Comprendre WBNP et SBNP

Table des matières

- Introduction
- Informations générales
  - WSA - Participation au réseau WebBase
  - ESA - Participation au réseau SenderBase
- Questions générales de sécurité
- Fonctionnement
  - Participation au réseau SenderBase (e-mail)
    - Statistiques partagées par appliance de messagerie
    - Statistiques partagées par adresse IP
    - Statistiques partagées par client SDS
    - Données de télémétrie AMP SBNP
  - Participation au réseau WebBase (Web)
    - Statistiques partagées par demande Web
    - Statistiques avancées sur les programmes malveillants par requête Web
    - Flux Statistiques sur les commentaires utilisateur
    - Exemple de données fournies - Participation standard
    - Exemple de données fournies - Participation limitée
    - Décodage WBNP complet
    - Statistiques partagées par demande Web
    - Statistiques avancées sur les programmes malveillants par requête Web
    - Flux Statistiques sur les commentaires utilisateur
- Contenu de Talos Detection
- Axé sur les menaces
- Informations connexes

Introduction

Ce document décrit le chemin de retour des données télémétriques vers Cisco et Talos.

Informations générales

Les produits Cisco de sécurisation du contenu du web et de la messagerie électronique peuvent fournir des données télémétriques à Cisco et Talos afin d'accroître l'efficacité de la catégorisation du web dans l'appliance de sécurisation du web (WSA) et de connecter la réputation IP de l'appliance de sécurisation de la messagerie (ESA).

Les données de télémétrie sont fournies pour le WSA et l'ESA sur la base d'une option.

Les données sont transmises via des paquets chiffrés SSL codés binaires. Les pièces jointes fournies fournissent des informations sur les données, le formatage spécifique et les descriptions des données transmises.

Les données WebBase Network Participation (WBNP) et SenderBase Network Participation (SBNP) ne sont pas visibles dans un journal direct ou un format de fichier. Ces données sont transmises sous forme chiffrée. À aucun moment ces données ne sont « au repos ».

WSA - Participation au réseau WebBase

Cisco reconnaît l'importance de préserver votre confidentialité et ne collecte ni n'utilise d'informations personnelles ou confidentielles telles que des noms d'utilisateur et des phrases de passe. De plus, les noms de fichiers et les attributs d'URL inclus avec le nom d'hôte sont masqués pour garantir la confidentialité.

En ce qui concerne les transactions HTTPS décryptées, le réseau SensorBase ne reçoit que l'adresse IP, le score de réputation Web et la catégorie d'URL du nom de serveur dans le certificat.

Pour obtenir des informations complètes, consultez le Guide de l'utilisateur WSA pour la version d'AsyncOS for Web Security actuellement en cours d'exécution sur votre appliance.

Reportez-vous à la section Cisco SensorBase Network du Guide de l'utilisateur ESA.

ESA - Participation au réseau SenderBase

Si vous participez au réseau SenderBase, vous permettez à Cisco de collecter des statistiques agrégées sur le trafic des e-mails au sein de votre entreprise, ce qui augmente l'utilité du service pour tous les utilisateurs. La participation est volontaire. Cisco collecte uniquement des données récapitulatives sur les attributs des messages et des informations sur la manière dont les différents types de messages ont été traités par les appareils Cisco. Par exemple, Cisco ne collecte pas le corps du message ni l'objet du message. Les informations d'identification personnelle et les informations qui identifient votre entreprise restent confidentielles.

Pour obtenir des informations complètes, consultez le Guide de l'utilisateur ESA pour connaître la version d'AsyncOS for ESA Security actuellement exécutée sur votre appliance.

Reportez-vous au chapitre SenderBase Network Participation du Guide de l'utilisateur.

Questions générales de sécurité

Où sont stockées les données collectées ?

La télémétrie des appareils est stockée dans les data centers Cisco basés aux États-Unis.

Qui a accès aux données collectées et stockées ?

L'accès est limité au personnel de Cisco SBG qui analyse/utilise les données pour créer des informations exploitables.

Quelle est la durée de conservation des données collectées ?

Il n'existe aucune stratégie de rétention/d'expiration des données concernant la télémétrie des appliances. Les données peuvent être conservées indéfiniment ou peuvent être supprimées pour diverses raisons, y compris, mais sans s'y limiter, le sous-échantillonnage/agrégation, la gestion du stockage, l'âge, la pertinence par rapport aux menaces actuelles/futures, etc.

Les numéros de série ou les adresses IP publiques du client sont-ils stockés dans la base de données de catégorisation Talos ?

Non, seules les URL et les catégories sont conservées. Le paquet WBNP ne contient pas d'informations IP source.

Fonctionnement

Cette section détaille le fonctionnement, le type de données (par description) et un exemple de données pour démontrer les informations qui seraient transmises :

- SBNP : types de données spécifiques (champs) et exemples de données liés à la sécurité de la messagerie
- WBNP : types de données spécifiques (champs) et exemples de données liés à la sécurité Web
- Fonctionnement de la détection des menaces - Présentation générale de la détection des menaces du point de vue opérationnel

Participation au réseau SenderBase (e-mail)

Statistiques partagées par appliance de messagerie

Élément	Exemple de données
Identifiant MGA	MGA 10012
Horodatage	Données de 8h à 8h05 le 1er juillet 2005
Numéros de version du logiciel	MGA version 4.7.0
Numéros de version du jeu de règles	Ensemble de règles antispam 102
Intervalle de mise à jour antivirus	Mises à jour toutes les 10 minutes
Taille de quarantaine	500 Mo
Nombre de messages de quarantaine	50 messages actuellement en quarantaine
Seuil de score de virus	Envoyer les messages en quarantaine au niveau de menace 3 ou supérieur
Somme des scores de virus pour les messages entrant en quarantaine	120
Nombre de messages entrant en quarantaine	30 (donne un score moyen de 4)
Durée de quarantaine maximale	12 heures
Nombre de messages de quarantaine contre les attaques ventilés par motif d'entrée et de sortie de la quarantaine, en corrélation avec le résultat de l'antivirus	50 entrées en quarantaine en raison de la règle .exe 30 sorties de la quarantaine en raison d'une libération manuelle, et les 30 étaient positives pour le virus
Nombre de messages de quarantaine contre les attaques ventilés par action entreprise à la sortie de la quarantaine	10 messages avaient des pièces jointes supprimées après avoir quitté la quarantaine
Somme du temps pendant lequel les messages étaient mis en quarantaine	20 heures

Statistiques partagées par adresse IP

Élément	Exemple de données	Participation Standard	Participation limitée
Nombre de messages à différentes étapes de l'appliance	Vue par le moteur antivirus : 100 Vue par le moteur antispam : 80		
Somme des scores et verdicts relatifs à l'antispam et à l'antivirus	2 000 (somme des scores antispam pour tous les messages vus)		
Nombre de messages atteignant différentes	100 messages correspondent aux règles A et B		

combinaisons de règles antispam et antivirus	50 messages ont atteint la règle A uniquement		
Nombre de connexions	20 connexions SMTP		
Nombre total de destinataires non valides	50 destinataires au total 10 destinataires non valides		
Nom(s) de fichier haché(s) : (a)	Un fichier <one-way-hash>.pif a été trouvé dans une pièce jointe d'archive appelée <one-way-hash>.zip.	Nom De Fichier Sans Fusion	Nom de fichier haché
Nom(s) de fichier masqué(s) : (b)	Un fichier aaaaaa0.aaa.pif a été trouvé dans un fichier aaaaaa.zip.	Nom De Fichier Sans Fusion	Nom de fichier obscurci
URL Nom d'hôte (c)	Un lien a été trouvé dans un message vers www.domain.com	Nom d'hôte URL non masqué	Nom d'hôte URL obscurci
Chemin d'URL obscurci (d)	Un lien a été trouvé dans un message vers le nom d'hôte www.domain.com, et avait le chemin aaa000aa/aa00aaa.	Chemin d'URL non masqué	Chemin d'URL obscurci
Nombre de messages par résultat d'analyse du spam et des virus	10 spam positif 10 Spam négatif 5 Spam suspecté 4 Virus positifs 16 Virus négatifs 5 Virus non analysable		
Nombre de messages par verdicts antispam et antivirus différents	500 courriers indésirables, 300 courriers indésirables		
Nombre de messages dans les plages de tailles	125 dans la plage 30K-35K		
Nombre de types d'extension	300 pièces jointes « .exe »		

différents			
Corrélation des types de pièces jointes, du type de fichier réel et du type de conteneur	100 pièces jointes portant l'extension « .doc », mais en réalité « .exe » 50 pièces jointes sont des extensions « .exe » dans un fichier zip		
Corrélation de l'extension et du type de fichier réel avec la taille des pièces jointes	30 pièces jointes étaient des fichiers .exe compris entre 50 et 55 000		
Nombre de messages par résultat d'échantillonnage stochastique	Échantillonnage de 14 messages ignoré 25 messages en file d'attente pour échantillonnage 50 messages analysés à partir de l'échantillonnage		
Nombre de messages dont la vérification DMARC a échoué	34 messages ont échoué à la vérification DMARC		

Remarques :

(a) Les noms de fichiers sont codés dans un hachage unidirectionnel (MD5).

(b) Les noms de fichiers sont envoyés sous une forme masquée, avec toutes les lettres ASCII minuscules ([a-z]) remplacées par « a », toutes les lettres ASCII majuscules ([A-Z]) remplacées par « A », tous les caractères UTF-8 multi-octets remplacés par « x » (pour assurer la confidentialité des autres jeux de caractères), tous les chiffres ASCII ([0-9]) remplacés.

(c) Les noms d'hôte URL pointent vers un serveur Web fournissant du contenu, comme le fait une adresse IP. Aucune information confidentielle, comme les noms d'utilisateur et les mots de passe, n'est incluse.

(d) Les informations URL incluses avec le nom d'hôte sont masquées pour garantir que les informations personnelles de l'utilisateur ne sont pas révélées.

Statistiques partagées par client SDS

Élément	Exemple de données
Horodatage	
Version du client	
Nombre de demandes adressées au Client	
Nombre de demandes formulées par le client SDS	
Résultats temporels pour les recherches DNS	
Résultats du temps de réponse du serveur	
Durée d'établissement de la connexion au serveur	
Nombre de connexions établies	
Nombre de connexions ouvertes simultanées au serveur	
Nombre de demandes de service à WBRS	
Nombre de demandes qui ont atteint le cache WBRS local	
Taille du cache WBRS local	
Résultats du temps de réponse du WBRS distant	

Données de télémétrie AMP SBNP

Format	Exemple de données
amp_verdicts' : { ("verdict", "spyname", "score", "uploaded", "file_name"),	
("verdict", "spyname", "score", "uploaded", "file_name"),	
("verdict", "spyname", "score", "uploaded", "file_name"),	
.....	
("verdict", "spyname", "score", "uploaded", "file_name"),	
}	
Description	
Verdict - de la requête de réputation AMP	malveillant/propre/inconnu
Spyname : nom du programme malveillant détecté	[Test de cheval de Troie]
Score : score de réputation attribué par AMP	[1-100]
Téléchargement - Cloud AMP indiqué pour le téléchargement du fichier	1
Nom du fichier - Nom de la pièce jointe	abcd.pdf

Participation au réseau WebBase (Web)

Statistiques partagées par demande Web

Élément	Exemple de données	Participation Standard	Participation limitée

Version	coeus 7.7.0-608		
Numéro de série			
Facteur d'échantillonnage SBNP (volume)			
Facteur d'échantillonnage SBNP (taux)	1		
IP et port de destination		segments de chemin d'URL non masqués	segments de chemin d'URL hachés
Catégorie de programme malveillant choisie par Anti-Spyware	Ignoré		
Score WBRS	4.7		
Verdict de catégorie de malware McAfee			
URL du référent		segments de chemin d'URL non masqués	segments de chemin d'URL hachés
ID du type de contenu			
Étiquette de décision ACL	0		
Catégorisation Web héritée			
Catégorie Web CIWUC et source de décision	{'src' : 'req', 'cat' : '1026'}		
Nom de l'application AVC	Publicités et suivi		

Type d'application AVC	Réseaux publicitaires		
Comportement des applications AVC	Non sécuritaire		
Suivi des résultats AVC internes	[0,1,1,1]		
Suivi des agents utilisateurs via une structure de données indexée	3		

Statistiques avancées sur les programmes malveillants par requête Web

Statistiques AMP	
Verdict - de la requête de réputation AMP	malveillant/propre/inconnu
Spyname : nom du programme malveillant détecté	[Test de cheval de Troie]
Score : score de réputation attribué par AMP	[1-100]
Téléchargement - Cloud AMP indiqué pour le téléchargement du fichier	1
Nom du fichier - Nom de la pièce jointe	abcd.pdf

Flux Statistiques sur les commentaires utilisateur

Statistiques partagées par utilisateur final Mauvaise catégorisation Commentaires	
Élément	Exemple de données
ID du moteur (numérique)	0

Code de catégorisation Web hérité	
Source de catégorisation Web CIWUC	« resp » / « req »
Catégorie Web CIWUC	1026

Exemple de données fournies - Participation standard

```
# categorized
"http://google.com/": {    "wbrs": "5.8",
    "fs": {
          "src": "req",
          "cat": "1020"
    },
}

# uncategorized
"http://fake.example.com": {    "fs": {
      "cat": "-"
    },}
```

Exemple de données fournies - Participation limitée

- Demande initiale du client : www.example.com/Sample-Web-Request-Path
- Message consigné (dans le serveur de télémétrie) : http://www.example.com/76bd845388e0

Décodage WBNP complet

Statistiques partagées par appliance Cisco :

Élément	Exemple de données
Version	coeus 7.7.0-608
Numéro de série	0022190B6ED5-XYZ1YZ2
Maquette	S660

Webroot activé	1
AVC activé	1
Sophos activé	0
Catégorisation côté réponse activée	1
Moteur Anti-Spyware activé	default-2001005008
Version SSE du logiciel anti-espion	default-2001005008
Version des définitions Spycat Anti-Spyware	default-8640
Version DAT de la liste de blocage des URL anti-spyware	
URL anti-spyware Phishing Version DAT	
Version DAT des cookies anti-spyware	
Blocage du domaine anti-spyware activé	0
Seuil de risque de menace anti-spyware	90
McAfee activé	0
Version du moteur McAfee	
Version des fichiers DAT McAfee	default-5688
Niveau de détail WBNP	2
Version du moteur WBRS	freebsd6-i386-300036

Versions des composants WBRS	categories=v2-1337979188, ip=default-1379460997, keyword=v2-1312487822, prefixcat=v2-1379460670, rule=default-1358979215
Seuil de liste de blocage WBRS	-6
Seuil de liste d'autorisation WBRS	6
WBRS activé	1

Mobilité sécurisée activée	0
Moniteur de trafic de couche 4 activé	0
Version de la liste de blocage Moniteur de trafic L4	default-0
Liste de blocage Admin Moniteur de trafic de couche 4	
Ports de liste de blocage admin du Moniteur de trafic de couche 4	
Liste autorisée Moniteur du trafic de couche 4	
Ports de liste d'autorisation Moniteur de trafic de couche 4	
facteur d'échantillonnage SBNP	0.25
Facteur d'échantillonnage SBNP (volume)	0,1
Version du SDK SurfControl (héritée)	default-0
Version complète de la base de données SurfControl (héritée)	default-0

Version du fichier SurfControl Local Incremental Accumulation (hérité)	default-0
Version du moteur Firestone	default-210016
Version DAT Firestone	v 2-310003
Version du moteur AVC	default-110076
Version DAT AVC	default-1377556980
Version du moteur Sophos	default-1310963572
Version DAT Sophos	default-0
Analyse adaptative activée	0
Seuil de score de risque d'analyse adaptative	[10, 6, 3]
Seuil de facteur de charge adaptatif	[5, 3, 2]
SOCKS activé	0
Total des transactions	

Total des transactions	
Total des transactions autorisées	
Nombre total de transactions détectées par programme malveillant	
Nombre total de transactions bloquées par la stratégie Admin	
Total des transactions bloquées par le score WBRS	

Total des transactions à risque élevé	
Total des transactions détectées par le Moniteur de trafic	
Nombre total de transactions avec les clients IPv6	
Nombre total de transactions avec les serveurs IPv6	
Total des transactions utilisant le proxy SOCKS	
Total des transactions des utilisateurs distants	
Total des transactions des utilisateurs locaux	
Total des transactions autorisées avec le proxy SOCKS	
Total des transactions des utilisateurs locaux autorisés à utiliser le proxy SOCKS	
Total des transactions des utilisateurs distants autorisés à utiliser le proxy SOCKS	
Nombre total de transactions bloquées via le proxy SOCKS	
Total des transactions des utilisateurs locaux bloquées à l'aide du proxy SOCKS	
Total des transactions des utilisateurs distants bloquées à l'aide du proxy SOCKS	

Secondes depuis le dernier redémarrage	2843349
Utilisation du processeur (%)	9.9
Utilisation de la mémoire vive (%)	55.6

Utilisation du disque dur (%)	57.5
Utilisation de la bande passante (/s)	15307
Ouvrir les connexions TCP	2721
Transactions par seconde	264
Latence client	163
Taux d'accès au cache	21
Utilisation du processeur proxy	17
Utilisation du processeur WBRS WUC	2.5
Journalisation de l'utilisation CPU	3.4
Utilisation du processeur de reporting	3.9
Utilisation du processeur Webroot	0
Utilisation du processeur Sophos	0
Utilisation du processeur McAfee	0
sortie de l'utilitaire vmstat (vmstat -z, vmstat -m)	
Nombre de stratégies d'accès configurées	32
Nombre de catégories Web personnalisées configurées	32
Fournisseur d'authentification	De base, NTLMSSP

Domaines d'authentification	Nom d'hôte, protocole et autres éléments de configuration du fournisseur d'authentification

Statistiques partagées par demande Web

Élément	Exemple de données	Participation Standard	Participation limitée
Version	coeus 7.7.0-608		
Numéro de série			
Facteur d'échantillonnage SBNP (volume)			
Facteur d'échantillonnage SBNP (taux)	1		
IP et port de destination		segments de chemin d'URL non masqués	segments de chemin d'URL hachés
Catégorie de programme malveillant choisie par Anti-Spyware	Ignoré		
Score WBRS	4.7		
Verdict de catégorie de malware McAfee			
URL du référent		segments de chemin d'URL non masqués	segments de chemin d'URL hachés
ID du type de contenu			

Étiquette de décision ACL	0		
Catégorisation Web héritée			
Catégorie Web CIWUC et source de décision	{'src' : 'req', 'cat' : '1026'}		
Nom de l'application AVC	Publicités et suivi		
Type d'application AVC	Réseaux publicitaires		
Comportement des applications AVC	Non sécuritaire		
Suivi des résultats AVC internes	[0,1,1,1]		
Suivi des agents utilisateurs via une structure de données indexée	3		

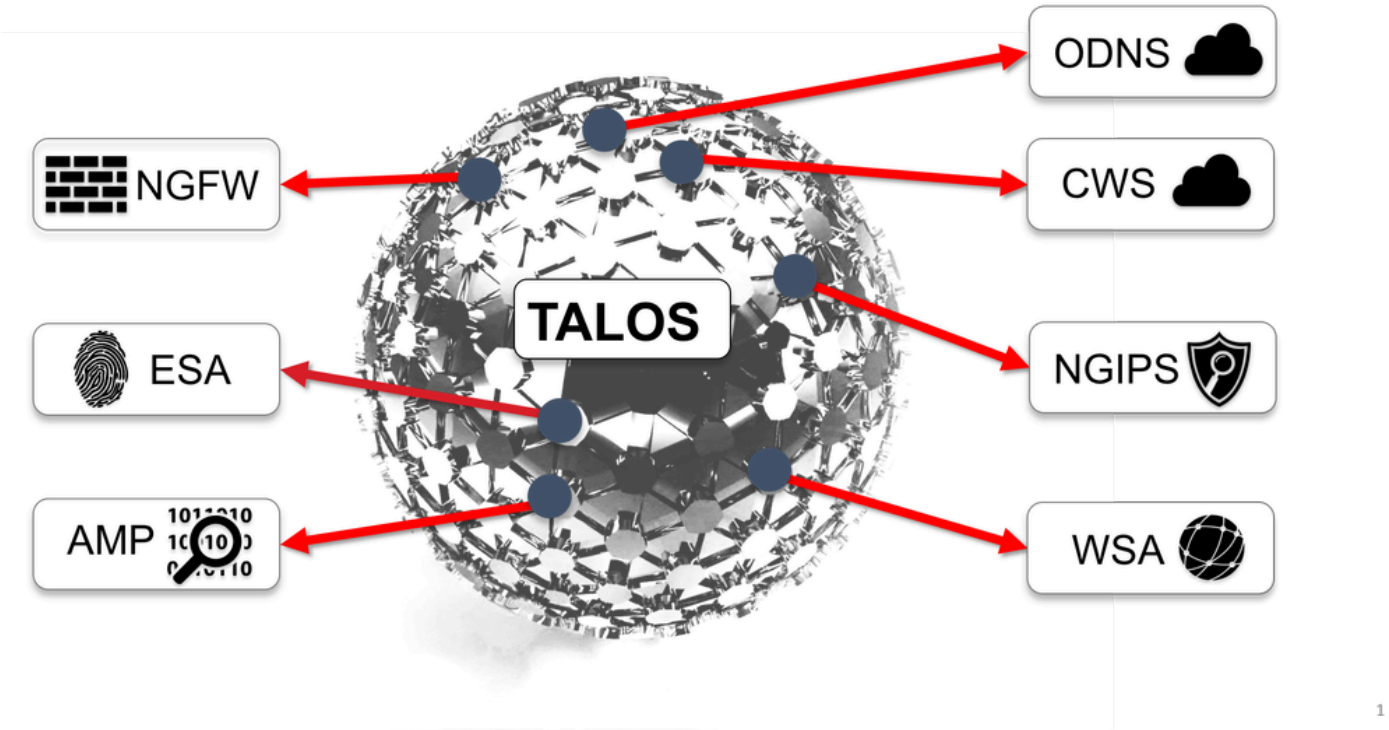
Statistiques avancées sur les programmes malveillants par requête Web

Statistiques AMP	
Verdict - de la requête de réputation AMP	malveillant/propre/inconnu
Spyname : nom du programme malveillant détecté	[Test de cheval de Troie]
Score : score de réputation attribué par AMP	[1-100]
Téléchargement - Cloud AMP indiqué pour le téléchargement du fichier	1
Nom du fichier - Nom de la pièce jointe	abcd.pdf

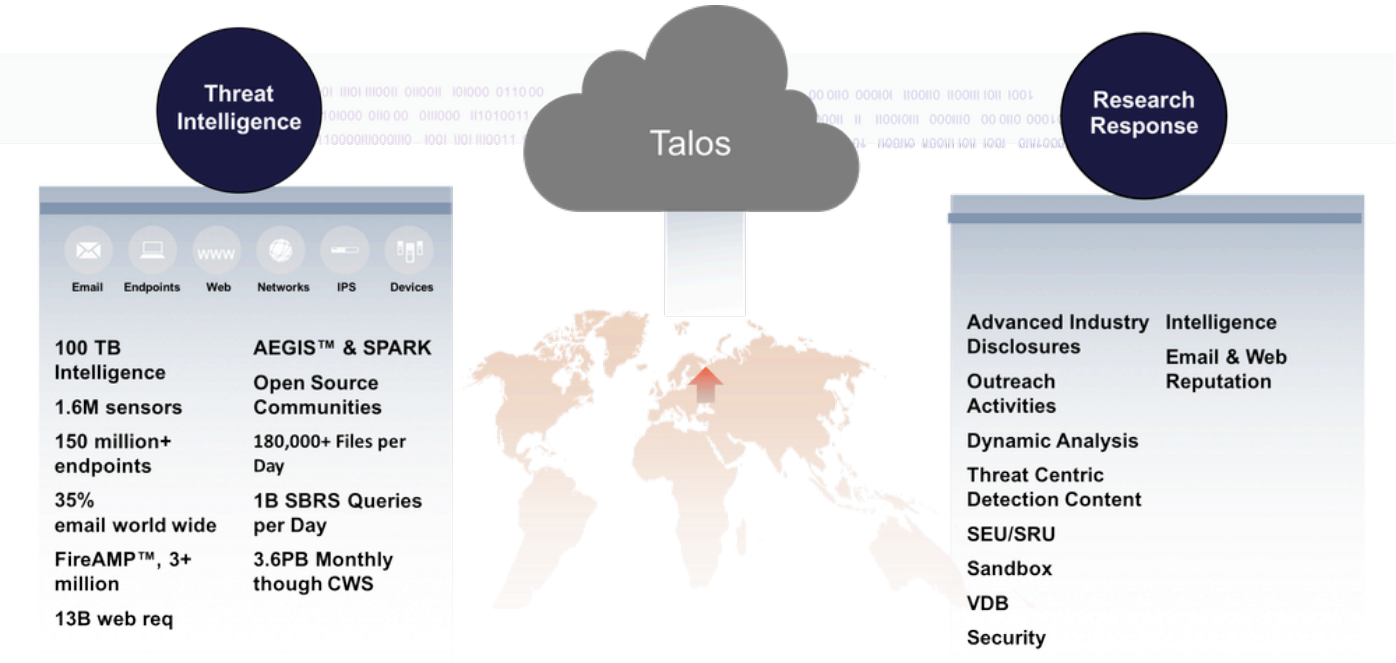
Flux Statistiques sur les commentaires utilisateur

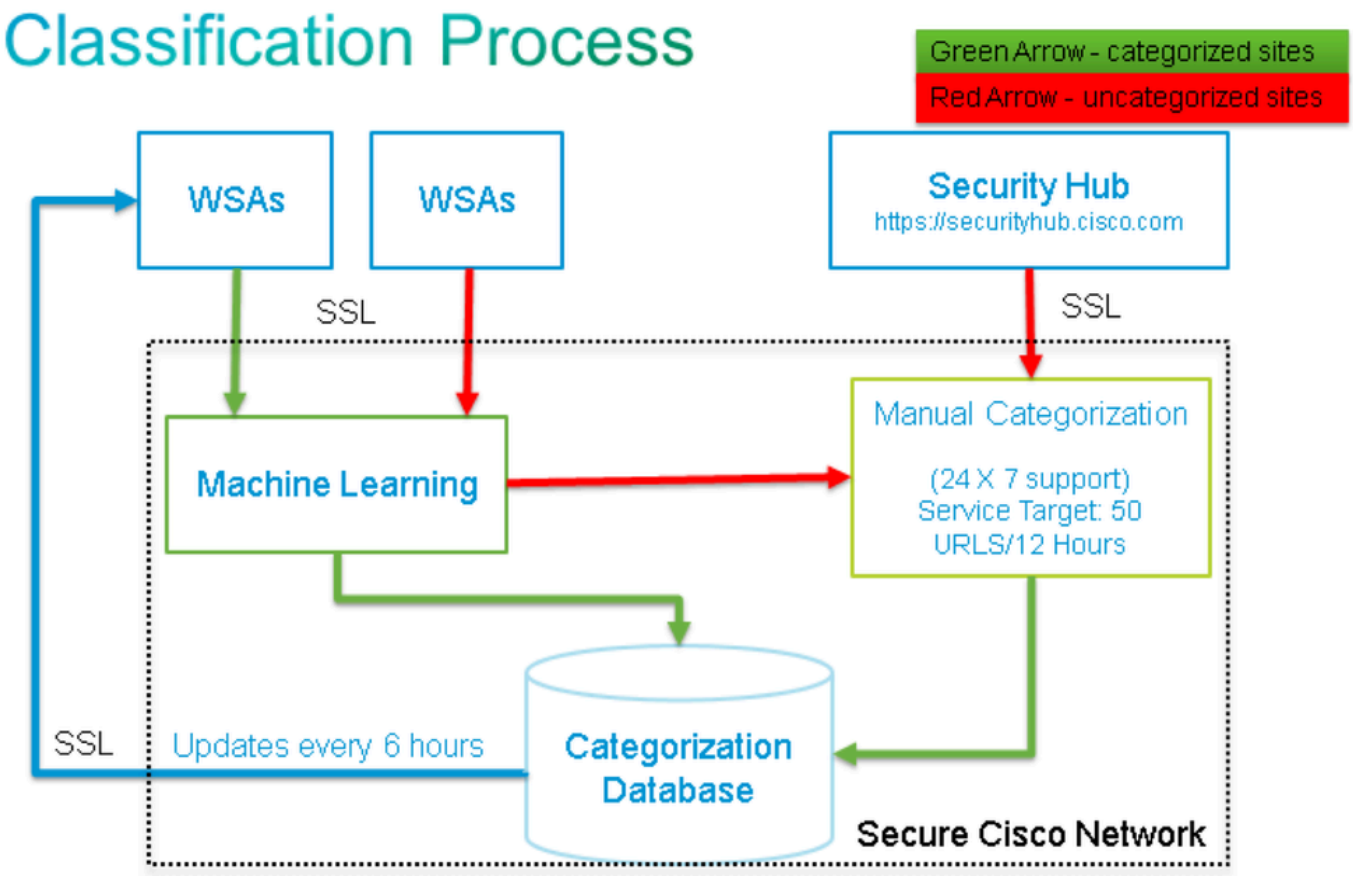
Statistiques partagées par utilisateur final Mauvaise catégorisation Commentaires	
Élément	Exemple de données
ID du moteur (numérique)	0
Code de catégorisation Web hérité	
Source de catégorisation Web CIWUC	« resp » / « req »
Catégorie Web CIWUC	1026

Contenu de Talos Detection



Axé sur les menaces





Informations connexes

- [Appareil de sécurité Web Cisco - Page produit]
- [Appliance de sécurisation de la messagerie Cisco - Page produit]

- Documentation et assistance techniques

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.