هيئة تنظيم الاتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

الاستراتيجية الوطنية للأمن السيبراني

@THEUAETRA
www.tra.gov.ae

الحاجة لاستراتيجية الأمن السيبراني

تضاعف عدد حوادث الأمن السيبراني

عالمياً في العام الماضي، مما تسبب بخسائر كبيرة في الاقتصاد العالمي

2x

عدد حوادث الأمن السيبراني عالمياً
(2017-2016)

42%

زيادة عدد الاختراقات الأمنية للبيانات عالميًا
(2017-2015)

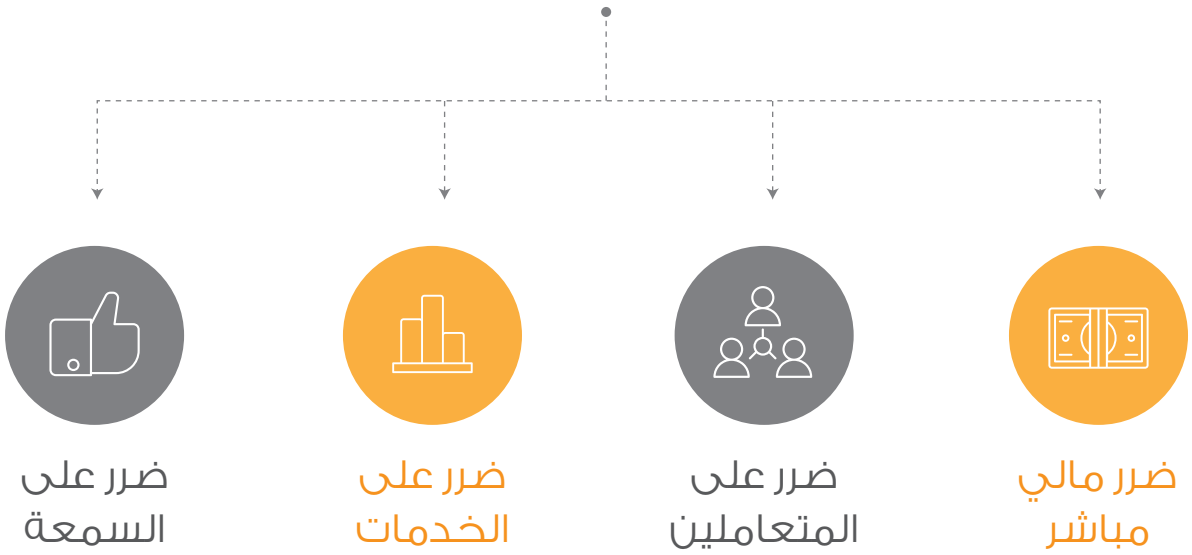
608

الخسائر السنوية بسبب الجرائم السيبرانية عالمياً
(مليار دولار أميركي، 2017-2014)

3.9

معدل الخسائر الإجمالية لاختراقات البيانات
(مليار دولار أمريكي، 2018-2017)

أضرار حوادث الأمن السيبراني تتجاوز الخسائر الاقتصادية



اعتمدنا ثلاثة مصادر رئيسية

لتطوير الاستراتيجية الوطنية للأمن السيبراني في دولة الإمارات العربية المتحدة

تقارير عالمية

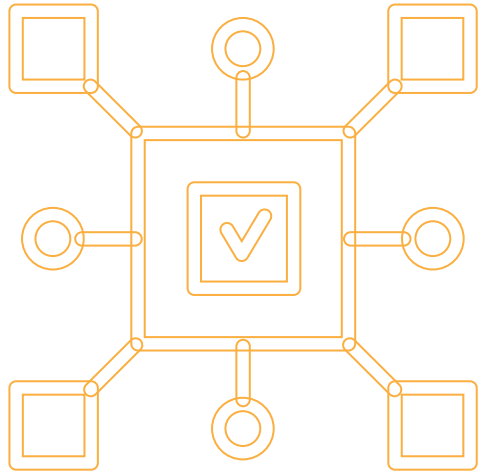
تحليل أكثر من 50 مصدراً من المؤشرات والمنشورات العالمية

خبراء الأمن السيبراني

فريق من الخبراء العالميين من ذوي الخبرة الكبيرة في مواضيع الأمن السيبراني

مقارنات مرجعية مع 10 دول

مقارنة معيارية مع 10 دول رائدة في مجال أنظمة الأمن السيبراني



تطلعاتنا حول الاستراتيجية الوطنية للأمن السيبراني

رؤيتنا حول الاستراتيجية الوطنية للأمن السيبراني في الدولة

خلق بيئة سيبرانية آمنة ومرنة في الدولة تساعد على تمكين الأفراد من تحقيق طموحاتهم وتمكين الشركات من التطور

رؤيتنا تشمل جميع شرائح المجتمع

تطلعاتنا

تعزيز ثقة أفراد المجتمع
للمشاركة بشكل آمن في العالم الرقمي

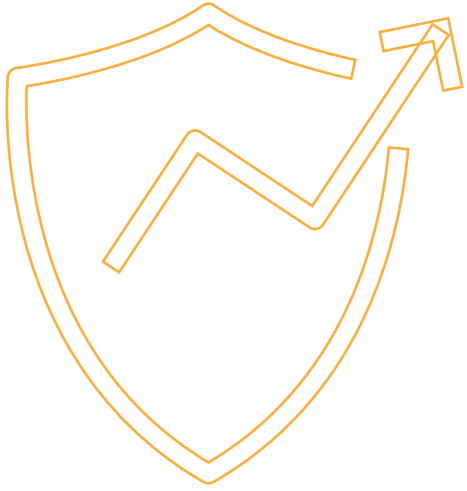
تعزيز الابتكار في مجال الأمن السيبراني

ترسيخ ثقافة الاستثمار في الأمن السيبراني

تمكين الشركات الصغيرة
من حماية نفسها ضد الهجمات السيبرانية

حماية المعلومات الحساسة والبنية التحتية للدولة

بناء كادر بشري على مستوى عالمي في مجال الأمن
السيبراني في الدولة



محاور الاستراتيجية

لتحقيق هذه التطلعات

نعمل على إنشاء منظومة متكاملة للأمن السيبراني من خلال تنفيذ **60** مبادرة ضمن **5** محاور

قوانين ولوائح الأمن السيبراني

- التطرق إلى جميع أنواع الجرائم السيبرانية
- حماية التقنيات الحالية والناشئة
- تعزيز حماية الشركات الصغيرة والمتوسطة

بيئة حيوية للأمن السيبراني

- دعم الشركات الناشئة وتعزيز البحث والتطوير
- تطوير القدرات
- تعزيز وعي الأفراد
- تشجيع التميز

الخطة الوطنية للاستجابة للحوادث السيبرانية

- وسيلة موحدة للإبلاغ عن الحوادث السيبرانية
- نموذج موحد لتقييم الخطورة وخطة للتعامل مع الحوادث
- مشاركة المعلومات الاستخبارية بين الجهات

برنامج حماية البنية التحتية للمعلومات الحيوية

- تحديد الأصول الحيوية في الدولة
- وضع معايير عالمية لإدارة المخاطر
- وضع عمليات فعالة للإبلاغ والامتثال والاستجابة

الشراكات

- القطاع الحكومي
- القطاع الخاص
- المؤسسات الأكاديمية
- الجمعيات والمنظمات الدولية

قوانين ولوائح الأمن السيبراني

تصميم إطار قانوني وتنظيمي شامل للأمن السيبراني

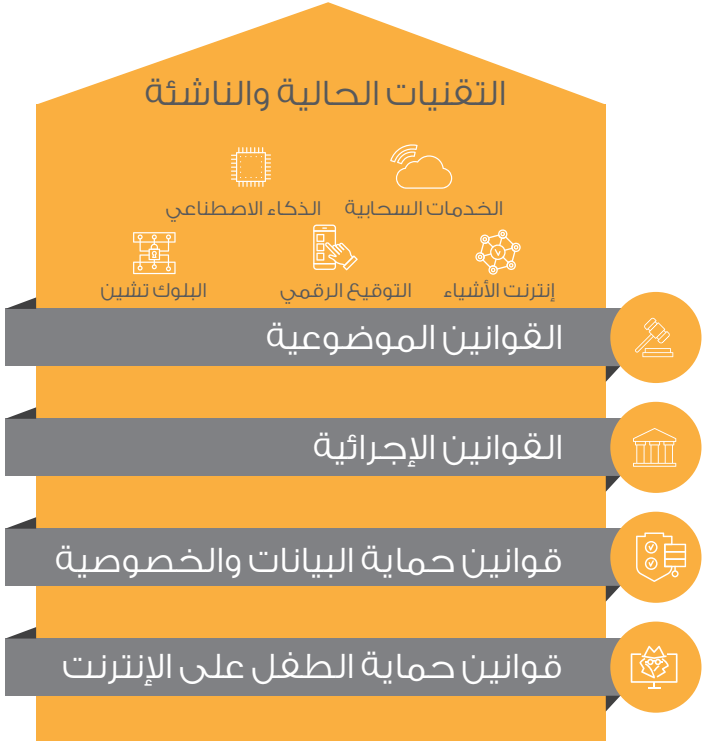
تطلعاتنا

وضع إطار قانوني لمعالجة جميع أنواع الجرائم السيبرانية

بناء إطار تنظيمي لحماية التقنيات الحالية والناشئة

القوانين

ستتحقق من خلال إطار قانوني وتنظيمي شامل



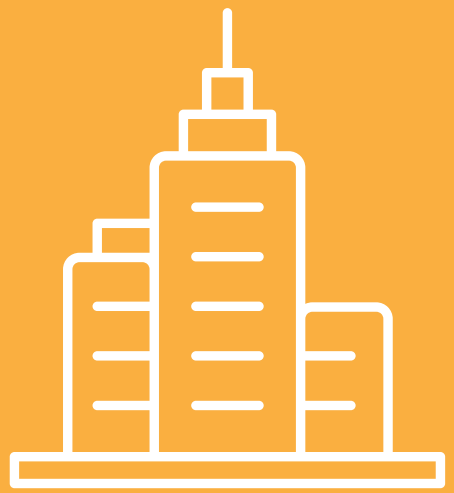
تعزيز حماية الشركات الصغيرة والمتوسطة في الدولة

تطلعاتنا

- تقديم إرشادات للحماية من التهديدات السيبرانية الأكثر شيوعًا
- تقديم حوافز لتنفيذ الإرشادات الموصى بها
- وضع أنظمة داعمة لتمكين الشركات الصغيرة والمتوسطة من تنفيذ الإرشادات

ستتحقق من خلال إطار قانوني وتنظيمي شامل

- تطوير معيار للأمن السيبراني خاص بالشركات الصغيرة والمتوسطة
- إلزام موردي الجهات الحكومية بحيازة شهادة تطبيق الأمن السيبراني
- تطوير بوابة موحدة للشركات الصغيرة والمتوسطة لتمكينها من تنفيذ المعيار



بيئة حيوية للأمن السيبراني

تمكين المنظومة من الاستفادة من الإمكانات الضخمة التي يوفرها الأمن السيبراني

تطلعاتنا

- الاستفادة من سوق الأمن السيبراني في الدولة الذي تصل قيمته إلى 1.8 مليار درهم
- المشاركة بفعالية في سوق الأمن السيبراني في منطقة الشرق الأوسط وشمال أفريقيا

ستتحقق من خلال 24 مبادرة عبر 7 محاور

- خلق الحاجة
- تسهيل ممارسة الأعمال
- تسهيل الحصول على التمويل
- دعم قطاع الأعمال
- الثقافة والوعي
- التعليم وتنمية المهارات
- الابتكار واعتماد التكنولوجيا

تطوير قدرات أكثر من 40,000 من المتخصصين في الأمن السيبراني

تطلعاتنا

- تشجيع المهنيين والطلبة على الانخراط في مجال الأمن السيبراني
- بناء القدرات في الأمن السيبراني بما يلبي تطلعات الدولة
- تطوير منظومة متكاملة في مجال التدريب في الأمن السيبراني

ستتحقق من خلال 12 مبادرة

- الأفراد: 7 مبادرات
- جهات التدريب: 5 مبادرات

زيادة وعي أفراد المجتمع بالأمن السيبراني

تطلعاتنا

- تعزيز وعي أفراد المجتمع حول المخاطر المتعلقة بالإنترنت
- تشجيع اتباع الممارسات الآمنة في التعامل مع التقنية
- تشجيع المؤسسات على نشر الوعي السيبراني بفاعلية

ستتحقق من خلال 12 مبادرة تستهدف شرائح مختلفة من المجتمع

- الأطفال واليافعين
- طلبة الجامعات
- الموظفون
- ربات المنازل وكبار المواطنين
- أصحاب الهمم

مكافأة التميز في مجال الأمن السيبراني من خلال برامج الجوائز الوطنية

تطلعاتنا

- تشجيع المؤسسات على إطلاق برامج في الأمن السيبراني
- إلهام رواد الأعمال للابتكار في مجال الأمن السيبراني
- دعم الأبحاث الخلاقة في المؤسسات الأكاديمية
- تشجيع الطلبة على الانخراط في مجال الأمن السيبراني

ستتحقق من خلال مكافأة مساهمات المؤسسات والأفراد

المؤسسات	6 جوائز
الأفراد	6 جوائز

الخطة الوطنية للاستجابة للحوادث السيبرانية

وضع خطة وطنية فعالة للاستجابة للحوادث السيبرانية لتمكين الاستجابة السريعة والمنسقة في الدولة

تطلعاتنا

- تنظيم آلية الكشف عن حوادث الأمن السيبراني والإبلاغ عنها
- إنشاء منهجية موحدة لتقييم درجة خطورة الحوادث لتوفير الدعم المناسب
- بناء قدرات وطنية على مستوى عالمي للاستجابة لجميع أنواع الحوادث السيبرانية

ستتحقق من خلال 4 مبادرات رئيسية

- وسيلة موحدة للإبلاغ عن الحوادث السيبرانية
- توفير التقارير الإرشادية للحماية من التهديدات
- الرصد الفعال للتهديدات السيبرانية
- تبادل المعلومات الاستخبارية بين الجهات المختلفة

برنامج حماية البنية التحتية للمعلومات الحيوية

حماية الأصول الحيوية لدولة الإمارات العربية المتحدة في 9 قطاعات

تطلعاتنا

حماية الأصول في 9 قطاعات حيوية في الدولة

- الطاقة
- الاتصالات وتقنية المعلومات
- القطاع الحكومي
- الكهرباء والمياه
- القطاع المالي والتأمين
- خدمات الطوارئ
- الخدمات الصحية
- المواصلات
- الغذاء والزراعة

سيتم تحقيقها من خلال برنامج متكامل لحماية البنية التحتية للمعلومات الحيوية

- تحديد القطاعات الحيوية والأصول والمخاطر المرتبطة بها
- وضع معايير عالمية لإدارة المخاطر
- تطبيق إجراءات فعالة للإبلاغ والامتثال والاستجابة

الشراكات

دعم عمل المنظومة بأكملها من خلال شراكات محلية وعالمية

الشراكات هي المحرك الأساسي لتحقيق أهدافنا وطموحاتنا في الأمن السيبراني سوية

الحوكمة

لتطبيق الاستراتيجية بالشكل الأمثل، سنفعّل مجموعة من فرق العمل الوطنية

تسع لجان للقطاعات لتنفيذ برنامج حماية البنية التحتية للمعلومات الحيوية

- الطاقة
- الاتصالات وتقنية المعلومات
- القطاع الحكومي
- الكهرباء والمياه
- القطاع المالي والتأمين
- خدمات الطوارئ
- الخدمات الصحية
- المواصلات
- الغذاء والزراعة

وفريقين لتنفيذ الخطة الوطنية للاستجابة للحوادث السيبرانية

اللجنة الوطنية للاستجابة للحوادث السيبرانية (NRC)

اتخاذ القرارات الاستراتيجية المتعلقة بالخطة الوطنية للاستجابة للحوادث السيبرانية

وحدة الاستخبارات السيبرانية (CIU)

تمكين مشاركة المعلومات الاستخبارية بين المؤسسات لتحسين الاطلاع على التهديدات السيبرانية

ستقوم الهيئة العامة لتنظيم قطاع الاتصالات بمراقبة تقدم وأثر الاستراتيجية الوطنية للأمن السيبراني من خلال 20 مؤشر أداء محدد وواضح

جمع البيانات من مصادر متعددة

1. **بيانات الهيئة الداخلية** مخرجات البيانات الصادرة عن فرق المبادرة في الهيئة، الفريق الوطني للاستجابة لطوارئ الحاسب الآلي، وغيرهم
2. **بيانات المنظومة المتكاملة** لجان القطاعات التنفيذية لبرنامج حماية البنية التحتية للمعلومات الحيوية، اللجنة الوطنية للاستجابة للحوادث السيبرانية، وحدة الاستخبارات السيبرانية، الجهات المختصة بتنفيذ القانون، وغيرها
3. **بيانات المصادر العالمية** التقارير، والمعلومات الاستخبارية، وغيرها

سيساعدنا في متابعة تنفيذ الاستراتيجية

- متابعة سير العمل على الاستراتيجية الوطنية للأمن السيبراني
- مؤشريّ أداء استراتيجيين
- 17 مؤشر أداء تشغيلي

www.tra.gov.ae