

Cybersécurité : Sophos s'offre SOC.OS

Sophos poursuit ses [emplettes](#). L'éditeur britannique de logiciels de cybersécurité confirme l'acquisition de [SOC.OS](#), fournisseur d'une solution cloud de triage automatique d'alertes de sécurité. Le montant de l'opération est resté confidentiel.

Basée à Milton Keynes (Angleterre) depuis son lancement en 2020, l'entreprise SOC.OS est une émanation de BAE Systems – Digital Intelligence Solutions. Sa technologie consolide et priorise des volumes élevés d'alertes provenant de multiples produits et de plateformes.

« La fatigue des alertes et le manque de visibilité éreintent les équipes de sécurité partout dans le monde. Le tout sur fond d'évolution constante des cybermenaces et de pénurie de compétences. Ces équipes peuvent s'appuyer sur de nouveaux produits et services innovants pour les aider à résoudre des incidents plus complexes en moins de temps », [a expliqué](#) Dave Mareels, CEO et cofondateur de SOC.OS.

« Pour bon nombre des équipes concernées, cependant, la complexité et le coût des solutions de sécurité classiques font obstacle à leur adoption. En joignant nos forces à celles de Sophos, nous pouvons relever ces défis ensemble, de front. Et fournir des produits et services performants, accessibles et au meilleur coût à ceux qui en ont le plus besoin, à l'échelle mondiale », a-t-il ajouté.

Réponse gérée aux incidents

En acquérant SOC.OS, Sophos veut encore étoffer son portefeuille de solutions MTR (Managed Threat Response) et XDR (Extended Detection & Response).

« Sophos MTR est l'une des nouvelles offres connaissant la plus forte croissance dans l'histoire de la société [...] La demande numéro un d'amélioration de la part des clients porte sur une meilleure intégration avec les environnements de sécurité existants », a déclaré Joe Levy, CTO & Product Officer chez Sophos. « Grâce à la technologie innovante de SOC.OS, nous allons pouvoir précisément répondre [à cette attente] ».

Il s'agit, par ailleurs, d'étendre l'écosystème de cybersécurité ACE (Adaptive cybersecurity ecosystem) de Sophos. « SOC.OS va fournir à notre écosystème un éventail élargi de données télémétriques tierces, offrant aux analystes de sécurité une meilleure visibilité sur les événements et alertes qui importent », a ajouté le CTO. « SOC.OS propose une liste impressionnante d'intégrations qui bénéficieront aux clients et [accompagneront] le développement et l'extension de capacités XDR et MDR leaders sur le marché. Nous sommes donc ravis d'accueillir chez nous l'équipe et la technologie de SOC.OS. »

Sophos, entreprise [détenue par Thoma Bravo](#), le fonds d'investissement américain, envisage d'autres opérations de croissance externe à moyen terme.