cso

cso

> *Catalogue généré le 2026-05-11*

En une phrase

Mode « Chief Security Officer » : Claude audite ton projet à la recherche de failles de sécurité, secrets exposés, dépendances vulnérables et risques d'attaque.

Quand l'utiliser

- Avant de déployer une application sensible (qui touche à de l'argent, des données personnelles, de l'auth)
- Quand tu veux vérifier qu'aucun mot de passe ou clé API ne traîne dans ton historique git
- Quand tu veux un audit OWASP Top 10 (les dix grandes catégories de vulnérabilités web)
- Après avoir ajouté de nouvelles dépendances, pour vérifier qu'elles ne contiennent pas de failles connues
- Périodiquement (par exemple chaque mois) pour suivre l'évolution de la sécurité de ton projet

Comment l'invoquer

- **Slash command** : `/cso` (à taper dans Claude Code)
- **Voice triggers** : « see-so » · « see so » · « security review » · « security check » · « vulnerability scan » · « run security »
- **Phrases déclencheurs (texte)** : "security audit" / "threat model" / "pentest review" / "owasp review" / "CSO review"

- **Auto-invocation** : Sur demande explicite

Description détaillée

`/cso` lance un audit de sécurité à la fois sur ton code et sur ton infrastructure. Le skill détecte d'abord ton stack technique (Node, Python, Ruby, Go, etc.) puis cartographie la surface d'attaque : endpoints publics, routes authentifiées, points d'upload de fichiers, intégrations externes, webhooks, jobs en arrière-plan.

Il enchaîne plusieurs phases. **Archéologie des secrets** : il fouille l'historique git pour repérer les clés AWS (`AKIA…`), clés OpenAI (`sk-…`), tokens GitHub, etc. qui auraient pu être commit par erreur. **Chaîne de dépendances** : il lance `npm audit` ou équivalent, repère les scripts d'install suspects dans tes dépendances de production. **Pipeline CI/CD** : il vérifie tes workflows GitHub Actions (actions non pinnées, `pull_request_target` dangereux, injection de scripts). **OWASP Top 10 + STRIDE** : injections SQL, XSS, CSRF, contrôles d'accès cassés, etc.

Deux modes existent. **Daily** est silencieux (signale seulement à 8/10 de confiance, zéro bruit). **Comprehensive** est l'audit mensuel approfondi (à 2/10, tout sort). Tu peux aussi cibler des sous-périmètres : `--infra`, `--code`, `--skills`, `--diff` (limité aux changements de ta branche). À chaque exécution, les résultats sont stockés pour suivre les tendances dans le temps.

Source

- **Plugin** : `gstack`
- **Nom interne** : `cso`
- **Fichier** : `/home/thymon/.claude/skills/gstack/cso/SKILL.md`

Revision #2
Created 2026-05-11 21:18:54 UTC by thymon
Updated 2026-05-11 21:36:36 UTC by thymon