Threat intelligence : Thales livre la plateforme Cybels Analytics

Le groupe technologique français Thales a confirmé le lancement de Cybel Analytics. Une plateforme de détection/prévention « en temps réel » d'attaques cyber.

La solution logicielle est basée sur des technologies d'intelligence artificielle (IA) et d'analyse de mégadonnées (Big data) conçues par l'industriel. Elle peut être déployée sur site (dans un centre opérationnel de sécurité – SOC) ou en tant que service dans le cloud.

L'ensemble repose sur l'approche TrUE AI (pour une IA fiable, compréhensible et éthique) promue par Thales. Les algorithmes d'intelligence artficielle proposées par le groupe à ses clients peuvent ainsi être enrichis par les utilisateurs eux-mêmes pour répondre aux besoins spécfifiques de leur organisation. Et ce via l'interface graphique de la solution.

« Cybels Analytics a été développée par nos équipes à partir des contraintes quotidiennes des analystes en cybersécurité : l'augmentation de la masse de données, les délais de détection et d'investigation parfois longs et la difficulté à qualifier des situations non-connues », a déclaré Laurent Maury, vice-président cybersécurité et systèmes d'information critiques chez Thales.

Détection en temps réel et chasse à froid

L'outil est conçu pour s'adapter au contexte métier des utilisateurs de différents secteurs d'activité, défense et aérospatiale en tête. Avec Cybels Analytics, les grands groupes et administrations publiques devraient pouvoir : « gagner du temps dans les phases de détection et d'investigation » d'attaques informatiques, a souligné Thales.

L'entreprise met en exergue les fonctionnalités suivantes de Cybel Analytics :

– la détection en temps réel d'attaques. Une fonction basée sur l'analyse avancée des menaces existantes (en lien direct avec la base de cyber threat intelligence de Thales) ;
– l'identification et la prévention de cyberattaques avancées et inédites (« hunting » ou chasse à froid) à partir de données hétérogènes (réseaux, terminaux, logs…).

L'objectif étant de réduire la durée de détection d'attaques cyber complexes « généralement de plus de trois mois à en moyenne quelques jours », a précisé l'industriel.