ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

UIT-T X.1645 (09/2023)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

Sécurité de l'informatique en nuage – Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage

---

Exigences relatives à une plate-forme d'appréciation des conditions de sécurité pour l'informatique en nuage

RECOMMANDATIONS UIT-T DE LA SÉRIE X

Réseaux de données, communication entre systèmes ouverts et sécurité

RÉSEAUX PUBLICS DE DONNÉES	X.1-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	X.850-X.899
TRAITEMENT RÉPARTI OUVERT	X.900-X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	X.1000-X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	X.1100-X.1199
SÉCURITÉ DU CYBERESPACE	X.1200-X.1299
APPLICATIONS ET SERVICES SÉCURISÉS (2)	X.1300-X.1499
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	X.1500-X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	X.1600-X.1699
Aperçu de la sécurité de l'informatique en nuage	X.1600-X.1601
Conception de la sécurité de l'informatique en nuage	X.1602-X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	**X.1640-X.1659**
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660-X.1679
Sécurité de l'informatique en nuage (autres)	X.1680-X.1699
COMMUNICATIONS QUANTIQUES	X.1700-X.1729
SÉCURITÉ DES DONNÉES	X.1750-X.1799
SÉCURITÉ DES IMT-2020	X.1800-X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1645

Exigences relatives à une plate-forme d'appréciation des conditions de sécurité pour l'informatique en nuage

Résumé

L'appréciation des conditions de sécurité du réseau (NSSA) découle du concept d'appréciation de la situation. Elle comprend généralement quatre processus, à savoir l'acquisition des données, l'analyse des conditions de sécurité, l'évaluation des conditions de sécurité et la projection de la tendance relative aux conditions de sécurité. Elle présente en outre les capacités suivantes: 1) détection et surveillance continue de diverses menaces d'attaque, de comportements anormaux et de leur champ d'influence; 2) exploration des données, analyse des données et traçage des comportements anormaux; 3) prédiction de la sécurité et alerte avancée; 4) visualisation des conditions de sécurité.

Pour les fournisseurs de services d'informatique en nuage, la plate-forme NSSA joue un rôle important en ce qu'elle permet d'améliorer la protection de la sécurité de l'informatique en nuage, la capacité de détecter les atteintes à la sécurité ou des comportements anormaux et la capacité de prise de décisions en matière de sécurité et d'intervention en cas d'urgence. Elle peut même contribuer à améliorer le mécanisme d'alerte avancée pour l'informatique en nuage.

La Recommandation UIT-T X.1645 présente d'abord le concept de la NSSA et son développement, analyse les avantages liés à la NSSA lorsqu'il s'agit de faire face aux problèmes de sécurité en matière d'informatique en nuage et décrit les exigences relatives à une plate-forme NSSA pour l'informatique en nuage.

Historique *

Édition	Recommandation	Approbation	Commission d'études	ID unique
1.0	UIT-T X.1645	08-09-2023	17	11.1002/1000/15527

Mots clés

Analyse des mégadonnées, informatique en nuage, appréciation des conditions de sécurité du réseau, appréciation de la situation.

* Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1645

Exigences relatives à une plate-forme d'appréciation des conditions de sécurité pour l'informatique en nuage

1 Domaine d'application

La présente Recommandation présente l'appréciation des conditions de sécurité du réseau (NSSA), ainsi que les exigences de la plate-forme NSSA pour l'informatique en nuage. Elle s'applique aux fournisseurs de services d'informatique en nuage.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à étudier la possibilité d'appliquer les éditions les plus récentes des recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

Aucun.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 informatique en nuage [b-UIT-T Y.3500]: modèle permettant d'offrir un accès via le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, approvisionnées et administrées à la demande et en libre-service.

3.1.2 service en nuage [b-UIT-T Y.3500]: une ou plusieurs capacités offertes via l'informatique en nuage invoquées à l'aide d'une interface définie.

3.1.3 client de services en nuage [b-UIT-T Y.3500]: partie à une relation commerciale aux fins de l'utilisation de services en nuage.

3.1.4 fournisseur de services en nuage [b-UIT-T Y.3500]: partie qui met à disposition des services en nuage.

3.1.5 vulnérabilité [b-NIST-SP-800-30]: faiblesse dans un système d'information, les procédures de sécurité système, les contrôles internes ou la mise en œuvre, qui pourrait être exploitée par une source de menace.

3.1.6 renseignements sur les menaces [b-UIT-T X.1217]: ensemble d'informations organisées, analysées et affinées sur les attaques potentielles et actuelles qui peuvent menacer une organisation.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 appréciation de la situation: capacité à évaluer l'état actuel des éléments dans un environnement donné, ainsi que leurs relations sur plusieurs dimensions, y compris le temps et l'espace.

NOTE – Pour ce faire, il convient de collecter des données provenant de diverses sources, en combinant ces données et en les analysant. L'objectif de l'appréciation de la situation consiste à intégrer et analyser des informations provenant de diverses sources afin d'obtenir une compréhension globale de sa signification.

3.2.2 appréciation des conditions de sécurité du réseau (NSSA): capacité à identifier et à évaluer les principaux éléments de sécurité du réseau et à les classer selon des règles qui s'appuient sur des dimensions temporelles et spatiales.

NOTE – Ces informations permettent d'évaluer la situation générale du réseau et à prévoir les tendances émergentes en matière de sécurité des réseaux moyennant des techniques telles que l'analyse statistique, l'exploration des données et l'intelligence artificielle. Les données qui en découlent peuvent être présentées dans des formats lisibles par l'homme ou en tant que contribution à l'automatisation de la sécurité du réseau.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

C&C commande et contrôle (*command and control*)

CRUD créer, lire, mettre à jour et supprimer (*create, read, update, and delete*)

CSC client de services en nuage (*cloud service customer*)

CSP fournisseur de services en nuage (*cloud service provider*)

DDoS déni de service réparti (*distributed denial of service*)

DGA algorithme de génération de domaines (*domain generation algorithm*)

HBase base de données Hadoop (*Hadoop database*)

IA intelligence artificielle

IDS système de détection des intrusions (*intrusion detection system*)

IPS système de prévention des intrusions (*intrusion prevention system*)

JDBC connectivité de base de données Java (*Java database connectivity*)

MPP traitement massivement parallèle (*massively parallel processing*)

NoSQL non relationnel (*not only structured query language*)

NSSA appréciation des conditions de sécurité du réseau (*network security situational awareness*)

ODBC connectivité de base de données ouverte (*open database connectivity*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SQL langage de requête structuré (*structured query language*)

VM machine virtuelle (*virtual machine*)

VPN réseau privé virtuel (*virtual private network*)

WAF application web de pare-feu (*web application firewall*)

5 Conventions

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie, et par rapport à laquelle aucun écart n'est autorisé pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument obligatoire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

Dans la présente Recommandation et dans ses appendices, on trouve les expressions doit, ne doit pas, devrait et peut. Celles-ci doivent respectivement être interprétées comme correspondant aux expressions il est obligatoire, il est interdit, il est recommandé et peut, à titre d'option. Lorsque ces expressions apparaissent dans un appendice ou dans des parties dans lesquelles il est expressément indiqué qu'elles sont données à titre d'information, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Introduction relative à l'appréciation des conditions de sécurité du réseau

Aujourd'hui, les attaques de réseau sont élaborées pour atteindre des objectifs précis, dans la mesure où les auteurs d'attaques ont généralement des plans rigoureux, qui permettent généralement une pénétration à long terme. De même, les dispositifs de défense de la sécurité présentent une caractéristique typique de "confrontation temporelle". Dans l'architecture de sécurité traditionnelle, divers composants ou produits de sécurité sont déployés avec leurs propres règles de protection, politiques d'alerte, mécanismes de traitement et de stockage des journaux, sans toutefois bénéficier d'un mécanisme de coordination entre les composants et les produits. Cela provoque un effet d'îlotage qui affaiblit la capacité de défense contre des attaques avancées plus secrètes et plus professionnelles.

L'appréciation des conditions de sécurité du réseau (NSSA) découle du concept d'appréciation de la situation, et constitue une application spécifique de la sécurité des réseaux. Elle comprend généralement quatre processus: l'acquisition des données, l'analyse des conditions de sécurité, l'évaluation des conditions de sécurité et la projection de la tendance relative aux conditions de sécurité. Elle présente en outre les capacités suivantes:

– Détection et surveillance continue de diverses menaces d'attaque, de comportements anormaux et de leur champ d'influence.
– Exploration des données, analyse des menaces et traçabilité des comportements anormaux.
– Prédiction de la sécurité et alerte avancée.
– Visualisation des conditions de sécurité.

Dans le contexte de la sécurité des réseaux, l'asymétrie d'information fait référence à un scénario dans lequel un auteur d'attaque possède davantage de connaissances sur les systèmes, le réseau ou les processus d'une organisation que l'organisation elle-même. Dans une telle situation, les auteurs d'attaques se trouvent dans une position avantageuse lorsqu'il s'agit d'élaborer des stratégies et de mettre en œuvre des attaques. La NSSA revêt une grande importance dans le traitement de l'asymétrie de l'information entre l'attaque et la défense, et également dans l'accélération de la réponse aux incidents et la traçabilité.

Dans le même temps, les progrès accomplis dans les domaines de l'analyse des mégadonnées, de l'informatique en nuage et de l'intelligence artificielle (IA) offrent d'immenses possibilités et capacités au développement de la NSSA. Par exemple, la NSSA peut efficacement prendre en charge le stockage, l'utilisation et l'exploitation massive des journaux de sécurité grâce à l'analyse des mégadonnées, afin d'assurer une surveillance permanente des conditions de sécurité du réseau à grande échelle; le développement de l'IA peut fournir davantage de méthodes d'analyse et de capacités de prévision des risques dans le cadre de la NSSA, ce qui peut effectivement améliorer la précision des prévisions; et le développement de l'informatique en nuage peut fournir une architecture d'infrastructure plus flexible et plus stable à la NSSA.

Le cadre type d'une plate-forme NSSA est présenté dans la Figure 6-1:

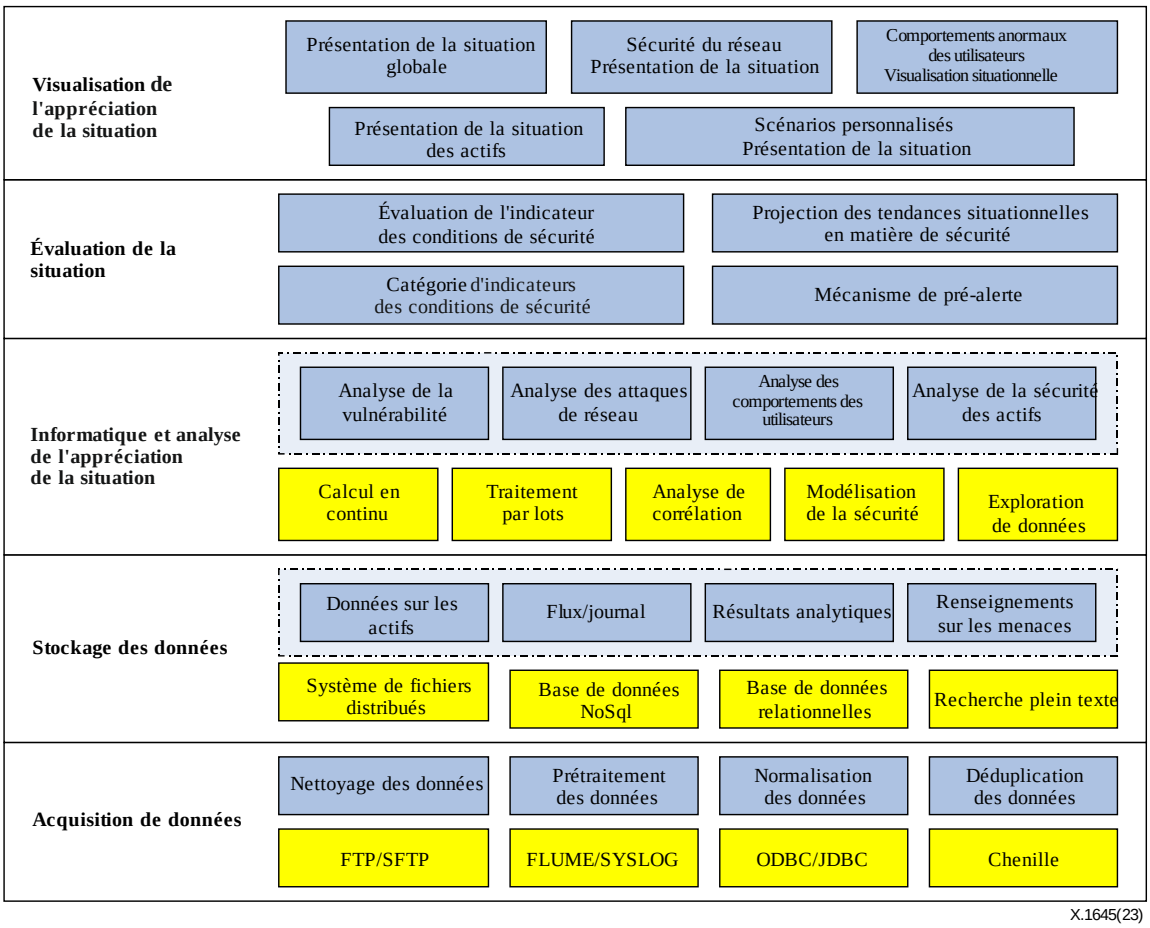

Figure 6-1 – Cadre de la plate-forme d'appréciation des conditions de sécurité du réseau

7 Analyse

Dans le cadre des progrès rapides de la technologie et de la maturité de son écosystème, l'informatique en nuage constitue une nouvelle génération d'infrastructures essentielles de l'information. Bien que l'informatique en nuage offre de nombreux avantages, elle est également confrontée à des problèmes de sécurité beaucoup plus importants, notamment en ce qui concerne l'exploitation et la maintenance, tels que les suivants:

1) En raison de l'augmentation rapide de l'échelle, divers types de composants de sécurité déployés dans l'infrastructure de l'informatique en nuage impliquent des données de sécurité massives et des avertissements répétés. Ce scénario rend difficile la tâche des ingénieurs chargés de l'exploitation et de la maintenance dans un laps de temps limité.

2) La plupart des composants de sécurité sont isolés les uns des autres, ce qui entraîne manifestement un effet d'îlotage. Cela rend difficile la mise en place d'un mécanisme de défense bien coordonné dans un environnement de l'informatique en nuage.

3) L'environnement de l'informatique en nuage est généralement complexe, et peut comprendre un nuage public, un nuage privé ainsi qu'un nuage hybride. Il est donc difficile pour les fournisseurs de services d'informatique en nuage et même pour les utilisateurs de l'informatique en nuage de prendre des décisions raisonnables en matière de sécurité, en raison de l'absence d'une perspective macroscopique et globale.

La NSSA permet de résoudre ces problèmes. Basée sur la technologie des mégadonnées, la NSSA peut efficacement prendre en charge le stockage, l'utilisation et l'exploration de données de journaux de sécurité massifs et hétérogènes. En outre, grâce à l'analyse de corrélation de multiples données différentes, il est possible d'organiser efficacement différents composants de sécurité, d'améliorer la capacité de détection des menaces et d'accroître l'efficacité des ingénieurs en sécurité. La NSSA fournit également une capacité visuelle de l'ensemble de l'appréciation des conditions sécurité pour l'informatique en nuage. Dans le même temps, il est utile d'utiliser la technologie de l'IA dans la NSSA, ce qui permet d'améliorer la capacité de détection, de diagnostic et de prédiction de l'appréciation des conditions de sécurité pour l'informatique en nuage.

Par conséquent, la NSSA joue un rôle important dans l'amélioration de la protection de la sécurité de l'informatique en nuage, de la prise de décision en matière de sécurité et de la capacité d'intervention en cas d'urgence, et peut donc contribuer à améliorer le mécanisme d'alerte précoce pour les fournisseurs de services d'informatique en nuage.

Dans le même temps, une plate-forme NSSA déployée dans l'informatique en nuage nécessite les capacités particulières suivantes:

1) L'acquisition des données doit s'adapter aux changements dynamiques des actifs dans l'informatique en nuage, dans la mesure où les actifs de l'informatique en nuage peuvent être créés et supprimés de manière plus souple et plus fréquente que dans le cadre de l'architecture informatique traditionnelle.
2) La plate-forme NSSA doit s'adapter aux caractéristiques d'un service d'informatique en nuage, telles que le partage des ressources multi-locataires et la gestion élastique des ressources, ce qui peut entraîner un changement rapide des sources de données. L'évolution rapide des locataires et de leurs services entraînerait une modification de l'acquisition des données pour la plate-forme NSSA.
3) La plate-forme NSSA doit continuer à interagir et à coopérer avec la plate-forme de gestion de l'informatique en nuage pour accéder aux différents types de données, tels que l'état de fonctionnement et les journaux de sécurité des ressources d'informatique en nuage, afin d'obtenir une vue d'ensemble approfondie des ressources d'informatique en nuage. La NSSA ne peut par exemple contourner la plate-forme de gestion en nuage afin d'observer les connexions de réseau entre les machines virtuelles de la même couche réseau de niveau 2 du modèle OSI.
4) La plate-forme NSSA doit permettre d'accéder à des données provenant de plusieurs nuages, afin d'offrir aux utilisateurs une perspective d'actifs unifiés, que ce soit dans un nuage hybride ou dans un nuage public.

L'application et le déploiement de la NSSA offrent des solutions possibles aux défis techniques susmentionnés. La NSSA peut détecter divers événements de sécurité et comportements anormaux de manière complète et précise dans le temps et l'espace, analyser divers éléments de sécurité, comprendre les conditions globales de sécurité et prédire ses tendances, ce qui contribuera à améliorer la capacité opérationnelle de sécurité des fournisseurs d'informatique en nuage, à prendre en charge la prise de décision en matière de sécurité et la réponse aux incidents, ainsi qu'à améliorer le mécanisme d'alerte précoce en matière de sécurité.

8 Exigences relatives à une plate-forme d'appréciation des conditions de sécurité pour l'informatique en nuage

8.1 Exigences en matière d'acquisition de données

8.1.1 Mécanisme d'acquisition de données

Les nœuds d'acquisition d'une plate-forme NSSA devraient permettre de collecter différents types de données, tels que les journaux du trafic réseau, les journaux système, les journaux des intergiciels et les journaux de sécurité de l'infrastructure informatique en nuage, dans le cadre d'une approche active ou passive. Une approche active recueille des données en surveillant ou en balayant périodiquement des cibles, tandis qu'une approche passive recueille des données en recevant ou en important principalement des données provenant de différentes sources.

1) L'acquisition de données doit prendre en charge l'approche active, telle que la collecte de données par balayage, par exploration ou par protocole simple de gestion de réseau (SNMP).

2) L'acquisition de données doit obligatoirement prendre en charge l'approche passive, telle que la réception de données par le protocole syslog ou le canal NetFlow, et l'importation manuelle de données.

La capacité d'acquisition des données doit s'adapter aux environnements d'informatique en nuage comme suit:

1) Il est recommandé que l'acquisition de données prenne en charge la collecte de données dans différents nuages, tels que les nuages multiples et les nuages hybrides.

2) Il est recommandé que l'acquisition des données s'adapte aux changements dynamiques des ressources dans les environnements d'informatique en nuage.

3) Il est recommandé que l'acquisition de données prenne en charge la collecte des journaux de données du trafic réseau est-ouest des plates-formes d'informatique en nuage.

Les nœuds d'acquisition d'une plate-forme NSSA doivent également disposer des capacités suivantes:

1) Les nœuds d'acquisition doivent obligatoirement filtrer les données et examiner la validité des données, notamment le type de données et la plage de valeurs, et filtrer les données non valides conformément à des politiques préconfigurées.

2) Il est recommandé que les nœuds d'acquisition appliquent un mécanisme de recollecte des données en cas d'échec de la collecte.

8.1.2 Source de données

Une plate-forme NSSA doit permettre d'appliquer des opérations de création, de lecture, de mise à jour et de suppression (CRUD) à ses données, et de collecter les types de données suivants:

1) Elle doit obligatoirement permettre de collecter les données relatives aux actifs des plates-formes d'informatique en nuage, telles que les données relatives aux pools de ressources virtuelles, aux équipements de réseau, aux hôtes, aux équipements de sécurité, aux systèmes, aux logiciels et aux plates-formes de gestion de l'informatique en nuage.

2) Elle doit obligatoirement permettre de collecter différents types de données de journaux, telles que les journaux d'accès au web, les journaux de sécurité, les journaux d'exploitation commerciale et les journaux de connexion, à partir de sources multiples, telles que les hôtes, les intergiciels et les plates-formes de gestion de l'informatique en nuage, et de recevoir les résultats de l'analyse des journaux provenant d'autres systèmes.

3) Elle doit obligatoirement permettre de collecter diverses données sur les vulnérabilités à partir de multiples équipements et composants des plates-formes d'informatique en nuage, telles que les vulnérabilités liées au débordement de tampon, à l'injection, à la logique commerciale, à la conception, à la configuration, etc.

4) Elle doit obligatoirement permettre de collecter les données de multiples événements d'attaques réseau, telles que les attaques DDoS, les attaques par exploitation de vulnérabilités et les accès non autorisés.

5) Elle doit obligatoirement permettre de collecter des renseignements sur les menaces, tels que des renseignements sur les IP/domaines/URL, les échantillons malveillants, les listes noires de commande et de contrôle (C&C) et les vulnérabilités.

8.1.3 Prétraitement des données

Afin de satisfaire aux exigences de qualité des données, la plate-forme NSSA doit obligatoirement mettre en œuvre le nettoyage et le filtrage des données, la normalisation, la corrélation et la validation, la fusion et la déduplication des données collectées, puis stocker les données normalisées.

1) Nettoyage des données: la plate-forme NSSA doit permettre le nettoyage des données en cas d'erreurs, d'incomplétude, d'invalidité et d'autres problèmes présents dans les données collectées, notamment comme suit:
   - Elle doit obligatoirement prendre en charge la conversion, le traitement et le filtrage des données en cas de formats incohérents, d'erreurs de saisie et de données incomplètes.
   - Il est recommandé de prendre en charge le filtrage et le nettoyage des données sur la base d'opérations conditionnelles, de correspondances d'expressions régulières et de calculs d'expressions.
   - Il est recommandé de prendre en charge la déduplication des données.
2) Normalisation des données: la plate-forme NSSA doit permettre un formatage uniforme de différents types de données hétérogènes et la préservation des données collectées originales, notamment comme suit:
   - Elle doit obligatoirement prendre en charge la normalisation des champs de données sur la base des règles de champ de chaque type de données.
   - Il est recommandé de prendre en charge le formatage uniforme du contenu brut à l'aide d'expressions régulières.
   - Il est recommandé de favoriser la conservation des données d'origine recueillies, afin de faciliter l'analyse de la traçabilité et le développement personnalisé.
3) Corrélation et validation des données: il est recommandé que la plate-forme NSSA prenne en charge la corrélation des données et la validation des données normalisées, qui comprennent les informations sur les utilisateurs, les informations sur les actifs, les informations sur la localisation géographique et les renseignements sur les menaces. Il est également recommandé de prendre en charge la sélection de données et de champs particuliers à valider.
4) Fusion de données: il est recommandé que la plate-forme NSSA prenne en charge la fusion de données normalisées sur la base de règles configurées, et qu'elle prenne en charge la sélection de données et de champs particuliers à fusionner.

8.1.4 Exigences en matière de sécurité liée à l'acquisition de données

1) La plate-forme NSSA doit obligatoirement prendre en charge le contrôle d'accès aux nœuds d'acquisition et surveiller le processus de collecte des données en émettant des alertes en temps utile en cas d'événements anormaux.
2) Il est obligatoire de restreindre strictement l'emplacement de stockage temporaire des données pendant le processus de collecte des données, qui ne peut pas être modifié arbitrairement.

3) La plate-forme NSSA doit obligatoirement prendre en charge les classifications et identifications hiérarchiques des données collectées et mettre en œuvre des mesures de sécurité telles que le cryptage des données sensibles, parmi lesquelles les données relatives aux actifs, les données opérationnelles et les données de journaux.

4) La plate-forme NSSA doit obligatoirement prendre en charge le masquage et la désensibilisation des données sensibles avant le prétraitement et l'analyse, et répondre aux exigences de conformité des données collectées en matière de sécurité.

5) La plate-forme NSSA doit obligatoirement conserver les données collectées et les journaux opérationnels, afin de pouvoir générer des alertes en temps utile en cas d'événements anormaux, et de procéder à des audits, y compris effectuer les actions suivantes:

- Il est obligatoire d'auditer les opérations des utilisateurs et des administrateurs afin de détecter, d'alerter et de répondre aux comportements malveillants tels que l'utilisation abusive de données.
- Il est recommandé de signaler les interruptions de transmission pendant la collecte des données.
- Il est recommandé d'émettre une alerte si le stockage des données dépasse un seuil prédéfini pendant la collecte et la transmission des données.

8.2 Exigences en matière de stockage des données

Le stockage des données de la plate-forme NSSA doit appliquer des techniques de mégadonnées pour répondre aux exigences de stockage des données multi-sources, multi-dimensionnelles et à croissance continue générées par l'environnement de l'informatique en nuage, telles que les résultats d'analyse et les renseignements sur les menaces externes. La plate-forme NSSA doit prendre en charge les mécanismes de stockage en fonction des différents domaines et classifications des divers types de données, et répondre aux exigences des différentes méthodes d'analyse et d'isolation des données. Dans le même temps, la plate-forme NSSA doit garantir la disponibilité, l'intégrité et la confidentialité des données stockées.

8.2.1 Catégorisation du stockage des données

Il est recommandé que la plate-forme NSSA prenne en charge le stockage de données non structurées, de données structurées et de données semi-structurées en fonction de diverses sources de données et qu'elle prenne en charge plusieurs catégories de stockage de données, y compris le stockage de données relationnelles, les bases de données non relationnelles (NoSQL), le stockage de fichiers distribués et la recherche plein texte distribuée.

Les catégories de stockage de données de la plate-forme NSSA sont recommandées tel que décrit dans le Tableau 8-1.

Tableau 8-1 – Catégorisation des données

Source de données	Contenu de données	Volume de données	Catégorisation du stockage (recommandé)
Hébergeur du nuage/conteneur/ OS	Journaux d'exploitation, journaux de sécurité, données sur l'état de fonctionnement, fichiers de configuration, etc.	Grand	Stockage de fichiers distribués/recherche plein texte distribuée/bases de données NoSQL
Plate-forme de gestion en nuage	Journaux d'accès, journaux d'exploitation, fichiers de configuration, données sur le déroulement des opérations, etc.	Moyen	Stockage de fichiers distribués/recherche plein texte distribuée/bases de données NoSQL
Équipement de réseau	Journaux des routeurs, des commutateurs et de la plate-forme réseau, tables de routage, fichiers de configuration, etc.	Grand	Stockage de fichiers distribués/recherche plein texte distribuée/bases de données NoSQL
Équipements de sécurité	Journaux des pare-feu, système de détection des intrusions (IDS), système de prévention des intrusions (IPS), réseau privé virtuel (VPN), application web de pare-feu (WAF), fichiers de configuration, etc.	Grand	Stockage de fichiers distribués/recherche plein texte distribuée/bases de données NoSQL
Système d'applications	Journaux de bases de données, intergiciels, systèmes d'applications, fichiers de configuration, etc.	Grand	Stockage de fichiers distribués/recherche plein texte distribuée/bases de données NoSQL
Données de base	Données sur les actifs, données sur les comptes, dictionnaire IP, données sur les services, etc.	Moyen	Bases de données rationnelles/recherche plein texte distribuée/bases de données NoSQL
Trafic réseau	Données DPI, données de flux réseau, etc.	Massif	Stockage de fichiers distribués
Renseignements sur les menaces	Renseignements stratégiques, renseignements tactiques, informations sur la sécurité, etc.	Moyen	Stockage de fichiers distribués/recherche plein texte distribuée/bases de données NoSQL
Résultats de l'analyse	Événements de sécurité, données de conformité, indices de sécurité, etc.	Moyen	Bases de données rationnelles/saisie plein texte distribuée/bases de données NoSQL

8.2.2 Exigences techniques en matière de stockage des données

La plate-forme NSSA doit développer une architecture de stockage de données élastique et évolutive pour répondre à la croissance continue du volume de données, ainsi qu'aux exigences de classification des données et de stockage hiérarchique. Le cycle de vie du stockage des données doit également varier en fonction des règles de conformité, des exigences de l'entreprise et des coûts économiques.

1) Il est recommandé que la plate-forme NSSA prenne en charge les bases de données rationnelles courantes. Il est recommandé que les bases de données rationnelles prennent en charge une interface d'accès au modèle relationnel complet, y compris l'interface SQL standard, l'interface standard de développement d'applications (JDBC, ODBC, etc.).

2) Il est recommandé que la plate-forme NSSA prenne en charge les principales bases de données NoSQL.

3) Il est recommandé que la plate-forme NSSA prenne en charge les composants typiques des mégadonnées, tels que Hive, HBase et les composants MPP, afin de supporter des fonctionnalités étendues.

4) Il est recommandé que la plate-forme NSSA adopte des composants de recherche plein texte, qui permettent la saisie par mot-clé, la recherche multi-mots, la recherche combinée de texte intégral et d'autres champs, ainsi que la correspondance par préfixe, la correspondance floue et d'autres conditions de recherche.

5) Il est recommandé que la plate-forme NSSA adopte des composants de bus de messages distribués, tels que Kafka, RabbitMQ, etc. Les composants du bus de messages distribués doivent prendre en charge des fonctions telles que la compression des données, la définition de la durée de conservation des données et la suppression automatique des données périmées.

6) Il est recommandé que la plate-forme NSSA prenne en charge le stockage en ligne et les mécanismes de sauvegarde pour garantir la disponibilité des données.

7) Il est recommandé que la plate-forme NSSA prenne en charge le stockage des métadonnées, notamment:

- Les métadonnées techniques et leur utilisation pour la maintenance des données, telles que la manière dont les données sont stockées pour permettre un accès efficace aux données.
- Les métadonnées de gestion, telles que les politiques de contrôle d'accès aux données, et les résultats du traitement des données.

8.2.3 Exigences de sécurité en matière de stockage des données

1) La plate-forme NSSA doit obligatoirement développer des mécanismes de contrôle d'accès aux données, tels que le contrôle d'accès au stockage des données basé sur les rôles, pour empêcher les accès non autorisés.

2) La plate-forme NSSA doit obligatoirement prendre en charge le chiffrement du stockage des données importantes ou sensibles. Il est recommandé de clarifier les exigences en matière de chiffrement du stockage des différents types de données sur la base de la classification des données et de la définition hiérarchique, telles que les exigences en matière d'algorithmes de chiffrement des données et de gestion des clés de chiffrement.

3) La plate-forme NSSA doit obligatoirement mettre en œuvre des techniques et des mesures de contrôle appropriées pour garantir l'intégrité du stockage des données et la cohérence des données sur plusieurs copies.

4) La plate-forme NSSA doit obligatoirement mettre en œuvre des techniques et des mesures de contrôle appropriées pour garantir la disponibilité du stockage des données. Sur la base des principes de classification des données, il est recommandé de clarifier les politiques de sauvegarde et de récupération des différentes données, telles que les modes de sauvegarde et les exigences en matière de période de stockage et de temps de récupération.

5) Il est recommandé que la plate-forme NSSA teste périodiquement les mécanismes de stockage des données afin de vérifier les capacités d'identification des défaillances des données et de reconstruction des sauvegardes.

6) La plate-forme NSSA doit obligatoirement générer tous les journaux de traitement du stockage des données, afin de garantir la traçabilité des processus de stockage des données et de fournir des capacités d'alerte en cas de comportements anormaux.

8.3 Exigences en matière de calcul et d'analyse situationnels

Le calcul et l'analyse situationnels de la plate-forme NSSA comprennent principalement le moteur de calcul et d'analyse et les modules fonctionnels d'analyse situationnelle.

1) Le moteur de calcul et d'analyse fournit des capacités informatiques de modélisation et d'analyse des menaces pour les modules de fonction d'analyse situationnelle. Le moteur de calcul et d'analyse comprend des cadres de modélisation de la sécurité et de traitement des données massives, tels que le moteur de calcul hors ligne et le calcul en temps réel.

2) Les modules de fonction d'analyse situationnelle réalisent principalement l'analyse situationnelle de la sécurité du réseau dans l'environnement de l'informatique en nuage sur la base de l'exploration des données et de l'analyse des menaces sur diverses données d'actifs agrégées, telles que les événements de sécurité, les données de journaux et les données de trafic du réseau.

3) Pour améliorer l'efficacité des calculs et de l'analyse, il est obligatoire d'élaborer une représentation unifiée des différents événements de sécurité et des informations sur les actifs avant la modélisation de la sécurité, ce qui peut être réalisé par la vectorisation du contexte. La méthode de vectorisation fait correspondre le contexte à un espace euclidien, et sert généralement de base à l'adoption de divers algorithmes d'intelligence artificielle pour le calcul de la similarité et de la corrélation.

8.3.1 Exigences relatives au moteur de calcul et d'analyse

8.3.1.1 Modélisation de la sécurité

La modélisation de la sécurité doit obligatoirement inclure la modélisation de la corrélation, la modélisation statistique, la modélisation de la corrélation des renseignements sur les menaces et la modélisation de l'intelligence artificielle, afin de fournir des capacités d'analyse et d'exploration approfondies des données situationnelles de base.

1) **Modélisation des corrélations**: une méthode de correspondance basée sur des règles est utilisée pour effectuer des associations logiques et des analyses de correspondance des caractéristiques sur des événements hétérogènes et hétérogènes.
   - Il est obligatoire de prendre en charge l'analyse de corrélation logique basée sur la causalité des incidents de sécurité.
   - Il est obligatoire de prendre en charge la corrélation de données hétérogènes multi-sources sous de multiples aspects, tels que le temps et l'espace.
   - Il est recommandé de prendre en charge le regroupement des informations d'alerte en fonction des situations dynamiques de la sécurité du réseau, afin de réduire le nombre d'alertes et d'améliorer l'efficacité de la réponse.

2) **Modélisation statistique**: utilisation de méthodes statistiques pour calculer les caractéristiques quantitatives de divers événements, telles que la fréquence et la période d'occurrence, et obtenir la répartition des données relatives aux événements, des principales caractéristiques, de la tendance des séries temporelles, de l'existence éventuelle de valeurs anormales et des résultats sommaires des événements.
   - Il est recommandé de prendre en charge la réalisation d'analyses statistiques des événements de sécurité, des comportements de sécurité, des menaces de sécurité et d'autres caractéristiques, et de détecter les caractéristiques statistiques importantes des menaces de sécurité à partir de diverses sources de données.

3) **Association de renseignements sur les menaces**: il est recommandé de prendre en charge l'intégration des capacités de renseignement sur les menaces, afin de détecter des événements précis basés sur les renseignements sur les menaces dans l'environnement de l'informatique en nuage.

4) **Modélisation de l'IA**: il est recommandé de prendre en charge divers algorithmes d'intelligence artificielle intégrés, notamment l'algorithme de chronométrage, l'algorithme de classification, l'algorithme de regroupement et d'autres prototypes d'algorithmes, afin de fournir aux utilisateurs des capacités d'apprentissage et d'analyse des données arbitraires, ainsi que d'analyser les menaces de sécurité avancées et les menaces inconnues.

- Il est recommandé de prendre en charge les algorithmes courants, tels que l'analyse de grappes, l'analyse d'association, l'analyse d'arbre de décision, l'analyse de régression et d'autres algorithmes d'analyse de l'intelligence artificielle/apprentissage automatique.
- Il est recommandé que la plate-forme NSSA prenne en charge la gestion centralisée de la modélisation et de la politique de sécurité pour faciliter une exécution efficace ainsi qu'un déploiement rapide.

8.3.1.2 Cadre de calcul pour les mégadonnées

Il est obligatoire de prendre en charge les cadres de calcul hors ligne et en temps réel, afin de réaliser le traitement par lots de données statiques et l'analyse en temps réel de données dynamiques (données en continu).

1) **Cadre de calcul hors ligne**: il est obligatoire pour prendre en charge les déploiements d'algorithmes hors ligne, les modèles d'entraînement et les scénarios d'apprentissage automatique. Les analystes peuvent utiliser le moteur d'analyse hors ligne pour exploiter les données en profondeur, en ayant un retour d'information immédiat sur les résultats de l'algorithme, ce qui permet d'entraîner les modèles.
2) **Cadre de calcul en continu et en temps réel**: il est recommandé que le cadre de calcul en temps réel prenne en charge une architecture distribuée et que la capacité de stockage puisse être ajustée de manière dynamique. La haute disponibilité et la séparation des politiques de lecture et d'écriture peuvent garantir la lecture et l'écriture séparées des données lors de l'analyse des données hors ligne.

8.3.2 Exigences des modules fonctionnels d'analyse situationnelle

Sur la base du moteur de calcul et d'analyse, les modules de fonction d'analyse situationnelle établissent des capacités d'analyse basées sur des scénarios pour diverses données relatives aux actifs, les événements de sécurité, les données de journaux, les données de trafic et d'autres données, et fournissent des scénarios d'analyse de la sécurité basés sur des données multiples afin d'obtenir des alertes de sécurité basées sur des scénarios et des capacités d'alerte précoce. Les modules fonctionnels d'analyse situationnelle comprennent l'analyse de la sécurité du réseau, l'analyse de la sécurité des actifs et l'analyse du comportement des utilisateurs à haut risque dans l'environnement de l'informatique en nuage.

8.3.2.1 Analyse de la sécurité des réseaux

Le module d'analyse de la sécurité du réseau doit obligatoirement être capable d'analyser diverses situations d'attaque du réseau, telles que le trafic réseau anormal, la propagation de programmes malveillants et l'accès à des noms de domaine malveillants dans l'environnement de l'informatique en nuage, ainsi que de retracer leurs tendances de variation.

1) Il est recommandé de prendre en charge la détection et l'analyse statistique de la situation générale des attaques courantes, et d'analyser les tendances de variation de la situation actuelle des attaques.

- Il est recommandé de prendre en charge les fonctions de détection et d'analyse des attaques réseau basées sur des données multi-sources, qui comprennent les intrusions de réseau, les attaques web, les logiciels malveillants, les attaques DDoS, la reconnaissance de réseau, les activités suspectes et d'autres types d'attaques de réseau.

- Il est recommandé de prendre en charge l'analyse statistique des différents types d'attaques de réseau et l'analyse de la variation des tendances dans le cadre de différents types d'attaques.

2) Il est recommandé de prendre en charge la détection et l'analyse statistique de la situation générale du trafic réseau anormal dans l'environnement de l'informatique en nuage, et d'analyser la variation de tendance du trafic réseau anormal actuel.

   - Il est recommandé de prendre en charge l'identification anormale du trafic réseau, et de pouvoir détecter et analyser le trafic anormal des protocoles basés sur les ports de virus communs.
   - Il est recommandé de prendre en charge l'analyse statistique du trafic réseau anormal, ainsi que la fusion et les statistiques du trafic anormal des protocoles, et d'analyser la tendance du trafic anormal.

3) Il est recommandé de prendre en charge l'analyse de la situation générale de la propagation des programmes malveillants tels que les virus, les vers et les chevaux de Troie dans l'environnement de l'informatique en nuage, et d'analyser les tendances actuelles en matière de propagation des programmes malveillants.

4) Il est recommandé de prendre en charge la détection et l'analyse statistique des hôtes C&C de botnets et des hôtes zombies, ainsi que l'analyse de la propagation et de la variation des tendances des botnets.

5) Il est recommandé de prendre en charge l'analyse des statistiques d'accès et la propagation des noms de domaine malveillants, des adresses IP C&C et des noms de domaine d'algorithme de génération de domaines (DGA).

6) Il est recommandé de prendre en charge le modèle de chaîne d'attaque pour retracer la source des événements d'attaque en classant les événements de sécurité générés en fonction du processus d'attaque, qui comprend la collecte d'informations, l'intrusion dans le réseau, la C&C, la pénétration horizontale, l'atteinte des objectifs et le nettoyage des preuves.

7) Il est recommandé de prendre en charge l'analyse des informations relatives aux auteurs d'attaques sur la base des renseignements sur les menaces.

8.3.2.2 Analyse de la sécurité des actifs

Il est obligatoire de prendre en charge l'analyse de l'état de sécurité des différents actifs de la plate-forme d'informatique en nuage. Il est recommandé d'analyser l'état de la sécurité de l'infrastructure d'informatique en nuage, des machines virtuelles, des conteneurs et des systèmes d'entreprise à l'aide des journaux des équipements de sécurité, des journaux des systèmes, des résultats de l'analyse des vulnérabilités et d'autres données. Les types d'analyse comprennent l'analyse des attaques du système et l'analyse des vulnérabilités du système.

8.3.2.3 Analyse des informations sur les actifs

1) Il est obligatoire de prendre en charge l'analyse statistique des actifs, y compris l'analyse basée sur les classifications, les catégorisations et les priorités d'actifs, ainsi que les mises à jour de l'état des actifs, telles que l'ajout ou la suppression d'actifs.

2) Il est obligatoire de prendre en charge l'analyse de la distribution des actifs, y compris l'analyse basée sur les informations géographiques des actifs, les appartenances aux départements et les applications web importantes.

3) Il est obligatoire de rechercher et d'afficher des informations sur les actifs en fonction de leur adresse IP, de leur classification, de leur priorité et de leur emplacement géographique.

8.3.2.4 Analyse des menaces pesant sur les actifs

1) Il est obligatoire de prendre en charge l'analyse des menaces d'attaque du système, y compris la détection de la destruction des journaux, la détection de l'escalade des privilèges du système, la détection des journaux d'erreurs et la détection des attaques par force brute. L'analyse peut être mise en œuvre sur la base de l'analyse de corrélation des données relatives aux actifs, aux journaux des appareils, aux journaux des systèmes hôtes, aux données des systèmes de sécurité et aux renseignements sur les menaces.

2) Il est obligatoire de prendre en charge l'analyse statistique et l'analyse des tendances des menaces pesant sur les actifs.

8.3.2.5 Analyse de la vulnérabilité des actifs

1) Il est obligatoire de prendre en charge l'analyse de corrélation des résultats de l'analyse de la vulnérabilité des actifs et des journaux de détection des dispositifs de sécurité pour effectuer l'analyse de l'utilisation de la vulnérabilité, y compris l'analyse de la vulnérabilité des machines hôtes/machines virtuelles/conteneurs et l'analyse de la vulnérabilité des applications, ainsi que l'analyse statistique des actifs présentant un risque d'exploitation de vulnérabilités en fonction du temps, du système d'entreprise, du niveau de vulnérabilité et d'autres données de dimensionnement.

8.3.2.6 Analyse de la conformité des configurations des actifs

1) Il est obligatoire de prendre en charge l'analyse des résultats de conformité de la configuration des systèmes d'exploitation, des logiciels de virtualisation, des bases de données, des équipements de réseau et des intergiciels dans l'environnement de l'informatique en nuage.

2) Il est obligatoire de prendre en charge l'analyse statistique des éléments non conformes qui ont été détectés, ainsi que l'analyse des risques liés à l'utilisation d'éléments non conformes par des agresseurs pour attaquer des actifs.

8.3.2.7 Analyse du comportement des utilisateurs

Il est recommandé de prendre en charge la détection et l'analyse des comportements anormaux des utilisateurs internes accédant à la plate-forme d'informatique en nuage, et des comportements anormaux des actifs et des systèmes d'entreprise, ainsi que l'analyse de profilage du comportement des utilisateurs.

1) Il est recommandé de prendre en charge l'analyse des comportements anormaux des utilisateurs, notamment les opérations anormales portant sur des données sensibles, la connexion à des comptes expirés, la diffusion illégale, l'exécution de commandes sensibles, l'attaque par force brute et la connexion à une adresse anormale.

2) Il est recommandé de prendre en charge le profilage basé sur le comportement des utilisateurs internes, y compris les caractéristiques de comportement individuel des utilisateurs et les caractéristiques de groupe.

3) Il est recommandé de prendre en charge la personnalisation des règles de comportement anormal et des modèles de comportement.

4) Il est recommandé de prendre en charge l'analyse des comportements anormaux sur la base des profils d'utilisateurs et de comparer les comportements individuels ou collectifs d'une journée avec les données de comportement historiques afin d'extraire les anomalies.

5) Il est recommandé de prendre en charge l'analyse des comportements anormaux de diverses ressources d'informatique en nuage et de pouvoir identifier les comportements anormaux susceptibles de se produire dans un environnement d'informatique en nuage, tels que les comportements anormaux des hébergeurs, les outils anormaux du système d'appel, les comportements anormaux du réseau et les sorties de communication illégales.

8.4 Exigences en matière d'évaluation situationnelle

L'évaluation situationnelle de la plate-forme NSSA est recommandée pour prendre en charge l'évaluation situationnelle dynamique de l'état général de la sécurité dans l'environnement de l'informatique en nuage, en prédisant la tendance situationnelle, sur la base de l'analyse des données de sécurité multidimensionnelles, des résultats de l'analyse de sécurité de la plate-forme d'informatique en nuage et de la modélisation de l'évaluation de la catégorie de l'indice situationnel. Elle permet d'émettre des alertes précoces et d'interagir avec les mécanismes de prise de décision en matière de sécurité et d'intervention d'urgence du fournisseur de services en nuage (CSP)/client de services en nuage (CSC).

8.4.1 Évaluation de la situation

L'évaluation de la situation en matière de sécurité porte sur la situation globale de la plate-forme en nuage, la situation en matière de sécurité des actifs en nuage, les menaces, les vulnérabilités, les attaques de réseau et l'état de disponibilité de la plate-forme en nuage et de ses composants.

1) Il est obligatoire de collecter les informations sur les actifs en tant que source de données pour créer une catégorie d'indice d'évaluation des conditions de sécurité. Les informations sur les actifs doivent inclure la version spécifique des systèmes d'exploitation, des intergiciels, des applications et des bases de données, la topologie du réseau, la valeur des actifs, etc. afin de générer des indicateurs d'évaluation raisonnables.

2) Il est obligatoire de prendre en charge une catégorie d'indice d'évaluation des conditions de sécurité de la plate-forme d'informatique en nuage, en créant des indicateurs généraux dans une échelle unifiée destinés à mesurer les conditions de sécurité, ainsi qu'en quantifiant divers éléments des conditions de sécurité du réseau.

   - Il est recommandé de créer des indicateurs qualitatifs et quantitatifs dans le cadre de l'évaluation de la situation du réseau. Les indicateurs qualitatifs sont des évaluations subjectives basées sur des analyseurs professionnels de la sécurité. Par exemple, les analyseurs de sécurité peuvent attribuer des niveaux de gravité à des vulnérabilités ou à des attaques de réseau sur la base de leur expérience. Les indicateurs quantitatifs proviennent de la collecte et de l'analyse de données brutes.
   - Il est recommandé de prendre en charge les calculs de similarité et de corrélation dans le cadre du traitement des indicateurs de menaces, y compris les suivants:
     – Il est recommandé d'utiliser le calcul de similarité du contexte de menace pour reconnaître les menaces qui surgissent facilement, telles que le balayage, le piratage par force brute et les attaques DDoS, afin d'éviter les changements radicaux d'un indicateur spécifique causés par un grand nombre d'alarmes répétées.
     – Il est recommandé d'utiliser l'analyse de corrélation entre les informations sur les menaces et les actifs pour reconnaître les menaces d'attaques aveugles et de tentatives massives, afin de permettre au personnel de sécurité de trouver rapidement les indicateurs à haut risque qui nécessitent réellement une réponse.
     – Il est recommandé d'adopter un cadre algorithmique unifié pour réaliser l'analyse de corrélation et l'analyse de similarité, tel que l'angle cosinus. Le cadre algorithmique unifié peut évidemment réduire les coûts de maintenance liés à l'utilisation des algorithmes.
   - Il est recommandé de créer l'indicateur général et les indicateurs de subdivision pour l'évaluation des conditions de sécurité du réseau. L'indicateur général reflète les caractéristiques globales de l'évaluation de la sécurité de la plate-forme d'informatique en nuage; les indicateurs de subdivision peuvent être décomposés pour différents composants ou systèmes, qui reflètent les différences entre les résultats de l'évaluation de la situation pour divers composants/systèmes.

- Il est recommandé de prendre en charge la création des catégories d'indicateurs de situation, notamment les catégories suivantes:
  - Il est recommandé de prendre en charge la création d'indicateurs opérationnels pour les plates-formes d'informatique en nuage, tels que l'utilisation des pools de ressources en nuage et les délais d'accès des entreprises.
  - Il est recommandé de prendre en charge la création d'indicateurs de menaces pour la sécurité des réseaux, y compris divers incidents de sécurité des réseaux, qui peuvent être calculés et évalués en fonction de leur fréquence et de leur gravité.
  - Il est recommandé de prendre en charge la création d'indicateurs permettant d'évaluer la sécurité des actifs en nuage, tels que les menaces et les vulnérabilités des actifs, y compris la gravité des vulnérabilités, et d'évaluer si les vulnérabilités ont été corrigées ou non.
  - Il est recommandé de prendre en charge la création d'indicateurs de sécurité du comportement des utilisateurs, tels que les accès anormaux, les connexions et les téléchargements de logiciels malveillants. En outre, il est obligatoire d'adopter des techniques de protection de la confidentialité des utilisateurs, telles que la désensibilisation des données et l'anonymisation des données pour protéger la confidentialité des utilisateurs.

3) Il est recommandé d'élaborer un mécanisme ou un modèle complet d'évaluation des conditions de sécurité, basé sur des catégories d'indicateurs hiérarchiques et multidimensionnels.

- Il est obligatoire de prendre en charge la normalisation des différents indicateurs de subdivision, y compris les indicateurs qualitatifs et quantitatifs, afin d'éviter que les résultats de l'évaluation ne soient faussés par des différences d'unité et d'ampleur. Il est recommandé d'adopter des techniques de conversion pour convertir les indicateurs qualitatifs en valeurs numériques en vue d'un calcul ou d'une analyse plus poussés.
- Il est recommandé de prendre en charge les mécanismes d'évaluation multidimensionnelle de la situation, y compris l'évaluation axée sur les risques, l'évaluation axée sur les menaces ou la modélisation basée sur des données de séries temporelles.
- Il est recommandé de prendre en charge différents modèles d'évaluation, y compris des modèles basés sur des modèles mathématiques théoriques ou des raisonnements fondés sur la connaissance.
- Il est recommandé de prendre en charge une méthode d'évaluation hiérarchique ascendante en traitant de manière exhaustive les indicateurs de situation des niveaux inférieurs, puis en calculant les résultats de l'évaluation de la situation des niveaux supérieurs, et en calculant progressivement l'évaluation globale des conditions de sécurité.
- Dans les méthodes d'évaluation hiérarchique, il est recommandé d'appuyer le calcul de similarité sur l'interprétabilité d'une valeur d'évaluation d'une situation spécifique, en la comparant aux valeurs historiques et proches. Afin d'obtenir une valeur d'évaluation finale, un vecteur multidimensionnel peut être élaboré en choisissant les résultats précédents d'un niveau spécifique, qui peut être utilisé pour calculer la similarité des valeurs historiques proches par le cosinus d'angle, la distance espace-vecteur et d'autres algorithmes. Le calcul des similitudes permet au personnel de sécurité de détecter les anomalies plus facilement et de mieux comprendre la situation.

4) Il est recommandé de prendre en charge les capacités à retracer efficacement les évaluations historiques des conditions de sécurité de la plate-forme en nuage, en mettant en œuvre le prétraitement des journaux, l'indexation des champs clés, la recherche plein texte et l'interrogation floue.

8.4.2 Projection de la tendance situationnelle

Sur la base de l'acquisition et du suivi de l'état de sécurité de l'environnement d'informatique en nuage, de l'extraction des éléments de sécurité et des indicateurs clés qui peuvent entraîner des changements dans la situation du réseau, la plate-forme NSSA est recommandée pour aider à prédire la tendance globale en matière de sécurité, la tendance de sécurité des composants de subdivision et les risques de sécurité potentiels sur la base de modèles de projection des conditions de sécurité orientés vers la plate-forme en nuage.

1) Il est obligatoire de prendre en charge la construction d'une catégorie d'indicateurs hiérarchiques et multidimensionnels sur la base des données collectées et des résultats analysés, ainsi que de prévoir la tendance de la situation à l'aide de modèles de prévision pertinents.

2) Il est recommandé de prendre en charge les modèles de prédiction courants, y compris les modèles de prédiction de régression basés sur l'apprentissage automatique, les modèles d'apprentissage profond et les modèles de prédiction basés sur les équations différentielles dans les domaines professionnels.

3) Il est recommandé de prendre en charge les résultats de la prédiction informatique en fusionnant différents modèles de prédiction afin d'améliorer la précision de la prédiction. Il s'agit notamment de:

   - Contrôler la précision de chaque modèle en calculant les valeurs de la fonction de perte entre la prédiction et les résultats des données.
   - Combiner les résultats de chaque modèle à l'aide de pondérations, et procéder à des ajustements adaptatifs des pondérations entre les modèles. Par exemple, le poids de chaque modèle peut être ajusté de manière adaptative sur la base du résultat du contrôle de la fonction de perte; l'entraînement hors ligne des données les plus récentes peut également être déclenché automatiquement pour mettre à jour le modèle et améliorer la précision.

8.4.3 Mécanismes de pré-alerte

La plate-forme NSSA doit fournir des mécanismes d'alerte précoce concernant les risques de sécurité potentiels dans l'environnement de l'informatique en nuage, sur la base des résultats de l'analyse de la sécurité, de l'évaluation situationnelle et des prédictions de la situation.

1) Il est recommandé de fournir des alertes précoces sur les vulnérabilités des actifs en établissant une corrélation entre les vulnérabilités et les données de renseignement sur les menaces, les données relatives aux événements de sécurité, etc. et d'analyser la vulnérabilité des actifs de la plate-forme en nuage.

2) Il est recommandé de prendre en charge les alertes précoces d'attaques potentielles de réseau sur la base de la tendance de prédiction, y compris les balayages malveillants, les attaques web, les attaques DDoS, les attaques consistant à deviner les mots de passe et les attaques de vulnérabilité du système.

3) Il est recommandé de prévoir des alertes précoces en cas de comportement anormal de l'utilisateur sur la base de la prédiction des tendances, notamment en cas d'opérations anormales sur des données sensibles, de connexion à un compte expiré, d'exécution de commandes à haut risque, etc. Avant d'émettre des alertes, il est obligatoire d'utiliser des techniques de désensibilisation et d'anonymisation des données afin de protéger la confidentialité des utilisateurs.

4) Il est recommandé de favoriser les alertes précoces sur les menaces de sécurité non détectées en associant les comportements anormaux détectés, les renseignements sur les menaces et les journaux originaux, etc.

5) Les mécanismes d'alerte précoce sont les suivants:

- Il est recommandé de permettre l'émission d'alertes précoces basées sur des politiques préconfigurées, qui peuvent être personnalisées en conséquence.
- Il est recommandé de prendre en charge la gestion hiérarchique des alertes précoces et de classer les niveaux d'alerte en fonction de leur importance et de leur gravité.
- Il est recommandé de prendre en charge l'émission d'alertes par l'intermédiaire d'API, ce qui permet aux systèmes tiers de recevoir des alertes et de réagir en conséquence.

8.5 Exigences en matière de visualisation de la situation

La plate-forme NSSA doit obligatoirement permettre d'afficher les conditions de sécurité de plusieurs scénarios, notamment les conditions globales de sécurité, les conditions de sécurité du réseau, les conditions de sécurité des actifs et les conditions de sécurité personnalisées. Parallèlement, il est recommandé d'utiliser plusieurs types d'aperçus pour afficher les informations détaillées relatives aux conditions de sécurité, telles que la carte radar, la carte des informations de corrélation et la carte des trajectoires des menaces et de permettre l'exploration des informations détaillées sur la sécurité.

8.5.1 Visualisation des conditions globales de sécurité

1) Il est recommandé de présenter des états d'évaluation de la sécurité globale de la plate-forme d'informatique en nuage au moyen de scores ou de notes.

2) Il est recommandé de présenter graphiquement les conditions globales de sécurité de la plate-forme d'informatique en nuage, notamment le classement des risques, la tendance des attaques de réseau, les vulnérabilités et les comportements à haut risque des utilisateurs.

3) Il est recommandé de présenter les conditions de sécurité des différents locataires, des différentes opérations commerciales et des différents actifs, etc. dans la plate-forme d'informatique en nuage, et de les comparer aux données historiques pour dégager des tendances.

4) Il est recommandé de prendre en charge la présentation en temps réel des alarmes agrégées des événements de sécurité du réseau, des comportements anormaux des utilisateurs et de l'état de la sécurité des actifs dans la plate-forme d'informatique en nuage, ainsi que de prendre en charge l'exploration des détails de ces alarmes sous forme de graphiques.

8.5.2 Visualisation des conditions de sécurité du réseau

1) Il est recommandé de présenter les risques de sécurité du réseau de la plate-forme d'informatique en nuage sous forme de graphiques multidimensionnels, notamment les résultats de l'analyse statistique des attaques de réseau, les types d'attaques de réseau, la distribution géographique des attaques de réseau, le trafic de réseau anormal, l'IP source et l'IP de destination des attaques.

2) Il est recommandé de présenter des alarmes de sécurité en temps réel de la plate-forme d'informatique en nuage, telles que les attaques de réseau, le trafic réseau anormal et les programmes malveillants. Les informations relatives aux alarmes comprennent l'horodatage, le type de sécurité, le niveau de gravité, l'adresse IP source et l'adresse IP destination des attaques.

3) Il est recommandé de prendre en charge l'exploration d'informations détaillées sur les conditions de sécurité du réseau.

8.5.3 Visualisation des conditions de sécurité des actifs

1) Il est recommandé de présenter graphiquement des informations relatives aux actifs de la plate-forme d'informatique en nuage, telles que l'échelle des actifs, les types d'actifs, la propriété des actifs et la répartition des actifs.

2) Il est recommandé de présenter graphiquement divers résultats d'analyse statistique de la plate-forme d'informatique en nuage, notamment les vulnérabilités des actifs, les attaques de réseau et les erreurs de configuration.

3) Il est recommandé de prendre en charge les risques de sécurité en temps réel des différents actifs de la plate-forme d'informatique en nuage dans plusieurs dimensions, notamment le nom de l'actif, les adresses IP de l'actif, les types d'attaques, les types de vulnérabilités, le nombre de vulnérabilités et les erreurs de configuration.

4) Il est recommandé de prendre en charge l'exploration d'informations détaillées sur les conditions de sécurité des actifs.

8.5.4 Visualisation situationnelle des comportements anormaux des utilisateurs

1) Il est recommandé de présenter les comportements anormaux des utilisateurs des plates-formes d'informatique en nuage dans plusieurs dimensions, notamment les types de comportements anormaux, les tendances de comportements anormaux et les utilisateurs anormaux (comptes ou IP).

2) Il est recommandé de présenter des alarmes de sécurité en temps réel concernant les comportements anormaux des utilisateurs de la plate-forme d'informatique en nuage, notamment l'heure de l'alarme, les types d'alarme, les niveaux de gravité et l'utilisateur (compte) anormal.

3) Il est recommandé de prendre en charge l'exploration des informations sur le comportement anormal des utilisateurs.

8.5.5 Visualisation personnalisée des conditions de sécurité

Il est recommandé de prendre en charge la configuration d'aperçus situationnels personnalisés de scénarios commerciaux spécifiques, et d'importer des configurations graphiquement ou par des scripts, en fonction des exigences commerciales, des rôles de gestion et d'autres exigences individuelles de la plate-forme d'informatique en nuage.

Bibliographie

[b-UIT-T-X.1217] Recommandation UIT-T X.1217 (2021), *Lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication.*

[b-UIT-T X.1601] Recommandation UIT-T X.1601 (2016), *Cadre de sécurité applicable à l'informatique en nuage.*

[b-UIT-T Y.3500] Recommandation UIT-T Y.3500 (2014) | ISO/IEC 17788:2014, *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire.*

[b-NIST-SP-800-30] Publication spéciale du NIST 1800-30 Révision 1 (2012), *Guide pour l'évaluation des risques.*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Publié en Suisse
Genève, 2024