Nous éprouvons continuellement la sécurité de nos solutions

Deep InfoSec réalise des analyses automatisées quotidiennes, des tests d’intrusion annuels sur ses solutions, des évaluations régulières associant expertise humaine et IA et des exercices adversariaux continus. Les résultats alimentent les corrections du code, des configurations, des identités, des dépendances et des contrôles d’exploitation, puis les vérifications de remédiation.

Notre cycle de sécurité

Deep InfoSec réalise des analyses automatisées quotidiennes, des tests d’intrusion annuels sur ses solutions, des évaluations régulières associant expertise humaine et IA et des exercices adversariaux continus. Les résultats alimentent les corrections du code, des configurations, des identités, des dépendances et des contrôles d’exploitation, puis les vérifications de remédiation.

Deep Advisor — chemins d’attaque

Deep Advisor explore des hypothèses de chemins d’attaque au-delà des vulnérabilités isolées : accessibilité, privilèges et services exposés. Il rattache chaque chemin à des mesures correctives et permet aux analystes de réduire les enchaînements exploitables. Cette analyse complète les scanners et les tests manuels.

Ce que reçoit le client

Les travaux produisent un périmètre d’essai, des constats, des responsables de correction, des preuves de revalidation et des enregistrements d’amélioration.

Notes de mise en œuvre

Analyse de sécurité quotidienne

Les contrôles automatisés portent sur les dépendances, les configurations, les points exposés et les composants accessibles. Les constats sont attribués aux équipes concernées.

Tests d’intrusion annuels et exercices adversariaux

Les essais autorisés examinent les frontières de déploiement et le comportement réel. Les évaluations humaines et assistées par IA interrogent régulièrement d’autres hypothèses.

Prédiction et mesures de Deep Advisor

Les hypothèses de chemins d’attaque associent actifs exposés, privilèges et dépendances. Chaque chemin est relié à une mesure corrective et à un essai de vérification.

Contrôle technique et transmission

Chaque constat prioritaire comporte des preuves, un responsable, une correction et un contre-test. Les dossiers sont exploitables par les équipes de production et les évaluateurs compétents.

sales.security@deepinfosec.com | https://deepinfosec.com