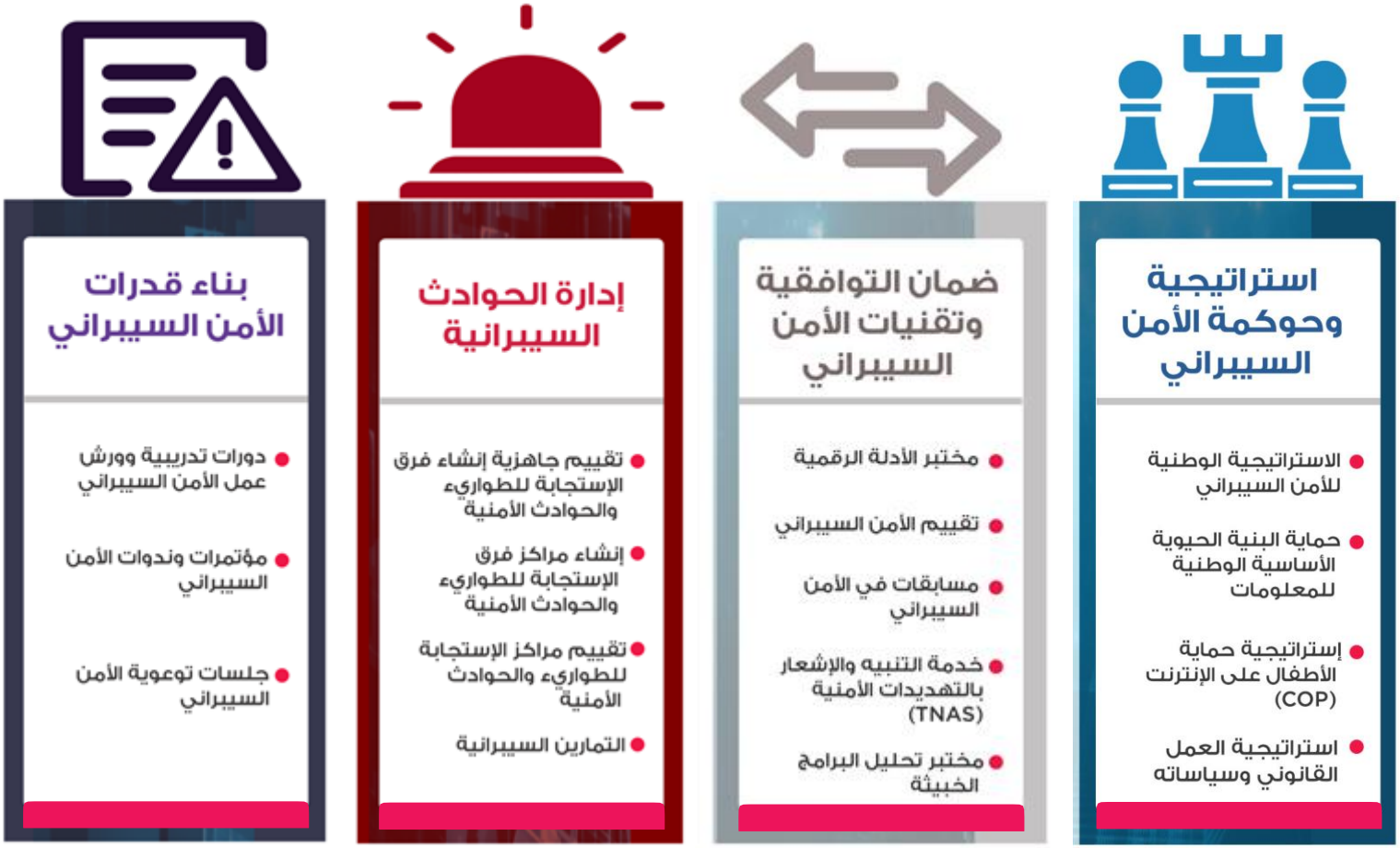
المركز العربي الإقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

المركز العربي الإقليمي للأمن السيبراني

دليل الخدمات

مخطط دليل الخدمات

يقدم المركز العربي الإقليمي للأمن السيبراني (ITU-ARCC) مجموعة متنوعة من خدمات الأمن السيبراني من أجل مواجهة التحديات والمخاطر الأمنية وتحقيق أهداف المركز. وتتوافق هذه الخدمات مع "جدول أعمال الأمن السيبراني العالمي" والتي تهدف بدورها إلى تحسين الثقة والأمن في المجتمع المعلوماتي – تم إطلاق جدول أعمال الأمن السيبراني في 17 مايو عام 2007 من أجل تعزيز التعاون الدولي ووضع استراتيجيات تعزز الوضع الأمني العالمي – ويقدم المركز العربي الخدمات التالية:



استراتيجية وحوكمة الأمن السيبراني

استراتيجية وحوكمة الأمن السيبراني

المركز العربي الإقليمي للأمن السيبراني بشكل وثيق مع الحكومات والقطاع العام لتطوير استراتيجيات الأمن السيبراني الوطنية، وتتضمن هذه الاستراتيجيات البرامج الفعالة في تحسين قدرات الأمن السيبراني وسد الثغرات في بيئة الأمن السيبراني.

- الاستراتيجية الوطنية للأمن السيبراني
- أستراتيجية العمل القانوني وسياساته
- إستراتيجية حماية الأطفال (COP) على الإنترنت
- حماية البنية الحيوية الأساسية الوطنية للمعلومات

الاستراتيجية الوطنية للأمن السيبراني

مقدمة

يعمل الخبراء في المركز العربي الإقليمي للأمن السيبراني بشكل وثيق مع الحكومات والقطاع العام لتطوير إطار عمل وطني لإدارة تطبيق استراتيجية وطنية للأمن السيبراني. والتي تتضمن برامج فعّالة لتعزيز قدرات الأمن السيبراني وسد الثغرات في بيئة الأمن السيبراني.

الأهداف

الأهداف الرئيسية للاستراتيجية الوطنية للأمن السيبراني هي:

- دراسة الحالة الراهنة للأمن السيبراني في الدول المختلفة واحتياجاتها وطرق إدارة المخاطر.
- دراسة المتطلبات والترتيبات اللازمة في المؤسسات والمنظمات لتطوير استراتيجية الأمن السيبراني الوطني الشاملة.
- تقديم التوصيات العامة لتحسين وضع الأمن السيبراني في الدول من أجل تطبيق الاستراتيجية الوطنية للأمن السيبراني.
- تنفيذ التدريب اللازم لنقل المعرفة المطلوبة في المفاهيم الأساسية المرتبطة بالأمن السيبراني الوطني مثل مفاهيم التطوير والتنفيذ والاستمرارية على المدى الطويل.

المخرجات

حلقة عمل الاستراتيجية الوطنية للأمن السيبراني بالإضافة إلى تقرير عام لنتائج التوصيات وخطة العمل لتأسيس وتحسين الاستراتيجية الوطنية للأمن السيبراني.

حماية البنية الوطنية الحيوية الأساسية للمعلومات

مقدمة

إن نجاح البنية الأساسية الوطنية من أهم عوامل نجاح القطاع الحكومي، حيث يعزز ازدهار هذه البنية من الاقتصاد الوطني، وبنفس الوقت يؤدي العجز والتراجع في هذه البنية إلى تراجع الاقتصاد الوطني.

الأهداف

فيما يلي الأهداف الرئيسية لإطار عمل البنية الوطنية الحيوية الأساسية للمعلومات

- تقييم الحالة الراهنة للبنية الأساسية لتقنية المعلومات وتشغيلها على المستوى الوطني والقطاعات المختلفة.
- دراسة وتقييم العمليات الحالية والأجهزة الإدارية والمؤسسات التي تسعى لتنفيذ إطار عمل الأمن السيبراني الوطني.
- معالجة المخاوف القائمة من خلال تحليل الثغرات في القطاعات الحيوية ومدى مشاركتها في خطة حماية البنية الحيوية الأساسية الوطنية للمعلومات.
- تقييم مدى الحاجة لبناء منصة مركزية تعالج المخاطر المرتبطة بالبنية الحيوية الأساسية للمعلومات على المستوى الوطني للدولة.

المخرجات

تقرير شامل يظهر النتائج الأساسية والتوصيات

استراتيجية حماية الأطفال على الإنترنت(COP)

مقدمة

يعتبر برنامج حماية الأطفال على الإنترنت من المبادرات التي أسسها الاتحاد الدولي للاتصالات (ITU) عام 2008 كجهد مشترك ضمن "جدول أعمال الأمن السيبراني العالمي". وتشكل هذه المبادرة شبكة تعاون دولية تهدف لحماية الأطفال عبر العالم من المخاطر السيبرانية وذلك من خلال توفير الإجراءات القانونية والتقنية والتنظيمية وتوفير القدرات اللازمة والتدابير الدولية المشتركة.

الأهداف

فيما يلي الأهداف الرئيسية لإستراتيجية حماية الأطفال على الإنترنت:

- تحديد المخاطر والثغرات الأمنية التي يتعرض لها الأطفال في الفضاء السيبراني.
- أيجاد الوعي اللازم لدى واضعي السياسات والصناعات التقنية وأهالي الأطفال والجهات التعليمية وحتى الأطفال أنفسهم.
- تطوير الأدوات العملية التي يمكن استخدامها لتقليل المخاطر.
مشاركة المعرفة والخبرات اللازمة لتأسيس فضاء سيبراني آمن

المخرجات

أستراتيجية حماية الأطفال على الإنترنت (COP)، والذي يوفر الأساس العالمي الذي يمكن من خلاله تحقيق الحماية للأطفال في الفضاء السيبراني على المستوى الوطني والإقليمي.

استراتيجية العمل القانوني وسياساته

مقدمة

يعد تبني التشريعات القانونية المناسبة جزءا لا يتجزأ من وضع استراتيجية وطنية للأمن السيبراني، مما يقدم الحماية اللازمة ضد إساءة استخدام تقنية المعلومات والاتصالات من قبل الجهات الإجرامية. كما يجب موائمة هذه التشريعات مع السياسات والممارسات الإقليمية والعالمية. ومن أجل ضمان بيئة إنترنت آمنة واستخدام منصف للجميع ومحاربة الجرائم السيبرانية يقوم المركز العربي الإقليمي بمساعدة الدول الأعضاء في الاتحاد الدولي للاتصالات في وضع التشريعات المناسبة وملائمتها مع إطار العمل القانوني وسياساته

الأهداف

يعتبر الهدف الرئيسي لإستراتيجية العمل القانوني وسياساته هو تقييم المسائل التالية وقياس نضوج المستوى القانوني للدول مقارنة بأفضل الممارسات الدولية:

- التدابير القانونية والاستجابة
- الجرائم الإلكترونية وقيود الاستخدام على تقنيات محددة
- حماية البيانات والملكية الفكرية
- التحقيقات الرقمية والأدلة الإلكترونية
- الخدمات الإلكترونية والتوقيع الرقمي.

المخرجات

تقرير موسّع للنتائج والمقترحات، حيث تظهر فيه نتائج إطار العمل القانوني وسياساته في وضع خارطة الطريق التي تحدد بدورها أولوية الأعمال ضمن إطار العمل القانوني للأمن السيبراني.

ضمان التوافقية وتقنيات الأمن السيبراني

ضمان التوافقية وتقنيات الأمن السيبراني

تهدف خدمات ضمان التوافقيه في تحقيق الأمن السيبراني وتقنياته إلى تقديم التدابير التقنية وتدابير الالتزام بالمعايير. ويستخدم الخبراء في المركز العربي الإقليمي للأمن السيبراني أفضل المعايير التقنية العالمية مثل الآيزو 27001 التي تمكن الدول الأعضاء من تحديد المواضع الواجب تحسينها أمنياً.

مختبر الأدلة الرقمية

تقييم الأمن السيبراني

خدمة التنبيه والإشعار بالتهديدات الأمنية (TNAS)

مسابقات في الأمن السيبراني

مختبر تحليل البرامج الخبيثة

مختبر الأدلة الرقمية

مقدمة

يعد علم الأدلة الرقمية تخصصاً يجمع ما بين الجانب القانوني وعلوم الحاسوب من أجل جمع وتحليل البيانات من الحواسب والشبكات والاتصالات اللاسلكية ووسائط التخزين بحيث يمكن تقديمها كدليل يؤخذ به في المحاكم.

الأهداف

الأهداف الرئيسية ما يلي:

- تسهيل عمل مركز الأدلة الرقمية (DFC)
- تزويد المركز الوطني للإستجابة للطوارىء والحوادث الأمنية (CIRT) بالقدرات المطلوبة في مجال الأدلة الرقمية.
- تحسين الخدمات التي يقدمها المركز الوطني للإستجابة للطوارىء والحوادث الأمنية (CIRT) في مجال تحديد وتفادي والاستجابة وإيجاد الحلول للحوادث الأمنية.

المخرجات

تقديم الوثائق المتعلقة بالأدلة الرقمية والتجهيزات المادية والحلول وتنفيذها والتدريب اللازم في مجال الأدلة الرقمية.

تقييم الأمن السيبراني

مقدمة

يعد الهدف العام لتقييم الأمن السيبراني هو مراجعة وتقييم مستوى المخاطر المرتبط بالتطبيقات البرمجية من حيث وجود ثغرات أمنية فيها واحتمالية كشف البيانات الحساسة المرتبطة بالبنية الأساسية للمؤسسه. ويستخدم الخبراء في المركز العربي الإقليمي للأمن السيبراني أفضل الطرق المناسبة والفعالة عند تنفيذ التقييم الأمني. ويتم التقييم في بيئة اختبار خاصة لضمان عدم تأثر الأنظمة الفعالة في الدولة أثناء الاختبار.

الأهداف

تعد الأهداف الرئيسية للتقييم الأمني ممثلة بما يلي:

- تنفيذ مراجعة التقييم الأمني لمؤسسات للدول الأعضاء.
- تحديد الثغرات المرتبطة بالبنية الأساسية لتقنية المعلومات والاتصالات والتطبيقات البرمجية في المؤسسة.
- تقييم فعالية الضوابط الأمنية الحالية وقدرتها في حماية البنية الأساسية من الهجمات.
- توفير خطة المعالجة أو خطة تقليل المخاطر التي تم تحديدها من أجل تقليل المخاطر المرتبطة بالبنية الأساسية للمؤسسة وبالتالي تحسين الوضع الأمني بشكل عام.

المخرجات

تقرير تقييم الأمن السيبراني، ويتضمن النتائج الرئيسية والتوصيات.

مسابقات في الأمن السيبراني

مقدمة

تقدم هذه التدريبات الفرصة لتنمية المهارات التقنية لدى المشاركين من خلال أنشطة الاختراق الأخلاقي خلال منافسات الأمن السيبراني، ويكون الهدف تمكين الفريق الوطني للمخاطر الأمنية المتقدمة من القيام بتقييم الثغرات بشكل طارئ أو القيام باختبارات الاختراق للبنية الأساسية للخدمات الإلكترونية من أجل تحديد الثغرات الأمنية الموجودة واقتراح الحلول اللازمة للتقليل من المخاطر الأمنية بشكل عام.

الأهداف

تتمثل الأهداف الرئيسية من هذه المنافسات في ما يلي:

- تقديم الفرصة للمشاركين لاختبار تجربة الاختراق الأخلاقي بشكل عملي وفعلي.
- تمكين المؤسسات من معرفة المشاكل والثغرات في البيئات الأمنية المرتبطة بمؤسساتهم.
- تعزيز روح الفريق ونقل المعرفة بين الخبراء

المخرجات

التدريبات المختلفة، تقديم المشورات حول المخاطر والثغرات

خدمة التنبيه والإشعار بالتهديدات الأمنية(TNAS)

مقدمة

يقدم المركز العربي الإقليمي للأمن السيبراني هذه الخدمة من خلال نشر المعلومات التي تصف الهجمات الخارجية والثغرات الأمنية والتهديدات والفيروسات والبرامج الخبيثة، وتقديم التوصيات على المدى القصير للقيام بالاستجابة لهذه التهديدات.
ويتم من خلال هذه الخدمة إرسال التنبيهات عند وجود مشكلة قائمة من أجل تنبيه المؤسسات المختلفة عن هذه المخاطر وتقديم التوجيهات اللازمة لحماية الأنظمة المختلفة أو استرجاع الأنظمة المتأثرة.

الأهداف

إرسال المعلومات المتعلقة بالمخاطر المرتقبة والثغرات الأمنية في الوقت المناسب.

المخرجات

التدريبات المختلفة، تقديم المشورات حول المخاطر والثغرات

مختبر تحليل البرامج الخبيثة

مقدمة

يقوم المركز العربي الإقليمي للأمن السيبراني من خلال المركز الوطني للإستجابة للحوادث الأمنية والطوارىء في دولة قطر بالتحليل الثنائي للملفات من أجل تحديد المخاطر المحتملة أو تقصي الدلائل على وجود محتوى ضار. هذه الملفات يتم جمعها كأدلة وإرسالها للقيام بعملية التحليل. ويتم جمع هذه الملفات أحيانا من البيانات التي تم استعادتها بعد التعرض للهجمات الإلكترونية، أو عمليات التجسس أو تعرض البنية الأساسية للاختراق.

الأهداف

جمع وتحليل المخاطر الأمنية من أجل تحديد تأثيراتها الأوسع على الدول

المخرجات

تقرير شامل يظهر تأثيرات الملفات الثنائية على المعلومات والموارد المتأثرة بالهجمات السيبرانية.

إدارة الحوادث السيبرانية

إدارة الحوادث السيبرانية

يعمل فريق المركز العربي الإقليمي للأمن السيبراني مع الشركاء على مساعدة وتشجيع الدول الأعضاء في الاتحاد الدولي للاتصالات في إنشاء فرق وطنية للاستجابة للطوارىء للحوادث الأمنية، حيث تأخذ هذه الفرق مسؤولية وطنية لتكون مركزا موثوقاً لتنسيق جهود الأمن السيبراني.
كما تساعد هذه الخدمة في تقييم مقدرات فرق الاستجابة للحوادث الأمنية في الحكومات والقطاع العام، وتحديد الثغرات وتقديم خارطة الطريق لتحسين هذه الفرق.

- تقييم مراكز الإستجابة للطوارىء والحوادث الأمنية
- إنشاء مراكز فرق الإستجابة للطوارىء والحوادث الأمنية
- تقييم جاهزية إنشاء فرق الإستجابة للطوارىء و الحوادث الأمنية
- التمارين السيبرانية

تقييم جاهزية إنشاء فرق الإستجابة للطوارىء والحوادث الأمنية

مقدمة

الغاية الرئيسية لهذه الخدمة هي مساعدة الدول التي تم تحديدها في تقييم جاهزيتها لبناء فريقها الوطني للطوارئ واللاستجابة لحوادث الأمن السيبراني. ويمتلك هذا الفريق القدرات اللازمة لتحديد والاستجابة للحوادث وإدارة المخاطر الأمنية وتحسين الوضع الأمني للدولة بشكل عام.

الأهداف

تكمن الأهداف الرئيسية لتقييم جاهزية إنشاء فرق الاستجابة للطوارىءوالحوادث الأمنية في ما يلي:

- دراسة وتحليل الوضع الحالي للأمن السيبراني في الدولة واحتياجاته.
- تقديم التوصيات العامة لتحسين الوضع الأمني في الدولة.
- دراسة واقتراح المتطلبات المؤسساتية وإجراء الترتيبات اللازمة لإنشاء الفرق الوطنية للاستجابة للحوادث.
- تنفيذ التدريبات اللازمة لبناء الموارد البشرية ونقل المعرفة والمهارات اللازمة لتشغيل واستمرارية الفرق الوطنية للاستجابة للحوادث الأمنية والتنسيق بينها وبين الوكالات المرتبطة بها محليا ودولياً.

المخرجات

تقرير جاهزية إنشاء فرق الاستجابة للطوارىء والحوادث الأمنية، ويحتوي على الحالة الراهنة لوضع الأمن السيبراني في الدولة والتوصيات المرتبطة بذلك.

إنشاء مراكز فرق الاستجابة للطوارىء والحوادث الأمنية

مقدمة

تتضمن هذه الخدمة مساعدة الحكومات في تشكيل فرق الاستجابة للطوارىء والحوادث الأمنية (CIRT)، إضافة لتطوير قدرات هذه الفرق لتأخذ مسؤولياتها الوطنية، ويتم ذلك ضمن ثلاث مراحل. وتتمثل الرؤية العامة بتسهيل تنفيذ الاستراتيجية العالمية للأمن السيبراني للأتحاد الدولي للاتصالات في الدول المختلفة. وتأخذ هذه الفرق مسؤولية وطنية لتكون مركزا موثوقاً لتنسيق جهود الأمن السيبراني في التحديد والحماية والاستجابة وإدارة المخاطر الأمنية.

الأهداف

تتمثل الأهداف الرئيسية لهذه الخدمة بما يلي:

- إنشاء الفرق الوطنية للاستجابة لحوادث الأمن السيبراني وتفعيلها بحيث تكون قادرة على دعم المؤسسات بالخدمات الأساسية للاستجابة للحوادث.
- بناء قدرات الموارد البشرية في مجال الأمن السيبراني وتدريب الحكومات على تشغيل فرق الاستجابة للطوارىء والحوادث الأمنية.
- تحسين الجاهزية الوطنية في تحديد ومنع حوادث الأمن السيبراني والاستجابة لها وإيجاد الحلول اللازمة في المؤسسات التي تشرف عليها فرق الاستجابة.
- ضمان الاستغلال الأمثل لفرق الاستجابة للطوارىء والحوادث الأمنية وضمان تشغيلها من خلال بناء هذه الفرق وتعزيز قدراتها بحيث تكون في أعلى جاهزية للاستجابة للحوادث الأمنية.
- تنفيذ ومراجعة واختبار العمليات اليومية ومساراتها وتطوير سير العمليات وأدوات فرق الاستجابة.

المخرجات

وثيقة تصميم فريق الاستجابة للطوارىء والحوادث الأمنية وخطة التنفيذ، دليل العمليات القياسية، كتيبات التشغيل، المواد التدريبية والأدوات المختلفة.

تقييم مراكز الإستجابة للطوارىء والحوادث الأمنية

مقدمة

الهدف الرئيسي من تحليل الثغرات هو دراسة وتقييم جاهزية البنية الحكومية الحالية لبناء فرق الاستجابة والقدرات اللازمة في هذه الفرق من أجل ضمان الإدارة الملائمة للحوادث الأمنية ومحاولات الاختراق والحالات الطارئة، ومعالجتها ضمن المعايير القياسية ووفق أفضل الممارسات.
ويتم تحليل الثغرات بالاستناد إلى مجموعة محددة من الشروط والعوامل التي يتم استخدامها في تقدير الوضع الراهن لفرق الاستجابة مقارنة بمعايير القياس. كما يتم استخدام بيانات التحليل من قبل أصحاب القرار لتحديد فيما إذا كانت الحالة الراهنة لفرق الاستجابة مقبولة أو أنها تحتاج للمزيد من التحسينات.

الأهداف

الأهداف الرئيسية لتحليل الثغرات في هذه الخدمة:

- دراسة كافة السياسات الحالية والإجراءات والنماذج التي تم وضعها للاستجابة للحوادث والاختراقات أو عمليات الاستجابة للحالات الطارئة.
- مراجعة عملية تقييم المخاطر الحالية المستخدمة في تحديد الحوادث الأمنية والاختراقات وعمليات الاستجابة للحالات الطارئة.
- تقييم الأدوات التي تم تصميمها واستخدامها لمنع واكتشاف الحوادث الأمنية أو الاختراقات.
- تقديم تقرير التوصيات الشاملة لمعالجة الثغرات الحالية إن وجدت وذلك وفق أفضل الممارسات.

المخرجات

تقرير عن ثغرات فرق الاستجابة للطوارىء والحوادث الأمنيه وتتضمن كافة نقاط الضعف والتوصيات اللازمة لسد هذه الثغرات.

التمرينات السيبرانية

مقدمة

يتم تنفيذ التمرينات السيبرانية حتى يتمكن المشاركين من الاختبار العملي لحوادث حقيقية وبناء على حالات قد حدثت فعلياً، ويتكون المشاركين عادة من فرق الاستجابة للطوارىء للحالات الطارئة او المختصين بالأمن السيبراني. كما توفر هذه التمرينات الفرصة لهذه الفرق لاختبار مهاراتهم ومعرفتهم في الاستجابة لهذه الهجمات. كما يسبق التمرين حلقة عمل تتناول مجموعة من العناوين الهامة في معالجة حالات الاستجابة للطوارئ.

الأهداف

الهدف الرئيسي من التمرين السيبراني هو تفعيل التواصل وروح الفريق وقدرات الاستجابة للحوادث لدى الفرق المشاركة، من أجل ضمان توحيد الجهود في مواجهة التهديدات السيبرانية في المنطقة.

المخرجات

تنفيذ التمرين السيبراني وتقرير المشاركة للمؤسسات المختلفة.

بناء القدرات في الأمن السيبراني

بناء القدرات في الأمن السيبراني

إن بناء القدرات في الأمن السيبراني يساعد على بناء قدرات المؤسسة وتطوير حلول وثقافة فعّالة وتلقائية، بالإضافة إلى أن هذه الخدمة تقوم برفع الوعي على مستوى المجتمع والمجموعات وعلى المستوى الوطني أيضاً كما تساهم هذه الخدمة بتوفير برامج تدريبية في الأمن السيبراني وبرامج التطوير.

- دورات تدريبية وورش عمل الأمن السيبراني
- مؤتمرات وندوات الأمن السيبراني
- جلسات توعويه للأمن السيبراني

دورات تدريبية وورش عمل الأمن السيبراني

مقدمة

يساعد بناء القدرات في الأمن السيبراني الدول في بناء أمن سيبراني مؤسساتي وتطوير حلول وثقافة فعّالة وتلقائية.
يوفر المركز العربي الإقليمي للأمن السيبراني برامج تدريبية وورش عمل محددة بمحتوى مخصص للأمن السيبراني بناء على طلب الشركاء أو بناء على المهارات التي تم تحديدها في أي مجال من مجالات الأمن السيبراني.

الأهداف

الهدف الرئيسي هو توفير برامج تدريبية احترافية وورش عمل للتغلب على التحديات الحالية والمستقبلية في مجال أمن المعلومات، كما يتم ذلك من خلال دراسة حالات محددة وقصص النجاح التي تظهر كيفية تغلب المؤسسات على الهجمات السيبرانية.

المخرجات

برامج تدريبية تخصصية ذات محتوى مخصص، حلقات عمل الأمن السيبراني

مؤتمرات وندوات الأمن السيبراني

مقدمة

ينظم المركز العربي الإقليمي للأمن السيبراني المؤتمرات والندوات على المستوى الوطني والإقليمي والدولي والتي من شأنها التركيز على المواضيع العامة من تدابير الأمن السيبراني وآخر المستجدات.
وحيث أن الحضور في هذه المؤتمرات يشتمل على ممثلين من الدول الأعضاء وأصحاب المصلحة وأفراد من جهات مختلفة، فإن هذه المؤتمرات تعمل كمحفز فعّال في هذه الدول لمعالجة الحالة الراهنة وخلق تواصل شفاف يعزز التعاون والتكامل في بناء بنية الأمن السيبراني الوطنية.

الأهداف

إن الهدف الرئيسي للمؤتمرات والندوات هو توفير نظرة عامة على إيجاد وتطوير والمحافظة على أمن المعلومات وحمايتها من التهديدات المختلفة على المستوى الوطني والإقليمي والدولي، وذلك من خلال توفير التعليم والمعلومات عن الطرق التي تقلل المخاطر وتخفف من نتائج الهجمات السيبرانية.

المخرجات

المؤتمرات والندوات والقمم والمنتديات

جلسات توعوية للأمن السيبراني

مقدمة

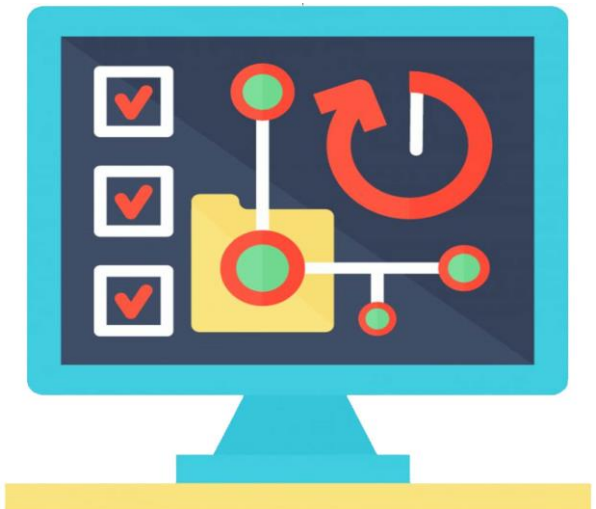
إن أي شخص يعمل في بيئة تقنية معلوماتية لابد أن يكون عرضة للتهديدات التي تواجهها هذه البيئات من حيث الاستخدام الاعتيادي لها. ومن أجل الاستفادة القصوى من التقنيات يجب على المستخدمين امتلاك المعرفة بالممارسات والطرق الآمنة من أجل تقليل المخاطر المرتبطة باستخدام هذه التقنيات.

الأهداف

مساعدة مستخدمي التقنيات على فهم أسس أمن المعلومات والتهديدات المرتبطة باستخدام تقنية المعلومات والاتصالات والممارسات الأمنية التي تساعد في تقليل الحوادث الأمنية

المخرجات

جلسات التوعية، الحملات والمنافسات.



ITUARCC ITU-ARCC iturcc