Les impacts de la cloudification sur la surveillance opérationnelle

Laurent Cordival, Florian Boudot

Beijaflore, 13 Avenue du Recteur Poincaré, 75016 Paris, France
Lcordival073@beijaflore.com

Abstract.

Les évolutions technologiques, comme la conteneurisation et les micro-services ainsi que les changements de pratique (VM éphémères, DevOps etc…) sont autant de changements auxquels les centres de sécurité opérationnelle (SOC) doivent faire face.
Afin de maintenir la qualité de leur dispositif de cyberdéfense, les responsables sécurité et responsables SOC doivent gérer les impacts de l'utilisation de service Cloud. Cette adaptation est un premier changement dans les procédures et outils des SOC. Une deuxième adaptation encore plus structurante est à prendre en compte avec l'utilisation très fréquence de multiples fournisseurs de services cloud.
Les difficultés d'adaptation des processus et d'organisations aux clouds par les grands comptes compliquent la tâche du SOC, bien que l'intégration des applications cloud dans son périmètre soit une étape indispensable à la sécurisation du système d'information.
Pour pallier à ces problématiques, ainsi qu'au modèle multi-cloud, les SOCs s'adaptent et se tournent vers les capacités de surveillance dont disposent les CSP. Ces services ne suffisent pas à établir une surveillance complète, mais permet au SOC de se concentrer davantage sur le déploiement d'outil de surveillance applicative et de gestion des accès (CASB, CMS).
Les évolutions et travaux entrepris par les CSP tendent vers la standardisation des services de détection, une modélisation des alertes détectés et le développement d'interface d'investigation pour les clients chez les fournisseurs.

Keywords:
SOC, SIEM, Puits de données, sondes de détection, CASB, intégration de service cloud, CSP, SaaS, cyber défense, Machine Learning