Publicado el Manual de Usuario de la herramienta en el portal del CERT Gubernamental Nacional

REYES herramienta del CCN-CERT para el intercambio de información y conocimiento de ciberamenazas

- **El Manual, enmarcado dentro de las Guías CCN-STIC (426), incluye una descripción general del modelo, la interfaz de usuario y su uso en la creación, visualización y exportación de eventos.**

- **A esta instancia de REYES sólo pueden acceder los usuarios del SAT de Internet.**

Madrid, 27 de enero de 2016.- El CCN-CERT ha hecho pública la **Guía CCN-STIC 426 REYES. Manual de Usuario**, un compendio de lo más sustancial de esta plataforma de intercambio de información y conocimiento de ciberamenazas, a la que, de momento, sólo pueden solicitar su acceso aquellas organizaciones que estén dados de alta en el Sistema de Alerta Temprana (SAT) del CERT Gubernamental Nacional.

La Guía recoge una descripción general de este sistema, basado en la tecnología MISP (*Malware Information Sharing Platform*), y especialmente ideado para ofrecer un modo de intercambio de información entre distintas organizaciones que internamente generan ciberinteligencia. De hecho, el sistema ofrece una base de datos centralizada de eventos de ciberseguridad en un formato estructurado compatible con iniciativas como OpenIOC o STIX, y con funcionalidades como correlación de eventos en base a sus atributos, importación y exportación de estos eventos en distintos formatos (XML, texto plano, OpenIOC, YARA, STIX, CSV, etc.).

El Manual incluye, además de una descripción general de este modelo, distintos aparatados como la *Interfaz de usuario*, el *Uso de Reyes* (creación, visualización y exportación de eventos), las *Categorías disponibles* o la *Exportación automática y manual de eventos*. Del mismo modo, y como anexos, se desarrollan *Ejemplos de peticiones automáticas* e *Integración de REYES con DNS BIND*.

Guías CCN-STIC

Puede encontrarse más información en las siguientes Guías CCN-STIC:

- **Guía CCN-STIC-423 Indicadores de Compromiso**, que muestra las herramientas existentes para identificar indicadores de compromiso (IoC), así como los pasos que se deben dar para actuar frente a amenazas desconocidas. También se

muestran las etapas necesarias para compartir estos ficheros de inteligencia en la plataforma disponible REYES , así como los pasos de creación y exportación de manera manual.

- **Guía CCN-STIC-424 Intercambio de Información de Ciberamenazas**. STIX-TAXII, que presenta las últimas tendencias en materia de compartición de la información y de los estándares más utilizados en el sector (STIX, TAXII) así como las numerosas ventajas de su uso para la mejora de las capacidades defensivas de una organización. Se ofrece, además, un caso práctico de uso con la herramienta REYES en el que se pueden seguir las operaciones básicas – como importar y exportar inteligencia -, todo ello basado en un ataque conocido.
- **Guía CCN-STIC-425 Ciclo de Inteligencia y Análisis de Intrusiones**, cuyo objeto es ofrecer una explicación, simple y concisa, de lo que en ciberseguridad constituye la llamada Ciberinteligencia y el Ciclo de Inteligencia, desarrollando una de sus fases más significativas: el Análisis. Con este propósito se desarrolla un Modelo para el Análisis Formal de Intrusiones.
- **Guía CCN-STIC-426 REYES.** Manual de Usuario. Esta Guía recoge los principales aspectos de la herramienta REYES como plataforma desplegada por el CCN-CERT para el intercambio de información y conocimiento sobre ciberamenazas.

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del ENS.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, a sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/
@CCNCERT

LinkedIn

YouTube http://youtu.be/5XxS9mZZfKs

COMUNICADO CCN-CERT

27 de enero de 2016