

Cifrado de datos y comunicaciones

The Fraud Explorer cifra los datos en tránsito y en reposo con diversos algoritmos y mecanismos. El agente envía los datos a la consola en nube o local a través de protocolos TCP y UDP y para cada uno de ellos se tiene cifrado AES-128, además de capas adicionales de protección como la de HTTPS. Una vez los datos están en reposo, se mantienen cifrados en las bases de datos.

Debido a la gran cantidad de datos y a la velocidad con los que estos ingresan a la plataforma para ser analizados, el mecanismo de cifrado y descifrado de datos elegido tuvo que ser cuidadosamente implementado para evitar la saturación de los recursos usados para encriptar y desencriptar.

Es por ello que se eligió el algoritmo de cifrado AES-128 y no AES-256, porque éste último necesita de mucha más potencia computacional, en cambio AES-128 es perfecto para operaciones de alta demanda y ofrece un excelente cifrado para propender por la seguridad de la información.

Además de cifrar los datos antes de ser enviados, estos son transmitidos usando un canal seguro que también cuenta con cifrado, es decir, nuestra solución usa un **doblo cifrado de datos**.

Una vez estos datos cifrados llegan a **The Fraud Explorer**, el algoritmo se encarga de descifrarlos y procesarlos para tratar de encontrar en ellos indicios de comportamientos anti éticos. En caso de que se encuentren, se genera una alerta que a su vez sigue estando cifrada en reposo en el motor **Elasticsearch**.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Este software está siendo desarrollado por [NOFRAUD.la](#). Este contenido es privado y únicamente está disponible para clientes de NOFRAUD. Está prohibida su publicación en fuentes abiertas o disponibles al público.

Revision #6

Created 10 December 2024 23:03:12 by Julian Rios

Updated 23 July 2025 03:11:48 by Julian Rios