FICHE PRODUIT

MANDIANT®
A FireEye® Company

Services d'intervention sur incidents

Analysez, endiguez et neutralisez les incidents de sécurité critiques de façon rapide et efficace, à n'importe quelle échelle.

ÉTUDE DE CAS : MANDIANT EN ACTION

Forte d'un parc informatique de dizaines de milliers d'ordinateurs à travers le monde, cette société internationale de services aux entreprises a fait appel à Mandiant pour intervenir sur une violation potentielle de données clients critiques.

Jour 1 : Quatre heures après la notification de l'attaque, Mandiant a enclenché le déploiement de sa solution cloud d'analyse forensique sur 18 000 systèmes.

- L'investigation a débuté le même jour.
- Des preuves avérées d'une compromission ont été identifiées quatre heures après le début de l'enquête.

Jour 6 : L'essentiel du travail d'enquête a été bouclé. Plus de 18 000 terminaux ont été analysés, avec un diagnostic en direct des réponses des systèmes implémentées sur 80 terminaux.

Jour 7 : Attaque entièrement neutralisée, sans aucune perturbation des activités de l'entreprise. Mandiant a continué à surveiller le réseau pour prévenir toute tentative de récidive.

Jour 11 : Retour à la normale des activités du client.
Toutes les tâches ont été effectuées à distance.

Mandiant agit en première ligne dans le domaine de la cybersécurité et de la cyberveille depuis 2004. 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.

Nos équipes allient des compétences investigatives et une expertise en remédiation acquises lors de milliers d'interventions sur le terrain. Pour mener à bien leur mission, elles font appel à la fois à une cyberveille avancée et à des technologies FireEye de pointe pour la protection du réseau et des terminaux.

Forts de cette longue expérience au contact direct d'incidents de sécurité majeurs, nous sommes mieux placés que quiconque pour accompagner nos clients dans la gestion de tous les aspects d'un incident — de l'intervention technique à la gestion de crise.

Leurs opérations d'investigation et de remédiation gagnent ainsi en efficacité et en rapidité pour leur permettre de se concentrer à nouveau sur l'essentiel : leur cœur de métier.

Présentation
L'utilisation conjointe de solutions hébergées sur site et dans le cloud permet de démarrer immédiatement une investigation sur un incident, tout en respectant les préoccupations des clients quant à la confidentialité de leurs données. En quelques heures, Mandiant peut commencer à analyser les informations et le trafic réseau de milliers de terminaux. Grâce à un accès instantané au référentiel de cyberveille constitué par nos chercheurs de première ligne, auquel viennent s'ajouter d'autres sources, les équipes d'intervention sur incidents de Mandiant bénéficient des informations les plus récentes sur les tactiques, techniques et procédures des attaquants.

Mandiant est bien conscient du fait qu'une intervention efficace sur un incident ou une violation de sécurité ne se limite pas à investiguer, neutraliser la menace et restaurer les systèmes. Nos équipes accompagnent également les dirigeants de l'entreprise sur tous les aspects communication et gestion de crise, notamment les questions d'ordre juridique et réglementaire, ou encore les relations publiques. La gestion de crise est indispensable pour limiter l'atteinte à l'image de marque et les éventuelles poursuites judiciaires.

Tableau 1. Les domaines d'intervention type de Mandiant :

Vol de capital intellectuel	Vol de secrets commerciaux ou d'autres informations sensibles
Crime financier	Vol de données de cartes de paiement, transferts de fonds illicites via les systèmes ACH et EFT, extorsions et ransomwares
Informations d'identification personnelle (PII)	Divulgation d'informations utilisées pour identifier des personnes
Données médicales personnelles (PHI)	Divulgation de données médicales personnelles
Menaces internes	Activités abusives ou illégales réalisées par des salariés, des fournisseurs et d'autres collaborateurs internes à l'entreprise
Actes de sabotage	Attaques dont le seul but est de nuire à l'entreprise ciblée, en rendant impossible toute restauration des systèmes ou des informations

FireEye

LA DIFFÉRENCE MANDIANT

- **Experts de l'investigation :** Les équipes Mandiant possèdent des compétences et une expérience acquises lors de milliers d'investigations parmi les plus vastes et les plus complexes au monde.
- **Cyberveille :** Le système de cyberveille de pointe de FireEye intègre les renseignements recueillis lors de nos interventions sur incidents ainsi qu'une masse d'informations collectées par les technologies FireEye et les sources iSIGHT.
- **Technologies :** Sur site ou dans le cloud, les technologies FireEye dernier cri permettent de démarrer immédiatement les investigations. Elles nous aident notamment à intervenir rapidement et à plus grande échelle, offrant une visibilité sur le trafic réseau et les terminaux Microsoft Windows, Linux et Mac OS X. Une solution automatisée d'exécution en environnement sandbox, reposant sur la technologie MVX de FireEye Network Security, identifie les menaces qui échappent aux solutions de détection basées sur les signatures.
- **Gestion de crise :** Nos équipes d'intervention possèdent une longue expérience de la communication de crise dont ils peuvent faire profiter nos clients — qu'il s'agisse de communications internes, de relations publiques ou d'obligations en matière de divulgation.
- **Analyse antimalware :** Des chercheurs et des informaticiens spécialisés dans la rétroconception analysent les malwares découverts lors d'une investigation afin d'en comprendre les fonctions et le mode opératoire.

Notre méthodologie

La méthodologie d'investigation de Mandiant inclut une analyse des hôtes et du réseau pour établir un diagnostic global et complet de l'environnement. Nos interventions sont conçues pour aider les clients à réagir de façon appropriée et revenir rapidement à la normale, tout en assurant le respect de leurs obligations réglementaires et en préservant leur image de marque. Les investigations de Mandiant portent sur ces principaux points de contrôle :

- Applications, réseaux, systèmes et comptes d'utilisateur affectés par l'incident
- Malwares utilisés et vulnérabilités exploitées
- Informations volées ou consultées

Analyse de l'incident

1. **Déploiement de technologies / investigation des pistes initiales :** Nous déployons des technologies adaptées pour résoudre l'incident de façon rapide et efficace. En parallèle, nous étudions les pistes initiales fournies par le client pour établir des indicateurs de compromission (IoC) qui permettront d'identifier les activités de l'attaquant, tout en analysant l'environnement pour dégager tous les indices d'une activité malveillante.

2. **Planification de la gestion de crise :** Nous accompagnons les dirigeants, les équipes juridiques, les chefs de département et les responsables de la sécurité dans l'élaboration d'un plan de gestion de crise.

3. **Délimitation du périmètre de l'incident :** Nous surveillons en temps réel les activités de l'attaquant et recherchons des preuves forensiques d'activités malveillantes antérieures, afin de déterminer l'étendue de l'incident.

4. **Analyse approfondie :** Nous analysons les actions effectuées par l'attaquant pour identifier le vecteur d'attaque initial, établir une chronologie de l'attaque et identifier l'étendue de la compromission. Cette analyse peut inclure les éléments suivants :
   - Analyse en direct des réponses des systèmes
   - Analyse forensique
   - Analyse du trafic réseau
   - Analyse des journaux
   - Analyse antimalware

5. **Évaluation des dommages :** Nous identifions les applications, les systèmes et les sites affectés ainsi que les informations divulguées.

6. **Remédiation :** Nous mettons au point une stratégie d'endiguement et de remédiation sur mesure, basée à la fois sur les actions de l'attaquant et les impératifs de l'entreprise. Cette démarche a pour but de bloquer l'accès à l'attaquant et de renforcer la sécurité globale de l'environnement pour prévenir toute récidive, ou tout au moins en limiter les dommages.

Livrables

Rapports de synthèse, d'investigation et de remédiation conformes aux exigences d'audits externes.

- **Rapport de synthèse :** Synthèse générale décrivant la chronologie de l'intervention et le processus d'investigation, les principaux résultats et les activités d'endiguement/éradication.
- **Rapport d'investigation :** Détails sur la chronologie de l'attaque et son mode opératoire. Ce rapport recense les ordinateurs, sites et comptes d'utilisateur affectés, ainsi que les informations volées ou exposées au risque.
- **Rapport de remédiation :** Détails sur les mesures d'endiguement/éradication appliquées, y compris des recommandations stratégiques pour renforcer la sécurité de l'entreprise.

Vous pensez être victime d'un incident de sécurité ? Écrivez-nous à **investigations@mandiant.com** ou rendez-vous sur **https://www.fireeye.com/company/incident-response.html**

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