

The background features a dark blue circuit board pattern with light blue traces and green component pads. Two horizontal bands of blue dots, representing binary code, are positioned on either side of the text. The text itself is a large, bold, white sans-serif font.

CYBERSHIELD AI

المشكلة

تعاني المؤسسات من تهديدات أمنية متزايدة، حيث يتم استغلال الثغرات الأمنية قبل أن تتمكن فرق الأمن السيبراني من اكتشافها وإصلاحها. من أهم المشاكل التي تواجهها المؤسسات:

1. اكتشاف الثغرات متأخراً بعد استغلالها من قبل المختربين.
2. الاعتماد على أدوات فحص يدوية يتطلب وقتاً وجهداً كبيراً من خبراء الأمن.
3. عدم قدرة بعض الشركات الصغيرة على توظيف مختصي أمن سيبراني لحماية أنظمتها.
4. عدم توفر حلول أمنية ذكية يمكنها إصلاح الثغرات تلقائياً قبل أن تسبب في أضرار.
5. الاعتماد على تقارير معقدة يصعب على غير المختصين فهمها أو اتخاذ قرارات بناءً عليها.

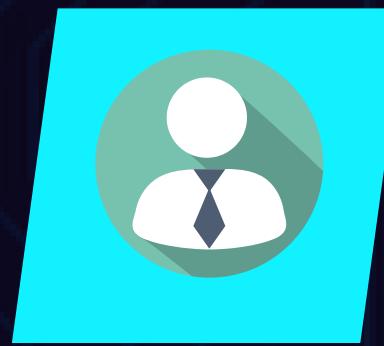
الحل المُؤتمر

الفكرة الأساسية

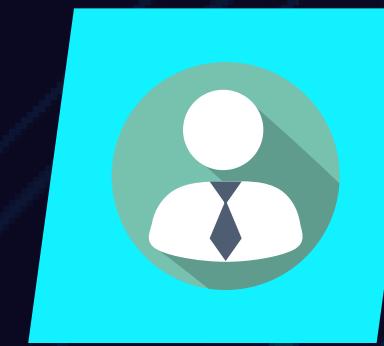
يهدف هذا المشروع إلى تطوير نظام أمني ذكي ومبتكر يعتمد على الاختراق الذاتي (Self-Pentest) باستخدام الذكاء الاصطناعي، للكشف عن الثغرات الأمنية بشكل تلقائي، وتحليل مستوى خطورتها، ومن ثم تقديم توصيات أو تنفيذ إصلاحات تلقائية (Auto-Remediation) لحماية الشبكات والتطبيقات من الهجمات السيبرانية.

يعمل النظام عن طريق محاكاة الهجمات الدقيقة على الأنظمة المستهدفة، باستخدام أدوات مسح متقدمة مثل Nmap وMetasploit، ثم يقوم الذكاء الاصطناعي بتحليل النتائج وتحديد نقاط الضعف، وتقديم حلول مقترنة أو تنفيذ إصلاحات بشكل آلي.

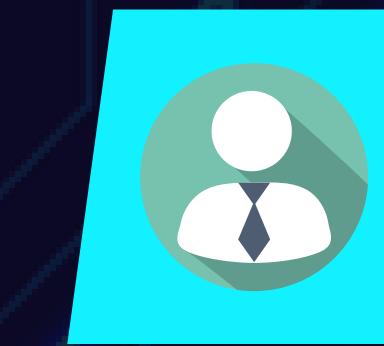
الفريق



محمد علي الصقور



محمد صالح القحطاط



طلال عوض ال عمر



محمد معدي ال عمر



صياد صالح ال حارث

THANK YOU