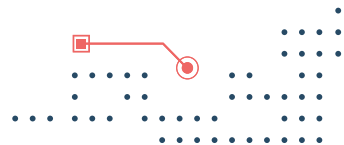




المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

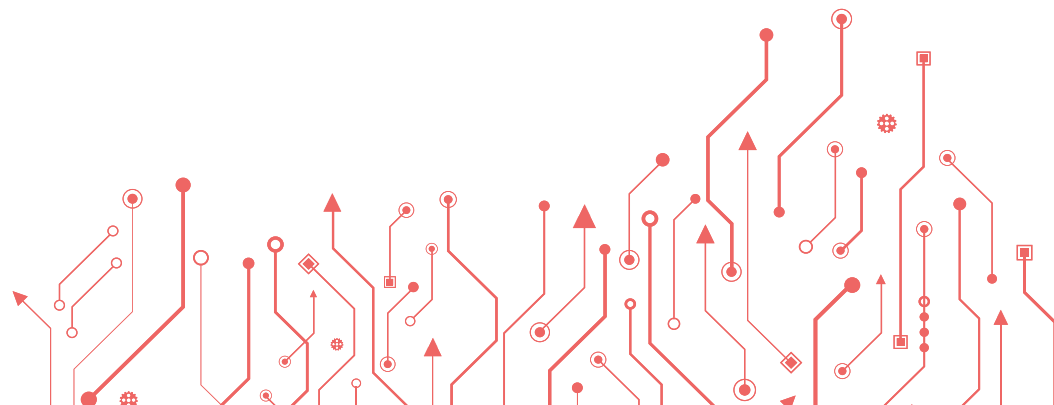
ابدأ حياتك المهنية في الأمن السيبراني





مرحباً.....

حياتك المهنية في مجال الأمن
السيبراني تبدأ هنا!

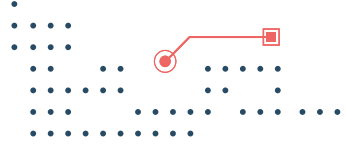


تحلم بأن تصبح خبيرًا في
مجال الأمن السيبراني؟

استكشف كيف تحول
هذا الحلم إلى واقع مهني!

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"



أبدأ مسيرتك المهنية في مجال الأمن السيبراني

أعزائي الطلبة!

هل تعلم أن العالم يحتاج حوالي 1.8 مليون متخصص مؤهل في الأمن السيبراني للحفاظ على أمن أنظمة الحاسوب والشبكات من الوصول غير المصرح به والهجمات السيبرانية؟ إذا كنت مهتماً بمجال الأمن السيبراني، فأليك ما يمكنك القيام به الآن:



01

أقرأ عن المهن في مجال الأمن السيبراني للتعرف على الوظائف المختلفة في هذا المجال.



02

انضم أو بادِر بإنشاء نادٍ في مجال تقنية المعلومات أو الأمن السيبراني في مدرستك.



03

اسأل معلميك حول مفاهيم الأمن السيبراني في فصولك الدراسية.



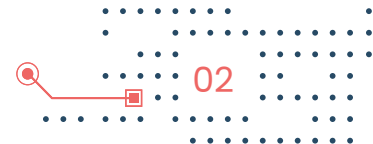
04

اشترك في دورات الرياضيات المتقدمة أو العلوم أو المواد الإبداعية، مثل: الكتابة والفن.

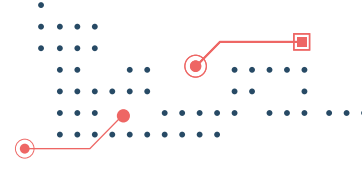


05

اسأل أخصائي التكنولوجيا بالمدرسة عن فرص وظيفية للأمن السيبراني.



02



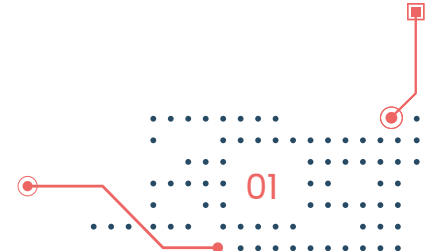
اكتشف الأمن السيبراني

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

إذا كانت إجابتك نعم، تساءل وفكر

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

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



01

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

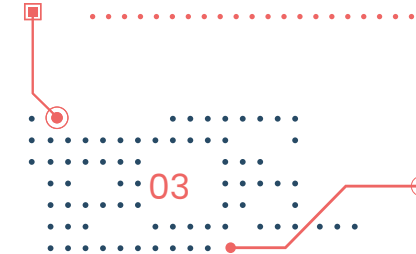
طرق أخرى تُمكنك من التقدم في هذا المجال

ملاحظات

.....

.....

.....



03

الخيارات المهنية

استكشف التخصصات التالية واكتب وصفاً موجزاً لها:

خبير التشفير



خبير تحليل الأدلة الرقمية / فاحص أدلة رقمية



أخصائي أمن سيبراني - الاستجابة للحوادث الأمنية



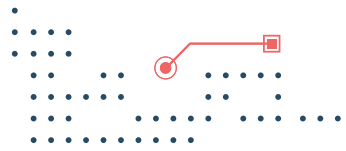
مستشار قانوني في الأمن السيبراني



مهندس أمن سيبراني



04



أخصائي دعم فني



محقق الجرائم السيبرانية



محلل لغة متعدد التخصصات



مدير أمن نظم المعلومات



أخصائي اختبار وتقييم النظام



أخصائي تشغيل سيبراني



محلل تقييم الضعف الأمني



مطور برامج

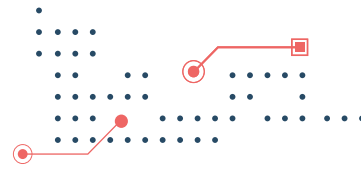


مسؤول الأنظمة / مدير الشبكات



مدير تقنية المعلومات





محل سلامة المعلومات



مخطط العمليات السيبرانية



اخصائي اختبار الاختراق

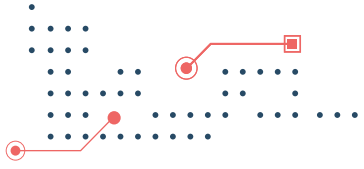


مدير المعرفة



محل التهديد والتحذير السيبراني





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



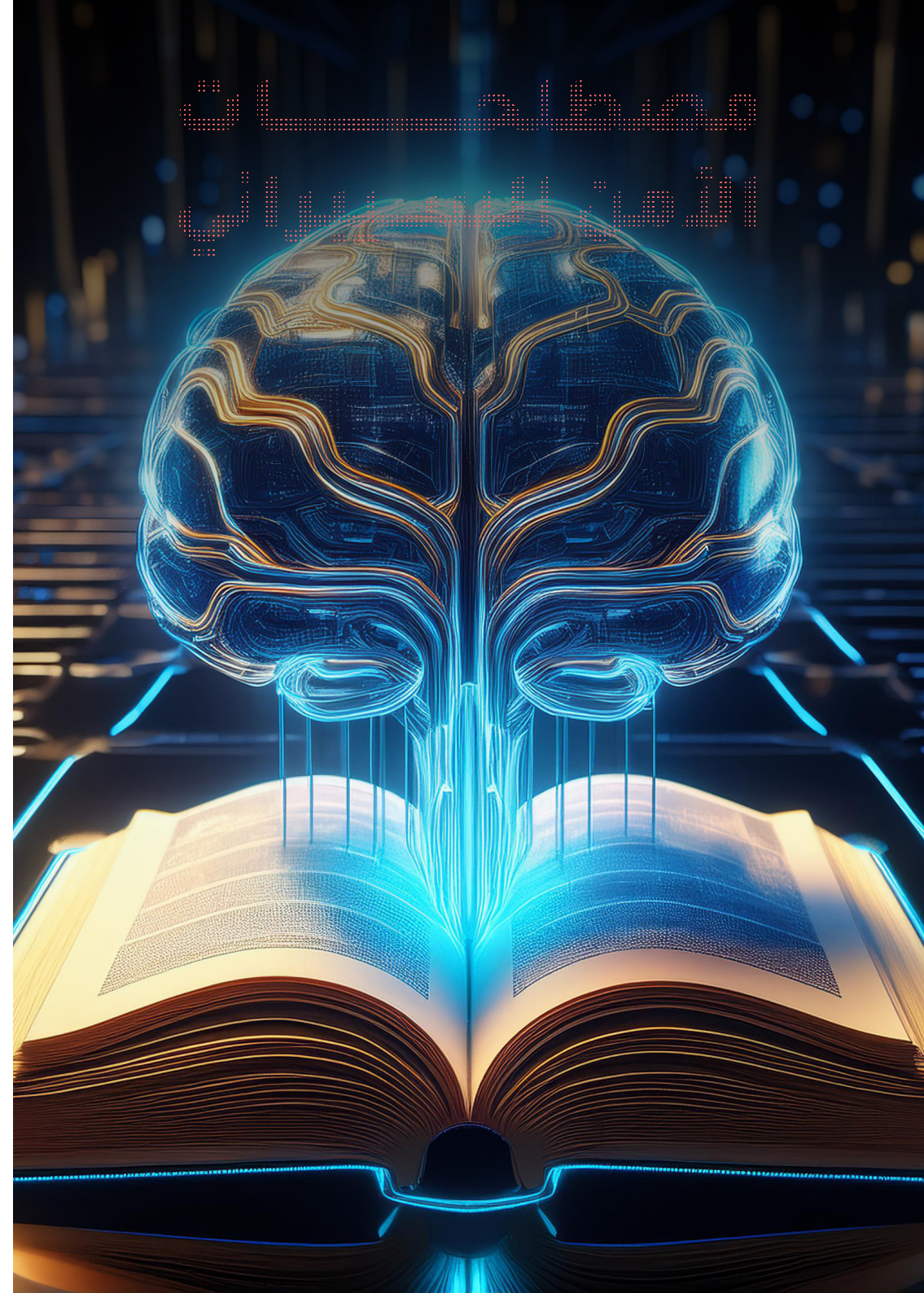
الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت، وشبكات الاتصالات، وأنظمة الحاسب، والأجهزة المتصلة بالإنترنت؛ إلى جانب العتاد وأجهزة التحكم المرتبطة بها.

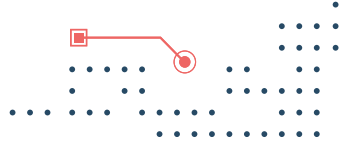
03 البنية التحتية الوطنية الحساسة



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.
- تأثير كبير على الأمن الوطني و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.





08 المسؤولية



القدرة على تتبع مسار نشاط أو حدث معين حتى الوصول إلى الطرف المسؤول؛ من منشئ النشاط. ويدعم ذلك عدم الإنكار، تشخيص الخطأ، اكتشاف ومنع التسلات، وإجراءات ما بعد الاكتشاف كالتعافي والإجراءات القانونية.

09 التحقق من الهوية



التأكد من هوية المستخدم، أو العملية، أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد التقنية. وليس له علاقة بتحديد حقوق الوصول الموارد والأصول التقنية.

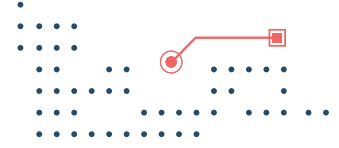
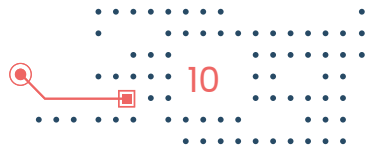
10 التحقق من الهوية متعددة العناصر



نظام أمني يتحقق من هوية المستخدم؛ يتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر:

- المعرفة: شيء يعرفه المستخدم (مثل كلمة المرور).
- الحيازة: شيء يملكه المستخدم (مثل برنامج أو جهاز توليد أرقام عشوائية أو رسائل قصيرة مؤقتة لتسجيل الدخول) ويطلق عليه (one-time password)
- الملازمة: صفة أو سمة حيوية متعلقة بالمستخدم نفسه فحسب (مثل بصمة الإصبع).

ملاحظات



04 التوافر



ضمان إمكانية الوصول والاستخدام عند الطلب، من مستخدم أو إجراء أو نظام مصرح له بشكل يعتمد عليه.

05 السلامة



الحماية ضد تعديل المعلومات أو تخريبها بشكل غير مصرح به، كما تشمل ضمان عدم الإنكار للمعلومات والأصالة.

06 السرية



خاصية عدم الإفصاح عن المعلومات لمستخدم أو إجراء أو نظام غير مصرح له إلا في حالة وجود تصريح لهم للوصول إليها.

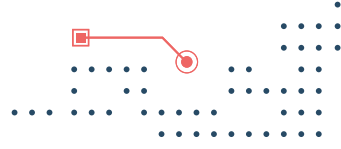
07 توكيد المعلومات



التدابير التي تحمي المعلومات، وأنظمة المعلومات، من خلال ضمان توافرها وسلامتها وأصالتها، وعدم الإنكار للمعلومات وسريتها.

ملاحظات





15 دفاع امني متعدد المستويات

مفهوم يُعنى بوضوح مستويات دفاعية متعددة من الضوابط الأمنية وذلك بالتكامل بين الأشخاص، التقنية والقدرات التشغيلية.



16 هجوم سيبراني

استغلال غير مشروع لأنظمة الحاسب، والشبكات، والمنظمات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية: بهدف إحداث أضرار. وتشمل أي نوع من الأنشطة الخبيثة التي تحاول الوصول غير المشروع أو تعطيل، أو منع، أو تدمير موارد النظم المعلوماتية، أو المعلومات نفسها.



17 هجمات حجم الخدم الموزعة

هي محاولات لتعطيل النظام، وجعل خدماته غير متوافرة: عن طريق إرسال طلبات كثيرة من أكثر من مصدر في الوقت نفسه.



18 رسائل التصيّد الإلكتروني

التنكر على هيئة جهة جديرة بالثقة عن طريق رسائل بريدية إلكترونية للحصول على معلومات حساسة، مثل أسماء المستخدمين، وكلمات المرور، أو تفاصيل بطاقة الائتمان، وذلك لأسباب ونوايا ضارة خبيثة.

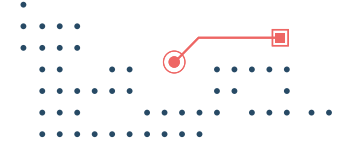
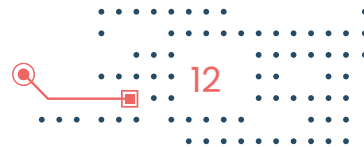
ملاحظات

.....

.....

.....

.....



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.

ملاحظات

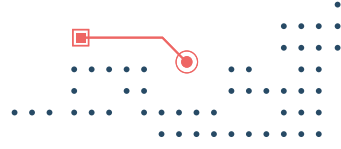
.....

.....

.....

.....





24 جدار الحماية



عتاد أو برمجيات، تحد من حركة مرور بيانات الشبكة؛ وفقاً لمجموعة من قواعد تمكين الوصول، التي تحكم ما هو مسموح مصرح به: من عدمه.

25 ثغرة



أي نوع من نقاط الضعف في نظام الحاسب، أو برامج أو تطبيقاته، أو في مجموعة من الإجراءات، مما يجعل الأمن السيبراني عرضة للتهديد.

26 تقييم الثغرات



عملية فحص ممنهجة لنظم المعلومات أو التطبيقات لتحديد مستوى الضوابط الأمنية، وتحديد أوجه القصور فيها، وتوفير البيانات التي يمكن من خلالها التنبؤ بفعالية الضوابط الأمنية، والتأكد من كفاءتها بعد التنفيذ.

27 اختبار الاختراق



عملية اختبار نظام، أو شبكة، أو موقع إلكتروني، أو تطبيق هواتف ذكية؛ للكشف عن ثغرات، يمكن أن تُستغل لتنفيذ اختراق سيبراني.

ملاحظات

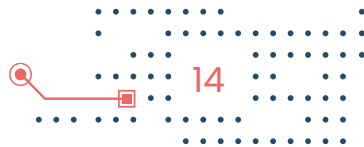
.....

.....

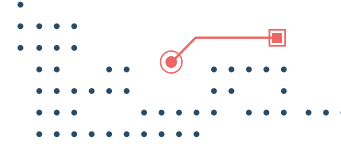
.....

.....

.....



14



19 المعلومات الاستباقية للتهديدات



معلومات منظمة قد تم تحليلها حول الهجمات الأخيرة، والحالية، والمحتلة، والتي يمكن أن تشكل تهديداً سيبرانياً للمنظمة.

20 مشاركة المعلومات



تبادل البيانات والمعلومات، أو المعرفة -أو كليهما- لاستخدامها في إدارة المخاطر والتهديدات أو الاستجابة للأحداث السيبرانية.

21 البرمجيات الضارة



برنامج يصيب الأنظمة بطريقة خفية (في الغالب) بغاية انتهاك سرية أو سلامة أو توافر بيانات الضحية أو تطبيقاته أو نظم التشغيل الخاصة به.

22 برمجيات الفدية



برمجيات ضارة تجعل بيانات وأنظمة الضحية غير قابلة للاستخدام لحين دفعه لمبلغ مالي.

23 التعافي من الكوارث



الأنشطة والبرامج والخطط المصممة: لإرجاع الوظائف وخدمات الأعمال الحساسة للجهة: إلى حالتها الطبيعية، وذلك بعد التعرض إلى هجمات سيبرانية أو تعطل لهذه الخدمات والوظائف.

ملاحظات

.....

.....

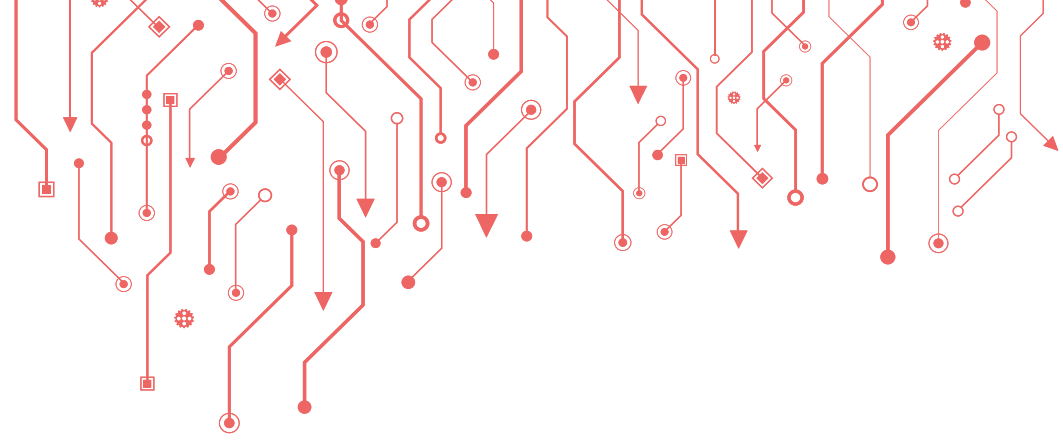
.....

.....

.....



13



مع تحيات
المركز الوطني للأمن السيبراني

www.ncsc.gov.bh
#الأمن_السيبراني



