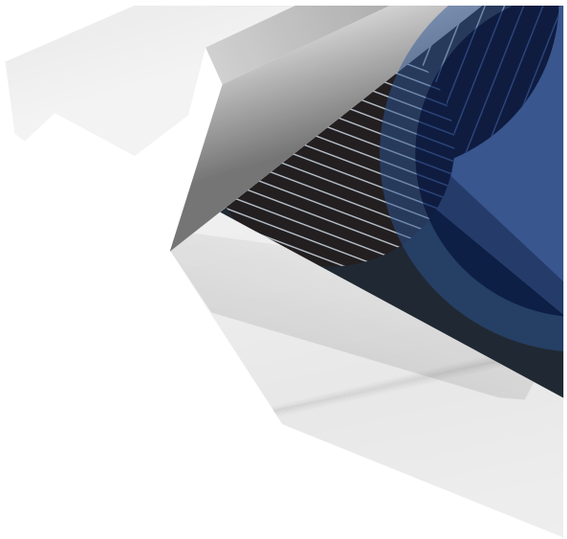

FICHE PRODUIT

Portfolio FireEye Threat Intelligence

Une Threat Intelligence évolutive pour une contextualisation à tous les niveaux de l'entreprise

EN BREF

- Amélioration des investigations et des plans de réponse grâce à une Threat Intelligence contextuelle directement exploitable
- Visibilité sur le cycle de vie des attaques grâce à des informations sur les phases précédant et suivant le lancement d'une attaque
- Accès à des informations exploitables et adaptées à vos besoins en sécurité

La réponse face aux menaces en présence

Les entreprises sont engagées dans un combat inégal contre des attaquants habiles et organisés, qui bénéficient d'importants moyens et utilisent des techniques très ciblées. Par conséquent, les équipes de sécurité éprouvent régulièrement des difficultés à identifier les cybermenaces les plus graves et à les traiter par ordre de priorité.

La plupart des entreprises s'en remettent à des flux de Threat Intelligence tactique basés sur des signatures pour assurer leur sécurité. Or, ces derniers sont incapables d'anticiper les attaques ou d'offrir le contexte nécessaire pour les neutraliser. Pire, ils augmentent le volume d'alertes en générant des faux positifs, ce qui complique considérablement la détection des attaques et induit un sentiment de sécurité trompeur. D'où l'importance pour les entreprises d'exploiter une Threat Intelligence adaptée. Elles renforceront ainsi leurs capacités de détection et de réponse, tout en améliorant l'efficacité de leurs opérations.

Des informations contextualisées pour neutraliser les menaces

Plateforme unique sur le marché, FireEye Threat Intelligence est est le fruit de la collaboration de plus de 150 chercheurs et experts en sécurité FireEye. Ces spécialistes s'appuient sur plusieurs décennies d'expérience pour fournir des renseignements sur les cybercriminels, leurs motivations, leurs intentions et leurs méthodes.
Avantages pour les entreprises :

- Gestion et diagnostic proactifs des risques
- Détection et prévention des attaques
- Contextualisation des alertes générées

FireEye Threat Intelligence se fonde sur trois sources principales :

- Des informations contextuelles issues de l'environnement de développement des attaques avant même qu'elles ne soient lancées

- Une visibilité fournie par les intervenants de première ligne face aux cybermenaces les plus avancées partout dans le monde
- La technologie MVX™ capable d'identifier des attaques jamais observées auparavant

Grâce à une Threat Intelligence complète et directement exploitable, les entreprises peuvent mieux gérer les risques et intervenir en cas d'attaque.

Une Threat Intelligence modulable en fonction de vos besoins

FireEye aide votre entreprise à opérationnaliser sa Threat Intelligence, avec à la fois une solution autonome et une intégration de données aux technologies FireEye, notamment DTI (Dynamic Threat Intelligence) et ATI (Advance Threat Intelligence).

Threat Intelligence autonome

FireEye Threat Intelligence s'intègre à n'importe quelle solution de sécurité FireEye, mais aussi à toutes vos infrastructures et tous vos outils existants. Cette solution complète fournit des renseignements à la fois d'ordre tactique, opérationnel et stratégique. FireEye Threat Intelligence va bien plus loin que les simples flux de données fournis par les solutions classiques : elle propose des informations prospectives et contextuelles, essentielles pour établir des défenses proactives, prioriser les alertes et ressources, et améliorer l'intervention sur incidents.

Elle se décline en plusieurs formats et propose un accès direct aux analystes et un support client dédié. Formats disponibles :

- Interconnexions machine-to-machine (M2M) via la Threat Intelligence API
- Informations lisibles par l'humain via le portail FireEye Intelligence
- Analyse quotidienne (Threat Media Highlights) des principaux événements de sécurité dans le monde

Cette Threat Intelligence peut être adaptée au rôle ou à la fonction des utilisateurs. Novices ou chevronnées, les équipes de sécurité disposent ainsi du contexte nécessaire pour décrypter les intentions et activités des attaquants. Les abonnements FireEye Threat Intelligence se déclinent en cinq cas d'usage : tactique, opérationnel, intégré, décisionnel et axé sur les vulnérabilités.

Threat Intelligence intégrée aux technologies FireEye

Souscrire aux abonnements Threat Intelligence pour vos technologies FireEye vous permet d'améliorer vos capacités de détection, d'investigation et de réponse à incident. Ces abonnements complémentaires vous sont proposés lors de l'achat de produits de détection et d'investigation FireEye et se déclinent en deux options : DTI et ATI.

Dynamic Threat Intelligence (DTI)

Le moteur FireEye Multi-Vector Virtual Execution (MVX) intègre des fonctions de machine learning et d'analyse qui décodent les intentions des attaquants ainsi que leurs tactiques, techniques et procédures pour vous offrir des fonctions de détection inégalées. Mis à jour toutes les heures, DTI vous permet d'identifier les attaques les plus récentes, repérées au sein du réseau mondial de clients de FireEye.

Advanced Threat Intelligence (ATI)

Lorsque FireEye détecte une attaque, ATI vous en fournit le contexte nécessaire pour prioriser vos ressources et mettre en place un plan de réponse approprié. Cybercriminels à l'origine de la menace, motivations possibles des attaques, informations générales et sectorielles sur les malwares utilisés et d'autres indicateurs… toutes ces informations sont autant de données précieuses pour rechercher les auteurs d'attaque au sein de votre environnement.

La différence FireEye Threat Intelligence

FireEye Threat Intelligence fournit des éclairages approfondis sur les attaquants, leurs motivations, leurs intentions et leurs méthodes.

- Visibilité inégalée sur le cycle de vie complet d'une attaque ainsi que les motivations, outils et procédures des attaquants. Accès en amont et en temps réel aux informations sur les menaces les plus récentes et les plus élaborées grâce aux centaines d'analyses de l'écosystème de développement des attaques. Plus de dix ans d'expérience dans l'investigation de cyberattaques majeures et connaissances codifiées des objectifs des attaquants issues d'un réseau mondial de 16 millions de nœuds virtuels de détection des menaces.
- Moteur d'analyse flexible et évolutif pour traquer des attaquants dont les méthodes ne cessent d'évoluer. Base de données de graphes mathématiques alimentée par plus de 125 millions de postes, qui modélise de façon dynamique les relations et tactiques employées par les groupes de cyberattaquants, leurs opérations et leurs commanditaires.
- Experts spécialisés dans différents domaines pour surveiller et analyser les aspects politiques et financiers de plus de 16 000 cybermenaces dans le monde.

Ce genre de Threat Intelligence permet aux équipes de sécurité de réduire la surface d'attaque et de passer d'une posture réactive, basée sur les alertes et gourmande en ressources, à une démarche proactive, permettant de réagir efficacement et rapidement aux menaces.

Tableau 1. Visibilité sur la chaîne d'attaque étendue

	DTI	ATI	FireEye Threat Intelligence
Phase de l'attaque dont est issue l'information	Attaque	Attaque	Avant, pendant et après l'attaque
Type d'information	Tactique	Contextuelle	Outils complets d'analyse et de Threat Intelligence
Détection par les appliances FireEye	X		
Profils de détection pour les appliances FireEye		X	
Corrélation des alertes FireEye en fonction des emplacements géographiques et secteurs d'activité		X	
Attribution d'alertes FireEye à des auteurs de menaces connus		X	
Profils des groupes de cyberattaquants			X
Profils sectoriels			X
Profils des familles de malwares			X
Actualité des menaces			X
Indicateurs de menace via l'API			X
API et kit de développement logiciel (SDK) pour intégration avec des outils non-FireEye			X
Plug-in de navigateur pour l'analyse, les recherches et l'accès aux alertes sur le portail Threat Intelligence			X
Attribution des indicateurs de menace à des auteurs de menaces connus			X
Couverture étendue des auteurs de menaces			X
Threat Intelligence décisionnelle			X
Suivi des vulnérabilités des systèmes d'entreprise			X
Suivi des vulnérabilités des infrastructures critiques			X
Suivi des exploitations			X
Contexte des alertes dans l'infrastructure informatique existante			X

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. | info@FireEye.com

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