FIREEYE™

FICHE PRODUIT

Purple Team Assessment

Formez votre équipe de sécurité sur des scénarios d'attaque réalistes pour améliorer ses capacités de détection et de réponse

AVANTAGES

- Entraînez votre équipe de sécurité à combattre des incidents en conditions réelles, sans risque ni conséquence néfaste pour votre entreprise
- Évaluez et améliorez la capacité de votre équipe de sécurité à prévenir, détecter et intervenir sur des incidents dans des mises en situation réelles mais sans danger
- Testez et réglez les détails techniques de vos systèmes de défense pour optimiser l'efficacité de votre détection et réponse à incident
- Adoptez le framework MITRE ATT&CK
- Identifiez les failles dans vos contrôles de sécurité actifs et passifs
- Améliorez les capacités d'intervention de votre entreprise sur de futurs incidents

Pourquoi choisir FireEye Mandiant ?
Depuis 2004, FireEye Mandiant agit en première ligne sur le front de la cybersécurité et de la Cyber Threat Intelligence (CTI). Nos experts de la réponse à incident opèrent sur les violations de sécurité les plus complexes et les plus médiatisées qui soient. Ils possèdent une connaissance approfondie des auteurs de menaces établis et émergents dont ils suivent l'évolution constante des modes opératoires.

Présentation du service
L'équipe de simulation d'attaque FireEye Mandiant Purple Team évalue la capacité de vos équipes de sécurité à prévenir, détecter et répondre à des attaques concrètes. Elle s'appuie pour cela sur la dernière Threat Intelligence disponible, ainsi que sur la plateforme FireEye Verodin d'instrumentation de la sécurité (SIP, Security Instrumentation Platform). Les scénarios mis en scène sont particulièrement réalistes et adaptés à votre domaine d'activité.

Pour souligner les failles dans votre environnement technologique, la Purple Team ne part pas de l'hypothèse selon laquelle vos opérations de sécurité fonctionnent comme prévu. Contrairement aux tests d'intrusion conçus pour identifier des erreurs de configuration ou des correctifs manquants sur un système de votre infrastructure réseau, le Purple Team Assessment est un exercice collaboratif qui s'appuie sur Verodin pour dresser un bilan précis et quantifiable de l'efficacité de votre sécurité.

Ce service s'adresse aux entreprises souhaitant tester et améliorer les capacités de leurs équipes, processus et technologies de sécurité à prévenir et neutraliser les attaques ciblées à chaque phase de leur cycle.

Notre méthodologie
La Purple Team commence par analyser les données CTI pour dresser un tableau des types de compromissions et des groupes les plus actifs dans votre secteur d'activité. Elle crée ensuite des scénarios Verodin SIP pour reproduire les modes opératoires typiques de ces groupes. L'idée est de tester la capacité de votre équipe de sécurité à détecter et répondre aux attaques les plus actives dans votre secteur, dans des conditions proches de la réalité.

Pour tester les performances de votre équipe tout au long du cycle d'attaque, le Purple Team Assessment procède étape par étape, sur la base d'exercices inspirés de scénarios plausibles et concrets.

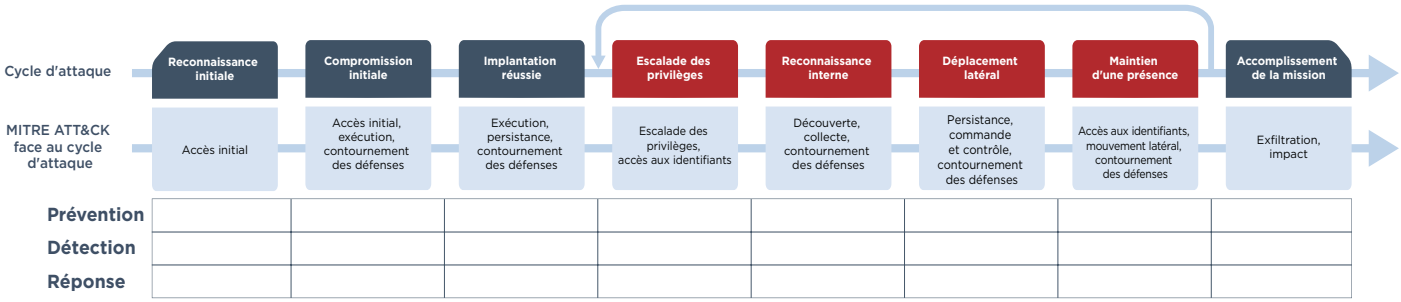

Figure 1. La Purple Team de Mandiant teste les capacités de l'équipe de sécurité du client à chaque phase du cycle de l'attaque.

À chaque phase de l'attaque, votre équipe de sécurité travaille au contact direct d'un consultant Red Team et d'un consultant IR (Incident Response) de FireEye Mandiant pour vous aider à détecter les activités simulées. En cas de détection, la Purple Team épaule votre équipe de sécurité pour organiser la riposte adéquate et mettre en place des procédures garantes d'une neutralisation efficace. Si votre équipe ne parvient pas à repérer l'activité malveillante, nos consultants l'aideront à mieux utiliser ses technologies de journalisation, de surveillance et d'alertes pour le prochain exercice de simulation. Ils peuvent également souligner des améliorations technologiques nécessaires.

Calendrier et livrables de la mission

La simulation d'attaque Purple Team Assessment s'étend généralement sur trois semaines : deux semaines pour la phase de test et une semaine pour la rédaction du rapport.

LIVRABLES

Un rapport détaillé qui contient :

- Des scores de vos capacités de détection observées lors des attaques simulées
- Une synthèse
- Une explication des détails techniques et de l'évaluation des capacités de votre équipe, avec des instructions pas à pas pour retracer le cheminement ayant conduit à ces résultats
- Les conclusions preuves à l'appui, ainsi que des stratégies de remédiation
- Des recommandations stratégiques pour améliorer la sécurité opérationnelle à plus long terme

Des rapports techniques et exécutifs peuvent être rédigés sur demande.

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

© 2019 FireEye, Inc. Tous droits réservés. FireEye est une marque déposée de FireEye, Inc. Tous les autres noms de marques, de produits ou de services sont ou peuvent être des marques commerciales ou des marques de service de leurs propriétaires respectifs.
M-EXT-DS-FR-FR-000229-01

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Cyber Threat Intelligence (CTI). Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI 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.