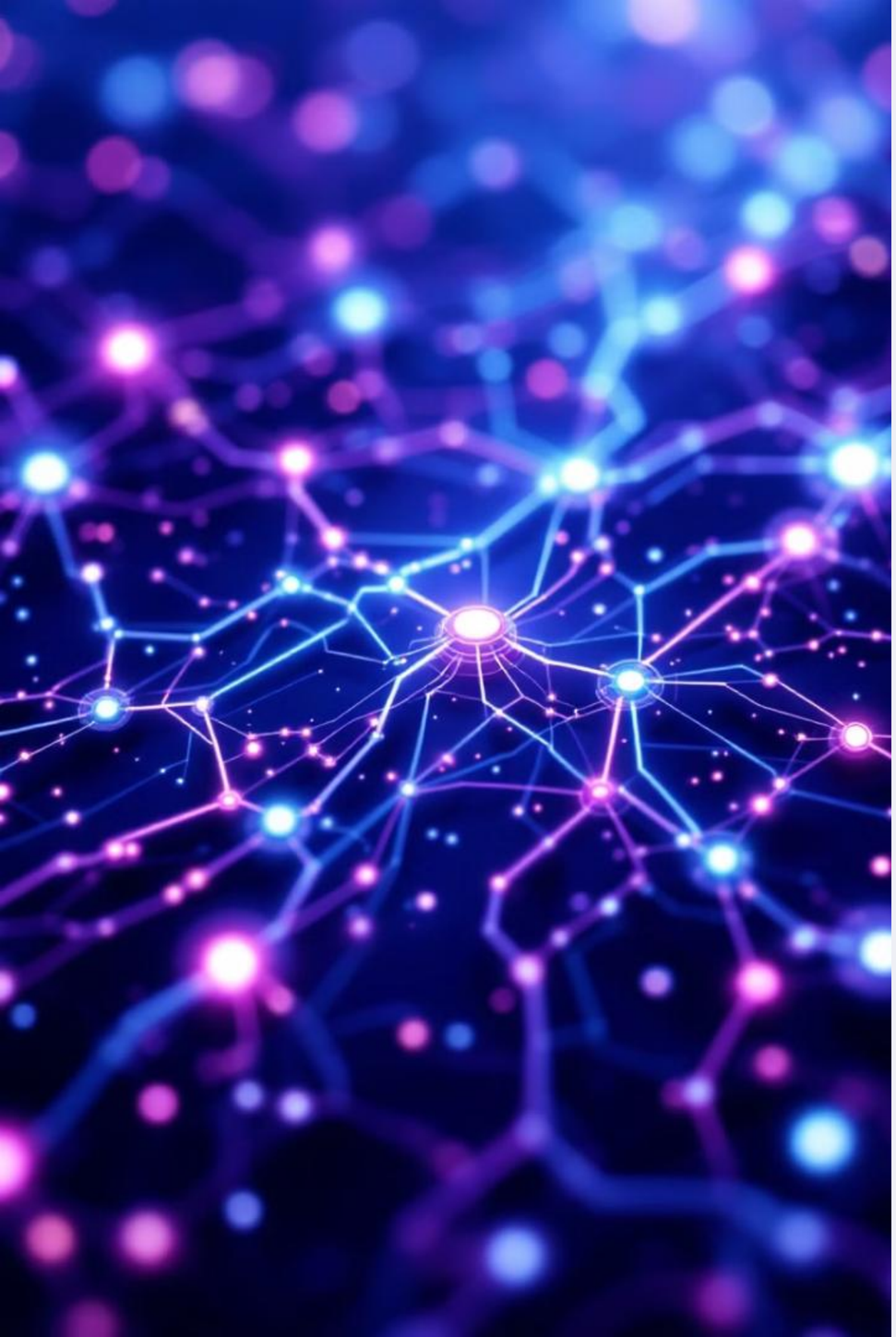
الامن السيبراني
Cybersecurity

م.م حيدر عبد الكريم الجنابي



ما الأمن السيبراني Cybersecurity؟

تعريف مفهوم الأمن السيبراني Cyber Security يتضح من تحليل المصطلح ذاته، فالمصطلح يتألف من كلمتين:

- الأمن Security وتعني الحماية والتأمين
- والسيبراني Cyber تعني إلكتروني أو عبر الإنترنت.

وعلى هذا فالمقصود بالأمن السيبراني هو تأمين الأجهزة الإلكترونية وتوفير الأمان لشبكات الإنترنت والأنظمة البرمجية وحماية البيانات الرقمية المهمة من أي تهديدات أو أخطار إلكترونية تؤدي إلى اختراقها وزعزعة استقرارها.

فالأمن السيبراني معنيّ من حيث الأصل بصد الهجمات الإلكترونية وتأمين الأنظمة والأجهزة الإلكترونية، ويحدث ذلك التأمين عن طريق توفير طبقات متعددة من الحماية تتوزع على الأنظمة والشبكات بمنهجيات معينة لكي يتعذر اختراقها، ومن ثم تُحفَظ البيانات الحساسة، ويتم تأمين سير عمليات التفاعل التجارية وغيرها عبر الفضاء الإلكتروني لضمان جريانها بسلاسة وأمان.

المخاطر	المجال	الهدف
الوصول غير المصرح به، التلف، الاستخدام غير القانوني.	يشمل الأجهزة والحسابات والشبكات والبرمجيات.	حماية البيانات والأنظمة من التهديدات الإلكترونية.

مقدمة عن الأمن السيبراني

المخاطر

الوصول غير المصرح به، التلف، الاستخدام غير القانوني.

المجال

يشمل الأجهزة والحسابات والشبكات والبرمجيات.

الهدف

حماية البيانات والأنظمة من التهديدات الإلكترونية.

ما مجالات الأمن السيبراني؟

1. أمن البنية التحتية الحيوية Critical infrastructure security
2. أمن الشبكة Network security
3. أمن نقاط النهاية Endpoint security
4. أمن التطبيقات Application security
5. الأمن السحابي Cloud security
6. امن المعلومات Information security
7. أمن الهاتف Mobile security

كيف يعمل الأمن السيبراني؟

يعمل الأمن السيبراني من خلال عملية منظمة تتألف بالأساس من 3 جوانب، هي الوقاية والرصد والصد، يستهدف من خلالها حماية الأنظمة والشبكات والبيانات الرقمية من الوصول غير المصرح به أو السرقة أو التلف.

1- الوقاية

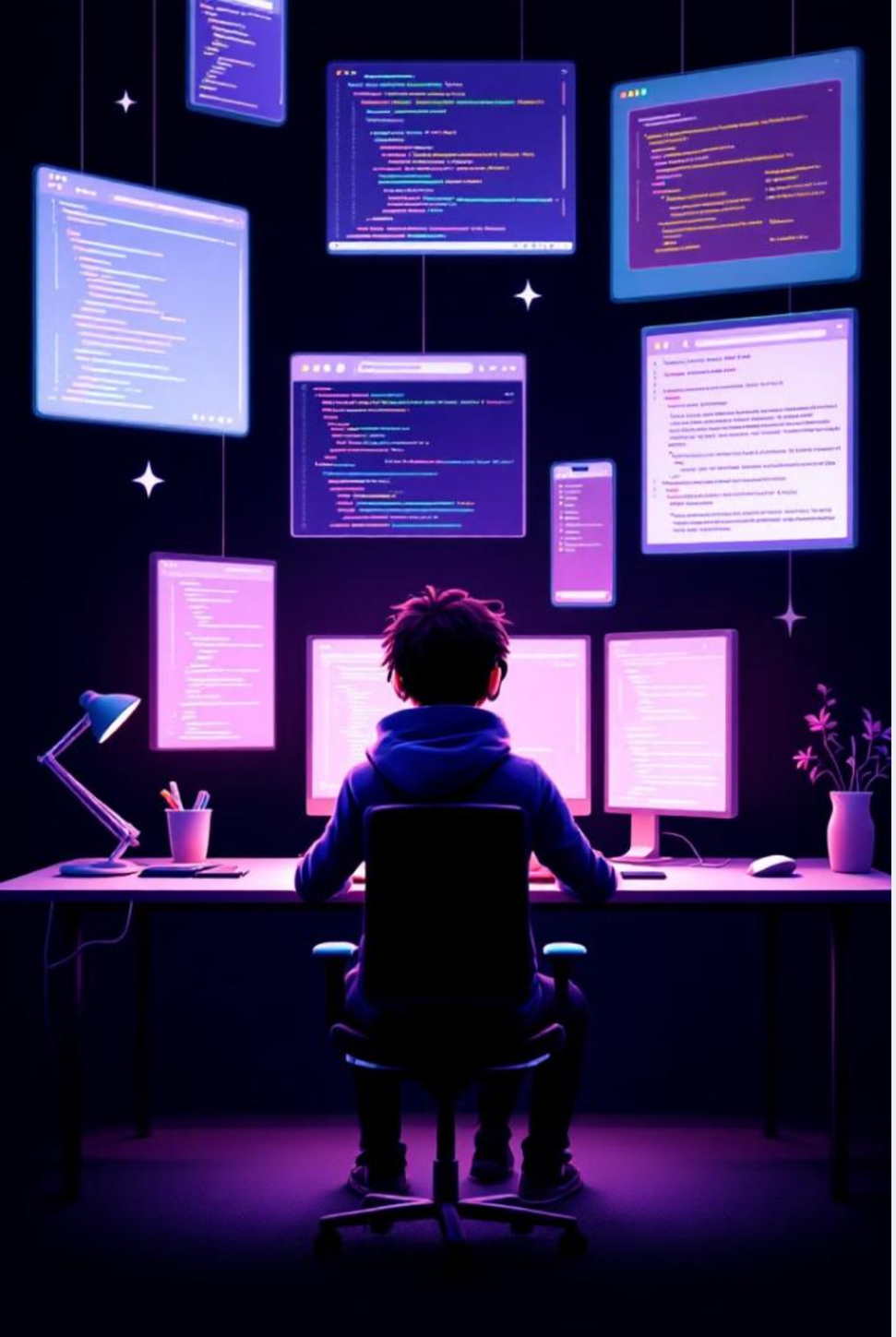
جانب الوقاية يتضمن التنفيذ الاستراتيجي للتدابير الأمنية التي تهدف إلى تجنب الوصول غير المصرح به بشكل استباقي وإحباط الاختراقات المحتملة. يعد هذا الموقف الاستباقي أمرًا بالغ الأهمية لإنشاء بيئة رقمية محصنة تعمل كرادع ضد الجهات الخبيثة التي تسعى إلى استغلال نقاط الضعف.

2- الرصد

يؤدي جانب الرصد دورًا محوريًا في الأمن السيبراني، إذ يحدد التهديدات المحتملة ومواطن الضعف داخل النظام. يتضمن ذلك استخدام أدوات مراقبة متقدمة وأنظمة كشف التسلل وغيرها من التقنيات المتطورة لفحص حركة الزيارات على الشبكة وسلوك النظام. إن الرصد الدقيق في الوقت المناسب أمرًا أساسيًا لكي تبقى متقدمًا بخطوة على الاختراقات الأمنية المحتملة، مما يسمح بتنفيذ تدابير سريعة وفعالة.

3- الصد

جانب الصد هو الجانب الثالث في الأمن السيبراني، والذي يستلزم اتخاذ الإجراءات اللازمة لاحتواء حادثة خرق أمني. والسرعة في اتخاذ تلك الإجراءات عند حدوث خرق تكون عنصرًا حاسمًا وبالغ الأهمية.



مخاطر الهجمات السيبرانية وأنواعها

الفيروسات

تتلف الأجهزة والبيانات.

البرمجيات الخبيثة

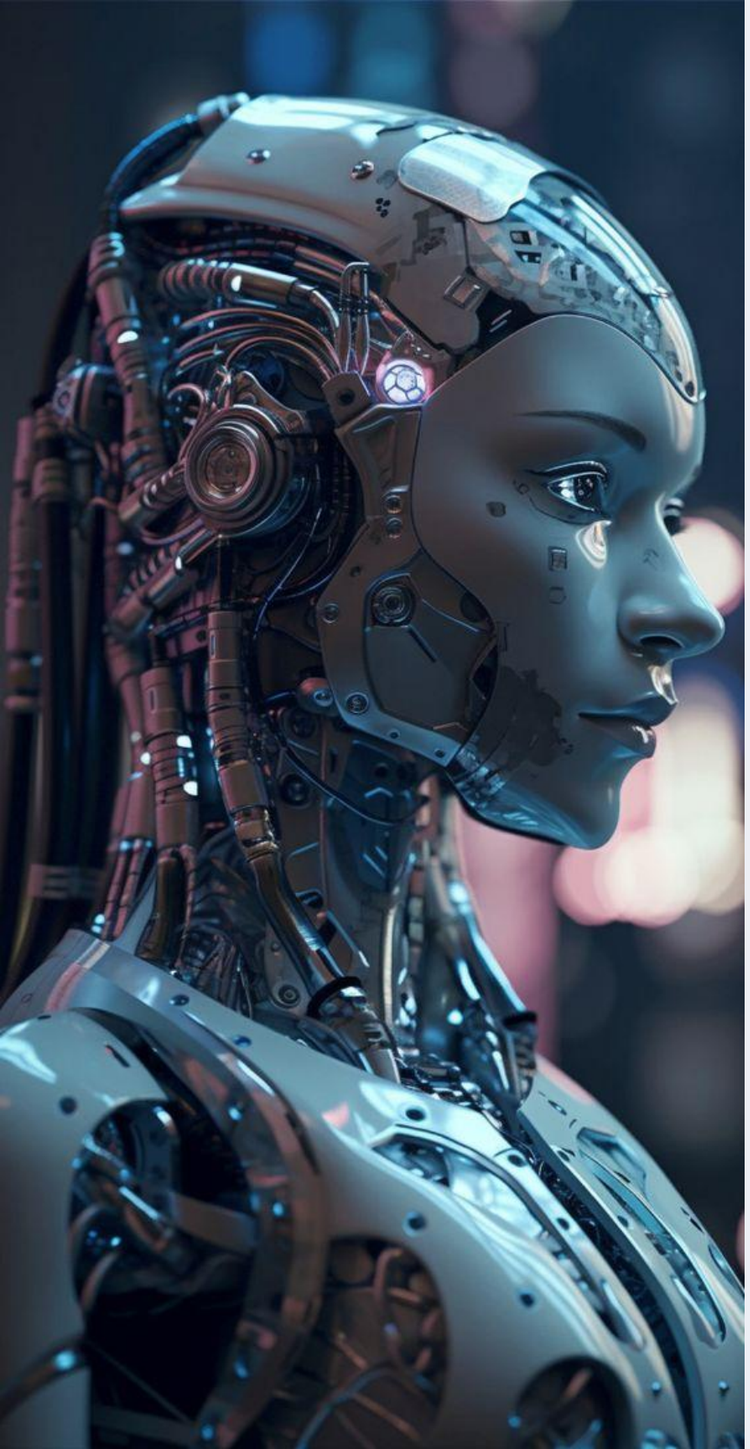
تسرق البيانات أو تتحكم في الجهاز.

الهجمات الموزعة

تعطل خدمات الإنترنت.

هجمات التصيد الاحتيالي

تستهدف سرقة بيانات شخصية.



الخطوات الأساسية لحماية الأجهزة الإلكترونية

كلمة مرور قوية

واستخدم كلمات مرور مختلفة لكل حساب.

برامج مكافحة الفيروسات

حافظ على تحديثه بشكل منتظم.

تحديثات الأمان

قم بتثبيت أحدث تحديثات البرامج.

شبكة Wi-Fi امنة

استخدم شبكات Wi-Fiموثوقة فقط.

تأمين الحسابات والبيانات الشخصية

1

التحقق من الهوية

استخدم عوامل مصادقة متعددة.

2

إدارة كلمة المرور

استخدم كلمات مرور قوية وفريدة.

3

الحذر من روابط مشبوهة

لا تنقر على روابط غير موثوقة.

4

تحديثات البرامج

حافظ على برامجك محدثة.

منصات التواصل الاجتماعي والأمن السيبراني

خصوصية البيانات

1 وتعني الحفاظ باكبر صورة ممكنة على خصوصية البيانات وعدم السماح للاخرين بالاطلاع عليها

التحقق من المصدر

2 تجنب مشاركة معلومات شخصية مع اي مصدر والتحقق منه ومن صحة بياناته

التوعية بالمخاطر

3 تعرف على مخاطر الهجمات والسبل الممكنة في زيادة الوعي الخاص بالافراد ضد الهجمات الالكترونية

حماية الأعمال التجارية من التهديدات الإلكترونية

1

التوعية

تدريب الموظفين.

2

التقنية

حلول أمنية قوية.

3

الاستجابة

خطط للتعامل مع الهجمات.

دور التوعية والتدريب في الأمن السيبراني

1

المعرفة

زيادة الوعي بالمخاطر.

2

الممارسات

تدريب على أفضل ممارسات الأمن.

3

الاستجابة

التدريب على كيفية الاستجابة للهجمات.

خاتمة وتوصيات للحفاظ على الأمن السيبراني

1

التوعية

تثقيف وتدريب مستمر.

2

التقنية

استخدام حلول أمنية قوية.

3

التعاون

مشاركة المعلومات مع خبراء الأمن.

THANKS