

DOCUMENTO DE PROFUNDIZACIÓN

Teoría de la Información y la Comunicación

Estudio de Caso Aplicado

Estudio de Caso Aplicado

Análisis del Flujo Informativo en un SIEM Organizacional

Propósito: Aplicar tipos de comunicación y cálculo de entropía en un entorno realista de ciberseguridad.

Contexto del Caso

Una empresa del sector financiero implementa un sistema SIEM que recibe registros de:

- Servidor de autenticación
- Firewall perimetral
- Sistema de correo corporativo

Durante una semana se registraron los siguientes eventos de autenticación:

Evento Frecuencia

Login exitoso 800

Login fallido 200

Actividades

1. Identifique el tipo de comunicación predominante entre el servidor y el SIEM.
2. Modele la fuente como variable aleatoria discreta.
3. Calcule la probabilidad de cada evento.
4. Determine la entropía del sistema.
5. Interprete si la incertidumbre es alta o baja.
6. Analice qué ocurriría si los intentos fallidos aumentan a 400.