محتوى اثرائي

الأمن السيبراني والجرائم الالكترونية

AL KHABEER
معهد الخبير العالي للتدريب

إعداد وتنفيذ

معهد الخبير العالي للتدريب

2024

ما المقصود بالأمن السيبراني وأهميتة

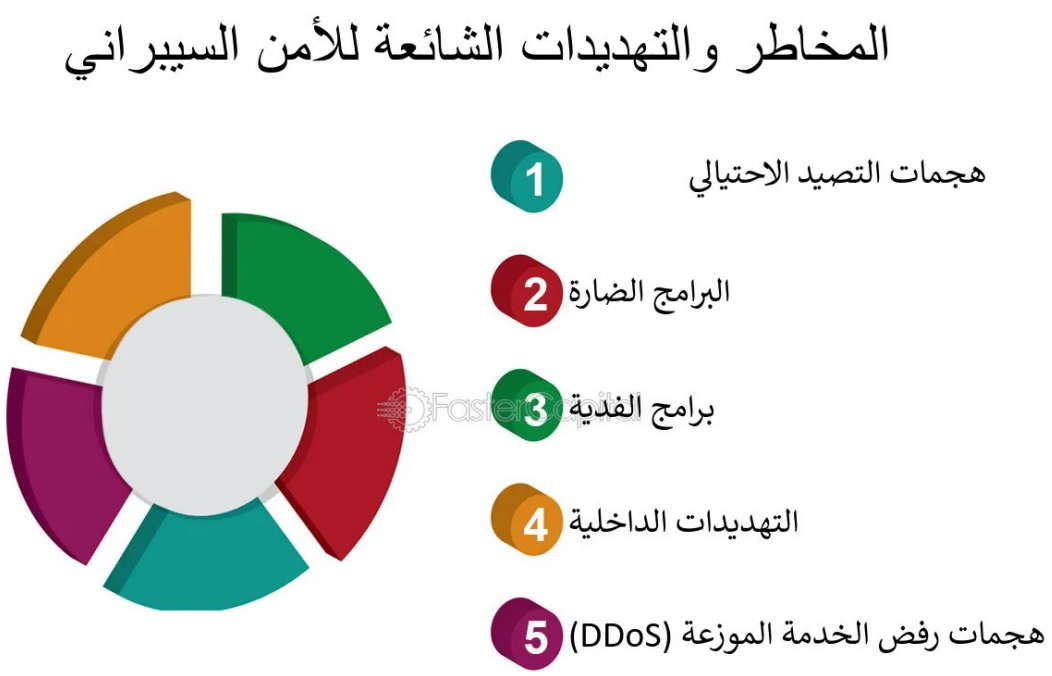
ما المقصود بالأمن السيبراني؟

الأمن السيبراني هو ممارسة حماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة. تتحمل المؤسسات مسؤولية تأمين البيانات للحفاظ على ثقة العملاء والامتثال للمتطلبات التنظيمية.

ما أهمية الأمن السيبراني؟

تستخدم الشركات في مختلف القطاعات، مثل الطاقة والنقل وتجارة التجزئة والتصنيع، الأنظمة الرقمية والاتصال عالي السرعة لتوفير خدمة عملاء فعّالة وإجراء عمليات تجارية ميسورة التكلفة.

ما هي أنواع الهجمات التي يحاول الأمن السيبراني الدفاع عنها؟



يسعى محترفو الأمن السيبراني إلى احتواء التهديدات الحالية والجديدة التي تتسلل إلى أنظمة الكمبيوتر بطرق مختلفة، والحدّ منها. نقدم أدناه بعض الأمثلة على التهديدات السيبرانية الشائعة .

- ❖ **البرمجيات الخبيثة:**
- ❖ **برامج الفدية:**
- ❖ **هجوم الوسيط:**
- ❖ **التصيد الاحتيالي:**
- ❖ **الهجوم الموزَّع لتعطيل الخدمة (DDoS) :**
- ❖ **تهديد داخلي:**

ما هي أنواع الأمن السيبراني؟

يعالج نهج فعّال للأمن السيبراني المخاوف التالية داخل المؤسسة .

- ❖ **الأمن السيبراني للبنية الأساسية بالغة الأهمية:**
- ❖ **أمان الشبكة:**
- ❖ **أمن السحابة:**
- ❖ **أمان إنترنت الأشياء (IoT):**
- ❖ **أمان البيانات:**
- ❖ **أمان التطبيقات:**
- ❖ **أمان نقاط النهاية:**
- ❖ **التعافي من الكوارث وتخطيط استمرارية الأعمال:**

من هم فرق Blue Team و Red Team: الأدوار والوظائف والأهمية في الأمن السيبراني؟

ما هو Blue Team ؟

كيف يعمل فريق Blue Team ؟

ما هو Red Team ؟

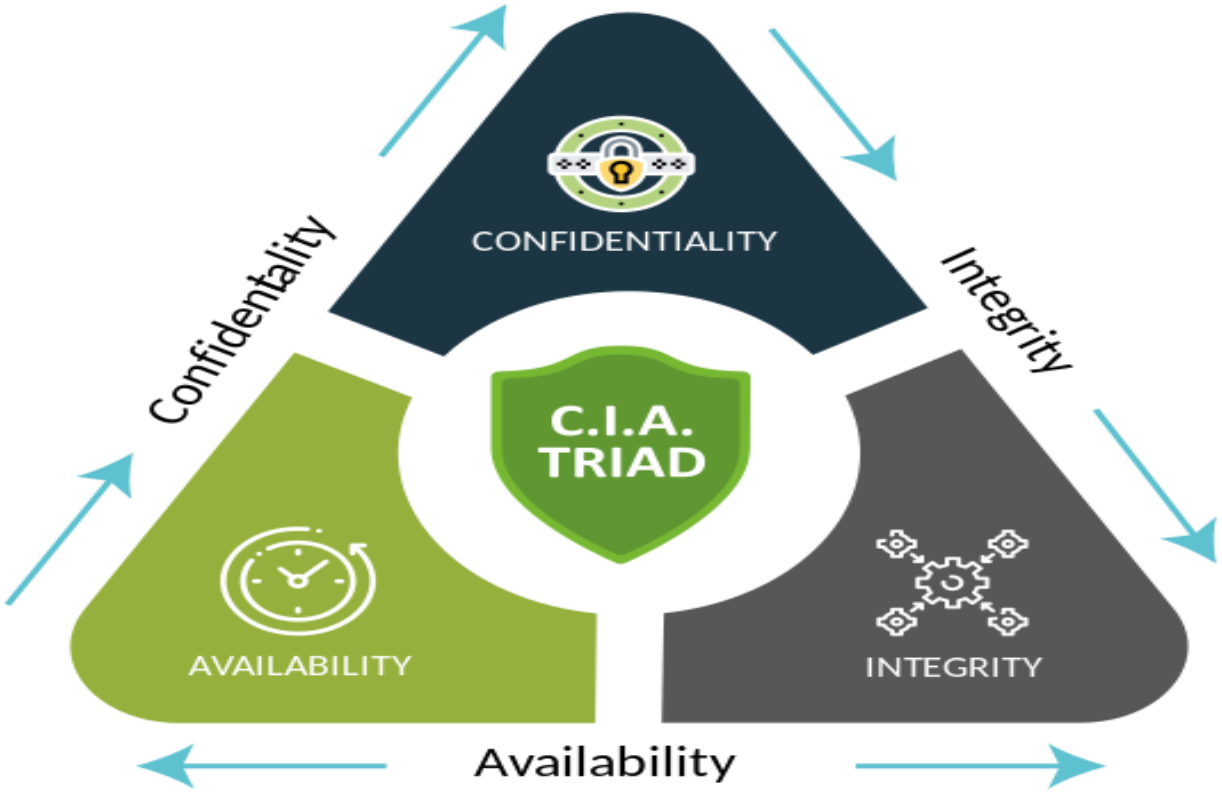
كيف يعمل فريق Red Team ؟

الأدوار في المنظمة:

دور فريق Blue Team:

دور فريق Red Team:

ماهو مفهوم مثلث CIA وما ارتباطه بالأمن السيبرانى؟



مثلث CIA هو نموذج للأمن السيبراني يهتم بأمن البيانات ويعد بمثابة دليل لأمن المعلومات للمنظمات ويتضمن ثلاث مكونات رئيسية لأمن البيانات وهي : السرية (Confidentiality) والنزاهة (Integrity) والتوافر. (Availability)

فالسرية تُعنى بضمان خصوصية البيانات بواسطة تقييد الوصول باستخدام المصادقة الثنائية ووضع اسم المستخدم وكلمة السر وتأتي النزاهة مؤكدة على دقة وصحة المعلومات ويكون دور التوافر أن يضمن توفر المعلومات للأشخاص المخول لهم في أي وقت .

أمن المعلومات قائم على هذا المثلث ، فيجب أن تكون المعلومة سرية (confidentiality) ولايُسمح لأحد بأن يتم التعديل عليها, وأن تكون مثلما أُرسلت تصل (Integrity) ويلزم أن تكون متوفرة (Availability) عندما يتم طلبها، ولكن عندما تكون لدي معلومة موضوعة في مكان ما ومقفل عليها فلن استفيد منها.

لماذا يعتبر مثلث CIA مهم للمنظمات والشركات؟

بطبيعة الحال فإن أي هجوم إلكتروني يحاول انتهاك او اختراق على الأقل واحده من مبادئ مثلثCIA ، ففهم هذا النموذج لأمن البيانات يكون مساعد للمختصين في مجال الأمن السيبراني على تحديد المخاطر بكل دقة وبشكل واضح وحماية الشبكات من أي نشاط غير مصرح به عن طريق سياسات أمن المعلومات المناسبة .

ويمكن القول مجملاً أن مثلث CIA يعتبر هام وحجر اساس للمنظمات لأنه يساعد في حماية البيانات المهمة والمعلومات من التسريب ويضمن أن تكون المعلومات دقيقة وصحيحة وغير متلاعب بها، ويضمن توفر البيانات والمعلومات في وقت الحاجة، أيضاً العمل بمبادئ هذا المثلث يساعد في تحسين سمعة المنظمة وضمان استمرارية الأعمال بشكل آمن.

ما هي مخاطر الأمن السيبراني؟

التهديدات السيبرانية الشائعة للبيانات الحساسة

قبل التعرف على طريقة تقييم المخاطر السيبرانية يجب النظر أولاً على مفهوم مخاطر الأمن السيبراني ومراحل إدارتها، يشير مفهوم مخاطر الأمن السيبراني إلى التهديدات والهجمات الإلكترونية المسببة لتعطيل أنظمة التكنولوجيا للمؤسسات وخدماتها الإلكترونية، وهي مخاطر يتعرض لها الأفراد أيضًا.