MANDIANT®

FICHE PRODUIT

FireEye Threat Intelligence Application Programming Interface (API)

Intégrez Mandiant Threat Intelligence à vos systèmes de sécurité

FONCTIONNALITÉS

L'API FireEye vous permet d'intégrer la Threat Intelligence de FireEye et de l'adapter à vos enjeux de sécurité. Au menu :

- **Structured Threat Information Expression (STIX) 2.1 –** Le format de données utilisé (JSON) facilite l'échange de Threat Intelligence tout en préservant les relations entre objets de données.
- **Livraison rapide –** Découplage des indicateurs et des rapports, et livraison en quasi temps réel dans certains cas pour plus de réactivité et d'exploitabilité.
- **Score de fiabilité –** Notation de la fiabilité des indicateurs sur une échelle de 0 à 100.
- **Digital Threat Monitoring –** Les clients peuvent recevoir et filtrer (selon les options utilisateur paramétrées) de vastes quantités de données provenant de Mandiant Digital Threat Monitoring.
- **Métadonnées avancées –** Des champs de métadonnées sont inclus pour la révocation d'indicateurs et l'ajout de références externes aux rapports.
- **Reporting flexible –** Création de rapports CTI dans des formats lisibles par les machines (STIX 2.1) et les humains (PDF, HTML).
- **Recherches de Threat Intelligence –** Recherches basées sur des schémas d'attaque ou des relations pour mieux cibler l'information et recevoir des résultats pertinents.

La Mandiant Threat Intelligence API a été spécialement conçue pour intégrer la Threat Intelligence de Mandiant aux flux CTI de nos clients. Ces derniers disposent ainsi de tous les éléments nécessaires pour fiabiliser leurs décisions de sécurité au quotidien.

Cette API permet d'intégrer une Threat Intelligence de pointe à vos processus de protection, de détection, d'investigation et de réponse. Elle se fond dans votre infrastructure de sécurité et dans vos outils de gestion de la conformité. Mandiant Threat Intelligence API sert de trait d'union entre vos technologies de sécurité et la plateforme cloud Mandiant Threat Intelligence, le référentiel CTI le plus complet de la planète hébergeant plus d'une décennie de données.

Options d'intégration simples et flexibles

La Mandiant Threat Intelligence API permet une intégration machine-à-machine des données CTI les mieux contextualisées du marché. Elle fournit un accès automatisé aux indicateurs de compromission (adresses IP, noms de domaines, URL exploités, etc.), mais aussi des informations sur les auteurs d'attaques. L'API est compatible avec de multiples langages de programmation : Python, Java, PHP, C++ et C#. Pour plus d'infos, consultez la **documentation Mandiant Threat Intelligence API complète en ligne**.

Tableau 1. Caractéristiques de la Mandiant Threat Intelligence API v.3.	
Indicateurs	Indicateurs sans rapport et rapports avec indicateurs (indicateurs non rattachés à des rapports ET indicateurs provenant de rapports)
Rapports	Formats compatibles : • HTML • PDF • STIX 2.1 JSON
Auteurs / Malwares	Auteurs, familles de malwares et relations répertoriés dans les indicateurs et rapports
Recherches	Recherches basées sur les relations et schémas d'attaque
Recherches croisées	Recherches basées sur les relations

Applications

L'accès instantané à Mandiant Threat Intelligence vous permet de fiabiliser vos décisions, processus et priorités les plus critiques. Vous passez ainsi d'une posture réactive à une approche résolument proactive. L'API a un rôle essentiel à jouer dans plusieurs aspects de votre écosystème de sécurité :

- **Opérations de sécurité –** Comparez les indicateurs de compromission (IOC) avec les événements identifiés par votre solution SIEM ou vos plateformes d'analyse de sécurité, distinguez les alertes importantes des éléments parasites et automatisez la sélection des événements à traiter en priorité.
- **Réponse à incident –** Accédez à des données CTI complètes directement au sein des systèmes de réponse à incident, d'analytique et d'analyse forensique que vous utilisez quotidiennement.
- **Gestion des vulnérabilités et des correctifs –** Recevez des données sur les vulnérabilités et exploits, souvent avant même leur recensement dans la National Vulnerability Database américaine ou l'attribution d'une référence CVE.
- **Opérations réseau –** Bénéficiez d'indicateurs de compromission extrêmement fiables pour neutraliser les attaques en toute confiance.

Pour découvrir comment Mandiant vous aide à connaître la menace pour mieux la combattre, rendez-vous sur : **www.FireEye.com/intel**

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 Mandiant Solutions

Mandiant Solutions conjugue une CTI leader, une expérience de terrain et une validation continue des systèmes de sécurité pour donner aux entreprises les outils dont elles ont besoin pour augmenter l'efficacité de leur sécurité et réduire leur exposition au risque.

MANDIANT®