# Cyberdefense

# Threat-Led Penetration Testing

## Pour que vous puissiez vous focaliser sur l'essentiel

Dans le contexte actuel, marqué par une évolution continue des menaces, les entreprises ont besoin d'une approche ciblée pour tester la sécurité informatique de leur environnement.

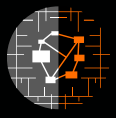
Threat-Led Penetration Testing (TLPT) va au-delà des tests traditionnels en intégrant des renseignements en temps réel sur les menaces pour simuler les actions de véritables acteurs malveillants. En imitant les méthodes d'adversaires sophistiqués, le TLPT offre aux organisations une évaluation réaliste de leur posture de sécurité ainsi que de leur capacité à détecter, répondre et atténuer les menaces avancées.

Cette méthode permet de rendre les efforts de test plus pertinents face aux menaces spécifiques à votre activité, tout en étant plus efficaces grâce à l'intégration de renseignements sur les dernières méthodes d'attaque, le TLPT veille à ce que votre stratégie de sécurité (et vos investissements) soient en adéquation avec les risques majeurs de votre industrie.

## Principaux avantages du Threat-Led Penetration

- **Analyse adaptée:** En se concentrant sur les menaces propres à votre secteur, nous fournissons une évaluation réaliste de vos vulnérabilités. Cela garantit que les tests techniques ultérieurs reflètent les risques réels auxquels vous êtes confronté.
- **Gestion ciblée des risques:** Notre approche permet de hiérarchiser les menaces les plus critiques pour votre entreprise, vous aidant ainsi à allouer vos ressources de manière plus efficace et à traiter en priorité les préoccupations de sécurité les plus urgentes.
- **Sécurité renforcée:** Contrairement aux méthodes de test traditionnelles, cette approche permet de découvrir des vulnérabilités qui pourraient autrement passer inaperçues. En évaluant non seulement les systèmes, mais aussi vos processus métier et vos collaborateurs, nous renforçons considérablement votre posture de sécurité globale et protégeons mieux vos actifs et vos données
- **Conformité réglementaire:** Pour les entreprises soumises à des réglementations (telles que DORA, TIBEREU, etc.), notre test basé sur les menaces permet d'assurer la conformité tout en fournissant des rapports détaillés pour les audits.
- **Amélioration continue de la sécurité:** L'intégration du renseignement sur les menaces dans votre stratégie de sécurité permet une amélioration continue en fournissant des informations en temps réel sur les menaces émergentes, les vulnérabilités et les schémas d'attaque. Cela permet à votre équipe d'ajuster proactivement les défenses, d'identifier les lacunes et de mettre en œuvre des mesures de sécurité ciblées pour anticiper l'évolution des risques.

## Le Threat-Led Penetration Testing par Orange Cyberdefense



Nos consultants vous aideront à identifier votre paysage de menaces et à créer des scénarios personnalisés en fonction de vos risques les plus probables.



Vous recevrez un rapport détaillé et personnalisé, offrant des informations exploitables sur les menaces actuelles ainsi que sur les domaines nécessitant des tests techniques.



En combinant notre expertise technique avec le renseignement sur les menaces, nous réalisons des tests de sécurité de suivi qui produisent des insights pratiques pour réduire les risques liés à vos menaces les plus probables.

# Méthodologie et Approche

Notre évaluation se déroule en deux phases : la phase de **Threat Intelligence Gathering** et la phase de **Intelligence-Driven Penetration Testing**, où les insights recueillis lors de la première phase orientent des attaques de test d'intrusion ciblées.

## Phase 1 : Threat Intelligence Gathering

Dans cette phase, nous nous concentrons sur la compréhension du profil de menace actuel de votre organisation :

- **Collecte de données :** nous recueillons des informations pertinentes provenant de diverses sources de renseignement sur les menaces afin d'identifier et d'évaluer les risques potentiels spécifiques à votre entreprise.
- **Implication des parties prenantes:** réunions de suivi avec les parties prenantes clés de votre organisation pour clarifier les informations recueillies et garantir leur exactitude.
- **Analyse:** nos consultants analysent les données recueillies en dehors du site, en utilisant leur expertise pour évaluer votre exposition aux menaces.
- **Rapport final:** un rapport complet détaillant votre paysage de menaces, avec des recommandations spécifiques pour des scénarios techniques afin d'orienter la phase de test d'intrusion.

## Phase 2 : Intelligence-Driven Penetration Testing

Suite aux insights de la phase 1, nous procédons à des tests d'intrusion ciblés :

- **Penetration Testing:** notre équipe teste les scénarios techniques identifiés lors de la phase 1, en utilisant des techniques d'attaque du monde réel adaptées aux risques spécifiques de votre organisation.
- **Rapport détaillé:** un rapport technique documentant les attaques effectuées, les vulnérabilités découvertes et les résultats, fournissant des insights exploitables pour améliorer votre posture de sécurité.

## Pourquoi Orange Cyberdefense?

Chez Orange Cyberdefense, nous combinons une expertise avancée en sécurité offensive avec une intelligence sur les menaces approfondie et constamment mise à jour pour offrir des tests d'intrusion axés sur les menaces, qui reproduisent les méthodes des attaquants du monde réel.

Opérant à travers 32 centres de livraison et 18 SOCs dans le monde, et soutenus par plus de 300 professionnels de la cybersécurité, nous réalisons des évaluations à la fois évolutives et très ciblées.

Reconnu par Gartner et IDC, nous offrons une transparence totale grâce à notre plateforme Core Fusion et un accompagnement personnalisé via des responsables de la prestation de services dédiés. Nos tests axés sur les menaces fournissent des insights stratégiques pour révéler les points faibles, remettre en question la détection et la réponse, et renforcer la résilience globale.

Avec nous, votre cybersécurité reste aiguisée, adaptable et prête à relever tous les défis.

