

Cybersécurité : SentinelOne dope Singularity à l'IA

[SentinelOne](#), fournisseur de solutions « autonomes » de sécurité des Endpoints, a dévoilé Singularity, sa plateforme XDR (eXtended Detection and Response) en mode cloud.

Portée par l'intelligence artificielle (IA), l'offre regroupe en une même plateforme des capacités de protection (EPP) et de détection/réponse (EDR) des terminaux, de sécurité de l'Internet des objets (IoT) et de protection des charges de travail dans le Cloud (CWPP).

L'éditeur américain de solutions s'appuie sur ses technologies existantes pour ajouter une couche de sécurité en temps réel à la supervision du réseau et des actifs qui s'y connectent. Le tout est accessible depuis une solution centralisée aux équipes en charge de la sécurité IT.

Les fournisseurs de services managés de sécurité et les responsables de la sécurité des systèmes d'information ([RSSI](#)) sont ciblés.

Regrouper EPP et EDR

« Les RSSI d'aujourd'hui, n'exigent pas plus de données. Ils veulent du contexte et de l'intelligence pour rendre leurs données existantes exploitables et pertinentes », a commenté Tomer Weingarten, CEO et cofondateur de SentinelOne.

Avec Singularity, cette approche s'applique « depuis les postes de travail et les dispositifs IoT, jusqu'aux conteneurs et aux workloads cloud, en passant par les serveurs et les machines virtuelles dans les datacenters », a ajouté le dirigeant.

D'autres fournisseurs de solutions ont fait le choix d'une fusion entre EDR et EPP, dont Palo Alto Networks, Trend Micro, enSilo ([acquis par Fortinet](#)) et bien d'autres.

Tous ambitionnent de proposer aux clients et partenaires des systèmes de détection/protection en temps réel dopés à l'apprentissage automatique pour endiguer le [flot de cybermenaces](#) et distinguer les connexions légitimes de tentatives hostiles.