FIREEYE™

FICHE PRODUIT

Abonnements Threat Intelligence

Des données qui profitent à toute votre entreprise

EN BREF

- Profitez d'une mine d'informations CTI exploitables sur de nombreux sujets
- Étendez votre visibilité au-delà du cycle classique d'une attaque en y ajoutant du contexte et en y assignant un niveau de priorité
- Protégez plus efficacement vos ressources et limitez les risques pour votre entreprise
- Concentrez vos programmes et ressources de sécurité sur les attaques les plus susceptibles de vous frapper
- Profitez d'une Threat Intelligence tactique, stratégique et opérationnelle
- Traitez les alertes par priorité pour corriger les vulnérabilités informatiques les plus urgentes.

Aujourd'hui, les cybercriminels sont souvent mieux formés, financés et équipés qu'un grand nombre d'équipes de sécurité. D'où la complexité et la puissance destructrices croissantes de leurs attaques. Pour faire face à ces nouvelles menaces, il faudrait une véritable armée d'experts en sécurité. Une option très onéreuse quand on sait que ces profils sont très demandés.

Les directions de la sécurité des systèmes d'information (DSSI) cherchent en permanence à acquérir des compétences et améliorer leur efficacité pour renforcer leurs capacités de réponse à des menaces réelles. Cependant, le budget alloué est souvent limité.

Les abonnements FireEye Threat Intelligence permettent de résoudre cette équation. Très économique, cette solution vous livre une véritable mine d'informations de sécurité, tant sur les plans tactique, que stratégique et opérationnel.

Tableau 1. Avantages de FireEye Threat Intelligence.

Permet d'identifier...	Avantages
les menaces et les hackers susceptibles de cibler votre entreprise, votre secteur d'activité ou votre région	Déploiement de mesures de sécurité ciblées sur ce type d'attaques
les alertes à investiguer en priorité, avec toutes les informations contextuelles nécessaires	Détection plus rapide, réduction de l'accoutumance aux alertes et développement des connaissances des équipes
les vulnérabilités à corriger en priorité, car déjà exploitées dans des entreprises similaires.	Priorisation des actions correctives et réduction des probabilités de compromission.

Afin de répondre aux besoins spécifiques de chaque entreprise, FireEye propose différentes formules d'abonnement Threat Intelligence :

- **Fusion :** Informations détaillées sur les menaces passées, actuelles et éventuellement futures. Prestations incluses : contenu des forfaits Operational, Cyber Crime, Cyber Espionage, une grande partie de l'offre Cyber Physical et une version de FireEye Digital Threat Monitoring.
- **Operational :** Analyse technique des malwares et modes opératoires utilisés par les hackers. Vous disposez d'un accès à une base de données répertoriant les caractéristiques des malwares et les profils des hackers, ainsi qu'à des indicateurs de compromission (IOC) lisibles par machine pour une meilleure vision d'ensemble.
- **Cyber Physical :** Informations exploitables sur les cybermenaces pesant sur les environnements industriels et les technologies opérationnelles (OT). Comprend toute la Threat Intelligence FireEye ciblée sur les systèmes de contrôle industriels (ICS) et les technologies opérationnelles.
- **Cyber Crime :** Analyse approfondie et pistage des hackers spécialisés dans le crime financier : motivations, cibles privilégiées et modes opératoires.
- **Cyber Espionage :** Informations sur des groupes APT connus (y compris les États commanditaires, les entités ciblées et les modes opératoires) pour aider les équipes de sécurité à mieux comprendre et déjouer les menaces immédiates ou en gestation.
- **Strategic :** Bilans des menaces par secteurs et régions clés du globe : contexte géopolitique, évolution du champ des cybermenaces et prévisions des évolutions à court et à long terme.
- **Vulnerability :** Inventaire des failles logicielles identifiées sur de nombreuses technologies, le tout assorti d'une analyse par FireEye des risques associés et des mesures correctives recommandées.

Ces informations sont généralement présentées sous forme de rapports. Le cas échéant, nous proposons également des IOC et des données lisibles par machines qui pourront s'intégrer à vos solutions de sécurité existantes (SIEM ou gestionnaire de failles). Nos abonnements FireEye Threat Intelligence donnent également accès aux ressources suivantes :

- **Portail FireEye Intelligence :** Vous pouvez y consulter vos rapports d'analyse, mais également toute la base de données de votre abonnement Threat Intelligence. La base est interrogeable selon différents critères de recherche : groupes de hackers, malwares, secteurs d'activité, etc. Vous pouvez également télécharger les IOC associés à chaque type de CTI.
- **Accès aux analystes :** Nos analystes spécialisés en Threat Intelligence et en audit technique vous aideront à mieux appréhender les menaces et leurs auteurs. Vous aurez ainsi une bien meilleure idée des risques et événements de sécurité qui vous concernent directement.
- **Options de déploiement :** Vous pouvez choisir la fréquence et le format des rapports d'analyse, notamment par e-mail ou note de synthèse.
- **Bulletin d'analyse quotidien :** Cet e-mail quotidien suit pour vous toute l'actualité de la sécurité et vous livre une analyse complète des événements qui font le buzz. Vous profitez ainsi d'une revue de presse commentée par FireEye, avec un fact-checking et des compléments d'informations qui vous aideront à mieux comprendre la menace et les moyens de s'en protéger.
- **Intelligence API :** Ce point d'intégration machine-to-machine vous permet d'exploiter toute la Threat Intelligence et les IOC de FireEye sur vos propres systèmes de sécurité, de gestion des opérations réseaux, de gestion des vulnérabilités et de réponse à incident.
- **Plugin de navigateur :** Ce plugin permet d'intégrer FireEye Threat Intelligence à votre navigateur web. Il analysera automatiquement les caractéristiques techniques (adresse IP, domaine, hachage) de toute page consultée, interrogera l'Intelligence API pour toute CTI pertinente et créera un lien vers cette information le cas échéant.
- **Outils d'analyse :** Les clients peuvent recourir à ces utilitaires pour interroger FireEye Threat Intelligence sur un nom de domaine, une adresse IP ou une menace potentielle. Ils peuvent également y importer des fichiers suspects pour analyse.

Dans un secteur de la sécurité en constante évolution, même les meilleurs experts ne peuvent pas tout savoir sur les hackers, les menaces, les vulnérabilités, les méthodes de remédiation et les techniques de traque. Avec les abonnements FireEye Threat Intelligence, vos équipes de sécurité ont accès aux connaissances, à l'expérience, à la visibilité et aux capacités d'analyse d'un acteur de premier plan dans la lutte contre le cybercrime. Elles profiteront ainsi d'une mine d'informations compilées au fil des ans par les plus grands experts en cybersécurité.

L'avantage FireEye

Grâce à une surveillance minutieuse de l'activité cybernétique et des opérations de Threat Intelligence de grande envergure, FireEye a su acquérir une connaissance incomparable des cybermenaces et de leurs auteurs. Nous recoupons les données télémétriques avec nos informations sur les attaquants, les victimes et les campagnes pour produire une Threat Intelligence d'une précision inégalée. Pour ce faire, nous déployons les grands moyens :

- Des chercheurs en sécurité dans 22 pays et parlant plus de 30 langues. Ces experts de terrain sondent le deep web et le dark web pour mieux connaître les méthodes, les motivations et les infrastructures technologiques des attaquants.
- Plus de 15 000 capteurs réseau bidirectionnels installés chez nos clients pour tout savoir des menaces qui les frappent.
- Les enseignements tirés des investigations d'attaques et des modes opératoires d'attaques réussies observés par FireEye Mandiant, leader mondial de la réponse à incident.
- La base de données la plus complète du secteur, qui regroupe toutes les informations recueillies par nos experts et nos technologies lors de chaque événement et incident analysé.
- FireEye figure dans la catégorie Leader du Forrester New Wave™: External Threat Intelligence Services (3ème trimestre 2018).

SUPPORT CLIENT DÉDIÉ

Nous proposons trois formules de prestation et de support :

NIVEAU 1

Baseline : Ressources et processus de base pour l'utilisation du portail Threat Intelligence et la configuration de l'Intelligence API selon les besoins de votre entreprise.

NIVEAU 2

Intelligence Coordination : Les prestations de l'offre Baseline, plus : un Intelligence Enablement Manager (IEM) attitré, la possibilité de consulter les analystes CTI de FireEye, des comptes-rendus de sécurité trimestriels et des bilans formels semestriels.

NIVEAU 3

Intelligence Optimization : Les prestations Intelligence Coordination, plus : un analyste Intelligence Optimization attitré, un accès plus poussé aux analystes CTI de FireEye, des rapports personnalisés, des ateliers stratégiques et des séances d'information sur les menaces.

Pour en savoir plus, rendez-vous sur : **https://www.fireeye.com/solutions/cyber-threat-intelligence-subscriptions.html** et consultez le **rapport Forrester**.

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 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.

FIREEYE™