CYBER DEFENSE AUTOMATION AND ANALYSIS FRAMEWORK

OBJETIVO GENERAL

Desarrollar un sistema de automatización integrado que mejore la eficiencia y efectividad del Centro de Operaciones de Seguridad (SOC) mediante el uso de APIs y herramientas de Big Data para un análisis y reporte integral de sus mejores prácticas, insights y utilidades.

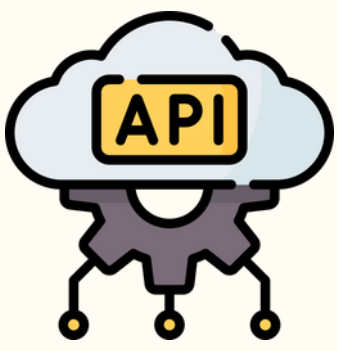
OBJETIVOS ESPECIFICOS

1 INVESTIGAR

Identificar y analizar las capacidades de las APIs de cada herramienta de ciberseguridad seleccionada, realizando revisiones de documentación y pruebas de funcionalidad, para entender mejor las capacidades de las herramientas y optimizar su uso.

2 SCRIPTS PY

Establecer conexiones API con las herramientas de seguridad seleccionadas, implementando protocolos y métodos de autenticación adecuados, para garantizar una integración fluida y eficiente que permita la recolección de información.



3 REPORTES

Desarrollar un formato estándar para los reportes basado en los datos extraídos, creando plantillas con secciones predefinidas, para asegurar que los reportes sean claros, coherentes y faciliten la toma de decisiones informadas.

4 DASHBOARDS

Realizar visualización de los datos mediante el uso de Looker Studio, creando dashboards interactivos que permitan el análisis visual y la identificación de patrones en la información, para mejorar la interpretación y la toma de decisiones basadas en los datos presentados.

5 DOCUMENTACIÓN

Documentar las mejores prácticas de las herramientas de seguridad del proyecto en GitHub, recopilando información y experiencias relevantes, para proporcionar un recurso accesible que optimice su uso y facilite el aprendizaje del equipo y otros interesados.