Flux d'informations sur les menaces - Kaspersky Network Security Threat Data Feeds

kaspersky prêts pour l'avenir

La protection des terminaux ne suffit pas.

Une protection au niveau du réseau est également nécessaire.

Voici pourquoi :

- La protection contre les différents types d'attaques doit être organisée en plusieurs couches
- Certains hôtes de votre environnement ne disposent pas d'une protection des terminaux, par exemple les serveurs critiques pour l'entreprise ou les hôtes d'un réseau industriel
- Certains hôtes « protégés » peuvent ne pas être à jour sur le plan des signatures, des hachages et des règles de détection

Flux d'informations sur les menaces - Kaspersky Network Security Threat Data Feeds

De nos jours, presque toutes les entreprises disposent d'un pare-feu de nouvelle génération (NGFW). Il s'agit de l'un des contrôles modernes de sécurité des réseaux les plus efficaces, qui augmente les niveaux de protection des réseaux d'entreprise contre les cyberattaques.

La majorité des pare-feu de nouvelle génération (NGFW) sont non seulement capables de tirer parti des connaissances internes sur les cybermenaces, mais offrent également des fonctionnalités permettant d'utiliser des listes dynamiques d'indicateurs de compromission (IoC) provenant de sources externes pour bloquer les cybermenaces en temps réel

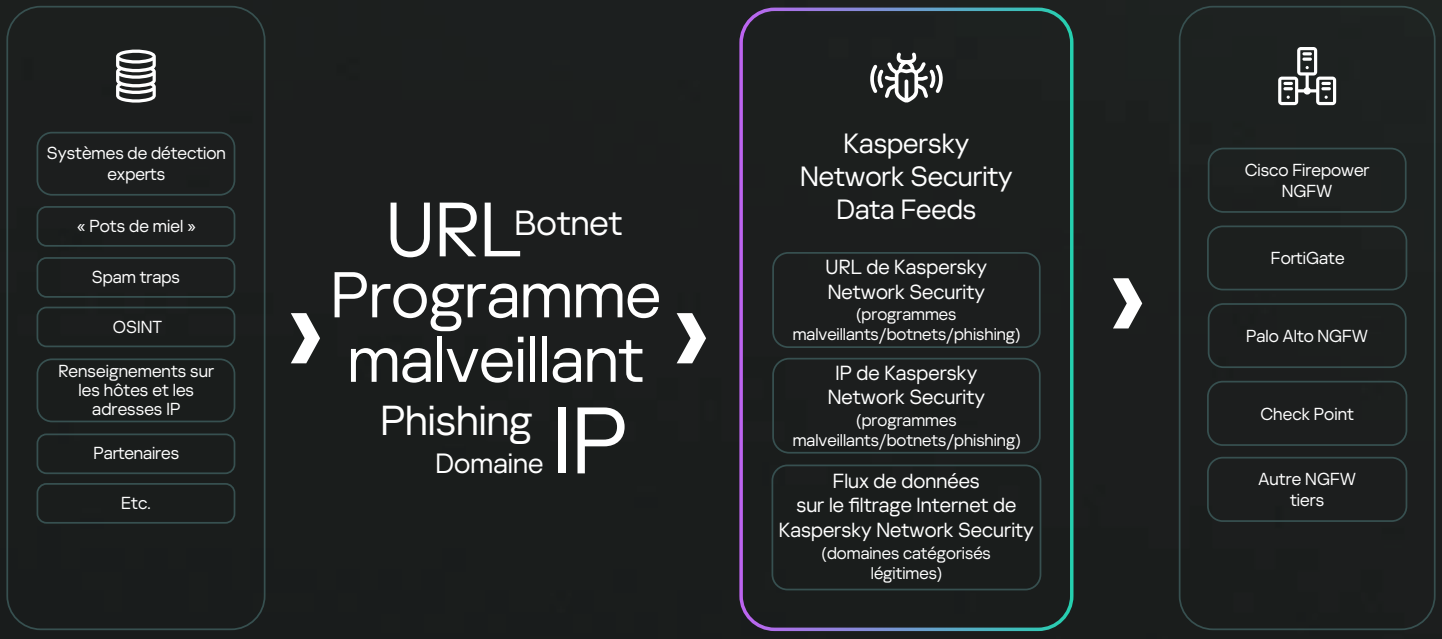
Il est pratiquement impossible de configurer rapidement les règles de détection du NGFW pour toujours garder une longueur d'avance sur les adversaires. C'est pourquoi il est indispensable de disposer d'une Threat Intelligence externe. Celle-ci apporte un niveau de protection important à votre environnement, qui risque autrement de ne pas être assuré.

Kaspersky propose des collections d'IoC spécialement créés qui, lorsqu'ils sont importés dans un pare-feu de nouvelle génération, améliorent considérablement le niveau de protection du réseau de l'entreprise contre les menaces les plus répandues, sans intégration ou configuration compliquée, et en conservant la topologie actuelle du réseau.

Les flux d'informations sur les menaces de Kaspersky Network Security reposent sur les flux d'informations de Kaspersky Threat Intelligence et contiennent des listes régulièrement mises à jour de divers types d'IoC (adresses IP et domaines). L'utilisation de ces informations vous permet de surveiller et de bloquer l'accès des utilisateurs aux ressources dangereuses du réseau.

En savoir plus

Intégrations des flux d'informations de Kaspersky Network Security



Collecte et traitement des données

Les flux d'informations de Kaspersky Network Security sont composés de plusieurs listes, chacune se concentrant sur un type particulier de cybermenace. Les flux contiennent les listes d'adresses IP présentant le score de menace le plus élevé et les domaines de premier et de deuxième niveau des ressources qui sont connues pour diffuser des programmes malveillants, agir en tant que centres de commande et de contrôle (C&C) de botnets ou héberger des ressources de phishing.

Les flux d'informations sont agrégés à partir de sources ultra-fiables, hétérogènes et fusionnées, comme Kaspersky Security Network et nos robots proactifs d'indexation, notre service de contrôle des botnets (qui surveille les botnets, leurs cibles et activités 24 h/24, 7 j/7, 365 j/an), les services de renseignements sur les hôtes et les adresses IP.

Toutes les données agrégées sont soigneusement analysées et affinées en temps réel à l'aide de plusieurs techniques de retraitement : critères statistiques, sandbox, moteurs heuristiques, outils de similarité, profils de comportement, validation par des analystes et vérification de listes blanches.

Bénéfices

Mises à jour en temps réel

Les flux d'informations (Data Feeds) sont automatiquement générés en temps réel en se basant sur des résultats recueillis dans le monde entier, ce qui fournit des taux de détection et des niveaux de précision élevés.

Kaspersky Security Network offre une visibilité sur une grande partie du trafic Internet, couvrant des dizaines de millions d'utilisateurs finaux dans plus de 213 pays

Prise en charge native

Prise en charge native des pare-feu de nouvelle génération (NGFW) les plus connus :

- Cisco
- FortiGate
- Palo Alto
- Autres NGFW tiers (avec fonctionnalité de listes dynamiques externes et prise en charge de l'authentification de base)

Authentification sécurisée

Les flux d'informations offrent une gamme de méthodes d'authentification adaptées aux différents besoins de sécurité et aux préférences d'intégration

Intégration facile

Des guides de configuration étape par étape supplémentaires pour chaque pare-feu de nouvelle génération pris en charge et une assistance technique de Kaspersky facilitent la configuration et apportent une valeur ajoutée instantanée

Disponibilité permanente

Tous les flux sont générés et surveillés par une infrastructure hautement tolérante aux pannes, assurant une disponibilité permanente

Données intégralement vérifiées

Les flux d'informations truffés de faux positifs sont problématiques, car ils peuvent bloquer des ressources légitimes.

Les flux d'informations de Kaspersky Network Security appliquent des filtres et des tests extrêmement complets pour garantir la diffusion de données intégralement vérifiées

Avantages

Renforcez votre défense du réseau

avec des IoC mis à jour en permanence pour bloquer automatiquement les cybermenaces les plus répandues

Empêchez l'exfiltration de données sensibles

et de la propriété intellectuelle des machines infectées à l'extérieur de votre organisation

Bloquez rapidement les cybermenaces

pour protéger votre organisation contre les cybermenaces et maintenir la continuité de vos activités

Kaspersky Threat Data Feeds

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture