PUCE Virtual

DOCUMENTO DE PROFUNDIZACIÓN

Estructura de Datos

Estudio de caso 1: Preparación de un Proyecto para implementar un sistema de Análisis de Seguridad

Estudio de caso 1: Preparación de un Proyecto para implementar un sistema de Análisis de Seguridad

Contexto

Una institución educativa en Quito ha incrementado el uso de plataformas digitales (aulas virtuales, sistemas administrativos y redes internas). Esto ha generado un aumento en la cantidad de datos y eventos de seguridad, sin contar con un sistema eficiente para su monitoreo y análisis.

Problema

La institución presenta varias debilidades:

- No existe un sistema centralizado de monitoreo de seguridad.
- Los registros (logs) no se analizan en tiempo real.
- Se han detectado accesos sospechosos sin una respuesta oportuna.
- El sistema actual no es escalable ni fácil de mantener.

Solución Propuesta

Diseñar e implementar un sistema de análisis de seguridad basado en:

- Recolección y centralización de logs.
- Análisis algorítmico eficiente (búsqueda, detección de patrones).
- Uso de grafos para representar relaciones en la red.
- Arquitectura modular que garantice escalabilidad y mantenibilidad.

Estrategia:

- Implementar el sistema de forma incremental (por módulos).
- Priorizar la detección de accesos no autorizados.
- Utilizar estructuras de datos eficientes (listas, árboles, grafos).
- Incorporar reglas dinámicas para facilitar actualizaciones.
- Validar cada fase mediante pruebas funcionales.

Implementación

Para la implementación de la solución se lo realiza en 6 fases:

Fase 1: Recolección de logs desde servidores y red.
Fase 2: Centralización de datos en un sistema único.

Fase 3: Análisis mediante algoritmos eficientes (búsqueda y detección).
Fase 4: Modelado de la red con grafos para identificar patrones de ataque.
Fase 5: Generación de alertas automáticas.
Fase 6: Monitoreo continuo y mejora del sistema.

Se utiliza **Python** para el desarrollo inicial, con código modular y escalable.
Resultados e Impacto en ciberseguridad

Una vez ejecutadas las fases de implementación se obtienen los siguientes resultados enfocados a la ciberseguridad.

- Reducción del tiempo de detección de incidentes.
- Identificación de accesos sospechosos en tiempo casi real.
- Mejor organización y análisis de los datos de seguridad.
- Mayor capacidad de adaptación ante nuevas amenazas.
- Base sólida para implementar soluciones más avanzadas (SIEM)..

Reflexión Técnica

Este proyecto demuestra que:

- Un buen diseño arquitectónico es clave para la eficiencia del sistema.
- La elección de algoritmos impacta directamente en el rendimiento.
- La escalabilidad y mantenibilidad son esenciales en entornos reales.
- La integración de teoría (algoritmos, estructuras) con práctica permite soluciones efectivas en ciberseguridad.