CISCO
SECURE

دراسة نتائج الأمان

وحدة التخزين 2

تعظيم أفضل خمس ممارسات أمنية

المحتويات

(إعادة) تقديم Fab Five (الممارسات الخمس المذهلة)

سعت دراسة نتائج الأمان من Cisco لعام 2021 إلى قياس الأمور الأكثر أهمية في إدارة الأمن السيبراني. وتحقيقًا لهذه الغاية، قمنا بفحص 25 ممارسة أمان عامة واختبرنا كيفية ارتباط كل منها بتحقيق 11 نتيجة على مستوى البرنامج. يمكنك عرض ارتباطات نتائج الممارسة هذه عبر تصوُّر تفاعلي على موقع دراسة نتائج الأمان من Cisco لعام 2021 على الويب، أو تنزيل التقرير الكامل.

ومن خلال الاختبار، اكتشفنا أن خمس ممارسات من أصل 25 تميّزت عن البقية من حيث المساهمة الإجمالية في نجاح برنامج الأمان عبر جميع النتائج التي تم قياسها.

وفي الصفحات التالية، نركّز على دوافع "الممارسات الخمس المذهلة" لنجاح برنامج الأمان لتحديد الاستراتيجيات لزيادة فعاليتها إلى أقصى حد. "الممارسات الخمس المذهلة" هي:

التحديث الاستباقي للتكنولوجيا	تتمتع المؤسسة باستراتيجية استباقية لتحديث التكنولوجيا للبقاء على اطّلاع دائم بأفضل تقنيات تكنولوجيا المعلومات والأمان المتاحة.
التكنولوجيا ذات التكامل الجيد	تتكامل تقنيات الأمان لدينا بشكل جيد وتعمل معًا بفاعلية.
الاستجابة للحوادث في الوقت المناسب	تتيح إمكانيات الاستجابة للحوادث إمكانية التحقيق في أحداث الأمان ومعالجتها في الوقت المناسب وعلى نحو فعال.
الاكتشاف الدقيق للتهديدات	توفر إمكانيات اكتشاف التهديدات وعيًا دقيقًا بأحداث الأمان المحتملة دون وجود نقاط عمياء هامة.
التعافي الفوري من الكوارث	تقلل إمكانيات التعافي من التأثير وتضمن مرونة وظائف الأعمال التي تتأثر بالحوادث الأمنية.

الفعالية الواسعة لهذه الممارسات تطرح السؤال، "لماذا؟" ما الذي يجعلها أساسية للغاية لتحقيق النجاح؟ ما هي العوامل التي تجعلها أكثر أو أقل فعالية؟ كيف يجب على الشركات تنفيذ هذه الممارسات لتعظيم النتائج؟ هذه هي أنواع الأسئلة التي نريد استكشافها في هذا التكرار لدراسة النتائج الأمنية.

وفي الصفحات التالية، نركّز على دوافع "الممارسات الخمس المذهلة" لنجاح برنامج الأمان لتحديد الاستراتيجيات لزيادة فعاليتها إلى أقصى حد. نقوم بذلك من خلال دراسة استقصائية مزدوجة التعمية يتم إجراؤها بشكل مستقل لأكثر من 5,100 متخصص في تكنولوجيا المعلومات والأمان حول العالم. نحن نتعمّق في البيانات، ونستخرج النتائج البارزة، ونشارك النقاط الهامة التي تم فحصها للمساعدة في فتح آفاق جديدة من الإنجازات الأمنية لمؤسستك.

الاكتشافات الرئيسية

لقد سألنا أكثر من 5,100 متخصص في تكنولوجيا المعلومات والأمان في 27 بلدًا عن أساليب مؤسساتهم لتحديث البنية التقنية للأمان ودمجها، واكتشاف التهديدات والاستجابة لها، والاحتفاظ بالمرونة عند وقوع الكوارث. كما قد تتخيل، فقد شاركوا مجموعة واسعة من الرؤى والنضالات والاستراتيجيات والنجاحات. لقد حللنا كل استجابة بطرق متعددة، واستخلصنا النتائج الرئيسية مثل تلك الموضّحة أدناه.

تحديث البنية التقنية ودمجها

- تساهم تكنولوجيا المعلومات الحديثة والمتكاملة بشكل جيد في نجاح البرنامج بشكل عام أكثر من أي ممارسة أو تحكم أمني آخر.
- من السهل للغاية تحديث البنى التقنية الأحدث المستندة إلى السحابة بانتظام لمواكبة الأعمال.
- المؤسسات التي تأتي مصدرها بشكل أساسي من مورّد واحد تضاعف فرصها في إنشاء حزمة تقنية متكاملة.
- من المرجح أن تحقق تقنيات الأمان المتكاملة سبع مرات مستويات عالية من أتمتة العمليات.

اكتشاف التهديدات السيبرانية والاستجابة لها

- تشهد برامج SecOps المستندة إلى الأشخاص والعمليات والتكنولوجيا الأقوياء زيادة في الأداء بمقدار 3.5 مرة مقارنةً بتلك التي لديها موارد أضعف.
- يُنظر إلى فِرق الاكتشاف والاستجابة الخارجية على أنها متفوقة، لكن الفِرق الداخلية تُظهر متوسط وقت استجابة أسرع (6 أيام مقابل 13 يومًا).
- تزداد احتمالية الإبلاغ عن قدرات الاكتشاف والاستجابة القوية للفِرق التي تستخدم معلومات التهديدات بشكل مكثف بمقدار الضعف.
- تعمل الأتمتة على مضاعفة أداء الأشخاص الأقل خبرة، وتجعل الفِرق القوية شبه مؤكدة بنسبة (95%) لتحقيق نجاح SecOps.

كن مرنًا عند وقوع كارثة

- إن المؤسسات التي تخضع للإشراف على مستوى مجلس الإدارة لاستمرارية الأعمال والتعافي من الكوارث هي الأكثر احتمالاً (11% فوق المتوسط) للإبلاغ عن امتلاكها لبرامج قوية.
- لا تتحسن احتمالية الحفاظ على مرونة الأعمال حتى تغطي استمرارية الأعمال وقدرات التعافي من الكوارث ما لا يقل عن 80% من الأنظمة الهامة.
- إن المؤسسات التي تختبر بانتظام قدراتها على استمرارية الأعمال والتعافي من الكوارث بطرق متعددة تزداد احتمالية حفاظها على مرونة الأعمال بمقدار 2.5 مرة.
- تزداد احتمالية تحقيق المؤسسات التي تضع الممارسة القياسية لهندسة الفوضى لمستويات عالية من المرونة بمقدار الضعف.

نبذة عن الاستطلاع

أخذ العينات	المشاركون	التحليل
تعاقدت Cisco مع شركة أبحاث استقصائية، تُدعى YouGov، لإجراء دراسة استقصائية مجهولة الهوية بالكامل في منتصف عام 2021 استخدمت أسلوب أخذ العينات العشوائية الطبقية.	استجاب 5123 من المتخصصين النشيطين في مجال تكنولوجيا المعلومات والأمان والخصوصية من 27 دولة. يمكن العثور على الخصائص السكانية للعينة في الملحق.	وأجرى معهد Cyentia Institute تحليلاً مستقلاً لبيانات الاستطلاع نيابةً عن Cisco وأنشأ كل النتائج المعروضة في هذه الدراسة.

5.123 من المتخصصين النشطين في مجالات تكنولوجيا المعلومات والأمان والخصوصية من **27** بلدًا شاركوا في الاستقصاء

"يتعين علينا أن نعلم أننا نفعل كل ما في وسعنا للحفاظ على أمان كل شيء. فنحن نعلم مدى تقدم المهاجمين، وهم يزدادون تقدمًا ولديهم تقنيات جديدة كل يوم. ونريد أن نحافظ على أمان أجهزتنا ومستخدمينا وشركتنا، لذلك نريد تضييق سطح الهجوم لأي انتهاكات أمنية محتملة".

إريك ج. ماندیلا، مساعد المدير،
البنية التحتية للتكنولوجيا، Allied Beverage Group

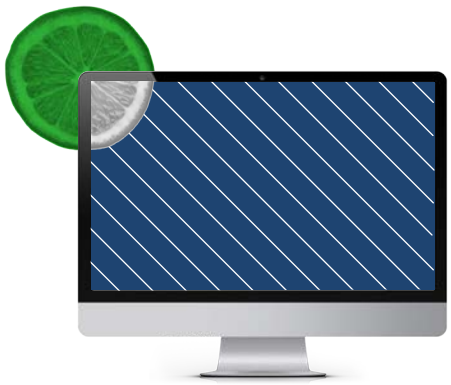
قراءة المزيد

استراتيجيات للتحديث الاستباقي للتكنولوجيا

وجدت دراستنا السابقة أن أحد النُهج الاستباقية لتحديث أفضل تقنيات تكنولوجيا المعلومات والأمان والحفاظ عليها ساهم في نجاح برنامج الأمن السيبراني أكثر من أي ممارسة أخرى. وهذا ليس بالأمر الهين بالنظر إلى جميع الممارسات التي اختبرناها البالغ عددها 25 والتي تُعد على نطاق واسع "أفضل الممارسات" في حد ذاتها. لذا، فقد حرصنا على التعمُّق في ما يجعل هذه الممارسة فعّالة للغاية في دراسة المتابعة هذه.

بما أننا نبدأ في التعمُّق أكثر في استراتيجيات تحديث التكنولوجيا، فلنقم باختبار مراقبة سريع لحداثة البنية التحتية الحالية. لقد سألنا المشاركين في الاستقصاء عن نسبة تقنيات الأمان النشطة القديمة لديهم. في المتوسط، تُعد 39% من تقنيات الأمان التي تستخدمها المؤسسات قديمة. يزعم ما يقرب من 13% من المستجيبين أن ما لا يقل عن 8 من أصل 10 أدوات أمان يستخدمونها تُظهر أعمارهم.

قد تساعد هذه الحقيقة وحدها في شرح الكثير من الفوائد التي نراها من استراتيجية التحديث الاستباقي للتكنولوجيا. ظاهريًا، توفر التقنيات الحديثة قدرات متقدمة لمواجهة حشد دائم التطور من التهديدات السيبرانية. ولكن هناك ما هو أكثر من ذلك، لذلك دعونا نستمر في البحث في الأسئلة التي طرحناها عن البيانات.



في المتوسط، تُعد 39% من تقنيات الأمان التي تستخدمها المؤسسات قديمة.

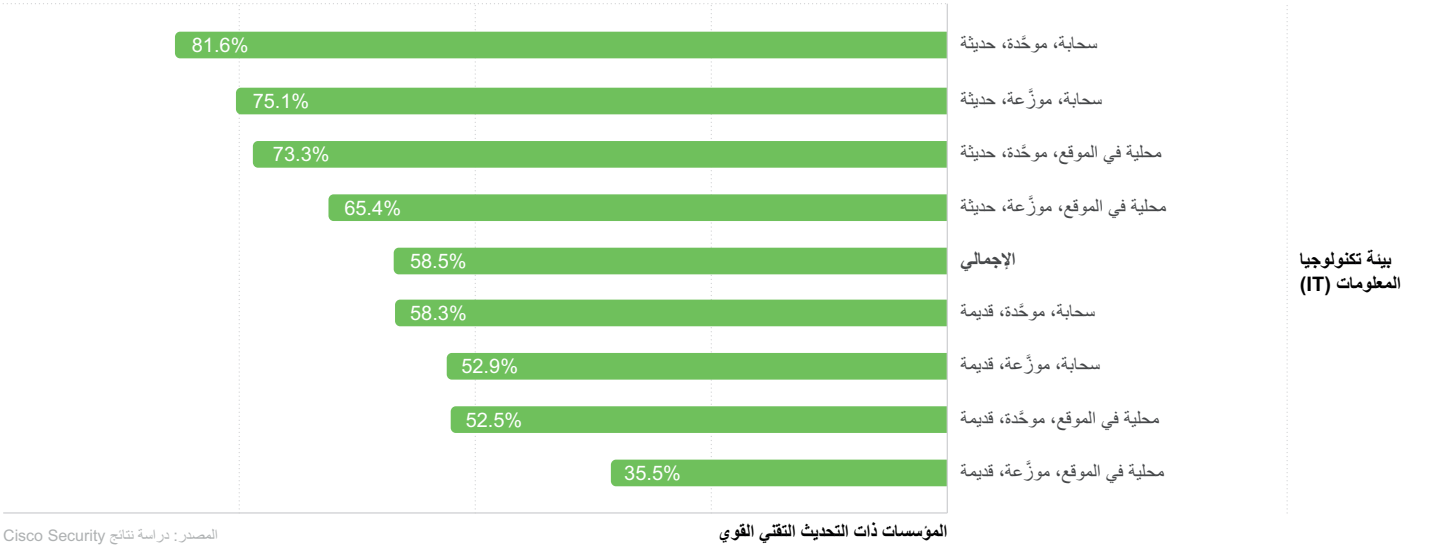
هل سمات البنية التحتية تؤثر على مبادرات التحديث؟

في الدراسة الأصلية، توقعنا أن البُنى التقنية الأكثر حداثة والقائمة على السحابة قد تكون أكثر فاعلية لأنها أسهل في الإدارة ولديها إجراءات أمان مدمجة. وكخطوة نحو اختبار هذه الفرضية، طلبنا من المشاركين وصف البنية التحتية لتقنيتهم بشكل عام باختيار مجموعة من الواصفات المتدرجة، بما في ذلك:

- السحابة مقابل الموقع المحلي
- الحديثة مقابل القديمة
- الموحّدة مقابل الموزّعة

هل تساهم سمات البُنى التقنية المختلفة هذه في فعالية إمكانيات التحديث التقني؟ إلى حد كبير، وفقًا للشكل 1. **تزداد احتمالية قيام المؤسسات ذات البُنى التقنية الحديثة والموحّدة والقائمة على السحابة للضعف بالإبلاغ عن إمكانات تحديث تقنية قوية أكثر من تلك التي تستخدم تقنيات قديمة وموزّعة ومحلية.** قبل التلويح بهذا المخطط في الاجتماع التالي لاستراتيجية الترحيل إلى السحابة، لاحظ أن المؤسسات ذات البيئات الداخلية في الغالب ما تزال تعمل بشكل أفضل، شريطة أن تكون قد قامت بتحديث تقنية المعلومات.

من المؤكد أن كونك متوافقًا مع السحابة يجعل من السهل فك قيود استراتيجية التحديث التقني الخاصة بك، ولكن كونك قديمًا فهذه في المشكلة الأكثر إلحاحًا هنا. عندما يصبح الحفاظ على تحديث البنية التقنية القديمة معركة شاقة، فقد تحرز تقدمًا أكبر في الانتقال إلى بنية تقنية جديدة بدلاً من الاستمرار في تعديل البنية التقنية القديمة. ذلك ليس دائمًا ممكنًا أو فعّالاً من حيث التكلفة مع البنية التقنية القديمة أو المهمة، بالطبع، ولكن المبدأ العام ما يزال ساريًا.



المصدر: دراسة نتائج Cisco Security

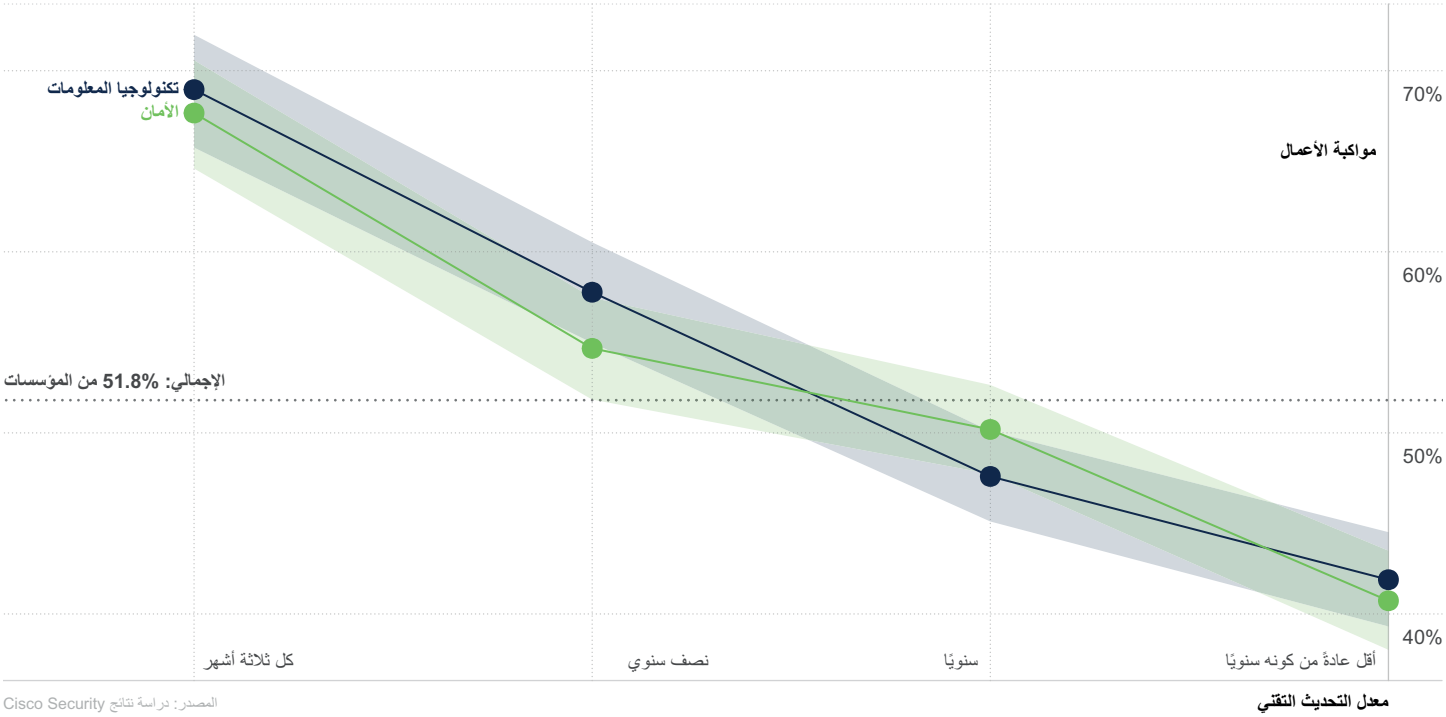
الشكل 1: تأثير سمات بنية تقنية المعلومات على أداء التحديث التقني

81.6%

من المؤسسات ذات البنى التقنية الحديثة والموحدة والقائمة على السحابة تعلن عن إمكانيات قوية لتحديث التقنية

هل الترقيات المتكررة تساعد في مواكبة الأمان للأعمال؟

بحسب دراسة النتائج الأمنية لعام 2021، كانت النتيجة الأكثر ارتباطًا باستراتيجية التحديث الاستباقي للتكنولوجيا هي تمكين برنامج الأمان من مواكبة متطلبات الأعمال ونموها. في الواقع، كانت هذه أقوى مجموعة من الممارسات والنتائج عبر الدراسة بأكملها.



المصدر: دراسة نتائج Cisco Security

الشكل 2: تأثير تكرار التحديث التقني على قدرة برنامج الأمان على مواكبة الأعمال[1]

لقد سألنا المؤسسات عن معدل تكرار ترقيات تكنولوجيا المعلومات والأمان الخاصة بها، وقارننا هذه الإجابات بالقدرة المعلنة لبرنامج الأمان على مواكبة الأعمال. هل هناك علاقة بين هذين المتغيرين؟ نعم بالفعل؛ لقد وجدنا تحسنًا مطردًا في هذه النتيجة الرئيسية مع زيادة إيقاع الترقيات. **بشكل عام، من المرجح أن تتفوق المؤسسات التي تقوم بترقية تكنولوجيا المعلومات وتقنيات الأمان كل ثلاثة أشهر بنسبة 30% في مواكبة الأعمال أكثر من تلك التي تقوم بالترقية كل بضع سنوات فقط.** يبدو وكأنه ملصق تحفيزي جيد لفِرق تكنولوجيا المعلومات المرهقة: ابق على اطّلاع واستمر.

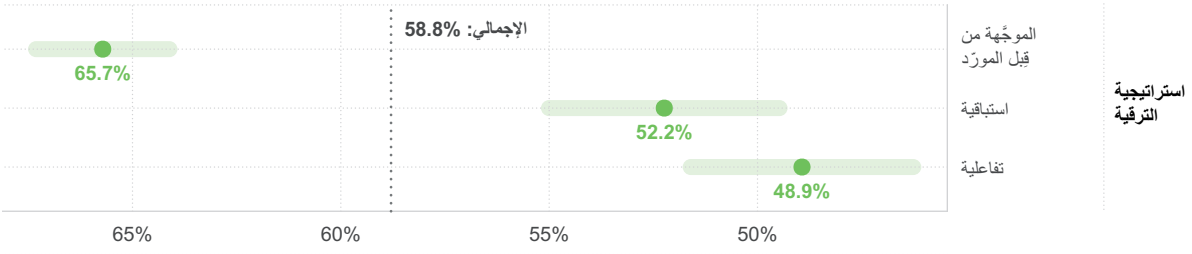
[1] طوال التقرير، سنقوم بتسمية الأرقام بالقيمة "الإجمالية" لممارسة أو نتيجة معينة. تمثل هذه القيمة متوسط القيمة بين جميع المشاركين في الاستطلاع الذين أجابوا على تلك المجموعة المحددة من الأسئلة. يتم توفيرها كمرجع، ويجب أن ترشدك إلى فهم من يقوم بعمل أفضل من المتوسط، ومن التي لا ترقى إلى ذلك. كما أننا نعرض عدم اليقين من خلال أشرطة الخطأ أو المناطق المظللة في بعض المخططات. عندما تتداخل هذه المجالات مع سطر "الإجمالي"، فهذا يعني أنه لا يمكننا الاستدلال على أن هذا الجانب المعين من برنامج الأمان له أي تأثير على النتيجة أو الممارسة التي نقوم بفحصها.

ما (أو مَن) الذي يجب أن يدفع جهود التحديث التقني؟

لقد أثبتنا أن الترقيات المتكررة تساهم في تمكين الأعمال، ولكن ما الذي - أو مَن الذي - يجب أن يدفع عملية إنجاز تلك الترقيات؟ لقد طلبنا من المستجيبين تحديد الدوافع الأساسية لمؤسستهم لتحديث تقنيات الأمان، وانقسمت إجاباتهم إلى ثلاث فئات عامة:

- **المستند إلى المورّد:** يتم تحديد الجدول الزمني بواسطة مزوّد SaaS أو يكون جزءًا من مبادرة أكبر لدمج المورّدين (برنامج التشغيل الأكثر شيوعًا)
- **الاستباقي:** وفقًا لجدول زمني محدد مسبقًا أو عندما تتطلب ميزات جديدة أو حالات استخدام ترقية (ثاني أكثر الحالات شيوعًا)
- **التفاعلي:** استجابةً لحادثة ما، عندما تصبح التقنية قديمة، أو لتلبية متطلبات الامتثال (الأقل شيوعًا)

تُعد برامج التشغيل هذه مثيرة للاهتمام بحد ذاتها، ولكن ما نريد معرفته حقًا هو ما إذا كانت هذه الدوافع مرتبطة بنهج أقوى لتحديث التقنية. توجد الإجابة في الشكل 3، والذي يشير بشكل أساسي إلى أن مبادرات التحديث التقني تكون أكثر نجاحًا عندما يتعامل معها المورّدون (أو على الأقل يشاركون بنشاط في تحقيقها). **أبلغ أقل من نصف هؤلاء الذين لديهم نهج تفاعلي عن إمكانات تحديث قوية، مقارنةً بما يقرب من ثلثي مَن تتم مزامنتها مع دورات تحديث المورّد.**



المصدر: دراسة نتائج Cisco Security

الشكل 3: تأثير برامج التشغيل الأساسية للترقيات على أداء تحديث تقنية الأمان

لقد أدركنا الأمر — كل هذا يبدو مشكوكًا فيه حقًا أنه قادم من مورّد منتجات الأمان وتقنية المعلومات. لكننا بصراحة لم يكن لدينا أي تأثير على هذه النتيجة. تم إجراء الاستطلاع من قِبل شركة أبحاث مستقلة وذات سمعة طيبة، ولم يكن لدى المشاركين أي فكرة عن رعاية Cisco للاستطلاع، وحلّل معهد Cyentia الذي يحظى باحترام كبير البيانات لاستنباط ما تراه في الشكل 3. وللحصول على إجراء جيد، سنكون أكثر حذرًا في تفسير هذه النتائج.

ونعتقد أن الكثير من التحسينات التي تُعزى إلى العلاقات التي يحركها المورّدون إلى البُنى السحابية/بُنى SaaS تكون أكثر ملاءمة للترقيات المتكررة. كما سنلاحظ أن هذا قد يتعلق بدرجة أقل بكون المورّدين رائعين وأكثر حول الهروب من العقبات الداخلية والمستنقعات السياسية التي تميل إلى إعاقة جداول التحديث التقني.

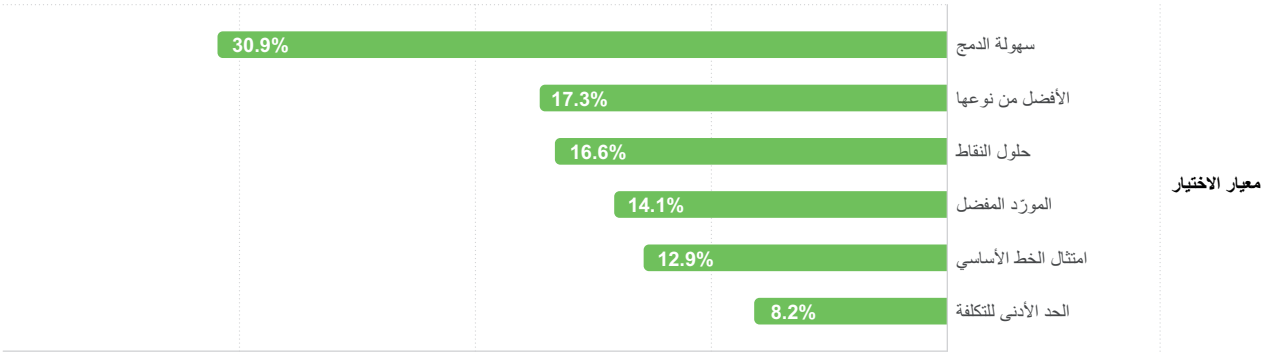
على حد تعبير Rob Base و DJ EZ Rock، "يتطلب الأمر خيارين لجعل الأمور تسير بشكل صحيح. يتطلب الأمر خيارين لجعله بعيدًا عن الأنظار." مَن كان يعلم أنهم مهندسو أمان! اجعل استراتيجية التحديث الخاصة بك بعيدة المنال من خلال تسخير القصور الذاتي لشركاء حلول التكنولوجيا لديك لدفع نتائج المهمة.

65.7%

من المؤسسات التي تُجري مزامنة مع دورات تحديث المورّدين عن إمكانات تحديث تقنية قوية

هل تريد الترقية من أجل القدرة أو التوافق؟

غطى القسم السابق السيناريوهات التي تحث المؤسسات على ترقية التقنيات، والآن سننظر في سبب اختيارهم لحل على آخر. ينقل الشكل 4 ما أخبرنا به المستجيبون حول معايير الاختيار الخاصة بهم. يُعد الدمج الجيد مع التقنية الحالية هو التفضيل الواضح، يليه الحلول التي تقدّم أفضل الإمكانيات أو التي تلبي احتياجات معينة. ربما يكون من المدهش أن يقع تصنيف تقليل التكاليف في المرتبة الأخيرة.



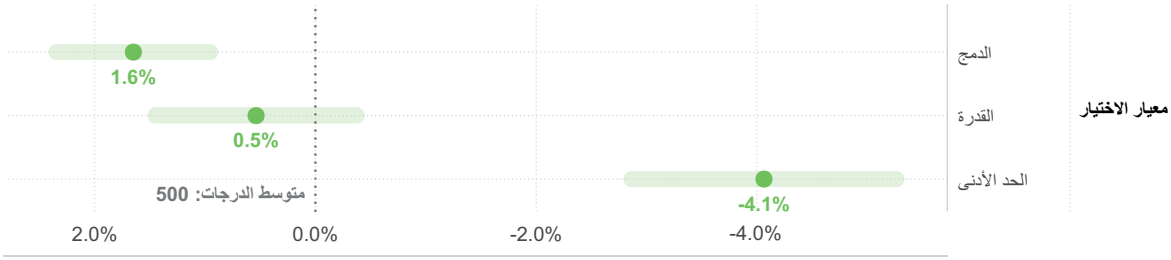
المصدر: دراسة نتائج Cisco Security

الشكل 4: معايير الاختيار الأساسية عند تحديث منتجات الأمان

كل هذا رائع وجيد، لكن هل أي من هذا مهم على الإطلاق فيما يتعلق ببناء برنامج أمان ناجح؟ للإجابة على ذلك، قمنا بتجميع معايير الاختيار من الشكل 4 في ثلاث فئات:

- **الحد الأدنى:** حل أدنى تكلفة؛ الامتثال للخط الأساسي
- **سهولة الدمج:** الدمج مع التقنية الحالية؛ استخدام المورّدين المفضلين
- **القدرة:** الأفضل في الفئات؛ حلول النقاط

ثم قمنا باختبار هذه الفئات مقابل النتيجة الإجمالية التي تم إنشاؤها لكل مؤسسة بناءً على مستوى إنجازها عبر 11 نتيجة أمان. ليس للقيمة المطلقة للدرجة معنى معين، ولكنها توفر نقطة مقارنة لاستراتيجيات التحديث التقني المختلفة. **كما هو موضّح في الشكل 5، يؤدي تحديد أولويات التكامل والقدرات إلى تحقيق النتائج أكثر من اختيار المنتجات استنادًا إلى تقليل التكلفة أو تلبية متطلبات الامتثال الأساسية. ولكن النهج المستند إلى الدمج هو النهج الوحيد الذي يتفوق بشكل كبير على المتوسط.**



المصدر: دراسة نتائج Cisco Security

الشكل 5: تأثير معيار تحديد التقنية على درجة نتائج الأمان الإجمالية

لاحظ أن الاختلافات الوادرة هنا صغيرة للغاية فيما يتعلق بالنجاح الإجمالي للبرنامج. ومن المحتمل أن ما نراه هنا حقًا هو نافذة تطل على الأولويات والممارسات الأوسع نطاقًا لبرنامج الأمان. ولكن يقترح ذلك أن المشكلات الأبسط مثل سبب اختيارنا لمنتج على آخر تستحق دراستها. وإذا كنتَ تكافح لتصنيف الميزات عند تحديث حلول الأمان أو ترقيتها، ففكّر في ذلك كتبرير منطقي لدفع التوافق والسعة فوق تقليل التكلفة.

ما هي درجة نتائج الأمان؟

لقد سألنا المشاركين عن مستوى نجاح مؤسستهم عبر 12 نتيجة مختلفة من نتائج برنامج الأمان. عملت النسخة الأولى من دراسة نتائج الأمان على تحليل هذه النتائج بالتفصيل، وسترى بعضًا منها يتم فحصه بشكل فردي في هذه الدراسة، أيضًا. ولكننا أردنا أيضًا إنشاء درجة مجمّعة توضّح مستوى إنجاز كل مؤسسة عبر كل 12 نتيجة كمقياس لكيفية أداء برنامج الأمان بشكل عام. ونشير إلى ذلك على أنه "درجة نتائج الأمان"، وسترى أنه تمت الإشارة إليها عدة مرات في هذا التقرير.

للحصول على الدرجة، استخدمنا تقنية إحصائية خيالية تُسمى "نظرية الاستجابة للعناصر". تُمكّننا هذه التقنية من تصنيف المؤسسات بناءً على كيفية أدائها عبر كل النتائج، مع مراعاة حقيقة أن بعض النتائج قد يكون تحقيقها أصعب من غيرها في الوقت نفسه. تتمثل هذه التقنية المجرّبة والصحيحة في كيفية إنشاء درجات الاختبارات الموحّدة. ليس للقيمة المطلقة للدرجة معنى معين، ولكنها توفر نقطة مقارنة بين البرامج.

"يجب أن يكون كبار موظفي أمن المعلومات (CISOs) مؤثرين ومعلمين على حد سواء. إذا أردنا أن نكون فعالين قدر الإمكان، فنحن بحاجة إلى أن نكون في طليعة قرارات الاستراتيجية التي يتم اتخاذها في مؤسساتنا. لكن بينما نحاول إقناع الناس بأن الأمن مهم، وأننا بحاجة إلى الاستثمارات المناسبة للقيام بذلك بشكل جيد، وأنه يجب علينا المشاركة في كل جانب من جوانب العمل، يجب علينا في الوقت نفسه القيام بعملية التعليم. لا يتمتع معظم المدراء التنفيذيين بخلفية أمنية، لذلك يتعين علينا إعلامهم بكل خطوة على الطريق حول أنواع المخاطر التي نقدمها مع كل قرار نتخذه."

هيلين باتون، كبير مسؤولي أمن المعلومات (CISO) استشاري، Cisco @CisoHelen

استمع إلى دور هيلين في الدور المتطور لكبير مسؤولي أمن المعلومات (CISO) في هذه الحلقة المثيرة للاهتمام من بودكاست "قصص الأمان" على موقعنا

تحقيق تقنيات أمان متكاملة جيدًا

بحسب دراسة نتائج الأمان الأخيرة لدينا، تساهم تقنيات الأمان المتكاملة جيدًا التي تعمل بشكل فعّال مع بنية تقنية أوسع لتكنولوجيا المعلومات في احتمالية نجاح كل نتائج البرنامج. وطرحنا مجموعة من الأسئلة المُصممة للتعمُّق في العوامل الكامنة وراء هذا العمل الجدير بالثناء، بدءًا من النوايا الكامنة وراء عمليات دمج تقنية الأمان.

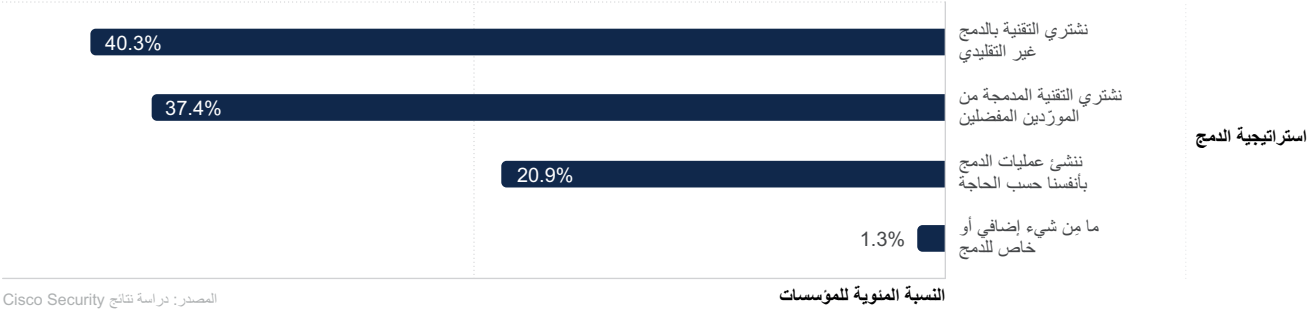
ووفقًا للمشاركين، يتمثل الدافع الأكثر شيوعًا لدمج تقنيات الأمان في تحسين كفاءة المراقبة والتدقيق. كما يتردد صداه معنا، حيث نعرف الألم والإحباط الناتج عن الاضطرار إلى التحقق من العديد من وحدات التحكم أو لوحات المعلومات لتجميع بعض مظاهر ما يحدث عبر الشبكة. كما كانت الأتمتة والتعاون أسهل من المحفزات الشائعة لدمج تقنيات الأمان (المزيد حول الأخير سيأتي قريبًا). لقد اختبرنا هذه الدوافع مقابل مستويات الدمج التقني ونتائج البرنامج التي تم الإعلان عنها، ولكن لم يكن الارتباط قويًا. ربما يكون السؤال عن "الماهية" أو "الكيفية" أكثر أهمية من السؤال عن "السبب" عند دمج تقنيات الأمان؟ لنتعمّق في هذا الموضوع أكثر قليلاً في الأسئلة التالية.

ووفقًا للمشاركين، يتمثل الدافع الأكثر شيوعًا لدمج تقنيات الأمان في تحسين كفاءة المراقبة والتدقيق.

هل تريد الشراء أو البناء للحصول على تقنية مدمجة جيدًا؟

نحن نعرف من الدراسة السابقة أن دمج تقنيات الأمان يحفز النتائج، ولكن ما هي أفضل طريقة لتحقيق حِزمة تقنية متكاملة للغاية؟ هل تريد شراءها بتلك الطريقة؟ هل تريد البناء للملاءمة؟ هل تريد فقط تركها كما هي؟ دعونا نرى ما إذا كان يمكننا معرفة ذلك.

لقد سألنا المؤسسات عن نهجها المعتاد لتكامل تقنية الأمان، ويرصد الشكل 6 الإجابات. **وبشكل عام، ستفضل أكثر من ثلاثة أرباع المؤسسات شراء حلول مدمجة بدلاً من إنشائها.** ومن بين هذه المؤسسات، تختار أكثر من 40% التقنيات التي تأتي بعمليات دمج غير تقليدية في بنيتها التقنية الموجودة. ويأخذ أكثر من 37% منها هذه الخطوة إلى الأمام وتفضل الحصول على حلول من مورّد واحد حتى تكون مدمجة جيدًا في الأصل أو جزءًا من نظام أساسي أكبر. ويرغب ما يزيد قليلاً عن 20% منها في بناء عمليات الدمج بأنفسهم، شريطة أن يناسب المنتج احتياجاتهم. ويتبع البعض منها نهج عدم التدخل.



المصدر: دراسة نتائج Cisco Security

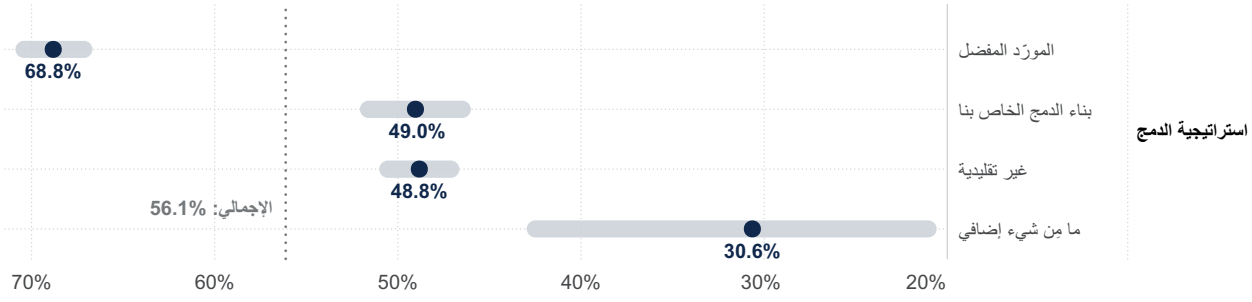
الشكل 6: النُهج الشائعة لدمج تقنية الأمان بين جميع المؤسسات

بوجه عام، أكثر من 3/4 المؤسسات تفضل شراء حلول متكاملة بدلًا من تطويرها

يقيّم الشكل 7 ما إذا كان أي من نُهج الدمج هذه يحدث فرقًا أم لا. ونحن نرى هنا موضوعًا يشير مجددًا إلى الفوائد من التعاون مع المورّدين للحفاظ على التقنية الحديثة والمدمجة جيدًا. **وكما هو موضّح في المخطط، من المحتمل أن يزيد التمسك بمورّد مفضل من تحقيق تقنيات أمان مدمجة جيدًا بمقدار أكثر من الضعف مقارنةً بنهج عدم التدخل (حوالي 69% مقابل حوالي 31%).** وبالإضافة إلى ذلك، ووفقًا لبحثنا، تظل هذه النتيجة متسقة عبر جميع أحجام المؤسسات، على الرغم من أن فوائد استخدام مورّد مفضل أعلى إلى حدٍ ما بالنسبة للشركات الصغيرة والمتوسطة الحجم مقابل المؤسسات الكبيرة.

ونعم، نحن ندرك أن هناك نتيجة أخرى ملائمة بصورة مريبة تأتي من شركة بمحفظة أمان مدمجة وشاملة. وبالتأكيد، يسعدنا أن نرى أنّ هذه النتيجة تدعم استراتيجية Cisco... ولكن تذكّر أن هذه كانت دراسة مزدوجة التعمية ونحن لم نتلاعب بهذه النتيجة على الإطلاق.

وليس من المستغرب ذلك، لقد أصبحت المؤسسات التي لم تقم بأي شيء إضافي لدمج تقنيات الأمان نبوءة ذاتية التحقق. **ومع ذلك، نحن نتوقع أن البعض سيتفاجأ بمعرفة أنه لا يوجد أي فرق بشكل ظاهري بين تلك المؤسسات التي تشتري المنتجات بعمليات الدمج غير التقليدية وتلك المؤسسات التي تبني عمليات الدمج من تلقاء نفسها.** تبلغ أقل بقليل من نصف (~ 49%) المؤسسات التي تستخدم كل من هذه الأساليب عن مستويات تكامل قوية.



المصدر: دراسة نتائج Cisco Security

الشكل 7: تأثير نُهج الدمج الشائعة على مستوى دمج تقنية الأمان

سحابي، مع فرصة للدمج

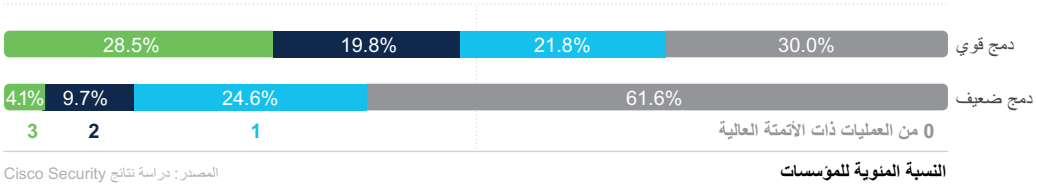
لقد سمعنا من الكثير من المؤسسات التي تكافح بشأن قرار بدء (أو توسيع) جهود دمج تقنية الأمان الخاصة بها في بيئات السحابة أو في البيئات المحلية. إذا كان هذا يمثلك، فلدينا بعض البيانات التي قد تساعد في ذلك التقييم. ويتمثل الخبر السار في أن الكثير من المشاركين في الاستطلاع أبلغوا عن نتائج جيدة في كل من البيئات المحلية وبيئات السحابة. ومع ذلك، يبدو أنه من الأسهل بشكل كبير تحقيق دمج تقني قوي في السحابة.

المصدر: دراسة نتائج Cisco Security

الشكل 8: تأثير بيئات السحابة مقابل البيئات المحلية على مستوى دمج تقنية الأمان

هل يساعد الدمج الأتمتة؟

بالرجوع إلى بداية هذا القسم، الأتمتة ليست هي الدافع الأكثر شيوعًا للدمج التقني. ولكن 44% من المؤسسات تصفها بأنها بمثابة حافز. وبجانب الدوافع، هل هناك دليل على أن التقنيات المدمجة جيدًا تتيح بالفعل أتمتة أفضل لعمليات الأمان؟ تشير الأدلة المقدمة في الشكل 9 إلى أن الأمر على هذه الحالة بالفعل.



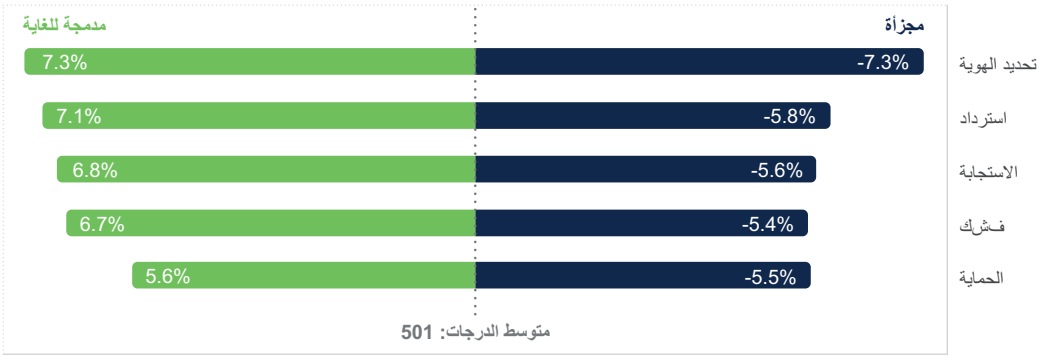
الشكل 9: تأثير الدمج التقني على مدى أتمتة عملية الأمان

يميّز الشريطان الأفقيان في الشكل 9 المؤسسات بناءً على مستوى دمج تقنية الأمان الخاص بها (القوي مقابل الضعيف). تُمثل المقاطع الملونة عدد عمليات الأمان الرئيسية (مراقبة الأحداث، وتحليل الحوادث، والاستجابة للحوادث) المدعومة بأتمتة ناضجة. نسبة المؤسسات التي ليس لديها أتمتة أعلى من ضعف تلك التي لديها تكامل ضعيف. **وعلى العكس من ذلك، فإن أولئك الذين لديهم تقنيات أمان متكاملة كانوا أكثر عُرضة بمقدار سبع مرات تقريبًا لتحقيق مستويات عالية من الأتمتة لجميع هذه العمليات الثلاث (4.1% مقابل 28.5%).** هذا يبدو وكأنه دافع مقنع بالفعل!

ما هي الوظائف التي يجب توفير التكامل لها؟

بعد ذلك، سألنا المشاركين عن مستوى تكاملهم بين التقنيات التي تدعم الوظائف الأساسية الخمس لإطار عمل الأمن السيبراني NIST (CSF). لقد أجابوا على نطاق يتراوح بين التقنيات شديدة التجزئة (التقنيات المنعزلة التي تعمل في الغالب في عزلة) إلى التقنيات المتكاملة للغاية (التقنيات المنسّقة التي تعمل كوحدة وظيفية). ثم أنشأنا نموذجًا لتحديد التأثير على النتيجة الإجمالية للأمان لكل مؤسسة.

النتائج في الشكل 10 متسقة بوضوح عبر الوظائف الخمس. **العمل على إلغاء التجزئة ودمج أي من مجالات NIST CSF الوظيفية يتوافق مع زيادة في نجاح برنامج الأمان (أكثر من 11% وحتى 15% تقريبًا).** وبالتالي، فإن الإجابة على سؤالنا الاعتباري هي "جميعها". لكن وظيفة "تحديد الهوية" المتكاملة بدرجة عالية توفر أكبر دفعة إذا كنت تتساءل من أين تبدأ.



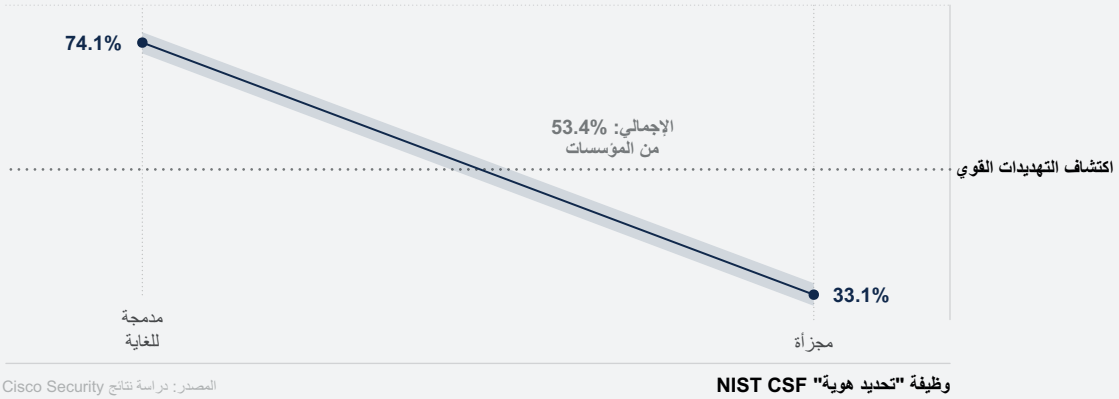
الشكل 10: تأثير تكامل وظائف NIST CSF على الرصيد الإجمالي لنتائج الأمان

لا يسعنا إلا أن نرى صلة بين هذه الحقيقة وما تعلمناه في القسم السابق حول المراقبة والتدقيق والتعاون كونها الدوافع الأقوى لدمج التكنولوجيا. وتبدو هذه الأشياء، معًا، تدافع عن الأهمية الأساسية لإمكانية الرؤية الجيدة عبر المؤسسة. من المنطقي بالتأكيد أن النهج المجزأ بغرض "وضع فهم تنظيمي لإدارة خطر الأمن السيبراني على الأنظمة والأشخاص والأصول والبيانات والإمكانات" (لغة CSF) لن ينتهي بشكل جيد. سترى أن هذا الموضوع معزز بشكل أكبر عندما ننتقل إلى قسم "اكتشاف التهديدات والاستجابة للحوادث".

عند التكامل، وتحديد الهوية، والمعلومات

خارج الرسم البياني الذي ناقشناه للتو، تشير البيانات في جميع أنحاء هذه الدراسة باستمرار إلى العلاقة الحاسمة بين التكامل وتحديد الهوية والمعلومات. إذا لم تتمكن من تحديد هوية أحد الأصول أو التهديدات، فلن تعرف أنه موجود، وبالتالي لن تكون مهتمًا بما يكفي لإنشاء دفاع مستنير حتى يفوت الأوان.

يوضح الشكل 11 هذا المفهوم جيدًا. عقدنا مقارنة مستوى الدمج المُعلَن عنه لكل مؤسسة ضمن وظيفة "تحديد الهوية" في إطار NIST CSF مع قدرتها على اكتشاف التهديدات بدقة في وقت مناسب. **تكون المؤسسات ذات الأنظمة المتكاملة بدرجة عالية لتحديد هوية الأصول والمخاطر شديدة الأهمية معززة بإمكانات أقوى بكثير (+41%) للكشف عن التهديدات.** لذا، بالمعنى الحقيقي، فإن محاربة التجزئة ومحاربة الأعداء يسيران جنبًا إلى جنب!



الشكل 11: تأثير تكامل وظيفة تعريف NIST CSF على قدرات اكتشاف التهديدات

تكون المؤسسات ذات الأنظمة المتكاملة بدرجة عالية لتحديد هوية الأصول والمخاطر شديدة الأهمية معززة

+41%

بإمكانيات أقوى للكشف عن التهديدات.

"تتيح الأتمتة لمهندسينا إمكانية الاستجابة للتهديدات الناشئة في الوقت المناسب. ويمكننا الآن التركيز على الحصول على مفاهيم الأمان بشكل صحيح بدلاً من التحديث المستمر للقواعد ومراقبة الشبكة على مدار الساعة طوال أيام الأسبوع. تخوض Cisco الصعاب وتستخرج المعلومات التي نحتاجها حتى نتمكن من القيام بعمل أفضل في تأمين بنيتنا التحتية وصيانتها. لقد منحتنا المزيج المثالي من ذكاء الآلة والذكاء البشري".

ستيف إرزبيرجر، كبير مسؤولي التكنولوجيا (CTO)،
Frankfurter Bankgesellschaft (Schweiz) AG

قراءة المزيد

تطوير إمكانات اكتشاف التهديدات والاستجابة للحوادث

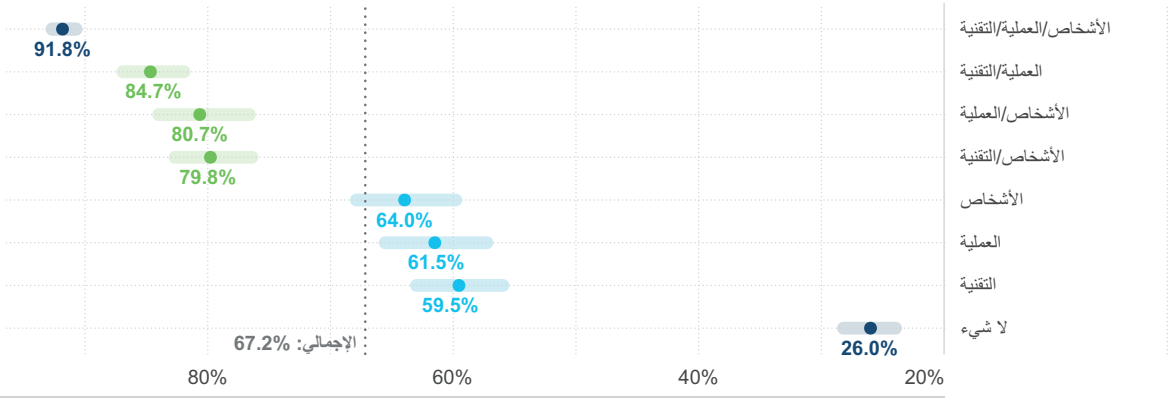
يغطي هذا القسم مجالين منفصلين من مجالات ممارسات الأمان كان من شأنهما أن خلقا بنفسيهما "الوظائف الرائعة الخمس". ولكن نظرًا لأن قسم اكتشاف التهديدات والاستجابة للحوادث (IR) غالبًا ما يشارك الأشخاص والعمليات والتقنيات تحت شعار العمليات الأمنية (SecOps)، فقد طرحنا مجموعة من الأسئلة الشائعة فيما بينها. وبالتالي، فمن المنطقي تحليلها في نفس القسم بهذه الدراسة.

تحقق جميع المؤسسات تقريبًا (حوالي 92%) التي تتمتع بالقوة في مجالات الأشخاص والعمليات والتقنيات، إمكانيات متقدمة في اكتشاف التهديدات والاستجابة لها.

هل نمنح الأولوية للأشخاص أم للعملية أم للتكنولوجيا؟

بالحديث عن الأشخاص والعمليات والتكنولوجيا (التي كانت تُعرَف سابقًا بثلاثية p-p-t)، فلنبدأ تحقيقنا من تلك النقطة. غالبًا ما توصف وظائف الأمن بأنها مزيج من العناصر الثلاثة، لا سيما في مجال الكشف عن التهديدات والاستجابة للحوادث. لكن هل أي جزء من هذا الثالوث الأمني أكثر أهمية من الآخرين؟ أتعرف إلى أين يتجه هذا الأمر؛ دعنا ننتقل إلى التحليل.

بدءًا من الجزء السفلي من الشكل 12، نرى أن ربع البرامج فقط التي تفتقر إلى القوة في جميع أضلاع مثلث p-p-t (الأفراد-العمليات-التكنولوجيا) تُعبر عن ثقتها في العمليات الأمنية (SecOps) الخاصة بها. إن اكتساب القوة في مجال واحد - الأشخاص أو العمليات أو التكنولوجيا - يعزز تلك النسبة المئوية حتى حوالي 60% إلى 64%، حسب المجال. يبدو أن القوة في مجال الأشخاص تمنح ميزة طفيفة، لكن فواصل الثقة الزمنية المتداخلة تحذر من الإفراط في تناول هذه الحقيقة. المهم أن أيًا من هذه الأشياء يقدم نقطة انطلاق جيدة لبناء إمكانات أفضل للكشف والاستجابة.



المصدر: دراسة نتائج Cisco Security

الشكل 12: تأثير قوة مجال الأشخاص والعمليات والتكنولوجيا على إمكانات اكتشاف التهديدات والاستجابة للحوادث

بمتابعة الشكل 12 لأعلى، يؤدي تنفيذ أمرين بشكل جيد إلى نقل برامج SecOps بشكل ملحوظ أعلى من المتوسط وإلى تحسين الإمكانات بحوالي 15% إلى 20% مقارنةً بتلك التي يتم فيها تنفيذ أمر واحد فقط بشكل جيد. مرة أخرى، لا يهم حقًا أي اقتران تختاره بين مجالات الأشخاص أو العمليات أو التقنيات. أنت فقط بحاجة إلى القوة في أي مجالين. من الجيد معرفة أن هناك بعض حرية الاختيار في تصميم خارطة طريق SecOps لمؤسستك، أليس كذلك؟

وهذا يقودنا إلى برامج النخبة في الشكل 12 التي تمكنت من تحقيق ثلاثية SecOps. **تحقق جميع المؤسسات تقريبًا (حوالي 92%) التي تتمتع بالقوة في مجالات الأشخاص والعمليات والتقنيات، إمكانيات متقدمة في اكتشاف التهديدات والاستجابة لها.** وهذا يمثل زيادة في الأداء بمقدار 3.5 أضعاف مقارنة ببرامج SecOps التي لا تتمتع بالقوة في أي من هذه المجالات! لذا، ابدأ حيثما يمكنك تحقيق أكبر قدر من التقدم، ولكن لا تتوقف حتى تصل إلى القمة في ثالوث p-p-t (الأشخاص والعمليات والتقنيات).

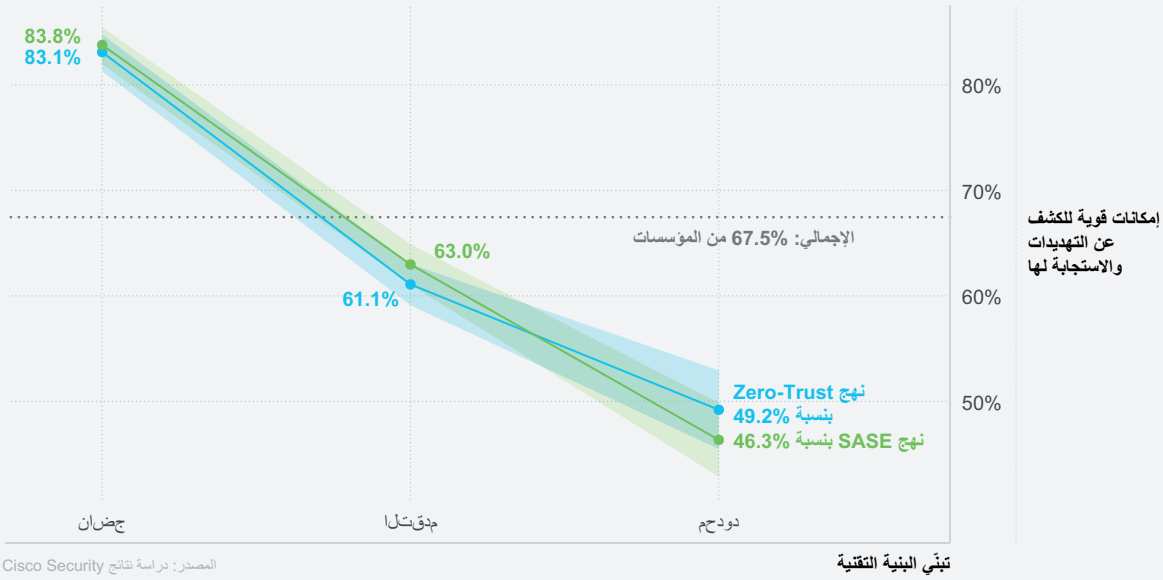
المؤسسات ذات الإمكانيات القوية في جوانب الأشخاص والعمليات والتقنية تشهد

3.5 أضعاف

زيادة في الأداء الخاص باكتشاف التهديدات والاستجابة لها مقارنةً بتلك التي تفتقر إلى القوة في جميع هذه المجالات

هل يعمل نهج انعدام الثقة (Zero Trust) و SASE على تمكين SecOps بشكل أفضل؟

ندرك أن أدوات التوصيف المجردة مثل "التكنولوجيا القوية" تجعل من الصعب تكوين نقاط هامة سريعة ملموسة من النتائج المذكورة أعلاه. لهذا السبب طرحنا بضعة أسئلة للمتابعة حول بنى تقنية محددة. لقد سألنا المشاركين في الاستطلاع عن تبنيهم لنهج انعدام الثقة (Zero Trust) ونهج حافة خدمة الوصول الآمن (SASE) للوصول إلى فهم أفضل لكيفية تأثير هذين النهجين على إمكانات اكتشاف التهديدات والاستجابة للحوادث (وبالتالي نتائج برنامج الأمان).



المصدر: دراسة نتائج Cisco Security

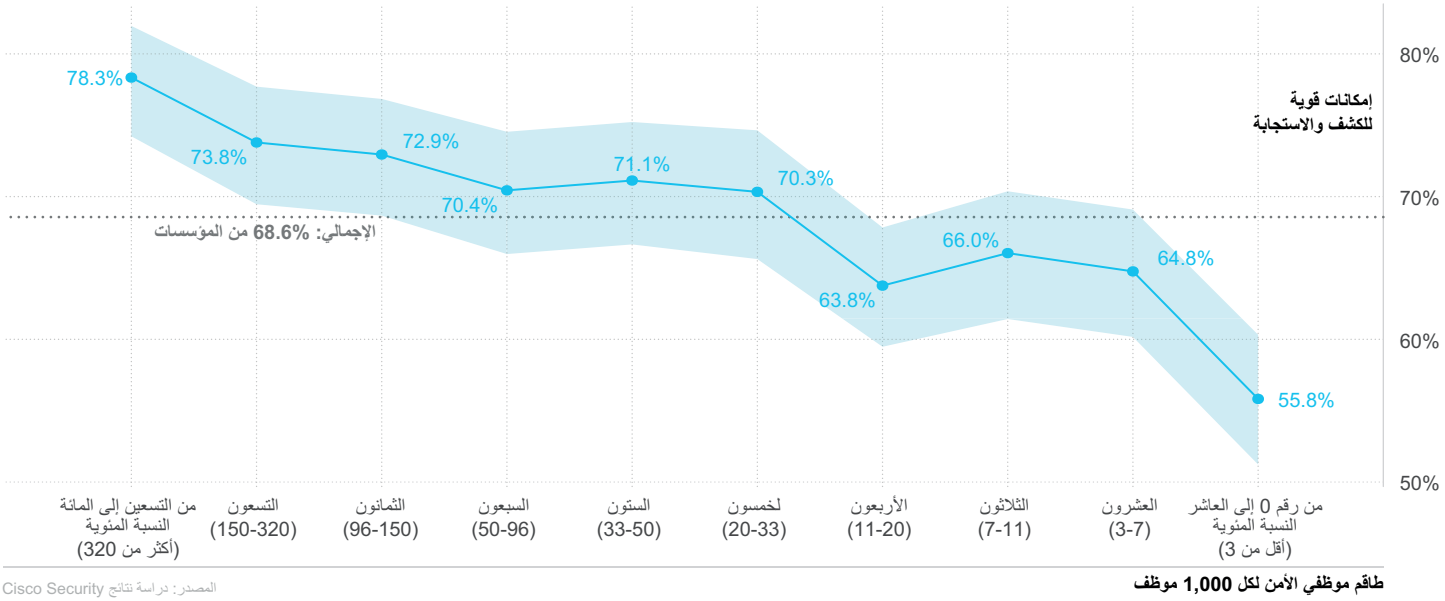
الشكل 13: تأثير البنى التقنية لنهجي Zero Trust و SASE على إمكانات اكتشاف التهديدات والاستجابة للحوادث

المؤسسات التي تدّعي أن لديها سُبُل تنفيذ ناضجة لنهج Zero Trust أو SASE تكون أكثر عرضة بنسبة 35% تقريبًا للإبلاغ عن العمليات الأمنية (SecOps) القوية مقارنةً بتلك المؤسسات ذات سُبُل التنفيذ الناشئة. تؤكد هذه النتائج الدليل الذي شاركناه سابقًا حول الفوائد العديدة التي يمكن أن تجلبها البنى التقنية الحديثة لبرامج الأمن السيبراني.

هل توفر مزيد من الأشخاص يعني متاعب أقل؟

نعلم أن توفر أشخاص جيدين هو أمر مهم لبناء إمكانات قوية للكشف عن التهديدات والاستجابة للحوادث. ولكن هل من الأفضل التركيز على إضافة مزيد من الأشخاص أم شحذ مهارات الأشخاص الموجودين لديك؟ من الواضح أن ذلك يجب ألا يكون حصريًا بشكل متبادَل، ولكن يبقى السؤال - هل نرى أي دليل على أن الكمية أو الجودة أكثر أهمية عندما يتعلق الأمر بتطوير فِرق SecOps الناجحة؟

للإجابة على ذلك السؤال، بدأنا أولاً بحساب نسبة موظفي SecOps إلى إجمالي الموظفين لجميع المؤسسات. ثم قمنا بمقارنة تلك النسبة بالقوة المُعلَن عنها لإمكانات الكشف والاستجابة. يصور الشكل 14 نتيجة تلك الحسابات، وعلى الرغم من أنه لا يجيب بشكل كامل عن سؤال الكمية أو الجودة، إلا أنه يقدم بعض النقاط الهامة السريعة.



المصدر: دراسة نتائج Cisco Security

الشكل 14: تأثير نسبة التوظيف الأمني على إمكانات اكتشاف التهديدات والاستجابة للحوادث

أول هذه النقاط السريعة أن نسب التوظيف الأمني ترتبط بإمكانات أفضل للكشف عن التهديدات والاستجابة لها. المؤسسات ذات النسب الأعلى تزيد احتمالات أن تعلن عن إمكانات أقوى بنسبة تزيد قليلاً عن 20% مقارنة بتلك ذات النسب الأدنى. ولكن — انظر كيف يتقاطع الخط المُنقَّط الذي يشير إلى المتوسط الإجمالي عبر الكثير من فاصل الثقة الزمني المظلل في الشكل 14؟ ذلك يعني في الأساس أن المؤسسات غير الموجودة على الأطراف القصوى من مقياس التوظيف (غالبيتها) يُحتمَل بنفس القدر أن تعلن عن برامج SecOps قوية.

ماذا يعني كل هذا حقًا؟ حسنًا، يمكننا القول بثقة إن المؤسسات التي لديها فرق أمنية ضخمة يُرجَّح أن تحقق إمكانات قوية لاكتشاف التهديدات والاستجابة لها أكثر من تلك ذات الأطقم صغيرة العدد. لكن عدد الموظفين وحده لن يساعد في التخلص من كل متاعب SecOps لديك أو يضمن النجاح. علاوةً على ذلك، فحتى الفروق بين أصغر وأكبر نسبة توظيف لا تأخذ في الحسبان تعزيز الأداء المرتبط بامتلاك موارد بشرية قوية في القسم السابق. **وبالتالي، يُترَك لنا أن نستنتج أن الجودة متساوية - وربما أكثر في - الأهمية من الكمية عندما يتعلق الأمر ببناء فرق قوية لاكتشاف التهديدات والاستجابة لها.**

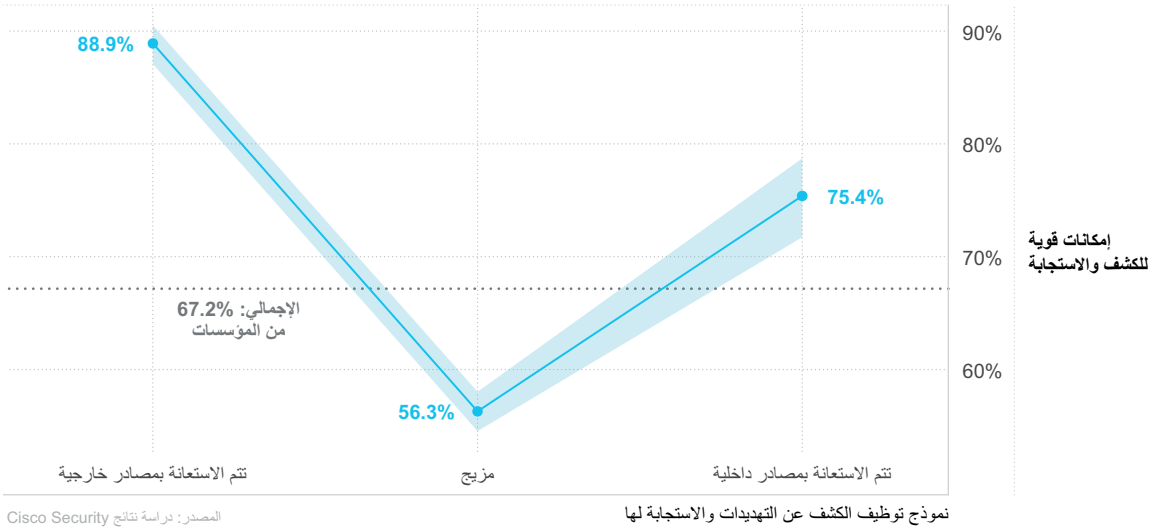
لا تزال الفرق الأمنية تواجه نقصًا حادًا في الموظفين.

مع تقلص الموارد وتزايد التهديدات، يعاني العديد من المتخصصين في الأمن السيبراني من إجهاد واستنزاف شديدين. ما هي التدابير الاستباقية التي يمكننا اتخاذها للمساعدة في شعورهم بالرفاهية؟ في هذا الكتاب الإلكتروني، طلبنا من قادة الصناعة والممارسين مشاركة رؤاهم التحليلية وقصصهم حول إدارة الصحة العقلية.

توظيف كوادر SecOps: هل هي مسؤولية فردية أم جماعية؟

إذًا، فإن نجاح SecOps لا يقتصر فقط على عدد الموظفين، ولكن هل تؤثر نماذج التوظيف على النتائج؟ عند تساوي جميع العوامل، هل من الأفضل الاستعانة بمصادر خارجية أو الاستعانة بمصادر داخلية أو مشاركة المسؤوليات للكشف عن التهديدات والاستجابة لها؟ دعونا نرى كيف تجيب البيانات عن هذا السؤال - ولكن احذر - فإن نتائجها تبدو متناقضة نوعًا ما حيال هذا الأمر.

سألنا المشاركين في استطلاع الرأي عن نماذج التوظيف لديهم ثم عقدنا مقارنة لتلك النماذج مع تصنيف إمكانات الكشف والاستجابة لديهم. **كما هو موضح في الشكل 15، كان من المرجح أن تعلن المؤسسات التي استعانت بشكل كبير بمصادر داخلية أو خارجية لتوظيف الفِرق (بزيادة 20% إلى 30%، على الترتيب) عن برامج SecOps قوية مقارنةً بتلك المؤسسات المتوفر لديها نموذج توظيف مختلط.** نظرًا لأن معظم المؤسسات قالت إنها تستخدم شكلاً من أشكال النموذج المختلط، فقد اعتقدنا أنه سيكون من المفيد النظر إلى هذا الأمر من منظور مختلف قبل أن نحكم عليها جميعًا بالفشل لمجرد أن الاستطلاع (يبدو أنه) يشير إلى هذه النتيجة.



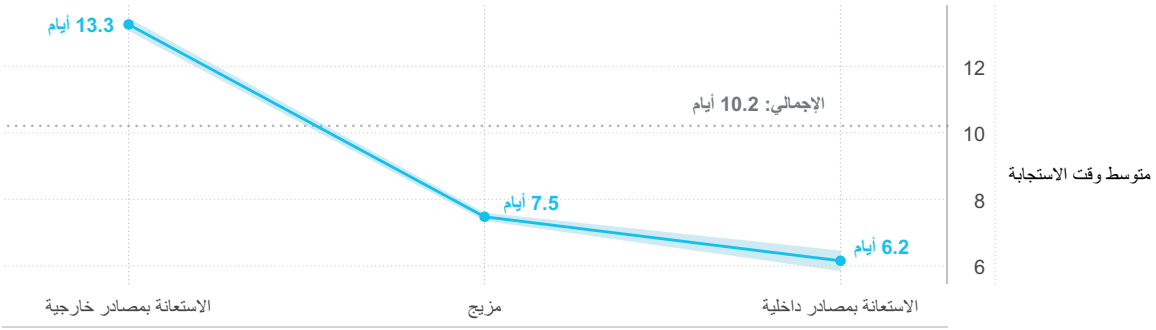
الشكل 15: تأثير نماذج التوظيف على الإمكانات الملموسة لاكتشاف التهديدات والاستجابة للحوادث

المنظمات ذات الفِرق التي يغلب عليها الاستعانة بمصادر خارجية أو داخلية تشهد

20 إلى 30%

زيادة في احتمالية الإعلان عن برامج قوية لعمليات الأمان (SecOps) مقارنةً بتلك المؤسسات التي تتبع نموذج توظيف مختلط

بالإضافة إلى مطالبة المشاركين في الاستطلاع بتقييم القوة الملموسة لإمكانات الكشف والاستجابة، حاولنا أيضًا الحصول على مقاييس أكثر موضوعية للمقارنة. أحد تلك المقاييس هو "متوسط وقت الاستجابة" (MTTR)، أو متوسط الوقت اللازم لإصلاح أو احتواء حادث أمني. في تحليل الخلفية الخاص بنا خارج هذا التقرير، تميل هذه المقاييس غالبًا إلى الاتفاق بشكل مباشر مع التقييمات الشخصية. لكنّ المنظورين يناقض بعضهما البعض في هذه الحالة، كما يتضح من الشكل 16.



الشكل 16: تأثير نماذج التوظيف على متوسط الوقت اللازم للاستجابة للحوادث الأمنية[2]

استنادًا إلى جانب القصة الذي يقدمه الشكل 16، تتمتع المؤسسات المتوفر لديها فرق داخلية لاكتشاف التهديدات والاستجابة لها بمعدل MTTR أقل من نصف النماذج التي يتم فيها الاستعانة بمصادر خارجية (حوالي 6 أيام مقابل 13 يومًا). تلك المؤسسات ذات نماذج التوظيف الهجينة تستقر في المنتصف (حوالي 8 أيام)، بمعدلات MTTR ليست بنفس سرعة الفرق الداخلية ولكنها أسرع بكثير من نظرائها التي يتم فيها الاستعانة بمصادر خارجية في الغالب.

من الواضح أن لدينا مأزقًا صغيرًا هنا. ما هو المقياس (المنظور أم القياس) الصحيح، والأهم من ذلك، أي مقياس يجب أن تستمع إليه فيما يتعلق باتخاذ قرارات الاستعانة بمصادر التوظيف. سنراوغ عمدًا هنا ونقول "كلاهما" و "لا أحد منهما" (مهلاً، لا تلومونا على اتباع الأدلة المتضاربة للبيانات هنا).

بالطبع، تتضمن المعالجة العديد من العناصر والتبعيات. قد تعتمد المؤسسة على مُورد لإصدار تصحيح/إصلاح للأخطاء لحل الثغرة الأمنية بشكل كامل. ويحتاج ذلك التصحيح بعد ذلك إلى اختبار معملي في بيئتها قبل نشره لمرحلة الإنتاج. يكفي أن نقول إن هناك الكثير من الأجزاء المتحركة المعنية.

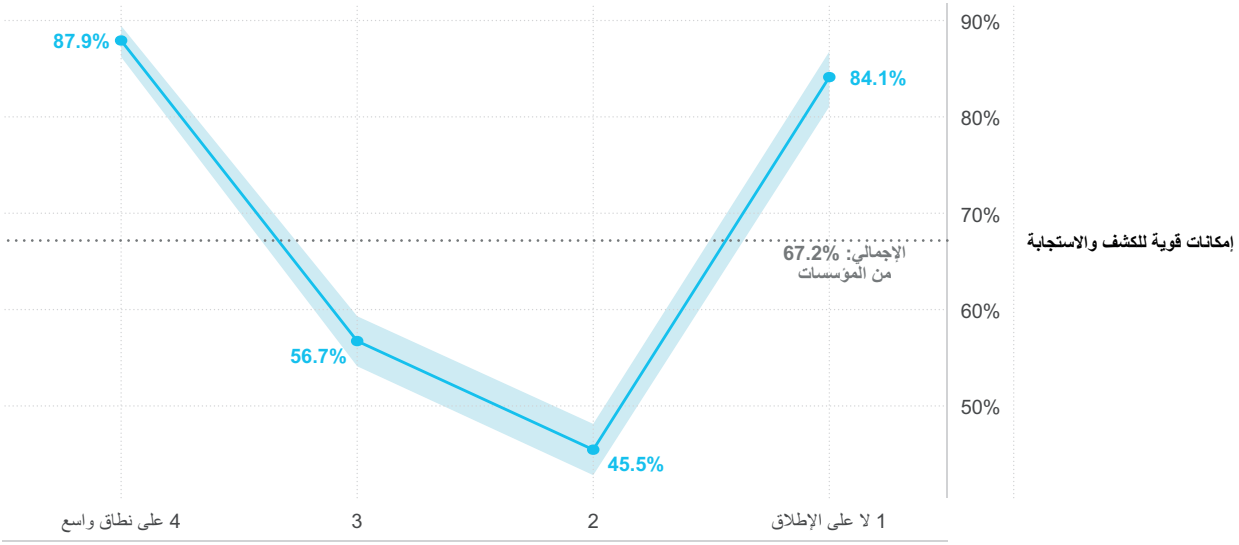
في الحقيقة، من الصعب معرفة ما يحدث هنا على وجه اليقين. ربما تعد محاولة جمع المقاييس عبر استطلاع أمرًا مضللًا. ربما تكون تقييمات MTTR والإمكانات مختلفة بما يكفي للحصول على برنامج "قوي" للاكتشاف والاستجابة بشكل عام، ولكن بمعدلات معالجة أبطأ. ربما تكون هذه البرامج أبطأ لأنها أكثر شمولاً. ربما يستغرق التنسيق مع الموظفين الخارجيين وقتًا أطول. ربما يكون هناك شعور بالثقة لأننا "ندفع للخبراء مقابل أداء هذا الأمر وقد نجحوا في تغطيته." ربما نشهد إصدارًا لـ SecOps يخص تأثير دانينغ-كروجر. ربما يكون كل هذا وأكثر. وبسبب ذلك، نقترح استخدام هذا القسم لإثارة المناقشات بدلاً من اتخاذ القرارات.

[2] نستخدم قيمة المتوسط الهندسي في هذا المخطط لأنه أكثر تمثيلاً للقيمة "النمطية". كانت نسبة MTTR المعلَن عنها عادةً أقل من 3-2 أسابيع، ولكن أفاد المشاركون في الاستطلاع أحيانًا أنها تبلغ شهورًا (أو سنوات!). يؤدي استخدام المتوسط الهندسي إلى تمثيل القيمة "النمطية" بشكل أفضل دون أن تنحرف بسبب تلك القيم الكبيرة للغاية.

هل من الذكاء استخدام الاستخبارات؟

بالحديث عن تأثير دانينغ-كروجر، فذلك إعداد مثالي لهذا القسم. سألنا المشاركين في الاستطلاع عن استخدام استخبارات التهديدات السيبرانية في برنامج العمليات الأمنية (SecOps) لديهم. تقول معظم المؤسسات (85%) إنها تستخدم الاستخبارات على مستوى ما، لكن أقل من ثلثها (31%) تزعم أنها تستخدمه على نطاق واسع. هل تؤدي هذه الاستخبارات إلى اكتشاف للتهديدات واستجابة لها على نحو أفضل وأذكى وأسرع؟ حسنًا... فلنُلق نظرة على الشكل 17.

من الغريب أن معظم المؤسسات التي لا تستخدم ذكاء التهديدات على الإطلاق تعتقد أنها تبلي بلاءً حسنًا. يتبادر إلى الذهن القول المأثور القديم "الجهل نعمة"، خاصة وأن الخوض بحرص في استخدام الاستخبارات يبدو أنه يبدد تلك المفاهيم (بهبوط مستوى الثقة من حوالي 84% إلى 46%). **المؤسسات التي تستخدم ذكاء التهديدات بشكل مكثف تزداد للضعف احتمالية إعلانها عن إمكانات قوية للاكتشاف والاستجابة مقارنةً بتلك ذات معدل الاستخدام الأقل. وفي مثال تتوافق فيه المقاييس وتقييمات الإمكانات، تحقق تلك المؤسسات التي تستفيد من الذكاء بدرجة أكبر بكثير معدلات MTTR تبلغ حوالي نصف تلك الخاصة بالمؤسسات التي لا تستخدم الذكاء.**



المصدر: دراسة نتائج Cisco Security

الشكل 17: تأثير استخدام الذكاء الإلكتروني على إمكانات اكتشاف التهديدات والاستجابة للحوادث

قال عالم النفس ومؤلف الكتب الأكثر مبيعًا دانيال كانيمان ذات مرة ، "نحن لا نرى جهلنا. لدينا فكرة قليلة جدًا عن مدى ضآلة معرفتنا". يشير الشكل 17 إلى أنه بمجرد أن تعرف المؤسسات القليل عن التهديدات المصنفة ضدها، فإنها تدرك أن هناك الكثير الذي لا تعرفه. يبدأ الاستخدام المكثف لذكاء التهديدات في إعادة بناء تلك الثقة - إلا أنها ليست عمياء الآن.

المؤسسات التي تستخدم ذكاء التهديدات على نطاق واسع تزيد لديها بمقدار

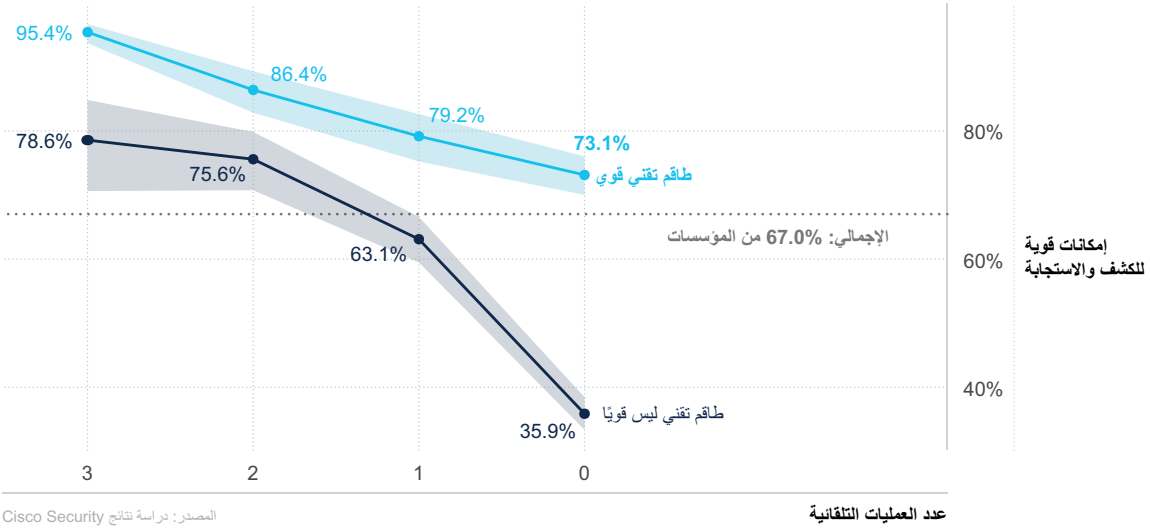
الضعف

احتمالية أن تعلن عن إمكانيات قوية لاكتشاف التهديدات والاستجابة لها

هل الأتمتة بديل للعامل البشري؟

بعد قراءة هذا العنوان، ربما تفترض أنه سؤال بلاغي. ليس بهذه السرعة. مع خطر إثارة حفيظة مجتمع الأمان بأكمله، سنذهب إلى طرف (البيانات) هنا لنقترح أن الأتمتة يمكن، في الواقع، أن تحل محل الأشخاص. ولكن استمر في القراءة قبل أن تقرر حذف هذا التقرير وإضافتنا إلى قائمة جهات الاتصال المحظورة لديك. <نفس عميق>

يتضمن الشكل 18 عناصر رأيتها من قبل في مخططات منفصلة - طاقم الأمن والأتمتة. يقارن الخطان بين نوعين مختلفين من برامج SecOps. يمثل الأول (الخط الأزرق الداكن) المؤسسات التي ليس لديها موارد بشرية قوية، في حين أن تلك التي تتمتع بتلك الرفاهية يمثلها الخط الأزرق الفاتح. في كلا السيناريوهين، يُظهر الانتقال من اليسار إلى اليمين تأثير زيادة مستويات الأتمتة على إمكانات اكتشاف التهديدات والاستجابة للحوادث (IR).



المصدر: دراسة نتائج Cisco Security

الشكل 18: تأثير التوظيف وقوة الأتمتة على إمكانات اكتشاف التهديدات والاستجابة للحوادث

لنبدأ مع "المؤسسات التي تفتقد تلك الإمكانية". حوالي ثلث المؤسسات فقط التي تفتقد طاقم العمل الأمني القوي ولا تعمل على أتمتة أي عمليات رئيسية تعلن عن إمكانات قوية للكشف والاستجابة. يرتفع ذلك المستوى كثيرًا عندما تتم أتمتة أحد مجالات العملية الثلاثة التي استفسرنا عنها (مراقبة التهديدات، تحليل الأحداث، الاستجابة للحوادث). تعمل أتمتة اثنين من تلك العناصر على زيادة القيمة بشكل إضافي، وتعمل أتمتة العناصر الثلاثة كلها على زيادة أداء الموظفين الأقل خبرة بمفردهم لأكثر من الضعف. **أكثر من ثلاثة أرباع برامج SecOps التي تفتقد لموارد التوظيف القوية لا تزال قادرة على تحقيق إمكانات قوية من خلال مستويات عالية من الأتمتة.**

الآن تتبع عينك أو إصبعك من أقصى نقطة على يمين الخط الأزرق الداكن إلى النقطة الأولى من الخط الأزرق الفاتح. هل فهمت المعنى؟ **برنامج SecOps مع طاقم عمل أضعف يستخدم معدلات أتمتة متقدمة قريب من نفس البرنامج مع طاقم عمل قوي وأتمتة ضعيفة.** أو فلنقُل بشكل مختلف، يمكن أن تكون الأتمتة القوية بديلاً لطاقم العمل القوي. هل فهمت - لن نكذب عليك!

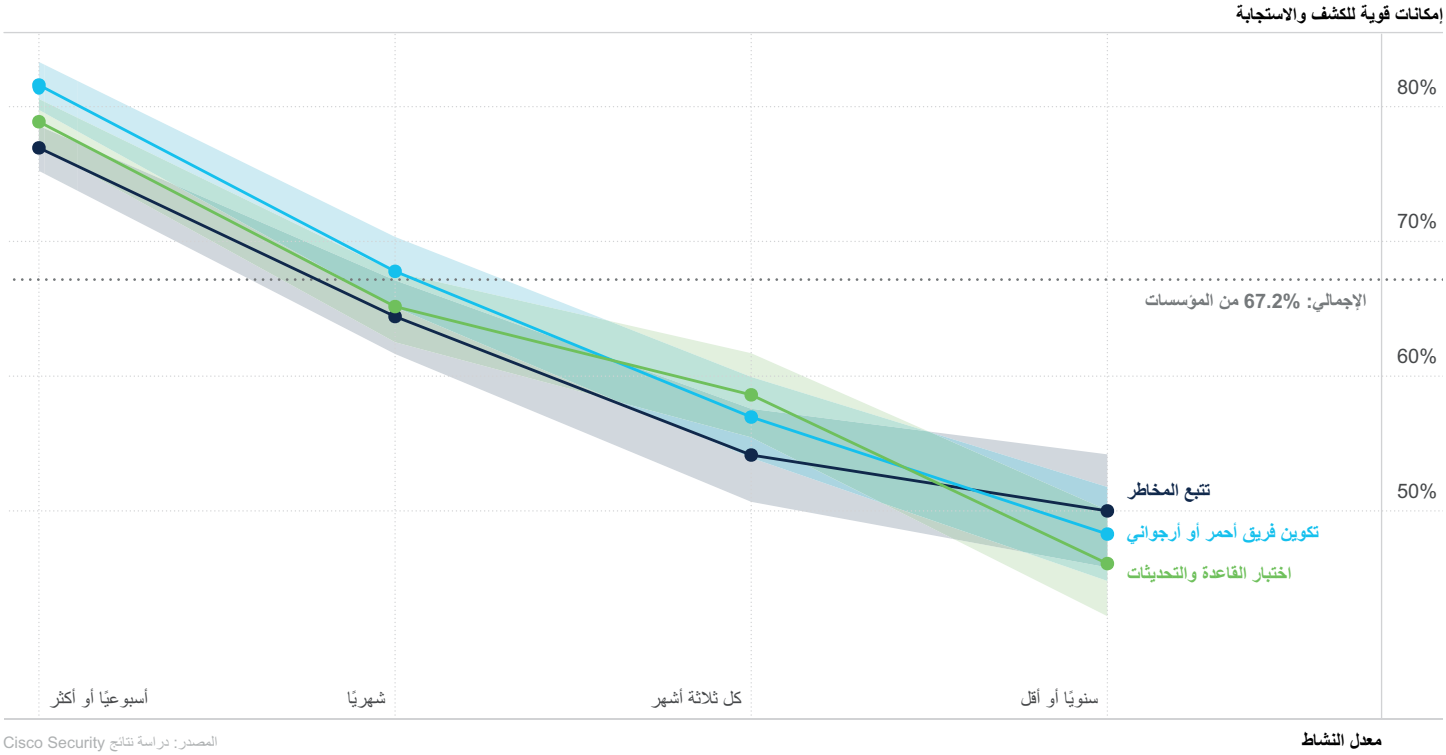
لكن الإنسان في مواجهة الآلة ليس في الحقيقة هو النقطة الرئيسية أو الدرس الأكثر أهمية من الشكل 18. إن اتباع الخط الأزرق عبر مستويات متتالية من الأتمتة يقدم مبررًا مقنعًا للغاية لتحقيق كلا الهدفين. جميع برامج الأمان التي تمكنت من الجمع بين فريق قوي وأتمتة عمليات قوية للكشف عن التهديدات الرئيسية والاستجابة لها تكاد تكون مطمئنة تقريبًا (بنسبة أكبر من 95%) من نجاح برامج SecOps. لذلك، لا تستخدم الأتمتة كبديل للقوى العاملة الموهوبة. بل استخدمها لزيادة موهبتك من خلال السماح لهم بالتركيز على الأنشطة ذات الأولوية العالية.

ما المعدل الذي يجب أن ننفذ به الضبط الدقيق والتسلل والتصيّد؟

يمكن للمرء تسمية أي عدد من الأنشطة المتكررة التي يُحتمَل أن تحسن برامج الكشف عن التهديدات والاستجابة لها. في استطلاع غير رسمي أجريناه حول ذلك الموضوع، تمت التوصية بثلاثة أنشطة أكثر من أي أنشطة أخرى:

- اختبار قواعد الكشف وحالات الاستخدام وتحديثها
- التصيّد بشكل استباقي لعلامات النشاط الضار
- الانخراط في تمارين جماعية حمراء و/أو أرجوانية

لقد سألنا المشاركين في الاستطلاع عن معدل تنفيذ مؤسساتهم لكل من تلك الأنشطة ثم تحققنا من ذلك مقارنةً بالقوة المُعلن عنها لإمكانات الكشف عن التهديدات والاستجابة لها. لا يمكن أن يكون التوجه الناتج في الشكل 19 أكثر وضوحًا من ذلك.



المصدر: دراسة نتائج Cisco Security

الشكل 19: تأثير معدل تكرار النشاط على إمكانات اكتشاف التهديدات والاستجابة للحوادث

كل من الضبط الدقيق للقواعد، وتشكيل الفريق الأحمر/الأرجواني، والبحث عن التهديدات تتبع مسارًا مشابهًا. كلما زاد معدل تنفيذها، زادت استفادتها من برامج SecOps. **تشهد المؤسسات التي تُجري هذه الأنشطة أسبوعيًا على الأقل ارتفاعًا بنسبة 30% تقريبًا في الأداء مقارنة بتلك التي تجريها سنويًا أو بمعدل أقل.** إذًا، ما معدل تنفيذ مؤسستك لها؟ الجواب البسيط هو "كلما زاد المعدل، سيكون أفضل".

المؤسسات التي تباشر هذه الأنشطة مرة أسبوعيًا على الأقل تشهد تقريبًا

30%

ارتفاعًا في الأداء

"الأمان دائم التغير طوال الوقت ونحن بحاجة إلى اتباع توجهات الأمان هذه. [سابقًا]، أضعنا الكثير من الوقت في حل المشاكل والحوادث الأمنية. الآن وبعد أن نجحنا في تبسيط عمليتنا وتوفير الوقت أثناء التحقيقات، يمكننا متابعة توجهات الأمان الجديدة ودمج حلول الأمان الجديدة لتوفير بنية أساسية أكثر أمانًا لشبكتنا التعليمية".

بهروز إبراهيموف، كبير مهندسي أمن المعلومات، AzEduNet

قراءة المزيد

ضمان التعافي السريع من الكوارث والمرونة

يعدّ مدى التقلبات التي تمر بها "أولوية التفكير" في جوانب الأمن السيبراني المختلفة بمرور الوقت أمرًا مثيرًا للاهتمام. بعد التغاضي عن انتهاكات البيانات والتجسس الإلكتروني لعدد من السنوات، أصبح موضوع استمرارية الأعمال والتعافي من الكوارث (BCDR) مرة أخرى في مقدمة النقاط الهامة. وهناك سبب وجيه لذلك. لقد فرضت برامج الفدية الضارة المتفشية وحالات انقطاع مقدمي خدمات الاستضافة الرئيسيين، وما إلى ذلك، تغييرات كبيرة في الاستراتيجيات المتخَّذة لضمان المرونة في مواجهة التهديدات التي لا هوادة فيها.

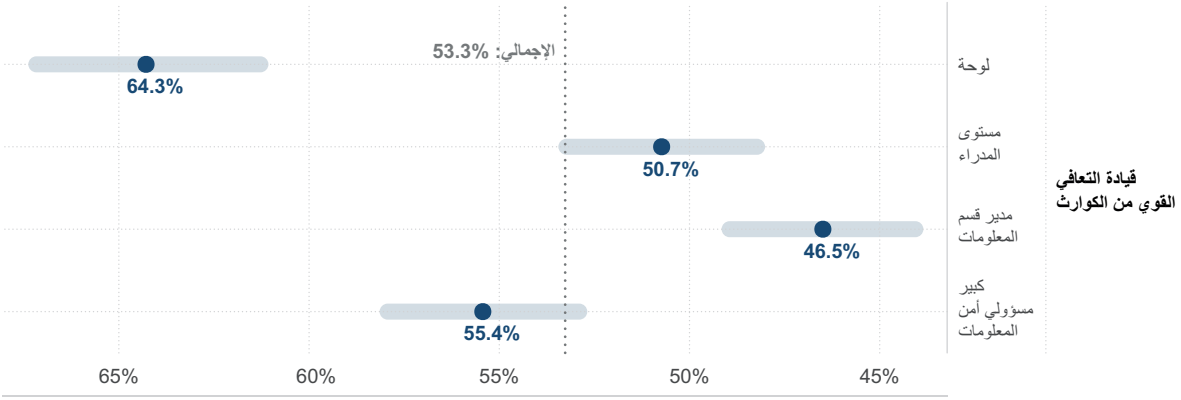
صنفت "دراسة النتائج الأمنية لعام 2021" التعافي الفوري من الكوارث باعتباره رابع أقوى مساهم في بناء برامج الأمن السيبراني الناجحة. فقد أظهرت هذه النتيجة ارتباطات مهمة مع جميع النتائج الـ 11 باستثناء واحدة (الثقافة الأمنية). ودعونا لندرس الاستراتيجيات المُتبَّعة لتعظيم فعالية هذه الممارسة وضمان المرونة، مع وضع ذلك في الاعتبار.

لقد فرضت برامج الفدية الضارة المتفشية وحالات انقطاع مقدمي خدمات الاستضافة الرئيسيين، وما إلى ذلك، تغييرات كبيرة في الاستراتيجيات المتخَّذة لضمان المرونة في مواجهة التهديدات التي لا هوادة فيها.

هل يجب أن يكون للتعافي من الكوارث إشراف على مستوى مجلس الإدارة؟

كنا نشعر بالفضول لمعرفة من كان يتولى الإشراف النهائي على إمكانات التعافي من الكوارث. اتضح أن المسؤولية تقع بشكل متساوٍ على عاتق كل من كبير مسؤولي المعلومات (CIO) وكبير مسؤولي أمن المعلومات (CISO) والأعضاء الآخرين غير المتخصصين في تكنولوجيا المعلومات (IT) في مستوى المدراء بالمؤسسة، مع تبعية مسؤولية ما يقرب من ربع عمليات BCDR بالمؤسسات لكل منهم. تُعد إمكانية الرؤية على مستوى مجلس الإدارة أقل شيوعًا من تلك العمليات، ولكنها تظل موجودة في 18% من المؤسسات في استطلاعنا.

عندما عقدنا مقارنة بين هذه الإجابات مع تقييم كل مشارك لإمكانات استمرارية الأعمال والتعافي من الكوارث، أصبح من الواضح أن مسألة الإشراف ليست مجرد فضول. **وفقًا للشكل 20، المؤسسات التي تخضع لإشراف مجلس الإدارة فيما يتعلق بعمليات BCDR هي الأرجح (بزيادة 11% عن المتوسط) للإعلان عن وجود برامج قوية.** تُظهر وظائف استمرارية الأعمال والتعافي من الكوارث التي كانت أولوية تبعيتها لكبير مسؤولي المعلومات (CIO) أدنى المعدلات التي تقل بشكل كبير عن المتوسط.



المصدر: دراسة نتائج Cisco Security

الشكل 20: تأثير الإشراف المؤسسي عالي المستوى على إمكانات التعافي من الكوارث

هناك العديد من التفسيرات المعقولة للنتائج في الشكل 20. نعتقد أن المؤسسات التي تجيب بمجلس الإدارة فيما يخص الإشراف على مسائل التعافي من الكوارث قد زادت مخاوفها بشأن المخاطر التشغيلية والمرونة. ويُفترض أن تُترجم تلك المخاوف إلى إشراف أكثر إحكامًا ودعم أقوى وميزانيات أكبر. لذلك، إذا كانت مؤسستك تكافح من أجل تحسين إمكانات التعافي من الكوارث، فقد يكون من المنطقي إنشاؤها من أعلى لأسفل بدلاً من العكس.

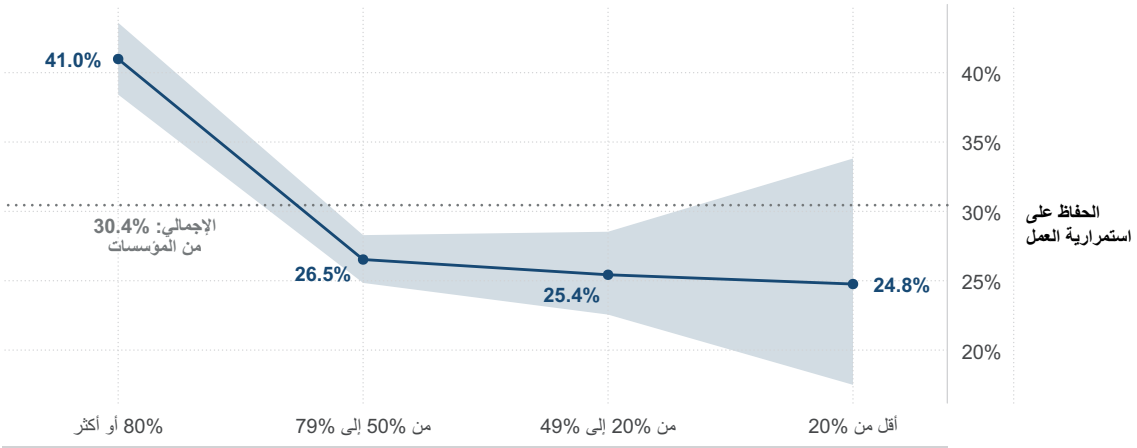
ماذا عن التشغيل اليومي للتعافي من الكوارث؟

بالإضافة إلى الإشراف النهائي، سألنا أيضًا عن المسؤول عن إدارة الجوانب الأكثر تكتيكية للتعافي من الكوارث. **تميل العمليات الموجودة داخل فرق الأمن السيبراني أو فرق استمرارية الأعمال المتخصصة إلى الإعلان عن أفضل أداء.** أما البرامج التي تديرها تكنولوجيا المعلومات (IT) فتكون أقل من تلك بوجه عام. ومن المثير للاهتمام، أن إمكانية الرؤية على مستوى مجلس الإدارة تبدو وكأنها تعمل كموجة صاعدة ترفع كل القوارب معها. كانت معدلات النجاح متساوية إحصائيًا بغض النظر عن مكان وقوع المسؤوليات اليومية طالما أن الإشراف النهائي يصل إلى مجلس الإدارة.

هل نطاق مواجهة الكوارث أمر مهم؟

ربما لن تُصدم عندما تعلم أن الكارثة لا تقع بشكل عملي في الوقت والمكان الذي تكون مستعدًا فيهما لها. لا تختلف كوارث الأمن السيبراني، وهذا هو السبب وراء كون الحكمة التقليدية في هذا المجال هي الاستعداد لجميع الاحتمالات بأفضل ما يمكنك. وهذا القول أسهل من فعله بالطبع.

وإثباتًا لتلك الحقيقة، تذكر أقل من ثلاث مؤسسات من أصل عشر أن وظائف التعافي من الكوارث تغطي ما لا يقل عن 80% من الأنظمة الحيوية. ونصف عدد المؤسسات يقع المعدل لديها في نطاق 50% إلى 79%، وأقل من 20% منها تقر بمعدلات تغطية أقل من ذلك. للوهلة الأولى، لا يبدو ذلك سيئًا للغاية. فبعد كل ذلك، تنجح معظم المؤسسات في تغطية أغلب الأنظمة الهامة لديها. لسوء الحظ، تتجاهل تلك الحقيقة النزعة المزعجة بأن الكوارث تضرب أماكن غير متوقعة. تشير بياناتنا إلى أن هذا يحدث في كثير من الأحيان بمعدل أكثر مما نود الاعتراف به.



المصدر: دراسة نتائج Cisco Security

الشكل 21: تأثير تغطية الأصول الحيوية على إمكانات التعافي من الكوارث

يقيس الشكل 21 نتيجة جديدة تمت إضافتها لهذه الدراسة بهدف قياس قدرة المؤسسة على الحفاظ على استمرارية العمل خلال الأحداث التخريبية. اتضح أنها واحدة من النتائج الثلاث التي ذكر المشاركون في الاستطلاع أنهم يواجهون أكبر صعوبة في تحقيقها. وذلك يجعل الأمر أكثر أهمية لإيجاد طرق فعالة لتحسين احتمالية النجاح.

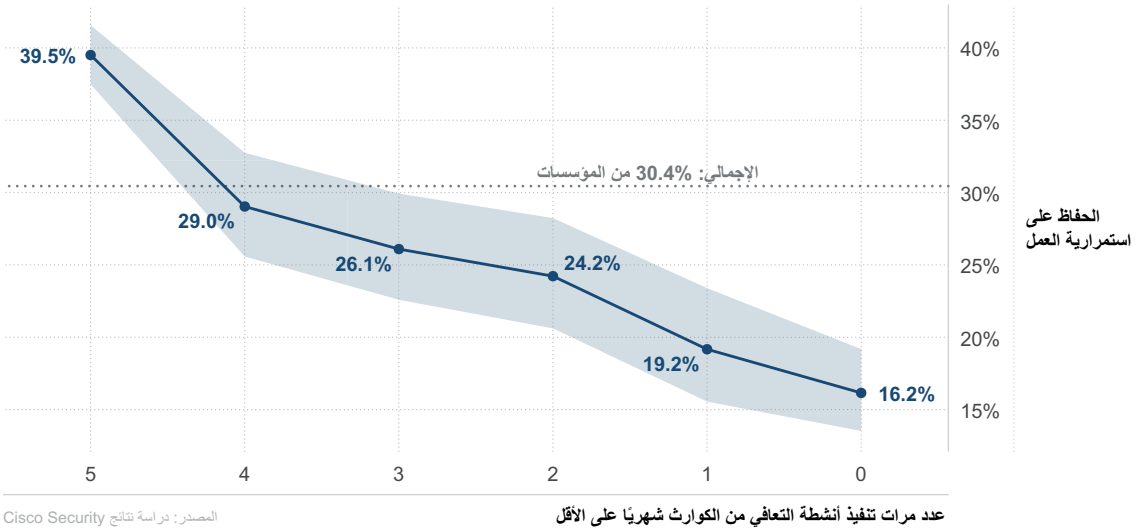
توجد رسالة مهمة في الشكل 21 حول الحفاظ على استمرارية الأعمال. **وبالتحديد، لا يوجد تقريبًا أي تحسن في احتمالية تحقيق هذه النتيجة إلى أن تغطي إمكانات BCDR ما لا يقل عن 80% من الأنظمة الحيوية.**

يكاد يكون من المؤكد أن هذا يعود إلى النزعة الخارقة للكوارث التي تضرب حيثما لا نكون مستعدين لها. الدرس المستفاد هنا هو أنه لا يمكننا توقع أن تؤدي الاستثمارات في استمرارية الأعمال والتعافي من الكوارث إلى نتائج فورية أو نتائج مكافئة. ربما لا تكون هذه رسالة ترحيب، ولكن مرة أخرى، الكارثة ليست شخصًا مرحبًا به أبدًا.

هل الممارسة تجعل عملية التعافي من الكوارث مثالية؟

سنفصح عن إجابة هذا السؤال ونقدم الإجابة مباشرة. لا، للأسف ليس الأمر كذلك. لكنها تجعلها الحال أفضل بكثير مقارنة بعدم الممارسة على الإطلاق. أفضل لأي مدى؟ تابع القراءة...

يقول المثل العسكري المعروف، "ما مِن خطة تبقى بعد أول لقاء مع العدو". لقد اتضح أن هذا ينطبق بشكل جيد على ساحة المعارك الإلكترونية، وهناك العديد من الطرق المختلفة لاختبار إمكانات BCDR، بما في ذلك الإرشادات التفصيلية للخطة، وتمارين الطاولة، والاختبار المباشر، والاختبار الموازي، واختبار الإنتاج الكامل. لقد سألنا المشاركين في الاستطلاع عن معدل مشاركة مؤسساتهم في مثل هذه التمارين، وعقدنا مقارنة لذلك مع احتمالية الحفاظ على استمرارية الأعمال.



الشكل 22: تأثير ممارسات الاختبار على إمكانات التعافي من الكوارث

لم تتفوق أي من هذه الممارسات على غيرها من حيث الفعالية، ولكنها جميعًا ساهمت بشكل جماعي بقدر ما لتحقيق مرونة أفضل. **كانت المؤسسات التي شاركت بانتظام في جميع الأنواع الخمسة من اختبارات التعافي من الكوارث أرجح بمرتين ونصف في الحفاظ على استمرارية الأعمال بنجاح مقارنةً بتلك المؤسسات التي لم تشارك في أي منها.** ما النقطة الهامة؟ لا تترك المرونة للصدفة. ضع إمكاناتك في استمرارية الأعمال والتعافي من الكوارث تحت اختبار الضغط بانتظام من زوايا مختلفة متعددة.

المؤسسات المشاركة بانتظام في جميع الأنواع الخمسة من اختبارات التعافي من الكوارث تزيد لديها بمعدل

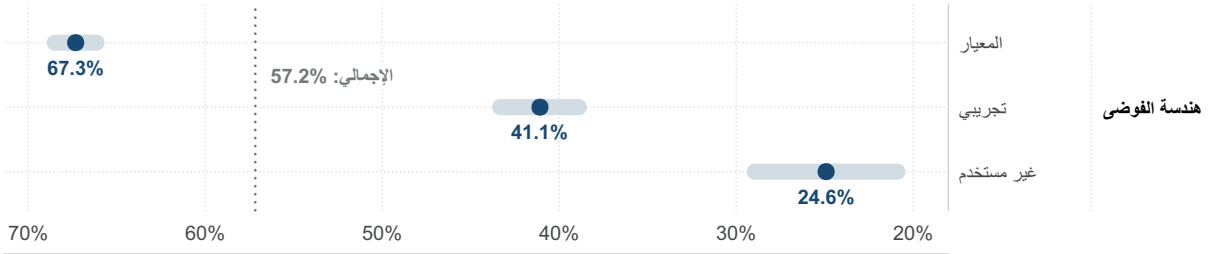
2.5 أضعاف

احتمالية الحفاظ على استمرارية العمل بنجاح

هل يجب أن نطلق العنان لأداة Chaos Monkey؟

فيما يتعلق بموضوع وضع خطة التعافي من الكوارث لديك تحت اختبار الضغط، دعونا نصل إلى أقصى قدر من "الضغط". نحن نتحدث عن هندسة الفوضى، حيث يتم تعطيل الأنظمة بشكل دوري (عن قصد) لاختبار قدرتها على تحمل الظروف والأحداث غير المتوقعة. هل يمكن أن يساعد وضع عوائق في مسارات أنظمة تكنولوجيا المعلومات (IT) والأمان لديك في جعل مؤسستك أكثر مرونة؟ حسنًا، لقد أتيت إلى المكان الصحيح لمعرفة ذلك.

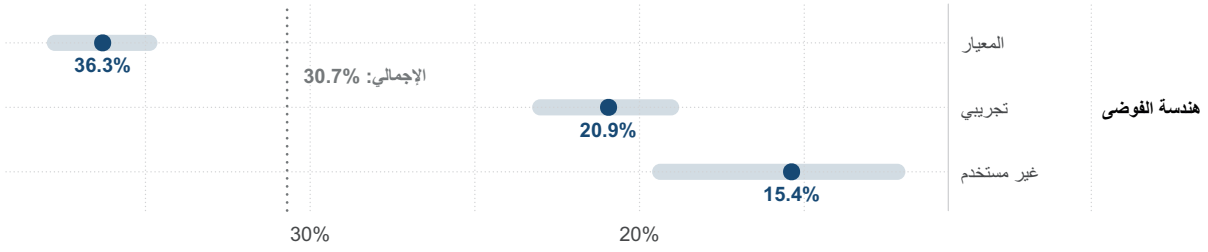
لقد سألنا المشاركين في الاستطلاع عن مدى انخراط مؤسساتهم في هندسة الفوضى، وعلمنا أنها أكثر شيوعًا مما توقعنا. من الجدير بالذكر أننا لاحظنا وجود علاقة بين هذه الممارسة والتكامل التقني. وفقًا للشكل 23، تعلن أكثر من ثلثي المؤسسات التي تعتبر هندسة الفوضى فيها ممارسة قياسية عن تقنيات متكاملة للغاية تدعم إمكانات التعافي لديها. ليس من الواضح ما إذا كان التكامل يستلزم أو يتيح إمكانية حدوث هندسة الفوضى. كما هو الحال مع العديد من الأشياء في هذا المجال، فمن المحتمل أن يكون الأمر يتعلق بالأمرين معًا. راقب هذا التخصص الناشئ - خاصة إذا كنت مسؤولاً عن عمليات BCDR في بيئة تكنولوجيا معلومات (IT) معقدة ومتكاملة للغاية.



المصدر: دراسة نتائج Cisco Security

الشكل 23: العلاقة بين هندسة الفوضى ومستوى تكامل تكنولوجيا المعلومات (IT)

تقدم مقارنة مدى استخدام هندسة الفوضى مع نتيجة الحفاظ على مرونة الأعمال في الشكل 24 سببًا مقنعًا لدعوة أداة Chaos Monkey إلى شبكتك. **المؤسسات التي تطبّق معايير هندسة الفوضى يُرجح أن تحقق مستويات أعلى من النجاح لهذه النتيجة بضعفين مقارنة بالمؤسسات التي لا تستخدمها.** إذا صدمتك هذه النتيجة، فلست وحدك. الخبر السار هو أنه يمكنك أن تصدم أداة Monkey قبل أن تصدمك هي من جديد من خلال استغلالها للعمل لصالحك من خلال ممارسة هندسة الفوضى.



المصدر: دراسة نتائج Cisco Security

الشكل 24: تأثير هندسة الفوضى على الحفاظ على مرونة الأعمال

الخاتمة والتوصيات

لقد بدأنا بممارسات الأمان التي تم تحديدها على أنها فعالة للغاية في دراسة سابقة، وجمعنا المزيد من المعلومات عبر استطلاع جديد لمعرفة ما يحقق لها أكبر فاعلية، وشاركنا تلك الدروس معك. نأمل أن تغادر هذا التقرير بالعديد من النصائح العملية حول كيفية جعل برنامج الأمن السيبراني أكثر نجاحًا.

لكن لا يضر أبدًا التفكير في نتائج دراسة كهذه والاستماع إلى ما تم سلبه من الآخرين. لقد طلبنا من فريقنا الاستشاري من كبار مسؤولي أمن المعلومات (CISO) ذوي الخبرة التعليق على كل مجال من مجالات الممارسة التي تمت دراستها. وأدرجنا أهم توصياتهم أدناه. يمكنك العثور على مزيد من الأفكار والنقاط الهامة في سلسلة مدوناتنا "دراسة نتائج الأمان".

التحديث الاستباقي للتكنولوجيا

"تعد مشكلة الديون الأمنية أمرًا مهمًا. بالنسبة لكبير مسؤولي أمن المعلومات (CISO)، يتمثل الطريق إلى الأمام في تطوير استراتيجية "الشراء والاحتفاظ ثم البيع". تعرف على ما لديك، وحدد بنية تقنية قابلة للتكيف، وقلل من مخاطر التبعية، وقم بتنفيذ حلقة مراجعة متكررة لدورات التحديث المستقبلية."

ريتشارد آرشديكون، كبير مسؤولي أمن المعلومات (CISO) استشاري، Cisco

التكنولوجيا ذات التكامل الجيد

"نعلم أن تكنولوجيا المعلومات (IT) الحديثة وذات التكامل الجيد تساهم في نجاح برنامج الأمان بشكل عام، لذلك، نقدم إليك هنا بعض الإجراءات التي يمكنك اتخاذها لتحسين بيئتك: ابحث عن حلول الأمان المستندة إلى السحابة، واستكشف فرص الأتمتة، وتأكد من اشتمال متطلبات الشراء على إمكانات تكامل التكنولوجيا."

هيلين باتون، كبير مسؤولي أمن المعلومات (CISO) استشاري، Cisco @CisoHelen

الاستجابة للحوادث في الوقت المناسب

"يوفر الموظفون الأقوياء لفِرق الاستجابة للحوادث (IR) ميزة. هذه نقطة انطلاق جيدة ولكن يجب تنفيذها جنبًا إلى جنب مع العناصر الأخرى. عندما تجمع المؤسسات بين قوة الأشخاص والعمليات والتكنولوجيا، فإنها تحقق قدرات متقدمة للكشف عن التهديدات والاستجابة لها".

ديف لويس، كبير مسؤولي أمن المعلومات (CISO) استشاري، Cisco @gattaca

الاكتشاف الدقيق للتهديدات

"اختر أعلى الأشخاص مهارة لفرق SecOps لديك، لأن المهارة أهم من عدد الموظفين المجرد. إذا لم تتمكن من الحصول على مستوى الخبرة الذي تحتاجه، فيمكن أن تساعدك الأتمتة في سد الفجوة مع الموظفين المبتدئين لديك والحصول على نتائج قوية كما لو كان لديك المزيد من الموظفين ذوي الخبرة".

ويندي ناذر، كبير مسؤولي أمن المعلومات (CISO) استشاري، Cisco @wendynather

التعافي الفوري من الكوارث

"تسلط النتائج الواردة في هذا التقرير الضوء على قيمة استمرارية الأعمال وإمكانات التعافي من الكوارث، ولكنها لا تعرضها بمعزل عن وظائف الأمان الأخرى. ينبغي تقاسم تحديد أولوية الموارد وتصنيف مخاطرها مع وظائف إدارة المخاطر الأخرى. وبالمِثل، ينبغي الوصول إلى تكامل محكم بين إدارة الأصول وإدارة التهديدات لضمان عمل جميع الفِرق بشكل متناسق".

فولفجانج غورليخ، كبير مسؤولي أمن المعلومات (CISO) استشاري، Cisco @jwgoerlich

لمحة عن Cisco Secure

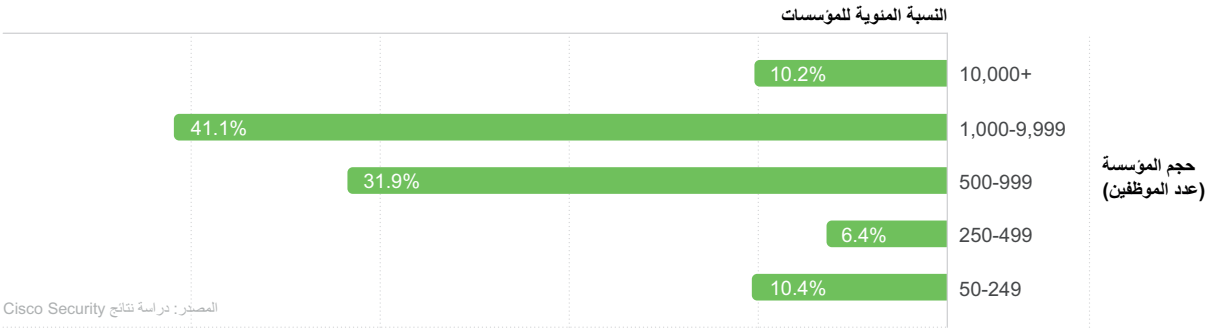
لطالما رسخت Cisco نفسها كشركة رائدة عالميًا في مجال التكنولوجيا التي تدعم الإنترنت، مع بناء مجموعة مفتوحة ومتكاملة من حلول الأمن السيبراني على طول الطريق. ونعتقد أنه ينبغي تصميم الحلول الأمنية للعمل كفريق. يجب أن تتعلّم من بعضها البعض. ويجب أن تنظر بعين الاعتبار وتستجيب كوحدة منسقة. وعندما يحدث ذلك، يصبح الأمان أكثر منهجية وفعالية. لقد وثق عملاؤنا بنا لسنوات كأكبر مزود في العالم للبنية التحتية لتكنولوجيا المعلومات (IT) وخدمات الشبكات وكأكبر شركة في العالم في مجال الأمن السيبراني المؤسسي على السواء.

وقد تم تصميم Cisco Secure على مبدأ تحقيق أمان أفضل، لا أكثر. فهو يوفر نهجًا مبسطًا للأمان يركز على العميل ويضمن سهولة النشر والإدارة والاستخدام - وتناغم كل تلك العناصر معًا. دافعنا هو حقيقة أن الأشخاص وعملاءنا هم في صميم ما نفعله. ونتفهم أن العملاء يريدون تجاوز التعقيد والضجيج وأن يشعروا بالثقة في أمانهم، بالتركيز على النتائج. وهذا يتطلب التبسيط دون المبالغة في ذلك. منصتنا القائمة على السحابة من الأصل تعد قفزة عملاقة إلى الأمام في ذلك الإطار.

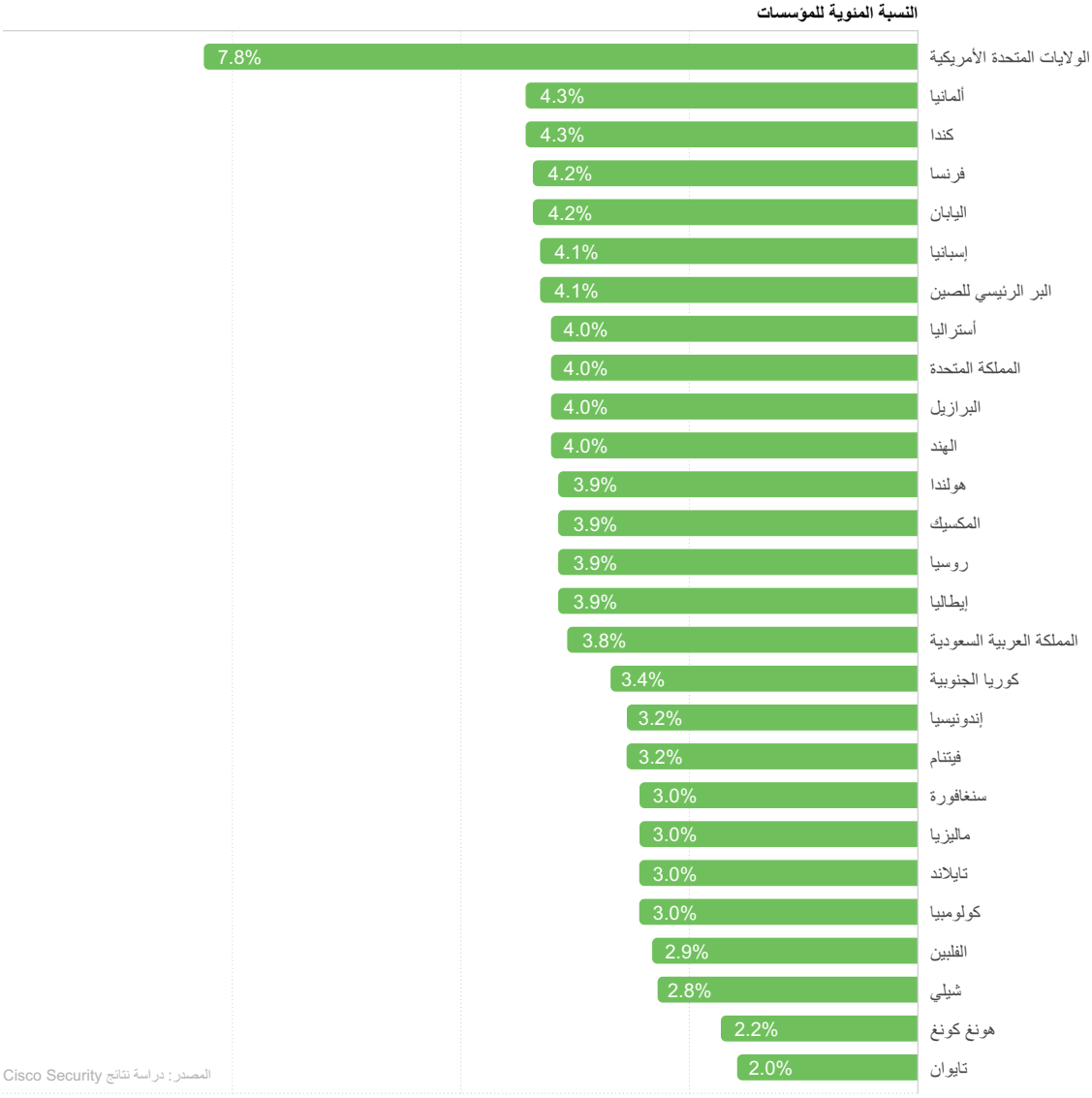
حيث نعمل على تمكين مجتمع الأمان من خلال الموثوقية والثقة بأنهم في مأمن من التهديدات الآن ومستقبلاً عند استخدام منصة Cisco SecureX. نحن نساعد 100 بالمائة من شركات Fortune 100 في تأمين العمل - أينما يكون - باستخدام المنصة الأوسع والأكثر تكاملاً. تعرّف على مزيد من المعلومات حول الكيفية التي تعمل بها على تبسيط التجارب وتسريع النجاح، وحماية المستقبل على cisco.com/go/secure.

الملحق: الخصائص السكانية للعينة الاستقصائية

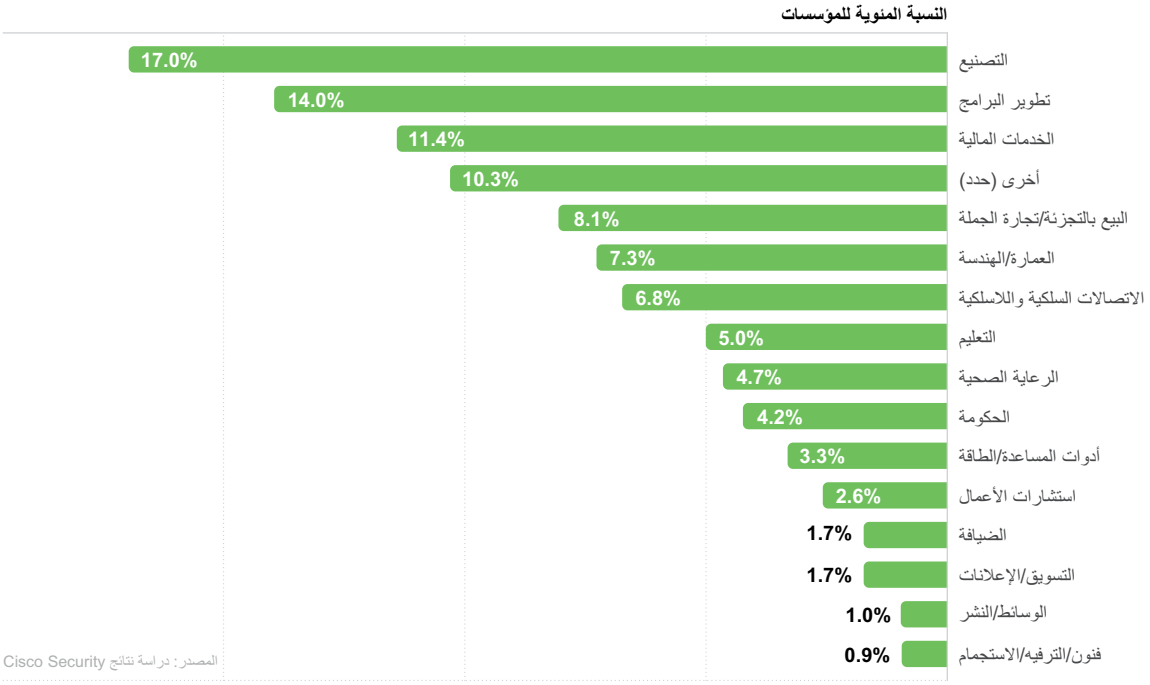
في هذا الملحق، قمنا بتضمين الخصائص السكانية للعينة من 5123 إجابة مؤهلة لهذا الاستطلاع. نأمل أن يساعد هذا التضمين أولئك الذين يحاولون تمييز تمثيلية هذه النتائج.



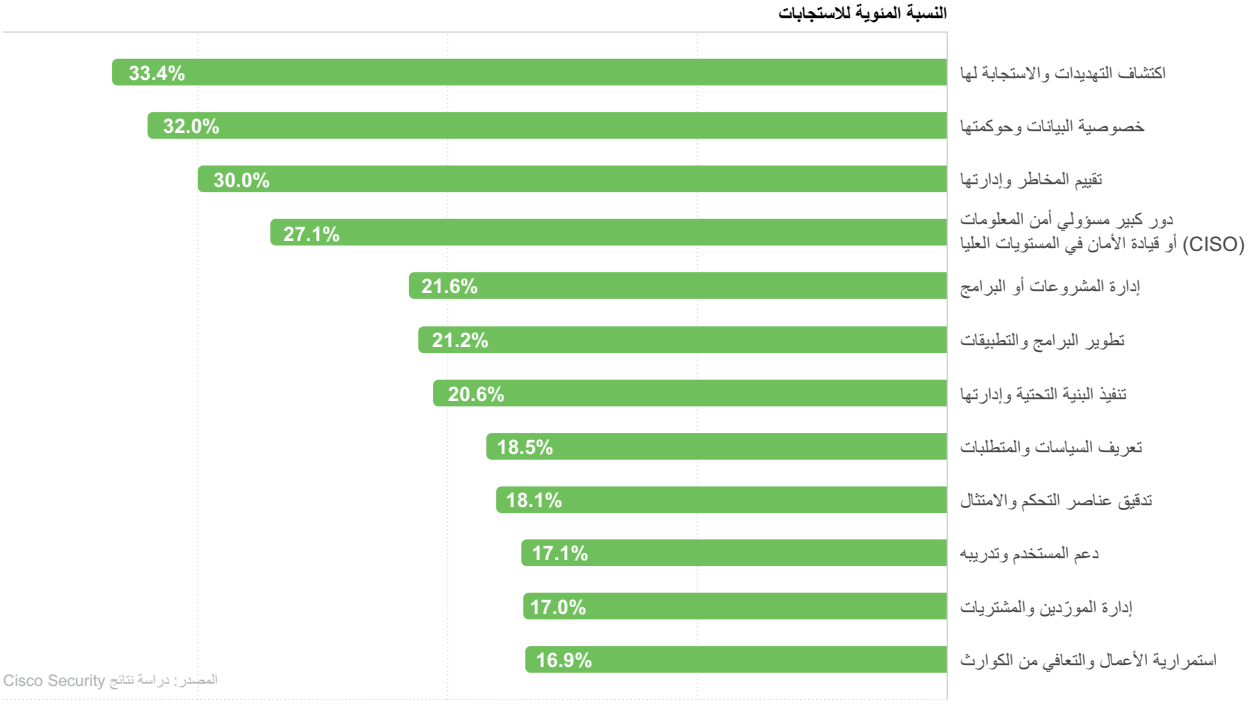
الشكل A1: عدد الموظفين للمؤسسات المشاركة



الشكل A2: الأسواق التي توجد بها مقار المؤسسات المشاركة



الشكل A3: الصناعات التي تمثلها المؤسسات المشاركة



الشكل A4: مسؤوليات الوظيفة الأساسية بين المشاركين في الاستطلاع

CISCO
SECURE

المقر الرئيسي في الأمريكتين
شركة Cisco Systems.
سان خوسيه، كاليفورنيا

المقر الرئيسي في دول آسيا والمحيط الهادئ
Cisco Systems (USA)، Pte. Ltd.
سنغافورة

المقر الرئيسي في أوروبا
Cisco Systems International BV
Amsterdam، The Netherlands

تم النشر في ديسمبر 2021

The bridge to possible