cloud security alliance

CSA

CISCO

المنشور

إعداد شبكاتك لـ "عاصفة الذكاء الاصطناعي"

تقوية شبكتك ضد الهجمات المتسارعة للذكاء الاصطناعي

شكر وتقدير

المؤلف:

ريتش موغول

التصميم الجرافيكي

ستيفن سميث

نبذة عن الراعي

تحتل شركة Cisco (NASDAQ: CSCO) مكانة الريادة عالميًا في مجال التكنولوجيا، وقد أحدثت ثورة في طريقة الاتصال والحماية اللازمة للمؤسسات في عصر الذكاء الاصطناعي. لأكثر من 40 عامًا، قامت شركة Cisco بربط العالم بشكل آمن. فبفضل حلولها وخدماتها المعتمدة على الذكاء الاصطناعي والرائدة في مجالها، تتيح Cisco لعملائها، وشركائها، ومجتمعاتها فرص الابتكار، وتحسين الإنتاجية، وتعزيز المرونة الرقمية.

https://www.cisco.com/site/ae/ar/solutions/artificial-intelligence/security-in-ai-era.html

جدول المحتويات

مقدمة

إن التطورات في نماذج الذكاء الاصطناعي تُغير العلاقة بين المهاجمين والمدافعين، مما يقوض افتراضات المخاطر التاريخية التي استخدمناها لتطوير برامجنا الأمنية. كما يتضح من إصدار نماذج ذات قدرات متقدمة، مثل Mythos وChatGPT 5.5 (والمفصلة في "عاصفة ثغرات الذكاء الاصطناعي")، فإن النماذج تتطور بسرعة وتحسن قدرتها على اكتشاف الثغرات الجديدة، وإنشاء استغلالات جديدة، والانخراط في هجمات مؤتمتة معقدة ومتعددة المراحل. لقد أظهرت لنا السنوات القليلة الماضية أن قدرات النماذج الرائدة اليوم ستتم مواكبتها بسرعة من خلال نماذج أساسية متاحة على نطاق واسع، وفي النهاية نماذج محلية مفتوحة الوزن.

لم تعد نماذج المخاطر الأساسية التي استخدمناها لبناء برامجنا الأمنية صالحة. كان اكتشاف الثغرات الأمنية الجديدة وإنشاء ثغرات استغلال جديدة يستغرق شهورًا أو حتى سنوات، ولكنه الآن يستغرق ساعات. كانت تلك الاكتشافات، واستخدامها في الهجمات، تتطلب مهارات تقنية واسعة النطاق، لكن تلك الحواجز تنهار بسرعة. تتغير اقتصاديات الدفاع السيبراني؛ فمع انخفاض متطلبات الوقت والمهارة اللازمة للهجوم، لم تعد جداولنا الزمنية الدفاعية التاريخية فعالة، ونحن بحاجة إلى إعادة توجيه برامجنا.

بينما يُمكّن الذكاء الاصطناعي كلاً من المهاجمين والمدافعين، إلا أنه لا يفعل ذلك على قدم المساواة. كما هو موضح في Core Collapse، هناك عدم تناسق رياضي أساسي: يتمكن المهاجمون من تركيز كل جهودهم على مشكلة واحدة (العثور على ثغرة أمنية *هنا*، أو تطوير استغلال *لهذا*، أو مهاجمة *هذا* الهدف)، بينما يواجه المدافعون التعقيد التوافقي المتمثل في الاضطرار إلى الدفاع عن جميع الموارد من جميع المهاجمين ومن جميع الاستغلالات المحتملة طوال الوقت.

ويتضح هذا بسهولة من خلال النظر إلى تأثير ثغرة أمنية واحدة تم الكشف عنها حديثًا. يمكن للمهاجمين استخدام الذكاء الاصطناعي لتطوير ثغرة أمنية بسرعة وبدء هجمات آلية. يتعين على المدافعين، حتى مع وجود التحديث في متناول اليد، تحديد كل مورد يحتاج إلى التحديث، واختباره، ثم نشره دون تعطيل التطبيقات قيد التشغيل. إنها منافسة تجري وفق قوانين فيزيائية مختلفة، بغض النظر عن مدى براعتنا.

توجد استراتيجيات قائمة تساعد على إعادة التوازن إلى المعادلة. بمرور الوقت، ومع تقييم جميع البرامج الجديدة وتحصينها قبل إصدارها باستخدام LLMs، يمكننا أن نتوقع انخفاض العدد الإجمالي للثغرات الأمنية في البرامج. وبصفتنا مدافعين اليوم، يمكننا أيضاً إضافة حدود أمنية *لزيادة التعقيد التوافقي للهجمات الناجحة*.

إن بناء القدرة على الصمود أمام المهاجمين المدعومين بالذكاء الاصطناعي يشمل جميع جوانب التكنولوجيا، ويتجاوز بكثير ما يمكن لفرق الأمن إدارته بنفسها. نحن بحاجة إلى زيادة الحواجز الأمنية في جميع المجالات، بدءًا من الهويات وأحمال العمل، وصولاً إلى الحاويات وواجهات برمجة التطبيقات والنقاط الطرفية.

تُعد الشبكات واحدة من أهم أدواتنا لفرض هذه الحدود، ولكن أمن الشبكة وتصميمها ونماذج تشغيلها في معظم الشبكات الفعلية قيد الإنتاج غالباً ما تكون غير كافية. على الرغم من سنوات من التقدم والاستثمار، لا يزال لدينا الكثير من الشبكات المسطحة، ونعتمد في كثير من الأحيان على أجهزة قديمة، ولدينا عمليات تشغيل وأمن الشبكة غير مهيأة للاستجابة السريعة والأتمتة. قد يستغرق تغيير قاعدة جدار الحماية، وهو أمر بسيط، أسابيع أو شهورًا في المؤسسات ذات الشبكات المعقدة.

لزيادة تعقيد المهاجمين (وتكاليفهم)، ينبغي أن تقوم شبكاتنا بما يلي:

- تسريع وتيرة التصحيحات بشكل سريع واستهداف التصحيحات بشكل مستمر.
- تقليل نطاق الانفجار من خلال تحسين تجزئة الشبكة والحد من مواقع تعرض البيانات عالية القيمة.
- أضف طبقات دفاعية *متسلسلة متعددة، وليست متوازية*، لإجبار المهاجمين على تجاوز حدود متعددة. على سبيل المثال، جدران حماية متعددة في طبقات مختلفة ضمن مجموعة تطبيقات واحدة.
- احصل على الدعم من خلال عمليات تشغيلية سريعة الاستجابة يمكنها التكيف بالسرعة التي تتغير بها بيئة التهديد.

إن استخدام قدرات الذكاء الاصطناعي المتقدمة لأغراض دفاعية سيمكن في نهاية المطاف المؤسسات الماهرة في استخدام الذكاء الاصطناعي من الحصول على توقيت تنافسي بما يكفي لتحمل سرعة المهاجم في تطوير الثغرات الأمنية. في هذه الأثناء، ستكون حدود الأمان هي الأداة لإبطاء الهجمات ومنحنا الوقت لتحديث عمليات النشر.

يقدم هذا البحث إرشادات لمسؤولي الشبكات وأمان الشبكات. لا يمكننا تلبية متطلبات المرونة الجديدة لدينا من خلال دفاعات الشبكة وحدها، ولكن زيادة حدود أمان الشبكة هي واحدة من أكثر الأماكن فعالية للبدء.

تحديث الشبكات للدفاع المستجيب

كقطاع صناعي، قمنا بتحديث شبكاتنا لأكثر من عقد من الزمان، بدءًا من تحسين دفاعاتنا المحيطية وصولاً إلى زيادة تجزئة الشبكة، وقد تسارع هذا الأمر في السنوات الأخيرة. لقد دفعنا الانتقال إلى السحابة إلى أبعد من ذلك، لأن الشبكات السحابية يتم تعريفها بواسطة البرامج بشكل افتراضي، والشبكات التي يتم تعريفها بواسطة البرامج تجعل إنشاء الحدود والتقسيم وتغييرها أسهل بكثير.

لكننا واجهنا تحديات حقيقية ومشروعة في تحديث هذه الشبكات على نطاق واسع. لا تزال العديد من الشبكات المادية، إن لم يكن معظمها، مسطحة نسبيًا من الداخل. حتى الشبكات السحابية، التي تتميز بمرونة عالية وسهولة في التقسيم، ودائمًا ما تكون محددة بالبرامج، ليست دائمًا أفضل، ويرجع ذلك إلى حد كبير إلى عمليات الترحيل التي نسختها تصميمات مراكز البيانات القديمة. غالباً ما ركزت عمليات تنفيذ Zero Trust بشكل أكبر على تأمين القوى العاملة وحافة الحرم الجامعي، وأقل على مركز البيانات وحركة البيانات بين التطبيقات (الشرقية الغربية). نحن لا نمتلك بالضرورة شبكاتنا الخاصة ونديرها، ونواجه قيودًا على إمكانية مراقبة طرف خارجي.

بدأت العديد من المنظمات في تطبيق التجزئة الدقيقة، ولكن عادةً ما يكون ذلك فقط لمجموعات فرعية صغيرة من شبكاتها (بسبب تعقيدات التنفيذ). معظم أجهزتنا قديمة، ويصعب تحديثها وتستغرق وقتًا طويلاً. وعملياتنا التشغيلية منهجية عن قصد: خارج المحيط، لم نكن بحاجة أبدًا إلى تصحيح الشبكة الداخلية بسرعة، لذلك ركزت عملياتنا على الحافة، مع تحرك الترقيع الداخلي بشكل أبطأ بكثير.

لم يكن أي من هذا خطأً؛ لقد كان رد فعل معقولاً على المخاطر التي واجهناها. معظم توصياتنا الواردة في هذا البحث معروفة جيدًا وقيد التنفيذ. تكمن المشكلة في أن الذكاء الاصطناعي يغير المخاطر والجداول الزمنية. ولا يقتصر الأمر على المحيط فحسب، بل تصبح حواجز شبكتنا الداخلية توسعًا مهمًا للحدود الأمنية التي تعتبر ضرورية لخنق مزايا الذكاء الاصطناعي للمهاجم. تعني الشبكات المسطحة نطاق انفجار أكبر عند انفجار شيء ما. لا يمكن للتغيير البطيء والمنهجي أن يواكب تطور الثغرات الأمنية الذي يتم الآن في غضون ساعات. وتصبح الأجهزة التي لا يمكنك إصلاحها بسرعة، حتى لو كانت خلف جدران الحماية، مصدرًا لمسؤولية أكبر بكثير.

والخبر السار هو أننا نعرف بالفعل ما يجب فعله، لكن التحدي الجديد هو التنفيذ. نحن بحاجة إلى التحرك بوتيرة سريعة لأن افتراضات المخاطر الأساسية التي استخدمناها لتبرير الأولويات والجداول الزمنية التاريخية لم تعد سارية. يمكن أن تكون أساسيات أمان الشبكة لدينا المتمثلة في التجزئة وقابلية التصحيح والعمليات الاستجابية فعالة للغاية في تحقيق التوازن، ولكننا نحتاج الآن إلى التنفيذ بمزيد من الدقة، وبترتيب ذي أولوية، وفي أطر زمنية ضيقة.

كما يجب أن تعمل هندسة/عمليات الشبكة وأمن الشبكة جنبًا إلى جنب لمعالجة هذه المشاكل. تشمل الحلول أنظمة معزولة، مما يتطلب مزيجًا من البنى الأساسية، وتصحيح الأخطاء وإدارة الثغرات الأمنية، والدفاعات الأمنية الخاصة مثل NGFWs وWAF. أما بقية هذا البحث فيوضح عناصر التحديث، ثم كيفية الوصول إلى ذلك على مراحل.

كتل البناء والمعالجة

هناك ثلاثة أبعاد لتحديث الشبكات للاستجابة لمخاطر الذكاء الاصطناعي المعادي:

- **نموذج التشغيل/العمليات:** بما أننا بدأنا بتمديد الأسلاك إلى الصناديق والدفاع عن عناوين IP بطيئة التغيير، فإن عمليات الشبكة وأمان الشبكة تميل إلى أن تكون منهجية، خاصة بالنسبة لتحديثات الأجهزة والتغييرات الهيكلية. تم تصميم هذه العمليات للبيئات ذات التبعيات

المادية. ركزت عملية التصحيح على الحافة، مع اعتبار الأجهزة الداخلية ثانوية لأنها أقل خطورة. قامت معظم الشبكات بتطبيق دفاعات من طبقة واحدة أو طبقتين، تركز على حركة المرور بين الشمال والجنوب للحماية من تهديدات الإنترنت. الحوسبة السحابية أكثر ديناميكية، ولكن بشكل غير متساوٍ، بناءً على النضج، والاعتماد على النقل المباشر، والتبعيات الهجينة. التحول من *المشاريع الدورية إلى العمليات المستمرة*. ليس فقط من أجل التحديثات والتصحيحات، ولكن من أجل التقسيم نفسه: إضافة الحدود والحفاظ عليها أثناء البناء، بدلاً من اعتمادها كبنية واحدة مكتملة. فكر في الأمر على أنه حلقتين تعملان بشكل متوازٍ:

- **حافظ على الشبكة مصححة وحديثة**: الهدف هو التصحيح المستمر بالإضافة إلى إيقاع التحديث ذي الأولوية، حتى لا تتعثر أبدًا في الدفاع عن شيء لا يمكنك إصلاحه. تاريخيًا، كان هذا الأمر يمثل تحديًا كبيرًا لأجهزة الشبكة، ولهذا السبب نوصي بالتعامل مع هذا الأمر كعملية تشغيلية جديدة والبدء بالموارد الخارجية. يمكن ويجب دمج هذا في برنامج *VulnOps* الخاص بك. كما هو موضح بشكل أكبر في تقرير Vulnerability Storm، فإن VulnOps يتعامل مع إدارة الثغرات الأمنية كبرنامج على غرار DevOps مع أتمتة مستمرة.
- **تحديث التجزئة والعزل**: الانتقال نحو التجزئة الدقيقة وإضافة وصيانة حدود متعددة باستمرار (شمال، جنوب، شرق، وغرب) مع تغير التطبيقات، ويتم ذلك من خلال مزيج من الطوبولوجيا والدفاعات الأمنية.

- **البنية التحتية:** الشبكة نفسها هدف، ونتوقع أن نشهد زيادة في حجم الثغرات الأمنية واستغلالها في أجهزة وبرامج الشبكة المستخدمة في الهجمات الآلية. هذا يحدث بالفعل اليوم؛ ففي الأسابيع التي كنا نكتب فيها هذه الورقة، كانت هناك حملات متعددة تستهدف البنية التحتية للشبكة. يجب أن تكون الشبكات:
  - **حاليًا**: أجهزة مُحدّثة لم تنتهِ صلاحيتها ولا تزال مدعومة.
  - **قابلة للتصحيح:** ليس فقط الأجهزة المحدثة، ولكن أيضًا مدمج في برنامج تحديث قادر على التحديث في غضون ساعات، وليس أسابيع.
  - **الشبكات المعرفة بواسطة البرامج:** كما هو موضح جيدًا في الحوسبة السحابية، فإن الشبكات المعرفة بواسطة البرامج (SDN) أكثر مرونة وغالبًا ما تكون قائمة على الرفض الافتراضي (اعتمادًا على النظام الأساسي، على سبيل المثال، محيط البرمجيات المعرف (SDP))، حيث تكون التجزئة هي الحالة الأساسية بدلاً من كونها إضافة.
- **البنية التقنية:** تحدد البنية التقنية الحدود التي تزيد من التعقيد والتكاليف على المهاجمين. لا يمكننا بالضرورة الانتقال فورًا إلى حماية كل أصل بجدار ناري على كل مستوى، لكننا نبني على هذه الأسس:
  - **أمان المحيط:** إنه ما نميل إلى أن نكون الأفضل فيه اليوم، وهذه الحاجة لا تزول. لكن، كما سترى، نحن بحاجة إلى مواءمتها مع نموذج التشغيل الأكثر استمرارية لدينا، وفي بعض الحالات، قد نرغب في تنوع أكبر في المنصات وزيادة تجزئة المحيط.
  - **التجزئة الكلية:** تجزئة أفضل لوحدات الأعمال، ومجموعات التطبيقات، وبيئات التشغيل. الهدف هو حصر نصف قطر الانفجار في "مكدس" واحد داخل الشبكة.
  - **التجزئة الدقيقة:** إضافة حدود داخل طبقات مجموعة التطبيقات، مع زيادة الحدود بين التطبيقات والخدمات.
  - مبدأ **Zero Trust:** يجمع بين تلك الحدود وسياسة الهوية والسياق التي يتم التحقق منها باستمرار، بحيث يتم منح الوصول لكل طلب بدلاً من موقع الشبكة. لم يعد الاعتماد على عنوان IP أو شبكة VLAN يصبح ديناميكيًا، وأقل امتيازًا، ومرتبطًا بالهوية والمخاطر بدلاً من بنية الشبكة. يتضمن ذلك تقنيات مثل المحيط المعرّف بالبرمجيات (SDP).

ويرتكز كل هذا على الرؤية (ما لدينا وأين وكيف تم تكوينه)، والنسب (من يملك ماذا وهو المسؤول عن القرارات التجارية والتقنية)، ومن الناحية المثالية، القياس عن بعد في الوقت الفعلي. *لا تقلل من شأن تعقيد تلبية هذه التوصيات*، لكن التقنيات الحديثة تجعل الأمر أكثر قابلية للتحقيق، خاصة على أساس كل مشروع على حدة.

يمكننا أيضًا استخدام أدوات الذكاء الاصطناعي بأنفسنا للاختبار والتحسين المستمر. قم بتوجيه أنظمة إدارة التعلم الخاصة بك إلى شبكتك، وقم بتزويدها بأدوات تقييم (آمنة)، واستخدم تلك النتائج لمعرفة نقاط قوتك وضعفك من منظور المهاجم.

كل هذا يستغرق وقتًا، وأحيانًا سنوات، وقد بدأت بالفعل الهجمات المعادية التي يقودها الذكاء الاصطناعي. نوصي باتباع نهج مرحلي، ذي أولوية، قائم على المخاطر، والذي يمكن أن يوفر نتائج ملموسة بسرعة وبشكل أكثر واقعية، مع الاستمرار في تشكيل أساس جيد لتحقيق الأهداف طويلة المدى.

نقطة مهمة: يمكن تشغيل المراحل التالية بالتوازي، كجزء من عملية تشغيل مستمرة. ليس من الضروري إكمال مرحلة واحدة بالكامل قبل الانتقال إلى المرحلة التالية.

المرحلة 1: التجديد والتعزيز ذو الأولوية والتركيز

سيبدأ المهاجمون بما يمكنهم الوصول إليه، وبصفتنا مدافعين، فإننا نهتم بما سيؤذينا أكثر عندما يتم اختراقه. وبالتالي، فإن الخطوة الأولى هي تحديد نقاط الضعف الخارجية لديك ومواءمة ذلك مع أولويات مؤسستك.

في هذه المرحلة، فكر "من الخارج إلى الداخل، الأصول الرئيسية أولاً". تبدأ بتحديد سطح الهجوم المواجه للإنترنت، مع تحديد أهم أصولك الرقمية (الجواهر الثمينة). عند تحديد سطح الهجوم، فإننا نعني *كل شيء*. كل جهاز وكل خدمة، *بما في ذلك جميع أجهزة وخدمات الأمان والشبكة*. أي شيء وكل شيء يمس الإنترنت ويمكن الوصول إليه من الخارج. لا تنس الأصول مثل خوادم VPN والمكاتب البعيدة وأجهزة توجيه الحافة وأجهزة الأمان الافتراضية القائمة على السحابة.

الأصول الرقمية الحيوية، أو "سطح الحماية"، هي تلك التطبيقات والخدمات التي من شأنها أن تضر بالعمل بشكل كبير إذا تعرضت للاختراق في خرق للبيانات أو هجوم تخريبي. بالنسبة لهذه الخدمات، أنت بحاجة إلى خريطة كاملة للاتصال وتدفق البيانات. غالبًا ما تكون هذه أسئلة عمل لا تستطيع فِرق الشبكة والأمان الإجابة عليها بأنفسهم.

ثم قم بإجراء الارتباط المتبادل. بالنسبة للأصول الحيوية المحددة، من الخارج إلى الداخل ما هي أجهزة الشبكات المتصلة بها. جدران الحماية، وWAF، والموجهات، والمبدلات، وشبكات VPN (التي قد لا تكون واضحة)... كل ذلك. استخدم هذا المخطط لتحديد الإجراءات التالية:

الحالة	الإجراء المُوصى به
انتهاء عمر الجهاز (EoL)	تحديث الأجهزة: التمزيق والاستبدال
الجهاز في الدعم الموسع	الاستبدال في أقرب وقت ممكن
متأخرة في مستوى التحديث عن المستوى الحالي	التصحيح على الفور
لم يتم نشر الجهاز مع HA (فعلي أو افتراضي)	إضافة زوج HA لدعم التصحيح دون زمن تعطل
لا يدعم الجهاز التحديثات في يوم الإصدار بسبب قيود في العملية أو قيود في الأجهزة/البرامج	أضف إلى برنامج VulnOps لدعم تحديثات يوم الإصدار، أو قم بتحديث الأجهزة لتتوافق مع تصحيحات يوم الإصدار.

وهناك أيضاً بعض الإجراءات التكتيكية التي يجب اتخاذها على جميع هذه الأجهزة. ومرة أخرى، لا نفترض أن هذه الأمور سهلة، لكنها دفاعات قيّمة للغاية تساعد في منع العديد من أساليب الهجوم المستخدمة حاليًا:

- يتطلب الأمر استخدام المصادقة متعددة العوامل (MFA) للإدارة كحد أدنى، ومن الأفضل أن تتم إدارة النظام عبر وسيط إدارة الوصول المتميز (PAM).
- قم بتعطيل واجهات الإدارة المعرضة للإنترنت أو منطقة الشبكة المحايدة (DMZ). تشمل واجهات الإدارة إمكانية الوصول الإداري إلى الأجهزة، ووحدات التحكم في الشبكات المعرفة بالبرمجيات، ومحطات الإدارة الأخرى. يجب عليهم رفض جميع حركات المرور من الشبكات غير الموثوق بها.
- تمكين تصفية الخروج. يساعد ذلك على تقليل عمليات رد الاتصال والتحكم في أوامر المهاجم. تذكر أن هذا يجب أن يشمل التصفية المستندة إلى نظام أسماء النطاقات (DNS) وليس عناوين IP فقط.
- إذا كنت تستخدم أي برامج نصية أو أكواد أتمتة تتعلق بإدارة الشبكة/الأمان، فقم بتقييمها بحثًا عن الأسرار المخزنة، واستخدم أداة إدارة دورة حياة البرمجيات (LLM) لتقييمها بحثًا عن عيوب أمنية.
- قم بوضع جدار حماية تطبيقات الويب (WAF) أمام جميع التطبيقات المتصلة بالإنترنت (الأجهزة، أو الأجهزة الافتراضية، أو الخدمات السحابية).

تركز هذه المرحلة الأولى على تعزيز ما لدينا، وضمان قدرتنا على تحديثه باستمرار في المستقبل. نقوم بإزالة أدوات الشبكة والأمان عالية الخطورة والتي من المرجح أن تتعرض للخطر. لا قيمة للحدود الأمنية إذا أصبحت نقطة دخول للهجوم.

مضاعفة الحماية: حماية شبكات تكنولوجيا التشغيل والشبكات ذات الأهمية العالية

قد يكون من الصعب أو المستحيل تصحيح أنظمة التحكم الصناعية/التكنولوجيا التشغيلية بوتيرة منتظمة، إن أمكن ذلك على الإطلاق. بينما كانت التكنولوجيا التشغيلية تعيش في بيئات معزولة، قمنا على مدى عقود بربطها بشكل متزايد بشبكات تكنولوجيا المعلومات، مما فتح طرقًا من الإنترنت. إنها أهداف رئيسية، وبنية تحتية حيوية، وغير مناسبة للدفاع ضد الوتيرة السريعة للذكاء الاصطناعي في اكتشاف الثغرات الأمنية، وعمليات الاستغلال، والهجمات.

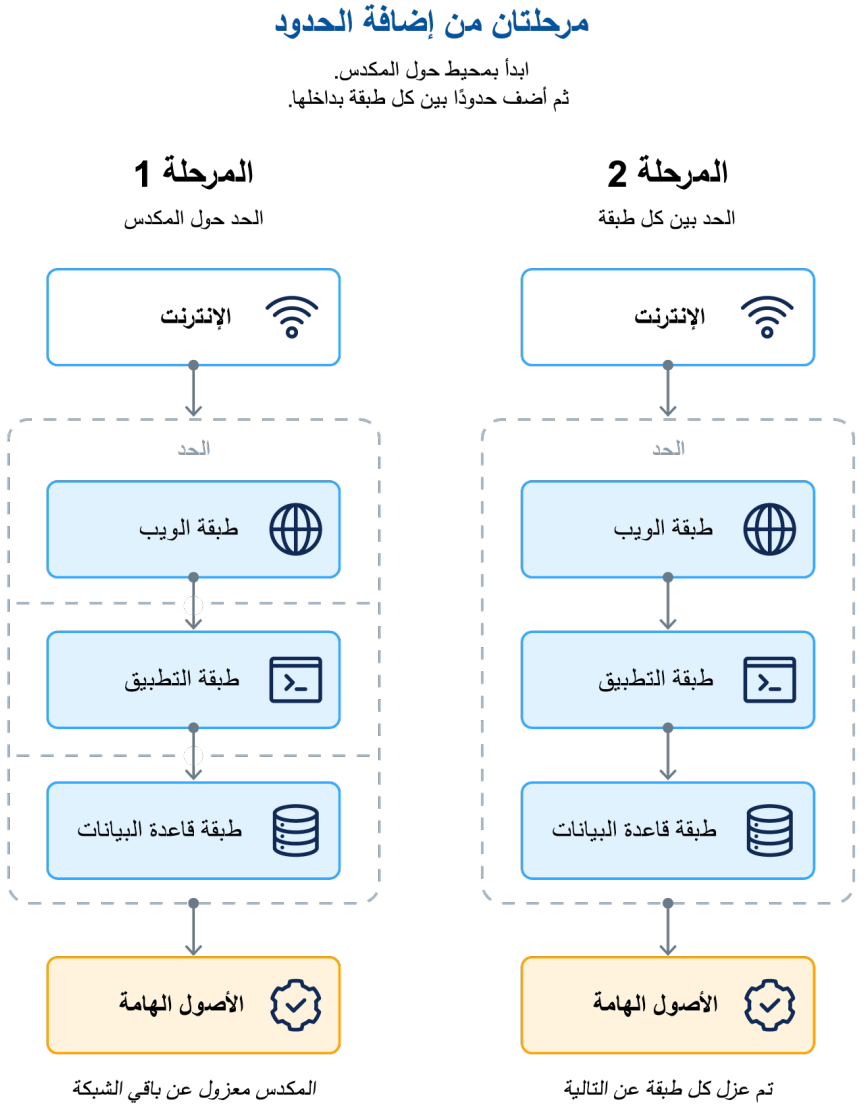
يجب فصل هذه الشبكات عن أي مسار إلى الإنترنت. إذا لم يكن ذلك ممكنًا، ففكر في تقنيات ذات اتجاه واحد لجمع القياس عن بُعد مثل ثنائيات البيانات. إذا لم يكن ذلك ممكنًا ، فاستخدم عدة جدران حماية مضمنة (2 أو أكثر) من الجيل التالي من مورّدين مختلفين يتم تحديثها باستمرار، حتى يحتاج المهاجم إلى عمليات استغلال zero day متعددة من أجل الوصول إلى شبكة التكنولوجيا التشغيلية.

المرحلة 2: إضافة حدود مركزة وذات أولوية

تركز المرحلة 1 على تقوية الأصول المعروفة وإزالة الأجهزة والبرامج القديمة التي لا يمكن تصحيحها، أو التي لا يمكنها مواكبة وتيرة التصحيحات المدعومة بالذكاء الاصطناعي. تبدأ المرحلة 2 بإضافة حدود أمنية لزيادة التعقيد التجميعي للمهاجم وتقليل نصف قطر الانفجار للهجمات الناجحة.

تتمثل الخطوة الأولى أساسًا في التجزئة الكلية: عزل المكدس بحيث لا يصبح التنازل عن الموارد الأقل قيمة والأقل حماية على نفس الشبكة هو الطريق السهل إلى المكدس ذي الأولوية. هناك العديد من تقنيات الشبكات التي يمكنك تطبيقها هنا، بما في ذلك إضافة جدران الحماية، وعزل الشبكة (الشبكات) الفرعية والمسار (المسارات)، والانتقال إلى شبكة افتراضية معزولة، والعزل باستخدام عناصر تحكم SDN، أو الانتقال إلى مبدأ Zero Trust. يُعد العزل من هجمات الشرق والغرب هو الأولوية الأولى، على افتراض أنك قد قويت بالفعل ضد الهجمات من الشمال (الإنترنت) في المرحلة 1.

إذا اخترت العزل باستخدام أدوات داخل المضيف، فيجب أن تعمل هذه الأدوات على مستوى منخفض، ومن الناحية المثالية خارج نظام التشغيل (برنامج مراقبة الأجهزة الظاهرية) أو وكيل محصن تتم إدارته خارجيًا بحيث لا يتمكن المهاجم الذي يصل إلى المضيف من تعطيل أمان الشبكة ببساطة.



الخطوة الثانية، والخطوة التي ستستغرق وقتًا أطول ومن المحتمل أن تتطلب تقنيات جديدة، هي إضافة حدود مضمنة*إضافية*. تركّز خطواتنا السابقة على تقليل المسار السهل، لكن هذه الخطوة تضيف تكاليف إضافية وحقيقية على المهاجم. يجب أن تتحدث كل طبقة من التطبيق فقط إلى الطبقة أعلاها والطبقة أدناها، وفقط على المنافذ والبروتوكولات المتوقعة. SDN هو الخيار الأفضل، وغالبًا ما يكون تنفيذ هذا النمط أسهل بكثير في البيئات السحابية والبيئات الافتراضية بالكامل.

المرحلة 3: التوسيع والتحسين

تركز المرحلتان 1 و2 بشكل كبير على حماية أصولنا الأكثر أهمية بسرعة. نقوم باستبدال الأجهزة والبرامج القديمة، ونحدث كل شيء، ونعزل عن الموارد الأقل حماية، ثم نبدأ في إضافة حدود أمنية لزيادة تكلفة المهاجم وتعقيده. ضع في اعتبارك أن هذا ليس سوى جانب الشبكة وأمان الشبكة من المعادلة؛ وفقًا لإرشاداتنا حول الاستعداد لعاصفة الثغرات الأمنية في الذكاء الاصطناعي، هناك مبادرات موازية أخرى لا تقل أهمية.

تتعلق المرحلة 3 بتوسيع هذه الدفاعات وتحسينها إلى باقي شبكاتنا. من الناحية المثالية، ننتقل من الشبكات المسطحة، إلى التجزئة الكلية، وإلى التجزئة الدقيقة، ثم إلى مبدأ Zero Trust. على الرغم من أن الانتقال مباشرة إلى نموذج Zero Trust هو الأمثل، إلا أنه قد لا يكون قابلاً للتحقيق على المدى القصير. بالنسبة للتجزئة الكلية، نبدأ في عزل وحدات العمل ومناطق الثقة.

تقود التجزئة الدقيقة الحدود إلى أعباء العمل والخدمات الفردية، لذلك كل واحد يتحدث فقط عما يحتاج إليه بالفعل. يمكن أن يكون هذا بطيئًا ومكلفًا على نطاق واسع، وعادة ما يتم تنفيذه على أساس كل مشروع على حدة. يمكن أن يستغرق الأمر سنوات، ويتطلب تدفقًا حقيقيًا وتخطيطًا للتبعية قبل تغيير أي شيء، ويمكن أن يكسر الإنتاج إذا استعجلت.

في CSA، نُعرّف التجزئة الدقيقة على أنها جزء من Zero Trust، ولكن بالنسبة لبعض مسؤولي الشبكات والأمان، فإنهم متمايزون ولكنهم متداخلون إلى حد ما. يمكن تنفيذ التجزئة الدقيقة كشبكة فقط وعزلها على أساس كل أصل وكل تطبيق، مع إضافة Zero Trust للهوية والسياق إلى قرارات الاتصال.

Zero Trust هي المكان الذي يجتمع فيه كل هذا. بمجرد تحديد حدودك بدقة واتباع سياساتك لأعباء العمل والهويات بدلاً من موقع الشبكة، فأنت بذلك تصرح بالوصول لكل اتصال. هذا عائق كبير للمهاجمين كما تم إثباته بالفعل في السحابة. انتبه لنقاط الاختناق أثناء تقدمك: يصبح موفرو الهوية ونقاط التحكم الموحدة الأخرى أهدافًا ذات قيمة عالية تحديدًا لأن كل شيء يثق بهم، لذلك فهم يحظون بمزيد من التدقيق والمزيد من الحدود، وليس أقل.

خلال هذه المرحلة، من المهم للغاية إلقاء نظرة فاحصة على عمليات الإدارة التقنية والواجهات. تتطلب الشبكات تحديثات مستمرة تتجاوز مجرد التصحيح، وتُعد واجهات الإدارة هذه هدفًا ناضجًا.

لا يتم "تنفيذ" أيًا من هذا على الإطلاق، وتلك هي الفكرة. إن الشبكات التي ستصمد أمام الهجمات التي يقودها الذكاء الاصطناعي لن تكون تلك التي أنهت مرحلة ما، بل ستكون تلك التي جعلت التجزئة والتصحيح وقابلية الرؤية مستمرة، بحيث يتم شحن كل تطبيق جديد بحدوده الموجودة بالفعل، وكل استغلال جديد يصطدم بشبكة مصممة لتكلف المهاجم أكثر مما يكلفك. ستستمر الحوادث، كما أن تحسين قياس الشبكة عن بُعد يصقل فِرق الاستجابة للحوادث.

انتقال صعب، مستقبل مشرق

لا توجد أي من التقنيات الواردة في هذه الورقة جديدة، ولكن نطاقها وحجمها وجداولها الزمنية للتنفيذ تختلف عن الطريقة التي كنا نعمل بها. كل شيء تمت مناقشته هو مبدأ أمني أساسي، تم اختبار الكثير منه في بيئات مختلفة. لكننا، كمتخصصين في الشبكات والأمن، يجب علينا دائماً الموازنة بين الاحتكاك والمخاطر. إن إضافة ضوابط أمنية تزيد من التكلفة والتعقيد، ويمكن أن تبطئ أجزاء من العمل. توصياتنا ليست سهلة دائمًا، وبالتأكيد ليست مجانية. نحن ببساطة لا نرى أي بدائل.

يغير الذكاء الاصطناعي افتراضات المخاطر الأساسية التي بنينا ممارساتنا الحالية حولها. فهو يُمكّن نطاقًا أوسع من المهاجمين ذوي المهارات المنخفضة من العمل على مقربة من صائدي الثغرات الأمنية وخبراء اختبار الاختراق من النخبة. لا يمكننا الاعتماد على وجود أسابيع أو أشهر لتصحيح الحافة، وسنوات لتصحيح البنية التحتية الداخلية لدينا. لا يمكننا أن نفترض أن المهاجمين لن يتمكنوا من التنقل في بنياتنا الداخلية المعقدة. لا يمكننا أن نتوقع أن يكون خادم VPN واحد غير محدث يستخدمه فرع واحد فقط آمناً لأن أي مهاجم لن يهتم بذلك.

قد تكون الحسابات الرياضية مواتية للأمن الهجومي اليوم، لكن الطريق لتحقيق التوازن في المعادلة واضح. في نهاية المطاف، ستكون جميع البرامج أكثر أمانًا بطبيعتها قبل إصدارها، حيث سنقوم بدمج قدرات الذكاء الاصطناعي نفسها بشكل كامل في تطوير البرامج وتقييمات الأمان. مع تحديث شبكاتنا والتوجه نحو Zero Trust، فإننا نزيد من عدد الحدود الأمنية التي يحتاج المهاجمون إلى تجاوزها، مما يزيد من تكلفتهم وتعقيدهم التجميعي. عندما نتمكن من إجراء عمليات التصحيح والتحديث بشكل مستمر، فإننا نقلل من الوقت المتاح لهم للعمل.

هذا المزيج هو الذي يغير المعادلة لصالحنا، وحتى التغييرات الصغيرة يمكن أن تجلب فوائد كبيرة. قم بتحديث نموذج التشغيل الخاص بك ليكون أكثر استجابة وقم بدمج VulnOps. ركّز على حماية أصولك الأكثر أهمية أولاً. تأكد من استخدامك للأجهزة والبرامج المحدثة التي يمكن تصحيحها في اليوم الذي يتم فيه إصدار التصحيحات. انقل قدر الإمكان إلى الشبكات المعرفة بالبرمجيات (SDNs)، والتي تشمل معظم الشبكات الافتراضية والسحابية، لأن هذه الشبكات تجعل عملية تقسيم البيانات أسهل بكثير في التنفيذ والصيانة. ابدأ بتقسيم الشبكة من الشرق إلى الغرب لعزل المكدسات الفردية، ولكن اتجه نحو زيادة الحدود المضمنة من الشمال إلى الجنوب، وفي النهاية توجه إلى Zero Trust وSDP.

Zero Trust أو zero days، هو اختيارك.

لن تكون المؤسسات التي تزدهر في عصر الذكاء الاصطناعي هي تلك التي تقضي على كل ثغرة أمنية. بل ستكون التي تقلل باستمرار من التعرضات القابلة للاستغلال بشكل أسرع مما يمكن للمهاجمين الاستفادة منه. العوائق تكسب الوقت وتزيد من تكاليف المهاجم. إن هذا المزيج من تقليل السطح وسرعة رد الفعل والحدود الأمنية هو الذي يخلق مرونة حقيقية.