Brochure de la solution

Sophos Emergency Incident Response

Assistance complète, de l'investigation au rétablissement

Réponse immédiate aux menaces actives

Chaque seconde compte lorsque votre entreprise est victime d'une attaque. Lorsqu'un incident se produit, vous avez besoin de rapidité, d'efficacité, ainsi que de compétences et d'expertise pluridisciplinaire en matière de cybersécurité. Vous devez également disposer d'une visibilité et d'une connaissance approfondies du paysage mondial des cybermenaces, ainsi que des dernières tactiques et techniques utilisées par les acteurs malveillants.

Sophos Emergency Incident Response est là pour vous lorsque vous faites face à une cyber urgence. Notre équipe d'experts pluridisciplinaires intervient rapidement et met à profit ses années d'expérience et ses connaissances pour trier, contenir et neutraliser rapidement les menaces actives, et expulser les adversaires afin d'éviter des dommages supplémentaires. Sophos s'appuie sur les enseignements tirés de milliers d'interventions pour recommander des améliorations et des mesures préventives qui ne se contentent pas de traiter la cause profonde de l'incident, mais contribuent également à renforcer votre résilience face à de futures attaques.

Renforcer de manière proactive les défenses et la posture de sécurité

Le service Sophos Emergency Incident Response adopte une approche collaborative et interactive, en travaillant avec votre équipe pour évaluer rapidement la situation, contenir et éliminer la menace si nécessaire, et fournir des conseils pratiques pour le rétablissement. Notre équipe fournit des services d'analyse forensique, d'analyse des malwares, de chasse aux menaces et de renseignements sur les menaces obtenus par les équipes de recherche Sophos X-Ops et Counter Threat Unit afin de détecter et d'éliminer les menaces. Nous faisons appel à des experts pluridisciplinaires (tels que des pen-testeurs et des chercheurs en menaces) pour garantir la mitigation complète des risques et la récupération.

Détection et investigation

Contact initial et investigation

Sophos se concentre exclusivement sur la distribution immédiate d'agents vers les actifs détectables, afin de garantir une réponse aussi rapide que possible. Cette assistance à distance permet de collecter des données d'investigation afin de faciliter l'analyse initiale, de mettre en place des mesures de confinement appropriées et de déterminer si des technologies supplémentaires sont nécessaires pour étendre rapidement la visibilité tout au long de l'intervention.

Avantages clients

- Renforcez votre équipe grâce à des compétences et une expertise transversales en matière d'investigation numérique et de réponse aux incidents.
- Réduisez l'impact d'un incident et le risque de récidive grâce à une compréhension complète de la menace.
- Améliorez la visibilité, obtenez des informations factuelles et trouvez rapidement des réponses afin de déterminer les mesures appropriées à prendre.

Investigation approfondie

Capture des données : actifs, services affectés, impact sur l'activité, autres vecteurs d'attaque.

Analyse forensique itérative et analyse des menaces : les chercheurs, chasseurs, pentesters et autres analystes contribuent à une compréhension globale de la menace.

Planification de la remédiation : commencez à planifier les mesures de remédiation, parallèlement et en coordination avec l'investigation.

Réduction de la surface d'attaque : Sophos peut fournir des informations interactives sur les acteurs malveillants afin de valider les contrôles et d'identifier des points de réentrée supplémentaires pour une atténuation complète des risques.

Négociation de la rançon : des négociateurs expérimentés s'appuient sur leur connaissance approfondie des auteurs de ransomware pour faciliter les négociations et offrir des conseils afin de récupérer les données de manière sûre et rentable auprès des acteurs malveillants.

Remédiation

Sécurisation et validation

Renforcement ciblé de la sécurité : l'équipe IR guide et soutient les efforts tactiques de renforcement des contrôles de sécurité qui empêcheront la réintroduction de l'acteur malveillant.

Confinement : pour couper les canaux Command-and-Control de l'acteur malveillant.

Expulsion des acteurs malveillants : pour expulser l'adversaire d'un réseau confiné, il faut éliminer de manière coordonnée ses techniques et réinitialiser les domaines compromis.

Récupération

Récupération du système et des données : pour aider à reconstruire les systèmes, assainir les données et remettre les systèmes en production, l'équipe IR de Sophos travaille avec des partenaires de confiance afin de fournir des services de récupération de manière transparente et sécurisée.

Validation des hôtes : grâce à notre technologie d'agent de pointe, nous veillons à ce que les hôtes restaurés soient opérationnels.

Suivi

Amélioration

Sophos s'appuie sur les enseignements tirés de milliers d'interventions pour vous aider à implémenter des améliorations dans votre procédure de réponse et pour formuler des recommandations stratégiques qui vous aideront à élaborer une feuille de route visant à transformer votre cybersécurité. À la fin de l'intervention, nous pouvons vous fournir un rapport d'incident officiel détaillant les mesures prises, les découvertes faites et des recommandations à long terme sur la manière d'atténuer la récurrence de menaces similaires à l'avenir.

Fonctionnalités du service

- Identification et neutralisation rapides des menaces actives.
- Déploiement rapide de technologies.
- Capture et analyse forensique des données pour identifier les indicateurs de compromission (IoC) et traquer l'activité des adversaires.
- Chasse aux menaces afin d'identifier les activités annexes des acteurs malveillants.
- Capacités techniques, de gestion des incidents et de conseil à distance et sur site.
- Équipe de réponse aux incidents mondiale expérimentée et accréditée, habituée aux scénarios de cybermenaces courants et inhabituels.
- Renseignements sur les menaces spécifiques aux incidents et informations sur les techniques actuelles utilisées par les adversaires.
- Négociation experte de la rançon.
- Rapport post-incident détaillant les mesures prises, les découvertes et les recommandations.

Pourquoi choisir Sophos pour la réponse aux incidents ?

À chacune de ses interventions d'urgence, Sophos apporte une vaste expérience en matière de cybersécurité. Nous fournissons une assistance complète en matière de réponse aux incidents à un large éventail d'organisations, tous secteurs et types d'incidents confondus, qu'il s'agisse de petits problèmes liés à un seul système compromis ou de situations de crise à l'échelle de l'entreprise qui perturbent ou entravent considérablement les opérations commerciales.

Notre équipe de haut vol s'appuie sur l'expertise et l'expérience acquises au sein d'équipes nationales, militaires et organisationnelles de réponse aux incidents de sécurité informatique (CSIRT), ainsi que d'organismes chargés de l'application de la loi et de renseignement. Elle combine une compréhension pratique des principales pratiques de cybersécurité avec une réponse aux incidents de première ligne, les renseignements sur les menaces fournis par nos équipes de recherche X-Ops et Counter Threat Unit, les résultats des tests et évaluations de sécurité, et l'analyse de la sécurité afin d'accélérer les investigations et de permettre une reprise en toute confiance.

Vous subissez une attaque active ?

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

Allemagne : +49 611 711 86 766

Australie : +61 272 084 454

Autriche : +43 7 3265575520

Canada : +1 778 589 7255

États-Unis : +1 408 746 1064

France +33 1 86 53 98 80

Italie : +39 02 94752 897

Royaume-Uni : +44 1235 635 329

Suisse : +41 44 515 2286

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

Email : EmergencyIR@sophos.com

Pour en savoir plus :

sophos.fr/emergency-response

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

2025-06-04 BRFR (MP)

SOPHOS