FICHE PRODUIT

MANDIANT®
A FireEye® Company

Simulations d'attaque (Red Team Operations)

Testez vos capacités à protéger vos ressources les plus précieuses à partir de scénarios d'attaques ciblées et réalistes

AVANTAGES

- Déterminez les risques pour vos données et leur vulnérabilité face aux attaques
- Évaluez la sécurité de votre environnement face à une attaque où « tous les coups sont permis »
- Testez la capacité de votre équipe de sécurité à prévenir, détecter et intervenir sur des incidents dans des mises en situation réelles, mais sans danger réel
- Identifiez et corrigez les vulnérabilités de sécurité complexes avant qu'un attaquant ne les exploite
- Effectuez un bilan-risque factuel, avec en prime des recommandations pour le renforcement de votre sécurité

Pourquoi choisir Mandiant ?
Mandiant, une entreprise FireEye, possède plus de dix ans d'expérience de première ligne dans le domaine de la cybersécurité et de la Cyber Threat Intelligence (CTI). Nos experts en intervention sur incidents ont opéré sur les violations de sécurité les plus complexes et les plus médiatisées que l'on ait connues. Ils possèdent une connaissance approfondie des auteurs de menaces établis et émergents, ainsi que de leurs outils, tactiques et procédures en constante évolution.

Présentation du service
Le service de simulation d'attaque de la Red Team consiste à mettre en scène un scénario d'attaque réaliste, où « tous les coups sont permis ». Nos hackers éthiques simulent le comportement d'un attaquant et emploient tous les moyens nécessaires pour atteindre les objectifs établis conjointement (sans bien sûr mettre en danger votre entreprise). La simulation reproduit fidèlement les méthodes d'une attaque furtive en recourant aux même outils, tactiques et procédures que ceux observés sur des cas d'incidents récents. Cette mise en situation permet ainsi d'évaluer les capacités de votre équipe de sécurité à détecter et neutraliser une attaque en cours.

Exemples d'objectifs

Pirater les e-mails de l'équipe de direction ou de développeurs	S'introduire dans un environnement segmenté qui contient des données stratégiques ou sensibles	Prendre le contrôle d'un terminal automatisé, par exemple un équipement IoT, un appareillage médical ou un système industriel

Méthodologie
En premier lieu, nous commençons par décider ensemble si la Red Team devrait ou non posséder des connaissances sur votre environnement. Mandiant s'appuie sur son vaste champ d'expérience pour identifier les points les plus à risque pour le cœur de vos activités.

FireEye

L'équipe Red Team suit les différentes phases du cycle d'une attaque.

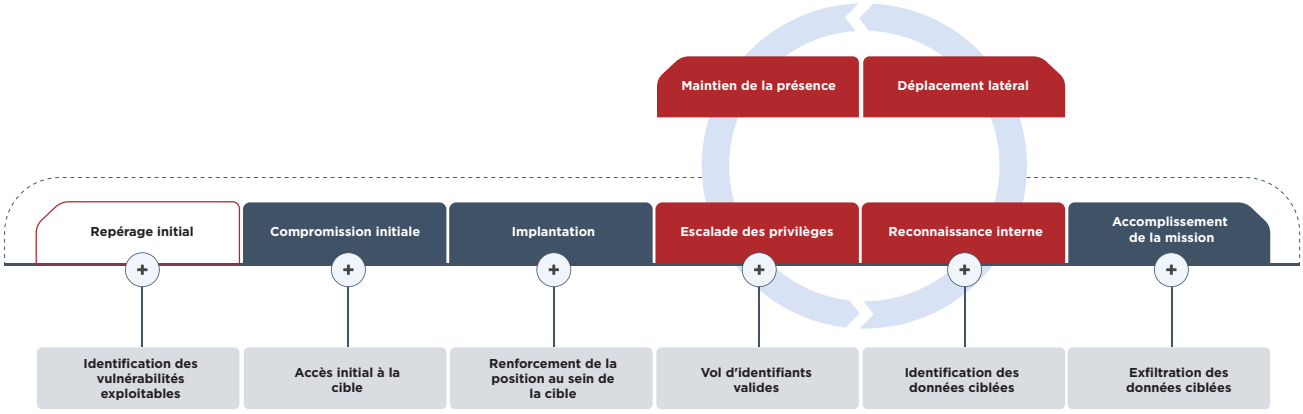

Figure 1. Cycle d'une attaque

Une fois les objectifs définis, la simulation débute par une phase de reconnaissance et de repérages de l'environnement cible. Pour ce faire, Mandiant s'appuie sur une combinaison d'outils et de techniques de renseignements internes et d'origine source ouverte (ROSO).

La Red Team tente ensuite d'obtenir l'accès initial à l'environnement, soit par une exploitation des vulnérabilités identifiées, soit par des techniques d'ingénierie sociale. Elle reprend ainsi des techniques utilisées lors d'attaques réelles afin d'obtenir un accès privilégié aux systèmes du client.

Une fois l'accès obtenu, la Red Team essaie d'élargir ses privilèges dans le but de s'implanter durablement au sein de l'environnement au moyen d'une infrastructure de contrôle-commande (CnC), exactement comme dans une attaque réelle.

Une fois leur présence établie, les hackers éthiques de Mandiant tente d'atteindre leurs objectifs au travers de méthodes les plus discrètes possibles.

Pourquoi choisir la Red Team ?
Les simulations d'attaque sont recommandées aux entreprises qui veulent :

- *Évaluer leurs capacités de détection et de riposte* Si vos équipes de sécurité se disent prêtes à contrer des incidents, mieux vaut tout de même en être sûr : testez ses capacités de réaction en conditions réelles — mais sans avoir à prendre le moindre risque.
- *Susciter une prise de conscience et démontrer l'impact d'une attaque.* La Red Team de Mandiant se comporte comme n'importe quel cybercriminel et se base uniquement sur des informations disponibles en ligne pour tenter d'accéder à votre environnement à partir d'Internet. Si elle réussit dans sa mission, elle vous permettra d'identifier les failles à combler en priorité et vous apportera tous les arguments nécessaires à une augmentation de vos budgets de sécurité.

PRESTATIONS ET LIVRABLES DE LA MISSION

- Document de synthèse destiné aux managers et équipes dirigeantes
- Documentation technique présentant des procédures détaillées pour vous permettre d'établir une reconstitution
- Bilan-risque factuel pour vous aider à déterminer la pertinence de l'analyse au regard de votre environnement
- Recommandations tactiques pour un renforcement immédiat de la sécurité
- Recommandations stratégiques pour améliorer la sécurité à plus long terme
- Expérience concrète acquise au contact direct d'un incident réaliste, sans aucune prise de risque ni mauvaise publicité

Pour en savoir plus, rendez-vous sur **www.fireeye.fr**

FireEye, France |
Nextdoor Cœur Défense
110 Esplanade du Général de Gaulle 92931
Paris La Défense
Cedex 92974 | +33 1 70 61 27 26 |
france@FireEye.com | www.FireEye.fr
FireEye, Inc. | 601 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | info@FireEye.com

À propos de FireEye, Inc.
FireEye est spécialisé dans la cybersécurité axée sur la cyberveille. Prolongement naturel et évolutif des opérations de sécurité des clients, la plate-forme unique de FireEye combine des technologies de sécurité innovantes, des services de cyberveille d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques. FireEye compte plus de 5 000 clients dans 67 pays, dont plus de 40 % figurent au classement Forbes Global 2000.

FireEye