Participação de rede de base da Web (WBNP) e Participação de rede de base de remetente (SBNP)

Contents

Introduction

Os produtos Cisco Web e Email Content Security podem fornecer dados de telemetria à Cisco e à Talos para aumentar a eficácia da categorização da Web no Web Security Appliance (WSA) e conectar a reputação de IP para o Email Security Appliance (ESA).

Os dados de telemetria são fornecidos para o WSA e o ESA numa base de "opt-in".

Os dados são transmitidos através de pacotes criptografados SSL codificados binários. Os anexos fornecidos abaixo fornecerão informações sobre os dados, formatação específica e descrições dos dados que estão sendo transmitidos. Os dados de participação de rede WebBase (WBNP) e de participação de rede SenderBase (SBNP) não podem ser visualizados em um log direto ou formato de arquivo. Esses dados são transmitidos em forma criptografada. Em momento algum estes dados estão "em repouso".

WSA - Participação de rede WebBase

A Cisco reconhece a importância de manter sua privacidade e não coleta ou usa informações pessoais ou confidenciais, como nomes de usuário e senhas. Além disso, os nomes de arquivos e os atributos de URL que seguem o nome do host são obscurecidos para garantir a confidencialidade.

Quando se trata de transações HTTPS descriptografadas, a Rede SensorBase recebe somente o endereço IP, a pontuação de reputação da Web e a categoria de URL do nome do servidor no certificado.

Para obter informações completas, consulte o Guia do usuário do WSA para obter a versão do AsyncOS para Web Security em execução no momento em seu dispositivo. Consulte "A rede Cisco SensorBase" no Guia do usuário.

ESA - Participação de rede SenderBase

Os clientes que participam da rede SenderBase permitem que a Cisco colete estatísticas agregadas de tráfego de e-mail sobre sua organização, aumentando a utilidade do serviço para todos que o utilizam. A participação é voluntária. A Cisco coleta somente dados resumidos sobre atributos de mensagens e informações sobre como diferentes tipos de mensagens foram tratadas pelos dispositivos da Cisco. Por exemplo, a Cisco não coleta o corpo da mensagem ou o assunto da mensagem. As informações e informações pessoais que identificam sua empresa são mantidas confidenciais.

Para obter informações completas, pAnalise a EGuia do usuário SA para a versão do AsyncOS para ESA Security atualmente em execução em seu dispositivo. Consulte o capítulo "Participação de rede SenderBase" no Guia do usuário.

Perguntas frequentes sobre preocupações gerais de segurança

Pergunta:	Onde os dados coletados são armazenados?
Resposta:	A telemetria do dispositivo é armazenada em data centers com base nos EUA da Cisco.
Pergunta:	Quem tem acesso aos dados coletados e armazenados?
Resposta:	O acesso é limitado ao pessoal do Cisco SBG que analisa/usa os dados para criar inteligência acionável.
Pergunta:	Qual é o tempo de retenção dos dados coletados?
Resposta:	Não há política de retenção/expiração de dados com relação à telemetria do dispositivo. Os da podem ser mantidos indefinidamente ou podem ser apagados por várias razões, incluindo, ent outras, a desamostragem/agregação, a gestão do armazenamento, a idade, a relevância para ameaças atuais/futuras, etc.
Pergunta:	O(s) número(s) de série do cliente ou o(s) endereço(s) IP público(ais) estão armazenados no b de dados de categorização do Talos?
Resposta:	Não, apenas URL e categorias são retidas. O pacote WBNP não contém informações de IP de origem.

Operação

Abaixo está a operação detalhada, o tipo de dados (por descrição) e um exemplo de dados para demonstrar as informações que seriam transmitidas:

- SBNP - Tipos de dados específicos (campos) e dados de exemplo relacionados ao Email Security
- WBNP - Tipos de dados específicos (campos) e dados de exemplo relacionados ao Web Security
- Operação de detecção de ameaças - visão geral da detecção de ameaças do ponto de vista operacional

Participação de rede SenderBase (E-mail)

Estatísticas compartilhadas por e-maildispositivo

Item	Exemplo de dados
Identificador MGA	MGA 10012
Timestamp	Dados das 8h às 8h05 em 1º de julho de 2005
Números de versão de software	MGA versão 4.7.0
Números de versão do conjunto de regras	Conjunto de regras antisspam 102
Intervalo de atualização de antivírus	Atualizações a cada 10 minutos
Tamanho da quarentena	500 MB
Contagem de Mensagens de Quarentena	50 mensagens atualmente em quarentena
Limite de pontuação de vírus	Enviar mensagens para quarentena no nível de ameaça 3 ou superior
Soma de pontuações de vírus para mensagens que entram em quarentena	120
Contagem de mensagens entrando em quarentena	30 (pontuação média de 4)
Tempo máximo de quarentena	12 horas
Contagem de mensagens de quarentena detectadas pela razão de terem entrado e saído da quarentena correlacionada com o resultado do antivírus	50 entrando em quarentena devido à regra .ex saindo da quarentena devido à versão manual todos os 30 eram positivos para vírus
Contagem de mensagens de quarentena detectadas pela ação tomada ao sair da quarentena	10 mensagens tinham anexos removidos após da quarentena
Soma das mensagens mantidas em quarentena	20 horas

Estatísticas compartilhadas por endereço IP

Item	Exemplo de dados	Participação padrão	Participação limitada
Contagem de mensagens em vários estágios no dispositivo	Visto pelo mecanismo antivírus: 100 Visto pelo mecanismo antisspam: 80		
Soma de pontuações e vereditos de antivírus e antisspam	2.000 (soma das pontuações antisspam para todas as mensagens vistas)		
Número de mensagens atingindo diferentes combinações de regras de antivírus e antisspam	100 mensagens atingem as regras A e B Apenas 50 mensagens atingem a regra A		
Número de conexões	20 conexões SMTP		
Número total de destinatários inválidos	50 destinatários no total 10 destinatários inválidos		

Nome(s) de arquivo com hash: (a)	Um arquivo <one-way-hash>.pif foi encontrado dentro de um anexo de arquivo chamado <one-way-hash>.zip.	Nome de arquivo não encontrado	Nome do arq com hash
Nome(s) de arquivo ofuscado(s): (b)	Um arquivo aaaaaaa0.aaa.pif foi encontrado dentro de um arquivo aaaaaaa.zip.	Nome de arquivo não encontrado	Nome de arq obscuro
Nome de host do URL (c)	Foi encontrado um link em uma mensagem para www.domain.com	Nome de host de URL não abreviado	Nome de ho URL obsolet
Caminho de URL obscuro (d)	Foi encontrado um link dentro de uma mensagem para o nome de host www.domain.com, e tinha o caminho aaa000aa/aa00aaa.	Caminho de URL não ofuscado	Caminho de obscuro
Número de mensagens por resultados de verificação de spam e vírus	10 spam positivo 10 spam negativo 5 Suspeito de spam 4 vírus positivos 16 vírus negativos 5 vírus não verificável		
Número de mensagens de diferentes vereditos de antivírus e antisspam	500 spam, 300 ham		
Contagem de mensagens em intervalos de tamanho	Intervalo de 30.000 a 35.000		
Contagem de diferentes tipos de extensão	300 anexos ".exe"		
Correlação de tipos de anexo, tipo de arquivo verdadeiro e tipo de contêiner	100 anexos que têm uma extensão ".doc", mas que na verdade são ".exe" 50 anexos são extensões ".exe" em um zip		
Correlação entre extensão e tipo de arquivo verdadeiro e tamanho do anexo	30 anexos eram ".exe" no intervalo de 50 a 55K		
Número de mensagens pelos resultados da amostragem estocástica	14 mensagens ignoradas 25 mensagens na fila para amostragem 50 mensagens digitalizadas por amostragem		
Número de mensagens que falharam na verificação de DMARC	34 mensagens falharam na verificação de DMARC		

Notas:

(a) Os nomes de arquivos serão codificados em um hash de 1 via (MD5).

(b) Os nomes de arquivos serão enviados em forma ofuscada, com todas as letras minúsculas ASCII ([a-z]) substituídas por "a", todas as letras maiúsculas ASCII ([A-Z]) substituídas por "A", todos os caracteres UTF-8 multibytes substituídos por "x" (para fornecer privacidade para outros conjuntos de caracteres), todos os dígitos ASCII ([0-9]) substituídos.

(c) Os nomes de host de URL apontam para um servidor Web que fornece conteúdo, da mesma forma que um endereço IP. Não há informações confidenciais, como nomes de usuário e senhas.

d) As informações de URL que seguem o nome do host são obscurecidas para garantir que nenhuma informação pessoal do usuário seja revelada.

Estatísticas compartilhadas por cliente SDS

Item	Exemplo de dados
TimeStamp	
Versão do cliente	
Número de solicitações feitas ao cliente	
Número de solicitações feitas do cliente SDS	
Resultados de tempo para pesquisas de DNS	
Resultados do tempo de resposta do servidor	
Tempo para estabelecer conexão com o servidor	
Número de conexões estabelecidas	
Número de conexões abertas simultâneas com o servidor	
Número de solicitações de serviço ao WBRS	
Número de solicitações que atingem o cache WBRS local	
Tamanho do cache WBRS local	
Resultados do tempo de resposta do WBRS remoto	

Dados de telemetria do AMP SBNP

Formato	Exemplo de dados
amp_verdicts' : { ("veredit", "spyware name", "score", "uploaded", "file_name"), ("veredito", "spyware name", "score", "uploaded", "file_name"), ("veredito", "spyware name", "score", "uploaded", "file_name"), ... ("veredito", "spyware name", "score", "uploaded", "file_name"), }	
Descrição	
Veredito - da consulta de reputação da AMP	mal-intencionado/limpo/desconhecido
Spyname - Nome do malware detectado	[Teste de troia]
Pontuação - Pontuação de reputação atribuída à AMP	[1-100]
Upload - A nuvem da AMP indicou para carregar o arquivo	1
Nome do arquivo - Nome do arquivo anexo	abcd.pdf

Participação de rede WebBase (Web)

Estatísticas compartilhadas por solicitação da Web

Item	Exemplo de dados	Participação padrão	Participação limitada
Versão	código 7.7.0-608		

Serial Number			
Fator de amostragem SBNP (Volume)			
Fator de amostragem SBNP (Taxa)	1		
IP de destino e porta		segmentos de caminho de URL não ofuscados	segmentos de camin de URL com hash
Categoria de malware escolhida pelo antisspyware	Ignorado		
Pontuação WBRS	4.7		
Veredito da categoria de malware da McAfee			
URL de referência		segmentos de caminho de URL não ofuscados	segmentos de camin de URL com hash
ID do tipo de conteúdo			
Etiqueta de decisão ACL	0		
Categorização da Web antiga			
Categoria da Web do CIWUC e fonte de decisão	{'src': 'req', 'cat': '1026'}		
Nome do aplicativo AVC	Anúncios e rastreamento		
Tipo de aplicativo AVC	Redes de anúncios		
Comportamento do aplicativo AVC	Não seguro		
Rastreamento interno de resultados de AVC	[0,1,1,1]		
Rastreamento de agente de usuário via estrutura de dados indexada	3		

Estatísticas avançadas de malware por solicitação da Web

Estatísticas da AMP

Veredito - da consulta de reputação da AMP	mal-intencionado/limpo/desconhecido
Spyname - Nome do malware detectado	[Teste de troia]
Pontuação - Pontuação de reputação atribuída à AMP	[1-100]
Upload - A nuvem da AMP indicou para carregar o arquivo	1
Nome do arquivo - Nome do arquivo anexo	abcd.pdf

Feed de estatísticas de feedback do usuário final

Estatísticas compartilhadas por usuário final
Descategorização Feedback

Item	Exemplo de dados
ID do motor (numérico)	0
Código de categorização da Web legada	
Fonte de categorização da Web CIWUC	"resp" / "req"
Categoria da Web do CIWUC	1026

Exemplo de dados fornecidos - Participação-padrão

```
# categorized
"http://google.com/": {    "wbrs": "5.8",
```

```
   "fs": {
         "src": "req",
         "cat": "1020"
   },
}

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

Exemplo de dados fornecidos - Participação limitada

- Solicitação original do cliente: www.gunexams.com/Non-Restricted-FREE-Practice-Exams
- Mensagem registrada (no servidor de telemetria): http://www.gunexams.com/76bd845388e0

Decodificação WBNP Completa

Estatísticas compartilhadas por aplicativo da Cisco

Item	Exemplo de dados
Versão	código 7.7.0-608
Serial Number	0022190B6ED5-XYZ1YZ2
Modelo	S660
Webroot habilitado	1
AVC habilitado	1
Sophos habilitado	0
Categorização do lado da resposta habilitada	1
Mecanismo antispyware ativado	padrão-2001005008
Versão do Anti-Spyware SSE	padrão-2001005008
Versão de definições de spyware antisspyware	padrão-8640
Versão do DAT da lista de bloqueio de URLs antisspyware	
Versão do DAT de phishing de URL antisspyware	
Versão DAT de cookies antisspyware	
Bloqueio de domínio antisspyware ativado	0
Limite de risco de ameaça antisspyware	90
McAfee habilitado	0
Versão do McAfee Engine	
Versão do McAfee DAT	default-5688
Nível de detalhes do WBNP	2
versão do mecanismo WBRS	freebsd6-i386-300036
versões de componentes WBRS	categorias=v2-1337979188,ip=default-1379460997,palavra-chave=v2-1312487822,prefixcat=v2-1379460670,rule=default-1358979215
Limite da lista de bloqueio do WBRS	-6
Limite de lista de permissão WBRS	6
WBRS ativado	1
Mobilidade segura habilitada	0
L4 Traffic Monitor ativado	0

Versão da lista de bloqueio do L4 Traffic Monitor	default-0
Lista de bloqueio do administrador do L4 Traffic Monitor	
Portas da lista de bloqueio do administrador do L4 Traffic Monitor	
Lista de permissão do L4 Traffic Monitor	
Portas da lista de permissão do L4 Traffic Monitor	
Fator de amostragem SBNP	0.25
Fator de amostragem SBNP (Volume)	0,1
Versão do SurfControl SDK (legado)	default-0
Versão completa do banco de dados do SurfControl (legado)	default-0
Versão do arquivo de acumulação incremental local do SurfControl (legado)	default-0
versão do Firestone Engine	default-210016
versão do Firestone DAT	v2-310003
versão do AVC Engine	default-110076
versão AVC DAT	padrão-1377556980
Versão do mecanismo Sophos	padrão-1310963572
versão de DAT do Sophos	default-0
Varredura adaptável habilitada	0
Limite de pontuação de risco de varredura adaptável	[10, 6, 3]
Limite do fator de carga da varredura adaptável	[5, 3, 2]
SOCKS ativados	0
Total de transações	
Total de transações	
Total de transações permitidas	
Total de transações detectadas por malware	
Total de transações bloqueadas pela política de administração	
Total de transações bloqueadas pela pontuação do WBRS	
Total de transações de alto risco	
Total de transações detectadas pelo monitor de tráfego	
Total de transações com clientes IPv6	
Total de transações com servidores IPv6	
Total de transações usando proxy SOCKS	
Total de transações de usuários remotos	
Total de transações de usuários locais	
Total de transações permitidas usando proxy SOCKS	
Total de transações de usuários locais permitidas usando proxy SOCKS	
Total de transações de usuários remotos permitidas usando proxy SOCKS	
Total de transações bloqueadas usando proxy SOCKS	
Total de transações de usuários locais	

bloqueadas usando proxy SOCKS	
Total de transações de usuários remotos bloqueadas usando proxy SOCKS	
Segundos desde a última reinicialização	2843349
Utilização da CPU (%)	9.9
Utilização de RAM (%)	55.6
Utilização de disco rígido (%)	57.5
Utilização de largura de banda (s/s)	15307
Conexões TCP abertas	2721
Transações por segundo	264
Latência do cliente	163
Taxa de acertos de cache	21
Utilização de CPU de proxy	17
Utilização da CPU WUC WBRS	2.5
Registro da utilização da CPU	3.4
Geração de relatórios de utilização da CPU	3,9
Utilização de CPU Webroot	0
Utilização da CPU do Sophos	0
Utilização de CPU McAfee	0
saída do utilitário vmstat (vmstat -z, vmstat -m)	
Número de políticas de acesso configuradas	32
Número de categorias da Web personalizadas configuradas	32
Provedor de autenticação	Básico, NTLMSSP
Domínios de autenticação	Nome de host, protocolo e outros elementos de configuração do provedor de autenticação

Estatísticas compartilhadas por solicitação da Web

Item	Exemplo de dados	Participação padrão	Participação limitada
Versão	código 7.7.0-608		
Serial Number			
Fator de amostragem SBNP (Volume)			
Fator de amostragem SBNP (Taxa)	1		
IP de destino e porta		segmentos de caminho de URL não ofuscados	segmentos de camin de URL com hash
Categoria de malware escolhida pelo antisspyware	Ignorado		
Pontuação WBRS	4.7		
Veredito da categoria de malware da McAfee			
URL de referência		segmentos de caminho de URL não ofuscados	segmentos de camin de URL com hash
ID do tipo de conteúdo			
Etiqueta de decisão ACL	0		
Categorização da Web antiga			
Categoria da Web do CIWUC e fonte de decisão	{'src': 'req', 'cat': '1026'}		
Nome do aplicativo AVC	Anúncios e		

	rastreamento
Tipo de aplicativo AVC	Redes de anúncios
Comportamento do aplicativo AVC	Não seguro
Rastreamento interno de resultados de AVC	[0,1,1,1]
Rastreamento de agente de usuário via estrutura de dados indexada	3

Estatísticas avançadas de malware por solicitação da Web

Estatísticas da AMP

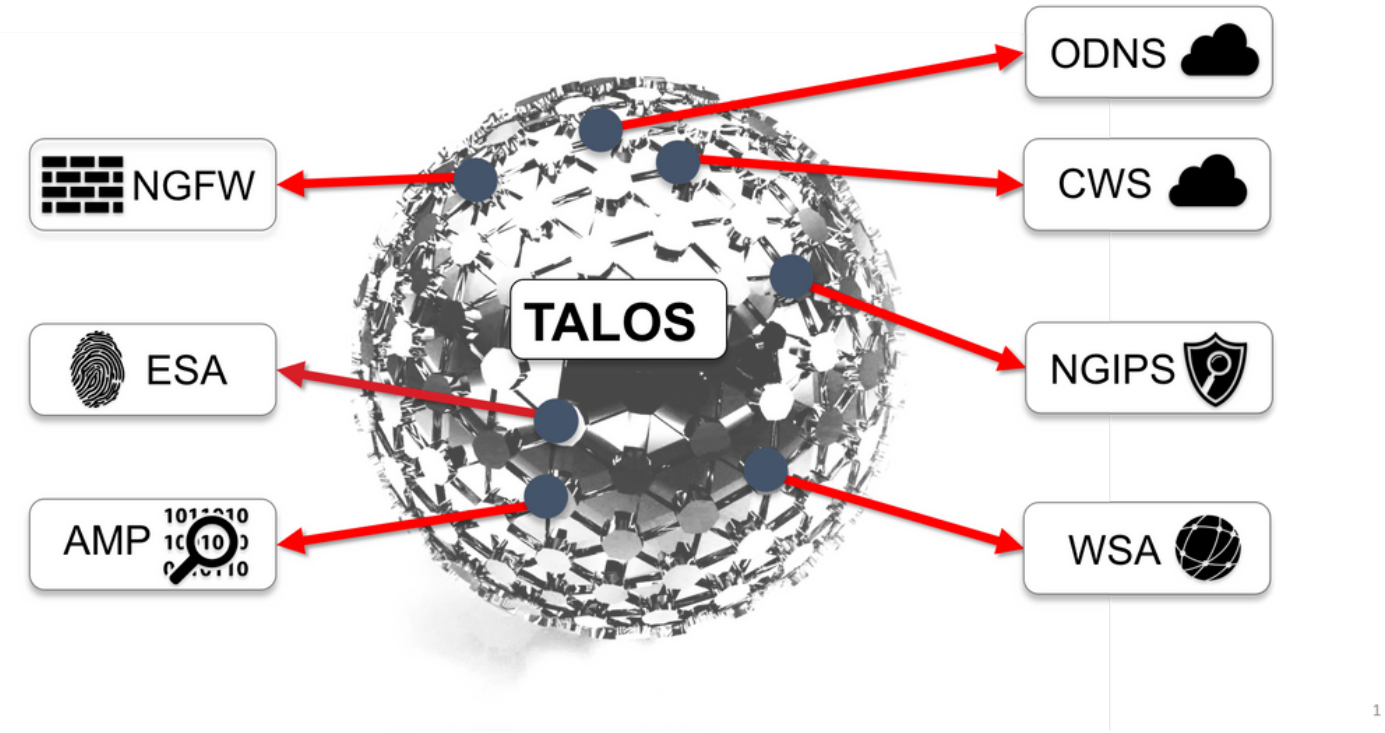
Veredito - da consulta de reputação da AMP	mal-intencionado/limpo/desconhecido
Spyname - Nome do malware detectado	[Teste de troia]
Pontuação - Pontuação de reputação atribuída à AMP	[1-100]
Upload - A nuvem da AMP indicou para carregar o arquivo	1
Nome do arquivo - Nome do arquivo anexo	abcd.pdf

Feed de estatísticas de feedback do usuário final

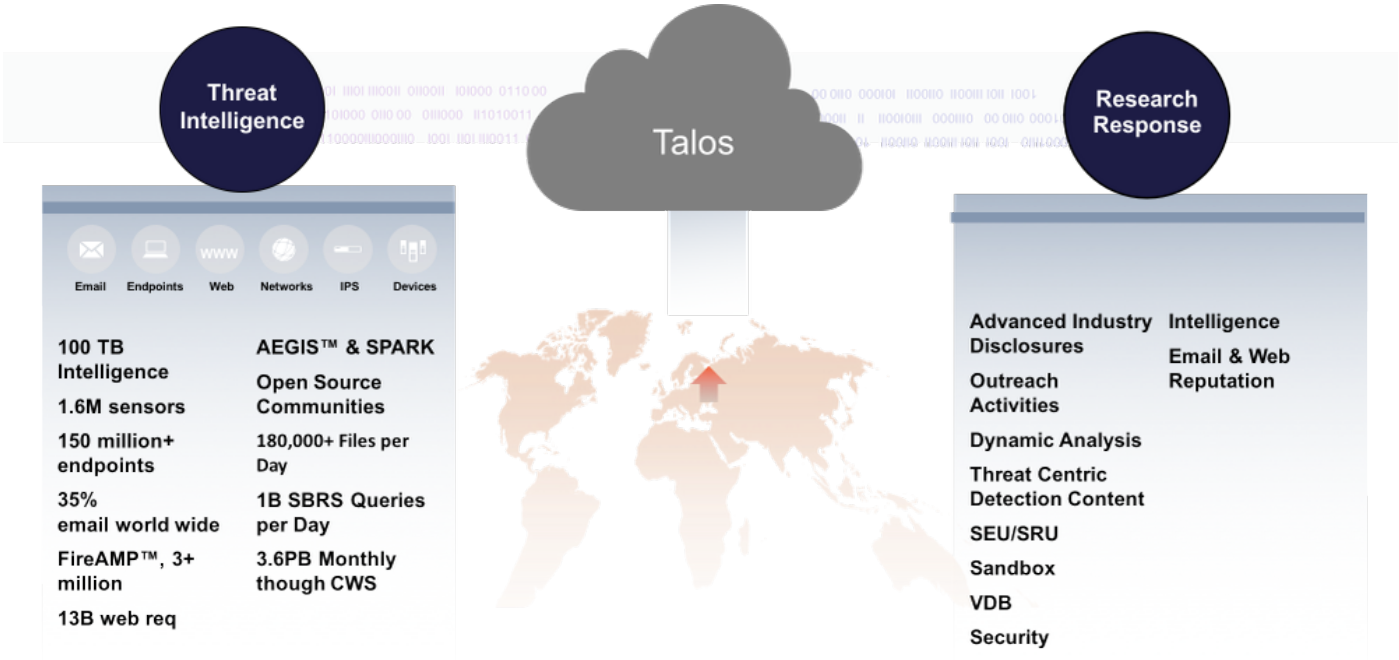
Estatísticas compartilhadas por usuário final
Descategorização Feedback

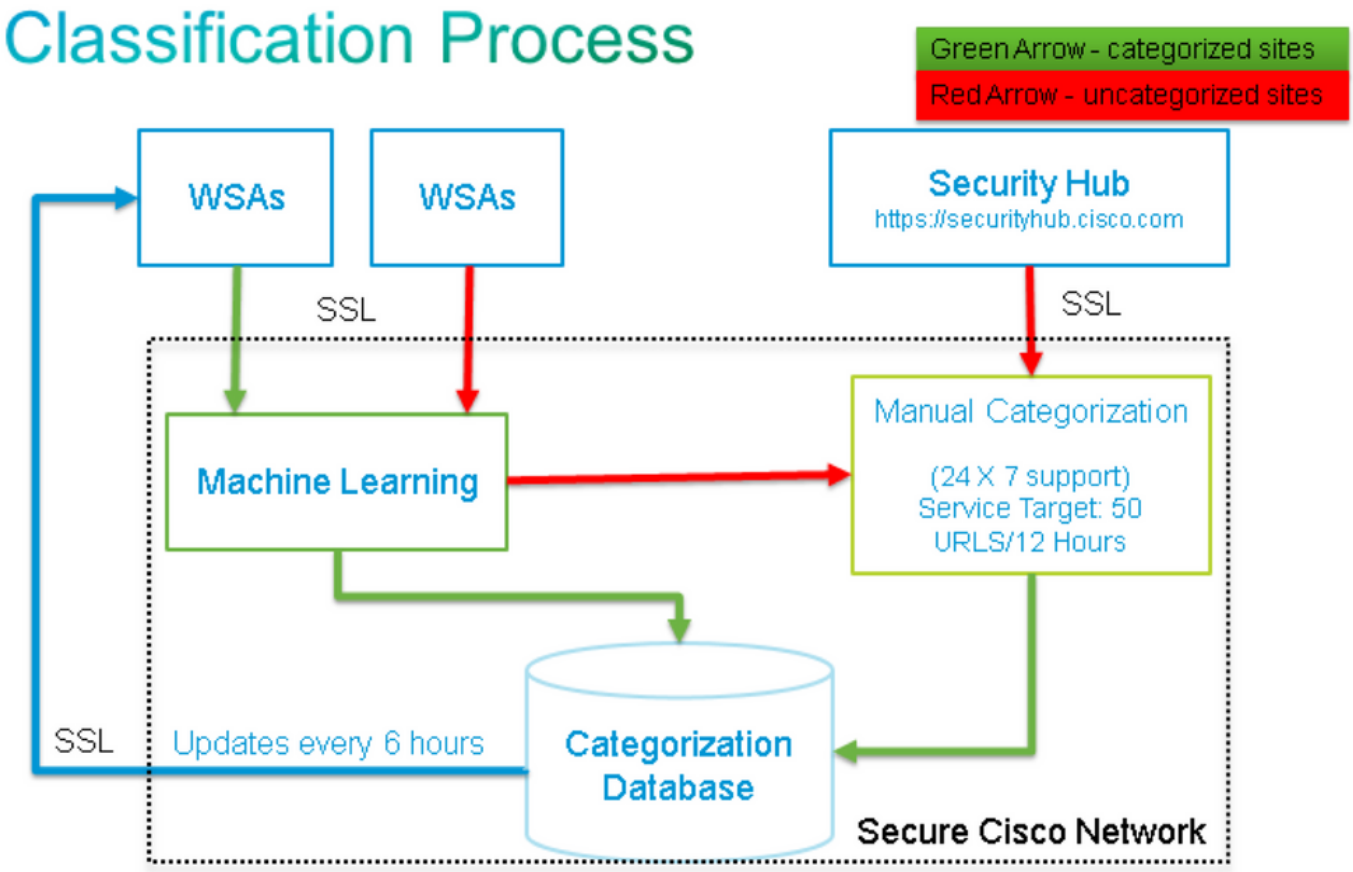
Item	Exemplo de dados
ID do motor (numérico)	0
Código de categorização da Web legada	
Fonte de categorização da Web CIWUC	"resp" / "req"
Categoria da Web do CIWUC	1026

Conteúdo de detecção de Talos



Focado na ameaça





Informações Relacionadas

- [Cisco Web Security Appliance - Página de produto]
- [Cisco Email Security Appliance - Página de produto]
- [Suporte Técnico e Documentação - Cisco Systems]