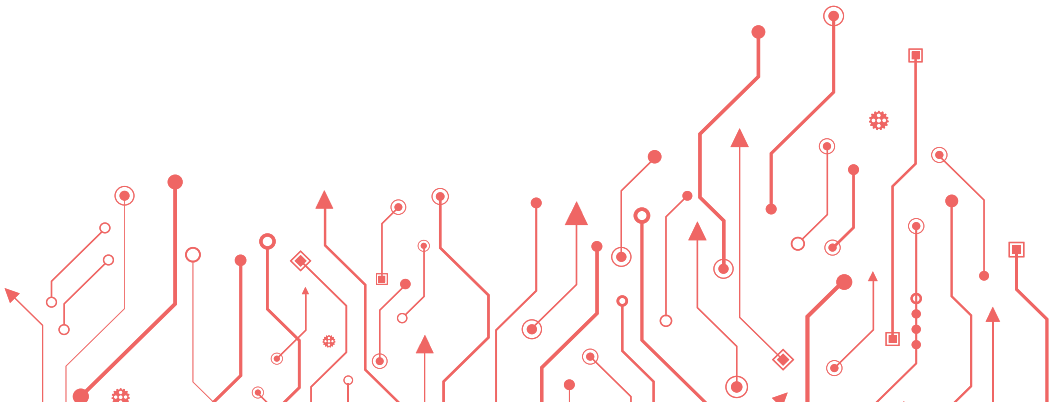

المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER
ابدأ
حياتك المهنية في
الأمن السيبراني

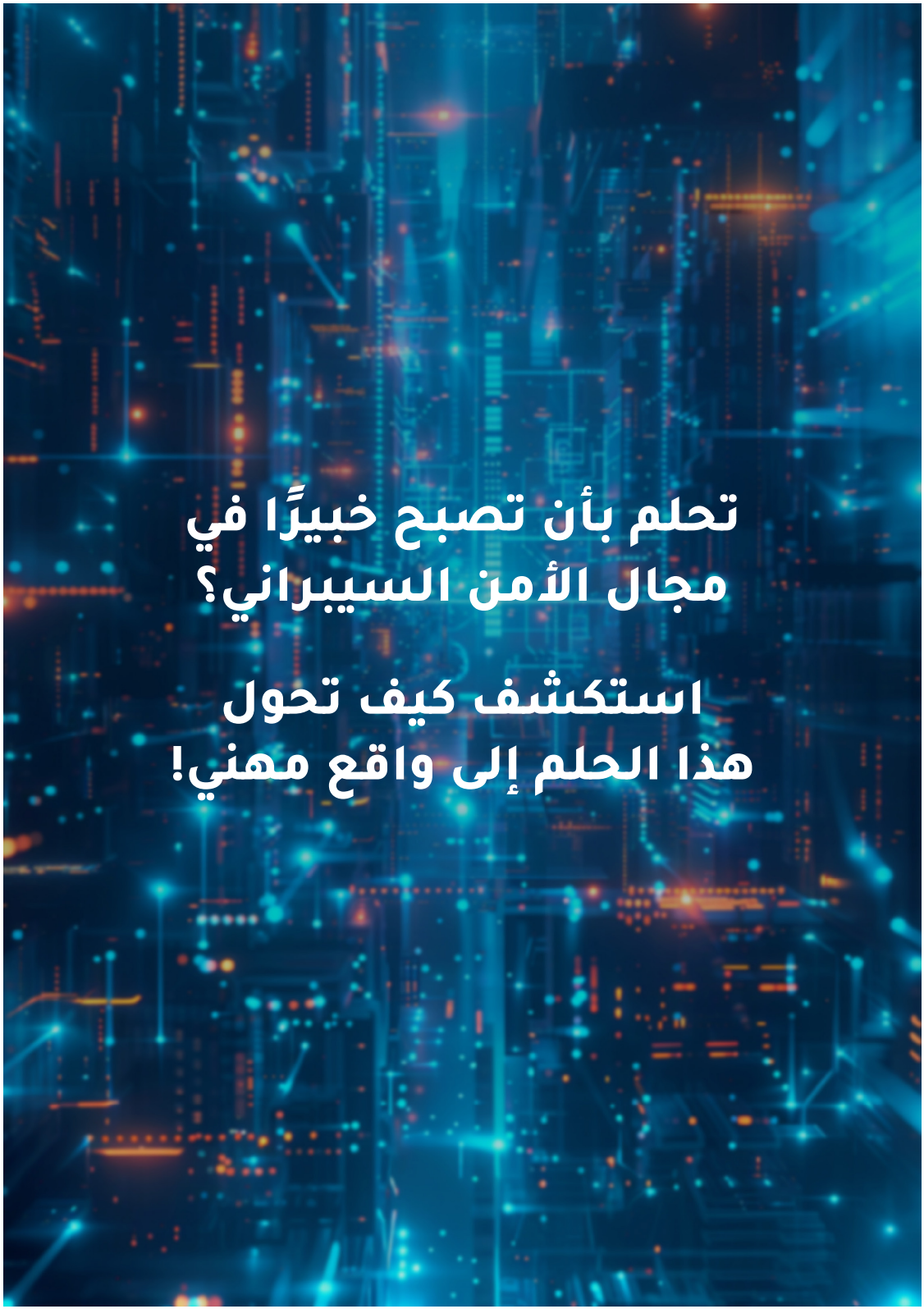
مرحباً.....

حياتك المهنية في مجال الأمن
السيبراني تبدأ هنا!



مرحبًا "بكم في عالم مهنة الأمن السيبراني"

"في عصرنا الرقمي، أصبح الأمن السيبراني أمراً بالغ الأهمية، حيث يوفر فرصاً متنوعة للحماية من التهديدات الإلكترونية. يجمع هذا المجال بين مهارات التكنولوجيا والتفكير النقدي في حل التحديات والإبداع والتطوير بهدف حماية الأفراد والمؤسسات والدول. يقدم لك هذا الكتيب المعرفة حول مصطلحات الأمن السيبراني الأساسية والتخصصات المختلفة بهذا المجال، بالإضافة إلى تسليط الضوء على المسارات الوظيفية المحتملة التي ستساعدك على استكشاف الأثر الذي يمكنك إحداثه ودورك في تأمين عالمنا الرقمي"


تحلم بأن تصبح خبيرًا في
مجال الأمن السيبراني؟
استكشف كيف تحول
هذا الحلم إلى واقع مهني!

اكتشف الأمن السيبراني

هل أنت مهتم باستكشاف عالم الأمن السيبراني واختيار هذا المجال كمهنة؟

إذا كانت إجابتك نعم، تساءل وفكر

- هل تحب العمل على التقنيات الحديثة؟ نعم أو كلا
- هل تستمتع بإيجاد حلول مبتكرة للتحديات؟ نعم أو كلا
- هل تعلم أن كل شيء نستخدمه اليوم متصلاً بالإنترنت بطريقةٍ ما؟ نعم أو كلا
- هل يوجد عدد كافياً من خبراء الأمن السيبراني لحمايتنا من التهديدات السيبرانية؟ نعم أو كلا
- هل لديك الرغبة لتصبح مدافعاً وتحمي الفضاء السيبراني؟ نعم أو كلا

الأمن السيبراني: ممارسات الحماية والدفاع للبنى التحتية التقنية والتي تتضمن البيانات وشبكات وأجهزة تكنولوجيا المعلومات والاتصالات من المخاطر والهجمات السيبرانية المحتملة.

أبدا مسيرتك المهنية في مجال الأمن السيبراني

أعزائي الطلبة!
هـل تعلـم أن العالـم يحتـاج حوالـي **1.8 مليـون متخصص مؤهل فـي الأمن السـيبراني** للحفـاظ علـى أمن أنظمة الحاسـوب والشـبكات من الوصـول غير المصرح بـه والهجمات السيبرانية؟ إذا كنت مهتماً بمجال الأمن السيبراني، فإليك ما يمكنك القيام به الآن:

01

أقـرأ عـن المهـن فـي مجـال الأمـن السـيبراني للتعـرف علـى الوظائـف المختلفة في هذا المجال.

02

انضم أو بادر بإنشاء نادٍ في مجال تقنية المعلومـــات أو الأمـــن السيبرانـــي في مـدرستك.

03

اسأل معلميك حول مفاهيم الأمـن السيبراني في فصولك الدراسية.

04

اشـــترك في دورات الرياضيـــــات المتقدمـــة أو العلـــوم أو المـــواد الإبداعية، مثل: الكتابة والفن.

05

اسـأل أخصائـــي التكنولوجيـــــا بالمدرسة عـن فـرص وظيفية للأمـن السيبراني.

أبدا الآن!

دروس بإمكانك البدء فيها في المرحلة الثانوية

- [ ] علوم الرياضيات المتقدمة
- [ ] الكتابة الإبداعية (الإنجليزية والعربية والإعلام)
- [ ] أخلاقيات الإنترنت
- [ ] الموضوعات المتعلقة بتكنولوجيا المعلومات

تخصصات المرحلة الجامعية

- [ ] علوم الحاسوب
- [ ] تكنولوجيا المعلومات
- [ ] الأمن السيبراني
- [ ] الذكاء الاصطناعي والأمن السيبراني
- [ ] هندسة الحاسوب
- [ ] علم البيانات وتقنيات الحوسبة السحابية

طرق أخرى تُمكنك من التقدم في هذا المجال

- [ ] المشاركة في مسابقات الأمن السيبراني المحلية أو في برامج المخيمات الصيفية بذات المجال.
- [ ] قم باستشارة معلميك أو المشرف حول المسارات الوظيفية في الأمن السيبراني.
- [ ] ابدي اهتمامك واسأل معلميك عن مفاهيم الأمن.

ملاحظاتي

الخيارات المهنية

استكشف التخصصات التالية واكتب وصفًا موجزًا لها:

خبير التشفير

أخصائي أمن سيبراني -الاستجابة للحوادث الأمنية

خبير تحليل الأدلة الرقمية / فاحص أدلة رقمية

مستشار قانوني في الأمن السيبراني

مهندس أمن سيبراني

مدير أمن نظم المعلومات

محلل لغة متعدد التخصصات

مطور برامج

محلل تقييم الضعف الأمني

مدير تقنية المعلومات

محقق الجرائم السيبرانية

أخصائي دعم فني

أخصائي تشغيل سيبراني

أخصائي اختبار وتقييم النظام

مسؤول الأنظمة / مدير الشبكات

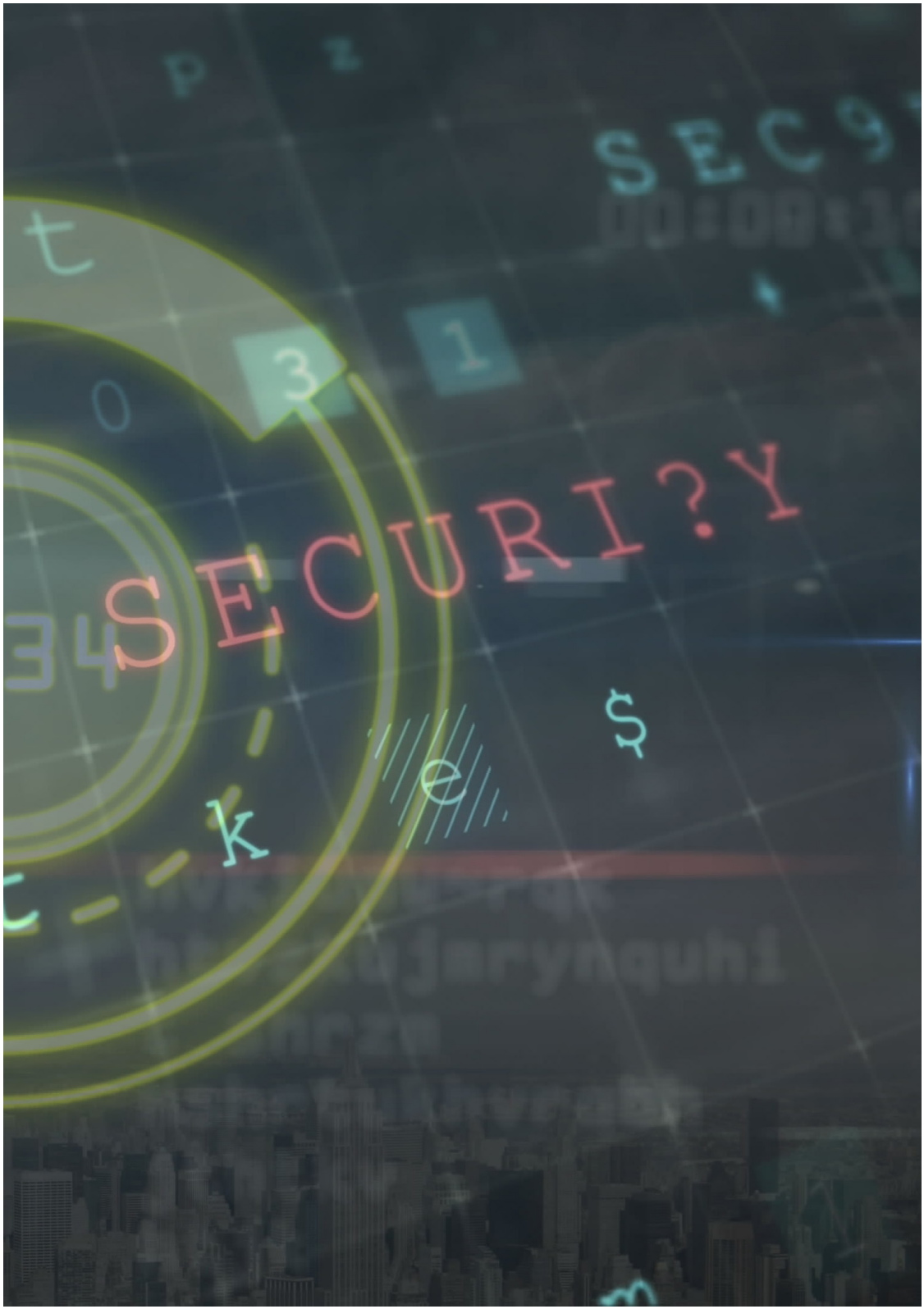
مخطط العمليات السيبرانية

محلل سلامة المعلومات

مدير المعرفة

اخصائي اختبار الاختراق

محلل التهديد والتحذير السيبراني


SECURI?Y

وسائط الذكاء الاصطناعي

مصطلحات الأمن السيبراني

فيما يلي 27 مصطلحًا أساسيًا في الأمن السيبراني والمفاهيم التي يمكنك تعلمها لبدء المعرفة في هذا المجال:

01 الأمن السيبراني

حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من عتاد وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات، والأمن الإلكتروني، والأمن الرقمي ونحو ذلك.

02 الفضاء السيبراني

الشبكة المترابطة من البنية التحية لتقنية المعلومات، والتي تشمل الإنترنت، وشبكات الاتصالات، وأنظمة الحاسب، والأجهزة المتصلة بالإنترنت؛ إلى جانب العتاد وأجهزة التحكم المرتبطة بها.

03 البنية التحتية الوطنية الحساسة

هي العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها) التي يؤدي فقدانها أو تعرضها لانتهاكات أمنية إلى:

- أثر سلبي كبير على توافر الخدمات الأساسية، أو تكاملها، أو تسليمها بما في ذلك الخدمات التي يمكن أن تؤدي في حالة تعرض سلامتها للخطر؛ إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات - مع مراعاة الآثار الاقتصادية و/أو الاجتماعية على المستوى الوطني.
- تاثير كبير على الأمن الوطني و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.

04 التوافر

ضمـان إمكانيـة الوصـول والاسـتخدام عنـد الطلـب، مـن مسـتخدم أو إجـراء أو نظـام مصرح له بشكل يعتمد عليه.

05 السلامة

الحمايـة ضـد تعديـل المعلومات أو تخريبها بشـكل غيـر مصرح به، كما تشـمل ضمان عدم الإنكار للمعلومات والأصالة.

06 السرية

خاصيـة عـدم الإفصاح عن المعلومات لمسـتخدم أو إجراء أو نظام غيـر مصرح له إلا في حالة وجود تصريح لهم للوصول إليها.

07 توكيد المعلومات

التدابيـر التـي تحمـي المعلومـات، وأنظمـة المعلومـات، مـن خلال ضمـان توافرهـا وسلامتها وأصالتها، وعدم الإنكار للمعلومات وسريتها.

ملاحظاتي

08 المسؤولية

القـدرة على تتبع مسـار نشـاط أو حدث معين حتـى الوصول إلى الطرف المسـؤول؛ من منشـئ النشـاط. ويدعـم ذلك عدم الإنكار، تشـخيص الخطأ اكتشـاف ومنع التسـللات، وإجراءات ما بعد الاكتشاف كالتعافي والإجراءات القانونية.

09 التحقق من الهوية

التأكـد مـن هويـة المسـتخدم، أو العمليـة، أو الجهـاز، وغالبـاً ما يكـون هذا الأمر شـرطاً أساسـياً للسـماح بالوصول إلى الموارد التقنية. وليس له علاقـة بتحديد حقوق الوصول الموارد والأصول التقنية.

10 التحقق من الهوية متعددة العناصر

نظـام أمنـي يتحقـق من هويـة المسـتخدم؛ يتطلب اسـتخدام عدة عناصر مسـتقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر:

- المعرفة: شيء يعرفه المستخدم (مثل كلمة المرور).
- الحيـازة: شـيء يملكـه المسـتخدم (مثـل برنامـج أو جهاز توليـد أرقام عشـوائية أو رسائل قصيرة مؤقت لتسجيل الدخول) ويطلق عليه (one-time password)
- الملازمة: صفة أو سـمة حيوية متعلقة بالمسـتخدم نفسـه فحسـب (مثل بصمة الإصبع).

ملاحظاتي

11 التصريح

تعريف حقوق/تراخيص الوصول إلى الموارد الأصول المعلوماتية والتقنية للجهة بشكل عام، والتحكم بمستويات الوصول على وجه الخصوص، والتأكد منها.

12 أصل

الموارد الملموسة، أو غير الملموسة، ذات قيمة للجهة، بما في ذلك الموظفين، والتقنيات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات، والمعلومات والخصائص (مثل: سمعة الجهة وهويتها وقدراتها المعرفية أو المهنية).

13 التشفير

القواعد التي تشمل على مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به والتعديل غير المكتشف، بحيث لا يمكن للأشخاص غير المعنيين قرائتها ومعالجتها.

14 صمود الأمن السيبراني

القدرة الشاملة للجهة على التصدي للحوادث السيبرانية وامتصاص الأضرار والتعافي منها في الوقت المناسب.

ملاحظاتي

15 دفاع امني متعدد المستويات

مفهـوم يُعنى بوضوح مسـتويات دفاعية متعـددة من الضوابط الأمنيـة وذلك بالتكامل بين الأشخاص، التقنية والقدرات التشغيلية.

16 هجوم سيبراني

اسـتغلال غيـر مشـروع لأنظمة الحاسـب، والشـبكات، والمنظمات التـي يعتمد عملها علـى تقنيـة المعلومات والاتصـالات الرقمية؛ بهدف إحـداث أضرار. وتشـمل أي نوع من الأنشـطة الخبيثـة التي تحاول الوصول غير المشـروع أو تعطيل، أو منـع، أو تدمير موارد النظم المعلوماتية، أو المعلومات نفسها.

17 هجمات حجم الخدم الموزعة

هـي محـاولات لتعطيل النظـام، وجعل خدماتـه غير متوافـرة؛ عن طريق إرسـال طلبات كثيرة من أكثر من مصدر في الوقت نفسه.

18 رسائل التصيّد الإلكتروني

التنكـر علـى هيئة جهـات جديرة بالثقـة عن طريق رسـائل بريدية إلكترونيـة للحصول على معلومـات حساسـة، مثـل أسـماء المسـتخدمين، وكلمات المـرور، أو تفاصيـل بطاقة الائتمان، وذلك لأسباب ونوايا ضارة خبيثة.

ملاحظاتي

19 المعلومات الاستباقية للتهديدات

معلومـات منظمـة قد تـم تحليلها حـول الهجمات الاخيـرة، والحاليـة، والمحتملة، والتي يمكن أن تشكل تهديداً سيبرانياً للمنظمة.

20 مشاركة المعلومات

تبـادل البيانـات والمعلومـات، أو المعرفـة -أو كليهمـا- لاسـتخدامها فـي إدارة المخاطر والتهديدات أو الاستجابة للأحداث السيبرانية.

21 البرمجيات الضارة

برنامـج يصيـب الأنظمـة بطريقـة خفية (فـي الغالب) بغايـة انتهاك سـرية أو سلامة أو توافر بيانات الضحية أو تطبيقاته أو نظم التشغيل الخاصة به.

22 برمجيات الفدية

برمجيـات ضـارة تجعل بيانات وأنظمـة الضحية غير قابلة للاسـتخدام لحين دفعه لمبلغ مالي.

23 التعافي من الكوارث

الأنشـطة والبرامـج والخطط المصممة؛ لإرجـاع الوظائف وخدمات الأعمال الحساسـة للجهـة؛ إلـى حالتهـا الطبيعيـة، وذلـك بعـد التعـرض إلـى هجمـات سـيبرانية أو تعطل لهذه الخدمات والوظائف.

ملاحظاتي

24 جدار الحماية

عتـاد أو برمجيـات، تحد من حركة مرور بيانات الشـبكة؛ وفقـاً لمجموعة من قواعد تمكين الوصول، التي تحكم ما هو مسموح مصرح به؛ من عدمه.

25 ثغرة

أي نـوع مـن نقـاط الضعف في نظـام الحاسـب، أو برامـج أو تطبيقاته، أو فـي مجموعة من الإجراءات، مما يجعل الأمن السيبراني عرضه للتهديد.

26 تقييم الثغرات

عمليـة فحـص ممنهجـة لنظـم المعلومـات أو التطبيقـات لتحديـد مسـتوى الضوابط الأمنيـة، وتحديـد أوجـه القصـور فيهـا، وتوفيـر البيانـات التـي يمكـن مـن خلالهـا التنبـؤ بفعالية الضوابط الأمنية، والتأكد من كفائتها بعد التنفيذ.

27 اختبار الاختراق

عمليـة اختبـار نظام، أو شـبكة، أو موقـع إلكترونـي، أو تطبيق هواتف ذكية؛ للكشـف عن ثغرات، يمكن أن تُستغل لتنفيذ اختراق سيبراني.

ملاحظاتي

مع تحيات

المركز الوطني للأمن السيبراني

www.ncsc.gov.bh

#الأمن_السيبراني