إطار المعهد الوطني الأمريكي للمعايير والتقنية NIST للأمن السيبراني (CSF)

مواءمة إطار المعهد الوطني للمعايير والتقنية للأمن السيبراني (NIST CSF) في سحابة AWS

يناير 2019

[التحول الآمن للحوسبة السحابية]

الإشعارات

هذه الوثيقة مُقدمة بغرض توفير المعلومات فقط. وهي تحتوي على عروض منتجات AWS وممارساتها الحالية في تاريخ إصدار هذه الوثيقة، والتي تخضع للتغيير دون إشعار مسبق. والعملاء مسؤولون عن تقييمهم المستقل للمعلومات الموجودة في هذه الوثيقة وعن أيّ استخدام لمنتجات AWS أو خدماتها، والتي تتاح كل منها "كما هي" بدون ضمان من أيّ نوع، سواء صريح أو ضمني. ولا تمثل هذه الوثيقة أيّ ضمانات أو إقرارات أو التزامات تعاقدية أو شروطًا أو تأكيدات من AWS أو أيٍّ من الشركات التابعة لها أو مورديها أو الجهات المرخصة التابعة لها. وتحكم اتفاقية AWS مسؤوليات AWS والتزاماتها نحو عملائها، وهذه الوثيقة لا تمثل جزءًا من أيّ اتفاقية مبرمة بين AWS وعملائها، كما لا تمثل تعديلاً لها.

المحتويات

نبذة مختصرة

يتزايد اعتراف الحكومات وقطاعات الصناعة والمنظمات في جميع أنحاء العالم بإطار الأمن السيبراني (CSF) كخط أساس موصى به للأمن السيبراني للمساعدة في تحسين إدارة مخاطر الأمن السيبراني ومرونة أنظمتها. وتقوم هذه الورقة بتقييم إطار المعهد الوطني للمعايير والتقنية للأمن السيبراني والعديد من عروض سحابة AWS، التي يمكن لعملاء القطاعين العام والتجاري استخدامها للمواءمة مع إطار NIST CSF، لتحسين وضع الأمن السيبراني لديك. كما توفر شهادة مصدقة من جهة خارجية تؤكد توافق خدمات AWS مع ممارسات إدارة المخاطر لإطار NIST CSF، مما يسمح لك بحماية بياناتك بشكل صحيح عبر AWS.

الجمهور المستهدف

هذه الوثيقة مخصصة للمهنيين في مجال الأمن السيبراني أو مسؤولي إدارة المخاطر أو غيرهم من صانعي القرار على نطاق المنظمة الذين ينظرون في كيفية تنفيذ إطار جديد للأمن السيبراني أو تحسين إطار قائم في منظمتهم. للحصول على تفاصيل حول كيفية إعداد خدمات AWS المحددة في هذه الوثيقة وفي مصنف العميل المرتبط (انظر الملحق "أ")، تواصل مع مهندس حلول AWS الخاص بك.

مقدمة

تم نشر إطار المعهد الوطني للمعايير والتقنية لتحسين الأمن السيبراني في البنية التحتية الحيوية (إطار المعهد الوطني للمعايير والتقنية للأمن السيبراني، أو CSF) في الأصل في فبراير 2014 استجابة إلى الأمر التنفيذي الرئاسي رقم "13636"، "تحسين بنية تحتية حيوية للأمن السيبراني، دعت إلى وضع إطار طوعي لمساعدة المنظمات على تحسين الأمن السيبراني وإدارة المخاطر ومرونة أنظمتهم.

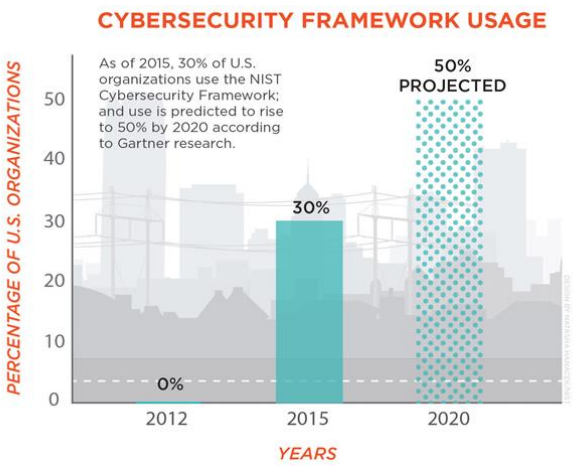
وقد تعاون المعهد مع مجموعة كبيرة من الشركاء من الحكومة والصناعة والأوساط الأكاديمية لأكثر من عام لوضع مجموعة من المبادئ التوجيهية والممارسات السليمة قائمة على توافق الآراء. وقد عزز قانون تعزيز الأمن السيبراني لعام 2014 شرعية إطار CSF وسلطته من خلال تقنينه واعتماده الطوعي كقانون، إلى أن أصدر الأمر التنفيذي الرئاسي بشأن "تعزيز الأمن السيبراني للشبكات الاتحادية والبنية التحتية الحيوية"، الموقع في 11 مايو 2017، تكليفًا باستخدام إطار CSF لجميع الكيانات الاتحادية في الولايات المتحدة.

وعلى الرغم من أن الهدف كان اعتماد المجموعة التأسيسية لتخصصات الأمن السيبراني، التي تُشكِّل إطار CSF، من قطاع البنية التحتية الحيوية، فإنها قد حظيت بدعم الحكومة والصناعة كخط أساس موصى به لاستخدامها من قبل أي منظمة، بغض النظر عن قطاعها أو حجمها. فالصناعة تتخذ بشكل متزايد إطار CSF مرجعًا لها كمعيار فعلي للأمن السيبراني.

أصدرت منظمة المعايير الدولية، في فبراير 2018، معيار "ISO/IEC 27103:2018 — تقنية المعلومات — تقنيات الأمن."
ويوفر هذا المعيار إرشادات لتنفيذ إطار للأمن السيبراني يستفيد من المعايير الحالية. وفي الواقع، فإن معيار **ISO 27103 يروج لنفس المفاهيم وأفضل الممارسات الواردة في إطار NIST CSF**؛ وعلى وجه التحديد، إطار يركز على النتائج الأمنية القائمة على خمس وظائف (التحديد، والحماية، والكشف، والاستجابة، والاسترداد) والأنشطة التأسيسية التي تتصل بالمعايير والاعتمادات والأطر الحالية.
ويمكن أن يساعد اعتماد هذا النهج المنظمات على تحقيق النتائج الأمنية، مع الاستفادة من كفاءات إعادة الاستخدام بدلاً من إعادة العمل.

وقد ذكرت شركة جارتنر أن إطار CSF يُستخدم من قبل حوالى 30 بالمائة من منظمات القطاع الخاص الأمريكية، ومن المتوقع أن يصل إلى 50 المائة بحلول عام 2020.[1] واعتبارًا من إصدار هذا التقرير، استخدم 16 قطاعًا من قطاعات البنية التحتية الحيوية في الولايات المتحدة إطار CSF، وقد قامت أكثر من 21 ولاية بتنفيذه.[2] وبالإضافة إلى منظمات البنية التحتية وغيرها من منظمات القطاع الخاص، تعمل بلدان أخرى، بما فيها إيطاليا وإسرائيل، على استخدام إطار CSF كأساس لمبادئها التوجيهية الوطنية المتعلقة بالأمن السيبراني.

ومنذ السنة المالية لعام 2016، تم تنظيم مقاييس قانون تحديث أمن المعلومات الفيدرالي (FISMA) للوكالة الفيدرالية للولايات المتحدة على أساس إطار CSF، والآن يشار إليها باسم



المرجع: ناتاشا هاناسك / المعهد الوطني للمعايير والتقنية NIST
https://www.nist.gov/industry-impacts/cybersecurity

"المعيار لإدارة مخاطر الأمن السيبراني والحد منها". ووفقا لتقرير قانون تحديث أمن المعلومات الفيدرالي للسنة المالية لعام 2016 المقدم إلى الكونغرس، قام مجلس المفتشين العامين المعني بالنزاهة والكفاءة بمواءمة مقاييس المفتشين العاميين مع الوظائف الخمس لإطار CSF، من أجل تقييم أداء الهيئة وتعزيز المقاييس والمعايير المتسقة والقابلة للمقارنة بين تقييمات كبير موظفي المعلومات والمفتشين العاميين.

وقد تجلى أكثر تطبيقات إطار CSF شيوعًا في ثلاثة سيناريوهات متميزة:

1. تقييم وضع الأمن السيبراني على نطاق المؤسسة ونضجه في المنظمة من خلال إجراء تقييم على أساس نموذج إطار CSF (الوضع الحالي) يحدد الوضع المطلوب للأمن السيبراني (الوضع المستهدف)، وتخطيط وتحديد أولويات الموارد والجهود لتحقيق الوضع المستهدف.
2. تقييم المنتجات والخدمات الحالية والمقترحة لتحقيق الأهداف الأمنية المتوائمة مع الفئات والفئات الفرعية لإطار CSF، لتحديد الثغرات في القدرات والفرص المتاحة للحد من التداخل / الازدواجية في القدرات من أجل تحقيق الكفاءة.
3. مرجع لإعادة هيكلة فرق الأمن والعمليات الأمينة والتدريب الأمني لديهم.

تحدد هذه الوثيقة القدرات الرئيسية لعروض خدمات AWS المتاحة عالميًا والتي يمكن للوكالات الفيدرالية والولايات والوكالات المحلية في الولايات المتحدة، وأصحاب البنية التحتية الحيوية العالمية والمشغلين، فضلا عن الشركات التجارية العالمية، الاستفادة منها من أجل المواءمة مع إطار CSF (أيّ الأمن في السحابة). كما توفر الدعم لتحقيق مواءمة خدمات سحابة AWS مع إطار CSF، كما أقره مُقيِّم جهة خارجية (أيّ أمن السحابة) على أساس

1 nist.gov/industry-impacts/cybersecurity.https://www
2 المرجع نفسه.

معايير الامتثال، بما في ذلك FedRAMP Moderate[3] وISO 9001/27001/27017/27018[4]. وهذا يعني أنه يمكنك أن تثق في أن خدمات AWS تحقق الأهداف الأمنية والنتائج المحددة في إطار CSF، وأنه يمكنك استخدام حلول AWS لدعم المواءمة الخاصة بك مع إطار CSF وأيّ معيار امتثال مطلوب. وبالنسبة للهيئات الفيدرالية في الولايات المتحدة، على وجه الخصوص، يمكن للاستفادة من حلول AWS تسهيل امتثالك لمقاييس الإبلاغ في قانون تحديث أمن المعلومات الفيدرالي. وهذا المزيج من النتائج من شأنه أن يتيح لك الثقة في أمان ومرونة البيانات الخاصة بك أثناء ترحيل الأعمال الحيوية إلى سحابة AWS.

الفوائد الأمنية لاعتماد إطار المعهد الوطني للمعايير والتقنية للأمن السيبراني

يقدم إطار CSF بنية بسيطة، ولكنها فعَّالة، تتكون من ثلاثة عناصر - الأساس، والطبقات، والأوضاع. يمثل الأساس مجموعة من ممارسات الأمن السيبراني، والنتائج، وضوابط الأمن التقنية والتشغيلية والإدارية (يشار إليها بالمراجع المعلوماتية) التي تدعم وظائف إدارة المخاطر الخمس - التحديد والحماية والكشف والاستجابة والاسترداد. وتُميز الطبقات قدرة المؤسسة ونضجها لإدارة ضوابط ووظائف إطار CSF، وتهدف الأوضاع إلى الوصول إلى حالات الأمن السيبراني "كما هي" و"المستقبلية" للمنظمة. وهذه العناصر الثلاثة مجتمعة تُمكِّن المنظمات من تحديد أولويات مخاطر الأمن السيبراني والتصدي لها بما يتفق مع احتياجات أعمالها ومهامها.

ومن المهم ملاحظة أن تنفيذ عناصر "الأساس" و"الطبقات" و"الأوضاع" هي مسؤولية المنظمة التي تعتمد إطار CSF (على سبيل المثال، هيئة حكومية، مؤسسة مالية، شركة تجارية مبتدئة، وما إلى ذلك). وتركز هذه الوثيقة على قدرات وحلول AWS التي تدعم "الأساس" الذي يمكن أن يُمكنك من تحقيق النتائج الأمنية (أيّ الفئات الفرعية) في إطار CSF. كما أنها تصف خدمات AWS التي تم اعتمادها بموجب "FedRAMP Moderate" و"ISO 9001/27001/27017/27018" بالتماشي مع إطار CSF.

ويشير "الأساس" إلى الضوابط الأمنية من المعايير المعتمدة على نطاق واسع والمعترف بها دوليا مثل "ISO/IEC 27001" و"NIST 800-53" وأهداف الرقابة للمعلومات والتقنية ذات الصلة (COBIT) وأفضل 20 ضابطًا من الضوابط الأمنية الحيوية لمجلس الأمن السيبراني (CCS) ومعايير ISA/ANSI-62443 – الأمان لأنظمة التحكم والأتمتة الصناعية. وفي حين أن هذه القائمة تمثل بعض المعايير الأكثر شهرة على نطاق واسع، فإن إطار CSF يشجع المنظمات على استخدام أيّ دليل ضوابط لتلبية احتياجاتها التنظيمية على أفضل وجه. وقد صُمم إطار CSF بحيث يكون ملائم للأحجام والقطاعات والبلدان؛ ولذلك ينبغي لمنظمات القطاعين العام والخاص أن تتأكد من إمكانية تطبيق إطار CSF، بغض النظر عن نوع الكيان أو موقع الدولة.

ويشجع إطار CSF المنظمات على استخدام أيّ دليل ضوابط لتلبية احتياجاتها التنظيمية على أفضل وجه. وقد صُمم إطار الأمن السيبراني بحيث يكون ملائم للأحجام والقطاعات والبلدان؛ ولذلك ينبغي لمنظمات القطاعين العام والخاص أن تتأكد من إمكانية تطبيق إطار CSF، بغض النظر عن نوع الكيان أو موقع الدولة.

---

3 البرنامج الفيدرالي لإدارة المخاطر والتخويل (FedRAMP) هو البرنامج الموحد للحكومة الأمريكية على النطاق الفيدرالي للحصول على إذن أمن الخدمات السحابية. تم تصميم نهج "التنفيذ مرة واحدة، والاستخدام عدة مرات" في البرنامج الفيدرالي لإدارة المخاطر والتخويل لتقديم فوائد كبيرة، مثل زيادة الاتساق والموثوقية في تقييم الضوابط الأمنية، وخفض التكاليف لمقدمي الخدمات وعملاء الهيئات، وتبسيط عمليات تقييم الترخيص المكرر عبر الهيئات التي تحصل على نفس الخدمة.

4 يُعتبر ISO 27001/27002 معيار أمان عالمي معتمد على نطاق واسع يحدد المتطلبات وأفضل الممارسات لنهج منتظم لإدارة معلومات الشركة والعملاء ويستند إلى تقييمات دورية للمخاطر تتناسب مع سيناريوهات التهديد المتغيرة باستمرار. ومعيار ISO 27018 هو مدونة قواعد ممارسات تركز على حماية البيانات الشخصية في السحابة. وهو يستند إلى معيار أمن المعلومات "ISO 27002"، ويقدم إرشادات التنفيذ بشأن ضوابط معيار "ISO 27002" المطبقة على معلومات التعريف الشخصية على السحابة العامة. كما يقدم مجموعة من الضوابط الإضافية والتوجيهات المرتبطة بها، التي تهدف إلى معالجة متطلبات حماية بيانات التعريف الشخصية على السحابة العامة التي لا تتناولها مجموعة الضوابط لمعيار "ISO 27002" الحالي.

حالات استخدام إنفاذ إطار المعهد الوطني للمعايير والتقنية للأمن السيبراني

الرعاية الصحية

أكملت وزارة الصحة و الخدمات البشرية الأمريكية تحديد قاعدة الأمان لقانون إخضاع التأمين الصحي لقابلية النقل والمساءلة لسنة 1996 (HIPAA)[5] لإطار NIST CSF. وبموجب قانون إخضاع التأمين الصحي لقابلية النقل والمساءلة، فإنه يجب على الكيانات المشمولة والشركاء التجاريين الالتزام بقاعدة الأمان لقانون إخضاع التأمين الصحي لقابلية النقل والمساءلة HIPAA، لضمان سرية وسلامة وتوافر المعلومات الصحية المحمية.[6] وحيث إن قانون إخضاع التأمين الصحي لقابلية النقل والمساءلة HIPAA لا يحتوي على مجموعة من الضوابط التي يمكن تقييمها أو عملية اعتماد رسمية، فإن الكيانات المشمولة والشركاء التجاريين، مثل AWS، مؤهلون لقانون إخضاع التأمين الصحي لقابلية النقل والمساءلة HIPAA استنادًا إلى التوافق مع الضوابط الأمنية لـ NIST 800-53 التي يمكن اختبارها والتحقق منها من أجل وضع الخدمات في قائمة الأهلية لقانون إخضاع التأمين الصحي لقابلية النقل والمساءلة. ويعزز التخطيط بين إطار NIST CSF وقاعدة الأمان لقانون إخضاع التأمين الصحي لقابلية النقل والمساءلة طبقة إضافية من الأمان، حيث إن التقييمات التي أجريت لفئات معينة من إطار NIST CSF قد تكون أكثر دقة وتفصيلاً من تلك التي أجريت بموجب شروط قاعدة الأمان ذات الصلة في قانون إخضاع التأمين الصحي لقابلية النقل والمساءلة.

الخدمات المالية

مجلس تنسيق قطاع الخدمات المالية الأمريكي[7] (FS-SCC) يتألف من 70 جمعية ومؤسسة ومرافق/بورصات للخدمات المالية، وقد وضع ملف خاص بالقطاع - نسخة مخصصة من إطار NIST CSF تتناول الجوانب الفريدة للقطاع ومتطلباته التنظيمية. ويعتبر ملف الأمن السيبراني الخاص بقطاع الخدمات المالية، الذي تمت صياغته بالتعاون مع الهيئات التنظيمية، وسيلة لمواءمة المتطلبات التنظيمية المتعلقة بالأمن السيبراني. فعلى سبيل المثال، وضع مجلس تنسيق قطاع الخدمات المالية الأمريكي فئة "استراتيجية إدارة المخاطر" في تسعة متطلبات تنظيمية مختلفة، وقرر أن اللغة والتعاريف، وإن كانت مختلفة، تتناول إلى حد كبير الهدف الأمني نفسه.

التبني الدولي

استفادت بلدان كثيرة، خارج الولايات المتحدة، من إطار NIST CSF لأغراض الاستخدام التجاري والعام. وكانت إيطاليا واحدة من أوائل الدول التي اعتمدت إطار NIST CSF، ووضعت استراتيجية وطنية للأمن السيبراني وفقًا للوظائف الخمس. وفي يونيو 2018، قامت المملكة المتحدة بمواءمة معيار الحد الأدنى للأمن السيبراني - الإلزامي لجميع الإدارات الحكومية - مع الوظائف الخمس. بالإضافة إلى ذلك، قامت إسرائيل واليابان بترجمة إطار NIST CSF إلى لغة كل منهما، مع قيام إسرائيل بإنشاء منهجية للدفاع السيبراني استنادًا إلى تكيفها الخاص مع إطار NIST CSF. وأجرت أوروغواي عملية تخطيط لإطار CSF وفقًا لمعايير ISO، من أجل تعزيز الروابط مع الأطر الدولية. وسويسرا واسكتلندا وأيرلندا وبرمودا أيضًا من بين قائمة البلدان التي تستخدم إطار NIST CSF لتحسين الأمن السيبراني والمرونة عبر منظمات القطاعين العام والتجاري.

---

5 يتضمن قانون إخضاع التأمين الصحي لقابلية النقل والمساءلة HIPAA أحكامًا لحماية أمن وخصوصية المعلومات الصحية المحمية. وتشمل المعلومات الصحية المحمية مجموعة كبيرة جدًا من البيانات الصحية التعريفية الشخصية والبيانات المتعلقة بالصحة، بما في ذلك معلومات التأمين والفواتير، وبيانات التشخيص، وبيانات الرعاية السريرية، ونتائج المختبرات، مثل الصور ونتائج الاختبارات. وتنطبق قواعد قانون إخضاع التأمين الصحي لقابلية النقل والمساءلة HIPAA على الكيانات المشمولة، والتي تشمل المستشفيات، ومقدمي الخدمات الطبية، والخطط الصحية التي يرعاها أصحاب الأعمال، ومرافق البحوث، وشركات التأمين التي تتعامل مباشرة مع المرضى وبياناتهم. شرط قانون إخضاع التأمين الصحي لقابلية النقل والمساءلة HIPAA لحماية المعلومات الصحية المحمية يمتد ليشمل الشركاء التجاريين أيضًا.

6 وتشمل المعلومات الصحية المحمية مجموعة كبيرة جدًا من البيانات الصحية التعريفية الشخصية والبيانات المتعلقة بالصحة، بما في ذلك معلومات التأمين والفواتير، وبيانات التشخيص، وبيانات الرعاية السريرية، ونتائج المختبرات، مثل الصور ونتائج الاختبارات.

7 https://www.fsscc.org/About-FSSCC

خدمات AWS التي تُمكِّن المواءمة مع إطار المعهد الوطني للمعايير والتقنية للأمن السيبراني CSF

يقدم هذا القسم لمحة عامة عن قدرات AWS التي يمكنك الاستفادة منها للمواءمة مع عنصر "الأساس" لإطار CSF لتحقيق "الأمان في السحابة". يقدم الملحق "أ" قائمة كاملة بخدمات AWS التي تتماشى مع الفئات والفئات الفرعية الوظيفية. ودمج هذه الأدوات كجزء من مجموعة التقنيات في مؤسستك يُمكن أن يساعد على إنشاء حلول مؤتمتة ومبتكرة وآمنة لتعزيز وضع الأمن السيبراني لديك.

وكل فئة فرعية للوظائف الرئيسية لإطار CSF قد تم تقييمها وتقديمها من قبل مُقيّم مستقل من جهة خارجية لاستيفاء المعايير التالية:

- مصممة بنا يتماشى مع خدمة (خدمات) AWS المطبقة
- خدمة (خدمات) AWS المطبقة المعتمدة بموجب "FedRAMP Moderate" و/أو "27018/27017/27001/9001 SO".

بالإضافة إلى تناول هذا القسم "للأمان في السحابة"، فإنه يحدد أيضًا كيفية مواءمة خدمات AWS مع إطار CSF لتحقيق "أمان السحابة". وتثبت شهادة الجهة الخارجية أن خدمات AWS تتوافق مع إطار CSF استنادًا إلى معايير الامتثال التي تم تعيينها إلى الفئات الفرعية لإطار CSF، وتحديدًا، " FedRAMP Moderate" و"27018/27017/27001/9001". وهذا يعني أنه يمكن أن تثق في أن خدمات AWS تحقق الأهداف الأمنية في إطار CSF، وأنه يمكنك استخدام حلول AWS لتحقيق أفضل الممارسات والنتائج للأمان والمرونة المحددة في إطار CSF.

بينما تعمل هذه الورقة كمصدر لتقديم إدارة مخاطر دورة الحياة التنظيمية التي تربط أهداف الأعمال والمهمات بأنشطة الأمن السيبراني، توفر AWS أيضًا مصادر أخرى لأفضل الممارسات للعملاء الذين ينقلون منظماتهم إلى السحابة (إطار AWS Cloud Adoption) والعملاء الذين يعملون على تصميم أو بناء أو تحسين الحلول على AWS (إطار Well-Architected).[8] وتوفر هذه الموارد أدوات تكميلية لدعم المنظمة في بناء ونضج برامجها وعملياتها ومما رساتها لإدارة مخاطر الأمن السيبراني في السحابة. وبشكل أكثر تحديدًا، يمكن وثيقة المعلومات لإطار NIST CSF إلى جانب أيٍّ من أدلة أفضل الممارسات هذه، حيث تكون بمثابة الأساس لبرنامج الأمان الخاص بك باستخدام إطار Cloud Adoption أو إطار Well- Architected كغطاء لتفعيل النتائج الأمنية لإطار CSF في السحابة.

وبالنسبة للعملاء الذين ينتقلون إلى السحابة، فإن إطار AWS Cloud Adoption يقدم إرشادات تدعم كل وحدة في مؤسستك بحيث تفهم كل منطقة كيفية تحديث المهارات وتكييف العمليات الحالية وإدخال عمليات جديدة للاستفادة القصوى من الخدمات التي تقدمها الحوسبة السحابية.
وقد نجحت آلاف المؤسسات في جميع أنحاء العالم في ترحيل أعمالها إلى السحابة، معتمدين على إطار AWS Cloud Adoption لتوجيه أعمالهم. توفر AWS وشركاؤنا الأدوات والخدمات التي يمكن أن تساعدك في كل خطوة على الطريق لضمان الفهم والانتقال الكاملين.

https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

8 يوثق إطار Well-Architected AWS أفضل الممارسات المعمارية لتصميم وتشغيل أنظمة موثوقة وآمنة وفعَّالة من حيث التكلفة في السحابة. فهو يوفر مجموعة من الأسئلة الأساسية التي تسمح لك بفهم ما إذا كانت بنية معينة تتماشى بشكل جيد مع أفضل الممارسات السحابية.
https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

التحديد	الحماية	الكشف	الاستجابة	الاسترداد
إدارة الأصول	التحكم في الوصول	الحالات الشاذة والأحداث	تخطيط الاستجابة	تخطيط الاسترداد
بيئة الأعمال	التوعية والتدريب	المراقبة الأمنية المستمرة	الاتصالات	التحسينات
الحوكمة	أمن البيانات	عمليات الكشف	التحليل	الاتصالات
تقييم المخاطر	إجراءات وعمليات حماية المعلومات		التخفيف	
استراتيجية تقييم المخاطر	الصيانة		التحسينات	
إدارة مخاطر سلسلة التوريد	الوقاية			
	التقنية			

الفئات الفرعية
(108 الأنشطة الأمنية القائمة على النتائج)

الوظيفة الأساسية لإطار CSF: التحديد

يتناول هذا القسم الفئات الست التي تُشكِّل وظيفة "التحديد": إدارة الأصول، وبيئة الأعمال، والحوكمة، وتقييم المخاطر، واستراتيجية إدارة المخاطر، وإدارة مخاطر سلسلة التوريد، التي "تعزز فهمًا تنظيميًا لإدارة مخاطر الأمن السيبراني للأنظمة والأشخاص والأصول والبيانات والقدرات". ويمكن العثور على مخطط تفصيلي لخدمات AWS إلى "الفئات الفرعية" الفردية وبيانات مسؤولية AWS والعملاء في الملحق "أ".

الفئات الفرعية للوظائف الرئيسية لإطار CSF للتحديد:

إدارة الأصول (ID.AM): يتم تحديد وإدارة البيانات والموظفين والأجهزة والأنظمة والمرافق التي تمكن المنظمة من تحقيق أغراض العمل بما يتفق مع أهميتها النسبية لأهداف العمل واستراتيجية المخاطر الخاصة بالمنظمة.

بيئة الأعمال (ID.BE): يتم فهم وتقديم الأولوية لمهمة المنظمة وأهدافها وأصحاب المصلحة وأنشطتها؛ وتُستخدم هذه المعلومات لإثراء الأدوار والمسؤوليات وقرارات إدارة المخاطر في مجال الأمن السيبراني.

الحوكمة (ID.GV): يتم فهم السياسات والإجراءات والعمليات لإدارة ومراقبة المتطلبات التنظيمية والقانونية والمخاطر والبيئية والتشغيلية للمنظمة، كما يتم إخبار إدارة مخاطر الأمن السيبراني.

تقييم المخاطر (ID.RA): تدرك المنظمة مخاطر الأمن السيبراني على العمليات التنظيمية (بما في ذلك المهمة أو الوظائف أو الصورة أو السمعة) والأصول التنظيمية والأفراد.

استراتيجية إدارة المخاطر (ID.RM): يتم تحديد أولويات المنظمة والقيود والتحمل للمخاطر والافتراضات، واستخدامها لدعم قرارات المخاطر التشغيلية.

إدارة مخاطر سلسلة التوريد (ID.SC): يتم تحديد أولويات المنظمة والقيود والتحمل للمخاطر والافتراضات، واستخدامها لدعم قرارات المخاطر المرتبطة بإدارة مخاطر سلسلة التوريد. وقد أنشأت المنظمة ونفذت عمليات لتحديد مخاطر سلسلة التوريد وتقييم هذه المخاطر وإدارتها.

مسئولية العملاء

تحديد أصول تقنية المعلومات وإدارتها هو الخطوة الأولى في حوكمة تقنية المعلومات وأمنها على نحو فعَّال، ومع ذلك فقد كان أحد أصعب التحديات. اعترف مركز أمن الإنترنت (CIS)[9] بالأهمية الأساسية لجرد الأصول، وقد قام بتخصيص جرد الأصول المادية غير المادية كضوابط رقم 1 و2 من أهم 20 ضابطًا لديه. ومع ذلك، كان من الصعب إجراء جرد دقيق لتقنية المعلومات، سواء من الأصول المادية أو الأصول غير المادية، والاحتفاظ به بالنسبة للمنظمات من جميع الأحجام والموارد. فحلول الجرد محدودة من حيث القدرة على تحديد جميع أصول تقنية المعلومات والإبلاغ عنها في جميع أنحاء المؤسسة لأسباب مختلفة، مثل تجزئة الشبكة التي تمنع الخدمة من "الرؤية" والإبلاغ من أجزاء مختلفة من شبكة المؤسسة، أو وكلاء برامج نقطة النهاية لا يتم نشرهم بشكل كامل أو لا يعملون بشكل كامل، وعدم التوافق عبر مجموعة كبيرة من التقنيات المتباينة. و مما يؤسف له أن الأصول "المفقودة" أو غير المحسوبة تشكل أكبر المخاطر. فإذا لم يتم تعقبها، فمن المرجح أنها لا تتلقى أحدث التصحيحات والتحديثات، ولا يتم استبدالها خلال تحديثات دورة الحياة، وقد يُسمح للبرامج الضارة باستغلال الأصول والاحتفاظ بها.

الانتقال إلى AWS يقدم ميزتين من المزايا الرئيسية التي يمكن أن تخفف من التحديات، مع الحفاظ على مخزونات الأصول في بيئة محلية. أولًا، تتحمل AWS المسؤولية وحدها عن إدارة الأصول المادية التي تُكوّن البنية التحتية لسحابة AWS. وهذا يمكن أن يقلل بشكل كبير من عبء إدارة الأصول المادية للعملاء لتلك الأعمال التي يتم استضافتها في AWS. وسيظل العميل مسؤولاً عن الاحتفاظ بمخزونات الأصول المادية للمعدات التي يحتفظ بها في بيئته (على سبيل المثال، مراكز البيانات، والمكاتب، وإنترنت الأشياء الموزع، والقوى العاملة المتنقلة، وما إلى ذلك). والميزة الثانية هي القدرة على تحقيق رؤية عميقة وجرد الأصول للأصول غير المادية المستضافة في حساب AWS الخاص بالعميل. قد يبدو ذلك وكأنه ادعاء جريء، ولكن يصبح الأمر واضحًا بسرعة لأنه لا يهم إذا تم تشغيل مثيل EC2 (الخادم الافتراضي) أو إيقاف تشغيله، وسواء تم تثبيت عامل نقطة النهاية وتشغيله، بغض النظر عن شريحة الشبكة التي عليها الأصل، أو أيّ عامل آخر. وسواء كنت تستخدم وحدة تحكم AWS كواجهة مرئية للتأشير والنقر، من خلال واجهة سطر الأوامر (CLI)، أو واجهة برمجة التطبيقات (API)، يمكن للعملاء الاستعلام والحصول على رؤية لأصول خدمة AWS. وهذا يقلل من عبء المخزون على العميل بالنسبة للبرامج التي يتم تثبيتها على مثيلات EC2 وماهية أصول البيانات التي يخزنها في AWS. وتمتلك AWS أيضًا خدمات يمكنها أداء هذه الإمكانية، مثل Amazon Macie،[10] والتي يمكنها تحديد البيانات المخزنة في أمازون S3 وتصنيفها وتسميتها وتطبيق القواعد عليها.

يمكن للمؤسسة التي تفهم رسالتها وأصحاب المصلحة لديها وأنشطتها الاستفادة من العديد من خدمات AWS لأتمتة العمليات وتعيين مخاطر الأعمال لأنظمة تقنية المعلومات، وإدارة أدوار المستخدمين. فعلى سبيل المثال، يمكن استخدام Identity and Access Management (IAM) لتعيين أدوار الوصول على أساس أدوار الأعمال للأشخاص والخدمات. ويمكن استخدام العلامات للخدمات والبيانات لتحديد أولويات المهام الآلية وإدراج قرارات المخاطر المحددة مسبقا، أو بوابات توقف لشخص لتقييم البيانات المقدمة وتحديد الاتجاه الذي ينبغي أن يتخذه النظام.

---

9 https://www.cisecurity.org/controls/

10 https://aws.amazon.com/macie/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CSecurity%7CMacie%7CUS%7CEN%7CText&sc_content=macie_e&sc_detail=aws%20macie&sc_category=Security&sc_segment=293651803573&sc_matchtype=e&sc_country=US&skwcid=AL!4422!3!293651803573!e!!g!!aws%20macie&ef_id=WMf1pwAAALNCC8Y3:20180918152026:s

الحوكمة هي "البطل المجهول" للأمن السيبراني. فهي تضع الأساس وتحدد المعيار للأشخاص والعمليات والتقنية. توفر AWS العديد من الخدمات والقدرات مثل AWS IAM، وAWS Organizations، وAWS Config، وAWS Systems Manager، وAWS Service Catalog، وغيرها من الخدمات التي يمكن للعملاء استخدامها لتنفيذ الحوكمة ومراقبتها وإنفاذها. يمكن للعملاء الاستفادة من امتثال AWS لأكثر من 50 معيارًا مثل FedRAMP، وISO، وPCI DSS[11]. وتوفر AWS معلومات حول المخاطر وبرنامج الامتثال لتمكين العملاء من دمج ضوابط AWS في إطار الحوكمة الخاص بهم. يمكن أن تساعد هذه المعلومات العملاء في توثيق إطار كامل للرقابة والحوكمة، مع إدراج AWS كجزء مهم من ذلك الإطار. تحدد الخدمات مثل Amazon Inspector نقاط الضعف التقنية التي يمكن إدخالها في وضع المخاطر وعملية الإدارة.[12] وتزيد الرؤية المحسنة التي توفرها السحابة من دقة وضع المخاطر للعميل، مما يسمح باتخاذ قرارات المخاطر استنادًا إلى بيانات أكثر جوهرية.

مسؤولية AWS

تحافظ AWS على إدارة صارمة لمراقبة الدخول من خلال توفير الوصول إلى مركز البيانات والمعلومات للموظفين والمقاولين الذين لديهم حاجة تجارية مشروعة لمثل هذه الامتيازات. وعندما لا يكون الموظف حاجة متعلقة بالعمل للحصول على هذه الامتيازات، يتم إلغاء وصوله على الفور، حتى لو استمر في العمل كموظف في أمازون أو Amazon Web Services. يتم تسجيل جميع عمليات الوصول الفعلية إلى مراكز البيانات من قبل موظفي AWS وتدقيقها بشكل روتيني. وتحد الضوابط الموجودة من الوصول إلى النظم والبيانات، وتقدم وصولاً إلى النظم، أو تقييد البيانات ورصدها. بالإضافة إلى ذلك، يتم عزل بيانات العملاء ومثيلات الخادم منطقيًا عن العملاء الآخرين بشكل افتراضي. ويتم مراجعة التحكم في وصول المستخدم صاحب الامتياز من قبل مدقق مستقل خلال عمليات تدقيق AWS SOC 1 وISO 27001 وPCI وFedRAMP.

تشمل أنشطة إدارة المخاطر في AWS دورة حياة تطوير النظام (SDLC)، والتي تتضمن أفضل الممارسات في هذه الصناعة ومراجعات التصميم الرسمية من قبل فريق أمن AWS، ونمذجة التهديدات، وإكمال تقييمًا للمخاطر.
وبالإضافة إلى ذلك، تخضع بيئة الرقابة في AWS لتقييمات منتظمة للمخاطر الداخلية والخارجية. كما تعمل AWS مع هيئات التصديق الخارجية ومدققي حسابات مستقلين لاستعراض واختبار بيئة الرقابة الشاملة في AWS.

لقد وضعت إدارة AWS خطة عمل استراتيجية تشمل تحديد المخاطر وتنفيذ الضوابط للتخفيف من المخاطر أو إدارتها. وتقوم إدارة AWS بإعادة تقييم خطة العمل الاستراتيجية مرتين كل سنة على الأقل. تتطلب هذه العملية من الإدارة أن تحدد المخاطر في مجالات مسؤوليتها وأن تنفذ التدابير المناسبة المصممة للتصدي لتلك المخاطر. وبالإضافة إلى ذلك، تخضع بيئة الرقابة في AWS لتقييمات مختلفة للمخاطر الداخلية والخارجية. فقد قامت فرق الامتثال والأمن في AWS بإنشاء إطار عمل وسياسات لأمن المعلومات تستند إلى إطار أهداف الرقابة للمعلومات والتقنية ذات الصلة (COBIT)، ودمجت بشكل فعَّال إطار ISO 27001 المستند إلى ضوابط "ISO 27002"، ومبادئ خدمات الثقة للمعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) ،

11 معيار أمان بيانات صناعة بطاقات الدفع (المعروف أيضًا باسم PCI DSS) هو معيار أمان معلوماتي يتم إدارته من قِبل مجلس معايير الأمان لـ PCI (https://www.pcisecuritystandards.org/), والذي تم تأسيسه بواسطة American Express وDiscover Financial Services وJCB International وMasterCard Worldwide وVisa Inc. ينطبق معيار PCI DSS على جميع الكيانات التي تقوم بتخزين بيانات حامل البطاقة (CHD) و/أو بيانات التوثيق الحساسة (SAD) أو معالجتها أو نقلها بما في ذلك التجار ومعالجي المعلومات والمشترين والمصدرين ومقدمي الخدمات.

12 https://aws.amazon.com/inspector/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CSecurity%7CInspector%7CUS%7CEN%7CText&sc_content=aws_inspector_e&sc_detail=aws%20inspector&sc_category=Security&sc_segment=293647559947&sc_matchtype=e&sc_country=US&sc_kwcid=AL!4422!3!293647559947!e!!g!!aws%20inspector&ef_id=WMf1pwAAALNCC8Y3:20180918153103:s

و PCI DSS v3.2، والمنشور رقم " 800-53 Rev 4" للمعهد الوطني للمعايير والتقنية NIST (الضوابط الأمنية الموصى بها لنظم المعلومات الفيدرالية). تحافظ AWS على سياسة الأمان، وتقدم التدريب الأمني للموظفين، وتقوم بمراجعة أمان التطبيقات. وهذه المراجعات تُقيِّم سرية البيانات ونزاهتها وتوافرها، فضلاً عن توافقها مع سياسة أمن المعلومات. تقوم خدمة AWS Security بمسح جميع عناوين IP لنقطة نهاية الخدمة التي تستخدم الإنترنت بشكل منتظم للبحث عن نقاط الضعف (لا تتضمن هذه المسوحات مثيلات العملاء). وتُخطر خدمة Security AWS الأطراف المناسبة لمعالجة أيّ نقاط ضعف محددة. وبالإضافة إلى ذلك، تُجري شركات أمنية مستقلة تقييمات منتظمة للتهديدات التعرض للمخاطر الخارجية. وتُصنَّف النتائج والتوصيات الناتجة عن هذه التقييمات وتُقدَّم إلى قيادة AWS. تُجرى هذه الفحوصات بطريقة معينة من أجل صحة البنية التحتية الأساسية لنظام AWS واستدامتها ولا يقصد بها استبدال عمليات مسح نقاط الضعف الأمنية الخاصة بالعميل المطلوبة لتلبية متطلبات الامتثال المحددة الخاصة بهم.

تحتفظ AWS باتفاقات رسمية مع الموردين الرئيسيين من الأطراف الخارجية، وتُنفِّذ آليات إدارة العلاقات المناسبة، بما يتماشى مع علاقتها بالأعمال. وتتم مراجعة عمليات إدارة الجهات الخارجية في AWS من قبل مدققين مستقلين كجزء من الامتثال المستمر لـ AWS مع SOC و ISO 27001 . وتمشيا مع معايير ISO 27001، يتم تعيين مالك لأصول أجهزة AWS، ويتم تتبعها ومراقبتها من قبل موظفي AWS مع أدوات إدارة المخزون الخاص بـ AWS. فريق سلسلة التوريد والمشتريات في AWS يُحافظ على العلاقات مع جميع موردي AWS. يرجى الرجوع إلى معايير ISO 27001؛ الملحق "أ"، الحقل 8 للحصول على مزيد من التفاصيل. وقد تم التحقق من صحة AWS واعتمادها من قبل مدقق مستقل لتأكيد التوافق مع معيار شهادة ISO 27001.

الوظيفة الأساسية لإطار CSF: الحماية

يتناول هذا القسم الفئات الست التي تُشكِّل وظيفة "الحماية": التحكم في الوصول، والتوعية والتدريب، وأمن البيانات، وإجراءات وعمليات حماية المعلومات، والصيانة، والتقنية
الوقائية. كما يُسلط الضوء على حلول AWS التي يمكنك الاستفادة منها للتوافق مع هذه الوظيفة. ويمكن العثور على مخطط تفصيلي لخدمات AWS إلى "الفئات الفرعية" الفردية وبيانات مسؤولية AWS والعملاء في الملحق "أ".

الفئة الفرعية للوظائف الرئيسية لإطار CSF للحماية:

إدارة الهوية والتوثيق والتحكم في الوصول (PR.AC): يقتصر الوصول إلى الأصول المادية وغير المادية والمرافق المرتبطة بها على المستخدمين المصرح لهم والعمليات والأجهزة المصرح لها، ويتم إدارته بما يتفق مع المخاطر المقدرة للوصول غير المصرح به إلى المعاملات والأنشطة المصرح بها.

التوعية والتدريب (PR.AT): يتم تزويد موظفي المؤسسة وشركائها بالتثقيف في مجال الأمن السيبراني وتدريبهم على أداء واجباتهم ومسؤولياتهم المتعلقة بالأمن السيبراني بما يتماشى مع السياسات والإجراءات والاتفاقات ذات الصلة.

أمن البيانات (PR.DS): تتم إدارة المعلومات والسجلات (البيانات) بما يتوافق مع استراتيجية المخاطر الخاصة بالمؤسسة لحماية سرية المعلومات وسلامتها وتوافرها.

إجراءات وعمليات حماية المعلومات (PR.IP): يتم الحفاظ على السياسات الأمنية (التي تتناول الغرض والنطاق والأدوار والمسؤوليات والالتزام الإداري والتنسيق بين الكيانات التنظيمية)، والعمليات والإجراءات واستخدامها لإدارة حماية نظم المعلومات والأصول.

الصيانة (PR.MA): تتم صيانة وإصلاح نظم المعلومات والرقابة الصناعية بما يتفق مع السياسات والإجراءات.

التقنية الوقائية (PR.PT): يتم إدارة الحلول الأمنية التقنية لضمان أمن ومرونة الأنظمة والأصول، بما يتفق مع السياسات والإجراءات والاتفاقات ذات الصلة.

مسئولية العملاء

عند النظر إلى تحقيق الأهداف الأمنية الثلاثة المتمثلة في السرية والنزاهة والتوافر، قد يكون من الصعب جدًا تحقيق الهدف الثالث في بيئة محلية مع مركز بيانات واحد أو اثنين فقط. وهذه هي إحدى أكبر الفوائد لمزودي الخدمة السحابية الفائقة، ولـ AWS على وجه الخصوص، وذلك بسبب بنية البنية التحتية. ويمكنك توزيع التطبيق الخاص بك عبر مناطق متعددة لتوافر الخدمات، والتي تكون مناطق عزل الأخطاء غير المادية داخل المنطقة. إذا تم تصميم بياناتك وتطبيقاتك بشكل صحيح مع إمكانات إدارة السعة المحسنة والتحجيم التلقائي، فلن تتأثر بياناتك أو تطبيقاتك من توقف مركز بيانات واحد. وإذا كنت تستفيد من جميع مناطق توافر الخدمات في منطقة (حيث يوجد ثلاثة أو أكثر)، فقد لا يزال فقدان اثنين من مراكز البيانات لا يمثل أيّ تأثير على التطبيق الخاص بك. وبالمثل، تقوم خدمات، مثل خدمة تخزين Amazon Simple Storage Service (S3) تلقائيًا بنسخ البيانات الخاصة بك إلى ما لا يقل عن ثلاثة مناطق لتوافر الخدمات في المنطقة لضمان التوافر بنسبة 99.99 ٪ واستمرارية البيانات بنسبة 99.999999999%.

يمكن تحقيق السرية من خلال التشفير عند الراحة والتشفير أثناء النقل باستخدام خدمات تشفير AWS، مثل تشفير Elastic Block Store (EBS)، وتشفير S3، وتشفير قاعدة البيانات الشفافة لخادم RDS SQL Server وRDS Oracle، وبوابة VPN Gateway، أو التشفير باستخدام حل التشفير الموجود لديك.

تدعم AWS تشفير TLS/SSL لجميع نقاط النهاية لـ API والقدرة على إنشاء أنفاق VPN لحماية البيانات أثناء النقل. كما توفر AWS خدمة إدارة المفاتيح ووحدة أمان الأجهزة المخصصة لتشفير البيانات أثناء الراحة. يمكنك اختيار تأمين بياناتك باستخدام قدرات AWS المقدمة، أو استخدام أدوات الأمان الخاصة بك.

ويمكن تسهيل السلامة بمجموعة متنوعة من الوسائل. فخدمتي Amazon CloudWatch وAmazon CloudTrail لديهما عمليات تحقق من السلامة، ويمكن للعملاء استخدام التوقيعات الرقمية لسجلات ومكالمات API، والمجموع الاختياري MD5 يمكن استخدامه في أمازون S3، ومن ثَمَّ هناك العديد من الحلول الخارجية من شركائنا. توفر Amazon Config حتى سلامة بيئة AWS الخاصة بالعميل من خلال مراقبة التغييرات.

داخل بيئة AWS الخاصة بالعميل، فإن خدمات AWS مثل AWS IAM، وAWS Cognito و(AWS Single Sign-On (SSO ، وAWS Cloud Directory وAWS Directory Service، والمزايا مثل Multi-Factor Authentication، تتيح لك تنفيذ وإدارة وتأمين ومراقبة والإبلاغ عن هويات المستخدم ومعايير المصادقة وحقوق الوصول.

أنت مسؤول عن تدريب الموظفين لديك والمستخدمين النهائيين على سياسات وإجراءات إدارة البيئة الخاصة بك. للحصول على التدريب الفني، تقدم AWS ويقدم شركاؤنا في التدريب تدريبًا شاملاً لمختلف الأدوار، مثل مهندسي الحلول، وموظفي SysOps، والمطورين، وفرق الأمن.[13]

مسؤولية AWS

تستخدم AWS مفهوم أقل الامتيازات، حيث يتم منح صلاحيات الموظفين على أساس حاجة العمل والمسؤوليات الوظيفية، وتوفير الوصول المؤقت القائم على الأدوار فقط إلى الموارد والبيانات المطلوبة في ذلك الوقت.

وتوفر AWS الوصول إلى مركز البيانات المادي فقط للموظفين المعتمدين. يجب على جميع الموظفين الذين يحتاجون إلى الوصول إلى مركز البيانات التقدم أولاً بطلب الوصول وتقديم مبرر عمل صالح. يتم تلبية هذه الطلبات على أساس مبدأ أقل الامتيازات، حيث يجب أن تحدد الطلبات إلى أيّ طبقة من مركز البيانات يحتاج الفرد إلى الوصول إليها، وتكون محددة زمنيًا. ويتم مراجعة الطلبات والموافقة عليها من قبل الموظفين المعتمدين، ويتم إلغاء الوصول بعد انتهاء الوقت المطلوب. وبمجرد منح الإذن، يقتصر الأفراد على المناطق المحددة في الأذونات الممنوحة لهم.

يتم طلب وصول جهة خارجية من قبل موظفي AWS المعتمدين، الذين يجب عليهم التقدم بطلب للحصول على وصول جهة خارجية وتقديم مبرر عمل صالح. يتم تلبية هذه الطلبات على أساس مبدأ أقل الامتيازات، حيث يجب أن تحدد الطلبات إلى أيّ طبقة من مركز البيانات يحتاج الفرد إلى الوصول إليها، وتكون محددة زمنيًا. وتتم الموافقة على هذه الطلبات من قبل الموظفين المعتمدين، ويتم إلغاء الوصول بعد انتهاء وقت الطلب. وبمجرد منح الإذن، يقتصر الأفراد على المناطق المحددة في الأذونات الممنوحة لهم. ويجب على أيّ شخص يُمنح شارة الزائر أن يقدم بطاقة هوية عند وصوله إلى الموقع وأن يتم تسجيل الدخول ومرافقته من قبل موظفين معتمدين.

نفذت AWS سياسات وإجراءات رسمية وموثقة للتوعية الأمنية والتدريب

---

13 يمكن الاطلاع على التدريب المتاح على شبكة الإنترنت وفي الفصول الدراسية على: https://aws.amazon.com/training. هناك أيضا العديد من الكتب التي تغطي جوانب عديدة من نظام AWS، ويمكن الاطلاع عليها على: https://www.amazon.com من خلال البحث عن "AWS". يمكن الاطلاع على المستندات التقنية لـ AWS على: https://aws.amazon.com/whitepapers

للموظفين والمقاولين، الذي يتناول الغرض والنطاق والأدوار والمسؤوليات والالتزام الإداري والتنسيق بين الكيانات التنظيمية والامتثال.

توثق شهادات FedRAMP و ISO 27001 الخاصة بـ AWS بالتفصيل السياسات والإجراءات التي تقوم بموجبها AWS بتشغيل وصيانة ومراقبة واعتماد ونشر وإعداد التقارير ورصد جميع التغييرات التي تطرأ على بيئتها وبنيتها التحتية، فضلاً عن كيفية توفير AWS للدعم الاحتياطي والاستجابة لحالات الطوارئ للبنية التحتية المادية. بالإضافة إلى ذلك، توثق الشهادات بالتفصيل الطريقة التي تتم بها الموافقة على جميع الصيانة عن بعد لخدمات AWS، وكيفية تنفيذها وتسجيلها ومراجعتها، وذلك لمنع الوصول غير المصرح به. كما أنها تتناول الطريقة التي تقوم بها AWS لتنظيف الوسائط وتدمير البيانات. تستخدم AWS المنتجات والإجراءات التي تتماشى مع المبادئ التوجيهية لتنظيف الوسائل بالمنشور الخاص NIST 800-88. وأنت أيضًا مسؤول عن إعداد السياسات والعمليات والإجراءات لحماية البيانات.

لدعم متطلبات الفوترة والصيانة، يتم تعيين مالك لأصول أجهزة AWS، ويتم تتبعها ومراقبتها بأدوات إدارة المخزون الخاص بـ AWS. ويتم تنفيذ إجراءات صيانة مالك أصول AWS من خلال استخدام أداة خاصة مع عمليات التحقق المحددة التي يجب أن تكتمل وفقًا لجدول الصيانة الموثق. يقوم مراجعو حسابات الجهة الخارجية باختبار ضوابط إدارة الأصول AWS من خلال التحقق من أن مالك الأصول موثق وأن حالة الأصول يتم فحصها بصريًا وفقًا لسياسة إدارة الأصول الموثقة.

ويُمكن أيضًا أن تُحسن خدمات AWS إلى حد كبير إدارة وأداء صيانة الأنظمة لعملائنا. أولاً، استنادًا إلى البنية التحتية لـ AWS التي تمت مناقشتها أعلاه مع منطقة توافر الخدمات، يمكن للتطبيق الذي تم تصميمه للتوافر العالي عبر المناطق المتعددة لتوافر الخدمات أن يسمح لك بفصل أنشطة الصيانة. ويمكنك أن تأخذ الأصول داخل منطقة توافر الخدمات خارج الشبكة للصيانة دون التأثير على أداء التطبيق العام، حيث إن الأصول المكررة في المناطق الأخرى لتوافر الخدمات تتوسع وتلتقط وتتحمل العبء. يُمكن إكمال منطقة توافر خدمات واحدة في كل مرة صيانة، ويمكن أتمتة الصيانة مع بوابات الإيقاف والإبلاغ حسب الحاجة. بالإضافة إلى ذلك، يمكن تحويل هياكل كاملة من بيئة DevTest (زرقاء) إلى بيئة عمليات (خضراء)، والعكس بالعكس، حينما تكون هذه الطريقة مطلوبة.

الوظيفة الأساسية لإطار CSF: الكشف

يتناول هذا القسم الفئات الثلاث التي تُشكِّل من وظيفة "الكشف": الحالات الشاذة والأحداث، والمراقبة الأمنية المستمرة، وعمليات الكشف. نحن نلخص حلول AWS الرئيسية التي يُمكنك الاستفادة منها للتوافق مع هذه الوظيفة. ويمكن العثور على مخطط تفصيلي لخدمات AWS إلى "الفئات الفرعية" الفردية وبيانات مسؤولية AWS والعملاء في الملحق "أ".

الفئة الفرعية للوظائف الرئيسية لإطار CSF للكشف:

الحالات الشاذة والأحداث (DE.AE): يتم الكشف عن النشاط الشاذ في الوقت المناسب وفهم التأثير المحتمل للأحداث.

المراقبة الأمنية المستمرة (DE.CM): يتم رصد نظام المعلومات والأصول على فترات لتحديد أحداث الأمن السيبراني والتحقق من فعَّالية تدابير الحماية.

عمليات الكشف (DE.DP): يتم الاحتفاظ بعمليات وإجراءات الكشف واختبارها لضمان الوعي المناسب للأحداث الشاذة في الوقت المناسب.

مسئولية العملاء

القدرة على جمع الأحداث ذات الصلة بالأمن وتوليفها والتنبيه بها هي أمر أساسي لأيّ برنامج إدارة مخاطر الأمن السيبراني. وتوفر الطبيعة التي تحركها واجهة برمجة التطبيقات للتقنية السحابية مستوى جديد من الرؤية والأتمتة لم يكن ممكنًا من قبل. فمع كل إجراء تم اتخاذه ونتج عنه سجل تدقيق واحد أو أكثر، توفر AWS كمًا هائلًا من معلومات الأنشطة المتاحة للعملاء ضمن هيكل حسابهم. ومع ذلك، فإن حجم البيانات يمكن أن يُشكِّل تحدياتها الخاصة.
فكما يقول المثل، فإن "العثور على إبرة في كومة قش" هو مشكلة حقيقية، ولكن السعة والقدرات التي توفرها السحابة تكون مناسبة تمامًا لحل هذه التحديات؛ فمع البنية التحتية المناسبة لمعالجة السجلات والأتمتة وتحليل البيانات، من الممكن تحقيق الكشف عن الأحداث الحرجة والاستجابة لها في وقت شبه حقيقي، مع تصفية النتائج الإيجابية الزائفة والمخاطر المنخفضة/المقبولة.

تتمتع AWS بالعديد من الخدمات التي يمكن استخدامها كجزء من استراتيجية شاملة للعمليات الأمنية للرصد المستمر والكشف عن التهديدات. فعلى المستوى الأساسي، هناك خدمات مثل AWS CloudTrail[14] لتسجيل جميع مكالمات API، حيث يمكن توقيع السجلات رقميًا وتشفيرها، ثم تخزينها في حاوية أمازون S3 آمنة. فسجلات التدفق للسحابة الخاصة الافتراضية (VPC)[15] تعمل على رصد أنشطة الشبكة للدخول والخروج من السحابة الخاصة الافتراضية لديك. وتوجد أيضًا Amazon CloudWatch[16]، التي تراقب بيئة AWS لديك وتقدم تنبيهات مشابهة لنظام إدارة أحداث المعلومات الأمنية (SIEM)، ويمكن استيعابه في النظام المحلي لإدارة أحداث المعلومات الأمنية لدى العميل.

وهناك أيضًا خدمات متقدمة أخرى، مثل Amazon GuardDuty[17] التي تربط النشاط داخل بيئة AWS لديك مع معلومات التهديدات من مصادر متعددة توفر سياق مخاطر إضافية وكشف الحالات الشاذة. وخدمة Amazon Macie هي خدمة متقدمة أخرى يمكنها تحديد البيانات الحساسة وتصنيفها وتسميتها وتتبع موقعها والوصول إليها. وقد يختار بعض العملاء الاستفادة من خدمات الذكاء الاصطناعي (AI) لدى AWS وتعلم الآلة (ML) لنمذجة وتحليل بيانات السجلات.

مسؤولية AWS

توفر AWS تنبيهات في وقت شبه حقيقي عندما تُظهر أدوات رصد AWS مؤشرات على التعرض للخطر أو التعرض المحتمل للخطر، استنادًا إلى آليات الإنذار الدنيا التي تحددها فرق الأمن وخدمة AWS.
تربط AWS المعلومات المكتسبة من أنظمة الرصد المادية وغير المادية لتعزيز الأمن على أساس الحاجة.
فعند تقييم واكتشاف المخاطر، تقوم أمازون بتعطيل الحسابات التي تعرض الاستخدام الشاذ الذي يطابق خصائص الجهات الفاعلة السيئة.

ويتم تدريب موظفي AWS على كيفية التعرف على الحوادث الأمنية المشتبه بها ومكان الإبلاغ عنها. وعند الاقتضاء، يتم إبلاغ السلطات المعنية بالحوادث.
تحتفظ AWS بصفحة ويب لنشرات الأمان الخاصة بـ AWS[18] لإعلام العملاء بالأحداث المتعلقة بالأمان والخصوصية التي تؤثر على خدمات AWS. يمكن للعملاء الاشتراك في موجز RSS لنشرات الأمان للإبقاء على الاطلاع بالإعلانات الأمنية على صفحة ويب نشرات الأمان. يحافظ فريق دعم العملاء

14 https://aws.amazon.com/cloudtrail/
15 https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
16 https://aws.amazon.com/cloudwatch/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CManagement%20Tools%7CCloudWatch%7CUS%7CEN%7CText&sc_content=cloudwatch_e&sc_detail=aws%20cloudwatch&sc_category=Management%20Tools&sc_segment=293615620998&sc_matchtype=e&sc_country=US&s_kwcid=AL!4422!3!293615620998!e!!g!!aws%20cloudwatch&ef_id=WMf1pwAAALNCC8Y3:20180918153820:s
17 https://aws.amazon.com/guardduty/
18 https://aws.amazon.com/security/security-bulletins

على صفحة ويب لوحة معلومات سلامة الخدمات[19] لتنبيه العملاء إلى أيّ مشكلات تؤثر بشكل عام على التوافر.

الوظيفة الأساسية لإطار CSF: الاستجابة

يتناول هذا القسم الفئات الخمس التي تُشكِّل وظيفة "الاستجابة": تخطيط الاستجابة، والاتصالات، والتحليل، وعمليات التخفيف، والتحسينات. كما نلخص أيضًا حلول AWS الرئيسية التي يُمكنك الاستفادة منها للتوافق مع هذه الوظيفة. ويمكن العثور على مخطط تفصيلي لخدمات AWS إلى "الفئات الفرعية" الفردية وبيانات مسؤولية AWS والعملاء في الملحق "أ".

الفئة الفرعية للوظائف الرئيسية لإطار CSF للاستجابة:

تخطيط الاستجابة (RS.RP): يتم تنفيذ عمليات وإجراءات الاستجابة والاحتفاظ بها، لضمان الاستجابة في الوقت المناسب لأحداث الأمن السيبراني المكتشفة.

التخفيف (RS.MI): يتم تنفيذ الأنشطة لمنع توسع الحدث، والتخفيف من آثاره، والقضاء على الحادث.

الاتصالات(RS.CO): تنسق أنشطة الاستجابة مع أصحاب المصلحة الداخليين والخارجيين، حسب الاقتضاء، لتشمل الدعم الخارجي من هيئات إنفاذ القانون.

التحليل (RS.AN): يُجري التحليل لضمان الاستجابة الكافية ودعم أنشطة الاسترداد.

التحسينات (RS.IM): تحسين أنشطة الاستجابة التنظيمية بإدراج الدروس المستفادة من أنشطة الاكتشاف/الاستجابة الحالية والسابقة.

مسئولية العملاء

الوقت بين الكشف والاستجابة هو أمر بالغ الأهمية. وتعمل خطط الاستجابة المنفذة بشكل جيد والقابلة للتكرار على تقليل التعرض والاسترداد السريع. كما تتيح الأتمتة الذي تم تمكينها بواسطة السحابة تنفيذ كتب الخطط المتطورة كمدونة قواعد مع أوقات استجابة أسرع بكثير.

فبمجرد وضع علامة على مثيل أمازون EC2، على سبيل المثال، يمكن للأتمتة عزل المثيل، وأخذ لقطة تحليلية، وتثبيت أدوات التحليل، وربط المثيل المشتبه به بمحطة عمل تحليل الأدلة، وقطع تذكرة لمحلل أمن سيبراني. وتعمل الإمكانات المذكورة أدناه على تسهيل إنشاء عمليات مؤتمتة لإضافة السرعة والاتساق إلى عمليات الاستجابة للحوادث. علاوة على ذلك، تسمح لك هذه الأدوات بالاحتفاظ بسجل الاتصالات لاستخدامها في مراجعة ما بعد الحدث.

وفي حين أن السحابة توفر قدرات لتبسيط وتعجيل جمع المعلومات ونشرها، فيوجد دائمًا عنصرًا بشريًا يشارك في تنسيق الاستجابة. يتطلب تحليل الأمن السيبراني إجراء تحقيق، وأدلة، وفهمًا للحادث؛ ويتطلب ذلك بالضرورة مستوى معين من التفاعل البشري. على الرغم من أن خدمات AWS لا توفر تحليلات مباشرة للحوادث، إلا أنها تقدم خدمات للمساعدة في تنفيذ عملية رسمية وتقييم مدى التأثير.

---

19 http://status.aws.amazon.com/

مسؤولية AWS

لقد نفذت AWS برنامجًا وسياسة رسمية موثقة للاستجابة للحوادث. وتتناول السياسة الغرض والنطاق والأدوار والمسؤوليات والالتزام الإداري.

تستخدم AWS نهجًا من ثلاث مراحل لإدارة الحوادث:

1. مرحلة التنشيط والإخطار
2. مرحلة الاسترداد
3. مرحلة إعادة البناء

لضمان فعَّالية خطة إدارة الحوادث لدى AWS، تُجري AWS اختبار الاستجابة للحوادث؛ ويوفر هذا الاختبار تغطية ممتازة لاكتشاف العيوب وحالات الفشل والعيوب غير المعروفة مسبقًا. وبالإضافة إلى ذلك، فإنه يسمح لفرق الأمن والخدمة في أماوقت لاختبار النظم لمعرفة التأثير المحتمل على العملاء وإعداد مزيد من الموظفين للتعامل مع الحوادث، مثل الكشف والتحليل، والاحتواء، والمكافحة، والاسترداد، والأنشطة اللاحقة للحوادث.

يتم تنفيذ خطة اختبار الاستجابة للحوادث سنويًا، بالاقتران مع خطة الاستجابة للحوادث. ويتم مراجعة تخطيط إدارة الحوادث في AWS والاختبار ونتائج الاختبار من قبل مدققي حسابات جهة خارجية.

الوظيفة الأساسية لإطار CSF: الاسترداد

يتناول هذا القسم الفئات الثلاث التي تُشكِّل وظيفة "الاسترداد": تخطيط الاسترداد، والتحسينات، والاتصالات. كما نلخص أيضًا حلول AWS الرئيسية التي يُمكنك الاستفادة منها للتوافق مع هذه الوظيفة. ويمكن العثور على مخطط تفصيلي لخدمات AWS إلى "الفئات الفرعية" الفردية وبيانات مسؤولية AWS والعملاء في الملحق "أ".

الفئة الفرعية للوظائف الرئيسية لإطار CSF للاسترداد:

تخطيط الاسترداد (RC.RP): يتم تنفيذ عمليات وإجراءات الاسترداد والحفاظ عليها لضمان استعادة النظم أو الأصول المتضررة من أحداث الأمن السيبراني في الوقت المناسب.

التحسينات (RC.IM): تحسين عمليات وتخطيط الاسترداد بإدراج الدروس المستفادة في الأنشطة المستقبلية.

الاتصالات (RC.CO): يتم تنسيق أنشطة الاستعادة مع الأطراف الداخلية والخارجية، مثل مراكز التنسيق، ومقدمي خدمات الإنترنت، وأصحاب الأنظمة المهاجمة، والضحايا، وفرق CSIRT الأخرى، والبائعين.

مسئولية العملاء

يتحمل العملاء مسؤولية تخطيط واختبار وتنفيذ عمليات الاسترداد لتطبيقاتهم وبياناتهم للحفاظ على استمرارية أعمالهم. وقد يأتي سبب انقطاع الخدمة من العديد من المصادر المختلفة. وتوفر خدمات AWS العديد من القدرات المتقدمة للتعافي الذاتي والاسترداد الآلي. على سبيل المثال، فإن استخدام مجموعات التكيف التلقائي عبر المناطق المتعددة لتوافر الخدمات يُتيح للبنية التحتية مراقبة صحة مثيلات EC2 واستبدال مثيل فاشل بسرعة بـ Amazon Machine Image (AMI) جديدة.

بالإضافة إلى ذلك، يمكن لخدمات Amazon CloudWatch وAWS Lamda وقدرات الخدمة/الخدمات الأخرى أتمتة إجراءات الاسترداد لتشمل كل شيء، بدءًا من نشر بيئة وتطبيق AWS بالكامل، وتجاوز الفشل إلى منطقة AWS مختلفة، واستعادة البيانات من النسخ الاحتياطية، وأكثر من ذلك.

وأخيرا، فإن الإجراءات التي تنطوي على العلاقات العامة، وإدارة السمعة، وإبلاغ أنشطة الاسترداد تتعلق بكيفية تعامل المنظمة مع الحدث الذي أثر على بيئتها، والذي يكون، في هذه الحالة، هو العميل.

مسؤولية AWS

البنية التحتية المرنة لدى AWS، والأتمتة الموثوق بها، والعمليات المنضبطة، والأشخاص الاستثنائيون قادرون على التعافي من الأحداث بسرعة كبيرة وبالحد الأدنى (إن وجد) من التعطيل لعملائنا.

تقدم خطة استمرارية الأعمال لدى AWS تفصيلاً للنهج ثلاثي المراحل الذي طورته AWS لاستعادة وإعادة تشكيل بنية AWS التحتية:

- مرحلة التنشيط والإخطار
- مرحلة الاسترداد
- مرحلة إعادة البناء

يضمن هذا النهج أن AWS تؤدي جهود استرداد النظام وإعادة التشكيل بتسلسل منهجي، مما يحقق أكبر قدر من فعَّالية جهود الاسترداد وإعادة التشكيل وتقليل وقت انقطاع النظام بسبب الأخطاء وحالات الإغفال.

وتمتلك AWS ببيئة مراقبة أمنية منتشرة في كل مكان في جميع المناطق. وتم تصميم كل مركز بيانات وفقًا للمعايير المادية والبيئية والأمنية في تكوين نشط دائمًا، حيث يتم استخدام نموذج تكرار "n+1" لضمان توفر النظام في حالة فشل المكون. تحتوي المكونات (N) على مكون واحد مستقل للنسخ الاحتياطية على الأقل (+1)، وبالتالي فإن مكون النسخ الاحتياطي يكون نشطًا في العملية، حتى إذا كانت كافة المكونات الأخرى تعمل بشكل كامل. ومن أجل القضاء على نقاط الفشل الفردية، يتم تطبيق هذا النموذج في جميع أنحاء AWS، بما في ذلك تنفيذ مركز البيانات والشبكة. فجميع مراكز البيانات تكون على الإنترنت وتخدم حركة المرور؛ لا يوجد مركز بيانات "محلي". ففي حالة الفشل، توجد قدرة كافية لتمكين حركة المرور من أن تكون متوازنة للمواقع المتبقية.

مواءمة خدمات AWS مع إطار CSF

قامت AWS بتقييم مواءمة خدماتنا السحابية مع إطار CSF لإثبات "أمن السحابة". وفي عالم متزايد الترابط، فمن الضروري تطبيق ممارسات قوية لإدارة مخاطر الأمن السيبراني لكل نظام مترابط لحماية سرية البيانات وسلامتها وتوافرها. يتوقع عملاؤنا من القطاعين العام والخاص أن نستخدم الأمن الأفضل في فئته لحماية خدماتنا السحابية والبيانات التي تتم معالجتها وتخزينها في تلك الأنظمة. ومن أجل حماية البيانات والأنظمة بفعَّالية عالية، لا يمكن أن يكون الأمان أمرًا ثانويًا، بل هو جزء لا يتجزأ من إدارة دورة حياة الأنظمة لدينا. وهذا يعني أن الأمان يبدأ في المرحلة 0 (أيّ بدء تشغيل الأنظمة)، ويتم تقديمه بشكل مستمر كجزء أساسي من نموذج تقديم الخدمات لدينا.

حلول AWS المتاحة اليوم لعملائنا من القطاعين العام والتجاري، حسبما تم التحقق من صحتها من قبل مُقيّم جهة خارجية لدينا، تتماشى مع إطار المعهد الوطني للمعايير والتقنية للأمن السيبراني.

وتحتفظ كل من هذه الخدمات بالاعتماد الحالي بموجب "FedRAMP Moderate" و/أو "ISO 27001". عند نشر حلول AWS، يمكن للمنظمات أن تتأكد من أن خدمات AWS تدعم أفضل ممارسات إدارة المخاطر المحددة في إطار CSF ويمكنها الاستفادة من هذه الحلول لمواءمتها الخاصة مع إطار CSF.

وتمارس AWS نهجًا صارمًا يستند إلى المخاطر لأمن خدماتنا وحماية بيانات العملاء. فنحن نطبق عمليتنا الخاصة لضمان الأمن الداخلي لخدماتنا، والتي تُقيّم فعَّالية الضوابط الإدارية والفنية والتشغيلية اللازمة للحماية من التهديدات الأمنية الحالية والناشئة التي تؤثر على مرونة خدماتنا. ويخضع مقدمو الخدمات السحابية التجارية الفائقة، مثل AWS، بالفعل لمتطلبات أمنية قوية في شكل شهادات أمنية خاصة بقطاع معين، ووطنية ودولية (على سبيل المثال FedRAMP، و ISO 27001 ، وPCI DSS، وSOC، إلخ) تعالج بشكل كافٍ مخاوف المخاطر التي يحددها عملاء القطاعين العام والخاص في جميع أنحاء العالم.

وتتبنى AWS نهج أمان عالٍ عبر جميع خدماتنا على أساس نهج "الذروة" الخاص بنا لجميع عملائنا. وهذا يعني أننا نأخذ أعلى مستوى تصنيف لنقل البيانات وتخزينها في الخدمات السحابية الخاصة بنا ونطبق نفس مستويات الحماية على جميع خدماتنا وعلى جميع عملائنا. ومن ثم، يتم ترتيب هذه الخدمات للحصول على شهادة اعتماد وفقًا لأعلى حد امتثال، والتي تترجم إلى العملاء الذين يستفيدون من مستويات مرتفعة من الحماية لبياناتهم التي تتم معالجتها وتخزينها في السحابة لدينا. حلول AWS المتاحة اليوم لعملائنا من القطاعين العام والتجاري، حسبما تم التحقق من صحتها من قبل مُقيّم جهة خارجية لدينا، تتماشى مع الوظائف الأساسية لإطار CSF. وتحتفظ كل من هذه الخدمات بالاعتماد الحالي بموجب "FedRAMP Moderate" و/أو "ISO 27001 ". عند نشر حلول AWS، يمكن للمنظمات أن تتأكد من أن خدمات AWS تدعم أفضل ممارسات إدارة المخاطر المحددة في إطار CSF ويمكنها الاستفادة من هذه الحلول لمواءمتها الخاصة مع إطار CSF. يرجى الرجوع إلى الملحق "ب" للاطلاع على خطاب شهادة الجهة الخارجية.

الخاتمة

تُقر كيانات القطاعين العام والخاص بالقيمة الأمنية في اعتماد إطار NIST CSF في بيئاتها. وتوجه الهيئات الاتحادية في الولايات المتحدة، على وجه الخصوص، إلى مواءمة ممارساتها في مجال إدارة مخاطر الأمن السيبراني والإبلاغ عنها مع إطار CSF. فحكومات الولايات الأمريكية والحكومات المحلية الأمريكية والحكومات غير الأمريكية ومشغلو البنية التحتية الحيوية والمنظمات التجارية يُقيّمون مدى توافقهم مع إطار CSF، فهم بحاجة إلى الأدوات والحلول المناسبة لتحقيق وضع آمن ومتوافق للمخاطر التنظيمية والنظام.

يمكنك تعزيز وضع الأمن السيبراني لديك من خلال الاستفادة من AWS كجزء من تقنية مؤسستك لبناء حلول مؤتمتة ومبتكرة وآمنة لتحقيق نتائج الأمان في إطار CSF. ويمكنك اكتساب طبقة إضافية من الأمان بالتأكد من أن خدمات AWS تستخدم أيضًا ممارسات إدارة المخاطر السليمة المحددة في إطار CSF، والتي تم التحقق من صحتها من قبل مُقيّم جهة خارجية.

الملحق "أ" - مصفوفة مسؤوليات العميل وخدمات AWS للمواءمة مع إطار CSF

يُساعد جدول بيانات مصفوفة مسؤوليات العميل وخدمات AWS للمواءمة مع إطار CSF العملاء على تخطيط مواءمتهم مع إطار NIST CSF. ويقع جدول البيانات هذا تحت علامة التبويب المصنفات (Workbooks) داخل قسم الموارد (Resources) في موقع AWS Compliance.

الملحق "ب" - التحقق من مُقيِّم الجهة الخارجية

Kratos SecureInfo
,Sullyfield Circle 14130
Suite H
20151 Chantilly, VA
هاتف: 1-888-677-9351
www.kratossecureinfo.com

١٩ سبتمبر ٢٠١٨
Amazon Web Services
عناية: جنيفر غراي
الأمن - استراتيجية النمو | كبير المديرين، تصميم الخدمات

عزيزتي السيدة غراي،
بناء على طلبك، توليت مهمة مراجعة المتطلبات المنصوص عليها في إطار المعهد الوطني للمعايير والتقنية للأمن السيبراني، الإصدار 1.1، بتاريخ 16 أبريل 2018، وقمت بتحليل المتطلبات المبينة في نص وظيفة وتنظيم إطار NIST CSF فيما يتعلق بـ AWS والبنى المرجعية المرتبطة للحوسبة السحابية. وهذه المتطلبات تُدرج في متطلبات الرقابة الأمنية التي وضعها معهد NIST، الموثقة في المنشور الخاص NIST Special Publication (SP) 800-53.

وبالنسبة لمراجعتي، قمت بالتحقق من اقتباسات إطار NIST CSF التي تحدد متطلبات الرقابة الأمنية بالمنشور "SP 800-53 ". بالإضافة إلى ذلك، قمت بمراجعة خدمات AWS التي خضعت لاعتمادات "FedRAMP Moderate" و" ISO 9001 / 27001 / 27017 / 27018 " التي تلبي متطلبات الاقتباس أو الرقابة المتاحة للعملاء للنشر. وأثناء التحقق من صحة الخدمة، حددت الاقتباسات الإضافية التي قد تحتوي على خدمات محددة النطاق التي تلبي المتطلبات. وجميع الخدمات الموصى بإدراجها تم التحقق من صحتها وفقًا لنطاق اعتمادات FedRAMP Moderate وISO الخاصة بـ AWS.

وكشفت نتائج التحليل أنه على الرغم من عدم الحاجة إلى إطار امتثال معين في هذا الوقت، فقد استوفت AWS القصد من هذه الاقتباسات من خلال خدمات AWS في نطاق FedRAMP وISO.

واستنادًا إلى تحليلي لمصنف تخطيط الوظائف الأساسية لإطار CSF الذي قدمته AWS وفهمنا لبيئة AWS، فإن رأي Kratos Secureinfo هو أن AWS قد أثبتت بشكل كاف مواءمة امتثالها لإطار NIST CSF من خلال تنفيذ الضوابط الأمنية ذات الصلة في FedRAMP وISO.

إذا كان لديكم أيّ أسئلة حول مراجعة التصميم التي أجريتها، الرجاء الاتصال بي مباشرة على (571)-308-3397 أو عن طريق البريد الإلكتروني على Emily.Cummins@KratosSecureinfo.com.

مع خالص التقدير،
إميلي كامينز
كبير مستشاري الأمن
Kratos SecureInfo