Nueva guía de ENISA: Información procesable para respuestas a incidentes de seguridad

ENISA ha publicado una guía de buenas prácticas sobre Información procesable para respuestas a incidentes de seguridad, que tiene como finalidad describir los retos a los que se enfrentan los equipos de respuesta a emergencias informáticas (CERT, por sus siglas en inglés) a nivel nacional, así como otras organizaciones de seguridad, cuando intentan generar soluciones prácticas a partir de grandes cantidades de datos.

El estudio ofrece una amplia visión general del actual panorama de intercambio de información en el contexto de la generación de información procesable, identifica las normativas y herramientas actuales, informa sobre las mejores prácticas y las deficiencias existentes, y ofrece recomendaciones de mejora.

La parte principal del informe describe cómo se obtiene, se utiliza y se comparte de manera sistemática la información procesable. El modelo conceptual propuesto, que constituye la base del estudio, presenta un programa generalizado de procesamiento de información consistente en cinco pasos: recopilación, preparación, almacenamiento, análisis y distribución. El propósito de este modelo es facilitar la manera en que los CERT tratan la información, a fin de simplificar el proceso de gestión de incidentes.

El Director Ejecutivo de ENISA, Udo Helmbrecht, comentó: *"Los CERT son la vanguardia de nuestra ciberdefensa. Dado que su tarea diaria se basa en el procesamiento de cantidades de datos cada vez mayores, el reto es comprender el sentido de dichos datos y generar resultados procesables y prácticos. La información procesable se considera un elemento fundamental para la respuesta a los incidentes. Este estudio es el primer intento de proporcionar una guía de referencia sobre esta cuestión para los CERT. ENISA acoge con satisfacción la oportunidad de poder ofrecer su apoyo al trabajo sobre el terreno mediante informes, investigación y un mayor desarrollo de las herramientas".*

El estudio investiga las deficiencias observadas en los procesos de gestión de información procesable por parte de los CERT y facilita un conjunto de recomendaciones generales para las organizaciones responsables de la diseminación de información. La conclusión general es que los intercambios de información todavía no han alcanzado un estado de madurez suficiente y que deberá seguir desarrollándose el entorno en el que se comparte la información para que las ventajas que suponen dichos intercambios puedan aprovecharse plenamente.

Se incluyen tres estudios de casos que cubren varios aspectos de la gestión de información procesable por parte de los CERT. Estos escenarios reflejan los procesos operativos de los auténticos CERT y las características de las herramientas que se emplean, indicando cómo pueden aplicarse para mejorar la capacidad de los CERT a la hora de elaborar, compartir y utilizar la información procesable.

Inventario para el intercambio de información

A modo de complemento, el estudio incluye un inventario titulado Normativas y herramientas para el intercambio y el tratamiento de información procesable, que puede aplicarse a actividades de intercambio de información. El inventario explora las relaciones entre diferentes normativas, facilitando así una mejor comprensión de los protocolos subyacentes.

La primera parte del inventario cubre un total de 53 normativas diferentes sobre el intercambio de información, una mezcla de formatos, protocolos, enfoques técnicos y marcos de uso común, que se desglosan en siete categorías principales basadas en el alcance de las normativas.

La segunda parte del inventario describe 16 herramientas y plataformas relevantes para el intercambio y tratamiento de información procesable. Se trata, en su mayor parte, de soluciones de código abierto que están a disposición de los CERT.

Ejercicio práctico: Utilización de indicadores para mejorar las capacidades de defensa de la información procesable.

Como parte del proyecto, se ha creado un nuevo escenario de ejercicio práctico de carácter formativo, destinado a miembros de CERT y otros profesionales informáticos responsables de las respuestas a incidentes de seguridad.

El objetivo del ejercicio es enseñar cómo crear e implementar indicadores de compromiso mediante la plataforma de Investigación Colaborativa de Amenazas (CRIT, por sus siglas en inglés). Además, el ejercicio también muestra cómo aprovechar la CRIT para visualizar las relaciones entre diferentes elementos de una campaña, cómo extraer indicadores a partir de datos de incidentes, desarrollar medidas mitigadoras y realizar un seguimiento de dichas medidas. El ejercicio fue creado para un enfoque más estructurado de la gestión de indicadores y, en última instancia, un mejor equipamiento para garantizar la seguridad de las redes.

Informes completos:

- Información procesable para respuestas a incidentes de seguridad
- Normativas y herramientas para el intercambio y el tratamiento de información procesable
- Utilización de indicadores para mejorar las capacidades de defensa de la información procesable

Notas para los editores:

https://www.enisa.europa.eu/activities/cert/support/awa

https://www.enisa.europa.eu/activities/cert/support/proactive-detection

Entrevistas: Cosmin Ciobanu, Experto en SRI, **correo electrónico:** Cosmin.Ciobanu@enisa.europa.eu, **teléfono:** (+30) 2814 409663.