

Cyberdefense as a Service, la réponse d'Atheos au ministère de la Défense

La proactivité s'impose pour faire face à l'évolution des menaces qui pèsent sur le système d'information. Ces dernières se font de plus en plus ciblées, ce qui les rend moins détectables dans la masse, et rend par la même les systèmes de défense déployés particulièrement inefficaces.

Le chemin sinueux de la cyberdéfense

Le livre blanc sur la Défense et la Sécurité Nationale, publié voici quelques mois, a défini Internet comme un domaine de confrontation militaire. **Jean-Yves Le Drian**, ministre de la Défense, commentant l'ambition de la politique de sécurité proposée par la publication du livre, a indiqué que l'objectif est « *d'être en mesure d'identifier l'origine des attaques, d'évaluer les capacités offensives des adversaires potentiels et l'architecture de leurs systèmes, et de pouvoir ainsi les contrer.* »

Le ministre pointait directement les systèmes d'information de l'État, mais également « *des opérateurs d'importance vitale et des industries stratégiques* ». Une stratégie qui ne peut que profiter à tous... à condition de disposer des ressources nécessaires pour développer les outils de défense, ce que certains observateurs critiquent, évoquant des effectifs d'experts réduits et la nécessité de les 'professionnaliser', ce qui reporterait l'effet des politiques mises en place à plusieurs années.

Cyberdefense as a Service

L'annonce par Atheos de son offre 'Cyberdefense as a Service', qui sera disponible en septembre, apparaît comme une réponse cinglante aux critiques. L'éditeur propose une solution de surveillance proactive des événements de sécurité du système d'information, disponible en mode SaaS (*Software as a Service*).

L'objectif est de permettre aux entreprises d'accéder à un service – disponible immédiatement et par abonnement, sans investissement préalable – qui détecte les signaux faibles, annonciateurs de potentiels incidents de sécurité.

Dans son communiqué, Atheos présente Cyberdefense as a Service au travers de ses fonctionnalités :

- surveillance périodique de détection des vulnérabilités (externes, internes et fuites d'informations sur Internet) ;
- surveillance permanente des signaux faibles pour déceler les cyberattaques véhiculées au travers des flux mail et web ;
- un framework de reporting unifié basé sur des indicateurs autoporteurs liés à la connaissance de la criticité des actifs ;
- un service d'alerte et de veille pour une notification dans les 24 heures après détection d'un événement ;
- un service d'expertise et d'analyse à la demande pour l'aide aux diagnostics, à la recherche de compromission et à la remédiation ;
- une notation mensuelle de type « AAA » de l'exposition au risque et de son évolution en fonction des métiers du client.

Encore un petit effort...

Atheos n'est pas la première société spécialiste de la sécurité du SI et de l'IAM (*Identity and Access Management*) à proposer une stratégie et des outils de sécurité proactifs. C'est d'ailleurs devenu un domaine en pointe dans le Big Data analytique, par la nécessité de disposer de très gros volumes de données afin de détecter les 'petits' incidents potentiellement porteurs de danger pour le SI.

En revanche, c'est la réactivité de la solution, avec une annonce de « *notification dans les 24 heures après détection d'un événement* », qui nous paraît faible, là où ses concurrents ciblent le temps réel.

C'est certes loin d'être un détail, mais l'on se félicitera de la réactivité de nos entreprises pour répondre aux enjeux de la sécurité de nos systèmes d'information. Et en particulier de la démonstration qu'elles disposent de solutions qui apportent dès aujourd'hui ces réponses, n'en déplaise aux oiseaux de mauvais augure qui oublient que la France dispose d'un réel savoir-faire en la matière.

Crédit photo © jcgjgphotography – shutterstock

Voir aussi

[Silicon.fr étend son site dédié à l'emploi IT](#)

[Silicon.fr en direct sur les smartphones et tablettes](#)