SIEM : ce que Gartner reproche aux 7 leaders de son Magic Quadrant 2020

Microsoft et Google bouleverseront-ils le marché des SIEM – Security Information and Event Management ou gestion des informations et des événements de sécurité- avec leurs offres cloud lancées l'an dernier ?

Gartner ne l'affirme pas, mais souligne l'intérêt de ses clients pour les offres en question. D'un côté, Azure Sentinel. De l'autre, Backstory, édité par Chronicle, société sœur de Google.

Ni l'une, ni l'autre ne figurent dans le Magic Quadrant que le cabinet américain vient de publier.

Cette édition 2020 distingue 7 « leaders » – tous d'origine américaine – ainsi désignés pour :

– leur aptitude à proposer des produits en accord avec les besoins généraux du marché ;

– leur capacité à développer une base de clients et de revenus.

Leurs solutions respectives ne sont pas exemptes de défauts, d'après Gartner.

1. **Dell Technologies (RSA)**

- Fonctions d'analyse comportementale (UEBA) moins développées que chez les principaux concurrents
- Pas d'offre SaaS (il faut s'appuyer sur des partenaires)
- Plate-forme complexe à déployer pour les entreprises du *mid-market*, dont certains rivaux couvrent mieux les besoins
- Brique SOAR instable : acquis par Palo Alto Networks, Demisto sera à terme remplacé par Threat Connect

2. **Exabeam**

- Activité développée essentiellement en Amérique du Nord : on portera d'autant plus attention à la disponibilité d'équipes à l'international
- Réseau de partenaires en développement
- Difficulté à définir les fonctionnalités pertinentes pour les industries verticales
- Intégration et déploiement à améliorer

Vers des SIEM cloud

3. **IBM**

- Modèles de tarification complexes, avec entre autres de nombreux *add-ons*
- Options limitées pour la collecte de données sur les points de terminaison
- UX en cours de modernisation
- Niveaux d'intégration variables avec les composants tiers

4. **LogRhythm**

- Pas de brique SOAR dédiée
- Architecture en cours de modernisation
- Retard face aux concurrents sur le monitoring IaaS
- Certaines capacités d'IA ne sont proposées qu'en mode cloud

5. **Rapid7**

- Peu de partenaires technologiques / intégration tierces pour le cœur SIEM
- Dépendance à des agents logiciels qui limitent les capacités de collecte de données sur les parcs IoT
- *Core* dépendant d'AWS
- Pistes d'amélioration pour le monitoring des applications

6. **Securonix**

- Certaines fonctionnalités dépendent fortement de partenaires technologiques

- Exécution marketing à améliorer à travers ce réseau de partenaires
- Complexité pour les organisations en dessous d'un certain niveau de maturité
- Expertise nécessaire pour tirer pleinement parti du SIEM

7. **Splunk**

- Rapport qualité-prix
- Contractualisation, support, flexibilité
- Absence de capteurs pour le réseau et les points de terminaison
- Brique UEBA pas encore intégrée au cœur SIEM

Gartner estime à 2,6 milliards de dollars le marché mondial du SIEM en 2018 (contre 2,3 milliards en 2017). La gestion des menaces en est le premier levier. Suivent le monitoring « générique » et la conformité.

Illustration principale via *Shutterstock.com*