McAfee Threat Intelligence Exchange

Partage de cyberveille entre solutions de sécurité

McAfee® Threat Intelligence Exchange joue le rôle d'un intermédiaire en données de réputation pour assurer une détection des menaces et une réponse adaptatives. Il combine la cyberveille locale des solutions de sécurité de votre entreprise aux informations sur les menaces transmises par des sources externes partout dans le monde. Il partage ensuite instantanément cette cyberveille collective avec votre écosystème de sécurité, ce qui permet aux solutions d'échanger des informations et d'agir immédiatement en fonction des informations partagées.

Création d'un écosystème collaboratif de cyberveille

Intermédiaire en données de réputation, McAfee Threat Intelligence Exchange combine des informations mondiales et locales. D'une part, la cyberveille issue de sources mondiales importées, comme McAfee Global Threat Intelligence (McAfee GTI), et d'autres sources telles que VirusTotal. D'autre part, la cyberveille collectée en local au sein de l'environnement, notamment les terminaux, les passerelles et les solutions d'analyse avancée. Grâce à DXL (Data Exchange Layer), McAfee Threat Intelligence Exchange partage instantanément cette cyberveille collective avec tous les éléments de votre écosystème de sécurité pour leur permettre de fonctionner de concert et renforcer la protection dans toute l'entreprise.

L'architecture d'intégration simplifiée de DXL réduit considérablement les coûts opérationnels et d'implémentation de nombreuses intégrations directes d'API, tout en offrant une efficacité opérationnelle et une sécurité inégalées. Conçu comme un cadre ouvert, DXL permet à toutes les solutions de sécurité de rejoindre dynamiquement l'écosystème McAfee Threat Intelligence Exchange, y compris les produits de sécurité d'autres éditeurs.

Adaptation et immunisation contre les menaces

Chaque information partagée, issue des multiples points de contrôle de votre réseau, contribue à l'amélioration des connaissances dans la lutte contre les menaces ciblées.

Principaux avantages

- La protection adaptative contre les menaces ramène le délai entre l'identification et la neutralisation d'une attaque ciblée avancée de plusieurs jours, semaines ou mois à quelques millisecondes.
- La cyberveille collaborative fournit des informations collectives sur les menaces provenant de sources de données mondiales combinées à des données de cyberveille locales.
- Les informations de sécurité pertinentes sont partagées en temps réel entre les solutions de sécurisation pour terminaux, passerelles, réseaux et centres de données.
- Vous disposez des données nécessaires pour prendre des décisions concernant des types de fichiers inconnus en fonction du contexte du terminal (attributs des fichiers, des processus et de l'environnement) et de données de cyberveille collectives.

Ces menaces étant conçues pour viser un objectif précis, les entreprises ont besoin d'un système de surveillance local pour identifier les tendances et toute attaque spécifique subie. Ces données contextuelles locales recueillies lors de l'attaque et combinées à une cyberveille mondiale permettent d'améliorer la prise de décision concernant des fichiers encore inconnus, ce qui accélère la détection et la protection.

Lorsqu'un fichier non identifié est détecté sur votre réseau, la solution de sécurité qui l'a repéré contacte McAfee Threat Intelligence Exchange pour déterminer si la réputation du fichier est disponible dans sa base de données. Des métadonnées descriptives, comme la prévalence dans l'entreprise et l'ancienneté, sont également conservées et intégrées dans la cyberveille collective. En plus d'interroger McAfee Threat Intelligence Exchange sur la réputation des fichiers, les solutions de sécurité intégrées peuvent également transmettre de nouvelles données de réputation fondées sur les verdicts locaux. Ces nouvelles réputations sont ensuite distribuées en temps réel à tous vos systèmes. De plus, l'information est conservée de sorte que la menace sera immédiatement détectée si elle se présente sur un autre équipement ou serveur.

McAfee Threat Intelligence Exchange offre aux administrateurs la possibilité de personnaliser facilement la cyberveille. Ils peuvent compiler, remplacer, compléter et affiner cette vaste base de cyberveille afin de personnaliser la protection de leur environnement et de leur entreprise. Ces données de cyberveille hiérarchisées et optimisées localement offrent une protection immédiate contre les attaques futures.

Protection renforcée par des points de mise en œuvre

Les solutions intégrées installées dans tout le réseau (du terminal à la périphérie) appliquent des stratégies en fonction de la réputation disponible, des métadonnées ou d'une combinaison de données. Pour prendre des décisions précises et éclairées, McAfee Endpoint Security, une solution étroitement intégrée, tire parti de la cyberveille mondiale et de la cyberveille locale. Un exemple de cyberveille locale : les métadonnées des fichiers, par exemple leur prévalence dans l'entreprise et leur ancienneté, ou encore les données de réputation locales fournies par d'autres composants de sécurité. Ainsi, une application personnalisée qui ne possède pas de réputation mondiale mais qui a une prévalence élevée dans l'entreprise ne génère pas une réputation combinée malveillante et sera probablement autorisée à s'exécuter. En revanche, un fichier inconnu dans l'entreprise, sans réputation locale ou mondiale mais dont la compression est suspecte, risque de générer un niveau de confiance bas et de déclencher un blocage, une analyse plus approfondie par d'autres moteurs McAfee Endpoint Security, ou encore une analyse sandbox par McAfee Advanced Threat Defense ou McAfee Cloud Threat Detection.

Real Protect, la fonction d'apprentissage automatique de McAfee Endpoint Security, et le confinement d'application dynamique renforcent encore la détection et la protection sur les terminaux. Real Protect effectue des recherches dans le cloud sur la cyberveille la plus récente, complétées par une analyse pré- et post-exécution. Le confinement d'application dynamique bloque les activités malveillantes

Principaux avantages (suite)

- L'intégration est simplifiée grâce à DXL. Les coûts opérationnels et d'implémentation sont réduits grâce à la connexion des solutions de sécurité McAfee et celles d'autres éditeurs pour opérationnaliser votre cyberveille sur les menaces en temps réel.

Les attaques ciblées avancées, un défi de taille

Conçues pour contrecarrer les mécanismes de détection et s'implanter à long terme au sein d'une entreprise, les attaques ciblées avancées continuent de frapper durement les entreprises et d'exfiltrer des données de valeur. Selon des données récemment publiées dans l'étude de Verizon *2015 Data Breach and Investigations Report* (Rapport d'enquête 2015 sur les compromissions de données), 70 à 90 % des échantillons de logiciels malveillants sont propres à chaque entreprise, faisant de la détection des indicateurs de menaces uniques le plus grand défi de notre époque[1].

Pour plus d'informations, visitez notre site à l'adresse **www.mcafee.com/fr/products/threat-intelligence-exchange.aspx**.

sur le terminal, protégeant ainsi le premier système exposé à une nouvelle menace pendant qu'une analyse complémentaire est effectuée.

Tous les avantages de la collaboration

Analyse avancée des menaces

Si un fichier donné nécessite des informations plus détaillées, il peut être envoyé automatiquement par McAfee Threat Intelligence Exchange vers les solutions d'analyse avancée de McAfee (comme McAfee Advanced Threat Defense ou McAfee Cloud Threat Detection) pour obtenir des renseignements supplémentaires sur les nouvelles menaces potentielles et déterminer la réputation du fichier en question. Tout est automatisé, documenté et partagé via DXL pour protéger l'ensemble de votre écosystème de sécurité.

Gestion des événements de sécurité

McAfee Enterprise Security Manager permet de réaliser une analyse plus approfondie lors de l'examen des indicateurs de compromission identifiés à l'aide de McAfee Threat Intelligence Exchange. L'accès aux informations de sécurité historiques et la possibilité de créer des listes de surveillance automatisées assurent aux entreprises une sécurité plus performante.

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr