الاتحـــاد الدولـــــي للاتصـــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1603

(2018/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – تصميم أمن الحوسبة السحابية

متطلّبات أمن البيانات لخدمة مراقبة الحوسبة السحابية

التوصيـــة ITU-T X.1603

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
القياسات البيومترية عن بَعد	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية	X.1349–X.1340
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	**X.1639–X.1602**
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

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

التوصيـــة ITU-T X.1603

متطلبات أمن البيانات لخدمة المراقبة في الحوسبة السحابية

ملخص

تحلل التوصية ITU-T X.1603 متطلبات أمن البيانات لخدمة المراقبة في الحوسبة السحابية وتشمل متطلبات نطاق بيانات المراقبة، ودورة حياة هذه البيانات، والمتطلبات الأمنية للحصول عليها، والمتطلبات الأمنية لحفظها. وتشمل متطلبات نطاق بيانات المراقبة كلاً من نطاق المراقبة اللازم الذي ينبغي أن يوفره مقدمو الخدمة السحابية (CSP) للحفاظ على أمن الخدمة وأكبر نطاق مراقبة لمقدمي الخدمة السحابية. وتشمل دورة حياة بيانات المراقبة استحداث البيانات وحفظها واستخدامها ونقلها وعرضها والتخلص منها والنسخ الاحتياطي لها. وتحدد عملية الحصول على بيانات المراقبة المتطلبات الأمنية لتقنيات الحصول على البيانات في خدمة المراقبة، بينما تحدد عملية حفظ بيانات المراقبة المتطلبات الأمنية اللازمة لمقدمي الخدمة السحابية لحفظ بيانات المراقبة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1603	2018-03-29	17	11.1002/1000/13406

مصطلحات أساسية

الحوسبة السحابية، أمن البيانات، المراقبة.

* 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.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة 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).

ملاحظـــة

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

والتقيّد 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 "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" 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 تلقّى 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

التوصية ITU-T X.1603

متطلبات أمن البيانات لخدمة المراقبة في الحوسبة السحابية

1 مجال التطبيق

تصف هذه التوصية متطلبات أمن البيانات لخدمة المراقبة في الحوسبة السحابية. وتحلل التوصية التهديدات والتحديات المتعلقة بأمن البيانات المرتبطة بخدمة المراقبة في بيئة الحوسبة السحابية، وتصف متطلبات أمن البيانات في خدمة المراقبة بما في ذلك نطاق البيانات ودورة حياة البيانات وتحصيل البيانات وتخزين البيانات. ويمكن لمقدمي الخدمات السحابية (CSP)، الذين يقدمون خدمات المراقبة إلى عملاء الخدمة السحابية (CSC)، استخدام هذه التوصية.

2 المراجع

لا يوجد.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تعرِّف هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 **استيقان** [b-NIST-SP-800-53]: التحقّق من هوية المستعمل أو العملية أو الجهاز، غالباً كشرط أساسي للسماح بالنفاذ إلى الموارد في نظام المعلومات.

2.1.3 **قدرة** [b-ISO/IEC 19440]: القدرة على أداء نشاط معين.

3.1.3 **الحوسبة السحابية** [b-ITU-T Y.3500]: نموذج للتمكين من النفاذ الشبكي إلى مجموعة قابلة للزيادة ومرنة من الموارد المادية أو الافتراضية التي يمكن تقاسمها والتزود بها وإدارتها على أساس الخدمة الذاتية وعند الحاجة.

ملاحظة – تشمل أمثلة الموارد الخدمات وأنظمة التشغيل والشبكات والبرمجيات والتطبيقات ومعدات التخزين.

4.1.3 **خدمة سحابية** [b-ITU-T Y.3500]: قدرة أو عدد أكبر من القدرات تُقدم عن طريق الحوسبة السحابية (انظر الفقرة 3.1.3) وتُلبى باستخدام سطح بيني معلن.

5.1.3 **عميل الخدمة السحابية** [b-ITU-T Y.3500]: طرف (انظر الفقرة 15.1.3) يكون مرتبطاً بعلاقة تجارية لأغراض استخدام الخدمات السحابية (انظر الفقرة 4.1.3).

ملاحظة – لا تستوجب العلاقة التجارية بالضرورة وجود اتفاقات مالية.

6.1.3 **شريك في الخدمة السحابية** [b-ITU-T Y.3500]: طرف (انظر الفقرة 15.1.3) يشارك في دعم أنشطة إما مقدم الخدمة السحابية (انظر الفقرة 7.1.3) أو عميل الخدمة السحابية (انظر الفقرة 5.1.3)، أو كليهما.

7.1.3 **مقدم الخدمة السحابية** [b-ITU-T Y.3500]: طرف (انظر الفقرة 15.1.3) يتيح الخدمات السحابية (انظر الفقرة 4.1.3)

8.1.3 **مستعمل الخدمة السحابية** [b-ITU-T Y.3500]: شخص طبيعي أو كيان يعمل بالنيابة عنه يرتبط بأحد عملاء الخدمة السحابية (انظر الفقرة 5.1.3) ويستعمل الخدمات السحابية (انظر الفقرة 4.1.3).

ملاحظة – تشمل أمثلة هذه الكيانات الأجهزة والتطبيقات.

9.1.3 **الاتصالات كخدمة (CaaS)** [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرة المقدّمة لعميل الخدمة السحابية (انظر الفقرة 5.1.3) متمثلة بالاتصالات والتعاون في الوقت الفعلي.

ملاحظة – يمكن للاتصالات كخدمة أن توفر قدرات من نوع قدرات المنصة ومن نوع قدرات التطبيق على السواء.

10.1.3 **الحوسبة السحابية المشتركة** [b-ITU-T Y.3500]: نموذج لنشر الحوسبة السحابية تدعم فيه الخدمات السحابية (انظر الفقرة 4.1.3) حصراً مجموعة محددة من عملاء الخدمة السحابية (انظر الفقرة 5.1.3) التي تتشارك فيه، ويتم فيه التشارك في الاحتياجات والعلاقات فيما بينهم ويتحكم في الموارد المعتمدة عضو واحد من أعضاء المجموعة على الأقل.

11.1.3 **مشرف أعلى** [b-NIST-SP-800-125]: مكوّنة التمثيل الافتراضي التي تدير أنظمة التشغيل الخاصة بالضيوف على حاسوب مضيف وتتحكم بتدفق التعليمات بين أنظمة التشغيل الخاصة بالضيوف والتجهيزات المادية.

12.1.3 **البنية التحتية كخدمة (IaaS)** [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية (انظر الفقرة 5.1.3) من نوع قدرات البنية التحتية.

ملاحظة – لا يقوم عميل الخدمة السحابية (انظر الفقرة 5.1.3) بإدارة الموارد المادية أو الافتراضية الأساسية أو بالتحكم بها بل تكون لديه سيطرة على أنظمة التشغيل والخزن والتطبيقات المنتشرة التي تستخدم الموارد المادية والافتراضية. وقد تتوفر لدى عميل الخدمة السحابية (انظر الفقرة 5.1.3) أيضاً قدرة محدودة على التحكم ببعض مكونات الربط الشبكي (مثل جدران الحماية لدى المضيف).

13.1.3 **تعدد الشاغلين** [b-ITU-T Y.3500]: توزيع الموارد المادية والافتراضية بحيث يتم عزل الشاغلين المتعددين (انظر الفقرة 24.1.3) وحساباتهم وبياناتهم عن بعضهم البعض، ويكون النفاذ غير ممكن فيما بين بعضهم البعض.

14.1.3 **الشبكة كخدمة (NaaS)** [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرة المقدمة لعميل الخدمة السحابية (انظر الفقرة 5.1.3) متمثلة في قدرة توصيلية النقل والقدرات المتصلة بالشبكات.

ملاحظة – يمكن أن توفر الشبكة كخدمة أياً من أنواع القدرات السحابية الثلاثة.

15.1.3 **الطرف** [b-ISO/IEC 27729]: شخص طبيعي أو اعتباري، اكتسب الشخصية الاعتبارية أم لم يكتسبها، أو مجموعة تضم كليهما.

16.1.3 **المعلومات المحدِّدة لهوية شخص** [b-ISO/IEC 29100]: معلومات (أ) يمكن أن تستخدم للتعرّف إلى هوية الشخص الذي تتعلق به هذه المعلومات، أو (ب) قد تكون مرتبطة بشكل مباشر أو غير مباشر بهوية الشخص المراد التعرف عليه من خلالها.

17.1.3 **المنصات كخدمة (PaaS)** [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية (انظر الفقرة 5.1.3) من نوع قدرات المنصة.

18.1.3 **الخدمة السحابية الخاصة** [b-ITU-T Y.3500]: نموذج لنشر الحوسبة السحابية (4.1.3) يشارك فيه حصراً عميل واحد للخدمة السحابية (انظر الفقرة 5.1.3) ويتم في إطاره التحكم بالموارد من قبل عميل الخدمة السحابية (انظر الفقرة 5.1.3).

19.1.3 **الخدمة السحابية العامة** [b-ITU-T Y.3500]: نموذج لنشر الحوسبة السحابية (انظر الفقرة 4.1.3) يُحتمل أن يتوفر لأي عميل من عملاء الخدمة السحابية (انظر الفقرة 5.1.3) ويتم في إطاره التحكم بالموارد من قبل مقدم الخدمة السحابية (انظر الفقرة 7.1.3).

20.1.3 **ميدان أمني** [b-ITU-T X.810]: مجموعة عناصر وسياسة أمن وسلطة أمن ومجموعة أنشطة ذات صلة بالأمن تدار فيها العناصر من أجل الأنشطة المحددة طبقاً لسياسة الأمن وتعمد سلطة الأمن إلى تطبيق سياسة الأمن بالنسبة لميدان الأمن.

21.1.3 **حادث أمني** [b-ITU-T E.409]: الحادث الأمني هو أي حدث سلبي يمكن أن تُهدَّد فيه بعض جوانب الأمن.

22.1.3 **اتفاق على مستوى الخدمة (SLA)** [b-ISO/IEC 20000-1]: اتفاق موثّق مُبرم بين مقدم الخدمة والعميل تُحدَّد فيه الخدمات وأهداف الخدمات.

الملاحظة 1 – يمكن أيضاً أن يُبرم الاتفاق على مستوى الخدمة بين مقدم الخدمة ومورّد أو مجموعة داخلية أو عميل يقوم بدور المورّد.

الملاحظة 2 – يمكن أن يكون الاتفاق على مستوى الخدمة مدرجاً في عقد أو أي نوع آخر من الاتفاقات الموثّقة.

23.1.3 **البرمجيات كخدمة (SaaS)** [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية (انظر الفقرة 5.1.3) من نوع قدرات التطبيقات.

24.1.3 **شاغل** [b-ITU-T Y.3500]: مستعمل واحد أو أكثر من مستعملي الخدمات السحابية (انظر الفقرة 8.1.3) الذين يتقاسمون مجموعة من الموارد المادية والافتراضية.

25.1.3 **تهديد** [b-ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب قد يُلحق ضرراً بالنظام أو المنظمة.

26.1.3 **نقطة ضعف** [b-NIST-SP-800-30]: ثغرة أو مكمن ضعف في نظام المعلومات أو إجراءات أمن النظام أو أدوات الرقابة الداخلية أو التنفيذ يمكن استغلاله من قبل المصدر المهدِّد.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 **بيانات المراقبة**: بيانات المراقبة هي مخرجات خدمة المراقب السحابي التي تساعد مقدم الخدمة السحابية (CSP) وعملاء الخدمة السحابية (CSC) على إدارة المنصات السحابية والموارد السحابية.

2.2.3 **خدمة المراقب** [b-ITU-T Y.3502]: يراقب نشاط خدمة المراقب جودة الخدمة المقدَّمة فيما يتعلق بمستويات الخدمة على النحو المحدد في اتفاق مستوى الخدمة (SLA) بين عميل الخدمة السحابية ومقدم الخدمة السحابية.

3.2.3 **بيانات المراقبة الضرورية**: تُستخدم بيانات المراقبة الضرورية للالتزام باتفاقات مستوى الخدمة (SLA). ويمكن أن تساعد بيانات المراقبة الضرورية مقدم الخدمة السحابية (CSP) على إبقاء منصات الحوسبة السحابية آمنة ومستقرة. ويمكن أن تشمل بيانات المراقبة الضرورية، على سبيل المثال لا الحصر، بيانات مراقبة نظام الإدارة وبيانات مراقبة الموارد المادية وبيانات مراقبة الشبكة وما إلى ذلك. ويستخدم مقدمو الخدمات السحابية أساساً بيانات المراقبة الضرورية ولكن يمكن أيضاً إطلاع عملاء الخدمة السحابية (CSC) عليها.

4.2.3 **بيانات المراقبة الاختيارية**: تقدَّم بيانات المراقبة الاختيارية بناء على طلب عملاء الخدمة السحابية (CSC) ومن أجل تقديم خدمة المراقب السحابي. ويمكن أن تشمل بيانات المراقبة الاختيارية، على سبيل المثال لا الحصر، بيانات مراقبة الآلة الافتراضية، وبيانات مراقبة خدمة تخزين البيانات، وتطبيق عملاء الخدمة السحابية المعني ببيانات المراقبة السحابية، وما إلى ذلك.

5.2.3 **آلة افتراضية (VM)**: نسخة منطقية ومستقلة وفعالة تكون مطابقة لآلة حقيقية.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

API سطح بيني لبرمجة التطبيقات *(Application Programming Interface)*

BCP خطة الاستمرارية التجارية *(Business Continuity Plan)*

CaaS الاتصالات كخدمة *(Communications as a Service)*

CPU وحدة المعالجة المركزية *(Central Processing Unit)*

CSC عميل الخدمة السحابية *(Cloud Service Customer)*

CSN شريك في الخدمة السحابية *(Cloud Service Partner)*

CSP مقدم الخدمة السحابية *(Cloud Service Provider)*

CSU مستعمل الخدمة السحابية *(Cloud Service User)*

DDOS رفض الخدمة الموزّع *(Distributed Denial of Service)*

DNS نظام أسماء الميادين *(Domain Name System)*

DOS رفض الخدمة *(Denial of Service)*

IaaS البنية التحتية كخدمة *(Infrastructure as a Service)*

IAM إدارة خدمات الهوية والنفاذ *(Identity and Access Management)*

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IT تكنولوجيا المعلومات *(Information Technology)*

NaaS الشبكات كخدمة *(Network as a Service)*

OS نظام التشغيل *(Operating System)*

PaaS المنصات كخدمة *(Platform as a Service)*

PII المعلومات المحددة لهوية شخص *(Personally Identifiable Information)*

PKI البنية التحتية للمفاتيح العمومية *(Public Key Infrastructure)*

SaaS البرمجيات كخدمة *(Software as a Service)*

SIM وحدة هوية المشترك *(Subscriber Identity Module)*

SLA اتفاق على مستوى الخدمة *(Service Level Agreement)*

VM آلة افتراضية *(Virtual Machine)*

5 الاصطلاحات

يتعين فهم المصطلحات الأساسية التالية في هذه التوصية على النحو التالي:

"**يجب**" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

"**يوصى**" كلمة تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

"**يحظر**" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

"**من الجائز**" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه التوصية في نفس الوقت.

6 نظرة عامة

تحلل هذه التوصية متطلبات أمن البيانات لخدمة المراقبة في الحوسبة السحابية بما في ذلك نطاق بيانات المراقبة ودورة حياة بيانات المراقبة والتهديدات والتحديات الأمنية ومتطلبات أمن البيانات المتعلقة بالحوسبة السحابية.

ويصف نطاق بيانات المراقبة نمطين من بيانات المراقبة السحابية: ضروري واختياري، ويفسر كذلك حالات الاستخدام.

وتصف دورة حياة بيانات المراقبة، والتهديدات والتحديات الأمنية، التهديدات للمحتوى والأمن، وصعوبات جمع بيانات المراقبة السحابية وتخزينها واستخدامها والانتقال بها وتحليلها وعرضها وإتلافها والحصول على نسخ رديفة عنها.

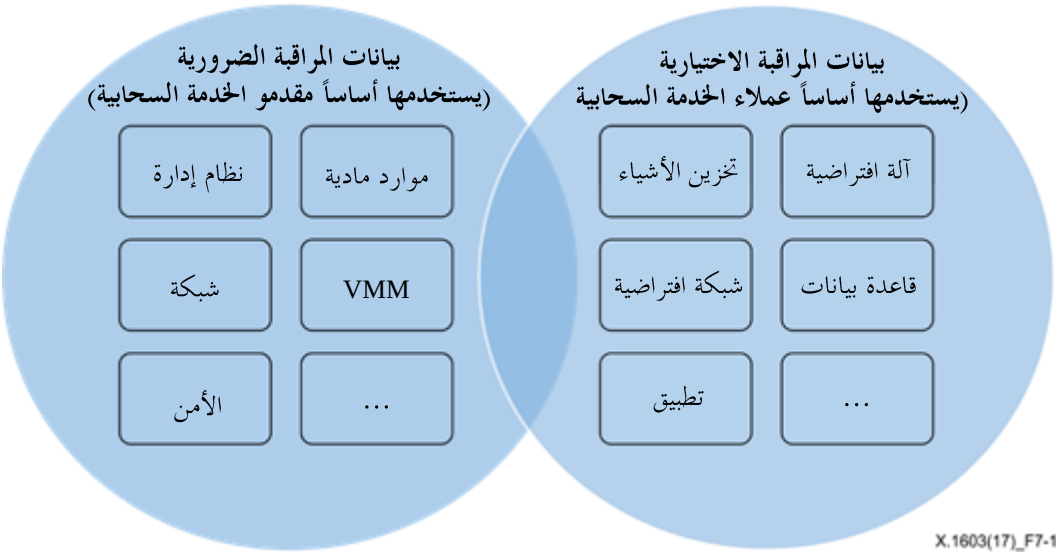
وتصف متطلبات أمن بيانات المراقبة المتطلبات التفصيلية لكل مرحلة من مراحل دورة حياة بيانات المراقبة السحابية.

7 نطاق بيانات المراقبة في الحوسبة السحابية

يوجد، في بيئة الحوسبة السحابية، نمطان من بيانات المراقبة: بيانات المراقبة الضرورية وبيانات المراقبة الاختيارية.

وبيانات المراقبة الضرورية هي التي تستخدم للالتزام باتفاقات مستوى الخدمة (SLA). ويمكن أن تساعد بيانات المراقبة الضرورية مقدم الخدمة السحابية في تشغيل منصة الحوسبة السحابية بشكل آمن ومستقر. ويمكن أن تشمل بيانات المراقبة الضرورية، على سبيل المثال لا الحصر، بيانات مراقبة نظام الإدارة، وبيانات مراقبة الموارد المادية، وبيانات مراقبة الشبكة. ويستخدم مقدمو الخدمات السحابية أساساً بيانات المراقبة الضرورية ولكن يمكن أيضاً إطلاع عملاء الخدمة السحابية (CSC) عليها.

أما بيانات المراقبة الاختيارية فهي البيانات التي تقدَّم بناء على طلب عميل الخدمة السحابية كي يقدم مقدم الخدمة السحابية خدمة المراقبة. ويمكن أن تشمل بيانات المراقبة الاختيارية، على سبيل المثال لا الحصر، بيانات مراقبة الآلة الافتراضية وبيانات مراقبة خدمة تخزين البيانات وبيانات عملاء الخدمة السحابية (CSC) المرتبطة بمراقبة تطبيقهم على الحيز السحابي.



الشكل 7-1 – حالات استخدام نمطين من بيانات المراقبة

ويستخدم مقدمو الخدمات السحابية أساساً بيانات المراقبة الضرورية ولكن يمكن أيضاً أن يستخدمها عملاء الخدمة السحابية (CSC). فعلى سبيل المثال، يستخدم مقدمو الخدمات السحابية أساساً بيانات مراقبة الموارد المادية السحابية للحفاظ على استقرار المنصة السحابية، ولكن يمكن أيضاً أن يستخدمها عملاء الخدمة السحابية إذا كانت الموارد المادية السحابية مقدمة إلى العملاء كخدمة.

وتقدَّم بيانات المراقبة الاختيارية كطلب من عملاء الخدمة السحابية وهم أيضاً من يستخدمونها بصورة رئيسية. ويمكن لمقدمي الخدمات السحابية أيضاً استخدام بيانات مراقبة اختيارية للالتزام باتفاقات مستوى الخدمة. فعلى سبيل المثال، يمكن أن يتطلب عملاء الخدمة السحابية بياناتهم المرتبطة بمراقبة تطبيقاتهم في الحيز السحابي. ويقدِّم مقدم الخدمة السحابية هذه البيانات التي تُستخدم لتحسين إدارة تطبيقاتهم في الحيز السحابي. فعلى سبيل المثال، يمكن لمقدم الخدمة السحابية استخدام بيانات مراقبة قاعدة البيانات كخدمة (DBaaS) للحفاظ على أمن واستقرار موارد قاعدة البيانات والخدمة في الحيز السحابي.

ويوضح الشكل 7-1 العلاقة بين هذين النمطين من بيانات المراقبة.

8 مراقبة دورة حياة البيانات في الحوسبة السحابية

تصف هذه الفقرة دورة حياة بيانات المراقبة في الحوسبة السحابية وتوضح الاختلافات الرئيسية بينها وبين دورة حياة البيانات الأخرى في الحوسبة السحابية.

1.8 جمع بيانات المراقبة

تنتج عملية جمع بيانات المراقبة عن تحصيل بيانات المراقبة ونقل تلك البيانات إلى مخدِّم تخزين. وتُنشأ معظم بيانات المراقبة باستخدام عميل الخدمة السحابية للخدمة السحابية. ويمكن أيضاً إنشاء بيانات المراقبة الضرورية من خلال أنشطة مراقبة خدمة سحابية أخرى.

2.8 تخزين بيانات المراقبة

بعد إنشاء مجموعة بيانات المراقبة، يمكن تخزين بيانات المراقبة السحابية في الموارد السحابية لعميل الخدمة السحابية محلياً أو في مخدمات تخزين بيانات المراقبة لدى مقدم الخدمة السحابية.

3.8 استخدام بيانات المراقبة

يمكن استخدام بيانات المراقبة للمحافظة على أداء وأمن المنصة السحابية والخدمة السحابية من جانب مقدم الخدمة السحابية؛ ويمكن أيضاً أن تستخدم للحفاظ على أداء الموارد السحابية وأمنها من جانب عملاء الخدمة السحابية (CSC).

4.8 انتقال بيانات المراقبة

عند انتقال الموارد السحابية، يمكن لبيانات المراقبة أن تنتقل إلى جانب الموارد السحابية.

5.8 تحليل بيانات المراقبة

يمكن لمقدم الخدمة السحابية وعميل الخدمة السحابية تحليل بيانات المراقبة لفهم حالة موارد المنصة السحابية من أجل تحسين إدارتها وتأمينها.

6.8 عرض بيانات المراقبة

يوصى بأن تكون بيانات المراقبة قابلة للعرض بطرق ذات مغزى ليستفاد منها في تحسين إدارة اتفاقات مستوى الخدمة والأمن السحابي. وبما أن حجم بيانات المراقبة السحابية يمكن أن يكون كبيراً جداً، يوصى بأن تلخَّص هذه البيانات بطريقة تمكن إدارتها وفهمها.

7.8 إتلاف بيانات المراقبة

للحفاظ على أمن بيانات المراقبة، يتعين على مقدم الخدمة السحابية أن يتلف بيانات المراقبة حسب طلب عملاء الخدمة السحابية (CSC).

ويمكن لمقدمي الخدمات السحابية أن يتلفوا اختيارياً بيانات المراقبة بعد فترة زمنية مناسبة تلي إنشاء بيانات المراقبة.

8.8 النسخ الرديف لبيانات المراقبة

يُتطلب إنشاء نسخ رديفة لبيانات المراقبة واستعادة البيانات من النسخ الرديفة.

9 التهديدات والتحديات الأمنية لمراقبة البيانات في الحوسبة السحابية

يرد وصف التهديدات والتحديات الأمنية لعميل الحوسبة السحابية ومقدم الحوسبة السحابية في الفقرتين 7 و8 على التوالي من التوصية [b-ITU-T X.1601]؛ وتواجه بيانات المراقبة السحابية أيضاً تهديدات وتحديات أمنية مماثلة معرفة في التوصية [b-ITU-T X.1601]. وتشمل بعض هذه التهديدات والتحديات الأمنية المتعلقة ببيانات المراقبة السحابية ما يلي على سبيل المثال لا الحصر:

أ) فقدان البيانات وتسربها؛

ب) النفاذ غير الآمن للخدمات؛

ج) النفاذ غير المرخص إلى الإدارة؛

د) التهديدات داخلية المصدر؛

ه) فقدان الثقة؛

و) غياب الإدارة؛

ز) فقدان الثقة؛

ح) عدم توفّر الخدمة؛

ط) سوء استعمال الملكية الفكرية؛

ي) تقاسم البيئة؛

ك) النزاع القضائي؛

ل) سوء التحول والتكامل.

وفي كل مرحلة من مراحل دورة حياة بيانات المراقبة، تواجه بيانات المراقبة السحابية بعض التهديدات والتحديات الأمنية الخاصة.

1.9 التهديدات والتحديات الأمنية في مرحلة جمع بيانات المراقبة

أ) جمع البيانات دون تخويل: يمكن أن يقوم مقدم الخدمة السحابية أو مهاجمون بجمع بيانات مراقبة عميل الحوسبة السحابية دون إذن أو تخويل.

ب) ثغرة أمنية في السطح البيني للتحصيل: يمكن أن يستخدم مهاجمون ثغرة أمنية في السطح البيني لتحصيل بيانات المراقبة.

ج) الانتحال: يمكن لمهاجمين انتحال صفة نظام إدارة أو مخدِّم تخزين البيانات لدى خدمة المراقبة السحابية، والتسبب بفقدان بيانات المراقبة.

د) العبث والاعتراض: يمكن لمهاجمين شن هجمات طرف متوسط بين طرفين أو هجمات أخرى على الشبكة للعبث ببيانات المراقبة أو اعتراضها.

هـ) النفاذ غير الآمن إلى الخدمات: في مرحلة جمع بيانات المراقبة، يمكن أن يتسبب النفاذ غير الآمن إلى السطوح البينية لجمع البيانات في فقدان بيانات المراقبة.

و) نفاذ الإدارة غير المخوَّل به: يمكن لنفاذ الإدارة غير المخوَّل به إلى نظام جمع بيانات المراقبة لدى مقدم الخدمة السحابية أو إلى نظام عميل الحوسبة السحابية أن يؤدي إلى فقدان بيانات المراقبة. فعلى سبيل المثال، قد يستغل مهاجمون ثغرة أمنية في النظام للحصول على نفاذ إدارة غير مخوَّل به إلى نظام عميل الحوسبة السحابية وتبديل عنوان بروتوكول الإنترنت في مقصد جمع المراقبة بالعنوان العائد إلى المهاجم.

2.9 التهديدات والتحديات الأمنية في مرحلة تخزين بيانات المراقبة

أ) فقدان البيانات وتسربها: بما أن بيئة الخدمة السحابية تنطوي عادةً على تعدد الشاغلين، فإن فقدان البيانات أو تسربها يشكل تهديداً خطيراً لعميل الخدمة السحابية ومقدم الخدمة السحابية. فقد يسبب غياب الإدارة المناسبة لمعلومات التجفير، مثل مفاتيح التجفير وشفرات الاستيقان وامتيازات النفاذ، أضراراً بالغة مثل فقدان البيانات وتسربها غير المتوقع إلى الخارج. وعلى سبيل المثال فإن النقص في الاستيقان والترخيص وضوابط المراجعة، والاستعمال غير المتوافق لمفاتيح التجفير و/أو الاستيقان، والإخفاقات التشغيلية، ومشاكل التخلص من المخلّفات، والمسائل القضائية والسياسية، ومصداقية مركز البيانات، والتعافي من الأعطال، هي كلها عوامل يمكن اعتبارها تهديدات كبرى.

ب) عدم توفر الخدمة: يمكن أن يهاجَم مخدِّم تخزين بيانات المراقبة بهجوم حرمان من الخدمة (DoS) أو هجوم حرمان من الخدمة موزَّع (DDoS)؛ وبالإضافة إلى ذلك، يمكن أن يتعطل عتاد تخزين بيانات المراقبة ويتسبب بفقدان البيانات أو إتلافها.

3.9 التهديدات والتحديات الأمنية في مرحلة استخدام بيانات المراقبة

أ) إساءة استخدام البيانات: يمكن لمقدم الخدمة السحابية أن يسيء استخدام بيانات مراقبة عميل الخدمة السحابية. إذ يمكن أن يستخدم مقدم الخدمة السحابية بيانات المراقبة للالتزام باتفاق مستوى الخدمة وتشغيل منصة الحوسبة السحابية ومواردها؛ ولكن يمكن أيضاً لمقدم الخدمة السحابية أن يستخدم بيانات مراقبة عميل الحوسبة السحابية لأغراض أخرى دون إذن العميل.

ب) تهديدات من الداخل: يمكن لموظف لدى مقدم الخدمة السحابية أو عميل الحوسبة السحابية إساءة استخدام بيانات مراقبة عميل الحوسبة السحابية لغير الأغراض المقصودة.

ج) ثغرة أمنية في النظام: يمكن فقدان بيانات المراقبة أثناء استخدامها بسبب ثغرات أمنية في النظام.

د) التنصت: يمكن أن يتنصت مهاجمون على بيانات المراقبة.

4.9 التهديدات والتحديات الأمنية في مرحلة انتقال بيانات المراقبة

أ) إساءة استخدام البيانات: يمكن لبيانات المراقبة أن تنتقل بين مواقع جغرافية مختلفة. ومن الأهمية بمكان عدم السماح بإساءة استخدام البيانات جراء انتقال بيانات المراقبة إلى مواقع مختلفة.

ب) الانتحال: يمكن لمهاجمين انتحال صفة نظام إدارة أو مخدِّم تخزين البيانات لدى خدمة المراقبة السحابية، والتسبب بفقدان بيانات المراقبة أو سوء استخدامها.

ج) العبث والاعتراض: يمكن لمهاجمين شن هجمات طرف متوسط بين طرفين أو هجمات أخرى على الشبكة للعبث ببيانات المراقبة أو اعتراضها.

5.9 التهديدات والتحديات الأمنية في مرحلة تحليل بيانات المراقبة

أ) إساءة استخدام البيانات: يمكن أن يسيء مقدمو الخدمة السحابية استخدام بيانات مراقبة عميل الحوسبة السحابية أثناء تحليل البيانات.

ب) ثغرة أمنية في النظام: يمكن فقدان بيانات المراقبة بسبب ثغرة أمنية في نظام تحليل البيانات.

ج) هجوم حرمان من الخدمة: يمكن أن يتعرض مخدِّم تحليل بيانات المراقبة لهجوم حرمان من الخدمة (DoS) أو هجوم حرمان من الخدمة موزَّع (DDoS).

6.9 التهديدات والتحديات الأمنية في مرحلة عرض بيانات المراقبة

أ) إساءة استخدام البيانات: يمكن أن يسيء مقدمو الخدمة السحابية استخدام بيانات مراقبة عميل الحوسبة السحابية أثناء عرض البيانات (أو أن يعرضوها بدون إذن عميل الخدمة السحابية).

ب) ثغرة أمنية في النظام: يمكن فقدان بيانات الإبلاغ والتحليل بسبب ثغرة أمنية في نظام عرض البيانات.

ج) التحريف: يمكن حرف بيانات مراقبة عميل الخدمة السحابية عن صحيح معناها أثناء عرض البيانات.

7.9 التهديدات والتحديات الأمنية في مرحلة إتلاف بيانات المراقبة

أ) الانتحال: يمكن لمهاجمين انتحال صفة نظام إدارة خدمة المراقبة السحابية، والتسبب بفقدان بيانات المراقبة الأخرى.

ب) ثغرة أمنية في نظام التشغيل: يمكن فقدان بيانات المراقبة أثناء استخدام البيانات بسبب ثغرة أمنية في النظام.

8.9 التهديدات والتحديات الأمنية في مرحلة النسخ الرديف لبيانات المراقبة

أ) ثغرة أمنية في نظام التشغيل: يمكن فقدان بيانات المراقبة أثناء النسخ الرديف للبيانات مما يؤدي إلى عجز عن استعادة البيانات بسبب ثغرة أمنية في النظام.

10 المتطلبات الأمنية لبيانات المراقبة في الحوسبة السحابية

تحدد هذه الفقرة متطلبات أمن البيانات لخدمة المراقبة في الحوسبة السحابية.

1.10 المتطلبات الأمنية لمراقبة جمع البيانات

إن متطلبات أمن البيانات الخاصة بجمع بيانات المراقبة تتضمن ما يلي:

أ) لا يُتطلب إنشاء بيانات مراقبة اختيارية إلا بناء على طلب عميل الخدمة السحابية؛

ب) يوصى بتقديم إشعار إلى عميل الخدمة السحابية عند إنشاء بيانات المراقبة الضرورية؛

ج) يوصى بإخطار عميل الخدمة السحابية بنطاق بيانات المراقبة؛

د) يُتطلب الحفاظ على سلامة ودقة بيانات المراقبة؛

ه) يوصى باستخدام التقنيات المعيارية لتحصيل البيانات؛

و) يوصى بتزويد السطوح البينية لتحصيل بيانات المراقبة بأساليب للتحكم في النفاذ مثل قائمة بيضاء وقائمة سوداء، وما إلى ذلك؛

ز) يوصى بتقديم أساليب تجفير لضمان أمن السطح البيني لتحصيل بيانات المراقبة؛

ح) يوصى باستخدام بروتوكولات الشبكة المعيارية بين الموارد السحابية ومخدمات تخزين بيانات المراقبة.

ويعرض الجدول 10-1 تقابلاً موجزاً بين التهديدات الأمنية لجمع بيانات المراقبة وبين المتطلبات الأمنية.

الجدول 10-1: جمع بيانات المراقبة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
جمع البيانات دون تخويل	أ)، ب)، ج)
الثغرات الأمنية في السطح البيني للتحصيل	د)، ه)، و)، ز)
الانتحال	د)، ه)، و)، ز)، ح)
العبث والاعتراض	ح)
النفاذ إلى الخدمة غير الآمن	ب)، د)، ه)، و)، ز)، ح)
النفاذ الإداري غير المخوّل به	د)، ه)، و)، ز)، ح)

2.10 المتطلبات الأمنية لتخزين بيانات المراقبة

إن متطلبات أمن البيانات الخاصة بتخزين بيانات المراقبة تتضمن ما يلي:

أ) يوصى بأن يقدم مقدم الخدمة السحابية الأساليب المناسبة للتحكم في النفاذ إلى مخدمات تخزين بيانات المراقبة؛

ب) يوصى بأن يحدد مقدم الخدمة السحابية الفترة الزمنية القصوى للاحتفاظ ببيانات المراقبة؛

ج) يوصى بأن يقدم مقدم الخدمة السحابية أساليب تجفير مناسبة لمراقبة البيانات.

ويعرض الجدول 10-2 تقابلاً موجزاً بين التهديدات الأمنية لتخزين بيانات المراقبة وبين المتطلبات الأمنية.

الجدول 10-2: تخزين بيانات المراقبة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

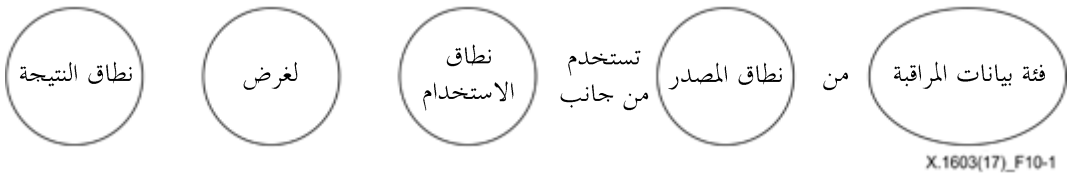
التهديدات الأمنية	المتطلبات الأمنية
فقدان البيانات وتسربها	أ)، ب)، ج)
عدم توفر الخدمة	أ)، ج)

3.10 المتطلبات الأمنية لاستخدام بيانات المراقبة

إن متطلبات أمن البيانات الخاصة باستخدام بيانات المراقبة تتضمن ما يلي:

أ) يُتطلب أن يحدد مقدم الخدمة السحابية بوضوح لعميل الخدمة السحابية كيفية استخدام بيانات المراقبة؛

ب) يوصى بأن يقدم مقدم الخدمة السحابية إلى عميل الخدمة السحابية إعلان رسمي عن استخدام بيانات المراقبة، مثل ذلك المبين في الشكل 10-1.



الشكل 10-1 – الإعلان الموصى به عن استخدام بيانات المراقبة

ج) يُتطلب أن يقدم مقدم الخدمة السحابية إشعاراً وأن يحصل على إذن عميل الخدمة السحابية قبل استخدام بيانات المراقبة لغير الغرض المقصود؛

د) يُتطلب أن يدعم مقدم الخدمة السحابية تسجيل استخدام بيانات المراقبة وتدقيقه.

ويعرض الجدول 10-3 تقابلاً موجزاً بين التهديدات الأمنية لاستخدام بيانات المراقبة وبين المتطلبات الأمنية.

الجدول 10-3: استخدام بيانات المراقبة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
إساءة استخدام البيانات	أ)، ب)، ج)، د)
التهديدات من الداخل	أ)، ب)، ج)، د)
الثغرات الأمنية في النظام	د)
التنصت	د)

4.10 المتطلبات الأمنية لانتقال بيانات المراقبة

إن متطلبات أمن البيانات الخاصة بانتقال بيانات المراقبة تتضمن ما يلي:

أ) يوصى بأن يقدم مقدم الخدمة السحابية إخطاراً إلى عميل الخدمة السحابية بشأن انتقال بيانات المراقبة؛

ب) يُتطلب أن يضمن مقدم الخدمة السحابية الإرسال الآمن أثناء انتقال بيانات المراقبة؛

ج) يُتطلب أن يدعم مقدم الخدمة السحابية تسجيل وتدقيق عمليات انتقال بيانات المراقبة.

ويعرض الجدول 10-4 تقابلاً موجزاً بين التهديدات الأمنية لانتقال بيانات المراقبة وبين المتطلبات الأمنية.

الجدول 10-4: انتقال بيانات المراقبة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
إساءة استخدام البيانات	أ)، ج)
الانتحال	ب)، ج)
العبث والاعتراض	ب)، ج)

5.10 المتطلبات الأمنية لتحليل بيانات المراقبة

إن متطلبات أمن البيانات الخاصة بتحليل بيانات المراقبة تتضمن ما يلي:

أ) يُتطلب أن يقدم مقدم الخدمة السحابية إخطاراً بشأن الغرض من مراقبة تحليل البيانات إلى عميل الخدمة السحابية؛

ب) يُتطلب من مقدم الخدمة السحابية تنفيذ دفاعات ضد الثغرات الأمنية في نظام تحليل بيانات المراقبة، فعلى سبيل المثال، ينبغي أن يمنع مقدم الخدمة السحابية فقدان البيانات وتسربها في نظام تحليل بيانات المراقبة.

ويعرض الجدول 10-5 تقابلاً موجزاً بين التهديدات الأمنية لتحليل بيانات المراقبة وبين المتطلبات الأمنية.

الجدول 10-5: تحليل بيانات المراقبة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
إساءة استخدام البيانات	أ)
ثغرة أمنية في النظام	ب)
هجوم حرمان من الخدمة (DoS)	ب)

6.10 المتطلبات الأمنية لعرض بيانات المراقبة

إن متطلبات أمن البيانات الخاصة بعرض بيانات المراقبة تتضمن ما يلي:

أ) يُتطلب أن يحافظ مقدم الخدمة السحابية على سلامة ودقة بيانات المراقبة المعروضة؛

ب) يُتطلب أن ينفذ مقدم الخدمة السحابية أساليب استيقان لحماية النفاذ إلى بيانات المراقبة المعروضة؛

ج) يُتطلب أن يدعم مقدم الخدمة السحابية دفاعات ضد الثغرات الأمنية في نظام عرض بيانات المراقبة، فعلى سبيل المثال، يمكن أن يستخدم مقدم الخدمة السحابية أساليب اختبار الاختراق لسد الثغرات الأمنية في نظام عرض بيانات المراقبة.

ويعرض الجدول 10-6 تقابلاً موجزاً بين التهديدات الأمنية لعرض بيانات المراقبة وبين المتطلبات الأمنية.

الجدول 10-6: عرض بيانات المراقبة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
إساءة استخدام البيانات	أ)، ب)
ثغرة أمنية في النظام	ب)، ج)
التحريف	أ)، ب)، ج)

7.10 المتطلبات الأمنية لإتلاف بيانات المراقبة

إن متطلبات أمن البيانات الخاصة بإتلاف بيانات المراقبة تتضمن ما يلي:

أ) يُتطلب أن يقدم مقدم الخدمة السحابية أساليب الإتلاف المناسبة لمراقبة البيانات؛

ب) يُتطلب أن يمنع مقدم الخدمة السحابية الإتلاف غير المقصود لبيانات المراقبة؛

ج) يُتطلب أن يمنع مقدم الخدمة السحابية الإتلاف غير الكامل لبيانات المراقبة؛

د) يُتطلب أن يمحو مقدم الخدمة السحابية أي مفاتيح تخص عميل الحوسبة السحابية في البيانات المشفرة؛

ه) يُتطلب أن يتلف مقدم الخدمة السحابية نسخ بيانات المراقبة؛

و) يُتطلب أن يقدم مقدم الخدمة السحابية إخطاراً بإتلاف بيانات المراقبة إلى عميل الخدمة السحابية.

ويعرض الجدول 10-7 تقابلاً موجزاً بين التهديدات الأمنية لإتلاف بيانات المراقبة وبين المتطلبات الأمنية.

الجدول 10-7: إتلاف بيانات المراقبة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
الانتحال	أ)، ب)، ج)، د)، ه)، و)
ثغرة أمنية في نظام التشغيل	ب)، ج)، د)، ه)، و)

8.10 المتطلبات الأمنية للنسخ الرديف لبيانات المراقبة

إن متطلبات أمن البيانات الخاصة بالنسخ الرديف لبيانات المراقبة تتضمن ما يلي:

أ) يُتطلب أن يقدم مقدم الخدمة السحابية أساليب نسخ رديف لمنع فقدان بيانات المراقبة؛

ب) يُتطلب أن يحافظ مقدم الخدمة السحابية على سلامة ودقة بيانات المراقبة المستعادة؛

ج) يُتطلب أن يدعم مقدم الخدمة السحابية تسجيل وتدقيق استعادة بيانات المراقبة.

ويعرض الجدول 10-8 تقابلاً موجزاً بين التهديدات الأمنية للنسخ الرديف لبيانات المراقبة وبين المتطلبات الأمنية.

الجدول 10-8: النسخ الرديف لبيانات المراقبة: التهديدات الأمنية وما يقابلها من المتطلبات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
ثغرة أمنية في نظام التشغيل	أ)، ب)، ج)

بيبليوغرافيا

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004*), Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open System Interconnection – Security frameworks for open system: Overview*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture.*

[b-ISO/IEC 19440] ISO/IEC 19440 (2007), *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 19944] ISO/IEC 19944 (2016), *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1 (2011), *Information technology –Service management – Part1: Service management system requirements*.

[b-ISO/IEC 27000] ISO/IEC 27000 (2016), *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27729] ISO/IEC 27729 (2012), *Information and documentation – International standard name identifier (ISNI).*

[b-ISO/IEC 29100] ISO/IEC 29100 (2011), *Information technology –Security techniques – Privacy framework.*

[b-NIST-SP-800-30] NIST Special Publication 800-30 (2012), *Guide for Conducting Risk Assessments.*

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev.3 (2009), *Recommended Security Controls for Federal Information Systems and Organizations*.

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies.*

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing.*

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، 2019