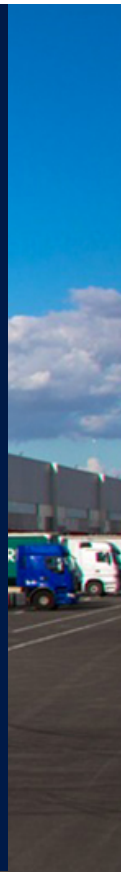
Une protection des données modernisée, autonome et évolutive

Le groupe ID Logistics, prestataire de service dans le domaine de la logistique contractuelle, se positionne comme le numéro 2 en France en nombre de parts de marché. La société, qui vient de fêter ses 20 ans d'existence, est spécialisée dans le transport et la logistique et opère principalement dans les secteurs de l'e-commerce, de la santé et de l'industrie. Elle est présente sur 350 sites répartis dans 17 pays d'Europe, d'Asie, d'Amérique et d'Afrique et compte environ 25 000 collaborateurs.

Selon Bruno Pruneyrac, Directeur de la Production Informatique chez ID Logistics, la société disposait jusqu'en 2021 d'une solution EDR historique qui ne répondait plus à ses besoins en matière de détection et de réponse aux menaces. Elle souhaitait également décharger ses équipes des tâches d'administration de la solution en question. La société a donc décidé de faire évoluer son équipement avec Sophos XDR et de faire appel au service managé Sophos Managed Threat Response (MTR).



CLIENT

ID LOGISTICS

Groupe ID Logistics
DSI ID Logistics

Industrie
Logistique contractuelle

Website
www.id-logistics.com

Nombre de sites
25 000 collaborateurs
Présence dans 17 pays

Solutions Sophos
Sophos XDR
Service Managed Threat Response

"Nous avons construit peu à peu une relation de confiance avec les équipes Sophos, qui disposent aujourd'hui d'une délégation pour prendre des décisions concernant les indicateurs de compromission en notre absence."

Bruno Pruneyrac, Directeur de la Production Informatique du Groupe ID Logistics

Défis pour l'organisation

Moderniser sa solution de sécurité pour répondre à l'évolution des menaces actuelles

Jusqu'au début de l'année 2021 , le groupe ID Logistics disposait d'une ancienne version EDR qui ne répondait plus aux besoins nouveaux de l'entreprise. La société était confrontée à une hausse significative du volume des alertes , probablement due à l'évolution des menaces pendant la pandémie de Covid-19, à la démocratisation du télétravail et à l'extension de sa surface d'exposition en raison de sa croissance.

Occupant un rôle central au sein de la chaîne d'approvisionnement par son activité dans le domaine de la logistique contractuelle, la Direction informatique de ID Logistics a donc décidé de moderniser ses outils de protection en matière de détection et de réponse aux menaces pour protéger au mieux ses systèmes et ses données de tous types de menaces.

En tant qu'entreprise de taille intermédiaire, ID Logistics ne dispose pas de spécialistes de la sécurité en interne. Il était donc important de décharger les administrateurs systèmes et réseau des tâches complexes et chronophages liées à l'administration de la solution, afin qu'ils puissent se concentrer davantage sur leur cœur de métier. C'est donc tout naturellement que la DSI d'ID Logistics a décidé de faire appel aux services managés de Sophos.

Solutions techniques

Une solution complète de détection et de réponse aux menaces et des services managés évolutifs

La Direction informatique du groupe ID Logistics s'est tournée vers la solution Sophos XDR dédiée à la détection et à la prévention des menaces, associée à la protection endpoint Sophos Intercept X, afin d'accélérer et d'améliorer le fonctionnement opérationnel de ses solutions de cybersécurité.

Grâce au service Managed Threat Response (MTR), ID Logistics a pu bénéficier de l'expertise de Sophos de manière évolutive, ce qui lui a permis de garder dans un premier temps le contrôle sur la visualisation et l'exploitation de la solution, puis de collaborer davantage avec les équipes du SOC de Sophos, avant de déléguer peu à peu les décisions aux experts de Sophos.

L'intelligence artificielle (IA) de la solution de Sophos est notamment capable de filtrer les vastes volumes d'informations pour détecter les véritables indicateurs de compromission. Elle est associée à l'intelligence humaine, qui fournit une analyse forensic de ces indicateurs et des incidents. Les spécialistes de Sophos sont notamment dotés d'une expertise qui améliore leurs capacités de détection liées aux signaux faibles, pour une protection complète des systèmes et des données 24h/24 et 7j/7.

Résultats

Une protection de confiance efficace et continue contre tous les types de menaces

Grâce à l'évolutivité de l'offre de Sophos, Bruno Pruneyrac et ses équipes ont pu construire progressivement une relation de confiance avec les experts de Sophos et se décharger de plus en plus des responsabilités liées à la détection et à la réponse aux menaces. L'offre MTR se caractérise par sa protection 24h/24 et 7j/7, avec des experts capabes de traiter au plus vite les indicateurs de compromission, y compris pendant les heures non ouvrées.

La solution a permis aux équipes ID Logistics d'éviter d'être confrontées à de faux positifs et de détecter un certain nombre de menaces à signaux faibles, en les corrélant à d'autres sources d'information et d'autres alertes sur plusieurs postes qui n'auraient probablement pas été repérés sans l'expertise de Sophos.

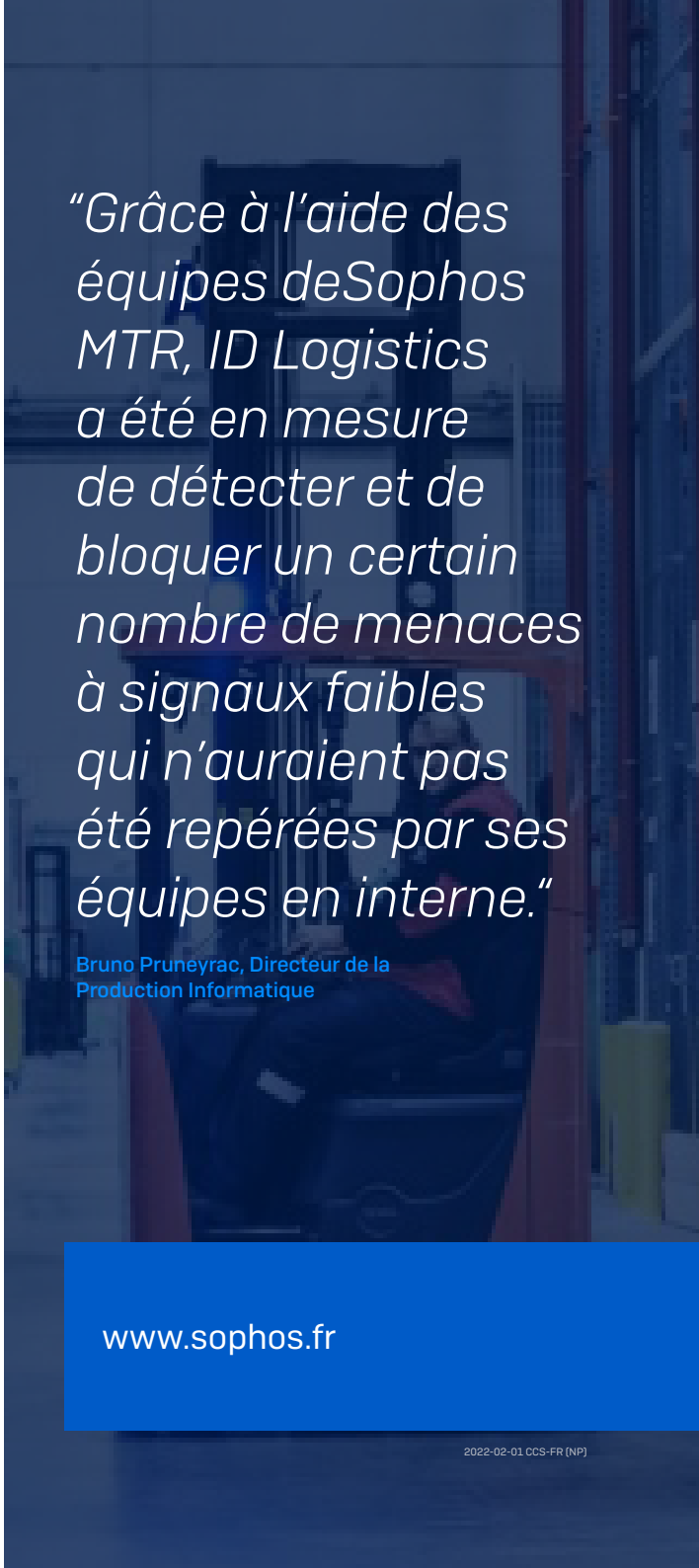
Forte de ces succès, la DSI du groupe ID Logistics envisage avec confiance la poursuite de son partenariat avec Sophos et souhaite amener d'autres pays du Groupe à adopter la solution, déléguer davantage de décisions aux services de sécurité MTR, afin de décharger encore davantage ses équipes, et ajouter de nouvelles sources de données de sécurité.

À propos du Groupe ID Logistics :

ID Logistics, dirigé par Eric Hémar, est un Groupe international de logistique contractuelle, ayant réalisé un chiffre d'affaires de 1 911 M€ en 2021. ID Logistics est présent sur plus de 350 sites implantés dans 17 pays représentant 7 millions de m² opérés en Europe, en Amérique, en Asie et en Afrique, avec 25 000 collaborateurs.

Disposant d'un portefeuille clients équilibré entre distribution, industrie, santé et e-commerce, ID Logistics se caractérise par des offres impliquant un haut niveau de technologie. Développant, à travers de multiples projets originaux une approche sociale et environnementale depuis sa création en 2001, le Groupe s'est aujourd'hui engagé résolument dans une politique RSE ambitieuse.

L'action ID Logistics est cotée sur le marché réglementé d'Euronext à Paris, compartiment A (Code ISIN : FR0010929125, Mnémo : IDL).



"Grâce à l'aide des équipes deSophos MTR, ID Logistics a été en mesure de détecter et de bloquer un certain nombre de menaces à signaux faibles qui n'auraient pas été repérées par ses équipes en interne."

Bruno Pruneyrac, Directeur de la Production Informatique

www.sophos.fr

SOPHOS

2022-02-01 CCS-FR (NP)