L-XPLOIT
OFFENSIVE CYBER EXPERTS

Offre de services

Catalogue 2024

L-XPLOIT

OFFENSIVE CYBER EXPERTS

Le Hacking Intelligent

Challenger vos systèmes d'informations est **impératif** pour protéger votre entreprise contre les cyberattaques.

L-XPLOIT CYBER EXPERTS

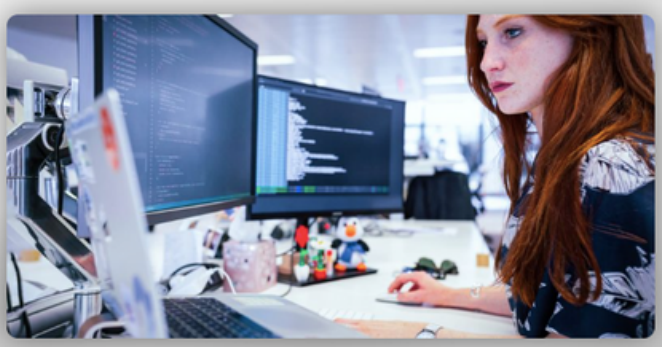
Votre partenaire expert en Cybersécurité Intelligente. Notre engagement fort se traduit par une détection proactive des cybermenaces, identifiant les risques potentiels pour les activités cruciales de votre entreprise. Avec une expertise technique avancée, nous vous guidons et formons de manière pragmatique pour renforcer votre sécurité informatique, assurant une protection solide contre les menaces actuelles et émergentes.

NOS VALEURS

L-Xploit incarne l'intelligence stratégique en cybersécurité. Nous croyons que chaque individu doit être informé et préparé face aux menaces numériques. Notre engagement : sensibiliser, agir et évoluer pour protéger chaque entreprise.

NOTRE MISSION

L-Xploit s'engage à propulser votre entreprise vers un futur sécurisé. Nous offrons des solutions intégrales, des formations pointues et des réponses agiles face aux incidents. Notre mission : garantir votre tranquillité face aux cybermenaces.



Un test d'intrusion permet d'identifier les vulnérabilités d'un système informatique comme le ferait le cyber pirate.

Nos méthodes, alliant tests manuels, outils automatisés et techniques d'ingénierie sociale, permettent de prioriser et corriger ces vulnérabilités, renforçant ainsi votre sécurité globale.

PENTEST WHITE BOX

Le test d'intrusion en boîte blanche implique une connaissance approfondie de l'architecture, du code source et de l'infrastructure du système à tester. L'équipe de sécurité dispose d'informations complètes pour simuler des attaques ciblées et évaluer les vulnérabilités.

PENTEST GREY BOX

Le test d'intrusion en boîte grise combine des éléments du test en boîte blanche et en boîte noire. L'équipe de sécurité dispose d'une connaissance partielle du système à tester, simulant ainsi les attaques avec certaines informations, mais sans accès complet aux détails internes du système.

PENTEST BLACK BOX

Le test d'intrusion en boîte noire simule une attaque externe sans aucune connaissance préalable du système à tester. Les testeurs jouent le rôle d'un attaquant externe et tentent de découvrir les vulnérabilités à partir de zéro, en évaluant les systèmes et les réactions du point de vue d'un intrus potentiel.

La sécurité informatique nous concerne tous.
Notre panel de formation est conçu pour répondre aux besoins de tous les collaborateurs en entreprise, initiés ou non aux enjeux et bonnes pratiques en matière de sécurité informatique.

INITIÉS **EXPERTS**

Hacking Éthique, Sensibilisation à la cybersécurité, Sécuriser un poste de travail...

- CONFÉRENCES
- TABLES RONDES
- WORKSHOPS
- COACHING CTF
- ÉVÈNEMENTS CYBERSÉCURITÉ

Veille

Initial Access Brokers
Surfaces d'attaque
Info Stealers

La surveillance de vos surfaces d'attaques externes et des Initials Access Brokers vous permet de maîtriser et de résoudre les problèmes avant même que les pirates s'en aperçoivent.

SURFACE EXPOSÉE :
Vos actifs volontairement exposés : Shadow IT, Clouds, Bases de données exposées, Buckets, Blob, Documentation interne, réseaux sociaux, Sites web, Applications en lignes.

SURFACE INTERNE :
La cible des ransomwares et des APT : Serveurs, Active Directory, Laptops, Infrastructure Legacy, R&D, Données sensibles, Secrets commerciaux.

SURFACE INCONTRÔLÉE :
Vos informations, exposées par d'autres : DarkWeb, revente d'accès, revente de données, fuites d'identifiants, fake news, trolls, usurpations de comptes.

Tech Monitoring

La surveillance de vos technos vous permet de rester informés dès qu'une vulnérabilité est détectée afin de renforcer la sécurité, prévenir les incidents, optimiser les performances.

- CVE
- 0 Day
- CTI

Reponse à incident

Containement
Eradication

Détecter, enquêter et réagir rapidement suite à une cyber attaque afin de minimiser les dommages liés à une violation de données.

Des procédures claires et l'utilisation d'outils de détection sont les fondements de notre approche.

Les 5 phases de nos interventions en cas d'incident :

Préparation :

- Nous identifions les vulnérabilités et les risques potentiels.
- Nous élaborons des contre-mesures pour y remédier.

Détection & Analyse :

- Nous mettons en oeuvre des outils pour détecter les menaces.
- Nous identifions le type et le niveau des menaces.

Confinement et Éradication :

- Nous isolons le système affecté et supprimons la première menace.
- Nous mettons en place les correctifs adéquats.

Rétablissement :

- Nous restaurons le système affecté et appliquons les sauvegardes nécessaires.

Améliorations continues :

- Nous effectuons une analyse post-incident et traitons les points à améliorer.

SAS L-XPLOIT CYBER EXPERTS

+33 6 46 55 61 79

www.lxploit.com

global@lxploit.com

SPAC®
Smart Physical Access Control

RÉFÉRENCÉ SUR LA PLATEFORME
CYBERMALVEILLANCE.GOUV.FR
RÉPUBLIQUE FRANÇAISE