Temas candidatos para proyecto final

GESTIÓN DE PROYECTOS DE CIENCIA DE DATOS

Mitsiu Alejandro Carreño Sarabia - E23S-18014

Detección de anomalías de tráfico en servidores web

Tema:

Detección de anomalías de tráfico en servidores web

Título:

Desarrollo de sistema de detección y alerta de anomalías en tráfico de servidores web basado en aprendizaje automático

Detección de anomalías de tráfico en servidores web

Objetivo general:

Desarrollar una solución integral de monitoreo y detección de tráfico anómalo mediante la implementación de técnicas de aprendizaje automático para decidir las acciones preventivas y/o correctivas necesarias.

Detección de anomalías de tráfico en servidores web

Preguntas de investigación / Objetivos específicos:

- ¿De qué manera se analiza el tráfico web actualmente?
- Analizar las técnicas y procesos tanto tradicionales como de aprendizaje automático mediante los cuales se analiza tráfico web actualmente

Detección de anomalías de tráfico en servidores web

Preguntas de investigación / Objetivos específicos:

- ¿Qué elementos debe tener un sistema de alertas para ser útil (falsos negativos/falsos positivos, canales de comunicación, protocolos extras)?
- Enumerar las características y casos de uso de sistemas de monitoreo y alerta efectivos

Detección de anomalías de tráfico en servidores web

Objetivos específicos:

- Desarrollar un sistema detección de anomalías basado en aprendizaje automático

Justificación:

- Analizar los registros de tráfico web permite no solo entender la manera en que se consume la información que contiene un servidor, sino también detectar si el uso generalizado se transforma, o si existen anomalías que pueden ser malintencionadas. Dado el volumen de información que se genera, y la creciente sensibilidad de los datos alojados, aplicar herramientas de aprendizaje automático permitirá agilizar y perfeccionar cualquier proceso manual.