Présentation de solution

Opérationnalisation de la cyberveille sur les menaces

Derrière la vaste majorité des alertes légitimes envoyées à l'équipe de sécurité informatique se cache un agresseur qui exploite plusieurs techniques d'attaque pour s'infiltrer dans votre infrastructure et compromettre vos données et systèmes stratégiques. Les attaques multiphases ciblées comportent une série d'étapes constituant la chaîne d'une cyberattaque : la reconnaissance, l'analyse des vulnérabilités, l'exploitation et, enfin, l'exfiltration des données critiques de l'entreprise.

Les analystes en sécurité connaissent bien ces techniques et dépendent de la cyberveille sur les menaces pour obtenir des informations pertinentes sur les méthodes et les motivations d'une attaque. Ils peuvent détecter et neutraliser les menaces avancées, appliquer les mesures correctives appropriées et être mieux préparés à la prochaine alerte de sécurité. Trop souvent malheureusement, ils manquent de visibilité sur certains systèmes ou sont submergés par des données trop nombreuses et pas assez pertinentes. Selon l'étude du SANS Institute, *Who's Using Cyberthreat Intelligence and How?* (Qui utilise la cyberveille sur les menaces et comment), « seuls 11,9 % des personnes interrogées sont en mesure de rassembler les informations sur les menaces provenant de la multitude de sources, et 8,8 % seulement bénéficient d'une vue complète qui leur permet d'associer des événements aux indicateurs de compromission[1] ».

Un rapport publié il y a peu par Forrester révèle qu'au sein des entreprises américaines et européennes, 77 % des décideurs en matière de sécurité considèrent l'amélioration des systèmes de cyberveille comme une priorité[2]. Avec la cyberveille, les professionnels de la sécurité ont l'espoir d'être avertis quant aux cybercriminels qui ciblent leur pays, leur secteur d'activité, voire leur entreprise en particulier afin qu'ils puissent prendre les mesures qui s'imposent. Pourtant, les équipes de sécurité informatique restent confrontées à quelques défis de taille :

- Comment recueillir des informations sur les menaces auprès de sources externes et internes
- Comment corréler les données et prioriser les risques
- Comment communiquer la cyberveille aux contrôles de sécurité multifournisseurs installés dans l'entreprise
- Comment bénéficier d'une visibilité accrue sur l'environnement informatique pour réagir instantanément et de façon appropriée

À l'heure actuelle, les entreprises ont besoin d'une architecture ouverte et intégrée qui facilite l'adoption des systèmes de cyberveille et leur permet de profiter de ses avantages — qu'il s'agisse de recueillir des données de base sur les menaces, de procéder à des investigations numériques ou encore d'exploiter ces renseignements pour les intégrer aux fonctions d'analyse d'une solution SIEM. En d'autres termes, les utilisateurs doivent être en mesure d'exploiter et d'appliquer la cyberveille sur les menaces via des processus automatisés destinés à les analyser, à les synthétiser et à les gérer.

intel Security

Une nouvelle approche en matière de cyberveille pour contrer les menaces émergentes

Face à des attaques toujours plus complexes, précises et massives, les systèmes de cyberveille d'hier ne font plus le poids. Les enquêtes sur les attaques ciblées sont loin d'être simples. Le comportement dynamique des attaquants, la variété et la multiplication des sources locales et mondiales de cyberveille et la diversité des formats de données sur les menaces compliquent l'agrégation et la synthèse des informations dans les outils du centre des opérations de sécurité (SOC).

L'environnement multifournisseur que l'on retrouve dans la plupart des entreprises rend encore plus difficiles le partage des données d'événements et leur visibilité dans toute l'entreprise. Comme Gartner le souligne dans son rapport *Technology Overview for Threat Intelligence Platforms* (Technologies des plates-formes de cyberveille), « l'incapacité d'une entreprise à partager ses informations sur les menaces est une aubaine pour les cybercriminels. Ce partage est un multiplicateur de puissance et devient un élément clé pour lutter à armes égales contre des attaques et des auteurs de menaces toujours plus nombreux[3] ».

Cela étant, le simple partage de cyberveille sur les menaces n'aboutit pas nécessairement à une prévention et à des interventions efficaces. Un excès d'informations peut rapidement submerger les analystes en sécurité. La plupart des équipes de sécurité sont occupées par des processus manuels laborieux (voir Figure 1), à savoir l'analyse de millions d'événements de sécurité et de fichiers suspects dans l'espoir de donner un sens à des myriades de données et de reconstituer l'attaque ciblée. Au bout du compte, la précision et la vitesse du processus de réponse sont considérablement limités. Comme ces équipes disposent d'une compréhension très imparfaite des menaces, elles éprouvent de grandes difficultés à endiguer rapidement les attaques. Selon une étude réalisée en 2014 par Intel Security, *When Minutes Count* (Quand chaque minute compte), moins de 25 % des répondants affirment pouvoir détecter une attaque en quelques minutes[4].

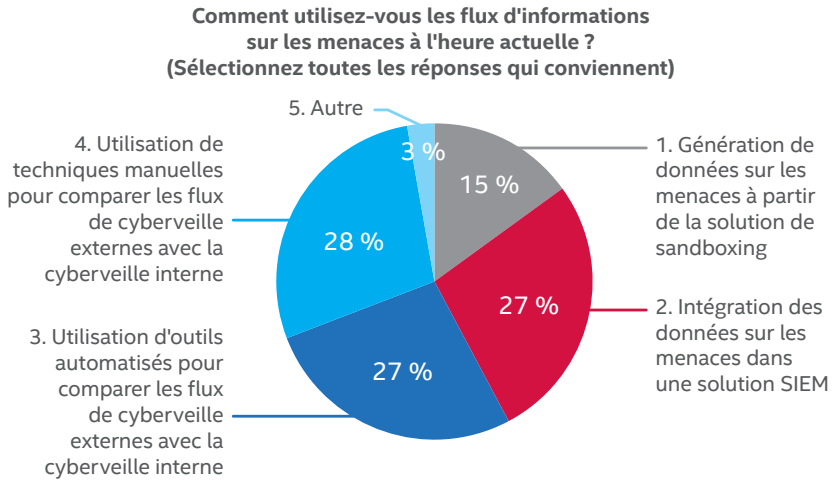

Figure 1. D'après une enquête menée par Intel Security lors de la conférence BlackHat 2015, de nombreux utilisateurs ont toujours recours à des techniques manuelles pour comparer les sources externes de cyberveille aux informations sur les menaces dont ils disposent en interne.

« Pour notre infrastructure de sécurité, il nous fallait plus qu'un simple fournisseur de technologies. Il était capital de collaborer avec un partenaire capable de nous aider à gérer des exigences clients très diversifiées et un environnement de menaces en constante mutation. McAfee est le partenaire que nous recherchions. Les informations de sécurité que nous recevons continuellement des solutions McAfee sont essentielles pour nous aider à conserver des opérations et des services de pointe. »

—Anurana Saluja
RSSI et Vice-président de la sécurité des informations
Sutherland Global Services

Opérationnalisation de la cyberveille sur les menaces

Une détection et neutralisation des menaces pilotées par la cyberveille nécessitent bien plus que l'importation manuelle hebdomadaire d'adresses IP malveillantes publiées sur un site web public, dans une table de suivi SIEM. Cela exige au contraire une acquisition en temps réel de la cyberveille et une corrélation de toutes les facettes d'une attaque, dont ses méthodes et les campagnes lancées dans le monde, afin que les entreprises puissent bloquer les menaces les plus furtives et adaptatives. Les centres SOC des entreprises ont besoin d'une méthodologie leur permettant d'« opérationnaliser la cyberveille sur les menaces » afin de dresser un tableau complet des attaques ciblant leur environnement. Ils doivent pouvoir faire le tri dans la masse de données à analyser et à corréler, mais aussi prioriser les informations sur les menaces pour identifier celles qui sont pertinentes selon leur secteur, leur emplacement géographique et leur entreprise particulière.

Ils doivent aussi être en mesure d'obtenir des informations sur les attaques uniques en cours, ainsi que sur les tendances qui se dégagent de l'historique des événements de sécurité. Comme le fait remarquer Forrester, l'opérationnalisation de la cyberveille est essentielle dans la mesure où 75 % des attaques se propagent d'une victime à une autre en l'espace de 24 heures. Les entreprises doivent combler la faille entre « la rapidité du partage et celle de l'attaque[5] ».

Mise à profit de l'architecture intégrée d'Intel Security

Intel Security offre une plate-forme unifiée et collaborative incluant tous les composants nécessaires à l'opérationnalisation de la cyberveille. Au nombre de ces composants, citons les sources mondiales de cyberveille, la création d'une cyberveille en local, le partage en temps réel de données sur les menaces dans l'infrastructure informatique, la gestion des événements et des informations de sécurité, ainsi que la distribution d'une protection adaptative automatisée.

Activité de cyberveille	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Collecte de données de cyberveille à partir de sources externes	Utilise des données au format STIX et importées de VirusTotal et de McAfee Global Threat Intelligence (McAfee GTI).	Importe les données de McAfee GTI.	Importe des données de McAfee GTI, des données au format TAXII/STIX et des flux HTTP d'informations sur les menaces via l'outil de gestion des cybermenaces McAfee Enterprise Security Manager.	McAfee GTI agrège les informations de cyberveille de nombreux partenaires Cyber Threat Alliance et de sources publiques. Il recueille des données sur les menaces au départ de millions de sondes sur les produits Intel Security déployés par des clients, tels que des solutions de protection des terminaux, de l'environnement web ou de la messagerie électronique, sans oublier les systèmes de prévention des intrusions sur le réseau et les pare-feux.
Collecte de données de cyberveille internes	Collecte des échantillons issus de McAfee VirusScan®, McAfee Application Control, McAfee Web Gateway, McAfee Advanced Threat Defense, McAfee Enterprise Security Manager et de produits d'autres éditeurs qui envoient des informations via McAfee Data Exchange Layer.	Utilise des échantillons transmis via McAfee Threat Intelligence Exchange ou le réseau à des fins de neutralisation.	Importe des données au format STIX/TAXII et via McAfee Data Exchange Layer.	
Génération de cyberveille locale	Enregistre des incidents de fichiers suspects et crée une base de données locale qui consigne le premier contact et la trajectoire des menaces.	Analyse et identifie les logiciels malveillants, génère une cyberveille locale sur les menaces et la distribue via McAfee Data Exchange Layer ou en tant qu'API STIX.	Crée des listes de suivi, des rapports et des vues de cyberveille, basés sur des événements corrélés.	
Distribution de cyberveille aux contrôles de sécurité	Via McAfee Data Exchange Layer	Via McAfee Data Exchange Layer et les API de produits	Via McAfee Data Exchange Layer, les API de produits et l'intégration de scripts	McAfee GTI est intégré avec de nombreux produits de sécurité Intel Security, notamment McAfee Web Gateway, McAfee Enterprise Security Manager et les solutions McAfee pour terminaux.
Visibilité sur la cyberveille collectée	Via les tableaux de bord McAfee Threat Intelligence Exchange	Via des rapports	Via des tableaux de bord, des vues et des rapports fournis dans des packs de contenu ou générés par les clients	Via McAfee Threat Center et le Rapport trimestriel de McAfee sur le paysage des menaces

Tableau 1. Plate-forme intégrée de cyberveille sur les menaces d'Intel Security

Acquisition, analyse et propagation

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) est un excellent point de départ pour mettre en place votre plate-forme intégrée de cyberveille sur les menaces. Ce service complet d'analyse de la réputation, délivré en temps réel et basé dans le cloud, est parfaitement intégré aux produits Intel Security et leur permet de bloquer rapidement les cybermenaces sur tous les vecteurs : fichiers, Web, messagerie électronique et réseau. McAfee GTI établit des scores de réputation pour des milliards de fichiers, d'URL, de domaines et d'adresses IP sur la base de données sur les menaces collectées auprès de nombreuses sources : des millions de sondes dans le monde contrôlées et analysées par McAfee Labs ; des flux d'informations sur les menaces transmis par les partenaires de recherche et Cyber Threat Alliance ; sans oublier une cyberveille multivecteur issue du Web, de la messagerie électronique et des réseaux. Alimenté par des flux de données pertinentes et de qualité, McAfee GTI offre des évaluations des risques précises qui facilitent la prise de décisions éclairées et permettent aux contrôles de bloquer, d'éliminer ou d'autoriser des fichiers, des applications et des activités, comme il convient.

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (SIEM) optimise l'acquisition et l'analyse de la cyberveille sur les menaces en proposant une plate-forme de consolidation, d'analyse et d'action pour chaque type d'information. Cette vue à 360° garantit une visibilité et une connaissance situationnelle complètes pour accélérer la détection et la neutralisation des attaques ciblées. Son système avancé de gestion des données a été spécialement conçu pour stocker et assimiler d'importants volumes de données contextuelles en temps réel.

McAfee Enterprise Security Manager collecte des données sur les activités et les événements de tous vos systèmes, bases de données, réseaux et applications. Il importe également des flux mondiaux sur les menaces et exploite les informations de cyberveille dans des formats et des mécanismes de transport standards tels que STIX (Structured Threat Information eXpression), TAXII (Trusted Automated eXchange of Indicator Information) et Cybox. Ces données sont généralement publiées par la communauté informatique ou des groupes sectoriels comme le centre FS-ISAC (Financial Services Information Sharing and Analysis Center). Grâce à des fonctions d'analyse avancées, il convertit les renseignements recueillis en informations de sécurité compréhensibles et directement exploitables. Plus important encore, il offre une visibilité accrue sur les menaces émergentes grâce à des vues en temps réel et à un accès à des données de sécurité historiques. Il est ainsi possible d'enquêter à rebours pour comprendre la prévalence et les comportements d'une attaque, mais aussi de créer des listes de suivi automatisées pour détecter l'occurrence ou la récurrence des événements à l'avenir. En optimisant la sensibilité de votre système aux événements identifiés comme malveillants, vous améliorez votre capacité à détecter les activités et les comportements suspects au cours des différentes phases de la chaîne d'attaque et vous priorisez plus efficacement votre réponse.

Figure 2. Vue de McAfee GTI

Cyber Threat Alliance

La **Cyber Threat Alliance** réunit des professionnels de la sécurité dont les entreprises partagent des informations sur les menaces entre elles et avec leurs clients pour améliorer les systèmes de défense contre les cyberpirates. Intel Security fait partie des membres fondateurs qui se sont mobilisé pour trouver les méthodes les plus efficaces pour partager des données sur les menaces, stimuler la collaboration entre les partenaires et progresser ensemble dans la lutte contre une cybercriminalité toujours plus sophistiquée.

McAfee GTI for Enterprise Security Manager exploite tous les avantages qu'offre la recherche McAfee Labs au profit de la surveillance de la sécurité d'entreprise. Ce flux d'informations riche et constamment mis à jour de McAfee GTI accroît la connaissance situationnelle en permettant une détection rapide des événements liés à des communications avec des adresses IP suspectes ou malveillantes. De plus, il offre aux administrateurs responsables de la sécurité la possibilité de déterminer quels hôtes ont communiqué ou communiquent actuellement avec des interlocuteurs malveillants.

McAfee Threat Intelligence Exchange

McAfee Threat Intelligence Exchange est le troisième composant que vous pouvez ajouter au cours du développement de votre écosystème de cyberveille intégré. Il agrège et partage des informations sur la réputation des fichiers dans l'ensemble de l'infrastructure de sécurité informatique. McAfee Threat Intelligence Exchange reçoit des informations sur les menaces au départ de McAfee GTI, de fichiers STIX importés, de flux sur les menaces transmis par McAfee Enterprise Security Manager ainsi que des informations provenant de multiples technologies et solutions (terminaux, contrôle des applications, appareils mobiles, passerelles, centres de données et sandboxing) d'Intel Security et d'autres éditeurs. La collecte des données sur tous les composants de votre infrastructure fournit des informations sur des menaces parfois uniquement présentes dans votre environnement, ce qui est souvent le cas avec les attaques ciblées. De leur côté, les informations sur la réputation des fichiers sont instantanément partagées dans l'ensemble de l'écosystème et transmises à tous les produits et solutions connectés à McAfee Threat Intelligence Exchange via McAfee Data Exchange Layer. Si, par exemple, McAfee Threat Intelligence Exchange distribue des informations sur un fichier exécutable malveillant, McAfee Data Loss Prevention reçoit ces données via McAfee Data Exchange Layer et entame un suivi de ce fichier pour détecter toute tentative d'accès à des fichiers sensibles.

Les données partagées via McAfee Data Exchange Layer incluent des informations sur la réputation des fichiers, l'intégrité des applications, la classification de données et les contextes utilisateur ; celles-ci sont distribuées aux produits intégrés. N'importe quel produit ou solution peut être intégré à McAfee Data Exchange Layer, puis configuré pour déterminer les informations qu'il est souhaitable de publier sur le système et celles auxquelles il faut souscrire.

McAfee Threat Intelligence Exchange collabore étroitement avec la solution de sandboxing avancée d'Intel Security, McAfee Advanced Threat Defense, qui lui transmet des données d'analyse sur les logiciels malveillants. Si un fichier est identifié comme malveillant, McAfee Threat Intelligence distribue une mise à jour de la réputation des fichiers à tous les systèmes connectés via McAfee Data Exchange Layer. Cette communication fonctionne dans les deux sens. Lorsque des fichiers à la réputation inconnue sont détectés sur les terminaux dotés de McAfee Threat Intelligence Exchange, ils peuvent être soumis à McAfee Advanced Threat Defense pour déterminer si l'objet est malveillant, ce qui élimine les « angles morts » générés par la distribution hors bande des charges actives. Ces deux solutions fonctionnent de concert pour assurer une protection automatisée et adaptative contre les menaces émergentes. Les informations sur les attaques détectées sont transmises à tout votre environnement pour permettre le blocage de la chaîne d'attaque avant qu'elle ne cause d'autres dégâts.

Figure 3. Tableau de bord de McAfee Threat Intelligence Exchange

McAfee Threat Intelligence Exchange assure une détection des menaces et une réponse adaptatives en opérationnalisant la cyberveille en temps réel sur l'ensemble des solutions de protection des terminaux, du réseau, du centre de données et de la passerelle. L'association et le partage instantané d'informations mondiales sur les menaces importées et de renseignements recueillis localement permettent à vos solutions de sécurité de fonctionner de concert pour échanger et réagir sur la base de cette cyberveille partagée.

Interruption de la chaîne d'attaque
Indépendamment du premier point de contact avec un fichier malveillant inconnu, lorsque la dangerosité de ce dernier est attestée, l'environnement connecté tout entier est informé immédiatement. Dès que McAfee Advanced Threat Defense identifie un fichier comme malveillant, McAfee Threat Intelligence Exchange publie cette information via une mise à jour de la réputation, distribuée via McAfee Data Exchange Layer à l'intention de tous les contrôles de sécurité de l'entreprise. De plus, les passerelles intégrées à McAfee Threat Intelligence Exchange empêchent le fichier de pénétrer dans l'entreprise. Grâce au partage coordonné de la cyberveille entre tous vos contrôles de sécurité, il est plus facile d'interrompre la chaîne d'attaque et de prévenir d'autres dommages, sans devoir intervenir manuellement.

Synthèse et application : une détection plus précise et des décisions plus avisées

Après avoir incorporé les données sur les menaces, McAfee Enterprise Security Manager devient votre fenêtre sur l'environnement d'entreprise. La solution établit des corrélations entre les flux de McAfee GTI et de McAfee Threat Intelligence Exchange, ainsi que les indicateurs de compromission aux formats STIX/TAXII et les données d'événements historiques ou détectés en temps réel lorsque des systèmes de votre réseau communiquent avec des interlocuteurs malveillants connus ou des domaines suspects. Le tableau de bord de gestion des menaces fournit aux analystes une vue unique et complète des indicateurs de menace recueillis, des sources d'information, du nombre d'occurrences des divers indicateurs ainsi que les détails les plus pertinents sur les indicateurs de compromission dans un format lisible.

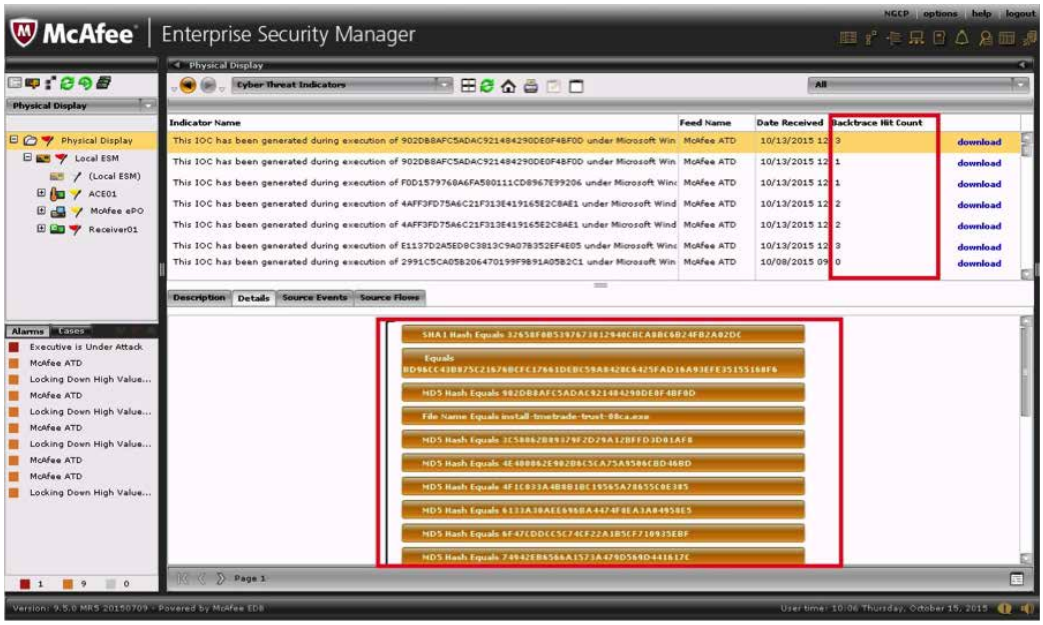

Figure 4. Indicateurs de cybermenace, occurrences détectées par la fonction Backtrace et détails d'un indicateur de compromission dans McAfee Enterprise Security Manager

L'utilisation conjointe du système SIEM d'Intel Security et d'autres outils de cyberveille collaboratifs contribue à réduire les coûts opérationnels associés à la configuration des règles de corrélation, un processus manuel souvent long et fastidieux. Par exemple, les analystes en sécurité peuvent examiner directement les dernières informations reçues sur les menaces dans un format lisible par l'homme, ce qui permet de mieux appréhender les menaces détectées. Mieux encore, la cyberveille sur les menaces peut être automatiquement intégrée par des règles de corrélation historique ou en temps réel, ce qui réduit d'autant le délai de détection d'activités malveillantes en cours et émergentes. Par ailleurs, les utilisateurs peuvent suivre la progression des menaces détectées dans l'environnement informatique, mais aussi via les informations contextuelles dans des vues d'alarme afin de prendre des décisions plus avisées. Tous ces renseignements recueillis améliorent et accélèrent les processus de détection et d'enquête des attaques ciblées.

Comme les menaces se propagent dans l'infrastructure informatique à la vitesse de l'éclair et sont conçues pour muter au fil du temps, McAfee Enterprise Security Manager peut périodiquement actualiser les informations collectées sur les menaces et éliminer les données plus anciennes et moins pertinentes. Ainsi, les serveurs de commande et de contrôle mis hors service ou les sites web nettoyés dont le score de réputation malveillante a diminué sont automatiquement supprimés pour éliminer les faux positifs susceptibles de détourner l'attention du personnel de sécurité des vraies menaces.

En résumé

Le système intégré de cyberveille sur les menaces d'Intel Security opérationnalise l'acquisition, la synthèse et la gestion des informations sur les menaces. Cela vous permet d'optimiser la précision de la détection des menaces, d'éliminer les processus manuels et d'empêcher les auteurs d'attaques de mettre à mal votre entreprise. Armé de meilleures informations et d'une visibilité accrue sur les activités malveillantes dans tout votre écosystème de sécurité, vous êtes mieux préparé à identifier et à neutraliser les attaques ciblées d'aujourd'hui et à prévenir celles de demain.

En savoir plus

Pour en savoir sur les composants de la plate-forme intégrée de cyberveille sur les menaces d'Intel Security, consultez les pages suivantes :

- **McAfee Global Threat Intelligence**
- **McAfee Threat Intelligence Exchange**
- **McAfee Advanced Threat Defense**
- **McAfee Enterprise Security Manager**
- **How to Use a TAXII Feed with McAfee Enterprise Security Manager (Utilisation d'un flux TAXII avec McAfee Enterprise Security Manager)**

Les produits Intel Security suivants prennent en charge les informations sur les menaces au format STIX :

- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Detection
- McAfee Enterprise Security Manager

1. **https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767**
2. **https://www.forrester.com/The+State+Of+The+Cyberthreat+Intelligence+Market/fulltext/-/E-RES123011**
3. **https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms**
4. **http://www.mcafee.com/fr/resources/reports/rp-when-minutes-count.pdf**
5. **https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf**

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com