Web Base Network Participation (WBNP) et Sender Base Network Participation (SBNP)

Contenu

Introduction

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

Les données télémétriques sont fournies pour l'ASM et l'ESA sur la base de l'option d'adhésion.

Les données sont transmises via des paquets chiffrés SSL codés en binaire. Les pièces jointes ci-dessous fournissent un aperçu des données, de leur mise en forme spécifique et des descriptions des données transmises. Les données WebBase Network Participation (WBNP) et SenderBase Network Participation (SBNP) ne sont pas visibles dans un fichier journal ou un journal direct. Ces données sont transmises sous forme chiffrée. Ces données ne sont jamais au repos.

WSA - Participation au réseau WebBase

Cisco reconnaît l'importance du maintien de votre vie privée et ne collecte ni n'utilise d'informations personnelles ou confidentielles telles que des noms d'utilisateur et des phrases de passe. En outre, les noms de fichiers et les attributs d'URL qui suivent le nom d'hôte sont brouillés pour garantir la confidentialité.

Lorsqu'il s'agit de transactions HTTPS déchiffrées, le réseau SensorBase reçoit uniquement l'adresse IP, le score de réputation Web et la catégorie d'URL du nom de serveur dans le certificat.

Pour plus d'informations, consultez le Guide de l'utilisateur WSA pour la version d'AsyncOS for Web Security actuellement exécutée sur votre appareil. Reportez-vous à la section « Réseau Cisco SensorBase » du Guide de l'utilisateur.

ESA - Participation au réseau SenderBase

Les clients participant au réseau SenderBase permettent à Cisco de collecter des statistiques agrégées sur le trafic de messagerie de leur entreprise, ce qui augmente l'utilité du service pour tous ceux qui l'utilisent. La participation est volontaire. Cisco collecte uniquement des données récapitulatives sur les attributs des messages et des informations sur la manière dont différents types de messages ont été traités par les appliances Cisco. Par exemple, Cisco ne collecte pas le corps du message ou l'objet du message. Les renseignements et les renseignements personnels qui identifient votre organisation demeurent confidentiels.

Pour plus d'informations, pExaminer le formulaire EGuide de l'utilisateur SA pour la version d'AsyncOS pour ESA Security actuellement en cours d'exécution sur votre appliance. Reportez-vous au chapitre « SenderBase Network Participation » du Guide de l'utilisateur.

Questions générales de sécurité - FAQ

Question :	Où sont stockées les données collectées ?
Réponse :	La télémétrie des appareils est stockée dans des data centers basés aux États-Unis de Cisco.
Question :	Qui a accès aux données collectées et stockées ?
Réponse :	L'accès est limité au personnel de Cisco SBG qui analyse/utilise les données pour créer des informations exploitables.
Question :	Quelle est la durée de conservation des données collectées ?
Réponse :	Il n'existe pas de stratégie de rétention/d'expiration des données concernant la télémétrie des appareils. Les données peuvent être conservées indéfiniment ou peuvent être supprimées pour diverses raisons, notamment, mais sans s'y limiter, l'échantillonnage/agrégation, la gestion du stockage, l'âge, la pertinence par rapport aux menaces actuelles/futures, etc.
Question :	Les numéros de série du client ou les adresses IP publiques sont-ils stockés dans la base de données de catégorisation Talos ?
Réponse :	Non, seules les URL et les catégories sont conservées. Le paquet WBNP ne contient pas d'informations IP source.

Opération

Ci-dessous, 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 - Vue d'ensemble de la détection des menaces du point de vue opérationnel

Participation au réseau SenderBase (e-mail)

Statistiques partagées par e-mailappareil

Élément	Exemples de données
Identificateur MGA	MGA 10012
Horodatage	Données de 8 h à 8 h 5 le 1er juillet 2005
Numéros de version logicielle	MGA version 4.7.0
Numéros de version de l'ensemble de règles	Ensemble de règles antispam 102
Intervalle de mise à jour antivirus	Mises à jour toutes les 10 minutes
Taille de la 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 d 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 maximale de quarantaine	12 heures
Nombre de messages de quarantaine d'attaques ventilés par raison de leur entrée et de leur sortie en quarantaine, en corrélation avec le résultat antivirus	50 entrées dans la quarantaine en raison de la règ .exe 30 quittant la quarantaine en raison d'une libé manuelle, et les 30 étaient tous positifs pour le viru
Nombre de messages de quarantaine d'attaques ventilés par l'action prise lors de la sortie de la quarantaine	Les pièces jointes de 10 messages ont été supprim après avoir quitté la quarantaine
Somme des messages de temps en quarantaine	20 heures

Statistiques partagées par adresse IP

Élément	Exemples de données	Participation standard	Participation limitée
Nombre de messages à différentes étapes au sein de l'appareil	Vue par le moteur antivirus : 100 Vu par le moteur antispam : 80		
Somme des scores et verdicts de l'antispam et de l'antivirus	2 000 (somme des scores antispam pour tous les messages affichés)		
Nombre de messages ayant atteint différentes combinaisons de règles	100 messages renvoient aux règles A et B 50 messages sur la règle A uniquement		

antispam et antivirus			
Nombre de connexions	20 connexions SMTP		
Nombre total et non valide de destinataires	50 destinataires au total 10 destinataires non valides		
Nom(s) de fichier haché(s) : (a)	Un fichier <hachage unidirectionnel>.pif a été trouvé dans une pièce jointe d'archive appelée <hachage unidirectionnel>.zip.	Nom de fichier anonyme	Nom de fichi haché
Nom(s) de fichier obfusé(s) : (b)	Un fichier aaaaaa0.aaa.pif a été trouvé dans un fichier aaaaaa.zip.	Nom de fichier anonyme	Nom de fichi brouillé
Nom d'hôte d'URL (c)	Un lien a été trouvé dans un message à www.domain.com	Nom d'hôte d'URL anonyme	Nom d'hôte d'URL obscu
Chemin d'URL obscurci (d)	Un lien a été trouvé à l'intérieur d'un message vers le nom d'hôte www.domain.com, et avait le chemin aaa000aa/aa00aaa.	Chemin d'URL non obscurci	Chemin d'UR obscurci
Nombre de messages par spam et résultats de l'analyse antivirus	10 Spam positif 10 Spam négatif 5 Spam suspecté 4 Virus positif 16 Virus Négatif 5 Virus non analysés		
Nombre de messages par verdicts antivirus et antispam	500 spams, 300 jambons		
Nombre de messages dans les plages de taille	125 dans une plage de 30 000 à 35 000		
Nombre de types d'extension différents	Pièces jointes “.exe ” 300		
Corrélation entre les types de pièces jointes, le type de fichier vrai et le type de conteneur	100 pièces jointes qui ont une extension ” “.doc mais qui sont en fait “.exe ” 50 pièces jointes sont des extensions ” “.exe dans un zip		
Corrélation entre l'extension et le type de fichier vrai et la taille de pièce jointe	30 pièces jointes ont été ” “.exe dans la plage 50-55 000		
Nombre de messages par résultats d'échantillonnage stochastique	Échantillonnage de 14 messages ignoré 25 messages mis 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 seront codés dans un hachage à sens unique (MD5).

b) Les noms de fichiers seront envoyés sous une forme obfusée, 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 protéger la confidentialité des autres jeux de caractères), tous les chiffres ASCII ([0-9])).

(c) Les noms d'hôte d'URL pointent vers un serveur Web fournissant du contenu, tout comme

une adresse IP. Aucune information confidentielle, comme les noms d'utilisateur et les mots de passe, n'est incluse.

d) Les informations URL qui suivent le nom d'hôte sont obfusées pour s'assurer que les informations personnelles de l'utilisateur ne sont pas révélées.

Statistiques partagées par client SDD

Élément	Exemples de données
Horodatage	
Version du client	
Nombre de demandes adressées au client	
Nombre de demandes effectuées auprès du client SDS	
Résultats des recherches DNS	
Résultats du temps de réponse du serveur	
Délai d'établissement de la connexion au serveur	
Nombre de connexions établies	
Nombre de connexions ouvertes simultanées au serveur	
Nombre de demandes de service au 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	Exemples de données
amp_verdicts' : { (« verdict », « nom_espion », « score », « téléchargé », « nom_fichier »), (« verdict », « nom_espion », « score », « téléchargé », « nom_fichier »), (« verdict », « nom_espion », « score », « téléchargé », « nom_fichier »), ... (« verdict », « nom_espion », « score », « téléchargé », « nom_fichier »), }	
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 à AMP	[1-100]
Upload - Cloud AMP indiqué pour télécharger le fichier	1
Nom du fichier - Nom de la pièce jointe	abcd.pdf

Participation au réseau WebBase (Web)

Statistiques partagées par demande Web

Élément	Exemples de données	Participation standard	Participation limitée
Version	ceus 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 brouillés	segments de chemin d'URL hachés
Catégorie de programmes malveillants choisis pour les logiciels anti-espions	Ignoré		
Score WBRS	4.7		
Verdict de catégorie de programmes malveillants McAfee			
URL de référence		segments de chemin d'URL non brouillés	segments de chemin d'URL hachés
ID de type de contenu			
Balise de décision ACL	0		
Catégorisation Web existante			
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 interne des résultats AVC	[0,1,1,1]		
Suivi des agents utilisateur via une structure de données indexée	3		

Statistiques avancées sur les programmes malveillants par demande 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 à AMP	[1-100]
Upload - Cloud AMP indiqué pour télécharger le fichier	1
Nom du fichier - Nom de la pièce jointe	abcd.pdf

Flux de statistiques sur les commentaires des utilisateurs finaux

Statistiques partagées par utilisateur final
Mauvaise catégorisation Commentaires

Élément	Exemples de données
ID du moteur (numérique)	0
Code de classification 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.gunexams.com/Non-Restricted-FREE-Practice-Exams
- Message enregistré (dans le serveur de télémétrie) : http://www.gunexams.com/76bd845388e0

Décodage WBNP complet

Statistiques partagées par appareil Cisco

Élément	Exemples de données
Version	ceus 7.7.0-608
Numéro de série	0022190B6ED5-XYZ1YZ2
Modèle	S660
Webroot activé	1
AVC activé	1
Sophos activé	0
Catégorisation côté réponse activée	1
Moteur anti-espion activé	default-2001005008
Version SSE Anti-Spyware	default-2001005008
Version des définitions de Spycat Anti-Spyware	default-8640
Version DAT de la liste de blocage des URL anti-espion	
Version DAT de phishing des URL anti-espion	
Version DAT des cookies anti-espion	
Blocage du domaine anti-espion activé	0
Seuil de risque de menace contre les logiciels espions	90
McAfee activé	0
Version de McAfee Engine	
Version DAT de McAfee	default-5688
Niveau de détail WBNP	2
Version du moteur WBRS	freebsd6-i386-300036
Versions des composants WBRS	catégories=v2-1337979188, ip=default-1379460997, mot clé=v2-1312487822, prefixcat=v2-1379460670,rule=default-1358979215
Seuil de liste de blocage WBRS	-6

Seuil 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 du Moniteur du trafic de couche 4	default-0
Liste de blocage Admin du Moniteur du trafic de couche 4	
Ports de la liste de blocage Admin du Moniteur du trafic de couche 4	
Autorisation du Moniteur du trafic de couche 4	
Ports autorisés du Moniteur du trafic de couche 4	
Facteur d'échantillonnage SBNP	0.25
Facteur d'échantillonnage SBNP (volume)	0,1
Version SDK de SurfControl (héritée)	default-0
Version de base de données complète SurfControl (héritée)	default-0
Version du fichier d'accumulation incrémentielle locale SurfControl (héritée)	default-0
Version du moteur Firestone	default-210016
Version DAT de 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 adaptatif	[10, 6, 3]
Seuil de facteur de charge d'analyse adaptatif	[5, 3, 2]
SOCKS activés	0
Transactions totales	
Transactions totales	
Total des transactions autorisées	
Nombre total de transactions détectées de programmes malveillants	
Nombre total de transactions bloquées par la stratégie d'administration	
Nombre total de transactions bloquées par score WBRS	
Total des transactions à risque élevé	
Nombre total de transactions détectées par Traffic Monitor	
Nombre total de transactions avec des clients IPv6	
Nombre total de transactions avec des serveurs IPv6	
Nombre total de transactions utilisant le proxy SOCKS	
Nombre total de transactions d'utilisateurs distants	
Total des transactions des utilisateurs locaux	
Nombre total de transactions autorisées à	

l'aide du proxy SOCKS	
Nombre total de transactions d'utilisateurs locaux autorisés à l'aide du proxy SOCKS	
Nombre total de transactions autorisées par les utilisateurs distants à l'aide du proxy SOCKS	
Nombre total de transactions bloquées à l'aide du proxy SOCKS	
Nombre total de transactions d'utilisateurs locaux bloquées à l'aide du proxy SOCKS	
Nombre total de transactions d'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 du client	163
Taux d'accès au cache	21
Utilisation du processeur proxy	17
Utilisation du CPU WUC WBRS	2.5
Journalisation de l'utilisation du processeur	3.4
Utilisation du processeur de reporting	3.9
Utilisation du processeur Webroot	0
Utilisation du processeur Sophos	0
Utilisation du processeur McAfee	0
vmstat, utilitaire sortie (vmstat -z, vmstat -m)	
Nombre de stratégies d'accès configurées	32
Nombre de catégories Web personnalisées configurées	32
Fournisseur d'authentification	Basic, NTLMSSP
Domaines d'authentification	Nom d'hôte du fournisseur d'authentification, protocole et autres éléments de configuration

Statistiques partagées par demande Web

Élément	Exemples de données	Participation standard	Participation limitée
Version	ceus 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 brouillés	segments de chemin d'URL hachés
Catégorie de programmes malveillants choisis pour les logiciels anti-espions	Ignoré		
Score WBRS	4.7		
Verdict de catégorie de programmes			

malveillants McAfee			
URL de référence		segments de chemin d'URL non brouillés	segments de chemin d'URL hachés
ID de type de contenu			
Balise de décision ACL	0		
Catégorisation Web existante			
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 interne des résultats AVC	[0,1,1,1]		
Suivi des agents utilisateur via une structure de données indexée	3		

Statistiques avancées sur les programmes malveillants par demande web

Statistiques AMP

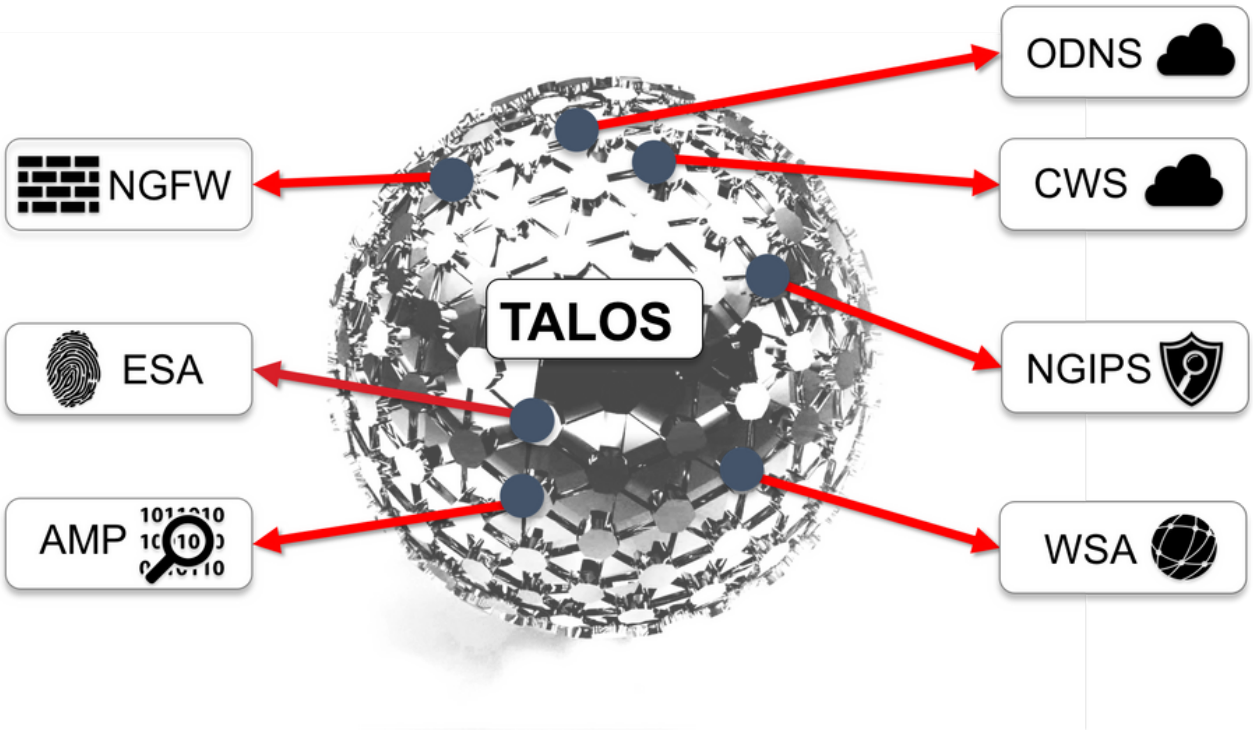
Verdict - de la requête de réputation AMP	malveillant/propre/inconnu
Spyname : nom du programme malveillant détecté.	[Test de cheval de Troie]
Score - score de réputation attribué à AMP	[1-100]
Upload - Cloud AMP indiqué pour télécharger le fichier	1
Nom du fichier - Nom de la pièce jointe	abcd.pdf

Flux de statistiques sur les commentaires des utilisateurs finaux

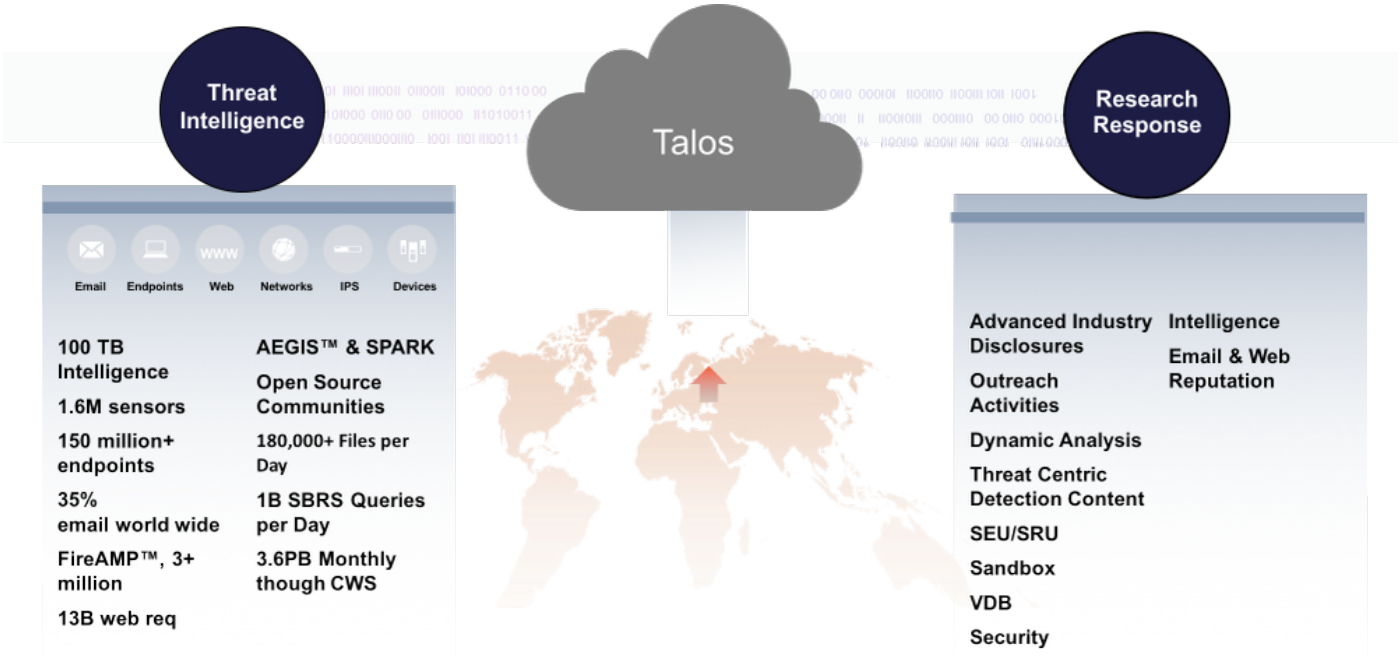
Statistiques partagées par utilisateur final Mauvaise catégorisation Commentaires

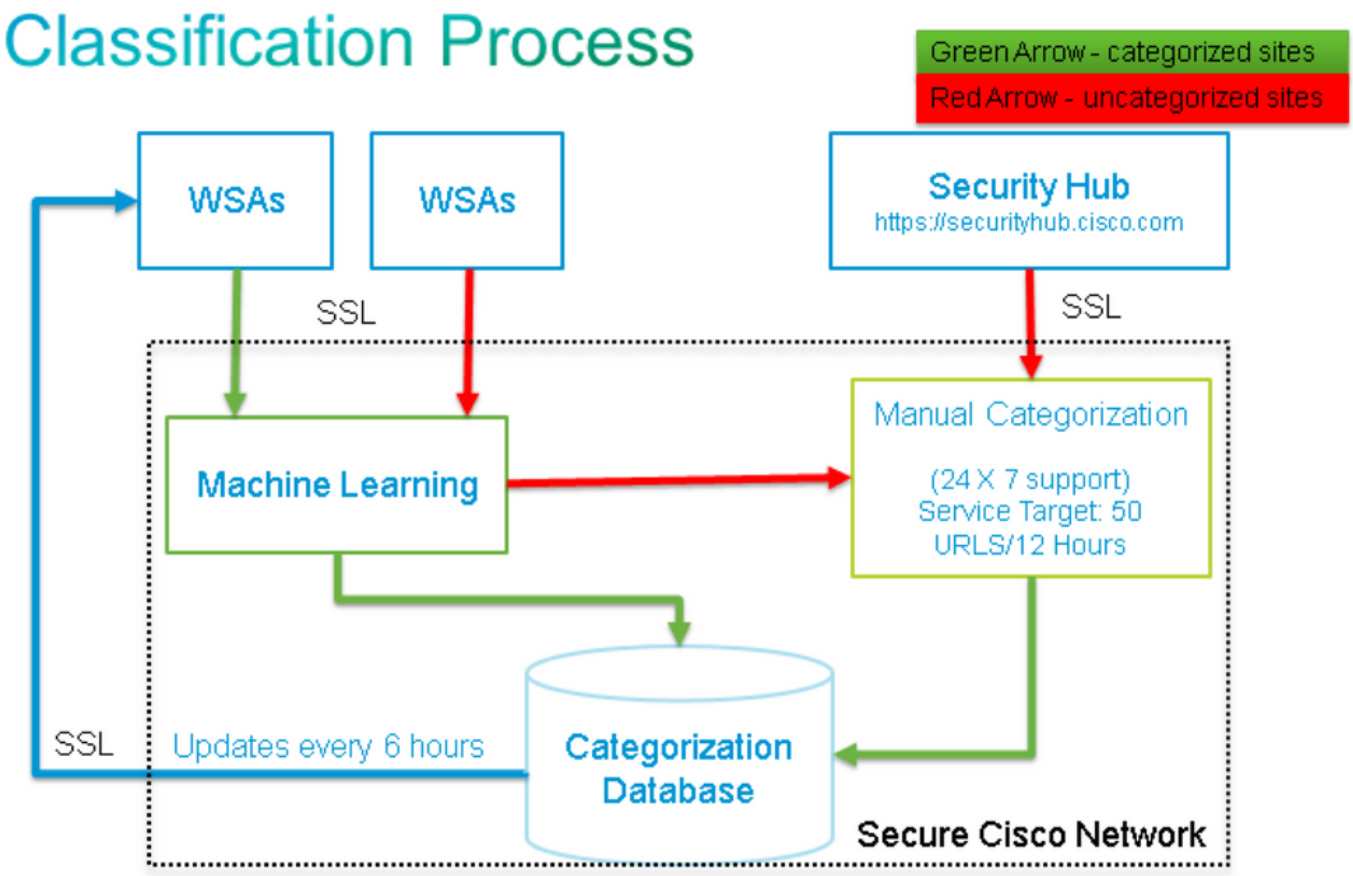
Élément	Exemples de données
ID du moteur (numérique)	0
Code de classification Web hérité	
Source de catégorisation Web CIWUC	‘resp’ / ‘req’
Catégorie Web CIWUC	1026

Contenu de la détection Talos



Axé sur les menaces





Informations connexes

- [Cisco Web Security Appliance - Page produit]
- [Appliance de sécurité de la messagerie Cisco - Page produit]
- [Support et documentation techniques - Cisco Systems]