FIREEYE™

FICHE PRODUIT

# Digital Threat Monitoring

## Système de pré-alerte couvrant tout votre environnement digital

### EN BREF

- Surveillance en temps réel des menaces digitales qui pèsent sur vos ressources
- Pré-alerte à la moindre mention ou au moindre signe de ciblage de votre entreprise ou de vos données
- Notification d'exposition ou de compromission de votre entreprise ou de vos données
- Threat Intelligence contextuelle fournie par des experts de la sécurité
- Opérations de reconnaissance adaptées aux spécificités de votre entreprise
- Accompagnement sur mesure par un analyste

Les cyberdéfenses traditionnelles sont conçues pour protéger tout ce qui se trouve à l'intérieur du réseau, c'est-à-dire en périphérie, sur les serveurs et sur les terminaux.

Mais dans le monde hyperconnecté d'aujourd'hui, il est indispensable d'étendre la protection aux ressources qui se situent au-delà de ce périmètre : votre marque, vos collaborateurs, votre communauté de partenaires, etc. Bref, que les ressources soient internes ou externes au pare-feu, le besoin en visibilité reste le même.

Fruit de l'alliance unique entre des technologies avancées et la Threat Intelligence la plus pointue du marché, FireEye Digital Threat Monitoring™ réduit le risque en vous apportant une visibilité totale sur les menaces auxquelles vos ressources sont exposées. Fuite d'identifiants, exposition publique de données, menaces sur les ressources, dommages financiers, perte de crédibilité… Digital Threat Monitoring vous aide à agir proactivement contre tous ces risques. Quant à nos experts en CTI, ils savent exploiter tout le potentiel de FireEye Threat Intelligence pour vous livrer des éclairages sur des facettes du web autrement inaccessibles.

**Plus de visibilité, plus d'éclairages**

Le service Digital Threat Monitoring (DTM) est équipé d'une technologie propriétaire de reconnaissance automatique, destinée à collecter et analyser les contenus issus du web public et du dark web. DTM cible principalement les sites que les attaquants utilisent pour communiquer. Le service effectue une analyse à partir de requêtes par mots-clés (marque, noms de dirigeants, entreprises partenaires…) que vous aurez vous-même définis, puis génère des alertes sur les correspondances suspectes.

Ces alertes peuvent être consultées sur le tableau de bord du portail FireEye Intelligence. Chaque alerte comporte divers attributs (statut, origine, gravité, etc.), ainsi que des informations visant à faciliter la gestion des ressources sous surveillance. Le tableau de bord donne également la possibilité d'enclencher des actions spécifiques (par ex. contacter un analyste FireEye) sur une ou plusieurs alertes.

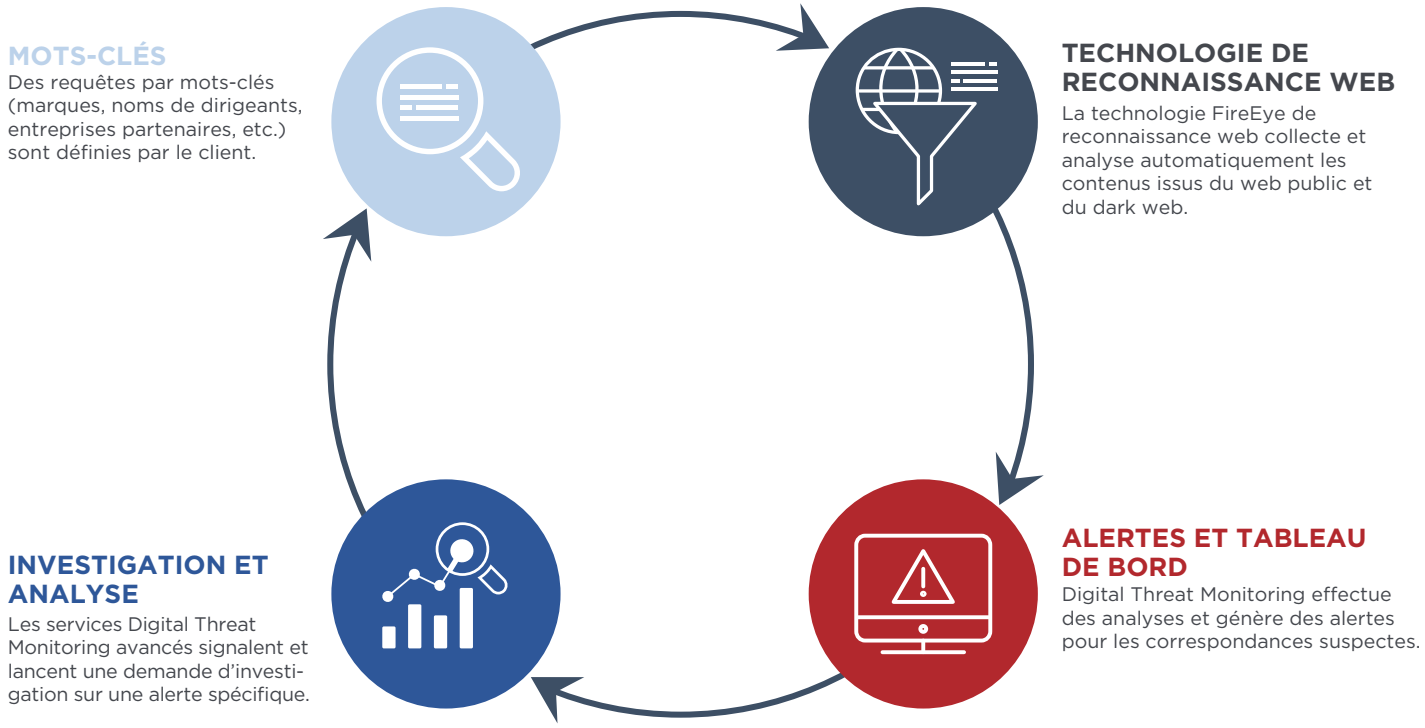


**Figure 1.** Fonctionnement de FireEye Digital Threat Monitoring

Les services Digital Threat Monitoring premium vous permettent de signaler et de lancer une demande d'investigation sur une alerte spécifique. Un analyste FireEye effectue alors un diagnostic détaillé qui vous aidera à mieux cerner la nature de la menace. Si besoin, il partagera avec vous toutes les informations utiles dont il dispose, ainsi que les données de la FireEye Threat Intelligence en lien avec le problème signalé.

**Tableau 1.** Description du service FireEye Digital Threat Monitoring

L'option de déploiement que vous choisissez dépend de la durée de la mission et du niveau de support dont vous avez besoin.

| Service | Description |
|---|---|
| **Digital Threat Assessment** | Bilan ponctuel réalisé sur 30 jours à l'aide de requêtes par mots-clés sélectionnées par le client. Les analystes FireEye délivrent un rapport sur les menaces identifiées, accompagné d'un ensemble d'éclairages utiles. |
| **Digital Threat Monitoring Standard (sur abonnement)** | Surveillance continue des requêtes par mots-clés sélectionnées par le client, sur le web public, le deep web et le dark web. Les correspondances suspectes génèrent des alertes consultables sur le portail FireEye Intelligence. |
| **Digital Threat Monitoring Advanced (sur abonnement)** | Prestations identiques à l'option Standard et jusqu'à 40 investigations réalisées par des analystes FireEye. |
| **Digital Threat Monitoring Enterprise (sur abonnement)** | Prestations identiques à l'option Standard et jusqu'à 80 investigations réalisées par des analystes FireEye. |

Le tableau suivant met en évidence les principales différences entre les différentes formules Digital Threat Monitoring.

**Tableau 2.** Comparatif des fonctionnalités du service Digital Threat Monitoring

| Prestations | Digital Threat Assessment | Digital Threat Monitoring Standard | Digital Threat Monitoring Advanced | Digital Threat Monitoring Enterprise |
|---|---|---|---|---|
| **Intégration** | Oui | Oui | Oui | Oui |
| **Mots-clés illimités** | Oui | Oui | Oui | Oui |
| **Nombre illimité d'utilisateurs** | – | Oui | Oui | Oui |
| **Alertes sur les menaces** | – | Oui | Oui | Oui |
| **Catégories de mots-clés** | Toutes | Toutes | Toutes | Toutes |
| **Investigations** | – | via le service Expertise On Demand | 40 par an / 10 par trimestre | 80 par an / 20 par trimestre |
| **Accès au portail FireEye Intelligence** | – | Oui | Oui | Oui |
| **Récapitulatif des alertes sur les menaces digitales** | – | Oui | Oui | Oui |
| **Gestion des mots-clés en self-service** | – | Oui | Oui | Oui |

**Système de pré-alerte face à des menaces en perpétuelle évolution**

FireEye Digital Threat Monitoring émet des alertes dès que votre marque, vos données ou les noms de vos dirigeants sont mentionnés, ciblés ou exposés. Cette solution permet d'identifier les compromissions, les expositions de données et les menaces digitales présentes à la fois sur web public, le deep web et le dark web. Objectif : vous éclairer sur le niveau d'exposition de votre entreprise et agir sur ces différents leviers de votre programme de sécurité :

- **Pertinence –** Opérations de reconnaissance adaptées aux spécificités de votre entreprise
- **Visibilité –** Notification d'exposition ou de compromission de votre marque ou de vos données
- **Préparation –** Pré-alerte à la moindre mention ou au moindre signe de ciblage de votre entreprise ou de vos données
- **Expertise –** Threat Intelligence contextuelle et analyses effectuées par les meilleurs experts en sécurité du marché
- **Menaces individuelles –** Collecte des données et génération d'alertes en temps réel selon le profil de menace digitale de votre organisation

Pour en savoir plus sur FireEye Digital Threat Monitoring et sa capacité à détecter les menaces au-delà de votre périmètre, rendez-vous sur **https://www.fireeye.fr/solutions/cyber-threat-intelligence/digital-threat-monitoring.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 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.