نسخة عام
2024

اليوبيل الفضي
٢٠٢٤-١٩٩٩

التقرير السنوي

المركز الوطني
للأمن السيبراني
National Cyber
Security Center

نسخة

2024

التقرير السنوي

حضرة صاحب الجلالة الهاشمية

الملك عبدالله الثاني ابن الحسين

المعظـم

صاحب السمو الملكي

الأميـر الحسيـن بـن عبدالله الثانـي

ولـي العهـد المعظـم

المحتويات

كلمـــة القـائم بأعمـال رئـيس المـركز الوطـني للأمـن السـيبراني

نتيجة للتوسع المستمر في التحول الرقمي والاعتماد المتنامي على الأنظمة الذكية في تقديم الخدمات العامة والخاصة، وفي ظل التطورات المتسارعة التي يشهدها العالم الرقمي، وتزايد التهديدات السيبرانية على المستويين الإقليمي والدولي، واصل المركز الوطني للأمن السيبراني خلال عام 2024 جهوده المتكاملة لتعزيز جاهزية المملكة في مواجهة المخاطر السيبرانية، من خلال تطوير البنية التحتية الرقمية، وتوسيع نطاق خدمات الحماية والاستجابة، وبناء القدرات الوطنية في مختلف القطاعات. وقد شملت إنجازات المركز هذا العام مجموعة من المحاور الحيوية، من أبرزها: العمليات السيبرانية، الاستخبارات السيبرانية، السياسات والامتثال، التدريب والتطوير، والاتصال والتعاون، في دلالة واضحة على حجم العمل المنجز والتقدم المحقق في تعزيز أمن الفضاء السيبراني الأردني.

وقد واكبت هذه الجهود قفزة نوعية حققتها المملكة الأردنية الهاشمية في مؤشر الأمن السيبراني العالمي لعام 2024، حيث تم تصنيف الأردن ضمن فئات متقدمة نسبيًا. واستمراراً للجهود الوطنية في تعزيز وحماية الفضاء السيبراني الأردني سيعمل المركز خلال الفترة المقبلة على إعداد استراتيجية وطنية للأمن السيبراني للأعوام 2025 – 2028 وبرنامج تنفيذي خاص بها لإقرارها من المجلس الوطني للأمن السيبراني لتعكس هذه الاستراتيجية أولويات المملكة في بناء منظومة مرنة للاستجابة للتحديات المستقبلية ولتكون إطاراً عملياً في بناء بيئة رقمية أكثر أماناً واستدامة.

وفي الختام، فإننا في المركز الوطني للأمن السيبراني نؤمن بأن الأمن الرقمي مسؤولية وطنية مشتركة، تتطلب يقظة مستمرة وتعاوناً فعّالاً، وسنواصل التزامنا بتعزيز جاهزية المملكة في هذا المجال الحيوي، وفق رؤية طموحة وركائز راسخة تترجم الرؤى الملكية السامية، وتتماشى مع تطلعات ومتابعة سمو ولي العهد في هذا المجال.

القائم بأعمال رئيس المركز الوطني للأمن السيبراني

د. أحـمـد عـبـد الـفـتـاح الـحـيـاصـات

1

نشأة المركز

تم إقرار قانون الأمن السيبراني رقم 16 لسنة 2019، بتاريخ 16 أيلول 2019 بهدف تنظيم جميع ما يتعلق بالأمن السيبراني الوطني، ولإدارة القدرات السيبرانية الوطنية وتوحيدها وتوجيهها بالاتجاه الذي يضمن استثمار الجهود واستغلالها بالشكل الأمثل، كما حدد هذا القانون الأدوار والواجبات والمسؤوليات على المستوى الوطني، وضَمِنَ القانون تأسيس مركز وطني للأمن السيبراني تُناط به مهام الأمن السيبراني على المستوى الوطني وبالتنسيق مع كافة الجهات المعنية بالأمن السيبراني بشكل متناغم يمنع تقاطع الواجبات وتداخل المسؤوليات.

بموجب هذا القانون تم تشكيل المجلس الوطني للأمن السيبراني والذي يتألف من رئيس يُعيّن بإرادة ملكية سامية وتسعة أعضاء يمثلون الجهات الوطنية التالية: وزارة الإقتصاد الرقمي والريادة، البنك المركزي الأردني، القوات المسلحة الأردنية-الجيش العربي، دائرة المخابرات العامة، مديرية الأمن العام، المركز الوطني للأمن وإدارة الأزمات، بالإضافة إلى ثلاثة أعضاء يسميهم مجلس الوزراء بناء على تنسيب رئيس المجلس لمدة سنتين قابلة للتجديد لمرة واحدة على أن يكون إثنان منهم من ذوي الخبرة من القطاع الخاص.

المادة (5) من قانون الأمن السيبراني الأردني رقم 16 لعام 2019، انشاء المركز الوطني للأمن السيبراني وتكليفه ببناء القدرات الوطنية للأمن السيبراني.

كما ويتمتع المركز الوطني للأمن السيبراني بشخصية اعتبارية ذات استقلال مالي وإداري ويرتبط برئيس الوزراء. وأنيط بالمركز الوطني للأمن السيبراني مهام بناء منظومة فعالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية المملكة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة واقتدار وبما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات.

المهـام والصلاحيـات

1) إعداد إستراتيجيات وسياسات ومعايير الأمن السيبراني ومراقبة تطبيقها ووضع الخطط والبرامج اللازمة لتنفيذها.

2) تطوير عمليات الأمن السيبراني وتنفيذها وتقديم الدعم والاستشارة اللازمين لبناء فرق عمليات الأمن السيبراني في القطاعين العام والخاص وتنسيق جهود الاستجابة لها والتدخل عند الحاجة.

3) تحديد معايير الأمن السيبراني وضوابطه وتصنيف حوادث الأمن السيبراني بموجب تعليمات يصدرها لهذه الغاية.

4) منح الترخيص لمقدمي خدمات الأمن السيبراني وفقاً للمتطلبات والشروط والرسوم المحددة بموجب نظام يصدر لهذه الغاية.

5) تبادل المعلومات وتفعيل التعاون والشراكات وإبرام الإتفاقيات ومذكرات التفاهم مع الجهات الوطنية والإقليمية والدولية ذات العلاقة بالأمن السيبراني.

6) تطوير البرامج اللازمة لبناء القدرات والخبرات الوطنية في مجال الأمن السيبراني وتعزيز الوعي به على المستوى الوطني.

7) التعاون والتنسيق مع الجهات ذات العلاقة لتعزيز أمن الفضاء السيبراني.

8) إعداد مشروعات التشريعات ذات العلاقة بالأمن السيبراني بالتعاون مع الجهات المعنية.

9) التقييم المستمر لوضع الأمن السيبراني في المملكة بالتعاون مع الجهات المعنية في القطاعين العام والخاص.

10) تحديد شبكات البنى التحتية الحرجة ومتطلبات استدامتها.

11) إنشاء قاعدة بيانات بالتهديدات السيبرانية.

12) تقييم النواحي الأمنية لخدمات الحكومة الإلكترونية.

13) تقييم وتطوير فرق الاستجابة لحوادث الأمن السيبراني.

14) إعداد سياسة تتضمن معايير أمن وحماية المعلومات.

15) دعم البحث العلمي في مجالات الأمن السيبراني بالتعاون مع الجامعات.

16) إجراء تمارين ومسابقات للأمن السيبراني.

17) إعداد مشروع الموازنة السنوية عن الوضع الأمني السيبراني للمكلة ورفعها للمجلس.

18) إعداد التقارير ربع السنوية عن الوضع الأمني السيبراني للمملكة ورفعها للمجلس.

19) أي مهام أو صلاحيات أخرى تنص عليها الأنظمة والتعليمات الصادرة استنادا الى احكام قانون الأمن السيبراني.

الأدوار الرئيسيــة للمركـز علـى المستـوى الوطنـي

الدور التنظيمـي/الرقابـي

يعمل المركز ايفاءً منه لهذا الدور المناط به، على بناء فضاء سيبراني أردني يتصف بالمرونة، يضمن الأمن والحماية السيبرانية لكافة الجهود الوطنية الرامية لإدارة عمليات التحول الرقمي ورقمنة الخدمات الحكومية، والأصول الرقمية المُشغلة والداعمة لهذه الخدمات، من خلال حوكمة الأمن السيبراني على المستوى الوطني، وبناء أُطر تنظيمية مُلزمة التنفيذ، موجبة المساءلة، لكافة القطاعات الوطنية الحكومية والخاصة.

الدور العـمليـاتـــي

يعمل المركز ايفاءً منه لهذا الدور المناط به، على التوسع في تقديم خدماته السيبرانية بكفاءة واقتدار للفئات الوطنية المستهدفة، وبما يضمن الجاهزية الفورية العملياتية والفنية والاستخبارتية، لإكتشاف ومنع واحتواء الحادثة السيبرانية وسرعة الاستجابة لها والحد من الضرر الناجم عنها، كما ويعمل المركز من خلال هذا الدور على تعزيز وتقوية مفهوم الأمن السيبراني وعملياته التشغيلية لدى كافة القطاعات الوطنية.

دور بناء القدرات الوطنية

يعمل المركز ايفاءً منه لهذا الدور المناط به، على بناء وتنمية القدرات الوطنية للمؤسسات والأفراد، ايماناً منه بأن العنصر البشري هو الدرع الواقي الأول والأهم بوجه أية هجمات أو تهديدات سيبرانية يتعرض لها فضاءنا السيبراني، حيث سعى المركز ومنذ نشأته على تمكين الأفراد والمؤسسات وتسليحهم بالمعرفة التوعوية والتثقيفية والعلمية، التي تكفل حماية كافة مستخدمي الفضاء الرقمي من أية مخاطر سيبرانية قد يتعرضون لها أو يتسببون بها.

التوجه الاستراتيجي

2026-2024

أولويات المركز الوطني للأمن السيبراني

البنـــاء

نسعى لبناء منظومة أمن سيبراني أردنية متطورة إداريا، عملياتياً ، فنياً وتنظيمياً في إدارة الأمن السيبراني، من خلال التطوير والتحسين المستمر لموارد المركز الإدارية والفنية والعملياتية وبنيته التحتية، وبما يساهم في توفير موارد مُمكنة، مُتطورة، قادرة على الإيفاء بمتطلباتها التي وجدت لأجلها، واستدامت نتائجها الباهرة، وبما يُمكن المركز من تحقيق رسالته بكفاءة، والقيام بالدور المناط به على المستوى الوطني.

الاســتجابة

نسعى لخلق منظومة وطنية متطورة ومستدامة لإدارة العمليات السيبرانية على المستوى الوطني، وبما يضمن التحري الدقيق والكشف المبكر والاستجابة الفعالة للحوادث والتهديدات السيبرانية التي تتعرض لها المملكة بكفاءة واقتدار، بالإضافة لتوفير الضوابط والإجراءات المناسبة لاحتواء الحادثة السيبرانية وسرعة الاستجابة لها والحد من الضرر الناجم عنها.

الصّمــود

نسعى لتفعيل دورنا الوطني في إدارة القدرات السيبرانية الوطنية وتوحيدها وتوجيهها بالاتجاه الذي يضمن توفير متطلبات الصّمود للمؤسسات الوطنية وقطاعات البنية التحتية الحرجة، وبما يكفي للصّمود بوجه هذه الهجمات والتهديدات السيبرانية، والحد من ضررها ، وتمكين المؤسسات والقطاعات التي تتعرض لها من التعافي لجميع المؤسسات والقطاعات الاستمرارية في تقديم الخدمات.

توفير الأُطر الوطنية القانونية مُلزمة التنفيذ والمسائلة لكل من يتسبب بالحاق الضرر بالأصول الرقمية للمملكة الأردنية الهاشمية.

التعــاون

نسعى لبناء علاقات تشاركية على المستوى المحلي والإقليمي والعالمي، تساهم في تنمية وتعزيز قدراتنا في تنفيذ المهام والواجبات المناطة بالمركز، وتعظيم الاستفادة من تجارب الدول الاخرى والخبرات المتراكمة لديهم في إدارة الأمن السيبراني.

التوجــه الاستراتيجــي (2024-2026)

الرؤيــة

مركزًا متميزًا إقليمياً في إدارة الأمن السيبراني استناداً للمعايير العالمية.

الرسالـة

نعمل ليكن المركز الوطني للأمن السيبراني مركزاً متميزاً إقليمياً في تقديم خدماته، فعالاً في تحقيق الأهداف الوطنية، استناداً للمعايير الدولية في إدارة الحوادث والتهديدات السيبرانية في بيئة عمل مشجعة على الإبداع، قائمة على التطوير والتحسين المستمر عملياتياً، فنياً وإدارياً.

القـيـم الجوهرية

- احـترافـيـة الأداء
- تـداول المعرفـة
- التعلـم المستمـر
- استشراف المستقبل
- المرونـة المؤسسيـة

الأهـداف الاستراتيجيــة للمركــز

الهدف الاستراتيجي الأول:

تعزيز القدرات المؤسسية للمنظومة الداخلية للمركز وبما يساهم برفــع كفـــاءة المركــز في تقديــم خدماتـــه وإدارة عملياتــه.

- تنمية وتدريب وتطوير الموارد البشرية ورفع كفاءتها.
- تعزيز الأداء المؤسسي وتقييمه.

الهدف الاستراتيجي الثانـي:

استدامــة إدارة العمليات السيبرانيــة بكفـاءة وفاعليــة

- ضمان الجاهزية الفورية لإدارة حوادث الأمن السيبراني والاستجابة لها، والتعامل مع الاضرار الناتجة عنها.
- الإدارة الإستباقية في التعامل مع التهديدات والثغرات السيبرانية.
- الإدارة الفعالة للمعلومات السيبرانية الاستخباراتية.

الهدف الاستراتيجي الثالـث:

قطاعات بنى تحتية وطنية مرنة سيبرانياً وقادرة على الصّمود في وجه الهجمات السيبرانية مع نهايــة عــام 2026.

- حوكمة الأمن السيبراني على المستوى الوطني.
- بناء القدرات السيبرانية لقطاعات البنى التحتية الحرجة.
- تعزيز الأمن السيبراني على المستوى الوطني.

الهدف الاستراتيجي الرابـع:

بناء علاقات تشاركية محلية، إقليمية، ودولية تساهم في تنمية وتعزيز منظومة عمل المركــز

- بناء وتعزيز العلاقات التعاونية الإقليمية والدولية في مجال الأمن السيبراني.
- بناء وتعزيز العلاقات التعاونية المحلية في مجال الأمن السيبراني.
- دعم المبادرات الوطنية والإقليمية المتعلقة بالأمن السيبراني.

الخدمات الرئيسية والإنـــجـــازات

العمليات السيبرانية

التوسع في تقديم الخدمات السيبرانية للمؤسسات الوطنية وشبكة الحوسبة السحابية

تم التوسع في تقديم خدمة المراقبة والتحليل على مدار الساعة للشبكات الحكومية وإدارة سجلاتها والحركات الرقمية، حيث تم إضافة ما مجموعه (5) مؤسسات جديدة لتصبح عدد المؤسسات المربوطة على نظام إدارة سجلات الاحداث(90) مؤسسة وتم اضافة ما يقارب (1109) خادم افتراضي تابع للمؤسسات الوطنية والمستضاف في شبكة الحوسبة السحابية الحكومية، حيثُ يمكّن هذا النظام المركزي من توفير رؤية شاملة للحركات على سجلات الشبكات، وتحديث هذه الحركات بهدف رصد أية تهديدات أو حوادث سيبرانية تتعرض لها، من خلال جمع البيانات وتحليلها وإصدار التنبيهات للمعنيين عن أية احداث مشبوهة تم رصدها بالإضافة لتوفير تقارير فنية مفصلة عن الأنشطة المرتبطة بالأحداث التي تم رصدها.

5	90	1109
مؤسسات جديدة	عـدد الــمؤسســات المربوطة على النظام	خـادم افتراضي تابع للمؤسسات الوطنية

نفذ المركز خلال الربـــع الأخير مــن عام 2024 **مشروع حماية واستجابة للأجهزة الطرفية (**Extended detection and response**) للمؤسسات الحكومية.**

حيث تم ربط ما مجموعه (70) مؤسسة حكومية على النظام حتى الآن، حيث يشمل المشروع (10000) خادم وجهاز داخل المؤسسات الحكومية ومركز البيانات الحكومي الموحد بهدف توفير للأصول الرقمية العاملة طبقة إضافية من الأمان من أية تهديدات أو اختراقات سيبرانية، وتمكينهم من رصد التهديدات السيبرانية التي قد يتعرضون لها وضمان استجابة فعالة للحوادث السيبرانية التي قد تستهدف الأجهزة والخوادم لديهم، وتاليا ما يوفره النظام المؤسسات:

- تحليل السلوك (Behavior Analysis) وتحليل وتحديد الأسباب الرئيسة (Root Cause Analysis). يقوم النظام على تحليل سلوك مستخدمي الأجهزة والأنظمة والتطبيقات للكشف عن أية حركات غير اعتيادية تشير لوجود هجمات سيبرانية.
- الكشف عن التهديدات المتطورة (Threat Advanced detection)، حيث يستخدم النظام تقنيات متطورة للكشف عن التهديدات السيبرانية المتطورة التي تستهدف الأجهزة والخوادم.
- الاستجابة الآلية (Automated Response)، يمكن للنظام أن يتخذ أية إجراءات آلية للتعامل مع التهديدات المكتشفة بالاعتماد على إجراءات محددة مسبقا (Play Books)، حيث يعمل النظام على عزل الأجهزة والخوادم المصابة، أو تقديم تقارير تفصيلية لاتخاذ الإجراءات المناسبة بناءً على الحركات المشبوهة التي تم رصدها.
- التحليل الذكي (Intelligent Analysis)، يستخدم النظام تقنيات التعلم الذاتي والذكاء الاصطناعي لتحليل البيانات وتحديد السلوكيات غير المعتادة بشكل أكثر دقة وفعالية.

خدمة المراقبة والتحليل

يقدم المركز الوطني للأمن السيبراني هذه الخدمة على مدار 7/24 بشكل أساسي للوزارات والمؤسسات الحكومية من خلال مراقبة الشبكات والأنظمة، حيث يتم جمع سجلات الأحداث وربطها بنظام مركزي) نظام إدارة سجلات الاحداث ((لتحليل التنبيهات الصادرة من الأنظمة والأجهزة للاكتشاف المبكر لحوادث الأمن السيبراني وفي حالة اكتشاف حادث أمني يقوم المركز بتبليغ الجهة المعنية وتقديم التوصيات اللازمة لمعالجة الحادث الأمني.

- تعامل المركز مع (6758) حادثة سيبرانية تعرض لها الفضاء السيبراني الأردني عام 2024 بزيادة وصلت إلى (175%) مقارنة بعام 2023، حيث يعزى سبب الزيادة الى التوسع في مراقبة الشبكات والأجهزة الحكومية بلغت نسبة الحوادث المكتشفة من قبل فريق المراقبة في المركز ما نسبته (97%) من هذه الحوادث والجدول ادناه يوضح عدد مقارنة بين عدد الحوادث لعام 2023 وعام 2024

	2024	2023
Quarter	no. of Incident	no. of Incident
1	2054	563
2	1582	524
3	1665	453
4	1457	915
	6758	2455

6758
حادثة سيبرانية عام ٢٠٢٤

%97
نسبة الحوادث المكتشفة من قبل فريق المركز

- أصدر المركز (6922) تحذير سيبراني بناءً على الحوادث السيبرانية التي تم رصدها أو اكتشافها مقارنة ب (2609) تحذير سيبراني عام 2023.

6922
تحذير سيبراني

- تعامل الفريق الوطني للاستجابة لحوادث الأمن السيبراني (JOCERT) مع (3%) من الحوادث السيبرانية التي تم رصدها واصدار (75) تقرير مرتبط بتلك الحوادث

75
تقرير مرتبط بالاستجابة لحوادث الأمن السيبراني

تصنيف الحوادث السيبرانية حسب درجة الخطورة على النحو التالي:

- لم يتم رصد أي حادث سيبراني مصنف **(شديدة الخطورة)** مقارنة بما نسبته **(1%)** لعام 2023.

%2

نسبة الحوادث السيبرانية الخطيرة

(2%) من الحوادث السيبرانية التي تعرض لها الفضاء السيبراني الأردني صنفت بحوادث **(خطيرة)**.

%88

نسبة الحوادث السيبرانية متوسطة الخطورة

(88%) من الحوادث السيبرانية التي تعرض لها الفضاء السيبراني صنفت بحوادث **(متوسطة الخطورة)**.

%10

نسبة الحوادث السيبرانية منخفضة الخطورة

(10%) من الحوادث السيبرانية التي تعرض لها الفضاء السيبراني صنفت بحوادث **(منخفضة الخطورة)**.

- تعامل المركز مع **(35%)** من الحوادث السيبرانية التي كانت تهدف لتنفيذ عمليات التجسس وقرصنة البيانات والمعلومات الرقمية

تصنيف الحوادث السيبرانية حسب نوع الحادث على النحو التالي:


(38%) من الحوادث ارتبطت بالفيروسات والبرمجيات الخبيثة


(16.84%) من الحوادث ارتبطت بمحاولة اختراق للمواقع الإلكترونية التابعة للمؤسسات الحكومية


(10.49%) من الحوادث كان سببها عدم التقيد بالسياسات والتوصيات المتعلقة بأمن المعلومات

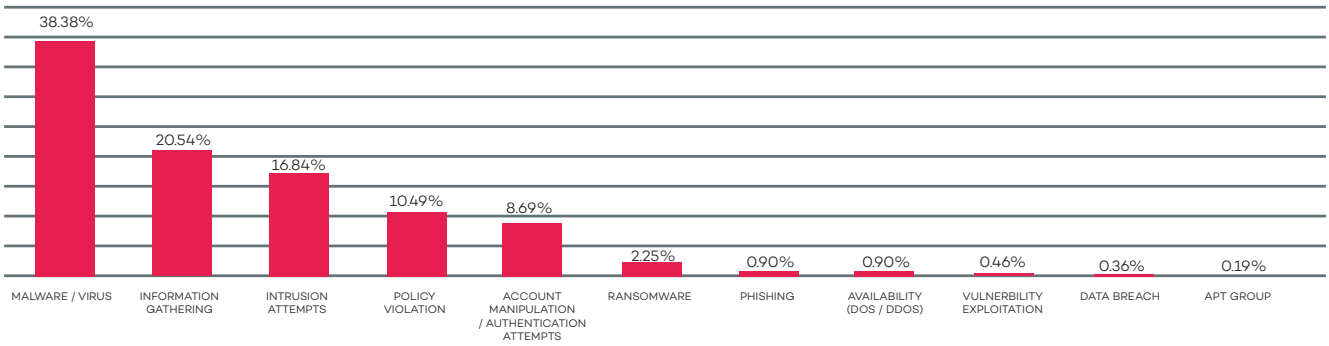

(0.19%) من الحوادث ارتبطت بمجموعات التهديد المتطورة


(2%) من الحوادث ارتبطت ببرامج الفدية


(1%) من الحوادث ارتبطت بحملات التصيد

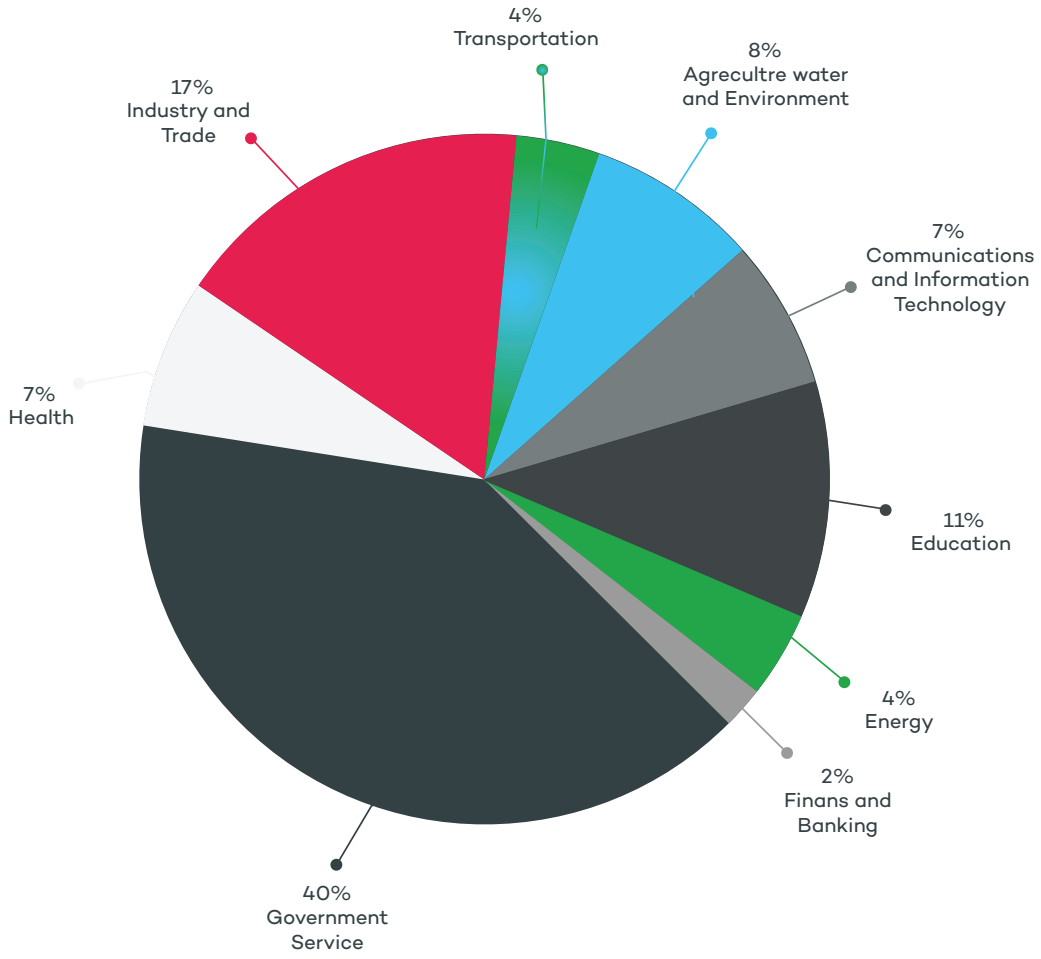

(31.48%) حوادث أخرى

الرسم أدناه يوضح توزيع الحوادث السيبرانية التي تعرضت لها الوزارات والمؤسسات الحكومية خلال عام 2024



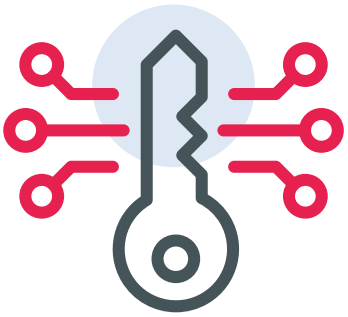
%97 من المؤسسات تعرضت لأكثر من حادثة سيبرانية خلال العام

تعامل الفريق الوطني للاستجابة لحوادث الأمن السيبراني مع حوادث امن سيبراني استهدفت قطاعات البنى التحتية على النحو التالي:



خدمة تحليل الأدلة الرقمية Digital Forensics

يقدم المركز الوطني للأمن السيبراني هذه الخدمة من خلال فريق متخصص يقوم بجمع الأدلة الرقمية السيبرانية من الأنظمة التي تعرضت لعمليات الاختراق وحفظها وتخزينها واجراء عمليات التحليل لاكتشاف الثغرات الأمنية التي أدت الى الحادث السيبراني. يتم تقييم دوافع وهوية المخترق وفهم الأساليب والاستراتيجيات التي تم استخدمها واسترجاع الملفات المحذوفة والمخفية وتحليل البرمجيات الخبيثة. يقوم المركز بإصدار تقرير عن نتائج تحليل الأدلة الرقمية يتضمن التفاصيل الفنية للحادث السيبراني ونتائج التحليل بالإضافة لتقديم التوصيات الفنية اللازمة للحد من حدوث الاختراقات.



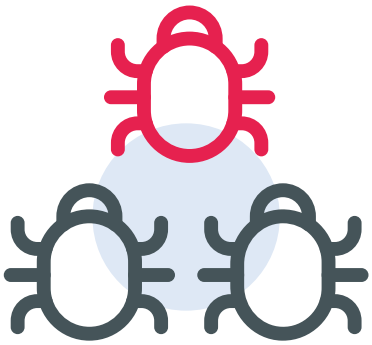
قام المركز بجمع (115) دليل رقمي خلال عمليات الاستجابة، حيث كانت الأدلة الرقمية مرتبطة ب (107) حادثة سيبرانية

115
دليل رقمي

107
حادثة سيبرانية

خدمة تحليل البرمجيات الخبيثة Malware Analysis

يقدم المركز الوطني للأمن السيبراني هذه الخدمة للوزارات والمؤسسات الحكومية والقطاع الخاص من خلال فريق فني متخصص وتهدف هذه الخدمة لتحليل البرمجيات الخبيثة بأنواعها المختلفة وتصنيفها ودراسة سلوكها على أنظمة التشغيل وتحليل مكوناتها.



135
برمجية خبيثة تم تحليلها

خدمة التقييم الفني الأمني Security Assessment

يقدم المركز الوطني للأمن السيبراني هذه الخدمة للوزارات والمؤسسات الحكومية والقطاع الخاص من خلال فريق فني متخصص وتهدف لتحسين وتطوير وحماية المنظومة الأمنية من خلال تقييم الوضع الأمني للشبكات وأجهزة الحماية، الأنظمة والتطبيقات، الخدمات الالكترونية وقواعد البيانات، أجهزة الحاسوب وأجهزة الخوادم الرئيسية. وبعد الانتهاء من عملية التقييم الأمني يقوم المركز بتزويد الجهة المعنية بتقرير مفصل عن الوضع الأمني متضمناً التوصيات الفنية والإجراءات السليمة الواجب اتباعها لتحقيق اقصى درجات الحماية على كافة مستويات المنظومة الأمنية.

تم اجراء تقييم أمني فني لعشر (10) شبكات تابعة لمؤسسات حكومية وخاصة منها (5) شبكات تم ربطها على نظام مراقبة سجلات الأحداث.

10
شبكات لمؤسسات حكومية تم تقييمها

5
شبكات تم ربطها على نظام المراقبة

خدمة تقييم الاختراق Compromise Assessment

يقدم المركز الوطني للأمن السيبراني هذه الخدمة للوزارات والمؤسسات الحكومية وقطاع خاص من خلال إجراء تقييم تقني على مستوى الشبكة للكشف عن وجود دلائل على تعرضها للاختراق بناءا على مؤشرات الاختراق المعروفة او تقنيات المهاجمين الشائعة.

تم اجراء تقييم اختراق لأربعة (4) شبكات تابعة لمؤسسات حكومية وجهات خاصة

4
شبكات تم تقييمها

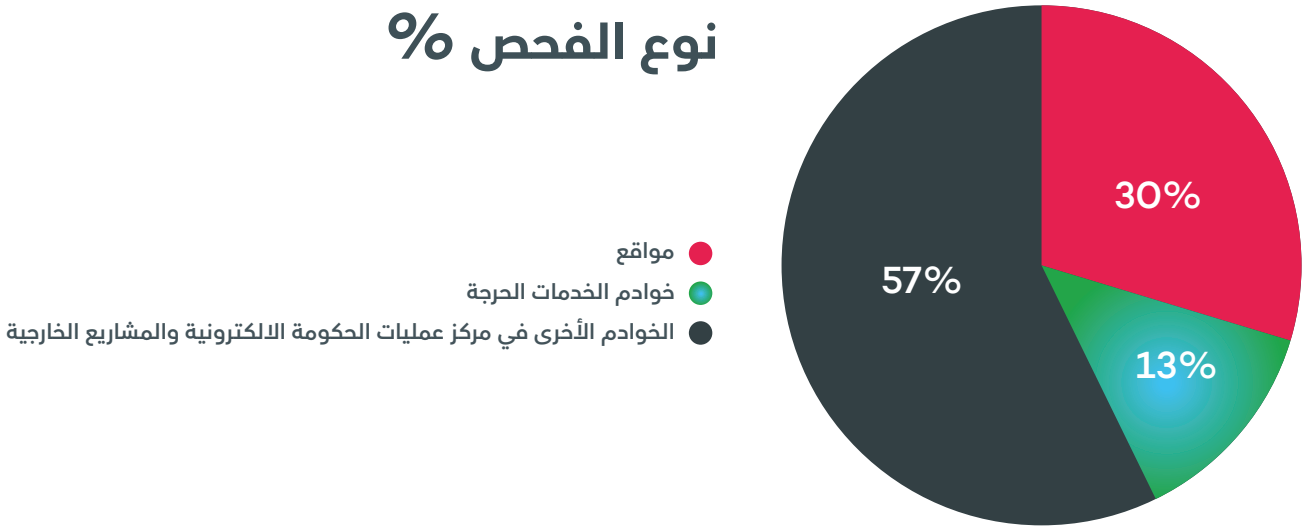
خدمة فحص الثغرات الأمنية
Vulnerability Assessment

يقوم المركز الوطني بتقديم خدمة الفحص الأمني للمواقع الالكترونية والخوادم والأجهزة للعديد من الوزارات والمؤسسات الحكومية وذلك للكشف عن الثغرات الامنية ونقاط الضعف فيها والعمل على ابلاغ الجهات المعنية بتقارير نتائج الفحص الامني لها ومتابعة حل واغلاق الثغرات الامنية فيها.

تم اكتشاف (7846) ثغرة أمنية بناءً على عمليات الفحص الأمني وتاليا جدول يوضح نسبة عمليات الفحص الأمني وعدد الثغرات

	عدد الثغرات	نسبة الفحوصات %
مواقع	2325	30.00%
خوادم الخدمات الحرجة	1038	13.00%
الخوادم الاخرى في مركز عمليات الحكومة الالكترونية والمشاريع الخارجية	4483	57.00%

نوع الفحص %



فحوصات أمنية للمواقع الالكترونية

تم رصد (2325) ثغرة امنية على المواقع الالكترونية بناءً على عمليات الفحص الأمني والجدول التالي يوضح عدد الثغرات الأمنية

تصنيف الثغرات على المواقع الالكترونية	المجموع
Critical	65
High	522
Medium	1738

فحوصات امنية للخوادم والأجهزة

- تم رصد ما مجموعه (5521) ثغرة على الخوادم والأجهزة بناءً على عمليات الفحص الأمني التي نفذت على (21690) من الأجهزة والخوادم.
- تم رصد ما مجموعه (1038) ثغرة على خوادم الخدمات الحرجة بناءاً على عمليات الفحص الأمني التي نفذت على (1647) من الأجهزة والخوادم.
- تم رصد ما مجموعه (4483) ثغرة على الخوادم الأخرى في مركز عمليات الحكومة الإلكترونية والمشاريع الخارجية بناءاً على عمليات الفحص الأمني التي نفذت على (20043) من الخوادم.

الخوادم الاخرى في مركز عمليات الحكومة الالكترونية والمشاريع الخارجية	مجموع الثغرات
Critical	772
High	1393
Medium	2318

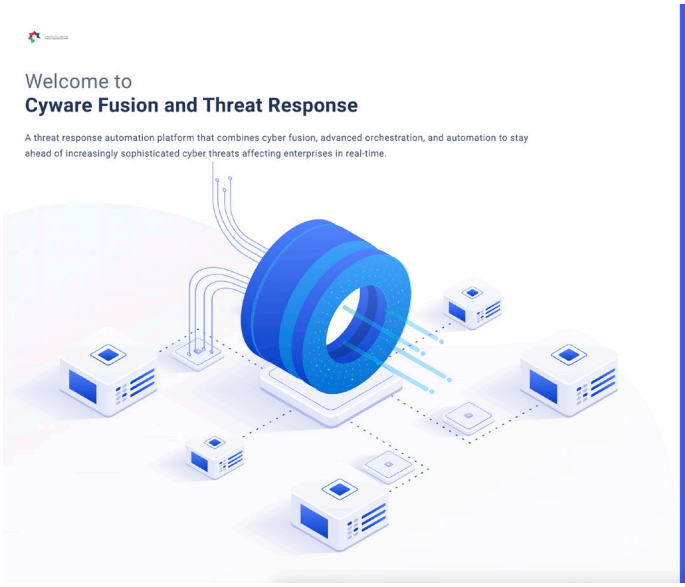
الخدمات الحرجة	مجموع الثغرات
Critical	212
High	420
Medium	406

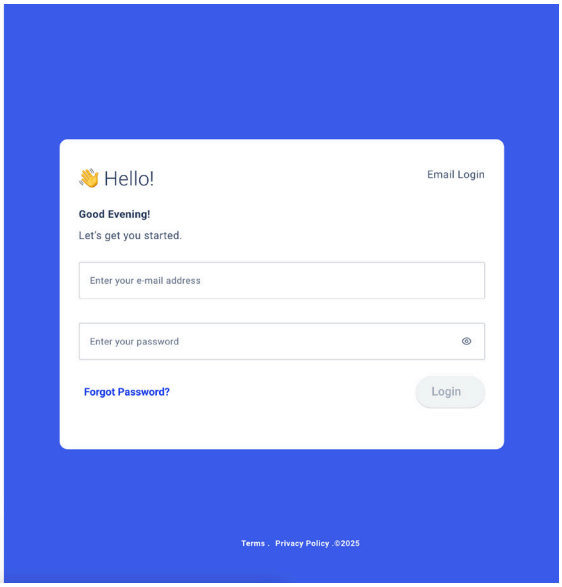
عمل المركز خلال عام 2024 على إطلاق مجموعة من

المنصات والمواقع الرقمية

إطلاق منصة إدارة الحوادث الأمنية (Incident Management System)

قام المركز الوطني للأمن السيبراني بداية العام 2024 بإطلاق منصة تفاعلية بين المركز والمؤسسات الحكومية تهدف على توحيد إدارة الحوادث الامنية وأتمتة سير وإجراءات عمل الاستجابة للتهديدات السيبرانية وتبادل المعلومات لتعزيز التعاون مع المؤسسات الحكومية، تعمل المنصة على تقليل أوقات الاستجابة وتحسين الكفاءة وتعزيز وضع الأمان في المؤسسات، مما يجعلها قابلة للتطوير والتكيف مع الاحتياجات الأمنية المتنوعة.



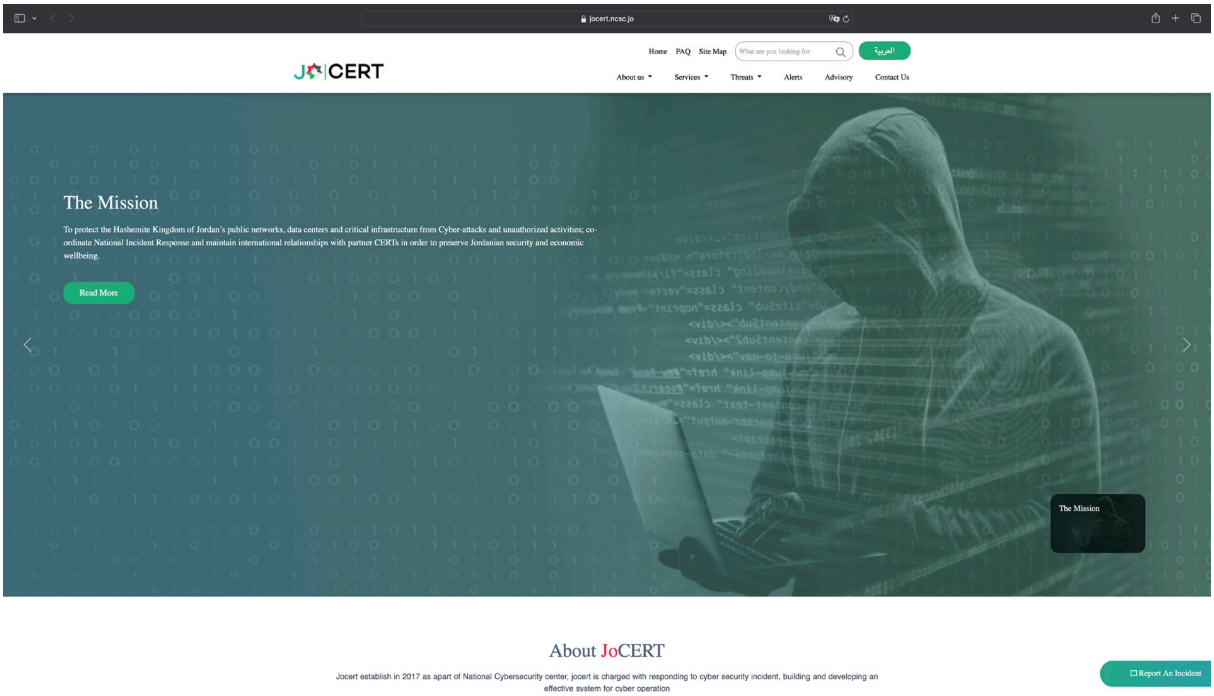


إطلاق نظام لأتمتة الإجراءات والاستجابة (Security Orchestration, automation & response)

قام المركز الوطني للأمن السيبراني بإطلاق نظام أتمتة الإجراءات والاستجابة يهدف إلى تعزيز عمليات الأمان من خلال أتمتة سير العمل، وتنظيم الأدوات، وتوحيد إدارة الحوادث. كما يعمل على تبسيط الاستجابات، وتقليل الجهد البشري، والاستفادة من معلومات التهديدات لاتخاذ قرارات أسرع تعمل على تحسين الكفاءة وتعزيز التعاون، و قدرة المؤسسات على اكتشاف التهديدات وتحليلها والاستجابة لها بشكل فعال.

تطوير موقع فريق الاستجابة الوطني (JoCERT)

تم إطلاق الموقع كمنصة مركزية لتعزيز الوعي بالأمن السيبراني وتنسيق الاستجابة للحوادث وتبادل المعرفة من خلال توفير قناة للإبلاغ عن حوادث الامن السيبراني التي تتعرض لها مؤسسات القطاع العام والخاص ونشر معلومات محدثة حول نقاط الضعف والتهديدات والاستشارات الأمنية بالإضافة لنشر التحذيرات الأمنية وتثقيف المستخدمين حول أفضل الممارسات للأمن السيبراني.



الاستخبارات السيبرانية

يسعى المركز الوطني للأمن السيبراني إلى التقييم المستمر للوضع الأمني السيبراني على المستوى الوطني، وذلك من خلال جمع وتحليل المعلومات السيبرانية ومشاركتها مع الجهات المعنية. يهدف هذا النهج إلى تعزيز فهم التهديدات والتحديات في الفضاء السيبراني الأردني، والتنبؤ بالمخاطر والأضرار المحتملة، بما يشمل الأنشطة الخبيثة، الثغرات الأمنية، والهجمات السيبرانية المتطورة. ويعمل المركز على تحقيق ذلك عبر تنفيذ مجموعة من العمليات والخدمات الرئيسية التي تُمكّنه من رصد التهديدات والتعامل معها بفعالية لحماية مكونات الفضاء السيبراني الأردني.

مشاركة معلومات التهديدات السيبرانية - منصة شارك

منصة شارك

تعتبر منصة مشاركة معلومات التهديدات السيبرانية **«شارك»** منصة آمنة وموثوقة لمشاركة المعلومات السيبرانية بين المؤسسات الوطنية وتبادلها، حيث توفر هذه المنصة معلومات عدة كمؤشرات الاختراق والثغرات الأمنية والتحليلات الرقمية وغيرها من المعلومات السيبرانية التي تحدد الاتجاهات والأنماط الجديدة والمتطورة للتهديدات والهجمات السيبرانية المختلفة.

- تم إعداد تقارير تفصيلية حول أهم وأحدث الهجمات والتهديدات السيبرانية التي تعرض لها الأردن ومنطقة الشرق الأوسط ونشرها على منصة مشاركة معلومات التهديدات السيبرانية وبواقع (66) تقرير خلال عام 2024.
- تم ربط عدد من المؤسسات الوطنية على منصة مشاركة معلومات التهديدات السيبرانية حيث بلغ عدد هذه المؤسسات (23) مؤسسة خلال عام 2024.

66
تقرير خلال عام 2024

23
مؤسسة تم ربطها على المنصة

الاستخبارات السيبرانية

مراقبة البصمة الرقمية Digital Footprint Monitoring

يقوم المركز بمراقبة التواجد الرقمي للمؤسسات الوطنية للكشف والإبلاغ في حال وجود ثغرات أو تسريبات أو أخطاء في الإعدادات التي يمكن استغلالها من قبل جهات التهديد السيبرانية المختلفة، وذلك من خلال متابعة مستمرة لواجهة التهديدات السيبرانية للأصول والخدمات الرقمية الخاصة بالمؤسسات ومراقبة حوادث التسريبات الخاصة ببيانات المؤسسات والتي يتم نشرها على شبكة الانترنت. وأهم ما تم إنجازه:

- مراقبة مستمرة لواجهة التهديدات السيبرانية للأصول والخدمات الرقمية الخاصة بالمؤسسات الوطنية حيث بلغ عدد التنبيهات التي تم رصدها (344) تنبيه.
- رصد (214) حادث تسريب للبيانات لمؤسسات وطنية.
- تجهيز (373) تقرير حول أهم الثغرات الأمنية التي يتم تتبعها من خلال مصادر ومنصات الاستخبارات السيبرانية.
- المراقبة المستمرة لعمليات انتحال جهات التهديد السيبرانية المختلفة للنطاقات والأصول الرقمية (Brand Protection) ولحوادث تغيير المحتوى للمواقع الالكترونية (Defacement) الخاصة بالمؤسسات الوطنية.

344

التنبيهات التي تم رصدها

214

حادث تسريب للبيانات

373

تقرير حول أهم الثغرات

التحقق الأمني Security Validation

يهدف المركز من خلال خدمة التحقق الأمني التأكد من كفاءة وفعالية الضوابط الأمنية الفنية في بيئة العمل للمؤسسات والوزارات الحكومية لغايات تحسين فعالية أنظمة الأمن والحماية الرقمية العاملة في هذه المؤسسات من حيث كيفية الاستجابة لسلوكيات الهجمات والتهديدات السيبرانية للحد منها.

- التوسع بعدد المؤسسات والوزرات الحكومية التي يتم تقديم الخدمة لها.

الاستخبارات السيبرانية

التقارير الأمنية السيبرانية الدورية

يقوم المركز بإعداد تقارير تسلط الضوء على الوضع الأمني السيبراني للمملكة وبشكل دوري، حيث تشمل معلومات وإحصائيات لأهم المؤشرات والحوادث والانشطة السيبرانية المرتبطة بالأردن والمنطقة.

✓ تم إصدار (28) تقرير أمني سيبراني حول الموقف الأمني الأردني.

28
تقرير أمني

خدمات فحوصات واختبارات الاختراق:

1)منصة مكافأة الثغرات واختبارات الاختراق الأردنية Bug Bounty Jo

Bug Bounty
Continuous Penetration Testing Platform

تعتبر منصة مكافأة الثغرات واختبارات الاختراق الأردنية Bug Bounty Jo الأولى من نوعها في الأردن، حيث تهدف لتمكين الجهات الحكومية والخاصة من اختبار وتحديد الثغرات ونقاط الضعف على أصولها الرقمية بسرعة وفعالية وكفاءة، وكما أنها تتيح للأفراد إمكانية التسجيل كفاحص اختراق أخلاقي للعمل عبر المنصة لغايات الفحص مقابل مكافئات مالية عند اكتشافهم لثغرات ونقاط ضعف مختلفة.

✓ تم اختبار الأصول الرقمية لعدة مؤسسات ووزارات حكومية من خلال منصة مكافأة الثغرات واختبارات الاختراق الأردنية حيث بلغ عدد الاختبارات المنفذة (56) اختبار.

56
اختبار للأصول الرقمية

الاستخبارات السيبرانية

2)فحص الاختراق Penetration Testing

يقوم المركز بتقديم خدمة تنفيذ فحوصات الاختراق لاختبار مدى سلامة وامن الأنظمة والمواقع والتطبيقات الالكترونية للمؤسسات والوزارات الحكومية بهدف تقييم مستوى الأمان والمخاطر في مواجهة محاولات الاختراقات السيبرانية والحماية منها من خلال تحديد الثغرات ونقاط الضعف واساليب الدخول للمخترقين لمعالجتها والحد منها.

- تم تنفيذ فحوصات الاختراق للمواقع والخدمات الإلكترونية الخاصة بالمؤسسات والوزارات الحكومية بواقع (114) فحص اختراق.

114

فحص اختراق

السياسات والامتثال

إقرار الإطار الوطني للأمن السيبراني

قام المركز الوطني للأمن السيبراني بإعداد مسودة الإطار الوطني للأمن السيبراني (JNCSF) وقد تم طرح الإطار للاستشارة العامة لمدة شهر على ضوء التغذية الراجعة والملاحظات التي تم ابداؤها من الجهات المعنية على الإطار تم رفع الإطار بصيغته النهائية للمجلس الوطني للأمن السيبراني والذي اقره بموجب قرار المجلس رقم 4 لسنة 2024 وذلك في جلسة المجلس المنعقدة بتاريخ 2024/5/1.

يهدف هذا الإطار إلى تلبية متطلبات الخطة الاستراتيجية الوطنية للأمن السيبراني، التي تدعو إلى تعزيز حوكمة الأمن السيبراني وإصدار الأطر التنظيمية اللازمة. و يمثل الإطار الوطني مجموعة من المعايير القياسية التي تحدد الحد الأدنى من المتطلبات الأمنية الواجب توفرها لدى المؤسسات.

يتميز الإطار بتطوره من حيث الفلسفة والمبادئ التي يستند إليها، كما وانه متوافق أيضًا مع الأطر العالمية المعروفة مثل معايير الآيزو (ISO) وإطار العمل الصادر عن المعهد الأمريكي للتكنولوجيا والمعايير (NIST). يركز الإطار على بناء القدرات لدى المؤسسات ورفع مستويات نضوج القدرات فيها ومساعدتها في تطور خطط مستقبلية لرفع مستوى الامن السيبراني وإدارة المخاطر المتعلقة بها. وقد ألزم قانون الأمن السيبراني جميع المؤسسات الحكومية والخاصة والأهلية بالامتثال للضوابط والمعايير الصادرة عن المركز.

أما فيما يتعلق بخطة تطبيق الإطار الوطني، فقد قام المركز بإنشاء خطة تنفيذية للإطار الوطني الأردني للأمن السيبراني لتطبيق الإطار في أكثر من 100 مؤسسة حكومية وقطاعات حرجة خلال سنة واحدة.

اصدار نظام ترخيص مقدمي خدمات الامن السيبراني

صدر نظام ترخيص مقدمي خدمات الامن السيبراني رقم (76) لسنة 2024 والذي يهدف الى إيجاد إطار تشريعي يعمل على ضمان جودة الخدمات المقدمة في مجال الامن السيبراني وينظم كافة الأمور المتعلقة بمقدمي خدمات الامن السيبراني من خلال الاشراف والرقابة والتدقيق على مقدمي الخدمة بما يكفل حماية حقوق مقدمي الخدمة ومتلقيها.

وبموجب هذا النظام يستلزم على الشركات الحصول على ترخيص من المركز الوطني للأمن السيبراني وفق متطلبات وشروط الحصول على الرخصة الوارد ذكرها في النظام والتعليمات التي ستصدر بمقتضاه ويحظر على أي جهة تقديم هذه الخدمات من دون الحصول على هذا الترخيص.

السياسات والامتثال

وقد تضمن النظام تحديد لخدمات الامن السيبراني التي تخضع للترخيص هي:

- خدمة الاستجابة لحوادث الامن السيبراني
- خـــدمة اســتشــارية الامن الســـــيبراني
- خـــدمة الامـــن الـــسيبـــرانـي الـــمدارة
- خـــدمة التـــحقيق الجـنائي الـــرقـمـــي
- خـــدمة فـــحـص الاخـــــــتراقـــــات
- خـــدمة الـــمســابقـــات الـسيبـرانـيـة
- خـــدمة تـــدقيق الامـــن الـــسيبـــرانـي
- خـــدمة بيـع مـنتجات الامـن السـيبراني
- خـــدمة الـتدريب فـي الامـن السـيبراني

وقد انتهى المركز من اعداد مسودة التعليمات الناظمة لخدمات الامن السيبراني و تم طرح استشارة عامة لتعليمات ترخيص خدمة بيع المنتجات الامن السيبراني و تعليمات ترخيص خدمة الاستجابة لحوادث الامن السيبراني بتاريخ 2024/12/2 ولمدة أسبوعين . توضح التعليمات شروط ومتطلبات الترخيص والتزامات مقدم الخدمة ومسؤوليات المركز . ويستقبل المركز طلبات الترخيص ورقيا والكترونيا وتم توفير منصة خاصة بترخيص خدمات الامن السيبراني وتعنى المنصة بإدارة عمليات الترخيص من تقديم طلبات الترخيص ومراقبة الامتثال للجهات المقدمة لخدمات الامن السيبراني حيث ان المنصة في صدد التنفيذ في بداية سنة 2025.

الانضمام للترتيبات الدولية للمعايير المشتركة كعضو مستهلك CCRA

وافق مجلس الوزراء على قرار المركز الوطني للأمن السيبراني بانضمام المملكة الى الترتيبات الدولية للمعايير المشتركة بهدف تعزيز موثوقية الأردن في مجال الامن السيبراني وتسهيل التعاون والاعتراف المتبادل في تقييم واعتماد منتجات الامن السيبراني، حيث سيمنح المركز وضع معايير واضحة لتبادل الاعتراف بشهادات **«الاعتراف بالمنتجات الرقمية»**، لجهة فحصها وضمان جودتها، وكذلك لضمان تقييم منتجات تكنولوجيا المعلومات وملفات تعريف الحماية وفقا لمعايير عالية ومتسقة، وتعزيز موثوقية هذه المنتجات.

تمثل الترتيبات الدولية للمعايير المشتركة مجموعة من الارشادات والمواصفات الدولية بين الدول المشاركة وتهدف الى تعزيز الاعتراف المتبادل بالتقييمات الأمنية لمنتجات تكنولوجيا المعلومات (ICT)، وتسعى هذه الترتيبات الى تعزيز الثقة في منتجات تكنولوجيا المعلومات من خلال معايير عالية ومتسقة، بحيث يمكن الوثوق بالمنتجات المعتمدة الخاصة بالأمن السيبراني من قبل احدى الدول المشاركة واستخدامها في دول الأعضاء الأخرى دون الحاجة الى اختبارات او تقييمات إضافية.

السياسات والامتثال

أما فيما يتعلق بالبنى التحتية الحرجة، فقد تم عام 2024 ما يلي :

- تنفيذ تقييم للنضوج السيبراني (Maturity Assessment) لقطاعات البنى التحتية الحرجة في الأردن، حيث هدفت عملية التقييم إلى تحديد درجة النضوج السيبراني في القطاعات المختلفة مما يساعد في تحديد أولويات العمل في المراحل القادمة للرفع من مستوى الأمن السيبراني في هذه القطاعات.

- إعداد مسودة استراتيجية الأمن السيبراني في قطاع الطاقة الأردني، حيث اشتمل هذه الاستراتيجية على أبرز الأهداف والخطط التنفيذية لرفع مستوى الأمن السيبراني في هذا القطاع الحيوي.

- وإعداد مسودة الضوابط الخاصة بالأمن السيبرانية في البنى التحتية الحرجة، حيث تستند هذه الضوابط على عدد من المعايير العالمية في الأمن السيبراني وتشمل شبكات تكنولوجيا المعلومات (IT) بالإضافة للشبكات التشغيلية (OT).

- تصنيف البنى التحتية الحرجة وتحديد مقدميها لدى قطاعي الطاقة والمياه في الأردن.

- تنفيذ تمرين سيبراني بالتعاون مع المفاعل النووي الأردني للبحوث والتدريب وجامعة الحسين التقنية، حيث شارك في التمرين عدد من المؤسسات الوطنية العاملة ضمن قطاعات البنية التحتية الحرجة.

- تنفيذ عدد من ورشات العمل مع الهيئات التنظيمية والرقابية للبنى التحتية الحرجة لتبادل الآراء ومشاركة الخبرات حول واقع الأمن السيبراني في هذه القطاعات.

السياسات والامتثال

الاستراتيجية الوطنية للأمن السيبراني :

سعى المركز الوطني للأمن السيبراني واستناداً للمهام المناطة له بموجب المادة (6/ب/1) من قانون الامن السيبراني لسنة 2019 وبالتنسيق مع الفريق الاستشاري للمجلس الوطني للأمن السيبراني، بإعداد مسودة الاستراتيجية الوطنية للأمن السيبراني للأعوام 2024-2028، وايماناً من المركز بضرورة العمل التشاركي والتعاوني مع كافة أصحاب العلاقة المعنيين من القطاعيين الحكومي والخاص، قام المركز بمناقشة مسودة الخطة التنفيذية للأعوام 2024-2028 مع أصحاب العلاقة المعنين لتكوين فهم أوسع وشمولي لتطلعات المركز وأصحاب العلاقة بالإضافة لتعزيز العلاقات الاستراتيجية معهم من خلال عقد سلسلة لقاءات وحوارات مع ضباط الارتباط من الأطراف المعنية لهذه الغاية ، حيث تم لاحقاً وبالتشارك مع الأطراف المعنية بإعداد خطة تنفيذية وطنية مُحددة بالأنشطة والمشاريع ومسؤوليات التنفيذ ضمن أُطر زمنية واضحة ، وبما يضمن كفاءة التنفيذ لمضمون الخطة الاستراتيجية الوطنية للأمن السيبراني 2024-2028.

بعد تحليل نتائج التحليل البيئي للعوامل العالمية التي تؤثر وتتأثر بها الأنظمة السيبرانية العالمية، وتحديد الفرص والتهديدات العالمية والسيناريوهات العالمية المتوقعة لهذه العوامل، وربطه بنقاط القوة في الفضاء السيبراني الأردني و التي تشكل عنصرا داعماً لعمليات التطوير والتحسين في الفضاء السيبراني الأردني، وتحليل فرص التحسين التي تتيح نظرة شمولية للمجالات الواجب تعزيز العمل على تطويرها وتحسينها، وبما يضمن تحقيق الرؤية الوطنية للفضاء السيبراني الأردني 2024-2028 تم توجيه البوصلة الاستراتيجية لأربعة أولويات استراتيجية يجب تظافر الجهود الوطنية وتكاملها للعمل عليها، وهي: الامن والموثوقية، المرونة السيبرانية، التحول السيبراني، التعاون والشراكات.

يسعى المركز من خلال الرؤية الاستراتيجية للفضاء السيبراني في الأردن العمل بجهود تعاونية وتكاملية ما بين القطاعات الوطنية الحكومية، الأمنية والخاصة، لضمان استدامة أمن واستقرار الفضاء السيبراني الأردني، وبما يضمن تحقيق السيادة الرقمية عل الأصول التكنولوجيا المادية والافتراضية للملكة الأردنية الهاشمية، وحماية كافة مستخدميها من الأفراد والمؤسسات، وجعل المملكة ردعاً منيعاً امام التهديدات والهجمات السيبرانية من خلال تعزيز المرونة السيبرانية على المستوى الوطني، والتي تُعد اللبنة الأولى التي تجعل من فضاءنا حصناً منيعاً قادر على الدفاع والصمود أمام النشاطات السيبراني الهادفة للعبث بأمنه الرقمي واستقرار بيئته السيبرانية من خلال المبادئ التوجيهية وهي فضاء سيبراني اردني، آمن وموثوق، قادر على الصمود، معتمد على القدرات الوطنية، مُعزز للاقتصاد والرفاه المجتمعي.

التدريب والتطوير

منذ تأسيسه كرّس المركز الوطني للأمن السيبراني جهوده الاستراتيجية لتطوير وبناء القدرات الوطنية في مختلف مجالات الأمن السيبراني، سواء كانت معرفية وتوعوية أو تقنية وعملية. فقد استشرف المركز منذ بداياته أهمية العنصر البشري كركيزة أساسية في تعزيز منظومة الأمن السيبراني، ودوره المحوري في تحقيق فضاء رقمي متين وقادر على التصدي للتهديدات السيبرانية والتعامل بفاعلية مع الحوادث الأمنية.

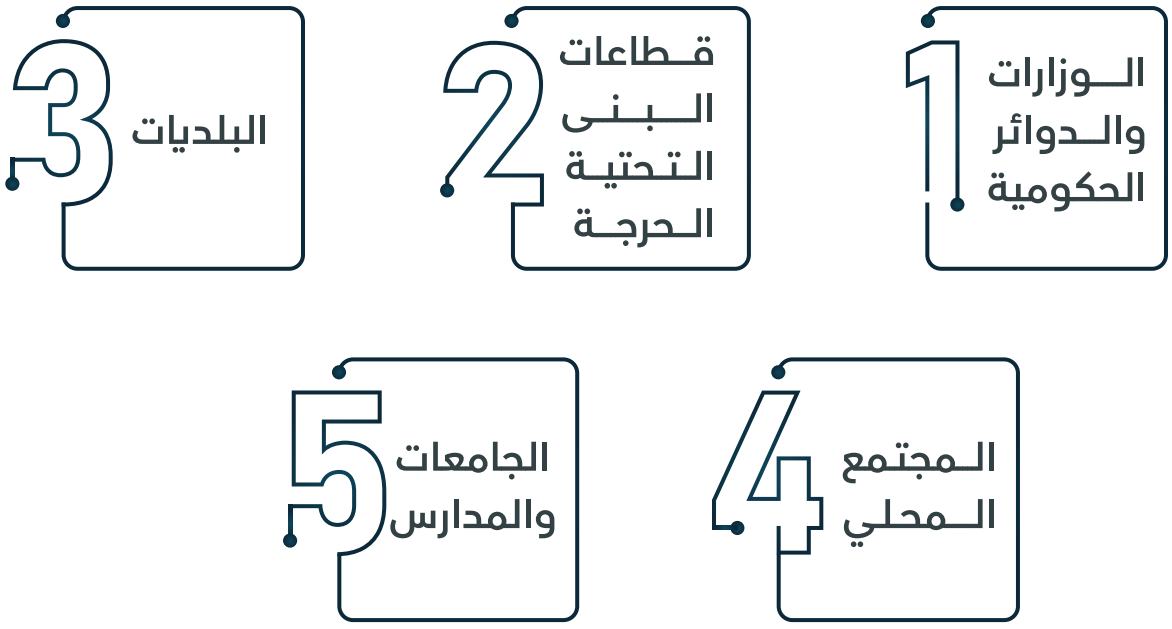
وانطلاقاً من هذا الإدراك العميق، عمل المركز على توجيه مساعيه نحو بناء منظومة مستدامة لتنمية القدرات الوطنية. وشمل ذلك تنظيم ورش عمل شاملة، وحملات توعوية مكثفة، ودورات تدريبية نوعية، وبرامج تأهيلية متخصصة. وقد تميزت هذه الأنشطة بالتنوع والشمولية، لتغطي كافة شرائح المجتمع الأردني، بما يضمن إشراك الجميع في تحقيق رؤية وطنية للأمن السيبراني المستدام.

وفيما يلي أبرز الإنجازات التي تحققت في هذا الإطار:

التوعية بماهية الأمن السيبراني

1. ورشات التوعية والتثقيف:

عقد المركز الوطني للأمن السيبراني 37 ورشة في مفاهيم الحماية السيبرانية والأمان الرقمي وأمن المعلومات، وتوضيح أفضل الإجراءات والمُمارسات الآمنة عبر الإنترنت، وكيفية الوقاية من حملات التصيد الاحتيالي وغيرها من التهديدات السيبرانية، وقد استفاد من هذه الورشات 2390 شخص من الفئات الآتية:



2. حملات توعوية:

أطلق المركز الوطني للأمن السيبراني العديد من حملات التوعية التي هدفت إلى تعزيز الوعي بالأمن السيبراني والمخاطر والتهديدات الموجودة في العالم الرقمي، وتم مُشاركة هذه الحملات من خلال نصوص ومقاطع فيديو تم تصميمها خصيصاً لكل حملة، ومن ثم بثها ومشاركتها عبر وسائل التواصل الاجتماعي المختلفة أو حتى عبر وسائل أخرى، وعلى النحو الآتي:

- **حملة توعية كبار السن:**
تم إطلاقها بالتعاون مع شركة زين، بهدف تقديم نصائح وارشادات أمان موجهة خصيصاً لفئة كبار السن، وكانت هذه النصائح على شكل مقاطع فيديو تمثيلية تم نشرها عبر وسائل التواصل الاجتماعي المختلفة.

- **حملة وطن واع:**
تم إطلاقها بالتعاون مع أمانة عمان الكبرى خلال شهر أكتوبر/تشرين أول (شهر التوعية بالأمن السيبراني عالمياً)؛ حيث تم خلالها تصميم العديد من المنشورات ومقاطع الفيديو التي تم نشرها على شاشات أمانة عمان المتواجدة في كافة أنحاء العاصمة، وبقيت الحملة مُستمرة بعد انتهاء شهر التوعية لتمتد أيضاً خلال شهر تشرين الثاني.

- **حملة استثمر بأمان:**
تم إطلاقها بالتعاون مع وزارة الاستثمار، بهدف تقديم نصائح سيبرانية لفئة رجال الأعمال والمُستثمرين حول كيفية تعزيز الامن السيبراني لمؤسساتهم سواء الكبيرة منها أو حتى الصغيرة، وذلك على شكل بروشورات رقمية تم نشرها عبر وسائل التواصل الاجتماعي المختلفة.

- **حملة مرئية على قنوات التلفاز:**
تم نشر بعض الفيديوهات التي تتضمن نصائح وإرشادات متعلقة بالأمن السيبراني وكيفية تحقيقه بالنسبة للأفراد على شاشات كل من التلفزيون الأردني وقناة المملكة الفضائية وذلك على مدار أسبوع كامل وفي أوقات مختلفة في كلا القناتين.

- **حملة Up to Date :**
هدفت الحملة لتعزيز الوعي بالإجراءات الصحيحة اثناء استخدام الفضاء الرقمي، وسبل حماية المعلومات والبيانات الشخصية والمؤسسية من محاولات عبث أو سرقة أو وصول غير مصرح به، استهدفت هذه الحملة وبشكل وجاهي موظفي تكنولوجيا المعلومات في العديد من المؤسسات الحكومية وقطاعات البنى التحتية الحرجة، من خلال إقامة يوم علمي متخصص في الأمن السيبراني وأهم ممارساته وأحدث استراتيجياته.

- **حملة تلميحة رقمية:**
تم إطلاقها بالتعاون مع منتدى المدن الذكية خلال شهر أكتوبر / تشرين أول (شهر التوعية بالأمن السيبراني عالمياً) وتضمنت عقد ورشات توعوية للعديد من موظفي بلديات المملكة على أفضل الممارسات في مجال الحماية الرقمية والأمن السيبراني.

- **حملة ذوي الاحتياجات الخاصة:**
تم إطلاق هذه الحملة بالتعاون مع المجلس الأعلى لرعاية ذوي الاحتياجات الخاصة، حيث تم تصميم فيديوهات توعوية بلغة الإشارة وتتضمن نصائح سيبرانية وتم نشرها عبر مواقع التواصل الاجتماعي المختلفة.

3. بودكاست حكاية سيبرانية:

استمراراً لمسيرة المركز الوطني للأمن السيبراني في مواكبة أحدث تقنيات التواصل الرقمي المستخدمة على نطاق واسع، واصل المركز تقديم سلسلة جديدة من البودكاست المتخصص **«حكاية سيبرانية»** ، وتضمنت السلسلة خلال العام 2024 خمسة حلقات حوارية متميزة استضافت مجموعة من الخبراء والمتخصصين في مجالي الأمن السيبراني وأمن المعلومات، بهدف نشر الوعي وتعزيز المعرفة في هذه المجالات الحيوية.

وهم كل من :

- **المهندس بسام المحارمة** - الرئيس السابق للمركز الوطني للأمن السيبراني

  عنوان الحلقة (الإطار الوطني الأردني للأمن السيبراني)

- **موظفو المركز (المهندس علاء الكساسبة والفاضلة جمانة أبو زايد)** - مدربين أمن سيبراني في المركز الوطني للأمن السيبراني

  عنوان الحلقة (دور التوعية في الحد من الهجمات الإلكترونية)

- **المهندس ماجد البقور** - مستشار الأمن السيبراني في شركة Fortinet

  عنوان الحلقة (أهمية أمن الحوسبة السحابية والممارسات)

- **دانية عبد اللوزي** - مدير استشارات في الأمن السيبراني في KPMG الشرق الأوسط

  عنوان الحلقة (أبرز التهديدات السيبرانية وكيفية التعامل معها)

- **السيد معتصم مريّان** - مدير وحدة الشؤون القانونية في المركز الوطني للأمن السيبراني

  عنوان الحلقة (نظام ترخيص مقدمي خدمات الأمن السيبراني)

4. منصة SafeOnline

استمراراً لجهود المركز الوطني للأمن السيبراني في تعزيز الوعي الرقمي، تم تغذية منصة «SafeOnline» بمحتوى توعوي متنوع يلبي احتياجات مختلف الفئات المستهدفة من الأفراد والمؤسسات. وتشمل المنصة، التي يمكن الوصول إليها عبر الرابط www.safeonline.jo، مجموعة واسعة من المواد التوعوية، مثل الخطوات والإجراءات التي تعزز الأمن السيبراني، وتفعل الحماية الرقمية، إضافة إلى المقالات العلمية المتخصصة في مختلف المفاهيم السيبرانية، والمحتوى المتنوع الذي يتناسب مع الفئات المستهدفة، ولتعزيز الوصول إلى محتواها التوعوي تم إدراج رابط المنصة ضمن قائمة الخدمات الحكومية في المواقع الإلكترونية الرسمية.

تعزيز القدرات وتعزيز المهارات لطلبة الجامعات والمدارس

ايماناً من المركز الوطني للأمن السيبراني بأهمية إعداد جيل مؤهل يمتلك المهارات اللازمة لمواجهة التحديات السيبرانية المتزايدة في العصر الرقمي، حيث يعد الاستثمار في تطوير المهارات وبناء القدرات البشرية حجر الأساس لتعزيز الأمن السيبراني على المستويين الوطني والدولي.

وانطلاقًا من هذه الرؤية، سعى المركز إلى تأهيل الطلبة في مختلف المراحل التعليمية، سواء في الجامعات أو المدارس، من خلال برامج تدريبية متخصصة ومسابقات تنافسية ومبادرات تعليمية تهدف إلى صقل مهاراتهم التقنية، وتعزيز وعيهم بالممارسات الأمنية، وتمكينهم من التصدي للتهديدات السيبرانية بفعالية.

وفي هذا السياق، أطلق المركز عددًا من المبادرات النوعية والبرامج التدريبية المتخصصة ، والتالي أبرزها :

1. معسكر نشامى السايبر

يهدف البرنامج إلى تطوير مهارات خريجي تخصصات تكنولوجيا المعلومات لطلبة الجامعات الأردنية في المجالات العملية للأمن السيبراني بالإضافة إلى المهارات الحياتية واللغة الإنجليزية وبشكل يؤهلهم جيداً لسوق العمل ومتطلباته وعلى مدار ثلاثة أشهر من التدريب المكثف ، وقد بلغ عدد المشاركين في **معسكر نشامى السايبر بنسختيه الرابعة والخامسة** 60 طالباً وطالبة.

2. مسابقة محاربو السايبر للجامعات

تم إطلاق **النسخة الثالثة من مسابقة محاربو السايبر للجامعات** التي شارك فيها ما يزيد عن 300 طالب وطالبة من مختلف الجامعات الحكومية والخاصة، وقد تأهل هؤلاء الطلبة للمسابقة النهائية بعد إجراء مسابقة تأهيلية أولية عبر الأون لاين لتصفية المشاركين.

3. مسابقة محاربو السايبر للمدارس

تم إطلاق **النسخة الأولى من مسابقة محاربو السايبر للمدارس**، والتي شارك فيها ما يزيد عن 200 طالب وطالبة من مدارس المملكة الأردنية الهاشمية؛ حيث تنافس اطلبة موزعين على 70 فريق لحل تحديات تقنية في العديد من مواضيع الأمن السيبراني كالثغرات والاختراق والهندسة العكسية وغيرها ، وقد تنوعت المدارس المشاركة في المسابقة ما بين مدارس حكومية ومدارس خاصة ومدارس عسكرية ومدارس تابعة لوكالة الأونروا.

4. تدريب تحديات التقاط العلم (CTF)

حرصاً من المركز الوطني للأمن السيبراني على تعزيز رفع قدرات الطلبة سواء الجامعيين منهم أو حتى طلبة المدارس، فقد نفذ المركز برنامجين تدريبيين في مجال التدريب على ما يُعرف **بتحديات التقاط العلم**، حيث شمل التدريب 32 جامعة وكلية وبعدد مشاركين بلغ 2661 طالب، وتدريب 21 مدرسة وبعدد مشاركين بلغ 487 طالب.

5. تدريب طلبة الجامعات (مسار)

يواجه الطلبة المقبلين على التخرج من تخصصات الأمن السيبراني صعوبة بالغة في العثور على فرص تدريبية لغايات استكمال متطلبات تخرجهم، وإدراكاً من المركز الوطني للأمن السيبراني بضرورة وأهمية تأهيل وإعداد طلبة قادرين على تحقيق متطلبات سوق العمل، أطلق المركز النسخة الأولى من برنامج (**مسار**) الذي يُعنى بتأمين تدريب ميداني لطلبة الجامعات الأردنية من تخصصات الأمن السيبراني، وشمل التدريب مجموعة كبيرة من الطلبة بلغ عددهم 280 طالب وطالبة من مختلف الجامعات الأردنية مع مراعاة الأقاليم الجغرافية.

6. رواد السايبر

واصل برنامج **رواد السايبر** مسيرته في عام 2024 مستهدفاً بشكل خاص طلبة الكشافة في المدارس، حيث ركز البرنامج على توعية الطلاب بمخاطر استخدام شبكة الإنترنت والمشكلات التي قد تنجم عنها، إلى جانب تدريبهم على أفضل الممارسات الأمنية أثناء استخدام الإنترنت والأجهزة الإلكترونية. كما شمل تعريفهم ببرامج حماية البيانات وكيفية توظيفها والاستفادة منها، بالإضافة إلى تمكينهم من أساليب حماية أنفسهم من المخاطر السيبرانية المحتملة أثناء التصفح الإلكتروني أو ممارسة الألعاب عبر الإنترنت. وقد استفاد من هذا البرنامج التدريبي 100 طالباً من مختلف مدارس المملكة.

تعزيز القدرات وتعزيز المهارات للموظفين والعاملين في القطاعات الوطنية

7. نظام إدارة التعليم (LMS)

واعي
منصة بناء القدرات الوطنية

تم الانتهاء من تدريب مجموعة من ضباط الارتباط لعدد من الوزارات والمؤسسات الحكومية على منصة إدارة التعليم (**واعي**) الخاصة بنشر التوعية السيبرانية بين الموظفين، حيث تم تدريب الدفعة الأولى كعينة بهدف اختبار وجود أي تحديات أو صعوبات في التعامل مع هذه المنصة ، وتجدر الإشارة إلى أن المنصة تتضمن مواد توعوية وتدريبية لتأهيل الموظفين وتوعيتهم حول أفضل الممارسات الأمنية أثناء تواجدهم على الشبكة الحكومية وتدريبهم على سياسات الأمن السيبراني المُطبقة في مؤسساتهم، بالإضافة إلى احتواءها على منصة يُمكن من خلالها اجراء اختبارات وحملات تصيد وهمية بهدف تدريب الموظفين على الدقة والحذر في التعامل مع البريد الإلكتروني الوارد وهو ما سينعكس بدوره على رفع مستوى صمود مؤسساتهم بوجه التهديدات السيبرانية وسرعة التعافي من الحوادث السيبرانية.

التوعية الإعلامية

في إطار جهود المركز الوطني للأمن السيبراني لتعزيز حضوره الإعلامي ونشر الوعي السيبراني، حقق المركز خلال عام 2024 سلسلة من الإنجازات المتميزة والتي ساهمت في زيادة انتشار رسائله التوعوية وتعزيز تفاعله مع الجمهور عبر مختلف المنصات الإعلامية والرقمية، وتالياً أبرزها:

- ارتفاع جمهور صفحات المركز الرسمية على منصات التواصل الاجتماعي بنسبة 167%.
- نشر 403 منشورات توعوية وتفاعلية على صفحات المركز الرسمية.
- رفع 154 مادة إعلامية ومحتوى توعوي على الموقع الإلكتروني الرسمي للمركز.
- نشر 255 خبراً وتقريراً عن المركز عبر القنوات التلفزيونية والإذاعية والمواقع الإخبارية.
- تحقيق 148 تغطية إعلامية لأخبار وفعاليات المركز عبر مختلف الوسائل الإعلامية.

%167
ارتفاع جمهور المركز على منصات التواصل الاجتماعي

403
منشورات توعوية

154
مادة إعلامية

255
خبرًا وتقريرًا عن المركز

148
تغطية إعلامية

الاتصال والتعاون

يواصل المركز الوطني للأمن السيبراني جهوده في تعزيز مكانة الأردن إقليميًا وعالميًا في مجال الأمن السيبراني، من خلال تحسين المؤشرات الدولية وتوسيع الشراكات الاستراتيجية. ويستعرض هذا المحور أبرز الإنجازات المحققة خلال عام 2024،

تحسين مرتبة الأردن في مؤشرات الأمن السيبراني العالمية

ضمن إطار الجهود الوطنية لتعزيز مكانة الأردن على خارطة الأمن السيبراني العالمية، حقق المركز الوطني للأمن السيبراني خلال عام 2024 إنجازات نوعية في المؤشرات الدولية ذات العلاقة، والتي تعكس حجم التقدم والالتزام الاستراتيجي في هذا المجال، حيث جاءت أبرز النتائج على النحو التالي:

- مؤشر الأمن السيبراني العالمي (GCI):

أحرز الأردن تقدمًا لافتًا بتحقيق المرتبة 27 عالميًا، قفزًا من ترتيب سابق منخفض، مما وضع المملكة ضمن الفئة الأعلى من تصنيف الدول في المؤشر. وقد بلغ عدد المراتب التي تقدم بها الأردن 44 مرتبة، مما يعد نقلة نوعية في المؤشرات الدولية للأمن السيبراني.

- الرقم القياسي الوطني للأمن السيبراني (NCSI):

سجل الأردن علامة 52.5 مقارنة بعلامة سابقة بلغت 28.57، مما يعكس تحسنًا ملموسًا في البنية التحتية، والجاهزية التشريعية، والإجراءات المؤسسية المتعلقة بالأمن السيبراني.

تعزيز الشراكات الوطنية

حرصًا على توسيع مجالات التعاون والتكامل المؤسسي، أبرم المركز الوطني للأمن السيبراني خلال عام 2024 عددًا من مذكرات التفاهم مع جهات وطنية، بهدف تعزيز تبادل المعرفة وتطوير القدرات المؤسسية. ومن أبرز الجهات التي تم توقيع مذكرات تفاهم معها:

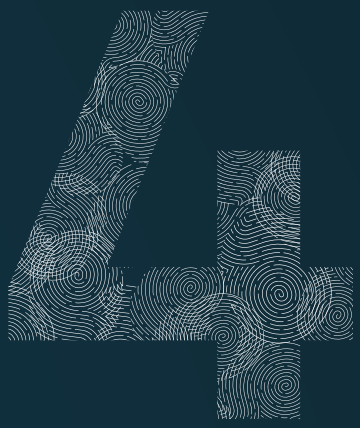
- مركز الملك عبد الله الثاني للتميز
- النيابة العامة
- جامعة الشرق الأوسط
- بورصة عمان

الاتصال والتعاون

المشاركة في المنتديات والمؤتمرات الدولية

سعياً لترسيخ الحضور الأردني في المنصات الدولية وتبادل الخبرات مع نظرائه من الجهات الإقليمية والعالمية، شارك المركز الوطني للأمن السيبراني خلال عام 2024 في عدد من الفعاليات الدولية البارزة في مجال الأمن السيبراني، من أبرزها:

- المشاركة في **مؤتمر** MWC Barcelona 2024 المقام في إسبانيا.
- المشاركة في **مؤتمر الخليج لأمن المعلومات** GISEC في دبي / الإمارات العربية المتحدة.
- المشاركة في **مؤتمر** Cyber Q في أبو ظبي / الإمارات العربية المتحدة.
- المشاركة في **مؤتمر بوخارست للأمن السيبراني** لعام 2024.
- المشاركة في **مؤتمر الدولي حول التحديات المرتبطة باستخدام قدرات الاختراق الإلكتروني غير المسؤول**، والمنعقد في لندن / المملكة المتحدة.
- المشاركة في فعاليات **مؤتمر** FINCON 2024 .
- زيارة **مركز الأمن السيبراني الوطني** في الإمارات العربية المتحدة.
- زيارة مركز العملاء التابع لـ Splunk Customer Briefing Center في المملكة المتحدة.
- المشاركة في **تمرين الأمن السيبراني الخاص بأنظمة التحكم الصناعية** في الولايات المتحدة الأمريكية.
- المشاركة في **اجتماعات الدائرة المستديرة للأمن السيبراني** في الأمم المتحدة، إضافة إلى **المنتدى الدولي للأمن السيبراني** في الولايات المتحدة الأمريكية.
- المشاركة في **اجتماع مجموعة العمل المختصة بالأمن السيبراني** والمنعقدة في جنيف / سويسرا.
- المشاركة في **الأسبوع الإقليمي للأمن السيبراني** الذي نظّمه الاتحاد الدولي للاتصالات في مسقط / سلطنة عُمان.
- المشاركة في **المنتدى الخامس للأمن السيبراني** والتدريبات السيبرانية الخاص بأوروبا والبحر الأبيض المتوسط، والمنعقد في بلغاريا.
- المشاركة في **الدورة الأولى لمجلس وزراء الأمن السيبراني العرب**، والتي عُقدت في الرياض / المملكة العربية السعودية.
- المشاركة في برنامج IVLP في الولايات المتحدة الأمريكية.
- المشاركة في أعمال **الدورة السابعة المعنية بأمن واستخدام تكنولوجيا المعلومات**، والمنعقدة في مقر الأمم المتحدة / نيويورك.
- المشاركة في **التمرين السيبراني الإقليمي** المقام في مراكش / المملكة المغربية.
- المشاركة في دورة تدريبية متخصصة في **«الأمن السيبراني والقانون الدولي»** في بروكسل / بلجيكا.
- المشاركة في تدريب تطبيقي حول تقنيات Fideiis SCOUT Box-IR Kit في دبي / الإمارات العربية المتحدة.



تطلعات المركز الوطني للأمن السيبراني لعام 2025

تطلعات المركز الوطني للأمن السيبراني لعام 2025

يسعى المركز الوطني للأمن السيبراني خلال عام 2025 إلى مواصلة تطوير البنية التحتية السيبرانية وتعزيز قدراته على مختلف المستويات، من خلال مجموعة من التطلعات الاستراتيجية، التي تشمل ما يلي:

- تطوير خدمات منصات الاستخبارات السيبرانية العاملة في المركز وتحسين كفاءتها، وزيادة عدد المؤسسات الوطنية المرتبطة بها والمستفيدة من خدماتها.
- التوسع في مراقبة البصمة الرقمية للمؤسسات الوطنية وزيادة عدد الجهات المشمولة بهذه الخدمة، مع تنويع المنصات والمصادر الرقمية المستخدمة.
- تحسين نظام إدارة معلومات الاستخبارات السيبرانية، من حيث عدد المنصات والمصادر المرتبطة به، وتعزيز دقته وسرعة استجابته.
- بناء مستودع بيانات مركزي (Security Data Lake) لتخزين وتحليل كميات كبيرة من سجلات الأحداث الأمنية وتحركات الشبكات.
- تطوير إجراءات المراقبة والتحليل في مركز العمليات السيبرانية لرفع مستوى الاكتشاف المبكر والاستجابة الفعالة.
- إنشاء مختبر وطني متخصص بتحليل الأدلة الرقمية (Forensic Lab) لتطوير قدرات الاستجابة للحوادث والتحقيق فيها.
- إنشاء نظام وطني لفحص وكشف التهديدات السيبرانية المحتملة (National Scanner) لرفع كفاءة الحماية الاستباقية.
- إطلاق لوحة تحكم تفاعلية (Dashboard) للمؤسسات الحكومية، تتيح متابعة الإحصائيات والتحذيرات الخاصة بها.
- إنشاء موقع بديل للتعافي من الكوارث (DR Site) لضمان استمرارية العمليات في حال توقف مركز العمليات الرئيسي.
- استكمال تنفيذ مشروع (Network Detection and Response) من خلال ربط 45 مؤسسة حكومية جديدة.
- تطوير البنية الفنية والعملياتية السيبرانية في 60 مؤسسة وطنية بناءً على مخرجات التقييمات الفنية لأصولها الرقمية.
- تطوير مبادرات نوعية تُسهم في رفع الجاهزية السيبرانية وحماية الفضاء الرقمي الأردني.
- توسيع برنامج «مسار» التدريبي ليشمل تخصصات جديدة وطلبة الدبلوم.
- عقد تصفيات تأهيلية لمسابقة «محاربو السايبر للمدارس» لقياس مستوى الطلبة وتحفيزهم.
- إنشاء منصة إلكترونية موحدة لبرامج رفع القدرات في الأمن السيبراني تستهدف طلبة المدارس والجامعات.
- تدريب موظفي القطاع العام في مجال الأمن السيبراني من خلال منصة التعليم الإلكتروني (LMS).
- عقد شراكات مع القطاع الخاص لتنفيذ حملات توعوية رقمية موجهة لفئات متنوعة مثل كبار السن، الأطفال، وأصحاب المشاريع الناشئة.
- إدخال مفاهيم الأمن السيبراني في النشاطات اللامنهجية داخل المدارس بالتعاون مع وزارة التربية والتعليم.
- تعزيز الإنتاج الإعلامي السيبراني المرئي والمسموع لتوسيع الوصول المجتمعي وتحقيق تأثير مستدام في الوعي الأمني.

المركز الوطني
للأمن السيبراني
National Cyber
Security Center

لجنة التقرير السنوي:

رئيس اللجنة:

السيد معتصم مرّيان

أعضاء اللجنة:

المهندس صهيب الروسان

المهندسة سوزان بني مصطفى

المهندس علاء الكساسبة

السيدة سارة الصرايرة

تصميم وإعداد:

الآنسة سارة الملكاوي

www.ncsc.jo