Participación de red de base web (WBNP) y participación de red de base de remitentes (SBNP)

Contenido

Introducción

Los productos Cisco Web and Email Content Security pueden proporcionar datos de telemetría a Cisco y Talos para aumentar la eficacia de la categorización web en el dispositivo de seguridad web (WSA) y conectar la reputación de IP para el dispositivo de seguridad de correo electrónico (ESA).

Los datos de telemetría se proporcionan para el WSA y el ESA sobre la base de la opción de inclusión.

Los datos se transmiten a través de paquetes cifrados SSL codificados binarios. Los documentos adjuntos que se proporcionan a continuación proporcionarán información sobre los datos, el formato específico y las descripciones de los datos que se transmiten. Los datos de participación de red WebBase (WBNP) y participación de red SenderBase (SBNP) no se pueden ver en un

formato de archivo o registro directo. Estos datos se transmiten de forma cifrada. En ningún momento estos datos están 'en reposo'.

WSA - Participación de red WebBase

Cisco reconoce la importancia de mantener su privacidad y no recopila ni utiliza información personal o confidencial, como nombres de usuario y frases de contraseña. Además, los nombres de archivo y los atributos de URL que siguen al nombre de host se confunden para garantizar la confidencialidad.

Cuando se trata de transacciones HTTPS descifradas, la red SensorBase sólo recibe la dirección IP, la puntuación de reputación web y la categoría URL del nombre del servidor en el certificado.

Para obtener información completa, revise la Guía del usuario de WSA para la versión de AsyncOS para Web Security que se ejecuta actualmente en su dispositivo. Consulte "La red Cisco SensorBase" en la guía del usuario.

ESA - Participación de red SenderBase

Los clientes que participan en SenderBase Network permiten a Cisco recopilar estadísticas de tráfico de correo electrónico agregadas sobre su organización, lo que aumenta la utilidad del servicio para todos los que lo utilizan. La participación es voluntaria. Cisco solo recopila datos resumidos sobre atributos de mensajes e información sobre cómo los distintos tipos de mensajes fueron manejados por los dispositivos de Cisco. Por ejemplo, Cisco no recopila el cuerpo del mensaje ni el asunto del mensaje. La información y la información de identificación personal que identifica a su organización se mantienen confidenciales.

Para obtener información completa, pRevisar la EGuía del usuario de SA para la versión de AsyncOS para la seguridad ESA que se ejecuta actualmente en su dispositivo. Consulte el capítulo "Participación de red SenderBase" en la guía del usuario.

Preguntas frecuentes sobre temas de seguridad general

Pregunta:	¿Dónde se almacenan los datos recopilados?
Respuesta:	La telemetría de los dispositivos se almacena en los Data Centers basados en Cisco US.
Pregunta:	¿Quién tiene acceso a los datos recopilados y almacenados?
Respuesta:	El acceso se limita al personal de Cisco SBG que analiza/utiliza los datos para crear inteliger procesable.
Pregunta:	¿Cuál es el tiempo de retención de los datos recopilados?
Respuesta:	No hay ninguna política de retención/vencimiento de datos con respecto a la telemetría del dispositivo. Los datos pueden mantenerse indefinidamente o eliminarse por diversas razones entre ellas, el muestreo/agregación descendente, la gestión del almacenamiento, la antigüed pertinencia para las amenazas actuales o futuras, etc.
Pregunta:	¿Se almacenan los números de serie de los clientes o las direcciones IP públicas en la base datos de categorización de Talos?
Respuesta:	No, sólo se conservan las URL y las categorías. El paquete WBNP no contiene información d de origen.

Operación

A continuación se detalla la operación, el tipo de datos (por descripción) y una muestra de datos para demostrar la información que se transmitiría:

- SBNP: tipos de datos específicos (campos) y datos de ejemplo relacionados con Email Security
- WBNP: tipos de datos específicos (campos) y datos de ejemplo relacionados con Web Security
- Operación de detección de amenazas: descripción general de la detección de amenazas desde una perspectiva operativa

Participación de red SenderBase (correo electrónico)

Estadísticas compartidas por correo electrónicodispositivo

Ítem	Datos de muestra
Identificador MGA	MGA 10012
Grupo fecha/hora	Datos desde las 8 AM hasta las 8:05 AM el 1 julio de 2005
Números de versión de software	Versión MGA 4.7.0
Números de versión del conjunto de reglas	Conjunto de reglas antispam 102
Intervalo de actualización del antivirus	Actualizaciones cada 10 minutos
Tamaño de cuarentena	500 MB
Recuento de mensajes de cuarentena	50 mensajes actualmente en cuarentena
Umbral de puntuación de virus	Enviar mensajes a cuarentena en el nivel de amenaza 3 o superior
Suma de las puntuaciones de virus para los mensajes que entran en cuarentena	120
Recuento de mensajes que entran en cuarentena	30 (genera una puntuación media de 4)
Tiempo máximo de cuarentena	12 horas
Recuento de mensajes de cuarentena de Outbreak desglosados por el motivo por el que entraron y salieron de cuarentena, correlacionados con el resultado de Anti-Virus	50 entraron en cuarentena debido a la regla 30 que abandonaron la cuarentena debido a liberación manual, y los 30 fueron virus posit
Recuento de mensajes de cuarentena de Outbreak desglosados por las medidas que se tomaron al salir de cuarentena	10 mensajes tenían adjuntos despojados des de salir de cuarentena
Suma de los mensajes de tiempo que se mantuvieron en cuarentena	20 horas

Estadísticas compartidas por dirección IP

Ítem	Datos de muestra	Participación estándar	Participación limitada
Recuento de mensajes en varias etapas del dispositivo	Visto por el motor antivirus: 100 Visto por el motor antispam: 80		
Suma de las puntuaciones y veredictos de Anti-Spam y Anti-Virus	2000 (suma de las puntuaciones anti-spam para todos los mensajes que se ven)		
Número de mensajes que	100 mensajes entran en las reglas A y B		

afectan a diferentes combinaciones de reglas Anti-Spam y Anti-Virus	50 mensajes entran en la regla A solamente		
Número de conexiones	20 conexiones SMTP		
Número de destinatarios totales e inválidos	50 destinatarios en total 10 destinatarios no válidos		
Nombres de archivo hash: (a)	Se encontró un archivo <one-way-hash>.pif dentro de un archivo adjunto llamado <one-way-hash>.zip.	Nombre de archivo no confundido	Nombre de archivo hash
Nombres de archivo desconcertados: (b)	Se encontró un archivo aaaaaaa0.aaa.pif dentro de un archivo aaaaaaa.zip.	Nombre de archivo no confundido	Nombre de archivo conf
Nombre de host de URL (c)	Se encontró un enlace dentro de un mensaje a www.domain.com	Nombre de host de URL sin complicaciones	Nombre de h de URL ocul
Ruta de URL desordenada (d)	Se encontró un link dentro de un mensaje al nombre de host www.domain.com, y tenía path aaa000aa/aa00aaa.	Ruta de URL sin confusión	Ruta de URL desordenada
Número de mensajes por resultados de análisis de spam y virus	10 Spam Positivo 10 Spam Negativo 5 Spam Sospechoso 4 Virus positivos 16 Virus Negativo 5 Virus no escaneable		
Número de mensajes por diferentes veredictos Anti-Spam y Anti-Virus	500 spam, 300 ham		
Recuento de mensajes en intervalos de tamaño	125 en la gama 30K-35K		
Recuento de diferentes tipos de extensión	300 adjuntos ".exe"		
Correlación de tipos de adjuntos, tipo de archivo verdadero y tipo de contenedor	100 adjuntos que tienen una extensión ".doc" pero que en realidad son ".exe" 50 adjuntos son extensiones ".exe" dentro de un zip		
Correlación de extensión y tipo de archivo verdadero con tamaño de archivo adjunto	30 adjuntos eran ".exe" dentro del intervalo de 50-55 000		
Número de mensajes por resultados de muestreo estocástico	14 mensajes omitieron el muestreo 25 mensajes en cola para muestreo 50 mensajes escaneados a partir del muestreo		
Número de mensajes que han fallado en la verificación de DMARC	34 mensajes han fallado en la verificación de DMARC		

Notas:

a) Los nombres de archivo se codificarán mediante un hash de 1 vía (MD5).

(b) Los nombres de archivo se enviarán de forma confusa, con todas las letras ASCII

minúsculas ([a-z]) sustituidas por "a", todas las letras ASCII mayúsculas ([A-Z]) reemplazadas por "A", los caracteres UTF-8 multibyte reemplazados por "x" (para proporcionar privacidad a otros conjuntos de caracteres), reemplazando todos los dígitos ASCII ([0-9]).

(c) Los hostnames de URL apuntan a un servidor web que proporciona contenido, de la misma manera que lo hace una dirección IP. No se incluye información confidencial, como nombres de usuario y contraseñas.

(d) La información de URL que sigue al nombre de host se confunde para asegurarse de que no se revele ninguna información personal del usuario.

Estadísticas compartidas por cliente SDS

Ítem	Datos de muestra
Grupo fecha/hora	
Versión del cliente	
Número de solicitudes realizadas al cliente	
Número de solicitudes realizadas del cliente SDS	
Resultados de tiempo para búsquedas de DNS	
Resultados del tiempo de respuesta del servidor	
Tiempo para establecer la conexión con el servidor	
Número de conexiones establecidas	
Número de conexiones abiertas simultáneas al servidor	
Número de solicitudes de servicio a WBRS	
Número de solicitudes que llegan a la caché WBRS local	
Tamaño de la caché WBRS local	
Resultados del tiempo de respuesta de WBRS remoto	

datos de telemetría SBNP de AMP

Formato	Datos de muestra
amp_verdicts' : { ("veredicto", "spyname", "score", "upload", "file_name"), ("veredicto", "spyname", "score", "upload", "file_name"), ("veredicto", "spyname", "score", "upload", "file_name"), ... ("veredicto", "spyname", "score", "upload", "file_name"), }	
Descripción	
Veredicto: de la consulta de reputación de AMP	malintencionado/limpio/desconocido
Nombre de espía: nombre del malware detectado	[Prueba de troyano]
Puntuación: puntuación de reputación asignada por AMP	[1-100]

Carga: nube de AMP indicada para cargar el archivo	1
Nombre de archivo: nombre del archivo adjunto	abcd.pdf

Participación de red WebBase (Web)

Estadísticas compartidas por solicitud web

Ítem	Datos de muestra	Participación estándar	Participación limitada
Versión	coeus 7.7.0-608		
Serial Number			
Factor de muestreo SBNP (volumen)			
Factor de muestreo SBNP (velocidad)	1		
IP y puerto de destino		segmentos de trayecto de URL sin confusión	segmentos de trayec URL hash
Categoría de malware seleccionada por Anti-Spyware	Omitido		
Puntuación de WBRS	4.7		
veredicto de categoría de malware de McAfee			
URL de referencia		segmentos de trayecto de URL sin confusión	segmentos de trayec URL hash
ID de tipo de contenido			
Etiqueta de decisión ACL	0		
Categorización web antigua			
Categoría web de CIWUC y fuente de decisión	{'src': 'req', 'cat': '1026'}		
Nombre de aplicación AVC	Anuncios y seguimiento		
Tipo de aplicación AVC	Redes de anuncios		
Comportamiento de la aplicación AVC	No Seguros		
Seguimiento de resultados de AVC interno	[0,1,1,1]		
Seguimiento de agentes de usuario a través de una estructura de datos indexada	3		

Estadísticas avanzadas de malware por solicitud web

Estadísticas de AMP

Veredicto: de la consulta de reputación de AMP	malintencionado/limpio/desconocido
Nombre de espía: nombre del malware detectado	[Prueba de troyano]
Puntuación: puntuación de reputación asignada por AMP	[1-100]
Carga: nube de AMP indicada para cargar el archivo	1
Nombre de archivo: nombre del archivo adjunto	abcd.pdf

Fuente de estadísticas de comentarios del usuario final

Estadísticas compartidas por usuario final
Clasificación errónea Comentarios

Ítem	Datos de muestra
ID del motor (numérico)	0
Código de categorización web heredada	
Origen de clasificación web de CIWUC	"resp"/"req"
Categoría web de CIWUC	1026

Datos de ejemplo proporcionados - Participación estándar

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

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

Datos de ejemplo proporcionados - Participación limitada

- Solicitud original del cliente: www.gunexams.com/Non-Restricted-FREE-Practice-Exams
- Mensaje registrado (en el servidor de telemetría): http://www.gunexams.com/76bd845388e0

Decodificación WBNP completa

Estadísticas compartidas por dispositivo de Cisco

Ítem	Datos de muestra
Versión	coeus 7.7.0-608
Número de serie	0022190B6ED5-XYZ1YZ2
Modelo	S660
Webroot habilitado	1
AVC habilitado	1
Sophos habilitado	0
Categorización del lado de respuesta activada	1
Anti-Spyware Engine habilitado	default-2001005008
Versión Anti-Spyware SSE	default-2001005008
Versión de definiciones de Spycat de Anti-Spyware	default-8640
Versión DAT de la lista de bloqueo de URL Anti-Spyware	
Versión DAT de Anti-Spyware URL Phishing	
Versión DAT de Anti-Spyware Cookies	
Bloqueo de dominio antispyware habilitado	0
Umbral de riesgo de amenaza antispyware	90
McAfee habilitado	0
Versión de McAfee Engine	
Versión DAT de McAfee	default-5688

Nivel de detalle de WBNP	2
Versión del motor WBRS	freebsd6-i386-300036
Versiones de componentes WBRS	category=v2-1337979188,ip=default-1379460997,palabra clave=v2-1312487822,prefixcat=v2-137946067,rule=default-1358979215
Umbral de lista de bloqueo WBRS	-6
Umbral de lista de permitidos WBRS	6
WBRS habilitado	1
Movilidad segura habilitada	0
Monitor de tráfico L4 habilitado	0
Versión de la lista de bloqueo del monitor de tráfico L4	default-0
Lista de bloqueo del administrador del monitor de tráfico L4	
Puertos de lista de bloqueo del administrador del monitor de tráfico L4	
Lista permitida del monitor de tráfico L4	
Puertos de lista permitida del monitor de tráfico L4	
factor de muestreo SBNP	0.25
Factor de muestreo SBNP (volumen)	0,1
Versión de SurfControl SDK (heredada)	default-0
Versión de base de datos completa de SurfControl (heredada)	default-0
Versión del archivo de acumulación incremental local SurfControl (heredado)	default-0
Versión de Firestone Engine	default-210016
Versión DAT de Firestone	v2-310003
Versión del motor AVC	default-110076
versión AVC DAT	default-1377556980
Versión del motor Sophos	default-1310963572
Versión DAT de Sophos	default-0
Exploración adaptativa activada	0
Umbral de puntuación de riesgo de escaneo adaptable	[10, 6, 3]
Umbral del factor de carga de escaneo adaptable	[5, 3, 2]
habilitado para SOCKS	0
Transacciones totales	
Transacciones totales	
Total de transacciones permitidas	
Total de transacciones detectadas de malware	
Total de transacciones bloqueadas por la política de administración	
Total de transacciones bloqueadas por puntuación WBRS	
Transacciones de alto riesgo totales	
Total de transacciones detectadas por el monitor de tráfico	
Transacciones totales con clientes IPv6	
Transacciones totales con servidores IPv6	

Total de transacciones mediante proxy SOCKS	
Total de transacciones de usuarios remotos	
Total de transacciones de usuarios locales	
Total de transacciones permitidas mediante proxy SOCKS	
Total de transacciones de usuarios locales permitidas mediante proxy SOCKS	
Total de transacciones de usuarios remotos permitidas mediante proxy SOCKS	
Total de transacciones bloqueadas mediante proxy SOCKS	
Total de transacciones de usuarios locales bloqueados mediante proxy SOCKS	
Total de transacciones de usuarios remotos bloqueados mediante proxy SOCKS	
Segundos desde el último reinicio	2843349
Utilización de CPU (%)	9.9
Utilización de RAM (%)	55.6
Utilización del disco duro (%)	57.5
Utilización del ancho de banda (por segundo)	15307
Conexiones TCP abiertas	2721
Transacciones por segundo	264
Latencia del cliente	163
Tasa de aciertos de caché	21
Utilización de CPU de proxy	17
Utilización de CPU WUC de WBRS	2.5
Utilización de CPU de registro	3,4
Utilización de CPU de informes	3,9
Utilización de CPU de Webroot	0
Utilización de CPU de Sophos	0
Utilización de CPU de McAfee	0
salida de la utilidad vmstat (vmstat -z, vmstat -m)	
Número de políticas de acceso configuradas	32
Número de categorías web personalizadas configuradas	32
Proveedor de autenticación	básico, NTLMSSP
Rangos de autenticación	Nombre de host del proveedor de autenticación, protocolo y otros elementos de configuración

Estadísticas compartidas por solicitud web

Ítem	Datos de muestra	Participación estándar	Participación limitada
Versión	coeus 7.7.0-608		
Serial Number			
Factor de muestreo SBNP (volumen)			
Factor de muestreo SBNP (velocidad)	1		
IP y puerto de destino		segmentos de trayecto de URL sin confusión	segmentos de trayec URL hash

Categoría de malware seleccionada por Anti-Spyware	Omitido
Puntuación de WBRS	4.7
veredicto de categoría de malware de McAfee	
URL de referencia	
segmentos de trayecto de URL sin confusión	segmentos de trayec URL hash
ID de tipo de contenido	
Etiqueta de decisión ACL	0
Categorización web antigua	
Categoría web de CIWUC y fuente de decisión	{'src': 'req', 'cat': '1026'}
Nombre de aplicación AVC	Anuncios y seguimiento
Tipo de aplicación AVC	Redes de anuncios
Comportamiento de la aplicación AVC	No Seguros
Seguimiento de resultados de AVC interno	[0,1,1,1]
Seguimiento de agentes de usuario a través de una estructura de datos indexada	3

Estadísticas avanzadas de malware por solicitud web

Estadísticas de AMP

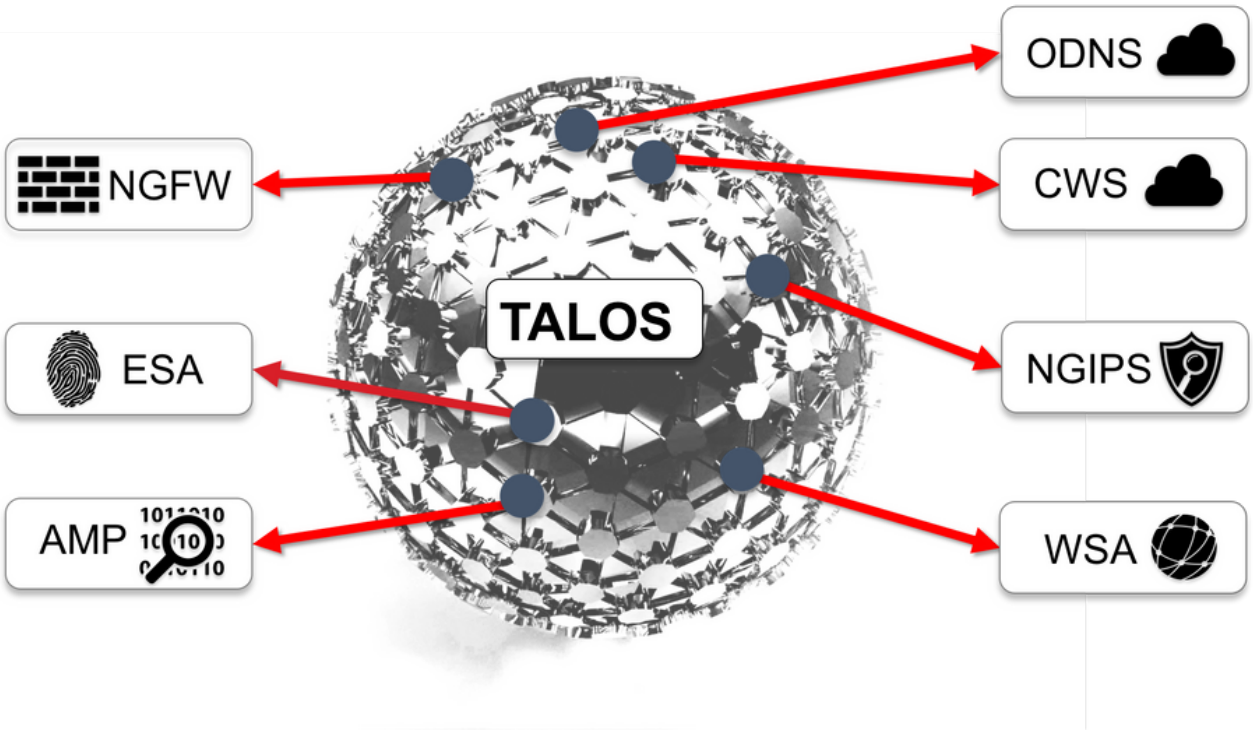
Veredicto: de la consulta de reputación de AMP	malintencionado/limpio/desconocido
Nombre de espía: nombre del malware detectado	[Prueba de troyano]
Puntuación: puntuación de reputación asignada por AMP	[1-100]
Carga: nube de AMP indicada para cargar el archivo	1
Nombre de archivo: nombre del archivo adjunto	abcd.pdf

Fuente de estadísticas de comentarios del usuario final

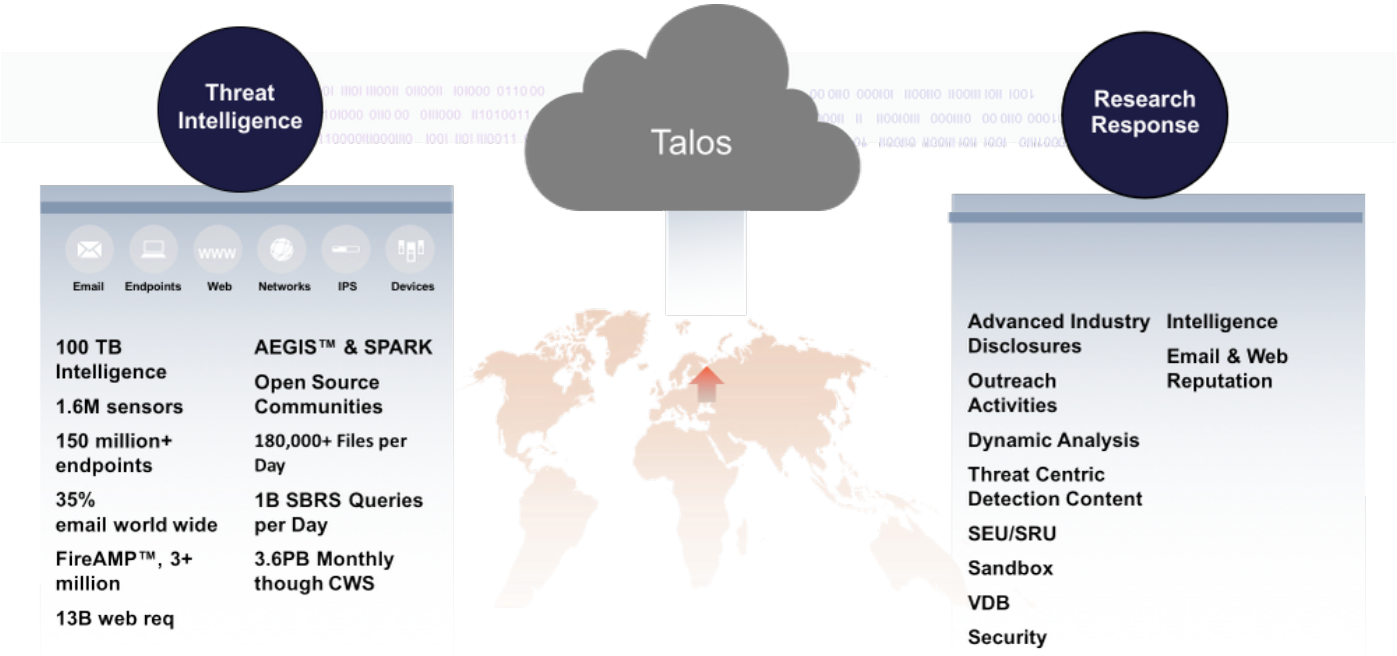
Estadísticas compartidas por usuario final Clasificación errónea Comentarios

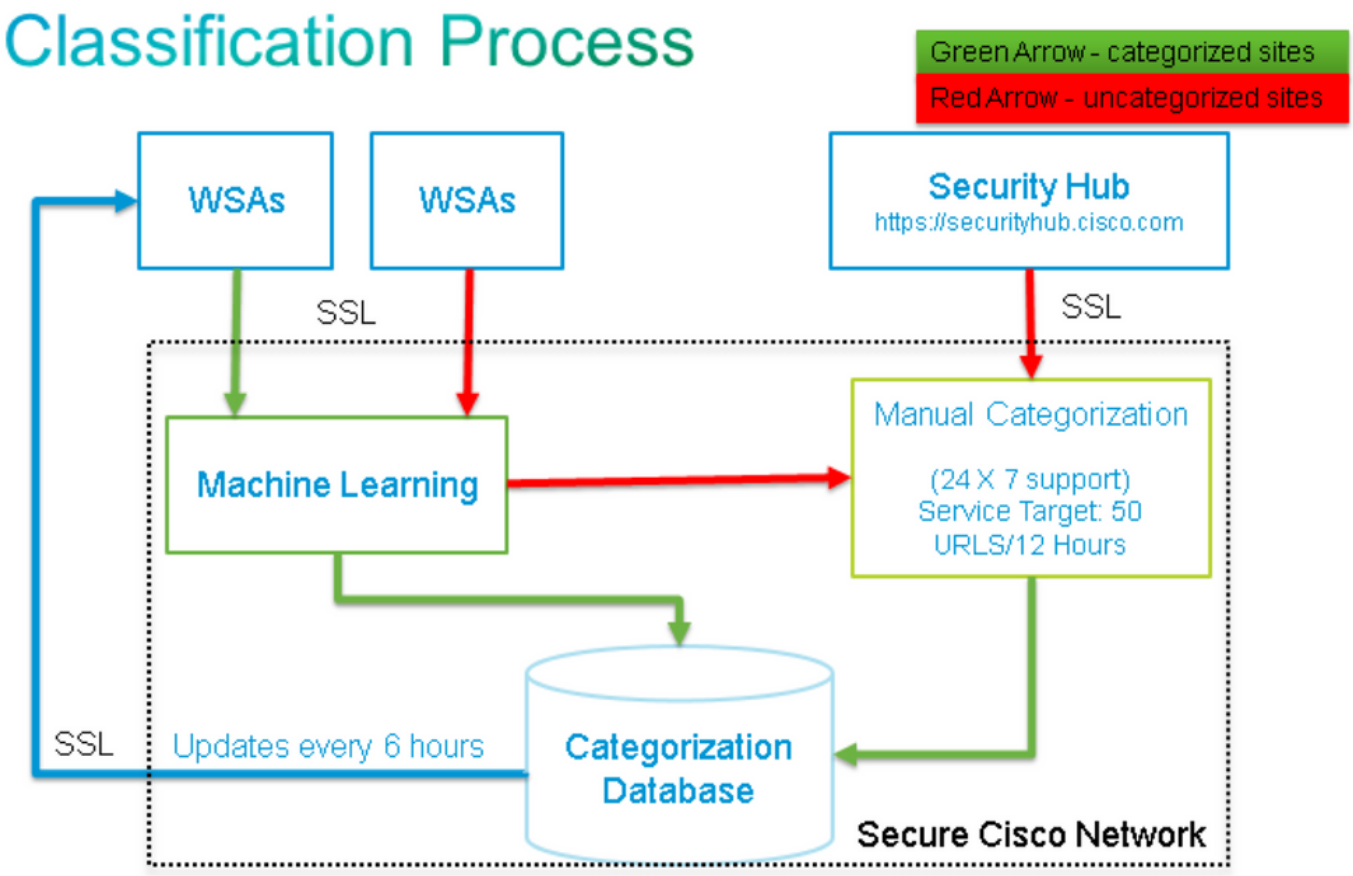
Ítem	Datos de muestra
ID del motor (numérico)	0
Código de categorización web heredada	
Origen de clasificación web de CIWUC	"resp"/"req"
Categoría web de CIWUC	1026

Contenido de detección de Talos



Centrado en las amenazas





Información Relacionada

- Cisco Web Security Appliance - Página de producto
- Página de producto de Cisco Email Security Appliance
- Soporte Técnico y Documentación - Cisco Systems