SIEM as a Service : la surveillance du SI bascule dans le Cloud

L'ouverture sur le Cloud, mais aussi au télétravail poussent de nombreuses entreprises à vouloir rehausser le niveau de sécurité de leur système d'information. Passer au stade supérieur implique la mise en place d'un SIEM, un projet traditionnellement long et couteux, que les offres « As a Service » cherchent à accélérer.

Véritable moteur du SOC, le SIEM (Security Information and Event Management) est une brique de sécurité qui se montre de plus en plus indispensable dans la protection du système d'information. Vers lui convergent toutes les données de fonctionnement des serveurs, des équipements réseaux et, de plus en plus, des postes de travail.

Le SIEM traine néanmoins une image de solution à la fois coûteuse en termes d'infrastructure, de licencing, mais aussi complexe à mettre en place.

Le « Move to Cloud » impacte la sécurité du SI

Cependant, le Cloud est en train de rebattre les cartes. Ainsi, la Forrester Wave publié par le cabinet américain au dernier trimestre 2020 mettait un acteur historique de ce marché IBM Security au coude à coude avec Splunk et Microsoft, des acteurs qui bousculent clairement le marché avec des offres « Cloud native ».

IBM, éditeur du SIEM QRadar, a bien évidemment perçu cette évolution du marché. « L'extension du périmètre à surveiller au Cloud public plaide en faveur du « SIEM as a Service » car les volumes de données de log ne cessent de croitre et l'élasticité du Cloud convient à merveille à la création de puits de logs de grande taille. » explique Guillaume Greber, Security Sales Leader chez IBM.

« De même que les algorithmes d'IA, de plus en plus indissociables de l'analyse des logs nécessitent beaucoup de ressources machine qu'ils peuvent trouver à foison dans le Cloud. » Outre une simplification de son pricing, IBM mise sur une stratégie hybride avec un logiciel qui peut être déployé en on-premise, installé sur un Cloud comme AWS ou Azure ou encore l'offre SaaS d'IBM Security : QRadar on Cloud. IBM Security a redéveloppé son SIEM historique pour le rendre beaucoup plus facile à déployer sur n'importe quel Cloud sous forme de conteneur.

Autre éditeur de SIEM On-Premise, LogPoint dont la version SaaS est sortie en fin d'année. Laurent Gentil, Enterprise Business Developer + Sales Engineering South EMEA chez l'éditeur souligne :
« Nous préparons notre offre SaaS mais notre SIEM exploite déjà le Cloud, notamment le volet UEBA qui consomme des données issues du SIEM et consomme des ressources de calcul dans le Cloud afin notamment de partager les modèles d'apprentissage. »

Celui-ci estime que toutes les entreprises ne vont pas migrer leur SIEM existant vers le Cloud :
« Pour une entreprise qui a un SIEM on-premise, celle-ci n'a pas tellement de raisons de migrer vers une offre « As a Service ». Une infrastructure bien dimensionnée et un bon Capacity Planning

permettent à une plateforme on-premise de continuer à fonctionner pour longtemps alors qu'un projet de transformation va consommer énormément de ressources et d'énergie. »

Des nouveaux entrants venus du Cloud

Les acteurs historiques du SIEM ont vu débarquer une armée de nouveaux entrants avec des offres Cloud. Parmi eux, un éditeur déjà présent d'une façon ou d'une autre dans toutes les entreprises, Microsoft.
L'américain a dévoilé Azure Sentinel en septembre 2019. Il s'agit d'un SIEM dont le développement avait été lancé en 2016 pour les SOC de l'éditeur où il traite 20 milliards d'événements par jour !

Si ce SIEM manquait de connecteurs lors de son lancement, celui-ci évolue rapidement. Avec son intégration étroite avec les services Cloud Azure mais aussi Office 365, Sentinel pourrait bien rafler la mise auprès des entreprises qui ont fait le choix de Microsoft comme fournisseur numéro 1 de leur stratégie « Move to Cloud ».

Pour celles qui privilégient une offre plus indépendante, Splunk semble clairement s'imposer sur le marché. Gartner lui accorde 29% de parts de marché sur les SIEMs, un exploit sur un marché aussi disputé. Pour Matthias Maier, Directeur Marketing Produit, EMEA Sécurité Splunk, la clé de ce succès réside tant dans la technologie délivrée que par la culture d'entreprise avec un fort accent mis sur l'écosystème et la communauté des utilisateurs, les « Splunkers ».

Une démocratisation du SIEM mais pas seulement

Si les grandes entreprises s'intéressent au SIEM dans le Cloud, beaucoup espèrent que le « As a Service » permettra aux ETI de hausser leur niveau de sécurité. C'est la volonté d'un acteur comme AntemetA qui propose une offre de SOC managés s'appuyant sur le SIEM d'Elastic.

Pour Etienne Lecoq, Sales & Marketing Director chez AntemetA, la clé d'entrée de ce marché, c'est l'Open Source mais aussi et surtout l'automatisation : « Aujourd'hui, plus de 80% des actions prises sur notre SOC sont déclenchées de façon automatique sur la base de scénarios et de règles prédéfinies. » L'automatisation est le seul moyen d'accroitre la capacité de réponse des petites entreprises en termes de délais mais aussi en terme économique.

Sur le sujet, lire aussi :

> SIEM : qui sont les principaux fournisseurs ?

> SIEM : qui se détache sur ce marché en densification ?