SOPHOS

FAQ commerciale et technique – Sophos Emergency Incident Response

FAQ externe

Présentation générale

Qu'est-ce le service Emergency Incident Response ?
Emergency Incident Response est un service d'urgence lorsque vous vous faites face à une cyberattaque, qui intervient rapidement pour évaluer, contenir et comprendre la menace, et vous offrir des conseils de remédiation. Notre équipe est composée d'experts pluridisciplinaires qui mettent à profit leurs années d'expérience et leurs connaissances pour trier, contenir et neutraliser rapidement les menaces actives, et expulser les adversaires afin d'éviter tout dommage supplémentaire.

Le service Emergency Incident Response vous aide également à déterminer si votre entreprise a été touchée par un incident et à comprendre l'ampleur de celui-ci. Le service fournit diverses activités d'investigation : identification de la cause première de l'incident, évaluation des comportements observés pour déterminer s'ils sont malveillants, chasse aux menaces et collecte de renseignements sur les menaces, et vous aide également à négocier la rançon.

À qui s'adresse le service Emergency Incident Response ?
Toute entreprise confrontée à un incident de sécurité actif, à une attaque récente nécessitant une investigation approfondie ou à une activité suspecte devant faire l'objet d'une investigation afin de déterminer si elle représente une menace.

Dois-je être client de Sophos pour acheter Emergency Incident Response ?
Non. Le service Emergency Incident Response est disponible à la fois pour les clients Sophos actuels, mais aussi pour les clients non Sophos.

Je suis victime d'une attaque active. Que dois-je faire ?
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

Contactez-nous par email à l'adresse EmergencyIR@sophos.com.

Le service Emergency Incident Response est-il assuré à distance ou sur site ?
Les deux options sont disponibles.

Quelle est la rapidité du service Emergency Incident Response ?
La plupart des clients sont pris en charge (onboarding) dans les 2 heures et font l'objet d'une priorisation (triage) sous 48 heures. Comme le service peut être entièrement assuré à distance, l'intervention peut commencer quelques heures seulement après votre premier contact avec Sophos.

En combien de temps serons-nous pris en charge ?
L'équipe Emergency Incident Response peut entamer le processus de prise en charge et commencer l'investigation dès qu'elle reçoit votre autorisation.

FAQ commerciale et technique – Sophos Emergency Incident Response

Quelle est la méthodologie du service Emergency Incident Response ?
Une fois que vous avez accepté le contrat de service, nous organisons une réunion de lancement (kickoff call). Si vous préférez, celle-ci peut se faire par email. L'investigation commence dès que nous avons compris vos objectifs pour la mission.

Le service Emergency Incident Response comprend différentes catégories de prestations. Lors de l'appel initial d'évaluation, nous travaillons avec vous pour identifier les catégories requises et estimer le nombre d'heures nécessaires.

Les catégories concernées comprennent la gestion de l'intervention (Engagement Management), la réponse aux incidents (Incident Response), l'analyse forensique (Digital Forensics), l'évaluation des compromissions (Compromise Assessment), la chasse aux menaces (Threat Hunting), la recherche et la collecte de renseignements sur les menaces (Threat Intelligence and Research), la négociation de la rançon (Ransom Negotiation), le rapport d'intervention (Engagement Report), l'assistance sur site (Onsite Support) (le cas échéant), l'analyse de la compromission de la messagerie professionnelle (Business Email Compromise) et le déploiement de logiciels (Software Deployment).

Dans quelle(s) langue(s) le service Emergency Incident Response est-il disponible ?
Le service est actuellement uniquement disponible en anglais et japonais. Vous devez parler anglais ou japonais avec une bonne maîtrise technique.

Sophos travaille-t-il avec ou remplace-t-il les services Digital Forensics and Incident Response (DFIR) ?
Emergency Incident Response est un service DFIR. Il n'est pas nécessaire de faire appel à une société de sécurité distincte pour les services DFIR, car l'étendue des services fournis dans le cadre de Emergency Incident Response peut inclure l'analyse forensique.

Dois-je installer la technologie Sophos sur mes terminaux ?
Non, le service Emergency Incident Response peut être assuré à l'aide de Sophos XDR, ou nous pouvons déployer le capteur Sophos XDR parallèlement à votre solution en place. Ces deux options nous permettent d'investiguer rapidement l'incident.

L'équipe Emergency Incident Response n'a pas besoin d'attendre la fin du déploiement pour prendre des mesures correctives afin de contenir et de neutraliser la menace. L'équipe exploitera toutes les données disponibles et utilisera les outils appropriés pour faciliter la réponse.

Comment le prix du service est-il calculé ?
Sophos estimera le nombre d'heures nécessaires pour répondre à l'incident en fonction des questions établies lors de l'appel initial d'évaluation. Vous ne payez que les heures réellement utilisées.

Faut-il prévoir des coûts supplémentaires ?
Si une intervention sur site est requise, les frais de déplacement vous seront facturés.

Pouvons-nous déployer Emergency Incident Response seulement sur un segment de notre environnement, ou faut-il que l'intégralité de notre environnement soit intégrée dans le service ?
Dans certaines situations, le service Emergency Incident Response peut être appliqué à une partie de votre environnement. Un spécialiste Emergency Incident Response vous fournira plus d'informations lors de l'appel initial d'évaluation.

Sophos peut-il travailler sur le contrat avec un intermédiaire représentant mon entreprise, tel qu'un cabinet d'avocats ?
Oui. Il est possible de travailler avec un intermédiaire.

Sophos peut-il déterminer quels fichiers ont été exfiltrés/volés lors de l'attaque ?
Le service Emergency Incident Response fait tout son possible pour déterminer quels fichiers (le cas échéant) ont été exfiltrés dans le cadre d'une attaque. Toutefois, cela n'est pas garanti, car cela dépend des données analysées dans le cadre de l'investigation.

Sophos déchiffrera-t-il pour moi les fichiers chiffrés par le ransomware ?
Non. Cela ne fait pas partie du service Emergency Incident Response.

Sophos m'aidera-t-il à négocier ou à faciliter le paiement de la rançon ?
Le service Emergency Incident Response comprend la négociation de la rançon avec les acteurs malveillants par des négociateurs spécialisés. Cependant, Sophos ne facilite pas le paiement des rançons, mais peut recommander et collaborer avec des tiers à cette fin si nécessaire.

2025-06-03 (WP-NP)

SOPHOS