ماذا لو استلهمنا من الطبيعة حلولاً جديدة للأمن السيبراني؟

38 سيبرانيات الطبيعة

قريب المدى | **متوسط المدى** | بعيد المدى

تطوير إطار عمل للأمن السيبراني مستوحى من الطبيعة لتحسين قدرة الأنظمة الرقمية على الكشف عن التهديدات الإلكترونية، والتعامل معها والتكيّف المستمر لمواجهتها.

المتغيرّات الغامضة

الأنظمة، التكنولوجيا

التوجهات العالمية الكبرى

تزايد الثغرات التكنولوجية الأمنية

الاتجاهات السائدة

المحاكاة الحيوية
الأمن السيبراني
الرشاقة الحكومية
التعاون الدولي
تحفيز الابتكار

التكنولوجيا

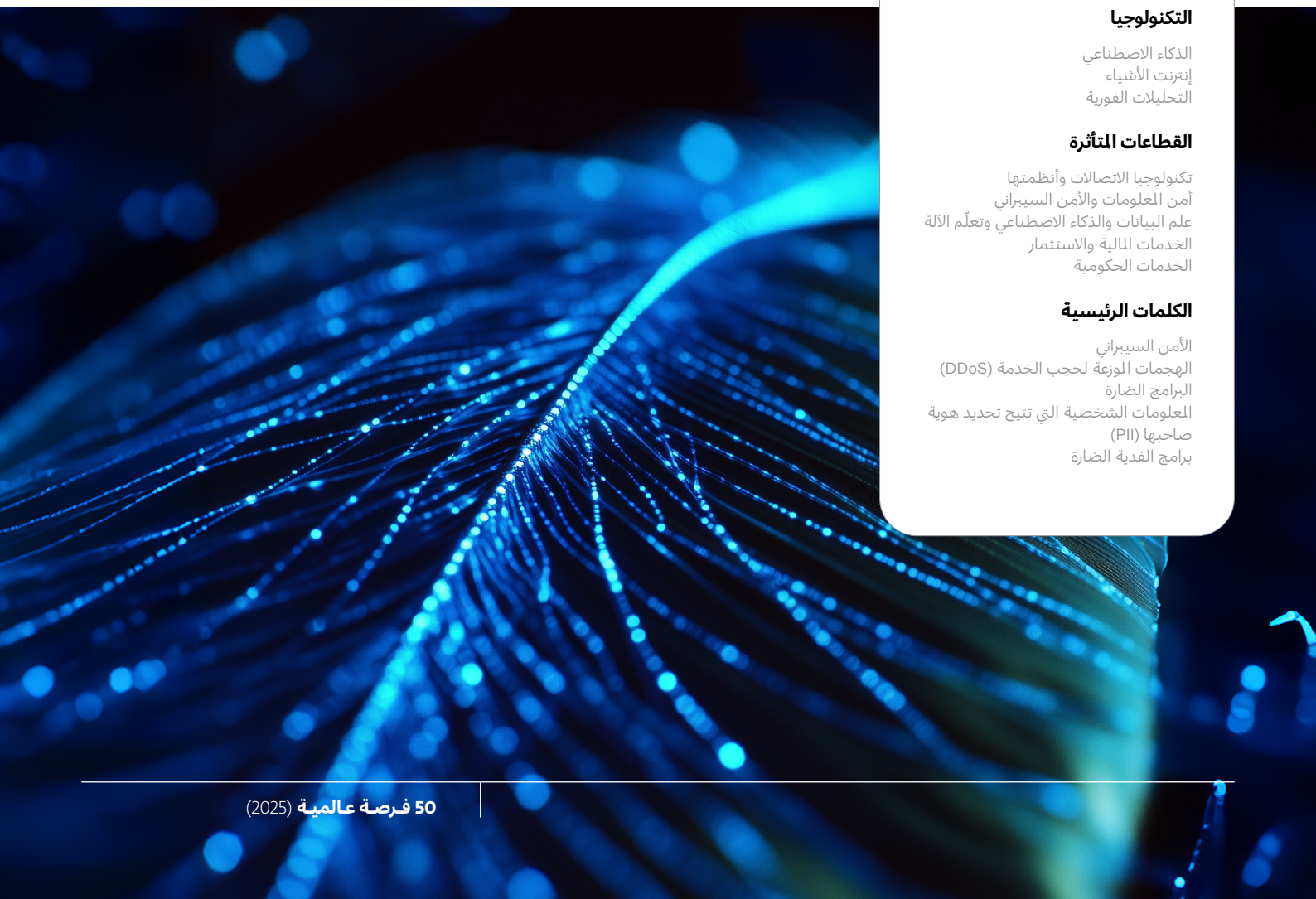
الذكاء الاصطناعي
إنترنت الأشياء
التحليلات الفورية

القطاعات المتأثرة

تكنولوجيا الاتصالات وأنظمتها
أمن المعلومات والأمن السيبراني
علم البيانات والذكاء الاصطناعي وتعلّم الآلة
الخدمات المالية والاستثمار
الخدمات الحكومية

الكلمات الرئيسية

الأمن السيبراني
الهجمات الموزعة لحجب الخدمة (DDoS)
البرامج الضارة
المعلومات الشخصية التي تتيح تحديد هوية صاحبها (PII)
برامج الفدية الضارة



الواقع الحالي

في عام 2020، زادت هجمات البرامج الضارة بنسبة تتجاوز 350% وبرامج الفدية الضارة بأكثر من 430%. واستمرت المخاطر السيبرانية في الارتفاع، حيث أكد 72% من المشاركين في استطلاع توقعات الأمن السيبراني العالمي (GCO) أن هناك ارتفاعاً في المخاطر السيبرانية.[1104] وزاد استخدام الذكاء الاصطناعي في الهجمات السيبرانية، التي أصبحت أوسع نطاقاً وأسرع وأكثر ذكاءً. فوفقاً لاستطلاع للرأي شمل أكثر من 800 من القادة في مجال تكنولوجيا المعلومات والأمن حول العالم، أقر 95% بأن الهجمات السيبرانية أصبحت أكثر تطوراً، حيث شهد 51% منهم هجمات مدعومة بالذكاء الاصطناعي، و36% هجمات باستخدام تقنيات التزييف العميق وهجمات على سلسلة التوريد، و35% هجمات على السحابة، و34% هجمات على تقنيات إنترنت الاشياء وشبكات الجيل الخامس.[1105]

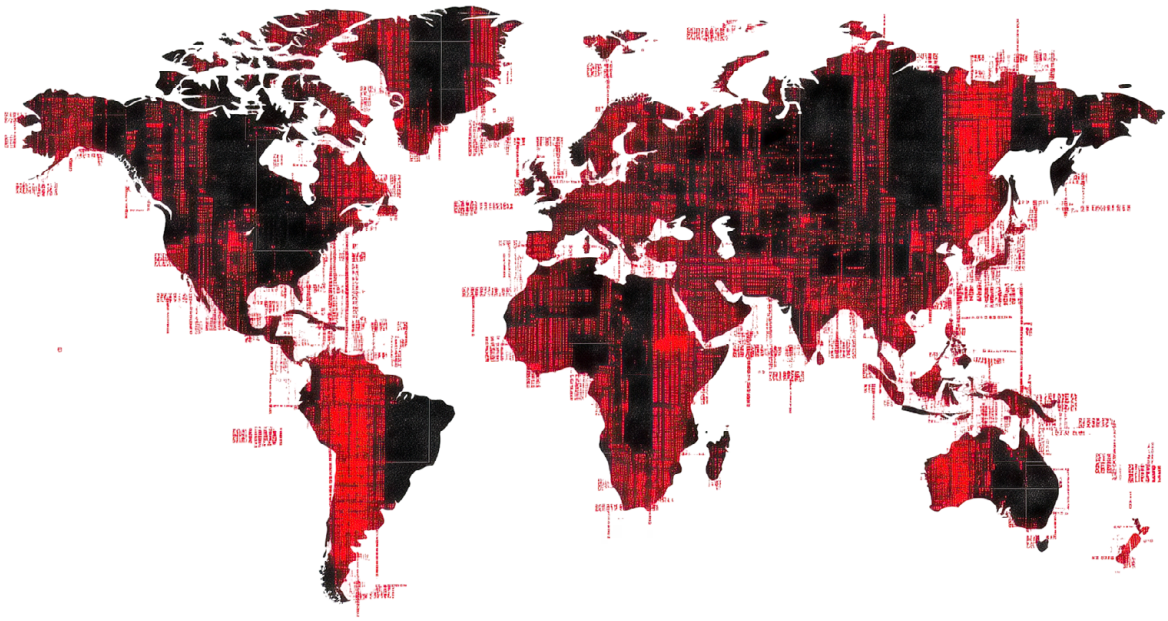
ومع هذا الارتفاع في الهجمات، تتزايد التكاليف المترتبة عن الجرائم الإلكترونية، حيث ارتفعت تكلفة اختراق البيانات في عام 2024 بنسبة 10% لتصل إلى 4.88 مليون دولار.[1106] ويُعد هذا الارتفاع الأكبر منذ جائحة كورونا، وذلك بسبب تأثير تعطل الأعمال والنفقات المترتبة على الاختراقات، حيث تتضمن حوالي 46% من الحالات تسريب معلومات شخصية تتيح تحديد هوية صاحبها.[1107] وقد سجلت الولايات المتحدة الأمريكية أعلى متوسط لتكاليف تلك الاختراقات، بواقع 9.36 مليون دولار، تليها منطقة الشرق الأوسط بقيمة 8.75 مليون دولار.[1108] ويظل قطاع الرعاية الصحية الأكثر تأثراً من بين القطاعات، حيث قد تصل تكاليف الاختراق الواحد إلى 9.77 مليون دولار.[1109] كما أن تأثير الاختراقات الإلكترونية لا تنحصر بالتكاليف المالية والاقتصادية، إذ تؤدي الجرائم الإلكترونية إلى تراجع ثقة المستخدمين، وقد تدمر سمعة الأفراد أو الشركات،[1110] كما قد يتعرض ضحايا هذه الخروقات إلى ضغوطات نفسية، مما قد يؤدي إلى تفكك المجتمعات.[1111]

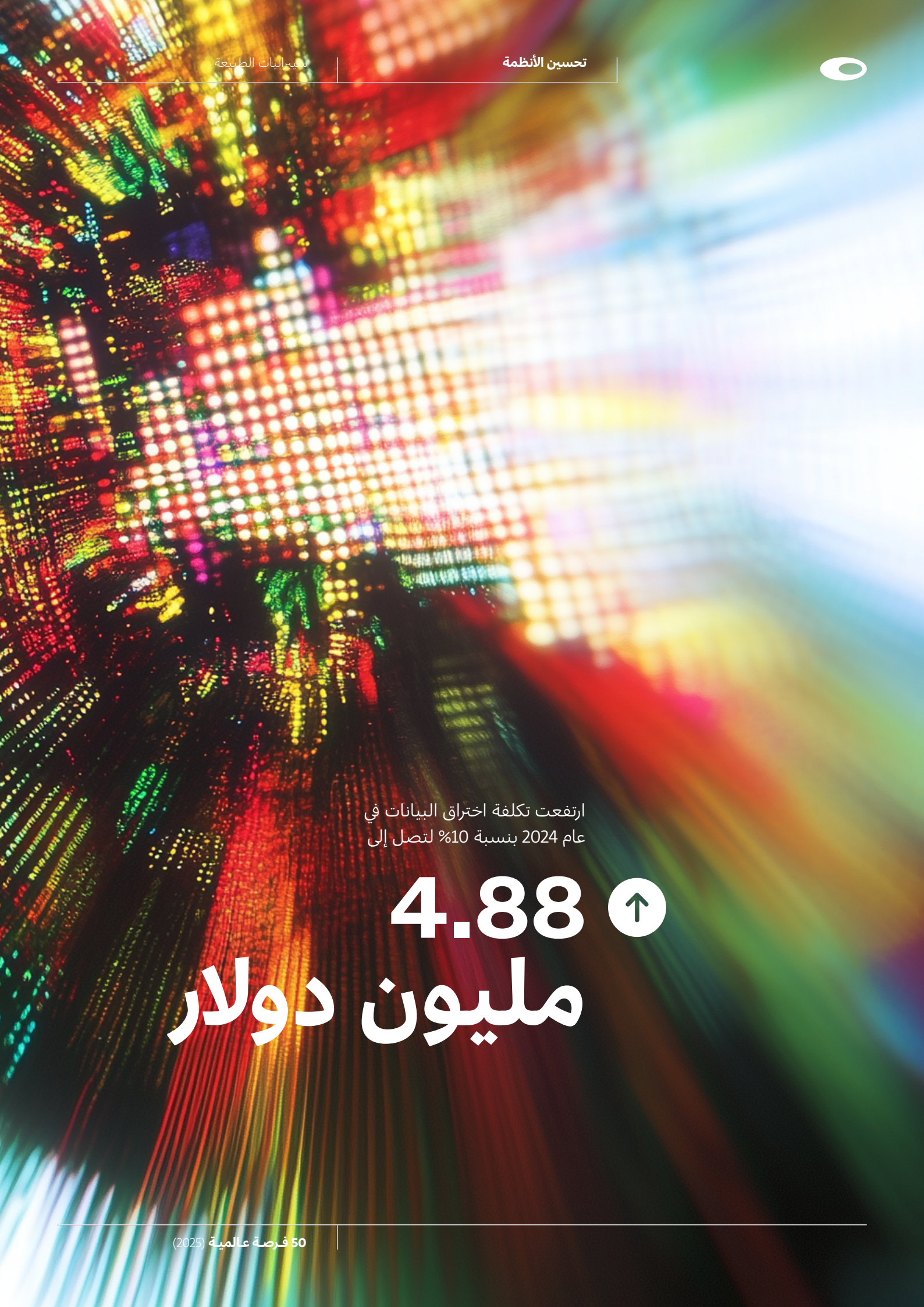
سجلت **الولايات المتحدة الأمريكية** أعلى متوسط لتكاليف اختراق البيانات، بواقع

9.36 مليون دولار

تليها **منطقة الشرق الأوسط** بقيمة

8.75 مليون دولار





ارتفعت تكلفة اختراق البيانات في
عام 2024 بنسبة 10% لتصل إلى

4.88 مليون دولار

الفرصة المستقبلية

تطوير نظام أمن سيبراني مستوحى من الطبيعة ويُحاكي استراتيجياتها من أجل بناء أنظمة مرنة وقادرة على التطور والتكيّف مع التهديدات السيبرانية والتعامل مع أشكالها الجديدة. ويعزز النظام من قدرات الكشف عن التهديديات والتعامل معها عبر تقنيات متقدمة مثل خوارزميات سرب الجسيمات (PSO) المستوحاة من السلوك الجماعي للأنظمة الطبيعية مثل أسراب الطيور،[1112] وذلك بالاستفادة من مبادئ التنظيم الذاتي، واللامركزية، والتبادل السريع للمعلومات. كما يضع هذا النظام معايير عالمية للأمن السيبراني تضمن الاستجابة السريعة والفعّالة للتهديدات الجديدة،[1113] عبر دمج المعارف من مجالات متعددة، مثل علم الأحياء والعلوم البيئية، ليستبدل الأساليب التقليدية ببروتوكولات قابلة للتطوّر، مما يعزز الكفاءة ويزيد من قدرة النظام على التكيّف مع التهديدات المتزايدة والمتغيّرة باستمرار.

الإيجابيات

تعزيز الأمن الرقمي، والتحسين الذاتي والتكيّف مع التهديدات المستحدثة، ودمج تطبيقات متعددة التخصصات تسهم في تحسين استراتيجيات الكشف عن الهجمات والاستجابة لها.

المخاطر

الثغرات الأمنية غير المتوقعة، وتجاوز الرقابة البشرية نتيجة التكيف السريع مع التهديدات المتغيرة، إلى جانب زيادة التعقيد والغموض.

تطوير نظام أمن سيبراني مستوحى من الطبيعة ويحاكي استراتيجياتها من أجل بناء أنظمة مرنة وقادرة على التطور و **الكشف عن التهديديات والتعامل معها عبر تقنيات متقدمة مثل خوارزميات سرب الجسيمات**