

Últimas noticias

Ya está disponible REYES, la plataforma del CCN-CERT para compartir información sobre ciberamenazas

11 Marzo 2017
por Redacción

La plataforma REYES, desarrollada por el CCN-CERT, agiliza la labor de análisis de incidentes al obtener información contextualizada y correlada con las principales fuentes de información existentes, tanto públicas como privadas. En su primera fase, está destinada a las organizaciones adheridas al Sistema de Alerta Temprana (SAT) del CERT Gubernamental Nacional.



El acceso a la plataforma está restringido a organizaciones que cuentan con un certificado del SAT-INET

Así, realizar una investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes es el principal objetivo de REYES, la herramienta desarrollada por el CCN-CERT y disponible, en su última versión, para las organizaciones adscritas al Sistema de Alerta Temprana, SAT.

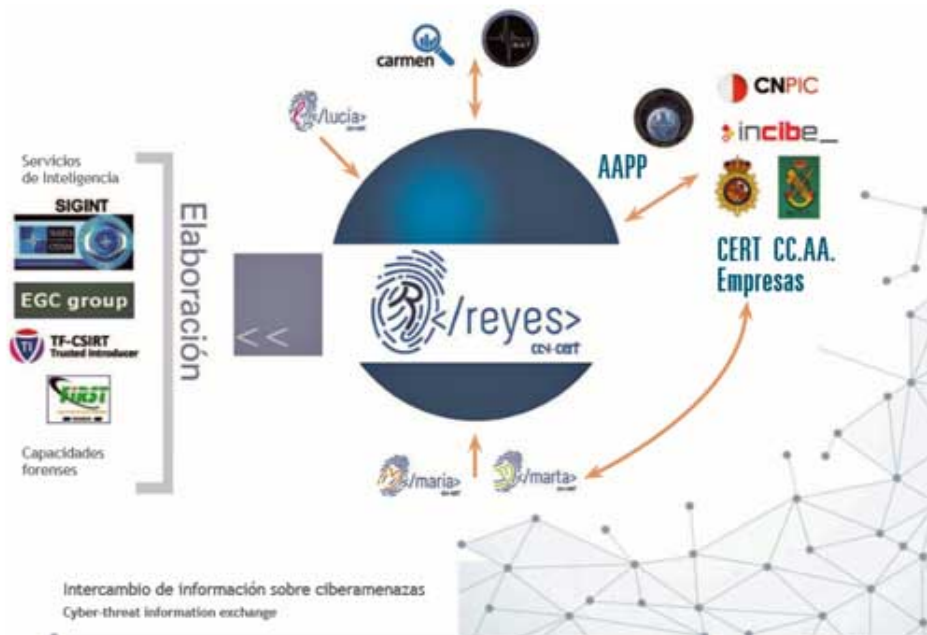


REYES está federada con organismos internacionales y recoge información de multitud de fuentes especialistas en ciberamenazas, contiene atributos y eventos malware contextualizados y permite la interacción con otras herramientas de análisis

Acceder a todo tipo de listas negras relacionadas con incidentes (APT, botnet, malware, ransomware, spam o TOR); entrar en otras herramientas como MISP (Malware Information Sharing Platform, a su vez federada con otras organizaciones como OTAN, FIRST, EGC y otros CERT), MARTA o el propio SAT y su gestor de reglas son algunas de las posibilidades que ofrece esta nueva plataforma con la que se pretende agilizar la labor de análisis y resolución de ciberincidentes, así como la compartición de información entre distintas organizaciones.



Además, existen distintos aspectos que hacen de REYES una herramienta única como son el que está federada con organismos internacionales y recoge información de multitud de fuentes especialistas en malware, así como que contiene atributos y eventos de malware contextualizados, permite la interacción con otras herramientas de análisis y realiza automáticamente la correlación entre los distintos elementos de ciberinteligencia que contiene.



REYES está basada en la tecnología MISP que implementa la plataforma de intercambio de ciberinteligencia

La herramienta está basada en la tecnología MISP (Malware Information Sharing Platform), un sistema ya funcional y utilizable por las organizaciones para implementar una plataforma para intercambio de ciberinteligencia.

Puesto que su principal caso de uso es el de intercambio de información, la herramienta está especialmente ideada para ofrecer un modo de intercambio para distintas organizaciones que internamente generan ciberinteligencia.



Inicialmente fue desarrollada por las fuerzas armadas belgas pero desde 2012 se ha cedido abiertamente a la comunidad con una licencia de código abierto y participan diversos equipos de respuesta a incidentes como NATO NCIRC, CIRCL, y CERT-EU



Los usuarios del sistema tienen por tanto la oportunidad de facilitar y consumir elementos de ciberinteligencia.

Inicialmente fue desarrollada por las fuerzas armadas belgas pero desde 2012 se ha cedido abiertamente a la comunidad con una licencia de código abierto y participan diversos equipos de respuesta a incidentes como NATO NCIRC, CIRCL y CERT-EU.

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.).

Hay que señalar que el acceso a esta plataforma está restringido a todas aquellas organizaciones que cuentan con un certificado del SAT-INET (con las mismas credenciales) y se realiza a través del enlace: <https://reyes.ccn-cert.cni.es>

Más información sobre esta plataforma y las distintas Guías CCN-STIC en www.ccn-cert.cni.es/herramientas-de-ciberseguridad/reyes.html

<http://www.techweek.es/seguridad/noticias/1017745004801/ya-disponible-reyes-plataforma-ccn-cert-compartir-informacion-ciberamenazas.1.html>