Agentforce: حين تغذّي رسائل البريد الواردة وكيلاً ذكيًا يجب أن تشمل الحوكمة هذا المسار



يشير تقرير عن Salesforce Agentforce إلى أن ميزتين قياسيتين، هما Flow الذي يمرّر البيانات إلى موجّه الوكيل وEmail-to-Case لاستقبال الرسائل، قد تُربطان معًا، فتظهر أسئلة حوكمة قد لا تغطيها ضوابط البرمجيات التقليدية.

- في Agentforce، الطريقة الموصى بها لتشغيل الوكيل عند وقوع حدث هي Flow يمرّر بيانات السجل إلى موجّه الوكيل.
- تحوّل Email-to-Case وWeb-to-Case رسائل العملاء الواردة إلى سجلات حالات، وتُستخدم عادةً في دعم شركات الطيران والفنادق.
- كل ميزة منهما قياسية وموثّقة وتعمل كما صُمّمت.
- محور القلق هو ربط الميزتين معًا، وأن حوكمة صُمّمت للبرمجيات قد لا تناسب الوكلاء الموروثين.

تناول مقال حديث في The Hacker News نمطًا في Salesforce Agentforce لا يُعدّ ثغرة بالمعنى المعتاد، بل ميزتين موثّقتين تعملان كما صُمّمتا، وتتحولان إلى مسألة حوكمة عند الجمع بينهما.

ما الذي يصفه المصدر

في Agentforce، الأسلوب الموصى به لجعل الوكيل يستجيب للأحداث هو Flow. فعند إنشاء سجل أو تحديث حالة، يمرّر الـFlow البيانات إلى موجّه الوكيل. وبشكل منفصل، تحوّل Email-to-Case وWeb-to-Case رسائل العملاء الواردة إلى سجلات حالات، وهي الطريقة التي تدير بها جهات مثل شركات الطيران والفنادق استقبال طلبات الدعم.

وفكرة المصدر أن ربط هاتين الميزتين يخلق مسارًا من رسائل خارجية إلى موجّه الوكيل. ويرى العنوان أن الحوكمة المصممة للبرمجيات التقليدية لا تناسب الوكلاء الموروثين في مثل هذا المسار. والمقتطف المتاح لا يذكر خطوات هجوم أو نتائج محددة، لذلك لا نتجاوز ما ورد.

لماذا يهم المؤسسات المنظمة

قد تكون لدى المؤسسات التي تستخدم Salesforce لخدمة العملاء قنوات استقبال وأتمتة قائمة. وإضافة وكيل إلى Flow موجود تغيّر وظيفة مسار البيانات حتى لو لم يتغير أي مكوّن بمفرده. وقد تبقى الملكية والمراجعة وقبول المخاطر مبنية على التصميم السابق الخاص بالبرمجيات فقط.

والاستجابة الهادئة هي حصر المواضع التي يصل فيها نص وارد يتحكم فيه طرف خارجي إلى وكيل، والتأكد من وجود جهة مسؤولة عن هذا المسار.

ما يجب فعله الآن

1. حصر ما يمرّر بيانات الحالات أو السجلات إلى موجّهات وكلاء Agentforce من Flows.
2. تحديد قنوات الاستقبال مثل Email-to-Case وWeb-to-Case التي تغذّي تلك الـFlows.
3. تعيين مالك محدد لكل وكيل ولسير العمل الذي يشغّله، وتوثيق قبول المخاطر.
4. إدخال الوكلاء ضمن إدارة التغيير بحيث تستدعي إضافة وكيل إلى Flow قائم مراجعة.
5. التعامل مع نصوص العملاء الواردة كمدخلات غير موثوقة في تقييمات مخاطر الذكاء الاصطناعي والتطبيقات.