الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

تقرير حول

أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني 2025م

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

بالتعاون مع

IDC | BCG

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

تعد الهيئة الوطنية للأمن السيبراني، وفق تنظيمها الصادر بالأمر الملكي رقم (6801) في 1439/2/11 هـ الجهة المختصة في المملكة العربية السعودية بالأمن السيبراني، والمرجع الوطني في شؤونه. وتهدف الهيئة 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.

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 الثاني الذي يشمل نتائج دراسة البيانات وتحليلها التي جرى جمعها لعام 2024م، كما يقارن النتائج مع الإحصاءات الواردة في تقرير عام 2023م. ويقدم التقرير تحليلا مفصلا عن قطاع الأمن السيبراني، ويحدد العوامل الأساسية في توجيه المبادرات، والبرامج المستقبلية، في سبيل تعزيز النمو، والمساعدة في الحفاظ على مكانة المملكة عالميا في مجال الأمن السيبراني.

ينقسم التقرير إلى ثلاثة أبواب رئيسة:

1. **المنهجية:** يوضح هذا الباب 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 الباب نظرة تفصيلية عن قطاع الأمن السيبراني في المملكة، وتشمل حجم السوق البالغ (15.2) مليار ريال سعودي، وتوزيع الإنفاق حسب القطاع؛ إذ يشكل إنفاق جهات القطاع الخاص (68%) من حجم السوق، في حين يشكل إنفاق جهات القطاع العام (32%). كما يستعرض التقرير التوزيع الجغرافي لجانبيّ العرض والطلب، وعدد مقدمي منتجات وخدمات الأمن السيبراني المسجلين لدى الهيئة، البالغ عددهم (420) جهة، بالإضافة إلى مساهمة قطاع الأمن السيبراني في الناتج المحلي الإجمالي بالأسعار الجارية والتي بلغت (18.5) مليار ريال سعودي؛ إذ تمثل (0.40%) من الناتج المحلي الإجمالي و(0.71%) من الناتج المحلي للأنشطة غير النفطية.

3. **أبرز مؤشرات القوى العاملة في قطاع الأمن السيبراني:** يقدم هذا الباب حجم القوى العاملة في القطاع. وقد أظهرت الدراسة استمرار نمو عدد الكفاءات السيبرانية في المملكة؛ إذ وصلت إلى أكثر من (21) ألف مختص، تشكل نسبة الإناث منهم (32%)، مما يعكس جهود المملكة في ترسيخ الشمولية نحو توسيع قاعدة الكفاءات العاملة في القطاع.

مقدمـــة

يشـهد قطـاع الأمـن السـيبراني فـي المملكـة نمـوا وتطورا حيويا ملحوظا، وهو ما تؤكده المؤشرات الدولية؛ إذ حافظت المملكـة علـى المرتبـة الأولـى عالميـا فـي مؤشـر الأمـن السـيبراني ضمـن تقريـر (الكتاب السـنوي للتنافسـية العالمية للعـام 2025م) الصـادر عـن مركـز التنافسـية العالمـي التابـع للمعهـد الدولـي للتنميـة الإداريـة (IMD) بسويسـرا؛ وذلـك اسـتمرارا لمـا تحقـق فـي عـام 2024م. ويأتـي هـذا الترتيـب ترسـيخا لموقـع المملكـة الرائـد والمتقـدم في هـذا القطاع الحيـوي والواعـد؛ إذ سـبق وأن أكدته مؤشـرات دولية أخرى، ومنهـا تصنيـف المملكـة أنموذجـا رائـدا فـي الفئـة الأعلـى (Role-Modelling) للمؤشـر العالمـي للأمـن السـيبراني 2024م، الصـادر عـن منظمـة الأمـم المتحـدة عبـر وكالتهـا المتخصصـة بتكنولوجيـا المعلومـات والاتصـالات (ITU).

ويبـرز فـي ذلـك النمـوذج السـعودي فـي الأمـن السـيبراني بوصفـه أنموذجـا معياريـا للتميـز؛ بمـا نتـج عنه من تحسـينات اقتصاديـة وأمنية، فهو شـمولي فـي تناوله لمجـالات الأمن السـيبراني التشـريعية، والأمنية، والاقتصادية؛ حيث يرتكز هذا النمـوذج علـى المركزيـة فـي حوكمـة الأمـن السـيبراني على المسـتوى الوطني؛ شـاملة أعمـال التقييم، والاسـتجابة وبناء القـدرات الوطنيـة، ولامركزيـة التشـغيل المناطة بهـا الجهات الوطنية.

ويسـهم النموذج السعودي في الإدارة والرقابة الفعالة على المشـهد السـيبراني الوطني بأكمله؛ بما يعظم من مكاسـب المملكـة، ويرتقـي بمكانتها الدولية، ويمكّـن الجهات الوطنية فـي الوقت نفسـه من القيـام بمهماتهـا واختصاصاتها، ورفع جاهزيتها التشغيلية.

وبنـاء علـى الدراسـة المرجعيـة التـي أجريـت العـام الماضـي، أعـادت الهيئـة الوطنيـة للأمـن السـيبراني تطبيـق إطارهـا البحثـي القائـم علـى الأدلـة؛ لإعـداد التحليـل الاقتصـادي السـنوي الثاني للقطـاع في المملكة، بالتعـاون مع مجموعة بوسـطن الاستشـارية (BCG)، ومؤسسـة البيانـات الدوليـة (IDC). وتتّبع دراسـة عام 2025م أفضل الممارسـات العالمية في اختيـار العينات والتحقق، والنمذجـة الاقتصادية، وحققت مسـتوى ثقـة إحصائيـا بنسـبة (98%) وبهامـش خطـأ يبلـغ حوالـي (3.5%). وفي هذا السـياق، تسـلّط مجموعـة البيانات المسـتخلصة الضـوء علـى هيكلية السـوق، والمسـاهمة في الناتـج المحلـي الإجمالـي، ودور القـوى العاملـة فـي تنميـة القطاع.

كلمة شركاء إعداد التقرير

في ظل التطور المتسارع الذي يشهده قطاع الأمن السيبراني في المملكة، بات من المُلح فهم سوق الأمن السيبراني ومتغيراته على نحو مفصل، فقد أصبح القطاع ركيزة مهمة لحماية الأمن الوطني، وأحد أعمدة التنويع الاقتصادي وتعزيز مقومات الاستدامة في المملكة. ويتسم القطاع اليوم باتساع قاعدة قدرات مقدمي منتجاته وخدماته، وبنمو مطّرد للكوادر الوطنية، بما يشكل منظومة متكاملة، تعزز الثقة في الخدمات، والبنى التحتية في المملكة.

ويأتي هذا التقرير في إصداره السنوي الثاني، الذي تعده الهيئة الوطنية للأمن السيبراني بالتعاون مع مجموعة بوسطن الاستشارية (BCG) ومؤسسة البيانات الدولية (IDC). وقد استند إعداده على دراسة شاملة جمعت بين الاستبانات، وجلسات النقاش مع الجهات الحكومية، ومنشآت القطاع الخاص ذات البُنى التحتية الحساسة، وبقية منشآت القطاع الخاص، بالإضافة إلى مقدمي منتجات وخدمات الأمن السيبراني، وفق منهجية دقيقة. ويهدف التقرير إلى تقديم تصور واضح ودقيق لقطاع الأمن السيبراني في المملكة، مرتكزا على ثلاثة محاور رئيسة، هي: سوق الأمن السيبراني، ومساهمة القطاع في الاقتصاد الوطني، والقوى العاملة في الأمن السيبراني.

فعلى صعيد سوق الأمن السيبراني، يبيّن التقرير إجمالي الإنفاق لدى الجهات الحكومية، ومنشآت القطاع الخاص ذات البُنى التحتية الحساسة، وبقية منشآت القطاع الخاص باختلاف أنشطتها وأحجامها. كما يستعرض تصنيف منتجات وخدمات الأمن السيبراني، لتكوين فهم شامل عن سوق الأمن السيبراني في المملكة من جانبي العرض والطلب.

كما يتناول التقرير الأثر الاقتصادي للأمن السيبراني، من خلال تقييم مساهمته المباشرة وغير المباشرة في الاقتصاد الوطني؛ وذلك استنادا إلى معايير دولية معتمدة وأطر إحصائية رسمية تكفل موثوقية النتائج وقابليتها للمقارنة. كما يستعرض التقرير جانب القوى العاملة، ونمو الكفاءات الوطنية، وتعزيز البرامج التعليمية، التي تضمن الاستدامة للقطاع.

ومن خلال تقديم صورة متكاملة عن حجم القطاع وبنيته وأثره الاقتصادي؛ تعد مخرجات هذا العمل أداة إستراتيجية لصناع القرار وأصحاب المصلحة، بما توفره من مرئيات تسهم في صياغة السياسات، وتوجيه الاستثمارات، وتعزيز ريادة المملكة في مجال الأمن السيبراني.

شركاء إعداد التقرير

BCG IDC

1. المنهجية

استخدمت الهيئة الوطنية للأمن السيبراني الإطار البحثي، الذي أعدته مسبقا، 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(26) مجموعة أنشطة، و(102) نوعا من المنتجات والخدمات.

وباستخدام هذا التصنيف؛ عمل الفريق 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 المتطرفة، والمطابقة مع الإحصاءات الرسمية. وهذه الإجراءات أدت إلى تحقيق مستوى ثقة إحصائي يزيد على (98%) بهامش خطأ قدره (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 عالميا. ولقد ترجمت نماذج حجم الإيرادات، وحجم الطلب، وحجم القوى العاملة، والمساهمة في الناتج المحلي الإجمالي هذه المدخلات الأولية إلى أبرز المؤشرات التي ذكرت في هذا التقرير؛ لضمان دقة الأرقام إحصائيا، وإمكانية مقارنتها بشكل سنوي.

1.1. تصنيف المنتجات والخدمات في قطاع الأمن السيبراني

جرى تطوير تصنيف شامل للمنتجات والخدمات في قطاع الأمن السيبراني (الملحق 1)؛ بالتعاون مع العديد من المؤسسات البحثية، وشركات تحليل سوق الأمن السيبراني الرائدة. وخضعت العديد من الشركات العالمية ومقدمي منتجات وخدمات الأمن السيبراني للتقييم، بغرض تغطية تفاصيل قطاع الأمن السيبراني على نحو شامل ومرن؛ على أن يجري تحديثه عند الحاجة؛ لعكس التطور في السوق وتقنياته. وقد اشتمل تصنيف المنتجات والخدمات في قطاع الأمن السيبراني، على (102) منتج وخدمة، جرى تقسيمها إلى ثلاثة مستويات، كما هو موضح في الشكل التالي.

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 التصنيف إلى جهات حكومية، وجهات من القطاع الخاص تملك أو تشغّل أو تستضيف البنى التحتية الحساسة، والجهات الأخرى في القطاع الخاص بمختلف الأحجام، والأنشطة، وكذلك مقدمي خدمات ومنتجات الأمن السيبراني، وأخيرا المختصين العاملين في مجال الأمن السيبراني والمؤسسات التعليمية. وقد قام فريق الدراسة بنشر استبيان وطني مدعوم بجلسات مركّزة للنقاش، وكذلك المقابلات الشخصية المستهدفة.

وقد نتج عن ذلك إعداد مجموعة بيانات أساسية؛ تضم إفادات جرى التحقق منها، وتغطي الجهات المعنية بجانب الطلب، والشركات 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 البيانات الوطني؛ بدءا من جمع البيانات ووصولا إلى نمذجتها. وتضمنت تلك المعايير استخدام عمليات التحقق الآلي، والمراجعات اليدوية؛ للكشف عن القيم المتطرفة، وغيرها من المعايير. كما جرى عقد عدد من جلسات المتابعة، التي أجريت مع المشاركين في الاستبيان، والمقابلات مع الخبراء على مستوى قطاع الأمن السيبراني؛ للتحقق من صحة النتائج الرئيسة، واختبار المرئيات؛ بهدف ضمان دقة وموثوقية مخرجات الدراسة مما يمنح الثقة لصناع القرار والمستثمرين، ورواد الأعمال.

%98
مستوى الثقة الإحصائي

%3.5
هامش الخطأ

ضمنت المنهجية مستوى ثقة إحصائي عالي، وهامش خطأ محدود؛ نتيجة لارتفاع 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. وقد 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.

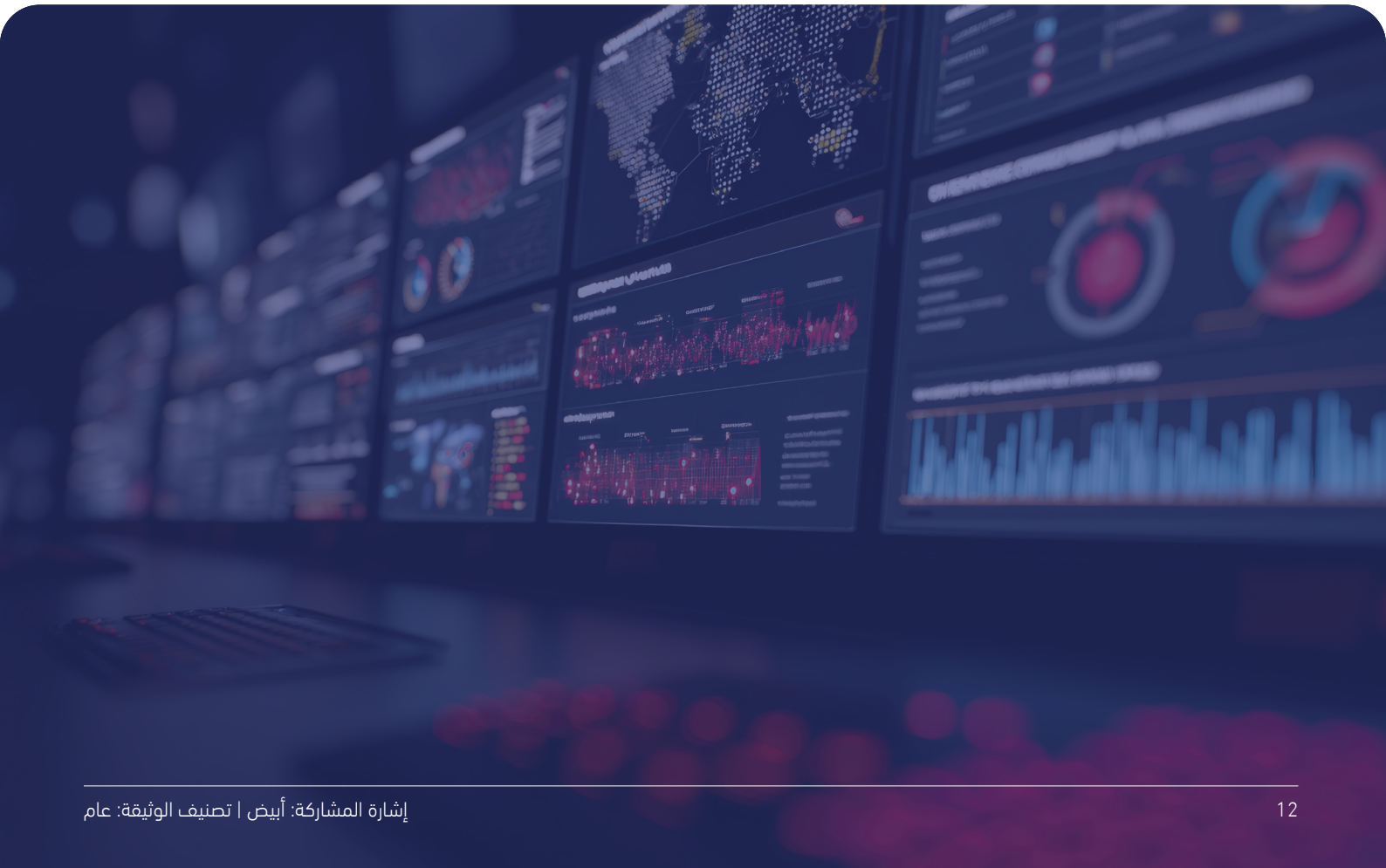
كما تم استخدام النمذجة الاقتصادية بالمواءمة مع منهجية الهيئة العامة للإحصاء؛ لتقدير مساهمة القطاع في الناتج المحلي الإجمالي، وبالتالي تحديد الأثر الاقتصادي للقطاع في المملكة، أخذا بعين الاعتبار إيرادات مقدمي المنتجات والخدمات، وضرائب الشركات، والدعم المقدم لها، ودخل العاملين في المجال. وتم استخدام جداول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

5.1. إعداد المخرجات

جرى استخراج مرئيات نوعية عن سوق الأمن السيبراني في المملكة، ومساهمته الاقتصادية، استنادا إلى نتائج النماذج الإحصائية والاقتصادية. ومن أبرز هذه المرئيات:

1. حجم سوق الأمن السيبراني
2. مساهمة قطاع الأمن السيبراني في الناتج المحلي الإجمالي
3. كوادر الأمن السيبراني

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



أبرز النتائج

حجم سوق الأمن السيبراني في المملكة

15.2 مليار ﷼

المساهمة في الناتج المحلي الإجمالي بالأسعار الجارية

18.5 مليار ﷼

%0.40

مساهمة القطاع في الناتج المحلي الإجمالي

%0.71

مساهمة القطاع في الناتج المحلي للأنشطة غير النفطية

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

420
عدد مقدمي المنتجات والخدمات

17
منشأة كبيرة

74
منشأة متوسطة

166
منشأة صغيرة

163
منشأة متناهية الصغر

توزيع الإيرادات حسب حجم مقدمي المنتجات والخدمات

الفئة الصغرى		الفئة الكبرى	
الشركات متناهية الصغر	الشركات الصغيرة	الشركات المتوسطة	الشركات الكبيرة
%1.0	%13.0	%43.3	%42.7

أبرز منتجات وخدمات الأمن السيبراني في المملكة حسب حجم السوق

- أمن الشبكات
- أمن الأجهزة الطرفية وإدارتها
- حلول عمليات الأمن السيبراني
- الاستشارات الإدارية في الأمن السيبراني
- أمن البيانات

كوادر الأمن السيبراني في المملكة

21.3 ألف
مختص بالأمن السيبراني

%32
مشاركة المرأة

5 آلاف
خريج من برامج ومسارات الأمن السيبراني في المملكة


3967945
3852575
2126548
4395792
4637457

2. أبرز المؤشرات الاقتصادية في قطاع الأمن السيبراني

1.2. سوق الأمن السيبراني في المملكة

1.1.2. حجم السوق

بلغ حجم سوق الأمن السيبراني في المملكة (15.2) مليار ريال سعودي خلال عام 2024م وبنسبة نمو بلغت (14%) عن العام السابق. وأسهم في هذا النمو، مبادرات الهيئة الوطنية للأمن السيبراني التمكينية للجهات الوطنية، والجهود الرامية لتعزيز المحافظة على الأمن الوطني من المخاطر التي يشهدها الفضاء السيبراني؛ مما أدى إلى رفع مستوى الوعي، والامتثال بالضوابط، والاستثمار في الأمن السيبراني لدى الجهات العاملة في المملكة. إذ بلغ مجموع إنفاق الجهات الحكومية (4.8) مليار ريال سعودي يشكل (32%) من حجم السوق، وبلغ مجموع إنفاق منشآت القطاع الخاص (10.3) مليار ريال سعودي، ويشكل (68%) من حجم السوق؛ منها (3.0) مليارات ريال سعودي أنفقتها منشآت القطاع الخاص ذات البنى التحتية الحساسة. ومع ارتفاع الإنفاق على منتجات وخدمات الأمن السيبراني في جميع القطاعات؛ فإن عدم تغير الحصص النسبية بشكل كبير يدل على نضج السوق ونموه المتوازن.

2.1.2. الإنفاق حسب حجم الجهات في المملكة

جرى تصنيف الجهات في المملكة حسب الحجم بناء على تصنيف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت). وعند تحليل إنفاق الجهات على منتجات وخدمات الأمن السيبراني في المملكة؛ يتبيّن أن معظم الإنفاق لدى الجهات الحكومية ومنشآت القطاع الخاص ذات البنى التحتية الحساسة يتركز في الجهات الكبيرة. إذ بلغت نسبة الإنفاق لكل من الجهات الكبيرة في القطاع العام ومنشآت القطاع الخاص ذات البنى التحتية الحساسة نحو (94%) من إجمالي إنفاقها؛ نظرا لطبيعة أعمالها، وحجم البنى التحتية التقنية لتلك الجهات.

وفيما يتعلق ببقية منشآت القطاع الخاص فإن الإنفاق يتوزع على مختلف أحجامها بطريقة مختلفة. إذ تشكل المنشآت الصغيرة (39%) من إجمالي الإنفاق، تليها المتوسطة بنسبة (34%)؛ نظرا لكونهما تمثلان الشريحة الأكبر من المنشآت.

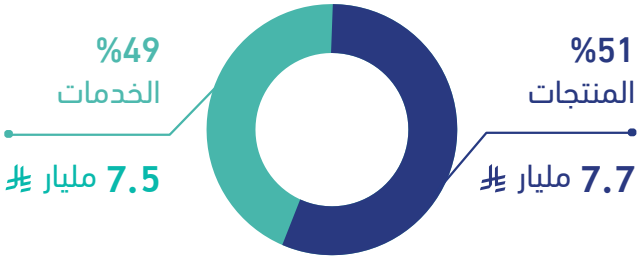
15.2 مليار ﷼

	مجموع الإنفاق (مليار ريال)	الجهات الكبيرة	الجهات المتوسطة	الجهات الصغيرة	الجهات متناهية الصغر
الجهات الحكومية	4.8	%94	%6	%0.2	-
منشآت القطاع الخاص ذات البنى التحتية الحساسة	3.0	%94	%6	%0.3	-
بقية منشآت القطاع الخاص	7.3	%18	%34	%39	%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 (7.7) مليار ريال سعودي، ويشكل ذلك (51%) من حجم السوق، في حين بلغ الإنفاق على الخدمات (7.5) مليار ريال سعودي، وهو ما يشكل (49%) من حجم السوق.

وعند النظر إلى أبرز المنتجات والخدمات حسب حجم الإنفاق لعام 2024م، يتبين بروز مجالات أمن الشبكات، وأمن الأجهزة الطرفية وإدارتها، وحلول عمليات الأمن السيبراني، والاستشارات الإدارية في الأمن السيبراني، وأمن البيانات، وهذا ما يؤكد استمرار الجهات بإعطاء الأولوية لمجالات الدفاع، والاستجابة للتهديدات السيبرانية منذ العام السابق.

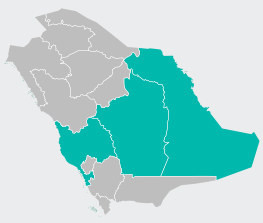


أبرز منتجات وخدمات الأمن السيبراني في المملكة

- أمن الشبكات
- أمن الأجهزة الطرفية وإدارتها
- حلول عمليات الأمن السيبراني
- الاستشارات الإدارية في الأمن السيبراني
- أمن البيانات

4.1.2. التوزيع الجغرافي لجانب الطلب

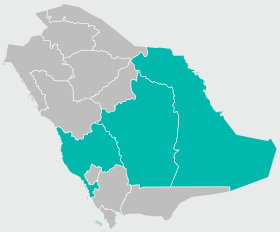
يستمر تركز التوزيع الجغرافي لجهات جانب الطلب؛ إذ تتخذ (73%) من الجهات منطقة الرياض، ومكة المكرمة، والمنطقة الشرقية مقرا رئيسا لها. وهو ما يعكس الثقل الاقتصادي لهذه المناطق، ويتسق مع التقارير الاقتصادية والتجارية.



%73
من جهات الطلب تتركز في منطقة الرياض، ومكة المكرمة، والمنطقة الشرقية.

5.1.2. التوزيع الجغرافي لجانب العرض

يتسق التوزيع الجغرافي لجانب العرض مع جانب الطلب، فتتواجد (98%) من المراكز الرئيسة لمقدمي منتجات وخدمات الأمن السيبراني المسجلين لدى الهيئة الوطنية للأمن السيبراني في كل من منطقة الرياض، ومنطقة مكة المكرمة، والمنطقة الشرقية. وتضم منطقة الرياض (77%) من مقدمي المنتجات والخدمات، ومنطقة مكة المكرمة (11%)، والمنطقة الشرقية (10%). ويتوافق هذا التوزيع مع المناطق ذات التركيز الاقتصادي الأعلى في المملكة.



%98

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

6.1.2. تصنيف مقدمي منتجات وخدمات الأمن السيبراني حسب الحجم

يستند تصنيف حجم المنشآت التي تقدم منتجات وخدمات الأمن السيبراني في المملكة إلى تعريف الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت). وبناء 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 وضوحا وعمقا لتكوين تصوّر دقيق للسوق.

ويمثل مقدمو المنتجات والخدمات من الفئة الصغرى (78%) 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 دورا جوهريا 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 رسوخا وخبرة في منظومة الأمن السيبراني في المملكة؛ تعزيز الأمن السيبراني، ورفع القدرة على مواجهة الأزمات بشتى أنواعها.

	تصنيف (منشآت)	عدد مقدمي المنتجات والخدمات	النسبة من مجموع مقدمي المنتجات والخدمات
الفئة الكبرى	كبيرة متوسطة	91	%22
الفئة الصغرى	صغيرة متناهية الصغر	329	%78

2.2. مساهمة قطاع الأمن السيبراني في الناتج المحلي الإجمالي

بلغت نسبة نمو مساهمة قطاع الأمن السيبراني في الناتج المحلي الإجمالي بالأسعار الجارية لعام 2024م (19%) مقارنة بالعام السابق، إذ تقدر حجم مساهمة القطاع بحوالي (18.5) مليار ريال سعودي. وتمثل هذه المساهمة (0.40%) من الناتج المحلي الإجمالي للمملكة، منها (9) مليارات ريال سعودي، ناتجة عن الأنشطة المباشرة لمقدمي منتجات وخدمات الأمن السيبراني، و(9.5) مليار ريال سعودي من الأنشطة غير المباشرة.

وعند النظر إلى الناتج المحلي للأنشطة غير النفطية، فإن مساهمة قطاع الأمن السيبراني فيه قد بلغت (0.71%)، بارتفاع قدره (11%) مقارنة بالعام الماضي؛ حسب آخر الأرقام المنشورة من قبل الهيئة العامة للإحصاء.

18.5 مليار ﷼

%0.40

مساهمة القطاع في الناتج المحلي الإجمالي

%0.71

مساهمة القطاع في الناتج المحلي للأنشطة غير النفطية

3. أبرز مؤشرات القوى العاملة في قطاع الأمن السيبراني

1.3. حجم كوادر الأمن السيبراني في المملكة

بلغ إجمالي عدد مختصي الأمن السيبراني في المملكة أكثر من (21) ألف مختص خلال عام 2024م، ليسجل بذلك نموا سنويا قدره (9%). ويعمل (2.4) ألف مختص في جهات القطاع العام، في حين يعمل (18.9) ألف مختص لدى منشآت القطاع الخاص، بما في ذلك جهات القطاع الخاص ذات البنى التحتية الحساسة، ومقدمي خدمات ومنتجات الأمن السيبراني. ويُبرز هذا التوزيع الأثر المحوري للقطاع الخاص في نمو القدرات الوطنية للأمن السيبراني، وتعزيز نطاقها.

21.3 ألف
مختص بالأمن السيبراني

2.3. مشاركة المرأة

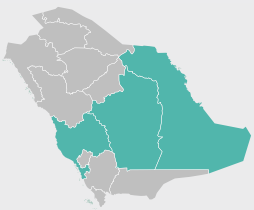
في الوقت الذي تمثل المرأة عالميا ما نسبته (24%)[1] فقط من إجمالي عدد العاملين في مجال الأمن السيبراني، فقد بلغت نسبة مشاركة المرأة في قطاع الأمن السيبراني في المملكة (32%). ويشير هذا إلى التزام المملكة بترسيخ الشمولية، وتوسيع قاعدة الكفاءات العاملة بفضل الدعم والرعاية التي يحظى بهما قطاع الأمن السيبراني في المملكة، من قبل القيادة الرشيدة -أيدها الله.

32%
مشاركة المرأة

3.3. التوزيع الجغرافي

عند النظر إلى التوزيع الجغرافي لمختصي الأمن السيبراني في المملكة، نجد أن (92%) من مختصي الأمن السيبراني يتركزون في منطقة الرياض، ومنطقة مكة المكرمة، والمنطقة الشرقية. وهو ما يتماشى مع التوزيع الاقتصادي للمنشآت على مستوى المملكة.

92%
من مختصي الأمن السيبراني يتواجدون في الرياض، ومكة المكرمة، والمنطقة الشرقية.



1. المتوسط العالمي بناء على: "تقرير القوى العاملة في مجال الأمن السيبراني لعام 2024م: سد النقص في القوى العاملة والمهارات"، GCF & BCG، لعام 2024م.

4.3. مستويات الخبرة

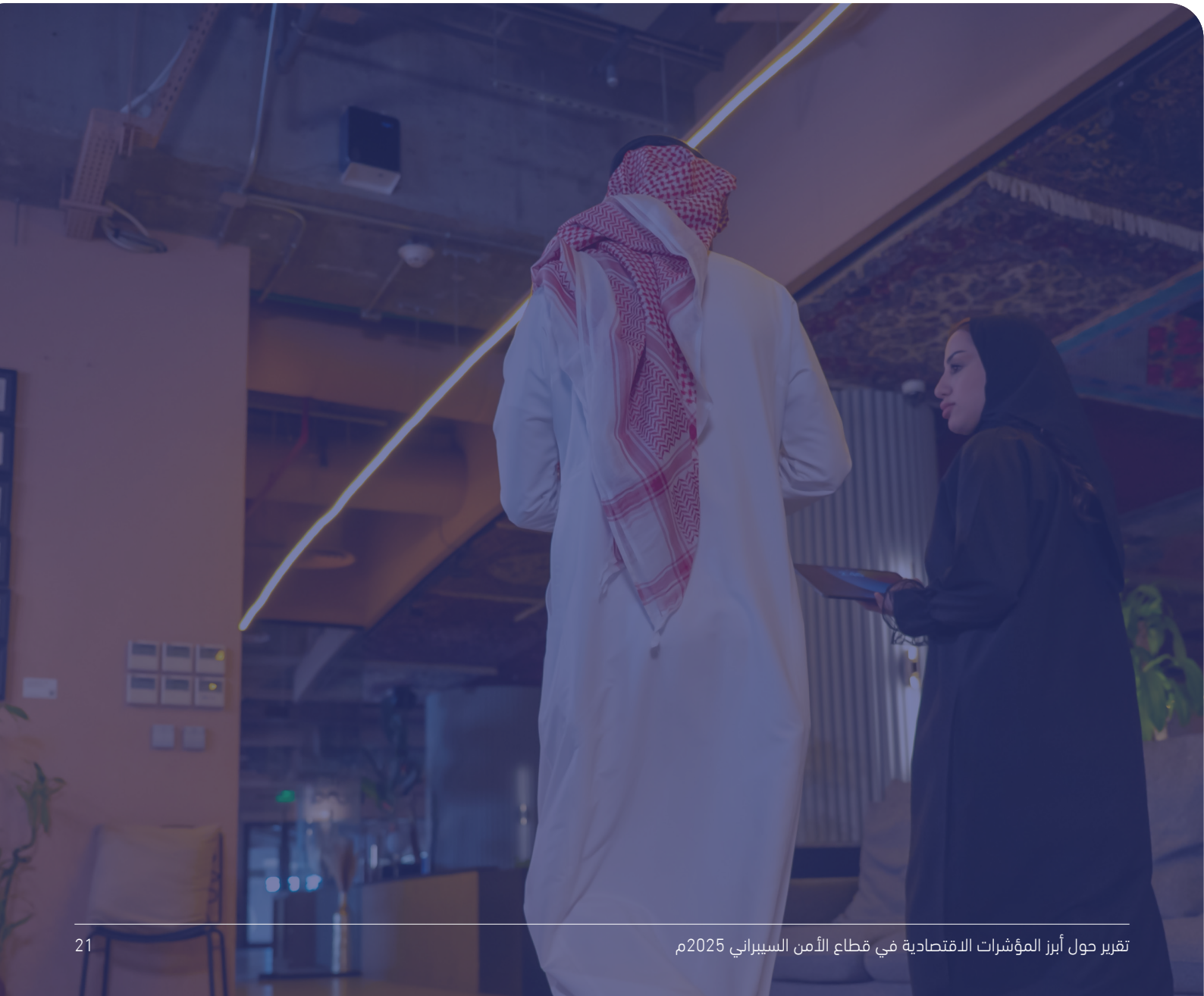
من حيث مستويات الخبرة؛ فإن ما يقارب (57%) من مختصي الأمن السيبراني في المملكة تقل خبرتهم عن (7) سنوات، وهو ما يشير إلى التدفق الكبير للكفاءات الواعدة؛ وهو نتيجة مباشرة لنمو المخرجات الأكاديمية، ولمبادرات تطوير القوى العاملة التي تقودها الهيئة، بدعم من شركاء منظومة الأمن السيبراني من المؤسسات التعليمية. وعلى المدى القريب؛ يتوقع أن يتغير هذا التركيب مع اكتساب المزيد من المختصين خبرات أعلى عبر برامج التطوير المهني، والشهادات الاحترافية، وهو الأمر الذي يُسهم في استمرار نمو القطاع وتعزيز استدامته.

5.3. التعليم في الأمن السيبراني

على مدى الأعوام الستة الماضية؛ ارتفع عدد البرامج والمسارات الأكاديمية المتخصصة في مجال الأمن السيبراني إلى أكثر من ثلاثة أضعاف.وقد جاء ذلك نتيجة لمبادرات الهيئة، وجهود المؤسسات التعليمية؛ بسبب الطلب المتزايد على المختصين المؤهلين، وجاذبية قطاع الأمن السيبراني، بوصفه مسارا مهنيا واعدا. ففي عام 2024م بلغ عدد خريجي برامج الأمن السيبراني ومساراته أكثر من (5) آلاف خريج، وهو ما يزيد على ضعفي عدد خريجي العام السابق. ويشير هذا الارتفاع إلى نضوج متسارع في مخرجات المؤسسات التعليمية للكوادر الوطنية المؤهلة لدخول سوق العمل، والإسهام في القيمة الاقتصادية المستقبلية لقطاع الأمن السيبراني.

5 آلاف

خريج من برامج ومسارات
الأمن السيبراني في المملكة.



ملحق (أ)

تصنيف المنتجات والخدمات في قطاع الأمن السيبراني

المستوى الأول

يوضح المستوى الأول التصنيف الأساسي لأنشطة سوق الأمن السيبراني كمنتجات, 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 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**
2-1	الاستشارات الإدارية في الأمن السيبراني
2-2	تقييم الالتزام بالضوابط السيبرانية
2-3	تقييم المخاطر السيبرانية

4-2	التقييمات الفنية في الأمن السيبراني
5-2	الاستشارات التقنية في الأمن السيبراني
6-2	الاستجابة والتحقيق في الحوادث السيبرانية
7-2	مكافأة اكتشاف الثغرات 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 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 بدءا 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 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 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 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 أيضا 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 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 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 خصيصا 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 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 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 مسبقا.
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 استنادا 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 آليا 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 الأعمال في الحوسبة السحابية	حلول أمن الحوسبة السحابية، التي تحمي الأعمال 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 الإستراتيجية وتقديم التوصيات.

1-1-2	تطوير إستراتيجية الأمن السيبراني وخارطة الطريق	الخدمات الاستشارية في الأمن السيبراني لوضع إستراتيجية 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 إستراتيجية الأمن السيبراني والمعايير الداخلية والخارجية للجهة.
3-1-2	تطوير نموذج قدرات الأمن السيبراني	الخدمات الاستشارية في الأمن السيبراني لتطوير قدرات الأمن السيبراني في الجهة 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 وفقا لمعيار الاعتماد المعترف به خارجيا وبناء 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 وفقا 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 البيئة التقنية.		
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 بشكل 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 بشكل استباقي (تصيد التهديدات) أو تفاعلي (تقييم الاختراق) استجابة 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	مراجعة إعدادات الأمن السيبراني	الخدمات الفنية في الأمن السيبراني لمراجعة التكوين الأمني للأجهزة وتحديد التكوينات الخاطئة وفرص تعزيزها.
8-4-2	التقييم السيبراني والاعتماد للحلول	الخدمات الفنية في الأمن السيبراني لتقييم الحل واعتماده وفقا لمعايير اعتماد مُعترَف بها خارجيا.
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).

7-2 مكافأة اكتشاف الثغرات السيبرانية

الخدمات المقدمة لبرامج اكتشاف الثغرات السيبرانية.

1-7-2	خدمات برامج مكافأة اكتشاف الثغرات السيبرانية (bug bounty)	الخدمات التقنية للأمن السيبراني لتشغيل برنامج يحفّز المخترقين الأخلاقيين لإجراء تقييمات مستقلة والإفصاح المسؤول.

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

4-1 إدارة مركز عمليات الأمن السيبراني

مراقبة الأمن السيبراني وتحديد التهديدات وتصعيد الحوادث.

4-1-1	مراقبة الأمن السيبراني	إدارة خدمات مركز العمليات الأمنية المُدارة التي تُركّز على مراقبة تنبيهات الأمن السيبراني عن بعد من حلول الأمن السيبراني.
4-1-2	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.

4-2 حلول الأمن السيبراني كخدمة

خدمات الأمن السيبراني المتصلة بالإسناد الخارجي لحلول الأمن السيبراني، بما يشمل إدارة الحلول والعمليات.

4-2-1	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.

4-3 الإسناد الخارجي للقوى العاملة في الأمن السيبراني

خدمات الأمن السيبراني المتصلة بإسناد القوى العاملة في الأمن السيبراني إلى الجهات.

4-3-1	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

5-1 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.

5-2 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.

5-3 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).

5-4 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 يعد عرضة للتغيير في أي وقت دون إشعار مسبق.

حقوق الملكية

الهيئة الوطنية
للأمن السيبراني

National Cybersecurity Authority

الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority