Elastic Security 9.6 يضيف وكلاء ذكاء اصطناعي لفرز تنبيهات مركز العمليات الأمنية



يقدّم Elastic Security 9.6 ميزة AlertZero، وهي وكلاء ذكاء اصطناعي لفرز التنبيهات والبحث عن التهديدات، مع حماية من برمجيات الفدية على Linux و143 قاعدة كشف لمنصات الذكاء الاصطناعي.

- يجمع AlertZero وكلاءه (Workers) في أربعة فرق: الفرز، وصيد التهديدات، وهندسة الكشف، والتحقيق الجنائي؛ وتضم النسخة التجريبية ستة وكلاء.
- ثلاثة مستويات للاستقلالية (يدوي، بمساعدة، بإشراف) تحدد ما إذا كان تنفيذ الإجراء يتطلب موافقة المحلل.
- يوسّع Elastic Defend حماية الفدية القائمة على السلوك إلى Linux ويضيف فحص ذاكرة العمليات بتواقيع YARA مخصصة.
- 143 قاعدة كشف في SIEM تغطي وكلاء البرمجة المختطفين وخوادم MCP الخبيثة وتسريب بيانات الاعتماد في الأوامر والاختراق (jailbreak) ومفاتيح API المسروقة.

- يُتوقع توفر الإصدار في Elastic Cloud Hosted وElastic Self-Managed مطلع ديسمبر.

أعلنت Elastic عن Elastic Security 9.6، وأبرز إضافاته AlertZero، وهي مجموعة وكلاء ذكاء اصطناعي تعمل في الخلفية على فرز التنبيهات والبحث عن التهديدات وضبط قواعد الكشف.

آلية عمل AlertZero

تُسمّى الوكلاء Workers وتُنظَّم في أربعة فرق: الفرز، وصيد التهديدات، وهندسة الكشف، والتحقيق الجنائي. وتضم النسخة التجريبية ستة وكلاء. يعمل كل وكيل وفق جدول زمني أو عند وقوع أحداث مثل ورود تنبيه جديد، ثم يقترح إجراءً، كإغلاق تنبيه كاذب أو عزل جهاز، مرفقًا بالأدلة الداعمة.

ويمكن للفرق اختيار أحد ثلاثة مستويات للاستقلالية. ففي الوضع اليدوي يتطلب كل إجراء موافقة المحلل. وفي وضع المساعدة يستطيع الوكلاء فحص القواعد وفجوات التغطية بأنفسهم، لكن التغييرات تبقى بحاجة إلى موافقة. أما في وضع الإشراف فتُنفَّذ إجراءات محددة دون موافقة مسبقة ويراجعها المحللون لاحقًا. وتعمل الإجراءات المعتمدة بصلاحيات المحلل وتُسجَّل كقرارات صادرة عنه. كما يختار العملاء فئة النموذج، بما فيها النماذج مفتوحة الأوزان والمستضافة ذاتيًا.

تغييرات أخرى في الإصدار 9.6

يوسّع Elastic Defend حماية الفدية القائمة على السلوك إلى أجهزة Linux، ويتيح فحص ذاكرة العمليات بتواقيع YARA مخصصة. ويضيف الإصدار 143 قاعدة كشف في SIEM لتهديدات الذكاء الاصطناعي، مرتبطة بإطاري MITRE ATLAS وMITRE ATT&CK، مع تحسين ربط الهويات عبر بيانات الأجهزة والهوية والسحابة. كما تدعم أداة Automatic Migration تعديل القواعد المترجمة من Splunk وQRadar وMicrosoft Sentinel عبر المحادثة.

التوفر

AlertZero متاح كنسخة تجريبية تقنية في Elastic Cloud Serverless. وتتوقع Elastic توفر 9.6، بما فيه ميزات Elastic Defend الجديدة، في Elastic Cloud Hosted وSelf-Managed مطلع ديسمبر. وعلى الجهات التي تدرسه أن تعامل مستوى الاستقلالية كقرار حوكمة لا كإعداد افتراضي.

ما يجب فعله الآن

1. إذا كنتم تستخدمون Elastic، فراجعوا ملاحظات الإصدار 9.6 وخططوا للاختبار عند توفره في نموذج النشر لديكم مطلع ديسمبر.
2. ابدؤوا أي تجربة لـ AlertZero بالوضع اليدوي، وحدّدوا الإجراءات التي يجوز نقلها لاحقًا إلى وضع الإشراف إن وُجدت.
3. تأكدوا من تسجيل موافقات المحللين على الإجراءات التي تقترحها الوكلاء بما يتوافق مع متطلبات المساءلة والتدقيق في مركز العمليات.
4. حدّدوا مكان معالجة النماذج، وهل تحتاجون إلى نماذج مستضافة ذاتيًا قبل إرسال بيانات التنبيهات إلى خدمة ذكاء اصطناعي.
5. قارنوا قواعد كشف تهديدات الذكاء الاصطناعي الجديدة باستخدام مؤسستكم لوكلاء البرمجة وخوادم

.MCP