Sophos Rapid Response

Réponse immédiate aux menaces actives

Sophos Rapid Response est un service fourni par une équipe d'experts en réponse aux incidents qui identifie et neutralise de manière ultra-rapide les menaces actives ciblant votre entreprise.

Chaque seconde compte lors d'une attaque

Pour répondre à une menace active, il est impératif que le délai entre l'identification initiale de la compromission et la remédiation complète de la menace soit aussi court que possible. Quand un adversaire progresse dans la chaîne de frappe, une course contre la montre est engagée pour s'assurer qu'il ne puisse pas atteindre ses objectifs.

Avec Sophos Rapid Response, nous vous aidons à sortir rapidement de la zone de danger grâce à notre équipe d'intervention à distance disponible 24 h/24 et 7 j/7 composée d'experts en réponse aux incidents, d'analystes et de chasseurs de menaces. Notre équipe va :

- Prendre rapidement des mesures pour trier, contenir et neutraliser les menaces actives
- Expulser les adversaires de votre parc IT pour prévenir d'autres dommages
- Surveiller et répondre aux menaces 24 h/24 et 7 j/7 pour renforcer votre protection
- Recommander en temps réel des actions de prévention pour résoudre les causes profondes
- Déployer rapidement des technologies Sophos basées dans le Cloud sur l'ensemble de votre parc
- Analyser des données supplémentaires provenant de technologies tierces
- Fournir un compte-rendu post-incident de la menace détaillant notre investigation

Avantages principaux

- Identification et neutralisation rapides des menaces actives
- Réponse aux incidents et surveillance 24/7 pendant 45 jours
- Un interlocuteur et expert en réponse dédié
- Compte-rendu post-incident de la menace détaillant les actions prises
- Coûts prévisibles, fixes et sans frais cachés
- Conçu pour être couvert par assurance
- Évoluez en toute transparence vers un abonnement Sophos Managed Detection and Response (MDR) après Sophos Rapid Response

Fonctionnalités de Sophos Rapid Response

Sophos Rapid Response inclut toutes les fonctionnalités du service Sophos MDR Complete ainsi qu'un certain nombre d'avantages supplémentaires.

	Sophos Rapid Response
MDR Complete en mode de réponse « Autoriser »	✔
Surveillance, chasse aux menaces et réponse 24 h/24, 7 j/7	✔
Interlocuteur dédié en cas de menace active et ligne téléphonique directe	✔
Analyse de données supplémentaires provenant de technologies tierces	✔
Devis accéléré et activation du compte le jour même	✔
Compte-rendu post-incident de la menace, détaillant le processus d'investigation	✔

SOPHOS

Neutralisation de la menace active

L'équipe Sophos Rapid Response est spécialisée dans la neutralisation des menaces actives. Qu'il s'agisse d'un accès non autorisé aux ressources, d'une infection ou d'une compromission tentant de contourner vos contrôles de sécurité, nous avons déjà tout vu et tout stoppé avec succès.

Notre équipe d'experts en réponse aux incidents fait partie de Sophos Managed Detection and Response (MDR), notre service de chasse aux menaces, de détection et de réponse, disponible 24 h/27 et 7 j/7, qui recherche, identifie, analyse et répond de manière proactive aux menaces au nom de nos clients dans le cadre d'un service entièrement managé.

Intérêts communs

Les services de réponse aux incidents (IR) traditionnels sont facturés à l'heure, au risque de sous-estimer le temps nécessaire pour neutraliser complètement une menace. Ainsi, vous devrez peut-être payer des heures supplémentaires. Ou encore cela incite le service IR à surévaluer le nombre d'heures nécessaires pour la réponse.

Sophos Rapid Response propose un modèle de tarification fixe sans coûts cachés, déterminé par le nombre d'utilisateurs et de serveurs dans votre parc. De plus, comme le service est disponible à distance, des actions de réponse peuvent être lancées dès le premier jour. Il est dans notre intérêt, et dans le vôtre, de vous faire sortir de la zone de danger aussi rapidement que possible, car le temps n'est pas une variable du coût.

Déploiement rapide

Pour garantir la réponse la plus rapide possible, le processus de déploiement rapide de Sophos est axé sur la distribution immédiate des agents Sophos MDR sur les postes et les serveurs détectables.

Après avoir développé une stratégie de remplacement en utilisant des utilitaires de suppression pour remplacer les produits existants, une équipe distante d'ingénieurs de déploiement consulte chaque client Rapid Response pour initier un plan d'action personnalisé, en utilisant des outils d'automatisation pour le déploiement de masse sur le réseau.

L'équipe travaille en collaboration afin d'optimiser l'état de sécurité de l'agent Sophos MDR sur l'ensemble du réseau, en garantissant des configurations conformes aux bonnes pratiques pour accélérer l'investigation.

Méthodologie de Rapid Response

Une fois que le service Rapid Response est approuvé et que le client a accepté le contrat de service, nous intervenons immédiatement. La réponse comporte 4 étapes principales : prise en charge, priorisation, neutralisation et surveillance.

Prise en charge (Onboarding)

- Premier contact pour établir les préférences de communication et confirmer les mesures correctives (le cas échéant) qui ont déjà été prises
- Identification de l'ampleur et de l'impact de l'attaque
- Définition mutuelle d'un plan d'intervention
- Déploiement du logiciel du service

Triage

- Évaluation de l'environnement opérationnel
- Identification des indicateurs de compromission connus et des activités malveillantes
- Collecte de données et lancement de l'investigation
- Élaboration d'un plan de lancement des activités de réponse en concertation avec le client

Neutralisation (Neutralize)

- Suppression de l'accès des attaquants
- Neutralisation de toute autre atteinte aux actifs ou aux données
- Prévention de toute nouvelle exfiltration de données
- Recommandation d'actions préventives en temps réel pour remédier aux causes profondes

Surveillance (Monitor)

- Transition vers le service MDR Complete
- Suivi continu pour détecter toute récidive
- Livraison d'un compte-rendu post-incident de la menace

Compte-rendu détaillé de la menace

Une fois que nous avons neutralisé la menace active ciblant votre entreprise, nous vous fournissons un compte-rendu officiel de notre investigation, détaillant les mesures prises, nos découvertes, ainsi que des recommandations à long terme pour empêcher la réapparition de menaces similaires.

Surveillance et réponse 24/7 après l'incident

Dès que l'incident est résolu et que la menace immédiate pour votre entreprise est neutralisée, nous vous transférons vers notre service MDR de premier niveau, MDR Complete, qui traque, analyse, détecte et répond aux menaces de manière proactive 24 h/24 et 7 j/7.

Si la menace revient ou bien si une nouvelle menace émerge, notre équipe interviendra sans frais supplémentaires. Si vous êtes attaqués pendant 45 jours, nous vous protégeons pendant toute la durée de l'abonnement de 45 jours.

En proie à une attaque active ?

Appelez le numéro ci-dessous correspondant à votre pays pour être mis en relation avec l'un de nos conseillers.

Allemagne : +49 61171186766

Australie : +61 272084454

Autriche : +43 73265575520

Canada : +1 7785897255

France : +33 186539880

Italie : +39 02 94752 897

Royaume-Uni : +44 1235635329

USA : +1 4087461064

Suède : +46 858400610

Suisse : +41 445152286

Si tous les conseillers en incidents (Incident Advisors) sont occupés, veuillez laisser un message et quelqu'un vous rappellera dans les plus brefs délais.

En proie à une attaque active ?

Pour plus d'informations :
sophos.fr/rapidresponse

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

23-02-01 DS-FR (PC)

SOPHOS