هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة، أما البنود الملوّنة بالأخضر فهي أمثلة يجب حذفها، ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج استراتيجية الأمن السيبراني

استبدل <اسم الجهة> باسم الجهة في جميع صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

1. اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
2. أضف "<الجهة>" في مربع البحث عن النص.
3. أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
4. اضغط على "المزيد" وتأكّد من اختيار "Match case".
5. اضغط على "استبدل الكل".
6. أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لتضيف نص

الإصدار: اضغط هنا لتضيف نص

المرجع: اضغط هنا لتضيف نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لتضيف نص	<أدخل التوقيع>

نسخ الوثيقة

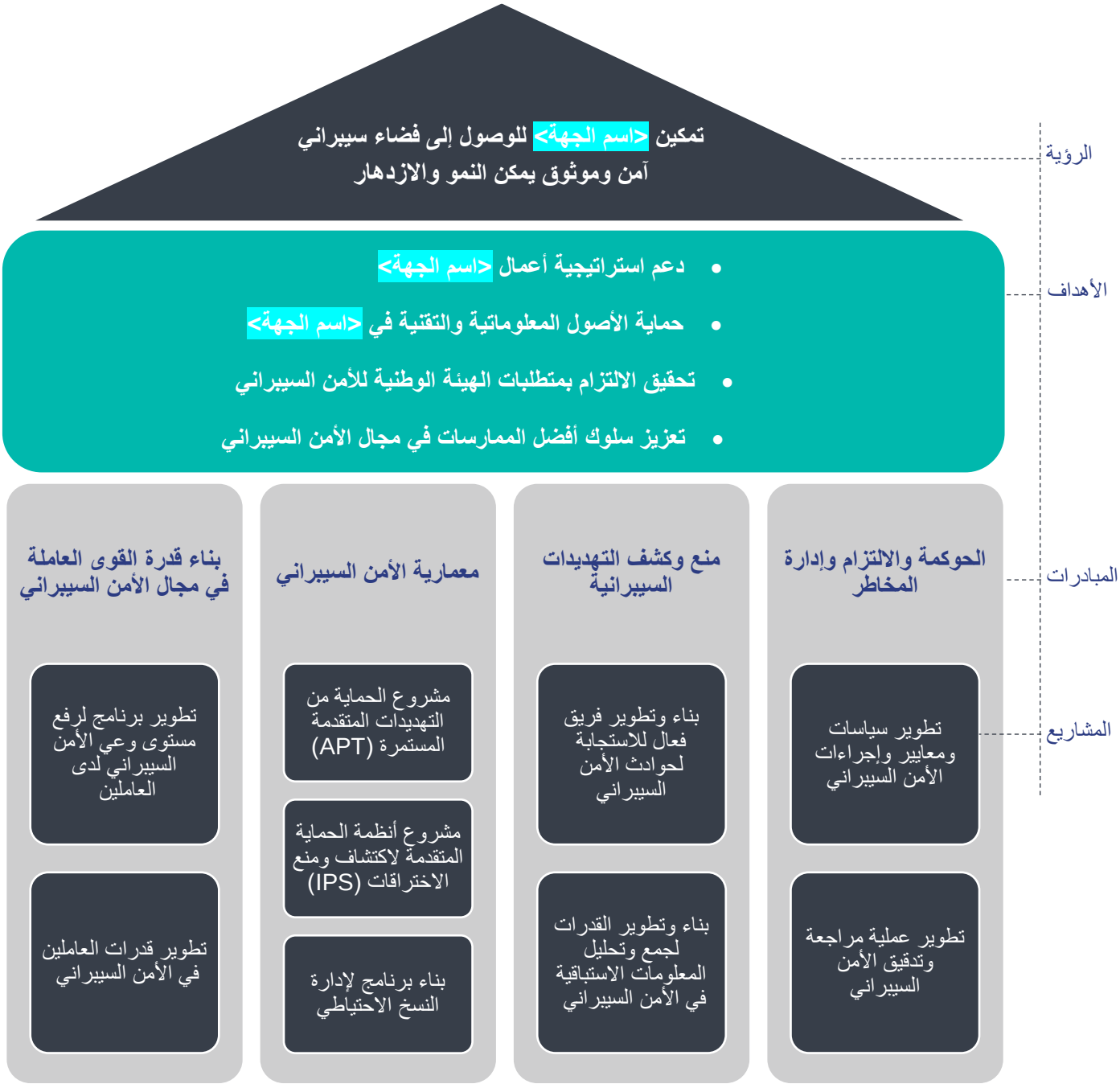
النسخة	التاريخ	عُدّل بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لتضيف نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

الملخص التنفيذي

تسعى <اسم الجهة> إلى تطوير قدراتها في مجال الأمن السيبراني، والمحافظة عليه وتعزيزه في <اسم الجهة> وحمايتها من المخاطر السيبرانية الداخلية والخارجية، وقد أعدّت <اسم الجهة> هذه الاستراتيجية الخاصة بالأمن السيبراني من أجل مواجهة التهديدات وتقليل المخاطر السيبرانية ودعم استراتيجية أعمال <اسم الجهة>.

الشكل أدناه مثال يوضح الملخص التنفيذي لاستراتيجية الأمن السيبراني.
الرؤية والأهداف والمبادرات والمشاريع في هذا النموذج تعتبر أمثلة. الهدف منها توضيح آلية بناء استراتيجية الأمن السيبراني لدى الجهة.



رسم توضيحي1 الملخص التنفيذي لإستراتيجية الأمن السيبراني

مقدمة

تسعى <اسم الجهة> إلى تطوير قدراتها في مجال الأمن السيبراني بهدف تحسين مستوياته، والمحافظة عليه وتعزيزه في <اسم الجهة> وحمايتها من المخاطر السيبرانية الداخلية والخارجية، وقد أعدّت <اسم الجهة> هذه الاستراتيجية الخاصة بالأمن السيبراني لدعم استراتيجية أعمال <اسم الجهة> ومواجهة التهديدات وتقليل المخاطر السيبرانية.

وتستهدف هذه الاستراتيجية بصورة أساسية كلاً من <رئيس الإدارة المعنية بالأمن السيبراني>، وأعضاء اللجنة الإشرافية للأمن السيبراني، ومشرفي الأمن السيبراني في <اسم الجهة>، وغيرهم من المتخصّصين في هذا المجال. وتقع مسؤولية الأمن السيبراني على عاتق جميع العاملين في <اسم الجهة>، ويشمل ذلك الأطراف الخارجية.

وقد صُمّمت استراتيجية الأمن السيبراني لتقديم التوصيات المتعلّقة بأعمال الأمن السيبراني في <اسم الجهة> بشكل يتوافق مع طبيعة العمل، وذلك لتمكين مبادرات الأعمال، وتقديم رؤية واضحة وموحّدة ونشرها بين كافة إدارات وأقسام <اسم الجهة> والجهات والشركات التابعة لها.

وتهدف هذه الوثيقة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي استراتيجية الأمن السيبراني جميع أعمال <اسم الجهة>، وستحرص <اسم الجهة> بدورها والجهات والشركات التابعة لها على تنفيذها.

قم بإزالة التظليلات الصفراء إذا كانت الجهة لا تنوي إضافة أي جهات فرعية تابعة لها في استراتيجياتها للأمن السيبراني.

وتنطبق هذه الاستراتيجية على الجهات والشركات التالية:

1- <اسم الجهة 1>.
2- <اسم الجهة 2>.
3- ...

وبما أن المبادرات المُحدّدة في هذه الاستراتيجية تنطبق على الجهات والشركات وتؤثّر عليها، فإنه من المقرّر الاتفاق على تنفيذها بالتنسيق مع هذه الجهات.

رؤية الأمن السيبراني (Cybersecurity Vision)

1- تقدم رؤية الأمن السيبراني وصفاً موجزاً للمكانة التي تطمح <اسم الجهة> للوصول إليها من حيث وضع أمنها السيبراني خلال السنوات الثلاث المقبلة، كما تصف الوضع المستهدف مستقبلاً للأمن السيبراني في <اسم الجهة>.

2- أخذت <الإدارة المعنية بالأمن السيبراني> بالاعتبار الأهداف الخاصة بـ<اسم الجهة> لضمان توافقها مع رؤية الأمن السيبراني.

من أجل صياغة رؤية الأمن السيبراني، حاول الإجابة على الأسئلة التالية:

السؤال الأول: ما هو التأثير الجوهري الذي سيُحدثه الأمن السيبراني في المجتمع والأعمال والعالم؟

السؤال الثاني: كيف ستتعامل إدارة الأمن السيبراني مع المستفيدين من خدمات الجهة؟

السؤال الثالث: كيف ستكون الثقافة السائدة في الجهة وما الدور الذي ستكون مسؤولة عنه في حياة العاملين والمستفيدين؟

السؤال الرابع: كيف ستساهم الجهة والإدارة في تحقيق رؤية الاستراتيجية الوطنية للأمن السيبراني؟

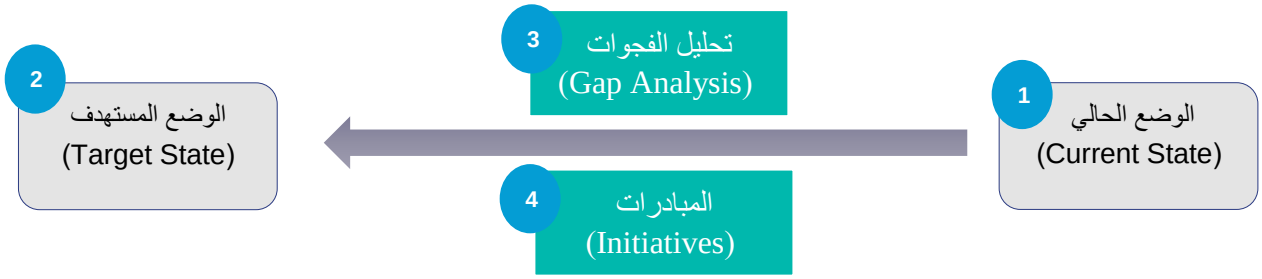
رؤية الأمن السيبراني

تمكين <اسم الجهة> للوصول إلى فضاء سيبراني آمن وموثوق يمكن النمو والازدهار

الرؤية والأهداف والمبادرات والمشاريع وآلية تقييم الوضع الحالي في هذا النموذج تعتبر أمثلة. الهدف منها توضيح آلية بناء استراتيجية الأمن السيبراني لدى الجهة

مدخلات الاستراتيجية (Inputs into the Strategy)

تعدّ رؤية المملكة العربية السعودية وتوجّهاتها في مجال الأمن السيبراني من المدخلات الأساسية في تطوير استراتيجية الأمن السيبراني الخاصة بـ<اسم الجهة>، بالتالي، من المهم فهم دور <اسم الجهة> ومساهمتها في الاستراتيجية الوطنية للأمن السيبراني من أجل مواءمة أهداف استراتيجيتها للأمن السيبراني مع أهداف الاستراتيجية الوطنية.

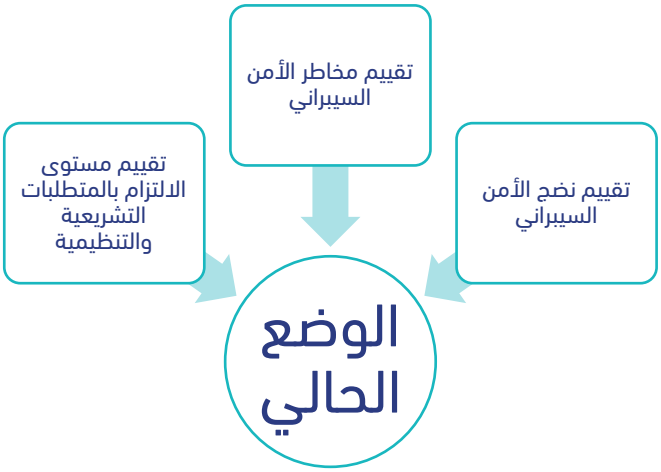


رسم توضيحي 2: مكونات الاستراتيجية

الوضع الحالي للأمن السيبراني (Cybersecurity Current State)

تعرض الأنشطة الموضّحة أدناه أمثلة على المدخلات التي تُشكّل استراتيجية الأمن السيبراني الخاصة بـ<اسم الجهة> وفقاً للاستراتيجية الوطنية للأمن السيبراني، والهدف من هذه الأنشطة هو تحديد الوضع المستهدف للأمن السيبراني مقارنةً مع الوضع الحالي:

1- تقييم مستوى الالتزام بالمتطلبات التنظيمية والتشريعية، مثل الضوابط الأساسية للأمن السيبراني (ECC)
2- تقييم مخاطر الأمن السيبراني (Cybersecurity Risk Assessment "CSRA")
3- تقييم نضج الأمن السيبراني (Cybersecurity Maturity Assessment "CSMA")



رسم توضيحي 3: آلية تحديد الوضع الحالي

الرؤية والأهداف والمبادرات والمشاريع وآلية تقييم الوضع الحالي في هذا النموذج تعتبر أمثلة. الهدف منها توضيح آلية بناء استراتيجية الأمن السيبراني لدى الجهة

أهداف الأمن السيبراني (Cybersecurity Objectives)

حُدّدت أهداف الأمن السيبراني وفقاً لرؤية الأمن السيبراني ونتائج الأنشطة التي تم توضيحها في قسم الوضع الحالي للأمن السيبراني، وهي كالتالي:

1- **دعم استراتيجية أعمال <اسم الجهة>:** ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل <اسم الجهة> في تحقيق الأهداف والمتطلبات التشريعية والتنظيمية ذات العلاقة.
2- **حماية الأصول المعلوماتية والتقنية في <اسم الجهة>**: توفير الحلول التقنية اللازمة لحماية الأصول المعلوماتية والتقنية في<اسم الجهة>.
3- **تعزيز سلوك أفضل الممارسات في مجال الأمن السيبراني:** تطوير العاملين بالمهارات والمؤهلات في مجال الأمن السيبراني، وتعزيز الوعي بالأمن السيبراني من خلال قنوات متعددة، وبناء ثقافة إيجابية للأمن السيبراني.

تحليل الفجوات (Gap Analysis)

بناءً على نتائج تقييم مستوى الالتزام بتطبيق الضوابط الأساسية للأمن السيبراني، وتقييم مخاطر الأمن السيبراني، وتحليل تأثير الأعمال، وتقييم نضج الأمن السيبراني، يتم إجراء التحليل الرباعي (SWOT) لـ<اسم الجهة> لتحليل الفجوات بين الوضع الراهن والوضع المستهدف للأمن السيبراني في <اسم الجهة>، ويوضح هذا

اختر التصنيف

التحليل مواضع القوة والضعف لدى <اسم الجهة>، ومواضع الفرص التي يمكن لـ<اسم الجهة> استغلالها والتهديدات التي تواجهها.

	مفيدة	ضارّة
داخلية	**القوّة** العناصر الداخلية التي تمتاز بها <اسم الجهة> تفعيل حلول أمن أجهزة المستخدمين بشكل كافٍ على جميع الخوادم وأجهزة المستخدمين. تطبيق حلول أمن البريد الإلكتروني. تطبيق حلول التشفير الكامل. <أدخل نقطة القوّة 1>، <أدخل نقطة القوّة 2>، ...	**الضعف** العناصر الداخلية التي تؤثر سلباً على <اسم الجهة> عدم وجود الوعي الكافي بالأمن السيبراني وتهديداته ومخاطره لدى العاملين. عدم وجود حلول للحماية من التهديدات المتقدمة والمستمرة. عدم وجود تقنيات أمن أسماء النطاقات. <أدخل نقطة الضعف 1>، <أدخل نقطة الضعف 2>، ...
خارجية	**الفرص** العناصر الخارجية التي يُمكن استغلالها لمصلحة <اسم الجهة> يعمل الكثير من الخريجين السعوديين الموهوبين والأكفاء في مجال الأمن السيبراني. إنشاء الهيئة الوطنية للأمن السيبراني التي تدعم الجهات في الاستجابة لحوادث الأمن السيبراني. مبادرة CyberPro لتدريب متخصصين في مجال الأمن السيبراني. <أدخل الفرصة 1>، <أدخل الفرصة 2>، ...	**التهديدات** العناصر الخارجية التي قد تسبّب بعض المشاكل لـ<اسم الجهة> تغيّر الأنظمة التقنية بصورة متكرّرة و/أو قلّة الأنظمة المتعلّقة بالأمن السيبراني. التقدم السريع والمستمر في التقنية. <أدخل التهديد 1>، <أدخل التهديد 2>، ...

عناصر القوة والضعف والفرص والتهديدات في هذا النموذج تعتبر أمثلة. الهدف منها توضيح آلية بناء استراتيجية الأمن السيبراني لدى الجهة

مبادرات الأمن السيبراني (Cybersecurity Initiatives)

1- تتضمّن مبادرات الأمن السيبراني جميع المشاريع والبرامج المطلوبة لتنفيذ أهداف استراتيجية الأمن السيبراني، وتُشكَّل هذه المبادرات بناءً على رؤية الأمن السيبراني وأهدافها:

- **الحوكمة والالتزام وإدارة المخاطر:** تشتمل المبادرة على مشاريع وبرامج في الحوكمة والمخاطر والالتزام لتعزيز الأمن السيبراني في <اسم الجهة> وبناء الخطط الاستراتيجية في الأمن السيبراني.
- **منع وكشف التهديدات السيبرانية:** تشتمل المبادرة على مشاريع وبرامج تساعد <اسم الجهة> على كشف ومنع التهديدات الداخلية والخارجية.
- **معمارية الأمن السيبراني:** تشتمل المبادرة على مشاريع وبرامج تساعد <اسم الجهة> على زيادة مستوى نضجها في الأمن السيبراني وحماية <اسم الجهة> من المخاطر السيبرانية.
- **بناء قدرة القوى العاملة في مجال الأمن السيبراني:** تشتمل هذه المبادرة على مشاريع وبرامج تهدف إلى رفع الوعي بالأمن السيبراني وتعزيز العاملين في <الإدارة المعنية بالأمن السيبراني> بالمهارات والمؤهلات في مجال الأمن السيبراني.

2- يُوضّح الجدول أدناه علاقة أهداف الأمن السيبراني مع مبادرات الأمن السيبراني.

الأهداف / المبادرات	الحوكمة والالتزام وإدارة المخاطر	منع وكشف التهديدات السيبرانية	معمارية الأمن السيبراني	بناء قدرة القوى العاملة في مجال الأمن السيبراني
دعم استراتيجية أعمال <اسم الجهة>	√	-	-	-
حماية الأصول المعلوماتية والتقنية في <اسم الجهة>	-	√	√	-
تعزيز سلوك أفضل الممارسات في مجال الأمن السيبراني	-	-	-	√

3- سعياً لتحقيق الأهداف المتعلّقة بالأمن السيبراني، قسّمت <اسم الجهة> المبادرات السيبرانية إلى مشروع واحد أو أكثر لتحديد مؤشر قياس الأداء وطريقة قياسه.

#	مبادرات الأمن السيبراني	مشاريع الأمن السيبراني
1	**الحوكمة والالتزام وإدارة المخاطر**	تطوير سياسات ومعايير وإجراءات الأمن السيبراني
		تطوير عملية مراجعة وتدقيق الأمن السيبراني
		تطوير إطار لإدارة الأمن السيبراني
2	**منع وكشف التهديدات السيبرانية**	بناء وتطوير فريق فعال للاستجابة لحوادث الأمن السيبراني
		بناء وتطوير فريق لجمع وتحليل المعلومات الاستباقية في الأمن السيبراني
3	**معمارية الأمن السيبراني**	مشروع الحماية من التهديدات المتقدمة المستمرة (APT)
		مشروع أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (IPS)
		بناء برنامج لإدارة النسخ الاحتياطي
4	**بناء قدرة القوى العاملة في مجال الأمن السيبراني**	تطوير برنامج لرفع مستوى وعي الأمن السيبراني لدى العاملين
		تطوير قدرات العاملين في الأمن السيبراني

الأهداف والمبادرات والمشاريع وآلية تقييم الوضع الحالي في هذا النموذج تعتبر أمثلة. الهدف منها توضيح آلية بناء استراتيجية الأمن السيبراني لدى الجهة

من أجل تحديد كيفية قياس مبادرات الأمن السيبراني، حاول الإجابة على السؤال التالي:

السؤال: ما الذي سنعرضه على مدير الإدارة المعنية بالأمن السيبراني كمؤشر على فاعلية أداء مبادرة الأمن السيبراني؟

يجب أن تكون مؤشرات قياس الأداء الرئيسية "SMART":

- محددة (Specific) - يجب أن تستهدف منطقة محددة للتحسين.
- قابلة للقياس (Measurable) - ينبغي أن تحدد أو تشير على الأقل إلى مؤشر تقدم.
- قابلة للتحقيق (Achievable) - يجب أن تُوضح النتائج التي يمكن تحقيقها بشكل واقعي في ضوء الموارد المتاحة.
- مسؤولة (Responsible) - يجب تطويرها بحيث تُعرف المسؤولية بوضوح.
- مرتبطة بالوقت (Time-Related) – يجب أن تحدد متى يمكن تحقيق النتائج.

يجب أن تتبع مؤشرات الأداء الرئيسية نهجاً كمياً ونوعياً مع التركيز على كلٍ من التأثير والنتائج.

اختر التصنيف

4- يمكن قياس مبادرات الأمن السيبراني من خلال المقاييس التالية.

#	مبادرة الأمن السيبراني	مؤشر الأداء الرئيسي التشغيلي للأمن السيبراني	المستهدف		
			السنة الأولى	السنة الثانية	السنة الثالثة
1	**بناء قدرة القوى العاملة في مجال الأمن السيبراني**	عدد رسائل البريد الإلكتروني التي أرسلت للتوعية بالأمن السيبراني	6	12	24
		عدد جلسات التدريب التي عُقدت حول الأمن السيبراني	5	10	15
2	**الحوكمة والالتزام وإدارة المخاطر**	النسبة المئوية للخطط والإجراءات التي تم اختبارها مقابل التي تم تطويرها	%80	%90	%100
<#>	<أدخل مبادرة الأمن السيبراني>	<أدخل مؤشر الأداء الرئيسي التشغيلي>	<#>	<#>	<#>

من أجل قياس وتقييم مؤشرات قياس الأداء لمبادرات الأمن السيبراني، اتبع المبادئ التالية:

- النظر في اعتماد إطار تحسين مستمر لبرنامج الأمن السيبراني (على سبيل المثال: دورة PDCA وفقاً لمعايير ISO 27001).
- تَذكّر نطاق المؤشر، والنتائج المتوقعة، ووتيرة القياس.
- تنفيذ مبدأ "فصل المهام" - تعيين طرف مستقل (مثل مشرف أو طرف خارجي موثوق به) لقياس مؤشر الأداء الرئيسي.
- تمكين الطرف المستقل ومنحه الصلاحيات والأدوار والمسؤوليات المناسبة.
- النظر في تقييم بعض مؤشرات الأداء الرئيسية من خلال الاستبيانات واستطلاعات الرأي.
- تطوير إطار لجمع البيانات للحصول على البيانات ذات الصلة لتقييم وقياس مؤشرات الأداء الرئيسية، ويجب أن تكون عملية جمع البيانات شاملة.
- تطوير تقرير يصف النتائج المحققة وتوقعات التقييم التالي.

خارطة طريق الأمن السيبراني (Cybersecurity Roadmap)

1- تحديد خطة عمل لتحقيق أهداف استراتيجية الأمن السيبراني.

2- تُوفّر الاستراتيجية العناصر الأساسية لخطّة العمل والمكوّنة من مبادرات الأمن السيبراني التي بدورها تُحقّق أهداف الأمن السيبراني في حال تنفيذها (الأهداف مذكورة بالتفصيل في قسم أهداف الأمن السيبراني).

3- تُصاغ خطّة عمل الاستراتيجية وفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4- تتضمّن خطّة عمل الاستراتيجية بنوداً خاصة بالمراقبة ومؤشرات قياس الأداء لتحديد مستوى النجاح، مما يُمكّن من تقديم الملاحظات إلى <رئيس الإدارة المعنية بالأمن السيبراني> واللجنة الإشرافية للأمن السيبراني، ويُتيح ذلك إدخال التعديلات على الخطّة وضمان تنفيذ مبادرات الأمن السيبراني بصورة صحيحة لتحقيق الأهداف.

5- توضح خارطة طريق الأمن السيبراني طريقة توزيع المبادرات المقرّر تنفيذها على مدى الثلاث سنوات القادمة، إذ تُمنَح الأولوية لمبادرات الأمن السيبراني بناءً على نتائج تحليل المخاطر وتحليل تأثير الأعمال (BIA) المؤضّحة في قسم تقييم المخاطر وتحليل تأثير الأعمال، كما تمنح خارطة الطريق الأولوية للتعامل مع المخاطر العالية، بالإضافة إلى التعامل مع الأنظمة الحسّاسة، وتم تطوير خارطة طريق الأمن السيبراني في ورقة العمل أدناه.

خارطة طريق الأمن السيبراني

خارطة طريق الأمن السيبراني.xlsx

لتعبئة ورقة العمل، اتّبع الخطوات التالية:
1. اضغط مرّتين على أيقونة ورقة العمل.
2. اتبع التعليمات وقم بتعبئة ورقة العمل بالمعلومات المناسبة.
3. أغلق ورقة العمل.

قائمة المبادرات والمشاريع

1- أعدّت <اسم الجهة> بيانات تفصيلية للمبادرات والمشاريع المستهدفة في استراتيجية الأمن السيبراني وفقاً لورقة العمل التالية:

بيانات مبادرات ومشاريع الأمن السيبراني

بيانات مبادرات ومشاريع الأمن السيبراني.xlsx

المبادرات والمشاريع وآلية تقييم الوضع الحالي في هذا النموذج تعتبر أمثلة. الهدف منها توضيح آلية بناء استراتيجية الأمن السيبراني لدى الجهة

ميزانية الأمن السيبراني (Cybersecurity Budget)

الغرض من ميزانية الأمن السيبراني هو تحديد الميزانية اللازمة لتنفيذ خطّة عمل الأمن السيبراني والمبادرات، والحصول على الاعتمادات اللازمة لتخصيصها من قبل <الإدارة المعنية بالشؤون المالية>.

خصائص الميزانية

1- <الإدارة المعنية بالأمن السيبراني> مسؤولة عن إعداد الميزانية الخاصة بالأمن السيبراني باعتبارها أفضل طريقة لضمان توفير التقنيات والأدوات المتعلقة بالأمن السيبراني، كما يتولّى <رئيس الإدارة المعنية بالأمن السيبراني> مسؤولية تقديم ملخّص عن النفقات المتعلّقة بميزانية الأمن السيبراني إلى <صاحب الصلاحية>.

2- يتم تخصيص ميزانية للأمن السيبراني لتغطي جميع تكاليف خطة عمل الأمن السيبراني، لذلك يجب أن تكون دقيقة ومنطقية وشاملة للمبالغ المتوقع صرفها.

3- يجب أن تكون ميزانية الأمن السيبراني متوافقة مع السياسات والمتطلبات التشريعية والتنظيمية والأوامر والقرارات ذات العلاقة.

4- تُحدّد ميزانية الأمن السيبراني بناءً على دورة الميزانية السنوية الخاصة بـ<اسم الجهة>.

5- تخضع ميزانية الأمن السيبراني إلى مراجعة دورية وفقاً للسياسات والإجراءات المعتمدة في <اسم الجهة>.

مكوّنات الميزانية

1- تشتمل ميزانية الأمن السيبراني على المكوّنات التالية:

1-1 ميزانية تشغيل الإدارة المعنية بالأمن السيبراني، وتشمل الآتي:

اختر التصنيف

1-1-1 تكلفة موظفي الأمن السيبراني.

2-1-1 تكلفة الخدمات الاستشارية.

3-1-1 تكلفة الخدمات التقنية.

4-1-1 تكاليف أخرى.

2-1 ميزانية مبادرات الأمن السيبراني، وتشمل الآتي:

1-2-1 تكاليف غير متكرّرة لإنشاء الإدارة المعنية بالأمن السيبراني والعمليات ذات العلاقة لتنفيذ استراتيجية الأمن السيبراني.

2-2-1 تكاليف متكرّرة تغطي تدابير الأمن السيبراني (مثل: إدارة الأمن السيبراني، والمراقبة، وإعداد التقارير، والالتزام، وغيرها).

3-2-1 تكلفة برامج تطوير المهارات المتخصصة والتدريب اللازم لموظفي الأمن السيبراني مثل الدورات التدريبية والمؤتمرات.

4-2-1 تكلفة خدمات الإسناد الخارجي.

حساب ميزانية الأمن السيبراني

عند حساب ميزانية الأمن السيبراني، يجب على الجهة إجراء البحوث المناسبة فيما يتعلق بمتوسط التكاليف، ويشمل ذلك تكلفة التقنيات وتكلفة الموظفين (أي الرواتب) وتكلفة البنية التحتية وما إلى ذلك. يجب أن تكون الجهة على دراية بنماذج التسعير المختلفة وينبغي توحيد النماذج للمقارنة بفعالية. على سبيل المثال، قد تتبع بعض البرمجيات نموذج تسعير لكل مستخدم، بينما قد تتبع برمجيات أخرى نموذج تسعير لكل جهاز أو نموذج تسعير الدفع مرة واحدة. يجب على الجهة مراعاة قدرة أداء الإدارة المعنية بالأمن السيبراني، كما يجب أن تضع افتراضات حول ما إذا كانت المبادرات ستنفذ داخلياً أو بمساعدة طرف خارجي أو استشاري.

1- تم حساب ميزانية الأمن السيبراني الخاصة بـ<اسم الجهة> وفقاً لورقة العمل التالية:

حساب ميزانية الأمن السيبراني

ميزانية الأمن السيبراني.xlsx

لتعبئة ورقة العمل، اتّبع الخطوات التالية:
1. اضغط مرّتين على أيقونة ورقة العمل.
2. اتبع التعليمات وقم بتعبئة ورقة العمل بالمعلومات المناسبة.
3. أغلق ورقة العمل.

2- ميزانية الأمن السيبراني التي خصّصتها <اسم الجهة> لاستراتيجية الأمن السيبراني التي ستستمر للسنوات الثلاث القادمة هي: <تحدد من قبل الجهة> ريال سعودي.

الأدوار والمسؤوليات

1- **راعي ومالك الوثيقة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **تحديث الوثيقة ومراجعتها:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ الوثيقة وتطبيقها:** <الإدارة المعنية بالأمن السيبراني>.

اختر التصنيف