ميزانية مركز العمليات الأمنية لعام 2027: التركيز على وقت المحللين لا على حجم الإنفاق فقط



يرى مقال عن ميزانيات مراكز العمليات الأمنية لعام 2027 أن الخسارة الأكبر هي وقت المحللين، ويورد تقدير ANY.RUN باسترداد 450 ساعة لكل 1,000 تنبيه عبر تسريع التحليل والبحث في مؤشرات الاختراق.

- يطرح المقال ضغط ميزانية مركز العمليات الأمنية بوصفه مشكلة ضياع وقت المحللين لا حجم الإنفاق الكلي.
- تقدّر ANY.RUN إمكانية استرداد 450 ساعة عمل للمحللين لكل 1,000 تنبيه يجري التحقيق فيه.
- تأتي الوفورات المقدّرة من تسريع تحليل التهديدات والبحث في مؤشرات الاختراق (IOC).
- يذكر المقال التحقيقات اليدوية والفحوصات المتكررة والتصعيد غير الضروري كأبرز مستنزفات الموارد.
- المقتطف المتاح لا يفصّل الأولويات الخمس الواردة في العنوان.

ما الذي يطرحه المقال

يتساءل مقال نشره موقع The Hacker News حول تخطيط ميزانية مركز العمليات الأمنية لعام 2027 عمّا إذا كانت المشكلة الحقيقية ليست حجم ما ينفقه المركز، بل مقدار وقت المحللين الذي يُهدر. ويشير إلى أن التحقيقات اليدوية والفحوصات المتكررة والتصعيد غير الضروري ما زالت تستنزف الموارد.

ويورد المقال تقديراً من ANY.RUN مفاده أن فرق المراكز قد تسترد 450 ساعة عمل للمحللين عن كل 1,000 تنبيه يجري التحقيق فيه، وأن هذا المكسب ينتج عن تسريع تحليل التهديدات والبحث في **مؤشرات الاختراق** (IOC).

كيف نقرأ هذا الرقم

الرقم تقدير صادر عن مزوّد، ولا يوضح المقتطف المتاح المنهجية أو الافتراضات خلفه. لذا يُفضّل التعامل معه كدافع للقياس الداخلي لا كمعيار جاهز لمركزكم. كما لا يعرض المقتطف الأولويات الخمس المذكورة في العنوان، ولذلك لا نلخّصها هنا.

ومع ذلك تبقى الفكرة الأساسية مفيدة في دورات الميزانية؛ فتكاليف الكوادر والأدوات ظاهرة، أما الوقت المهدور في الفرز المتكرر فيصعب رصده ونادراً ما يُسجَّل كبند تكلفة.

الخلاصة العملية

قبل طلب ميزانية إضافية لعام 2027، يمكن لقائد المركز أن يحدد أولًا أين تذهب ساعات المحللين فعلياً. وتساعد البيانات المستمدة من معالجة التنبيهات لديكم على تعزيز أي طلب، سواء للأدوات أو الكوادر أو تحسين الإجراءات، أمام الإدارة المالية ولجان المخاطر.

ما يجب فعله الآن

1. قيسوا عدد ساعات المحللين المستهلكة لكل تنبيه يجري التحقيق فيه، مقسّمة بين الفرز والإثراء والتصعيد.
2. حدّدوا الفحوصات اليدوية المتكررة وحالات التصعيد غير الضرورية في الحالات الأخيرة، وضعوا قائمة بما يصلح للتحسين.
3. راجعوا طريقة بحث الفريق في مؤشرات الاختراق (IOC) وهل يمكن جعلها أسرع أو أكثر اتساقاً.
4. تعاملوا مع تقديرات الوفورات من المزوّدين، مثل 450 ساعة لكل 1,000 تنبيه، كفرضيات واختبروها ببياناتكم قبل اعتماد الميزانية.
5. اربطوا طلبات ميزانية 2027 بوفورات الوقت المقاسة وخفض المخاطر ليتمكن المسؤولون الماليون ولجان المخاطر من تقييمها.