ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1645 (09/2023)

SERIE X: Redes de datos, comunicaciones de sistemas abiertos y seguridad

Seguridad de la computación en nube – Prácticas óptimas y directrices en materia de seguridad de la computación en nube

---

Requisitos de una plataforma de conocimiento de la situación de seguridad de las redes para la computación en la nube

RECOMENDACIONES UIT-T DE LA SERIE X

Redes de datos, comunicaciones de sistemas abiertos y seguridad

REDES PÚBLICAS DE DATOS	X.1-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200-X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300-X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400-X.499
DIRECTORIO	X.500-X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850-X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900-X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	X.1000-X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	X.1100-X.1199
SEGURIDAD EN EL CIBERESPACIO	X.1200-X.1299
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	X.1300-X.1499
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	X.1500-X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	X.1600-X.1699
Visión general de la seguridad de la computación en nube	X.1600-X.1601
Diseño de la seguridad de la computación en nube	X.1602-X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	**X.1640-X.1659**
Aplicación práctica de la seguridad de la computación en nube	X.1660-X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680-X.1699
COMUNICACIÓN CUÁNTICA	X.1700-X.1729
SEGURIDAD DE LOS DATOS	X.1750-X.1799
SEGURIDAD EN LAS REDES IMT-2020	X.1800-X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1645

Requisitos de una plataforma de conocimiento de la situación de seguridad de las redes para la computación en la nube

Resumen

El conocimiento de la situación de seguridad de las redes (NSSA) se deriva del conocimiento de la situación. Suele incluir cuatro procesos, a saber, obtención de datos, análisis de la situación de seguridad, evaluación de la situación de seguridad y proyección de tendencias de la situación de seguridad, y normalmente incorpora las capacidades siguientes: 1) detección y supervisión constante de diferentes amenazas de ataque, comportamientos anómalos y su ámbito de influencia; 2) extracción de datos, análisis de amenazas y rastreo de comportamientos anómalos; 3) predicción y alerta temprana de situaciones relacionadas con la seguridad; 4) visualización de la situación de seguridad.

La plataforma NSSA desempeña una función importante para los proveedores de servicios de computación en la nube en la medida en que mejora la protección de seguridad de la computación en la nube, la capacidad para detectar violaciones de seguridad o comportamientos anómalos, la adopción de decisiones en materia de seguridad, la capacidad de respuesta de emergencia e, incluso, el mecanismo de alerta temprana de computación en la nube.

La Recomendación UIT-T X.1645 comienza presentando y desarrollando el concepto de NSSA; a continuación, se analizan las ventajas del NSSA para hacer frente a los problemas de seguridad de la computación en la nube y, por último, se documentan los requisitos de una plataforma NSSA para la computación en la nube.

Historia *

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	ITU-T X.1645	2023-09-08	17	11.1002/1000/15527

Palabras clave

Análisis de macrodatos, computación en la nube, conocimiento de la situación de seguridad de la red, conocimiento de la situación.

* Para acceder a la Recomendación, introduzca el URL https://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patentes/derechos de autor de *software*, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1645

Requisitos de una plataforma de conocimiento de la situación de seguridad de las redes para la computación en la nube

1 Alcance

En esta Recomendación se presentan el concepto de conocimiento de la situación de seguridad de las redes (NSSA) y los requisitos de una plataforma NSSA para la computación en la nube. Esta Recomendación está dirigida a los proveedores de servicios de computación en la nube.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 computación en la nube [b-UIT-T Y.3500]: Paradigma para dar acceso a la red a un conjunto elástico y ampliable de recursos físicos o virtuales compartibles con administración y configuración en autoservicio previa solicitud.

3.1.2 servicio en la nube [b-UIT-T Y.3500]: Una o varias capacidades que se ofrecen en la computación en la nube que se invoca a través de una interfaz definida.

3.1.3 cliente de servicios en la nube [b-UIT-T Y.3500]: Parte que mantiene una relación empresarial a los efectos de utilizar servicios en la nube.

3.1.4 proveedor de servicios en la nube [b-UIT-T Y.3500]: Parte que ofrece servicios en la nube.

3.1.5 vulnerabilidad [b-NIST-SP-800-30]: Punto débil de un sistema de información, de procedimientos de seguridad, de controles internos o de una implementación que podría explotar una fuente de amenaza.

3.1.6 inteligencia sobre amenazas [b-UIT-T-X.1217]: Conjunto de información organizada, analizada y depurada relativa a los ataques potenciales y reales que pueden amenazar a una organización.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 conocimiento de la situación: Capacidad para evaluar la situación en que se encuentran los elementos de un determinado entorno, así como sus relaciones en múltiples dimensiones, incluidos el tiempo y el espacio.

NOTA – Esto se consigue recabando datos de diversas fuentes, combinándolos y analizándolos. El objetivo del conocimiento de la situación es integrar y analizar la información de fuentes diversas para alcanzar una comprensión integral de su significado.

3.2.2 conocimiento de la situación de seguridad de las redes (NSSA): Capacidad de identificar y evaluar los principales elementos de seguridad de la red y de categorizarlos de acuerdo con normas basadas en las dimensiones temporal y espacial.

NOTA – Esa información evalúa la situación de seguridad global de la red y predice nuevas tendencias de la seguridad de la red mediante técnicas como el análisis estadístico, la extracción de datos y la inteligencia artificial. La información resultante puede presentarse en formato legible por el ser humano o como aportación a la automatización de la seguridad de la red.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

C&C	Instrucciones y control (*command and control*)
CRUD	Crear, leer, actualizar y suprimir (*create, read, update, and delete*)
CSC	Cliente de servicios en la nube (*cloud service customer*)
CSP	Proveedor de servicios en la nube (*cloud service provider*)
DDoS	Denegación de servicio distribuida (*distributed denial of service*)
DGA	Algoritmo de generación de dominio (*domain generation algorithm*)
Hbase	Base de datos Hadoop (*Hadoop database*)
IA	Inteligencia artificial
JDBC	Conectividad a bases de datos Java (*Java database connectivity*)
MPP	Procesamiento paralelo masivo (*massively parallel processing*)
NoSQL	No sólo lenguaje de consulta estructurado (*not only Structured Query Language*)
NSSA	Conocimiento de la situación de seguridad de las redes (*network security situational awareness*)
ODBC	Conectividad a bases de datos abiertas (*open database connectivity*)
SDI	Sistema de detección de intrusiones
SNMP	Protocolo de gestión de red simple (*simple network management protocol*)
SPI	Sistema de prevención de intrusiones
SQL	Lenguaje de consulta estructurado (*structured query language*)
VM	Máquina virtual (*virtual machine*)
VPN	Red privada virtual (*Virtual Private Network*)
WAF	Cortafuegos de aplicación web (*Web Application Firewall*)

5 Convenios

La expresión "**se requiere**" o "**se deberá**" indica un requisito que debe cumplirse estrictamente, sin permitir desviación alguna si se va a invocar la conformidad con la presente Recomendación.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. El cumplimiento de ese requisito no es necesario para declarar la conformidad.

En el cuerpo de la presente Recomendación y en sus apéndices pueden aparecer veces verbos que expresan obligación, prohibición, recomendación y posibilidad, en cuyo caso deben interpretarse en dicho sentido. Cuando estas expresiones o términos aparecen en apéndices o en partes incluidas explícitamente a título informativo no deben interpretarse en su sentido normativo.

6 Introducción al conocimiento de la situación de seguridad de las redes

Hoy en día los ataques a las redes se preparan con un objetivo preciso, los atacantes los planifican hasta el último detalle y es habitual que su penetración sea a largo plazo. En respuesta, las defensas de seguridad suelen contar con un componente de "confrontación temporal". En la arquitectura de seguridad tradicional varios componentes o productos de seguridad se despliegan únicamente con sus propias normas de protección, políticas de alerta, procesamiento de registros y mecanismos de almacenamiento, pero no hay un mecanismo de coordinación entre esos componentes y productos, por lo que se crea un efecto de aislamiento que debilita la capacidad de defensa contra los ataques más avanzados, discretos y profesionales.

El conocimiento de la situación de seguridad de las redes (NSSA, *network security situational awareness*) es un derivado del "conocimiento de la situación" y se aplica específicamente a la seguridad de las redes. Suele conllevar cuatro procesos: adquisición de datos, percepción de la situación de seguridad, evaluación de la situación de seguridad y predicción de la situación de seguridad, y normalmente incorpora las siguientes capacidades:

- detección y supervisión constante de diferentes amenazas de ataque, incluidos los comportamientos anómalos y su ámbito de influencia;
- extracción de datos, simulación, análisis de amenazas y trazabilidad de comportamientos anómalos;
- predicción de seguridad y alerta temprana;
- visualización de la situación de seguridad.

En el contexto de seguridad de la red, por asimetría de la información se entiende el caso en que un atacante conoce los sistemas, redes o procesos de una organización mejor que la organización misma. En esos casos los atacantes están en posición de ventaja a la hora de elaborar estrategias y llevar a cabo los ataques. El conocimiento de la situación de seguridad de la red es muy importante para eliminar la asimetría de la información entre ataque y defensa, así como para intervenir más rápidamente en caso de incidente y aplicar la trazabilidad.

Al mismo tiempo, el desarrollo del análisis de macrodatos, la computación en la nube y la inteligencia artificial (IA) ha traído consigo la oportunidad y el impulso necesarios para el desarrollo del NSSA. Por ejemplo, el NSSA puede soportar efectivamente el almacenamiento masivo de registros de seguridad, utilizando y recurriendo al análisis de macrodatos, para poder supervisar constantemente situaciones de seguridad de red a gran escala. El desarrollo de la IA puede ofrecer más métodos de análisis y capacidades de predicción de riesgos para el NSSA, lo que puede efectivamente mejorar la precisión de las predicciones; y el desarrollo de la computación en la nube puede ofrecer una arquitectura infraestructural más flexible y estable para el NSSA.

En la Figura 6-1 se muestra el marco típico de una plataforma de NSSA.

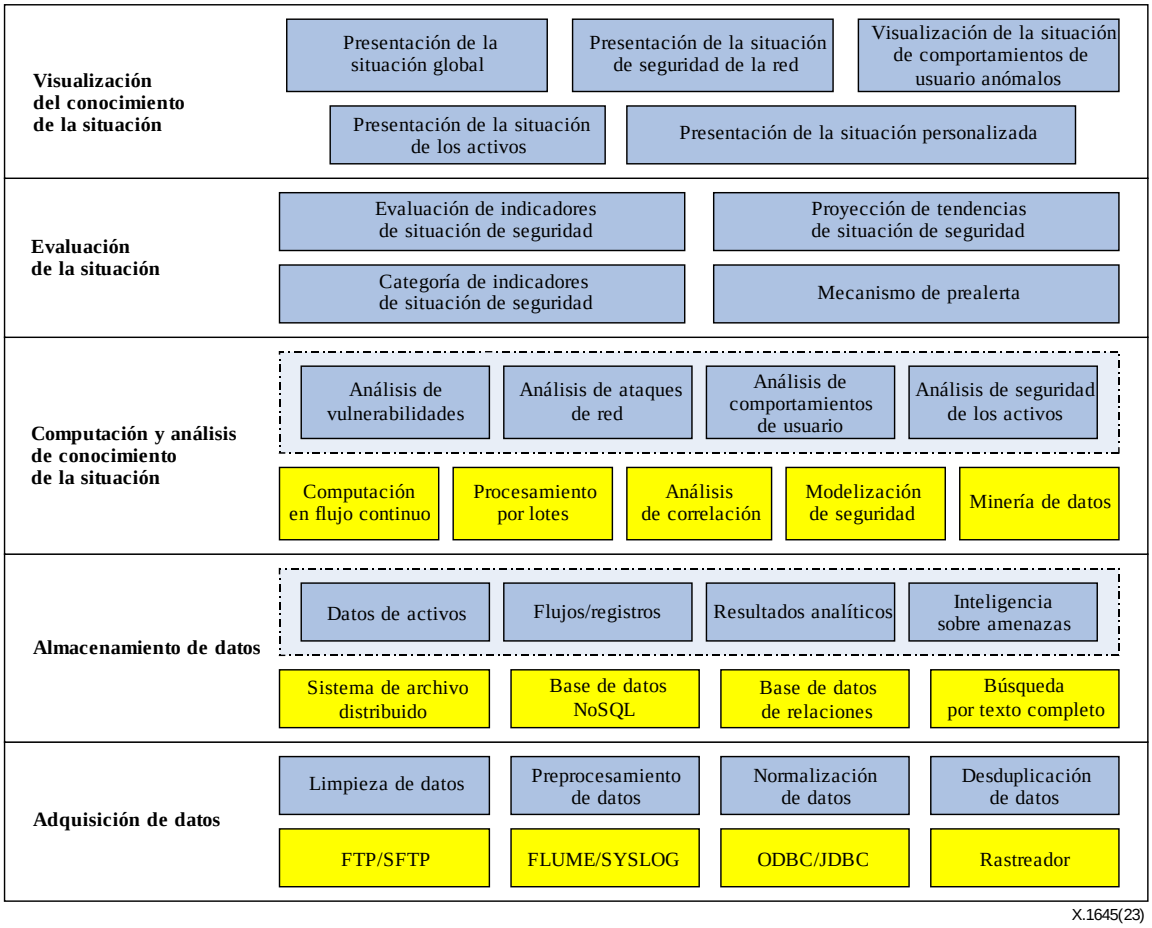

Figura 6-1 – Marco de la plataforma de conocimiento de la situación de seguridad de las redes

7 Análisis

Gracias al rápido desarrollo de la tecnología y a la madurez de su ecosistema, la computación en la nube representa una nueva generación de infraestructura esencial de la información. La computación en la nube ha traído consigo innumerables beneficios haciendo frente al mismo tiempo a muchos más problemas de seguridad, sobre todo en lo que se refiere a la operación y el mantenimiento, como los siguientes:

1) Al incrementarse rápidamente la escala, los distintos tipos de componentes de seguridad desplegados en la infraestructura de computación en la nube generan una cantidad masiva de datos de seguridad y repetidas alertas que el contexto hace difícil para los ingenieros de operación y mantenimiento tratar dentro de un periodo limitado de tiempo.

2) La mayoría de los componentes de seguridad están aislados unos de otros, creando así el evidente efecto de aislamiento. Resulta difícil aplicar un mecanismo de defensa bien coordinado en el entorno de computación en la nube.

3) El entorno de computación en la nube es normalmente complejo, pues puede incluir nubes públicas, nubes privadas y nubes híbridas. Por ese motivo es difícil tomar decisiones de seguridad razonables, ya que los proveedores de servicios de computación en la nube, e incluso los usuarios, carecen de una perspectiva global y macroscópica.

El NSSA puede solucionar esos problemas. Sobre la base de la tecnología de macrodatos, el NSSA puede efectivamente soportar el almacenamiento, la utilización y la extracción de datos de registros de seguridad masivos y heterogéneos. Además, gracias al análisis de correlación de múltiples datos distintos, se pueden organizar efectivamente distintos componentes de seguridad, mejorar la capacidad de detección de amenazas e incrementar la eficacia de los ingenieros de seguridad.

El NSSA permite asimismo visualizar el conocimiento de la situación de seguridad de la computación en la nube en su conjunto. Al mismo tiempo, conviene utilizar en el NSSA la tecnología de inteligencia artificial (IA) para mejorar las capacidades de detección, diagnóstico y predicción del conocimiento de la situación de seguridad de la computación en la nube.

Por consiguiente, el NSSA desempeña un papel importante en la mejora de la protección de la seguridad, la toma de decisiones de seguridad y la capacidad de respuesta en caso de emergencia de la computación en la nube, pudiendo incluso mejorar el mecanismo de alerta temprana de los proveedores de servicios de computación en la nube.

Por otra parte, para desplegar la plataforma NSSA en la computación en la nube es necesario contar con las siguientes capacidades concretas:

1) La adquisición de datos debe adaptarse a la modificación dinámica de los activos de computación en la nube, pues éstos pueden crearse y suprimirse con más flexibilidad y frecuencia que en la arquitectura de TI tradicional.
2) La plataforma NSSA debe adaptarse a las características del servicio de computación en la nube, como la utilización de recursos compartidos entre múltiples titulares y la gestión elástica de recursos, que pueden generar rápidos cambios en las fuentes de datos. La rápida modificación de los titulares y sus servicios redundará en consecuencia en una modificación de la adquisición de datos en la plataforma NSSA.
3) La plataforma NSSA debe seguir interactuando y cooperando con la plataforma de gestión de computación en la nube para acceder a los distintos datos, como el estado de ejecución y los registros de seguridad de los recursos de computación en la nube para lograr un conocimiento profundo de los recursos de computación en la nube. Por ejemplo, el NSSA no puede obviar la plataforma de gestión de la nube para observar las conexiones de red entre máquinas virtuales (VM, *virtual machine*) de la misma zona de red de capa 2 OSI.
4) La plataforma NSSA debe soportar la capacidad de acceder a los datos desde múltiples nubes para lograr una perspectiva unificada de los activos para los usuarios de nubes híbridas o nubes públicas.

La aplicación y despliegue del NSSA de las redes puede ofrecer soluciones a los retos técnicos expuestos. El NSSA puede detectar diversos eventos de seguridad y comportamientos anómalos de manera integral, precisa y depurada tanto en el tiempo como en el espacio, analizar diversos elementos de seguridad, comprender la situación de seguridad en su conjunto y predecir sus tendencias, lo que ayudará a la capacidad operativa de seguridad del proveedor de computación en la nube, ayudará a tomar decisiones sobre seguridad y a intervenir en caso de incidente y mejorará el mecanismo de alerta temprana de seguridad.

8 Requisitos de la plataforma de conocimiento de la situación de seguridad de las redes para la computación en la nube

8.1 Requisitos de adquisición de datos

8.1.1 Mecanismo de adquisición de datos

Los nodos de adquisición de la plataforma NSSA deben poder recabar activa o pasivamente distintos tipos de datos, por ejemplo, registros del tráfico de red, registros de sistema, registros de *software* intermedio (*middleware*) y registros de seguridad de la infraestructura de computación en la nube. Cuando se opta por el método activo, los datos se recaban supervisando o controlando periódicamente los objetivos, mientras que con el método pasivo los datos se obtienen principalmente al recibirlos o importarlos de distintas fuentes.

1) La adquisición de datos deberá soportar el método activo, que consiste, entre otras cosas, en obtener datos por barrido, rastreo o protocolo de gestión de red simple (SNMP, *simple network management protocol*).

2) La adquisición de datos deberá soportar el método pasivo, que consiste, entre otras cosas, en la recepción de datos por el protocolo syslog, el canal NetFlow, etc., y la importación manual de datos.

La capacidad de adquisición de datos debe adaptarse al entorno de computación en la nube como sigue:

1) Se recomienda que la adquisición de datos soporte la obtención de datos de distintas nubes, como multinubes, nubes híbridas, etc.

2) Se recomienda que la adquisición de datos se adapte a la modificación dinámica de los recursos del entorno de computación en la nube.

3) Se recomienda que la adquisición de datos soporte la obtención de registros de datos del tráfico de red este-oeste de las plataformas de computación en la nube.

Asimismo, los nodos de adquisición de la plataforma NSSA debe contar con las siguientes capacidades:

1) Los nodos de adquisición deberán filtrar los datos y examinar su validez, como el tipo de datos y la gama de valores, y filtrar los datos inválidos conforme a políticas predefinidas.

2) Se recomienda que los nodos de adquisición implementen un mecanismo de recaptura de datos en caso de fallo en la obtención.

8.1.2 Fuentes de datos

La plataforma NSSA debe soportar la aplicación de las operaciones crear, leer, actualizar y suprimir (CRUD, *create, read, update, and delete*) a sus datos y soportar la obtención de los siguientes tipos de datos:

1) Se requiere soportar la obtención de datos de activos de las plataformas de computación en la nube, como los relativos a los grupos de recursos virtuales, los equipos de red, los anfitriones, los equipos de seguridad, los sistemas, el *software*, las plataformas de gestión de computación en la nube, etc.

2) Se requiere soportar la obtención de diversos tipos de datos de registro, como los registros de acceso a la web, los registros de seguridad, los registros de operaciones comerciales, los registros de conexión, etc. de múltiples fuentes, como los anfitriones, el *middleware*, las plataformas de gestión de computación en la nube, etc., y soportar la recepción de los análisis de registros de otros sistemas.

3) Se requiere soportar la obtención de diversos datos de vulnerabilidades procedentes de múltiples equipos y componentes de las plataformas de computación en la nube, como las vulnerabilidades de desbordamiento de la memoria intermedia, las vulnerabilidades de inyección, las vulnerabilidades de lógica comercial, las vulnerabilidades de diseño y las vulnerabilidades de configuración, entre otras.

4) Se requiere soportar la obtención de daos de múltiples ataques a la red, como los ataques por denegación de servicio distribuida (DDoS, *distributed denial of service*), la explotación de vulnerabilidades, el acceso no autorizado, etc.

5) Se requiere soportar la obtención de datos de inteligencia sobre amenazas, como la inteligencia sobre amenazas de IP/dominio/URL, las muestras malignas, las listas negras de instrucciones y control (C&C, *command and control*), las vulnerabilidades, etc.

8.1.3 Preprocesamiento de datos

A fin de satisfacer los requisitos de calidad de datos, es necesario que la plataforma NSSA proceda a la limpieza, filtrado, normalización, correlación, compleción, fusión y desduplicación de los datos obtenidos y, posteriormente, almacene los datos normalizados.

1) Limpieza de datos: la plataforma NSSA debe soportar la limpieza de datos en caso de que los datos obtenidos adolezcan de errores, lagunas, elementos inválidos u otros problemas. Además:
   - se requiere soportar la conversión, procesamiento y filtrado de formatos de datos incoherentes, errores en la entrada de datos y datos incompletos;
   - se recomienda soportar el filtrado y limpieza de los datos en función de operaciones condicionales, correspondencias de expresión periódicas y cálculos de expresión;
   - se recomienda soportar la desduplicación de datos.
2) Normalización de datos: la plataforma NSSA debe soportar el formateado uniforme de diversos tipos de datos heterogéneos y la preservación de los datos originales obtenidos. Además:
   - se requiere soportar campos de datos normalizados sobre la base de normas de campos para cada tipo de datos;
   - se recomienda soportar el formateado uniforme del contenido bruto por expresión periódica;
   - se recomienda soportar la preservación de los datos obtenidos originales a fin de soportar el posterior análisis de trazabilidad y el desarrollo personalizado.
3) Correlación y compleción de datos: se recomienda que la plataforma NSSA soporte la correlación y compleción de datos normalizados, entre los que se cuentan la información de usuario, la información de activos, la información de ubicación geográfica, la información de inteligencia sobre amenazas, etc., y se recomienda soportar la selección de datos y campos concretos por completar.
4) Fusión de datos: se recomienda que la plataforma NSSA soporte la fusión de datos normalizados sobre la base de normas configuradas, y se recomienda soportar la selección de datos y campos concretos por fusionar.

8.1.4 Requisitos de seguridad de la adquisición de datos

1) Se requiere que la plataforma NSSA soporte el control de acceso de los nodos de adquisición y la supervisión del proceso de obtención de datos, así como la emisión de alertas puntuales en caso de eventos anómalos.
2) Se requiere restringir estrictamente el acceso al almacén temporal de datos durante el proceso de obtención, que no puede modificarse arbitrariamente.
3) Se requiere que la plataforma NSSA soporte la clasificación jerárquica y la identificación de los datos obtenidos y la aplicación de protecciones de seguridad, como la encriptación de datos sensibles, por ejemplo, datos de activos, datos operativos, datos de registro, etc.
4) Se requiere que la plataforma NSSA soporte la ocultación y desensibilización de los datos sensibles antes de su preprocesamiento y análisis, y satisfaga los requisitos de seguridad de los datos obtenidos.
5) Se requiere que la plataforma NSSA mantenga un registro operativo y de obtención para poder generar alarmas puntuales de auditoría y en caso de evento anómalo. Además:
   - Se requiere auditar las operaciones de usuarios y administradores para detectar comportamientos malignos, como la utilización indebida de los datos, etc., emitir las alertas correspondientes y responder en consecuencia.

- Se recomienda alertar de interrupciones en la transmisión durante la obtención de datos.
- Se recomienda emitir alertas en caso de que el almacén de datos rebase un umbral predeterminado durante la obtención y transmisión de los datos.

8.2 Requisitos de almacenamiento de datos

El almacenamiento de datos de la plataforma NSSA debe aplicar técnicas de macrodatos para ajustarse a las demandas de almacenamiento de datos multidimensionales, procedentes de múltiples fuentes y en constante crecimiento generados por el entorno de computación en la nube, como los resultados de análisis, la inteligencia sobre amenaza externa, etc. La plataforma NSSA debe soportar mecanismos de almacenamiento conforme a distintos dominios y clasificaciones de los diversos tipos de datos y satisfacer los requisitos de los distintos análisis de datos y métodos de aislamiento. Al mismo tiempo, la plataforma NSSA debe garantizar la disponibilidad, integridad y confidencialidad de los datos almacenados.

8.2.1 Categorización del almacenamiento de datos

Se recomienda que la plataforma NSSA soporte el almacenamiento de datos no estructurados, datos estructurados y datos semiestructurados, en función de diversas fuentes de datos, y soporte la categorización múltiple del almacenamiento de datos, incluido el almacenamiento de datos relacional, las bases de datos NoSQL (no sólo lenguaje de consulta estructurado), el almacenamiento de archivos distribuido y las búsquedas por texto completo distribuidas.

Se recomiendan las categorizaciones del almacenamiento de datos de la plataforma NSSA que se indican en el Cuadro 8-1.

Cuadro 8-1 – Categorización de datos

Fuente de datos	Contenido de datos	Volumen de datos	Categorización de almacenamiento (recomendada)
Anfitrión de la nube/contenedor/SO	Registros operativos, registros de seguridad, datos del estado de la ejecución, archivos de configuración, etc.	Grande	Almacenamiento de archivos distribuido/búsqueda por texto completo distribuida/base de datos NoSQL
Plataforma de gestión de la nube	Registros de acceso, registros operativos, archivos de configuración, datos de flujo de trabajo, etc.	Medio	Almacenamiento de archivos distribuido/búsqueda por texto completo distribuida/base de datos NoSQL
Equipo de red	Registros de encaminadores, conmutadores y plataforma de red, cuadro de encaminamiento, archivos de configuración, etc.	Grande	Almacenamiento de archivos distribuido/búsqueda por texto completo distribuida/base de datos NoSQL
Equipo de seguridad	Registros de cortafuegos, sistema de detección de instrusiones (SDI), sistema de prevención de instrusiones (SPI), red privada virtual (VPN), cortafuegos de aplicación web (WAF), archivos de configuración, etc.	Grande	Almacenamiento de archivos distribuido/búsqueda por texto completo distribuida/base de datos NoSQL

Cuadro 8-1 – Categorización de datos

Fuente de datos	Contenido de datos	Volumen de datos	Categorización de almacenamiento (recomendada)
Sistema de aplicación	Registros de bases de datos, *middleware*, sistemas de aplicación, archivos de configuración, etc.	Grande	Almacenamiento de archivos distribuido/búsqueda por texto completo distribuida/base de datos NoSQL
Datos básicos	Datos de activos, datos de cuentas, diccionario IP, datos de servicio, etc.	Medio	Base de datos racional/búsqueda por texto completo distribuida/base de datos NoSQL
Tráfico de red	Datos DPI, datos de flujo de red, etc.	Masivo	Almacenamiento de archivos distribuido
Inteligencia sobre amenazas	Inteligencia estratégica, inteligencia táctica, información de seguridad, etc.	Medio	Almacenamiento de archivos distribuido/búsqueda por texto completo distribuida/base de datos NoSQL
Resultados de análisis	Eventos de seguridad, datos de cumplimiento, índice de seguridad, etc.	Medio	Base de datos racional/extracción por texto completo distribuida/base de datos NoSQL

8.2.2 Requisitos técnicos de almacenamiento de datos

La plataforma NSSA debe desarrollar una arquitectura de almacenamiento de datos elástica y adaptable para ajustarse al crecimiento continuo del volumen de datos y a los requisitos de clasificación y almacenamiento jerárquico de los datos. Además, la duración del ciclo de almacenamiento de los datos variará en función de la reglamentación, los requisitos comerciales y el coste económico.

1) Se recomienda que la plataforma NSSA soporte las bases de datos racionales habituales. Se recomienda que la base de datos racional soporte una interfaz de acceso al modelo relacional completa, incluidas las interfaces SQL normalizadas y las interfaces de desarrollo de aplicaciones normalizadas (JDBC, ODBC, etc.).

2) Se recomienda que la plataforma NSSA soporte las bases de datos NoSQL habituales.

3) Se recomienda que la plataforma NSSA soporte los componentes de macrodatos típicos, como Hive, HBase, MPP, etc., para soportar funcionalidades ampliadas.

4) Se recomienda que la plataforma NSSA adopte componentes de búsqueda por texto completo, que deben soportar la extracción de palabras clave, la búsqueda por múltiples palabras clave, la combinación de búsquedas por texto completo y otros campos, así como soportar la correspondencia de prefijos, las correspondencias imperfectas y otras condiciones de extracción.

5) Se recomienda que la plataforma NSSA adopte componentes de bus de mensaje distribuido, como Kafka, Rabbit MQ y demás. Los componentes de bus de mensaje distribuido deben soportar funciones como la compresión de datos, la configuración del tiempo de retención de datos y la supresión automática de datos expirados, entre otras.

6) Se recomienda que la plataforma NSSA soporte el almacenamiento en línea y mecanismos de copia de seguridad para garantizar la disponibilidad de los datos.

7) Se recomienda que la plataforma NSSA soporte el almacenamiento de metadatos, entre otros:

   - metadatos técnicos, que se utilizan para el mantenimiento de los datos, por ejemplo, cómo se almacenan los datos para poder acceder a ellos eficazmente, etc.;

- metadatos de gestión, como la política de control de acceso a datos, los resultados del procesamiento de datos, etc.

8.2.3 Requisitos de seguridad del almacenamiento de datos

1) Se requiere que la plataforma NSSA desarrolle mecanismos de control de acceso a los datos, como el control de acceso a los datos por funciones, etc., para evitar accesos no autorizados.

2) Se requiere que la plataforma NSSA soporte la encriptación del almacenamiento de datos importantes o sensibles. Se recomienda aclarar los requisitos de encriptación del almacenamiento de los distintos tipos de datos sobre la base de la clasificación y definición jerárquica de los datos, como los requisitos de algoritmos de encriptación de datos y la gestión de claves de encriptación.

3) Se requiere que la plataforma NSSA aplique técnicas adecuadas y medidas de control para garantizar la efectiva integridad del almacenamiento de datos y la coherencia de las múltiples copias de datos.

4) Se requiere que la plataforma NSSA aplique técnicas adecuadas y medidas de control para garantizar la disponibilidad del almacenamiento de datos. Sobre la base de los principios de clasificación de datos, se recomienda aclarar las políticas de copia de seguridad y recuperación de los distintos datos, como los modos de copia de seguridad, los requisitos de duración del almacenamiento y el tiempo de recuperación, etc.

5) Se recomienda que la plataforma NSSA pruebe periódicamente los mecanismos de almacenamiento de datos para verificar las capacidades de identificación de fallos en los datos y de reconstrucción de copias de seguridad.

6) Se requiere que la plataforma NSSA genere todos los registros de procesamiento de almacenamiento de datos para garantizar la trazabilidad de los procesos de almacenamiento de datos y ofrezca capacidades de alerta en caso de comportamiento anómalo.

8.3 Requisitos de computación y análisis de la situación

La capacidad de computación y análisis de la situación de la plataforma NSSA comprende esencialmente el motor de computación y análisis y los módulos funcionales de análisis de la situación.

1) El motor de computación y análisis facilita capacidades de modelización de amenazas y computación de análisis a los módulos funcionales de análisis de la situación. El motor de computación y análisis comprende marcos de modelización de la seguridad y de computación de datos, como el motor de computación fuera de línea y la computación en tiempo real.

2) Los módulos funcionales de análisis de la situación se ocupan principalmente de analizar la situación de seguridad de las redes en el entorno de computación en la nube a partir de la minería de datos y el análisis de simulacros y amenazas en diversos datos de activos combinados, como eventos de seguridad, datos de registro, datos de tráfico de red, etc.

3) Para mejorar la eficacia del cálculo y el análisis, se requiere construir una representación unificada de diversos eventos de seguridad e información de activos antes de modelizar la seguridad, lo que puede lograrse mediante vectorización del contexto. Gracias a la vectorización, el contexto puede trasladarse a un espacio euclidiano, lo que suele ser indispensable para la aplicación de diversos algoritmos de IA para el cálculo de semejanza y el cálculo de correlación.

8.3.1 Requisitos del motor de computación y análisis

8.3.1.1 Modelización de seguridad

La modelización de seguridad debe comprender la modelización de correlación, la modelización estadística, la modelización de correlación de inteligencia sobre amenazas y la modelización de IA, ofreciendo así capacidades de minería y análisis detallado de los datos de situación básicos.

1) **Modelización de correlación**: se utiliza un método de correspondencia basado en reglas para realizar la asociación lógica y el análisis de correspondencia de características de eventos homogéneos y heterogéneos.
   - Se requiere soportar el análisis de correlación lógica basado en la causalidad de los incidentes de seguridad.
   - Se requiere soportar la correlación en múltiples aspectos, como el tiempo, el espacio, etc., de datos heterogéneos de fuentes diversas.
   - Se recomienda soportar la agrupación de informaciones de alerta en función de situaciones de seguridad de la red dinámicas a fin de reducir el número de alertas y mejorar la eficacia de la respuesta.
2) **Modelización estadística**: se utilizan métodos estadísticos para calcular las características cuantitativas de diversos eventos, como la frecuencia, el periodo de ocurrencia, etc., y obtener la distribución de los datos de eventos, sus principales características, tendencias de recurrencia temporal, presencia de valores anómalos, resultados resumidos de los eventos, etc.
   - Se recomienda soportar el análisis estadístico de eventos de seguridad, comportamientos de seguridad, amenazas de seguridad y otras características, y descubrir características estadísticas importantes de las amenazas de seguridad a partir de diversas fuentes de datos.
3) **Asociación de inteligencia sobre amenazas**: se recomienda soportar la integración de capacidades de inteligencia sobre amenazas para descubrir eventos de inteligencia precisos a partir de la inteligencia sobre amenazas en el entorno de computación en la nube.
4) **Modelización de IA**: se recomienda soportar diversos algoritmos de inteligencia artificial integrados, incluidos algoritmos de temporización, algoritmos de clasificación, algoritmos de agrupación y otros prototipos de algoritmos, que ofrecen a los usuarios capacidades de aprendizaje y análisis de datos arbitrarios, y analizar amenazas de seguridad avanzadas y amenazas desconocidas.
   - Se recomienda soportar los algoritmos comunes, como el análisis grupal, el análisis por asociación, el análisis de árbol de decisiones, el análisis de regresión y otros algoritmos de análisis de IA/aprendizaje automático.
   - Se recomienda que la plataforma NSSA soporte la gestión centralizada de la modelización y política de seguridad, etc. para facilitar la ejecución efectiva y un rápido despliegue.

8.3.1.2 Marco de computación de macrodatos

Es necesario soportar marcos de computación fuera de línea y en tiempo real para el procesamiento por lotes de datos estadísticos y el análisis en tiempo real de datos dinámicos (datos de difusión continua).

1) **Marco de computación fuera de línea**: se requiere soportar el despliegue de algoritmos fuera de línea, modelos de formación e hipótesis de aprendizaje automático. Los analistas pueden utilizar el motor de análisis fuera de línea para extraer datos en profundidad y conocer inmediatamente los resultados arrojados por el algoritmo, ofreciendo así capacidades de formación del modelo.

2) **Marco de computación de difusión continua en tiempo real**: se recomienda que el marco de computación en tiempo real soporte una arquitectura distribuida y que se pueda ajustar dinámicamente la capacidad de almacenamiento. Una alta disponibilidad y la separación de las políticas de lectura y escritura permiten garantizar la lectura y escritura independientes de los datos en el análisis de datos fuera de línea.

8.3.2 Requisitos de los módulos funcionales de análisis de la situación

Sobre la base del motor de computación y análisis, los módulos funcionales de análisis de la situación establecen capacidades de análisis de datos de activos, eventos de seguridad, datos de registro, datos de tráfico y otros datos en función de la situación, y definir hipótesis de análisis de seguridad a partir de múltiples datos a fin de ofrecer capacidades de alerta de seguridad y alerta temprana adaptadas a cada caso. Los módulos funcionales de análisis de la situación se encargan del análisis de seguridad de la red, el análisis de seguridad de los activos y el análisis del comportamiento de usuarios de alto riesgo en el entorno de computación en la nube.

8.3.2.1 Análisis de seguridad de la red

El módulo de análisis de seguridad de la red deberá tener la capacidad de analizar los diversos ataques a la red, como el tráfico de red anómalo, la propagación de programas malignos y el acceso maligno a nombres de dominio, entre otros, en el entorno de computación en la nube, además de la capacidad de rastrear sus tendencias de variación.

1) Se recomienda soportar la detección y el análisis estadístico de la situación general de ataques comunes y analizar las tendencias de variación del ataque en curso.
   - Se recomienda soportar las funciones de detección y análisis de ataques a la red a partir de datos de múltiples fuentes, entre las que se cuentan las intrusiones de red, los ataques a la web, el *malware*, los ataques DDoS, el reconocimiento de red, actividades sospechosas y otros tipos de ataques a la red.
   - Se recomienda soportar el análisis estadístico de diversos tipos de ataques de red y el análisis de la variación tendencial de diversos tipos de ataques.
2) Se recomienda soportar la detección y análisis estadístico de la situación global de tráfico de red anómalo en el entorno de computación en la nube y analizar la variación tendencial del tráfico de red anómalo presente.
   - Se recomienda soportar la identificación anómala de tráfico de red y poder detectar y analizar el tráfico anómalo de protocolos sobre la base de puertos de virus comunes.
   - Se recomienda soportar el análisis estadístico del tráfico de red anómalo, la fusión de estadísticas de tráfico anómalo de protocolos y el análisis de las tendencias del tráfico anómalo.
3) Se recomienda soportar el análisis de la situación global de la difusión de programas malignos, como virus, gusanos y troyanos en el entorno de computación en la nube, así como el análisis de las tendencias actuales de difusión de programas malignos.
4) Se recomienda soportar la detección y el análisis estadístico de anfitriones de redes robot (botnet) C&C, anfitriones zombis, y soportar el análisis de la difusión y la variación tendencial de las botnets.
5) Se recomienda soportar el análisis de las estadísticas de acceso y la propagación de nombres de dominio malignos, las direcciones IP de instrucciones y control y los nombres de dominio de algoritmo de generación de dominio (DGA, *domain generation algorithm*).
6) Se recomienda soportar el modelo de cadena de ataque para rastrear la fuente de los ataques mediante la clasificación de los eventos de seguridad generados en función del proceso de ataque, que comprende la obtención de información, la intrusión de red, las instrucciones y el control, la penetración horizontal, el logro de objetivos y la supresión de pruebas.

7) Se recomienda soportar el análisis de información del atacante a partir de la inteligencia sobre amenazas.

8.3.2.2 Análisis de seguridad de los activos

Se requiere soportar el análisis de la situación de seguridad de los diversos activos de la plataforma de computación en la nube. Se recomienda analizar la situación de seguridad de la infraestructura de computación en la nube, las máquinas virtuales, los contenedores y sistemas comerciales gracias a los registros de equipos de seguridad, los registros de sistema, los resultados de barrido de vulnerabilidades y demás datos. Este análisis puede ser de dos tipos: análisis de ataques al sistema y análisis de vulnerabilidades del sistema.

8.3.2.3 Análisis de la información sobre los activos

1) Se requiere soportar el análisis estadístico, incluido el basado en la clasificación, categorización y priorización, etc. de los activos, y la actualización del estado de los activos tras su adición o eliminación.
2) Se requiere soportar el análisis de la distribución de los activos, incluido el basado en la información geográfica, la pertenencia a un departamento, las aplicaciones web importantes, etc.
3) Se requiere soportar la búsqueda y visualización de información sobre los activos en función de las direcciones IP de los activos, las categorizaciones, las prioridades, la información geográfica, etc.

8.3.2.4 Análisis de amenazas a los activos

1) Se requiere soportar el análisis de amenazas de ataque al sistema, incluidas la detección de destrucción de registros, la detección de aumento de privilegios del sistema, la detección de registros erróneos, los ataques por fuerza bruta, etc. El análisis puede realizarse sobre la base del análisis de correlación de los datos de activos, los registros de dispositivos, los registros de sistema de los anfitriones, los datos de sistema de seguridad, la inteligencia sobre amenazas, etc.
2) Se requiere soportar el análisis estadístico y el análisis tendencial de las amenazas a los activos.

8.3.2.5 Análisis de vulnerabilidades de los activos

1) Se requiere soportar el análisis de correlación de los resultados del barrido de vulnerabilidades de los activos y los registros de detección de dispositivos de seguridad a fin de realizar un análisis de utilización de vulnerabilidades, incluidos el análisis de vulnerabilidades de anfitriones/VM/contenedores, el análisis de vulnerabilidades de las aplicaciones y el análisis estadístico del riesgo de explotación de vulnerabilidades en función del tiempo, el sistema comercial, el nivel de vulnerabilidad y otras dimensiones.

8.3.2.6 Análisis del cumplimiento de las configuraciones de activos

1) Se requiere soportar el análisis de los resultados de cumplimiento de la configuración de los sistemas operativos, el *software* de virtualización, las bases de datos, los equipos de red, el, *middleware*, etc. en el entorno de computación en la nube.
2) Se requiere soportar el análisis estadístico de elementos no conformes descubiertos y soportar el análisis de riesgos de los atacantes que utilizan elementos no conformes para atacar los activos.

8.3.2.7 Análisis de comportamiento de los usuarios

Se recomienda soportar la detección y el análisis de comportamientos anómalos de los usuarios internos que acceden a la plataforma de computación en la nube y de los comportamientos anómalos

de los activos y sistemas comerciales, así como el análisis de los perfiles de comportamiento de los usuarios.

1) Se recomienda soportar el análisis de comportamientos operativos de los usuarios anómalos, incluido el funcionamiento anómalo de datos sensibles, la conexión con cuentas expiradas, la divulgación ilegal, la ejecución de instrucciones sensibles, los ataques por fuerza bruta, la conexión a direcciones anormales, etc.

2) Se recomienda soportar la definición de perfiles sobre la base del comportamiento de los usuarios internos, incluidas las características comportamentales individuales y grupales de los usuarios.

3) Se recomienda soportar la personalización de las reglas de comportamiento anómalo y los modelos de comportamiento.

4) Se recomienda soportar el análisis de comportamiento anómalo sobre la base de los perfiles de usuario, y su comparación de comportamientos individuales o grupales puntuales con datos de comportamiento históricos a fin de detectar las anomalías.

5) Se recomienda soportar el análisis de comportamiento anómalo de diversos recursos de computación en la nube, que puede identificar los comportamientos anómalos que pueden darse en el entorno de computación en la nube, como el comportamiento anómalo de los anfitriones de la nube, las herramientas anómalas del sistema de llamadas, los comportamientos de red anómalos, las comunicaciones salientes ilícitas, etc.

8.4 Requisitos de la evaluación de la situación

Se recomienda que la evaluación de la situación de la plataforma NSSA soporte la evaluación de la situación dinámica de la situación de seguridad global del entorno de computación en la nube, prediciendo además las tendencias de la situación, sobre la base del análisis multidimensional de datos de seguridad, los resultados de los análisis de seguridad de la plataforma de computación en la nube y la modelización de la evaluación de la categoría del índice de situaciones. Todo ello soporta la emisión de alertas tempranas y la interactuación con los mecanismos de adopción de decisiones de seguridad y de respuesta en caso de emergencia del proveedor de servicios en la nube (CSP, *cloud service provider*)/cliente de servicios en la nube (CSC, *cloud service customer*).

8.4.1 Evaluación de la situación

El alcance de la evaluación de la situación de seguridad comprende la situación de la plataforma de la nube, la situación de seguridad de los activos de la nube, las amenazas, las vulnerabilidades, los ataques a la red, la disponibilidad de la plataforma de la nube y sus componentes, etc.

1) Se requiere obtener la información sobre los activos como fuente de datos para crear un índice de evaluación de la situación de seguridad. La información sobre los activos debe incluir la versión concreta de los sistemas operativos, el *middleware*, las aplicaciones y las bases de datos, la ubicación de la topología de red, el valor de los activos, etc., a fin de generar indicadores de evaluación razonables.

2) Se requiere soportar un índice de evaluación de la situación de seguridad de la plataforma de computación en la nube creando métricas generales en una escala unificada a fin de medir la situación de seguridad y cuantificar los diversos elementos de la situación de seguridad de las redes.

    - Se recomienda crear indicadores cualitativos y cuantitativos para evaluar la situación de las redes. Los indicadores cualitativos son evaluaciones subjetivas basadas en analizadores de seguridad profesionales. Por ejemplo, los analizadores de seguridad pueden asignar niveles de gravedad a determinadas vulnerabilidades o ataques a la red en función de su propia experiencia. Los indicadores cuantitativos proceden de la obtención y el análisis de datos brutos.

- Se recomienda soportar el cálculo de semejanza y el cálculo de correlación a la hora de considerar los indicadores de amenazas. Además:
  - Se recomienda utilizar el cálculo de semejanza del contexto de amenazas para reconocer las amenazas más habituales, como la intrusión, el acceso por fuerza bruta, los ataques DDoS, etc., a fin de evitar un cambio drástico de un indicador concreto a causa de un gran número de alarmas repetitivas.
  - Se recomienda utilizar el análisis de correlación entre amenazas e informaciones sobre los activos para reconocer amenazas de ataques ciegos y masivos y que el personal de seguridad pueda determinar rápidamente los indicadores de alto riesgo que realmente necesitan de su intervención.
  - Se recomienda adoptar un marco algorítmico unificado para efectuar el análisis de correlación y el análisis de semejanza, como el coseno angular, etc. Como es obvio, un marco algorítmico unificado puede reducir el coste de mantenimiento que supone la utilización de algoritmos.
- Se recomienda crear un indicador general y subdivisiones de indicadores para la evaluación de la situación de seguridad de la red. El indicador general refleja todas las características de la evaluación de la seguridad de la plataforma de computación en la nube; las subdivisiones pueden descomponerse en función de los distintos componentes o sistemas, reflejando así las diferencias en los resultados de la evaluación de la situación de los diversos componentes/sistemas.
- Se recomienda soportar la creación de categorías de indicadores de situación. Además:
  - se recomienda soportar la creación de indicadores operativos para la plataforma de computación en la nube, como utilización de grupos de recursos de la nube, retardo de acceso comercial, etc.;
  - se recomienda soportar la creación de indicadores de amenazas a la seguridad de la red, incluidos diversos incidentes de seguridad de la red, cuya frecuencia y gravedad pueden además calcularse y evaluarse;
  - se recomienda soportar la creación de indicadores para la evaluación de la seguridad de los activos de red, como las amenazas a los activos, las vulnerabilidades de los activos, la gravedad de las vulnerabilidades, las vulnerabilidades subsanadas, etc.;
  - se recomienda soportar la creación de indicadores para la seguridad del comportamiento de los usuarios, por ejemplo, si los usuarios efectúan accesos o conexiones anómalos, el comportamiento de descarga de *malware*, etc. Se requiere además adoptar técnicas de protección de la privacidad de los usuarios, como la desensibilización y la anonimización de los datos para proteger la privacidad de los usuarios.

3) Se recomienda soportar la construcción de un mecanismo global de evaluación de la situación de seguridad o la modelización basada en categorías de indicadores jerárquicos y multidimensionales.

- Se requiere soportar la normalización de las distintas subdivisiones de indicadores, tanto cualitativos como cuantitativos, a fin de evitar sesgos en los resultados de la evaluación por diferencias de unidad o magnitud. Se recomienda adoptar técnicas de conversión para convertir los indicadores cualitativos en valores numéricos para cálculos o análisis posteriores.
- Se recomienda soportar mecanismos de evaluación multidimensional de la situación, incluidas la evaluación de riesgos, la evaluación de amenazas o la modelización por series temporales, etc.
- Se recomienda soportar diversos modelos de evaluación, incluidos los basados en modelos teóricos matemáticos, modelos deductivos, etc.

- Se recomienda soportar un método de evaluación jerárquica ascendente, consistente en procesar los indicadores de situación de las capas inferiores y posteriormente calcular los resultados de evaluación de la situación de las capas superiores, calculando progresivamente la evaluación global de la situación de seguridad.
- En los métodos jerárquicos se recomienda soportar el cálculo de semejanzas para facilitar la interpretación de un valor de evaluación de la situación específico por comparación con los valores históricos y cercanos. A fin de obtener un valor de evaluación final puede construirse un vector multidimensional tomando sus resultados anteriores de un nivel específico, que puede utilizarse para calcular la semejanza con valores cercanos históricos mediante el coseno angular, la distancia del vector espacial u otros algoritmos. El cálculo de semejanza puede ayudar al personal de seguridad a detectar más fácilmente las anomalías y tener una mejor comprensión de la situación.

4) Se recomienda soportar capacidades de rastreo de las evaluaciones históricas de la situación de seguridad de la plataforma de la nube mediante el preprocesamiento de registros, la indización de campos clave, las búsquedas por texto completo, las búsquedas parciales, etc.

8.4.2 Proyección tendencial de la situación

A fin de conocer y hacer un seguimiento de la situación de seguridad del entorno de computación en la nube, extrayendo los elementos de seguridad e indicadores clave que puedan provocar cambios en la situación de la red, se recomienda que la plataforma NSSA soporte la predicción de tendencias globales de seguridad, tendencias de seguridad de los subcomponentes y de los riesgos de seguridad potenciales de acuerdo con los modelos de proyección de la situación de seguridad de la plataforma de la nube.

1) Se requiere soportar la construcción de categorías de indicadores jerárquicas y multidimensionales a partir de los datos obtenidos y de los resultados de los análisis, y la predicción de la tendencia de la situación conforme a los modelos de predicción pertinentes.

2) Se recomienda soportar los modelos de predicción habituales, incluidos los modelos de predicción por regresión de aprendizaje automático, los modelos de aprendizaje profundo y los modelos de predicción basados en ecuaciones diferenciales de campos profesionales, etc.

3) Se recomienda soportar el cálculo de los resultados de las predicciones mediante la fusión de diversos modelos predictivos para mejorar la exactitud de las predicciones, y concretamente:
   - supervisar la precisión de cada modelo calculando los valores de función de pérdida entre la predicción y los resultados factuales;
   - combinar los resultados de cada modelo mediante ponderaciones y ajustes de las ponderaciones de cada modelo. Por ejemplo, es posible adaptar las ponderaciones de cada modelo en función de los resultados de la supervisión de la función de pérdida. A fin de actualizar el modelo y mejorar la precisión también puede activarse la formación fuera de línea de los datos más recientes.

8.4.3 Mecanismos de prealerta

La plataforma NSSA debe ofrecer mecanismos de alerta temprana ante posibles riesgos de seguridad en el entorno de computación en la nube sobre la base de los resultados de los análisis de seguridad, la evaluación de la situación y las predicciones de la situación.

1) Se recomienda emitir alertas tempranas ante vulnerabilidades de los activos correlacionando las vulnerabilidades con los datos de inteligencia sobre amenazas, los eventos de seguridad relacionados, etc., y analizar las vulnerabilidades de los activos de la plataforma de la nube.

2) Se recomienda soportar alertas tempranas ante posibles ataques a la red a partir de las tendencias predictivas, incluidos barridos malignos, ataques a la red, ataques DDoS, ataques por tentativas de contraseña, ataques a vulnerabilidades del sistema, etc.

3) Se recomienda soportar alertas tempranas ante posibles comportamientos anómalos de los usuarios a partir de las tendencias predictivas, incluidas las operaciones de datos sensibles anómalas, la conexión a cuentas expiradas, la ejecución de instrucciones de alto riesgo, etc. Antes de emitir las alertas, es necesario utilizar técnicas de desensibilización y anonimización de los datos para proteger la privacidad de los usuarios.

4) Se recomienda soportar alertas tempranas ante amenazas de seguridad no detectadas mediante la asociación de comportamientos anormales detectados, la inteligencia sobre las amenazas y registros originales, etc.

5) Para los mecanismos de alerta temprana:

- se recomienda soportar la emisión de alertas tempranas sobre la base de políticas predefinidas y que puedan adaptarse en consecuencia;
- se recomienda soportar la gestión jerárquica de las alertas tempranas y categorizar los niveles de alerta en función de la importancia y la gravedad;
- se recomienda soportar la emisión de alertas mediante interfaces de programación de aplicaciones (API, *application programming interface*) a través de las cuales los sistemas terceros pueden recibir las alertas y responder convenientemente.

8.5 Requisitos de visualización de la situación

Se requiere que la plataforma NSSA soporte la visualización de múltiples situaciones de seguridad, incluidas la situación de seguridad global, la situación de seguridad de la red, la situación de seguridad de los activos, la situación de seguridad personalizada, etc. Al mismo tiempo se recomienda soportar la utilización de múltiples imágenes para visualizar la información detallada de cada situación de seguridad, como gráficos de radar, mapas de información de correlación, mapa de trayecto de amenazas, etc., y soportar la inspección de la información de seguridad detallada.

8.5.1 Visualización de la situación de seguridad global

1) Se recomienda soportar la presentación del estado de la evaluación de la seguridad global de la plataforma de computación en la nube mediante puntuaciones o notas.

2) Se recomienda presentar la situación de seguridad global de la plataforma de computación en la nube de manera gráfica, incluidas clasificaciones de riesgos, tendencias de ataques a la red, vulnerabilidades, comportamientos de usuario de alto riesgo, etc.

3) Se recomienda soportar la presentación de la situación de seguridad de distintos titulares, distintas operaciones comerciales y distintos activos, etc. en la plataforma de computación en la nube, así como la comparación con datos históricos para mostrar las tendencias.

4) Se recomienda soportar la presentación de alarmas combinadas en tiempo real de eventos de seguridad de la red, comportamientos de usuario anómalos y situación de seguridad de los activos en la plataforma de computación en la nube, y soportar la inspección gráfica de esas alarmas.

8.5.2 Visualización de la situación de seguridad de las redes

1) Se recomienda soportar la presentación gráfica multidimensional de los riesgos de seguridad de la plataforma de computación en la nube, incluidos los análisis estadísticos de los ataques a la red, los tipos de ataques a la red, la distribución geográfica de los ataques a la red, el tráfico de red anómalo, la IP de origen y la IP de destino de los ataques, etc.

2) Se recomienda soportar la presentación de alarmas de seguridad en tiempo real de la plataforma de computación en la nube, como los ataques a la red, el tráfico de red anómalo y los programas malignos, etc. La información sobre las alarmas debe incluir el sello de tiempo, el tipo de seguridad, el nivel de gravedad, la IP de origen y la IP de destino de los ataques, etc.

3) Se recomienda soportar la inspección de información detallada sobre la situación de seguridad de las redes.

8.5.3 Visualización de la situación de seguridad de los activos

1) Se recomienda soportar la presentación gráfica de la información sobre los activos de la plataforma de computación en la nube, como las escalas de activos, los tipos de activos, la propiedad de los activos, la distribución de los activos, etc.

2) Se recomienda soportar la presentación gráfica de los resultados de los diversos análisis estadísticos de la plataforma de computación en la nube, incluidas las vulnerabilidades de los activos, los ataques a la red y los errores de configuración, entre otros.

3) Se recomienda soportar riesgos de seguridad en tiempo real de los diversos activos de la plataforma de computación en la nube, incluidos el nombre del activo, la IP del activo, el tipo de ataque, el tipo de vulnerabilidad, el número de vulnerabilidades, los errores de configuración, etc.

4) Se recomienda soportar la inspección de información detallada sobre la situación de seguridad de los activos.

8.5.4 Visualización de la situación de comportamientos de usuario anómalos

1) Se recomienda soportar la presentación multidimensional de comportamientos de usuario anómalos en la plataforma de computación en la nube, incluidos los tipos de comportamientos anómalos, las tendencias de comportamientos anómalos, los usuarios anómalos (cuentas o IP), etc.

2) Se recomienda soportar la presentación de alarmas de seguridad en tiempo real de comportamientos de usuario anómalos de la plataforma de computación en la nube, incluidos la hora de la alarma, los tipos de alarmas, los niveles de gravedad y los usuarios (cuentas) anómalos, etc.

3) Se recomienda soportar la inspección detallada de la información sobre comportamientos de usuario anómalos.

8.5.5 Visualización de la situación de seguridad personalizada

Se recomienda soportar la configuración de las imágenes de situaciones personalizadas en función de diversas hipótesis de trabajo, y soportar la importación de configuraciones gráficas o de código, en función de los requisitos comerciales, las funciones de gestión y demás requisitos particulares de la plataforma de computación en la nube.

Bibliografía

[b-UIT-T-X.1217] Recomendación UIT-T X.1217 (2021), *Directrices para la aplicación de la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones*

[b-UIT-T X.1601] Recomendación UIT-T X.1601 (2016), *Marco de seguridad para la computación en la nube*

[b-UIT-T Y.3500] Recomendación UIT-T Y.3500 (2014) | ISO/CEI 17788:2014, *Tecnología de la información – Computación en nube – Visión general y vocabulario*.

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

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Publicado en Suiza
Ginebra, 2024