يوليو 2026

نموذج تشغيلي جديد للبنية التحتية الحيوية

موجز تنفيذي حول الدفاع السيبراني في عصر الذكاء الاصطناعي

جدول المحتويات

التحول إلى الدفاع المستمر

لقد غيرت نماذج الذكاء الاصطناعي الرائدة المشهد التهديدي بشكل جذري. تُحدد هذه الأنظمة الآن الثغرات الأمنية، وتُعدّ برمجيات استغلالها، وتربطها ببعضها لتشكيل مسارات هجوم، وذلك بسرعة الآلة. هذه ليست دورة مؤقتة يمكنك تجاوزها بتنفيذ تصحيحات. إنه تحول دائم في السرعة التي يمكن بها اختراق بيئتك.

قوتان تعيدان صياغة مفهوم المخاطر

01 لقد تجاوزت الأحداثُ وتيرةَ إصدار التحديثات البرمجية

كانت الفترة الزمنية الفاصلة بين الكشف عن الثغرة ووقوع هجوم فعلي تتقلص بسرعة. قلص الذكاء الاصطناعي الرائد الجدول الزمني إلى ساعات.

02 لقد تلاشت عوائق الدخول

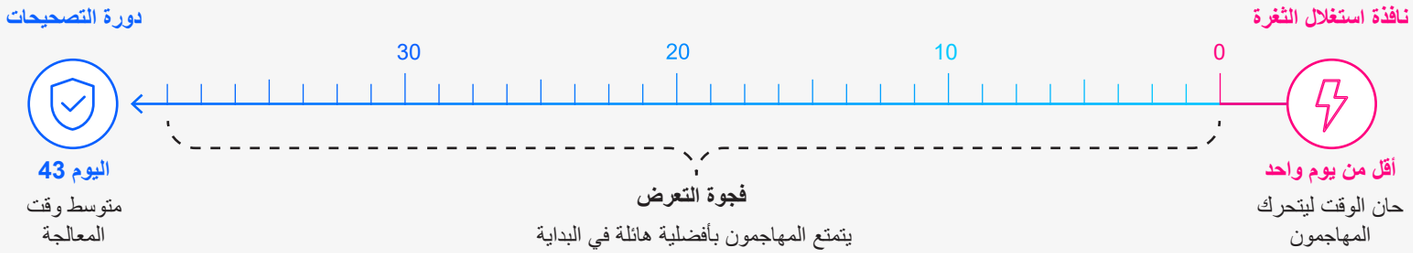
يمنح الذكاء الاصطناعي المهاجمين ذوي المهارات المحدودة القدرة على تنفيذ تقنيات متطورة كانت تتطلب في السابق موارد دول.

تتضافر هذه القوى وتتعاظم: إذ تؤدي سرعة الاستغلال إلى توسيع نطاق الثغرات التي يمكن للمهاجم الوصول إليها، بينما يؤدي انخفاض عوائق الدخول إلى توسيع دائرة المهاجمين القادرين على الوصول لتلك الثغرات. فرص أكثر، في أيدٍ أكثر، وبسرعة أعلى.

تواجه المؤسسات صعوبة في حماية هذا الواقع الجديد لسببين: البنية التحتية المتقادمة التي يتعذر تحديثها أو سد ثغراتها الأمنية، والمعالجات التي عفا عليها الزمن التي تتعامل مع أمن البنية التحتية باعتباره إجراءً يدوياً ودورياً.

يفترض النموذج التقليدي المستمر — القائم على التحصين والتحقق والصيانة — أن الخصوم يعملون ضمن قيود جدول الصيانة الخاص بك. إنهم لا يفعلون ذلك.

تكشف البيانات عن مخاطر هذا النهج: ففي عام 2025 ستستهدف 40% من أكثر الثغرات تعرضاً للاستغلال أنظمةً وصلت إلى نهاية عمرها الافتراضي. لا يزال المتوسط الزمني لمعالجة ثغرة أمنية حرجة يبلغ 43 يوماً. غير أن نافذة الاستغلال، أي الفترة الزمنية الفاصلة بين الكشف عن الثغرة وتحويلها إلى أداة هجومية، باتت تُقاس الآن بالساعات. في ظل هذا الواقع، لا تُعدُّ 43 يوماً تأخيراً. إنها اللعبة بأكملها.



40%

ثغرات مستهدفة تطال أنظمةً انتهت فترة دعمها

لا يمكن تصحيحها.
تبقى مكشوفة.

لماذا تُعد هذه الفجوة خطيرة للغاية:

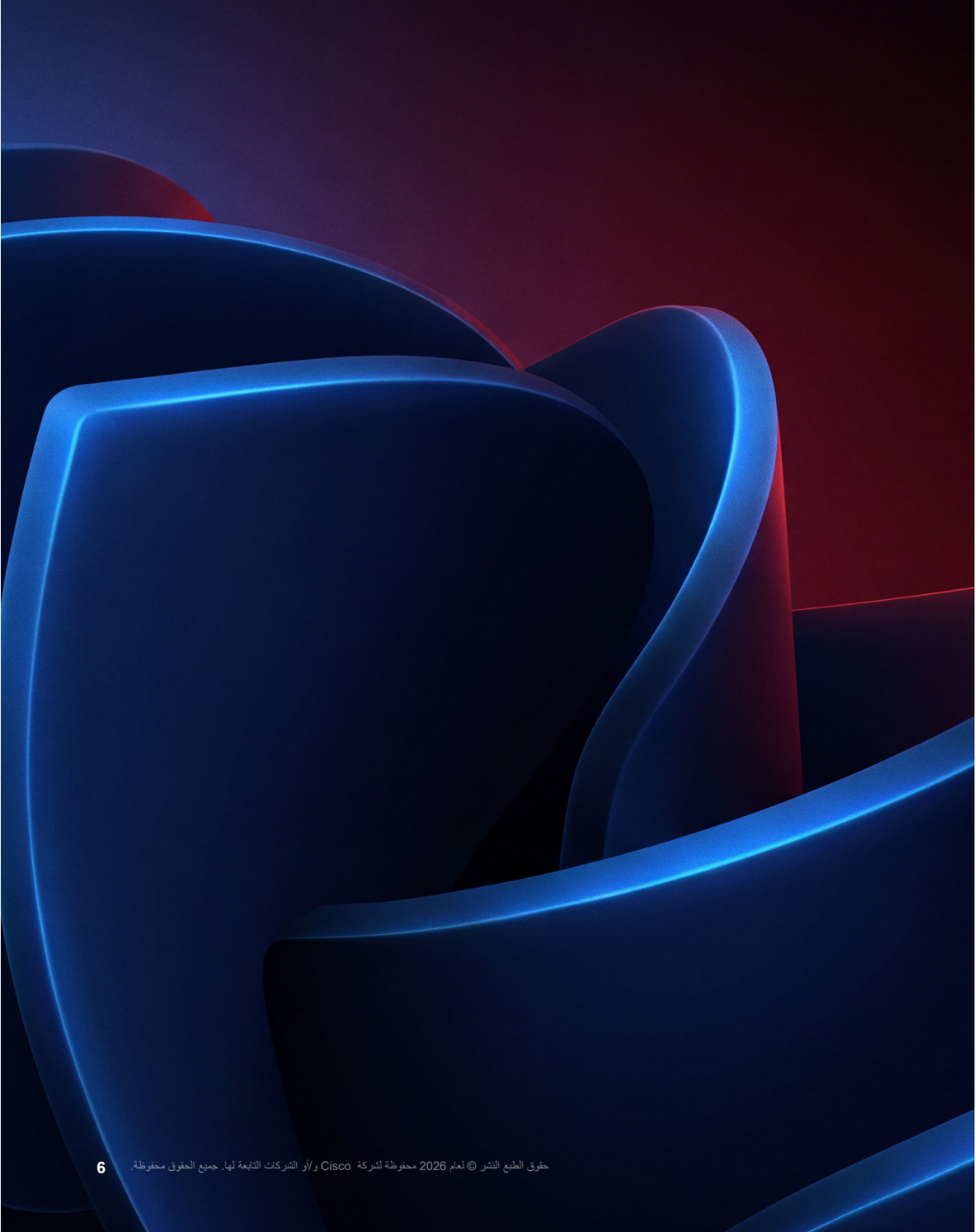
المصادر: *عام Talos قيد المراجعة* و*تقرير Verizon لعام 2026 حول تحقيقات اختراق البيانات*

إيقاع تشغيلي جديد

لا يمكنك التفوق على التهديدات المرتبطة بعصر الذكاء الاصطناعي باستخدام عمليات أو تقنيات قديمة. ما يلزم هو إرساء إيقاع تشغيلي مستمر: مواءمة عمليات تثبيت التصحيحات والترقيات مع وتيرة متكررة ومُتوقَّعة، وإخراج الأصول التي يتعذر تأمينها من الخدمة، والعمل بحزم على تقليل مستويات التعرض للمخاطر على مدار العام.

يستعرض هذا الموجز التنفيذي الخطوات العملية لحماية مؤسستك في عصر الذكاء الاصطناعي: تطوير نموذج التشغيل، وتحديث البنية التحتية، وتعزيز مستوى الأمن. راجع هذه الخطوات بالاشتراك مع مسؤولي الأمن والشبكات لديك؛ فاعتماد نهج يقتصر على نطاق واحد يفتح الباب أمام مخاطر غير ضرورية.

عندما تكون مستعداً للمضي قدماً، يمكن لفريق حسابات Cisco الخاص بك تزويدك بدليل عملي مفصل يمنح فرق الشبكات والأمن لديك توجيهات أكثر تعمقاً -وعلى مستوى الممارسة العملية- بشأن المعلومات الواردة في هذا الموجز.



من النظرية إلى الممارسة: الدفاع على نطاق الآلة

يُغير الذكاء الاصطناعي الرائد أساليب الهجوم والدفاع، ولكن ليس بالتساوي. كما وصف ريتش موغول، كبير المحللين في Cloud Security Alliance، في تقرير حديث، يتمتع المهاجمون بأفضلية حسابية؛ إذ لا يحتاجون سوى إلى العثور على ثغرة واحدة لاستغلالها. يجب على المدافعين تأمين كل مورد، وحمايته من كل مهاجم، في كل مرة. لا يمكنك التفوق على هذه الحسابات باستخدام العمليات التقليدية القديمة.
لاستعادة الأفضلية، أنت بحاجة إلى نموذج تشغيلي يساعد على تعزيز متانة الكود البرمجي، وتسريع عمليات سد الثغرات الأمنية، وتوفير حماية مستمرة وعلى نطاق واسع.

بدأت شركة Cisco بالفعل بتطبيق هذا النموذج

> في غضون ثمانية أسابيع فقط، قمنا بفحص 1.8 مليار سطر من التعليمات البرمجية عبر محفظة Cisco بأكملها؛ وهي عملية كان من شأنها أن تستغرق ثماني سنوات لو أنجزها فريق أبحاث الأمن لدينا. نحن لا نزال في البداية فقط.
>
> **أنتوني جريكو**
> نائب الرئيس الأول، و
> كبير مسؤولي الأمن والثقة في Cisco

يحتاج المدافعون إلى أكثر من مجرد إمكانية الوصول إلى نماذج ذكاء اصطناعي قوية. إنهم بحاجة إلى الخبرة ونموذج التشغيل لتحويل السرعة والنطاق اللذين يوفرهما الذكاء الاصطناعي إلى نتائج أمنية قابلة للتكرار. أثبتت منظمة Cisco Security and Trust هذا النهج داخل بيئتنا الخاصة أولاً، حيث جمعت بين الذكاء الاصطناعي الرائد والخبرة الأمنية والموارد المخصصة للعثور على الثغرات الأمنية وإصلاحها بشكل أسرع، وجعل التقييم قابلاً للتكرار، ونقل الوقاية إلى المراحل الأولية.

- **اكتشف المشكلات وعالجها بشكل أسرع:** من خلال المشاركة المبكرة في مبادرة Project Glasswing التابعة لشركة Anthropic وبرنامج Trusted Access for Cyber (TAC)، وظّفت Cisco نماذج ذكاء اصطناعي رائدة عبر محفظة حلولها، حيث قامت بتحليل 1.8 مليار سطر برمجي مكتوب بأكثر من 25 لغة برمجية في غضون ثمانية أسابيع. أظهر العمل كيف يمكن للمدافعين الاستفادة من سرعة الذكاء الاصطناعي وقدرته على العمل على نطاق واسع لتسريع اكتشاف الثغرات ومعالجتها في الأكواد البرمجية الفعلية للمؤسسات.
- **اجعل التقييم قابلاً للتكرار:** استنادًا إلى أعمال هندسة الأمن الداخلي تلك، قامت Cisco بنشر Foundry Security Spec مفتوحة المصدر، وهو مخطط تم اختباره عمليًا لبناء أنظمة تقييم أمنية فعّالة. يتيح هذا المخطط للمدافعين وسيلةً مستقلةً عن النماذج وعن البنية التقنية للانتقال من التنبيهات المليئة بالضجيج إلى نتائج محددة النطاق، ومُرتَّبة حسب الأولوية، وقابلة للتحقق.
- **نقل جهود الوقاية إلى مراحل مبكرة:** طوّرت Cisco مشروع Project CodeGuard وأتاحته كمصدر مفتوح، بهدف دمج قواعد "الأمان افتراضياً" في سير عمل البرمجة المعتمد على الذكاء الاصطناعي. عند دمجها مع Foundry Security Spec، يمكن تحويل الثغرات المؤكدة إلى قواعد قابلة لإعادة الاستخدام، مما يساعد في منع فئات الأخطاء المعروفة قبل وصولها إلى بيئة الإنتاج.

تحديد نموذج التشغيل الجديد للبنية التحتية الحيوية

نؤمن بأن المؤسسات بحاجة إلى التحول نحو نهج دفاعي مستمر عبر ثلاثة أبعاد: الوتيرة، والتحديث، والوضعية الدفاعية.

هذا النموذج المستمر يغير طريقة عملك: يصبح التحديث إيقاعًا مستمرًا بدلاً من كونه تدريبًا على الحريق، ويؤدي التحديث إلى تقليل المخاطر بدلاً من مجرد تحديث الأجهزة، ويقلل الوضع الأمني الديناميكي من نطاق تأثير أي اختراق.

	إن نهج ما بعد Mythos هو ترسيخ الأمر، وإثباته، والدفاع عنه باستمرار وبسرعة الآلة	**النهج القديم** عزّزه، أكد صحته، ولا تلمسْه
الإيقاع	ترقيات كبيرة كل 12 إلى 24 شهرًا	الجاهزية المستمرة للإصدار بنمط CI/CD
التحديث	معدات وبروتوكولات ونصوص برمجية متقادمة لا تزال قيد الاستخدام	الإزالة المستمرة لما يتعذر جعله آمناً
الوضع الأمني	استثناءات المخاطر الموثقة	تقليل التعرض المستمر والاحتواء

ابدأ من هنا: ثلاث أولويات

ببدأ التغيير بثلاث أولويات: تشغيل بنية تحتية مرنة لدعم أعمالك، ومعالجة البنية التحتية المتقادمة، وتعزيز مستوى أمنك العام. إليك ملخص لهذه المجالات ذات الأولوية، والأسئلة التي يمكنك طرحها على فريقك للبدء.

1. طوّر نموذجك التشغيلي لبنية تحتية مرنة

لم يعد تطبيق التصحيحات مشروعاً دورياً، بل أصبح قدرةً مستمرة. تفرض الحسابات هذا التحول: إذ تتزايد أعداد الأعطال التي تتطلب إصلاحاً في حين تتقلص النوافذ الزمنية المتاحة للصيانة، ولا يمكن للعمليات اليدوية التي تتم على مستوى كل جهاز على حدة سد هذه الفجوة، حيث يمكن للخصوم استغلال هذا التأخير. الحل هو وتيرة آلية يمكن التنبؤ بها، حيث تستوعب الأتمتة حجم العمل، وبالتالي يقضي المهندسين وقتهم في اتخاذ القرارات، وليس في التنفيذ على مستوى كل جهاز على حدة. ثم اجعل هذا الجدول الزمني ملزماً: حدد اتفاقيات مستوى الخدمة (SLAs) للمعالجة بناءً على فئة التعرض للمخاطر، بحيث يتم إغلاق الثغرات أو نقاط التعرض المواجهة للإنترنت في غضون أيام، ومعالجة الفئة التالية في الفترة الزمنية المحددة لها.

اسأل فريقك:

- ما هو المتوسط الحالي للوقت المستغرق من مرحلة التنبيه وحتى الإغلاق المُتحقَّق منه، مصنَّفاً حسب فئة التعرض؟
- ما هي الخطوات التي ما تزال يدوية؟

2. تحديث بنيتك التحتية

تنطوي الأصول غير المدعومة على مخاطر لا يمكن لأي تدبير وقائي معالجتها؛ فعند ظهور ثغرة أمنية جديدة، لن يكون هناك أي تصحيح متاح لها. لا يمكنك معالجة ما لم يعد المورّد يوفّر له الدعم والصيانة؛ فكل ما بوسعك فعله هو احتواء الموقف أو إخراج النظام من الخدمة. ولهذا السبب، لا تقتصر مناقشة التحديث على مجرد تجديد المعدات، بل تتعلق بالحد من المخاطر؛ إذ تستند الجدوى الاقتصادية للأمر إلى بيانات التعرض للمخاطر ودورة حياة الأصول، وليس إلى عمر المعدات. ولهذا السبب، لا تقتصر مناقشة التحديث على مجرد تجديد المعدات، بل تتعلق بالحد من المخاطر؛ إذ تستند الجدوى الاقتصادية للأمر إلى بيانات التعرض للمخاطر ودورة حياة الأصول، وليس إلى عمر المعدات.

اسأل فريقك:

- كم عدد الأصول التي تجاوزت تاريخ انتهاء الدعم أو اقتربت منه؟
- بماذا تتصل، وما هي تكلفة الاحتفاظ بها لعام آخر؟

3. تطوير وضعك الأمني

بات بإمكان الخصوم الذين يعتمدون على الذكاء الاصطناعي ربط الثغرات الأمنية ببعضها البعض بسرعة الآلة، مما يعرض بنيتك التحتية للخطر. قم بحماية الأصول المكشوفة لتقليل مساحة الهجوم. قسّم بيئتك لاحتواء الاختراقات والحدّ من نطاق تأثيرها. سُدَّ الفجوات المتعلقة بالهوية الخفية لمنع التصعيد. مع تزايد سرعة الهجمات وتجاوزها لقدرة الفرق البشرية، يحتاج مركز عمليات الأمن (SOC) لديك إلى الرؤية الشاملة، والأتمتة، وسير عمل الذكاء الاصطناعي الوكيلي لمواكبة هذا التسارع.

هذه الضوابط ليست جديدةً بأكملها، لكنَّ الحاجة الملحَّة إليها هي الأمر الجديد. إن تطبيقها الآن هو ما يجعلك متقدمًا بخطوة على المهاجم في المستقبل القريب، وليس فقط على ذلك المهاجم النادر والمتقدم تقنيًا في الوقت الراهن.

اسأل فريقك:

- إذا تمكن مهاجم من ترسيخ موطئ قدم له اليوم، فإلى أي مدى يمكنه التحرك عبر مسار الهجوم قبل أن نتمكن من احتوائه؟
- كيف سنعلم؟
- ما مدى سرعة استجابتنا؟

بمجرد تحديد هذه الأولويات الثلاث، يتحول التركيز من الاستراتيجية التقنية إلى التنفيذ التجاري وقياس النجاح.

قياس النجاح وتأمين الميزانية

قِس ما هو مهم، وضع إطارًا للاستثمار في سياق مخاطر الأعمال لضمان الحصول على الميزانية.

قياس النجاح

- **تتبَّع الوقت المستغرق من مرحلة تقديم المشورة وحتى الإغلاق.** القياس حسب فئة التعرض.
- **قياس عملة المجمّع.** تتبَّع النسبة المئوية للبيئة لديك التي تعمل بأحدث إصدار.
- **فرض اتفاقيات مستوى الخدمة (SLAs) الخاصة بالمعالجة.** ركِّز على اتفاقيات مستوى الخدمة القائمة على المستويات بدلاً من التعداد الأولي للثغرات الأمنية.
- **احتفظ بأدلة جاهزة للعرض على اللوحة.** احتفظ بسجلات الامتثال، والجداول الزمنية للمعالجة، وحالة الأصول جاهزةً للمدققين وشركات التأمين ضد المخاطر السيبرانية.
- **فرض المساءلة عن العمل القائم على المبادرة والفاعلية.** احرص على أن يكون كل إجراء ذي أثرٍ هام قابلاً للتدقيق والعكس، وأن يكون له مالك بشري مُحدَّد.

تمويل النموذج الجديد

- **حدد تسلسل الإنفاق.** اربط كل موجة من موجات التحديث بدورة الميزانية، مع إعطاء الأولوية للأصول الأكثر عرضة للمخاطر.
- **مواءمة الإنفاق مع التوقيت.** استخدم التمويل لتحويل النفقات الرأسمالية غير المخطط لها إلى دفعات يمكن التنبؤ بها.
- **حدده باعتباره متطلباً أمنياً.** التهديد يحدد الموعد النهائي. هذه ضرورة تجارية، وليست مجرد بند في قائمة أمنيات.
- **القدرة التشغيلية للصندوق.** خصِّص ميزانية للخدمات والشركاء لتوسيع نطاق جهود فريقك دون الحاجة إلى تعيين موظفين جدد.

أول 90 يومًا

إليك خمسة إجراءات يمكنك الموافقة عليها الآن. لا يتطلب أيٌّ منها تصميم البرنامج بالكامل أولاً، كما أن كلاً منها يُسهّل ما يليه.

1. **بدء تقييم التعرض.** أنشئ رؤية موحدة ومُرتَّبة حسب الأولوية، تُبيّن ما لديك، وما هو عرضة للمخاطر، وما هو غير مدعوم، وما يواجه تهديداً. سيكون هذا بمثابة مصدر الحقيقة المشترك لديكم.
2. **حدد اتفاقيات مستوى الخدمة الخاصة بالمعالجة حسب مستوى التعرض.** التزم بمعالجة نقاط التعرض المتاحة عبر الإنترنت أو تلك ذات الأهمية البالغة في غضون أيام، ومعالجة الفئة التالية في الفترة الزمنية الموالية، مع تقديم تقارير حول ذلك. هذا هو القرار المتعلق بالسياسة الذي يجعل الدفاع المستمر أمراً واقعاً.
3. **فعِّل نظام الإيقاع الدوري للعمل.** قم بتوحيد فترات التغيير والموافقة المسبقة على القوالب بحيث يصبح التحديث صيانة روتينية بدلاً من كونه استثناءً.
4. **قم بتسمية الموجة الأولى من أهداف التحديث.** حدد الأصول غير المدعومة ذات أعلى مخاطر وقم بتمويل استبدالها أولاً، مع بناء دراسة الجدوى على المخاطر وبيانات دورة الحياة واحتياجات العمل المستقبلية. تُعد عملية التحديث فرصةً لإنشاء بنية تحتية أكثر أماناً وجاهزيةً للمستقبل.
5. **قم بإجراء تمرين محاكاة للاستجابة في عصر الذكاء الاصطناعي.** محاكاة خصم يستغل ثغرة أمنية عند الحافة للتحرك الجانبي بسرعة الآلة، مع توحيد جهود الفرق بشأن الاستجابة.

كيف تقدم Cisco المساعدة

نحن في Cisco وشركاؤنا الموثوقون هنا لمساعدتكم على التعامل مع هذا الواقع الجديد. نقدم، بالتعاون مع شركائنا، خدمات احترافية لمساعدة مؤسستك في جميع هذه المجالات، بما في ذلك خدمات البنية التحتية المرنة من Cisco، التي توفر نهجاً منظماً ومُقسماً إلى ثلاث مراحل لتعزيز متانة البنية التحتية.

طوّر نموذجك التشغيلي لبنية تحتية مرنة:

ابتداءً من يوليو 2026، ستصدر شركة Cisco منتجاتها وفق جدول زمني ثابت مع إشعار مسبق، وبشكل متدرج بحيث لا يواجه أي فريق فترتين رئيسيتين في وقت واحد. نربط كل إشعار أمني بأصولك، ونرتب الأولويات بناءً على مستوى التعرض للمخاطر - وليس فقط درجة الخطورة - ثم نتحقق من تطبيق المعالجة بنجاح. عندما يتعذر نشر تصحيح برمجي أو ترقية في الوقت الراهن، توفر دروع وقت التشغيل الحماية للأصل دون التسبب في أي توقف عن العمل.

تحديث بنيتك التحتية:

نقدم عدة طرق لمساعدتك في تحديد أصول Cisco غير المدعومة والمعرضة للمخاطر، بالإضافة إلى توصيات لتعزيز أمان البنية التحتية وتفعيل تدابير حماية أمنية إضافية. عند التفكير في تحديث البنية التحتية واعتماد تقنيات عصرية، توصي Cisco بتبني بنية شبكية آمنة تدمج الأمن في صلب الشبكة ذاتها، وذلك من خلال آليات التقسيم القائمة على مبدأ "الهوية أولاً"، وسياسات موحدة، وآليات إنفاذ موزعة. وللمساعدة في هذا المسار، توفر Cisco Capital خيارات تمويلية لإدارة النفقات غير المخطط لها.

تطوير وضعك الأمني:

تؤمّن Cisco مسار الهجوم بالكامل: إدارة الهوية عبر الكيانات البشرية والآلية والذكاء الاصطناعي - وهو تمييز يزداد أهمية مع تزايد عدد العملاء؛ وفرض التجزئة لاحتواء الحركة الجانبية عند حدوث اختراق؛ وتسريع الكشف والاستجابة إلى سرعة الآلة، حيث يستوعب الذكاء الاصطناعي الحجم ويحتفظ المحللون بقرارات الحكم.

متابعة المحادثة

عندما تكون مستعداً للانتقال، تواصل مع فريق حسابات Cisco لمساعدتك في تحويل هذا الموجز إلى إجراءات عملية. يمكنهم إرشادك في هذه الرحلة، واطلاعك على خطة أكثر تفصيلاً وعملية تقييم مُصممة خصيصاً لتلائم مؤسستك وتحدياتها.

يُعد شركاء Cisco أيضاً مورداً ممتازاً. تتفاوت قدرات الشركاء، لذا عليك المواءمة بين نقاط قوة الشريك وبيئة عملك. تفضل بزيارة مركز شركاء Cisco للعثور على الخيار الأنسب.