

# DevSecOps : Sysdig unifie la sécurité cloud et conteneurs

L'éditeur logiciel Sysdig [a annoncé](#) enrichir sa plateforme de supervision [DevOps](#) d'une gestion de la posture de sécurité cloud (CSPM, cloud security posture management).

Cette capacité CSPM est basée sur [Cloud Custodian](#), une librairie open source qui permet de définir des règles de conformité et des contrôles de sécurité.

L'outil est compatible avec les principaux clouds publics.

Sysdig dit proposer gratuitement cette fonctionnalité CSPM pour un même compte cloud. L'entreprise ambitionne ainsi d'encourager les équipes DevSecOps à l'utiliser, et ce en complément des capacités de supervision basées sur Falco. Un moteur de détection d'intrusion open source en environnement Kubernetes, dorénavant porté par [la CNCF](#).

## Faire obstacle au mouvement latéral

Le but est de proposer aux utilisateurs de [Sysdig Secure DevOps Platform](#) une sécurité « unifiée » pour les conteneurs, Kubernetes et Linux, et les services cloud.

Il s'agit notamment de réduire la marge de manoeuvre d'attaquants informatiques qui utilisent le [mouvement latéral](#) et l'escalade des privilèges pour tenter d'accéder à des comptes sensibles. Les équipes en charge doivent pouvoir étudier le chemin emprunté par l'acteur malveillant, du point d'ancrage d'origine aux différentes étapes du parcours.

Sysdig veut ainsi fournir une solution qui permette d'identifier « toute la chaîne d'attaque » plus rapidement, pour réduire « de quelques semaines à quelques heures le temps de détection des menaces à travers les clouds et les conteneurs », a déclaré la firme.