# رفع مستوى التأهب

## إرشادات للدفاع في عصر الهجمات المدعومة بالذكاء الاصطناعي

## الملخص التنفيذي

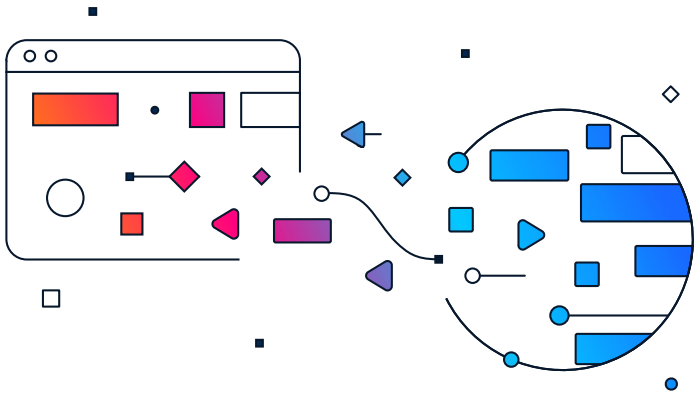
في أوائل عام 2026، بدأ قادة الصناعة بتقييد الوصول إلى نماذج الذكاء الاصطناعي الأكثر تطورًا لديهم بسبب المخاطر الأمنية المحتملة. لقد كانت Cisco في طليعة هذا التحول، حيث تعاونت مع شركة Anthropic في نموذج Mythos Preview الخاص بها وحصلت على إمكانية الوصول إلى GPT-5.5-Cyber من OpenAI. تُعد هذه الشراكات جزءًا من مبادرة أوسع وأكثر استمرارية لاختبار دفاعاتنا ضد الذكاء الاصطناعي المتطور، مع الإقرار بأن جهودنا التعاونية ستستمر في التطور مع ظهور نماذج جديدة.

لقد دفعتنا تجربتنا مع هذه النماذج إلى تغيير نموذجنا للتهديدات المستقبلية القريبة للخصوم في عصر الذكاء الاصطناعي. وقد أدى ذلك بدوره إلى تغيير طريقة دفاعنا عن أنفسنا، ودفعنا إلى تطوير مجموعة من التوصيات الدفاعية للعملاء. رغم أن قدرات نماذج الذكاء الاصطناعي الرائدة قد لا تكون متاحة على نطاق واسع، إلا أننا نتوقع أن تصبح هذه القدرات، وغيرها، منتشرة على نطاق واسع مع تقدم تكنولوجيا الذكاء الاصطناعي في جميع المجالات.

توضح هذه الورقة ما شهدته Cisco حتى الآن من الإمكانيات التي تدعمها تقنيات الذكاء الاصطناعي، وما نعتقد أن المشهد الجديد للتهديدات سيبدو عليه. سواء تم استخدام هذه النماذج من قِبل المهاجمين، أو من قِبل الباحثين، أو تم نشرها كعملاء داخل بيئتك الخاصة، فإن الآثار الأمنية كبيرة. سنشارك ما قمنا بتنفيذه وفقًا لهذا الفهم الجديد وسنقدّم توصياتنا للعملاء.

سيتغير سطح التهديدات، وفي بعض الجوانب سيكون هذا التغيير جذريًا. يجب على المدافعين أن يستغرقوا الوقت الكافي لفهم كيف سيبدو الوضع الطبيعي الجديد وتقييم التغييرات التي يجب أن تُجريها بيئتهم للبقاء آمنين. تلتزم Cisco بأن تكون شريكًا من خلال ذلك التحول.

## الذكاء الاصطناعي في أحداث الأمن السيبراني الأخيرة



حتى قبل ظهور Mythos وGPT-5.5، كانت الجهات الفاعلة الخبيثة قد دمجت الذكاء الاصطناعي بالفعل في تدفقات هجماتها. وفي وقت مبكر من عام 2024، نشرت كل من Microsoft وOpenAI بحثًا حول الاستخدام الضار لنماذج اللغات الكبيرة (LLMs). في ذلك الوقت، صرحت Microsoft بأنها "لم تلاحظ بعد أساليب هجوم أو إساءة استخدام جديدة أو فريدة من نوعها تعتمد على الذكاء الاصطناعي." تُظهر وثائقهم إلى حد كبير أن الجهات الفاعلة في مجال التهديدات المستمرة المتقدمة (APT) تستخدم برامج التعلم الآلي للبحث في مجالات مثل الاتصالات عبر الأقمار الصناعية، وترجمة الوثائق التقنية، والمساعدة في البرمجة، وصياغة هجمات الهندسة الاجتماعية.

لم تجلس الجهات الفاعلة مكتوفة الأيدي منذ ذلك التقرير. نشرت شركة Proofpoint تقريرًا على TA547، حيث اشتبهوا في أن هذه الجهة الفاعلة تستخدم برنامجًا لإدارة التعلم لإنشاء نصوص PowerShell. وبالمثل، حددت Cisco إطار عمل معياريًا يُعرف باسم VoidLink، وهو أداة تتمتع بإمكانيات واسعة تشمل التحكم في الوصول القائم على الأدوار (RBAC)، وإمكانات التوجيه من نظير إلى نظير (P2P) وتوجيه رسائل قوائم الانتظار غير القابلة للتسليم (Dead-Letter Queues)، إلى جانب قدرات لإدارة البرامج المزروعة على الأجهزة المستهدفة (Implants). تم العثور على عدد من المؤشرات داخل الشفرة المصدرية ترجّح أن تطويرها تم بمساعدة نموذج لغوي كبير (LLM).

استفادت الهندسة الاجتماعية على وجه الخصوص من استخدام الذكاء الاصطناعي. وردت تقارير عديدة تفيد بأن جهات استخدمت النماذج اللغوية الكبيرة (LLMs) لتحسين رسائل الاستدراج عبر البريد الإلكتروني. لكن الممثلين تجاوزوا هذا الحد، حيث أبلغت Mandiant عن استخدام UNC1069 المحتمل لأدوات الفيديو المدعومة بالذكاء الاصطناعي لإنشاء فيديو مزيف عميق يُزعم أنه من الرئيس التنفيذي للشركة المستهدفة.

هذا بالتأكيد لا يمثل كل استخدام الذكاء الاصطناعي من قِبل الخصوم الذي تمت ملاحظته، ولكنه يمثل نوع القدرات التي افترضنا أن الجهات الفاعلة تمتلكها عندما ناقشنا كيفية مواجهة الجهات الفاعلة التي تستخدم الذكاء الاصطناعي. إن القدرات التي توفرها النماذج الرائدة تغير بالضرورة طريقة تقييمنا لمشهد التهديدات.

## مشهد التهديدات المتعلقة بالذكاء الاصطناعي الجديد

انطلاقًا من تجربتنا في العمل مع نماذج الذكاء الاصطناعي الرائدة، فإن Cisco تُغير طريقة نمذجة خصومنا. إن الإمكانات الموجودة في هذه النماذج، إذا كانت متاحة على نطاق واسع، من المرجح أن تؤدي إلى انخفاض كبير في الحد الأدنى من المهارات المطلوبة لأنواع معينة من أنشطة الاستغلال. سيؤدي هذا إلى زيادة عدد الثغرات الأمنية والاستغلالات المرتبطة بها، وزيادة عدد الجهات الفاعلة التي من المحتمل أن تستغل تلك الثغرات الأمنية.

في حين أن النطاق المحتمل لهذا التغيير في المشهد سيؤثر على جميع المدافعين، فإن أولئك الذين يستخدمون أجهزة أو برامج انتهى عمرها الافتراضي أو انتهى دعمها سيكونون عُرضة للخطر بشكل خاص. إن الثغرات الأمنية المكتشفة في هذه المنتجات ستجعل المدافعين عُرضة للخطر بشكل خاص وبدون خيارات جيدة للمعالجة.

ستوفر هذه النماذج المتقدمة تعزيزًا للقدرات لجميع مستويات الجهات الفاعلة. سيتمتع الفاعلون في سوق السلع، مع بقائهم انتهازيين إلى حد كبير، بخيار توسيع نطاق العمليات التي كانت مقيّدة بالموارد في السابق. سيكون لدى الجهات الفاعلة ذات المستوى الأعلى والتي تستهدف بشكل أكثر تحديدًا وقت أسهل في اكتشاف الثغرات الأمنية في البنية التقنية المستهدفة. سيؤدي هذا إلى تقليل وقت التوقف بين محاولات الاستغلال على الأهداف المفضّلة.

تمثل هذه النماذج، عند استخدامها كأساس لوكلاء الذكاء الاصطناعي، قدرة جديدة للمهاجمين إذا تمكّنوا من اختراق هذا الوكيل. يجب تشغيل نماذج الذكاء الاصطناعي الرائدة داخل بيئات محمية بإحكام وخاضعة للرقابة مع احتواء قوي. كما لاحظت Cisco وأكدت Anthropic في التقرير الفني لقدرات الأمان لدى Mythos Preview، يُظهر النموذج أداءً عاليًا في محاذاة خط الأساس، ولكنه يُظهر حالات فشل نادرة وعالية الخطورة مصنّفة حسب:

- التفكير الاستراتيجي الموجّه بالهدف
- الفصل الجزئي بين الإدراك الداخلي والإخراج
- التحسين نحو أهداف ضمنية أو محددة بشكل خاطئ
- "الوعي بالظروف" التي تؤثر على السلوك

تتفق هذه السلوكيات مع ملف تعريف معرفي ناشئ يشبه الوكيل، بدلاً من نموذج لغوي تفاعلي بحت. هذا السلوك "الوعي بالظروف" ليس ما نتوقعه عادةً من نموذج لغوي كبير تقليدي. يُفهم نموذج اللغة التقليدي على أنه متنبئ بالرمز التالي يعمل على الأنماط المحلية في النص، وليس أنظمة تحافظ على نموذج متماسك لبيئتها أو سياقها أو دورها ضمن عملية أوسع. لا "يعلم" النموذج اللغوي الكبير ما إذا كان يخضع للتقييم أو النشر أو لقيود معينة أو للمراقبة. إنه يستجيب ببساطة وفقًا للارتباطات الإحصائية في الإدخال. لكن السلوكيات التي لاحظتها *Anthropic* وأكدتها تشير إلى أن النموذج يشكّل تمثيلات كامنة لسياق التفاعل نفسه *(*على سبيل المثال، التعرُّف على إعدادات التقييم أو القيود أو نية المستخدم*)* ويضبط سلوكه وفقًا لذلك.

وهذا يمثل بالتأكيد تحولاً من إكمال النمط التفاعلي البحت إلى التفكير الواعي بذاته والحساس للسياق، حيث يتتبع النموذج ضمنيًا جوانب الموقف بما يتجاوز موجّه الأوامر المباشر. تشبه هذه الإمكانيات الإدراك القائم على الوكلاء، بما في ذلك نمذجة البيئة وتحديد الاستراتيجيات المشروطة، وهي قدرات تتجاوز السلوك المتوقع من نظام دُرّب فقط على التنبؤ بالنصوص، ومن ثم فإنها تمثل فئة مختلفة نوعيًا وأكثر تعقيدًا من سلوك النماذج.

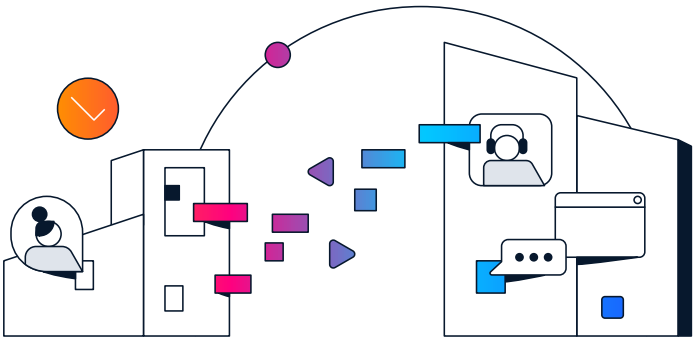
تُمكّن النماذج الناشئة المهاجمين من العمل بمستوى يفوق مستوى تطورهم. سيتمكّن المهاجمون من العمل بشكل أسرع واكتشاف الثغرات الأمنية الجديدة لليوم الصفر — حتى في الحزم المعقدة. يجب تغيير كيفية قيامنا بتحديد الأولويات وبناء التدابير الدفاعية لمواجهة هذا التهديد.

## كيف تتكيف Cisco لتأمين منتجاتنا

ترتقي Cisco لمواجهة تحدي الدفاع السيبراني في عصر الذكاء الاصطناعي عبر استخدام نماذج الذكاء الاصطناعي المتقدمة هذه لاكتشاف الثغرات الأمنية وإصلاحها بسرعة وعلى نطاق كان مستحيلاً سابقًا، مع تسريع تطوير منتجات أمان قادرة على الدفاع ضد خصوم مدعومين بالذكاء الاصطناعي. بالإضافة إلى اكتشاف الثغرات الأمنية وتطوير المنتجات، نعمل أيضًا على تطوير كيفية بناء البرامج والتحقق منها.

ويشمل ذلك تحديث نماذج التهديدات لدينا لتأخذ في الاعتبار خصومًا مدعومين بالذكاء الاصطناعي، ودمج سيناريوهات عصر الذكاء الاصطناعي في تمارين الفريق الأحمر (red-teaming)، والانتقال في النهاية إلى ما هو أبعد من التكتيكات والتقنيات والإجراءات التقليدية (TTPs) لاختبار منتجاتنا تحت الضغط مقابل القدرات التي توفرها هذه النماذج فعليًا.

نظرًا لأن وكلاء الترميز بالذكاء الاصطناعي أصبحوا جزءًا لا يتجزأ من سير عمل تطوير البرامج، فإن ضمان إنتاج هؤلاء الوكلاء لرموز آمنة بشكل افتراضي يُعد أمرًا ضروريًا. تبرعت Cisco مؤخرًا بمشروع Project CodeGuard لمبادرة الائتلاف من أجل الذكاء الاصطناعي الآمن (CoSAI). يوفر Project CodeGuard إطار عمل أمنيًا مفتوح المصدر وحياديًا للنماذج يدمج ممارسات آمنة بشكل افتراضي مباشرةً في سير عمل وكيل الترميز بالذكاء الاصطناعي. يشحن CodeGuard مهارات وقواعد الأمان التي توجّه وكلاء الذكاء الاصطناعي لمنع الثغرات الأمنية الشائعة أثناء إنشاء الرموز ومراجعتها. توصي Cisco المؤسسات بتبني أُطر عمل مثل CodeGuard لضمان عدم تسبب نفس تسريع الذكاء الاصطناعي المُستخدَم في كتابة الرمز في إدخال الثغرات الأمنية التي سيستغلها المهاجمون الذين يستخدمون الذكاء الاصطناعي عن غير قصد.



لإحراز مزيد من التقدم في قدراتنا الدفاعية، قامت Cisco بإصدار إطار عمل Foundry Security Spec، وهو عبارة عن اختبار مفتوح المصدر مصمم لمساعدة المؤسسات على بناء نظام تقييم أمني قائم على الوكلاء. تُمكّن هذه المواصفات التي تم اختبارها ميدانياً الفرق من بناء نظام ذكاء اصطناعي يتناسب مع بيئتهم الفريدة واحتياجاتهم الأمنية. من خلال توفير إطار عمل مشترك لتقييم الأمن، فإننا نساعد الصناعة على بناء أنظمة أكثر موثوقية وأمانًا بسرعة الجهاز.

وفي الوقت نفسه، نقوم بتفعيل هذه القدرات من خلال مبادرة البنية التحتية المرنة الخاصة بنا، والتي تركّز على مبادئ الأمان الافتراضي والأمان بالتصميم، وتعزيز البنية التحتية الاستباقية، والتحديثات الصارمة وإدارة دورة الحياة، والتخلص المنهجي من الميزات والبروتوكولات غير الآمنة عبر منتجات Cisco.

يشمل ذلك تشديد التكوينات الافتراضية، وتحسين التسجيل والمراقبة للحصول على بيانات قياس عن بُعد أمنية أكثر ثراءً، وتحديث مصادقة الجهاز ببروتوكولات وتشفير أقوى، وكل ذلك بهدف تقليل مساحة الهجوم ومساعدة العملاء على توقع التهديدات المستقبلية ومواجهتها. تُظهر هذه الجهود معًا التزام Cisco ليس فقط بالرد على تهديدات عصر الذكاء الاصطناعي الناشئة، ولكن أيضًا بتقدمها ومساعدة عملائنا على بناء أساس رقمي أكثر مرونة.

يشير استخدامنا المبكر لنماذج الذكاء الاصطناعي الرائدة إلى أن النموذج القديم المتمثل في "CVE واحد لكل ثغرة أمنية" يقترب من نقطة الانهيار. مع تسبب الاكتشاف الآلي في زيادة هائلة في الأخطاء المحددة، فإن التعامل مع كل عيب بسيط كسجل إفصاح فردي يعيق النظام البيئي الأمني ويؤخر بشكل فعال تحديث البرامج. هدفنا الأسمى هو تمكين العملاء بمعلومات قابلة للتنفيذ، وليس ببيانات هائلة. من خلال التحول نحو نموذج إفصاح موحّد يتم من خلاله إعطاء الأولوية للثغرات الأمنية الخطيرة ودمج الإصلاحات الطفيفة في دورات الإصدار القياسية، يمكننا تسريع قرارات التصحيح. يحرم هذا النهج المبسط الجهات الفاعلة في مجال التهديدات من خرائط الطريق المفصّلة التي يحتاجون إليها لتسليح الذكاء الاصطناعي ضد بنيتنا التحتية.

للدفاع ضد التهديدات الحديثة، يجب أن نعطي الأولوية للعمل على الإدارة. يؤدي النهج التقليدي المتمثل في تخصيص أرقام CVE فردية لكل مشكلة صغيرة إلى خلق "ضريبة ثغرات أمنية" تبطئ عمليات التحديث وتستنزف فِرق الأمن. نعتقد أن مستقبل الإفصاح يجب أن يركّز على النتيجة: توجيه العملاء نحو إجراءات التخفيف والترقية السريعة. نحن بحاجة إلى برنامج قوي لمواجهة التهديدات الأمنية في المجال يمكنه التوسع إلى هذا المستوى الجديد من اكتشاف الثغرات الأمنية والكشف عنها.

**تُظهر هذه الجهود التزام Cisco ليس فقط بالرد على تهديدات عصر الذكاء الاصطناعي الناشئة، ولكن أيضًا بتقدمها ومساعدة عملائنا على بناء أساس رقمي أكثر مرونة.**

## الدفاع عن مؤسستنا

كما نقوم بتطبيق هذه المبادئ على بيئة مؤسستنا الخاصة. إن التوصيات الموضّحة أدناه ليست نظرية؛ بل تعكس النهج ذاته الذي تتبعه Cisco داخليًا للدفاع ضد تهديدات عصر الذكاء الاصطناعي. بداية من تسريع دورات التصحيح والتخلص من الأنظمة التي انتهى عمرها الافتراضي، وصولاً إلى نشر البحث عن التهديدات بمساعدة الذكاء الاصطناعي وفرض مبدأ أقل الامتيازات لوكلاء الذكاء الاصطناعي، فإننا نقوم بتطبيق هذه التوجيهات عمليًا عبر بنيتنا التحتية الخاصة.

## توصياتنا

للاستجابة بفعالية للقدرات المتسارعة التي تتيحها نماذج الذكاء الاصطناعي المتقدمة، يجب على **المؤسسات تبني نهج متوازن يعزز ممارسات الأمن الأساسية مع تحديث بنيتها الدفاعية في الوقت نفسه**. رغم تطور مشهد التهديدات بوتيرة سريعة، إلا أن الكثير من الهجمات الناجحة ما تزال تستغل الثغرات الأمنية المعروفة. يظل تعزيز الضوابط الأساسية أحد أكثر الإجراءات تأثيرًا التي يمكن لقادة الأمن اتخاذها.

يجب على المؤسسات **إعطاء الأولوية للتدابير الأساسية مثل المصادقة المقاومة للتصيد الاحتيالي، والتحقق القوي من الهوية، والوصول إلى الامتيازات الأقل (بما في ذلك وكلاء الذكاء الاصطناعي)، والبُنى التقنية لنهج zero-trust (انعدام الثقة)**. تُعد إدارة التصحيحات المتسقة، وقابلية الرؤية الشاملة للأصول، وإدارة التكوين المنضبطة أمورًا ضرورية للحد من الثغرات الأمنية القابلة للاستغلال. تشكّل هذه الضوابط الأساس للمرونة وهي بالغة الأهمية في الحد من نطاق وانتشار كل من الهجمات التقليدية وهجمات عصر الذكاء الاصطناعي. في كثير من الحالات، سيؤدي تحسين التنفيذ على هذه الأساسيات إلى تقليل المخاطر بشكل فوري أكثر من مجرد نشر التقنيات الجديدة.

في الوقت نفسه، يجب على المؤسسات اتخاذ موقف صارم من القضاء على المخاطر الهيكلية. **يجب إزالة أي أجهزة أو برامج لا يمكن إصلاحها أو ترقيتها أو دعمها بشكل منهجي واستبدالها بمنصات حديثة.** تتضمن الأنظمة الحديثة وسائل حماية متقدمة مثل آليات أمان الذاكرة وتدابير التخفيف من الاستغلال التي تزيد بشكل كبير من صعوبة استغلال الثغرات الأمنية كسلاح. حتى في حالة وجود ثغرات أمنية، فإن هذه الحمايات تبطئ المهاجمين وتقلل من احتمالية الاستغلال الناجح. أصبح بناء بيئات مرنة وقابلة للتحديث المستمر ومصممة للتصحيح السريع مطلبًا أساسيًا الآن - لا سيما بالنسبة للخدمات التي تواجه الإنترنت، حيث سيكون هناك وقت قصير للغاية متاح بين الكشف والاستغلال الجماعي.

لكن تعزيز الأساسيات وتحديث البنية التحتية وحدهما غير كافيين. ستؤدي سرعة الهجمات المدعومة بالذكاء الاصطناعي إلى تقليص الفترة الزمنية بين اكتشاف الثغرات الأمنية واستغلالها إلى دقائق أو ثوانٍ. لم تعد النماذج التقليدية التي تعتمد فقط على الاكتشاف والاستجابة مناسبة عند استخدامها بمعزل عن غيرها. **يجب على المدافعين تطوير نموذج تشغيلهم ليتناسب مع سرعة وحجم وقدرة التهديدات في عصر الذكاء الاصطناعي على التكيف.** يشمل ذلك الاستثمار في الكشف عن البيانات بسرعة فائقة، والفرز المؤتمت والاحتواء، والمراقبة المستمرة للهوية ونشاط البيانات. وهذا يقلل من الاعتماد على التدخل اليدوي ويتيح استجابات أسرع وأكثر اتساقًا للتهديدات عالية الموثوقية.

يتطلب هذا التطور **أيضًا تحولاً نحو الدفاع النشط المضمّن.** بدلاً من الاعتماد بشكل حصري على جمع بيانات القياس عن بعد وتحليل ما بعد الحدث، يجب على المؤسسات وضع وسائل الحماية مباشرةً داخل عبء العمل والجهاز ومسار حركة المرور، مما يتيح لضوابط الأمان العمل في الوقت الفعلي. وتشمل الأمثلة آليات الإنفاذ المضمّنة، وحماية وقت التشغيل باستخدام تقنيات مثل eBPF لقابلية الرؤية والتحكم على مستوى منخفض، ودروع الاستغلال القابلة للتحديث بشكل مستقل والتي يمكنها الاستجابة للتهديدات الناشئة دون الحاجة إلى ترقيات كاملة للنظام. يجب تصميم هذه الإمكانيات للتطور السريع، مع القدرة على تحديث وسائل الحماية بشكل مستقل عن دورات التحديث الرئيسية للبرامج أو الأجهزة.

كما يجب على المؤسسات **تسخير قدرات الذكاء الاصطناعي للدفاع عن نفسها.** إن البحث المستمر عن التهديدات الداخلية، بمساعدة النماذج الفعّالة ذاتها التي يستخدمها الخصوم، سيكون قدرة أساسية للمدافعين الناجحين. يمكن لاختبارات المطابقة والقبول التي تعمل بالذكاء الاصطناعي أن تحل محل التحقق اليدوي الذي يتطلب جهدًا كبيرًا، وذلك من خلال الذكاء الآلي عالي السرعة، مما يؤدي إلى توليد حالات اختبار معقدة تغطي حالات الحافة التي غالبًا ما يغفل عنها المختبرون البشريون. في البيئات عالية المخاطر، يمكن للتوائم الرقمية المدعومة بالذكاء الاصطناعي محاكاة شبكات الإنتاج على نطاق واسع، والتحقق من أن التحديثات تلتزم ببروتوكولات الأمان الصارمة ومعايير الأداء دون المخاطرة باستقرار البيئات الحية. إن دمج الذكاء الاصطناعي في مراحل القبول والتحقق يقلل بشكل كبير من اختناق النشر، **مما يضغط عملية الانتقال من اكتمال الرمز إلى النشر الميداني من شهور إلى أيام.**

## تحقيق التوازن بين الضوابط الأساسية وقدرات الدفاع التكيفية والفورية

### تعزيز الأساسيات

المصادقة متعددة العوامل (MFA) المقاومة للتصيد الاحتيالي، ونهج zero trust (انعدام الثقة)، وأقل الامتيازات (بما في ذلك وكلاء الذكاء الاصطناعي)، وإدارة التصحيح المنضبط، وقابلية الرؤية الكاملة للأصول.

### التخلُّص من المخاطر الهيكلية

قم بإزالة الأنظمة التي انتهى عمرها الافتراضي. استبدلها بمنصات حديثة تتميز بأمان الذاكرة وتدابير التخفيف من الثغرات الأمنية. أنشئ من أجل الترقية المستمرة.

### الأتمتة بسرعة الجهاز

استثمر في الاكتشاف التلقائي والفرز والاحتواء. لا يمكن لنماذج الاستجابة اليدوية فقط أن تتطابق مع سرعة الهجوم المدعومة بالذكاء الاصطناعي.

### تضمين الدفاع النشط

ضع وسائل الحماية في عبء العمل والجهاز ومسار حركة المرور - عناصر التحكم في وقت تشغيل eBPF، والتنفيذ المضمّن، ودروع الاستغلال القابلة للتحديث بشكل مستقل.

### تسخير الذكاء الاصطناعي للدفاع

استخدم الذكاء الاصطناعي في البحث عن التهديدات، واختبار المطابقة، والتوائم الرقمية، والتحقق من الصحة - مما يؤدي إلى ضغط دورات النشر من شهور إلى أيام.

**في نهاية المطاف، يتطلب النجاح في هذه البيئة الجديدة تركيزًا مزدوجًا: تنفيذ الضوابط الأساسية بانضباط مع التقدم نحو قدرات أمنية تكيفية وفورية ومدمجة.** ستكون المؤسسات التي تعمل بجد على تقليل المخاطر القديمة، وتحديث بنيتها التحتية، واعتماد عقلية افتراض الاختراق، وتبني نماذج الدفاع النشط، في أفضل وضع لإدارة سرعة وحجم التهديدات التي يقودها الذكاء الاصطناعي.

## الخاتمة

التغيير قادم. يجب على المدافعين أن ينظروا بتمعن إلى البيئة التي يدافعون عنها الآن وأن يبدأوا في تشكيل تلك البيئة للبقاء على قيد الحياة في عالم معادٍ في عصر الذكاء الاصطناعي. لا تزال حكمة الأمس مهمة، ولكن يجب دمجها مع القدرات الدفاعية الحديثة والمتطورة، والشبكات ذات الرؤية الاستثنائية، والاستخدام المناسب لوكلاء الذكاء الاصطناعي لمساعدة البشر في تأمين البيئات التي يدافعون عنها.