Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1217

(01/2021)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Ciberseguridad

Directrices para la aplicación de la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones

Recomendación UIT-T X.1217

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	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	**X.1200–X.1229**
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1389
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
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	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

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

Recomendación UIT-T X.1217

Directrices para la aplicación de la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones

Resumen

Desde el punto de vista del operador de telecomunicaciones, por inteligencia sobre amenazas se entiende un conjunto de información organizada, analizada y depurada relativa a los ataques potenciales y reales que pueden amenazar a una organización. Esta inteligencia puede incluir también las motivaciones, intenciones, características y métodos de los atacantes, junto con su *modus operandi* o técnicas, tácticas y procedimientos.

En el ámbito de la seguridad de las redes y de la información, la aparición de incidentes de ciberseguridad a gran escala e inesperados ha desencadenado la necesidad urgente de disponer de inteligencia sobre amenazas. La inteligencia sobre amenazas puede ayudar a la organización a reducir el riesgo y mejorar su seguridad general. Se ha definido una taxonomía, una gramática y una presentación unificadas de la inteligencia sobre amenazas, para que ésta pueda ser compartida por diferentes organizaciones.

En la Recomendación UIT-T X.1217, tras un análisis general, se especifican directrices para aplicar la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1217	2021-01-07	17	11.1002/1000/14443

Palabras clave

Seguridad, inteligencia sobre amenazas.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

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 adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, 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 la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores 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

Página

1 Sumario 1

2 Referencias 1

3 Definiciones 1

3.1 Términos definidos en otros documentos 1

3.2 Términos definidos en esta Recomendación 2

4 Siglas y acrónimos 2

5 Convenios 3

6 Descripción de la inteligencia sobre amenazas 3

7 Resumen de cómo aplicar la inteligencia sobre amenazas en la explotación de las redes de telecomunicaciones 4

7.1 Recopilación de datos 5

7.2 Procesamiento y análisis de datos 6

7.3 Compartición y aplicación de inteligencia 6

8 Directrices para aplicar inteligencia sobre amenazas en la explotación de las redes de telecomunicaciones 7

8.1 Recopilación de datos 7

8.2 Procesamiento y análisis de datos 8

8.3 Compartición y aplicación de inteligencia 10

Bibliografía 12

Introducción

Desde el punto de vista del operador de telecomunicaciones, por inteligencia sobre amenazas se entiende un conjunto de información organizada, analizada y depurada relativa a los ataques potenciales y reales que pueden amenazar a una organización. Esta inteligencia puede incluir también las motivaciones, intenciones, características y métodos de los atacantes, junto con su *modus operandi* o técnicas, tácticas y procedimientos.

En el ámbito de la seguridad de las redes y de la información, la aparición de incidentes de ciberseguridad a gran escala e inesperados ha desencadenado la necesidad urgente de disponer de inteligencia sobre amenazas. La inteligencia sobre amenazas puede ayudar a la organización a reducir el riesgo y mejorar su seguridad general, por cuanto le permite comprender quién tiene más probabilidades de atacar, cuál es su objetivo, qué es lo que pretenden conseguir y por qué, y cómo planean hacerlo.

[OASIS STIXv2] define un lenguaje y formato de serialización para compartir inteligencia sobre ciberamenazas. [OASIS TAXIIv2] especifica un protocolo para compartir inteligencia sobre ciberamenazas a través de HTTPS. [UIT-T X.1215] describe cómo se puede utilizar el lenguaje de expresión estructurada de información sobre amenazas (STIX) para la inteligencia de ciberamenazas y la compartición de información.

Se ha definido una taxonomía, una gramática y una presentación unificadas de la inteligencia sobre amenazas, para que ésta pueda ser compartida por diferentes organizaciones. El siguiente problema que se ha de tomar en consideración es cómo utilizar la inteligencia sobre amenazas para resolver los problemas de seguridad en la red.

[OASIS OpenC2-L] especifica un lenguaje de comando y control (C2) para controlar las funciones de ciberseguridad. [OASIS OpenC2-H] especifica una interfaz de programación de aplicaciones (API) HTTPS para transportar comandos OpenC2 a los dispositivos de ciberseguridad. [OASIS OpenC2-P] especifica el uso del lenguaje OpenC2 para controlar cortafuegos sin estado. Los perfiles para otras funciones de ciberseguridad están en desarrollo en OASIS.

En esta Recomendación, tras un análisis general, se especifican directrices para aplicar la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones.

Recomendación UIT-T X.1217

Directrices para la aplicación de la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones

1 Sumario

En esta Recomendación, tras un análisis general, se especifican directrices para aplicar la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.1215] Recomendación UIT-T X.1215 (2019), *Expresión estructurada de información sobre amenazas: casos de uso*.

[OASIS OpenC2-H] OASIS Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0.
<https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html>

[OASIS OpenC2-L] OASIS Open Command Open Command and Control (OpenC2) Language Specification Version 1.0.
<https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs01/oc2ls-v1.0-cs01.html>

[OASIS OpenC2-P] OASIS Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0.
<https://docs.oasis-open.org/openc2/oc2slpf/v1.0/oc2slpf-v1.0.html>

[OASIS STIXv2] OASIS STIX 2.1 specifications.
<https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html>

[OASIS TAXIIv2] OASIS TAXII 2.1 specifications.
<https://docs.oasis-open.org/cti/taxii/v2.1/cs01/taxii-v2.1-cs01.html>

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 red robot (botnet) [b-UIT-T X.1231]: Robots (bots) de *software* maligno controlados a distancia que se ejecutan autónoma o automáticamente en los ordenadores infectados en conjunción con un servidor de instrucción y control que pertenece al robot principal (botmaster).

3.1.2 fraude [b-UIT-T Y.140.1]: Acto mediante el cual se consigue una ventaja pecuniaria por medio de una representación falsa o una acción no autorizada.

3.1.3 *malware* [b-UIT-T X.1211]: *Software* maligno diseñado específicamente para dañar o interrumpir un sistema atacando su confidencialidad, integridad y/o disponibilidad.

3.1.4 ***peska* (*phishing*)** [b-UIT-T X.1244]: Intento de adquirir de manera fraudulenta y delictiva información sensible, como nombres de usuario, contraseñas y datos bancarios, mediante la suplantación de una entidad fiable en las comunicaciones electrónicas.

3.1.5 **vulnerabilidad** [b-UIT-T X.1524]: Punto débil del *software* que puede utilizarse para acceder a un sistema o a la información que contiene.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 **depurado de datos**: Proceso para eliminar los datos irrelevantes y duplicar datos del conjunto original de datos, para suavizar los datos de ruido y procesar los valores faltantes y atípicos.

3.2.2 **recorte de datos**: Proceso para recortar datos inútiles o anómalos.

3.2.3 **desduplicación de datos**: Proceso para eliminar datos duplicados del conjunto original de datos.

3.2.4 **desensibilización de datos**: Proceso para ocultar los datos sensibles.

3.2.5 **filtrado de datos**: Proceso para eliminar datos irrelevantes y filtrar datos inconexos del conjunto original de datos.

3.2.6 **mapeo de datos**: Proceso para mapear datos desde el sistema origen de los datos hasta el sistema destino de los datos.

3.2.7 **fusión de datos**: Proceso para fusionar registros de datos similares en un solo registro.

3.2.8 **minería de datos**: Proceso de cálculo para descubrir patrones en grandes conjuntos de datos, utilizando métodos de inteligencia artificial, aprendizaje automático, estadística y sistemas de bases de datos.

3.2.9 **reducción de ruido de datos**: Proceso para suavizar los datos de ruido.

3.2.10 **muestreo de datos**: Técnica estadística utilizada para procesar los valores faltantes y atípicos.

3.2.11 **segmentación de datos**: Proceso para segmentar datos de diferentes niveles.

3.2.12 **clasificación de datos**: Proceso para clasificar los datos en un determinado orden o categoría.

3.2.13 **transformación de datos**: Proceso para transformar datos a un determinado formato y efectuar un cambio de escala a un intervalo específico.

3.2.14 **recopilación de incidentes**: Proceso para recabar datos acerca de incidentes de seguridad.

3.2.15 **conocimiento de la situación**: Proceso para mostrar la situación general y predecir posibles amenazas y ataques.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siglas y los acrónimos siguientes:

API	Interfaz de programación de aplicaciones (*application programming interface*)
CVE	Vulnerabilidades y riesgos corrientes (*common vulnerabilities and exposures*)
C&C	Instrucciones y control (*command and control*)
DDoS	Denegación del servicio distribuido (*distributed denial of service*)
DNS	Sistema de nombres de dominio (*domain name system*)
FW	Cortafuegos (*firewall*)

GW	Pasarela (*gateway*)
HTTPS	Protocolo de transferencia de hipertexto seguro (*hypertext transfer protocol secure*)
ID	Identidad
IDS	Sistema de detección de intrusiones (*intrusion detection system*)
IP	Protocolo Internet (*Internet protocol*)
IPS	Sistema de prevención de intrusiones (*intrusion prevention system*)
MD5	Algoritmo de compendio de mensajes 5 (*message digest algorithm 5*)
O&M	Operaciones y mantenimiento
SDN	Red definida por *software* (*software defined network*)
SIEM	Gestión de eventos y de seguridad de la información (*security information and event management*)
SoC	Centro de operaciones de seguridad (*security operation centre*)
STIX	Expresión estructurada de información sobre amenazas (*structured threat information expression*)
TAXII	Intercambio automatizado fiable de información de inteligencia (*trusted automated exchange of intelligence information*)
URL	Localizador uniforme de recursos (*uniform resource locator*)
WAF	Cortafuego de aplicación web (*web application firewall*)

5 Convenios

En esta Recomendación:

La expresión "se requiere" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con esta Recomendación.

La expresión "se recomienda" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión "se prohíbe" indica que el requisito que debe cumplirse estrictamente y del que no se permite desviación alguna si se pretende declarar la conformidad con esta Recomendación.

La expresión "puede opcionalmente" indica que el requisito se permite, sin que ello signifique que se recomienda. No se pretende implicar que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

6 Descripción de la inteligencia sobre amenazas

Desde el punto de vista del operador de telecomunicaciones, por la inteligencia sobre amenazas se entiende un conjunto de información organizada, analizada y depurada relativa a los ataques potenciales y reales que pueden amenazar a una organización. Esta información también puede incluir las motivaciones, intenciones, características y métodos de los atacantes, junto con su *modus operandi* o técnicas, tácticas y procedimientos.

En el contexto de la explotación de las redes de telecomunicaciones, por inteligencia sobre amenazas se entiende los conocimientos utilizados para prevenir o mitigar los ciberataques, incluidas las motivaciones, las intenciones, las características, los métodos, el *modus operandi*, las técnicas, las tácticas y los procedimientos de los atacantes. No está relacionada con la información de identificación personal.

En el ámbito de la seguridad de las redes y la información, la aparición de incidentes de ciberseguridad a gran escala e inesperados ha desencadenado la necesidad urgente de disponer de inteligencia sobre amenazas. La inteligencia sobre amenazas puede ayudar a la organización a reducir el riesgo y mejorar su seguridad general, por cuanto le permite comprender quién tiene más probabilidades de atacar, cuál es su objetivo, qué es lo que pretenden conseguir y por qué, y cómo planean hacerlo.

[OASIS STIXv2] define un lenguaje y formato de serialización para compartir inteligencia sobre ciberamenazas. [OASIS TAXIIv2] especifica un protocolo para compartir inteligencia sobre ciberamenazas a través de HTTPS. [UIT-T X.1215] describe cómo se puede utilizar el lenguaje de expresión estructurada de información sobre amenazas (STIX) para la inteligencia de ciberamenazas y la compartición de información.

Se ha definido una taxonomía, una gramática y una presentación unificadas de la inteligencia sobre amenazas, para que ésta pueda ser compartida por diferentes organizaciones. El siguiente problema que se ha de tomar en consideración es cómo utilizar la inteligencia sobre amenazas para resolver los problemas de seguridad en la red.

[OASIS OpenC2-L] especifica un lenguaje de comando y control (C2) para controlar las funciones de ciberseguridad. [OASIS OpenC2-H] especifica una API HTTPS para transportar comandos OpenC2 a los dispositivos de ciberseguridad. [OASIS OpenC2-P] especifica el uso del lenguaje OpenC2 para controlar cortafuegos sin estado. Los perfiles para otras funciones de ciberseguridad están en desarrollo en OASIS.

7 Resumen de cómo aplicar la inteligencia sobre amenazas en la explotación de las redes de telecomunicaciones

En la Figura 7-1 se ilustra cómo se aplica la inteligencia sobre amenazas en la explotación de las redes de telecomunicaciones.

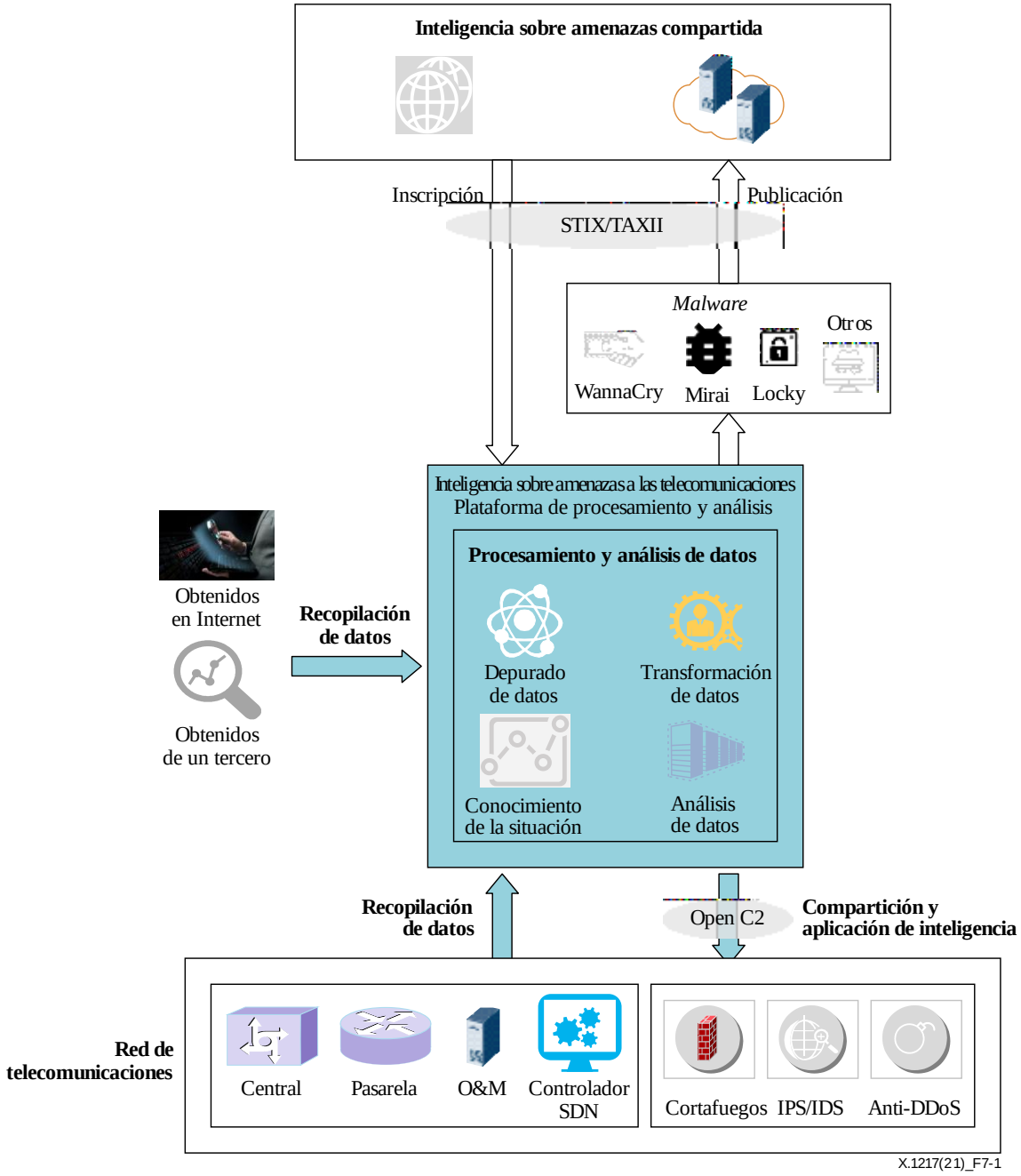

Figura 7-1 – Aplicación de la inteligencia sobre amenazas en la explotación de las redes de telecomunicaciones

De conformidad con la Figura 7-1, la aplicación de la inteligencia sobre amenazas a la explotación de las redes de telecomunicaciones consta de tres procesos principales, a saber: recopilación de datos; procesamiento y análisis de datos; y compartición y aplicación de inteligencia.

7.1 Recopilación de datos

Existen dos tipos de fuentes de datos de inteligencia sobre amenazas:

– los elementos de la red interna y de los dispositivos de seguridad;

– las fuentes externas.

Los datos procedentes de los elementos de la red interna y de los dispositivos de seguridad consisten principalmente en los registros, las alertas y las políticas de seguridad, por ejemplo, los registros de incidentes, los registros del sistema de nombres de dominio (DNS), los registros del cortafuegos, etc.

Existen fuentes específicas para recopilar datos del exterior, como búsquedas por Internet, adquisición de terceros mediante STIX/TAXII, etc. Los datos que se comparten son principalmente direcciones IP, dominios, URL, incidentes, vulnerabilidades, etc.

Es necesario realizar una desensibilización de los datos antes de su recopilación.

7.2 Procesamiento y análisis de datos

El procesamiento y análisis de datos consta de cuatro componentes funcionales: depurado de datos, transformación de datos, análisis de datos y conocimiento de la situación.

En la Figura 7-2 se ilustran los componentes funcionales del procesamiento y análisis de datos.

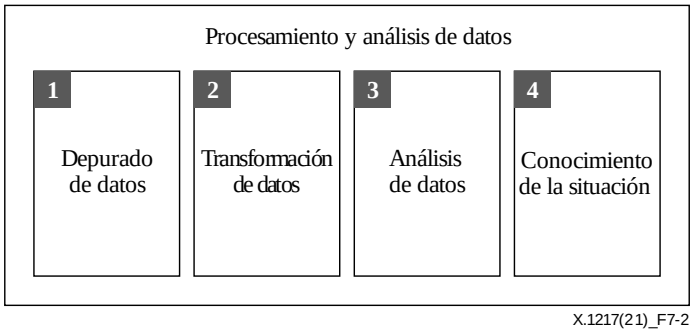

Figura 7-2 – Componentes funcionales del procesamiento y análisis de datos

– El depurado de datos elimina los datos irrelevantes y los duplicados del conjunto original de datos, reduce los datos de ruido y procesa los valores faltantes y atípicos.

– La transformación de datos consiste en la integración y normalización de datos:

  • La integración de datos consiste en unificar el almacenamiento datos procedentes de múltiples fuentes en un determinado formato.

  • La normalización de los datos consiste en eliminar la influencia de las dimensiones y la gama de valores entre los indicadores, y cambiar la escala de los datos a un intervalo específico, en particular la transformación de funciones y la construcción de atributos, etc.

– El análisis de datos utiliza diversos algoritmos para analizar los datos, extraer palabras clave, establecer reglas claras, correlacionar el análisis para obtener información de inteligencia sobre amenazas y analizar las medidas de respuesta correspondientes.

– El conocimiento de la situación incluye la visualización y la alerta predictiva:

  • La visualización consiste en la representación visual de la situación general basada en los datos analizados, como la categorización, clasificación, etc.

  • La alerta predictiva se refiere a la predicción de posibles amenazas, las vías de ataque, los métodos de ataque, etc., a partir del análisis de datos y de la situación general, así como la emisión de alertas inmediatas que permitan adoptar estrategias de seguridad para defenderse de los posibles ataques.

7.3 Compartición y aplicación de inteligencia

La compartición y la aplicación de inteligencia comprende dos aspectos:

- Basándose en la inteligencia sobre amenazas, los administradores de operaciones y mantenimiento pueden desplegar políticas de seguridad para proteger los elementos de la red y los dispositivos de seguridad.
- La inteligencia sobre amenazas puede ser compartida con terceros.

La inteligencia sobre amenazas que se comparte y aplica en la explotación de redes de telecomunicaciones consiste en la información de inteligencia propiamente dicha, información sobre la advertencia predictiva, contramedidas de seguridad de la red, etc.

Los objetos que comparten y aplican inteligencia en las redes de telecomunicaciones son los elementos de red y dispositivos de seguridad, como sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), cortafuegos y dispositivos anti-DDoS. Para aplicar instrucciones y control de seguridad en los dispositivos de seguridad, se recomienda utilizar las especificaciones OpenC2 de OASIS.

La compartición y la aplicación de inteligencia en las redes de telecomunicaciones tiene por objeto prevenir y reducir los incidentes de seguridad y, al mismo tiempo, lograr una respuesta rápida y eficiente a cada incidente de seguridad en la red de telecomunicaciones.

8 Directrices para aplicar inteligencia sobre amenazas en la explotación de las redes de telecomunicaciones

En la cláusula 7 se describen tres procesos principales, a saber, la recopilación, el procesamiento y el análisis de datos, la compartición y aplicación de inteligencia sobre amenazas en la explotación de redes de telecomunicaciones. En las cláusulas 8.1 a 8.3, se especifican las directrices para aplicar la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones.

8.1 Recopilación de datos

La recopilación de datos es condición necesaria para poder aplicar la inteligencia sobre amenazas, y tiene por objeto reunir toda la información y datos relacionados con la inteligencia sobre amenazas. Se recomienda incluir datos procedentes de los elementos de la red interna y los dispositivos de seguridad, por ejemplo, registros, alertas y políticas de seguridad. Asimismo, se recomienda incluir datos de fuentes externas, como los resultantes de búsquedas por Internet, los adquiridos de terceros, y así sucesivamente. Los datos que se comparten son principalmente direcciones IP, dominios, URL, incidentes, vulnerabilidades, etc.

Se recomienda la recopilación activa de datos para recabar datos tales como registros DNS, registros de cortafuegos, etc. Asimismo, se recomienda recopilar incidentes para recabar datos sobre incidentes de seguridad. También se recomienda recopilar inteligencia para acumular inteligencia crítica, como direcciones IP, dominios, URL, incidentes, vulnerabilidades, etc.

Si se recaban datos de los elementos de la red interna y de los dispositivos de seguridad, la recopilación de datos puede efectuarse con arreglo a los diferentes tipos de información, como la de incidentes o la de actividad de las redes robot.

La información del incidente puede recopilarse desde dispositivos IDS, IPS, cortafuegos de aplicaciones web (WAF), anti-DDoS, plataformas de gestión de eventos y de seguridad de la información (SIEM) y centros de operaciones de seguridad (SoC). Se recomienda que la información recabada sobre incidentes incluya el nombre, la descripción, la categoría y los activos afectados por el incidente. Se recomienda además incluir el momento en que ocurre el incidente. La actividad de las redes robot se puede recopilar a partir de los dispositivos DNS, IDS, WAF, dispositivos anti-DDoS, etc. Asimismo, se recomienda que la información recopilada acerca de la actividad de las redes robot incluya el nombre, la descripción, la categoría y los activos afectados. Se recomienda incluir también el momento en que se produce la actividad de las redes robot.

Si los datos se obtienen de Internet, la recopilación de datos puede realizarse de acuerdo con diferentes tipos, como información sobre vulnerabilidades, dominios maliciosos, direcciones URL maliciosas, direcciones IP maliciosas, información sobre incidentes, etc.

La información sobre vulnerabilidades se puede recopilar a partir de sitios web especializados en vulnerabilidades, como los sitios web sobre vulnerabilidades y riesgos corrientes (CVE). Se recomienda que la información recopilada sobre vulnerabilidades incluya la ID, el nombre, la descripción, el tipo, las versiones afectadas, los proveedores afectados, los productos afectados por la vulnerabilidad, etc.

El dominio malicioso y la información del URL pueden clasificarse en diferentes tipos de amenazas de instrucción y control (C&C), red robot, *malware*, código troyano, *peska*, fraude, etc. La información sobre el dominio y el URL maliciosos se pueden recopilar a partir de sitios web, informes de proveedores, informes de seguridad de terceros, etc. Se recomienda que la información recopilada acerca del dominio y el URL maliciosos incluya el servidor de nombres de dominio, el tipo de DNS, el tipo de amenaza, el nivel de crédito, etc.

La información sobre direcciones IP maliciosas puede recopilarse de varios sitios web y de algunos proveedores y empresas de seguridad, etc. Las direcciones IP maliciosas pueden clasificarse según el tipo de amenaza de DDoS, vulnerabilidad, fuente de correo basura, ataque web, red robot, *malware*, C&C, etc. Se recomienda que la información recopilada sobre las IP maliciosas incluya la dirección IP, el tipo de amenaza, el nivel de crédito, etc.

La información relativa a incidentes se puede recopilar a partir de las noticias sobre seguridad o de los informes de los proveedores. Se recomienda que la información recopilada sobre incidentes incluya el nombre, la descripción, la categoría y los activos afectados por el incidente.

Los datos adquiridos de terceros incluyen principalmente direcciones IP, nombres de dominio, URL, incidentes, vulnerabilidades, etc. La información de cada tipo es la misma que la de los anteriores.

Cuando los datos procedan de elementos de la red interna y dispositivos de seguridad, se recomienda que la recopilación se lleve a cabo mediante herramientas automatizadas o secuencias de instrucciones (*scripts*). Cuando los datos procedan de fuentes externas, se recomienda que la recopilación se realice mediante secuencias de instrucciones o mediante un mecanismo de compartición y compartición de datos. Se recomienda que el procesamiento ulterior de los datos recopilados se ajuste al formato normalizado definido por [OASIS STIXv2] y [OASIS TAXIIv2]. En el caso de la inteligencia sobre amenazas haya sido compartida, se recomienda que la recopilación de datos se ajuste al formato normalizado definido por [OASIS STIXv2] y [OASIS TAXIIv2].

Se recomienda realizar una desensibilización de los datos antes de su recopilación, por cuanto este proceso permite ocultar los datos sensibles originales con caracteres o datos, con el fin de proteger los datos de carácter sensible.

8.2 Procesamiento y análisis de datos

8.2.1 Depurado de datos

El depurado de los datos es una de las principales etapas a la hora de aplicar la inteligencia sobre amenazas, y tiene por objeto limpiar los datos recopilados para hacerlos uniformes y útiles, y prepararlos para su transformación y análisis.

– Se recomienda aplicar el filtrado de datos, la reducción del ruido de los datos y la eliminación de datos duplicados.

– Se recomienda aplicar el filtrado de datos, eliminar los datos irrelevantes y filtrar los datos inconexos en el conjunto original de datos.

– Se recomienda aplicar la reducción del ruido de datos y la eliminación de datos duplicados para suavizar los datos ruidosos y eliminar los datos duplicados en el conjunto original de datos.

Dado que los datos recopilados contienen distintos tipos de datos, como direcciones IP, dominios, URL, incidentes, vulnerabilidades, etc., el depurado de datos dependerá del tipo de datos recopilados.

La eliminación de datos duplicados elimina principalmente las duplicaciones para ahorrar espacio de almacenamiento. Los criterios son diferentes en función del tipo de datos. Para los datos relativos a IP, si la dirección IP es la misma y las otras partes del registro, como el tipo de amenaza, el nivel de crédito, son también idénticas, se considerará que es un dato duplicado y se eliminarán las duplicaciones, de lo contrario tendrán que fusionarse. En lo que respecta a datos relativos a dominios, si todos los registros del servidor de nombres de dominio, el tipo de DNS, el tipo de amenaza y el nivel de crédito son idénticos, se trata sin duda de datos duplicados y se eliminarán las duplicaciones, de lo contrario tendrán que fusionarse. Cuando se trata de información sobre vulnerabilidades, si la ID de la vulnerabilidad es idéntica, los datos están duplicados y se eliminarán las duplicaciones. Para otros tipos de datos, se recomienda calcular la tasa de similitud, y cuando ésta sea mayor que un determinado umbral, se procederá a la eliminación de duplicados.

Se recomienda fusionar la información similar en un mismo registro. Para los tipos de información sobre IP, dominio, URL e incidente, si hay varios registros con la misma IP, servidor de nombre de dominio, URL y descripción del incidente, se podrán fusionar en un mismo registro. Para otros tipos de datos se puede calcular la tasa de similitud, y si dicha tasa de similitud es inferior a cierto umbral, la información debe fusionarse.

– Se recomienda aplicar el muestreo, la fusión y la clasificación de datos para procesar los valores faltantes y atípicos, con el fin de que los datos sean más útiles para el procesamiento ulterior.
– Se recomienda utilizar herramientas automatizadas para el filtrado de datos y la eliminación de datos duplicados.

8.2.2 Transformación de datos

La transformación de datos consiste en eliminar la influencia de las dimensiones y la gama de valores entre los indicadores, y cambiar de escala los datos a un intervalo específico, en particular la transformación de funciones y la construcción de atributos, etc., y transformar los datos depurados a los datos de formato unificado, preparándose para el análisis de los datos.

Para llevar a cabo la transformación de los datos, se recomienda realizar el mapeo de datos, el recorte de datos y la segmentación de datos para modificar los datos por datos útiles con valor. Se recomienda la conversión ortográfica para convertir diferentes ortografías a la ortografía unificada. Asimismo, se recomienda normalizar el formato para hacer que los datos procedentes de múltiples fuentes tengan un formato determinado. Se recomienda aplicar la convergencia de datos para obtener un almacenamiento unificado de múltiples fuentes.

Los procedimientos de transformación de datos para cada tipo de dirección IP, dominio, URL y vulnerabilidad a incidentes son similares. Se recomiendan aplicar reglas de mapeo de datos para cada tipo, que pueden ser diferentes según el tipo de datos. Por ejemplo, la regla de mapeo de datos para la información sobre incidentes consiste en transformar el campo nombre, descripción, categoría y activos afectados en campos del formato estándar. Se recomienda mapear la información del cortafuegos (FW), es decir el sello de tiempo, el URL solicitado, el nombre del anfitrión, el tipo de ataque y el contenido del ataque, a un formato definido.

Para el recorte y la segmentación de datos, se recomienda que el proceso de transformación de datos se realice mediante herramientas automatizadas. Para la conversión ortográfica, se recomienda que el proceso de transformación de datos se realice mediante herramientas automatizadas. Para la normalización del formato, se recomienda que el proceso de transformación de datos se ajuste al formato normalizado definido por [OASIS STIXv2] y [OASIS TAXIIv2].

8.2.3 Análisis de datos

El análisis de datos, que es la etapa crucial para la aplicación de la inteligencia sobre amenazas, consiste en utilizar diversos algoritmos para analizar los datos transformados, extraer palabras clave, establecer reglas claras, correlacionar análisis, etc., para obtener información de inteligencia sobre amenazas y analizar las medidas correctivas correspondientes.

Para realizar el análisis de datos, se recomienda la recuperación y extracción de datos a fin de obtener información esencial de inteligencia sobre amenazas y poder crear alertas o tomar las medidas del caso. Asimismo, se recomienda realizar un análisis del comportamiento y un análisis de correlación de incidentes, a fin de encontrar información útil de inteligencia sobre amenazas, como dirección IP, nombre de dominio, compendio de información, información sobre el atacante, medidas de respuesta, etc. Se recomienda realizar el mapeo de conocimientos y búsqueda de amenazas para obtener información de inteligencia sobre amenazas profundas y adoptar las medidas y respuestas correspondientes.

Por ejemplo, el algoritmo de aprendizaje de máquina para los registros DNS puede utilizarse para detectar instrucciones y controles de redes robot. Se recomienda combinar los registros del cortafuegos con el origen de la amenaza, el tipo, el tiempo de ataque y cualquier otra información que permita calcular el nivel de la amenaza. La información de URL e IP puede utilizarse para calcular el nivel de reputación.

Se recomienda que los algoritmos de análisis de datos se ejecuten automáticamente. Se recomienda que el resultado del análisis de datos se ajuste al formato normalizado definido por [OASIS STIXv2] y [OASIS TAXIIv2].

8.2.4 Conocimiento de la situación

El conocimiento de la situación consiste en utilizar los datos analizados para hacer predicciones de tendencias y emitir alertas y, al mismo tiempo, mostrar la situación general.

Para poner en práctica el conocimiento de la situación, se recomienda la visualización de la situación para mostrar la situación general a través de los datos analizados. Se recomienda utilizar la predicción de tendencias y la emisión de alertas para prevenir posibles amenazas, vías de ataque, métodos de ataque, etc., mediante el análisis de los datos y la situación general, y emitir alertas tempranas para poder adoptar estrategias de seguridad que permitan defenderse de los posibles ataques. El método de conocimiento de la situación se basa en algoritmos que incluyen el aprendizaje automático, el análisis lineal, estadísticas de probabilidad y la inteligencia artificial.

Se recomienda que la predicción de tendencias y la alerta se realicen de forma automática. Se recomienda que los resultados de la predicción de tendencias y la alerta sigan el formato estándar definido por [OASIS STIXv2] y [OASIS TAXIIv2]. Para la presentación visual de la situación, se recomienda mostrar la situación general de los datos mediante herramientas de visualización.

8.3 Compartición y aplicación de inteligencia

La finalidad de compartir y aplicar la inteligencia es prevenir o reducir los incidentes de seguridad y lograr una respuesta rápida y eficiente a todos y cada uno de los incidentes de seguridad en la red de telecomunicaciones.

La inteligencia obtenida en la fase de procesamiento y análisis de datos, en particular la información sobre amenazas, la información de alerta predictiva, las medidas de seguridad de la red, las políticas de seguridad, etc., podría compartirse con diferentes departamentos y comunidades de operadores de telecomunicaciones. La inteligencia podría compartirse de varias formas, por ejemplo, mediante informes y avisos, o bien en la forma de indicadores de detección.

Se recomienda obtener información de inteligencia de los elementos de la red, los dispositivos de seguridad y los centros de alerta, etc. Los administradores de operaciones y mantenimiento podrían generar políticas de seguridad en función de la inteligencia obtenida y aplicar luego esas políticas en los elementos de la red y los dispositivos de seguridad. Los administradores también podrían actualizar el *software* y modificar la configuración de los elementos de red y los dispositivos de seguridad, si fuera necesario.

Se recomienda aplicar inteligencia basada en URL a la pasarela, que ésta podría utilizar luego para actualizar su política de seguridad filtrando los URL maliciosas con arreglo a una lista negra. Se recomienda aplicar la inteligencia a los sistemas IDS o IPS actualizando las reglas de protección mediante los URL correspondientes.

Se recomienda aplicar inteligencia basada en dominios maliciosos al servidor DNS, que éste podría utilizar luego para actualizar la configuración registrando los dominios maliciosos en una lista negra.

Se recomienda aplicar inteligencia basada en direcciones IP maliciosas al cortafuegos, que éste podría utilizar luego para actualizar su política de seguridad filtrando las direcciones IP maliciosas. También puede aplicarse a los sistemas IDS o al IPS actualizando las normas de protección mediante la correspondiente dirección IP.

Se recomienda aplicar inteligencia basada en vulnerabilidades a los elementos de la red, que éstos podrían utilizar para corregir las vulnerabilidades actualizando el *software* o el *hardware*. Entretanto, puede utilizarse opcionalmente para hacer aplicativos (*plug-in*) de detección, y luego para actualizar el escáner de detección. Otra posibilidad es aplicar la inteligencia a un sistema de respuesta a emergencias para identificar los incidentes y ayudar a tomar medidas para prevenir ataques.

Se recomienda que la inteligencia siga el formato normalizado definido por [OASIS STIXv2] y [OASIS TAXIIv2]. Se recomienda que las instrucciones y control de seguridad utilicen las especificaciones OASIS OpenC2.

Bibliografía

[b-UIT-T X.1211] Recomendación UIT-T X.1211 (2014), *Técnicas para prevenir ataques en la web*.

[b-UIT-T X.1231] Recomendación UIT-T X.1231 (2008), *Estrategias técnicas de lucha contra el correo basura*.

[b-UIT-T X.1244] Recomendación UIT-T X.1244 (2008), *Características generales de la lucha contra el correo basura (spam) en aplicaciones multimedios basadas en IP*.

[b-UIT-T X.1524] Recomendación UIT-T X.1524 (2012), *Lista de puntos débiles comunes*.

[b-UIT-T Y.140.1] Recomendación UIT-T Y.140.1 (2004), *Guía de atributos y requisitos para la interconexión entre operadores de redes públicas de telecomunicaciones y proveedores de servicio que intervienen en la prestación de servicios de telecomunicaciones*.

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

Impreso en Suiza
Ginebra, 2021