FIREEYE THREAT INTELLIGENCE

UNE VISIBILITÉ INÉGALÉE SUR LES ATTAQUANTS, LES VICTIMES ET LES RÉSEAUX DU MONDE ENTIER

PRÉSENTATION

Trop souvent, les entreprises sont engagées dans un combat inégal. Elles se retrouvent démunies face à des pirates habiles et organisés, qui bénéficient d'importants moyens et utilisent des techniques très ciblées. 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 cyberveille tactique basés sur des signatures pour assurer leur sécurité. Or, ceux-ci sont malheureusement dépassés et incapables d'anticiper les attaques ou d'offrir le contexte nécessaire pour les neutraliser. Pire encore, 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. Une solution de cyberveille appropriée peut aider les entreprises à améliorer leur capacité de détection et d'intervention tout en diminuant le coût total de possession.

FIREEYE ISIGHT INTELLIGENCE : DES INFORMATIONS CONTEXTUALISÉES POUR NEUTRALISER LES MENACES

FireEye iSIGHT® Intelligence assure aux entreprises une cyberveille tactique, opérationnelle et stratégique digne des moyens déployés par la puissance publique. En fournissant des informations pertinentes sur les attaquants, leurs motivations, leurs objectifs et leurs méthodes, la solution offre aux entreprises les avantages suivants :

- Gestion et diagnostic proactifs des risques
- Détection et prévention des attaques
- Établissement du contexte des alertes générées

FireEye iSIGHT Intelligence se fonde sur trois sources principales :

- Des informations contextuelles issues de l'environnement de développement des attaquants avant même qu'ils ne lancent les attaques
- 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 cyberveille complète et directement exploitable, les entreprises peuvent mieux gérer les risques et intervenir en cas d'attaques.

POINTS FORTS

- Accès à une cyberveille complète, issue de la surveillance de plus de 16 000 auteurs de menaces, d'interventions sur incidents menées depuis plus de 10 ans et de milliers de déploiements dans le monde
- Visibilité sur le cycle de vie des attaques grâce à une cyberveille détaillant les phases qui précèdent et suivent les attaques
- Abonnement à plus de 100 rapports mensuels de cyberveille stratégique détaillant les motivations des attaquants
- Amélioration des investigations et des plans d'intervention grâce à une cyberveille contextuelle directement exploitable

FireEye
SECURITY REIMAGINED

UNE CYBERVEILLE MODULABLE EN FONCTION DE VOS BESOINS

Selon les exigences de votre dispositif de sécurité, FireEye propose plusieurs options destinées à opérationnaliser votre cyberveille :

Solution de cyberveille autonome

La cyberveille de FireEye iSIGHT Intelligence peut être intégrée à l'infrastructure et aux outils existants. Il s'agit d'une solution de cyberveille tactique, opérationnelle et stratégique digne des moyens déployés par la puissance publique. Elle 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. En tant que solution autonome, iSIGHT est disponible aux formats suivants :

- Format M2M (machine-to-machine) via l'API iSIGHT
- Format lisible par l'homme sur le portail MySIGHT
- E-mail journalier « L'actualité des menaces » (Threat Media Highlights) pour une analyse des principaux événements de sécurité partout dans le monde

Les entreprises peuvent s'abonner et recevoir chaque mois plus de 100 rapports qui incluent une cyberveille stratégique détaillée sur les motivations des attaquants ainsi que des informations de cyberveille opérationnelle et tactique. Ces rapports permettent aux différents membres de l'équipe de sécurité de s'informer sur des sujets importants pour mieux répondre aux questions de leurs dirigeants.

Cyberveille intégrée à la technologie FireEye

Améliorez vos capacités de détection, d'investigation et d'intervention grâce aux abonnements iSIGHT Intelligence en complément de vos produits FireEye. Ces abonnements complémentaires vous sont proposés lors de l'achat de produits de détection et d'investigation FireEye et se déclinent en trois options.

Dynamic Threat Intelligence (DTI)

Le moteur FireEye Multi-Vector Virtual Execution (MVX) inclut des fonctionnalités d'apprentissage machine (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 d'intervention approprié. La cyberveille, qui inclut notamment le cyberpirate à l'origine de la menace, ses possibles motivations ainsi que des informations générales et sectorielles sur les malwares utilisés et d'autres indicateurs, sont autant de données précieuses pour rechercher les auteurs d'attaque au sein de votre environnement.

ATI+

Bénéficiez de notre service de surveillance des alertes critiques et de l'efficacité des détections, 24h/7j et 365 jours par an.

Par ailleurs, l'abonnement ATI+ vous donne accès à des dossiers complets, aux tendances, à l'actualité et l'analyse de groupes d'attaque avancés, ainsi qu'à des profils des secteurs d'activités ciblés, notamment les types de données convoitées.

Ce qui différencie notre cyberveille

- Visibilité inégalée sur le cycle de vie complet d'une attaque ainsi que les motivations, les outils et les procédures des attaquants. Visibilité et accès 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 11 millions d'appliances 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 cyberpirates, 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.

Grâce à FireEye iSIGHT Intelligence, les entreprises bénéficient d'une visibilité et d'une connaissance sans précédent des attaquants, de leurs motivations, de leurs objectifs et de leurs méthodes. Ainsi, elles diminuent la surface d'attaque et abandonnent une sécurité réactive, basée sur les alertes et gourmande en ressources, au profit d'une méthodologie proactive, permettant de réagir efficacement et rapidement aux menaces.

	DTI	ATI	ATI+	ISIGHT INTELLIGENCE
Phase de l'attaque dont est issue l'information	Attaque	Attaque	Attaque	Avant, pendant et après l'attaque
Type de cyberveille	Tactique	Opérationnelle	Stratégique	Cyberveille contextuelle et outils d'analyse
Détection par les appliances FireEye	✓			
Profils de détection pour les appliances FireEye		✓		
Corrélation des alertes FireEye et des informations de géolocalisation		✓		
Attribution d'alertes FireEye à des auteurs de menaces connus		✓		
Surveillance des alertes			✓	
Surveillance de l'intégrité des systèmes			✓	
Profils des groupes de cyberpirates			✓	✓
Profils sectoriels			✓	
Profils des familles de malwares			✓	
Actualité des menaces			✓	✓
Indicateurs de menace via l'API				✓
API et kit de développement logiciel (SDK) pour intégration avec des outils non-FireEye				✓
Plug-in de navigateur iSIGHT pour l'analyse, les recherches et l'accès aux alertes sur le portail iSIGHT Intelligence				✓
Attribution des indicateurs de menace iSIGHT à des auteurs de menaces connus				✓
Couverture étendue des auteurs de menaces				✓
Cyberveille décisionnelle				✓
Suivi des vulnérabilités des systèmes d'entreprise				✓
Suivi des vulnérabilités des infrastructures critiques				✓
Suivi des exploitations				✓
Contexte des alertes dans l'infrastructure informatique existante				✓

Pour plus d'informations sur FireEye, consultez notre site Web à l'adresse :
www.FireEye.fr

FireEye, France | 4, place de la Défense, Paris La Défense Cedex 92974 | +33 1 58 58 01 76 | france@FireEye.com
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | www.FireEye.com

www.FireEye.fr

FireEye