OpenAI وCisco تطلقان Shirudo: بيئة تشغيل مفتوحة المصدر لحماية Linux بمساعدة الذكاء الاصطناعي



أطلقت OpenAI وCisco أداة Shirudo المفتوحة المصدر لنظام Linux، وتتيح لوكلاء الذكاء الاصطناعي كتابة ضوابط eBPF لحماية الأنظمة من الثغرات ومنح الفرق وقتاً أطول لاختبار التصحيحات.

- Shirudo بيئة تشغيل مفتوحة المصدر لنظام Linux من OpenAI وCisco، والاسم يعني «الدرع» باليابانية.
- تتيح لوكلاء الذكاء الاصطناعي الدفاع عن الأنظمة دون توقف الخدمة.
- يكتب الوكلاء ضوابط eBPF ديناميكية لحماية الأنظمة من الاستغلال.
- الهدف المعلن منح المدافعين وقتاً أطول لاختبار التصحيحات ونشرها.

ما الذي أُعلن

أطلقت OpenAI وCisco بشكل مشترك أداة Shirudo، وهي بيئة تشغيل مفتوحة المصدر لنظام Linux مصممة لتمكين وكلاء الذكاء الاصطناعي من المساعدة في الدفاع عن الأنظمة دون التسبب في توقف الخدمة. ويعني الاسم «الدرع» باليابانية.

ووفق OpenAI، تتيح الأداة للوكلاء كتابة ضوابط **eBPF** ديناميكية تحمي الأنظمة من الاستغلال، والفائدة المعلنة هي منح المدافعين وقتاً أطول لاختبار التصحيحات ونشرها.

ما لم تذكره المصادر

التقرير المتاح موجز؛ فهو لا يوضح التوزيعات المدعومة، ولا الثغرات أو أنواع الاستغلال التي تغطيها الأداة، ولا آلية مراجعة الضوابط التي يكتبها الوكلاء أو اعتمادها، ولا الأثر المتوقع على الأداء. ولا ينبغي افتراض أن Shirudo بديل عن التصحيح، فالغرض المعلن كسب الوقت إلى حين اختبار التصحيحات ونشرها.

الدلالات العملية

بالنسبة للجهات التي تشغّل Linux في بيئات الإنتاج، تُعد فكرة التخفيف المؤقت على مستوى بيئة التشغيل ذات صلة بنوافذ التصحيح في البيئات المنظمة، حيث لا يمكن تجاوز إدارة التغيير والاختبار. وفي المقابل، فإن السماح لوكلاء الذكاء الاصطناعي بتوليد ضوابط تعمل داخل النواة يثير أسئلة حوكمة تتعلق بالاعتماد والتسجيل والتراجع.

والنهج المتزن هو متابعة وثائق المشروع مع نضجه، وتقييمه في بيئة غير إنتاجية، وربط أي استخدام بعمليات إدارة الثغرات والتغيير القائمة قبل التفكير في توسيع اعتماده.

ما يجب فعله الآن

1. متابعة وثائق Shirudo وملاحظات إصداراته قبل اتخاذ أي قرار باستخدامه.
2. اختباره أولًا في بيئة Linux غير إنتاجية فقط.
3. تحديد قواعد الاعتماد والتسجيل والتراجع لأي ضابط eBPF يولده الذكاء الاصطناعي.
4. إبقاء التصحيح هو المعالجة الأساسية، والنظر إلى الحماية أثناء التشغيل كإجراء مؤقت.
5. مواءمة أي تجربة مع إجراءات إدارة الثغرات وإدارة التغيير لديكم.