كبير مسؤولي أمن المعلومات في Google Cloud: يجب أن تكون إجراءات الوكلاء قابلة للتتبع والتدقيق والعكس



في مقابلة، يرى مسؤول أمن المعلومات في Google Cloud أن الدفاع بوتيرة بشرية لم يعد كافيًا أمام الهجمات الآلية، ويدعو إلى هويات مستقلة للوكلاء وسجلات قرارات محصّنة ضد العبث.

- يقول كريس بيتز إن الافتراض بأن سير العمل اليدوي بقيادة البشر سيبقى أساس الدفاع لم يعد صالحًا.
- يمكن للوكلاء الدفاعيين المستقلين تولي الإثراء والربط والفرز، ليبدأ المحللون من نتائج موثقة لا من تنبيهات خام.
- قد تعمل جهات التجسس المدعومة من دول دون عتبات التنبيه السلوكي، لكن بإمكان المدافعين ربط إشارات داخلية مثل صلاحيات الهوية ونشاط التشغيل.
- ينصح بالابتعاد عن حسابات الخدمة المشتركة ورموز المسؤول الشاملة نحو هوية بأقل الصلاحيات لكل وكيل، يجري التحقق منها لكل معاملة.

- على مجالس الإدارة أن تسأل: هل يمكن تتبع كل إجراء ينفذه وكيل وتدقيقه والتراجع عنه؟

في مقابلة مع موقع Help Net Security، عرض كريس بيتز، كبير مسؤولي أمن المعلومات في Google Cloud، رؤيته لتغير الأمن مع انتشار وكلاء الذكاء الاصطناعي. ينطلق من أن الافتراض القديم ببقاء سير العمل المعتمد على البشر أساسًا للدفاع لم يعد صالحًا، لأن المهاجمين يستخدمون الأتمتة لاستكشاف الشبكات والتحرك جانبيًا خلال دقائق.

تغيّر دور مركز العمليات

يصف بيتز وكلاء دفاعيين مستقلين يتولون إثراء البيانات وربطها وفرزها. وفي رأيه لا يلغي ذلك دور المحلل، بل يغيّر نقطة بدايته: يصبح التنبيه خلاصة موثقة لتحقيق آلي. وينتقل المحللون المبتدئون إلى وضع المبادئ وتحديد الشهية للمخاطر والتحقق من الإجراءات الآلية، المصممة بحيث يفهمها إنسان خلال 60 ثانية ويمكن عكسها خلال 30.

الهوية والرقابة

يشير إلى أن جهات التجسس كثيرًا ما تتجنب الأدوات الصاخبة السريعة وتبقى دون عتبات التنبيه السلوكي. لكن المدافعين يملكون الحقيقة الداخلية: مخططات صلاحيات الهوية وبنية الشبكة ومصدر الشيفرة ونشاط التشغيل. ويوصي بالتخلي عن نماذج الثقة المسطحة وحسابات الخدمة البشرية المشتركة ورموز المسؤول الشاملة، وبتوسيع التحقق ليشمل كل معاملة، بحيث يملك كل وكيل هوية بأقل الصلاحيات يمكن التحقق منها.

أما بالنسبة لمجالس الإدارة، فالسؤال المحوري هو: هل يمكن تتبع كل إجراء ينفذه وكيل وتدقيقه والتراجع عنه؟ ويشير إلى ضوابط مركزية مع سجلات قرارات محصّنة ضد العبث، تسجل المدخلات وتعليل النموذج والأدوات المستدعاة والمعاملات الممررة وسند السياسة الذي سمح بالإجراء.

المقابلة رأي صادر عن مسؤول في جهة موردة، لكن نقاط الحوكمة فيها عملية لأي مؤسسة تجرب وكلاء الذكاء الاصطناعي.

ما يجب فعله الآن

1. حصر وكلاء الذكاء الاصطناعي العاملين أو قيد التجربة في الإدارات، بما فيها ما تطلقه مساعدات البرمجة أو فرق الأعمال.
2. استبدال حسابات الخدمة المشتركة ورموز المسؤول الشاملة المستخدمة في الأتمتة بهويات منفصلة بأقل الصلاحيات لكل وكيل.
3. تحديد ما يجب أن يسجله أثر قرار الوكيل (المدخلات والتعليل والأدوات والمعاملات وسند السياسة) وحفظه في سجلات محصّنة ضد العبث.
4. اختبار إمكانية شرح الإجراءات الآلية المؤثرة والتراجع عنها بسرعة قبل توسيع استقلالية الوكلاء.
5. إدراج قابلية تتبع إجراءات الوكلاء وعكسها ضمن تقارير مخاطر الأمن السيبراني الدورية لمجلس الإدارة.