Brochure de la solution

SOPHOS

Services de conseils Sophos

Réduction proactive des risques et résilience face à l'évolution des cybermenaces

Évaluations de sécurité sur mesure, réalisées par des experts

La transformation numérique, l'essor de l'IA et l'évolution constante des cybermenaces sont autant de défis auxquels les entreprises doivent faire face aujourd'hui. Conscientes de l'importance de la cybersécurité, elles considèrent désormais cette question non seulement comme un défi technique, mais aussi comme une priorité stratégique. Une approche proactive et globale est nécessaire pour sécuriser les actifs numériques face à des adversaires sophistiqués, à une surveillance réglementaire accrue et aux attentes des parties prenantes. Les Services de conseil Sophos fournissent une expertise indépendante, une expérience et des stratégies sur mesure pour identifier les vulnérabilités systémiques, renforcer les défenses et améliorer la résilience des entreprises.

À l'aide de tactiques, techniques et procédures (TTP) réellement utilisées par les acteurs malveillants, nos experts en sécurité hautement certifiés testeront vos réseaux, vos systèmes et vos employés pour aider votre organisation à :

- Identifier les vulnérabilités avant que les attaquants ne puissent les exploiter.
- Renforcer les défenses contre les menaces sophistiquées.
- Répondre aux exigences de conformité réglementaire.
- Évaluer l'état de préparation à la réponse aux incidents.
- Instaurer la confiance avec les clients, les partenaires et les parties prenantes.

Renforcer de manière proactive les défenses et la posture de sécurité

Test d'intrusion (Pentesting)

Un test d'intrusion simule des cyberattaques réelles pour identifier les vulnérabilités des systèmes, des réseaux et des applications. Les testeurs expérimentés (hackers éthiques) tentent d'exploiter les vulnérabilités pour montrer ce qu'un attaquant pourrait réaliser.

Il existe deux grands types de tests d'intrusion. Les tests d'intrusion externe se limitent aux systèmes accessibles depuis Internet : sites Web, VPN, services publics, etc. Ils simulent une tentative d'intrusion dans votre périmètre depuis l'extérieur. Les tests d'intrusion interne simulent une menace interne ou un attaquant qui a déjà franchi le périmètre, en se concentrant sur les systèmes, les applications et les données au sein du réseau interne.

Pourquoi ce test est important :

- Il identifie les vulnérabilités cachées que les analyses de routine peuvent manquer.
- Il fournit des recommandations pratiques pour renforcer vos défenses.
- Il vous aide à rester conforme aux normes réglementaires (dont PCI DSS, HIPAA, RGPD, NIS, ISO 27001, SOC 2).
- Il démontre son engagement à l'égard d'une gestion proactive des risques.
- Il fournit une couverture complète des risques de sécurité périmétrique et interne.

Questions clés auxquelles il permet de répondre :

- Où se trouvent les vulnérabilités les plus critiques dans notre infrastructure ?
- Avec quelle facilité un attaquant pourrait-il pénétrer nos défenses depuis l'extérieur ?
- Quels sont les risques à l'intérieur de notre réseau si un attaquant y accède ?
- Quel est l'impact potentiel d'une attaque réussie ?
- Quelles mesures pouvons-nous prendre pour corriger les failles identifiées ?

Test d'intrusion du réseau sans fil

Un test d'intrusion du réseau sans fil évalue la sécurité du réseau et de l'infrastructure Wi-Fi d'une organisation et évalue leur conformité aux mandats appropriés. Les testeurs tentent d'exploiter les failles du chiffrement, de l'authentification et des contrôles d'accès.

Il existe deux types de tests d'intrusion du réseau sans fil. L'évaluation passive consiste à surveiller le trafic sans fil pour identifier les appareils non autorisés, les points d'accès indésirables et les erreurs de configuration sans tenter activement de se connecter. L'évaluation active simule une tentative d'exploitation de vulnérabilités du réseau sans fil par un attaquant en craquant le chiffrement, en contournant l'authentification ou en obtenant un accès non autorisé.

Pourquoi ce test est important :

- Il protège les données sensibles transmises sur les réseaux sans fil.
- Il identifie les points d'accès indésirables et les configurations incorrectes.
- Il garantit que les politiques de sécurité sans fil respectent les bonnes pratiques.
- Il réduit le risque de vol de données à cause de vulnérabilités sur le réseau Wi-Fi.
- Il évalue les risques d'exposition passive et d'exploitation active.

Questions clés auxquelles il permet de répondre :

- Les utilisateurs non autorisés peuvent-ils accéder à nos réseaux sans fil ?
- Utilisons-nous des méthodes de chiffrement et d'authentification sécurisées ?
- Des appareils indésirables sont-ils connectés à notre réseau ?
- Un attaquant peut-il contourner la protection de notre réseau sans fil ?
- Quelles mesures pouvons-nous prendre pour améliorer la sécurité du réseau sans fil ?

Évaluation de la sécurité des applications Web

Les applications Web traitent souvent des données commerciales et clients critiques, ce qui en fait des cibles privilégiées pour les attaquants. Les évaluations de la sécurité des applications Web garantissent la sécurité de vos applications Web en se concentrant sur les vulnérabilités courantes, notamment les injections SQL, le cross-site scripting (XSS) et les authentifications défaillantes.

Ces évaluations peuvent impliquer des tests en boite noire (black-box), dans lesquels le testeur simule le comportement d'un attaquant externe sans connaissance préalable du fonctionnement interne de l'application, ou des tests en boite blanche (white-box), dans lesquels le testeur a un accès complet au code source et à l'architecture, ce qui permet une analyse plus approfondie des vulnérabilités potentielles.

Pourquoi ce test est important :

- Il protège les données des clients et de l'entreprise traitées par les applications Web.
- Il identifie les défauts de codage et de configuration qui augmentent les risques.
- Il prend en charge la conformité aux normes telles que OWASP Top 10 et PCI-DSS.
- Il réduit le risque de défiguration de sites Web, de vol de données et d'atteinte à la réputation.
- Il fournit à la fois une perspective extérieure et une analyse approfondie de la sécurité des applications.

Questions clés auxquelles il permet de répondre :

- Nos applications Web sont-elles vulnérables aux méthodes d'attaque courantes ?
- Les données sensibles sont-elles exposées en raison de défauts de codage ou de configurations erronées ?
- Un attaquant externe peut-il exploiter des vulnérabilités ou existe-t-il des problèmes plus profonds dans le code ?
- Comment sécuriser l'authentification des utilisateurs et la gestion des sessions ?
- Quelles mesures de remédiation sont nécessaires pour corriger les vulnérabilités des applications Web ?

Résumé des services d'évaluation de la sécurité

Type d'évaluation	Se concentre sur	Réponses aux questions clés	Exemples de scénario
Test d'intrusion (Pentesting)	Infrastructure, systèmes et réseaux	Où sont nos vulnérabilités ? Comment un attaquant peut-il contourner nos défenses ?	Externe : test des sites Web et services destinés au public ; Interne : test des contrôles d'accès internes et de l'élévation des privilèges
Test d'intrusion du réseau sans fil	Sécurité Wi-Fi, chiffrement, contrôles d'accès	Notre réseau Wi-Fi est-il sécurisé ? Existe-t-il des appareils non autorisés ou indésirables ?	Test de la sécurité Wi-Fi du bureau ; Identification des points d'accès indésirables ; Tentative de connexion non autorisée
Évaluation de la sécurité des applications Web	Applications Web, erreurs de codage, authentification	Nos applis sont-elles sécurisées ? Les données sensibles sont-elles exposées ? Comment corriger les vulnérabilités ?	Test des portails clients, des sites de commerce électronique, des applis Web internes ; Identification de l'injection SQL, XSS, ou des failles d'authentification

Autres services de tests de cybersécurité

Aucune évaluation ou technique isolée ne saurait fournir une image exhaustive de la sécurité d'une entreprise. Chaque test a ses propres objectifs et ses propres niveaux de risque acceptables. Sophos peut travailler avec vous pour déterminer quelle combinaison d'évaluations et de techniques utiliser pour évaluer votre posture de sécurité et vos contrôles.

En savoir plus:
sophos.fr/advisory-services

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

2025-05-30 BRFR [MP]

SOPHOS