Web Base Network Participation(WBNP)およびSender Base Network Participation(SBNP)

内容

概要

Cisco WebおよびEメールコンテンツセキュリティ製品は、Webセキュリティアプライアンス(WSA)でのWeb分類とEメールセキュリティアプライアンス(ESA)のIPレピュテーションの接続の有効性を高めるために、CiscoおよびTalosにテレメトリデータを提供できます。

テレメトリデータは、WSAとESAに「オプトイン」ベースで提供されます。

データは、バイナリエンコードされたSSL暗号化パケットを介して送信されます。 次に示す添付ファイルは、送信されるデータに関するデータ、特定のフォーマット、および説明を示します。 WebBase Network Participation(WBNP)およびSenderBase Network Participation(SBNP)データは、直接ログまたはファイル形式では表示できません。 このデータは暗号化された形式で送信されます。 このデータは「保管中」ではありません。

WSA:WebBase Network Participation

シスコは、お客様のプライバシーを維持することの重要性を認識し、ユーザ名やパスフレーズなどの個人情報や機密情報を収集または使用しません。また、ホスト名に続くファイル名とURL属性は、機密性を確保するために難読化されます。

復号化されたHTTPSトランザクションに関しては、SensorBase Networkは、証明書内のサーバ名のIPアドレス、Webレピュテーションスコア、およびURLカテゴリのみを受信します。

詳細については、アプライアンスで現在実行されているAsyncOS for Web Securityのバージョンに関する『WSAユーザガイド』を参照してください。『ユーザガイド』の「Cisco SensorBaseネットワーク」を参照してください。

ESA:SenderBaseネットワークへの参加

SenderBaseネットワークに参加しているお客様は、シスコが組織に関する集約された電子メールトラフィック統計情報を収集できるため、サービスを使用するすべてのユーザに対してサービスの有用性が高まります。参加は任意です。シスコは、メッセージ属性の要約データと、さまざまなタイプのメッセージがシスコアプライアンスでどのように処理されたかに関する情報のみを収集します。たとえば、シスコはメッセージ本文やメッセージの件名を収集しません。個人を特定できる情報や組織を特定する情報は、機密情報として保護されます。

詳細については、 pEをリースレビューするSAユーザガイド を参照してください。『ユーザガイド』の「SenderBaseネットワークへの参加」の章を参照してください。

一般的なセキュリティの問題に関するFAQ

質問： 収集されたデータはどこに保存されますか。
解答： アプライアンステレメトリは、Cisco USベースのデータセンターに保存されます。
質問： 収集および保存されたデータへのアクセス権を持つユーザー
解答： アクセスは、データを分析/使用して実用的なインテリジェンスを作成するCisco SBG担当者に限れます。
質問： 収集されたデータの保持時間はどのくらいですか。
解答： アプライアンステレメトリに関するデータ保持/有効期限ポリシーはありません。データは無期限
質問： お客様のシリアル番号またはパブリックIPアドレスはTalos分類データベースに保存されていま
解答： いいえ。URLとカテゴリのみが保持されます。WBNPパケットには、送信元IP情報が含まれてい

稼動

次に、操作の詳細、データの種類（説明別）、および送信される情報を示すサンプルデータを示します。

- SBNP：電子メールセキュリティに関連する特定のデータ型（フィールド）およびサンプルデータ
- WBNP:Webセキュリティに関連する特定のデータ型（フィールド）およびサンプルデータ
- 脅威検出操作 – 運用の観点から見た脅威検出の概要

SenderBase（電子メール）ネットワークへの参加

電子メールごとに共有される統計情報アプライアンス

項目
MGA Identifier
タイムスタンプ
ソフトウェアバージョン番号
ルールセットのバージョン番号
ウイルス対策の更新間隔
検疫サイズ
検疫メッセージ数
ウイルススコアのしきい値
検疫に入るメッセージのウイルススコアの合計
検疫に入るメッセージの数
最大検疫時間
ウイルス対策の結果と関連付けられた、検疫に入った理由と検疫から切り離されたアウトブレイク検疫メ
隔離時に実行されたアクションによって分類されたアウトブレイク隔離メッセージの数
メッセージが検疫で保持された合計時間

IPアドレスごとに共有される統計情報

項目	サンプルデータ	標準参加	参加制限
アプライアンス内のさまざまな段階でのメッセージ数	アンチウイルスエンジンで確認：100 アンチスパムエンジンで確認：80		
アンチスパムおよびアンチウイルスのスコアと判定の合計	2,000 (すべてのメッセージのアンチスパムスコアの合計)		
さまざまなスパム対策ルールとウイルス対策ルールの組み合わせにヒットするメッセージの数	ルールAおよびBに100件のメッセージがヒット 50メッセージがルールAのみにヒット		
接続数	20 SMTP接続		
受信者の総数と無効な受信者の数	合計受信者50人 10人の無効な受信者		
ハッシュされたファイル名：(a)	<one-way-hash>.pifファイルが<one-way-hash>.zipという名前のアーカイブ添付ファイルの中で見つかりました。	難読化されていないファイル名	ハッシュされファイル名
難読化されたファイル名：(b)	aaaaaa0.aaa.pifファイルがaaaaaaa.zipファイル内で見つかりました。	難読化されていないファイル名	難読化されファイル名
URLホスト名(c)	www.domain.comへのメッセージ内にリンクが見つかりました	難読化されていないURLホスト名	難読化されURLホスト名
難読化されたURLパス(d)	ホスト名www.domain.comへのメッセージ内にリンクが見つかり、パスがaaa000aa/aa00aaaでした。	難読化されていないURLパス	難読化されURLパス
スパムおよびウイルススキャン結果によるメッセージ数	10スパム検出 10スパムネガ 5スパム容疑者 4ウイルス陽性 16ウイルス陰性 5ウイルススキャン不可		
さまざまなアンチスパムおよびアンチウイルスの判定によるメッセージの数	500スパム、300ハム		
サイズ範囲のメッセージ数	30 K ~ 35 Kの範囲で125		
さまざまな拡張タイプの数	300 ".exe"添付		

添付ファイルの種類、実際のファイルの種類、およびコンテナーの種類の関連付け	拡張子が".doc"で、実際には".exe"である100個の添付ファイル 50個の添付ファイルは、zip内の「.exe」拡張子です
拡張子と添付ファイルのサイズを含む真のファイルの種類の関連付け	30個の添付ファイルが50 ~ 55Kの範囲に含まれています。
確率的サンプリング結果別のメッセージ数	サンプリングをスキップした14メッセージ 25メッセージがサンプリングのためにキューに入れられる サンプリングから50メッセージをスキャン
DMARC検証に失敗したメッセージの数	34件のメッセージがDMARC検証に失敗しました

注：

(a)ファイル名は一方向ハッシュ(MD5)でエンコードされます。

(b)ファイル名は難読化された形式で送信され、小文字のASCII文字([a-z])はすべて「a」、大文字のASCII文字([A-Z])はすべて「A」、複数バイトのUTF-8文字はすべて「x」（他の文字セットのプライバシー提供）、すべてのASCII数字([0-9])に置換)。

(c) URLホスト名は、IPアドレスと同様に、コンテンツを提供するWebサーバを指します。ユーザ名やパスワードなどの機密情報は含まれません。

(d)ホスト名に続くURL情報を難読化し、ユーザの個人情報が公開されないようにする。

SDSクライアントごとに共有される統計情報

項目	サンプルデータ
Timestamp	
クライアントバージョン	
クライアントに対する要求の数	
SDSクライアントから行われた要求の数	
DNSルックアップの時間結果	
サーバ応答時間の結果	
サーバへの接続を確立する時間	
確立された接続数	
サーバーへの同時オープン接続数	
WBRSへのサービスリクエストの数	
ローカルWBRSキャッシュにヒットした要求の数	
ローカルWBRSキャッシュのサイズ	
リモートWBRSによる応答時間	

AMP SBNPテレメトリデータ

書式	サンプルデータ
amp_verdicts':{ ("判定", "spyname", "スコア", "アップロード", "ファイル名"), ("判定", "spyname", "score", "uploaded", "file_name"), ("判定", "spyname", "score", "uploaded", "file_name"), ...	

("判定", "spyname", "score", "uploaded", "file_name") ,
}

説明	
判定 – AMPレピュテーションクエリの	悪意のある/クリーン/不明
Spyname：検出されたマルウェアの名前	[トロイの木馬 – テスト]
スコア – AMPが割り当てたレピュテーションスコア	[1-100]
アップロード：ファイルのアップロードが指示されたAMPクラウド	1
File Name – 添付ファイルの名前	abcd.pdf

WebBase(Web)ネットワークへの参加

Web要求ごとに共有される統計情報

項目	サンプルデータ	標準参加	参加制限
バージョン	coeus 7.7.0-608		
シリアル番号			
SBNPサンプリング係数（ボリューム）			
SBNPサンプリング係数（レート）	1		
宛先IPおよびポート		難読化されていないURLパスセグメント	ハッシュされたURLセグメント
アンチスパイウェア選択マルウェアカテゴリ	スキップ		
WBRSスコア	4.7		
McAfeeマルウェアカテゴリ判定			
参照者URL		難読化されていないURLパスセグメント	ハッシュされたURLセグメント
コンテンツタイプID			
ACL決定タグ	0		
レガシーWebの分類			
CIWUC Webカテゴリと意思決定元	{'src':'req'、'cat':'1026'}		
AVCアプリケーション名	広告とトラッキング		
AVCアプリタイプ	広告ネットワーク		
AVCアプリケーションの動作	安全ではない		
内部AVC結果追跡	[0,1,1,1]		
インデックス付きデータ構造によるユーザエージェントトラッキング	3		

Web要求ごとの高度なマルウェア統計情報

AMP統計情報

判定 – AMPレピュテーションクエリの	悪意のある/クリーン/不明
Spyname：検出されたマルウェアの名前	[トロイの木馬 – テスト]
スコア – AMPが割り当てたレピュテーションスコア	[1-100]
アップロード：ファイルのアップロードが指示されたAMPクラウド	1
File Name – 添付ファイルの名前	abcd.pdf

エンドユーザフィードバック統計情報フィード

エンドユーザごとに共有される統計情報 誤分類 フィードバック

項目	サンプルデータ
エンジンID（数値）	0
レガシーWeb分類コード	
CIWUC Web分類ソース	'resp' / 'req'
CIWUC Webカテゴリ	1026

提供されるデータの例 – 標準参加

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

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

提供されるデータの例 – 参加が限られている

- クライアントからの元の要求：www.gunexams.com/Non-Restricted-FREE-Practice-Exams
- メッセージのログ（テレメトリサーバ内）:http://www.gunexams.com/76bd845388e0

フルWBNPデコード

Ciscoアプライアンスごとに共有される統計情報

項目	サンプルデータ
バージョン	coeus 7.7.0-608
シリアル番号	0022190B6ED5-XYZ1YZ2
モデル	S660
Webroot有効	1
AVC有効	1
Sophos有効	0
応答側の分類が有効	1
アンチスパイウェアエンジンが有効	default-2001005008
アンチスパイウェアSSEバージョン	default-2001005008
Anti-Spyware Spycat Definitionsバージョン	default-8640
アンチスパイウェアURLブロックリストDATバージョン	
アンチスパイウェアURLフィッシングDATバージョン	
アンチスパイウェアCookie DATバージョン	
アンチスパイウェアドメインブロッキングが有効	0
アンチスパイウェアの脅威リスクのしきい値	90
McAfee対応	0

McAfee Engineバージョン	
McAfee DATバージョン	default-5688
WBNP詳細レベル	0
WBRSエンジンバージョン	freebsd6-i386-300036
WBRSコンポーネントバージョン	categories=v2-1337979188,ip=default-1379460997,keyword=v2-1312487822,prefixcat=v2-1379460670,rule=default-1358979215
WBRSブロックリストしきい値	-6
WBRS許可リストしきい値	6
WBRS有効	1
セキュアモビリティ対応	0
L4トラフィックモニタが有効	0
L4トラフィックモニタブロックリストバージョン	default-0
L4トラフィックモニタ管理ブロックリスト	
L4トラフィックモニタ管理ブロックリストポート	
L4トラフィックモニタ許可リスト	
L4トラフィックモニタのAllowlistポート	
SBNPサンプリング因子	0.25
SBNPサンプリング係数（ボリューム）	0.1
SurfControl SDKバージョン（レガシー）	default-0
SurfControlフルデータベースバージョン（レガシー）	default-0
SurfControlローカル増分累積ファイルのバージョン（レガシー）	default-0
Firestoneエンジンバージョン	default-210016
Firestone DATバージョン	v2-310003
AVCエンジンバージョン	default-110076
AVC DATバージョン	default-1377556980
Sophosエンジンバージョン	default-1310963572
Sophos DATバージョン	default-0
適応型スキャンが有効	0
適応型スキャンリスクスコアのしきい値	[10 6 3]
適応型スキャン負荷係数しきい値	[5 3 2]
SOCKS対応	0
トランザクションの合計	
トランザクションの合計	
許可されたトランザクションの合計	
検出されたマルウェアの総トランザクション	
管理ポリシーによってブロックされたトランザクションの合計	
WBRSスコアでブロックされたトランザクションの合計	
リスクの高いトランザクションの合計	
トラフィックモニタによって検出されたトランザクションの合計	
IPv6クライアントとの総トランザクション	
IPv6サーバとの総トランザクション	
SOCKSプロキシを使用したトランザクションの合計	
リモートユーザからのトランザクションの合	

計	
ローカルユーザーからのトランザクションの合計	
SOCKSプロキシを使用して許可されるトランザクションの合計	
SOCKSプロキシを使用して許可されたローカルユーザーからのトランザクションの合計	
SOCKSプロキシを使用して許可されたリモートユーザからのトランザクションの合計	
SOCKSプロキシを使用してブロックされたトランザクションの合計	
SOCKSプロキシを使用してブロックされたローカルユーザーからのトランザクションの合計	
SOCKSプロキシを使用してブロックされたリモートユーザからのトランザクションの合計	
前回の再起動からの秒数	2843349
CPU使用率(%)	9.9
RAM使用率(%)	55.6
ハードディスク使用率(%)	57.5
帯域幅使用率 (/秒)	15307
オープンTCP接続	2721
1秒あたりのトランザクション数	264
クライアント遅延	163
キャッシュヒット率	21
プロキシCPU使用率	17
WBRS WUC CPU使用率	2.5
CPU使用率のロギング	3.4
CPU使用率のレポート	3.9
Webroot CPU使用率	0
Sophos CPU使用率	0
McAfee CPU使用率	0
vmstatユーティリティの出力(vmstat -z、vmstat -m)	
設定されているアクセスポリシーの数	32
設定済みのカスタムWebカテゴリの数	32
認証プロバイダー	基本、NTLMSSP
認証レルム	認証プロバイダーのホスト名、プロトコル、およびその他の構成要素

Web要求ごとに共有される統計情報

項目	サンプルデータ	標準参加	参加制限
バージョン	coeus 7.7.0-608		
シリアル番号			
SBNPサンプリング係数 (ボリューム)			
SBNPサンプリング係数 (レート)	1		
宛先IPおよびポート		難読化されていないURLパスセグメント	ハッシュされたURLセグメント
アンチスパイウェア選択マルウェアカテゴリ	スキップ		

WBRSスコア	4.7
McAfeeマルウェアカテゴリ判定	
参照者URL	難読化されていない　ハッシュされたURL URLパスセグメント　セグメント
コンテンツタイプID	
ACL決定タグ	0
レガシーWebの分類	
CIWUC Webカテゴリと意思決定元	{'src':'req'、 'cat':'1026'}
AVCアプリケーション名	広告とトラッキング
AVCアプリタイプ	広告ネットワーク
AVCアプリケーションの動作	安全ではない
内部AVC結果追跡	[0,1,1,1]
インデックス付きデータ構造によるユーザエージェントトラッキング	3

Web要求ごとの高度なマルウェア統計情報

AMP統計情報

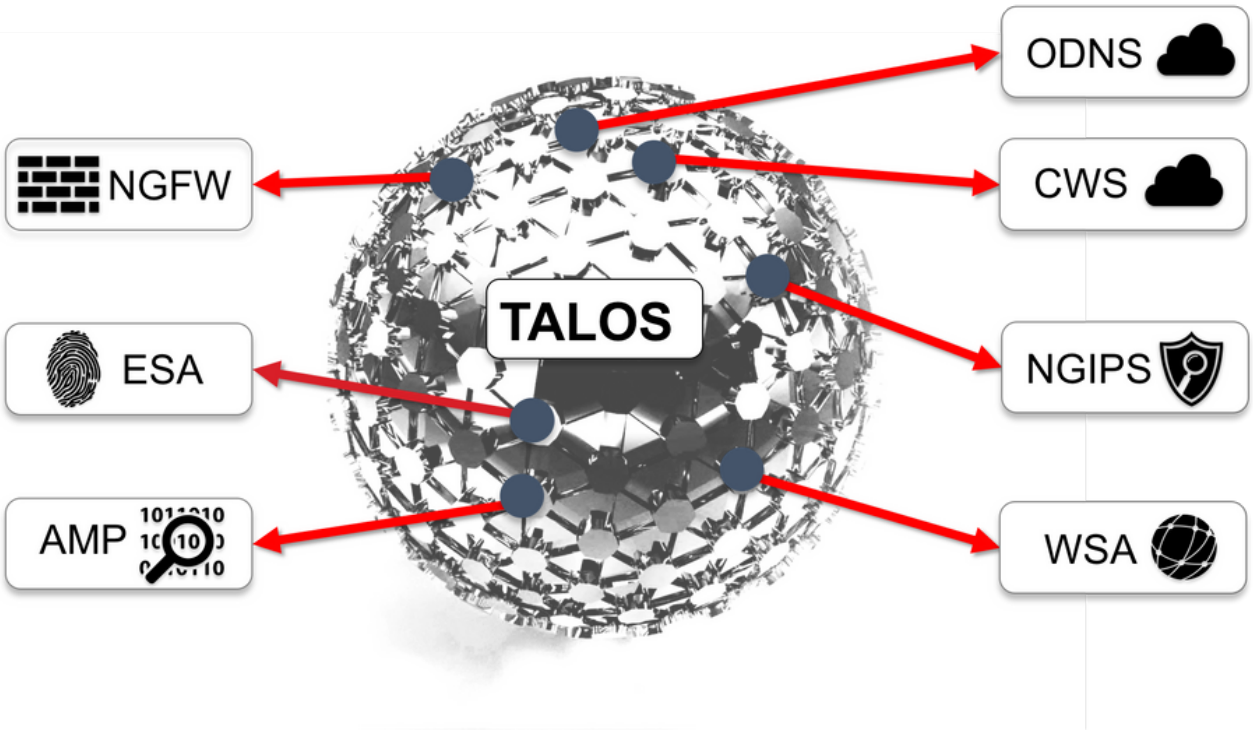
判定 – AMPレピュテーションクエリの	悪意のある/クリーン/不明
Spyname：検出されたマルウェアの名前	[トロイの木馬 – テスト]
スコア – AMPが割り当てたレピュテーションスコア	[1-100]
アップロード：ファイルのアップロードが指示されたAMPクラウド	1
File Name – 添付ファイルの名前	abcd.pdf

エンドユーザフィードバック統計情報フィード

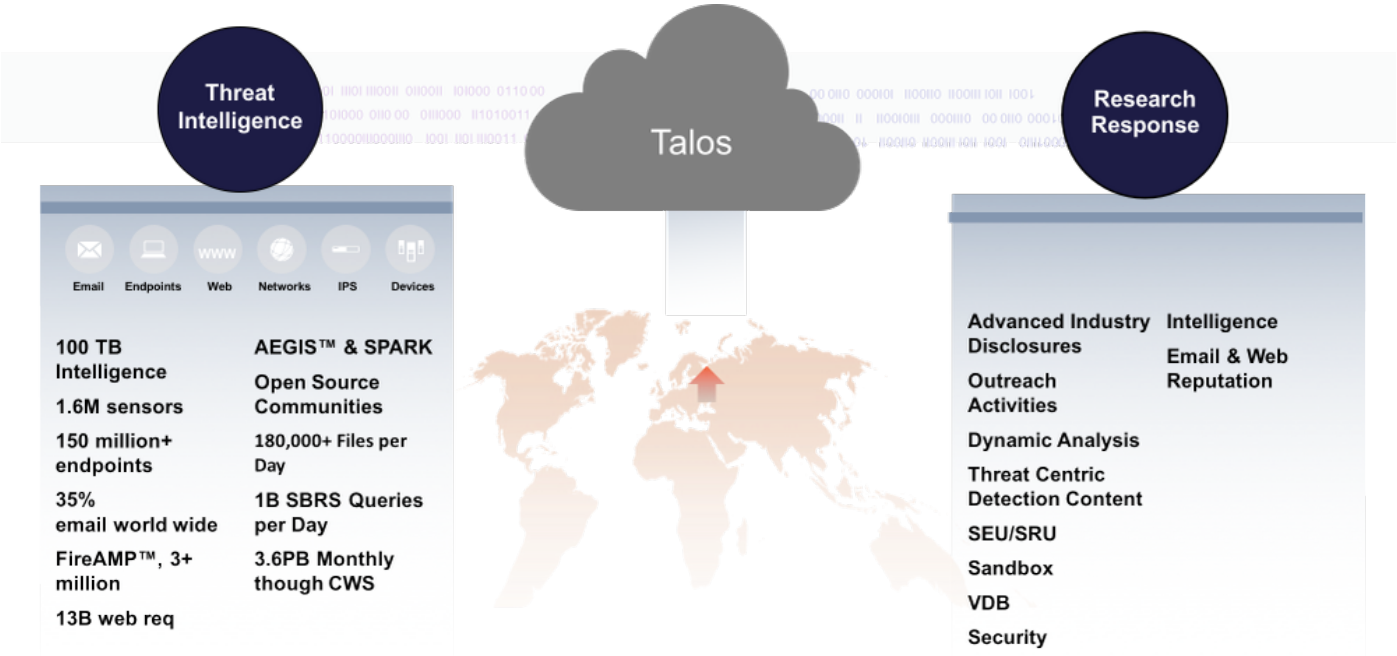
エンドユーザごとに共有される統計情報 誤分類 フィードバック

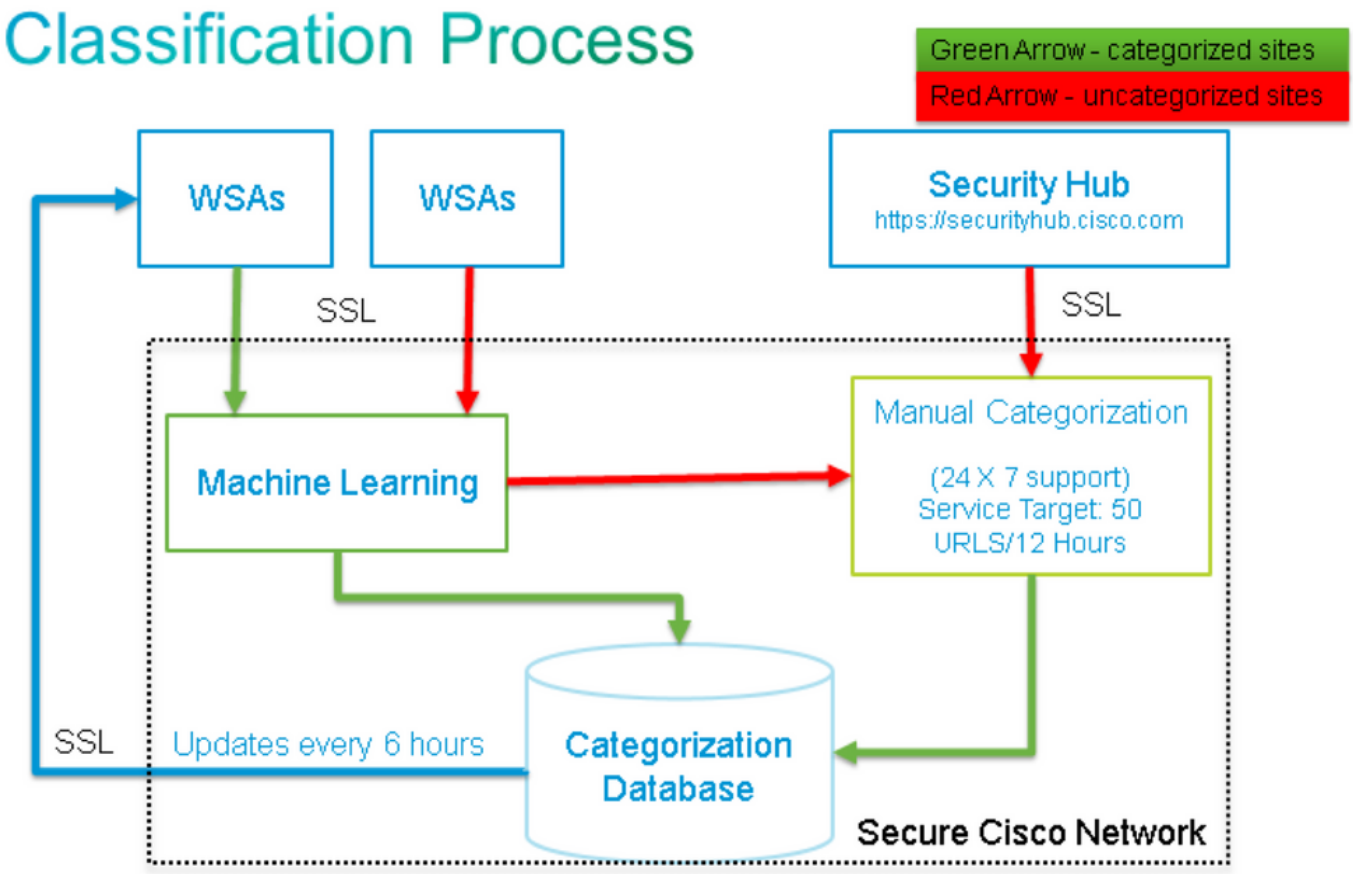
項目	**サンプルデータ**
エンジンID（数値）	0
レガシーWeb分類コード	
CIWUC Web分類ソース	'resp' / 'req'
CIWUC Webカテゴリ	1026

Talos検出コンテンツ


ODNS
NGFW
CWS
TALOS
ESA
NGIPS
AMP
WSA

脅威重視


Threat Intelligence
Talos
Research Response
Email
Endpoints
Web
Networks
IPS
Devices
100 TB Intelligence
1.6M sensors
150 million+ endpoints
35% email world wide
FireAMP™, 3+ million
13B web req
AEGIS™ & SPARK
Open Source Communities
180,000+ Files per Day
1B SBRS Queries per Day
3.6PB Monthly though CWS
Advanced Industry Disclosures
Outreach Activities
Dynamic Analysis
Threat Centric Detection Content
SEU/SRU
Sandbox
VDB
Security
Intelligence
Email & Web Reputation



関連情報

- Cisco Webセキュリティアプライアンス – 製品ページ
- Cisco Eメールセキュリティアプライアンス – 製品ページ
- テクニカル サポートとドキュメント – Cisco Systems