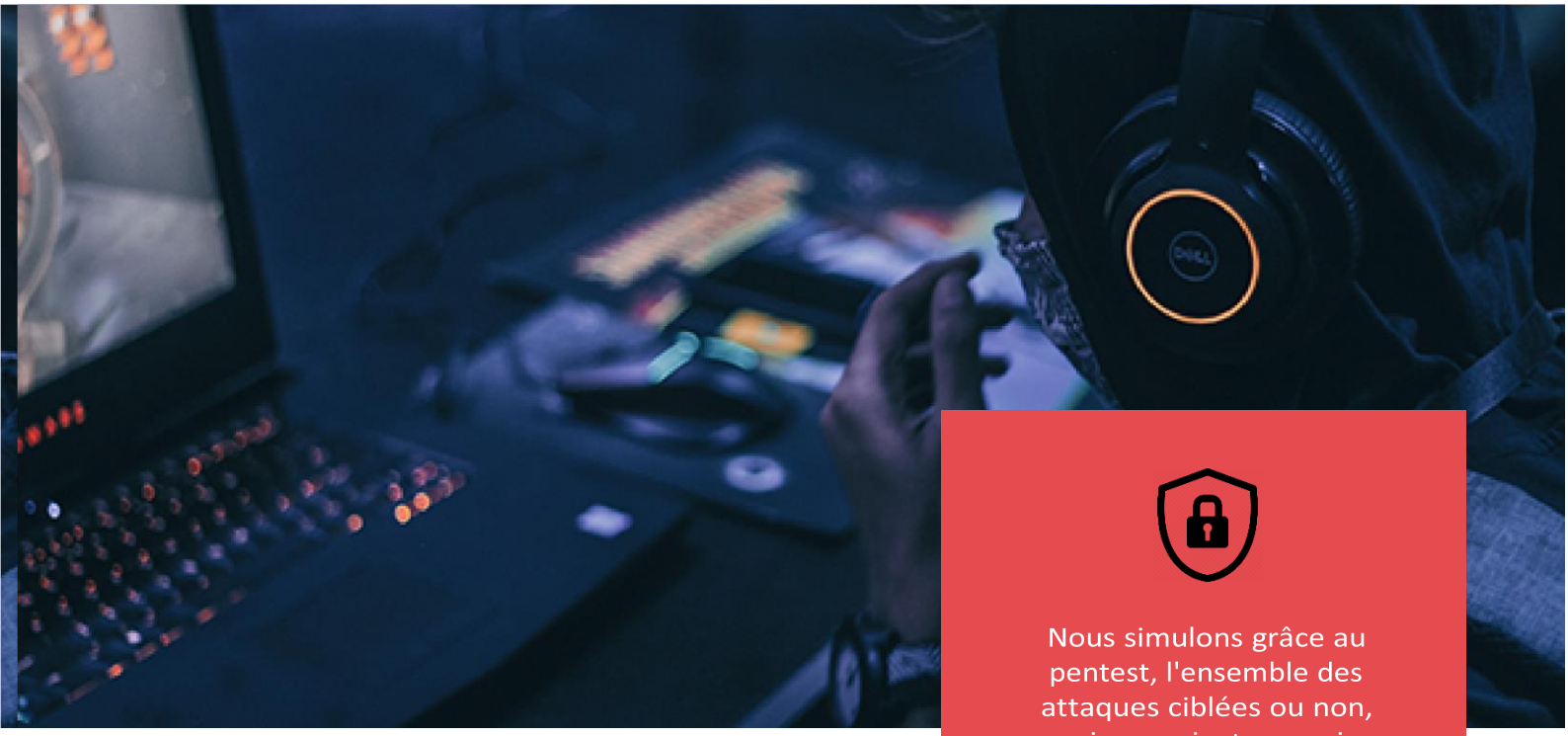
AMIOS
OPÉRATEUR INFORMATIQUE
ET TÉLÉCOM



Nous simulons grâce au pentest, l'ensemble des attaques ciblées ou non, qui pourraient survenir sur tout ou partie de votre système d'information.

AVEC AMIOS, REPÉREZ ET CORRIGEZ LES FAILLES ET VULNÉRABILITÉS EXPLOITABLES POUR OPTIMISER LA SÉCURITÉ DE VOS INFRASTRUCTURES.

Pentest

Évaluez la résistance de votre système d'information.

Prévenir, repérer et réagir contre le piratage et vol de données, la défiguration de site web, le hameçonnage, les attaques DDoS et autres virus, cryptolockers ou botnets automatisés, ...

GRÂCE AU PENTEST, ÉVALUEZ DE MANIÈRE FACTUELLE, LES RISQUES QUE VOUS ENCOUREZ.

Nos experts évaluent la complexité du test sur la base de plusieurs paramètres : accessibilité aux informations en phase amont, étendue du périmètre, nature de l'application auditée, maturité des mesures de sécurité en œuvre.

COMMENT APPROCHER L'ENVIRONNEMENT ET L'ORGANISATION ?

S'introduire dans votre système sans information.

Le test est réalisé à l'aveugle depuis l'extérieur dans les conditions les plus réalistes possibles sans considération sur la qualité de la configuration du système.

S'introduire en disposant d'un nombre limité d'informations.

Le pentesteur adopte la posture d'un collaborateur ou endosse le costume d'un hacker ayant obtenu l'accès à un compte utilisateur au sein de ladite organisation.

S'introduire en ayant accès à la totalité des informations.

Le but est de détecter un maximum de vulnérabilités et de vérifier que le système sera apte à redémarrer sans perte d'informations sur la base d'un travail effectué en collaboration avec vos équipes techniques.

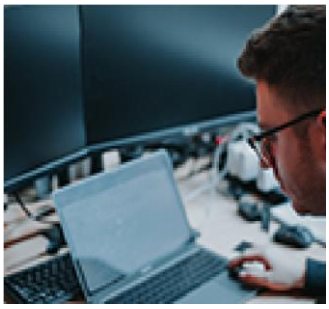
Quelle que soit l'approche retenue, nos experts peuvent intervenir sur différentes missions.

TEST D'INTRUSION EXTERNE

Accéder à un réseau exposé sur le WAN sans ressources ni connaissances.

Nos équipes tentent de recueillir des informations sensibles par le biais de renseignements de source ouverte (OSINT) et qui peuvent concerner vos collaborateurs, des mots de passe historiques violés, ...

TEST D'INTRUSION INTERNE



Examiner les réseaux et les systèmes informatiques à l'intérieur de leur environnement de travail.

Nos experts évaluent la résistance de votre environnement aux attaques qui émaneraient de vos collaborateurs ou dont la source serait d'autres utilisateurs d'un réseau privé.

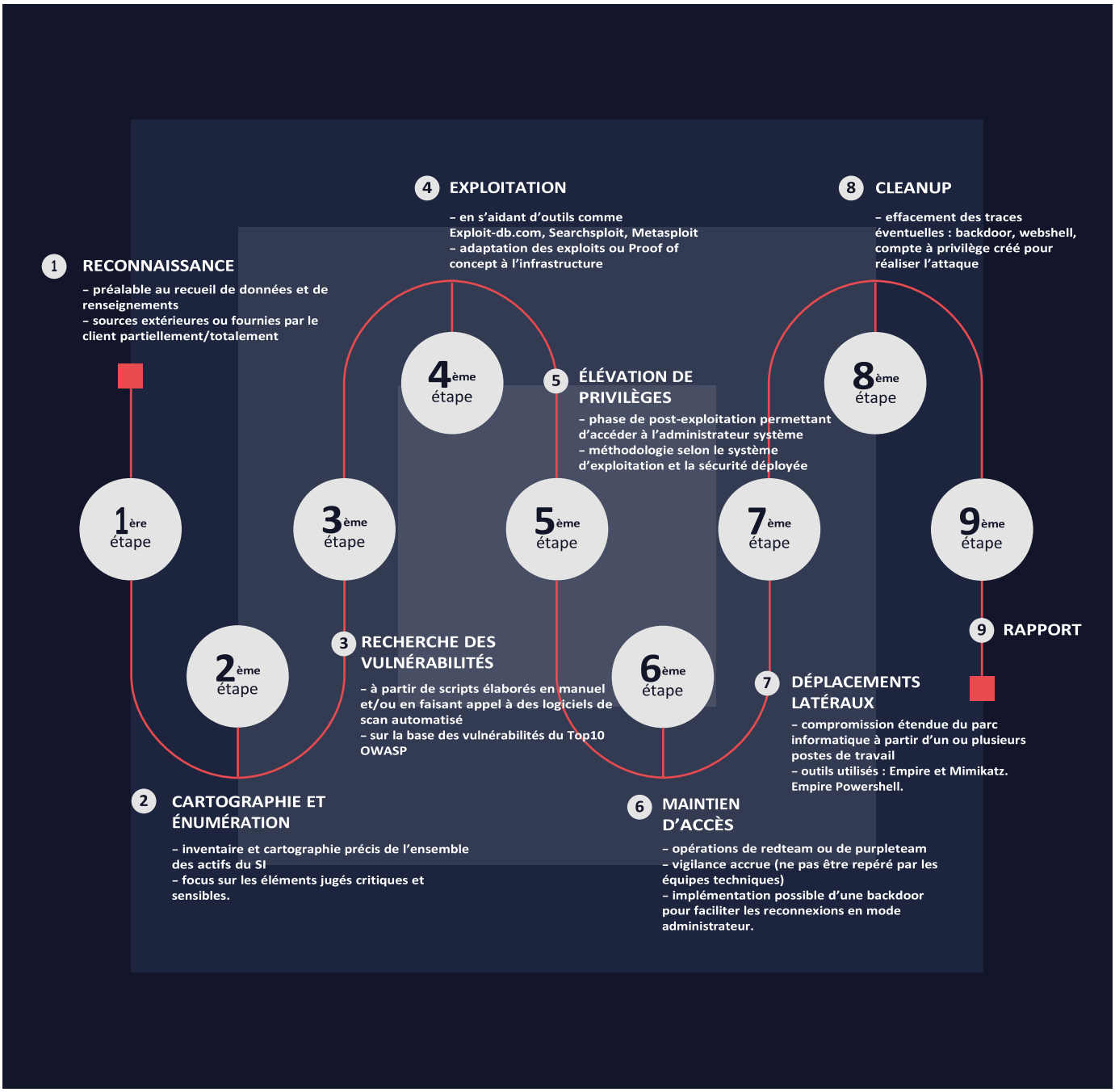
L'INGÉNIERIE SOCIALE

Vérifier le respect par les employés des politiques et des pratiques de sécurité préalablement définies.

Nous exploitons la psychologie humaine pour obtenir des données confidentielles plutôt qu'en cherchant une vulnérabilité logicielle. Le test repose sur les techniques de phishing ou phoning à partir de vos listes.

AMIOS, NOUS SOMMES PASSÉS MAÎTRES DANS L'ART DE CONDUIRE NOS MISSIONS DE PENTESTING.

Sur la base du besoin exprimé et suivant une méthodologie rigoureuse, nous étudions vos problèmes de configuration, de programmation, ainsi que les vulnérabilités des différents composants du périmètre testé afin de proposer un plan d'actions adapté de sécurisation de votre système d'information.



Nous testons l'efficacité de vos solutions de détection d'intrusion mais aussi LA RÉACTIVITÉ DE L'ÉQUIPE DE SÉCURITÉ ET LE COMPORTEMENT DES UTILISATEURS.

UNE OFFRE DE SERVICES À HAUTE VALEUR AJOUTÉE ET DES PRESTATIONS À VOS MESURES

Une fois l'étape de compréhension des besoins clients passée, nous annexons notre charte d'éthique à une convention d'audit rédigée et signée conjointement.

AVEC LA CONVENTION D'AUDIT AMIOS ETHIC, RIEN N'EST LAISSÉ AU HASARD :

- Objectif de l'intrusion
- Description de la mission
- Actions envisagées ainsi que les limites du test
- Prérequis éventuels
- Organisation de la mission

AMIOS
OPÉRATEUR INFORMATIQUE ET TÉLÉCOM

05 67 80 25 41
contact@amios.fr
Suivez-nous
414 rue de la découverte - Innopolis Hall B - 31670 Labège
WWW.AMIOS.FR

Parce que la réussite d'un test d'intrusion est tributaire du niveau de connaissances et du savoir-faire du prestataire, NOUS FAISONS APPEL AUX MEILLEURES COMPÉTENCES.