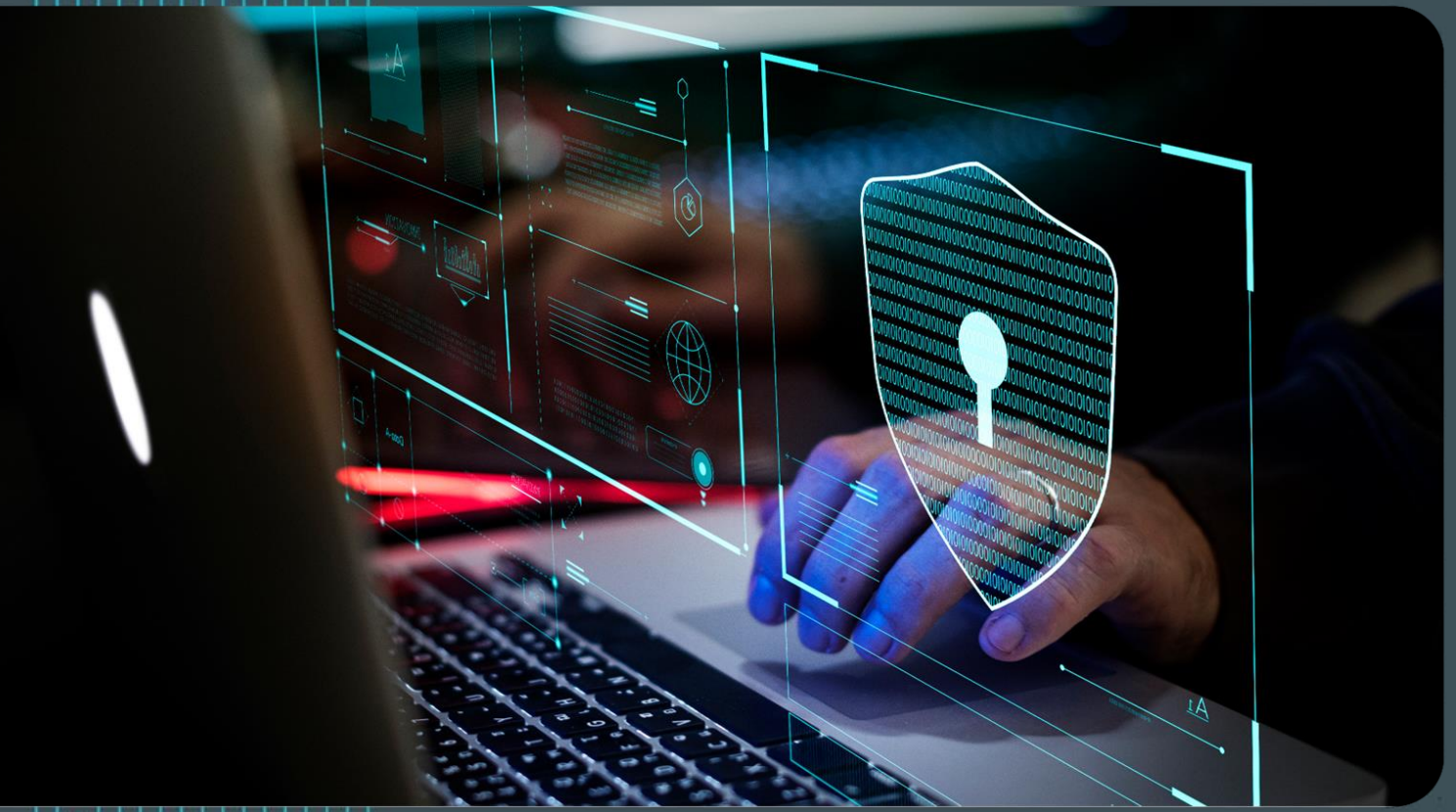
المركز الوطني
للأمن السيبراني
National Cyber
Security Center



الأمن السيبراني وأمن البنية التحتية

المقدمة

- الأمن السيبراني هو قضية وطنية تؤثر على أمن واستقرار الدولة.
- الأمن السيبراني هو أيضًا مشكلة تتعلق بالأعمال التجارية تؤثر على أداء وتنافسية المؤسسات.
- الأمن السيبراني نهجاً شاملاً واستباقياً يشمل جميع الأطراف المعنية والقطاعات.
- ستقدم هذه الدورة نظرة عامة على إطار الأمن السيبراني الوطني الأردني (JNCSF)، الذي يهدف إلى تعزيز الأمن السيبراني في البنية التحتية الوطنية.

ما هي البنية التحتية الوطنية؟

- تشير البنية التحتية الوطنية إلى الأنظمة والخدمات التي تعتبر أساسية لوظيفة البلد ورفاهيته لمواطنيه.
- تشمل البنية التحتية الوطنية قطاعات مثل الطاقة والمياه والنقل والصحة والاتصالات والتمويل.
- تعتمد البنية التحتية الوطنية بشكل متزايد على التكنولوجيا والإنترنت، مما يجعلها عرضة للتهديدات السيبرانية.

ما هي التهديدات السيبرانية للبنية التحتية الوطنية؟

- التهديدات السيبرانية هي الأنشطة الضارة التي تهدف إلى التسلل إلى سرية أو سلامة أو توافر البيانات أو الأنظمة أو الخدمات.
- يمكن أن تأتي التهديدات السيبرانية من مصادر مختلفة مثل القراصنة والإرهابيين.
- يمكن أن تكون للتهديدات السيبرانية تأثيرات مختلفة مثل الخسائر المالية والضرر بالسمعة واضطراب الخدمات أو الضرر الجسدي.

ما هي التحديات في حماية البنية التحتية الوطنية؟

حماية البنية التحتية الوطنية من التهديدات السيبرانية هو تحدي معقد ومتعدد الجوانب يشمل عوامل مختلفة مثل:

- تنوع وتعقيد قطاعات البنية التحتية وترابطاتها.
- طبيعة التهديدات السيبرانية وتطورها والتقنيات المستخدمة من قبل المهاجمين.
- نقص الوعي والمهارات بين مشغلي ومستخدمي البنية التحتية.
- الفجوات في الإطارات القانونية والتنظيمية والمعايير والإرشادات للأمن السيبراني.

الأمن في التصميم

- الأمن في التصميم هو القدرة على تصميم وتنفيذ خطة أمن شاملة للمؤسسة.
- تتضمن هذه القدرة إدخال تغييرات جوهرية في الهندسة المعمارية الحالية للمؤسسة، بما في ذلك أنظمتها وعملياتها وسياساتها.
- تتضمن هذه القدرة أيضًا اعتماد نهج "الأمن في التصميم"، مما يعني دمج الاعتبارات الأمنية في تصميم وتطوير جميع الأنظمة والعمليات منذ البداية.

الأمن في التصميم - الفوائد

من فوائد قدرة الأمن في التصميم:

- يوفر اتجاهًا وإطارًا واضحًا لاتخاذ القرارات بشأن الأمن السيبراني.
- يتيح للمؤسسة تركيز مواردها وجهودها على أهداف ومخاطر أكثر أهمية.
- يضمن أن تكون التدابير الأمنية مدمجة في جميع جوانب أنظمة وعمليات المؤسسة، وليس مجرد إضافتها كخطوة متأخرة.
- يقلل من احتمالية وتأثير انتهاكات الأمن والحوادث.

الأمن في التطوير

- الأمن في التطوير هو القدرة على دمج الاعتبارات الأمنية في تطوير الأنظمة والعمليات.
- تتضمن هذه القدرة تطبيق أفضل الممارسات والمعايير الأمنية طوال دورة حياة عملية التطوير, ابتداء من التخطيط والتصميم وانتهاء بالاختبار والنشر.
- تتضمن هذه القدرة أيضًا ضمان تعريف وتلبية متطلبات الأمان، وإجراء اختبارات وتحقق من الأمان.

الأمن في التطوير - الفوائد

من فوائد قدرة الأمن في التطوير:

- يضمن أن تكون الأنظمة والعمليات آمنة وموثوقة من البداية، مما يقلل من الحاجة إلى إجراءات إصلاحية مكلفة ومستهلكة للوقت في وقت لاحق.
- يعزز جودة وأداء الأنظمة والعمليات، مما يعزز تجربة ورضا المستخدم.
- يزيد من الابتكار والتنافسية للمؤسسة، مما يمكنها من إنشاء منتجات وخدمات جديدة تلبي احتياجات وتوقعات العملاء.
- يدعم الامتثال للمتطلبات القانونية والتنظيمية والمطابقة مع المعايير وأفضل الممارسات في الصناعة.

الأمن في التسليم

- الأمن في التسليم هو القدرة على نشر وصيانة أنظمة وعمليات آمنة.
- تتضمن هذه القدرة ضمان أن تكون الأنظمة والعمليات مثبتة ومكونة ومُحَدّثة بأمان، وأن يتم تطبيق تصحيحات وتحسينات الأمان في الوقت المناسب.
- تتضمن هذه القدرة أيضًا ضمان أن تكون الأنظمة والعمليات متاحة وتعمل بالشكل الموطلوب ,وأن تقلل من اضطراب الخدمة أو تجنبه.

الأمن في التسليم - الفوائد

من فوائد قدرة الأمن في التسليم:

- يضمن أن تكون الأنظمة والعمليات محمية من الوصول أو التعديل غير المصرح به، وأن تكون البيانات محمية من الفقدان أو السرقة.
- يضمن أن تكون الأنظمة والعمليات متاحة وتعمل بالشكل الأفضل, وأن يتم تقليل أو تجنب اضطرابات الخدمة.
- يضمن أن تكون الأنظمة والعمليات قابلة للتوسع والتكيف، وأن تُدار وتُراقب التغييرات.
- يضمن أن تكون الأنظمة والعمليات متسقة ومتوافقة، وأن يتم تيسير التوافق والتكامل.

الأمن في التشغيل

- الأمن في التشغيل هو القدرة على مراقبة وإدارة أمن الأنظمة والعمليات.
- تتضمن هذه القدرة جمع وتحليل البيانات والمعلومات الأمنية، مثل السجلات والتنبيهات والتقارير، وتحديد والاستجابة للحوادث والأحداث الأمنية.
- تتضمن هذه القدرة أيضًا إجراء تدقيقات وتقييمات أمنية، وتنفيذ تحسينات وتعزيزات أمنية.

الأمن في التشغيل - الفوائد

من فوائد قدرة الأمن في التشغيل:

- يوفر رؤية وتحليلا لحالة وأداء الأمان للأنظمة والعمليات، ويمكن من الكشف عن التهديدات الأمنية ومنعها.
- يوفر مساءلة ودليلًا لإجراءات الأمان والنتائج، ويمكن من التحقق من التدابير الأمنية.
- يوفر ردود فعل وتعلمًا لتحسين الأمان، ويمكن تحسين العمليات والممارسات الأمنية بشكل مستمر.
- يوفر المرونة والاستعادة للحوادث والأحداث الأمنية، ويمكن استعادة العمليات الطبيعية وتقليل التأثيرات.

القدرات الأساسية

القدرات الأساسية هي التدابير الأمنية الأساسية التي لا غنى عنها لأي مؤسسة، بغض النظر عن حجمها أو قطاعها أو طبيعتها.

تشمل هذه القدرات ما يلي:

الحوكمة: إنشاء وتنفيذ سياسة واستراتيجية وإطار أمني يحدد أهداف الأمن للمؤسسة والأدوار والمسؤوليات.

التوعية والتدريب: توفير وتعزيز برامج وأنشطة التعليم والتوعية الأمنية التي تعلم وتمكّن موظفي المؤسسة والأطراف المعنية.

إدارة المخاطر: تحديد وتقييم ومعالجة المخاطر الأمنية التي تؤثر على أنظمة وعمليات وبيانات المؤسسة.

إدارة الحوادث: إعداد وتنفيذ خطة استجابة لحوادث الأمن تحدد إجراءات المؤسسة والإجراءات للتعامل معها ومحاولة إيجاد الحلول.

القدرات الأساسية - الفوائد

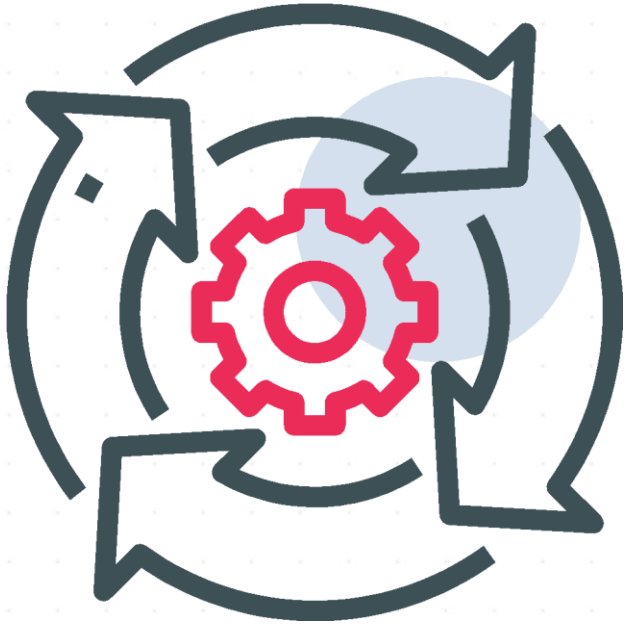
من فوائد القدرات الأساسية:

- نها توفر الأساس والمتطلبات الدنيا لوضع المؤسسة للأمن وأدائها.
- أنها تضمن أن تلتزم المؤسسة بالقوانين والتنظيمات والمعايير والإرشادات للأمن السيبراني.
- أنها تضمن أن المؤسسة لديها نهج واتجاه واضح ومتسق للأمن السيبراني.
- أنها تضمن أن لدى المؤسسة المهارات والموارد اللازمة للأمن السيبراني.

الأمن في المسؤولية الوطنية للأمن السيبراني

- الأمن في المسؤولية الوطنية للأمن السيبراني هو القدرة على التعاون والتنسيق مع الكيانات والأطراف الأخرى لتعزيز الأمن السيبراني الوطني.
- تتضمن هذه القدرة مشاركة المعلومات والخبرة، والمشاركة في المبادرات والبرامج، ودعم جهود المركز الوطني للأمن السيبراني وسلطات أخرى ذات الصلة.
- تتضمن هذه القدرة أيضًا المساهمة في تطوير وتنفيذ استراتيجية الإطار الوطني للأمن السيبراني، والمواءمة مع الأهداف والمبادئ الوطنية للأمن السيبراني.

الأمن في المسؤولية الوطنية للأمن السيبراني - الفوائد



من فوائد قدرة الأمن في المسؤولية الوطنية للأمن السيبراني:

- إنه يعزز التعاون والتنسيق بين الكيانات والأطراف الوطنية، ويعزز ثقافة الثقة والتشاركية.
- إنه يحسن الوعي والاستعداد لدى الكيانات والأطراف الوطنية، ويعزز المرونة والاستجابة للأمن السيبراني الوطني.
- يدعم تحقيق ومواءمة الأهداف والمبادئ الوطنية للأمن السيبراني، ويسهم في الأمن الوطني والاستقرار.
- يعزز السمعة والتقدير للأمن السيبراني الوطني، ويعرض الإنجازات والقدرات الوطنية.

الاستنتاج

- إن الأمن السيبراني مشكلة وطنية ومشكلة مؤسسية تؤثر على أمن واستقرار البلد وأداء وتنافسية المؤسسة.
- إن الأمن السيبراني يتطلب نهجًا شاملًا ومبادرًا يشمل جميع الأطراف والقطاعات.

شكرا لكم نتمنى لكم

السلامة في العالم الرقمي