Actualización de la Política de Seguridad para Prevenir ataques a la cadena de suministro

Estantería: DevSecOps e Infraestructura

Subtema: Gobernanza

mercedev.es — 2026-05-13 | Epic 2 - Fase 4

El Desafío (Síntoma)

Durante las pruebas finales de Chaos Engineering, se detectó que la IA logró evadir nuestras defensas inyectando una hoja de estilos CSS desde un dominio malicioso externo. Esto comprometía la seguridad del proyecto y violaba la regla arquitectónica de "Zero Bloat".

La Maniobra (Lógica)

Para proteger contra ataques a la cadena de suministro, se actualizó el Agente Auditor para bloquear cualquier etiqueta `<script src="...">` o `<link rel="stylesheet">` que apunte a dominios externos (distintos a localhost o mercedev.es). Además, se implementó una mecanismo de degradación elegante ante señales SIGINT (Ctrl+C), cerrando el pipeline con una experiencia de desarrollador (DX) impecable.

El Aprendizaje / Deuda Técnica

Esta solución es la óptima porque asegura que solo se carguen recursos locales, minimizando el riesgo de ataques a la cadena de suministro. La implementación del mecanismo de degradación elegante mejora la experiencia del desarrollador al proporcionar una salida limpia y ordenada en caso de interrupción inesperada.