التوصية

ITU-T X.1645 (09/2023)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية

متطلبات منصة الوعي الظرفي بأمن الشبكة لأغراض الحوسبة السحابية

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
الدليل	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	X.1099-X.1000
تطبيقات وخدمات آمنة (1)	X.1199-X.1100
الأمن السيبراني	X.1299-X.1200
تطبيقات وخدمات آمنة (2)	X.1499-X.1300
تبادل معلومات الأمن السيبراني	X.1599-X.1500
أمن الحوسبة السحابية	X.1699-X.1600
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
الاتصالات الكمومية	X.1729-X.1700
أمن البيانات	X.1799-X.1750
أمن شبكات الاتصالات المتنقلة الدولية–2020	X.1819-X.1800

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

التوصية ITU-T X.1645

متطلبات منصة الوعي الظرفي بأمن الشبكة لأغراض الحوسبة السحابية

ملخص

يُشتقّ الوعي الظرفي بأمن الشبكة (NSSA) من مفهوم "الوعي الظرفي". وعادةً ما يتضمن أربع عمليات: الحصول على البيانات، وتحليل الوضع الأمني، وتقييم الوضع الأمني، وتوقع اتجاه الوضع الأمني، ويتمتع عموماً بالقدرات التالية: 1) الكشف عن مختلف تهديدات الهجوم والسلوكيات الشاذة ونطاق تأثيرها ومراقبتها بشكل مستمر؛ 2) استخلاص البيانات وتحليل التهديدات وتتبع السلوكيات الشاذة؛ 3) التنبؤ الأمني والإنذار المبكر؛ 4) تصور الوضع الأمني.

وبالنسبة لموردي خدمات الحوسبة السحابية، تؤدي منصة الوعي الظرفي بأمن الشبكة (NSSA) دوراً مهماً في تحسين الحماية الأمنية للحوسبة السحابية، والقدرة على اكتشاف الثغرات الأمنية أو السلوكيات الشاذة، والقدرة على اتخاذ القرارات الأمنية والتصدي للطوارئ، بل يمكنها أن تساعد في تحسين آلية الإنذار المبكر للحوسبة السحابية.

وستقدم التوصية ITU-T X.1645 أولاً مفهوم الوعي الظرفي بأمن الشبكة وتطويره، وستناقش مزايا الوعي الظرفي بأمن الشبكة في التعامل مع التحديات الأمنية للحوسبة السحابية، ثم تهدف إلى توثيق متطلبات منصة الوعي الظرفي بأمن الشبكة لأغراض الحوسبة السحابية.

التسلسل التاريخي*

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد
1.0	ITU-T X.1645	2023-09-08	17	11.1002/1000/15527

مصطلحات أساسية

تحليل البيانات الضخمة، الحوسبة السحابية، الوعي الظرفي بأمن الشبكة، الوعي الظرفي.

* للنفاذ إلى توصية، ترجى كتابة العنوان https://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد.

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 سواءً 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/حقوق تأليف ونشر برمجيات 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 قواعد البيانات ذات الصلة لقطاع تقييس الاتصالات (ITU-T) في موقع قطاع تقييس الاتصالات http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1645

متطلبات منصة الوعي الظرفي بأمن الشبكة لأغراض الحوسبة السحابية

1 مجال التطبيق

تعرض هذه التوصية الوعي الظرفي بأمن الشبكة (NSSA) ومتطلبات منصة الوعي الظرفي بأمن الشبكة لأغراض الحوسبة السحابية. وتنطبق هذه التوصية على مقدمي خدمة الحوسبة السحابية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص أحكام هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، 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. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

لا توجد.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

تعرِّف هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الحوسبة السحابية (cloud computing) [b-ITU-T Y.3500]: نموذج للتمكين من النفاذ الشبكي إلى مجموعة قابلة للزيادة ومرنة من الموارد المادية أو الافتراضية التي يمكن التشارك بها وتهيئتها على أساس الخدمة الذاتية وإدارتها حسب الطلب.

2.1.3 خدمة سحابية (cloud service) [b-ITU-T Y.3500]: قدرة أو عدد أكبر من القدرات تُقدَّم عن طريق الحوسبة السحابية وتُستدعى باستعمال سطح بيني معرَّف.

3.1.3 عميل الخدمة السحابية (cloud service customer) [b-ITU-T Y.3500]: طرف يكون مرتبطاً بعلاقة تجارية لأغراض استعمال الخدمات السحابية.

4.1.3 مقدم الخدمة السحابية (cloud service provider) [b-ITU-T Y.3500]: طرف يتيح الخدمات السحابية.

5.1.3 نقطة ضعف (vulnerability) [b-NIST-SP-800-30]: مكمن ضعف في نظام المعلومات أو إجراءات أمن النظام أو أدوات الرقابة الداخلية أو التنفيذ يمكن استغلاله من جانب مصدر التهديد.

6.1.3 المعلومات المتعلقة بالتهديدات (threat intelligence) [b-ITU-T X.1217]: هي مجموعة معلومات منظمة تم تحليلها وتحسينها بشأن الهجمات الحالية والمحتملة التي قد تهدد منظمةً ما.

2.3 المصطلحات المعرّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 الوعي الظرفي (situational awareness): القدرة على تقييم الحالة الراهنة للعناصر في بيئة معينة، وعلاقاتها بأبعاد متعددة، بما في ذلك الوقت والمكان.

ملاحظة – يتحقق ذلك بجمع البيانات من مصادر متنوعة، وتجميع تلك البيانات، ثم تحليلها. والهدف من الوعي الظرفي هو دمج وتحليل المعلومات الواردة من مصادر مختلفة للتوصل إلى فهم شامل لمعناها.

2.2.3 الوعي الظرفي بأمن الشبكة (network security situational awareness) (NSSA): القدرة على تحديد وتقييم العناصر الأساسية لأمن الشبكة وتصنيفها وفقاً لقواعد تستعمل الأبعاد الزمنية والمكانية.

ملاحظة – تُستخدم هذه المعلومات لتقييم الحالة الأمنية الكلية للشبكة، والتنبؤ بالاتجاهات الأمنية الناشئة في الشبكات من خلال تقنيات مثل التحليل الإحصائي واستخلاص البيانات والذكاء الاصطناعي. ويمكن عرض الرؤى الناتجة في أنساق يمكن أن يقرأها الإنسان أو كمدخلات في أتمتة أمن الشبكة.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

AI	الذكاء الاصطناعي *(Artificial Intelligence)*
C&C	القيادة والتحكم *(Command and Control)*
CRUD	استحداث وقراءة وتحديث وحذف *(Create, Read, Update and Delete)*
CSC	عميل الخدمة السحابية *(Cloud Service Customer)*
CSP	مقدم الخدمة السحابية *(Cloud Service Provider)*
DDoS	الحرمان من الخدمة الموزَّع *(Distributed Denial of Service)*
DGA	خوارزمية إنشاء الميادين *(Domain Generation Algorithm)*
HBase	قاعدة بيانات Hadoop *(Hadoop Database)*
IDS	نظام كشف الاقتحام *(Intrusion Detection System)*
IPS	نظام منع الاقتحام *(Intrusion Prevention System)*
JDBC	توصيلية قاعدة بيانات Java *(Java Database Connectivity)*
MPP	معالجة متوازية كثيفة *(Massively Parallel Processing)*
NoSQL	لا تقتصر على لغة الاستجواب المهيكلة *(Not only Structured Query Language)*
NSSA	الوعي الظرفي بأمن الشبكة *(Network Security Situational Awareness)*
ODBC	التوصيلية المفتوحة لقاعدة البيانات *(Open Database Connectivity)*
SNMP	بروتوكول إدارة الشبكة البسيط *(Simple Network Management Protocol)*
SQL	لغة الاستجواب المهيكلة *(Structured Query Language)*
VM	الآلة الافتراضية *(Virtual Machine)*
VPN	شبكة خاصة افتراضية *(Virtual Private Network)*
WAF	جدار حماية تطبيقات الويب *(Web Application Firewall)*

5 الاصطلاحات

كلمات "**يلزم/يُتطلب/يتعين**" التي تدل على متطلب يجب التقيد به تماماً ولا يسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

كلمة "**يُوصى**" التي تدلّ على متطلب يُوصى به لكنه غير إلزامي في المطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

وفي متن هذه التوصية وملحقاتها، تظهر كلمات يتعين، ويتعين ألا، وينبغي، ويمكن. وفي هذه الحالة يكون تأويلها، على التوالي، على "يجب"، أو "يلزم"، أو "مطلوب"، و"يجب ألا"، أو "يلزم ألا"، أو "يحظر"، و"يوصي"، و"يجوز اختيارياً"، أو "من الجائز اختيارياً". ويأوّل انتفاء القصد المعياري عند ظهور مثل هذه العبارات أو الكلمات الرئيسية في تذييل أو في مادة موسومة صراحةً على أنها إعلامية.

6 تعريف بالوعي الظرفي بأمن الشبكة

في الوقت الحاضر، يجري تطوير هجمات على الشبكة نحو أهداف محددة، وعادةً ما تكون خطط المهاجمين محكمةً، ويشيع التغلغل الطويل الأجل. وفي المقابل، يتسم الدفاع الأمني بميزة "المواجهة الزمنية" النمطية. وفي معمارية الأمن التقليدية، تُنشر مكونات أو منتجات أمنية متنوعة مع ما يخصها من قواعد حماية، وسياسات تحذير، وآليات معالجة سجلات وتخزين، ولكنها تفتقر إلى آلية تنسيق بين المكونات والمنتجات. ويؤدي ذلك إلى مؤثرات التقوقع التي تضعف القدرة الدفاعية ضد هجمات متطورة أكثر سريةً ومهنيةً.

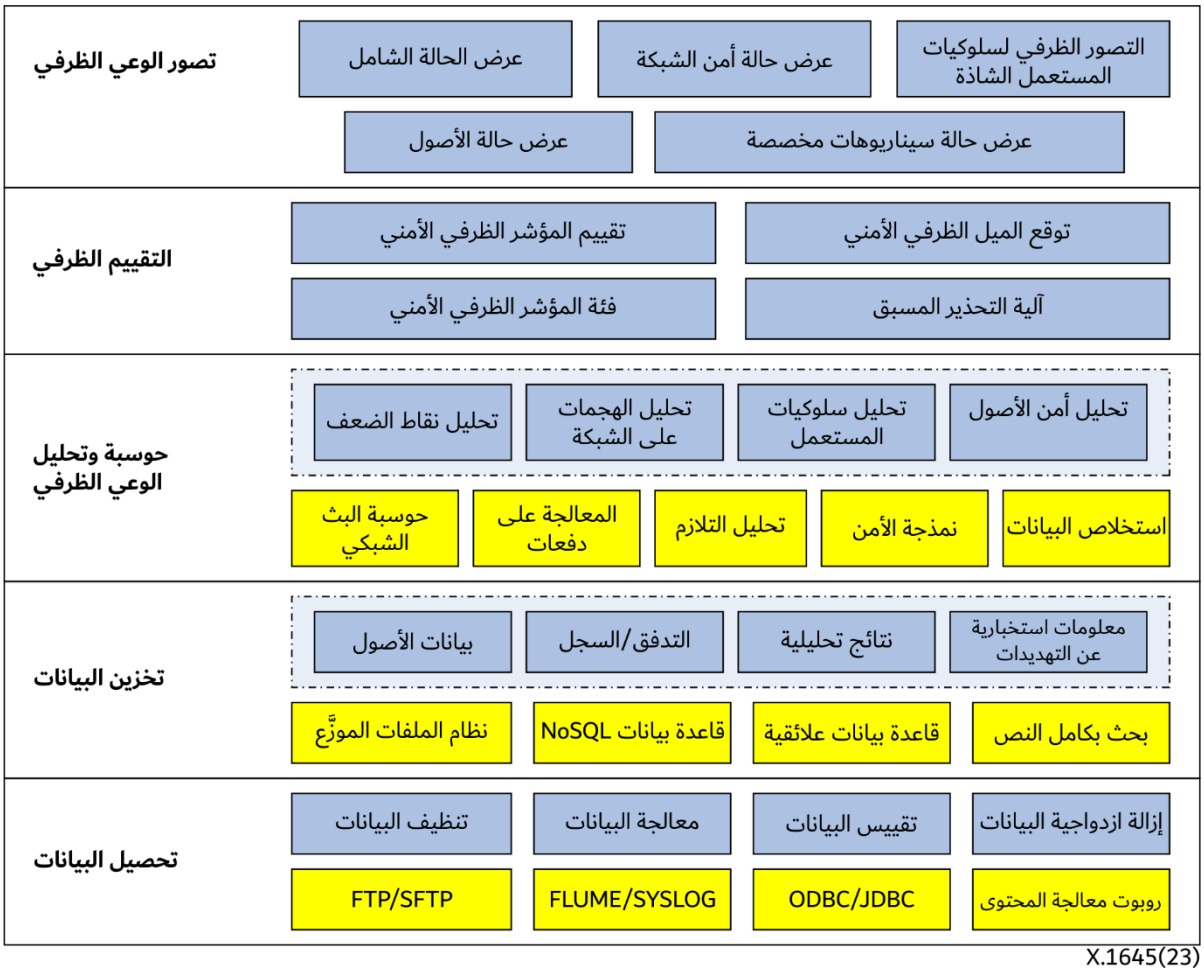
ويُشتقّ الوعي الظرفي بأمن الشبكة (NSSA) من مفهوم "الوعي الظرفي" وهو تطبيق معين في أمن الشبكة. وعادةً ما يتضمن أربع عمليات: الحصول على البيانات، والوقوف على الوضع الأمني، وتقييم الوضع الأمني، وتوقع اتجاه الوضع الأمني، ويتمتع عموماً بالقدرات التالية:

- الكشف عن مختلف تهديدات الهجوم بما في ذلك السلوكيات الشاذة ونطاق تأثيرها، ومراقبتها بشكل مستمر؛
- استخلاص البيانات وسبرها وتحليل التهديدات وتتبع السلوكيات الشاذة؛
- التنبؤ الأمني والإنذار المبكر؛
- تصور الوضع الأمني.

وفي سياق أمن الشبكة، يشير عدم تناظر المعلومات إلى سيناريو يمتلك فيه المهاجم معلومات أكثر من المنظمة نفسها عن أنظمتها أو شبكتها أو عملياتها. وفي مثل هذه الحالة، يكون المهاجمون في وضع أميَز فيما يتعلق بوضع الاستراتيجيات وتنفيذ الهجمات. ويكتسي الوعي الظرفي بأمن الشبكة أهميةً كبيرةً لمواجهة عدم تناظر المعلومات بين الهجوم والدفاع، وكذلك لتسريع التصدي للحوادث وإمكانية التتبع.

وفي الوقت نفسه، أتاح تطوير تحليل البيانات الضخمة والحوسبة السحابية والذكاء الاصطناعي (AI) فرصاً وقدرةً كبيرةً على تطوير الوعي الظرفي بأمن الشبكة. فعلى سبيل المثال، يمكن للوعي الظرفي بأمن الشبكة أن يدعم بفعالية التخزين الكثيف لسجلات الأمن والاستفادة منها واستخلاصها من خلال تحليل البيانات الضخمة، لتحقيق المراقبة المستمرة لحالات أمن الشبكة على نطاق واسع؛ ويمكن أن يقدم تطوير الذكاء الاصطناعي المزيد من أساليب التحليل وقدرات التنبؤ بالمخاطر للوعي الظرفي بأمن الشبكة، بما يمكن أن يحسّن بفعالية دقة التنبؤ؛ ويمكن أن يقدم تطوير الحوسبة السحابية معمارية بنية تحتية أكثر مرونةً واستقراراً للوعي الظرفي بأمن الشبكة.

ويرد في الشكل 6-1 الإطار النمطي لمنصة الوعي الظرفي بأمن الشبكة.



X.1645(23)

الشكل 6-1 – إطار منصة الوعي الظرفي بأمن الشبكة

7 التحليل

مع التطور السريع لتكنولوجيا الحوسبة السحابية ونضج نظامها الإيكولوجي، تمثل الحوسبة السحابية جيلاً جديداً من البنى التحتية الحرجة للمعلومات. وقد جلبت الحوسبة السحابية الكثير من الفوائد، بينما تواجه أيضاً قدراً أكبر بكثير من إشكالات الأمن وخاصة في التشغيل والصيانة، على غرار ما يلي:

1) مع الزيادة السريعة في الحجم، تنطوي أنواع متنوعة من المكونات الأمنية المنشورة في البنية التحتية للحوسبة السحابية على كميات هائلة من البيانات الأمنية والتحذيرات المتكررة. ويصعِّب هذا السيناريو على مهندسي التشغيل والصيانة التعامل معها ضمن نافذة زمنية محدودة.

2) تُعزَل معظم مكونات الأمن عن بعضها البعض، مما يجلب طبعاً مؤثر تقوقع. وسيصعِّب ذلك من تقديم آلية دفاع منسقة تنسيقاً جيداً في بيئة الحوسبة السحابية.

3) تتسم بيئة الحوسبة السحابية بالتعقيد عادةً وقد تتضمن منصةً سحابيةً عموميةً ومنصةً سحابيةً خاصةً ومنصةً سحابيةً هجينةً. ويصعِّب ذلك من اتخاذ قرارات أمنية معقولة نظراً لغياب منظور كلي وكامل لدى مقدمي خدمة الحوسبة السحابية وحتى لدى مستعملي الحوسبة السحابية.

ويُعتبر الوعي الظرفي بأمن الشبكة نهجاً مناسباً لحل هذه المشاكل. وبناءً على تكنولوجيا البيانات الضخمة، يستطيع الوعي الظرفي بأمن الشبكة أن يدعم بفعالية تخزين السجلات الأمنية الضخمة وغير المتجانسة واستعمالها واستخلاص البيانات منها. وعلاوةً على ذلك، يمكن، من خلال تحليل تلازم بيانات مختلفة متعددة، تنظيم مختلف المكونات الأمنية بفعالية وتحسين قدرة اكتشاف التهديدات وزيادة كفاءة مهندسي الأمن. ويمكن للوعي الظرفي بأمن الشبكة أن يقدم أيضاً قدرةً مرئيةً للوعي الكامل بالوضع الأمني

للحوسبة السحابية. وفي الوقت نفسه، من المناسب استعمال تكنولوجيا الذكاء الاصطناعي في الوعي الظرفي بأمن الشبكة الذي يمكن أن يساعد على تحسين قدرات الكشف والتشخيص والتنبؤ للوعي الظرفي بأمن الحوسبة السحابية.

وبالتالي، تؤدي منصة الوعي الظرفي بأمن الشبكة دوراً مهماً في تحسين الحماية الأمنية للحوسبة السحابية، والقدرة على اتخاذ القرارات الأمنية والتصدي للطوارئ، ومن ثم، يمكنها أن تساعد في تحسين آلية الإنذار المبكر لدى مقدمي خدمة الحوسبة السحابية.

وفي الوقت نفسه، بالنسبة لمنصة الوعي الظرفي بأمن الشبكة المنشورة في الحوسبة السحابية، فإنها تتطلب قدرات معينة على النحو التالي:

1) ينبغي أن تكيف عملية تحصيل البيانات التغيرات الدينامية للأصول في الحوسبة السحابية، حيث يمكن إنشاء أصول الحوسبة السحابية وإزالتها بصورة أكثر مرونةً وبتواتر أعلى بالمقارنة مع المعمارية التقليدية لتكنولوجيا المعلومات.

2) ينبغي لمنصة الوعي الظرفي بأمن الشبكة أن تكيف خصائص خدمة الحوسبة السحابية مثل التشارك في موارد الشاغلين المتعددين وإدارة الموارد المرنة، مما قد يؤدي إلى تغير سريع في مصادر البيانات. ومن شأن التغير السريع للشاغلين وخدمتهم أن يؤدي بما يقابل ذلك إلى تغيير تحصيل البيانات لمنصة الوعي الظرفي بأمن الشبكة.

3) ينبغي أن تواصل منصة الوعي الظرفي بأمن الشبكة التفاعل والتعاون مع منصة إدارة الحوسبة السحابية للنفاذ إلى مختلف أنواع البيانات مثل حالة التشغيل وسجلات أمن موارد الحوسبة السحابية لتحقيق رؤية عميقة/إدراك عميق لموارد الحوسبة السحابية، فعلى سبيل المثال لا يستطيع الوعي الظرفي بأمن الشبكة تجاوز منصة الإدارة السحابية لرصد توصيلات الشبكة بين الآلات الافتراضية في نفس منطقة شبكة الطبقة 2 من التوصيل البيني للأنظمة المفتوحة (OSI).

4) ينبغي لمنصة الوعي الظرفي بأمن الشبكة (NSSA) أن تدعم القدرة على النفاذ إلى البيانات من منصات سحابية متعددة لتحقيق منظور الأصول الموحدة للمستعملين إما في منصة سحابية هجينة أو منصة سحابية عمومية.

ويقدم تطبيق ونشر الوعي الظرفي بأمن الشبكة حلولاً ممكنةً للتحديات التقنية المذكورة أعلاه. ويمكن للوعي الظرفي بأمن الشبكة أن يستشعر مختلف الأحداث الأمنية والسلوكيات غير الطبيعية بشكل شامل وصحيح ودقيق بأبعاد الزمان والمكان على حد سواء، وأن يحلل العناصر الأمنية المتنوعة ويفهم الحالة الأمنية بأكملها ويتنبأ باتجاهاتها، مما سيساعد على تحسين قدرات التشغيل الأمني لدى مقدم الحوسبة السحابية ودعم اتخاذ القرارات الأمنية والتصدي للحوادث، وتحسين آلية الإنذار المبكر الأمني.

8 متطلبات منصة الوعي الظرفي بأمن الشبكة لأغراض الحوسبة السحابية

1.8 متطلبات تحصيل البيانات

1.1.8 آلية تحصيل البيانات

ينبغي أن تدعم عقد التحصيل لمنصة الوعي الظرفي بأمن الشبكة (NSSA) جمع أنواع مختلفة من البيانات، مثل سجلات حركة الشبكة، وسجلات النظام، وسجلات البرمجيات الوسيطة، وسجلات أمن البنية التحتية للحوسبة السحابية، في نهج نشط أو منفعل. ويجمع النهج النشط البيانات عن طريق المراقبة الدورية للأهداف أو مسحها، في حين أن النهج المنفعل يجمع البيانات عن طريق تلقي البيانات أو استيرادها بشكل أساسي من مصادر بيانات مختلفة.

1) يُتطلب أن يدعم تحصيل البيانات النهج النشط، مثل جمع البيانات من خلال المسح أو روبوت معالجة المحتوى أو البروتوكول البسيط لإدارة الشبكة (SNMP).

2) يُتطلب أن يدعم تحصيل البيانات النهج المنفعل، مثل تلقي البيانات بواسطة البروتوكول syslog، أو قناة NetFlow، واستيراد البيانات يدوياً.

وينبغي لقدرة تحصيل البيانات أن تتكيف مع بيئات الحوسبة السحابية بالأساليب التالية:

1) يوصى بأن يدعم تحصيل البيانات جمع البيانات عبر مختلف المنصات السحابية، مثل المنصات السحابية المتعددة والمنصات السحابية الهجينة.

2) يوصى بأن يستوعب تحصيل البيانات تغيرات الموارد الدينامية في بيئات الحوسبة السحابية.

3) يوصى لتحصيل البيانات بدعم جمع سجلات بيانات حركة الشبكة من الشرق إلى الغرب في منصات الحوسبة السحابية.

وينبغي أن تمتلك عقد التحصيل لمنصة الوعي الظرفي بأمن الشبكة (NSSA) القدرات التالية:

1) يُتطلب من عقد التحصيل أن تقوم بتصفية البيانات وفحص صحة البيانات، مثل نوع البيانات ومدى القيمة، وتصفية البيانات غير الصالحة وفقاً للسياسات المشكَّلة مسبقاً.

2) ويوصى بأن تنفذ عقد التحصيل آليةً لإعادة جمع البيانات في حالة حدوث أعطال في الجمع.

2.1.8 مصدر البيانات

ينبغي لمنصة الوعي الظرفي بأمن الشبكة (NSSA) أن تدعم عمليات طلب استحداث وقراءة وتحديث وحذف (CRUD) لبياناتها وأن تدعم جمع أنماط البيانات التالية:

1) يُتطلب دعم جمع بيانات أصول منصات الحوسبة السحابية مثل بيانات أصول مجموعات الموارد الافتراضية ومعدات الشبكة والجهات المضيفة والمعدات والأنظمة والبرمجيات الأمنية ومنصات إدارة الحوسبة السحابية.

2) يُتطلب دعم جمع مختلف أنواع بيانات السجلات، من قبيل سجلات النفاذ إلى الويب وسجلات الأمن وسجلات تشغيل الأعمال وسجلات تسجيل الدخول، من مصادر متعددة مثل الحواسيب المضيفة والبرمجيات الوسيطة ومنصات إدارة الحوسبة السحابية، ودعم تلقي نتائج تحليل السجلات من الأنظمة الأخرى.

3) يُتطلب أن تدعم جمع بيانات مواطن الضعف المختلفة من عدة معدات ومكونات منصات الحوسبة السحابية، مثل مواطن ضعف فيض الدارئ، ومواطن ضعف الحقن، ومواطن ضعف منطق الأعمال، ومواطن ضعف التصميم، ومواطن ضعف التشكيلة، وما إلى ذلك.

4) يُتطلب دعم جمع بيانات أحداث هجوم متعددة على الشبكة، مثل هجمات الحرمان من الخدمة الموزع (DDoS) وهجمات استغلال مواطن الضعف والنفاذ غير المجاز.

5) يُتطلب دعم جمع بيانات استخباراتية عن التهديدات، مثل بيانات استخباراتية عن التهديدات لبروتوكول الإنترنت/الميدان/محدِّد موقع الموارد الموحد (URL)، والعينات الخبيثة، والقائمة السوداء للقيادة والتحكم (C&C)، ومواطن الضعف.

3.1.8 المعالجة المسبقة للبيانات

لتلبية متطلبات جودة البيانات، يُتطلب من منصة الوعي الظرفي بأمن الشبكة (NSSA) تنفيذ تنظيف البيانات واصطفاؤها، وتقييسها وإنشاء تلازمها واكتمالها ودمجها واستنساخها في البيانات المجمعة، ثم تخزين البيانات المقيَّسة.

1) تنظيف البيانات: ينبغي لمنصة الوعي الظرفي بأمن الشبكة (NSSA) أن تدعم تنظيف البيانات في حال وجود إشكالات تتعلق بالأخطاء وعدم الاكتمال وعدم الصلاحية وغيرها من الإشكالات في البيانات المجمعة، بما في ذلك من خلال ما يلي:

- يُتطلب دعم تحويل البيانات ومعالجتها وتصفيتها تحرياً عن أنساق البيانات غير المتسقة وأخطاء إدخال البيانات وعدم اكتمالها.
- يوصى بدعم تصفية البيانات وتنظيفها استناداً إلى عمليات شرطية ومطابقة التعبير العادي وحسابات التعبير.
- يوصى بدعم إزالة تكرار البيانات.

2) تقييس البيانات: ينبغي لمنصة الوعي الظرفي بأمن الشبكة (NSSA) أن تدعم الأنساق الموحدة لمختلف أنواع البيانات غير المتجانسة وأن تحفظ البيانات الأصلية المجمعة، بما في ذلك من خلال ما يلي:

- يُتطلب دعم تقييس حقول البيانات على أساس قواعد حقول كل نمط من أنماط البيانات.
- يوصى بدعم الأنساق الموحدة للمحتوى الخام بواسطة التعبير العادي.
- يوصى بدعم الحفاظ على البيانات الأصلية المجمعة لدعم التحليل اللاحق لإمكانية التتبع والتطوير المخصص.

3) تلازم البيانات واكتمالها: يوصى بأن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) تلازم البيانات المقيَّسة واكتمالها بما يشمل معلومات المستعمل ومعلومات الأصول ومعلومات الموقع الجغرافي ومعلومات استخباراتية عن التهديدات، ويوصى بدعم اختيار بيانات ومجالات بعينها لاستكمالها.

4) دمج البيانات: يوصى بأن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) دمج البيانات المقيَّسة بناءً على القواعد المشكَّلة، ويوصى بدعم اختيار بيانات وحقول معينة لدمجها.

4.1.8 متطلبات أمن تحصيل البيانات

1) يُتطلب أن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) التحكم في النفاذ إلى عقد التحصيل ومراقبة عملية جمع البيانات مع إنذارات في الوقت المناسب في حال وقوع أحداث شاذة.

2) يُتطلب تقييد موقع تخزين البيانات المؤقت بشكل صارم أثناء عملية جمع البيانات التي لا يمكن تعديلها بشكل اعتباطي.

3) يُتطلب أن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) التصنيفات التراتبية وتعريفات البيانات التي جُمعت وأن تنفذ الحماية الأمنية مثل التجفير للبيانات الحساسة، مثل بيانات الأصول والبيانات التشغيلية وبيانات السجل.

4) يُتطلب أن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) إخفاء البيانات وإزالة الحساسية من البيانات الحساسة قبل المعالجة المسبقة للبيانات المجمعة وتحليلها وتلبية متطلبات الالتزام الأمني.

5) يُتطلب من منصة الوعي الظرفي بأمن الشبكة (NSSA) الحفاظ على سجل مجمع وتشغيلي للتمكن من توليد إنذارات بالأحداث الشاذة والتدقيق في الوقت المناسب، بما في ذلك ما يلي:

- يُتطلب تدقيق عمليات المستعملين والمديرين لكشف السلوكيات الضارة والإنذار بها والتصدي لها مثل إساءة استعمال البيانات.
- يوصى بالتنبيه بشأن انقطاعات الإرسال أثناء جمع البيانات.
- يوصى بالتنبيه إذا تجاوز تخزين البيانات عتبةً محددةً مسبقاً أثناء جمع البيانات وإرسالها.

2.8 متطلبات تخزين البيانات

ينبغي أن يطبق تخزين بيانات منصة الوعي الظرفي بأمن الشبكة (NSSA) تقنيات البيانات الضخمة لتلبية طلبات التخزين لبيانات النمو المستمر متعددة المصادر ومتعددة الأبعاد التي تولدها بيئة الحوسبة السحابية، مثل نتائج التحليل والمعلومات الاستخباراتية المتعلقة بالتهديدات الخارجية. ينبغي لمنصة الوعي الظرفي بأمن الشبكة أن تدعم آليات التخزين وفقاً لميادين وتصنيفات مختلفة لأنماط البيانات المتنوعة وأن تلبي متطلبات مختلف أساليب تحليل البيانات وعزلها. وفي الوقت نفسه، ينبغي أن تضمن منصة الوعي الظرفي بأمن الشبكة تيسر بيانات التخزين وسلامتها وكتمها.

1.2.8 تصنيف تخزين البيانات

يوصى بأن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) تخزين البيانات غير المهيكلة والبيانات المهيكلة والبيانات شبه المهيكلة وفقاً لمصادر البيانات المتنوعة وأن تدعم تصنيفات تخزين البيانات المتعددة، بما في ذلك تخزين البيانات العلائقية وقاعدة بيانات لا تقتصر على لغة الاستجواب المهيكلة (NoSQL) وتخزين الملفات الموزع والبحث الموزع عن النص الكامل.

ويوصى باستعمال تصنيفات تخزين البيانات في منصة الوعي الظرفي بأمن الشبكة (NSSA) على النحو المبين في الجدول 8-1.

الجدول 8-1 تصنيف البيانات

مصدر البيانات	محتويات البيانات	حجم البيانات	تصنيف التخزين (الموصى به)
مضيف المنصة السحابية/الحاوية/ نظام التشغيل	سجلات التشغيل وسجلات الأمن وبيانات حالة التشغيل وملفات التشكيلة، وما إلى ذلك.	كبير	تخزين ملفات موزَّع/البحث الموزّع عن نص كامل/قاعدة بيانات NoSQL
منصة إدارة الحوسبة السحابية	سجلات النفاذ وسجلات التشغيل، وملفات التشكيلة، وبيانات تدفق العمل، وما إلى ذلك.	متوسط	تخزين ملفات موزَّع/البحث الموزّع عن نص كامل/قاعدة بيانات NoSQL
معدات الشبكة	سجلات منصة المسيّرات والمبدلات والشبكة، وجدول التسيير وملفات التشكيلة، وما إلى ذلك.	كبير	تخزين ملفات موزَّع/البحث الموزّع عن نص كامل/قاعدة بيانات NoSQL
معدات الأمن	سجلات جدار الحماية، ونظام كشف الاقتحام (IDS)، ونظام منع الاقتحام (IPS)، والشبكة الخاصة الافتراضية (VPN)، وجدار الحماية لتطبيقات الويب (WAF)، وملفات التشكيلة، وما إلى ذلك.	كبير	تخزين ملفات موزَّع/البحث الموزّع عن نص كامل/قاعدة بيانات NoSQL
نظام التطبيق	سجلات قاعدة البيانات والبرمجيات الوسيطة وأنظمة التطبيقات وملفات التشكيلة، وما إلى ذلك.	كبير	تخزين ملفات موزَّع/البحث الموزّع عن نص كامل/قاعدة بيانات NoSQL
البيانات الأساسية	بيانات أصول، وبيانات حساب، وقاموس بروتوكول الإنترنت وبيانات الخدمة، وما إلى ذلك.	متوسط	تخزين ملفات موزَّع/البحث الموزّع عن نص كامل/قاعدة بيانات NoSQL
حركة الشبكة	بيانات DPI، وبيانات تدفق الشبكة، وما إلى ذلك.	كثيف	تخزين ملفات موزَّع
استخبارات عن التهديدات	الاستخبارات الاستراتيجية، والاستخبارات التكتيكية، والمعلومات الأمنية، وما إلى ذلك.	متوسط	تخزين ملفات موزَّع/البحث الموزّع عن نص كامل/قاعدة بيانات NoSQL
نتائج التحليل	الأحداث الأمنية، وبيانات المطابقة، الرقم القياسي للأمن، وما إلى ذلك.	متوسط	تخزين ملفات موزَّع/الاستخراج الموزّع لنص كامل/قاعدة بيانات NoSQL

2.2.8 المتطلبات التقنية لتخزين البيانات

ينبغي لمنصة الوعي الظرفي بأمن الشبكة (NSSA) أن تطور معماريةً مرنةً وقابلةً للتوسع لتخزين البيانات كي تلبي النمو المستمر في حجم البيانات ومتطلبات تصنيف البيانات والتخزين التراتبي. وينبغي أيضاً أن تتنوع دورة حياة تخزين البيانات وفقاً للوائح المطابقة ومتطلبات الأعمال والتكاليف الاقتصادية.

1) يوصى بأن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) قواعد البيانات العقلانية السائدة. ويوصى بأن تدعم قاعدة البيانات العقلانية سطحاً بينياً كاملاً للنفاذ إلى نموذج علائقي، بما في ذلك السطح البيني المعياري للغة الاستجواب المهيكلة (SQL) والسطح البيني المعياري لتطوير التطبيقات (JDBC، ODBC، وما إلى ذلك).

2) يوصى بأن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) قواعد بيانات NoSQL السائدة.

3) يوصى بأن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) مكونات البيانات الضخمة النمطية، مثل مكونات Hive وHBase وMPP، لدعم الخواص الوظيفية الموسعة.

4) يوصى بأن تعتمد منصة الوعي الظرفي بأمن الشبكة (NSSA) مكونات البحث عن النص الكامل التي ينبغي أن تدعم استخراج الكلمات الرئيسية، والبحث متعدد الكلمات الرئيسية، وتوليفة البحث عن النص الكامل وفي مجالات أخرى، وتطابق البادئات والتطابق التقريبي، وشروط الاستخراج الأخرى.

5) يوصى بأن تعتمد منصة الوعي الظرفي بأمن الشبكة (NSSA) مكونات ناقل الرسائل الموزع مثل Kafka وRabbit MQ وما إلى ذلك. وينبغي لمكونات ناقل الرسائل الموزع أن تدعم وظائف ضغط البيانات وضبط وقت الاحتفاظ بالبيانات وحذف البيانات المنتهية الصلاحية تلقائياً.

6) يوصى بأن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) آليات التخزين والنسخ الاحتياطي عبر الإنترنت لضمان تيسر البيانات.

7) يوصى بأن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) تخزين البيانات الشرحية، ويشمل ذلك أساساً:

- البيانات الشرحية التقنية، واستعمالها في صيانة البيانات، مثل كيفية تخزين البيانات لتحقيق نفاذ فعال إلى البيانات.
- البيانات الشرحية للإدارة، مثل سياسة التحكم في النفاذ إلى البيانات، ونتائج معالجة البيانات.

3.2.8 متطلبات أمن تخزين البيانات

1) يُتطلب أن تطور منصة الوعي الظرفي بأمن الشبكة (NSSA) آليات التحكم في النفاذ إلى البيانات، مثل التحكم في النفاذ إلى البيانات القائم على الأدوار، لمنع النفاذ غير المجاز.

2) يُتطلب أن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) تجفير تخزين البيانات للبيانات المهمة أو الحساسة. ويوصى بتوضيح متطلبات تجفير التخزين لمختلف أنماط البيانات استناداً إلى تصنيف البيانات وتعريفها التراتبي، مثل متطلبات خوارزميات تجفير البيانات وإدارة مفاتيح التجفير.

3) يُتطلب أن تنفذ منصة الوعي الظرفي بأمن الشبكة (NSSA) تقنيات وتدابير تحكم ملائمة لضمان فعالية سلامة تخزين البيانات واتساق البيانات متعددة النسخ.

4) يُتطلب أن تنفذ منصة الوعي الظرفي بأمن الشبكة (NSSA) تقنيات وتدابير تحكم ملائمة لضمان تيسر تخزين البيانات. واستناداً إلى مبادئ تصنيف البيانات، يوصى بتوضيح سياسات النسخ الاحتياطي والاستعادة لمختلف البيانات، مثل أساليب النسخ الاحتياطي، ومتطلبات فترة التخزين ووقت الاستعادة.

5) يوصى لمنصة الوعي الظرفي بأمن الشبكة (NSSA) باختبار آليات تخزين البيانات بصورة دورية للتحقق من قدرات التعرف على أعطال البيانات وإعادة بناء النسخ الاحتياطي.

6) يُتطلب أن تنتج منصة الوعي الظرفي بأمن الشبكة (NSSA) جميع سجلات معالجة تخزين البيانات لضمان إمكانية تتبع عمليات تخزين البيانات، وأن تقدم قدرات إنذار بشأن السلوكيات الشاذة.

3.8 متطلبات الحوسبة الظرفية والتحليل الظرفي

إن حساب الحالة وتحليلها في منصة الوعي الظرفي بأمن الشبكة (NSSA) يتضمن بشكل أساسي محرك الحوسبة والتحليل والوحدات الوظيفية لتحليل الحالة.

1) يقدم محرك الحوسبة والتحليل قدرات حاسوبية لنمذجة التهديدات وتحليلها لوحدات وظيفة التحليل الظرفي. ويتضمن محرك الحوسبة والتحليل نمذجة الأمن وأطر حوسبة البيانات الضخمة مثل محرك الحوسبة خارج الخط والحوسبة في الوقت الفعلي.

2) تُحقق وحدات وظيفة التحليل الظرفي تحليل حالة أمن الشبكة في بيئة الحوسبة السحابية استناداً إلى استخراج البيانات والسبر وتحليل التهديدات عبر مختلف بيانات الأصول المجمعة مثل الأحداث الأمنية وبيانات السجل، وبيانات حركة الشبكة.

3) لتحسين كفاءة الحساب والتحليل، يُتطلب بناء تمثيل موحد لمختلف الأحداث الأمنية ومعلومات الأصول قبل نمذجة الأمن، وهو ما يمكن تحقيقه من خلال تحديد متجهات السياق. ويرسم أسلوب تحديد المتجهات خارطة ارتباطات السياق بالفضاء الإقليدي، وهو يشكل عادةً فرضية اعتماد حساب التشابه وحساب التلازم بواسطة خوارزميات ذكاء اصطناعي متنوعة.

1.3.8 متطلبات محرك الحوسبة والتحليل

1.1.3.8 نمذجة الأمن

يُتطلب أن تشمل نمذجة الأمن نمذجة التلازم والنمذجة الإحصائية ونمذجة تلازم استخبارات عن التهديدات ونمذجة الذكاء الاصطناعي، بما يقدم قدرات التحليل والاستخراج المتعمقة والتنقيب للبيانات الظرفية الأساسية.

1) **نمذجة التلازم:** يُستعمل أسلوب المطابقة القائمة على القواعد لإقامة ارتباط منطقي وتحليل مطابقة السمات في أحداث متجانسة وغير متجانسة.

- يُتطلب أن تدعم تحليل التلازم المنطقي على أساس سببية الحوادث الأمنية.
- يُتطلب أن تدعم التلازم بين البيانات غير المتجانسة متعددة المصادر من جوانب متعددة، مثل الوقت والمكان.
- يوصى أن تدعم تجميع معلومات التنبيه وفقاً للمواقف الدينامية لأمن الشبكة لتقليل عدد التنبيهات وتحسين كفاءة الاستجابة.

2) **النمذجة الإحصائية:** تُستعمل أساليب إحصائية لحساب الخصائص الكمية لمختلف الأحداث، مثل التواتر وفترة الحدوث، والحصول على توزيع بيانات الأحداث والخصائص الرئيسية واتجاه السلاسل الزمنية وما إذا كانت هناك قيم شاذة ونتائج ملخص الأحداث.

- يوصى بدعم إجراء تحليل إحصائي للأحداث الأمنية والسلوكيات الأمنية والتهديدات الأمنية والخصائص الأخرى، واكتشاف الخصائص الإحصائية المهمة للتهديدات الأمنية من مصادر البيانات المختلفة.

3) **ارتباط الاستخبارات عن التهديدات:** يوصى بدعم تكامل قدرات استخبارات التهديدات، لاكتشاف أحداث استخباراتية دقيقة بناءً على معلومات عن التهديدات في بيئة الحوسبة السحابية.

4) **نمذجة الذكاء الاصطناعي:** يوصى بدعم مختلف خوارزميات الذكاء الاصطناعي المدمجة، بما في ذلك خوارزمية التوقيت وخوارزمية التصنيف وخوارزمية التجميع والنماذج الخوارزمية الأولية الأخرى، بما يقدم للمستعملين قدرات التعلم والتحليل لبيانات عشوائية، وبتحليل التهديدات الأمنية المتقدمة والتهديدات المجهولة.

- يوصى بدعم الخوارزميات السائدة، مثل تحليل المجموعة وتحليل التلازم وتحليل شجرة اتخاذ القرار والتحليل التراجعي وخوارزميات الذكاء الاصطناعي/تعلم الآلة الأخرى.
- يوصى بأن تدعم منصة الوعي الظرفي بأمن الشبكة (NSSA) الإدارة المركزية لنمذجة الأمن والسياسات، لتيسير التنفيذ الفعال والنشر السريع.

2.1.3.8 إطار حوسبة البيانات الضخمة

يُتطلب دعم أطر الحوسبة خارج شبكة الإنترنت وفي الوقت الفعلي على السواء، لتحقيق معالجة البيانات على دفعات وتحليل البيانات الدينامية (بيانات البث الشبكي) في الوقت الفعلي.

1) **إطار الحوسبة خارج شبكة الإنترنت:** يُتطلب دعم نشر الخوارزميات ونماذج التدريب وسيناريوهات تعلم الآلة خارج شبكة الإنترنت. ويمكن للمحللين أن يستعملوا محرك التحليل خارج الإنترنت للتعمق في استخراج البيانات، بما يتيح الحصول على تعقيبات فورية على نتائج خرج الخوارزمية، وتقديم قدرات تدريب النموذج.

2) **إطار حوسبة البث الشبكي في الوقت الفعلي:** يوصى بأن يدعم إطار الحوسبة في الوقت الفعلي معمارياً موزَّعةً، وبإمكانية تعديل سعة التخزين دينامياً. ويمكن للتيسر الكبير والفصل بين سياسات القراءة والكتابة أن يضمن قراءةً وكتابةً منفصلةً للبيانات عند تحليل البيانات خارج شبكة الإنترنت.

2.3.8 متطلبات الوحدات الوظيفية للتحليل الظرفي

تُنشئ وحدات وظيفة التحليل الظرفي، استناداً إلى محرك الحوسبة والتحليل، قدرات تحليل قائمة على سيناريوهات مختلف بيانات الأصول، والأحداث الأمنية، وبيانات السجل، وبيانات الحركة وغيرها من البيانات، وتقدم سيناريوهات تحليل أمني قائمة على بيانات متعددة لتحقيق تنبيهات أمنية قائمة على السيناريوهات وقدرات الإنذار المبكر. وتشمل الوحدات الوظيفية للتحليل الظرفي التحليل الأمني للشبكة وتحليل أمن الأصول وتحليل سلوك المستعمل عالي الخطورة في بيئة الحوسبة السحابية.

1.2.3.8 تحليل أمن الشبكة

يُتطلب أن تتمكن وحدة تحليل أمن الشبكة من تحليل مختلف حالات الهجوم على الشبكة، من قبيل الحركة الشاذة في الشبكة وانتشار البرامج الضارة والنفاذ إلى أسماء الميادين الخبيثة، في بيئة الحوسبة السحابية، فضلاً عن القدرة على تتبع اتجاهات تغايرها.

1) يوصى بدعم الكشف والتحليل الإحصائي للوضع العام للهجمات الشائعة وتحليل الاتجاهات المتغيرة لحالة الهجوم الراهن.

- يوصى بدعم وظائف كشف هجوم على الشبكة وتحليله استناداً إلى بيانات متعددة المصادر تشمل التسللات إلى الشبكة والهجمات عبر الويب والبرمجيات الضارة وهجمات الحرمان من الخدمة الموزَّع (DdoS) واستطلاع الشبكة والأنشطة المشبوهة وأنواع أخرى من الهجمات على الشبكة.
- يوصى بدعم التحليل الإحصائي لمختلف أنواع الهجمات على الشبكة وتحليل تغير الاتجاهات في مختلف أنماط الهجمات.

2) يوصى بدعم كشف الوضع العام لحركة الشبكة الشاذة في بيئة الحوسبة السحابية وتحليله الإحصائي وتحليل تغير حركة الشبكة الراهنة الشاذة.

- يوصى بدعم التعرف على حركة الشبكة الشاذة، وبالقدرة على كشف وتحليل الحركة الشاذة للبروتوكولات القائمة على منافذ فيروسية مشتركة.
- يوصى بدعم التحليل الإحصائي لحركة الشبكة الشاذة ودمج إحصاءات حركة البروتوكول الشاذة وتحليل اتجاه الحركة الشاذة.

3) يوصى بدعم تحليل الوضع العام لانتشار البرامج الخبيثة مثل الفيروسات والديدان البرمجية وأحصنة طروادة البرمجية في بيئة الحوسبة السحابية وتحليل الاتجاهات الراهنة في انتشار البرامج الخبيثة.

4) يوصى بدعم الكشف والتحليل الإحصائي لمضيفي القيادة والتحكم في الشبكة الروبوتية ومضيفي الحواسيب المسخَّرة ودعم تحليل انتشار الشبكات الروبوتية وتنوع اتجاهاتها.

5) يوصى بدعم تحليل النفاذ الإحصائي وانتشار أسماء الميادين الخبيثة وعناوين بروتوكول الإنترنت للقيادة والتحكم وأسماء ميادين خوارزمية إنشاء الميادين (DGA).

6) يوصى بدعم نموذج سلسلة الهجوم لتتبع مصدر أحداث الهجوم، من خلال تصنيف الأحداث الأمنية المتولدة وفقاً لعملية الهجوم التي تتضمن جمع المعلومات والتسلل إلى الشبكة والقيادة والتحكم والتغلغل الأفقي وتحقيق الهدف وتنظيف الأدلة.

7) يوصى بدعم تحليل المعلومات عن المهاجم استناداً إلى المعلومات الاستخباراتية عن التهديدات.

2.2.3.8 تحليل أمن الأصول

يُتطلب دعم تحليل الوضع الأمني لمختلف أصول منصة الحوسبة السحابية. ويوصى بتحليل حالة أمن البنية التحتية للحوسبة السحابية والآلات الافتراضية والحاويات وأنظمة الأعمال من خلال سجلات معدات الأمن وسجلات النظام ونتائج مسح مواطن الضعف وغيرها من البيانات. وتشمل أنماط التحليل تحليل الهجمات على النظام وتحليل مواطن ضعف النظام.

3.2.3.8 تحليل معلومات الأصول

1) يُتطلب دعم التحليل الإحصائي للأصول، بما في ذلك التحليل القائم على تصنيفات الأصول وفئاتها وأولوياتها، وتحديثات حالة الأصول، من قبيل إضافة الأصول أو إزالتها.

2) يُتطلب دعم تحليل توزيع الأصول، بما في ذلك التحليل القائم على أساس المعلومات الجغرافية للأصول وممتلكات الإدارات وتطبيقات الويب المهمة.

3) يُتطلب دعم البحث عن معلومات الأصول وعرضها وفقاً لعناوين بروتوكول الإنترنت للأصول والتصنيفات والأولويات والمعلومات الجغرافية.

4.2.3.8 تحليل تهديد الأصول

1) يُتطلب دعم تحليل التهديد بهجوم على النظام، بما في ذلك كشف تدمير السجل، وكشف تصعيد امتيازات النظام، وكشف سجل الأخطاء، والهجوم المستنفد لجميع الاحتمالات. ويمكن تنفيذ التحليل بناءً على تحليل تلازم بيانات الأصول، وسجلات الجهاز وسجلات النظام المضيف، وبيانات نظام الأمن، والاستخبارات عن التهديدات.

2) يُتطلب دعم التحليل الإحصائي وتحليل اتجاهات التهديدات للأصول.

5.2.3.8 تحليل مَواطن ضعف الأصول

1) يُتطلب دعم تحليل تلازم نتائج مسح مَواطن الضعف في الأصول وسجلات كشف جهاز الأمن لإجراء تحليل لاستغلال مواطن الضعف، بما في ذلك تحليل مَواطن ضعف الآلة المضيفة/الآلة الافتراضية/الحاوية وتحليل مَواطن الضعف في التطبيق، والتحليل الإحصائي للأصول المعرضة لخطر استغلال مواطن الضعف وفقاً إلى الوقت ونظام الأعمال ومستوى الضعف وبيانات الأبعاد الأخرى.

6.2.3.8 تحليل الالتزام بتشكيلات الأصول

1) يُتطلب دعم تحليل نتائج الالتزام بتشكيلات أنظمة التشغيل، وبرمجيات التمثيل الافتراضي، وقواعد البيانات، ومعدات الشبكة، والبرمجيات الوسيطة في بيئة الحوسبة السحابية.

2) يُتطلب دعم التحليل الإحصائي للبنود غير المطابقة المكتشَفة؛ ودعم تحليل مخاطر مهاجمين يستعملون بنوداً غير مطابقة لمهاجمة الأصول.

7.2.3.8 تحليل سلوك المستعمل

يوصى بدعم كشف وتحليل السلوكيات الشاذة للمستعملين الداخليين الذين ينفذون إلى منصة الحوسبة السحابية، والسلوكيات الشاذة لأنظمة الأصول والأعمال، فضلاً عن تحليل البيانات الوصفية لسلوكيات المستعملين.

1) يوصى بدعم تحليل سلوكيات تشغيل المستعملين الشاذة، بما في ذلك العمليات الشاذة للبيانات الحساسة، وتسجيل الدخول إلى الحساب منتهي الصلاحية، والتواصل غير القانوني، وتنفيذ الأوامر الحساسة، وهجوم استنفاد جميع الاحتمالات، وتسجيل الدخول إلى عناوين شاذة.

2) يوصى بدعم تعريف البيانات الوصفية على أساس سلوكيات المستعمل الداخلية، بما في ذلك خصائص السلوك الفردي للمستعملين وخصائص المجموعة.

3) يوصى بدعم تكييف قواعد السلوك الشاذ ونماذج السلوك حسب الطلب.

4) يوصى بدعم تحليل السلوك الشاذ على أساس البيانات الوصفية للمستعمل ومقارنة السلوك الفردي أو الجماعي مع بيانات السلوك التاريخية لاستخراج الحالات الشاذة.

5) يوصى بدعم تحليل السلوك الشاذ لموارد الحوسبة السحابية المختلفة، وبالقدرة على تحديد السلوكيات الشاذة التي قد تحدث في بيئة الحوسبة السحابية، مثل السلوك الشاذ للمخدمات السحابية، وأدوات نظام الاتصال الشاذ، والسلوكيات الشاذة للشبكة، والاتصالات الخارجية غير القانونية.

4.8 متطلبات التقييم الظرفي

يوصى بتقييم ظرفي من منصة الوعي الظرفي بأمن الشبكة (NSSA) لدعم التقييم الظرفي الدينامي للحالة الأمنية الكلية في بيئة الحوسبة السحابية، والتنبؤ بالاتجاه الظرفي، استناداً إلى تحليل بيانات الأمن متعددة الأبعاد، ونتائج التحليل الأمني لمنصة الحوسبة السحابية ونمذجة تقييم فئة الرقم القياسي الظرفي. وهو يدعم إصدار الإنذارات المبكرة والتفاعل مع آليات اتخاذ القرار الأمني والاستجابة في حالات الطوارئ لدى مقدم الخدمة السحابية (CSP)/عميل الخدمة السحابية (CSC).

1.4.8 التقييم الظرفي

يشمل نطاق تقييم الوضع الأمني الوضع الشامل للمنصة السحابية والوضع الأمني للأصول السحابية والتهديدات ومواطن الضعف والهجوم على الشبكة وحالة تيسر المنصة السحابية ومكوناتها.

1) يُتطلب جمع معلومات الأصول كمصدر بيانات لبناء فئة الرقم القياسي لتقييم الوضع الأمني. وينبغي أن تشمل معلومات الأصول الإصدار المحدد من أنظمة التشغيل والبرمجيات الوسيطة والتطبيق وقاعدة البيانات، وموقع طوبولوجيا الشبكة، وقيمة الأصول، وما إلى ذلك، مما يمكن أن يساعد في توليد مؤشرات تقييم معقولة.

2) يُتطلب دعم فئة الرقم القياسي لتقييم الوضع الأمني لمنصة الحوسبة السحابية باستحداث مقاييس عامة في ميزان موحد لقياسات الوضع الأمني وبالتحديد الكمي لعناصر متنوعة في الوضع الأمني للشبكة.

- يوصى بوضع مؤشرات نوعية وكمية على السواء لتقييم حالة الشبكة. والمؤشرات النوعية هي تقييمات شخصانية قائمة على محللات الأمن المهنية. فعلى سبيل المثال، يمكن لمحللات الأمن أن تخصص مستويات من الشدة لمواطن ضعف أو هجمات معيَّنة على الشبكة استناداً إلى تجاربها. وتأتي المؤشرات الكمية من عمليات جمع البيانات الخام وتحليلها.
- يوصى بدعم حساب التشابه وحساب التلازم في التعامل مع مؤشرات التهديدات، بما في ذلك ما يلي:
  - يوصى باستعمال حساب تشابه سياق التهديدات للتعرف بسهولة على تهديدات مستفحلة مثل المسح وفك الشفرة باستنفاد جميع الاحتمالات وهجمات الحرمان من الخدمة الموزع، لتجنب تغييرات جذرية في مؤشر محدد سببها عدد كبير من الإنذارات المتكررة.
  - يوصى باستعمال تحليل التلازم بين معلومات عن التهديدات والأصول للتعرف على تهديدات الهجوم الأعمى والمحاولات الكثيفة التي من شأنها أن تساعد الموظفين الأمنيين في العثور بسرعة على المؤشرات عالية الخطورة التي تحتاج بالفعل إلى ردودهم.
  - يوصى باعتماد إطار خوارزمية موحدة لتحقيق تحليل التلازم وتحليل التشابه مثل جيب التمام لزاوية. ومن الواضح أن الإطار الموحد للخوارزميات يمكن أن يقلل من تكلفة صيانة استعمال الخوارزميات.
- يوصى بإنشاء مؤشر عام ومؤشرات تقسيم فرعي لتقييم حالة أمن الشبكة. ويبين المؤشر العام الخصائص الإجمالية لتقييم أمن منصة الحوسبة السحابية، ويمكن تقسيم مؤشرات التقسيم الفرعي وفق مختلف المكونات أو الأنظمة التي تبين الاختلافات في نتائج التقييم الظرفي لمختلف المكونات/الأنظمة.
- يوصى بدعم استحداث فئات مؤشر ظرفي، تتضمن ما يلي:
  - يوصى بدعم وضع مؤشرات تشغيلية لمنصات الحوسبة السحابية مثل استعمال مجموعات الموارد السحابية وتأخيرات النفاذ إلى الأعمال.
  - يوصى بدعم استحداث مؤشرات لتهديدات ضد أمن الشبكة، بما في ذلك مختلف حوادث أمن الشبكة التي تمكن مواصلة حسابها وتقييمها من حيث تواتراتها ومدى خطورتها.
  - يوصى بدعم إنشاء مؤشرات لتقييم أمن الأصول السحابية، مثل التهديدات للأصول، ومواطن ضعفها، بما في ذلك شدة هشاشتها، وما إذا كان قد تم تصحيح مواطن الضعف.

- يوصى بدعم استحداث مؤشرات لأمن سلوك المستعمل، ومثال ذلك شذوذ نفاذ المستعملين وتسجيل دخولهم وسلوكيات تحميل البرمجيات الضارة. ويُتطلب أيضاً اعتماد تقنيات لحماية خصوصيات المستعمل، من قبيل إزالة حساسية البيانات وإغفال هوية البيانات لحماية خصوصيات المستعمل.

3) يوصى بدعم إنشاء آلية شاملة لتقييم الوضع الأمني أو نمذجة تقوم على فئات مؤشرات تراتبية ومتعددة الأبعاد.

- يُتطلب دعم تقييس المؤشرات الفرعية المختلفة، بما في ذلك المؤشرات النوعية والكمية، لتجنب نتائج التقييم المتحيزة بسبب الاختلافات في الوحدات والمطال. ويوصى باعتماد تقنيات تحويل لتحويل المؤشرات النوعية إلى قيم رقمية من أجل القيام بمزيد من الحوسبة أو التحليل.
- يوصى بدعم آليات تقييم الوضع متعدد الأبعاد، بما في ذلك التقييم الموجه نحو المخاطر أو التقييم الموجه نحو التهديدات أو النمذجة القائمة على بيانات السلاسل الزمنية.
- يوصى بدعم مختلف نماذج التقييم، بما فيها النماذج القائمة على النماذج النظرية الرياضية، أو التعليل القائم على المعرفة.
- يوصى بدعم أسلوب تقييم تراتبي تصاعدي، من خلال معالجة مؤشرات حالة الطبقات السفلى معالجةً شاملةً، ثم حساب نتائج تقييم الوضع في الطبقات العليا، ثم حساب التقييم الشامل لحالة الأمن تدريجياً.
- في أساليب التقييم التراتبي، يوصى بدعم حساب التشابه لقابلية تفسير قيمة تقييم حالة محددة، مقارنةً مع القيم التاريخية والقريبة. وبالنسبة لقيمة التقييم النهائية، يمكن إنشاء متجه متعدد الأبعاد باختيار نتائج سابقة له عند مستوى محدد، ويمكن استعماله لحساب تشابه القيم التاريخية القريبة بواسطة جيب التمام ومسافة المتجه المكاني وخوارزميات أخرى. ويمكن أن يساعد حساب التشابه موظفي الأمن في العثور على الشذوذ على نحو أسهل وفهم الوعي الظرفي بشكلٍ أسهل.

4) يوصى بدعم قدرات لتتبع تقييمات الحالات الأمنية التاريخية للمنصة السحابية بكفاءة من خلال تنفيذ المعالجة المسبقة للسجل وفهرسة المجالات الرئيسية والبحث عن النص الكامل والاستفسار التقريبي.

2.4.8 توقع التوجه الظرفي

يوصى لمنصة الوعي الظرفي بأمن الشبكة (NSSA) أن تدعم التنبؤ بالتوجه الأمني العام والتوجه الأمني لمكون التقسيم الفرعي والمخاطر الأمنية المحتملة استناداً إلى نماذج توقع التوجه الظرفي المتمحور حول المنصة السحابية وبناءً على تحصيل حالة أمن بيئة الحوسبة السحابية وتتبعها، واستخلاص العناصر والمؤشرات الأمنية الرئيسية التي يمكن أن تتسبب في تغييرات في وضع الشبكة.

1) يُتطلب دعم بناء فئة مؤشرات تراتبية ومتعددة الأبعاد استناداً إلى البيانات المجمعة والنتائج المحلَّلة والتنبؤ بالتوجه الظرفي من خلال نماذج التنبؤ ذات الصلة.

2) يوصى بدعم نماذج التنبؤ السائدة، بما في ذلك نماذج التنبؤ التراجعي القائمة على تعلم الآلة، ونماذج التعلم العميق، ونماذج التنبؤ القائمة على معادلات تفاضلية في المجالات المهنية.

3) يوصى بدعم نتائج التنبؤ الحاسوبي بدمج نماذج تنبؤ مختلفة لتحسين دقة التنبؤ، وعلى وجه التحديد عن طريق:

- مراقبة دقة كل نموذج بحساب قيم دالة الخسارة بين نتائج التنبؤ والبيانات.
- الجمع بين نتائج كل نموذج من خلال أوزان الترجيح، وإجراء تعديلات تكييفية على أوزان الترجيح بين النماذج. فعلى سبيل المثال، يمكن تعديل وزن ترجيح كل نموذج تعديلاً تكييفياً بناءً على نتيجة مراقبة دالة الخسارة؛ ويمكن أيضاً إطلاق تدريب لأحدث البيانات خارج الإنترنت تلقائياً لتحديث النموذج وتحسين الدقة.

3.4.8 آليات الإنذار المسبق

ينبغي أن تقدم منصة الوعي الظرفي بأمن الشبكة (NSSA) آليات الإنذار المبكر بالمخاطر الأمنية المحتملة في بيئة الحوسبة السحابية، استناداً إلى نتائج التحليل الأمني والتقييم الظرفي والتنبؤات الظرفية.

1) يوصى بتقديم إنذارات مبكرة بشأن مواطن ضعف الأصول عبر إقامة التلازم بين مواطن الضعف وبيانات الاستخبارات المتعلقة بالتهديدات وبيانات الأحداث الأمنية ذات الصلة وما إلى ذلك، وبتحليل مواطن ضعف أصول المنصة السحابية.

2) يوصى بدعم الإنذارات المبكرة بالهجمات المحتملة على الشبكات على أساس توجه التنبؤ، بما في ذلك المسح الضار وهجمات الويب وهجمات الحرمان من الخدمة الموزع (DDoS) وهجمات تخمين كلمة المرور وهجمات على مواطن الضعف في الأنظمة.

3) يوصى بدعم الإنذارات المبكرة بسلوكيات المستعمل الشاذة المحتملة بناءً على توقع التوجه، بما في ذلك عمليات البيانات الحساسة الشاذة، وتسجيلات الدخول إلى الحساب منتهية الصلاحية، وتنفيذ الأوامر عالية الخطورة، وما إلى ذلك. وقبل إصدار الإنذارات، يُتطلب استعمال إزالة حساسية البيانات وتقنيات إغفال هوية البيانات لحماية خصوصيات المستعمل.

4) يوصى بدعم الإنذارات المبكرة بالتهديدات الأمنية غير المكتشفة عبر إقامة التلازم بين السلوكيات الشاذة المكتشفة والمعلومات الاستخبارية المتعلقة بالتهديدات وسجلاتها الأصلية، وما إلى ذلك.

5) تشمل آليات الإنذار المبكر ما يلي:

- يوصى بدعم إصدار إنذارات مبكرة على أساس سياسات مسبقة التشكيل يمكن تفصيلها حسب الاقتضاء وفقاً لذلك.
- يوصى بدعم الإدارة التراتبية للإنذارات المبكرة وتصنيف مستويات الإنذار حسب الأهمية والشدة.
- يوصى بدعم إصدار الإنذارات من خلال السطوح البينية لبرمجة التطبيقات، والتي من خلالها يمكن لأنظمة أطراف ثالثة تلقي الإنذارات والاستجابة لها وفقاً لذلك.

5.8 متطلبات العرض المرئي الظرفية

يُتطلب من منصة الوعي الظرفي بأمن الشبكة (NSSA) أن تدعم عرض الحالة الأمنية للسيناريوهات المتعددة، بما في ذلك الحالة الأمنية الشاملة وحالة أمن الشبكة وحالة أمن الأصول، وأن تفصل الحالة الأمنية حسب الاقتضاء. وفي الوقت نفسه، يوصى بدعم استعمال أنماط متعددة من طرق العرض لعرض المعلومات التفصيلية لحالة الأمن، مثل المخطط الراداري، وخارطة معلومات التلازم، وخريطة مسار التهديد، وبدعم سبر المعلومات الأمنية التفصيلية.

1.5.8 العرض المرئي الظرفي للأمن الشامل

1) يوصى بدعم عرض حالات تقييم الأمن الشامل لمنصة الحوسبة السحابية بواسطة علامات أو درجات.

2) يوصى بدعم عرض الوضع الأمني الشامل لمنصة الحوسبة السحابية بيانياً، بما في ذلك تصنيف المخاطر وتوجه الهجمات على الشبكات ومواطن الضعف وسلوكيات المستعمل عالية المخاطر وما إلى ذلك.

3) يوصى بدعم عرض الوضع الأمني لمختلف الشاغلين ومختلف عمليات الأعمال والأصول المختلفة، وما إلى ذلك، في منصة الحوسبة السحابية ومقارنته بالبيانات التاريخية لإظهار التوجهات.

4) يوصى بدعم عرض الإنذارات المجمعة بشأن أحداث أمن الشبكة في الوقت الفعلي وسلوكيات المستعملين الشاذة وحالة أمن الأصول في منصة الحوسبة السحابية، وبدعم تفاصيل سبر هذه الإنذارات بيانياً.

2.5.8 العرض المرئي الظرفي لأمن الشبكة

1) يوصى بدعم عرض المخاطر الأمنية لشبكة منصة الحوسبة السحابية بيانياً في أبعاد متعددة، بما في ذلك نتائج التحليل الإحصائي للهجمات على الشبكة وأنواع الهجمات على الشبكة والتوزع الجغرافي للهجمات على الشبكة والحركة الشاذة في الشبكة وبروتوكول الإنترنت لمصدر الهجمات وبروتوكول الإنترنت لمقصد الهجمات.

2) يوصى بدعم تقديم الإنذارات الأمنية في الوقت الفعلي لمنصة الحوسبة السحابية، من قبيل الهجمات على الشبكة والحركة غير العادية للشبكة الشاذة في الشبكة والبرامج الضارة. وتشمل معلومات الإنذار الختم الزمني ونوع الأمن ومستوى الشدة وبروتوكول الإنترنت لمصدر الهجمات وبروتوكول الإنترنت لمقصد الهجمات.

3) يوصى بدعم سبر المعلومات التفصيلية عن معلومات حالة أمن الشبكة.

3.5.8 العرض المرئي الظرفي لأمن الأصول

1) يوصى بدعم عرض معلومات أصول منصة الحوسبة السحابية بيانياً مثل مقاييس الأصول وأنماط الأصول وملكية الأصول وتوزيعات الأصول.

2) يوصى بدعم عرض مختلف نتائج التحليل الإحصائي لمنصة الحوسبة السحابية بيانياً، بما في ذلك مواطن ضعف الأصول والهجمات على الشبكة وأخطاء التشكيلة.

3) يوصى بدعم عرض المخاطر الأمنية في الوقت الفعلي لمختلف أصول منصة الحوسبة السحابية في أبعاد متعددة، بما في ذلك اسم الأصل وبروتوكول الإنترنت وأنواع الهجمات وأنواع مواطن الضعف وعدد نقاط الضعف وأخطاء التشكيلات.

4) يوصى بدعم سبر المعلومات التفصيلية عن وضع أمن الأصول.

4.5.8 العرض المرئي الظرفي لسلوكيات المستعمل الشاذة

1) يوصى بدعم عرض سلوكيات المستعمل الشاذة في منصات الحوسبة السحابية في أبعاد متعددة، بما في ذلك أنواع السلوك الشاذ وتوجه السلوك الشاذ والمستعملين (الحسابات أو بروتوكول الإنترنت) الشواذ.

2) يوصى بدعم عرض الإنذارات الأمنية في الوقت الفعلي لسلوكيات المستعمل الشاذة في منصة الحوسبة السحابية، بما في ذلك وقت الإنذار وأنماط الإنذار ومستويات الشدة والمستعمل (الحساب) الشاذ.

3) يوصى بدعم سبر المعلومات التفصيلية عن السلوك الشاذ للمستعمل.

5.5.8 العرض المرئي الظرفي للأمن المكيَّف حسب الاقتضاء

يوصى بدعم تشكيل عروض ظرفية مخصصة لسيناريوهات عمل محددة، ودعم تشكيلات الاستيراد بيانياً أو بواسطة البرمجيات النصية، وفقاً لمتطلبات العمل وأدوار الإدارة وغيرها من فرادى متطلبات منصة الحوسبة السحابية.

بيبليوغرافيا

[b-ITU-T X.1217] Recommendation ITU-T X.1217 (2021), *Guidelines for applying threat intelligence in telecommunication network operation.*

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2016), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-NIST-SP-800-30] NIST Special Publication 1800-30 Revision 1 (2012), *Guide for Conducting Risk Assessments*.

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، 2024