Sophos Compromise Assessment

Débusquez les signes de violation avant que votre entreprise ne soit affectée

L'année dernière, les entreprises ont consacré en moyenne 37 jours et 2,4 millions de dollars à la détection de violations de sécurité et à leur remédiation. Assuré par une équipe d'experts en réponse aux incidents, le service Sophos Compromise Assessment est le moyen le plus rapide et le plus efficace d'identifier les activités des attaquants dans votre environnement, à la fois passées ou toujours actives, aidant ainsi votre entreprise à prendre des mesures rapides et décisives.

Identification des attaques récentes ou toujours actives

Assuré par une équipe d'experts spécialisés dans la chasse aux menaces et dans la réponse aux incidents, le service Sophos Compromise Assessment identifie rapidement la violation de vos défenses par un attaquant, quantifie le niveau de risque pour votre entreprise et fournit des conseils précis sur les mesures à prendre pour éliminer la menace.

Dotée d'une forte expérience dans la réponse aux menaces les plus sophistiquées d'aujourd'hui, l'équipe Sophos Incident Response (IR) Services identifie les indicateurs de compromission (IoC) à l'aide d'une investigation ciblée des actifs potentiellement compromis. Le résultat : un audit de sécurité complet et rapide qui aide votre entreprise à gérer les risques de sécurité et de conformité tout en maintenant son efficacité opérationnelle.

Méthodologie de Sophos Compromise Assessment

L'équipe Sophos IR Services maintient une communication directe avec votre entreprise à chaque phase de l'audit, afin d'apporter plus de précisions sur la menace, l'exposition aux risques et les mesures à prendre pour résoudre l'incident et traiter la cause profonde.

1. **Premier contact de coordination (Initial Coordination Call)** - L'audit de sécurité débute par un échange d'informations efficace sur la menace, l'identification des points de contact principaux et la confirmation à la fois du processus d'investigation et de l'ampleur du déploiement.
2. **Déploiement des outils d'investigation (Deployment of Investigation Tools)** - L'installation guidée de la plateforme Sophos hébergée dans le Cloud garantit la collecte immédiate des données sur les appareils répertoriés, permettant ainsi à l'équipe Sophos IR Services de procéder à un audit rigoureux de l'état de sécurité des appareils.
3. **Investigation sur la menace et évaluation des risques (Threat Investigation and Risk Assessment)** - Si une menace active est confirmée, l'équipe Sophos IR Services contacte immédiatement vos principaux points de contact pour les informer et discuter des risques de propagation de l'incident et des mesures urgentes à prendre.
4. **Synthèse téléphonique et rapport écrit (Summary Call and Written Report)** - Vous recevez un rapport technique et un résumé détaillant les preuves de l'activité malveillante, votre exposition aux risques et des conseils pour éliminer la menace et traiter la cause profonde.

Ces 4 phases du service Sophos Compromise Assessment sont habituellement exécutées dans les 7 jours suivant le premier contact de coordination.

Avantages principaux

- Identifiez rapidement si un attaquant opère à votre insu dans votre environnement
- Quantifiez le risque potentiel d'un incident de sécurité généralisé
- Communiquez directement avec une équipe d'experts spécialisés dans la chasse aux menaces et dans la réponse aux incidents à chaque étape de l'investigation
- Recevez une analyse complète sur les activités de l'attaquant, l'exposition aux risques, ainsi que des conseils pour éliminer la menace et éradiquer la cause profonde.
- Soutien des initiatives de gestion des risques et de conformité, ainsi que les efforts de diligence raisonnable associés aux activités de fusion et d'acquisition.

SOPHOS

Investigation complète et rapide

Le service Sophos Compromise Assessment analyse et identifie tout le spectre des activités des attaquants, notamment :

- Activités suspectes sur le réseau
- Mouvements latéraux
- Fichiers anormaux ou malveillants
- Exécution automatisée de malwares
- Accès non autorisés
- Élévation de privilèges
- Contournement des défenses
- Vol d'identifiants
- Exfiltration de données
- Scripts non vérifiés

Après l'audit de sécurité

Si l'équipe Sophos IR Services confirme qu'un attaquant a violé vos défenses, compromettant ainsi vos données et votre activité, vous pouvez rejoindre le service Sophos Rapid Response de manière prioritaire. Ce service complet de réponse aux incidents va trier, contenir et neutraliser la menace active sur l'ensemble de votre environnement informatique. Une équipe d'intervention à distance, opérant 24 h/24 et 7 j/7, intervient rapidement pour expulser l'attaquant de votre environnement et recommander des actions préventives en temps réel pour s'attaquer à la cause profonde.

Si aucun signe de compromission n'est détecté, le service Sophos Managed Detection and Response (MDR) peut doter votre entreprise de services managés de détection et de réponse opérationnels 24 h/24, 7 j/7. Notre équipe d'experts spécialisés dans la chasse aux menaces et dans la réponse aux incidents, disponibles 24 h/27 et 7 j/7, chasse et valide de manière proactive les menaces et les incidents potentiels. L'équipe prend des mesures en continu pour intercepter, contenir et neutraliser les menaces évolutives, et elle fournit des conseils pratiques pour traiter la cause profonde des incidents et améliorer votre posture de sécurité.

En proie à une attaque active ?

Sophos Rapid Response vous permet de 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. La prise en charge (onboarding) s'effectue en quelques heures seulement et la plupart des clients bénéficient du processus de priorisation (triage) sous 48 h permettant de définir les actions à mener.

Si vous faites face à une attaque active, envoyez un email à l'équipe Rapid Response à l'adresse rapidresponse@sophos.com ou appelez à tout moment le numéro ci-dessous correspondant à votre pays pour parler avec l'un de nos conseillers :

États-Unis : +1 408 746 1064

Australie : +61 272 084 454

Canada : +1 778 589 7255

France : +33 1 86 53 98 80

Allemagne : +49 611 711 86 766

Royaume-Uni : +44 1235 635 329

Suède : +46 858400610

Italie : +39 02 947 52897

Autriche : +43 73265575520

Suisse : +41 445152286

Pays-Bas : +31 162708600

Espagne : +34 913758065

En proie à une attaque active ?

Bénéficiez d'une assistance ultra-rapide avec Sophos Rapid Response

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

2023-06-27 DS-FR (PC)

SOPHOS