الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1060

(2021/06)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن المعلومات والشبكات – إدارة الأمن

إطار لإنشاء مركز دفاع سيبراني وتشغيله

التوصية ITU-T X.1060

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	**X.1050–X.1069**
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	X.1140–X.1149
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1360–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1389
أمن سجل الحسابات الموزع	X.1400–X.1429
أمن سجل الحسابات الموزع	X.1430–X.1449
البروتوكول الأمني (2)	X.1450–X.1459
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولّد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
أمن شبكات الجيل الخامس	X.1800–X.1819

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1060

إطار لإنشاء مركز دفاع سيبراني وتشغيله

ملخص

تُعرِّف التوصية ITU-T X.1060 مركز الدفاع السيبراني (CDC) على أنه كيان له دور مركزي في منظمة ما لمواجهة مخاطر الأمن السيبراني. ويرد وصف العمليات الثلاث للبناء والإدارة والتقييم التي ينبغي لمركز الدفاع السيبراني تنفيذها عملياً في شكل إطار. وترد أيضاً الخدمات التي ينبغي أن تكون لدى المنظمة من أجل تنفيذ تدابير أكثر تحديداً للأمن السيبراني.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1060	2012-06-29	17	11.1002/1000/14721

مصطلحات أساسية

مركز دفاع سيبراني، فريق الاستجابة للحوادث الحاسوبية، مركز العمليات الأمنية (SOC).

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

مقدمة

لمخاطر الأمن السيبراني في أي منظمة تأثيرات كبيرة على أنشطتها العامة. والمخاطر التي تواجهها المنظمات هي التغيرات البيئية، من المنظورين الاجتماعي والعملي على السواء، والضغوط الخارجية من خلال اللوائح والتهديدات المتزايدة. وبالتالي، فإن الإدارة العليا، بصفتها الإدارة التنفيذية (CxO)، مسؤولة عن إدارة الضوابط للمؤسسة بأكملها لمواجهة هذه المخاطر والتغييرات. وكأحد الجوانب المهمة لتنفيذ الضوابط في مجال الأمن السيبراني، من المتوقع أن يتولى منصب القيادة فيما يتعلق بوضع ومراقبة السياسات الأمنية بما يتماشى مع أهداف العمل كبير مسؤولي الأمن (CSO) أو كبير مسؤولي أمن المعلومات (CISO). ومن أجل تنفيذ التدابير الأمنية عملياً، من الضروري وجود كيان يدعم أنشطة كبير مسؤولي الأمن أو كبير مسؤولي أمن المعلومات مع الإدارة الإستراتيجية على المستوى التنظيمي. ويوصف هذا الكيان في هذه التوصية بأنه مركز الدفاع السيبراني (CDC).

وتوفر هذه التوصية إطاراً لإنشاء وإدارة مركز الدفاع السيبراني وتقييم فعاليته. ويبين الإطار الكيفية التي ينبغي أن يحدد بها مركز الدفاع السيبراني وينفذ خدمات الأمن لتحقيق أمن المنظمة. ويساعد هذا الإطار المنظمة على مواجهة مخاطر الأمن السيبراني.

إطار لإنشاء مركز دفاع سيبراني وتشغيله

1 مجال التطبيق

تحدد هذه التوصية إطاراً للمنظمات لإنشاء مركز دفاع سيبراني (CDC) وإدارته وتقييم فعاليته. ويبين الإطار الكيفية التي ينبغي أن يحدد بها مركز الدفاع السيبراني وينفذ خدمات الأمن لتحقيق أمن المنظمة.

وهذه التوصية مخصصة لأولئك المسؤولين عن الأمن على مستوى الإدارة العليا للمنظمة، مثل كبير مسؤولي الأمن (CSO) أو كبير مسؤولي أمن المعلومات (CISO) ومشرفي الأمن الذين يساعدونهم.

2 المراجع

تضم توصيات قطاع تقييس الاتصالات المذكورة أدناه وغيرها من المراجع أحكاماً تؤلف، من خلال الإشارات الواردة إليها في هذا النص، أحكاماً لهذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة؛ يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. ولا تضفي الإشارة إلى وثيقة ما في هذه التوصية على تلك الوثيقة في حد ذاتها صفة التوصية.

لا توجد.

3 التعاريف

1.3 مصطلحات معرّفة في مكان آخر

تستخدم هذه التوصية التعريف التالي المعرّف في مصادر أخرى:

1.1.3 الاستعانة بمصادر خارجية (outsourcing) [b-ITU-T X.1053]: عندما تسند شركة ما واحدة أو أكثر من عملياتها و/أو وظائفها الداخلية لشركة خارجية. والاستعانة بمصادر خارجية ينقل موارد الشركة إلى شركة خارجية ويحتفظ بالقدرة على إدارة العلاقة مع العمليات المسندة لمصادر خارجية.

2.3 مصطلحات معرّفة في هذه التوصية

تعرّف هذه التوصية المصطلح التالي:

1.2.3 مركز الدفاع السيبراني (cyber defence centre) (CDC): كيان داخل المنظمة يقدم خدمات الأمن لإدارة مخاطر الأمن السيبراني المتعلقة بأنشطتها التجارية.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

APT تهديد مستمر متقدم *(Advanced Persistent Threat)*

CDC مركز الدفاع السيبراني *(Cyber Defence Centre)*

CISO كبير مسؤولي أمن المعلومات *(Chief Information Security Officer)*

CSIRT فريق الاستجابة للحوادث الأمنية الحاسوبية *(Computer Security Incident Response Team)*

CSO كبير مسؤولي الأمن *(Chief Security Officer)*

CxO الإدارة التنفيذية *(C-suite)*

IDS نظام كشف الاقتحام *(Intrusion Detection System)*

IPS نظام منع الاقتحام *(Intrusion Prevention System)*

IT تكنولوجيا المعلومات *(Information Technology)*

SIEM إدارة المعلومات والأحداث الأمنية *(Security Information and Event Management)*

SLA اتفاق مستوى الخدمة *(Service Level Agreement)*

WAF جدر حماية تطبيقات الويب *(Web Application Firewall)*

5 الاصطلاحات

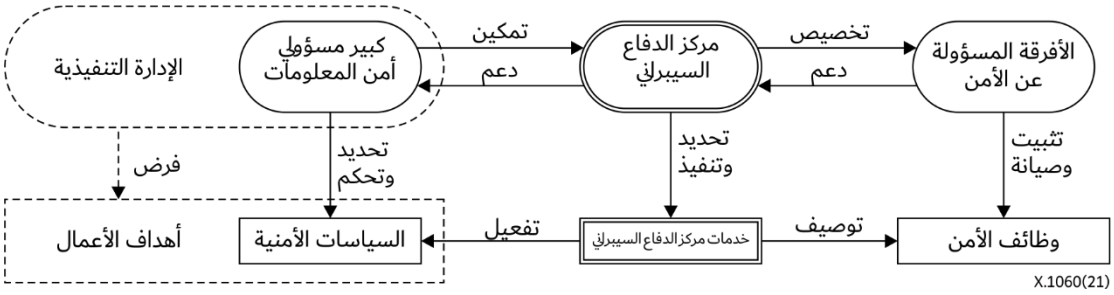
لا توجد.

6 هيكل هذه التوصية

في هذه التوصية، يرد شرح مفهوم مركز الدفاع السيبراني في الفقرة 7. وتقدم الفقرة 8 نظرة عامة على إطار إنشاء وتشغيل مركز الدفاع السيبراني. ويرد وصف الإطار بالتفصيل في الفقرات اللاحقة: عملية إنشاء مركز الدفاع السيبراني (الفقرة 9)؛ وعملية إدارة مركز الدفاع السيبراني (الفقرة 10)؛ وعملية تقييم مركز الدفاع السيبراني (الفقرة 11). وفي الفقرة 12، يرد وصف شامل لخدمات الأمن التي يقدمها مركز الدفاع السيبراني كواحدة من أفضل الممارسات، ويرد وصف كل خدمة بمزيد من التفصيل في الملحق A.

7 نظرة عامة على مركز الدفاع السيبراني

تعمل المنظمات على إنجاح أعمالها. ومن أجل إدارة المخاطر التي تتعرض لها الأنشطة التجارية، يقوم كبير مسؤولي أمن المعلومات (CISO) بصياغة السياسات الأمنية، لا سيما من منظور الأمن السيبراني. ومركز الدفاع السيبراني هو كيان ينفذ السياسات الأمنية، وعلى وجه التحديد خدمات مركز الدفاع السيبراني، التي تتكون من أنشطة أمنية يتم تنفيذها من قبل أفرقة مسؤولة عن الأمن. وقد تحدد خدمات مركز الدفاع السيبراني وظائف الأمن كقدرات لنظام يقوم بأداء المعالجة المتعلقة بالأمن. ويوضح الشكل 1 أصحاب المصلحة وأدوارهم في تشغيل مركز الدفاع السيبراني.



الشكل 1 – أصحاب المصلحة وأدوارهم في تشغيل مركز الدفاع السيبراني

وطبقاً لحجم ونوع المنظمة، قد يكون مركز الدفاع السيبراني وحدة مستقلة أو لجنة أو فريقاً مصغراً. وبغض النظر عن شكله، ينبغي أن يكون موجوداً ككيان في المنظمة، وأن يكون لديه السلطة والموارد اللازمة لتنفيذ خدمات الأمن لتمكين المنظمة من التمتع بالأمن. وينبغي أن تتماشى خدمات الأمن هذه مع السياسات الأمنية وأن تضمن جودة الأنشطة الأمنية؛ وينبغي الاتفاق على مستوى كل خدمة صراحةً من خلال ترتيب موثق، مثل اتفاق مستوى الخدمة (SLA). يتم تقييم الجودة الشاملة لإحدى خدمات أمن المركز CDC من خلال التدابير المحددة في الفقرة 4.9.

8 إطار إنشاء وتشغيل مركز الدفاع السيبراني

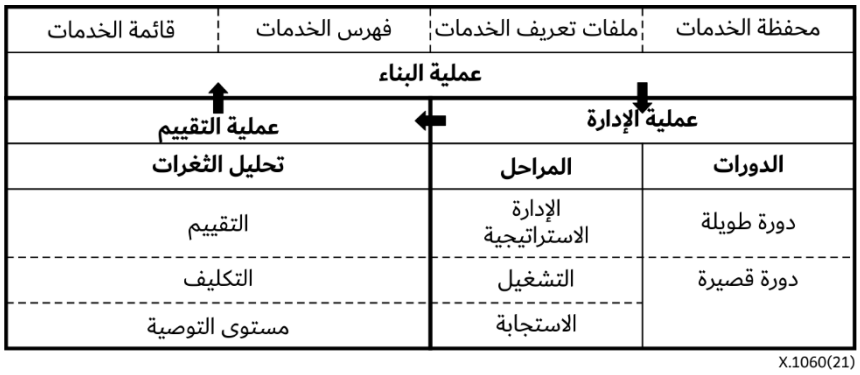
يعرض الشكل 2 إطار عمل إطار إنشاء وتشغيل مركز الدفاع السيبراني. ويتضمن الإطار ثلاث عمليات: البناء والإدارة والتقييم. ولضمان أمن المنظمة، ينبغي إنشاء مركز الدفاع السيبراني وإدارته بشكل مناسب. وينبغي أيضاً تقييمه في الوقت المناسب وبطريقة منتظمة وتحسينه باستمرار. ويمكّن هذا الإطار المنظمة من رعاية الأنشطة الأمنية.

وفي عملية البناء، ينبغي النظر في الأنشطة الأمنية في المنظمة. ويرد سرد أفضل الممارسات لخدمات أمن المركز CDC في الملحق A. ويمكن لأي منظمة إنشاء فهرس الخدمات الخاص بها عن طريق تحديد الخدمات من القائمة وإضافة الخدمات الخاصة بالمنظمة. وينبغي أن تنشئ كل خدمة في الفهرس أيضاً ملف تعريف يتضمن: المالك (الملاك)، والأدوار والمسؤوليات، ونوع تكليفات الخدمة (من الداخل، أو من خلال الاستعانة بمصادر خارجية أو توليفة من الإثنين). وبمجرد إنشاء ملف تعريف الخدمة، ينبغي تحديد الدرجة الحالية والمستهدفة لكل خدمة من خدمات المركز CDC من أجل عملية التقييم.

وتتكون عملية الإدارة من ثلاث مراحل ودورتين. حيث تدير مرحلة الإدارة الإستراتيجية الأنشطة العامة لمركز الدفاع السيبراني، وتدير مرحلة التشغيل العمل الروتيني المتعلق بالمراقبة والتحليل، وتدير مرحلة الاستجابة الاستجابات لحالات الطوارئ. وتجري هذه المراحل في دورات قصيرة وطويلة؛ حيث تتطلب مرحلتا التشغيل والاستجابة قرارات في الوقت المناسب على دورات قصيرة. وفي الوقت نفسه، ينبغي أن تنظر الإدارة الإستراتيجية في التحسين طويل الأجل جنباً إلى جنب مع المخرجات من الدورات القصيرة في دورة طويلة. وعادةً ما يتطلب التحسين طويل الأجل اتخاذ قرارات بشأن الاستثمارات التجارية الجديدة والتعديلات الجذرية في هياكل النظام.

وتقوم عملية التقييم بتقييم فهرس خدمات المركز CDC وملف التعريف والمحفظة الخاصة بكل خدمة (انظر الشكل 4)، والتي يجب تقييمها بشكل موضوعي في كل وقت ممكن.

وتنبغي مراجعة نتائج التقييم وإظهارها في جميع عمليات المركز CDC الثلاث. وينبغي إنشاء دورة متكررة من عمليات البناء والإدارة والتقييم لتحسين الأنشطة الأمنية ورعايتها في المنظمة.



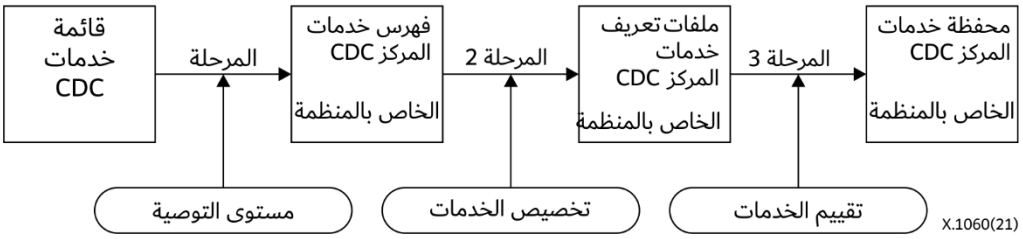
الشكل 2 – إطار إنشاء وتشغيل مركز الدفاع السيبراني

9 عملية البناء

1.9 نظرة عامة

لمركز الدفاع السيبراني عملية بناء لتحديد خدمات الأمن التي يجب تنفيذها في المنظمة. ويتم اختيار الخدمات المرشحة للتنفيذ من قائمة خدمات المركز CDC، والتي تستند إلى أفضل الممارسات في المنظمة. وللاطلاع على قائمة خدمات المركز CDC، انظر الفقرة 12.

ويعرض الشكل 3 المراحل الثلاث لبناء خدمات المركز CDC.



الشكل 3 – مراحل بناء الخدمات لمركز الأمن السيبراني

1) المرحلة 1: إنشاء فهرس خدمات مركز الدفاع السيبراني

ينبغي للمنظمة أن تقوم أولاً بإنشاء فهرس خدمات مركز الدفاع السيبراني.

وفي هذه المرحلة، تُستخرج الخدمات المرشحة للتنفيذ من قائمة الخدمات العامة. ويرد وصف تفاصيل القائمة العامة في الفقرة 12. وإذا كانت هناك خدمات مفقودة، ينبغي تحديد هذه الخدمات وإضافتها مجدداً إلى فهرس خدمات مركز الدفاع السيبراني.

2) المرحلة 2: إنشاء ملفات تعريف خدمات مركز الدفاع السيبراني

بالنسبة للخدمات المدرجة في فهرس خدمات مركز الدفاع السيبراني، ينبغي للمنظمة تحديد أدوار ومسؤوليات الأفرقة التي تقدم الخدمات. وفي هذه المرحلة، ينبغي مراعاة عملية تخصيص خدمات مركز الدفاع السيبراني الموصوفة في الفقرة 3.9.

وبالتالي ينبغي للمنظمة إعداد ملفات تعريف خدمات مركز الدفاع السيبراني.

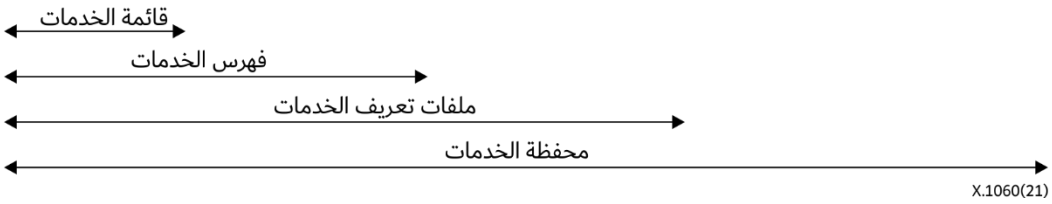
3) المرحلة 3: إنشاء محفظة خدمات مركز الدفاع السيبراني

بعد تحديد ملفات تعريف خدمات مركز الدفاع السيبراني، ينبغي للمنظمة قياس درجة الخدمة الحالية (كما هي) لكل خدمة وتحديد درجة خدمة مستهدفة متوسطة أو طويلة الأجل (في المستقبل).

وبمجرد تحديد الدرجة الحالية والمستهدفة، ينبغي للمنظمة إعداد محفظة خدمات مركز الدفاع السيبراني.

ويبين الشكل 4 مثال مصفوفة لخدمات مركز الدفاع السيبراني. وتُملأ هذه المصفوفة بعد المراحل من 1 إلى 3.

الخدمة	مستوى التوصية	تخصيص الخدمة	درجة الخدمة	
			الحالية	المستهدفة
مثال الخدمة 1	أساسية	الاستعانة بمصادر داخلية (AB Dept.)	3	5
مثال الخدمة 2	عادية	الاستعانة بمصادر داخلية (Z-MSSP)	2	4
مثال الخدمة 3	متقدمة	غير قابلة للتخصيص	1	2



الشكل 4 – مصفوفة خدمات لمركز الدفاع السيبراني

2.9 مستوى توصية خدمة مركز الدفاع السيبراني

لتنفيذ أنسب خدمات المركز CDC في منظمة ما، يمكن النظر في مدى ضرورة كل خدمة على المستويات الخمسة المدرجة في الجدول 1. ويمكن توضيح أولوية تنفيذ الخدمة من خلال قياس هذه المستويات.

الجدول 1 – مستوى توصية خدمة مركز الدفاع السيبراني

الوزن	الوصف
غير ضرورية	تعتبر الخدمات غير ضرورية
أساسية	الحد الأدنى من الخدمات الواجب تنفيذها
عادية	الخدمات التي يوصى بتنفيذها عادة
متقدمة	الخدمات المطلوبة لتحقيق دورة رفيعة المستوى لمركز الدفاع السيبراني
اختيارية	الخدمات المنتقاة بشكل عشوائي طبقاً للأداء المتوقع من مركز الدفاع السيبراني

3.9 تخصيص خدمات مركز الدفاع السيبراني

ينبغي للمنظمة أن توضح على وجه التحديد الفريق الذي ينبغي له أن ينفذ خدمة مركز الدفاع السيبراني. وبناءً على القدرات اللازمة لتنفيذ الخدمات في المنظمة، ينبغي للمنظمة تخصيص خدمة المركز CDC، والذي قد يشمل الاستعانة بمصادر خارجية. انظر الجدول 2.

الجدول 2 – تخصيص خدمات مركز الدفاع السيبراني

النوع	الوصف
الاستعانة بمصادر داخلية	يقوم فريق داخل المنظمة بتقديم الخدمات. وينبغي للمنظمة تحديد الفريق المسؤول.
الاستعانة بمصادر خارجية	يقوم فريق من خارج المنظمة بتقديم الخدمات. وينبغي للمنظمة تحديد المتعاقد الخارجي.
توليفة من الإثنين	تستخدم المنظمة الاستعانة بمصادر داخلية والاستعانة بمصادر خارجية معاً. وينبغي للمنظمة أن تحدد فريقاً مسؤولاً ومتعاقداً خارجياً.
غير مخصصة	على الرغم من أن المنظمة تعترف بالخدمة، فإنه لا يوجد كيان مكلف بها في المنظمة.

وينبغي عند استخدام الاستعانة بالمصادر الخارجية توضيح النقطتين ألف وباء.

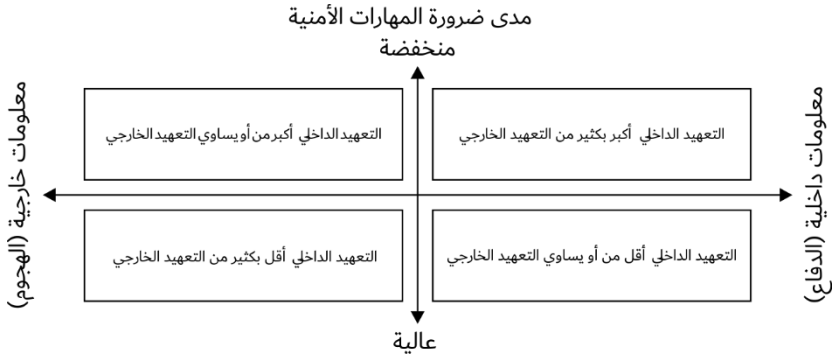
ألف) طبيعة المعلومات المتداولة

ينبغي للمنظمة تصنيف طبيعة المعلومات المتداولة، بما في ذلك التعاريف أو التمييز بين ما هو "الداخلي" و"الخارجي" بالنسبة للمنظمة. فعلى سبيل المثال، في حالة الحوادث، ينبغي اعتبار المعلومات التي تتضمن الضرر أو التأثير الناجم عن هجوم ما داخلية، بينما تعتبر المعلومات المتعلقة بالهجوم نفسه خارجية.

باء) الحاجة إلى مهارات أمنية متخصصة

ينبغي للمنظمة النظر فيما إذا كانت المهارات المتخصصة في مجال الأمن مطلوبة لتقديم الخدمة.

ويمكن تصنيف خدمات مركز الدفاع السيبراني إلى مجموعات رباعية من I) إلى IV) بناءً على هذين المؤشرين. انظر الشكل 5.



الشكل 5 – المجموعات الرباعية للتعهيد

I) التعهيد الداخلي أكبر بكثير من التعهيد الخارجي

عندما لا تكون الخبرة الأمنية مطلوبة للتعامل مع المعلومات السرية داخل المنظمة، تكون الاستعانة بمصادر داخلية هي الأمثل، ولا يفضل الاستعانة بمصادر خارجية.

II) التعهيد الداخلي أكبر من أو يساوي التعهيد الخارجي

إذا لم تكن الخبرة المطلوبة عالية جداً، وعلى الرغم من أنها معلومات خارجية بالنسبة للمنظمة، ينبغي تنفيذ النشاط والإدارة بشكل أساسي من قبل المنظمة وبدعم من خلال الاستعانة بمصادر خارجية.

III) التعهيد الداخلي أقل بكثير من التعهيد الخارجي

من أجل التعامل مع المعلومات، التي تدور بشكل أساسي حول الهجمات، التي تعتبر خارجية بالنسبة للمنظمة، ينبغي تنفيذ الخدمة من قبل منظمة ذات مهارات متخصصة (على سبيل المثال، الاستعانة بمصادر خارجية). وما لم يكن الخبراء ذوو المهارات المتخصصة متاحين داخلياً، يصعب المنظمة تنفيذ الخدمة بمفردها.

IV) التعهيد الداخلي أقل من أو يساوي التعهيد الخارجي

عندما تكون هناك حاجة إلى مهارات متخصصة للتعامل مع المعلومات الداخلية داخل المنظمة، ينبغي تنفيذ النشاط بشكل أساسي من قبل منظمة متخصصة (على سبيل المثال، الاستعانة بمصادر خارجية)، والتي ينبغي للمنظمة إدارتها ودعمها.

4.9 تقييم خدمات مركز الدفاع السيبراني

عند إنشاء محفظة خدمات المركز CDC، ينبغي تقييم حالة التنفيذ في الوضع الحالي والمستهدف لكل خدمة باستخدام درجات الخدمة المدرجة في الجدول 3. وجدير بالذكر أن أنواع الخدمات المختلفة، على سبيل المثال، التعهيد الداخلي والتعهيد الخارجي، ينبغي تقييمها من خلال المعايير المخصصة لدرجات الخدمة.

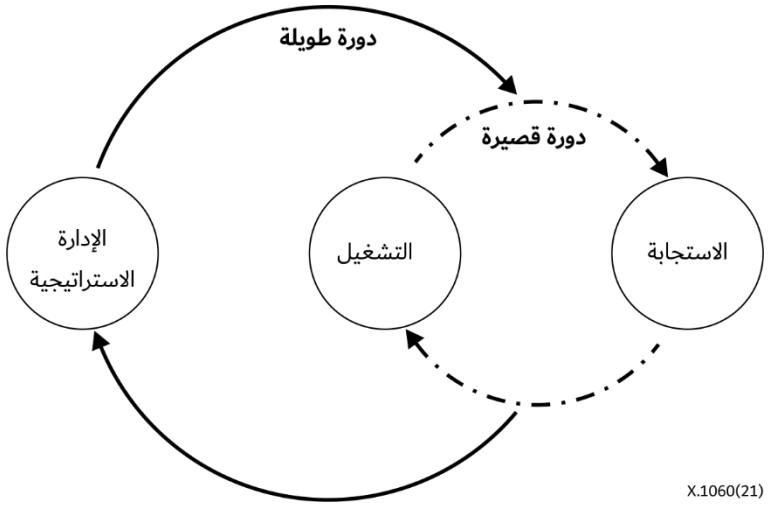
الجدول 3 – درجات خدمات مركز الدفاع السيبراني

بالنسبة للتعهيد الداخلي	
يتم تفويض العملية الموثقة من قبل كبير مسؤولي أمن المعلومات أو أي مدير آخر بالمنظمة لديه المسؤوليات المناسبة	+5 نقاط
العملية موثقة ويمكن لآخرين القيام بدور المشغل الحالي	+4 نقاط
العملية غير موثقة، ويمكن لآخرين القيام بدور جزئي للمشغل الحالي بصورة مؤقتة	+3 نقاط
العملية غير موثقة، ويمكن للمشغل الحالي القيام بدور ما	+2 (نقطتان)
العملية لا تعمل	+1 نقطة واحدة
تقرر عدم التنفيذ عن طريق التعهيد الداخلي	غير متاحة

بالنسبة للتعهيد الخارجي	
يتم فهم محتوى الخدمة والمخرجات المتوقعة وتكون مخرجاتها كما هو متوقع	+5 نقاط
يتم فهم محتوى الخدمة والمخرجات المتوقعة ولكن مخرجاتها ليست كما هو متوقع	+4 نقاط
عدم فهم إما محتوى الخدمة أو المخرجات المتوقعة	+3 نقاط
عدم فهم كل من محتوى الخدمة والمخرجات المتوقعة	+2 (نقطتان)
لم تتم مراجعة المخرجات ولا التقرير	+1 نقطة واحدة
تقرر عدم التنفيذ عن طريق التعهيد الخارجي	غير متاحة

10 عملية الإدارة

يمكّن المركز CDC الأنشطة الأمنية في جميع أنحاء المنظمة من خلال تنفيذ عملية إدارة المركز CDC بما في ذلك ثلاث مراحل ودورتان كما هو موضح في الشكل 6.



الشكل 6 – عملية إدارة مركز الدفاع السيبراني

(1) مرحلة الإدارة الاستراتيجية

تتحمل الإدارة الإستراتيجية المسؤولية والمساءلة عن جميع الخدمات الإستراتيجية ذات الصلة بالتعاريف والتصميم والتخطيط والإدارة وإصدار الشهادات وما إلى ذلك والتي تضمن تطوير مركز الدفاع السيبراني على المدى الطويل.

(2) مرحلة التشغيل

ينبغي إجراء الصيانة للإطار المقدم في مرحلة التشغيل. وهذا هو العمل في الوقت العادي أو المعتاد ويتضمن عادةً الأنشطة الروتينية، مثل تحليل الكشف عن الحوادث، ومراقبة أنظمة الاستجابة الأمنية وصيانتها. وغالباً ما يُطلق على الفريق الذي يقوم بهذه العمليات اسم مركز العمليات الأمنية (SOC).

(3) مرحلة الاستجابة

ينبغي تنفيذ الاستجابة للحادث عند اكتشاف حدث من خلال التحليل في مرحلة التشغيل. وهذه المرحلة هي دائما حالة طارئة. وغالباً ما يُطلق على أولئك الذين يستجيبون للحادث فريق الاستجابة للحوادث الأمنية الحاسوبية (CSIRT).

ولا تقتصر المدخلات لمرحلة الاستجابة على تلك الواردة من مرحلة التشغيل، ولكن ينبغي للفريق أيضاً تغطية الاستجابة على التقارير أو الإخطارات من الأطراف الثالثة.

ألف) الدورة القصيرة

يُجرى التشغيل والاستجابة يومياً. وفي هذه العمليات، تظهر عادة المشكلات في سير الأعمال وفي نظام الاستجابة الأمنية. لذلك، فإن التحسين المستمر لحل هذه المشكلات، على سبيل المثال، التشغيل الآلي البسيط للمهام البسيطة، وتحسين الأدوات لتحليل الدقة ومراجعة عناصر التقرير، أمور ضرورية في حدود الموارد (الأشخاص، والميزانية، والنظام) المخصصة في دورة قصيرة.

باء) الدورة الطويلة

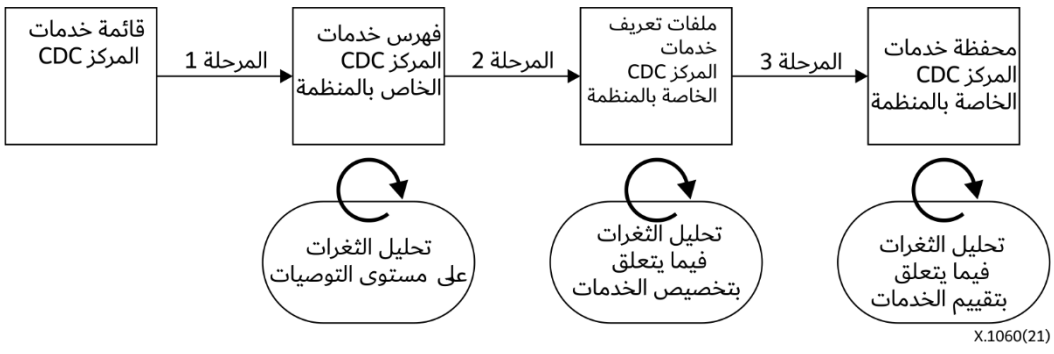
يجب تطبيق المراجعة التي تتطلب تخصيص موارد جديدة على دورة طويلة.

وإذا ظهرت أي مشكلات لا يمكن حلها بواسطة النظام الحالي عند مراجعة الدورة القصيرة، ينبغي أن تكون الاستجابة رؤية أو خطة طويلة الأجل، على سبيل المثال، إدخال منتج أمني جديد، ومراجعة جذرية للسياسات الأمنية وتغير واسع النطاق في تشكيلة الأنظمة الأمنية.

11 عملية التقييم

1.11 نظرة عامة

يجب تقييم فهرس وملف تعريف ومحفظة خدمة المركز CDC التي تمت صياغتها في عملية البناء في الوقت المناسب وبطريقة منتظمة. يوضح الشكل 7 عملية تقييم خدمات المركز CDC.



الشكل 7 – عملية تقييم مركز الدفاع السيبراني

2.11 تقييم فهرس خدمات مركز الدفاع السيبراني

ينبغي إجراء تحليل للثغرات على مستوى توصيات خدمات المركز CDC. وتكون المراجعة مطلوبة بسبب التغيرات في البيئة والتهديدات، خاصة أنه ينبغي إعادة فحص الخدمات "غير الضرورية" ومراجعتها لضمان عدم وجود إسقاطات. وينبغي تقييم فهرس خدمات المركز CDC عندما تدخل الشركة تغييرات، مثل بدء أنشطة تجارية جديدة، والاستجابة لمخاطر وتهديدات جديدة.

3.11 تقييم ملفات تعريف خدمات مركز الدفاع السيبراني

ينبغي إجراء تحليل للثغرات فيما يتعلق بعمليات تخصيص خدمات المركز CDC. ومن خلال تحديد تخصيصات الخدمات، يمكن التخلص من الخدمات "غير قابلة للتخصيص"، ويمكن للمؤسسة أن تتوقع تحسين مستوى الاكتمال من خلال مراجعتها. وينبغي تقييم ملفات تعريف خدمات المركز CDC عند حدوث تغييرات تنظيمية، مثل تغييرات المنظمة الداخلية لنوع التعهيد الداخلي وتغييرات المتعاقد الخارجي لنوع التعهيد الخارجي.

4.11 تقييم محفظة خدمات مركز الدفاع السيبراني

يجب إجراء تحليل ثغرات لدرجة خدمة المركز CDC للخدمات الفردية. وينبغي توضيح الفارق بين الدرجة المستهدفة في المستقبل والدرجة في الوضع الراهن حتى تتمكن المنظمة من التركيز على ما يحتاج إلى تحسين، وتأكيد درجة خدمة المركز CDC مرة أخرى واستخلاص المشكلات. وينبغي تقييم محفظة خدمات المركز CDC بانتظام.

12 فئات وقائمة خدمات مركز الدفاع السيبراني

فئات وقائمة خدمات المركز CDC مطلوبة في عمليات البناء والإدارة (انظر الفقرتين 9 و10).

تحتوي خدمات المركز CDC على تسع فئات خدمة:

A) الإدارة الاستراتيجية لمركز الدفاع السيبراني؛

B) التحليل في الوقت الفعلي؛

C) التحليل المتعمق؛

D) الاستجابة للحوادث؛

E) الفحص والتقييم؛

F) جمع معلومات التهديدات وتحليلها وتقييمها؛

G) تطوير منصات مركز الدفاع السيبراني وصيانتها؛

H) دعم الاستجابة للاحتيال الداخلي؛

I) العلاقة النشطة بالأطراف الخارجية.

A) الإدارة الاستراتيجية لمركز الدفاع السيبراني

تشمل هذه الفئة السياسات وتخطيط الموارد لجميع الأنشطة الأمنية المذكورة في الفئات من A) إلى I) في المنظمة، بما في ذلك مركز الدفاع السيبراني لضمان استقرار تشغيله.

B) التحليل في الوقت الفعلي

تراقب هذه الفئة وتحلل السجلات والبيانات باستمرار من الأنظمة المختلفة، مثل أجهزة الشبكة والمخدمات والمنتجات الأمنية. والهدف هو اكتشاف التهديدات في الوقت الفعلي، مما يسمح باستجابة سريعة ومناسبة للحادث.

C) التحليل المتعمق

هذه فئة مرتبطة بالحادث، مثل التحقيق في الأنظمة المتأثرة، ومراجعة البيانات المخترقة، وتحليل الأدوات والأساليب المستخدمة في الهجوم.

والهدف هو توضيح النطاق الكامل للحادث وتحديد أثره.

D) الاستجابة للحوادث

تتخذ هذه الفئة إجراءات محددة بناءً على نتائج التحليل في الوقت الفعلي ومعلومات التهديد لردع التهديدات والقضاء عليها.

والهدف هو تقليل التأثير على النظام والأعمال، بما في ذلك التنسيق وإعداد التقارير مع أصحاب المصلحة.

E) الفحص والتقييم

هذه الفئة مخصصة لتقييم مواطن ضعف الأنظمة المطلوب حمايتها، والتدريب على الاستجابة للحوادث وتقييمها. والغرض من هذه الفئة هو تحسين مستوى الأمن.

F) جمع معلومات التهديدات وتحليلها وتقييمها

تجمع هذه الفئة معلومات التهديدات حول مواطن الضعف والهجمات (المعلومات الخارجية) المتاحة على الإنترنت وتعالج المعلومات المتعلقة بالتحليل في الوقت الفعلي والاستجابة للحوادث (المعلومات الداخلية).

والهدف هو تحسين دقة التحليل في الوقت الحقيقي والاستجابة للحوادث، وتحسين الأصول الأمنية.

G) تطوير منصات مركز الدفاع السيبراني وصيانتها

تقوم هذه الفئة بإدارة أو تحسين أو تطوير أنظمة جديدة (على سبيل المثال، منتجات أمنية وقواعد بيانات مجموعة السجلات والأنظمة التشغيلية) الضرورية للاستجابة الأمنية.

والهدف هو تحقيق أنشطة أمنية سلسة ومستدامة في الفئات الأخرى.

H) دعم الاستجابة للاحتيال الداخلي

تجمع هذه الفئة بيانات المراجعة لدعم الاستجابة للاحتيال الداخلي.

والغرض من هذه الفئة هو دعم الاستجابة للاحتيال الداخلي ومنعه من خلال توفير السجلات والتحليلات.

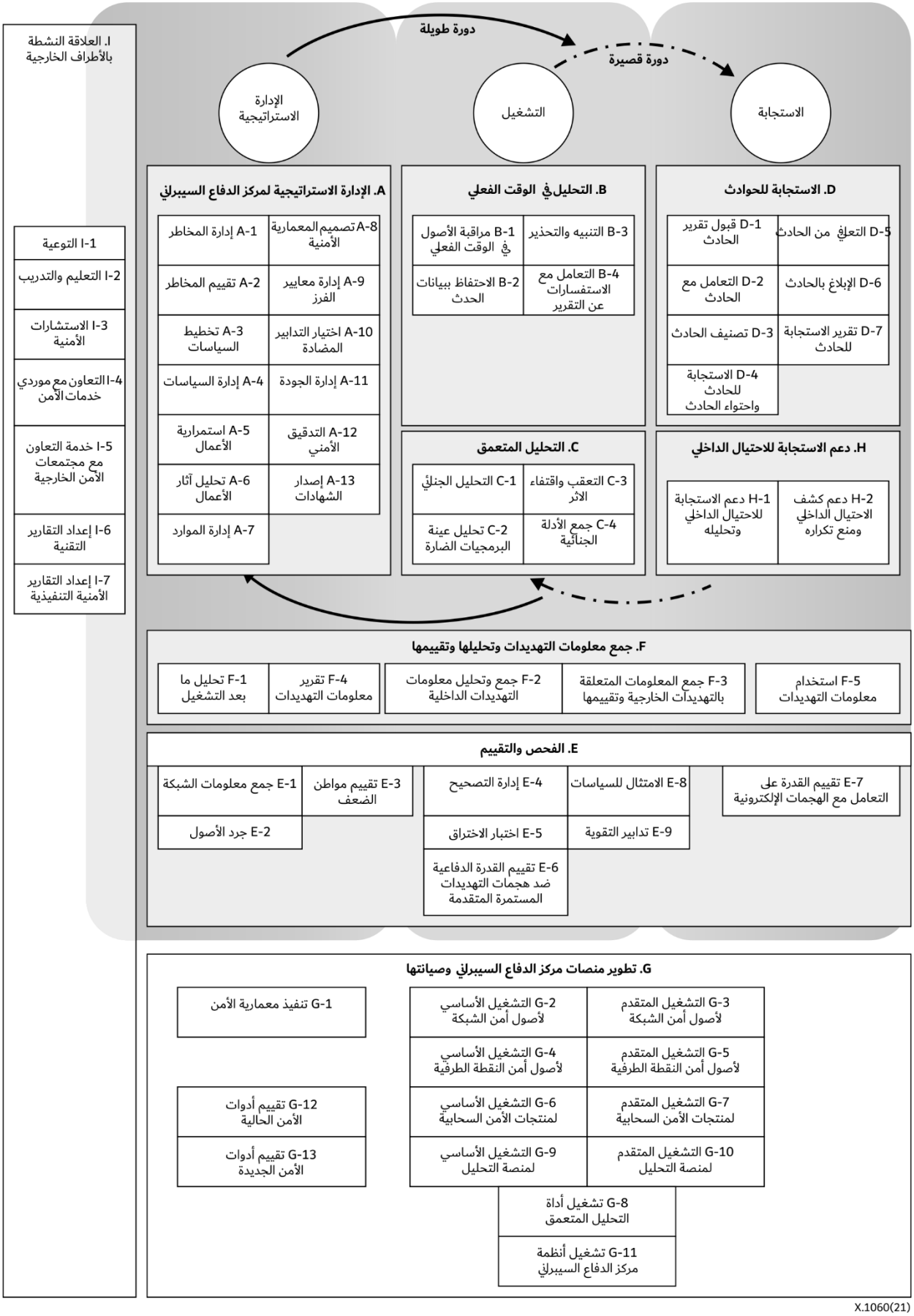
I) العلاقة النشطة بالأطراف الخارجية

تشمل هذه الفئة التنسيق والتعاون مع أصحاب المصلحة الداخليين والمنظمات الخارجية.

والهدف هو تحسين المستوى الأمني للمنظمة، وزيادة قيمة الأمن للمنظمة، وبالتالي زيادة تطوير وتقوية المنظمة.

يوضح الشكل 8 التقابل بين فئات الخدمات وعمليات الإدارة، ويسرد الجدول 4 الخدمات.

وترد الأوصاف التفصيلية لكل خدمة في قائمة خدمات مركز الدفاع السيبراني في الملحق A.



الشكل 8 – فئات خدمات مركز الدفاع السيبراني

الجدول 4 – فئات خدمات مركز الدفاع السيبراني

A	الإدارة الاستراتيجية لمركز الدفاع السيبراني
A-1	إدارة المخاطر
A-2	تقييم المخاطر
A-3	تخطيط السياسات
A-4	إدارة السياسات
A-5	استمرارية الأعمال
A-6	تحليل آثار الأعمال
A-7	إدارة الموارد
A-8	تصميم المعمارية الأمنية
A-9	إدارة معايير الفرز
A-10	اختيار التدابير المضادة
A-11	إدارة الجودة
A-12	التدقيق الأمني
A-13	إصدار الشهادات
B	**التحليل في الوقت الفعلي**
B-1	مراقبة الأصول في الوقت الفعلي
B-2	الاحتفاظ ببيانات الحدث
B-3	التنبيه والتحذير
B-4	التعامل مع الاستفسارات عن التقرير
C	**التحليل المتعمق**
C-1	التحليل الجنائي
C-2	تحليل عينة البرمجيات الضارة
C-3	التعقب واقتفاء الاثر
C-4	جمع الأدلة الجنائية
D	**الاستجابة للحوادث**
D-1	قبول تقرير الحادث
D-2	التعامل مع الحادث
D-3	تصنيف الحادث
D-4	الاستجابة للحادث واحتواء الحادث
D-5	التعافي من الحادث
D-6	الإبلاغ بالحادث
D-7	تقرير الاستجابة للحادث
E	**الفحص والتقييم**
E-1	جمع معلومات الشبكة
E-2	جرد الأصول
E-3	تقييم مواطن الضعف
E-4	إدارة التصحيح
E-5	اختبار الاختراق
E-6	تقييم القدرة الدفاعية ضد هجمات التهديدات المستمرة المتقدمة
E-7	تقييم القدرة على التعامل مع الهجمات الإلكترونية
E-8	الامتثال للسياسات
E-9	تدابير التقوية

F	جمع معلومات التهديدات وتحليلها وتقييمها
F-1	تحليل ما بعد التشغيل
F-2	جمع وتحليل معلومات التهديدات الداخلية
F-3	جمع المعلومات المتعلقة بالتهديدات الخارجية وتقييمها
F-4	تقرير معلومات التهديدات
F-5	استخدام معلومات التهديدات
G	**تطوير منصات مركز الدفاع السيبراني وصيانتها**
G-1	تنفيذ معمارية الأمن
G-2	التشغيل الأساسي لأصول أمن الشبكة
G-3	التشغيل المتقدم لأصول أمن الشبكة
G-4	التشغيل الأساسي لأصول أمن النقطة الطرفية
G-5	التشغيل المتقدم لأصول أمن النقطة الطرفية
G-6	التشغيل الأساسي لمنتجات الأمن السحابية
G-7	التشغيل المتقدم لمنتجات الأمن السحابية
G-8	تشغيل أداة التحليل المتعمق
G-9	التشغيل الأساسي لمنصة التحليل
G-10	التشغيل المتقدم لمنصة التحليل
G-11	تشغيل أنظمة مركز الدفاع السيبراني
G-12	تقييم أدوات الأمن الحالية
G-13	تقييم أدوات الأمن الجديدة
H	**دعم الاستجابة للاحتيال الداخلي**
H-1	دعم الاستجابة للاحتيال الداخلي وتحليله
H-2	دعم كشف الاحتيال الداخلي ومنع تكراره
I	**العلاقة النشطة بالأطراف الخارجية**
I-1	التوعية
I-2	التعليم والتدريب
I-3	الاستشارات الأمنية
I-4	التعاون مع موردي خدمات الأمن
I-5	خدمة التعاون مع مجتمعات الأمن الخارجية
I-6	إعداد التقارير التقنية
I-7	إعداد التقارير الأمنية التنفيذية

الملحق A

قائمة خدمات مركز الدفاع السيبراني مع أوصافها

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

1.A الفئة A: الإدارة الاستراتيجية لمركز الدفاع السيبراني

1.1.A A-1. إدارة المخاطر:

تهدف خدمة إدارة المخاطر إلى تنفيذ الأنشطة المنسقة بما في ذلك الأنشطة من A-2 إلى A-13 لتوجيه ومراقبة المنظمة فيما يتعلق بالمخاطر.

2.1.A A-2. تقييم المخاطر

تقدم خدمة تقييم المخاطر لمحة عن مستوى المخاطر في المنظمة من حيث الأصول والتهديدات والتدابير الأمنية.

3.1.A A-3. تخطيط السياسات

تدعم خدمة تخطيط السياسات جميع أنشطة تعيين سياسات أمنية محددة وتجميع المبادئ التوجيهية.

4.1.A A-4. إدارة السياسات

تتمثل خدمة إدارة السياسات في إجراء مراجعات دورية لتقييم القواعد السياساتية والتنظيمية، والامتثال للمتطلبات الجديدة أو الخارجية (مثل اللوائح والمبادئ التوجيهية).

5.1.A A-5. استمرارية الأعمال

تدعم خدمة استمرارية الأعمال الوظائف التشغيلية اللازمة لضمان التنفيذ والتطبيق السليمين لخطة استمرارية الأعمال الخاصة بالمنظمة.

6.1.A A-6. تحليل آثار الأعمال

تتمثل خدمة تحليل آثار الأعمال في إجراء تقييم منهجي للتأثيرات المحتملة الناتجة عن الأحداث أو السيناريوهات المختلفة. وتساعد هذه الخدمة المنظمات على فهم حجم الخسائر التي يمكن أن تحدث. وقد لا تغطي فقط الخسائر المالية المباشرة، ولكنها تغطي أيضاً التأثيرات الأخرى، مثل فقدان ثقة أصحاب المصلحة والإضرار بالسمعة.

7.1.A A-7. إدارة الموارد

تقوم خدمة إدارة الموارد بتخطيط الموارد (الموظفين، والميزانية، والأنظمة، وما إلى ذلك) اللازمة لدعم الأنشطة الأمنية وتخصيصها بشكل مناسب لكل خدمة.

8.1.A A-8. تصميم المعمارية الأمنية

تتمثل خدمة تصميم المعمارية الأمنية في إنشاء معمارية لتأمين الأعمال. ويمكن تطوير منصات مركز الدفاع السيبراني وصيانتها (الفئة G) من خلال تجميع مختلف القياسات الأمنية التي تأخذ في الاعتبار تصميم النظام وقيود العمليات التجارية (على سبيل المثال، سلسلة الإمداد).

9.1.A A-9. إدارة معايير الفرز

تهدف خدمة إدارة معايير الفرز إلى وضع معايير فرز محددة (أولوية الاستجابة) للأحداث (على سبيل المثال، الحوادث، ومواطن الضعف التي تم اكتشافها، ومعلومات التهديدات المكتشفة) ضمن النطاق المتفق عليه في السياسة العامة.

10.1.A A-10. اختيار التدابير المضادة

تهدف خدمة اختيار التدابير المضادة إلى دعم جميع أنشطة اختيار التدابير المضادة لمعايير الفرز (A-9) وأفضل التكنولوجيات فيما يتعلق بجميع التصرفات الأمنية.

11.1.A A-11. إدارة الجودة

تتمثل خدمة إدارة الجودة في فحص المشكلات المتعلقة بجودة الأنشطة الأمنية، سواء كان لها تأثير سلبي على الأعمال أم لا (على سبيل المثال، قابلية الاستخدام، والإنتاجية) على مدار فترة زمنية معينة (على سبيل المثال، أسبوع واحد أو شهر واحد).

12.1.A A-12. التدقيق الأمني

تقوم خدمة التدقيق الأمني بشكل منهجي وقابل للقياس بالتدقيق في كيفية قيام المنظمة بتنفيذ السياسات والضوابط الأمنية في موقع أو وقت معين. ويشارك موظفو مركز الدفاع السيبراني بشكل غير مباشر في أنشطة التدقيق من أجل توفير المعلومات والأدلة اللازمة عن حالة الضوابط المنفذة.

13.1.A A-13. إصدار الشهادات

تدعم خدمة إصدار الشهادات الأنشطة الضرورية للمنظمة كي تتوافق مع مختلف المعايير وأنظمة الاعتماد.

2.A الفئة B: التحليل في الوقت الفعلي

1.2.A B-1. مراقبة الأصول في الوقت الفعلي

تتمثل خدمة مراقبة الأصول في الوقت الفعلي في الإشراف على حالة الأنظمة أو الأنشطة المشبوهة من السجلات وتدفقات الشبكة وتحليلها، ودعم الفرز كحادث أو حدث لجمع المعلومات المطلوبة.

2.2.A B-2. الاحتفاظ ببيانات الحدث

تقوم خدمة الاحتفاظ ببيانات الأحداث بجمع الأحداث التي تم جمعها في عملية المراقبة والتحليل الأمنيين وتخزينها مركزياً.

3.2.A B-3. التنبيه والتحذير

تقوم خدمة التنبيه والتحذير بإخطار الوظيفة الداخلية المعنية بالأحداث بتسليط الضوء على المخاطر المحتملة على أصول المعلومات (على سبيل المثال، تنبيه الأجهزة الأمنية، والنشرات الأمنية، ومواطن الضعف وانتشار التهديدات).

4.2.A B-4. التعامل مع الاستفسارات عن التقرير

تتمثل خدمة التعامل مع الاستفسارات عن التقرير في الرد على الاستفسارات بشأن البيانات والتقارير المتعلقة بالتحليل.

3.A الفئة C: التحليل المتعمق

1.3.A C-1. التحليل الجنائي

تحلل خدمة التحليل الجنائي الأدلة الرقمية التي يتم جمعها من الأصول الأمنية وتتعلق بحدث ما للمساعدة في تحديد ما حدث.

2.3.A C-2. تحليل عينة البرمجيات الضارة

تهدف خدمة تحليل عينة البرمجيات الضارة إلى تحليل البرمجيات الضارة أو البرامج أو النصوص البرمجية التي ينشرها المهاجمون والتي يتم اكتشافها أثناء كل عملية من عمليات التحليل الجنائي.

3.3.A C-3. التعقب واقتفاء الاثر

هذه الخدمة هي قدرة المنظمة على تعقب وتتبع مصدر أي هجمات على بناها التحتية، وهو عامل نجاح حاسم لزيادة الحد من وقوع الحوادث ومنع الحوادث الأمنية. ويمكن للقدرة المعترف بها لتتبع وتعقب كل من المهاجمين الداخليين والخارجيين (على سبيل المثال، الإسناد الإلكتروني) استباق الهجمات المستقبلية.

4.3.A C-4. جمع الأدلة الجنائية

تجمع خدمة جمع الأدلة الجنائية الأدلة الإلكترونية الرقمية المتعلقة بحادث تم تقييمه وتحافظ عليها، وتطور وتحافظ على صلاحية الأدلة ("سلسلة أدلة العهدة").

4.A الفئة D: الاستجابة للحوادث

1.4.A D-1. قبول تقرير الحادث

خدمة قبول تقرير الحادث هي تلقي تقارير تحليلية للعمليات. ومع ذلك، قد تتلقى تقارير من منظمة أخرى داخل الشركة أو من منظمة خارجية.

2.4.A D-2. التعامل مع الحادث

خدمة التعامل مع الحادث هي خدمة التعامل مع الحوادث المقبولة وتنسيق الأنشطة بما في ذلك الأنشطة من D-3 إلى D-7.

3.4.A D-3. تصنيف الحادث

تهدف خدمة تصنيف الحادث إلى تصنيف الحادث للمساهمة في فهم مشترك لأنواع الحوادث التي تحدث وأسبابها.

4.4.A D-4. الاستجابة للحادث واحتواء الحادث

تهدف خدمة الاستجابة للحادث واحتواء الحادث إلى احتواء الحادث قبل أن ينتشر عبر جميع الموارد ويزيد من الضرر أو التأثير عليها.

5.4.A D-5. التعافي من الحادث

تهدف خدمة التعافي من الحادث إلى دعم استعادة وظائف الهدف إلى قابلية تشغيل النظام العادية الخاصة بالهدف.

6.4.A D-6. الإبلاغ بالحادث

تهدف خدمة الإبلاغ بالحادث إلى الإبلاغ عن وقوع الحادث إلى أفرقة الاستجابة للحوادث والأفرقة المعنية الأخرى.

7.4.A D-7. تقرير الاستجابة للحادث

تتمثل خدمة تقرير الاستجابة للحادث في استكمال وتوزيع تقرير الاستجابة للحوادث المغلقة (إذا كانت جهود الإجراءات المضادة مطولة، فسيتم تسليمها إلى الإدارة الإستراتيجية لمركز الدفاع السيبراني (الفئة A)). وإذا احتاج موظفو مركز الدفاع السيبراني إلى تقرير عن الحالة الراهنة أثناء التعامل مع حادث ما، فإن هذه الخدمة توزع تقريراً مؤقتاً.

5.A الفئة E: الفحص والتقييم

1.5.A E-1. جمع معلومات الشبكة

تتمثل خدمة جمع معلومات الشبكة في تلقي نظرة عامة عن تشكيلة الشبكة المراد حمايته.

2.5.A E-2. جرد الأصول

تهدف خدمة جرد الأصول إلى تحقيق إدارة المعلومات ذات الصلة بتعداد الأنظمة والأصول والتطبيقات التي تشكل البنية التحتية العامة للأعمال في نطاق دعم المركز CDC.

3.5.A E-3. تقييم مواطن الضعف

تهدف خدمة تقييم مواطن الضعف إلى فحص الشبكات والأنظمة والتطبيقات لتحديد مواطن الضعف وتحديد كيفية استغلالها والتوصية بكيفية التخفيف من المخاطر.

4.5.A E-4. إدارة التصحيح

تهدف خدمة إدارة التصحيح لدعم تثبيت أي تصحيحات أمنية مطلوبة، مع الحفاظ على تيسر خدمة تكنولوجيا المعلومات (IT).

5.5.A E-5. اختبار الاختراق

تتمثل خدمة اختبار الاختراق في الكشف عن مواطن الضعف الأمنية التي يمكن أن يستغلها المهاجمون وتسلط الضوء على أساليب الاختراق المحتملة (على سبيل المثال، اختبار الاختراق القائم على التهديد).

6.5.A E-6. تقييم القدرة الدفاعية ضد هجمات التهديدات المستمرة المتقدمة

خدمة تقييم القدرة الدفاعية ضد هجمات التهديدات المستمرة المتقدمة هي قياس مقاومة المنظمة للهجمات المستهدفة أثناء إجراء تدريب مستهدف عبر البريد الإلكتروني واختبارات الهندسة الاجتماعية.

7.5.A E-7. تقييم القدرة على التعامل مع الهجمات الإلكترونية

تتمثل خدمة تقييم القدرة على التعامل مع الهجمات الإلكترونية في تأكيد ما إذا كان يمكن تفعيل أنشطة الاستجابة الأمنية الفعلية استناداً إلى سيناريو يفترض وقوع هجوم وما إذا كان يمكن إنهاء الحادث دون تأخير (يُسمى تمرين استجابة لهجوم سيبراني).

8.5.A E-8. الامتثال للسياسات

تهدف خدمة الامتثال للسياسات إلى دعم التحقق من المطابقة والامتثال للسياسات الأمنية المحددة مسبقًا.

9.5.A E-9. تدابير التقوية

خدمة تدابير التقوية هي استمثال تشكيلة مكونات تكنولوجيا المعلومات لتحديد وتقييم وتطبيق التشكيلات الأمنية للأنظمة، والحد من مخاطر الهجمات أو القضاء عليها.

6.A الفئة F: جمع معلومات التهديدات وتحليلها وتقييمها

1.6.A F-1. تحليل ما بعد التشغيل

تصف خدمة تحليل ما بعد التشغيل تحليل حادث ما لضمان مراجعة وتحسين العمليات والأدوات لموظفي مركز الدفاع السيبراني.

2.6.A F-2. جمع وتحليل معلومات التهديدات الداخلية

تهدف خدمة جمع وتحليل معلومات التهديدات الداخلية إلى جمع المعلومات (المعلومات الداخلية) بشأن التحليل في الوقت الفعلي والاستجابة للحوادث.

3.6.A F-3. جمع المعلومات المتعلقة بالتهديدات الخارجية وتقييمها

تتمثل خدمة جمع المعلومات المتعلقة بالتهديدات الخارجية وتقييمها في جمع المعلومات (المعلومات الخارجية)، مثل مواطن الضعف الجديدة واتجاهات الهجمات وسلوك البرمجيات الضارة وعناوين بروتوكول الإنترنت الخبيثة أو معلومات الميادين.

4.6.A F-4. تقرير معلومات التهديدات

خدمة تقرير معلومات التهديدات هي تجميع لمعلومات التهديدات الداخلية والخارجية وتوثيقها، بما في ذلك جميع التفاصيل.

5.6.A F-5. استخدام معلومات التهديدات

تتمثل خدمة استخدام معلومات التهديدات في تجميع ونشر معلومات التهديدات لجميع فئات الاستجابة الأمنية.

7.A الفئة G: تطوير منصات مركز الدفاع السيبراني وصيانتها

1.7.A G-1. تنفيذ معمارية الأمن

تهدف خدمة تنفيذ معمارية الأمن إلى تنفيذ معمارية الأمن المصممة بواسطة الإدارة الإستراتيجية لمركز الدفاع السيبراني (الفئة A) باستخدام الأصول.

2.7.A G-2. التشغيل الأساسي لأصول أمن الشبكة

تتمثل خدمة التشغيل الأساسي لأصول أمن الشبكة في تشغيل أجهزة الشبكة، مثل جدر الحماية ونظام كشف الاقتحام/نظام منع الاقتحام (IDS/IPS) وجدر حماية تطبيقات الويب (WAF) والوكلاء.

3.7.A G-3. التشغيل المتقدم لأصول أمن الشبكة

تتمثل خدمة التشغيل المتقدم لأصول أمن الشبكة في إنشاء توقيعات مخصصة لمنظمة ما للمنتجات ذات إمكانات الكشف عن الهجمات، مثل الأنظمة IDS/IPS والجدر WAF، وتطبيقها إذا كان التوقيع المقدم من البائع غير كافٍ.

4.7.A G-4. التشغيل الأساسي لأصول أمن النقطة الطرفية

تهدف خدمة التشغيل الأساسي لأصول أمن النقطة الطرفية إلى تشغيل منتجات التدابير المضادة، مثل برمجيات مكافحة الفيروسات، عند النقاط الطرفية.

5.7.A G-5. التشغيل المتقدم لأصول أمن النقطة الطرفية

تتمثل خدمة التشغيل المتقدم لأصول أمن النقطة الطرفية في الكشف عن نشاط البرنامج المشبوه داخل النقطة الطرفية باستخدام منتج الحماية الخاص بها، وجمع حالة السجل وتحليلها، وتنفيذ العملية، وما إلى ذلك، وإذا لزم الأمر، تضع الخدمة مؤشرات مخصصة للاختراق لتمكين اكتشاف النقطة الطرفية.

6.7.A G-6. التشغيل الأساسي لمنتجات الأمن السحابية

تتمثل خدمة التشغيل الأساسي لمنتجات الأمن السحابية في تشغيل خدمات الأمن في السحابة.

7.7.A G-7. التشغيل المتقدم لمنتجات الأمن السحابية

تهدف خدمة التشغيل المتقدم لمنتجات الأمن السحابية في إنشاء توقيعات مخصصة لمنظمة ما لخدمات الأمن في سحابة مع إمكانات الكشف عن الهجمات. وإذا كان التوقيع المقدم من قبل البائع غير كافٍ، فإن الخدمة تطبق التوقيعات المخصصة.

8.7.A G-8. تشغيل أداة التحليل المتعمق

تهدف خدمة تشغيل أداة التحليل المتعمق إلى تشغيل الأدوات المستخدمة في التحليل المتعمق، مثل الأدلة الجنائية الرقمية وتحليل البرمجيات الضارة.

9.7.A G-9. التشغيل الأساسي لمنصة التحليل

تتمثل خدمة التشغيل الأساسي لمنصة التحليل في تشغيل البنية التحتية التحليلية التي تخزن بيانات السجل المطلوبة وتمكن من إجراء التحليل بشكل روتيني، بشكل أساسي من خلال التحليل في الوقت الفعلي، مثل إدارة المعلومات والأحداث الأمنية (SIEM).

10.7.A G-10. التشغيل المتقدم لمنصة التحليل

تهدف خدمة التشغيل المتقدم لمنصة التحليل إلى تحقيق تحليل أكثر تفصيلاً ودقة باستخدام الأنظمة الخاصة بالمنظمة للاحتفاظ بسجلات النظام وبيانات التقاط الرزم التي لا تستطيع الإدارات SIEM التجارية التقاطها، وتطوير خوارزميات تحليل مخصصة ومنطق لهذه البيانات، فضلاً عن النظام.

11.7.A G-11. تشغيل أنظمة مركز الدفاع السيبراني

تتمثل خدمة تشغيل أنظمة مركز الدفاع السيبراني في تشغيل الأنظمة التي تؤدي المهام المطلوبة لعمليات الاستجابة الأمنية، مثل أدوات الاستجابة الأمنية المختلفة التي تم وصفها آنفاً، وإنتاج التقارير المختلفة، والرد على الاستفسارات، ونظام إدارة مواطن الضعف.

12.7.A G-12. تقييم أدوات الأمن الحالية

تهدف خدمة تقييم أدوات الأمن الحالية إلى التحقق من التأثير على الأنظمة والعمليات الأخرى، بشكل أساسي من حيث التيسر، عند ترقية أو تغيير إعدادات الأدوات الحالية القائمة على الأمن.

13.7.A G-13. تقييم أدوات الأمن الجديدة

تهدف خدمة تقييم أدوات الأمن الجديدة إلى تصميم أصول أمن جديدة وتثبيتها، إذا كانت هناك حاجة إلى تدابير جديدة في الأنشطة الأمنية.

8.A الفئة H: دعم الاستجابة للاحتيال الداخلي

1.8.A H-1. دعم الاستجابة للاحتيال الداخلي وتحليله

تهدف خدمة دعم الاستجابة للاحتيال الداخلي وتحليله إلى دعم استجابة المنظمة للاحتيال الداخلي عند اكتشافه، من خلال تنظيم أنشطتها من السجلات التي تم جمعها بواسطة الأنشطة الأمنية.

2.8.A H-2. دعم كشف الاحتيال الداخلي ومنع تكراره

تهدف خدمة دعم كشف الاحتيال الداخلي ومنع تكراره إلى تحليل تفاصيل أنشطة الاحتيال الداخلي التي تم اكتشافها، والنظر فيما إذا كان من الممكن اكتشافها من السجلات، وإذا كان الأمر كذلك، يتم تنفيذ منطق الكشف.

9.A الفئة I: العلاقة النشطة بالأطراف الخارجية

1.9.A I-1. التوعية

تهدف خدمة التوعية إلى إيجاد وعي لدى لموظفين المعنيين في المركز CDC بشأنه، والتشجع على استخدام الأدوات الصحيحة وأفضل الممارسات والسياسات والموارد لضمان حماية أصول الأعمال.

2.9.A I-2. التعليم والتدريب

تهدف خدمة التعليم والتدريب إلى دعم أنشطة التدريب المتخصصة في مجالات الأمن للموظفين في المنظمات والتي يدعمها المركز CDC.

3.9.A I-3. الاستشارات الأمنية

تقدم خدمة الاستشارات الأمنية خدمات استشارية لوظائف الأعمال المختلفة فيما يتعلق بالأمن.

4.9.A I-4. التعاون مع موردي خدمات الأمن

تهدف خدمة التعاون مع موردي خدمات الأمن إلى بناء خط اتصال مباشر مع مورد أي منتج أمني أو خدمة أمنية تم شراؤهما، وتطلب الاستجابة لأي أوجه قصور موجودة في الاستجابة الأمنية وتبادل الملاحظات الإيجابية حول مجالات التحسين.

5.9.A I-5. خدمة التعاون مع مجتمعات الأمن الخارجية

تهدف خدمة التعاون مع مجتمعات الأمن الخارجية إلى تبادل المعلومات بشكل استباقي من خلال المشاركة في المجتمعات الخارجية. ويمكن أن تنعكس هذه المعلومات على الأنشطة الأمنية.

6.9.A I-6. تقديم التقارير التقنية

خدمة تقديم التقارير التقنية هي تقديم تقارير عن نتائج أنشطة المراقبة والإدارة. وتساعد هذه الأنشطة في إظهار مستوى أمن الأنظمة والبنية التحتية لتكنولوجيا المعلومات.

7.9.A I-7. إعداد التقارير الأمنية التنفيذية

تهدف خدمة إعداد التقارير الأمنية التنفيذية إلى إنتاج تقارير دورية وتحليلات إحصائية للإدارة العليا لتسليط الضوء على مستوى الأمن ومؤشرات الأداء التشغيلي لأي منظمة.

بيبليوغرافيا

[b-ITU-T X.1053] Recommendation ITU-T X.1053 (2017), *Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2021