CrowdSec Web UI: Gestión gráfica de CrowdSec

Introducción

CrowdSec Web UI es una interfaz web desarrollada para visualizar y gestionar la información generada por CrowdSec desde un navegador. Permite consultar alertas, decisiones activas, bloqueos manuales y estadísticas operativas sin depender constantemente de `cscli`.

Dentro del stack se sitúa sobre CrowdSec y su Local API (LAPI), proporcionando una capa gráfica para las tareas de supervisión y administración habituales.

Enfoque general

La aplicación se comunica directamente con la LAPI utilizando una cuenta de tipo *machine* registrada específicamente para este propósito.

A diferencia de una interfaz que consulta CrowdSec en tiempo real para cada operación, CrowdSec Web UI mantiene una base de datos SQLite local donde almacena alertas y decisiones sincronizadas desde la LAPI. Esto reduce el número de consultas necesarias, mejora el rendimiento de búsqueda y permite conservar histórico local incluso después de reinicios o actualizaciones del contenedor.

La arquitectura se compone de un frontend React y un backend Node.js que actúa como intermediario entre la interfaz y CrowdSec.

Desarrollo

Qué se hizo y por qué

Se desplegó CrowdSec Web UI mediante Docker como interfaz de administración para la instalación existente de CrowdSec.

La autenticación contra la LAPI requiere una identidad propia dentro de CrowdSec. Para ello se creó una nueva máquina denominada `crowdsec-web-ui` utilizando una contraseña dedicada:

```
sudo cscli machines add crowdsec-web-ui \
  --password CONTRASEÑA_SEGURA \
  -f /dev/null
```

La opción `-f /dev/null` evita que CrowdSec sobrescriba el fichero local de credenciales utilizado por la propia instalación. Su única función es registrar la nueva máquina en la base de datos interna para que posteriormente pueda autenticarse contra la LAPI.

La aplicación se configuró utilizando autenticación mediante usuario y contraseña, conectándose directamente a la API local de CrowdSec.

Para conservar el histórico y la información sincronizada se habilitó almacenamiento persistente sobre la ruta `/app/data`, donde la aplicación mantiene su base de datos SQLite y el resto de datos operativos.

Configuración utilizada

Repositorio en Gitea

Validación

La validación del despliegue se realizó verificando:

- Conectividad entre CrowdSec Web UI y la LAPI.
- Autenticación correcta mediante la cuenta `crowdsec-web-ui`.
- Sincronización de alertas y decisiones existentes.
- Creación de bloqueos manuales desde la interfaz.
- Persistencia de la información tras reiniciar el contenedor.
- Actualización automática del histórico almacenado en SQLite.

Decisiones importantes

CrowdSec Web UI no incorpora ningún mecanismo de autenticación propio. El acceso a la interfaz debe protegerse mediante un sistema externo cuando se publica detrás de un reverse proxy.

La aplicación mantiene una copia local sincronizada de la información obtenida desde CrowdSec. Esto mejora notablemente la velocidad de consulta, especialmente en instalaciones con grandes volúmenes de alertas o múltiples máquinas protegidas.

El uso de una cuenta específica para la interfaz evita reutilizar las credenciales internas de CrowdSec y permite aislar el acceso a la LAPI de forma más limpia.

Resumen breve

CrowdSec Web UI añade una capa gráfica sobre CrowdSec para consultar alertas, administrar decisiones y supervisar la actividad detectada por el motor de seguridad. Utiliza una cuenta dedicada para acceder a la LAPI y mantiene una base de datos SQLite local para mejorar rendimiento, escalabilidad y conservación del histórico.

Referencias

- Repositorio oficial de CrowdSec Web UI
- Documentación oficial de CrowdSec

Revision #1
Created 2026-06-03 20:26:05 UTC by Juan Francisco
Updated 2026-06-03 20:40:28 UTC by Juan Francisco