مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مركز محمد بن راشد للابتكار الحكومي
MOHAMMED BIN RASHID CENTRE FOR GOVERNMENT INNOVATION

ابتكر
IBTEKR

2025

رؤية دولة الإمارات العربية المتحدة للأمن السيبراني

خارطة طريق نحو المستقبل

جـــدول المحتويـات

كلمة سعادة هدى الهاشمي

مساعدة وزير شؤون مجلس الوزراء لشؤون الاستراتيجية

في ظل التحديات الرقمية المتزايدة التي تواجهها الحكومات حول العالم، أصبحت الحاجة إلى الابتكار في القطاع الحكومي أكثر إلحاحًا من أي وقت مضى. ولم يعد الأمن السيبراني مجرد وظيفة تقنية، بل أصبح ركيزة أساسية لتعزيز الأمن الوطني الرقمي، وترسيخ ثقة المجتمع، ودعم مسيرة التقدّم الاقتصادي.

تقف دولة الإمارات العربية المتحدة في طليعة الدول التي تقود هذا التحول، ليس فقط من خلال الاستثمار في التقنيات المتقدمة، بل أيضًا عبر تطوير نماذج عملية قابلة للتطبيق يمكن للجهات الحكومية الأخرى الاستفادة منها. ويسلط هذا التقرير الضوء على تلك التجارب الرائدة، ويعرض كيف تحوّل دولة الإمارات الأفكار إلى نتائج ملموسة عبر مبادرات وطنية، وشراكات فعالة بين القطاعين الحكومي والخاص، وثقافة مؤسسية تقوم على التجربة والتعلّم. ويتضمن التقرير ابتكارات وتجارب دولية رائدة في مجال الأمن السيبراني والابتكار في القطاع الحكومي من فرق المتطوعين السيبرانيين في الولايات المتحدة، إلى التحديات الوطنية للابتكار في ماليزيا، وصولاً إلى مجمّعات الأمن السيبراني المتعددة القطاعات في فرنسا. وتشكل هذه النماذج العالمية مصدر إلهام غني للخبراء وصنّاع السياسات الباحثين عن حلول عملية ومبتكرة لمستقبل العمل الحكومي.

ومن خلال برامج محاكاة الهجمات السيبرانية، وحملات التوعية الوطنية، والحلول الدفاعية المدعومة بالذكاء الاصطناعي، والتمارين الدولية، تواصل دولة الإمارات تقديم نموذج رائد يُظهر كيف يمكن للجهات الحكومية أن تتعامل بمرونة وفعالية مع التحديات الرقمية المتجددة، مع ترسيخ ثقافة التميز والاستباقية. إن هذه المبادرات ليست مجرد رؤى نظرية، بل تجسيد واقعي لنماذج قابلة للتطبيق تقدم دروساً قيّمة للحكومات في مختلف أنحاء العالم.

ونؤمن بأن تبادل هذه الخبرات يُسهم في تعزيز التعلم المشترك ويقوي منظومة الأمن الجماعي. ونأمل أن يفتح هذا التقرير بابًا للحوار، ويحفّز التفكير الخلّاق، ويساهم في دفع حركة عالمية أوسع من الحكومات التي تسعى إلى التقدّم والبقاء في الصدارة معًا.

كلمة سعادة د. محمد حمد الكويتي

رئيس الأمن السيبراني لحكومة دولة الإمارات

في عصر يقود فيه التحول الرقمي جميع جوانب التقدم الاقتصادي والاجتماعي، أصبح الأمن السيبراني ركيزة أساسية في تعزيز مرونة الدول وقدرتها على مواجهة التحديات. وتدرك دولة الإمارات العربية المتحدة أن الثقة في الفضاء السيبراني ليست مجرد ضرورة فنية، بل هي ضرورة استراتيجية تعزز الابتكار والازدهار والتعاون الدولي.

ظل مجلس الأمن السيبراني الإماراتي، منذ تأسيسه عام 2020، مكرَّساً لترسيخ مكانة الدولة كقوة عالمية رائدة في مجال الثقة والمرونة الرقمية. واسترشاداً بالرؤية الطموحة للاستراتيجية الوطنية للأمن السيبراني 2025-2031، عمل المجلس على تطوير الأطر، وبناء شراكات استراتيجية، وتعزيز القدرات اللازمة لحماية البنية التحتية الحيوية، وتمكين التبني الآمن للتكنولوجيات الناشئة، وغرس ثقافة الوعي والابتكار في المجتمع. وتعكس هذه الرؤية إيمان دولة الإمارات الراسخ بأن الثقة في الفضاء السيبراني لا تقتصر على كونها حاجة فنية، بل هي محفّز للابتكار والازدهار والتعاون الدولي.

لقد شهدنا في السنوات الأخيرة تصاعداً في التهديدات السيبرانية التي يمكنها تعطيل البنية التحتية الحيوية وتعريض الأمن الوطني للخطر. فمن هجمات الفدية التي تستهدف أنظمة الرعاية الصحية إلى اختراقات البيانات التي تؤثر في المؤسسات الحكومية والجهات العامة والخاصة على حد سواء، يظل أثر هذه الأزمات السيبرانية بالغاً وعميقاً. هذه التهديدات لا تعرض أصولنا الرقمية للخطر فسحب، بل تعرض السلامة العامة والثقة أيضاً للخطر.

تؤكد هذه الحقيقة المخاطر المتزايدة التي تشكلها التهديدات السيبرانية على نطاق عالمي، وتُبرز الحاجة إلى اليقظة المستمرة وتبنّي إجراءات أمنية متقدمة. وتتحمل قطاعات المال والرعاية الصحية والطاقة، على وجه الخصوص، العبء الأكبر من هذه التهديدات. ولمواجهتها بفاعلية، لا بد لنا من اعتماد نهج استباقي يُركز على الابتكار واستشراف الأزمات. فقدرات النمذجة التنبؤية الآن تسمح للسلطات المختصة باتخاذ قرارات سريعة ومدروسة – ليس لمجرد الاستجابة للطوارئ، بل للتنبؤ بها أيضاً. وهذا يمثل تحولاً جذرياً في كيفية مواجهتنا للتهديدات السيبرانية المتسارعة.

إن الاستثمار في الابتكار في مجال الأمن السيبراني يضمن تطوير تحليلات تنبؤية، وتقييمات فورية للبيانات، ومحاكاة لسيناريوهات الطوارئ. وتوفر هذه الأدوات رؤى قيّمة تعزز من الجاهزية والاستجابة، من خلال نمذجة أوضاع مختلفة تتيح للمؤسسات والحكومات الاستعداد لسيناريوهات متعددة، وتحسين خطط الطوارئ، وتخصيص الموارد بفاعلية أعلى استناداً إلى التقييمات الفورية.

نواجه اليوم قضية ملحة تمسنا جميعاً، ألا وهي تزايد وتيرة الأزمات السيبرانية وتعقيدها في عالمنا المترابط. وفي خضم هذه التحديات، تبرز ضرورة الاستفادة من التكنولوجيات المتقدمة لتعزيز المرونة الوطني من خلال الابتكار وتنمية المواهب وتقوية الخبرات.

وقد أثمرت جهودنا اعترافاً دولياً غير مسبوق. فقد استضافت دولة الإمارات تدريبات سيبرانية عالمية بمشاركة أكثر من 120 جهة وطنية من أكثر من 133 دولة، في إنجاز يُعد محطة بارزة في مسيرة تعزيز التعاون الدولي. وتُوّجت هذه الجهود بتحقيق 11 رقماً قياسياً في موسوعة غينيس خلال معرض جيسيك 2025، وهذه شهادة على التزامنا بالريادة والابتكار.

إضافة إلى ذلك، تسهم منصات التكنولوجيا الرائدة مثل مركز عمليات الأمن السيبراني الوطني (NSOC)، ومحاكي "النبض" التدريب السيبراني "Pulse" ومنصة تبادل المعلومات الاستخباراتية "Crystal Ball" في وضع معايير عالمية جديدة للجاهزية الفنية والمرونة التشغيلية والتعاون الاستراتيجي.

ومع تطلّعنا إلى المستقبل، ستواصل دولة الإمارات ريادتها في تعزيز التعاون الدولي، وتطوير رأس المال البشري، وتأمين الابتكار الرقمي. إننا ملتزمون التزاماً راسخاً بضمان بقاء الفضاء السيبراني مصدراً للفرص والثقة لمواطنينا، ودعامة أساسية لاقتصادنا، وشريكاً موثوقاً لجميع حلفائنا في جميع أنحاء العالم.

ملخـــص تنفيـــذي

أصبح الأمن السيبراني واحداً من التحديات العالمية الأكثر إلحاحاً في عصرنا. فقد أدى التسارع في تبنّي الذكاء الاصطناعي، والخدمات السحابية، وإنترنت الأشياء، وقريباً الحوسبة الكمومية، إلى توسيع مساحة الهجمات الرقمية بسرعة غير مسبوقة. وأخذت الجهات الفاعلة في مجال التهديد السيبراني تزداد تطوراً وتعقيداً، كما شوهد ذلك في حملات الهجوم الخاطف "blitz" التي استهدفت دولة الإمارات في عام 2025، وشملت 82.7 مليون محاولة استغلال، و500 حادثة فدية، و1.8 مليار عملية مسح في غضون بضعة أشهر فقط.

وفي الوقت نفسه، تشهد المنظومات العالمية هجمات الفدية تنوعاً كبيراً، حيث زاد عدد المجموعات النشطة بنسبة 58% خلال عام 2024، في حين يمكّن الذكاء الاصطناعي من الاحتيال بالتزييف العميق، وأتمتة البرمجيات الخبيثة، وإنشاء أُطر هجومية ذاتية التشغيل. لذلك انتقل التشفير ما بعد الكمومي من مرحلة النظرية ليصبح ضرورة ملحة مع تبنّي الخصوم لاستراتيجيات "احصد الآن وفك التشفير لاحقاً".

وفي مواجهة هذا المشهد، اتخذت دولة الإمارات خطوات حاسمة لحماية مستقبلها الرقمي. وتوفر الاستراتيجية الوطنية للأمن السيبراني (2025–2031) خريطة طريق شاملة مكونة من ستة أهداف: تعزيز المرونة، وحماية المجتمع، وبناء الثقة الرقمية، وتمكين الابتكار الآمن، وتنمية المواهب، وقيادة الشراكات العالمية. وتنسجم تنفيذها (المتمثلة في الحوكمة، والحماية والدفاع، والابتكار، والبناء، والشراكة) مع رؤية الإمارات لتصبح مركزاً رقمياً عالمياً موثوقاً.

يسلط هذا التقرير الضوء على تقدُّم دولة الإمارات وابتكاراتها، بما في ذلك:

التمرين السيبراني العالمي 2025: أضخم تمرين سيبراني في العالم شاركت فيه 124 جهة من أكثر من 133 دولة، بسيناريوهات قادها كل من الاتحاد الدولي للاتصالات (ITU)، ومركز الأمم المتحدة لمكافحة الإرهاب (UNCCT)، والإنتربول، ومنتدى فرق الاستجابة للحوادث والأمن (FIRST).

منصة الكرة البلورية "Crystal Ball": بيئة آمنة للتعاون الاستخباراتي الدولي. وقد تم تعزيزها في عام 2025 من خلال إدخال تحليلات مدعومة بالذكاء الاصطناعي، وتحسين إجراءات الانضمام، وإطلاق برنامج تبادل بين الحكومات.

منصة النبض السيبراني: منصة تدريبية رائدة تهدف إلى رفع جاهزية القوى العاملة وتعزيز مرونتها في مختلف القطاعات.

موسوعة غينيس للأرقام القياسية: تحقيق أحد عشر إنجازاً في معرض ومؤتمر جيسيك 2025 تم تسجيلها في موسوعة غينيس للأرقام القياسية، من بينها مشاركة أكبر عدد من الجنسيات في تمرين سيبراني واحد، وعقد أضخم جلسة توعية عالمية.

السياسات والأطر: تحديث معيار ضمان المعلومات، وسياسة حماية البنية التحتية للمعلومات الحيوية، وخط الأساس لمركز العمليات الأمنية، بالإضافة إلى جهود جديدة في مجال إنترنت الأشياء والحوسبة السحابية وتدفقات البيانات عبر الحدود.

تنمية المواهب: مبادرات مثل مختبرات X-Labs وأكاديمية جيسيك وحوار المسرّعات الحكومية لسد فجوة القوى العاملة وتمكين الكوادر الإماراتية في مجال الأمن السيبراني.

حالة الأمـن السيبراني في دولة الإمـــارات العربيـــة المتحـــدة

يشهد مشهد الأمن السيبراني في دولة الإمارات تطورًا سريعًا يعكس في الوقت نفسه الطموحات الرقمية للدولة وتزايد تعقيد الهجمات التي تستهدف بنيتها التحتية.

وتستضيف الإمارات حاليًا ما يقارب

223,800

أصل رقمي، وتشير التحليلات إلى أن نصف الثغرات الأمنية الأكثر خطورة يعود تاريخها إلى أكثر من خمس سنوات. وهذا التعرض القديم لا يزال يُستغل من قبل المهاجمين، مما يبرز أهمية الإدارة الاستباقية للتحديثات الأمنية والتقليل المنهجي من الثغرات على المستوى الوطني. وتُعتبر معالجة هذه الثغرات طويلة الأمد أمرًا بالغ الأهمية لضمان بقاء البنية التحتية الرقمية في الإمارات صامدة أمام الحملات السيبرانية المعقدة والمستمرة.

شهد نظام هجمات الفدية في الإمارات بين عامي 2023 و2024 تغيرات كبيرة تعكس تنوع الفاعلين والأساليب المستخدمة. فقد ارتفع عدد مجموعات الفدية النشطة بنسبة 58%، ما يؤكد ازدياد تعقيد البيئة التهديدية. ففي حين تراجعت حصة مجموعة LockBit3 من 31% في عام 2023 إلى 16% في عام 2024، برزت مجموعات جديدة مثل (13%) RansomHub، وDarkVault، وQilin، و RansomEXX، وKillSec. وفي المقابل، اختفت مجموعات أخرى مثل Clop من تقارير الإمارات، ما يشير إلى وجود اضطراب واستبدال داخل النظام البيئي لهجمات الفدية.

ولا يقل الأثر المالي للحوادث السيبرانية خطورة. ففي عام 2024، بلغ متوسط التكلفة العالمية لاختراق البيانات

$4.88 مليــون

نتيجة فقدان الأعمال، وتكاليف الاستجابة للعملاء، واحتواء الحوادث. وسجّل الشرق الأوسط، بما فيه دولة الإمارات، ثاني أعلى تكلفة للاختراقات عالميًا، مما يعكس الأهمية الاقتصادية للمنطقة وحجم الضغوط المالية الناتجة عن الهجمات السيبرانية.

أما نشاط هجمات الحرمان من الخدمة الموزعة (DDoS) فقد شهد انخفاضًا ملحوظًا في دولة الإمارات. ففي الفترة من النصف الأول من عام 2023 إلى النصف الأول من عام 2024، انخفضت الهجمات بنسبة

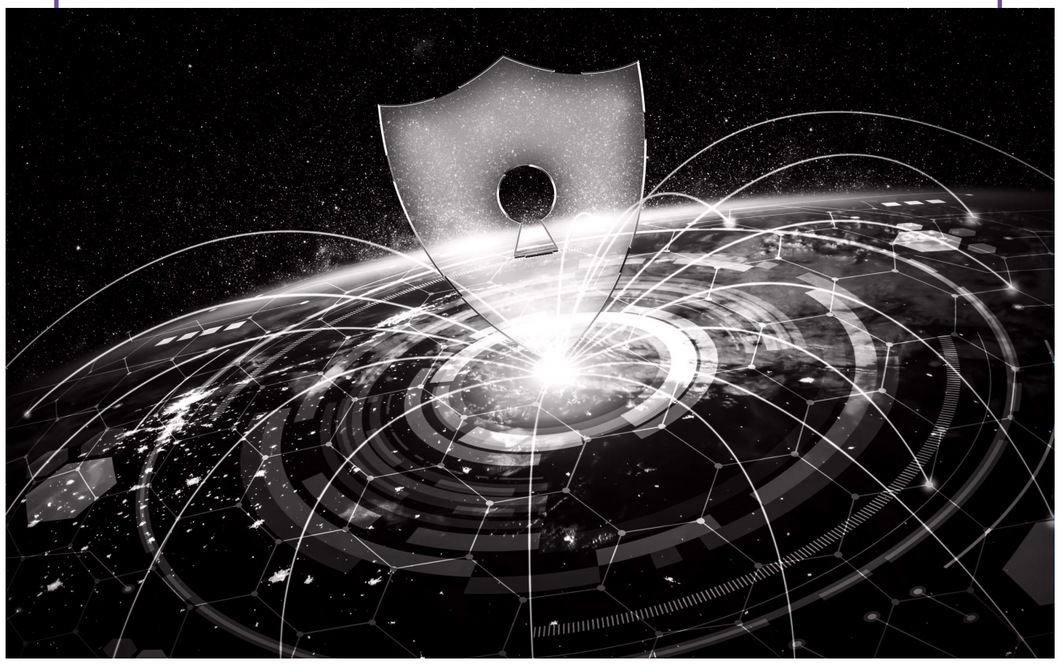
96%

مقارنة بالفترة نفسها من عام 2023، حيث تراجعت **من 58,538 حادثة إلى 2,301** فقط. كما انخفض أقصى معدل للنطاق الترددي المسجل **من 266.9 جيجابت/ثانية إلى 85.92 جيجابت/ثانية**، بينما تراجع متوسط مدة الهجوم إلى **18.53 دقيقة**. وتعكس هذه التحسينات صلابة أكبر للبنية التحتية، بالرغم من أن حجم هجمات الحرمان من الخدمة الموزعة عالميًا ارتفع ليقترب من 1 تيرابت/ثانية.

وفي المقابل، شهدت برمجيات سرقة المعلومات انتشارًا متزايدًا. ففي عام 2024، استحوذ **RedLine Stealer** على

69.9%

من الإصابات المسجّلة، يليه **META (13.1%)**، و**Lumma (12.6%)**، و**Vidar (4.4%)**. وأدت هذه الحملات إلى **تسريب أكثر من 238,000 كلمة مرور فريدة.** ومن المثير أن **77%** من هذه البيانات المسروقة كانت تفي بإرشادات NIST الخاصة بطول كلمات المرور، مما يوضح أن قوة كلمات المرور وحدها غير كافية إذا كانت الأجهزة أو الشبكات مخترقة ببرمجيات خبيثة. وهذا يؤكد أهمية تعدد طبقات الحماية، ومراقبة نقاط النهاية، واستخدام المصادقة المتعددة العوامل.



ووفقًا للتحليل الذي أجراه مركز العمليات الأمنية التابع لشركة CPX، كانت أنواع الحوادث الأكثر شيوعًا في دولة الإمارات خلال عام 2024 على النحو التالي:

32% أخطاء التهيئة

19% الاستخدام غير السليم أو النشاط غير القانوني

15% عمليات المسح والاستطلاع

12% التصيد الاحتيالي وانتحال الهوية

9% الشيفرات الخبيثة

9% الوصول غير المصرح به

4% هجمات تطبيقات الويب

ويبرز هذا التوزيع أن ضعف الحوكمة وأخطاء التهيئة لا تقل أثرًا عن الاستغلالات التقنية، مما يعزز الحاجة إلى صلابة ثقافية وتقنية في آن واحد.

كما ركّز المهاجمون بصفة خاصة على القطاعات ذات القيمة العالية. فقد كانت الجهات الأكثر استهدافًا في دولة الإمارات خلال 2024 هي:

34.9% الحكومة

21.3% القطاع المالي

14.1% قطاع الطاقة

11.6% التأمين

6.7% الرعاية الصحية

6.6% الدفاع

4.8% خدمات تقنية المعلومات

ويعكس هذا التركيز أولوية الخصوم في استهداف البنى التحتية الوطنية والاقتصادية، حيث تبقى الأنظمة الحكومية الهدف الرئيسي سواء للمجموعات المرتبطة بالدول أو لجماعات الجريمة الإلكترونية.

وبوجه عام، توضح هذه الاتجاهات أن بيئة الأمن السيبراني في دولة الإمارات ديناميكية ومعقدة للغاية، حيث تواجه الدولة خصومًا يتمتعون بنضج تشغيلي متزايد قادرين على شن حملات هجومية مكثفة، واستغلال ثغرات قديمة، وتطوير أساليب هجمات الفدية بسرعة، في وقت تعمل فيه دولة الإمارات على تعزيز دفاعاتها وتقليل نقاط الضعف، خاصة في مجال مواجهة هجمات الحرمان من الخدمة.

02

التحديـــات والتهديدات الرئيســـة

أخذ مشهد التهديدات السيبرانية يتطور بسرعة، مع ظهور تكتيكات وأساليب وإجراءات جديدة باستمرار. وأصبحت التهديدات اليوم تمتد من البرمجيات الخبيثة المولّدة بالذكاء الاصطناعي وحملات الفدية، إلى الهندسة الاجتماعية المدعومة بالتزييف العميق والتهديدات المتقدمة المستمرة المدعومة من جانب الدولة. ويزداد استغلال الخصوم لتعقيد الحوسبة السحابية وانتشار الهويات وأجهزة إنترنت الأشياء، بينما يقومون أيضاً بدمج الذكاء الاصطناعي في خططهم الهجومية.

وفي دولة الإمارات، شهد النصف الأول من عام 2025 تنفيذ أكثر من 82.7 مليون محاولة استغلال استهدفت بروتوكول كتلة رسائل الخادم (SMB) أعقبتها حملة هجوم خاطف (blitz) شملت 500 حادثة فدية، و28.7 مليون محاولة تجريب عشوائي لاختراق كلمات المرور (brute force)، ومليونا عملية تجنيد لشبكات البوت نت (botnet). هذا المزيج من الاتساع والسرعة والأتمتة يجعل من الصعب على المؤسسات البقاء في موقع متقدم وحماية أصولها الحيوية.

من التهديدات السيبرانية الأكثر إثارة للقلق والمتوقعة في عام 2025 ما يلي:

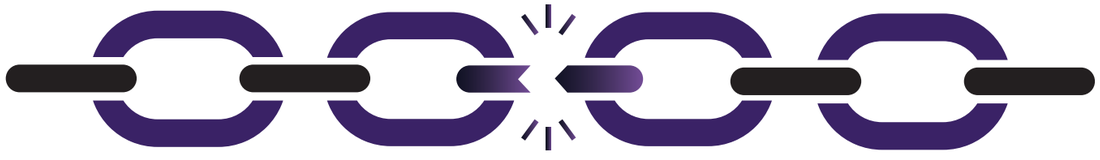
- الهندسة الاجتماعية المدعومة بالذكاء الاصطناعي والاحتيال بالتزييف العميق
- الهجمات على سلاسل توريد البرمجيات والمصادر المفتوحة
- نقص المواهب والمهارات في مجال الأمن السيبراني
- البرمجيات الخبيثة المدفوعة بالذكاء الاصطناعي والهجمات الخفية الخالية من البرمجيات الخبيثة
- تحديات التشفير ما بعد الكمومي
- الذكاء الاصطناعي الوكيلي وأطر الهجمات الذاتية التشغيل

الهندسة الاجتماعية المدعومة بالذكاء الاصطناعي والاحتيال بالتزييف العميق

تشهد عمليات الاحتيال بالهندسة الاجتماعية تزايداً ملحوظاً في استخدام الذكاء الاصطناعي وتكنولوجيا التزييف العميق، ما يمكّن من إنتاج رسائل تصيّد إلكتروني ومكالمات احتيالية وانتحال شخصيات بمقاطع فيديو بطريقة مقنعة للغاية. وفي دولة الإمارات، أدت حملات التصيّد المدعومة بالذكاء الاصطناعي التي استهدفت المؤسسات المالية وعمليات الانتحال الصوتي لمسؤولين تنفيذيين عبر التزييف العميق إلى خسائر كبيرة. وكان الأمر الأكثر إثارة للدهشة أن حملةً مرتبطة بإيران في عام ٢٠٢٤ نجحت في اختراق بثوث تلفزيونية إماراتية مستخدمة مذيعي أخبار مزيفين تم إنشاؤهم بتكنولوجيا التزييف العميق لنشر معلومات مضللة. وتؤكد هذه الحوادث أن أدوات الذكاء الاصطناعي التوليدي قد خفضت الحواجز أمام الجريمة السيبرانية، الأمر الذي يمكّن حتى الفاعلين غير الفنيين من صياغة هجمات استهدافية تتخطى الأنظمة الأمنية التقليدية.

الهجمات على سلاسل توريد البرمجيات والمصادر المفتوحة

تُعد اختراقات سلاسل التوريد أحد أخطر التهديدات السيبرانية في عام 2025، حيث يزداد استغلال الخصوم للاعتماديات (dependencies) وخطوط الإنشاء الآلية (build pipelines) وآليات نشر (deployment mechanisms) للتسلل إلى بيئات موثوقة. وقد شهدت دولة الإمارات أيضاً استهداف الخصوم لمكوّنات مفتوحة المصدر شائعة الاستخدام مثل OpenSSH وExim، حيث أثرت نقاط الضعف والتعرُّض الشائعة مثل ("regreSSHion") CVE-2024-6387 على أكثر من 16% من الأنظمة التي تم اختبارها. وتتماهى هذه الحملات مع موجة اختراقات عالمية خلال عام 2024، شملت منصات نقل الملفات والتحقق من الهوية واسعة الاستخدام. وللتصدي لهذه المخاطر، بدأت المؤسسات الإماراتية تتبنى مبادئ الأمن بالتصميم، واختبارات الوضع الأمني وفق معايير الشراكة الوطنية لضمان المعلومات (NIAP)، وهياكل الثقة الصفرية، ما يدمج المرونة مباشرةً في تطويرها وعملياتها.



نقص المواهب والمهارات في مجال الأمن السيبراني

يظل النقص في المواهب المتخصصة في الأمن السيبراني قضية ملحة في عام 2025، حيث تشير التقديرات إلى وجود أكثر من أربعة ملايين وظيفة شاغرة على مستوى العالم. ويشكل هذه الفجوة في القوى العاملة مخاطر كبيرة في ظل توسيع الخصوم لعملياتهم باستخدام الذكاء الاصطناعي والأتمتة. وبالنسبة لدولة الإمارات، أصبح بناء القدرات المحلية أولوية وطنية. وتعمل مبادرات مثل X-Labs، وأكاديمية جيسيك، وحوار المسرّعات الحكومية على إنشاء مسارات لتطوير المهارات، بينما أخذ التعاون بين القطاعين العام والخاص يوسّع فرص الوصول إلى التدريب المتقدم. إن تطوير قوة عاملة مؤهلة في مجال الأمن السيبراني أمر ضروري لضمان المرونة في مواجهة خصوم يزدادون تعقيداً وخطورة.

البرمجيات الخبيثة المدفوعة بالذكاء الاصطناعي والهجمات الخفية

في عام 2025، أصبحت البرمجيات الخبيثة المتقدمة أكثر قدرة على التكيّف والمراوغة. ويستخدم الخصوم أدوات مدفوعة بالذكاء الاصطناعي لتعديل البرمجيات الخبيثة آنياً، ما يمكنهم من تجاوز أنظمة الكشف القائمة على التوقيع.

وما زال نموذج برامج الفدية كخدمة (RaaS) يهيمن على المشهد، حيث شهدت دولة الإمارات زيادة بنسبة

زيادة بنسبة %58

في عدد مجموعات الفدية النشطة في عام 2024

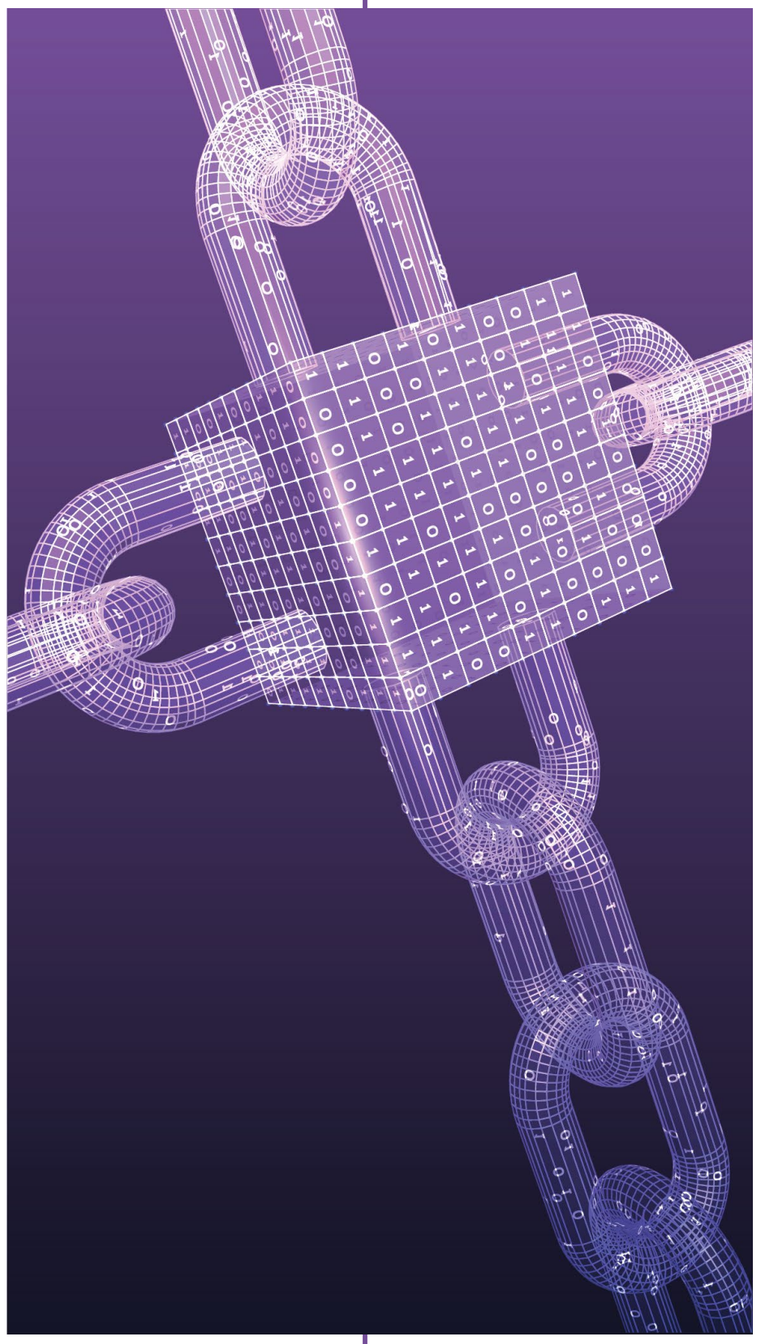
كما يستغل المهاجمون الثغرات المكتشفة حديثاً (مثل ثغرة OpenSSH CVE-2024-6387) لتنفيذ الأوامر البرمجية عن بُعد. وتؤكد هذه التطورات على الحاجة إلى نهج استباقي لكشف التهديدات، والمراقبة المستمرة، والإدارة الصارمة لتحديثات الأنظمة في جميع القطاعات.

تحديات التشفير ما بعد الكمومي

مع تبني الخصوم لاستراتيجيات "احصد الآن وفك التشفير لاحقاً"، اصبحت الحاجة ملحة إلى التشفير ما بعد الكمومي (PQC). وتعمل دولة الإمارات على التوافق مع جهود توحيد المعايير العالمية لتنفيذ خوارزميات قائمة على الشبكات وعلى الأكواد بحيث تكون قادرة على مقاومة فك التشفير الكمومي. ورغم التحديات التي يواجهها تبنّي التشفير من بعد الكمومي (مثل التعقيد وقابلية التشغيل البيني وتكاليف الانتقال)، فإن الاستثمار المبكر يُعد عاملاً حاسماً لضمان الأمن على المدى الطويل، خصوصاً في القطاعات الحكومية والمالية وقطاع الطاقة، حيث يجب الحفاظ على سرية البيانات الحساسة لعقود مقبلة.

الذكاء الاصطناعي الوكيلي وأطر الهجمات الذاتية التشغيل

يبرز الذكاء الاصطناعي الوكيلي (Agentic AI) - وهو أنظمة ذكاء اصطناعي مستقلة قادرة على متابعة أهدافها بشكل ذاتي - كأحد المخاطر الجديدة. وتشير الدلائل الأولية إلى أن الخصوم بدأوا في اختبار وكلاء ذكاء اصطناعي يمكنهم أتمتة عمليات الاستطلاع، وفحص الثغرات الأمنية، بل حتى تنفيذ عمليات الاستغلال من دون أي إشراف بشري. ورغم أن هذه القدرات ما زالت في مراحلها الأولى، فإن تسليح الذكاء الاصطناعي الوكيلي ينذر بتحوّل جذري في طبيعة التهديدات: من جريمة سيبرانية موجهة بشرياً إلى هجمات مستقلة تقودها الآلات. وفي هذا السياق، بدأت دولة الإمارات وشركاؤها في تقييم هذا الخطر المحتمل، مع إعطاء الأولوية لوضع أطر حوكمة الذكاء الاصطناعي واعتماد نماذج آمنة لتبني الذكاء الاصطناعي.



التحديـــات والتهديدات الرئيســـة

03

الابتكار في الأمن السيبراني

تعريف الابتكار في الأمن السيبراني

يشير الابتكار في مجال الأمن السيبراني إلى استحداث وتنفيذ أفكار أو تكنولوجيات أو عمليات جديدة تعزز المرونة في مواجهة التهديدات المتنامية. ويشمل ذلك تطوير أساليب مبتكرة للتعرف على الهجمات ومنعها وكشفها والتصدي لها والتعافي من آثارها.

وفي دولة الإمارات، يتجسد الابتكار في منصات مثل مركز عمليات الأمن السيبراني الوطني (NSOC)، ومنصة الكرة البلورية لتبادل معلومات التهديدات (Crystal Ball)، ومنصة النبض السيبراني (Pulse)، إضافة إلى برامج جديدة مثل X-Labs وأكاديمية جيسيك. وتمثل هذه الجهود منظومة متكاملة ترسّخ ثقافة التجريب وتدعم ريادة دول الإمارات في تعزيز الأمن السيبراني عالمياً.

أهمية الابتكار في الأمن السيبراني

يتطور مشهد الأمن السيبراني باستمرار، حيث تظهر تهديدات جديدة يومياً. ومن هنا تبرز أهمية الابتكار لعدة أسباب:

البقاء متقدماً على التهديدات: تتطلب التهديدات الجديدة تدابير مضادة جديدة. ويساعد الابتكار المؤسسات على البقاء متقدمة على مجرمي الفضاء السيبراني من خلال تطوير أساليب حماية متقدمة. ففي عام 2025 وحده، شن خصوم دولة الإمارات أكثر من 82.7 مليون محاولة استغلال، وحملة هجومية خاطفة (blitz) تضمنت 500 حادثة فدية و1.8 مليار عملية مسح إلكتروني.

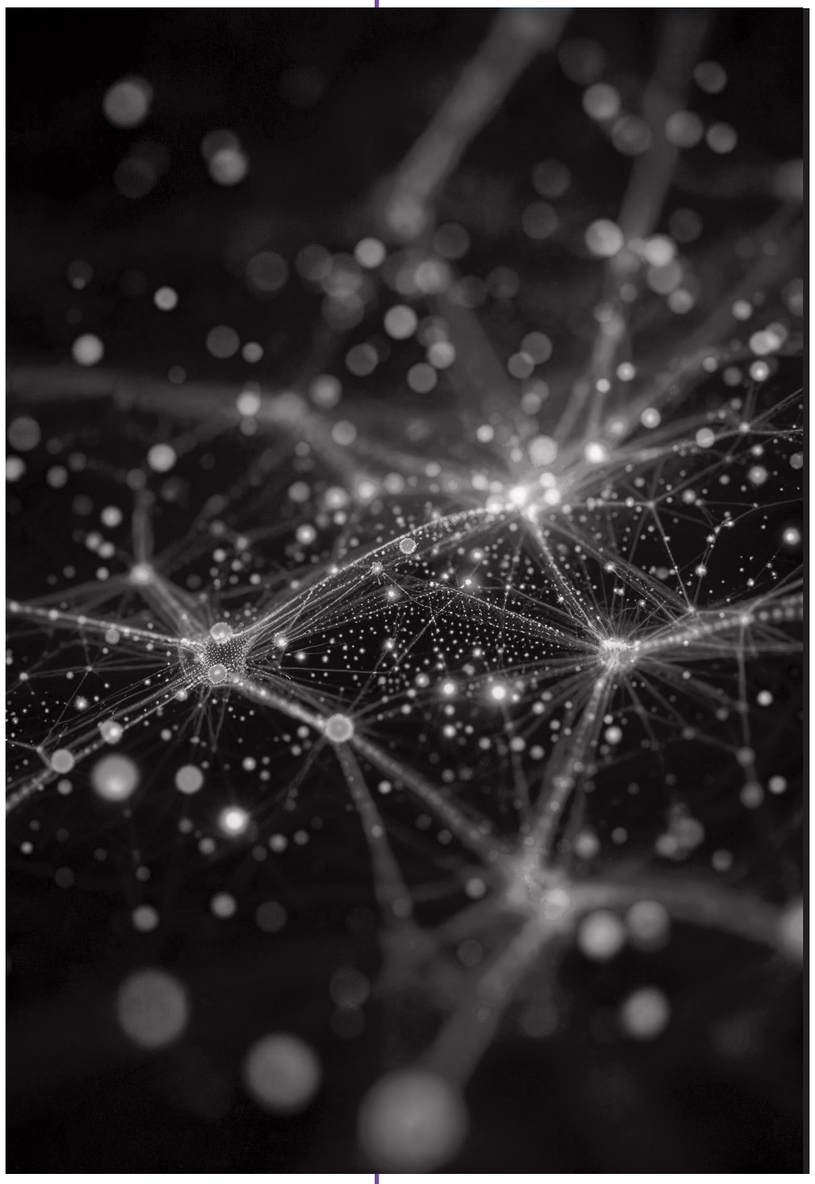
تعزيز الدفاعات: يمكن للحلول المبتكرة أن في تعزز التدابير الأمنية القائمة، ما يوفّر منظومة دفاعية أقوى ضد مواجهة الهجمات. فمن خفض هجمات الحرمان من الخدمة الموزع (DDoS) بنسبة 96% في عام 2024 إلى إحراز 11 رقماً قياسياً في موسوعة غينيس خلال فعاليات جيسيك 2025، أثبتت دولة الإمارات أن الابتكار يترجم مباشرة إلى مرونة ملموسة وقابلة للقياس.

تحسين الكفاءة: يمكن للتكنولوجيات المبتكرة أن تبسّط العمليات الأمنية، ما يجعلها أكثر كفاءة وفعالية من حيث التكلفة، كما هو الحال في منصة الكرة البلورية (Crystal Ball).

حماية البنية التحتية الحيوية: مع تزايد الاعتماد على الأنظمة الرقمية وتسارع وتيرة التحول الرقمي في دولة الإمارات عبر قطاعات المال والطاقة والنقل والحكومة وغيرها، تصبح حماية البنية التحتية الحيوية أمراً بالغ الأهمية لضمان بقائها في مأمن من التهديدات.

بناء الثقة: إن إظهار الالتزام بالابتكار في مجال الأمن السيبراني يقوي ثقة الجمهور ويعزز سمعة دولة الإمارات كمركز آمن للاستثمار العالمي.

الابتكـار فـي الأمن السيبراني



التوجهات العالمية وأفضل الممارسات
المعايير العالمية

تشكيل فيلق مدني سيبراني في ميشيغان
الولايات المتحدة الأمريكية

يدرك معظم الناس الفكرة وراء إدارة الإطفاء التطوعية. فعندما يندلع حريق ضخم ولا يوجد عدد كافٍ من رجال الإطفاء المتفرغين لمكافحته، يمكن لفيلق من المتطوعين المدربين المساعدة في إخماد النيران. وبدأت ولاية ميشيغان تأخذ فكرة إدارة الإطفاء التطوعية وتطبقها في مجال آخر لحماية سلامة المواطنين: فقد أنشأت فيلقاً مدنياً سيبرانياً تطوعياً، وتعمل على توسيعه بسرعة.

فيلق ميشيغان المدني السيبراني (MiC3) هو مجموعة من خبراء الأمن السيبراني المدربين الذين يتطوعون لتقديم المساعدة الفنية المتخصصة بهدف تعزيز قدرة الولاية على التعامل مع الحوادث السيبرانية بسرعة عند وقوعها. ويضم الفيلق متطوعين من قطاعات الحكومة والتعليم والأعمال. وقد جعلت ولاية ميشيغان من توسيع هذا الفيلق أولوية منذ عام 2017، إدراكاً منها أن التهديدات السيبرانية الموجهة إلى الحكومة تتسارع بوتيرة غير متوقعة.

بدأ فيلق ميشيغان المدني السيبراني (MiC3) كشراكة بين وزارة التكنولوجيا والإدارة والميزانية في الولاية، ونظام تسجيل المتطوعين في الولاية، وشبكة Merit. في البداية، اعتمد استقطاب المتطوعين على شبكة Merit وعلى التوصيات الشخصية. وكان على الراغبين في التطوع اجتياز تقييم عبر الإنترنت للتحقق من خبراتهم في الأمن السيبراني، ثم تحيل شبكة Merit المتقدمين المؤهلين إلى سجل المتطوعين التابع للولاية. وينضم المتطوعون إلى الفيلق بعد اجتياز فحص لاحق.

اليوم، أصبح باب العضوية مفتوحاً أمام المتخصصين في أمن المعلومات من المقيمين في ولاية ميشيغان. ويُشترط في المتقدمين أن تكون لديهم خبرة عملية لا تقل عن سنتين في مجال أمن المعلومات، ويفضل أن تكون في عمليات الأمن، أو الاستجابة للحوادث و/أو التحقيق الجنائي الرقمي أو الشبكي. ومنذ عام 2018، استقبل الفيلق نحو 200 عضو. ويُقدَّم طلب الانضمام عبر الموقع الإلكتروني لحكومة الولاية، وعلى المتقدم أن يثبت مهاراته في الأمن السيبراني، وأن يلتزم بالمشاركة في تدريب مخصص لمدة أسبوعين سنوياً كشرط للقبول.

في البداية، كان الأعضاء يُقسّمون إلى مجموعات للتعامل مع القضايا السيبرانية بناءً على القرب الجغرافي، لكن بسبب انتشار العمل عن بُعد في السنوات الأخيرة، يجري التفكير في التحوّل إلى مجموعات تركز على قطاعات مختلفة، مثل المال والرعاية الصحية وغيرها.

ومن الجوانب الملهمة أيضاً في البرنامج التزام ولاية ميشيغان بضمان إمكانية تكراره في ولايات أخرى في جميع أنحاء البلاد. فقد أشار نائب رئيس الأمن السيبراني في الولاية إلى أن نحو 15 ولاية أخرى أبدت اهتماماً بمعرفة كيفية إطلاق برامج مشابهة. بل إن دعا مركز أبحاث السياسات العامة The New American دعا إلى إنشاء برنامج وطني يضم 25,000 عضو على غرار برنامج ميشيغان (رغم أن هذا البرنامج لم يُنشأ حتى عام 2022، ظلت الفكرة تُطرح باستمرار وتكتسب اهتماماً وطنياً.

ومن المتوقع أن يزداد تأثير هذا الفيلق من المتطوعين السيبرانيين، خصوصاً بعد توقيع حاكم ميشيغان على تشريع يسهل استدعاء الفيلق وتوسيع نطاقه بحيث لا يقتصر على مساعدة حكومة ميتشغان فقط، بل يمكن أيضاً أن يساعد الحكومات المحلية والمنظمات غير الربحية والشركات في جميع أنحاء الولاية في حال حدوث اختراق أو هجوم سيبراني. ففي السابق، لم يكن يُمكن تفعيل الفيلق إلا بإعلان الحاكم عن "حالة طوارئ سيبرانية"، وهو أمر لم يحدث من قبل.

وأخيراً، لا يفيد فيلق المتطوعين الحكومة فقط، بل يفيد مجتمع الأمن السيبراني بأكمله في جميع أنحاء ميشيغان. فولاية ميتشغان لديها الآن خبراء في الأمن السيبراني موجودون في مجتمعات متباعدة ولا سبيل لديها للتواصل والتعرف على بعضهم البعض إلا عبر حضور الفعالية نفسها أو العمل في نفس المؤسسة. لذلك، بدأ الأعضاء تنظيم مكالمات جماعية شهرية لتحدث عن ما يحدث، وما سيأتي في برامجهم، والتواصل العام، وبناء الفرق، إضافة إلى الأسئلة والأجوبة. وتُعد هذه الأنشطة مفيدة جداً لمنظومة الأمن السيبراني في الولاية.

شبكة الابتكار في الأمن السيبراني
كندا

في فبراير 2022، ولمواجهة تحديات الأمن السيبراني من حيث البحث والتطوير والابتكار والتدريب، ولمساعدة المؤسسات والشركات في جميع أنحاء البلاد على إدارة التهديدات السيبرانية، أعلنت حكومة كندا عن تخصيص تمويل بقيمة 76.4 مليون دولار على مدى أربع سنوات لصالح الاتحاد الوطني للأمن السيبراني (NCC).

وبدأ الاتحاد الوطني للأمن السيبراني، بوصفه مستفيداً رئيسياً، في إنشاء شبكة الابتكار في الأمن السيبراني (CSIN)، وهي منصة حيوية لتطوير الأمن السيبراني في كندا. وتُعد هذه الشبكة منظومة وطنية كندية شاملة تضم مؤسسات التعليم العالي، وشركات خاصة كبيرة وصغيرة، وحكومات المقاطعات/الأقاليم والبلديات، ومنظمات غير ربحية. ويرتبط الأعضاء في شبكة تعاونية نشطة تنفّذ مشاريع مبتكرة للغاية يتم اختيارها استراتيجياً في مجالات البحث والتطوير والتتجير والتدريب.

وتشترك في قيادة الاتحاد الوطني للأمن السيبراني (NCC) وشبكة الابتكار في الأمن السيبراني (CSIN) خمس جامعات كندية: جامعة نيو برونزويك، وجامعة كالغاري، وجامعة رايرسون، وجامعة كونكورديا، وجامعة واترلو.

وستسهم الشبكة في تعزيز البحث والتطوير، وزيادة التتجير، وتنمية المواهب الماهرة المتخصصة في الأمن السيبراني في مختلف أنحاء كندا. وستموّل المشاريع العالية التأثير التي سيتم تنفيذها من خلال التعاون بين بين الجامعات والكليات وشركات القطاع الخاص بمختلف أحجامها والقطاع الحكومي والمنظمات غير الربحية من جميع مناطق كندا.

وبفضل الإستثمار الفيدرالي، سيبلغ لدى الاتحاد ميزانية أولية تزيد على 160 مليون دولار نقداً، إضافة إلى الإسهامات العينية من المؤسسات الداعمة. ويركّز الاتحاد على المساعدة في توسيع قطاع الأمن السيبراني التجاري في كندا، إلى جانب الإسهام في تعزيز الأمن السيبراني في البلاد.

وفي التقدم لقيادة الشبكة، عمل الاتحاد على نحو تعاوني مع أكثر من 140 باحثاً من 35 مؤسسة تعليم عال في كندا، و46 شركة من مختلف الأحجام، و26 منظمة غير ربحية، إضافة إلى حكومات إقليمية وهيئات حكومية.

وسيُطلب من الشبكة تقديم تكلفة مطابقة بنسبة 1:1 للإسهام الفيدرالي لمبلغ 80 مليون دولار إضافية على مدى أربع سنوات تُقدَّم في شكل مزيج من الإسهامات النقدية و/أو العينية. ومن المتوقع أن تأتي الإسهامات المطابقة من شركاء غير فيدراليين (مثل القطاع الخاص وحكومات الأقاليم/المقاطعات/البلديات وغيرها، مثل المنظمات غير الربحية، ومؤسسات التعليم العالي الكندية).

وفقاً لهيئة الإحصاء الكندية، أسهم قطاع الأمن السيبراني الكندي في الناتج المحلي الإجمالي بأكثر من 2.3 مليار دولار ووفّر 22,500 وظيفة في الاقتصاد الكندي في عام 2018. كما أفادت الشركات الكندية بأنها أنفقت 7 مليارات دولار في عام 2019 على منع الحوادث السيبرانية ورصدها والتعافي من تداعياتها. وستقود شبكة الابتكار في الأمن السيبراني مشاريع تدريبية تُعطي الأولوية لمفهوم التنوع والإنصاف والشمول. وبالإضافة إلى البحث والتدريب، ستقوم الشبكة بربط الباحثين ورواد الأعمال والمتخصصين في الأمن السيبراني والمتعلمين من خلال قنوات متعددة مثل مجموعات العمل والمؤتمرات وورش العمل والتحديات البحثية.

برنامج الدفاع السيبراني النشط
المملكة المتحدة

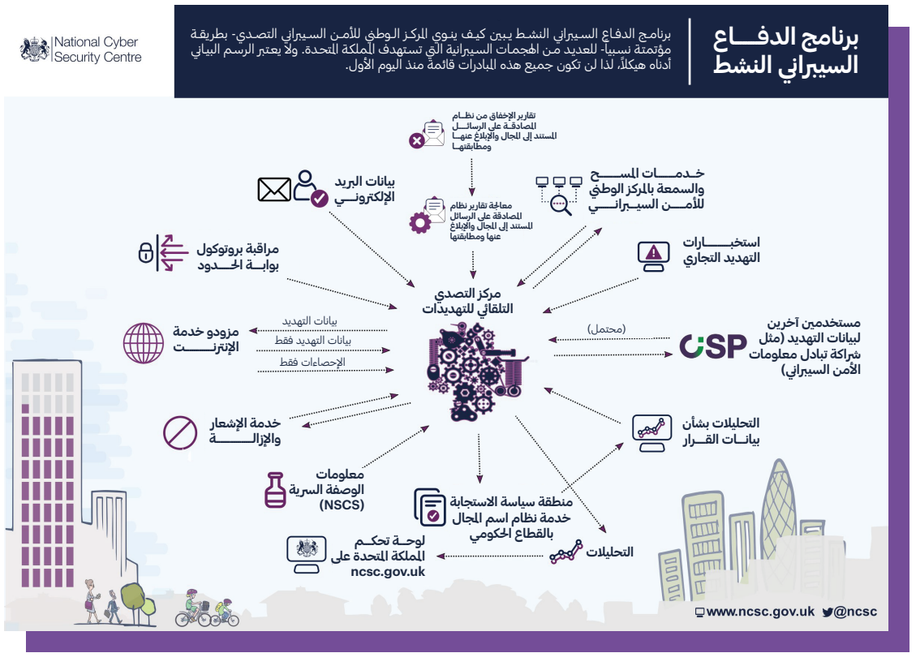
في المملكة المتحدة، تعرض أكثر من 40% من الشركات و20% من المؤسسات الخيرية هجوم أو اختراق سيبراني خلال عامي 2020-2021. وتشير الإحصاءات الرسمية إلى أن احتمال وقوع أي مقيم في بريطانيا ضحيةً لجريمة سيبرانية أو احتيال إلكتروني أكبر من احتمال تعرضه لأي جريمة أخرى. إضافة إلى ذلك، وربما نظراً إلى الثراء النسبي للمملكة المتحدة، من المرجح أن يستهدف مجرمو الفضاء السيبراني سكانها بمعدل يزيد على ضعف المتوسط العالمي، وأن يفوق العائد المادي لكل جريمة ضعف متوسط العالمي. ويشير أحد التقديرات إلى أن 4.6 مليارات جنيه إسترليني سُرقت من 17 مليون مستخدم للإنترنت في بريطانيا في عام 2017.

تم إطلاق برنامج الدفاع السيبراني النشط، الذي تموله الحكومة، لأول مرة في عام 2018. وكان هدفه الرئيسي هو منع المجرمين السيبرانيين من استخدام الشبكات والعلامات التجارية الحكومية لخداع مستخدمي الخدمات الحكومية والاحتيال عليهم. ولحسن الحظ، فإن معظم الجرائم السيبرانية غير معقّدة نسبياً، ويمكن للاستخدام الواعي للتكنولوجيات المتاحة أن يحد من حجمها وتأثيرها بشكل كبير. وقد تم نشر واختبار أدوات وفنيّات برنامج الدفاع السيبراني النشط بدايةً في القطاع العام، ويتم الآن الترويج لتوسيع استخدامها خارج نطاق الشبكات الحكومية لتعزيز الأمن السيبراني في القطاع الخاص والمجتمع المدني. غير أن هذا التوجه يثير تساؤلات حول التدخل الحكومي في القطاع الخاص وغيره، خصوصاً أن برنامج الدفاع السيبراني النشط أنشأه جزء من وكالة استخبارات الإشارات البريطانية ويتولى الإشراف عليه.

ويتمثل الهدف العام لبرنامج الدفاع السيبراني النشط في ضمان أن شبكات المملكة المتحدة وبياناتها وأنظمتها في المجالات العامة والتجارية والخاصة تتمتع بالمرونة أمام الهجمات السيبرانية ومحمية منها. هذا النهج يدرك إدراكاً صحيحاً أن من المستحيل ردع كل جهة خبيثة فاعلة في الفضاء الإلكتروني، سواء كانت دولة أو مجرماً أو إرهابياً أو أي مجموعة أو فرد آخر. لذا تبرز الحاجة إلى تحسين الدفاعات السيبرانية بحيث "تقلل بدرجة كبيرة من تعرضنا للحوادث السيبرانية، وتحمي أصولنا الأعلى قيمة، وتمكننا جميعاً من العمل بنجاح وازدهار في الفضاء الإلكتروني".

يتمثل الإسهام الفريد لبرنامج الدفاع السيبراني النشط في تبنيه نهجاً استباقياً لتحسين مخرجات الأمن السيبراني، باستخدام عمليات مؤتمتة نسبياً يمكنها التوسع بكفاءة وسرعة لحماية شبكات المملكة المتحدة ومستخدميها ومصالحها. ومنع البرنامج آلاف الهجمات وخفّض متوسط مدة اتصال مواقع التصيّد بالإنترنت من 27 ساعة إلى ساعة واحدة فقط.

وقد منع برنامج الدفاع السيبراني النشط آلاف الهجمات وقلص متوسط مدة اتصال موقع التصيد بالإنترنت من 27 ساعة إلى ساعة واحدة.



الشكل (1)

يعـالج برنامـج الدفـاع السـيبراني النشـط مشـكلة الهجمـات التقليديـة (commodity attacks)، وهي تلك الهجمات التي تتميز بكثافتها العددية وبساطتها التقنية نسبياً، وتشـمل أنواعاً متعـددة مـن البرمجيات الخبيثة التي تصيب الشـبكات والأنظمـة والمسـتخدمين بشـكل يومـي، إضافـة إلى أسـاليب متعـددة لسـرقة بيانـات الدخـول واختراق الحسـابات وغيرهـا. ولم يُصمـم البرنامـج للتعامـل مـع الجهـات الفاعلـة "المتطـورة تقنيـاً"، السياسـية أو الإجراميـة، التي تطـور وتنفـذ عمليـات أكثر تعقيـداً واسـتهدافاً ضـد أصـول المملكـة المتحـدة. فمسـؤولية التصـدي لهـذه التهديـدات المتطـورة تقـع على جهـات أخـرى تعمـل مـع شـركائها في أجهـزة الاسـتخبارات والجيـش والشـرطة على وضـع عمليـات مخصصـة لمواجهتها.

يقـوم برنامـج الدفـاع السـيبراني النشـط بأتمتـة الاسـتجابات للعديـد مـن الأنـواع مختلفـة مـن الهجمـات التقليديـة، بمـا في ذلـك التصيّـد، غير أن منظومـة الدفـاع السـيبراني النشـط تضم أيضـاً مجموعـة مـن العمليـات الأخـرى (انظر الشـكل رقم 1). وفيمـا يلي لمحـة عـن أنشـطته الأربـع الرئيسـة، التي تـم تفعيلهـا جميعـاً في البدايـة في القطـاع العـام فقـط:

خدمة الإزالة (Takedown Service):
تطلب مـن مـزوّدي خدمـات الاسـتضافة إزالـة المواقـع والمحتـوى الـذي ينتحـل صفـة حكومـة المملكـة المتحـدة وغيرهـا.

فحص البريد الإلكتروني (Mail Check):
يجعـل مـن الصعـب على المجـرمين توزيـع رسـائل إلكترونيـة تبـدو كأنهـا صـادرة عـن مصـدر موثـوق، مثـل مؤسسـة حكوميـة.

فحص المواقع الإلكترونية (Web Check):
يسـاعد مـالكي المواقـع الإلكترونيـة الحكوميـة على اكتشـاف الثغـرات والمشـاكل الأمنيـة الشـائعة.

نظام أسماء النطاقات الوقائي (Protective DNS):
يمنـع المسـتخدمين الحكوميين مـن الوصـول إلى المواقـع الإلكترونيـة الضـارة، مثـل تلـك المعروفـة بتوزيـع البرمجيـات الخبيثـة.

يشـمل برنامـج الدفـاع السـيبراني النشـط مجموعـة مـن المبـادرات الأخـرى، بمـا فيهـا مراقبـة البروتوكـولات. ويهـدف هـذا المكـوّن إلى تحسـين طريقـة تعامـل بروتوكـولات الإنترنـت والاتصـالات مـع تدفـق حركـة الإنترنـت، بمـا يجعـل مـن الصعـب سـرقة أصـول المملكـة المتحـدة واسـتخدامها، مـثلاً، في تنفيـذ هجمـات الحرمـان مـن الخدمـة الموزع. وينطبـق هـذا على القطـاعين العـام والخـاص على حـد سـواء بموجـب البروتوكـولات المشـتركة المسـتخدمة.

وأفاد أول تقرير سنوي عن برنامج الدفاع السيبراني النشط، الصادر في فبراير 2018، أن المواطـنين في المملكـة المتحـدة أصبحـوا موضوعيـاً أكثر أمانـاً في الفضـاء السـيبراني بفضـل هـذا البرنامـج. وفي أكتوبـر 2018، صـدرت بيانـات إضافيـة لدعـم هـذه المزاعـم. فعلى سـبيل المثـال، نجحـت خدمـة الإزالـة في خفـض حصـة المملكـة المتحـدة مـن هجمـات التصيّـد الإلكتروني العالميـة لأكثر مـن النصـف لتبلـغ 2.4% ، بعـد أن تمـت إزالـة نحـو 140,000 موقـع تصيّـد مسـتضاف في المملكـة المتحـدة، إضافـة إلى أكثر مـن 14,000 موقـع ينتحـل صفـة حكومـة المملكـة المتحـدة. وحظـر نظـام أسـماء النطاقـات الوقائي نحـو11,000 نطـاق ضـار كل شـهر، مـا جعلهـا غير متاحـة لمسـتخدمي الشـبكات الحكوميـة. كذلـك، وتمكّنـت أداة فحـص المواقـع الإلكترونيـة مـن اكتشـاف أكثر مـن 2,300 مشـكلة عاجلـة ضمـن المنظومـة الرقميـة للحكومـة، مـا سـمح بمعالجتهـا. وأظهـرت البيانـات أيضـاً ارتفاعـاً كبيـراً في معـدل اسـتخدام هـذه الخدمـات في المؤسسـات الحكوميـة.

خمسة مبادئ متشابكة يقوم عليها نهج برنامج الدفاع السيبراني النشط لتعزيز الأمن السيبراني في المملكة المتحدة:

المبدأ الأول هو أن برنامج الأمن السيبراني النشط في مرحلته الأولى اقتصر استخدامه على حماية القطاع العام فقط. وقد وصف المركز الوطني للأمن السيبراني (NCSC) هذا التوجّه بمبدأ "تجربة الحلول داخلياً أولاً"، أي أن الحكومة تجعل من نفسها حقل تجارب لهذه الحلول. والافتراض هنا هو أن الحكومة لن تطلب من أي أحد تطبيق حلول للأمن السيبراني لم تجربها على نفسها أولاً وتثبت فاعليتها.

المبدأ الثاني هو الأتمتة، حيث يعمل المركز الوطني للأمن السيبراني وشركاؤه على أتمتة أكبر قدر ممكن من العمليات اليومية لمكوّنات برنامج الدفاع السيبراني النشط. وينطبق هذا على أشكال المراقبة الفنية والفلترة المطلوبة من البرنامج، كما ينطبق أيضاً على إنتاج معلومات التهديدات وآليات إبلاغ الحكومة والشركاء الآخرين.

المبدأ الثالث هو أن برنامج الدفاع السيبراني النشط لا يمكن تركه للسوق وحده، بل يتطلب دوراً حاسماً من الحكومة التي لا تتردد في اتخاذ إجراءات مباشرة إذا عجزت السوق عن توفير حلول حماية كافية.

المبدأ الرابع يتعلق بالشفافية في إعداد التقارير. وفي هذا الصدد، ينشر برنامج الدفاع السيبراني النشط تقريراً سنوياً لرفع مستوى الوعي وجودة الأمن السيبراني.

المبدأ الخامس هو الشراكة، حيث تم تطوير العديد من مكونات برنامج الدفاع السيبراني النشط وتنفيذها بالشراكة مع مؤسسات خارج القطاع العام.

برنامج تحدي الابتكار الوطني
Cyber100 - ماليزيا

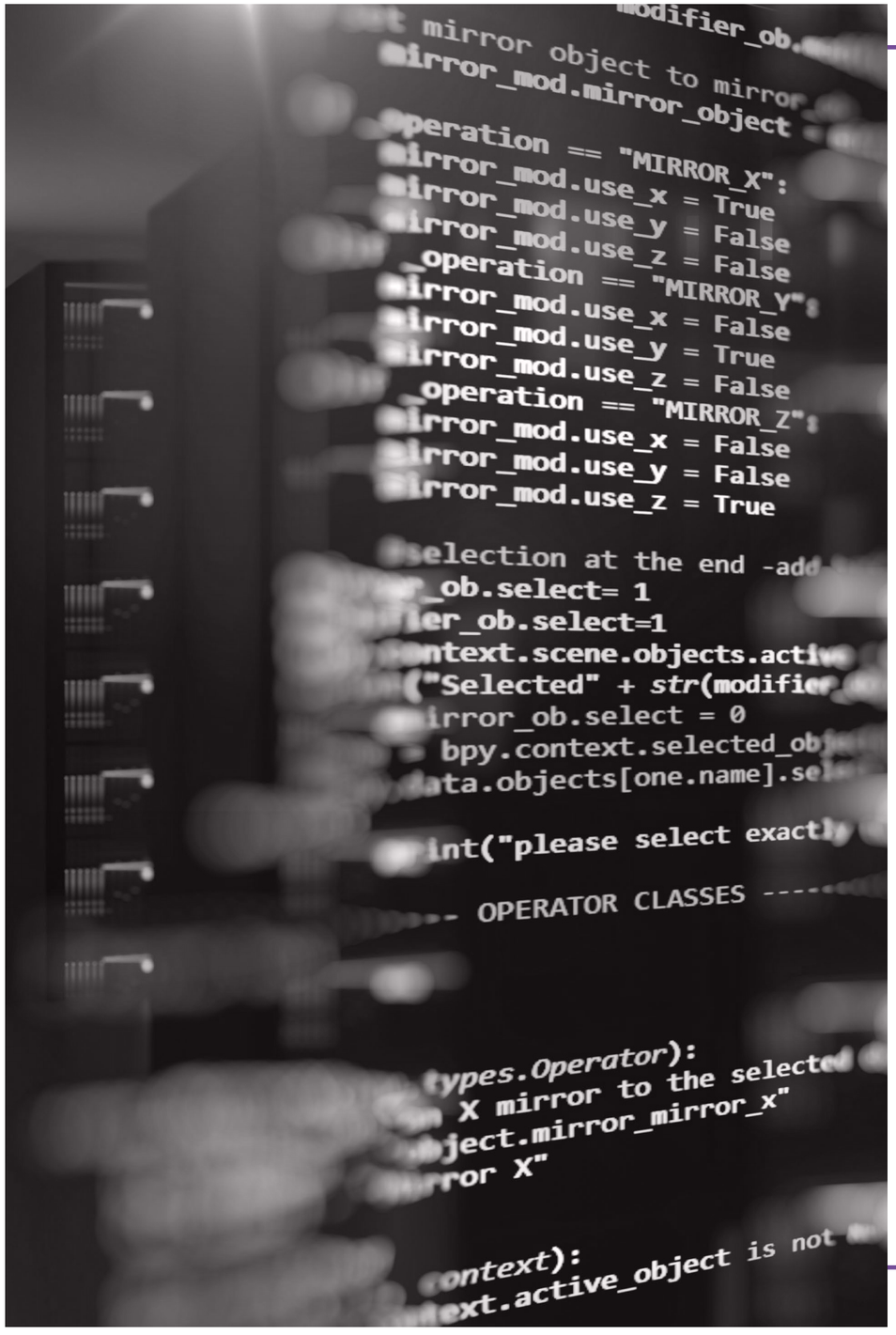
من أجل تلبية الطلب المتزايد باستمرار على حلول الأمن السيبراني، أطلقت مؤسسة الاقتصاد الرقمي الماليزية، بالتعاون مع الوكالة الوطنية للأمن السيبراني، برنامج التحدي الوطني للابتكار في الأمن السيبراني (Cyber100). ويسهم هذا التعاون بين الوكالة الوطنية للأمن السيبراني ومؤسسة الاقتصاد الرقمي الماليزية في خلق بيئة محلية مشجعة على الابتكار والبحث والتطوير. ويستضيف برنامج Cyber100 العديد من التحديات في مجال الأمن السيبراني على المستوى الوطني. ويتمثل هدفه في البحث حلول للمشاكل الخاصة بالصناعة، وتشجيع إنشاء تكنولوجيات محلية مبتكرة. وهذا يزيد من تعزيز مجتمع أمن المعلومات في ماليزيا ومكانة البلاد كمركز رقمي.

ويعد برنامج Cyber100 أول برنامج في ماليزيا لتحدي الابتكار في الأمن السيبراني. ويتضمن العديد من منصات وخدمات التوعية والابتكار التي تساعد في تطوير وتعزيز القدرات والإمكانات الوطنية في مجال الأمن السيبراني.

تم إطلاق تحدي Cyber100 في نوفمبر 2019 على أمل بناء دولة أكثر اتصالاً وأماناً. وبدأ التحدي بتقديم مشاركات من العديد من الشركات القائمة، ولم تصل منها إلى القائمة المختصرة سوى ست شركات فقط. وعلى عكس العديد من المسابقات التكنولوجية في الدول الأخرى، لا يشترط في المشاركين هنا أن يكونوا شركات ناشئة. وبعد ذلك اشتركت الشركات الست المختارة في برنامج توجيهي، ومن ثم قامت هذه الشركات بإطلاع أعضاء اللجنة على تقدُّمها. وفي المقابل، قدّم أعضاء اللجنة التوجيه والإرشادات لهذه الشركات وفقاً لما أحرزته من تقدم.

بعد انتهاء فترة البرنامج التوجيهي، طُلب من الشركات الست عرض وتوضيح تحدياتها وحلولها المقترحة لمعالجتها. وقد أتاح لها هذا العرض فرصة للحصول على تلقّي ملاحظات وتعليقات بشأن الحلول الخاصة بكل منها. وبنهاية برنامج Cyber100، أُتيحت فرصة لإخضاع الحلول التي قدّمتها الشركات الست لاختبار تجريبي واعتمادها من قِبل جهات أخرى بمساعدة من شركاء المنظومة الداعمة.

الابتكـار فـي الأمن السيبراني



تضمنت التحديات والحلول التي قدّمتها المجموعة الأولى من الشركات المختارة ما يلي:

شركة سيكيورمتريك Securemetric (وهي شركة رائدة في مجال الأمن السيبراني في جنوب شرق آسيا تتمتع بقدرات بحث وتطوير داخلية قوية في حلول التوقيع الرقمي والختم الزمني والمصادقة باستخدام تكنولوجيات البنية التحتية للمفاتيح العامة). **التحديات:** الهوية الأمنية الرقمية والمعاملات والتطبيقات. **الحلول:** استخدام الذكاء الاصطناعي لمنع الوصول غير المصرح به، ووضع معايير جديدة لكلمات المرور، وتطوير معايير جديدة للمصادقة الخالية من كلمات المرور.

شركة نيكسا جيت Nexagate (من أبرز مزوّدي خدمات واستشارات أمن تكنولوجيا المعلومات في ماليزيا). **التحدي:** مواجهة تحديات كبيرة في التخفيف من المخاطر السيبرانية، بما في ذلك تزايد متطلبات الامتثال، وارتفاع تكلفة نشر وصيانة الحلول الأمنية، ونقص المواهب في مجال الأمن السيبراني. **الحل:** إنشاء نظام إدارة موحد يُظهر المعلومات ذات الصلة لمختلف مستويات أصحاب المصلحة. وتقدّم المنصة ثلاثة مجالات رئيسية في مراقبة وضع الأمن السيبراني للمؤسسة، تشمل إدارة الامتثال وإدارة التهديدات وإدارة الحماية.

إدارة الحمـــاية	إدارة التهـديـدات	إدارة الامتثـال
لوحة ضبط الحماية	لوحة ضبط الأصول والتهديدات	لوحة ضبط نظام إدارة أمن المعلومات
أمن الشبكة	اكتشاف الأصول	إدارة المستندات
الحماية من هجوم قطع الخدمة الموزع	فحص نقاط الضعف	تتبع التنفيذ
حماية نقاط النهاية	تقرير نقاط الضعف	إدارة الحوادث والتغيير

شركة DNSVault ITP (حل فلترة النطاقات القائم على نظام أسماء النطاقات، وتستضيفه وتديره بيئة سحابية مشتركة). **التحدي:** تحظى الهجمات السيبرانية ضد الشركات الكبرى بتغطية إعلامية جيدة، في حين أن الهجمات ضد الشركات الصغيرة لا تحظى باهتمام يُذكر، وهذا يمكن أن يمنح الشركات الصغيرة شعوراً زائفاً بالأمان، رغم أنها عموماً أكثر عرضة للخطر من الشركات الكبيرة بسبب محدودية مواردها المخصصة للأمن السيبراني. **الحل:** أنظمة الأمن السحابية القابلة للتوسع تقلل من التكاليف العامة لتكنولوجيا المعلومات.

شركة تيكفورت Tecforte (شركة حائزة على جوائز، وهي متخصصةٍ في معلومات الأمن السيبراني وإدارة التهديدات). **التحدي:** يوجد عدد كبير جداً من الأجهزة الجديدة والتهديدات السيبرانية الجديدة يجعل من الصعب إدارتها ومراقبتها؛ وبسبب نقص الموارد والأدوات، يفشل الكثيرون في معالجة الأحداث والهجمات الأمنية في الوقت الفعلي. **الحل:** منصات استخبارات التهديدات التي تجعل عمليات الأمن السيبراني أكثر أماناً واستدامة من خلال الجمع بين كل ما يلزم لإدارة الأمن السيبراني بفاعلية في مكان واحدة.

شركة سيكيوركي SecureKi (متخصصة في تأمين وإدارة بيانات الاعتماد، ما يساعد العديد من العملاء على إيقاف الهجمات الاستهدافية، وتقليل التهديدات الداخلية، وتحقيق متطلبات الامتثال، وتحسين العمليات، وتأمين المؤسسات الهجينة. **التحدي:** الحاجة إلى تقليل مخاطر عدم الامتثال وتحسين الكفاءة التشغيلية من خلال تمكين دفاع الوصول المتميز. **الحل:** الجيل التالي من الإدارة الآلية لكلمات المرور المتميزة، مع التسجيل المرئي، والتحكم الدقيق في الوصول، والمصادقة المتعددة العوامل، وإمكانيات تسجيل الدخول الموحد للبنية التحتية.

شركة إي-لوك e-Lock (شركة رائدة في مجال أمن تكنولوجيا المعلومات تزوّد المؤسسات بحلول لمنع سرقات الهوية والهجمات السيبرانية المتقدمة وتهديدات سلامة بيانات المؤسسة). **التحدي:** تطور هجمات الفدية وبراعتها جعل من الصعب على برامج مكافحة الفيروسات العادية وجدران الحماية أن تكون فعالة في التصدي لها. **الحل:** حماية من طبقتين ضد برمجيات الفدية؛ حيث تتمثل الطبقة الأولى في حل الهجوم الفوري الذي ينشئ جداراً من التطبيقات الموثوقة ليوفر سياجاً من الحماية للأجهزة من التهديدات غير المعروفة، في حين تحمي الطبقة الثانية البيانات مع توفير نسخ احتياطية مشفرة وسلسلة في الوقت الفعلي.

استراتيجية الأمن السيبراني في ماليزيا 2020-2024

القاعدة الوطنية للابتكار والمواهب في مجال الأمن السيبراني
الصين

في كل عام، يتضاءل عرض متخصصي الأمن السيبراني في الصين أمام الطلب عليهم. وفي الواقع، لا يُشغَل سوى 5% فقط من الوظائف الشاغرة سنوياً. وعلى الرغم من العجز البالغ 1.4 مليون متخصص في مجال الأمن السيبراني، تُعد الصين بالفعل قوة سيبرانية تكاد تضاهي الولايات المتحدة، وتريد الآن إلى أن تصبح "قوة سيبرانية عظمى".

في قلب تلك المهمة يقع المجمّع الضخم التابع للمركز الوطني للأمن السيبراني الذي يُبنى حالياً في مدينة ووهان على مساحة تبلغ 40 كيلومتراً مربعاً ويُعرف رسمياً باسم القاعدة الوطنية للمواهب والابتكار في مجال الأمن السيبراني. لقد بدأ تشييد هذا المجمّع في عام 2019، وما زال قيد الإنشاء حتى اليوم، ويضم سبعة مراكز مخصصة للبحث العلمي وتنمية المواهب وريادة الأعمال، ومختبرين موجهين لدعم الحكومة، ومدرسة وطنية للأمن السيبراني.

يُعد المركز الوطني للأمن السيبراني مكوناً رئيسياً في استجابة الصين لتحديات الأمن السيبراني، وسيحسّن قدراتها السيبرانية من خلال التركيز على هدفين: تنمية المواهب وحفز الابتكار. وهذه "القاعدة" أشبه بمجمّع صناعي مترامي الأطراف أكثر من منشأة عسكرية مسوَّرة. ورغم وجود أربعة مجمعات أمن سيبراني وقواعد صناعية أصغر في كل من تشنغدو وشنغهاي وشانشي وتيانجين، فإن أياً منها لا يرقى إلى مستوى المركز الوطني للأمن السيبراني، إذ لا تتجاوز مجتمعة ربع مساحته، وتقل عنه بدرجات كبيرة من حيث حجم الاستثمار. ويُظهر هذا الحجم مدى أهمية المشروع في نظر صناع السياسات الصينيين، الذين يرون أن المركز الوطني للأمن السيبراني هو "القاعدة" الوحيدة التي تدمج الحكومة والصناعة والأوساط الأكاديمية والبحث والتطبيق التكنولوجي في إطار واحد.

وسيظهر أثر المركز قريباً - فقد فتحت المدرسة الوطنية للأمن السيبراني أبوابها للطلبة في أغسطس 2020، وسوف تتخرج أول دفعة منها في يونيو 2022. ومن هناك، سينضم هؤلاء الخريجون إلى صفوف العاملين المجال السيبراني، سواء في القطاع العام أو الخاص. وبصرف النظر عن القطاع الذي سينضمون إليه، سيستمر قادة الحكومة في الوصول إلى خريجي المركز الوطني للأمن السيبراني وابتكاراته. وبدلاً من تدريس المحتوى الأساسي، تهدف المدرسة إلى ضمان أن الأفضل والأذكى من كوادر الأوساط الأكاديمية والقطاع الخاص هم من يتولون تدريس الطلاب الواعدين تحت إشراف الحكومة وتوجيهها، مع تركيز خاص على المهارات العملية، والابتكار، وريادة الأعمال. ولتحقيق هذا، تحسب المدرسة التدريب العملي والمنافسات والأوراق البحثية المنشورة والابتكارات وبراءات الاختراع المكتسبة والشهادات المهنية ضمن متطلبات الدرجات العلمية. كما تولي المدرسة اهتماماً خاصاً لبرنامج الدكتوراه، حيث توفر مرشداً علمياً استراتيجياً ومرشداً مبتكراً متخصصاً في ريادة الأعمال لمساعدة مرشحي الدكتوراه على إجراء البحوث التطبيقية وتحويلها إلى مشاريع تجارية. ورغم أن عدد خريجي الدفعة الأولى يبلغ 1300 طالب فقط، يأمل صناع السياسات في رفع العدد إلى 2500 خريج سنوياً.

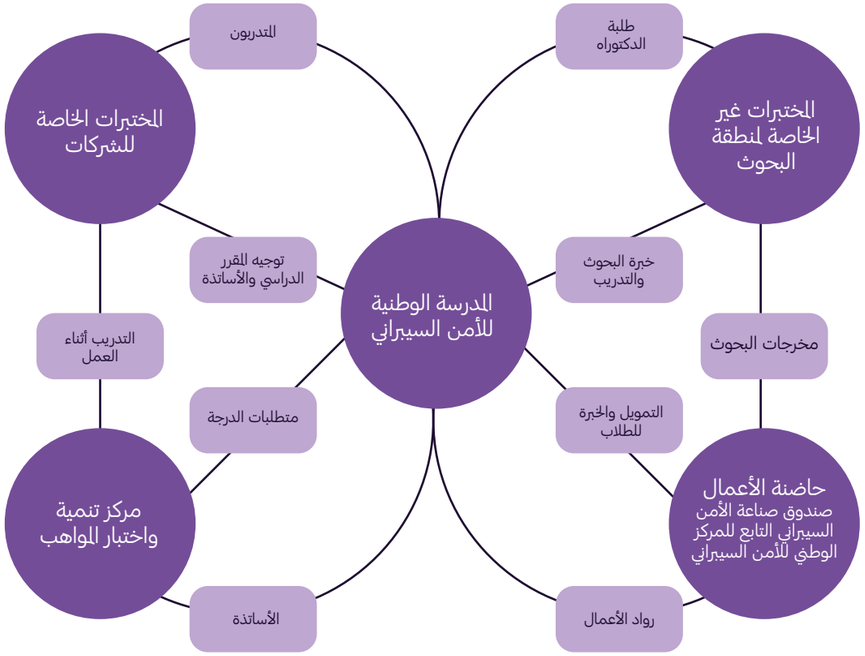
أما مركز تنمية واختبار المواهب، وهو المكوّن الثاني المعني بالمواهب، فيقدّم دورات تدريبية وشهادات لمهني الأمن السيبراني في بداية ومتوسط حياتهم المهنية. ويمتلك القدرة على تدريس ستة آلاف متدرّب شهرياً، أي ما يزيد على سبعين ألفًا سنوياً عند التشغيل الكامل. وباحتساب كلا المكوّنين، يمكن للمركز الوطني للأمن السيبراني تدريب أكثر من نصف مليون متخصص خلال عقد واحد.

ويُعد جذب أفضل متخصصي الأمن السيبراني في الصين إلى العمل داخل المركز الوطني للأمن السيبراني أمراً حاسماً لنجاحه. وتسعى قيادة الحزب الشيوعي الصيني إلى استقطاب نخبة المواهب السيبرانية في البلاد عبر توفير السكن والوظائف في نموذج يشبه "البلدة الصناعية" القديمة في الولايات المتحدة، لكن مع حوافز ومكافآت أكبر.

وستستخدم إدارة الفضاء السيبراني لبلدية ووهان والمدرسة الوطنية للأمن السيبراني الإعانات البحثية وجوائز المواهب لجذب المواهب إلى المركز الوطني للأمن السيبراني. كما ستقدّم لجنة الحزب والحكومة المحلية في ووهان منحة مالية لمرة واحدة بقيمة مليوني رنمينبي (309 آلاف دولار أمريكي تقريباً) لاستقطاب المتخصصين البارزين في الأمن السيبراني للتدريس في المدرسة، وهو مبلغ يعادل متوسط راتب 10 إلى 20 عاماً في مجال الأمن السيبراني، ويُعد من أكثر الحوافز سخاءً ضمن برامج استقطاب المواهب في الصين. وهناك برنامج آخر يستهدف الفرق البحثية التي تُعد أعمالها حيوية للأمن السيبراني، حيث ستقدم حكومة ووهان المحلية ما يصل إلى 100 مليون رنمينبي لدعم إنتقال هذه الفرق إلى المركز الوطني للأمن السيبراني. وتعمل هاتان السياستان معاً لضمان استقطاب أفضل الممارسين من دون التأثير في مسار الابتكار الجاري.

ورغم أن المركز الوطني للأمن السيبراني ما زال تحت التشييد، فقد أخذت الشركات تصطف لحجز مواقع لها داخل المشروع. وبحلول سبتمبر 2020، وافقت 114 شركة على إنشاء مقارّ لها في المركز، متعهدةً باستثمارات تجاوزت 71.5 مليار دولار أمريكي.

خريطة مفاهيم لمكونات المركز الوطني للأمن السيبراني



مركز التحقق من التكنولوجيا	مركز تقييم التكنولوجيا	مركز الحوسبة الخارقة والبيانات الكبيرة	برامج المواهب	مركز العرض	المركز التجاري

تعزيز الابتكار البحري ومرونة الأمن السيبراني
سنغافورة

كشفت سنغافورة عن خطط لدفع عجلة الابتكار وتعزيز مرونة الأمن السيبراني في قطاعها البحري من خلال مبادرات جديدة تشمل إعداد خريطة طريق لتوجيه المؤسسات العاملة في القطاع نحو تجريب ممارسات التصنيع بالإضافة (الطباعة الثلاثية الأبعاد). وقالت هيئة الملاحة البحرية والموانئ في سنغافورة إنها تسعى إلى تطوير قدرات الأمن السيبراني البحري بحيث تتمتع الصناعة بالمرونة والبنية التحتية اللازمة لإدارة الاضطرابات. كما قالت الدولة إنها تطمح إلى أن تصبح "وادي السيليكون للتكنولوجيا البحرية"، بالتركيز على الرقمنة والابتكار والشراكات. وقد أصدرت، على وجه التحديد، تقريراً يهدف إلى توفير خريطة طريق لمساعدة المؤسسات على تجريب ممارسات جديدة في مجال الطباعة الثلاثية الأبعاد. ووضّح التقرير الجديد قدرات الطباعة الثلاثية الأبعاد في المجال البحري في سنغافورة والدروس المستفادة من التجارب السابقة وعمليات التبنّي.

وللمزيد من تسريع التحول الرقمي في القطاع، أعلنت هيئة الملاحة البحرية والموانئ في سنغافورة أن الخطة الرقمية لصناعة النقل البحري قد تم توسيعها للسماح لنحو 3000 شركة صغيرة ومتوسطة الحجم عاملة في جميع قطاعات سوق النقل البحري بالتقدم بطلبات للحصول على مساعدة تمويلية مشتركة. وسيشمل ذلك الشركات الصغيرة والمتوسطة العاملة في القطاعات الفرعية مثل وسطاء الشحن البحري والمفتشين البحريين ومشغلي السفن، الذين يمكنهم الآن التقدم للحصول على دعم تمويلي ليتبنّوا الأدوات الرقمية المعتمدة مسبقاً. كما وقعت الهيئة اتفاقية مع سبع جهات عاملة في هذا المجال، من بينها إيستبورت مارين Eastport Maritime، وأوشن نتوورك إكسبريس Ocean Network Express، وأورينت مارين Orient Maritime Agencies، لتعزيز قدرات الأمن السيبراني في القطاع المحلي.

وسيتم بموجب هذا التعاون إنشاء مائدة مستديرة للأمن السيبراني البحري يوصي المشاركون خلالها بمبادرات تهدف إلى تحسين الشراكة في الأمن السيبراني البحري، بما في ذلك تبادل البيانات، وتعزيز المهارات السيبرانية البحرية المحلية، ورفع مستوى الوعي وكذلك إتاحة الوصول إلى الأدوات والمهارات البحرية الرقمية. ومن المقرر أن تعقد هذه المائدة المستديرة اجتماعها الأول في أواخر عام 2022 لمناقشة المبادرات على مدى السنوات الثلاث التالية لتعزيز الدفاع السيبراني ومهارات الأمن السيبراني البحري في سنغافورة.

وأشار قادة الحكومة إلى ضرورة دمج إدارة المخاطر السيبرانية البحرية في أنظمة إدارة السلامة في الشركات المشغّلة للسفن التي ترفع علم سنغافورة. وسيقدم صندوق المجموعة البحرية أيضاً دعماً تمويلياً مشتركاً لدورات تدريبية في الأمن في الأمن السيبراني لضمان أن العمال على وعي بالمخاطر ولديهم المعرفة والمهارات اللازمة لحماية أنفسهم من الهجمات السيبرانية. إضافة إلى ذلك، ظلت هيئة الملاحة البحرية والموانئ في سنغافورة تتعاون مع نظرائها من خلال شبكة مديري أمن المعلومات السيبرانية في سلطات الموانئ بهدف مشاركة البيانات وأفضل الممارسات.

إطلاق "مدينة سيبرانية" متخصصة
فرنسا

في بداية عام 2022، كشفت الحكومة الفرنسية عن مدينة سيبرانية مصممة لتجمع بين القطاعين العام والخاص للتصدي معاً للهجمات السيبرانية. ويأتي هذا بعد عام شهد ارتفاعاً قياسياً في هجمات الفدية، وفي وقت تستعد فيه الحكومات حول العالم – خصوصاً الحكومات الأوروبية - لاحتمال تعرضها لهجمات سيبرانية من موسكو رداً على العقوبات المفروضة بسبب أوكرانيا.

أُطلق على هذه المدينة السيبرانية الجديدة اسم "المجمّع السيبراني"، وتقع بالقرب من منطقة "لا ديفنس" التجارية في باريس، وجاءت بعد عام من إعلان استراتيجية الأمن السيبراني في فرنسا. وتبلغ ميزانية الاستراتيجية مليار يورو، وتهدف إلى تحسين مرونة الدولة وبناء صناعتها السيبرانية، حيث تسعى الحكومة إلى زيادات العائدات في قطاع الأمن السيبراني بمقدار ثلاثة أضعاف إلى 25 مليار يورو ومضاعفة عدد الوظائف إلى 75 ألف وظيفة، وإنشاء شركات فرنسية جديدة "عملاقة" في مجال الأمن السيبراني.

في المبنى الجديد، المعروف باسم المجمّع السيبراني والمكوّن من 13 طابقاً، ستتحقق الاستراتيجية السيبرانية للحكومة الفرنسية، لأنه يجمع بين الشركات الخاصة، الكبرى منها والناشئة، والهيئات العامة، والجيش، والإدارات الحكومية، والباحثين والطلاب في مجال الأمن السيبراني، وذلك لحشد الموارد وتعزيز التعاون. ووفقاً للحكومة، من الممكن أن يحدث توسع على المدى القصير في مدينة فرساي القريبة، إلى جانب خطط لإنشاء نسخ مناطقية من المجمع السيبراني خلال الأعوام المقبلة.

يتكون مبنى المجمّع السيبراني من:

12,000 متر مربع
من مساحات العمل الخاصة أو المشتركة.

3,000 متر مربع
مخصصة لمنصات المشاريع والابتكار.

2,000 متر مربع
مخصصة للتدريب.

مساحات مشتركة
تضم قاعة محاضرات وصالة عرض واستوديو تلفزيوني

من خلال نهج متعددة التخصصات، لا يكتفي المجمّع السيبراني بتشجيع التعاون بين القطاعين العام والخاص لمواجهة تهديد الهجمات السيبرانية المتزايد، بل يجمع أيضاً نخبة العقول في هذا المجال ليجعل من فرنسا مركزاً للابتكار السيبراني. كما سيوفر مكاناً لتطوير المهارات المهنية ولتنمية الوعي العام بأهمية الأمن السيبراني. وقد استُلهم المجمّع من نجاح إسرائيل في مشروع سايبر سبارك CyberSpark في بئر السبع، الذي بدأ كمرفق بحثي متخصص في الأمن السيبراني ثم تحوّل لاحقاً إلى مركز للشركات الناشئة والابتكار. وسيُوفّر مشروع المجمّع السيبراني منصة للتعاون بين مختلف أصحاب المصلحة، خصوصاً في مجال الاستجابة للحوادث السيبرانية.

يمكن أن يستوعب المجمّع السيبراني حالياً 1800 شخص في مبناه الذي تبلغ مساحته 26 ألف متر مربع، رغم أنه كان يضم 700 خبير فقط عند بداية إطلاقه. وتديره شركة مساهمة جديدة تملكها وتموّلها الدولة الفرنسية بنسبة 44%، ويتوزع باقي رأس المال بين نحو 90 مؤسسة تضم شركات فرنسية رائدة في هذا المجال.

وانضمت شركات فرنسية، مثل أورنج Orange وكابجيميناي Capgemini وتاليس Thales وأتوس Atos، إلى المجمّع كمستثمرين وشركاء، إلى جانب العديد من الشركات الناشئة والمؤسسات البحثية والجهات الحكومية ذات الصلة بالأمن السيبراني، بما في ذلك إدارة الدفاع السيبراني. وحتى الآن، أكّدت أكثر من 160 جهة من مختلف قطاعات الأعمال التزامها بالمشاركة في المجمّع الرقمي. كما ستؤسس وزارة الداخلية الفرنسية ووزارة القوات المسلحة والوكالة الوطنية لأمن نظم المعلومات والمعهد الوطني للبحوث في العلوم والتكنولوجيات الرقمية مكاتب لها في الموقع، لتشغل نحو 21% من مساحة المبنى.

تم الإعلان عن المجمّع السيبراني أولاً في صيف عام 2019، في ظل تصاعد المخاطر السيبرانية، حين أعلن الرئيس الفرنسي إيمانويل ماكرون عن إنشائه بهدف تعزيز التكامل داخل القطاع وتطوير حلول سيبرانية رائدة. وقد أعلنت القيادة الفرنسية أنها لا تريد الاعتماد على الخارج فيما يتعلق بالتكنولوجيات المتقدمة.

مبنى المجمّع السيبراني في "لا ديفنس"

أفضل الممارسات

بنية الثقة الصفرية (ZTA)

بنية الثقة الصفرية هي نموذج أمني يفترض أنه لا يوجد أحد ولا أي شيء جدير بالثقة بطبيعته، بغض النظر عن موقعه (داخل الشبكة أو خارجها). ويقوم هذا النموذج على مبدأ "لا تثق أبداً، تحقّق دائماً".

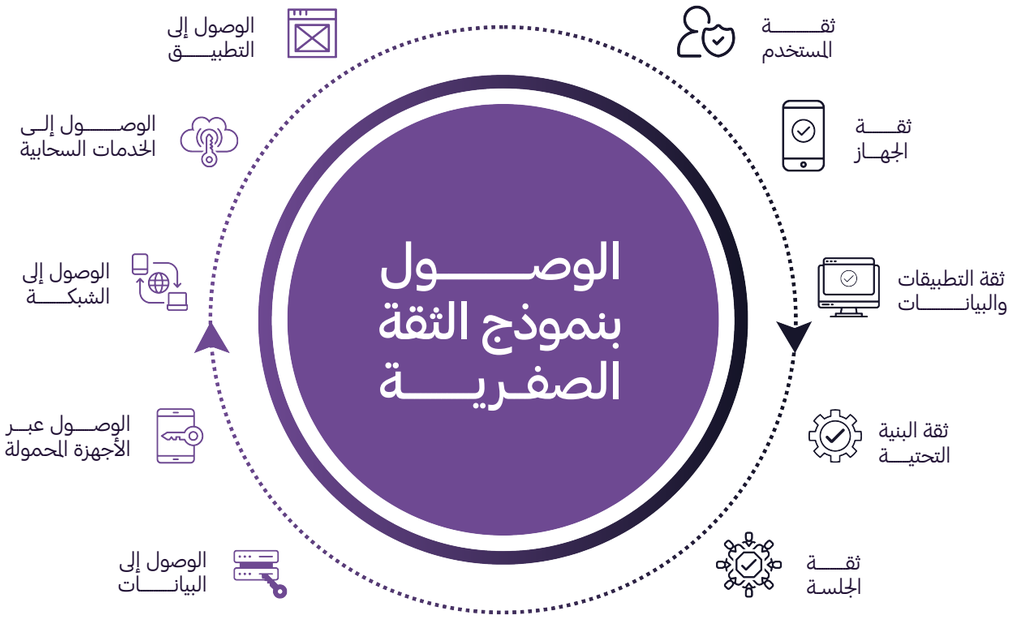
بنية الثقة الصفرية هي بنية أمنية تقوم على هذا المبدأ، وتركّز على:

- المصادقة القوية: يجب التحقق من كل مستخدم وكل جهاز قبل منح صلاحية الوصول.
- امتياز الحد الأدنى للوصول: لا يُمنح المستخدمون صلاحية الوصول إلا للبيانات والموارد التي يحتاجونها لأداء عملهم فقط.
- التحقق المستمر: تتم مراقبة وتقييم أمان المستخدم والجهاز بشكل متواصل.
- التجزئة الدقيقة: يتم تقسيم الشبكات إلى أجزاء صغيرة للحد من تأثير الاختراق.

فوائد بنية الثقة الصفرية:

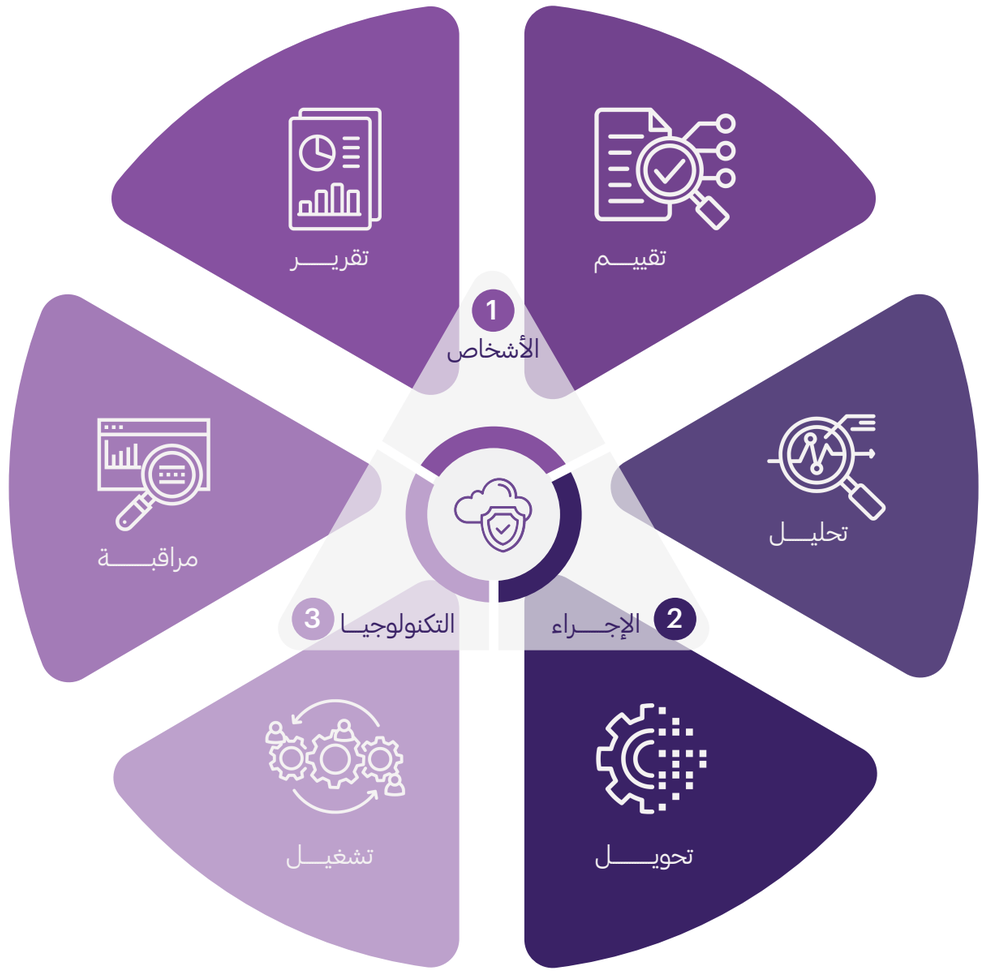
- تعزيز الأمن من خلال تقليص مساحة الهجوم.
- تحسين الحماية من اختراقات البيانات.
- رؤية أوضح للأنشطة داخل الشبكة.
- استجابة أسرع للحوادث السيبرانية.

جوهرياً، تنقل بنية الثقة الصفرية التركيز من حماية محيط الشبكة إلى حماية البيانات والموارد، بغض النظر عن مكان وجودها.



فوائد الأمن السحابي الأصلي

- تحسين الوضع الأمني.
- تسريع وقت طرح المنتج في السوق.
- تقليل مخاطر اختراق البيانات.
- تعزيز الامتثال.
- زيادة المرونة وقابلية التوسع.



الأمن السحابي الأصلي

الأمن السحابي الأصلي هو نهج شامل لحماية البيئات السحابية، حيث يدمج الأمن في دورة حياة تطوير البرمجيات منذ البداية. ويركّز على تأمين التطبيقات والمنصات والحاويات والبنية التحتية، مع معالجة التحديات الخاصة بالبيئات السحابية.

المكونات والاستراتيجيات الأساسية

التطوير والأمن والعمليات DevSecOps: دمج الأمن في عملية التطوير منذ البداية (shift-left) للكشف عن الثغرات ومعالجتها مبكراً.

منصة حماية التطبيقات السحابية الأصلية (CNAPP): منصة موحّدة توفر حماية شاملة للتطبيقات السحابية الأصلية طوال دورة حياتها.

بنية الثقة الصفرية: نموذج أمني يقوم على مبدأ "لا تثق أبداً، تحقّق دائماً"، ما يحد من الوصول إلى الموارد والبيانات.

إدارة الهوية والوصول (IAM): التحكم في الوصول إلى الموارد السحابية من خلال آليات مصادقة وتفويض قوية.

أمن البنية التحتية كتعليمة برمجية (Infrastructure as Code (IaC): تأمين البنى التحتية السحابية المعرّفة والمُدارة من خلال التعليمات البرمجية.

أمن الحاويات Container Security: حماية التطبيقات المعزولة داخل حاويات وبيئات التشغيل الخاصة بها.

حماية البيانات: حماية البيانات الحساسة من خلال التشفير، وضوابط الوصول، ومنع فقدان البيانات.

الرصد المتواصل والاستجابة المستمرة: الكشف الاستباقي عن التهديدات والاستجابة لها من خلال الرصد الفوري والاستجابة الآلية للحوادث.

إدارة الهوية المدعومة بتكنولوجيا البلوكتشين

تُعد إدارة الهوية المعتمدة على تكنولوجيا البلوكتشين نهجاً متطوراً لإدارة الهويات الرقمية والتحقق منها. وعلى عكس الأنظمة التقليدية التي تعتمد على سلطات مركزية، توفر تكنولوجيا البلوكتشين منصة لا مركزية وآمنة وشفافة.

السمات الرئيسة:

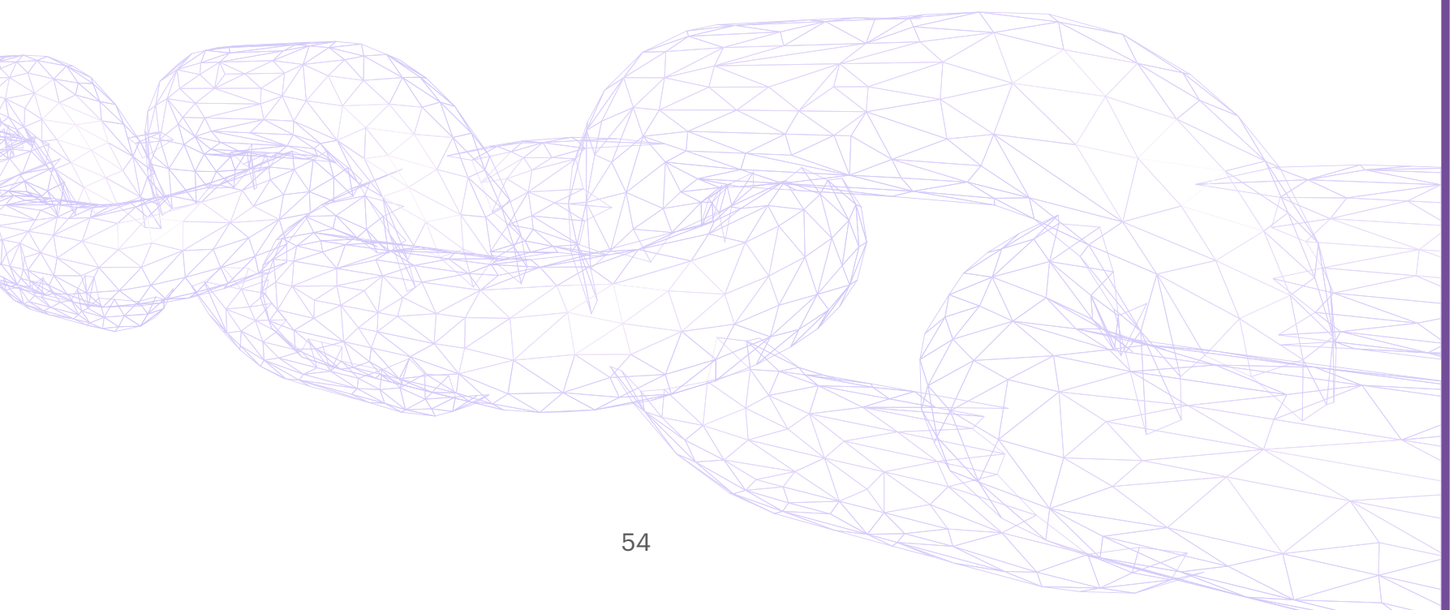
- **اللامركزية:** تُخزَّن بيانات الهوية غبر عُقَد متعددة، ما يقلل من مخاطر اختراق البيانات ونقاط الإخفاق الفردية.
- **الأمان:** تضمن آليات التشفير في البلوكتشين سلامة البيانات وحمايتها من التلاعب بها.
- **الخصوصية:** يتحكم المستخدمون في بياناتهم، ويحددون ما هي المعلومات التي يريدون مشاركتها ومع من يشاركونها.
- **الكفاءة:** تبسيط عمليات التحقق من الهوية يقلل التكاليف والوقت.
- **قابلية التشغيل البيني:** يمكن للأنظمة المختلفة مشاركة معلومات الهوية والتحقق منها بسهولة.

آلية العمل:

- **إنشاء الهوية:** يُنشئ المستخدم هوية رقمية، غالباً باستخدام نهج الهوية ذات السيادة الذاتية (SSI)، حيث يتحكمون في بياناتهم.
- **تخزين البيانات:** تُخزَّن معلومات الهوية على شبكة البلوكتشين كسلسلة من الكتل المشفّرة.
- **التحقق:** عند الحاجة إلى التحقق من الهوية، يمكن للمستخدم مشاركة سمات محددة بشكل انتقائي مع جهة التحقيق.
- **إدارة الموافقة:** يتمتع المستخدم بتحكم دقيق في بياناته، فيحدد من يمكنه الوصول إليها ولأي غرض.

الفوائد:

- تعزيز الأمن والخصوصية.
- الحد من حلال الاحتيال في الهوية.
- تحسين الكفاءة في التحقق من الهوية.
- زيادة الثقة والشفافية.
- تمكين الأفراد التحكم الكامل في بياناتهم.



منصّة الاستجابة الآلية للحوادث وتبادل المعلومات

تُعدّ منصّة الاستجابة الآلية للحوادث وتبادل المعلومات (AIRISP) حلاً تكنولوجياً متقدماً مصمماً لتبسيط وتعزيز عمليات الاستجابة للحوادث السيبرانية. وتجمع المنصّة بين الأتمتة والتعاون والذكاء لتحسين الكفاءة والفاعلية في إدارة الحوادث.

تشمل أبرز وظائف المنصّة ما يلي:

اكتشاف الحوادث والتنبيه عنها: تقوم المنصّة بتحديد الحوادث الأمنية المحتملة بشكل آلي استناداً إلى مصادر بيانات متعددة، وتصدر تنبيهات فورية عند رصدها.

تنسيق الحوادث: أتمتة المهام الروتينية مثل إنشاء تذاكر الحوادث، وتعيين فرق الاستجابة، وبدء كتيبات الإجراءات الخاصة بكل نوع من الحوادث.

دمج استخبارات التهديدات: تُدمج بيانات استخبارات التهديدات لتحسين تحليل الحوادث وتوجيه الاستجابة المناسبة.

التعاون والتواصل: تتيح المنصّة التعاون السلس بين فرق الأمن السيبراني وأصحاب المصلحة الآخرين من خلال أدوات اتصال متكاملة.

أتمتة إجراءات الاستجابة: تنفّذ المنصّة الإجراءات المحددة مسبقاً بناءً على خطورة الحادث ونوعه، ما يقلل من الحاجة إلى التدخل اليدوي.

تبادل المعلومات: تمكّن من تبادل بيانات ومعلومات الحوادث مع الشركاء الخارجيين بشكل آمن، ما يعزّز منظومة الدفاع الجماعي ضد الهجمات السيبرانية.

فوائد استخدام منصّة الاستجابة الآلية للحوادث وتبادل المعلومات AIRISP:

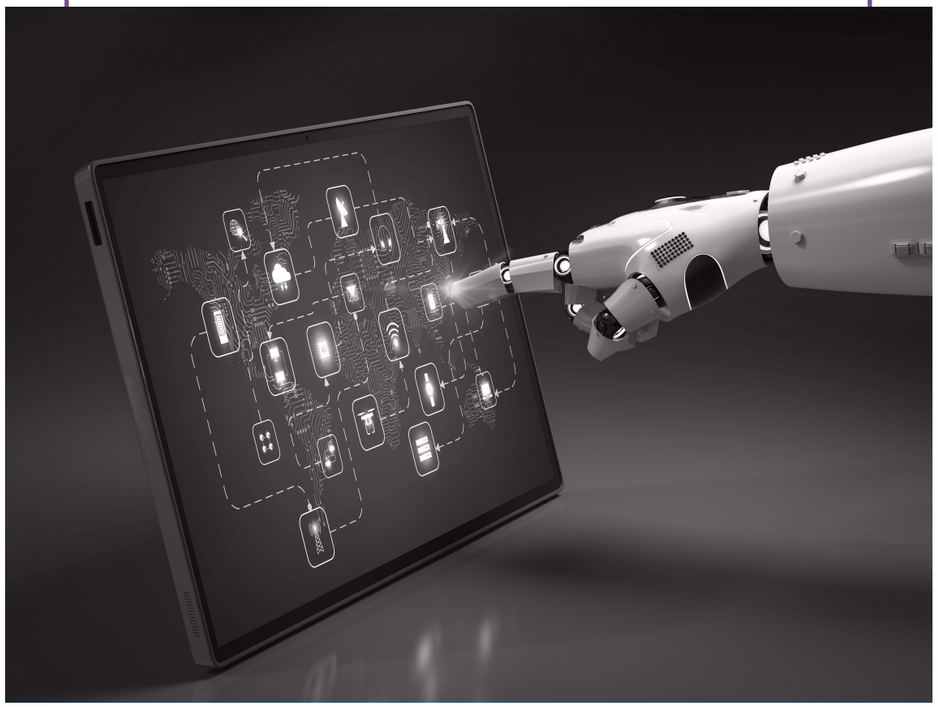
تسريع الاستجابة للحوادث: تُسهم الأتمتة في تسريع المراحل الأولى من معالجة الحوادث الأمنية.

تحسين إدارة الحوادث: تبسيط الإجراءات وتوشيح مسارات العمل تعزز يعزز الكفاءة العامة.

تعزيز القدرة على رؤية التهديدات: يتيح دمج معلومات استخبارات التهديدات فهماً أعمق لمشهد المخاطر السيبرانية.

تقوية التعاون: تُعزز المنصّة التواصل وتبادل المعلومات بين الفرق المختلفة.

الحد من تأثير الحوادث: تسريع احتواء الحوادث والتعافي منها من خلال إجراءات الاستجابة الآلية.



الألعاب التفاعلية وبيئات المحاكاة السيبرانية

تقوم الألعاب التفاعلية على إدخال عناصر من عالم الألعاب في مجالات غير ترفيهية، مثل التعليم أو بيئات العمل. وتهدف إلى رفع مستوى المشاركة والتحفيز والمتعة عبر استخدام عناصر مثل النقاط، والشارات، ولوحات الصدارة، والتحديات.

بيئات المحاكاة السيبرانية (Cyber Ranges)

هي بيئات محاكاة تتيح للأفراد أو الفرق ممارسة مهاراتهم في الأمن السيبراني ضمن بيئة آمنة ومتحكم بها. وتحاكي هذه البيئات الهجمات السيبرانية وسيناريوهات الدفاع الواقعية، ما يسمح للمشاركين بالتعلّم من أخطائهم دون عواقب حقيقية.

الدمج بين الألعاب التفاعلية وبيئات المحاكاة السيبرانية

يعزز الجمع بين هذين المفهومين تجربة التعلم بجعلها أكثر تشويقاً وتنافسيةً. ومن أبرز مكونات هذا الدمج:

- **أنظمة النقاط:** منح نقاط للمشاركين عند إتمام المهام أو التصدي للهجمات.
- **لوحات الصدارة:** ترتيب المتدربين وفق الأداء لتعزيز روح المنافسة.
- **الشارات والإنجازات:** منح جوائز رمزية تقديراً للتقدم والنجاح.
- **التحديات والمهام:** تصميم مسارات تعلم منظمة بأهداف واضحة.
- **السرد القصصي:** إدخال عنصر السرديات لجعل عملية التعلم أكثر تفاعلاً وغنى.

الابتكـار فـي الأمن السيبراني

الاستراتيجية الوطنية الإماراتية للأمن السيبراني (2025-2031)

مجلس الأمن السيبراني والاستراتيجية الوطنية

تأسس مجلس الأمن السيبراني في عام 2020 برئاسة سعادة الدكتور محمد حمد الكويتي، وهو السلطة الوطنية المسؤولة عن حماية المستقبل الرقمي للدولة. ويقود المجلس طموح دولة الإمارات لأن تكون رائدة عالميًا في الصمود السيبراني والثقة الرقمية، عبر العمل مع الحكومة، ومشغلي البنى التحتية الحيوية، والشركاء في القطاع الخاص، والأوساط الأكاديمية، والمنظمات الدولية. وتشمل مهام المجلس تطوير السياسات والمعايير، وبناء القدرات الوطنية، وتعزيز التعاون الدولي.

الاستراتيجية الوطنية الإماراتية للأمن السيبراني (2025-2031)

أطلقت دولة الإمارات استراتيجية وطنية طموحة للأمن السيبراني للفترة 2025-2031 لتأكيد مكانتها كقوة رائدة عالميًا في مجال الصمود السيبراني والثقة الرقمية. وبالاستناد إلى الأسس السابقة، تربط الاستراتيجية الجديدة الأمن السيبراني على نحو مباشر بالتحول الرقمي، وتنويع الاقتصاد، وأولويات الأمن الوطني. وتهدف إلى تمكين رؤية دولة الإمارات لتكون مركزًا رقميًا موثوقًا، يقود الابتكار ويتبنى بأمان التقنيات الناشئة مثل الذكاء الاصطناعي، والحوسبة الكمية، وشبكات الجيل الخامس/السادس، وإنترنت الأشياء.

الأهداف الاستراتيجية

تستند الاستراتيجية إلى ستة أهداف رئيسية:

- تعزيز الصمود السيبراني الوطني عبر البنية التحتية الحيوية والقطاعين الحكومي والخاص.
- حماية المواطنين والمجتمع من خلال ترسيخ الوعي والثقافة السيبرانية على جميع المستويات.
- ترسيخ الثقة في الاقتصاد الرقمي عبر ضمان أمن البيانات والمعاملات والتقنيات الناشئة.
- تمكين الابتكار والتقنيات المستقبلية من خلال اعتماد مبدأ الأمن في التصميم عند استخدام الذكاء الاصطناعي، والحوسبة السحابية، والبلوك تشين، والأنظمة الجاهزة للحوسبة الكمية.
- تطوير الكفاءات والقدرات الوطنية لسد فجوة المهارات في الأمن السيبراني وتعزيز خبرة الكوادر الإماراتية.
- قيادة الدبلوماسية السيبرانية والشراكات العالمية لتعزيز دور دولة الإمارات كمنصة للتعاون الدولي.

محاور التنفيذ

تُنظَّم عملية تنفيذ الاستراتيجية في خمسة محاور عمل رئيسية:

الحوكمة (Govern): وضع القوانين والمعايير والأطر التنظيمية المحدَّثة لحماية البنية التحتية الرقمية.

الحماية والدفاع (Protect & Defend): تعزيز قدرات الكشف والاستجابة عبر مراكز العمليات الأمنية المتقدمة، وأطر الاستجابة للحوادث، وجهوزية القطاعات.

الابتكار (Innovate): جعل دولة الإمارات منصة لتجريب الابتكارات السيبرانية، وتبني التقنيات الحديثة، وخلق بيئات جاذبة للبحث والتطوير والشركات الناشئة.

البناء (Build): تطوير القدرات الوطنية والصلابة عبر برامج تطوير القوى العاملة، ومبادرات البحث، وحملات التوعية.

الشراكة (Partner): توسيع التعاون مع الهيئات العالمية مثل الاتحاد الدولي للاتصالات، والإنتربول، ومركز مكافحة الإرهاب التابع للأمم المتحدة، ومنتدى الفرق المعنية بالأمن والاستجابة للحوادث (FIRST)، ومبادرة مكافحة برمجيات الفدية، إضافة إلى تعزيز الشراكات بين القطاعين العام والخاص.

مهمة مجلس الأمن السيبراني

تتمثل مهمة المجلس في تعزيز المرونة الوطنية من خلال ترسيخ الأمن السيبراني كركيزة أساسية للحياة الرقمية — بدءًا من حماية القطاعات والخدمات الحيوية، وصولًا إلى رفع مستوى الوعي لدى جميع أفراد المجتمع. ويعمل المجلس على ترسيخ ثقافة الأمن السيبراني، وتزويد المواطنين والمؤسسات بالأدوات اللازمة للتعامل مع التهديدات المتطورة، وضمان الثقة في النظام الرقمي لدولة الإمارات.

رؤية مجلس الأمن السيبراني

بناء فضاء سيبراني آمن وموثوق ومرن يمكّن من الابتكار ويحمي مجتمع دولة الإمارات واقتصادها وحكوماتها المستقبلية من الجرائم الإلكترونية والمخاطر الرقمية — بما يتماشى مع مئوية الإمارات 2071 ورؤية "نحن الإمارات 2031".

مهام مجلس الأمن السيبراني

تتماشى مهام المجلس مع الاستراتيجية الوطنية للأمن السيبراني (2025–2031)، حيث يُناط بالمجلس ما يلي:

- تطوير الاستراتيجية الوطنية للأمن السيبراني وتحديثها والإشراف عليها، ورفعها إلى مجلس الوزراء ومتابعة تنفيذها بالتنسيق مع جميع الجهات المعنية.
- اقتراح وإعداد التشريعات والسياسات والمعايير لتعزيز الأمن السيبراني عبر البنى التحتية الوطنية الحيوية، وأنظمة الحكومة، والتقنيات الناشئة مثل الذكاء الاصطناعي والحوسبة الكمّية.
- تصميم وتنفيذ إطار وطني للدفاع والاستجابة السيبرانية، يشمل إجراء تدريبات دورية، وتمارين محاكاة للأزمات، وتدريبات واسعة النطاق على الجاهزية.
- إنشاء منصات وطنية لتبادل المعلومات والحوكمة، بما يعزز الثقة بين الشركاء المحليين والدوليين من القطاعين العام والخاص.
- ضمان الامتثال والنضج في مجال الأمن السيبراني على نطاق الجهات الحكومية والبنى التحتية المعلوماتية الحيوية، بدعم من أطر مثل نظام ضمان أمن المعلومات في دولة الإمارات والبرنامج الوطني لاعتماد الأمن السيبراني.
- إنشاء واعتماد مراكز وطنية لعمليات الأمن السيبراني، وتعزيز الوعي الوطني الظرفي من خلال الرصد والكشف والاستجابة المنسقة.
- تطوير سياسات لاستيراد وتصدير واستخدام التقنيات الحرجة ذات الأبعاد السيبرانية بشكل آمن.
- قيادة جهود بناء القدرات وتطوير المواهب، مع توسيع مشاركة الكوادر الإماراتية في مجالات الأمن السيبراني، وتعزيز الشمولية للشباب والنساء وأصحاب الهمم.
- دفع البحث والابتكار والشراكات العالمية في مجال الأمن السيبراني، وترسيخ مكانة دولة الإمارات كقائد عالمي موثوق في الدبلوماسية السيبرانية والتعاون الدولي.

السياسات والأطر الحالية للأمن السيبراني

يهدف مجلس الأمن السيبراني إلى اقتراح السياسات والتشريعات لتحسين الأمن السيبراني في الدولة عبر جميع القطاعات المستهدفة ورفعها لمجلس الوزراء لاعتمادها وتنفيذها بالتعاون مع السلطات المعنية. وقد طوّر المجلس مجموعة من الوثائق ذات الأولوية لتعزيز الأمن السيبراني في الدولة، ومنها:

البرنامج الوطني لاعتماد الأمن السيبراني

مبادرة تهدف إلى تعزيز الثقة في منظومة الأمن السيبراني بالدولة من خلال رفع مستوى النضج الأمني بطريقة شفافة، استنادًا إلى أفضل الممارسات الدولية، وبما يوازن بين الكفاءة والأمن.

سياسة حماية البنى التحتية المعلوماتية الحرجة

تضع أسسًا لرفع مستوى الأمن والمرونة السيبرانية للبنى التحتية المعلوماتية الحرجة في الدولة، انسجامًا مع الأولوية الوطنية لدولة الإمارات بأن تكون رائدة عالميًا في مجال الأمن السيبراني، وكذلك لتنفيذ التدابير اللازمة نحو فضاء سيبراني مرن وآمن لبُناها التحتية المعلوماتية الحيوية.

خطة الاستجابة للحوادث السيبرانية

وُضعت لدعم تنفيذ الاستراتيجية الوطنية للأمن السيبراني من خلال إنشاء قدرة وطنية لإدارة الحوادث، وتحديد كيفية استعداد دولة الإمارات لمواجهة الحوادث السيبرانية الكبرى، والوقاية منها واكتشافها، والاستجابة لها، والتعافي والتعلم المستمر منها.

الحد الأدنى لقدرات مراكز عمليات الأمن السيبراني

يحدد الحد الأدنى من المتطلبات لمراكز عمليات الأمن السيبراني الخاصة بالبنى التحتية المعلوماتية الحيوية، وكذلك أهداف النضج لتعزيز المرونة السيبرانية الوطنية. وتستند هذه المبادرة إلى مكانة دولة الإمارات كقائد عالمي في مجال الأمن السيبراني، كما تسهم في تعزيز الوضع الأمني للمنظمات والأفراد داخل الدولة.

إطار تبادل معلومات الأمن السيبراني

يرسّخ إطارًا وطنيًا لتبادل معلومات الأمن السيبراني بما يعزز التعاون والتكامل بين مختلف أصحاب المصلحة، وبما يتماشى مع الأولوية الوطنية لدولة الإمارات في أن تكون رائدة عالميًا في مجال الأمن السيبراني، الأمر الذي يسهم في رفع مستوى الأمن السيبراني للمنظمات على مستوى الدولة.

السياسة الوطنية لأمن إنترنت الأشياء

تهدف لحماية استخدام تقنيات إنترنت الأشياء واعتمادها وتنفيذها، بما يتماشى مع الأولوية الوطنية لدولة الإمارات في أن تكون رائدة عالميًا في مجال الأمن السيبراني؛ ولتعزيز الوضع الأمني للمنظمات والأفراد داخل الدولة عند استخدام منتجات وحلول إنترنت الأشياء.

السياسة الوطنية لأمن الحوسبة السحابية

تهدف لتعزيز أمن استخدام الخدمات السحابية، انسجامًا مع الأولوية الوطنية بأن تكون دولة الإمارات رائدة عالميًا في الأمن السيبراني، والإسهام في تعزيز الوضع الأمني للمنظمات والأفراد داخل الدولة عند استخدام خدمات الحوسبة السحابية.

إطار الاستجابة للحوادث السيبرانية

يهدف إلى إنشاء قدرة وطنية لإدارة الحوادث السيبرانية وتحديد كيفية استعداد دولة الإمارات للحوادث السيبرانية الكبرى، والوقاية منها، وكشفها، والاستجابة لها، والتعافي منها؛ وذلك بما يتماشى مع الأولوية الوطنية لدولة الإمارات في أن تكون رائدة عالميًا في مجال الأمن السيبراني، ويسهم في تعزيز الوضع الأمني للمنظمات والأفراد داخل الدولة.

تحديث ضمان المعلومات في دولة الإمارات

وُضعت لائحة ضمان المعلومات في دولة الإمارات لتحديد المستوى المطلوب من حماية الأصول المعلوماتية والأنظمة الداعمة لها ضمن البنى التحتية الحيوية للدولة، وفُرضت لتكون الحد الأدنى من متطلبات الحماية في القطاع المصرفي الإماراتي.

ويجري حاليًا تحديث معيار ضمان المعلومات في دولة الإمارات ليجسد التغييرات الجوهرية التي طرأت على المشهدين التقني والأمني السيبراني منذ آخر تحديث لهذا المعيار.

وقد عقد مجلس الأمن السيبراني ورش عمل مع أعضاء لجنة السياسات، والجهات الوطنية، والمسؤولين في كل إمارة، والجهات التنظيمية القطاعية، والكيانات الرئيسة في الدولة. ويجري حاليًا تحديث إطار ضمان المعلومات في دولة الإمارات استنادًا إلى نتائج استبيان والملاحظات المستخلصة من ورش العمل الاستشرافية.

الاستراتيجيات والسياسات والأطر القادمة

استنادًا إلى الأساس المتين الذي أرسته الاستراتيجية الوطنية للأمن السيبراني، تعمل دولة الإمارات على تطوير جيل جديد من المبادرات لتعزيز مكانتها السيبرانية. وتهدف هذه الاستراتيجيات والسياسات والأطر القادمة إلى معالجة التحديات الناشئة، والاستفادة من التقدم التكنولوجي، وترسيخ مكانة دولة الإمارات كقائد عالمي في مجال الأمن السيبراني. وتشمل هذه المبادرات ما يلي:

السياسة الوطنية للتشفير: تهدف إلى تعزيز أمن البيانات، بما يتماشى مع الأولوية الوطنية لدولة الإمارات بأن تكون رائدة عالميًا في الأمن السيبراني، وتعزيز الوضع الأمني للمؤسسات والأفراد في الدولة عند التعامل مع البيانات الحرجة والشخصية.

السياسة الوطنية لأمن الأطراف الثالثة: تهدف إلى تعزيز أمن التعاملات مع مزوّدي الخدمات الخارجيين، بما يتماشى مع الأولوية الوطنية لدولة الإمارات بأن تكون رائدة عالميًا في الأمن السيبراني، وتعزيز الوضع الأمني للمؤسسات والأفراد في الدولة عند التعامل مع الأطراف الثالثة.

سياسة أمن تبادل البيانات: تهدف إلى تعزيز أمن تبادل البيانات، بما يتماشى مع الأولوية الوطنية لدولة الإمارات بأن تكون رائدة عالميًا في الأمن السيبراني، وتعزيز الوضع الأمني للمؤسسات والأفراد في الدولة عند تبادل البيانات التجارية الحرجة والبيانات الشخصية.

سياسة أمن البلوك تشين: تهدف إلى ضمان التنفيذ والتشغيل الآمنين للأنظمة القائمة على تقنيات البلوك تشين، بما يتماشى مع الأولوية الوطنية لدولة الإمارات بأن تكون رائدة عالميًا في الأمن السيبراني، وتعزيز الوضع الأمني للمؤسسات التي تعتمد هذه التقنية.

السياسة الوطنية للعمل عن بُعد بشكل آمن: تهدف إلى تعزيز أمن ترتيبات العمل عن بُعد، بما يتماشى مع الأولوية الوطنية لدولة الإمارات بأن تكون رائدة عالميًا في الأمن السيبراني، وتعزيز الوضع الأمني للمؤسسات والأفراد في الدولة الذين يستخدمون أنظمة العمل عن بُعد.

السياسة الوطنية لأمن الذكاء الاصطناعي: تهدف إلى تعزيز أمن تقنيات الذكاء الاصطناعي، بما يتماشى مع الأولوية الوطنية لدولة الإمارات بأن تكون رائدة عالميًا في الأمن السيبراني، وتعزيز الوضع الأمني للمؤسسات والأفراد في الدولة عند استخدام الذكاء الاصطناعي.

05

البرامـج الريادية والمبادرات العالمية لدولة الإمـــارات

برامج ومبادرات مجلس الأمن السيبراني

مبادرة النبض السيبراني

النبض السيبراني هي مبادرة أطلقها مجلس الأمن السيبراني لدولة الإمارات بهدف تعزيز الوعي والجاهزية في مجال الأمن السيبراني داخل الدولة. وتعد هذه المبادرة برنامجًا متكاملًا يضم العديد من المشاريع التي تركز على جوانب مختلفة من الأمن السيبراني. وتهدف هذه المبادرات إلى رفع مستوى الوعي، وتطوير قادة المستقبل، وتنفيذ تدريبات سيبرانية، وتعزيز قدرات المختصين في مجال الأمن السيبراني عبر جهود موجهة ومتنوعة.

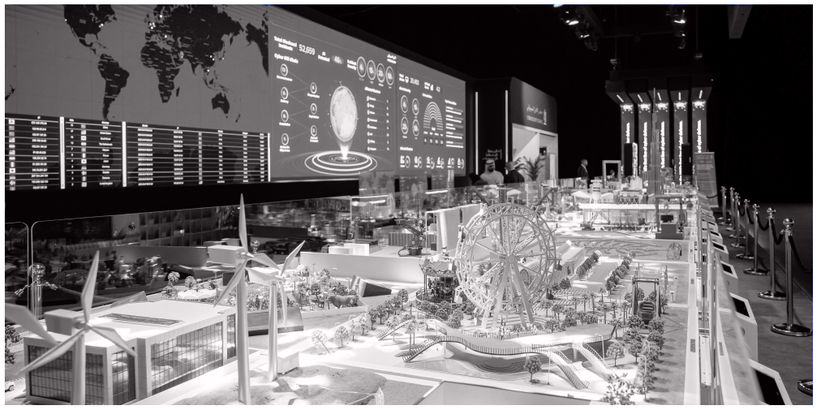
ويقوم برنامج النبض السيبراني بتنظيم وإجراء تدريبات سيبرانية عبر مختلف القطاعات مثل الغذاء، والرعاية الصحية، والخدمات المالية، والبنية التحتية الرقمية وغيرها. وتُصمَّم هذه التدريبات لتحسين جاهزية المؤسسات وقدرتها على الاستجابة للتهديدات السيبرانية، وتشمل محاكاة الاستجابة للحوادث وتمارين الاستعداد.

أما مكون "قادة المستقبل" فيركز على تطوير الجيل القادم من المتخصصين في الأمن السيبراني، وذلك من خلال اختيار طلاب الجامعات من مختلف أنحاء الدولة وتزويدهم بتدريب متخصص عبر أكاديمية مخصصة. ويستهدف البرنامج الشباب المهنيين والتنفيذيين الحكوميين والخريجين الجدد، مقدمًا لهم فرصًا للانخراط في مجال الأمن السيبراني من خلال ورش العمل، والمؤتمرات، والأنشطة التعليمية الأخرى.

كما تولي المبادرة اهتمامًا كبيرًا إلى "حملات التوعية السيبرانية" عبر حملات مصمَّمة خصيصا وموجهة لمختلف الشرائح الديموغرافية، بما في ذلك الأسر الشابة، والشباب، ورواد الأعمال، وكبار السن. وتشمل هذه الحملات موضوعات حيوية مثل أمن التسوق عبر الإنترنت، والترفيه الرقمي، والعمل والتعلم في العالم الرقمي، وحماية الأطفال عبر الإنترنت. وتنفَّذ حملات توعوية فصلية منتظمة لمعالجة تهديدات سيبرانية محددة وأفضل الممارسات في مواجهتها.

وقد حدد مجلس الأمن السيبراني أهدافًا طموحة لنيل العديد من الجوائز المرموقة مثل جائزة الإنجاز مدى الحياة وجائزة القيادة الفكرية في الأمن السيبراني للعام، وذلك لتعزيز سمعته العالمية وترسيخ مكانته داخل صناعة الأمن السيبراني.

إلى جانب ذلك، نجح المجلس في بناء شبكة واسعة وقوية من الشراكات، تشمل التحالفات المحلية والعالمية، ضمن نهج استراتيجي يهدف إلى تعظيم أثر مبادراته وترسيخ موقعه كلاعب رئيسي في مجال الأمن السيبراني.



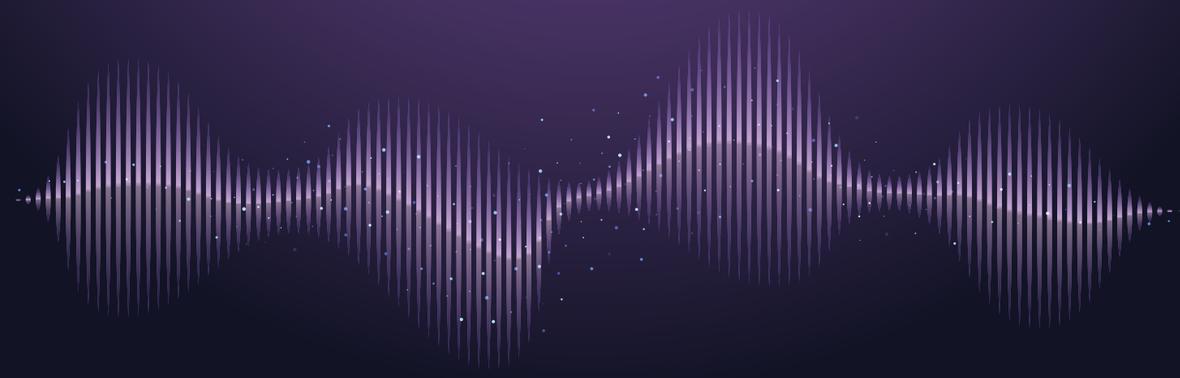
ملخص المشروع

يُعد "النبض" مختبر محاكاة سيبرانية متطور تابع لمجلس الأمن السيبراني في دولة الإمارات، وهو نموذج تنبؤي لمحاكاة الهجمات السيبرانية متعددة المراحل. ويمثل هذا النموذج المتطور محاكاة واقعية لأماكن رئيسية في دولة الإمارات، ما يتيح منصة لمحاكاة التهديدات السيبرانية وتحليلها وتقييمها في بيئة مسيطر عليها عبر القطاعات الحيوية في الدولة.

وقد حصل مشروع "النبض" على ثلاثة أرقام قياسية في موسوعة غينيس، ويُعد أحد أكبر وأحدث مختبرات المحاكاة السيبرانية في العالم من حيث الحجم، وعدد الأجهزة، وعدد السيناريوهات المتاحة. وقد ابتكر "النبض" نهجًا جديدًا في محاكاة وفهم التهديدات السيبرانية، مما يوفر تجارب فريدة لتدريب المتخصصين في الأمن السيبراني، واختبار استراتيجيات الدفاع، وتحسين قدرات الاستجابة للحوادث، وبناء مهارات دولة الإمارات في مجالات إنترنت الأشياء/نظام تحصيل البيانات والتحكم والأمن الصناعي.

أهداف المشروع: يهدف "النبض" إلى توفير تجربة مثمرة وجاذبة وملهمة قائمة على محاكاة واقعية لأماكن رئيسية في دولة الإمارات، بما يمنح مستوى غير مسبوق من الواقعية في التدريب على الأمن السيبراني ومحاكاة الأزمات، ويشكل نقلة نوعية في الاستعداد لمواجهة التهديدات السيبرانية والتصدي لها.

كما يتماشى هذا النهج المبتكر مع رؤية دولة الإمارات في أن تصبح مركزًا عالميًا للتكنولوجيا والابتكار الرقمي، من خلال توفير بيئة آمنة تُمكّن المؤسسات من ممارسة أنشطتها بثقة.



التمرين السيبراني العالمي في معرض ومؤتمر الخليج العالمي لأمن المعلومات (GISEC 2025)

يُعتبر التمرين السيبراني العالمي 2025، الذي استضافه مجلس الأمن السيبراني، أحد أضخم التمارين الدولية في مجال الأمن السيبراني حتى الآن، وهو مصمَّم لتعزيز القدرة العالمية على مواجهة التهديدات الرقمية المتطورة. وقد جمع التمرين 124 فريقا من الهيئات الوطنية للأمن السيبراني/فرق الاستجابة لطوارئ الحاسوب/فرق الاستجابة لحوادث الحاسوب/فرق الاستجابة لحوادث أمن الحاسوب من أكثر من 133 بلدًا، بمشاركة أكثر من 260 خبيرًا و15 شريكًا دوليًا، جميعهم تعاونوا وتنافسوا على منصة CYBER RANGES.

وتضمنت نسخة عام 2025 أربعة سيناريوهات متقدمة بالشراكة مع أبرز الجهات الدولية: الاتحاد الدولي للاتصالات، ومركز الأمم المتحدة لمكافحة الإرهاب، والإنتربول، ومنتدى الفرق المعنية بالأمن والاستجابة للحوادث (FIRST).

وركز التمرين على تعزيز الدفاع الجماعي عبر توحيد الفرق الدولية لتطوير استراتيجيات الاستجابة للحوادث، وتعزيز التعاون، وتبادل الخبرات في مواجهة الهجمات السيبرانية المعقدة.

وكان للتمرين عدة أهداف رئيسية، هي:

- توفير خبرة عملية مباشرة في كشف الحوادث السيبرانية والتحقيق فيها واحتوائها.
- تعميق معرفة المشاركين بالتكتيكات والتقنيات والإجراءات السيبرانية المعقدة.
- بناء القدرات في مجالات مثل صيد التهديدات، وتحليل السجلات وحركة ا لبيانات، وجمع المعلومات الاستخباراتية من الشبكة المظلمة.
- تعزيز التعاون بين الوكالات الوطنية للأمن السيبراني، وجهات إنفاذ القانون، و الشركاء متعددي الأطراف.

وشارك المتخصصون في سيناريوهات واقعية مثل: تحقيقات اختراق التهديدات المستمرة المتقدمة، وتحليل النشاط الإرهابي عبر الشبكة المظلمة، وتعطيل حملات التصيّد الإلكتروني في القطاع المالي، (العملية Black Ledger)، وتحديات فك تشفير هجمات الفدية. وقد اختبرت هذه السيناريوهات القدرات التقنية ومستوى التعاون الدولي.

وفي معرض ومؤتمر الخليج العالمي لأمن المعلومات (GISEC 2025)، دخل مجلس الأمن السيبراني موسوعة غينيس للأرقام القياسية محققًا 11 إنجازًا غير مسبوق، ما شكّل محطة فارقة في الاعتراف العالمي بدور دولة الإمارات الريادي في الأمن السيبراني. وقد عكست هذه الإنجازات حجم التمرين السيبراني العالمي والأنشطة المصاحبة وشموليتها وجانبها الابتكاري.

وعكست السجلات حجم المشاركة وتفرُّد التمارين التعاونية. وشملت الإنجازات الرئيسية ما يلي:

- أكبر عدد من الجنسيات المشاركة في مسابقة "التقاط العلم" في مجال الأمن السيبراني.
- أكبر جلسة توعية بالأمن السيبراني على مستوى العالم.
- أكبر عدد من السلطات الوطنية المشاركة في تمرين دولي واحد.
- أسرع وقت استجابة مُسجّل في سيناريو منسّق للتعامل مع حادث سيبراني.
- أوسع مشاركة للشركاء الدوليين في تمرين سيبراني، إلى جانب إنجازات أخرى.

ولم تعزز هذه الإنجازات دور دولة الإمارات كمحور عالمي للتعاون السيبراني فحسب، بل أظهرت أيضًا كيف يمكن للابتكار في التدريب والاستعداد أن يضع معايير جديدة على المستوى الدولي. كما رفع التكريم من مكانة الدولة أكثر على الصعيد العالمي، وأكد التزامها بتعزيز المرونة الجماعية في الأمن السيبراني.

منصة Crystal Ball في معرض ومؤتمر الخليج العالمي لأمن المعلومات (GISEC 2025)

تُعد Crystal Ball منصة دولية للتعاون في مجال استخبارات التهديدات السيبرانية، صُممت لتعزيز الثقة والشفافية والدفاع الجماعي، بما يتماشى مع أهداف مبادرة مكافحة برمجيات الفدية.

وخلال معرض ومؤتمر الخليج العالمي لأمن المعلومات 2025، عُقدت جلسة مغلقة لمنصة Crystal Ball، تضمنت كلمة افتتاحية لسعادة الدكتور محمد الكويتي، إلى جانب قادة بارزين من القطاع، حيث جرى التأكيد على دور المنصة في تمكين تبادل آمن وفوري للمعلومات الاستخباراتية بين الحكومات والشركاء الموثوقين، بما يضمن استجابات أسرع وأكثر تنسيقًا لمواجهة التهديدات السيبرانية المتطورة.

الأهداف والمبادئ (تركيز 2025):

- تعزيز إسناد الحوادث والهجمات من خلال تبادل المعلومات الاستخباراتية متعدد الجنسيات.
- دعم الردع من خلال تمكين استجابات مشتركة واستباقية تقلل من تأثير برامج الفدية والجرائم السيبرانية العالمية.
- ترسيخ ثقافة الثقة والشفافية، وإدماج ممارسات تبادل المعلومات في النظام البيئي الدولي للأمن السيبراني.
- تعزيز بناء القدرات عبر ضم المزيد من السلطات الوطنية وتمكين تبادل منظم بين الحكومات.

القدرات والوظائف

في عام 2025، وسّعت منصة Crystal Ball ميزاتها التعاونية، مما عزز مكانتها كركيزة أساسية في الجهود العالمية لمكافحة التهديدات السيبرانية وتبادل المعلومات الاستخباراتية حولها:

- تحليلات وتقارير مدعومة بالذكاء الاصطناعي لمساعدة محللي المعلومات الاستخباراتية بشأن التهديدات في تحديد الأنماط والانحرافات بسرعة.
- شبكة مغلقة وآمنة لتبادل معلومات الحوادث، متوافقة مع بروتوكولات عالمية موحدة.
- أدوات تعاون متكاملة لدعم التحقيقات المتعددة الأطراف عبر الحدود.
- إطلاق برنامج تبادل بين الحكومات أثناء المعرض، لتمكين التدفقات الاستخباراتية المنظمة والموثوقة.
- تحسين تجربة انضمام المستخدمين الجدد، بالاستفادة من دروس التمارين الدولية.
- دعم من الخبراء على مدار الساعة وإحاطات استخباراتية لضمان استمرارية العمليات.
- خاصية إنشاء الأحداث وتبادل المعلومات، بما يسمح للأعضاء بإطلاق تحقيقات تعاونية ثنائية أو متعددة الأطراف.

ومن خلال هذه التطويرات، تواصل المنصة ترسيخ مكانتها كمحور عالمي موثوق للتعاون في مجال التهديدات السيبرانية، مما يضع دولة الإمارات وشركاءها في طليعة تعزيز المرونة السيبرانية الدولية.

التوسّع البرنامجي في معرض ومؤتمر الخليج العالمي لأمن المعلومات (GISEC 2025)

بناءً على النجاحات التي حققتها النسخ السابقة، قدّمت نسخة عام 2025 من المعرض والمؤتمر برنامجًا موسّعًا من الفعاليات الجانبية والمنتديات المتخصصة لتعزيز تبادل المعرفة، وتطوير المهارات، ودعم التعاون متعدّد الأطراف. وأتاحت هذه المبادرات للمشاركين فرصًا مميزة للتدرّب على تقنيات متقدمة، واستكشاف أحدث الابتكارات التكنولوجية، والتواصل المباشر مع الأقران من مختلف أنحاء العالم.

الأهـــداف:

- توفير منصة متنوّعة تجمع بين التدريب العملي والحوار السياساتي.
- تعزيز النظام البيئي للأمن السيبراني عبر ربط الجهات الحكومية بالخبراء الصناعيين والأوساط الأكاديمية.
- إبراز أفضل الممارسات العالمية في الدفاع والمرونة والقيادة السيبرانية.
- رعاية الجيل القادم من المتخصصين عبر مسارات تعلم مخصصة.

أبرز عناصر البرنامج

مرحلة التدريب السيبراني العالمي

- إطلاق مسار مخصص يركز على أمن أنظمة التحكم الصناعية وتعزيز المرونة السيبرانية الوطنية.
- استضافة الجلسات 7–10 بمشاركة أكثر من 350 خبيرًا من وكالات حكومية، وقادة الصناعة، ومنظمات دولية.
- تبادل الخبرات حول حماية البنية التحتية الحرجة، واستخدام الذكاء الاصطناعي في الأمن، ورصد التهديدات الناشئة.

برنامج المسرّعات الحكومية

صُمّم برنامج المسرّعات الحكومية في معرض ومؤتمر الخليج العالمي لأمن المعلومات لجمع أصحاب المصلحة الرئيسيين في القطاع العام مع القادة الصناعيين وشركاء التكنولوجيا لتسريع تطوير واعتماد المبادرات السيبرانية المبتكرة في دولة الإمارات.

شارك فيه 76 مختصًا قُسّموا إلى 6 مجموعات ناقشت المحاور الرئيسية التالية: الحوسبة الكمية، الأمن السيبراني المتمحور حول المواطن، الدبلوماسية السيبرانية، الحدود الرقمية، التعليم التحويلي، التنمية المستدامة.

أكاديمية معرض ومؤتمر الخليج العالمي لأمن المعلومات

- قدّمت ست جلسات تدريبية متخصصة تستهدف المهنيين المبتدئين والخبراء المتمرسين.
- ركزت على تطوير المهارات في الاستدلال الجنائي الرقمي، وتحليل البرمجيات الخبيثة، وتقنيات استخبارات التهديدات.
- وسّعت قاعدة الكفاءات من خلال إشراك الطلاب والباحثين والمهنيين الناشئين.

مختبرات الاستكشاف

- سلسلة ورش عمل تعاونية مصممة للتركيز على المبادرات الوطنية وتقييم وضع الأمن السيبراني.
- تضمنت الجلسات ورش عمل المنصة الوطنية لضمان أمن المعلومات وتقييمات الجاهزية الوطنية.
- قدّمت تمارين عملية قائمة على سيناريوهات لاختبار الجاهزية الاستراتيجية والتقنية.

موائد مستديرة لرؤساء الأمن المعلوماتي

- نقاشات مغلقة وخاصة لكبار مسؤولي الأمن المعلوماتي والتنفيذيين.
- جلسات تحدثت فيها خدمات أمازون ويب عن "قيادة مؤسسات أمنية مرنة في عصر الذكاء الاصطناعي"، ومايكروسوفت عن "مستقبل الأمن في عصر الذكاء الاصطناعي".
- وفّرت حوارًا مباشرًا بين الأقران حول الحوكمة والمرونة والتحديات القيادية.

ومن خلال هذه المبادرات الموسعة، عزّز معرض ومؤتمر الخليج العالمي لأمن المعلومات 2025 مكانته كمنصة عالمية رائدة في التميّز السيبراني، جامعًا بين الاحترافية التقنية والحوار القيادي الاستراتيجي للنهوض بالمرونة الجماعية.

تقرير "الـ 50 عاماً المقبلة .. سيبرانياً"

تعاون مجلس الأمن السيبراني الإماراتي مع شركة "كي بي إم جي لوار جولف – KPMG" لاستشراف مستقبل الأمن السيبراني خلال الخمسين عامًا المقبلة. وركّز البحث على المسائل العديدة الناشئة عن تبنّي تكنولوجيا المعلومات، واستعرض الاتجاهات الحالية التي ستؤثر على حياتنا في العقود القادمة.

وقدّم التقرير رؤى مهمة بشأن خيارات السياسات المستقبلية التي يمكن لدولة الإمارات اعتمادها لتعزيز مرونتها السيبرانية على مدى الأعوام الخمسين المقبلة، بما في ذلك تطوير إطار قانوني تقدمي مدعوم بتشريعات جديدة.

البرنامج الوطني لمكافآت اكتشاف الثغرات (Bug Bounty)

أطلق مجلس الأمن السيبراني الإماراتي برنامجًا وطنيًا رائدًا لاكتشاف الثغرات، بالتعاون مع مشغلي الاتصالات الرئيسيين مثل اتصالات ودو، لتعزيز أمن البنية التحتية الرقمية الوطنية، وخاصة قطاعات الطاقة والاتصالات والدفاع.

ويعتمد البرنامج على الهاكرز الأخلاقيين والباحثين الأمنيين من جميع أنحاء العالم، للإبلاغ عن الثغرات الأمنية في النظم الرقمية في دولة الإمارات ضمن نموذج قائم على الحوافز. ويتيح هذا النهج الاستباقي للدولة تعزيز موقعها الدفاعي عبر الاستفادة من الخبرات العالمية في اختبار الاختراق وتقييم الثغرات.

الأهداف

الاستفادة من الخبراء المستقلين والباحثين الأمنيين للكشف عن الثغرات ونقاط الضعف.
تطبيق نظام قائم على الحوافز لمكافأة الاكتشاف والإفصاح المسؤول عن الثغرات.
بناء قدرة قائمة على النتائج من خلال التركيز على نوعية الثغرات المكتشفة وخطورتها.

برنامج القناص السيبراني

يهدف برنامج القناص السيبراني إلى رفع كفاءة كوادر تقنية المعلومات في الجهات الحكومية، خاصة على المستوى الاتحادي، من خلال تطوير خبرات متخصصة في مجالات مثل الاختراق الأخلاقي، والتحليل المتقدم للتهديدات، واختبارات الاختراق.

والمشاركون الرئيسيون في البرنامج هم موظفون اتحاديون ومتخصصون في الأمن السيبراني تقع على عاتقهم مسؤولية حماية البنية التحتية الوطنية الحرجة والتعامل مع التهديدات السيبرانية على المستوى الوطني.

الأهـــداف

تطوير خبرات سيبرانية متقدمة: تزويد المشاركين بمعرفة عالية المستوى للتعامل مع التهديدات السيبرانية المعقدة، بما في ذلك الهجمات على مستوى الدول.

تدريب عملي: من خلال المحاكاة، واختبارات الاختراق، وتمارين الفرق الحمراء والزرقاء التي تحاكي سيناريوهات الهجمات الواقعية.

جاهزية الدفاع الوطني: تعزيز استعداد المشاركين لحماية البنية التحتية الرقمية للدولة على المستويين الوطني والدولي.

مبادرة الحماية من هجمات الحرمان من الخدمة الموزعة

يتعاون مجلس الأمن السيبراني مع شركة اتصالات لتعزيز البنية التحتية الحيوية في دولة الإمارات من خلال تحسين وضعية الأمن للمؤسسات ورفع تصنيف الدولة في مؤشرات التنافسية العالمية.

وقد صُممت هذه المبادرات لتعزيز الوضع الأمني للمؤسسات في مواجهة التهديدات السيبرانية، مع التركيز على دعم وحماية البنية التحتية الحيوية للدولة. وتهدف هذه المبادرات إلى حماية كل من المؤسسات الحكومية والخاصة من الهجمات السيبرانية الخبيثة من خلال حلول التخفيف السحابي لهجمات الحرمان من الخدمة الموزعة. وتشمل الخدمات: الكشف عن التهديدات في الوقت الفعلي، والحماية متعددة الطبقات، والدعم الفني المتخصص عبر مركز عمليات الأمن. ومن خلال توفير الرؤية الكاملة، والتحكم، والقدرة على التوسع لمواجهة الهجمات واسعة النطاق بكفاءة، تضمن هذه المبادرات استمرارية العمليات التجارية دون انقطاع، وتمنح العملاء راحة البال.

برنامج التحقق من المواقع الإلكترونية

أداة التحقق من المواقع الإلكترونية (URL Checker)، المعروفة أيضًا باسم "StaySafe"، هي مبادرة للسلامة الرقمية أطلقها مجلس الأمن السيبراني في دولة الإمارات. وتُعد هذه الأداة خدمة مجانية عبر الإنترنت يمكن الوصول إليها من خلال الرابط staysafe.csc.gov.ae، حيث تساعد المستخدمين على التحقق من موثوقية المواقع الإلكترونية. وتقوم الأداة بتقييم ما إذا كان الموقع قد يكون متورطًا في هجمات التصيّد الاحتيالي، أو البرمجيات الخبيثة، أو غيرها من عمليات الاحتيال عبر الإنترنت، وذلك من خلال تقديم درجة موثوقية استنادا إلى رمز لوني توضّح مدى أمان الموقع. ويمكن للمستخدم ببساطة إدخال عنوان موقع الويب (URL) لمعرفة ما إذا كان آمنًا أو قد يشكل تهديدًا.

وقد طُوِّرت هذه الأداة بالتعاون مع شركة اتصالات وتحالف مكافحة الاحتيال العالمي، وذلك بهدف تعزيز حماية المستخدمين أثناء التصفح عبر الإنترنت والوقاية من الاحتيال السيبراني.

مبادرة الحل الأمني بالذكاء الاصطناعي "حماية"

يُعد الحل الأمني بمساعدة الذكاء الاصطناعي "حماية" خطوة متقدمة تهدف إلى تعزيز الأمن السيبراني الوطني عبر دمج تقنيات الذكاء الاصطناعي لمواجهة التهديدات السيبرانية الحديثة. وقد صُمِّمت "حماية" للاستفادة من التقنيات المعتمدة على الذكاء الاصطناعي لتأمين البنى التحتية الوطنية الحيوية مثل الطاقة، والاتصالات، والدفاع، والقطاع المالي.

الأهـــداف:

الدفاع بالذكاء الاصطناعي: تهدف المبادرة إلى الاستفادة من تقنيات الذكاء الاصطناعي للكشف عن التهديدات السيبرانية وتحليلها والتصدي لها بشكل أكثر كفاءة، بما في ذلك مواجهة هجمات الفدية والهجمات المدعومة بالذكاء الاصطناعي، لضمان حماية البنية التحتية الرقمية للدولة.

إجراءات استباقية للأمن السيبراني: تسعى مبادرة "حماية" إلى استخدام الذكاء الاصطناعي بشكل استباقي لمواجهة مجرمي الإنترنت قبل وقوع الهجمات. وتضع هذه المبادرة الإمارات في موقع متقدم لحماية الكيانات في القطاعين العام والخاص، من خلال جعل الذكاء الاصطناعي جزءًا أساسيًا من استراتيجيتها الدفاعية، خاصةً مع تزايد اعتماد المجرمين السيبرانيين على الذكاء الاصطناعي لاختراق الأنظمة.

التعاون والابتكار: يركّز البرنامج على التعاون بين مختلف القطاعات لتعزيز منظومة الأمن السيبراني، مع التأكيد على الابتكار المستمر والتكيف مع التهديدات المستجدة.

دعوة منظمة التعاون الإسلامي للعمل

لقد رسّخت دولة الإمارات العربية المتحدة موقعها كداعم رئيسي لتطوير الأمن السيبراني، سواء في الدول العربية أو على مستوى العالم. ويشمل ذلك رعايتها لأكبر حدث سنوي للأمن السيبراني، الذي أُقيم في العاصمة الإماراتية أبوظبي تحت شعار "الابتكار في الأمن السيبراني وتطوير الصناعة".

كما أسس مجلس الأمن السيبراني الإماراتي جبهة موحّدة بالتعاون مع الاتحاد الدولي للاتصالات، وهو وكالة الأمم المتحدة لتقنية المعلومات والاتصالات، ومنظمة التعاون الإسلامي.

وأصدرت الدول المشاركة الدعوة المشتركة للعمل "أبوظبي 2023"، مؤكدة التزامها بتعزيز الأمن السيبراني في ظل المشهد الرقمي المتغير باستمرار.

التزام: التعهد بتعزيز الثقة والأمن في استخدام تقنيات المعلومات والاتصالات.

تعزيز المرونة السيبرانية: دعوة القطاعات الصناعية إلى اعتماد أطر عمل قادرة على صد التهديدات وضمان استمرارية العمليات حتى أثناء الهجمات السيبرانية.

المشاركة: تبادل الخبرات وأفضل الممارسات المتعلقة بالتهديدات والأمن السيبراني بشكل فعّال.

التنسيق والمواءمة: السعي النشط نحو التنسيق والاندماج مع منظمات أخرى ذات صلة للاستفادة من خبراتها وتجنب تكرار الجهود.

البحث والتطوير: تشجيع الحكومات والأوساط الأكاديمية والقطاع الخاص على زيادة الاستثمار في مجالات البحث والتطوير في الأمن السيبراني.

تعزيز الاستراتيجيات السيبرانية: التعاون مع أصحاب المصلحة المعنيين لوضع وتحديث استراتيجيات سيبرانية شاملة ترتكز على سياسات تعزز الاستعداد والمرونة.

الشمول السيبراني: الدعوة إلى إدراج التعليم المتعلق بالأمن السيبراني في المراحل الأساسية، واستمراره في التعليم العالي والتطوير المهني المستمر.

اعتماد الذكاء الاصطناعي الأخلاقي: تعزيز اعتماد الذكاء الاصطناعي الأخلاقي من خلال تشجيع المؤسسات والشركات على إعطاء الأولوية للاعتبارات الأخلاقية في تطويره وتطبيقاته.

CyberE71

برنامج CyberE71 هو مبادرة عالمية تهدف إلى تسريع ودعم الشركات الناشئة في مجال الأمن السيبراني، أطلقه مجلس الأمن السيبراني الإماراتي لتعزيز منظومة الابتكار العالمية من خلال توحيد الشركات الناشئة تحت مظلة واحدة.

ويسعى البرنامج إلى تعزيز تبادل المعرفة، وتكثيف التعاون، وتقديم الدعم بما يساهم في تطوير القدرات السيبرانية على المستويين الإقليمي والعالمي. ويستند البرنامج إلى تحليل مقارن شامل لبرامج دعم وإنشاء الشركات الناشئة حول العالم، بما يضمن دمج أفضل الممارسات وتطبيق الاستراتيجيات الفعّالة.

وبالشراكة مع جهات مثل Area2071 وHub71 وواحة دبي للسيليكون، يوفّر برنامج CyberE71 بيئة متكاملة لدعم الشركات الناشئة في مجال الأمن السيبراني.
ويقدّم البرنامج إطاراً منظماً للتسريع يتضمن جلسات تدريب مكثفة، وفعاليات، واجتماعات استراتيجية، مع توفير أكثر من 900 ساعة من الإرشاد والتوجيه وإتاحة الوصول إلى 36 خبيراً رائداً في القطاع.

ويُركّز البرنامج على السهولة وقابلية التوسع من خلال عملية تسجيل مبسّطة وبوابة إلكترونية سهلة الاستخدام.

ويوفّر برنامج CyberE71 للشركات الناشئة الأدوات والمعرفة وروابط التواصل اللازمة للنجاح، مما يرسّخ مكانته كأحد البرامج الرائدة عالمياً في الابتكار السيبراني.
وينسجم البرنامج مع الأهداف الاستراتيجية لدولة الإمارات، حيث يعزز مناعة الأمن السيبراني عالمياً ويسهم في تنويع الاقتصاد. ومن خلال رعاية المواهب وتحفيز الابتكار، يدعم برنامج CyberE71 تحقيق رؤية الإمارات 2071 عبر مواجهة التحديات السيبرانية والمضي قدماً نحو اقتصاد قائم على المعرفة.

المركز الوطني للعمليات السيبرانية

أنشأت دولة الإمارات العربية المتحدة المركز الوطني للعمليات السيبرانية تحقيقًا لرؤية القيادة الرشيدة في حماية الوطن من الهجمات السيبرانية وتعزيز الأمن السيبراني الوطني. وتدرك الدولة تزايد عدد الحوادث السيبرانية وتعقيدها، وكذلك تأثيراتها السلبية على الوطن واقتصاده.

ويهدف المركز إلى توفير حل شامل وعملي لحماية الدولة من الهجمات السيبرانية، وقد بُني باستخدام حلول قابلة للتوسع تضم منهجيات أساسية، وتقنيات مُجرَّبة ميدانيًا، وقابلية التشغيل البشري، وبناء القدرات لمواجهة التهديدات السيبرانية.

وتعتمد عمليات المركز على منهجيات واضحة ومثبتة لمراقبة الوضع الوطني، واكتشاف الخصوم السيبرانيين، وتحليل ونشر المعلومات الاستخباراتية، وتقييم قدرة الدولة على مواجهة الهجمات السيبرانية. ومع إنشاء المركز، ستحقق دولة الإمارات رؤية وطنية موحدة وقدرة على التنسيق لمكافحة الهجمات السيبرانية، مستفيدة من تقنيات الذكاء الاصطناعي والأتمتة لمعالجة التحديات في مختلف المجالات السيبرانية عالميًا.

أهداف المركز الوطني للعمليات السيبرانية

رؤية شاملة للحالة السيبرانية: توفير لمحة عامة عن مشهد التهديدات عبر التعاون القطاعي والوطني.

معلومات آنية عن التهديدات: تقديم صورة أكبر عن النظام السيبراني الوطني شبه اللحظية.

تعزيز القدرات الحالية: تقديم معلومات قيّمة وذات صلة إلى جانب تحسين قدرات مراكز الأمن السيبراني المشاركة.

تمكين القوانين الوطنية للأمن: من خلال إيجاد أرضية مشتركة وطنية، ومعايير وتصنيفات موحدة بين مراكز العمليات المشاركة.

التوعية والتدريب الوطني: مشاركة التدريب والمعرفة بين المراكز المشاركة لتعزيز المرونة السيبرانية على مستوى الكيانات والوطن ككل.

يوم الدفاع السيبراني (تدريب الأمة)

يُعد يوم الدفاع السيبراني مبادرة تعليمية مبتكرة أطلقها مجلس الأمن السيبراني بهدف رفع وعي الطلبة بالأمن السيبراني وتدريبهم على بناء أنظمة آمنة لمواجهة الهجمات. وقد جاءت المبادرة بالشراكة مع عدة جهات استراتيجية في الدولة، من بينها: مجلس التعليم والموارد البشرية، ووزارة التربية والتعليم، ومؤسسة الإمارات للتعليم المدرسي، ودائرة التعليم والمعرفة، وهيئة التعليم الخاص بالشارقة. كما شاركت المدارس الخاصة في دبي بشكل فعّال، ما يعكس التزامًا جماعيًا بتزويد الطلبة بالمعرفة والمهارات الرقمية الأساسية.

الأهـداف:

- رفع وعي الطلبة بالأمن السيبراني ومخاطره.
- التركيز على أهمية الخصوصية الرقمية والسلوك الأخلاقي.
- تعزيز جودة الحياة الرقمية للطلبة.
- التصدي للمخاطر والتهديدات السيبرانية الناشئة.

المرأة في الأمن السيبراني

أطلقت دولة الإمارات مبادرة المرأة في الأمن السيبراني، المعروفة أيضًا باسم مبادرة نبض الأمن السيبراني للمرأة والأسرة، بالتعاون مع الاتحاد النسائي العام ومجلس الأمن السيبراني. وتهدف هذه المبادرة إلى تمكين المرأة في مجال الأمن السيبراني وتعزيز مهاراتها الرقمية.

ويركّز البرنامج على زيادة تمثيل المرأة في هذا القطاع الحيوي من خلال التدريب المتخصص، وتوفير الموارد القيّمة، وإتاحة فرص متنوعة لدعم مسيرتها المهنية وتطوير قدراتها في مجال الأمن السيبراني.

البرنامج الوطني لوعي الشباب بالأمن السيبراني

يُعد البرنامج الوطني لوعي الشباب بالأمن السيبراني جزءًا من جهود الدولة في تعليم وتمكين الشباب ليصبحوا خط الدفاع الأول ضد التهديدات السيبرانية. ويقوده مجلس الأمن السيبراني الإماراتي، مستهدفًا تحويل الجيل الجديد إلى حماة للأمن الرقمي.

المكونات الرئيسية للبرنامج:

ورش العمل والدورات التدريبية: تُركِّز على التخفيف من التهديدات السيبرانية مثل التصيّد الإلكتروني، والبرمجيات الخبيثة، والاختراقات. وتتناول هذه الجلسات سيناريوهات واقعية لجعل المشاركين الشباب أكثر قدرة على تحديد الحوادث السيبرانية والتعامل معها بفعالية.

الحملات والتمارين التفاعلية: يتضمن البرنامج عناصر تفاعلية مثل التمارين والمسابقات الخاصة بالأمن السيبراني لجذب الشباب وتحفيزهم. وتهدف هذه الأنشطة إلى بناء مهارات الأمن السيبراني في بيئة تعليمية ممتعة وتنافسية، من خلال محاكاة مواقف واقعية لهجمات سيبرانية.

حملات التوعية: تعزز المبادرة الوعي السيبراني من خلال حملات تعليمية حول السلوك الآمن على الإنترنت، وأخلاقيات الاستخدام الرقمي، وأهمية حماية البيانات الشخصية. وغالبًا ما تشمل هذه الحملات أنشطة عبر وسائل التواصل الاجتماعي ومحاضرات موجهة خصيصًا لفئة الشباب.

التعاون والشراكات: يُنفَّذ البرنامج بالتعاون مع المؤسسات التعليمية وشركاء من القطاع الخاص، لضمان اطلاع الطلاب على أحدث التطورات في مجال الأمن السيبراني. كما تسهم الشراكات مع مؤسسات مثل Core42 وKPMG في إثراء البرنامج بخبرات ورؤى من واقع الصناعة.

حملات التوعية بالأمن السيبراني
52 أسبوعًا من التوعية

أطلق مجلس الأمن السيبراني حملة "52 أسبوعًا من التوعية بالأمن السيبراني" في دولة الإمارات لنشر ثقافة الأمن السيبراني بين المواطنين والمقيمين. وتهدف المبادرة إلى تثقيف وتمكين الأفراد والمؤسسات لحماية أنفسهم من التهديدات الرقمية.
وقد حققت الحملة أثرًا واسعًا محليًا ودوليًا من خلال نشر معلومات وموارد مبسطة، ما ساعد الأفراد والمؤسسات على تبني ممارسات استباقية ضد الهجمات، إلى جانب تعزيز التعاون المجتمعي والدولي.

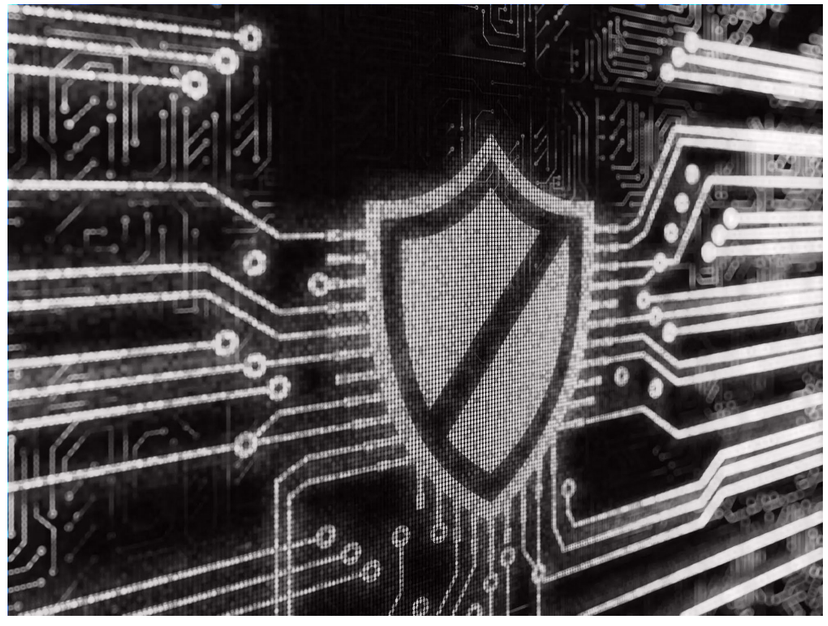
لقد حققت حملة "52 أسبوعًا من التوعية بالأمن السيبراني" أثرًا كبيرًا في تعزيز الوعي بالأمن السيبراني داخل دولة الإمارات وعلى الصعيد الدولي. فمن خلال نشر المعلومات والموارد بأسلوب يسهل الوصول إليه، بما في ذلك توفيرها للمؤسسات العامة والخاصة حول العالم، أسهمت الحملة في تمكين الأفراد والجهات من اعتماد تدابير استباقية لمواجهة التهديدات السيبرانية. كما ساعدت الحملة في تعزيز روح التعاون والانتماء المجتمعي بين الجهات المعنية بقطاع الأمن السيبراني العالمي.

الأهـــداف

- رفع الوعي العام بمخاطر الأمن السيبراني وأفضل الممارسات
- تعزيز التعليم من خلال توفير موارد تدريبية وبحثية لتعزيز مهارات الأمن السيبراني
- تشجيع التعاون بين الحكومة والقطاع الخاص والأوساط الأكاديمية للتصدي لتحديات الأمن السيبراني
- حماية البنية التحتية الحيوية من الهجمات السيبرانية

أبرز ملامح الحملة

- **مواضيع أسبوعية:** تغطي مجالات مثل التصيّد، والبرمجيات الخبيثة، والهندسة الاجتماعية، وحماية البيانات.
- **محتوى تعليمي:** يشمل المقالات، ومقاطع الفيديو، والرسوم التوضيحية.
- **موارد رقمية:** مثل الدورات الإلكترونية، والندوات الشبكية، وورش العمل.
- **مشاركة مجتمعية:** من خلال فعاليات عامة لتعزيز الحوار حول الأمن السيبراني.
- **شراكات:** مع المدارس والجامعات والشركات لتعزيز التوعية والتعليم.



منصة جاهز

تم إطلاق منصة "جاهز" من قبل الهيئة الاتحادية للموارد البشرية الحكومية في أواخر عام 2022، كأكبر منصة رقمية للتطوير والارتقاء بالمهارات المستقبلية لموظفي الحكومة في دولة الإمارات. تهدف المنصة إلى إعداد الكوادر الحكومية لمواجهة تحديات المستقبل عبر تجربة تعلم تفاعلية وشخصية.

وفي فترة وجيزة، وصلت المنصة إلى أكثر من 53,000 متعلم، من خلال 90 برنامجًا تدريبيًا تغطي 4 مجموعات أساسية من المهارات المستقبلية، و27 مهارة فرعية، و 163 وحدة تدريبية، بإجمالي يتجاوز 1.2 مليون ساعة تعلم.

وتستند المنصة إلى أكثر من 25 شريكًا استراتيجيًا، من بينهم مجلس الأمن السيبراني الإماراتي، حيث تم دمج محتوى متخصص في الأمن السيبراني لتعزيز المرونة الرقمية، وتجهيز الموظفين الحكوميين بالمهارات اللازمة لحماية الأنظمة ضد التهديدات الإلكترونية المتطورة.

شراكـات مجلـس الأمـن السـيبراني مع القطـاعين العـام والخـــاص

اتصالات

أبـرم مجلـس الأمـن السـيبراني شراكـة استراتيجيـة مـع شركـة اتصـالات، إحـدى أكبر مجموعـات الاتصـالات في الأسـواق الناشـئة عالميًـا، لتعزيـز مشـهد الأمـن السـيبراني في الدولـة. وتشـمل هـذه الشراكـة التعـاون مـع Help AG، الـذراع المعنيـة بالأمـن السـيبراني لشركـة اتصـالات الرقميـة، وذلـك في إطـار الجهـود المسـتمرة لتعزيـز البنيـة التحتيـة الحيويـة للدولـة، وتحسـين موقعهـا الريـادي في مؤشـرات التنافسـية العالميـة.

كمـا أطلـق المجلـس بالتعـاون مـع أكاديميـة اتصـالات برنامـج تدريـب "القنـاص السـيبراني" بمسـتوياته (1، 2، 3)، والمخصـص لتدريـب الكـوادر الحكوميـة والوطنيـة على مهـارات متقدمـة في الأمـن السـيبراني.

البرامـج الريادية والمبادرات العالمية لدولة الإمـــارات

الشراكات مع القطاع الأكاديمي

بوليتكنك أبوظبي

تم إنشاء مركز الابتكار "CyberPulse" في بوليتكنك أبوظبي بهدف سد الفجوة في المهارات السيبرانية وتدريب الجيل الجديد من المتخصصين. ويُعد المركز منصة للتعاون بين الأوساط الأكاديمية والصناعة، حيث يتيح للطلاب خبرة عملية مباشرة في مواجهة التهديدات والتقنيات السيبرانية الحديثة.

كما يعمل مركز الابتكار مع بوليتكنك أبوظبي على مواءمة البرامج الأكاديمية مع أحدث الاتجاهات العالمية في مجال الأمن السيبراني. وتشمل الأنشطة مشاريع بحثية مشتركة ومبادرات لتطوير حلول عملية للتحديات السيبرانية الحالية والمستقبلية، مما يساهم في تكوين كوادر وطنية عالية الكفاءة قادرة على تلبية الاحتياجات الوطنية والصناعية.

يُعد مركز التميّز في بوليتكنك أبوظبي، الذي تم تطويره بالتعاون مع مجلس الأمن السيبراني لدولة الإمارات العربية المتحدة، مبادرةً مهمة تهدف إلى تعزيز التعليم في مجال الأمن السيبراني وتنمية الكفاءات الوطنية في هذا القطاع الحيوي. ويأتي إنشاء هذا المركز ضمن الجهود الوطنية الأوسع الرامية إلى ترسيخ مكانة دولة الإمارات كقوة عالمية رائدة في مجال الأمن الرقمي ومواجهة التهديدات السيبرانية المتزايدة في المنطقة.

ويعمل مركز التميّز في بوليتكنك أبوظبي كمحور رئيسي لتدريب جيل المستقبل من المتخصصين في الأمن السيبراني، حيث يُوفّر بيئة تعليمية متكاملة تجمع بين المعرفة الأكاديمية والتطبيق العملي. ويساهم التعاون مع الشركاء من القطاع الخاص مثل شركة هواوي في تمكين الطلبة من اكتساب خبرات عملية مباشرة في التعامل مع التهديدات السيبرانية في الوقت الفعلي، مما يعزز جاهزيتهم للانتقال بسلاسة إلى سوق العمل وتلبية الطلب المتزايد على الكفاءات المؤهلة في هذا المجال الحيوي.

جامعة خليفة

يتمتّع مجلس الأمن السيبراني لدولة الإمارات العربية المتحدة وجامعة خليفة بعلاقة تعاون وثيقة تركز على تعزيز البحث والتعليم في مجال الأمن السيبراني.

ويتولى مجلس الأمن السيبراني مسؤولية صياغة السياسات والاستراتيجيات واللوائح الوطنية الخاصة بالأمن السيبراني، ويشمل دوره تطوير الأطر التي تضمن حماية البنية التحتية الرقمية للدولة والتصدي للتهديدات السيبرانية المستجدة.

أما جامعة خليفة، وهي من المؤسسات الأكاديمية الرائدة في دولة الإمارات، فتُعرف بتركيزها القوي على البحث العلمي والابتكار في مختلف المجالات، بما في ذلك الأمن السيبراني. وتتعاون الجامعة مع الجهات الحكومية والشركاء في القطاع الخاص لتعزيز المعرفة وتطوير الحلول في هذا المجال الحيوي. ويساهم بحثها العلمي بشكل فعّال في المبادرات الوطنية ويساعد على صياغة استراتيجيات فعّالة للأمن السيبراني.

وقد أسست جامعة خليفة شراكة استراتيجية مهمة مع مجلس الأمن السيبراني لدولة الإمارات من خلال إنشاء المركز الوطني للتميّز في الأمن السيبراني، الذي يُعد منصة وطنية رائدة في تطوير القدرات البحثية والتعليمية والتطبيقية في هذا القطاع.

ومن أبرز محاور هذه المبادرة:

- **أكاديمية الأمن السيبراني**
- **البحث والابتكار**
- **طوير الكفاءات والمهارات**
- **البنية التحتية للأمن السيبراني**

لوكهيد مارت

في معرض آيدكس 2025، وقّع مجلس التوازن ومجلس الأمن السيبراني وشركة لوكهيد مارتن مذكرة نوايا لإنشاء مركز التميز للأمن السيبراني. وتمثل هذه المبادرة محطة استراتيجية مهمة لدولة الإمارات، حيث تعزز طموحها في أن تصبح قوة عالمية رائدة في الأمن السيبراني. ويهدف مركز التميز إلى تعزيز المرونة الوطنية ودفع النمو الرقمي المستدام من خلال دمج التكنولوجيا المتقدمة، وتنمية رأس المال البشري، وتعزيز التعاون الدولي.

الأهداف الرئيسية:

تعزيز المرونة السيبرانية الوطنية عبر الأبحاث المتقدمة، والتدريب، وخدمات مراكز عمليات الأمن.

إنشاء "أودية سيبرانية" في مختلف إمارات الدولة لدعم الابتكار والشركات الناشئة.

تعزيز التعاون بين الحكومة والصناعة والقطاع الأكاديمي.

الأثـــر

سيساهم المركز في تعزيز الأمن الرقمي، وبناء الكفاءات الوطنية، ودعم التنويع الاقتصادي، وترسيخ مكانة دولة الإمارات كمركز عالمي للابتكار في مجال الأمن السيبراني.

جوجل كلاود

أطلقت دولة الإمارات، بالشراكة مع Google Cloud وMandiant، أول مركز تميز للأمن السيبراني في المنطقة بأبوظبي خلال آيدكس 2025. ويهدف المركز إلى تعزيز المرونة الوطنية عبر التدريب المتقدم، ومختبرات المحاكاة السيبرانية، وتبادل المعرفة مع الأوساط الأكاديمية والحكومة والصناعة.

ويركز المركز بشكل أساسي على تطوير القوى العاملة وخلق فرص عمل جديدة. وبحلول عام 2030، من المتوقع أن يوفّر أكثر من 20,000 وظيفة جديدة في مجالات متعددة، تشمل:

الدفاع السيبراني والاستجابة للحوادث

السياسات السيبرانية والحوكمة

أدوار التحول الرقمي الآمن

التعليم والتوعية

كما يدعم برنامج مسرّع الشركات الناشئة 25 شركة مبتكرة عبر الإرشاد وتقديم ما يصل إلى 300,000 دولار من أرصدة Google Cloud، مما يعزز ريادة الأعمال ويوفر فرصًا متخصصة في مجالات الابتكار، وتطوير المنتجات، والبحث والتطوير السيبراني.

واقتصاديًا، يُتوقع أن يسهم هذا المشروع في منع خسائر تصل إلى 6,8 مليارات دولار ناجمة عن الجرائم السيبرانية بحلول 2030، وجذب ما يقارب 1,4 مليار دولار من الاستثمارات الأجنبية، مما يعزز مكانة دولة الإمارات كدولة رائدة عالميًا في مجال الابتكار الأمني السيبراني وتطوير الكفاءات.

تعاون مجلس الأمن السيبراني مع الهيئات الدولية

يعزز مجلس الأمن السيبراني التعاون الدولي من خلال العمل مع شركاء حكوميين محليين رئيسيين مثل مكتب تبادل الخبرات الحكومية ومسرعات الحكومة الإماراتية لتصميم مبادرات مشتركة مع الحكومات الشريكة. ومن خلال برامج التسريع وتبادل الخبرات مع دول عدة، تمكنت دولة الإمارات من تعزيز تبادل أفضل الممارسات، وإطلاق مشاريع تجريبية مشتركة، وتنظيم تمارين لبناء القدرات، بما يساهم في تطوير معايير تشغيل متوافقة، والاستجابة السريعة للحوادث، وتعزيز المرونة السيبرانية الجماعية.

الإتحاد الدولي للاتصالات

بالتعاون مع الاتحاد الدولي للاتصالات، تم إطلاق مبادرة CyberPulse التي تركز على حماية الفضاء السيبراني الإماراتي عبر رفع مستوى الوعي العام وتعزيز الشعور بالمسؤولية الوطنية تجاه الدفاع السيبراني. وتشمل المبادرة ورش عمل، دورات تدريبية، وأنشطة متنوعة تهدف إلى تحسين الثقافة الرقمية والمرونة عبر مختلف قطاعات المجتمع، بما في ذلك الحكومة والأعمال والجمهور العام.

وقد حازت المبادرة على اعتراف دولي واسع، حيث فازت بجوائز مرموقة في فعاليات مثل جوائز القمة العالمية لمجتمع المعلومات (WSIS Prizes)، ما يعكس ريادة دولة الإمارات في توظيف التكنولوجيا المتقدمة لتحقيق التنمية المستدامة والتزامها بتوفير بيئة رقمية آمنة.

كما تؤدي مبادرة CyberPulse دورًا مهمًا في الجهود العالمية للأمن السيبراني من خلال مشاركتها في التمارين السيبرانية العالمية التي ينظمها الاتحاد الدولي للاتصالات، والتي تساعد على تعزيز قدرات الأمن السيبراني للدول الأخرى عبر تبادل المعرفة وتنظيم التمارين المشتركة. ويساهم هذا التعاون في مواءمة جهود الإمارات مع الأجندة العالمية للأمن السيبراني، ويعزز مكانتها كلاعب محوري في هذا المجال.

ويشارك مجلس الأمن السيبراني في التمارين السيبرانية العالمية التي تنظمها الاتحاد الدولي للاتصالات وغيرها من الهيئات الدولية، كما يقدّم الدعم لهذه المبادرات. وتسهم هذه المشاركة في مواءمة ممارسات الأمن السيبراني في دولة الإمارات مع المعايير العالمية، وتعزيز جاهزيتها للتصدي للتهديدات والهجمات السيبرانية.

البيت الأبيض

شاركت دولة الإمارات مؤخرًا في اجتماع المبادرة الدولية لمكافحة هجمات الفدية (CRI) الذي عُقد في سان فرانسيسكو بتنظيم من البيت الأبيض، وجمع 60 شريكًا عالميًا لمناقشة استراتيجيات مواجهة هذا التهديد المتنامي. وركّز الاجتماع على تعزيز الثقة، وتبادل المعلومات، وتطوير آليات الدفاع الجماعي بين الدول. وكان من أبرز محاور النقاش "منصة الكرة البلورية" (Crystal Ball Platform)، وهي نظام مدعوم بالذكاء الاصطناعي يهدف إلى تحسين التعاون العالمي في مجال تبادل التهديدات السيبرانية. وتؤكد مشاركة دولة الإمارات في هذا الحدث التزامها بجهود الأمن السيبراني على المستوى العالمي.

منظمة التعاون الإسلامي

نشط مجلس الأمن السيبراني في التعاون مع منظمة التعاون الإسلامي لتعزيز إجراءات الأمن السيبراني في الدول الأعضاء. ومؤخرًا، انتُخبت دولة الإمارات كنائب رئيس لفريق الاستجابة لطوارئ الحاسوب التابع للمنظمة خلال الأسبوع الإقليمي العاشر للأمن السيبراني للدول العربية والدول الأعضاء في المنظمة. ويعكس هذا المنصب القيادي مكانة دولة الإمارات المتقدمة على الساحة العالمية في مجال الأمن السيبراني، والتزامها بحماية البنى التحتية الرقمية في العالم الإسلامي.

كما شاركت دولة الإمارات في مائدة مستديرة رفيعة المستوى نظمها فريق الاستجابة لطوارئ الحاسوب التابع للمنظمة خلال المؤتمر العالمي للجوال 2024، وتركّزت النقاشات حول ترسيخ الثقة الرقمية والمرونة لدى أعضاء المنظمة، مع تسليط الضوء على قضايا محورية مثل أمن شبكات الجيل الخامس (5G)، وأمن الحوسبة السحابية، وإمكانية تشكيل مجموعة عمل جديدة مخصّصة لأمن الذكاء الاصطناعي وسلاسل التوريد.

وتعكس هذه الجهود النهج الاستباقي لدولة الإمارات في التعاون مع الشركاء الدوليين لمواجهة التهديدات السيبرانية المتطورة، وتعزيز الأمن الرقمي بين الدول الأعضاء في منظمة التعاون الإسلامي. كما تبرز التزامها بقيادة الجهود الإقليمية في هذا المجال، وترسيخ التعاون لضمان جاهزية الدول الأعضاء لمواجهة التحديات الرقمية المستقبلية.

آفاق الأمن السيبراني

اتجاهات الأمن السيبراني المستقبلية

ما الذي قد تحمله الخمسون سنة القادمة لمجال الأمن السيبراني؟ إن الاتجاهات الكبرى التي تُعيد تشكيل العالم تشمل:

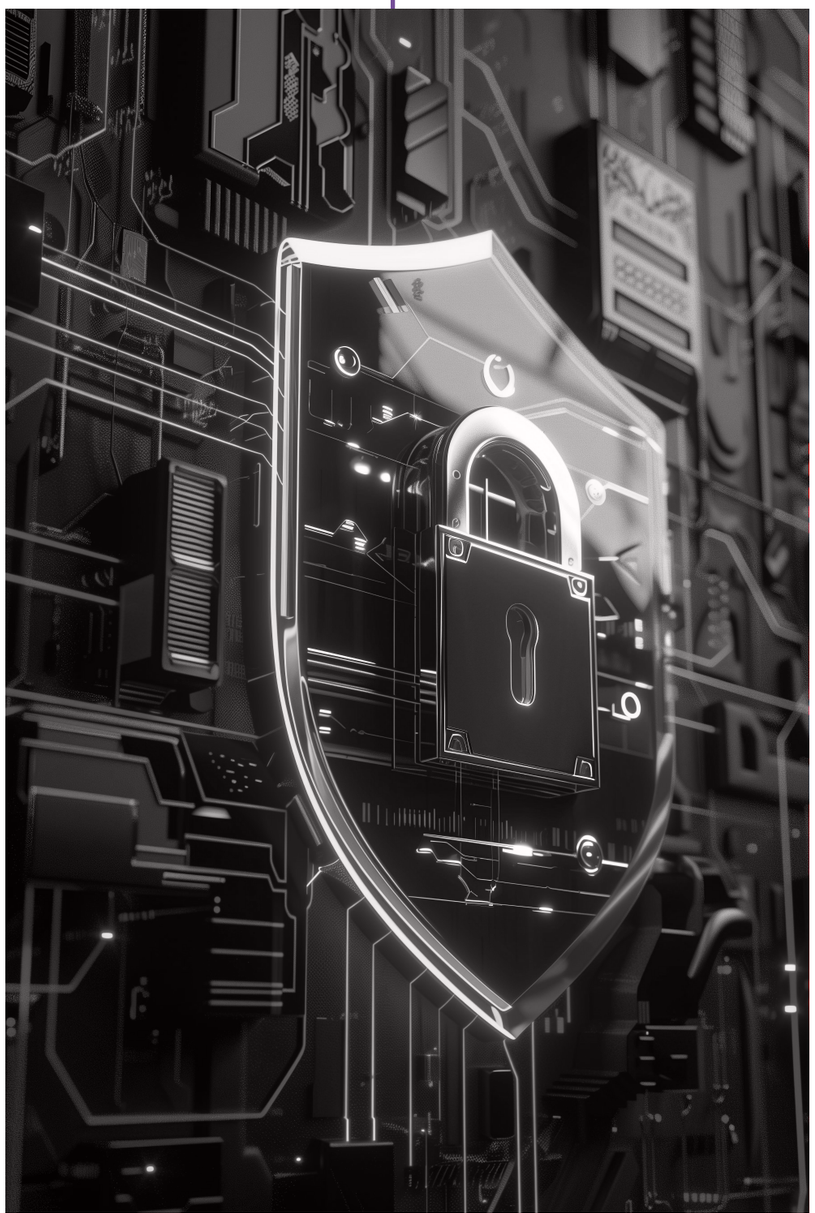
الديموغرافيا

من المتوقع أن يصل عدد سكان العالم إلى 9,7 مليارات نسمة بحلول عام 2050. وهذه التغيرات السكانية ستخلق تحديات متباينة، بدءًا من الشيخوخة السكانية وتراجع معدلات الخصوبة وزيادة أعباء الديون والضرائب في بعض الاقتصادات، وصولًا إلى التحديات المرتبطة بالبنى التحتية والتعليم في المناطق التي تشهد نموًا حضريًا متسارعًا مثل أفريقيا جنوب الصحراء وجنوب آسيا.

وفي دولة الإمارات، يُتوقع أن ينمو عدد السكان ليصل إلى 10,9 ملايين نسمة خلال العقدين المقبلين، مع تضاعف عدد سكان دبي نتيجة موجة الهجرة بعد الجائحة. وسيُسهم التنويع الاقتصادي واستقطاب الكفاءات الأجنبية بشكل رئيسي في هذا النمو السكاني.

التغير المناخي

تشير التقديرات إلى أن السياسات الحالية ستؤدي إلى ارتفاع في درجات الحرارة العالمية بمعدل 2,8 درجة مئوية بحلول عام 2100، مع تضاؤل الفرصة أمام العمل الدولي للحد من هذا الارتفاع إلى 1,5–2 درجة. وهذا التغير المناخي سينتج عنه تحديات خطيرة مثل انعدام الأمن الغذائي، ونزوح سكاني، وتدهور النظم البيئية، إلى جانب كونه شرارة محتملة لاندلاع النزاعات. وتتخذ دولة الإمارات خطوات متعددة للتعامل مع المخاطر الناجمة عن ارتفاع درجات الحرارة والجفاف، مركزة على إيجاد توازن بين مكاسب الوقود الأحفوري قصيرة المدى والمتطلبات الوجودية الناتجة عن تغيّر المناخ.



الآفاق المستقبلية للأمن السيبراني

التحديات الصحية

- تزايد مقاومة الميكروبات للمضادات الحيوية يرتبط بارتفاع خطر العدوى المتبادلة بين البشر والحيوانات، نتيجة انتقال مسببات الأمراض الحيوانية إلى الإنسان، وهو ما يتفاقم مع ازدياد الكثافة السكانية والتنقل البشري، مما يؤدي إلى ارتفاع مخاطر الأوبئة العالمية. كما أن ارتفاع متوسط الأعمار يفرض ضغوطًا متزايدة على أنظمة الرعاية الصحية، بسبب تزايد انتشار الأمراض المزمنة مثل السكري، وأمراض القلب والأوعية الدموية، والسرطان، وأمراض الجهاز التنفسي المزمنة.

- يهدف مشروع مئوية الإمارات 2071 إلى جعل دولة الإمارات أفضل دولة في العالم بحلول عام 2071، مع توفير رعاية صحية على أعلى المستويات العالمية. وتركّز أجندة الرعاية الصحية لمئوية 2071 على تعزيز السياحة العلاجية، وتطوير الطب عن بُعد، واستخدام الذكاء الاصطناعي والتقنيات السحابية في قطاع الصحة، إلى جانب وضع الأطر التنظيمية لاستخدام الصحة الإلكترونية.

الاتجاهات التكنولوجية

- **الذكاء الاصطناعي:** تسارع تطور الذكاء الاصطناعي العام وتوسع تطبيقاته المتخصصة في العقد المقبل.

- **فرط الاتصال:** تطوير البنية التحتية للشبكات بما يدعم النطاق العريض والتواصل المكثف بين الأجهزة، مما يُعزز تطور إنترنت الأشياء وانتشار المستشعرات والأجهزة الفاعلة في كل مكان.

- **الهندسة الحيوية:** ابتكارات في الأجهزة الطبية والزرعات (مثل الروابط العصبية والأطراف الصناعية المتقدمة)، والتلاعب بالجينوم لأغراض علاجية أو ضارة، وإنتاج علاجات دوائية مصممة خصيصًا.

- **الحوسبة الكمية:** تطور الحوسبة الكمية، التي تُحدث ثورة في نموذج الحوسبة الرقمية الحالي من خلال توفير زيادات هائلة في القدرة الحاسوبية، ويرتبط هذا التطور أيضًا بتقدم تقنيات الاتصال الكمي الآمن.

- **التكنولوجيا الفضائية:** استمرار سباق الفضاء مع انخفاض تكاليف الإطلاق وزيادة الوصول، وإطلاق بعثات ذاتية التشغيل متطورة، إلى جانب المخاطر المرتبطة بالحطام الفضائي والعمليات المضادة في الفضاء.

- **الروبوتات:** مجموعة واسعة من التطورات التي تجعل الروبوتات أكثر تطورًا وانتشارًا في جميع مجالات الحياة، بدءًا من التطبيقات الصناعية والعسكرية عالية الخطورة، مرورًا بالطائرات المسيّرة المتقدمة العاملة بشكل جماعي، ووصولًا إلى الروبوتات ذات الطابع البشري المستخدمة في الرعاية الشخصية والأجهزة الجراحية الروبوتية المصغّرة.

- **التصنيع الذكي:** تقدم الطباعة ثلاثية الأبعاد وإمكانية إنتاج أنظمة تصنيع شخصية ومصممة بدقة، مدعومة بنماذج التوصيل الفوري.

- **الاندماج النووي:** التوسع في استخدام تقنيات الاندماج النووي، بما في ذلك تطوير المفاعلات الدقيقة، مما يؤدي – إلى جانب النمو في مصادر الطاقة المتجددة – إلى تغييرات جذرية في الاعتماد على مصادر الطاقة القائمة على النفط والغاز.

- **الواقع المعزز:** تطوير أنظمة واقع معزز عالية الدقة وغير تدخّلية، إضافة إلى بيئات واقع افتراضي غامرة للغاية، وذلك بالتوازي مع التطورات المحتملة في تقنيات الزرعات العصبية والتحفيز العصبي.

تأمين رؤية دولة الإمارات

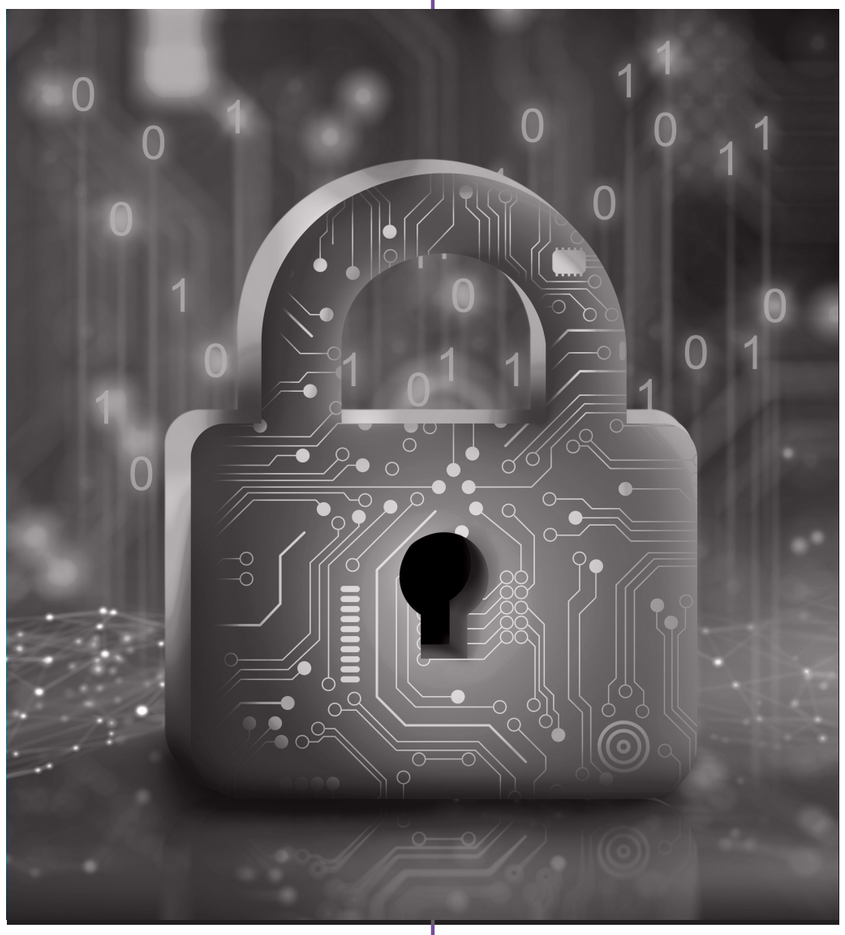
وضعت دولة الإمارات المبادئ التي ستبني عليها مسيرتها حتى عامها المئوي في 2071. وترسم هذه المبادئ خريطة الطريق الاستراتيجية لعصر جديد من النمو الاقتصادي والسياسي والاجتماعي، بدءًا من تعزيز الاتحاد ومؤسساته، وصولًا إلى جعل التنمية الرقمية والتقنية والعلمية في صميم التنمية الاقتصادية.

تهدف مبادرة رؤية الإمارات 2031 إلى تطوير قطاعات الصحة والتعليم والاستدامة والبنية التحتية، بما يعزز مكانة دولة الإمارات كمركز اقتصادي مهم وشريك عالمي. وتسعى المبادرة إلى رفع مستوى الرفاه المجتمعي، ودفع عجلة النمو الاقتصادي، وتعزيز الحضور الدولي، وتحسين أداء الحكومة من خلال الاستفادة من التقنيات المتقدمة.

ستشكّل هذه المبادئ خطوطًا إرشادية لجميع مؤسسات الدولة مع اقترابها من مرحلة جديدة من التنمية خلال العقود الخمسة المقبلة. وهي جزء من حملة مشاريع الخمسين، وتتمثل فيما يلي:

- **تعزيز الاتحاد:** سيبقى التركيز الوطني الأساسي على تعزيز الاتحاد، ومؤسساته، وتشريعاته، وقدراته، وموارده المالية.
- **أفضل اقتصاد:** سنسعى خلال الفترة المقبلة لبناء أفضل وأشد الاقتصادات ديناميكية في العالم.
- **رأس المال البشري:** المحرك الأساسي للنمو المستقبلي هو رأس المال البشري، وذلك من خلال تطوير المنظومة التعليمية، واستقطاب المواهب، والاحتفاظ بالمتخصصين، وبناء المهارات باستمرار.
- **العلاقات الجوارية:** حسن الجوار هو أساس الاستقرار. فالموقع الجغرافي والاجتماعي والثقافي للدولة في المنطقة يُمثل خط الدفاع الأول عن أمنها وسلامتها وتنميتها المستقبلية.
- **مركز للتميّز:** ترسيخ سمعة دولة الإمارات عالميًا مهمة وطنية لجميع المؤسسات. فدولة الإمارات وجهة موحّدة للأعمال والسياحة والصناعة والاستثمار.
- **احتضان الابتكار:** سيحدد التميّز الرقمي والتقني والعلمي لدولة الإمارات حدودها الاقتصادية والتنموية.

- **مجموعة محددة من القيم:** سيبقى النظام القيمي الأساسي في دولة الإمارات قائمًا على الانفتاح والتسامح، وحماية الحقوق، وسيادة العدالة والقانون.
- **المساعدات الإنسانية:** تُعد المساعدات الإنسانية الخارجية التي تقدمها دولة الإمارات جزءًا جوهريًا من رؤيتها وواجبها الأخلاقي تجاه الشعوب الأقل حظًا.
- **السلام والاستقرار:** الدعوة إلى السلام والانسجام والحوار والتفاوض لحل جميع النزاعات تمثل أساس السياسة الخارجية الإماراتية.



الختام والدعـوة إلـى العمـــل

استجابةً لهذه التحديات، يؤكد التقرير على ضرورة بذل جهد جماعي من قبل الحكومات والصناعات والمؤسسات الأكاديمية لتعزيز البنية التحتية للأمن السيبراني. ويشمل ذلك:

دعوة إلى العمل

تعزيز تدابير الأمن السيبراني

تطبيق أنظمة كشف واستجابة مدعومة بالذكاء الاصطناعي، مع التركيز على بنية انعدام الثقة. ومن الضروري أيضا الاستثمار في تنمية القوى العاملة لسد فجوة المواهب وتعزيز الجاهزية الدفاعية.

تشجيع التعاون بين القطاعين العام والخاص

تعزيز الابتكار عبر دعم الشراكات بين القطاعين العام والخاص، وخاصة في التقنيات الناشئة مثل البلوك تشين والذكاء الاصطناعي.

التركيز على التوعية والتعليم في مجال الأمن السيبراني

إطلاق حملات توعية وطنية وبرامج تدريب إلزامية لتمكين الأفراد من امتلاك المعرفة اللازمة للتصدي للتهديدات الحديثة.

الاستثمار في التقنيات الآمنة

زيادة الاستثمار في التقنيات المتقدمة مثل التشفير لما بعد الحوسبة الكمية (Post-Quantum Cryptography) لحماية البيانات الحساسة والبنى التحتية.

تعزيز أطر الاستجابة للحوادث السيبرانية

العمل على تطوير أطر الاستجابة للحوادث بشكل مستمر وتعزيز الإجراءات الاستباقية مثل برامج مكافآت اكتشاف الثغرات لتحديد نقاط الضعف قبل استغلالها.

الخـــاتمـــة

في عالمنا الرقمي المتزايد اليوم، تمثل تطورات التهديدات السيبرانية تحديات وفرصًا في الوقت ذاته على المستوى العالمي. ويؤكد هذا التقرير على الحاجة الملحة لمعالجة هذه المخاطر من خلال جهود منسقة، وتوظيف تقنيات متقدمة، وأطر سياسية استراتيجية.

وعلى الصعيد العالمي، أصبحت الهجمات السيبرانية أكثر تطورًا بفضل التقنيات الناشئة مثل الذكاء الاصطناعي، والحوسبة الكمية، وإنترنت الأشياء. ومع اعتماد الشركات والحكومات والأفراد بشكل متزايد على البنى التحتية الرقمية، فإن وتيرة هذه الهجمات وتأثيرها يتصاعدان بشكل ملحوظ.

وقد أظهرت دولة الإمارات قيادة قوية في مجال الأمن السيبراني، حيث رسخت مكانتها كمركز إقليمي وعالمي للابتكار في هذا المجال الحيوي. فقد أنشأت مجلس الأمن السيبراني لدولة الإمارات، وتواصل قيادة المبادرات الهادفة لحماية أصولها الرقمية وتأمين بنيتها التحتية الحيوية. وتوضح دراسات الحالة الواردة في هذا التقرير مجموعة من التهديدات السيبرانية مثل هجمات الفدية ونقاط الضعف في سلاسل التوريد، ما يبرز أهمية اليقظة المستمرة والابتكار.

وفي السنوات المقبلة، سيعتمد الأمن السيبراني على نهج متعدد الأبعاد يجمع بين التقدم التكنولوجي، وتطبيق السياسات بصرامة، وتعزيز التعاون بين القطاعين العام والخاص. وتُعد دولة الإمارات مثالًا قويًا من خلال تعزيزها للمرونة الرقمية، وتطبيق بروتوكولات أمنية متقدمة، وتعزيز الشراكات الدولية. ومع ذلك، فإن مواكبة التطورات التكنولوجية السريعة، لا سيما مع إدخال الحوسبة الكمية والذكاء الاصطناعي، يمثل تحديًا كبيرًا لمشهد الأمن السيبراني العالمي.

وتشير النتائج الأساسية في هذا التقرير إلى أن تبني استراتيجيات استباقية ومرنة سيكون أمرًا أساسيًا للتخفيف من التهديدات المستقبلية. ويشمل ذلك الاستثمار في الكفاءات البشرية المتخصصة في الأمن السيبراني، وتعزيز الابتكار عبر البحث والتطوير، وترسيخ ثقافة الوعي السيبراني في جميع قطاعات المجتمع. ومع استمرار دولة الإمارات في تعزيز قدراتها الدفاعية السيبرانية، فهي في موقع متميز لقيادة الجهود العالمية نحو تشكيل مستقبل رقمي آمن، يمهد الطريق لنمو اقتصادي مستدام ورفاه مجتمعي في عالم مترابط.