة الشرقية.

5.1.2 مقدمي منتجات وخدمات الأمن السيبراني

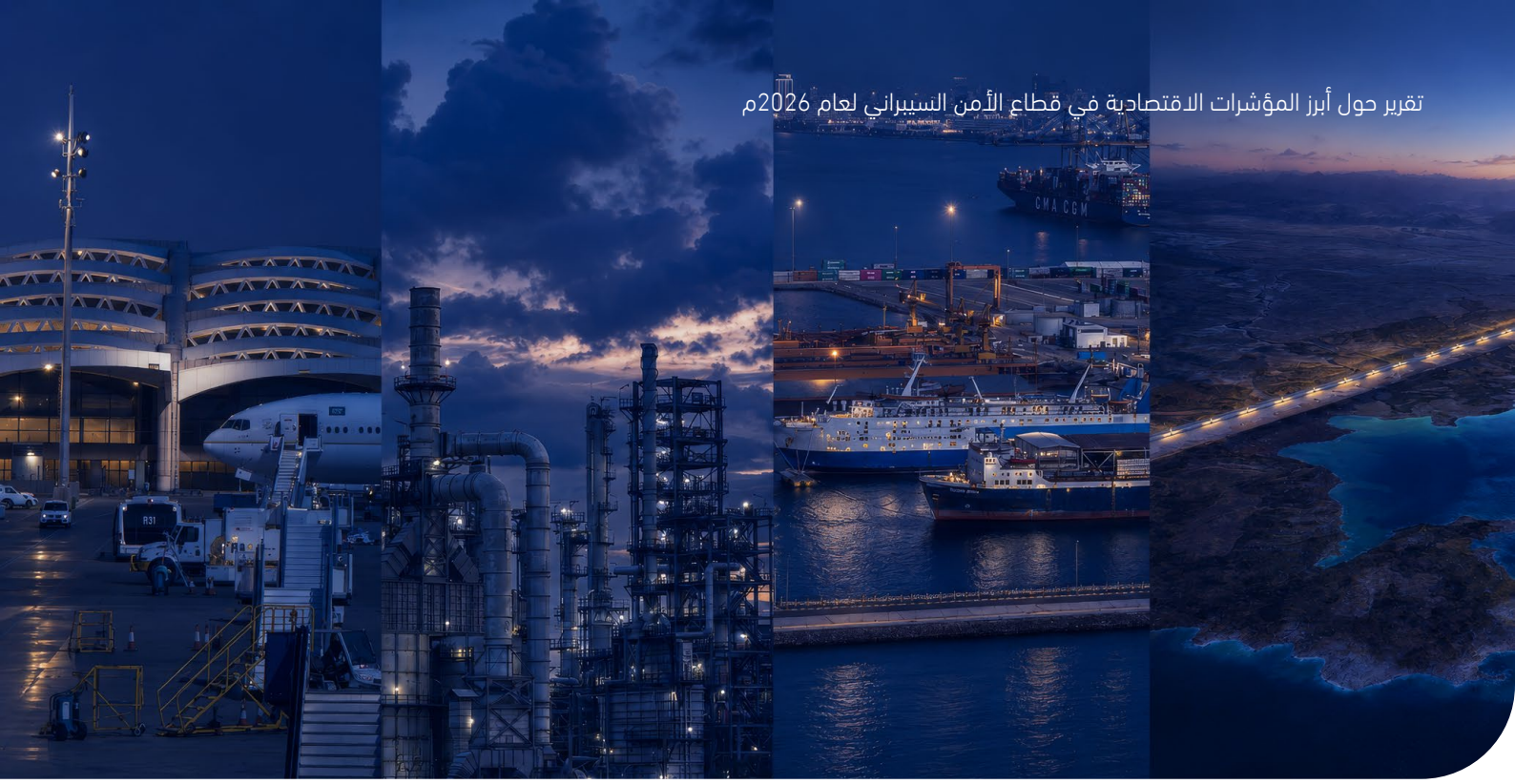
بلغ عدد مقدمي منتجات وخدمات الأمن السيبراني المسجلين لدى الهيئة (473) جهة في عام 2025م، مسجلًا معدل نمو سنوي مركبًا قدره (15.8%)، ويتسق هذا التوسع مع استمرار تنظيم قاعدة العرض وتوسيع نطاقها من خلال إطار الهيئة لتسجيل مقدمي منتجات وخدمات الأمن السيبراني، إلى جانب المبادرات الوطنية الرامية إلى تمكين رواد الأعمال، والمنشآت الناشئة، والشركات الوطنية الواعدة في مجال الأمن السيبراني.

ويستند تصنيف حجم المنشآت التي تقدم منتجات وخدمات الأمن السيبراني في المملكة إلى تعريف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت). وبناءً على الخصائص التشغيلية لمقدمي منتجات وخدمات الأمن السيبراني؛ فقد جرى دمج فئتي مقدمي المنتجات والخدمات المتوسطة، والكبيرة، في فئة واحدة باسم (الفئة الكبرى). كما جرى دمج فئتي مقدمي المنتجات والخدمات الصغيرة، ومتناهية الصغر، تحت مسمى (الفئة الصغرى). ويتيح هذا التصنيف إجراء مقارنات أكثر وضوحًا وعمقًا لتكوين تصوّر دقيق للسوق.

ويمثل مقدمو المنتجات والخدمات من الفئة الصغرى (78.4%) من مجموع مقدمي المنتجات والخدمات المسجلين لدى الهيئة الوطنية للأمن السيبراني، كما هو مبيّن في الجدول. وهذا ما يؤكد على كون منظومة الأمن السيبراني في المملكة حيوية، ومتنوعة، ومشجعة على ريادة الأعمال والابتكار، والمشاركة ذات النطاق الواسع على مستوى القطاع.

وفي حين أن مقدمي المنتجات والخدمات من الفئة الكبرى يمثلون الأقلية من مقدمي المنتجات والخدمات، إلا أن لهم دورًا جوهريًا على مستوى القطاع، لا سيما في توفير القدرات المتخصصة، ودعم الجهات العاملة في المملكة. ويتيح هذا المزيج المتوازن بين مقدمي المنتجات والخدمات من الفئة الصغرى، التي تمتاز بالمرونة وسرعة النمو، ومقدمي المنتجات والخدمات من الفئة الكبرى، التي تعد الأكثر خبرةً في منظومة الأمن السيبراني؛ تعزيز الأمن السيبراني، ورفع القدرة على مواجهة التهديدات بشتى أنواعها.

	تصنيف (منشآت)	عدد مقدمي المنتجات والخدمات	النسبة من مجموع مقدمي المنتجات والخدمات
الفئة الكبرى	كبيرة متوسطة	102	%21.6
الفئة الصغرى	صغيرة متناهية الصغر	371	%78.4



2.2 مساهمة قطاع الأمن السيبراني في الناتج المحلي الإجمالي

تقدر مساهمة قطاع الأمن السيبراني في الناتج المحلي الإجمالي بالأسعار الجارية لعام 2025م بنحو (20) مليار ريال سعودي، مسجلةً معدل نمو سنوي مركبًا قدره (13.2%)، وتمثل هذه المساهمة (0.42%) من الناتج المحلي الإجمالي للمملكة، منها (9.7) مليار ريال سعودي، مساهمة مباشرة لمقدمي منتجات وخدمات الأمن السيبراني،و(10.3) مليارات ريال سعودي مساهمة غير مباشرة، وعند النظر إلى الناتج المحلي للأنشطة غير النفطية، فإن نسبة مساهمة قطاع الأمن السيبراني فيه بلغت (0.71%).



مساهمة القطاع

20 مليار

%0.42

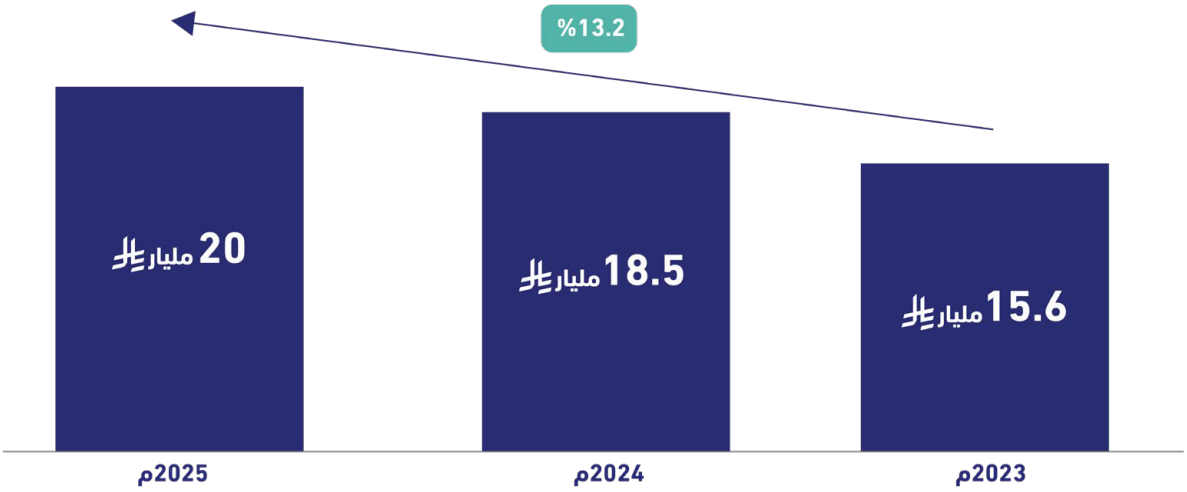
مساهمة القطاع في الناتج المحلي الإجمالي

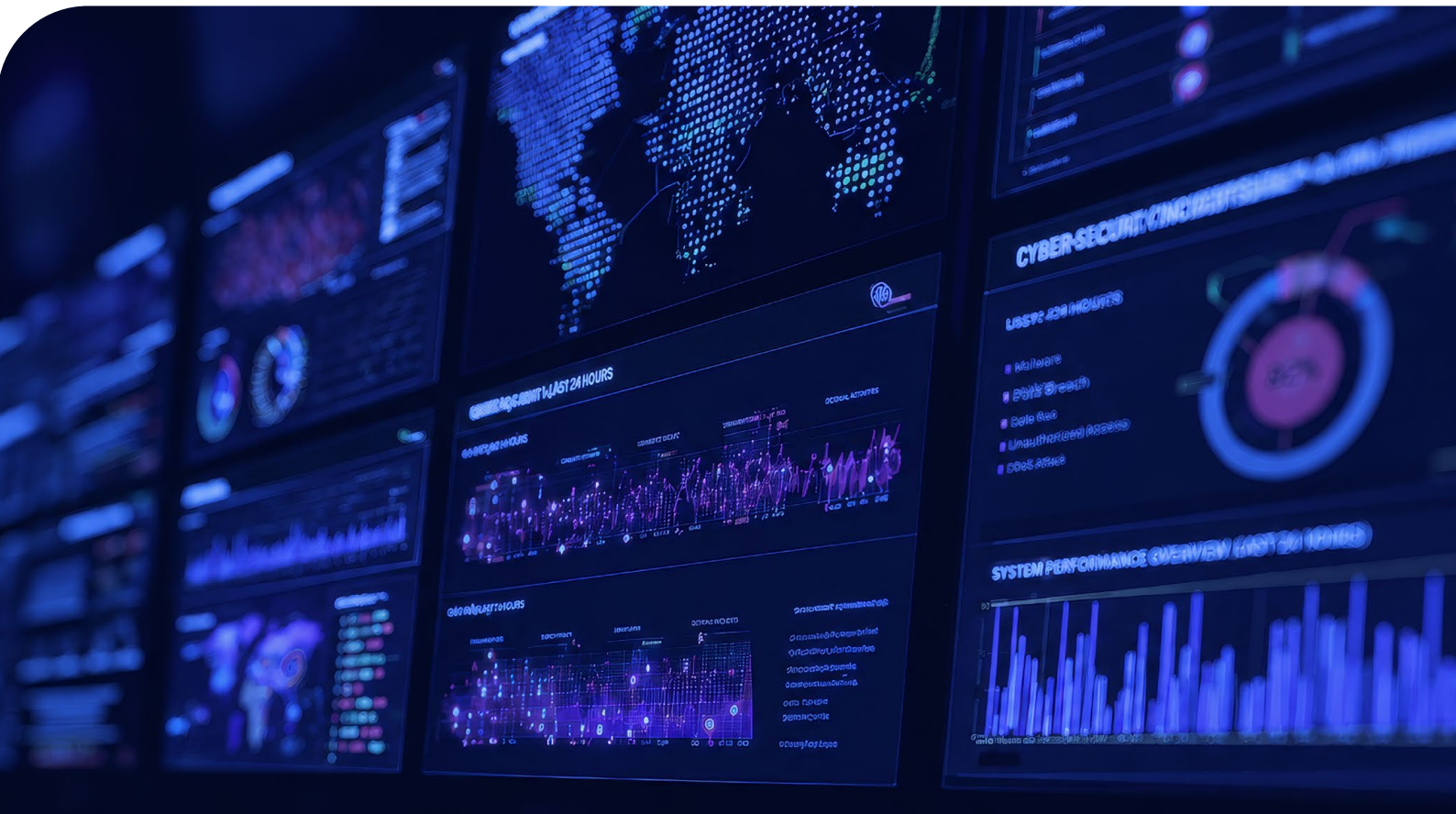
%0.71

مساهمة القطاع في الناتج المحلي للأنشطة غير النفطية

وبالنظر إلى معدل النمو السنوي المركب لمساهمة القطاع في الناتج المحلي الإجمالي، فقد بلغ (13.2%)، وذلك مع استمرار جهود تنظيم سوق الأمن السيبراني، وتوطين التقنيات السيبرانية، ودعم تسويق الابتكارات الوطنية تجاريًا؛ مما أسهم في زيادة القيمة المضافة التي يحققها مقدمو منتجات وخدمات الأمن السيبراني في المملكة، وتوسع الشراكات، وزيادة حجم الاستثمارات وفرص التوظيف.

معدل النمو السنوي المركب لمساهمة القطاع في الناتج المحلي





3 أبرز مؤشرات القوى العاملة في قطاع الأمن السيبراني

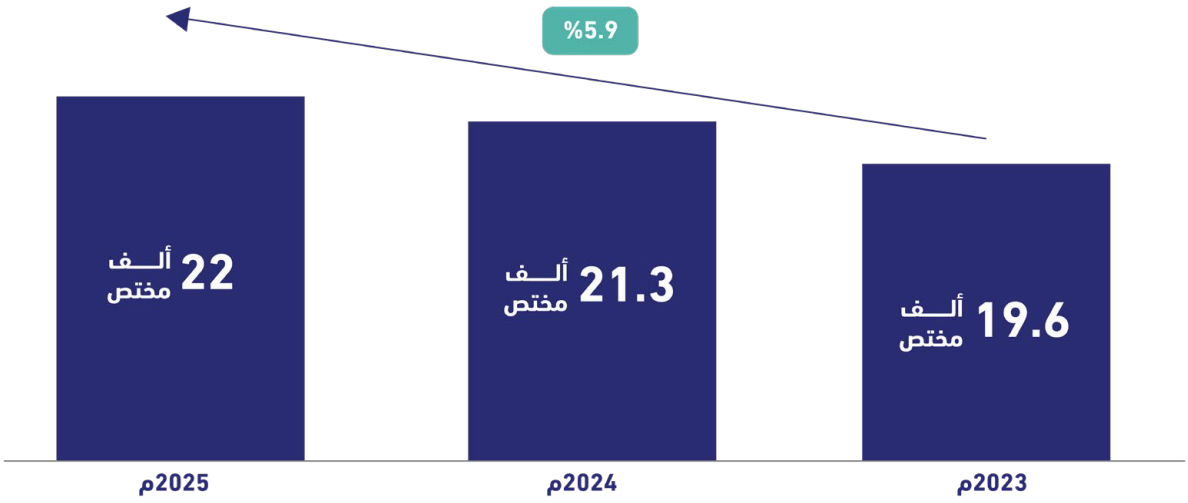
1.3 حجم كوادر الأمن السيبراني

تجاوز إجمالي عدد المختصين في الأمن السيبراني في المملكة (22) ألف مختص خلال عام 2025م، مسجلًا معدل نمو سنوي مركبًا قدره (5.9%). يعمل نحو (12%) من إجمالي المختصين في الأمن السيبراني في الجهات الحكومية، أي ما يعادل (2.7 ألف) مختص. في حين تشكل نسبة المختصين في منشآت القطاع الخاص ما يقارب (88%) من الإجمالي، أي ما يعادل (19.4 ألف) مختص، ويشمل ذلك منشآت القطاع الخاص ذات البنى التحتية الحساسة ومقدمي منتجات وخدمات الأمن السيبراني. ويُبرز هذا التوزيع الدور المحوري للقطاع الخاص في تنمية الكوادر الوطنية في مجال الأمن السيبراني. كما يعكس استمرار نمو القوى العاملة التوسع المتواصل في مسارات بناء القدرات الوطنية، التي تشمل التعليم العالي، والتدريب المتخصص، والتطوير المهني، بما يعزز قدرة القطاع على استقطاب الكفاءات الوطنية وتنميتها.

22 ألف

مختص في الأمن السيبراني

معدل النمو السنوي المركب للقوى العاملة في مجال الأمن السيبراني في المملكة



2.3 مشاركة المرأة

في الوقت الذي تمثل المرأة عالميًا ما نسبته (22%)[1] فقط من إجمالي عدد العاملين في مجال الأمن السيبراني، فقد بلغت نسبة مشاركة المرأة في قطاع الأمن السيبراني في المملكة (33%). ويشير هذا إلى التزام المملكة بترسيخ الشمولية، وتوسيع قاعدة الكفاءات العاملة بفضل الدعم والرعاية التي يحظى بهما قطاع الأمن السيبراني في المملكة، من قبل القيادة الرشيدة - أيدّها الله.

%33

مشاركة المرأة

3.3 التعليم في الأمن السيبراني

تواصل المؤسسات التعليمية في المملكة تعزيز مخرجاتها بمجال الأمن السيبراني، وذلك استجابةً للنمو المتسارع للطلب على الكفاءات المتخصصة، وما يوفره القطاع من فرص مهنية واقتصادية متنامية. وخلال عام 2025م، بلغ عدد خريجي البرامج والمسارات الأكاديمية المتخصصة بالأمن السيبراني بالمملكة أكثر من (6.7) ألف خريج بمعدل نمو سنوي مركب بلغ (83%)، في ارتفاع يعكس استمرار التوسع في تأهيل الكوادر الوطنية المتخصصة في هذا المجال. ويدلّ هذا النمو على قدرة المؤسسات التعليمية في المملكة على دعم سوق العمل بالكفاءات السيبرانية المؤهلة وتلبية احتياج القطاع من خلال تنامي البرامج والمسارات الأكاديمية المتخصصة بالأمن السيبراني المتواءمة مع الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم).

6.7 ألف

خريج من برامج ومسارات الأمن السيبراني في المملكة



(1) International Telecommunication Union (ITU). "Her CyberTracks", Accessed 22 July 2026. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Skills-Development/Her-CyberTracks.aspx

الخاتمة

تعكس المؤشرات الواردة في هذا التقرير استمرار نمو قطاع الأمن السيبراني في المملكة، وتنامي مساهمته في الناتج المحلي الإجمالي، واتساع قاعدة الكفاءات السيبرانية. وتبرز هذه النتائج أهمية تكامل جهود كافة الجهات من القطاع العام أو الخاص أو غير الربحي، والمؤسسات التعليمية، في دعم نمو قطاع الأمن السيبراني، وتعزيز دوره في الاقتصاد الوطني، وما يتيحه من فرص للاستثمار والابتكار وتنمية القدرات الوطنية.

وامتداداً للجهود الوطنية المبذولة وما تحقق من مكتسبات في قطاع الأمن السيبراني، تمضي الهيئة الوطنية للأمن السيبراني في تعزيز الأمن السيبراني في المملكة، وتحفيز نمو القطاع، وتشجيع الابتكار والاستثمار فيه، وتنمية قدراته الوطنية؛ بما يدعم بناء صناعة وطنية واعدة للأمن السيبراني، ويسهم في ترسيخ مكانة المملكة عالميًا في هذا المجال.

وستواصل الهيئة إعداد هذا التقرير بصورة دورية، وتحديث بياناته ومؤشراته، بالتعاون مع الجهات ذات العلاقة؛ لرصد تطورات القطاع، وقياس أثره الاقتصادي والتنموي، وتوفير سلسلة بيانات متسقة تتيح تتبع التغيرات والاتجاهات على المدى الطويل. ويأتي ذلك لتزويد متخذي القرار، والمستثمرين، والجهات المعنية والمختصين في منظومة الأمن السيبراني، بقاعدة مرجعية من البيانات والحقائق تدعم اتخاذ القرارات، وتسهم في توجيه المبادرات والبرامج المستقبلية، وتعزيز استدامة نمو القطاع في المملكة.

الملاحظات والمقترحات

ترحب الهيئة الوطنية للأمن السيبراني بالمقترحات حول هذا التقرير؛ بما يسهم في تعزيز مخرجاته في الإصدارات القادمة. ويمكن إرسال أي مقترحات بهذا الشأن عبر البريد الإلكتروني الآتي: studies@nca.gov.sa

ملحق (أ)

الملحق (أ): خدمات ومنتجات وحلول الأمن السيبراني

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 من 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 وترسل 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 وحضرها، بما يشمل الجيل القادم من جدار الحماية التي تتمتع بخصائص متقدمة 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 واليدوية، التي تسمح بتحليل المحتوى المريب في بيئة 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 وتصنيفها حسب التصنيف الملائم.
2-3-1	حلول منع فقدان البيانات (DLP)	حلول أمن البيانات المتاحة للأجهزة الطرفية والشبكات لمنع فقدات 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 البروتوكلات 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 بشكل 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 في 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 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	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 والتقنية التشغيلية.		
1-5-1	حلول إدارة كلمات المرور	حلول أمن الهوية وإدارتها المستخدمة في تخزين بيانات اعتماد المستخدمين وإدارتها بشكل 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 تصدّق 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 الهوية 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 والتقنية التشغيلية		
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	**حلول عمليات الأمن السيبراني**	
حلول الأمن السيبراني المستخدمة لتنفيذ أنشطة ومهام الأمن السيبراني اليومية.		
1-7-1	حلول الكشف والاستجابة الممتدة (XDR)	حلول أمنية متكاملة تُعنى بتوسيع نطاق عمليات الكشف عن التهديدات والاستجابة لها عبر بيئات متعددة (مثل: الشبكات، الأجهزة الطرفية، الخوادم، التطبيقات، السحابة، البريد الإلكتروني، الهوية)، وذلك من خلال دمج وتحليل البيانات الأمنية من مصادر متنوعة في منصة موحدة. تهدف إلى الوصول لرؤية شاملة، تحليل التهديدات المعقدة، وأتمتة الاستجابة بشكل استباقي.
2-7-1	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.
3-7-1	حلول تصيد التهديدات السيبرانية	حلول عمليات الأمن السيبراني التي تدعم الكشف الاستباقي للتهديدات النشطة والجهات التخريبية غير المعروفة مسبقًا.
4-7-1	حلول التحقيق الجنائي الرقمي	حلول عمليات الأمن السيبراني لتحديد الأدلة الإلكترونية والحصول عليها وتحليلها واستكمال التحقيقات بالاستعانة بالحاسوب.
5-7-1	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.
6-7-1	حلول المسح وتقييم الثغرات	حلول عمليات الأمن السيبراني التي من شأنها تحديد الثغرات الأمنية وتصنيفها وإدارتها.
7-7-1	حلول اختبار الاختراقات	حلول عمليات الأمن السيبراني للكشف عن نقاط الضعف التي يمكن استغلالها في الوضع الأمني، واختبارها وتصنيفها، مثل: رفع الامتيازات.
8-7-1	حلول إدارة الحوادث والتنسيق الأمني والأتمتة والاستجابة (SOAR)	حلول عمليات الأمن السيبراني التي من شأنها تنسيق الاستجابة إلى الأحداث الأمنية وأتمتتها وإدارتها.
9-7-1	حلول إدارة المعلومات والأحداث الأمنية (SIEM)	حلول عمليات الأمن السيبراني لجمع الأحداث وإدارة السجلات وتصحيح السجلات.
10-7-1	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 مثل مؤشرات الاختراق (IoC).
11-7-1	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.

8-1	**أمن الحوسبة السحابية**	
حلول الأمن السيبراني التي تتيح حماية التطبيقات القائمة على الحوسبة السحابية.		
1-8-1	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.
2-8-1	أمن الجهد السحابي	حلول أمن الحوسبة السحابية، التي تحمي الجهد أثناء التنقل بين بيئات الحوسبة السحابية المختلفة.
9-1	**أمن الأنظمة الخاصة**	
حلول الأمن السيبراني التي تتيح حماية الأنظمة الخاصة مثل التقنية التشغيلية (OT).		
1-9-1	حلول الأمن الصناعي	حلول أمن الأنظمة الخاصة لحماية أنظمة التحكم الصناعية (ICS)، والتقنية التشغيلية (OT) بما يشمل واجهة المستخدم والآلة (HMI)، والتحكم الإشرافي وتحصيل البيانات (SCADA)، والبيانات والأمن السيبراني لأنظمة التحكم الموزعة (DSC).
2-9-1	حلول أمن إنترنت الأشياء والأجهزة المدمجة	حلول أمن الأنظمة الخاصة التي تحمي الأجهزة غير التقليدية والأحادية الغرض والمتصلة بالإنترنت ضد التهديدات.
2	**خدمات الأمن السيبراني الاحترافية**	
1-2	**الاستشارات الإدارية في الأمن السيبراني**	
الخدمات الاحترافية في الأمن السيبراني لتحديد مجالات التحسين الإستراتيجية وتقديم التوصيات.		
1-1-2	تطوير إستراتيجية الأمن السيبراني وخارطة الطريق	الخدمات الاستشارية في الأمن السيبراني لوضع إستراتيجية الأمن السيبراني (مثل الرؤية والرسالة وغيرها) وخارطة طرق 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 إستراتيجية 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 بشمل الهيكل التنظيمي والأدوار والمسؤوليات والحوكمة وما إلى ذلك.
4-1-2	اعتماد وشهادات الأمن السيبراني للمنظمات	الخدمات الاستشارية في الأمن السيبراني لاعتماد الجهة مفقًا لمعيار الاعتماد المعترف به خارجيًا وبناءًا 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 الاحترافية في الأمن السيبراني لإجراء تقييمات الأمن السيبراني على مستوى الحوكمة، وبيئة تقنية المعلومات والتقنية التشغيلية في 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 التحسن.
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 وفقًا لمعيار محدد وباستخدام نموذج تقييم النضج، مثل: تقييم مدى نضج الأمن السيبراني في الجهة وفقًا لضوابط لأمن السيبراني الصادرة من الهيئة، أو تقييم مدى نضج الأمن السيبراني في الجهة وفقًا لنماذج نضج مُعترف بها عالميًا.
4-2-2	تدقيق/تقييم الالتزام بمتطلبات الأمن السيبراني	خدمات تقييم الأمن السيبراني للتحقق من الامتثال للأنظمة والضوابط والمعايير والأطر وغيرها الوطنية والعالمية الأخرى المتعلقة بالأمن السيبراني.

3-2	تقييم المخاطر السيبرانية	
الخدمات الاحترافية في تقييم المخاطر التي يتم إجراؤها لتحديد مخاطر الأمن السيبراني وتحديد إجراءات معالجة التهديدات وعوامل تهديد الأمن.		
1-3-2	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 الاحترافية في الأمن السيبراني التي تقييم نواحي بيئة تقنية المعلومات والتقنية التشغيلية في الجهة.		
1-4-2	تقييم الثغرات	الخدمات التقنية في الأمن السيبراني لتحديد الثغرات وتصنيفها وترتيبها حسب الأولوية في حل أو منظومة أو نظام أو شبكة محددة.
2-4-2	اختبار الاختراقات	الخدمات التقنية في الأمن السيبراني للعثور على الثغرات القابلة للاستغلال في حل أو منظومة أو نظام أو شبكة محددة وإظهارها بشكل استباقي، واختبار مدى استغلالها.
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 بشكل استباقي (تصيد التهديدات) أو تفاعلي (تقييم الاختراق) استجابة إلى العثور على مؤشرات الاختراق (IoCs).
5-4-2	خدمات الاختبارات لمحاكاة الهجمات السيبرانية	الخدمات الفنية في الأمن السيبراني المستخدمة في هجمات المخترقون الأخلاقيون (الفريق الأحمر "Red Teaming") على أنظمة الجهة كمحاكات لتهديد سيبراني حقيقي، فيما يحاول مدافعو الجهة (الفريق الأزرق "Blue Teaming") الدفاع عن أنظمة وشبكة الجهة. وتشمل كذلك الاختبارات التي تجمع بين الفريق المهاجم والفريق المدافع (الفريق البنفسجي "Purple Teaming").
6-4-2	تقييم أمن التطبيقات	الخدمات الفنية في الأمن السيبراني لتحديد العيوب والثغرات الأمنية في التطبيقات، مثل مراجعة شفرة المصدر واختبار أمن تطبيقات الويب واختبار أمن تطبيقات الأجهزة الذكية وما إلى ذلك.
7-4-2	مراجعة إعدادات الأمن السيبراني	الخدمات التقنية للأمن السيبراني لمراجعة التكوين الأمني للأجهزة وتحديد التكوينات الخاطئة وفرص تعزيزها.
8-4-2	التقييم السيبراني والاعتماد للحلول والمنتجات	الخدمات الفنية في الأمن السيبراني لتقييم الحل والمنتج (من أجهزة وبرمجيات) واعتماده وفقًا لمعايير اعتماد وطنية حسب ما يصدر عن الهيئة أو وفقاً لمعايير وشهادات مُعترف بها عالمياً.
5-2	خدمات برامج مكافأة اكتشاف الثغرات (Bug Bounty)	
الخدمات التقنية في الأمن السيبراني لتشغيل برنامج يحفّز المخترقين الأخلاقيين لإجراء تقييمات مستقلة والإفصاح عن المسؤول.		
1-5-2	خدمات برامج مكافأة اكتشاف الثغرات (Bug Bounty)	الخدمات التقنية في الأمن السيبراني لتشغيل برنامج يحفّز المخترقين الأخلاقيين لإجراء تقييمات مستقلة والإفصاح عن المسؤول.

6-2	**الاستشارات التقنية في الأمن السيبراني**	
الخدمات الاحترافية في الأمن السيبراني لتقديم التوصيات التقنية والأنشطة الاستشارية التقنية.		
1-6-2	تصميم معمارية الأمن السيبراني	الخدمات الفنية في الأمن السيبراني لتصميم البنية الأمنية للجهة باستخدام أفضل الممارسات ومبادئ التصميم الآمن.
2-6-2	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).
3-6-2	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.
7-2	**الاستجابة والتحقيق في الحوادث السيبرانية**	
الخدمات الاحترافية في الأمن السيبراني لتحليل ومعالجة الحوادث والاختراقات في الأمن السيبراني.		
1-7-2	الاستجابة للحوادث السيبرانية	خدمات الاستجابة لحوادث الأمن السيبراني لمساعدة الجهات في إدارة حوادث الأمن السيبراني وتحليلها واحتوائها ومعالجتها والتعلّم منها.
2-7-2	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).
3-7-2	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 السيبرانية)، وتحليلها وفحصها.
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 والجهات الوطنية وغيرها من المستخدمين المتقدمين.
2-3	**تكامل أنظمة الأمن السيبراني**	
خدمات الأمن السيبراني المقدمة من مورّدي الأمن السيبراني وموّردي 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 المُدارة للأمن السيبراني**	
1-4	**إدارة مركز عمليات الأمن السيبراني**	
خدمات مراقبة الأمن السيبراني وتحديد التهديدات وتصعيد الحوادث.		
1-1-4	خدمات مركز عمليات الأمن السيبراني المدار	الخدمات التي تحصل عليها الجهة المستفيدة من مقدم الخدمة؛ حسب الموضح في الإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدار.
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 تركز 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 دراسة سوق الأمن السيبراني في المملكة. ويقدم هذا التقرير معلومات عامة لأغراض إرشادية فقط، دون أي إقرارات أو تعهدات من أي نوع كان سواء بشكل صريح أو ضمني. ولا تتحمل الهيئة الوطنية للأمن السيبراني، ومجموعة بوسطن الاستشارية (BCG)، ومؤسسة البيانات الدولية (IDC) أي التزام أو مسؤولية من أي نوع. كما أنها غير مسؤولة عن أي نوع من العواقب ذات الصلة بمحتواه، والذي يُعدّ عرضة للتغيير في أي وقت دون إشعار مسبق.

حقوق الملكية

يُعدّ محتوى هذا التقرير مِلكًا للهيئة الوطنية للأمن السيبراني (الهيئة). وبناء عليه؛ لا يجوز نسخه، أو طباعته، أو تحميله إلا لغرض الاستخدام الشخصي أو الداخلي، غير التجاري. ولا يجوز إعادة استخدام أي جزء من محتوى هذا التقرير أو تخزينه في موقع آخر دون الحصول على موافقة خطية مسبقة من الهيئة.

الهيئة الوطنية
للأمن السيبراني

National Cybersecurity Authority


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority