Acceso y Uso de la Plataforma MISP para el Sector Eléctrico

Una guía completa para el registro y reporte de eventos

Introducción

La plataforma MISP (Open Source Threat Intelligence and Sharing Platform) es una herramienta esencial para el intercambio de inteligencia de amenazas, indicadores de compromiso (IoC) y otros datos relevantes dentro de comunidades de confianza. En el sector eléctrico, el CSIRT0 facilita este intercambio de información a través de la plataforma MISP, permitiendo una detección más rápida de ataques dirigidos y mejorando la tasa de detección, al mismo tiempo que se reducen los falsos positivos.

Solicitud de Acceso a la Plataforma MISP

Para que las empresas del sector eléctrico puedan vincularse al CSIRT0 a través de la plataforma MISP, es necesario seguir un proceso específico de solicitud de acceso. A continuación, se detallan los pasos a seguir:

- Enviar un correo electrónico a isoc@xm.com.co con los siguientes datos:
- Nombres completos.
- Correo electrónico corporativo.
- Clave pública PGP (consultar el manual de PGP para generarla).

Una vez validada la información, se suministrarán los datos de acceso a la plataforma MISP mediante correo electrónico, junto con las siguientes guías:

- Guía para el reporte de eventos en MISP
- Guia para la extracción de IOCs de correos phishing

Generación de la Clave Pública PGP

Como prerrequisito para el registro en la plataforma MISP, es necesario generar una clave pública PGP. Para ello, se recomienda seguir las instrucciones detalladas en el “Manual de uso de GPG4WIN_V4-4 en Windows y creación de llaves para el MISP”.

Reporte de Eventos en la Plataforma MISP

- Una vez que se tiene acceso a la plataforma MISP, es fundamental conocer el proceso para reportar eventos e indicadores de compromiso (Docs.). Para ello, se debe consultar la “ Guía para el reporte de eventos en MISP”, que proporciona

instrucciones detalladas sobre cómo crear eventos, añadir atributos y publicar la información.

Conclusión

El acceso y uso adecuado de la plataforma MISP es crucial para mejorar la ciberseguridad en el sector eléctrico. Siguiendo las instrucciones detalladas en esta guía y consultando los documentos de referencia, las empresas pueden integrarse eficazmente al CSIRT0 y contribuir al intercambio de inteligencia de amenazas, fortaleciendo así la seguridad de toda la comunidad.