

Netflix : l'armée des singes Open Source pour gérer une infrastructure AWS

Le plus gros client mondial d'Amazon Web Services, Netflix, a mis à disposition de tous, [sur GitHub](#), l'outil spécifique qu'il a développé pour **superviser la sécurité de son infrastructure Cloud**. Opérationnelle depuis 2011 (dans sa première version), cette solution de sécurité, de monitoring et d'analyse, appelée **Security Monkey**, vise à améliorer la connaissance des changements et risques sur un environnement AWS. C'est d'ailleurs en raison des lacunes d'AWS sur la traçabilité des changements et sur l'évaluation des risques que Netflix a décidé de se lancer dans le développement de Security Monkey il y a quatre ans.

D'autant que la société américaine, qui prépare son arrivée en France, est confrontée à des problématiques particulières. Sur la plate-forme du service de streaming, **du code est déployé des milliers de fois par jour** modifiant les paramètres de configuration selon le même rythme, explique l'équipe de sécurité de Netflix dans un [billet de blog](#). Cette dernière souhaitait donc mesurer comment ces changements affectaient la sécurité de la plate-forme.

Enregistrer les configurations de S3, IAM et EC2

Security Monkey **supervise les configurations de l'infrastructure Cloud** et y détecte d'éventuelles anomalies et risques. La solution se décompose en 3 modules : **Watcher** qui détecte et enregistre des changements de configurations dans les environnements AWS S3, IAM et EC2; **Notifier**, un système d'alerte; et **Auditor**, qui rapproche les règles métier des configurations AWS pour isoler des divergences et détecter des risques. S'y ajoute un système de gestion de règles, que les utilisateurs peuvent enrichir. Security Monkey fonctionne sur Ubuntu Linux et OS X.

Security Monkey rejoint **la Simian Army** (l'armée simiesque), une **suite d'outils développés par Netflix** pour tester la fiabilité, la sécurité ou la résilience d'AWS. Ces outils (Chaos Monkey, Latency Monkey, Conformity Monkey, Doctor Monkey, Janitor Monkey...) sont disponibles pour la plupart en Open Source.

Signalons que AWS propose ses propres outils de supervision de la sécurité (le service d'audit CloudTrails ou l'outil d'optimisation TrustedAdvisors, ce dernier étant encore en bêta). Mais, pour l'équipe de sécurité de Netflix, si AWS « *fournit une excellente visibilité sur les systèmes et configurations, les capacités qu'il offre en matière de surveillance des changements et d'évaluation sont limitées* ».

En complément :

[La mutuelle Smatis migre l'intégralité de son informatique sur AWS](#)

[Cloud : plus d'un milliard par trimestre pour AWS](#)

[Comment Sodexo cuisine AWS](#)