La minute de l'expert

Etienne Noiret, Senior Solution Engineer

Vous aviez suivi l'intégration native de Sentinel dans la plateforme Microsoft Defender permettant de piloter toutes les opérations du SOC depuis une console unique, qu'il s'agisse de prévention, détection ou réaction. Vous aviez aussi suivi l'annonce de l'intégration gratuite de Defender Threat Intelligence dans cette même plateforme. Place désormais à la phase suivante : annoncée l'été dernier, « Sentinel platform » est désormais disponible en GA.

Microsoft Sentinel SIEM, la solution de SIEM « cloud native » lancée en 2019 et récemment encore nominée pour la quatrième année de suite comme leader de son segment par le Gartner.

Microsoft Sentinel data lake : c'est le petit nouveau de la bande, qui permet de gérer la problématique de stockage à long terme de données verbeuses à moindre coût. Bon à savoir : toutes les données injectées dans Sentinel SIEM sont automatiquement dupliquées sans surcoût dans le data lake, qui contient donc en un seul endroit 100% des données et sert de stockage long terme (jusqu'à 12 ans), avec un facteur de compression x6 permettant d'économiser d'autant sur les coûts de stockage. Les données peuvent être requêtées à tout moment en KQL en ligne, via des jobs ou au travers de Notebooks pour ceux souhaitant faire de l'analyse avancée.

L'autre bonne nouvelle est liée au fait que Sentinel data lake est construit sur la technologie Microsoft Fabric, et nous apporte ainsi de nouvelles fonctionnalités déjà intégrées dans la plateforme :

- Un **serveur MCP** permet désormais à des agents d'accéder aux données du data lake et d'effectuer des analyses avancées via des interactions en langage naturel. On entre ainsi dans l'ère de l'IA agentique, allez voir ce qui a déjà été publié dans la marketplace.
- **Microsoft Sentinel Graph**, soit un ensemble de capacités permettant de ne plus raisonner de manière silotée mais de construire des graphes de relations entre entités (assets, TI, activités, données). Les premières applications sont déjà disponibles en ligne dans le portail unifié Defender : analyse de chemin d'attaques, analyse de blast radius, hunting à base de graphe, data risk graph dans Purview…

Pourquoi ne pas installer dès maintenant le plugin Sentinel dans Visual Studio et commencer à développer vos propres agents pour transformer votre SOC.