Azure Sentinel : Microsoft renforce son offre de sécurité avec un SIEM

Quelques jours avant la conférence RSA, Microsoft vient de présenter son nouveau service Azure Sentinel. Un module de gestion des informations et évènements de sécurité (SIEM) qui est directement implanté dans le cloud d'Azure.

Ainsi, il sait absorber et analyser de grandes quantités de données issues du cloud, comme celles de la suite Office 365. Il exploite aussi l'intelligence artificielle pour réduire le bruit et extraire les menaces réelles. Les résultats sont compilés dans un tableau de bord basé sur Azure.

Azure Sentinel gère le CEF

Azure Sentinel sait gérer le CEF (Common Event Format), et peut se connecter à d'autres outils de sécurité traditionnels (Check Point, Fortinet, Palo Alto, Symantec…). Pour le moment difficile d'en savoir plus sur Azure Sentinel. On ne connait ni son prix ni ses options, mais l'outil est déjà disponible en preview sur Azure.

En parallèle, Microsoft a également présenté Microsoft Threat Experts, un service qui se greffe à Windows Defender Advanced Threat Protection (ATP) et qui vient en soutien des équipes chargées de la sécurité.

Des experts de Microsoft peuvent analyser les données de sécurité d'un client et l'informer en cas de menaces ou d'intrusion. En complément, ces experts en sécurité peuvent aussi être sollicités par l'entreprise en cas de besoin en envoyant une simple requête. L'outil est également disponible en preview.