FICHE PRODUIT

MANDIANT®
A FireEye® Company

Diagnostic de compromissions

Identifiez les activités malveillantes présentes et passées dans votre environnement

LA DIFFÉRENCE MANDIANT

Mandiant, une entreprise FireEye, possède plus de 14 ans d'expérience de première ligne dans le domaine de la cybersécurité et de la cyberveille. Nos experts en interventions sur incidents ont opéré sur les violations de sécurité les plus complexes 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.

Avantages

- Analyse complète de l'environnement, avec un accent sur la recherche de preuves de compromissions présentes ou passées
- Visibilité sur les risques et expositions systémiques
- Identification des problèmes d'intégrité des dispositifs de sécurité
- Recommandations pour renforcer vos capacités d'intervention sur des incidents futurs
- Flexibilité des déploiements des technologies sur site ou dans le cloud

Dans l'état actuel de la cybersécurité, les violations de sécurité sont inévitables.

Kevin Mandia
PDG, FireEye

Le diagnostic de compromissions Mandiant se compose de trois ingrédients essentiels : 1) notre expérience approfondie des interventions sur les menaces APT, 2) les technologies FireEye et 3) un système de cyberveille leader du marché. Au programme :

- Identification des intrusions présentes ou passées dans votre entreprise
- Évaluation du risque par la détection des vulnérabilités, des failles dans l'architecture de sécurité, des usages inappropriés, des violations de politiques et des mauvaises configurations des systèmes
- Amélioration des capacités d'intervention de votre entreprise sur les incidents futurs

Diagnostics de compromissions : un impératif absolu
Les violations de sécurité dont parlent les médias ne représentent qu'une proportion infime des activités malveillantes perpétrées au niveau mondial. Si vous voulez éviter ce genre de publicité, vous devez établir avec certitude si votre entreprise a déjà été victime d'une compromission et identifier les moyens de réduire votre exposition au risque.

Notre méthodologie
Pour vous offrir un diagnostic rapide, complet et efficace, nous associons notre expérience approfondie de la neutralisation d'incidents à une cyberveille et un ensemble de technologies FireEye leaders. En plus d'identifier les activités malveillantes présentes ou passées dans votre environnement, le diagnostic permet de :

Contextualiser les données grâce à son système de cyberveille
Identification et analyse des motivations des attaquants pour savoir si votre entreprise est en ligne de mire

Identifier les risques
Identification des failles dans l'architecture et la configuration du dispositif de sécurité, y compris les logiciels et correctifs manquants

Faciliter les investigations futures
Recommandations visant à mieux préparer votre équipe de sécurité à ses prochaines interventions sur incidents

FireEye

Les consultants Mandiant exploitent les technologies FireEye pour trouver des preuves d'activités malveillantes sur les terminaux, le trafic réseau, les e-mails et les journaux d'autres dispositifs de sécurité. Ils ont également recours à des techniques d'analyse des données sans signature à la recherche d'attaques auparavant passées inaperçues. Libre aux clients de choisir la combinaison de technologies la mieux adaptée à leur environnement.

- Inspection des terminaux : les agents FireEye Endpoint Security analysent les terminaux Windows, Mac OS et Linux à la recherche d'activités malveillantes en temps réel, y compris les malwares et autres tactiques, techniques et procédures d'attaque. Mandiant vous donne le choix d'un déploiement sur site et dans le cloud.
- Inspection du réseau : les capteurs FireEye Network Security sont déployés en des points stratégiques de votre entreprise pour détecter des signes de compromission (communications CnC de malwares, accès à distance non-autorisés, vols de données, etc.).
- Inspection de la messagerie : sur site ou depuis le cloud, le système FireEye de surveillance de la messagerie peut être configuré pour une inspection passive des e-mails entrants et sortants. L'inspection dynamique des pièces jointes permet aux experts Mandiant d'identifier les intrusions avant même que les solutions basées sur des signatures ne réagissent.
- Inspection des journaux : les experts Mandiant s'appuient sur diverses technologies pour analyser les journaux d'applications et d'infrastructures, et identifier les activités malveillantes.

Inspection des terminaux

- Alertes en temps-réel sur les activités suspectes ou malveillantes
- Détection des malwares courants à l'aide du moteur antivirus intégré à l'agent FireEye
- Prise en charge des systèmes d'exploitation sur plusieurs plateformes
  - Windows
  - Mac OS
  - Linux
- Identification des anomalies susceptibles de révéler la présence de malwares avancés

Inspection du réseau

- Capture de paquets entiers avec signatures de détection personnalisées
- Détection et décodage automatiques du trafic CnC (commande et contrôle) des attaques

Inspection de la messagerie

- Détection des attaques par phishing utilisées par les hackers pour se réimplanter dans un environnement après qu'une attaque ait été neutralisée
- Exploitation de Multi-Vector Virtual Execution™ (MVX), un moteur sans signature conçu pour analyser les pièces jointes et URL des e-mails sur une matrice croisée d'applications, de navigateurs et de systèmes d'exploitation
- Analyses basées sur des images des systèmes d'exploitation Microsoft Windows et Apple Mac OS
- Recherche des menaces dissimulées dans les pièces jointes (y compris les fichiers cryptés et protégés par mot de passe)

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 6 600 clients dans 67 pays, dont plus de 45 % figurent au classement Forbes Global 2000.