ÉTUDE DE CAS CLIENTS

Cyber résilience dans tous les secteurs : la défense multisectorielle de Derhem

Derhem Holdings, l'un des plus grands groupes privés marocains, fait confiance à Sophos pour maîtriser tous les enjeux propres à une activité au sein d'une grande diversité de secteurs.

SOPHOS

DERHEM HOLDING

Secteur d'activité
Transport, logistique, pétrole et gaz, immobilier, pêche commerciale, exploitation de carrières et médias

Nombre d'utilisateurs
350

Solutions Sophos
Central Managed Detection and Response

Central Mobile Advanced

Central Email Advanced

Défis

- En tant que grande société holding, Derhem Holdings opère dans un large éventail de secteurs, qui ont tous leurs propres exigences réglementaires, risques spécifiques et types de données sensibles à protéger.
- La société, en constante croissance et expansion dans de nouveaux secteurs, a besoin d'une solution de cybersécurité adaptative capable d'évoluer avec elle.
- Les activités de la société ont un impact direct sur les infrastructures critiques du Maroc, ce qui en fait une cible potentielle de grande valeur pour les acteurs malveillants.
- Derhem investit actuellement dans la digitalisation de ses processus, ce qui augmente sa surface d'attaque et la quantité de données sensibles qu'elle conserve dans des endroits accessibles depuis le réseau.

Solutions Sophos

- Central Managed Detection and Response
- Central Mobile Advanced
- Central Email Advanced

Il peut être particulièrement difficile pour une entreprise de logistique de faire face aux enjeux de la cybersécurité : une chaîne d'approvisionnement en constante évolution, une surface d'attaque toujours plus grande, des acteurs malveillants cherchant à perturber les systèmes critiques et des systèmes informatiques hérités.

Alors, imaginez si cette entreprise de logistique devait également tenir compte des menaces liées à la cybersécurité dans les secteurs de la vente au détail, des stations-service, de la restauration et même des exploitations de carrières.

Derhem Holdings, l'un des plus grands groupes privés marocains opérant dans différents secteurs d'activité, doit composer avec toutes les contraintes inhérentes aux différents secteurs dans lesquels il évolue, notamment en matière de cybersécurité. Les exigences en matière de confidentialité et de données qui incombent aux infrastructures de pêche commerciale sont très différentes de celles des systèmes qui alimentent une chaîne de 50 stations-service. Et tandis que la société soutient également la recherche sur les vaccins contre le COVID-19, elle doit dans le même temps s'employer à protéger son réseau de carrières de 66 hectares situé dans le sud du Maroc.

> «Détecter une menace en quelques minutes plutôt qu'en plusieurs heures ou jours peut faire la différence entre une alerte maîtrisée et un incident majeur.»
>
> **Elhichamy Oussama, Responsable infrastructure et sécurité**

La diversité des activités de Derhem accroît la complexité des besoins de l'entreprise en matière de cybersécurité, chaque secteur ayant ses propres exigences réglementaires, données sensibles et risques spécifiques.

Comme la société s'adapte et évolue constamment, elle avait besoin d'une solution de cybersécurité évolutive. Depuis plusieurs années, Sophos fournit une solution universelle à Derhem Holding, qui s'est progressivement élargie à mesure que l'entreprise s'est étendue à de nouveaux secteurs.

«Notre relation avec Sophos a commencé à travers un besoin de modernisation de notre cybersécurité», explique Oussama Elhichamy, RSSI de l'entreprise. «Nous recherchions une solution capable de nous offrir une visibilité globale, une réponse rapide aux menaces, et une protection proactive sur différents types d'environnements.»

Extension à une couverture 24/7

La relation entre Derhem et Sophos a tout d'abord porté sur la protection de quelques éléments de l'infrastructure : Sophos Email Advanced et Sophos Mobile Advanced.

Puis, Derhem Holding ayant constaté l'évolutivité et la complémentarité des solutions Sophos, l'entreprise a ajouté les services Sophos MDR (Managed Detection and Response). Sophos MDR protège 24 h/24 et 7 j/7 les endpoints et les réseaux des entreprises de Derhem, chassant en continu les menaces et alertant leur équipe informatique interne en cas d'alerte importante.

Selon Oussama Elhichamy, Sophos MDR permet à son équipe informatique de gagner du temps et de se libérer d'une partie de sa charge de travail, car la solution priorise les nombreux faux positifs et les alertes de faible priorité, réduisant ainsi le nombre d'alertes à traiter manuellement.

De plus, la possibilité de gérer toutes les alertes et activités à partir d'une seule et même console via Sophos Central est très appréciée par l'équipe.

Récemment, Sophos MDR a alerté Derhem d'un comportement anormal sur un serveur critique. Les analystes de Sophos MDR ont identifié l'activité malveillante, l'ont isolée et neutralisée avant qu'elle ne compromette les opérations de Derhem.

Sophos et Derhem ont collaboré pour mettre en quarantaine la machine infectée afin de pouvoir effectuer une analyse forensique. Finalement, Sophos MDR a décelé diverses vulnérabilités non corrigées qui devaient être remédiées et a fourni des solutions supplémentaires pour renforcer la surveillance des autres endpoints de Derhem.

«Détecter une menace en quelques minutes plutôt qu'en plusieurs heures ou jours peut faire la différence entre une alerte maîtrisée et un incident majeur» a déclaré Oussama Elhichamy.

> «Nos activités touchent directement aux infrastructures critiques du pays, et toute interruption ou compromission pourrait avoir des répercussions importantes. Cela renforce notre devoir de protection, de résilience et d'anticipation des menaces cyber.»
>
> **Elhichamy Oussama, Responsable infrastructure et sécurité**

«Le temps, c'est littéralement de l'argent.»

Pour Derhem, il est tout particulièrement crucial de pouvoir détecter ce type de menaces (et éviter le pire scénario) en raison de sa proximité avec les infrastructures critiques marocaines. De fait, ses activités comprennent le transport maritime et la logistique à travers le Maroc, ainsi que la supervision du transport pétrolier à destination et en provenance de l'océan Atlantique et de la mer Méditerranée.

Toute interruption de ces services pourrait avoir un coût élevé pour Derhem, ainsi que pour la population et le gouvernement marocains qui dépendent largement de ces services et de l'énergie qu'ils fournissent.

Pour Oussama Elhichamy, «dans notre secteur, le temps c'est littéralement de l'argent.» «Nos activités touchent directement aux infrastructures critiques du pays, et toute interruption ou compromission pourrait avoir des répercussions importantes. Cela renforce notre devoir de protection, de résilience et d'anticipation des menaces cyber.»

Comme dans le cas où Sophos MDR a repéré cette intrusion, les solutions Sophos peuvent déceler une menace en quelques minutes, et non en quelques heures ou jours, ce qui peut faire la différence entre ce que Oussama Elhichamy appelle une «alerte maîtrisée» pouvant être rapidement corrigée et un incident majeur.

Sophos MDR répond et remédie à une menace en 38 minutes en moyenne, soit 96 % plus rapidement qu'une équipe de sécurité interne (SOC) moyenne.

De plus, en évitant les incidents coûteux, tels que l'exfiltration de données ou les interruptions de service, Sophos aide Derhem à préserver sa rentabilité et à protéger l'image de marque de l'entreprise.

Derhem entend poursuivre sa croissance et se prépare à ce que Sophos évolue à ses côtés.

La société a entrepris de numériser un grand nombre de ces processus, ce qui augmente également la quantité de données sensibles qu'elle stocke et l'étendue de sa surface d'attaque potentielle.

«Cela nécessite un renforcement continu de notre posture de cybersécurité. Sophos est un partenaire clé dans cette démarche de sécurisation proactive de notre transformation numérique», déclare Oussama Elhichamy.

Pour commencer à utiliser les solutions Sophos et trouver une solution adaptée à vos besoins, contactez un de nos experts dès aujourd'hui.

Pour commencer à utiliser les solutions Sophos et trouver une solution adaptée à vos besoins, contactez un de nos experts dès aujourd'hui.

2025-10-21 CCS-FR (NP) CRE-1960