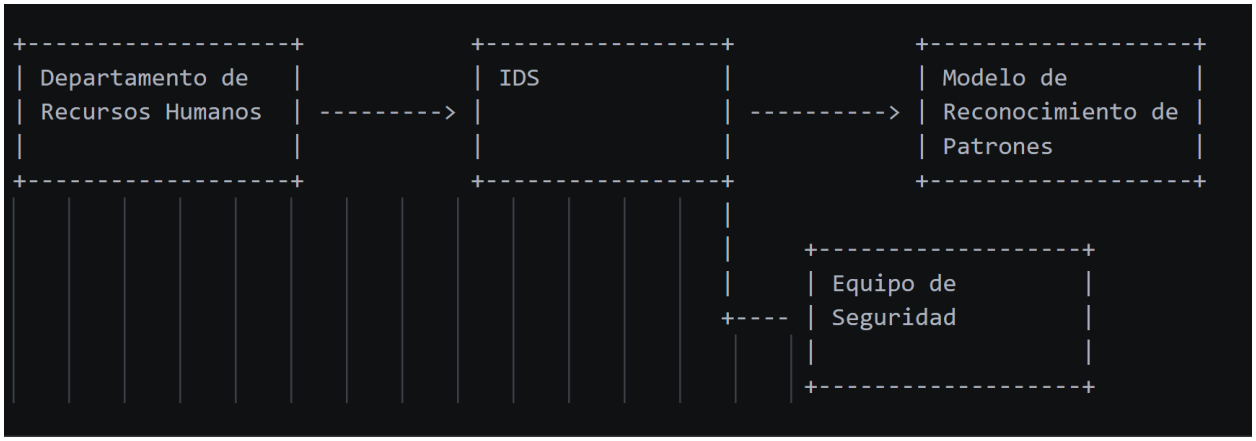
El laboratorio de ciberseguridad de una empresa necesita analizar los paquetes de red enviados entre el departamento de
Recursos humanos y el departamento de ventas, aplicando un modelo de reconocimiento de patrones para identificar
posibles anomalias de seguridad. Describe con palabras y diagramas que solucion propone y porque.
Tome en cuenta factores como rendimiento tiempo y de desarrollo en su proquesta.

PROPUESTA

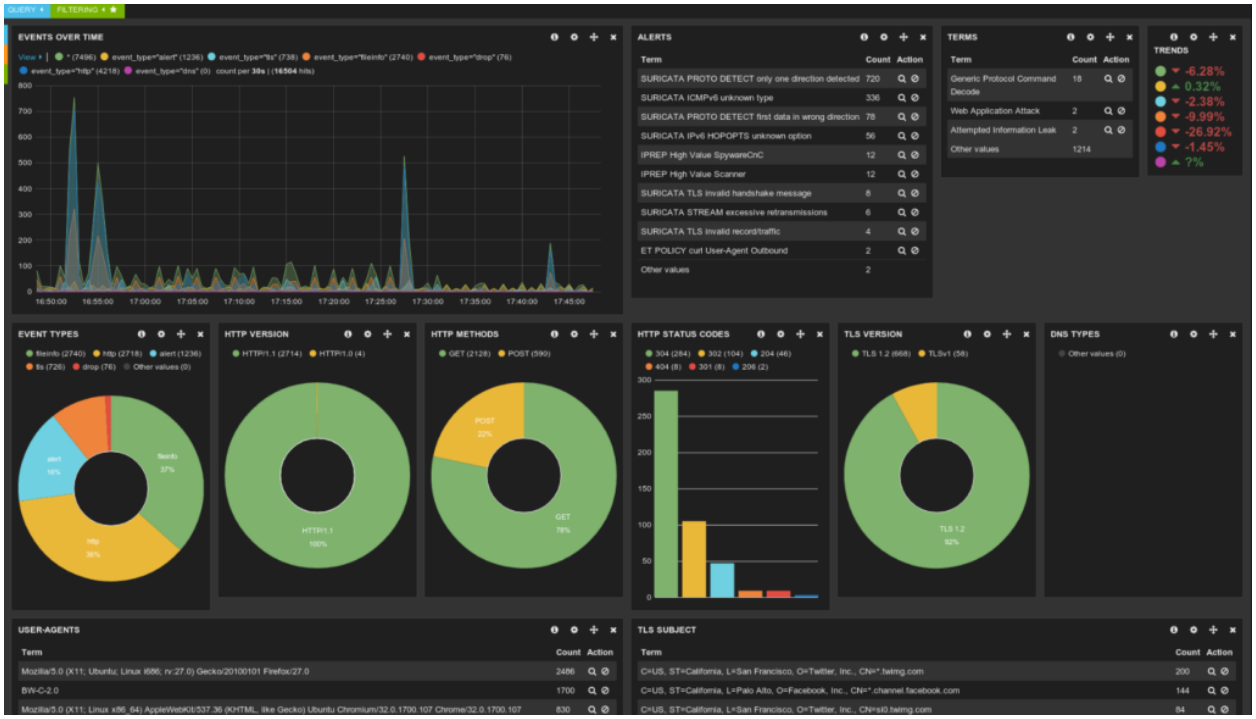
El IDS sería implementado como una solución de software que monitorearía el tráfico de red en tiempo real y aplicaría algoritmos de análisis de patrones para identificar posibles anomalías de seguridad. Estas anomalías podrían incluir comportamientos sospechosos, intentos de intrusión o actividades maliciosas en la red.



El tiempo de pleaneacion seleccion y desarrollo sera de 7 meses, con un equipo altamenete motivado coformado por 15 personas.

Tomando en cuenta factores de rendimoneto tenememos falsos postivos, dataset desbalanceados, tiempos de respuesta lentos, nivel de deteccion bajo.

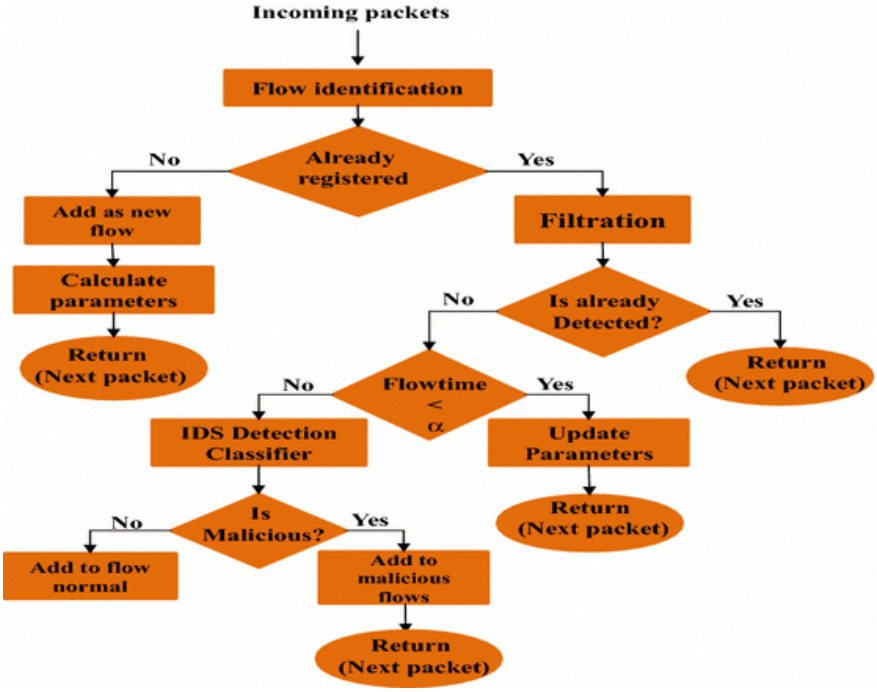
Propuesta de interface de IDS



El modelo de reconocimiento de patrones se basará en técnicas de aprendizaje automático y análisis estadístico para identificar patrones normales y anómalos en la comunicación entre los dos departamentos. El modelo se entrenará utilizando datos históricos de tráfico de red legítimo y se le proporcionará una etiqueta para distinguir entre tráfico normal y tráfico malicioso/anómalo.

Una de las principales ventajas de utilizar un modelo de reconocimiento de patrones en el IDS es su capacidad para aprender y adaptarse a nuevos patrones de amenazas a medida que se descubren. Esto significa que el sistema puede mejorar su eficacia con el tiempo a medida que se exponga a más datos y patrones de tráfico de red.

Tomemos como referencia este algoritmo que se usara como base para la implementacion.



En resumen, la solución propuesta utiliza un enfoque combinado de un IDS y un modelo de reconocimiento de patrones para analizar y detectar posibles anomalías de seguridad en los paquetes de red enviados entre los departamentos de Recursos Humanos y Ventas. Esto proporciona una detección avanzada de amenazas y patrones anómalos, sin comprometer el rendimiento de la red y permitiendo un desarrollo escalable.