مؤشرات الأمن المعدّة لعرضها في الاجتماعات قد لا تعكس واقع التعرض الحالي



يرى مقال في The Hacker News أن كثيراً من مؤشرات الأمن تُعدّ لتُعرض لا لتُستخدم، فلا تكشف ما يجري في البيئة أسبوعاً بعد أسبوع، وهي فجوة تزداد أهمية مع تسارع المهاجمين.

- يشير المقال إلى أن معظم مؤشرات الأمن تُصمَّم للعرض لا للاستخدام.
- تُجمع الأرقام غالباً قبيل المراجعة الربع سنوية وتُنقّح لتبدو مطمئنة.
- هذه الأرقام تطمئن الحاضرين في الاجتماع لكنها لا تصف حال البيئة في تلك الأسبوع.
- يربط المقال المشكلة بتحرك المهاجمين بسرعة الذكاء الاصطناعي.
- يشير محتوى مرتبط إلى تعرّض الهويات وتصعيد الصلاحيات عبر النطاقات بوصفهما مسارات هجوم ينبغي رسمها.

ينشر موقع The Hacker News مقالًا يلاحظ فيه أمراً بسيطاً عن واقع التقارير الأمنية: معظم المؤشرات تُبنى لتُعرض لا لتُستخدم. فبين مراجعة ربع سنوية وتحديث حالة تالٍ، تُجمع مجموعة أرقام وتُنقّح ثم تُقدَّم على أنها صورة لبرنامج سليم.

لماذا يهمّ ذلك

وفق المقال، تبدو هذه الأرقام مطمئنة داخل قاعة الاجتماع، لكنها لا تخبر أحداً تقريباً بما يجري فعلًا في البيئة خلال أسبوع بعينه. ويربط العنوان هذه الفجوة بتحرك المهاجمين بسرعة الذكاء الاصطناعي: فإذا لم تُحدَّث الصورة إلا قبل الاجتماع، تأخرت عن الواقع الذي يفترض أن تصفه.

والمقتطف الذي اطلعنا عليه قصير ولا يعرض منهجية الكاتب الكاملة ولا أرقاماً، لذلك نقتصر على فكرته المحورية.

تعرّض الهويات كموضوع ذي صلة

يشير محتوى ترويجي مرافق للمقال إلى قصص عن كيفية فتح تعرّض الهويات مسارات هجوم فعّالة، وعن رسم مسارات تصعيد الصلاحيات عبر النطاقات لقطع طرق الاختراق عند نقاط الاختناق الرئيسة. وهذا ليس من تحليل المقال نفسه، لكنه يدل على نوع الرؤية الحية القائمة على العلاقات التي يفضّلها على الملخصات الدورية.

والخلاصة العملية لقيادات الأمن والامتثال أن تسأل عن كل مؤشر يُرفع: هل هو محدَّث، ومن يتصرف بناءً عليه، وأي قرار يغيّره. فالأرقام التي توجد لدورة المراجعة فقط منتج تقارير لا أداة تشغيل.

ما يجب فعله الآن

1. راجع كل مؤشر في تقارير مجلس الإدارة واللجان وسجّل تاريخ آخر تحديث لبياناته.
2. حدد المؤشرات التي تُعدّ لدورات المراجعة فقط، واستبدلها أو عزّزها ببيانات قريبة من الزمن الحقيقي حيثما أمكن.
3. عيّن مالكاً وقراراً لكل مؤشر رئيس، بحيث يستدعي تغيّر الرقم إجراءً.
4. أدرج تعرّض الهويات ومسارات تصعيد الصلاحيات في تقارير التعرض.
5. واءم التقارير المحدّثة مع مراقبة الضوابط القائمة وفق ضوابط NCA ECC وإطار SAMA CSF.