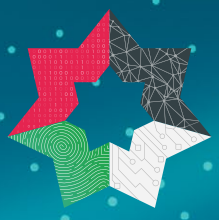
نسخة عام 2023

التقرير السنوي

فيديو الإنجازات



المركز الوطني
للأمن السيبراني
National Cyber
Security Center

نسخة

2023

التقرير السنوي

حضرة صاحب الجلالة الهاشمية

الملك عبدالله الثاني بن الحسين

المعظـم

صاحب السمو الملكي

الأميـر الحسيـن بـن عبدالله الثانـي

ولي العهـد المعظـم

المحتويات:

بالإمكان النقر على العنوان للذهاب إلى الصفحة المطلوبة

كلمـــة عطوفـــة رئيـــس المركـــز الوطنـــي للأمـــن السيبرانـــي

بالرغم من حداثة إنشاء المركز الوطني للأمن السيبراني، الا أن المركز استطاع خلال السنوات القليلة الماضية أن يؤطر ويُرسخ دورهُ الأساسي كجهة تنظيمية ورقابية على المستوى الوطني وكجهة مرجعية لكل القضايا المتعلقة بأمن الفضاء السيبراني الأردني وقد جاء التقرير السنوي الثاني لإبراز إنجازات المركز للعام الثالث والعشرين بعد الألفية الثانية والتي جاءت بحصيلة مضمونة استكمالاً للخُطى الثابتة التي كُنا قد أرسينا قواعدها في العام ٢٠٢٢م، واستكمالاً للنهج الذي عاهدناكم وأنفسنا عليه بأن نعمل بكل ما أُوتينا من عزيمةٍ وعلمٍ ومعرفة لتأمين الفضاء السيبراني الأردني وتعزيز مرونته السيبرانية بوجه كل من تُسّول له نفسه العبث بأمنه واستقراره، جاعلين منه وبالتعاون مع الشركاء فضاءً أردنياً رقمياً يُشار إليه بالبنان كركيزة أساسية مُساندة لمحركات النمو الاقتصادي الوطني، مُعززة للرفاه المُجتمعي، قادر على توفير متطلبات الأمن والحماية السيبرانية لكافة مستخدميه من الأفراد والمؤسسات

وعلى ذات النهج سارت خُطانا التي وُجهت لخلق فضاء سيبراني أردني قادر على التعلم ذاتياً قابل للتطور والتحسين المستمر، ضمن أربعة أولويات استراتيجية تُمكننا من الإدارة الحكيمة للفضاء السيبراني الأردني، كان أولها «أولوية البناء» التي سعينا من خلالها لتأسيس قدرات المركز عملياتياً، فنياً، وإدارياً ليكون منارةً أردنية قادرة على الإيفاء بمتطلباتها الوطنية بأعلى درجات الإحترافية في الأداء، وتلاها «أولوية الاستجابة» التي عملنا من خلالها على تمتين قدرات الفضاء السيبراني الأردني بما يكفل التحري الدقيق والكشف المبكر والاستجابة الفعالة للحوادث والتهديدات السيبرانية التي يتعرض لها الفضاء السيبراني الأردني وأُصوله الرقمية، وكانت أولوياتها الثالثة «أولوية الصّمود» والتي عملنا من خلالها على تفعيل دورنا الوطني لتمكين منشآتنا الحيوية وخدماتنا الرقمية الأساسية في التكيف و الصّمود في وجه أي تهديدات أو هجمات سيبرانية قد تتعرض لها من خلال الإدارة الاستباقية في التعامل مع المخاطر السيبرانية، وتطوير الأطر والسياسات والتعليمات الوطنية موجبة التنفيذ والمساءلة لكافة القطاعات الوطنية، أما أولويتنا الرابعة «أولوية التعاون» والتي أدركنا باكراً أهميتها، حيث لا يمكننا إدارة الفضاء السيبراني الأردني بمعزل عن التشاركية مع المؤسسات الوطنية في القطاعين العام والخاص، وكذلك التعاون على المستويين الإقليمي والدولي

ختاماً فأننا نتضرع الى المولى عز وجل أن يبقى هذا الوطن واحةَ أمن وأمان واستقرار تحت ظل راعي مسيرتنا المظفرة جلالة الملك عبد الله الثاني بن الحسين المعظم حفظة الله ورعاه وأن يديم الفضاء السيبراني الأردني منيعاً آمناً

رئيس المركز الوطني للأمن السيبراني

المهندس بسام تيسيـر المحارمـــة

التوجـه الاستراتيجـــي

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.

الاستجابـــة

نسعى لخلق منظومة وطنية متطورة ومستدامة لإدارة العمليات السيبرانية على المستوى الوطني، وبما يضمن التحري الحقيق 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.

الصّمـــود

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.

التعـــاون

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

صفحة المحتويات

التوجــه الاستراتيجــي (٢٠٢٤-٢٠٢٦)

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.

القيم الجوهرية

- احــترافـيـــة الأداء
- تــداول المعرفـــة
- التعلـــم المستمـر
- استشراف المستقبل
- المرونـة المؤسسيـة

الأهـداف الاستراتيجيــة للمركــز

الهدف الاستراتيجي الأول:

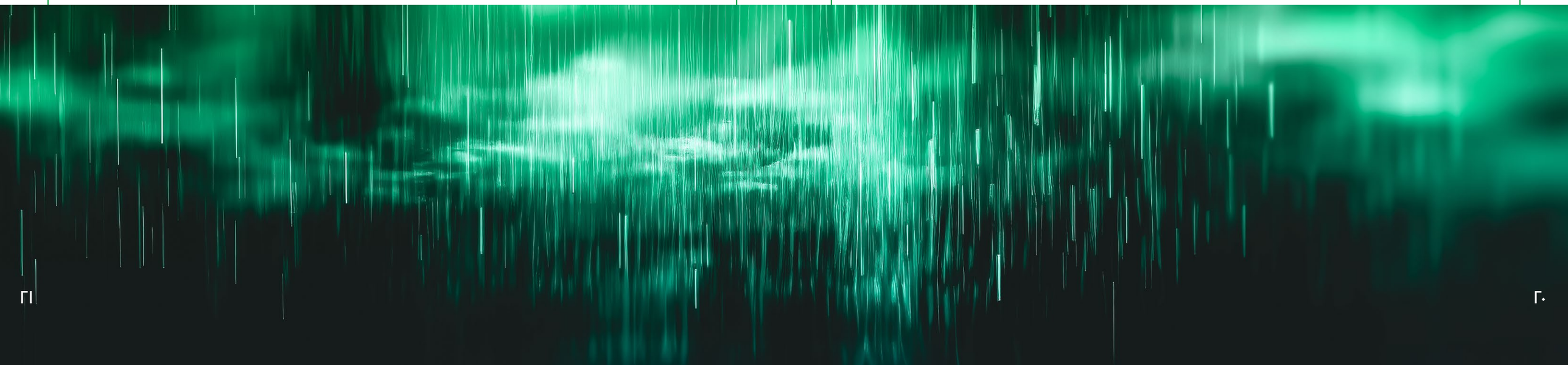
تعزيز القدرات المؤسسية للمنظومة الداخلية للمركز وبما يساهم برفـع كفـــاءة المركــز في تقديــم خدماتـــه وإدارة عملياتـــه.

- تعزيز القدرات المؤسسية للمنظومة الداخلية للمركز وبما يساهم برفع كفاءة المركز في تقديم خدماته وإدارة عملياته.
- تنمية وتدريب وتطوير الموارد البشرية ورفع كفاءتها.
- تعزيز الأداء المؤسسي وتقييمه.

الهدف الاستراتيجي الثانـي:

استدامــة إدارة العمليات السيبرانيــة بكفـاءة وفاعليـة

- 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.



الأهـداف الاستراتيجيــة للمركــز

الهدف الاستراتيجي الثالـث:

قطاعات بنى تحتية وطنية مرنة سيبرانياً وقادرة على الصّمود في وجه الهجمات السيبرانية مع نهايـــة عـــام ٢٠٢٦.

- 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 المركـز

- 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.

الهيكل التنظيمي

الرئيس

- مكتب الرئيس
- وحدة الرقابة الداخلية
- وحدة الشؤون القانونية
- وحدة التطوير المؤسسي و إدارة المشاريع

إدارة العمليات والاستخبارات السيبرانية

- مديرية العمليات السيبرانية
- مديرية الاستخبارات السيبرانية والموقف الأمني
- مديرية العمليات الفنية

مديرية الشؤون المالية

مديرية الموارد البشرية والشؤون الإدارية

إدارة السياسات والتعاون والتدريب

- مديرية التدريب والتطوير
- مديرية الاتصال والتعاون
- مديرية السياسات والامتثال

نشأة المركز

تم إقرار قانون الأمن السيبراني رقم ١٦ لسنة ٢٠١٩، بتاريخ ١٦ أيلول ٢٠١٩ 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 (٥) من قانون الأمن السيبراني الأردني رقم ١٦ لعام ٢٠١٩، 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.

صفحة المحتويات

المهـام والصلاحيـات

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

٢) 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.

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

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

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

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

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

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

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

١٠) تحديد شبكات البنى التحتية الحرجة ومتطلبات استدامتها.

١١) إنشاء قاعدة بيانات بالتهديدات السيبرانية.

١٢) تقييم النواحي الأمنية لخدمات الحكومة الإلكترونية.

١٣) تقييم وتطوير فرق الاستجابة لحوادث الأمن السيبراني.

١٤) إعداد سياسة تتضمن معايير أمن وحماية المعلومات.

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

١٦) إجراء تمارين ومسابقات للأمن السيبراني.

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

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

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

الأدوار الرئيسيــة للمركـز علـى المستـوى الوطنـي

الدور التنظيمــي/الرقابــي

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 العمـليـاتـــي

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.

3

الخدمات الرئيسية

التـــــي

يقدمهـا المركـــز

إدارة العمليــات السيبرانيــة

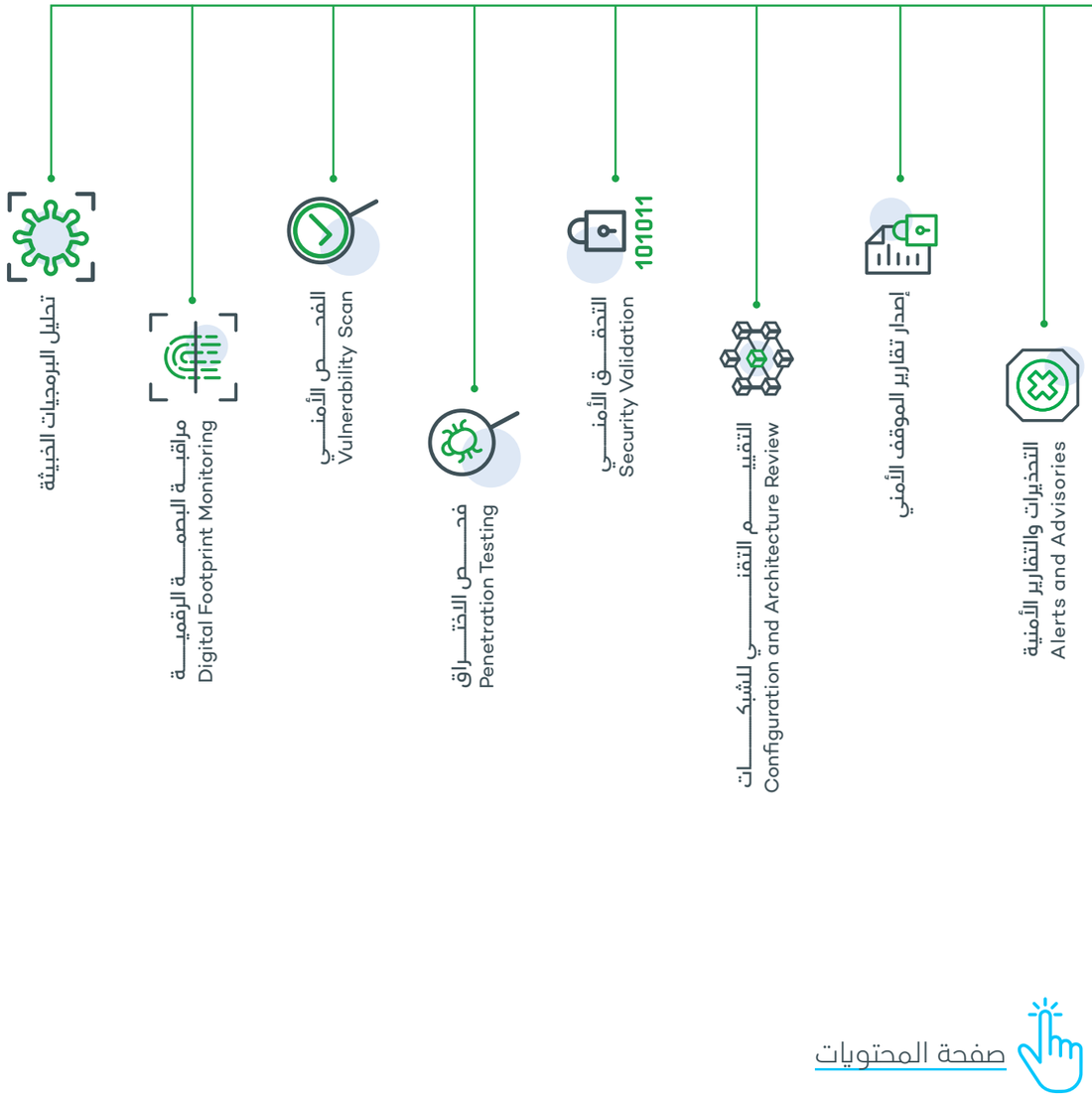
يعمل المركز على تعزيز حماية الفضاء السيبراني، وتحقيق الأمن والثقة لبياناته وأصولها الرقمية، من خلال عمليات المراقبة والتحليل للشبكات والأنظمة الحكومية، بهدف رصد واكتشاف أية حوادث سيبرانية تتعرض لها، كما ويقوم المركز بالتعامل مع الحادثة السيبرانية بعد وقوعها، بما في ذلك التحقيق في الحادثة، وتقييم الاضرار الناتجة عنها، واحتواء اثارها السلبية، وتقديم التقارير والتحليلات لتجنب تكرار وقوع ذات الحادثة مرة أخرى مستقبلاً.

حيث يعمل المركز على ذلك من خلال عملياته الرئيسية التالية:

الاستخبــارات السيبرانيــة

حيث يعمل المركز على جمع المعلومات السيبرانية وتحليلها لتكوين فهم شمولي للتهديدات والتحديات السيبرانية الأمنية التي تهدد الفضاء السيبراني الأردني، بما في ذلك الهجمات السيبرانية والأنشطة الخبيثة والثغرات الأمنية والتهديدات السيبرانية المتوقعة والمتطورة، التي تهدف إلى الاختراق أو التلاعب أو الضرر بمكونات الفضاء السيبراني الأردني، وبما يُمكن المركز من تقديم تصور شمولي للموقف الأمني سيبرانياً على المستوى الوطني.

حيث يعمل المركز على تحقيق ذلك من خلال عملياته الرئيسية التالية:



صفحة المحتويات

حوكمــة الأمــن السيبرانــي

يعمل المركز على بناء وتطوير مجموعة من الأُطر والسياسات والتشريعات والتعليمات التي تعزز أمن الفضاء السيبراني الأردني، وبما يضمن توفير الأُطر التشريعية مُلزمة التنفيذ موجبة المساءلة.

حيث يعمل المركز على تحقيق ذلك من خلال عملياته الرئيسية التالية:

بناء وتعزيز القدرات السيبرانية الوطنية

يعمل المركز على بناء القدرات الوطنية، ورفع مستوى الوعي والمعرفة في الأمن السيبراني، على المستوى الوطني، ولكافة الشرائح المجتمعية، حيث يعمل المركز على تحقيق ذلك من خلال عملياته الرئيسية التالية:

- التوعيــة والتثقيــف
- التدريــب وبنــاء المهــارات
- بناء العلاقات التعاونية والتشاركية

الإنجـازات ٢٠٢٣

في هذا الجزء من تقريرنا السنوي، سنعرض أهم الإنجازات التي حققها المركز تفصيلاً خـــلال العـــام ٢٠٢٣، حيـــث سنـــورد إنجازاتنـــا ضمـــن أربعـــة محـــاور رئيسيـــة:

وهي البنـــاء، الاستجابـــة، الصّمـــود والتعـــاون

1

البنـــاء

صفحة المحتويات

البنـــاء

على مدار عام، سعينا لتطوير البنية الفنية والعملياتية والإدارية للمركز، والرفع من كفاءتها، وتمتينها من خلال رفدها بأحدث الأدوات التكنولوجية والفنية التي تضمن جودة عملياتنا الداخلية في المركز، والتي من خلالها سنتمكن من تقديم خدماتنا السيبرانية بأعلى درجات الكفاءة والفاعلية، كما ولم نغفل عن أهمية الاستثمار بمواردنا البشرية، من خلال تنمية قدراتهم، والرفع من مهارتهم المعرفية ، انطلاقاً من إيماننا بأن أهم مورد يملكه المركز هو رأس ماله البشري، فعلى صعيد البناء تمكنا خلال عام ٢٠٢٣، من:

- تجهيز غرفة البيانات الرئيسية (Data center)، حيث تم تأسيس غرفة البيانات الرئيسية للمركز، استناداً لأحدث الأطر العالمية في مجال تأسيس وتشغيل مراكز البيانات، وكان ذلك بهدف إيجاد بيئة عمل شمولية، متكاملة ومتطورة، لإدامة عمل أجهزة وخوادم المركز والأنظمة العاملة فيه، كما تم تزويدها بنظام متطور لإطفاء الحريق ووحدات تكييف مركزية.

- **تحديث الأنظمة العاملة والخوادم**، تم تحديث الأنظمة واجهزة الخوادم (servers) العاملة في المركز ورفع قدرتها التخزينية والعملياتية، وبما يتماشى مع متطلبات التوسع في تقديم الخدمات السيبرانية على المستوى الوطني، كما تم العمل على تفعيل Exchange server، تمهيداً لفصل البريد الالكتروني الخاص بالعاملين على خوادم المركز الرئيسية، وإدارته بشكل كامل من قبل مديرية العمليات الفنية.

- تفعيل نظام المصادقة متعددة العوامل Multi-factor Authentication (MFA)، بهدف توفير الحماية الرقمية للأجهزة والأنظمة العاملة في المركز، حيث يضمن هذا النظام التحقق من هوية المستخدم قبل السماح له بالوصول إلى نظام أو جهاز أو خدمة معينة.

- العمل على استدامة توافر بيانات ومعلومات المركز، وحمايتها من العبث أو التخريب، حيث تم استحداث خادم جديد في المركز، بهدف توفير خدمات سحب النسخ الاحتياطية للأنظمة بشكل منتظم ودوري، وبحماية عالية جدا بحيث تمنع عمليات الوصول غير المصرح بها للبيانات والمعلومات.

- تم تطوير موقع التوظيف الخاص بالمركز (post.ncsc.jo) للتماشي مع الآلية المتبعة لتقديم طلبات التوظيف في المركز بطريقة آمنه وسلسة.

- **إطلاق منصة «شارك»** والتي يتم من خلالها تبادل المعلومات وتشارك التحذيرات والتنبيهات وأية معلومات تحتاجها فرق المركز المختلفة وأصحاب المصلحة والعلاقة.

- **تركيب مولدات طاقة كهربائية** عدد (٢) من نوع (KOHLER) بقدرة kva (٥٠٠) تعمل في حالات انقطاع التيار الكهربائي عن المركز.

- تم استحداث نظام UPS متكامل تم تصميمه على احدث الطرق العالميه في هذا المجال يعمل كمصدر للطاقة الاحتياطية لضمان بقاء الأجهزة وأنظمة المعلومات قيد التشغيل عند حدوث انقطاع أو تذبذب في التيار الكهربائي.

2

الاستجابة

العمليـــات السيبرانيـــة

● تشكيل الفريق الوطني للاستجابة لحوادث الأمن السيبراني

JoCERT (Jordan computer Emergency Response Team)

JO|CERT

التوسع في تقديم الخدمات السيبرانية للمؤسسات الوطنية

تم التوسع في تقديم خدمة المراقبة والتحليل على مدار الساعة للشبكات الحكومية وإدارة سجلاتها والحركات الرقمية، حيث تم إضافة ما مجموعه (٤٣) مؤسسة جديدة على نظام – Security information and event management SIEM، وبنسبة زيادة بلغت (١٠٨٪) مقارنة بعدد المؤسسات على النظام لعام ٢٠٢٢ ، حيث يُمَكّن هذا النظام المركز 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.

نفذ المركز خـــلال الربـــع الأخيـــر مـــن عام٢٠٢٣ للمؤسسات الحكومية مشـــروع (Network Detection and Response)

حيث تم ربط ما مجموعه (٢٠) مؤسسة حكومية على النظام خلال المرحلة الأولى من المشروع، وكان ذلك بهدف توفير طبقة إضافية من الأمان للأصول الرقمية العاملة في تلك المؤسسات من أية تهديدات أو اختراقات سيبرانية، وتمكينهم من رصد التهديدات السيبرانية التي قد يتعرضون لها و ضمان استجابة فعالة للحوادث السيبرانية التي قد تستهدف الشبكات لديهم،

حيث يُمكن النظام المؤسسات من:

- **رصد حركة البيانات (Traffic monitoring)**، من خلال مراقبة حركة البيانات داخل الشبكة للكشف عن أية أنماط غير عادية أو مشبوهة على تلك الشبكات.

- **تحليل السلوك (Behavior analysis)**، يقوم النظام على تحليل سلوك مستخدمي الأجهزة والأنظمة والتطبيقات، للكشف عن أية حركات غير اعتيادية تشير لوجود هجمات سيبرانية.

- **الكشف عن التهديدات المتطورة (advanced threat detection)**، حيث يستخدم النظام تقنيات متطورة للكشف عن التهديدات السيبرانية المتطورة التي تستهدف الأنظمة والشبكات.

- **الاستجابة الآلية (Automated Response)**، يمكن للنظام أن يتخذ أية إجراءات آلية للتعامل مع التهديدات المكتشفة، مثل عزل الشبكة والأنظمة المصابة، أو تقديم تقارير تفصيلية لإتخاذ 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 اكثر دقة وفعالية.

الحوادث السيبرانية 2023

شديـدة الخطـورة

Q4	Q3	Q2	Q1
0	3	5	12

خطيـــرة

Q4	Q3	Q2	Q1
20	117	103	132

- (٣٦٪) من هذه الحوادث السيبرانية تمت بهدف تنفيذ عمليات التجسس وقرصنة البيانات والمعلومات الرقمية.
- قام المركز بتحليل ما مجموعه (١٠٦) دليل رقمي، مرتبطة ب(٤٥) حادثة سيبرانية تطلبت عمليات الاستجابة لها جمع للأدلة الرقمية المرتبطة بالحادثة ، بالمقارنة بتحليل (٣٨) دليل رقمي لعام ٢٠٢٢.

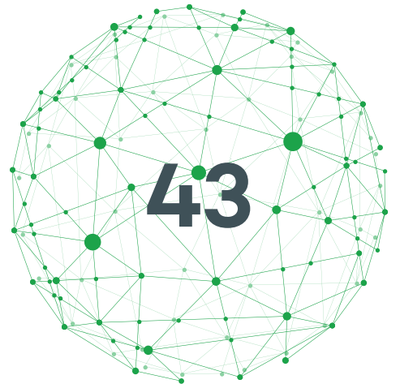
متوسطـة الخطـورة

Q4	Q3	Q2	Q1
703	296	355	375

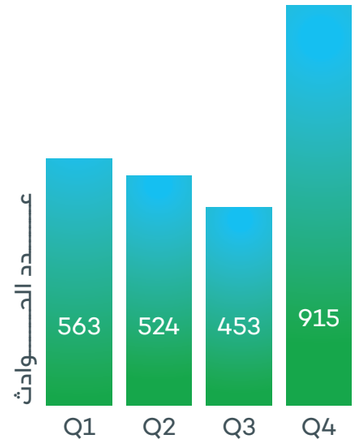
منخفضـة الخطـورة

Q4	Q3	Q2	Q1
192	37	61	44

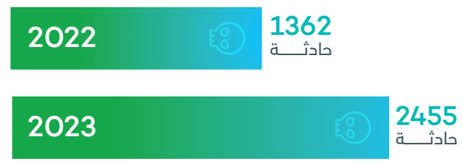
- تم تقييم (٤٣) شبكة ونظام تابعة للمؤسسات المربوطة على نظام مراقبة سجلات الاحداث (SIEM)، مقارنة بـ(٣٢) شبكة ونظام لعام ٢٠٢٢.



- تعامل المركز مع (٢٤٥٥) حادثة سيبرانية تعرض لها الفضاء السيبراني عام (٢٠٢٣)، أي بنسبة زيادة وصلت إلى (٨٠٪) مقارنة بعام ٢٠٢٢.



(٩٤٪) من هذه الحوادث تم اكتشافها ورصدها من خلال عمليات المراقبة والتحليل في المركز، وهذا ما يفسر نسبة الزيادة في الحوادث السيبرانية مقارنة بعام ٢٠٢٢.



- أصدر المركز (٢٦٠٩) تحذير سيبراني بناءً على الحوادث السيبرانية التي تم رصدها أو اكتشافها، مقارنة بـ(٩٢) تحذير سيبراني عام ٢٠٢٢.
- (٤٪) من الحوادث السيبرانية التي تم رصدها، تطلبت تواجد فريق الاستجابة الوطني JoCERT، وتم بناءً عليه اصدار ما مجموع (٤٧) تقرير مرتبط بتلك الحوادث.
- يتم التعامل مع الحوادث السيبرانية التي يتم رصدها داخلياً في المركز، أو ابلاغ المركز عنها من خلال فرق الاستجابة للحوادث السيبرانية الداخلية في المركز استناداً لتصنيف الحادثة السيبرانية، وعلى النحو التالي:

(١٪) من الحوادث التي تعرض لها الفضاء السيبراني الأردني صُنفت بحوادث (شديدة الخطورة) مقارنة بما نسبته (٢،٢٪) لعام ٢٠٢٢، حيث تُصنف الحادثة السيبرانية بشديدة الخطورة إذا أدت إلى تعطل الخدمات الأساسية بشكل كامل أو تسريب أو تدمير أو مسح للبيانات الحساسة ويكون تأثيره واضح على أكثر من بنية تحتية حرجة أو على أكثر من ثلث سكان المملكة.

(١٥٪) من الحوادث السيبرانية التي تعرض لها الفضاء السيبراني الأردني صُنفت بحوادث (خطيرة)، حيث تصنف الحادثة السيبرانية بحادثة خطرة، في الحالات التالية:

١. إذا كان مصدر الحادثة البرمجيات الخبيثة أو اختراق الشبكات والتي تؤثر على جزء محدود من الخدمات أو محاولات الاختراق غير المؤثرة على البيانات الحساسة والخدمات وكان الحادث على أكثر من بنية تحتية حرجة أو على أكثر من ثلث سكان المملكة.

٢. إذا كانت الحادثة السيبرانية تؤدي إلى تعطل الخدمات الأساسية بشكل كامل أو محدود أو تسريب أو تدمير أو مسح للبيانات الحساسة أو البرمجيات الخبيثة أو اختراق الشبكات وكان الحادث يقع على أي من الجهات التالية (بنية تحتية حرجة / أجهزة امنية / الوزارات والمؤسسات الحكومية/ الشركات المملوكة للحكومة أو التي تساهم فيها/ سلاسل التزويد التي تزود تلك الجهات).

٣. الحادثة السيبرانية التي تؤدي إلى تعطل كامل للخدمات الأساسية وكان تأثيره على مؤسسات التعليم العالي.

(٧٠٪) من الحوادث السيبرانية التي تعرض لها الفضاء السيبراني صُنفت بحوادث متوسطة الخطورة.

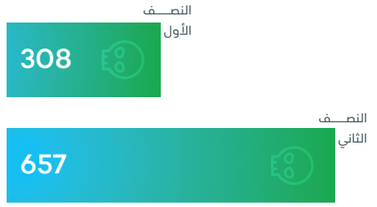
(١٤٪) من الحوادث السيبرانية التي تعرض لها الفضاء السيبراني صُنفت بحوادث منخفضة الخطورة.

العمليـــات السيبرانيـــة

الحوادث السيبرانية التي تعرض لها الفضاء السيبراني تفصيلاً:

• تم التعامل مع (٢٤٣) محاولة اختراق للمواقع الإلكترونية التابعة للمؤسسات الحكومية، مقارنة بـ(٦٩) حالة في عام ٢٠٢٢.

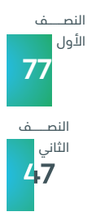
• (٥٩٪) من الحوادث التي تعرض لها الفضاء السيبراني الأردني عام ٢٠٢٣ ارتبطت بالفيروسات والبرمجيات الخبيثة.



• (١٠٪) كان سببها عدم التقيد بالسياسات والتوصيات المتعلقة بأمن المعلومات policy violation.

• (٦٪) من الحوادث التي تعرض لها الفضاء السيبراني الأردني عام ٢٠٢٣ ارتبطت بمجموعات التهديد المتطورة APT، مقارنة بـ(٥٫٢١٪) لعام ٢٠٢٢.

• (٥٪) من الحوادث التي تعرض لها الفضاء السيبراني الأردني عام ٢٠٢٣ ارتبطت ببرامج الفدية Ransomware.



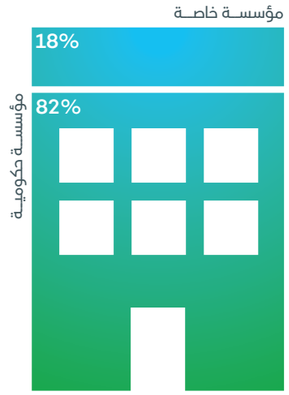
• (٤٪) من الحوادث التي تعرض لها الفضاء السيبراني الأردني عام ٢٠٢٣ ارتبطت بحملات تصيد Phishing، مقارنة بـ(٢٫٨٪) عام ٢٠٢٢.

	النصف الأول	النصف الثاني
الفيروسات والبرمجيات الخبيثة	٨٠٣	٦٥٧
السياسات والتوصيات المتعلقة بأمن المعلومات Policy Violation	١٦١	٦٤
بمجموعات التهديد المتطورة APT	٤٧	٨٩
ببرامج الفدية Ransomware	٧٧	٤٧
بحملات تصيد Phishing	٧١	٢٦

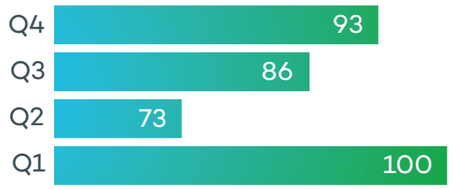
العمليـــات السيبرانيـــة

المؤسسات التي تعرضت لحوادث أمن سيبراني عام ٢٠٢٣

• تعرضت (١١٩) مؤسسة حكومية وخاصة لحوادث أمن سيبراني عام ٢٠٢٣، منها (٨٢٪) مؤسسات حكومية.



• (٩٣٪) من المؤسسات تعرضت لأكثر من حادثة سيبرانية خلال العام.



عدد المؤسسات التي تعرضت لحوادث سيبرانية **(مع التكرار)**

• (٣٪) من هذه المؤسسات تعرضت لأكثر من (١٠٠) حادثة سيبرانية خلال العام.

• (٧٪) من هذه المؤسسات تعرضت لأكثر من (٥٠) حادثة سيبرانية خلال العام.

• (١٣٪) من هذه المؤسسات تعرضت لأكثر من (٢٥) حادثة سيبرانية خلال العام.

	عدد المؤسسات	عدد الحوادث
الربـــع الأول	٩١	٥٦٣
الربـــع الثاني	٨٦	٥٢٤
الربـــع الثالث	٧٣	٤٥٣
الربـــع الرابع	١٠٠	٩١٥

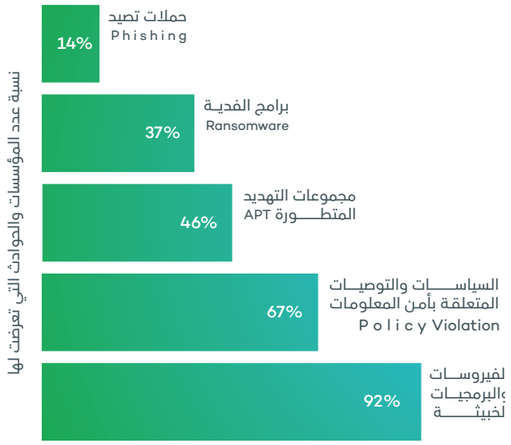
• (٤٦٪) من هذه المؤسسات تعرضت لحوادث مرتبطة بمجموعات التهديد المتطورة APT.

• (٣٧٪) من هذه المؤسسات تعرضت لحوادث مرتبطة ببرمجيات الفديـة Ransomware.

• (٩٢٪) من هذه المؤسسات تعرضت لحوادث مرتبطة بالفيروسات والبرمجيات الخبيثة.

• (٦٧٪) من هذه المؤسسات تعرضت لحوادث سببها عدم التقيد بالسياسات والتوصيات المتعلقة بأمن المعلومات policy violation.

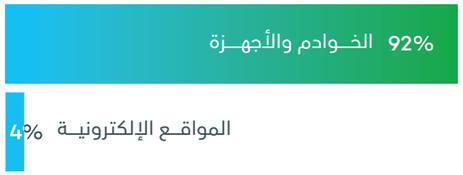
• (١٤٪) من هذه المؤسسات تعرضت لحوادث مرتبطة بحملات تصيد Phishing.



الاستخبـارات السيبرانيـــة

عمليـات الفحــص الأمنـي

• نفذ المركز ما مجموعه (١١٠٠٤) عملية فحص أمني للأصول الرقمية والتكنولوجية التابعة للمؤسسات الوطنية، (٩٦٪) من عمليات الفحص استهدفت الخوادم والأجهزة، و (٤٪) استهدفت المواقع الإلكترونية.



• تم اكتشاف (٣٨٥٠٤١) ثغـرة أمنيـة بنـاءً على عمليـات الفحـص الأمني.

	عـدد عمليـات الفحص الأمني	عدد الثغرات
الربـع الأول	١٩٩٠	٧٦٦٣٧
الربـع الثاني	٤٠٥٤	٩٩٢٩٧
الربـع الثالث	١٠٥٦	٨٣٤٤١
الربـع الرابع	٣٩١٣	١٢٥٦٦٦

المواقـع الإلكترونيـة

• تم رصد (٢٥٠٢) ثغرة أمنية على المواقع الإلكترونية بناءً على عمليات الفحص الأمني.

• (٦٣٪) من المواقع الإلكترونية التي تم تنفيذ عمليات الفحص الأمني لها مستضافة لدى مركز البيانات الحكومي، رُصد عليها ما نسبته (٦٢٪) من الثغرات الأمنية المكتشفة على المواقع الإلكترونية.

• بلغ عدد الثغرات الأمنية المكتشفة على المواقع الإلكترونية غير المستضافة لدى مركز البيانات الحكومي (٩٥٢) ثغرة أمنية.

	عـدد المواقع الإلكترونيـة	عـدد الثغرات المكتشفـة
الربـع الأول	١٠٥	٦٧٩
الربـع الثاني	٦٤	٣٥٠
الربـع الثالث	٨٨	٧٠٨
الربـع الرابع	١١٢	٧٦٥

الاستخبـارات السيبرانيـــة

الخـوادم والأجهـــزة

• تم رصد ما مجموعه (٣٨٢٥٣٩) ثغرة على الخوادم والأجهزة بناءً على عمليات الفحص الأمني، التي نُفذت على ما مجموعه (١٠٩٤١) من الأجهزة والخوادم.

• (٦٠٪) من الثغرات المكتشفة رُصدت على خوادم الخدمات الحرجة في مركز عمليات الحكومة الإلكترونية التي تم إجراء الفحص الأمني لها، حيث قام المركز بفحص ما مجموعه (٥٢١٣) من هذه الأجهزة والخوادم.

• تم اكتشاف (١٥٣٧١٠) ثغرة امنية على الخوادم الأخرى في مركز عمليات الحكومة الإلكترونية والمشاريع الخارجية التي تم إجراء الفحص الأمني لها.

	عـــدد المواقـع الخوادم والأجهزة	عدد الثغرات المكتشفـة
الربـع الأول	١٨٦٧	٧٥٩٥٨
الربـع الثاني	٣٩١٩	٩٨٩٤٧
الربـع الثالث	١٤٦٠	٨٢٧٣٣
الربـع الرابع	٣٦٩٥	١٢٤٩٠١

3

الصّمـــود

انطلاقاً من إدراك المركز لأهمية ترسيخ مبادئ المرونة السيبرانية للفضاء الرقمي الأردني، وتعزيز قدرته على الصّمود أمام أية تهديدات أو هجمات سيبرانية يتعرض لها، وبما يضمن استمرارية تقديم الخدمات الوطنية الرقمية التي ترتكز على أمن الفضاء السيبراني الأردني، ومرونة مكوناته المادية والتكنولوجية بالتعامل مع أية مخاطر أو هجمات سيبرانية تتعرض لها، عمل المركز خلال عام ٢٠٢٣ على ثلاثة محاور رئيسية تضمن ترسيخ مبادئ المرونة السيبرانية وهي:

١. حوكمة الأمن السيبراني على المستوى الوطني
٢. الإدارة الإستباقية في التعامل مع التهديدات السيبرانية
٣. تنمية القدرات الوطنية

١. حوكمـة الأمـن السيبرانـي علـى المستوى الوطنـي

● أنهى المركز خلال عام ٢٠٢٣ إعداد مسودة الإطار الوطني للأمن السيبراني وتم طرحها للاستشارة العامة، تمهيداً للسير بالإجراءات الناظمة لتعميمه على كافة المؤسسات والوزارات والهيئات الحكومية والخاصة، ليتخذ صفة الزامية التطبيق ووجوب المساءلة.

حيث تم عقد جلستين للتشاور بناءً على مخرجات مرحلة الاستشارة العامة، حضرها ما يزيد عن (١٠٠) شخص من أصحاب العلاقة والمعنيين. ومن الجدير بالذكر هنا، أن الإطار الوطني الأردني للأمن السيبراني، يهدف لتعزيز قدرة القطاعات الوطنية على التصدي للتهديدات والحوادث السيبرانية، وحماية الأصول الرقمية الحرجة المُشغلة للخدمات الأساسية على المستوى الوطني، حيث تضمن الإطار مجموعة من السياسات والإجراءات والتوجيهات التي تحدد الطرق السليمة التي يتم من خلال الامتثال لها حماية البيانات الرقمية، وسلامة أمنها، وبما يعزز صمود القطاعات الوطنية ويُمكّنها من مقاومة الآثار السلبية لأية حادثة سيبرانية قد تتعرض لها.

● قام المركز بتدريب موظفي (١٨٣) مؤسسة حكومية وخاصة، على مضمون الإطار الوطني الأردني للأمن السيبراني، حيث تم تدريب ما مجموعه (٢٠٢) موظف على المواضيع التالية:

• **دورة Framework Implementation**، تهدف الدورة لتوضيح الغاية من بناء الإطار الوطني للأمن السيبراني الأردني، وفهم قدرات ومكونات الإطار التي تساعد على بناء برنامج أمني يركز على الأعمال والمخاطر وفرص التطوير وتعزيز الأمن السيبراني.
• **دورة Framework Audit**، تهدف الدورة لتوضيح آلية تقييم مدى الالتزام والامتثال لمعايير وضوابط الإطار الوطني للأمن السيبراني الأردني من خلال مراجعة السياسات والاجراءات والضوابط والممارسات لضمان توافقها مع متطلبات وأهداف الإطار.

• **دورة ArchiMate**، تهدف الدورة لتوضيح مفهوم نمذجة الأعمال باستخدام برمجية ArchiMate ، من خلال استخدام أدوات لوصف وتحليل وتصور العلاقات والتفاعلات بين مكونات معمارية المؤسسة وتحديد مبدأ سير العمليات، وبما يساعد محللي الأمن السيبراني على تحليل عوامل المخاطر السيبرانية وتحديد طريقة ادارتها واحتوائها.

• **دورة Security Fundamentals**، تهدف الدورة لتكوين فهم سليم وشمولي في أساسيات الأمن السيبراني من مبادئ ومفاهيم وممارسات اساسية لحماية الأصول والأنظمة والشبكات الرقمية من التهديدات السيبرانية، كما وتشير الى تطوير البنية الأمنية القائمة على الأعمال وتحديد المخاطر المرتبطة بالهجمات السيبرانية وتقييمها والتخفيف من حدتها من خلال تنفيذ تدابير وضوابط استباقية وحلول تدعم أهداف العمل بشكل يمكن تتبعه

● نص قانون الأمن السيبراني رقم (٢٠١٩/١٦) في مضمون المادة (٤) «يتولى المجلس المهام والصلاحيات التالية...
أ. إقرار الاستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني»، واستناداً لأحكام المادة (٨/ب/أ) من ذات القانون، : «تلتزم الوزارات والدوائر الحكومية والمؤسسات الرسمية العامة والخاصة والأهلية باتباع السياسات والمعايير والضوابط الصادرة عن المركز لكل قطاع»، وعليه أصدر المركز خلال عام ٢٠٢٣ مايلي:

١. اصدار سياسة اعتماد منتجات الأمن السيبراني للوزارات والدوائر الحكومية، والتي جاء إصدارها بهدف ضمان سلامة سلاسل التوريد واستخدام المنتجات التكنولوجية و الرقمية الموثوق بها فقط، وذلك ادراكاً من المركز بأن أهم التهديدات التي تواجهها الشبكات المعلوماتية في جميع انحاء العالم، هي تلك المتأتية من سلاسل التوريد وما تعتريه من مخاطر ناتجة عن عدم وجود آليات للتحقق من موثوقية المنتجات والحلول. حيث جاءت هذه السياسة لتطبيق آليات واعتماد وتوظيف منتجات الأمن السيبراني في الجهات والوحدات الحكومية، ولتكن حجر الأساس التمهيدي لإعداد نظام وطني لاعتماد وترخيص جميع المنتجات والحلول الرقمية.

٢. إصدار معايير وضوابط الأمن السيبراني للجهات المتعاقدة مع الوزارات والدوائر الحكومية، والتي جاء إصدارها بهدف حماية البيانات والمعلومات الحكومية بكافة أنواعها وأشكالها ومستوى تصنيفها وفق سياسة تصنيف البيانات الحكومية لعام ٢٠٢٠، وقانون حماية أسرار ووثائق الدولة رقم (٥٠) لسنة ١٩٧١، حيث تضمنت هذه الضوابط حُسن إدارة أمن المعلومات الحكومية وحمايتها من أي دخول غير مشروع أو غير مصرح به، من قبل الجهات المُتعاقد معها

● بموجب المادة رقم (٦) من قانون الأمن السيبراني رقم (٢٠١٩/١٦) البند (٣/ب) أصدر المركز تعليمات تصنيف حوادث الأمن السيبراني لسنة ٢٠٢٣، حيث تم بمضمون هذه التعليمات تصنيف الحوادث التي يتعرض لها الفضاء السيبراني الأردني، تبعاً لنطاق تأثير الحادثة السيبرانية والجهات المتأثرة بها، وعلى النحو التالي:

• نطاق التأثير والتضمن:
- تعطل الخدمات الأساسية.
- تسريب أو تدمير أو مسح للبيانات الحساسة.
- البرمجيات الخبيثة أو اختراق الشبكات والتي تؤثر على جزء محدود من الخدمات.
- محاولات الاختراق غير المؤثرة على البيانات الحساسة والخدمات.
- عمليات المسح والاستطلاع المؤثرة على البيانات الحساسة والخدمات.

١. حوكمة الأمن السيبراني على المستوى الوطني

• الجهة المتأثرة:

- عدد قطاعات البنية التحتية الحرجة التي تأثرت بالحادثة السيبرانية.
- الأجهزة الأمنية والعسكرية.
- الوزارات والمؤسسات الحكومية.
- المؤسسات والشركات الخاصة.
- عدد سكان المملكة الذين تأثروا بالحادثة السيبرانية.
- سلاسل التزويد.
- الشركات المملوكة للحكومة أو التي تساهم فيها.

● نظام ترخيص مقدمي خدمات الأمن السيبراني

أنهى المركز خلال عام ٢٠٢٣ إعداد مسودة نظام ترخيص مقدمي خدمات الأمن السيبراني، والذي جاء إعداده بهدف تنظيم خدمات الأمن السيبراني في المملكة وضمان جودة الخدمات المقدمة من خلال الإشراف والرقابة والتحقيق على مقدم الخدمة بما يحفظ حقوق متلقي الخدمة ومقدمها، والنظام حالياً في عهدة ديوان التشريع والرأي لغايات اقراره بصورته النهائية استناداً للأصول التشريعية الناظمة لذلك.

● تعليمات معايير المخالفات وضوابطها والإجراءات المستحقة

أنهى المركز خلال عام ٢٠٢٣ إعداد مسودة تعليمات معايير المخالفات وضوابطها والإجراءات المستحقة، وذلك بهدف تمكين المركز من القيام بدوره في تنظيم سجل للمخالفات يُحدّد فيه اسم المخالف وتاريخ المخالفة ونوعها ووصف دقيق لها والقرار المتخذ بحق المخالف وأية بيانات أخرى يراها المركز ضرورية، والتعليمات حالياً في عهدة المجلس الوطني للأمن السيبراني، ليتم اقراره من خلالهم استناداً للصلاحيات الممنوحة للمجلس.

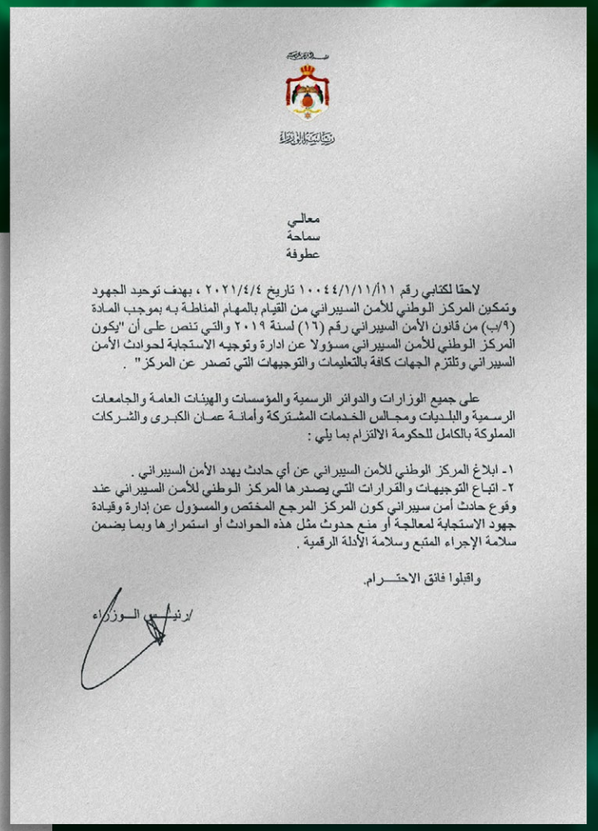
● المشاركة في إعداد تشريعات وأنظمة والتعليمات الوطنية ذات العلاقة

قانون حماية البيانات الشخصية رقم ١٧ لسنة ٢٠٢٣ (تعليمات التدابير الأمنية والتقنية والتنظيمية وتعليمات سجل حماية البيانات الشخصية ونظام الإفصاح عن البيانات ونظام حقوق الشخص المعني وإجراءات الموافقة المسبقة وسحبها).

● إقليمياً، شارك المركز في إعداد مشروع القانون العربي الاسترشادي (جامعة الدول العربية).

● عالمياً، شارك المركز في إعداد مسودة الاتفاقية الشاملة لمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية (الأمم المتحدة).

التعـــاميـــم



معالي
سماحة
عطوفة

لاحقا لكتابي رقم ١٠٠٤٤/١/١١/١١ تاريخ ٢٠٢١/٤/٤ ، بهدف توحيد الجهود وتمكين المركز الوطني للأمن السيبراني من القيام بالمهام المناطة به بموجب المادة (٩/ب) من قانون الأمن السيبراني رقم (١٦) لسنة ٢٠١٩ والتي تنص على أن "يكون المركز الوطني للأمن السيبراني مسؤولا عن ادارة وتوجيه الاستجابة لحوادث الأمن السيبراني وتلتزم الجهات كافة بالتعليمات والتوجيهات التي تصدر عن المركز" .

على جميع الوزارات والدوائر الرسمية والمؤسسات والهيئات العامة والجامعات الرسمية والبلديات ومجالس الخدمات المشتركة وأمانة عمان الكبرى والشركات المملوكة بالكامل للحكومة الالتزام بما يلي :

١- ابلاغ المركز الوطني للأمن السيبراني عن أي حادث يهدد الأمن السيبراني .
٢- اتباع التوجيهات والقرارات التي يصدرها المركز الوطني للأمن السيبراني عند وقوع حادث أمن سيبراني كون المركز المرجع المختص والمسؤول عن إدارة وقيادة جهود الاستجابة لمعالجة أو منع حدوث مثل هذه الحوادث أو استمرارها وبما يضمن سلامة الإجراء المتبع وسلامة الأدلة الرقمية .

واقبلوا فائق الاحتـــرام.

رئيس الوزراء

المركز الوطني للأمن السيبراني
National Cyber Security Center

• بموجب كتاب رئيس الوزراء رقم 99719/1/11/11 تاريخ 2023/1/1 تم التعميم على جميع وزارات الدولة والدوائر الرسمية والمؤسسات والهيئات العامة والجامعات الرسمية والبلديات ومجالس الخدمات المشتركة وامانه عمان الكبرى والشركات المملوكة بالكامل للحكومة الالتزام بما يلي:

- ابلاغ المركز الوطني للأمن السيبراني عن أي حادث يهدد الأمن السيبراني.
- اتباع التوجيهات والقرارات التي يصدرها المركز الوطني للأمن السيبراني عند وقوع حادث أمن سيبراني كون المركز المرجع المختص والمسؤول عن إدارة وقيادة جهود الاستجابة لمعالجة أو منع حدوث مثل هذه الحوادث او استمرارها وبما يضمن سلامة الاجراء المتبع وسلامة الأدلة الرقمية.

• بموجب كتاب رئيس الوزراء رقم 52334/1/11/11 تاريخ 2023/9/21 تم التعميم على جميع وزارات الدولة والدوائر الرسمية والمؤسسات والهيئات العامة تكثيف الأنشطة التوعوية المتعلقة بالأمن السيبراني خلال شهر أكتوبر ونشر مواد توعوية على صفحاتها الرسمية على منصات التواصل الاجتماعي واستخدام الوسم (الهاشتاق) الخاص بهذا الشهر (# شهر التوعية بالأمن السيبراني) عند نشر أي مواد ونصائح أمنية خاصة بالأمن السيبراني ورفع رابط منصة على المواقع الالكترونية الخاصة بها مع إمكانية الاستعانة بالمركز الوطني للأمن السيبراني عند تنظيم أي فعاليات او أنشطة تتعلق بالتوعية بالأمن السيبراني.

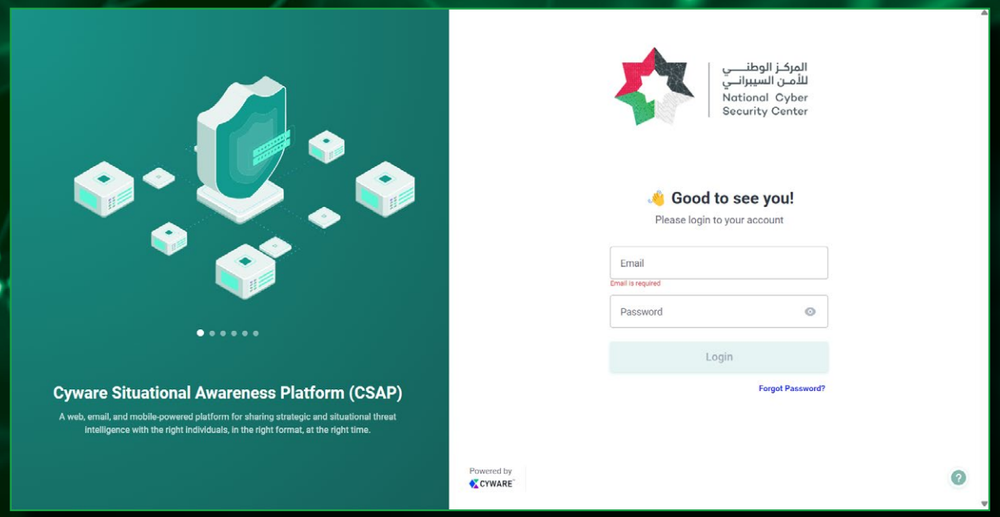
٢. الإدارة الإستباقية في التعامـل مع التهديـدات السيبرانية

عمل المركز خلال عام ٢٠٢٣، على إطلاق مجموعة من المنصات الرقمية، بهدف تعزيز مبدأ الإدارة الإستباقية في التعامل مع التهديدات السيبرانية، وإتخاذ الإجراءات الوقائية للتعامل مع أية تهديدات سيبرانية محتملة قبل حدوثها أو قبل تحولها لهجمات سيبرانية فعلية، تالياً أبرز إنجازاتنا لعام ٢٠٢٣ في ذات السياق:

● إطلاق منصة مشاركة معلومات التهديدات السيبرانية (منصة شارك)

هي منصة آمنة وموثوقة لمشاركة المعلومات السيبرانية بين المؤسسات والوزارات ذات العلاقة بالإدارة الإستباقية للتعامل مع التهديدات والهجمات السيبرانية، حيث توفر المنصة بيانات ومعلومات حول الهجمات السيبرانية، الثغرات الأمنية، التحليلات الرقمية، وغيرها من المعلومات السيبرانية الاستخباراتية التي تحدد الاتجاهات والأنماط الجديدة والمتطورة للهجمات والتهديدات السيبرانية

- توفير وسيلة آمنة وموثوقة لمشاركة المعلومات الاستخبارتية السيبرانية.
- تتيح إمكانية متابعة التهديدات السيبرانية الحالية والنشطة والمتطورة.
- دعم إجراءات الاستجابة السريعة والفعالة للتهديدات السيبرانية.
- دعم وتوثيق المعلومات والتقارير الفنية لتبادل الخبرات والمعرفة بين الأعضاء.



منصـة شـارك

● إطلاق منصة مكافأة الثغرات واختبارات الاختراق الأخلاقي - Bug Bounty

تعتبر منصة مكافأة الثغرات واختبارات الاختراق الأردنية Bug Bounty Jo الأولى من نوعها في الأردن، حيث تهدف لتمكين الجهات الحكومية والخاصة من اختبار وتحديد نقاط الضعف على منصاتها وأصولها الرقمية، وتتبع هذه المنصة منهجية اقتصادية تهدف لتقليل الإنفاق في عمليات اختبار الاختراق من أجل اكتشاف وتحديد نقاط الضعف في المنصات الرقمية والتركيز أكثر على الإنفاق على إصلاح هذه الثغرات.

حيث تتيح المنصة التسجيل للمؤسسات الحكومية والخاصة لغايات فحص أصولها الرقمية ، كما وتتيح المنصة للأفراد التسجيل كمُختبِر اختراق لغايات فحص الأصول الرقمية، مقابل جائزة مالية يُقدمها المركز لمُختبِر الاختراق في حال اكتشافه لأية ثغرة أو عمليات اختراق على تلك الأصول.

Bug Bounty
Continuous Penetration Testing Platform

انقـر هنـا

٣. تنميــة القــدرات والمهــارات الوطنيــة

يُعنى المركز الوطني للأمن السيبراني بشكل رئيسي في بناء القدرات الوطنية في مجالات الأمن السيبراني المختلفة، سواء المعرفية والتوعوية منها أو حتى التقنية العملية، حيث أدرك المركز وبشكل مُبكر أهمية العنصر البشري في سلسلة الأمان السيبراني وأثره الكبير في الوصول إلى فضاء سيبراني مقاوم للتهديدات وقادر على الصّمود بوجه الحوادث السيبرانية.

وانطلاقاً من هذا الأمر عزز المركز الوطني للأمن السيبراني جهوده على مستوى التطور وبناء القدرات حيث قام بعقد العديد من ورشات وحملات التوعية والدورات التدريبية والبرامج التأهيلية، وقد تنوعت هذه الأنشطة جميعاً لتشمل كافة أطياف المجتمع الأردني وفئاته المختلفة، تالياً أهم الإنجازات في ذات السياق:

التوعيــة بمـاهيــة الأمـن السيبرانــي:

● ورشات التوعية والتثقيف:

عقد المركز الوطني للأمن السيبراني ٥١ 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 ٢٦٩٨ شخص من الفئات الآتية:

- الجامعات والمدارس.
- موظفي المؤسسات الحكومية.
- مشغلي البنية التحتية الحرجة.
- القطاعات الصحية والمستشفيات.
- الملحقين الدبلوماسيين.
- الهيئات والمنظمات.

● حمـلات تـوعويـة:

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، وأطلق المركز خلال العام ٢٠٢٣م عدد من الحملات التوعوية ومنها الآتي:

٣. تنميــة القــدرات والمهــارات الوطنيــة

حملة تواصل بأمان:

هدفت الحملة لتعزيز الوعي بالإجراءات الصحيحة أثناء استخدام الفضاء الرقمي، وسبل حماية المعلومات والبيانات الشخصية من محاولات عبث أو سرقة أو وصول غير مصرح به، استهدفت هذه الحملة جميع مستخدمي حسابات التواصل الاجتماعي ومن مختلف الفئات العمرية، وتم الترويج لها الكترونياً من خلال إطلاق العديد من المنشورات ومقاطع الفيديو التي من شأنها ارشاد المُستخدمين بأهم إجراءات الأمان الواجب اتباعها أثناء استخدام وسائل التواصل المختلفة كالبريد الإلكتروني والمواقع الاجتماعية.

حملة من فريق المركز:

كان الهدف من إطلاق هذه الحملة، تعزيز المعرفة لدى كافة الشرائح المجتمعية بإجراءات وسُبل حماية البيانات الرقمية من أية هجمات سيبرانية قد تؤدي إلى اختراق البيانات الشخصية واستغلالها لارتكاب جرائم سيبرانية، حيث تم تكرار هذه الحملة مرتين على مدار العام، مُكونة من مقاطع فيديو موجهة من موظفي المركز، متضمنة أهم النصائح الأمنية والإرشادات السيبرانية الواجب مراعاتها والالتزام بها عند استخدم الفضاء الرقمي، كما تم تضمين الحملة فيديو توعوي خاص بالمرأة بالتزامن مع يوم المرأة ، حيث قدمت خلاله مجموعة من العاملات في المركز أهم النصائح الأمنية الموجهة للمرأة تحديداً عن كيفية تحقيق الأمن السيبراني والأمان الرقمي وبما يضمن حماية بياناتها الشخصية.

٣. تنميــة القــدرات والمهــارات الوطنيــة

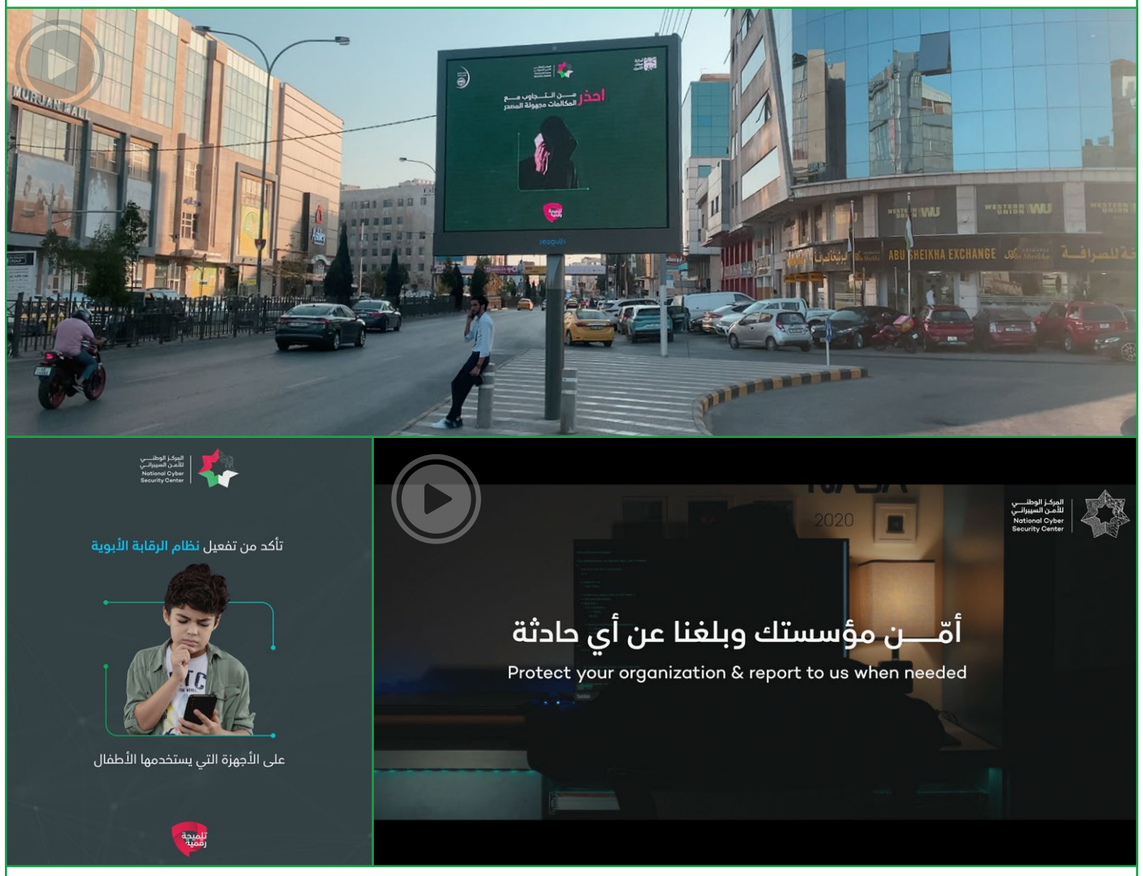
حملة اعرف لتحمي حالك الأولى:

ركزت هذه الحملة التي تم إطلاقها لمرتين خلال العام ٢٠٢٣م وبالتعاون مع صندوق المعونة الوطنية على تقديم ورشات توعية للموظفين في صندوق المعونة الوطنية بأهم طرق الوقاية من الاحتيال عبر الإنترنت وخاصة الاحتيال المالي الذي يهدد شريحة واسعة من المُستفيدين من الصندوق.

حملة اعرف لتحمي حالك الثانية:

تم إطلاق هذه الحملة بالتزامن مع موسم الحج و بالتعاون مع صندوق الحج الأردني، حيث تم تصميم منشورات إلكترونية لتوعية المواطنين بأهم التهديدات السيبرانية التي تنطلق مع اقتراب مواسم معينة كموسم الحج.

٣. تنميــة القــدرات والمهــارات الوطنيــة



حملة تلميحــة رقميــة:

تم إطلاق هذه الحملة خلال شهر تشرين الأول (شهر التوعية بالأمن السيبراني عالمياً)؛ حيث تم خلالها تصميم العديد من المنشورات ومقاطع الفيديو التي تم نشرها على مواقع التواصل الاجتماعي وشاشات أمانة عمان الكبرى، وبقيت الحملة مُستمرة بعد انتهاء شهر التوعية لتمتد أيضاً خلال شهر تشرين الثاني.

تلميحة رقمية

٣. تنميــة القــدرات والمهــارات الوطنيــة

حملـة وطـن واع:

تم إطلاق هذه الحملة بالتعاون مع أمانة عمان الكبرى، حيث تم خلالها تصميم العديد من مقاطع الفيديو وتم نشرها على شاشات أمانة عمان المتواجدة في كافة أنحاء العاصمة، وامتدت هذه الحملة على مدار عام ٢٠٢٣.

لا تشارك كلمات السر الخاصة بك مع أي أحد

حملـة اليوم العالمي لذوي الاحتياجات الخاصة:

تم البدء بهذه الحملة بتاريخ ٣ كانون الأول ٢٠٢٣ والذي صادف اليوم العالمي لذوي الاحتياجات الخاصة، وتم تسجيل وتصميم عدد من مقاطع الفيديو بلغة الإشارة، ومن الجدير بالذكر ان المركز باشر باعتماد لغة الإشارة بالعديد من حملاته التوعويـة الرقميـة منـذ مطلـع عام ٢٠٢٢.

٣. تنميــة القــدرات والمهــارات الوطنيــة

بودكاســت حكايــة سيبرانيــة:

إيماناً من المركز بالتماشي مع أحدث تقنيات التواصل المنتشرة بين مُستخدِمي الإنترنت، أطلق المركز بودكاست متخصص بمجال الأمن السيبراني بعنوان حكاية سيبرانية، حيث تم تسجيل وبث ست حلقات مع ستة من الخبراء والمختصين في مجال الأمن السيبراني وأمن المعلومات، حيث تضمنت الحلقات جلسات حوارية مع الضيوف متعلقة بالأمن السيبراني.

عطوفة المهندس بسـام المحارمـة
رئيس المركز الوطني للأمن السيبراني

عنـوان الحلقـة:
مـا هـو مفهوم الأمـن السيبرانـي

المهنـدس نضـال البيطـار
جمعية إنتاج

عنـوان الحلقـة:
الأمن السيبراني بين الفرص والتحديات

المهنـدس أيمـن مزاهـرة
الشريك المؤسس والرئيس التنفيذي
لشركة إس تي إس

عنـوان الحلقـة:
كيف يؤثر الأمن السيبراني على حياتنا اليومية

حكاية سيبرانية

٣. تنميــة القــدرات والمهــارات الوطنيــة

الدكتــورة إيمــان المومنــي
أستاذ مشارك في الأمن السيبراني في
الجامعة الأردنية

عنـوان الحلقـة:
ماذا تعرف عن الهجمات الخبيثة

المهنـدس منتصــر بديــر
المؤسس والرئيس التنفيذي
لشركة أمن التقنية

عنـوان الحلقـة:
كيف نحقق التوعية في الأمن السيبراني

الدكتور يعرب القضاة
قاض عسكري مختص في شؤون الأمن
السيبراني

عنـوان الحلقـة:
التشريعات الوطنية بالمرتبطة بالأمن السيبراني

حكاية سيبرانية

٣. تنميــة القــدرات والمهــارات الوطنيــة

تعزيـز القـدرات وتعزيـز المهـارات لطلبــة الجامعــات والمـدارس

● معسكــر نشامــى السايبــر

استمراراً من المركز لدوره في تأهيل قدرات الشباب في مجال الأمن السيبراني وتأهيل الطلبة وتحديداً الخريجين منهم، تم إطلاق معسكر نشامى السايبر بنسختيه الثانية والثالثة بعدد مشاركين بلغ ٣٠ طالباً وطالبة لكل نسخة، وجاء هذا الإطلاق بعد اختتام برنامج النسخة الأولى من المعسكر والذي تم إطلاقه خلال العام ٢٠٢٢م، ويهدف برنامج معسكر نشامى السايبر إلى تطوير مهارات خريجي تخصصات تكنولوجيا المعلومات ومن كافة 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 ، ويلقى هذا البرنامج التدريبي اهتماماً ومتابعة كبيرين من فئة الطلبة الخريجين وخاصة بعد قيام سمو ولي العهد الأمير الحسين بن عبدالله الثاني بإعادة نشر الإعلان الصادر عن المركز بخصوص عقد المعسكر بنسخته الثانية عبر منصة الإنستجرام، وتجدر الإشارة إلى أن خريجي هذا البرنامج التدريبي عادة ما يتحصلون على فرص وظيفية وبشكل مباشر وذلك لما يمتلكونه من مهارات فنية وعملية في مجال الأمن السيبراني وبما يلاءم متطلبات سوق العمل.

نشامى السايبر

٣. تنميــة القــدرات والمهــارات الوطنيــة

تعزيـز القـدرات وتعزيـز المهـارات لطلبــة الجامعــات والمـدارس

● مسابقــة محاربــو السايبــر

تم إطلاق النسخة الثانية من مسابقة محاربو السايبر التي شارك فيها ٢٠٠ طالب وطالبة من طلبة المدارس والجامعات في المملكة الأردنية الهاشمية، وتُعنى هذه المسابقة بتقديم تحديات تقنية على العديد من مواضيع الأمن السيبراني كالثغرات والاختراق والهندسة العكسية وغيرها وهو ما يُعرف بتحديات التقاط العلم (Capture The Flag).

محاربو السايبر

٣. تنميــة القــدرات والمهــارات الوطنيــة

تعزيـز القـدرات وتعزيـز المهـارات لطلبـة الجامعـات والمـدارس

● تدريـب تحديـات التقـاط العلـم (CTF)

نظراً للإقبال الكبير من الطلبة على المشاركة في مسابقة تحديات التقاط العلم أطلق المركز الوطني للأمن السيبراني برنامجاً تدريبياً موجهاً لطلبة جميع الجامعات الحكومية والخاصة لتدريبهم على تحديات التقاط العلم، حيث تم تدريب ٣٨٨٥ طالباً وطالبة

٣. تنميــة القــدرات والمهــارات الوطنيــة

تعزيـز القـدرات وتعزيـز المهـارات لطلبـة الجامعـات والمـدارس

● رواد السايبـر

تم إطلاق مشروع رواد السايبر في العام ٢٠٢٣م، بهدف تنمية الوعي لدى الطلاب، وتعليمهم مخاطر استخدام شبكة الإنترنت والمشكلات التي يمكن أن تنتج عنها ، وتثقيفهم و تدريبهم على أفضل الممارسات الأمنية أثناء استخدام الإنترنت والأجهزة الإلكترونية، وتعريفهم على برامج حماية البيانات وكيفية توظيفها والاستفادة منها، بالإضافة إلى تدريبهم على كيفية حماية أنفسهم من المخاطر السيبرانية التي يمكن أن تواجههم عبر الإنترنت أثناء اللعب أو من خلال التصفح الالكتروني ، وقد استفاد من هذا البرنامج التدريبي ٩٠ طالباً من مختلف مدارس المملكة.

روّاد السايبر

٣. تنميــة القــدرات والمهــارات الوطنيــة

تعزيز القدرات وتعزيز المهارات للموظفين والعاملين في القطاعات الوطنية

• نظام إدارة التعليم (LMS)

تم الإنتهاء من تجهيز منصة تدريبية خاصة لموظفي المؤسسات والدوائر الحكومية، حيث تتضمن المنصة مواد توعوية وتدريبية لتأهيل الموظفين وتوعيتهم حول أفضل الممارسات الأمنية أثناء تواجدهم على الشبكة الحكومية وتدريبهم على سياسات الأمن السيبراني المُطبّقة في مؤسساتهم، بالإضافة إلى احتواءها على منصة يُمكن من خلالها اجراء اختبارات وحملات تصيد وهمية بهدف تدريب الموظفين على الحقة والحذر في التعامل مع البريد الإلكتروني الوارد وهو ما سينعكس بدوره على رفع مستوى صمود مؤسساتهم بوجه التهديدات السيبرانية وسرعة التعافي من الحوادث السيبرانية.

• إطلاق منصة SafeOnline

أطلق المركز منصة خاصة بتوعية الأفراد والمؤسسات، وعبر الموقع الإلكتروني www.safeonline.jo حيث تنوع المحتوى التوعوي الموجود عبر المنصة ما بين خطوات وإجراءات من شأنها تعزيز الأمن السيبراني وتفعيل الحماية الرقمية للمُستخدِمين بالإضافة إلى المقالات العلمية المتخصصة في العديد من المفاهيم السيبرانية وغيرها من المحتوى الثري الذي راعى تلبية كافة أذواق المتلقين للمعلومة من خلال المقالات الطويلة والقصيرة والمنشورات السريعة ومقاطع الفيديو وغيرها، وتم توجيه كافة أشكال هذه المحتوى التوعوي لكل من فئتي الأفراد والأعمال، حيث تتضمن المنصة العديد من التصنيفات للمحتوى سواء في فئة الأفراد أو الأعمال.

Safe Online
ابـــق آمـنـًا

www.safeonline.jo

4

التعـــاون

أدرك المركز باكراً أهمية الانفتاح على الخبرات الإقليمية والعالمية في مجال الأمن السيبراني ، وأن الاستفادة من قصص نجاح الآخرين وممارساتهم الفضلى يُعزز بناء القدرات السيبرانية لأية دولة ويضيف على مهاراتها وأدواتها السيبرانية، لذا سعى المركز خلال العام ٢٠٢٣ لبناء العلاقات التعاونية والتشاركية على المستوى المحلي، الإقليمي والدولي، والمشاركة في الفعاليات العالمية التي تساهم في تعزيز وتطوير إدارة العمليات السيبرانية الناظمة لأمن وموثوقية الفضاء السيبراني الأردني، تالياً أبرز الإنجازات في ذات السياق.

عقد القمة الوطنية الأولى للأمن السيبراني

قمة الأردن الأولى للأمن السيبراني DOT CYBER SUMMIT

شهد يوم الاثنين الموافق الخامس والعشرين من أيلول للعـام ٢٠٢٣م إطلاق قمـة الأردن الأولـى للأمـن السيبرانـي DOT CYBER SUMMIT برعايـة وحضـور كريميـن مـن سمـو ولـي العهـد الأمير الحسين بن عبد الله الثانـي المعظـم

هدف القمة:

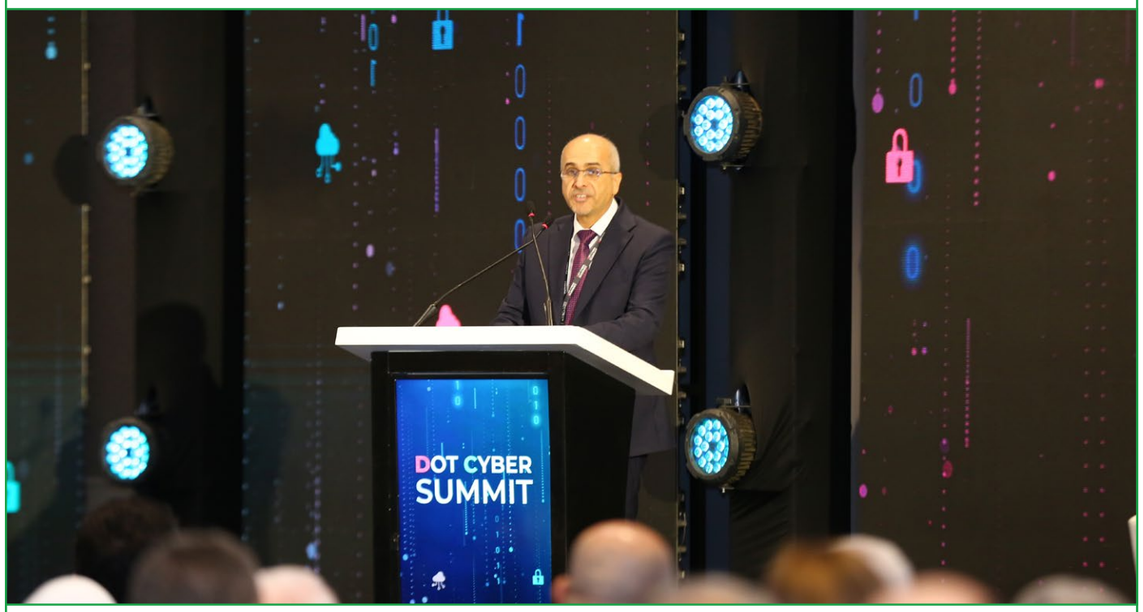
أتى عقد القمة لتكون ملتقىً للمسؤولين وأصحاب القرار ورجال الفكر والأعمال والمهتمين بقضايا ومواضيع الأمن السيبراني والسلامة الرقمية من القطاعات الحكومية والصناعية والأكاديمية، وبحيث يتم خلالها مناقشة قضايا تتعلق بالسياسات والاستراتيجيات السيبرانية والقضايا الدولية المتعلقة بالمخاطر والتهديدات السيبرانية التي تواجهها الدول والمجتمعات وآليات التعاون لمواجهتها ومكافحة انتشارها، وكذلك الاطلاع على تجارب الدول وما حققته من تقدم في مجال الأمن السيبراني والسلامة الرقمية.

مشاركة ولي العهد:

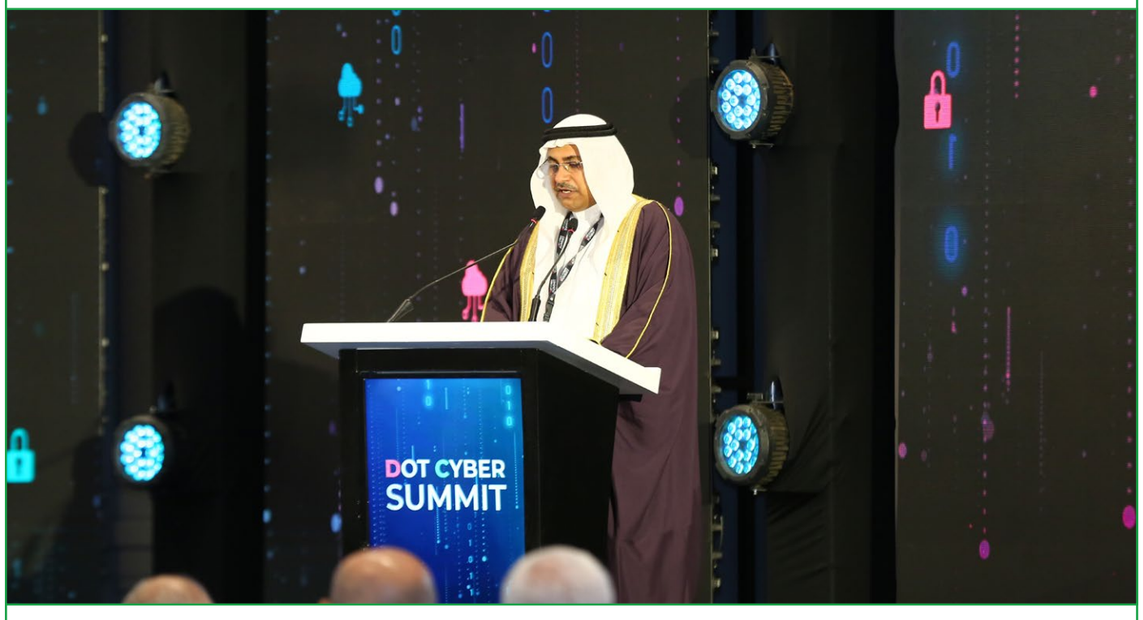
بحضور سمو ولي العهد رحب رئيس المركز الوطني للأمن السيبراني عطوفة المهندس بسام المحارمة بالمشاركين في القمة وأوضح أن القمة عبارة عن منصة للتحاور والتشارك والتعاون بين الدول وهدفها وضع الأردن على خارطة المنطقة والعالم في مجال الأمن السيبراني، مؤكدا أن لدى الأردن فرصة كبيرة أن يكون مميزا وقائدا في مجال الأمن السيبراني، وأضاف عطوفته أن القمة انعقدت في ظل تزايد المخاطر السيبرانية وتأثيرها المتعاظم على الأصعدة المالية والاجتماعية والسياسية.

أبرز الموضوعات:

شارك نحو ٤٥٠ مشاركاً في العديد من الجلسات النقاشية حول العديد من المواضيع والمجالات المتعلقة بالأمن السيبراني وأمن البيانات والمعلومات، كالأمان السحابي وحماية البيانات وتأثير التكنولوجيا المتقدمة مثل الذكاء الاصطناعي وإنترنت الأشياء على الأمن السيبراني وغيرها العديد من المواضيع الأخرى.



ولفت عطوفة رئيس المركز إلى أن انعقاد القمة في الأردن، الذي يمتلك كفاءات مميزة في الأمن السيبراني، من شأنه تعزيز دوره كمركز إقليمي رائد في هذا المجال، مبينا أن القمة تشكل فضاء للحوار والتعاون الإقليمي والدولي.



ثم القى رئيس البرلمان العربي عادل العسومي كلمة أشار فيها إلى إنه بالرغم من المزايا العديدة لتكنولوجيا المعلومات إلا أنها أفرزت الجرائم السيبرانية ذات الطبيعة المعقدة التي تهدد الأمن المجتمعي، إضافة للهجمات التي توظفها الجماعات الإرهابية.

وأضاف العسومي أن البرلمان العربي أولى الأمن السيبراني الأهمية؛ لأنه لا يمكن الابتعاد عنه في ظل الرقمنة وانتشارها، مشيراً إلى أن البرلمان العربي يؤمن بأهمية البنية التحتية المتماسكة والتشريعات لمكافحة الجريمة.

وبين أن حوكمة الأمن السيبراني ضرورة حتمية لحماية الاقتصاد الرقمي عبر إيجاد تشريعات متماسكة وكوادر مؤهلة ومتخصصة ووجود مرجعية للأمن السيبراني وتحقيق التوازن بين حماية الحريات والوقاية من الهجمات السيبرانية.

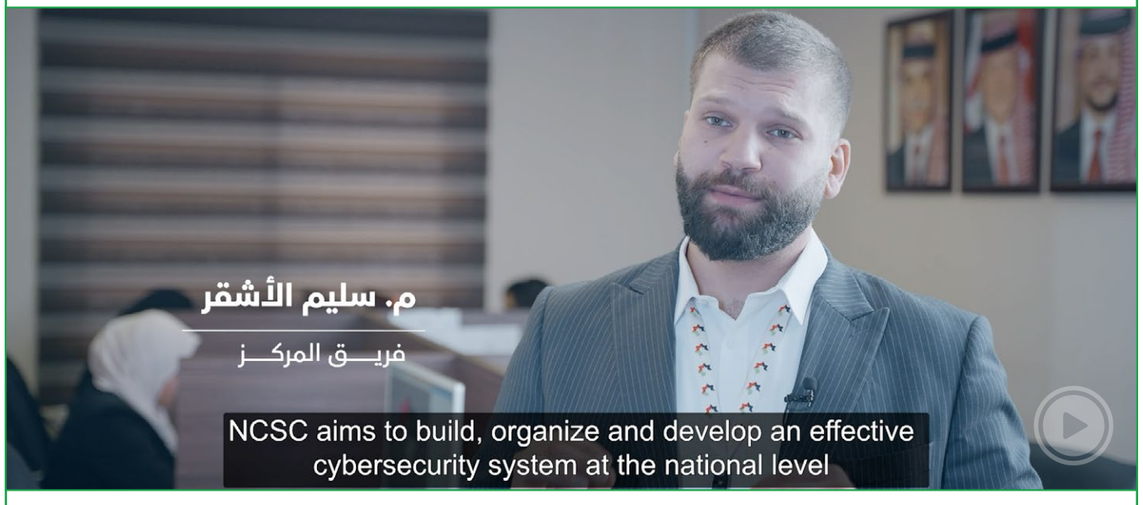
كما استمع سمو ولي العهد والحضور إلى مشاركة القائمة بأعمال نائب مساعد وزير الخارجية لأمن الفضاء الإلكتروني الدولي في مكتب الفضاء الإلكتروني والسياسة الرقمية التابع لوزارة الخارجية الأميركية ليزيل فرانز والتي أوضحت أن الحكومة الأميركية في إطار تعزيز التعاون الدولي وتقوية العلاقات البينية تعمل مع شركاء دوليين مثل الأردن لمواجهة التهديدات السيبرانية وتعزيز الأمن الرقمي والاستقرار الإقليمي.

وأضافت: "نحن نسعى لتطوير إطار الاستجابات ABA الذي أقرته جميع دول الأعضاء للتصدي لأي نشاط سيبراني خبيث يعكر صفو الاستقرار الدولي، ونعمل على تحسين القدرات التقنية لاكتشاف والتعامل مع الهجمات السيبرانية والتعافي منها".

وأكدت مندوبة الولايات المتحدة على أهمية بناء القدرات وتنمية الثقة من خلال تطبيق تدابير ملموسة وتطوير استراتيجيات وطنية متقدمة في مجال الأمن السيبراني، مع تحديث مستمر للاستراتيجيات والسياسات لمواكبة التطورات والتحديات الحديثة.

وأشارت إلى أن التعاون المتزايد والحوار المستمر بين الخبراء والمتخصصين الدوليين يسهمان في فتح آفاق جديدة للحلول والأفكار المبتكرة، مع تبادل الخبرات والمعرفة لتحقيق تنمية اقتصادية مستدامة وتعزيز الأمن الإلكتروني.

وبحسب فرانز تمثل هذه الجهود جزءاً من استراتيجية الولايات المتحدة الوطنية لتحسين القدرة على الاستجابة للتهديدات السيبرانية وتعزيز الأمان الرقمي، مع توجيه اهتمام خاص للتعاون الدولي والتنسيق بين الدول المختلفة لضمان بيئة سيبرانية أكثر أمانًا وشمولية



واختتم سمو ولي العهد مشاركته بأعمال القمة من خلال مشاهدة مقطع فيديو لمجموعة من موظفي المركز الوطني للأمن السيبراني.

الجلسـات الحواريــة والمواضيــع وورش العمـل

تم خلال القمة عقد العديد من الجلسات الحوارية التي تناولت موضوعات هامة في مجالات الأمن السيبراني، وتالياً بعض من هذه الورشات:

• جلسة نقاشية بعنوان: التعاون السيبراني عبر الحدود لحماية الدول

المتحدثـون:

• عطوفة المهندس بسام المحارمة رئيس المركز الوطني الأردني للأمن السيبراني.

• سعادة الدكتور محمد الكويتي رئيس مجلس الأمن السيبراني الإماراتي.

• معالي الدكتور أحمد عبد الحافظ نائب الرئيس لشؤون الأمن السيبراني بالجهاز القومي لتنظيم الاتصالات.

• سعادة المهندس بدر بن علي الصالحي مدير عام المركز الوطني العُماني للسلامة المعلوماتية ورئيس المركز العربي الإقليمي للأمن السيبراني.

• عرض تقديمي: تصميم دفاع ذكي ضد التهديدات المستقبلية

المتحدث:

• السيد رينزي جونغمان / مستشار استخبارات التهديدات السيبرانية، منطقة أوروبا والشرق الأوسط وأفريقيا الجنوبية في شركة مانديانت (Mandiant).

• جلسة نقاشية - بعنوان: نظرة خاطفة على تكنولوجيا المستقبل

المتحدثــون:

• معالي المهندس أحمد الهناندة المحترم – وزير وزارة الاقتصاد الرقمي والريادة.

• عطوفة المهندس بسام السرحان رئيس مجلس الإدارة والرئيس التنفيذي لهيئة تنظيم قطاع الاتصالات.

• عطوفة المهندس نضال البيطار رئيس جمعية شركات تقنية المعلومات الأردنية – إنتاج.

• الدكتورة/ عهود علي شهيل مدير عام دائرة عجمان الرقمية.

• عرض تقديمي: ما الذي يجب أن يعرفه أصحاب المصلحة حول تأثير الهجمات السيبرانية؟

المتحدث:

• المهندس ماهر جاد الله المدير الأول لمنطقة الشرق الأوسط وشمال أفريقيا في شركة Tenable.

• جلسة نقاشية - بعنوان: دور المدراء والرؤساء التنفيذيون في جعل الأمن السيبراني أولوية في مؤسساتهم

المتحدثــون:

• سعادة المهندس أمجد الصادق - المدير العام الإقليمي لشركة نتورك إنترناشيونال.

• سعادة المهندس عمر عايش - الرئيس التنفيذي لشركة الحوسبة الصحية- حكيم.

• سعادة السيدة سارة الطراونة - المدير التنفيذي لمركز إيداع الأوراق المالية (SDC).

• السيدة ربى درويش - المدير الإقليمي لبنك BMB - الأردن.

• عرض تقديمي: هل من الآمن الاستعانة بمصادر خارجية للخدمات السيبرانية؟

المتحدث:

• الدكتور سمير أبو طاحون - المؤسس المشارك والرئيس التنفيذي لمجموعة SMT.

• عرض تقديمي: المرونة السيبرانية للبنية التحتية الحيوية: رؤية متكاملة نحو مدينة معرفية آمنة

المتحدثـون:

• الدكتور حمد خليفة النعيمي رئيس قسم الاتصالات - مركز تكنولوجيا المعلومات في القيادة العامة لشرطة أبوظبي.

• الدكتور محمد خالد - رائد في مجال الفكر الرقمي والتحول الآمن.

• عرض تقديمي: ممارسة حوكمة الأمن السيبراني للمؤسسات

المتحدث:

• الدكتور الويسيوس تشيانغ / كبير مسؤولي الأمن لشركة هواوي في الشرق الأوسط وآسيا الوسطى.

• عرض تقديمي: التنقل في مصفوفة الأمن السيبراني مع استراتيجيات التقارب والدمج

المتحدث:

• المهندس مليح كيركجوز - مدير هندسة الحلول في Fortinet.

• عرض تقديمي: تأثير 5G وإنترنت الأشياء على الأطر السيبرانية؟

المتحدث:

• سعادة المهندس محمد الطعاني / مستشار تنظيم الاتصالات والأعمال.

• عرض تقديمي: الحوكمة والمخاطر

المتحدث:

• السيد جينارو سكالو - المدير في شركة آرتشر - أوروبا والشرق الأوسط وأفريقيا.

• عرض تقديمي: أولويات الاستجابة للحوادث السيبرانية لقادة الأعمال

المتحدث:

• السيد ستيوارت رووم (Stewart room) مسؤول قطاع التكنولوجيا والاتصال في شركة DWF العالمية.

• جلسة نقاشية - بعنوان: قوانين خصوصية البيانات وجاهزية القطاع

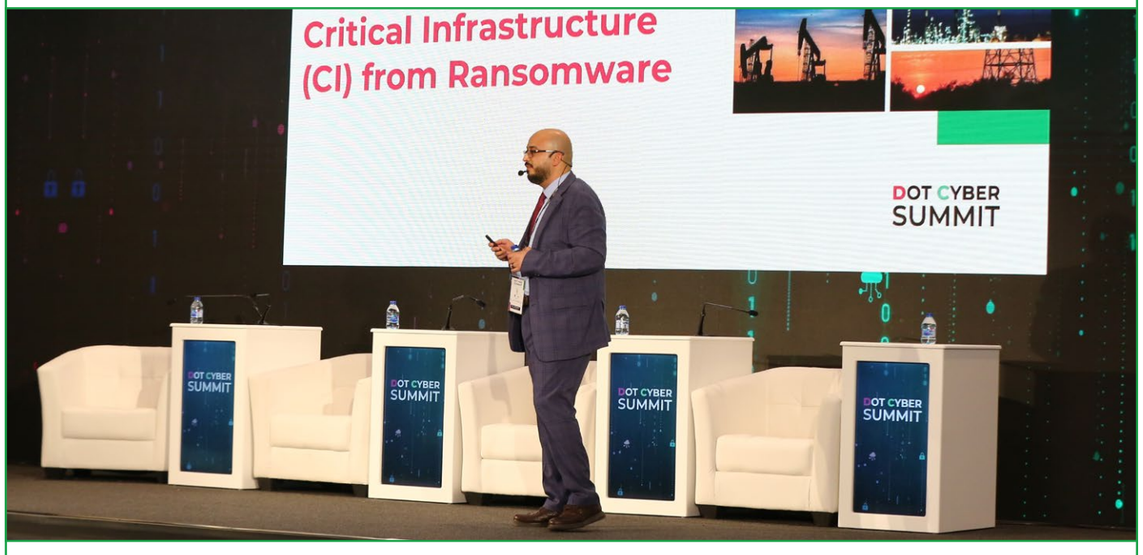
المتحدثـــون:

• سعادة السيد عمر النبر، عضو مجلس النواب الأردني.
• السيد وليد البشوتي - محامي/استشاري في مجال التكنولوجيا.

• عرض تقديمي: هل ستنفذ أدوات الذكاء الاصطناعي والروبوتات الهجوم السيبراني القادم؟

المتحدث:

• المهندس. تامر العجرمي / رئيس فرع ISACA في الأردن.



• عرض تقديمي: استراتيجيات الدفاع عن البنية التحتية الحيوية (CI) من برامج الفدية

المتحدث:

• المهندس عايض القرطا مهندس حلول العمليات الأمنية في أوروبا والشرق الأوسط وأفريقيا في شركة تريليكس.

• عرض تقديمي: التحديات التي تواجه إدارة سمعتك وبياناتك على الإنترنت

المتحدث:

• المهندس محمد الخضري - الرئيس التنفيذي لشركة Green Circle.

• جلسة نقاشية - بعنوان: الأوساط الأكاديمية وفجوة المهارات

المتحدثـــون:

• الدكتور إسماعيل الحنطي رئيس جامعة الحسين التقنية.
• المهندس أحمد الغرايبة - مدير عام مؤسسة التدريب المهني.
• الدكتورة رغدة الفاعوري المحترمة - رئيس هيئة تنمية وتطوير المهارات المهنية والتقنية.
• الدكتور نبيل الفيومي مدير عام جمعية المهارات الرقمية.

• ورشة ١ : حماية البنية التحتية الحيوية للتكنولوجيا التشغيلية

المتحدثــون:

- المهندس فهد فيصل - مدير تطوير أعمال الأمن السيبراني في شركة Fortinet.
- المهندس عمر البرغوثي - المدير الإقليمي لشركة Dragos.
- طارق عكرمة - قائد أعمال الأمن السيبراني، META في شركة Honeywell.
- فيكاس داهيا - قائد مبيعات الأمن السيبراني العالمي في Nokia.
- عثمان الدوامينة - المدير الإقليمي في Mandiant.

• ورشة عمل٢ : الأمن السيبراني والتمويل (البنوك المركزية)

المتحدثــون:

- المهندس علاء وريكات: رئيس قسم عمليات ومراقبة الأمن السيبراني - وحدة Jo-FinCERT في البنك المركزي الأردنــي.
- المهندس بهاء الشوبيري: رئيس قسم الرقابة على تكنولوجيا المعلومات في دائرة الرقابة على البنوك في البنــك المركــزي سلطة النقد الفلسطينية.

• ورشة عمل٣ : استخبارات التهديدات السيبرانية: من النظرية إلى التطبيق

المتحدثــون:

- المهندس جميل أبو عقل - مدير أول في Mandiant.
- المهندس صالح عبدالله - مهندس مبيعات استشاري Mandiant.

• ورشة ٤ : أطر الأمن السيبراني عبر بلدان متعددة

المتحدثــون:

- المهندس أدهم العتوم: مدير السياسات والامتثال في المركز الوطني للأمن السيبراني في الأردن.
- المهندس محمد عبد الرحيم: عضو المجلس الاستشاري والرئيس المشارك لفرع الشرق الأوسط وأفريقيا - معهد FAIR.
- المهندس ابراهيم العابد: مدير - الاستشارات الموثوقة وخدمات المخاطر في CPX.

تحسين مرتبة الأردن في مؤشرات الأمن السيبرانية العالمية

• مؤشر الأمن السيبراني العالمي (GCI)

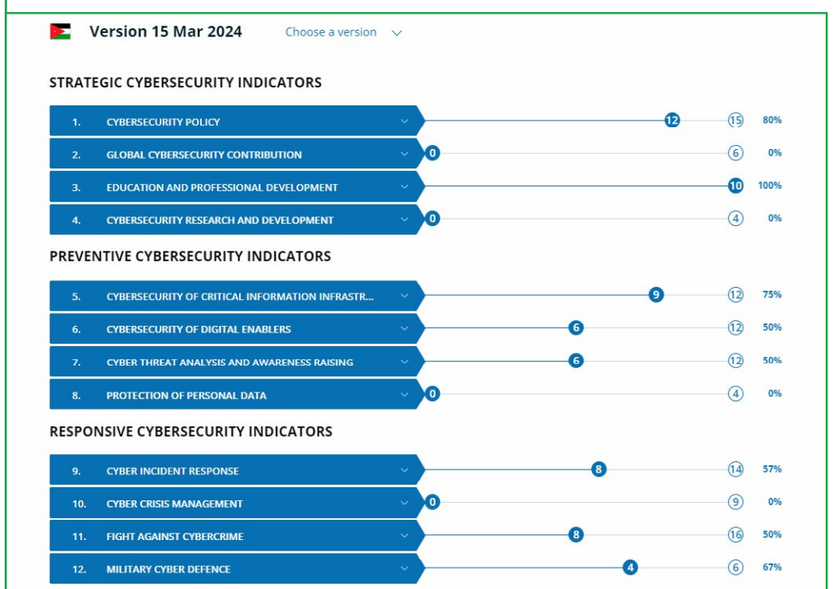
يهدف المؤشر لتقييم ومقارنة قدرة الدول على حماية أصولها الرقمية والتكنولوجيا من التهديدات والهجمات السيبرانية، وتحديد نقاط القوة ونقاط الضعف والتحديات التي تواجهها، وتتم عملية تصنيف الدول استناداً لمجموعة قدرات وهي:

(التدابير القانونية / التدابير التنظيمية / التدابير التقنية / تدابير بناء القدرات / تدابير التعاون)

حيث عمل المركز خلال عام ٢٠٢٣، على بناء قدرات وطنية تشاركية مع كافة المؤسسات المعنية التي تساهم من خلال المهام المناطة بها والإجراءات التنفيذية لعملياتها الرئيسية في رفع ترتيب الأردن في هذا المؤشر، وذلك من خلال تشكيل فريق وطني ضم أعضاء من مختلف المؤسسات الوطنية، وتم تعبئة التقرير التقييمي للمؤشر عن عام ٢٠٢٣، وبإنتظار اعلان النتائج ، علماً أن الأردن حصل على ترتيب ٧٢ في اخر تقييم تم عام ٢٠٢٠.

• الرقم القياسي الوطني للأمن السيبراني NCSI

إن الرقم القياسي الوطني للأمن السيبراني (NCSI) هو رقم قياسي عالمي يقيس تأهب البلدان لمنع التهديدات السيبرانية وإدارة الحوادث السيبرانية، يركز الرقم القياسي الوطني للأمن السيبراني (NCSI) على جوانب قابلة للقياس في الأمن السيبراني، حيث عمل المركز على رفع متطلبات رفع ترتيب الأردن في هذا الرقم عالميًا.



شراكـات المركـز التعاونيـة لعـام ٢٠٢٣

• جمعية إنتاج (قطاع خاص)

الهـدف مـن الشراكـة:

تعزيز الشراكة و تأطير التعاون و التنسيق بين الفريقين في عقد قمة الأمن السيبراني Dot Cyber Summit 2023.

• جامعة البلقاء (قطاع أكاديمي)

الهـدف مـن الشراكـة:

توثيق أواصر التعاون و تبادل الخبرات الأكاديمية و العلمية لتحقيق أهدافهما المشتركة و المتمثلة في بناء منظمة فعالة للأمن السيبراني على المستولى الوطني و تطويرها و تنظيمها.

• المركز المصري للإستعداد لطوارئ الحسابات و الشبكات – الجهاز القومي لتنظيم الإتصالات (قطاع خارجي - إقليمي)

الهـدف مـن الشراكـة:

تعزيز التعاون الوثيق و تبادل المعلومات المتعلقة بالأمن السيبراني.

• مجموعة مدينة العقبة الرقمية (قطاع خاص)

الهـدف مـن الشراكـة:

دعم جهود المركز و الإستفادة من البنى التحتية الرقمية الخاصة بمدينة العقبة الرقمية و بناء علاقة استراتيجية طويلة الأمد لعقد اتفاقيات في المستقبل تشمل أوجه التعاون و العمل المشترك.

• المركز العربي الإقليمي للأمن السيبراني و المركز الوطني للسلامة المعلوماتية (قطاع خارجي - إقليمي)

الهـدف مـن الشراكـة:

تحفيز و تشجيع تبادل المعرفة و التعاون في المصلحة المشتركة في مجال الأمن السيبراني.

• جامعة البترا (قطاع أكاديمي)

الهـدف مـن الشراكـة:

توثيق أواصر التعاون فيما بينهما و تبادل الخبرات العلمية و الأكاديمية بغية تحقيق أهدافهما المشتركة المتمثلة في بناء منظومة فعالة للأمن السيبراني على المستوى الوطني و تطويرها و تنظيمها.

• جامعة الزرقاء (قطاع أكاديمي)

الهـدف مـن الشراكـة:

توثيق أواصر التعاون فيما بينهما و تبادل الخبرات العلمية و الأكاديمية بغية تحقيق أهدافهما المشتركة.

• كلية لومينوس الجامعية التقنية (قطاع أكاديمي)

الهـدف مـن الشراكـة:

توثيق أواصر التعاون فيما بينهما و تبادل الخبرات العلمية و الأكاديمية بغية تحقيق أهدافهما المشتركة.

• مجموعة طلال أبو غزالة (قطاع خاص)

الهـدف مـن الشراكـة:

توثيق أواصر التعاون بين الطرفين و تبادل الخبرات العملية و العلمية و الأكاديمية بغية تحقيق أهداف الطرفين المشتركة في التعاون في مجال الأمن السيبراني

• جامعة الأميرة سمية للتكنولوجيا (قطاع أكاديمي)

الهـدف مـن الشراكـة:

توثيق أواصر التعاون بينهما و تبادل الخبرات العلمية و الأكاديمية و لتحقيق أهداف الطرفين المشتركة و المتمثلة في بناء منظومة فعالة للأمن السيبراني على المستوى الوطني و تطويرها و تنظيمها.

• مؤسسة إنجاز لتهيئة فرص الشباب الأردني (قطاع خاص)

الهـدف مـن الشراكـة:

تعزيـز التعـاون و التفاهـم بينهمـا ووضـع إطـار عمـل مشـترك لبنـاء القـدرات و التوعيـة و التثقيـف فـي مجـالات الأمـن السيبراني من خلال تصميم و تطوير مناهج أكاديمية سليمة و موثوقة ذات ارتباط بمتطلبات و معايير الأمن السيبراني تهدف إلى رفع الوعي لدى طلاب المدارس و الجامعات في مجال الأمن السيبراني

المنتديات و المؤتمرات العالمية التي شارك فيها المركز

- مؤتمر بعنوان مواجهة انتشار واستخدام القدرات للاختراق الالكتروني بشكل غير مسؤول
  لنـــدن
- المشاركة في دورة العمل المعنية بأمن واستخدام تكنولوجيا المعلومات والاتصالات
  نيويـــورك
- المشاركة في المؤتمر والمعرض العربي الدولي للأمن السيبراني
  البحريـــن
- المشاركة في الأسبوع الإقليمي للأمن السيبراني
  الإمـــارات /أبو ظبـــي
- مؤتمر الضمان السيبراني الوطني القطري بنسخته الثانية والمعني بحوكمة سلسلة توريد الأمن السيبراني
  الدوحـــة
- المشاركة في أعمال دورة العمل المعنية بأمن واستخدام تكنولوجيا المعلومات والاتصالات
  الأمـــم المتحـــدة/نيويـــورك
- حضور مؤتمر بعنوان Kaspersky security analyst summit 2023
  تايلنـــد
- المشاركة في مؤتمر Mandiant
  واشنطـن
- مؤتمر ليماســول
  قبـــرص
- مؤتمر مختص بكشف التهديدات المتطورة
  الإمـــارات
- مؤتمر و معرض GITEX
  الإمـــارات
- المؤتمر الدولي المعني بالأمن الحاسوبي في العالم النووي
  النمســا
- الأسبوع الإقليمي للأمن السيبراني في المنطقة العربية لعام ٢٠٢٤
  الإمـــارات
- مؤتمر Kaspersky CXO vault
  قبـــرص
- الاجتماع الثالث لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات
  تونـــس
- اجتماع لجنة إعداد مشروع قانون عربي استرشادي للاستخدام الأمن للفضاء السيبراني
  بيـــروت
- الاجتماع الرابع لفريق خبراء العرب المختصين في المجالات الأمنية والقانونية والفنية
  مصـــر
- المناورة السيبرانية الوطنية
  قطـــر
- An Analytics Experience Inspire 2023
  أمريكـــا
- GISEC 2023
  الإمـــارات

تطلعاتنا

تطلعاتنا لعام ٢٠٢٤

بين أيديكم وضعنا خلاصة عملنا الدؤوب على مدار عام، وما حققنا من إنجازات في هذا العام فهو بتوفيق من الله أولاً، وبفضل دعمكم ومساندتكم لنا أفراداً ومؤسسات ، فتأمين الفضاء السيبراني الأردني و الحفاظ على أمنه وصموده هو مسؤولية وطنية تشاركية، لكل منا دورٌ أُنيط به ليكن دعامةً أساسية تساند الجهود الوطنية الرامية لتمكين الفضاء السيبراني الأردني وتعزيز صموده ليبقى حصناً منيعاً بوجه التهديدات والاختراقات السيبرانية، عصيّاً أمام كل من تسول له نفسه العبث بأمنه وأمن مكوناته الرقمية

ولأننا ومنذ اليوم الأول لإرساء قواعد المركز الوطني للأمن السيبراني رفعنا الهمة وعزمنا على الوصول للقمة، فإننا نتطلع أن يكون العام الرابع والعشرين بعد الألفية الثانية، عاماً مليئاً بالإنجازات التي ستؤتي أُكلها بتمكين وتطوير الفضاء السيبراني الأردني واستكمال مسيرة الانطلاق نحو فضاء سيبراني أردني آمن وموثوق، مرن قادر على الصّمود، مُعزز للاقتصاد والرفاه المجتمعي، حيث سنعمل خلال عام ٢٠٢٤ على تنفيذ المشاريع الرئيسية التالية:

- تطوير البنية السيبرانية الفنية والعملياتية لما مجموعه (٦٠) مؤسسة وطنية، من خلال رفدها بالأنظمة والمعدات التكنولوجيا استناداً لمخرجات عمليات التقييم الفني لأصولها الرقمية وبما يساهم في حماية أصولها الرقمية، والحد من خطر تعرضها للتهديدات والحوادث السيبرانية.
- تنفيذ مشروع التدريب على متطلبات الامتثال للإطار الوطني للأمن السيبراني، لما مجموعه (١٠٠) مؤسسة وطنية.
- إطلاق تعليمات تراخيص مقدمي خدمات الأمن السيبراني، ليكن نواة الانطلاق لتفعيل نظام تراخيص الأمن السيبراني على المستوى الوطني.
- استكمال المرحلة الثالثة من ربط المؤسسات الحكومية على أنظمة مراقبة وتحليل الحوادث السيبرانية العاملة في المركز.
- تطوير بنية العمليات السيبرانية للمركز ، من خلال رفدها بأحدث الأدوات والمعدات التكنولوجية والأنظمة والمنصات العالمية التي تضمن الرفع من كفاءة الخدمات المقدمة من المركز.
- إطلاق نواة الأكاديمية الوطنية للأمن السيبراني.
- إطلاق جائزة التميز في الأمن السيبراني على المستوى الوطني.
- تطوير وتحسين برامج بناء القدرات الموجهة للشباب الأردني لتشمل فئات شبابية أكثر، واستناداً لمتطلبات سوق الأمن السيبراني محلياً وعالمياً.
- التوسع في بناء العلاقات التشاركية والتعاونية في الأمن السيبراني على المستويين الإقليمي والوطني.

صفحة المحتويات

المركز الوطني
للأمن السيبراني
National Cyber
Security Center

لجنة التقرير السنوي:

رئيس اللجنة:

المهندسة هبة علي أبو زيد

أعضاء اللجنة:

المهندس نادر الشماسنة

المهندس علاء الكساسبة

السيد عدي خريسات

تصميم وإعداد:

المهندس سليم الأشقر

www.ncsc.jo