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

목차

소개

Cisco Web and Email Content Security 제품은 텔레메트리 데이터를 Cisco 및 Talos에 다시 제공하여 WSA(Web Security Appliance)에서 웹 범주화의 효율성을 높이고 ESA(Email Security Appliance)에 대한 연결 IP 평판을 높일 수 있습니다.

텔레메트리 데이터는 WSA 및 ESA에 대해 '옵트인(opt-in)' 기준으로 제공됩니다.

데이터는 이진 인코딩 SSL 암호화 패킷을 통해 전송됩니다. 아래에 제공된 첨부 파일은 전송 중인 데이터에 대한 데이터, 특정 서식 및 설명을 제공합니다. WBNP(WebBase Network Participation) 및 SBNP(SenderBase Network Participation) 데이터는 직접 로그 또는 파일 형식으로 볼 수 없습니다. 이 데이터는 암호화된 형식으로 전송됩니다. 이 데이터는 '비활성'이 아닙니다.

WSA - WebBase 네트워크 참여

Cisco는 개인 정보 보호의 중요성을 인식하며, 사용자 이름 및 암호와 같은 개인 또는 기밀 정보를

수집하거나 사용하지 않습니다.또한 호스트 이름 뒤에 오는 파일 이름과 URL 특성은 기밀성을 보장하기 위해 난독 처리됩니다.

암호 해독된 HTTPS 트랜잭션의 경우 SensorBase 네트워크는 인증서에 있는 서버 이름의 IP 주소, 웹 평판 점수 및 URL 범주만 수신합니다.

자세한 내용은 어플라이언스에서 현재 실행 중인 AsyncOS for Web Security 버전에 대한 WSA 사용 설명서를 참조하십시오. 사용 설명서의 "Cisco SensorBase 네트워크"를 참조하십시오.

ESA - SenderBase 네트워크 참여

SenderBase 네트워크에 참여하는 고객은 Cisco에서 조직에 대한 집계된 이메일 트래픽 통계를 수집하여 이를 사용하는 모든 사용자의 서비스 유틸리티를 늘릴 수 있습니다.참여는 자발적인 것입니다.Cisco는 메시지 특성 및 Cisco 어플라이언스에서 처리하는 다양한 유형의 메시지에 대한 정보에 대한 요약 데이터만 수집합니다.예를 들어 Cisco는 메시지 본문이나 메시지 제목을 수집하지 않습니다.개인 식별 가능한 정보 및 조직을 식별하는 정보는 기밀로 유지됩니다.

자세한 내용은 pE 검토SA 사용 설명서 를 참조하십시오. 사용 설명서의 "SenderBase 네트워크 참여" 장을 참조하십시오.

일반 보안 문제 FAQ

질문: 수집된 데이터는 어디에 저장됩니까?
답변: 어플라이언스 텔레메트리는 Cisco 미국 기반 데이터 센터에 저장됩니다.
질문: 수집 및 저장된 데이터에 액세스할 수 있는 사람은 누구입니까?
답변: 액세스 권한은 데이터를 분석/사용하여 실행 가능한 인텔리전스를 생성하는 Cisco SBG 담당자로 됩니다.
질문: 수집된 데이터의 보존 시간은 얼마입니까?
답변: 어플라이언스 텔레메트리에 대한 데이터 보존/만료 정책이 없습니다.다운샘플링/어그리게이션, 스지 관리, 연한, 현재/미래의 위협과의 관련성 등을 포함하여 다양한 이유로 데이터를 무기한 보관하삭제할 수 있습니다.
질문: 고객 일련 번호 또는 공용 IP 주소가 Talos 분류 데이터베이스에 저장됩니까?
답변: 아니요. URL 및 범주만 유지됩니다.WBNP 패킷에 소스 IP 정보가 없습니다.

작업

아래 세부 정보 작업, 데이터 유형(설명 기준) 및 전송되는 정보를 보여 주는 샘플 데이터

- SBNP - 이메일 보안과 관련된 특정 데이터 유형(필드) 및 샘플 데이터
- WBNP - 웹 보안과 관련된 특정 데이터 유형(필드) 및 샘플 데이터
- 위협 탐지 작업 - 운영 관점에서 위협 탐지에 대한 일반적인 개요

SenderBase(이메일) 네트워크 참여

이메일별 공유 통계어플라이언스

항목	샘플 데이터
MGA 식별자	MGA 10012
타임스탬프	2005년 7월 1일 오전 8시부터 오전 8시 5

	지의 데이터
소프트웨어 버전 번호	MGA 버전 4.7.0
규칙 집합 버전 번호	안티스팸 규칙 집합 102
안티바이러스 업데이트 간격	10분마다 업데이트
쿼런틴 크기	500MB
쿼런틴 메시지 수	현재 쿼런틴된 메시지 50개
바이러스 점수 임계값	위협 레벨 3 이상의 격리로 메시지 전송
쿼런틴되는 메시지의 바이러스 점수 합계	120
쿼런틴에 들어가는 메시지 수	30(평균 점수 4점 획득)
최대 격리 시간	12시간
쿼런틴을 입력하고 종료한 이유에 의해 분석된 신종 바이러스 쿼런틴 메시지 수(안티바이러스 결과와 상관관계 있음)	.exe 규칙 30 수동 릴리스로 인해 쿼런틴, 인해 50 격리, 30 모두 바이러스 양성임
쿼런틴에서 나갈 때 수행한 작업으로 분석된 신종 바이러스 격리 메시지 수	쿼런틴을 종료한 후 첨부 파일이 제거된 지 10개
메시지가 쿼런틴된 시간의 합계	20시간

IP 주소당 공유되는 통계

항목	샘플 데이터	표준 참여	제한된 참여
어플라이언스 내의 다양한 단계에서 메시지 수	안티바이러스 엔진에서 확인:100 안티스팸 엔진에서 확인:80		
안티스팸 및 안티바이러스 점수 및 판정 합계	2,000(표시된 모든 메시지에 대한 안티스팸 점수 합계)		
서로 다른 안티스팸 및 안티바이러스 규칙 조합에 도달하는 메시지 수	100개의 메시지가 규칙 A와 B에 도달함 50개의 메시지가 규칙 A에 해당		
연결 수	20개의 SMTP 연결		
총 및 잘못된 수신자 수	총 수신자 50명 올바르지 않은 수신인 10명		
해시된 파일 이름:가.	<one-way-hash>.pif 파일이 <one-way-hash>.zip이라는 아카이브 첨부 파일 안에 있습니다.	난독 불가한 파일 이름	해시된 파일
난독 처리된 파일 이름:나.	aaaaaaa0.aaa.pif 파일이 aaaaaaa.zip 파일 내에서 발견되었습니다.	난독 불가한 파일 이름	난독 처리된 이름
URL 호스트 이름(c)	메시지 내에 www.domain.com에 대한 링크가 있습니다.	난독 불가한 URL 호스트 이름	난독 처리된 호스트 이름
난독 처리된 URL 경로(d)	메시지 안에 호스트 이름 www.domain.com에 대한 링크가 있으며 경로 aaa000aa/aa00aaa가 있습니다.	난독 불가 URL 경로	난독 처리된 경로
스팸 및 바이러스 검사 결과별 메시지 수	10개의 스팸 판정 10 스팸 음수 5 스팸 의심 4 바이러스 양성 16 바이러스 음수 5 바이러스 검사 불가		
다른 안티스팸 및 안티바이러스 판정에 의한 메시지 수	스팸 500개, 햄 300개		
크기 범위의 메시지 수	30K-35K 범위 125개		
서로 다른 확장 유형 수	300 ".exe" 첨부 파일		
첨부 파일 유형, True 파일 유형 및 컨테이너 유형의 상관관계	확장명이 ".doc"이지만 실제로는 ".exe"인 첨부 파일 100개 50개의 첨부 파일이 zip 내에 ".exe" 확장입		

	니다.
확장명 및 True 파일 유형과 첨부 파일 크기의 상관관계	첨부 파일 30개는 50-55K 범위 내에서 ".exe"였습니다.
확률적 샘플링 결과의 메시지 수	샘플링을 건너뛴 메시지 14개 샘플링을 위해 대기 중인 메시지 25개 샘플링에서 스캔한 메시지 50개
DMARC 확인에 실패한 메시지 수	DMARC 확인에 실패한 메시지 34개

참고:

(a) 파일 이름은 단방향 해시(MD5)로 인코딩됩니다.

(b) 파일 이름은 난독 처리된 형태로 전송되며 모든 소문자 ASCII 문자([a-z])가 "a"로 대체되고, 모든 대문자 ASCII 문자([A-Z])가 "A"로 대체되고, 멀티바이트 UTF-8 문자가 "x"로 대체되고(다른 문자 집합에 대한 프라이버시 제공) 모든 ASCII 숫자([0-9])가 대체됩니다.

다. URL 호스트 이름은 IP 주소와 마찬가지로 콘텐츠를 제공하는 웹 서버를 가리킵니다.사용자 이름 및 비밀번호와 같은 기밀 정보는 포함되지 않습니다.

라. 호스트 이름 다음에 오는 URL 정보는 사용자의 개인 정보가 표시되지 않도록 난독 처리됩니다.

SDS 클라이언트당 공유되는 통계

항목	샘플 데이터
타임스탬프	
클라이언트 버전	
클라이언트에 대한 요청 수	
SDS 클라이언트에서 수행한 요청 수	
DNS 조회의 시간 결과	
서버 응답 시간 결과	
서버 연결 설정 시간	
설정된 연결 수	
서버에 대한 동시 열린 연결 수	
WBRS에 대한 서비스 요청 수	
로컬 WBRS 캐시를 적중시킨 요청 수	
로컬 WBRS 캐시 크기	
원격 WBRS의 응답 시간 결과	

AMP SBNP 텔레메트리 데이터

형식	샘플 데이터
amp_판정:{ ("verdict", "spyname", "score", "uploaded", "file_name"), ("판정", "spyname", "score", "업로드됨", "file_name"), ("판정", "spyname", "score", "업로드됨", "file_name"), ... ("판정", "spyname", "score", "업로드됨", "file_name"), }	
설명	
판정 - AMP 평판 쿼리	악성/정상/알 수 없음
Spyname - 탐지된 악성코드의 이름	[트로이 목마-테스트]

점수 - AMP에서 할당한 평판 점수	[1-100]
업로드 - 파일 업로드에 표시된 AMP 클라우드	1
파일 이름 - 파일 첨부 파일의 이름	abcd.pdf

WebBase(웹) 네트워크 참여

웹 요청당 공유된 통계

항목	샘플 데이터	표준 참여	제한된 참여
버전	7.7.0-608		
일련 번호			
SBNP 샘플링 계수(볼륨)			
SBNP 샘플링 계수(속도)	1		
대상 IP 및 포트		난독 처리된 URL 경로 세그먼트	해시된 URL 경로 세트
안티스파이웨어 선택 악성코드 범주	건너뛰었습니다.		
WBRS 점수	4.7		
McAfee 악성코드 카테고리 판정			
참조 URL		난독 처리된 URL 경로 세그먼트	해시된 URL 경로 세트
콘텐츠 형식 ID			
ACL 결정 태그	0		
레거시 웹 분류			
CIWUC 웹 카테고리 및 결정 출처	{'src':'req', 'cat':'1026'}		
AVC 앱 이름	광고 및 추적		
AVC 앱 유형	광고 네트워크		
AVC 앱 동작	안전하지 않음		
내부 AVC 결과 추적	[0,1,1,1]		
인덱싱된 데이터 구조를 통한 사용자 에이전트 추적	3		

웹 요청당 지능형 악성코드 통계

AMP 통계

판정 - AMP 평판 쿼리	악성/정상/알 수 없음
Spyname - 탐지된 악성코드의 이름	[트로이 목마-테스트]
점수 - AMP에서 할당한 평판 점수	[1-100]
업로드 - 파일 업로드에 표시된 AMP 클라우드	1
파일 이름 - 파일 첨부 파일의 이름	abcd.pdf

최종 사용자 피드백 통계 피드

최종 사용자당 공유 통계 잘못된 분류 피드백

항목	샘플 데이터
엔진 ID(숫자)	0
레거시 웹 분류 코드	
CIWUC 웹 분류 소스	'resp' / 'req'
CIWUC 웹 범주	1026

제공된 데이터의 예 - 표준 참여

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

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

제공된 데이터의 예 - 제한된 참여

- 클라이언트의 원래 요청:www.gunexams.com/Non-Restricted-FREE-Practice-Exams
- 기록된 메시지(원격 분석 서버에 있음):http://www.gunexams.com/76bd845388e0

전체 WBNP 디코딩

Cisco 어플라이언스별로 공유되는 통계

항목	샘플 데이터
버전	7.7.0-608
일련 번호	0022190B6ED5-XYZ1YZ2
모델	S660
Webroot 사용	1
AVC 사용	1
Sophos 사용	0
응답 측 분류 사용	1
안티스파이웨어 엔진 사용	기본-2001005008
안티스파이웨어 SSE 버전	기본-2001005008
안티스파이웨어 Spycat 정의 버전	default-8640
안티스파이웨어 URL 차단 목록 DAT 버전	
안티스파이웨어 URL 피싱 DAT 버전	
안티스파이웨어 쿠키 DAT 버전	
안티스파이웨어 도메인 차단 사용	0
안티스파이웨어 위협 위험 임계값	90
McAfee 사용	0
McAfee 엔진 버전	
McAfee DAT 버전	default-5688
WBNP 세부 정보 레벨	2
WBRS 엔진 버전	freebsd6-i386-300036
WBRS 구성 요소 버전	categories=v2-1337979188,ip=default-1379460997,키워드=v2-131248822,prefixcat=v2-1379460670,rule=default-13599791999927777777777722222222
WBRS 차단 목록 임계값	-6
WBRS 허용 목록 임계값	6
WBRS 사용	1
보안 모빌리티 사용	0

L4 트래픽 모니터 사용	0
L4 트래픽 모니터 차단 목록 버전	기본-0
L4 트래픽 모니터 관리 차단 목록	
L4 트래픽 모니터 관리 차단 목록 포트	
L4 트래픽 모니터 허용 목록	
L4 트래픽 모니터 허용 목록 포트	
SBNP 샘플링 요소	0.25
SBNP 샘플링 계수(볼륨)	0.1
SurfControl SDK 버전(레거시)	기본-0
SurfControl 전체 데이터베이스 버전(레거시)	기본-0
SurfControl 로컬 증분 누적 파일 버전(레거시)	기본-0
Firestone Engine 버전	default-210016
Firestone DAT 버전	v2-310003
AVC 엔진 버전	default-110076
AVC DAT 버전	default-1377556980
Sophos 엔진 버전	default-1310963572
Sophos DAT 버전	기본-0
적응형 스캐닝 사용	0
적응형 스캐닝 위험 점수 임계값	[10, 6, 3]
적응형 스캐닝 로드 팩터 임계값	[5, 3, 2]
SOCKS 사용	0
총 트랜잭션	
총 트랜잭션	
총 허용 트랜잭션	
발견된 총 악성코드 트랜잭션	
관리 정책에 의해 차단된 총 트랜잭션	
WBRS 점수로 차단된 총 트랜잭션	
위험 부담이 높은 총 트랜잭션 수	
트래픽 모니터에서 탐지된 총 트랜잭션	
IPv6 클라이언트가 있는 총 트랜잭션	
IPv6 서버가 있는 총 트랜잭션	
SOCKS 프록시를 사용하는 총 트랜잭션	
원격 사용자의 총 트랜잭션	
로컬 사용자의 총 트랜잭션	
SOCKS 프록시를 사용하여 허용되는 총 트랜잭션	
SOCKS 프록시를 사용하여 허용된 로컬 사용자의 총 트랜잭션	
SOCKS 프록시를 사용하여 허용된 원격 사용자의 총 트랜잭션	
SOCKS 프록시를 사용하여 차단된 총 트랜잭션	
SOCKS 프록시를 사용하여 차단된 로컬 사용자의 총 트랜잭션	
SOCKS 프록시를 사용하여 차단된 원격 사용자의 총 트랜잭션	
마지막 다시 시작 이후 초	2843349
CPU 사용률(%)	9.9
RAM 사용률(%)	55.6
하드 디스크 사용률(%)	57.5
대역폭 사용률(/초)	15307
TCP 연결 열기	2721
초당 트랜잭션 수	264

클라이언트 레이턴시	163
캐시 적중률	21
프록시 CPU 사용률	17
WBRS WUC CPU 사용률	2.5
로깅 CPU 사용률	3.4
보고 CPU 사용률	3.9
Webroot CPU 사용률	0
Sophos CPU 사용률	0
McAfee CPU 사용률	0
vmstat 유틸리티 출력(vmstat -z, vmstat -m)	
구성된 액세스 정책 수	32
구성된 사용자 지정 웹 범주 수	32
인증 공급자	기본, NTLMSSP
인증 영역	인증 공급자 호스트 이름, 프로토콜 및 기타 구성 요소

웹 요청당 공유된 통계

항목	샘플 데이터	표준 참여	제한된 참여
버전	7.7.0-608		
일련 번호			
SBNP 샘플링 계수(볼륨)			
SBNP 샘플링 계수(속도)	1		
대상 IP 및 포트		난독 처리된 URL 경로 세그먼트	해시된 URL 경로 세트
안티스파이웨어 선택 악성코드 범주	건너뛰었습니다.		
WBRS 점수	4.7		
McAfee 악성코드 카테고리 판정			
참조 URL		난독 처리된 URL 경로 세그먼트	해시된 URL 경로 세트
콘텐츠 형식 ID			
ACL 결정 태그	0		
레거시 웹 분류			
CIWUC 웹 카테고리 및 결정 출처	{'src':'req', 'cat':'1026'}		
AVC 앱 이름	광고 및 추적		
AVC 앱 유형	광고 네트워크		
AVC 앱 동작	안전하지 않음		
내부 AVC 결과 추적	[0,1,1,1]		
인덱싱된 데이터 구조를 통한 사용자 에이전트 추적	3		

웹 요청당 지능형 악성코드 통계

AMP 통계

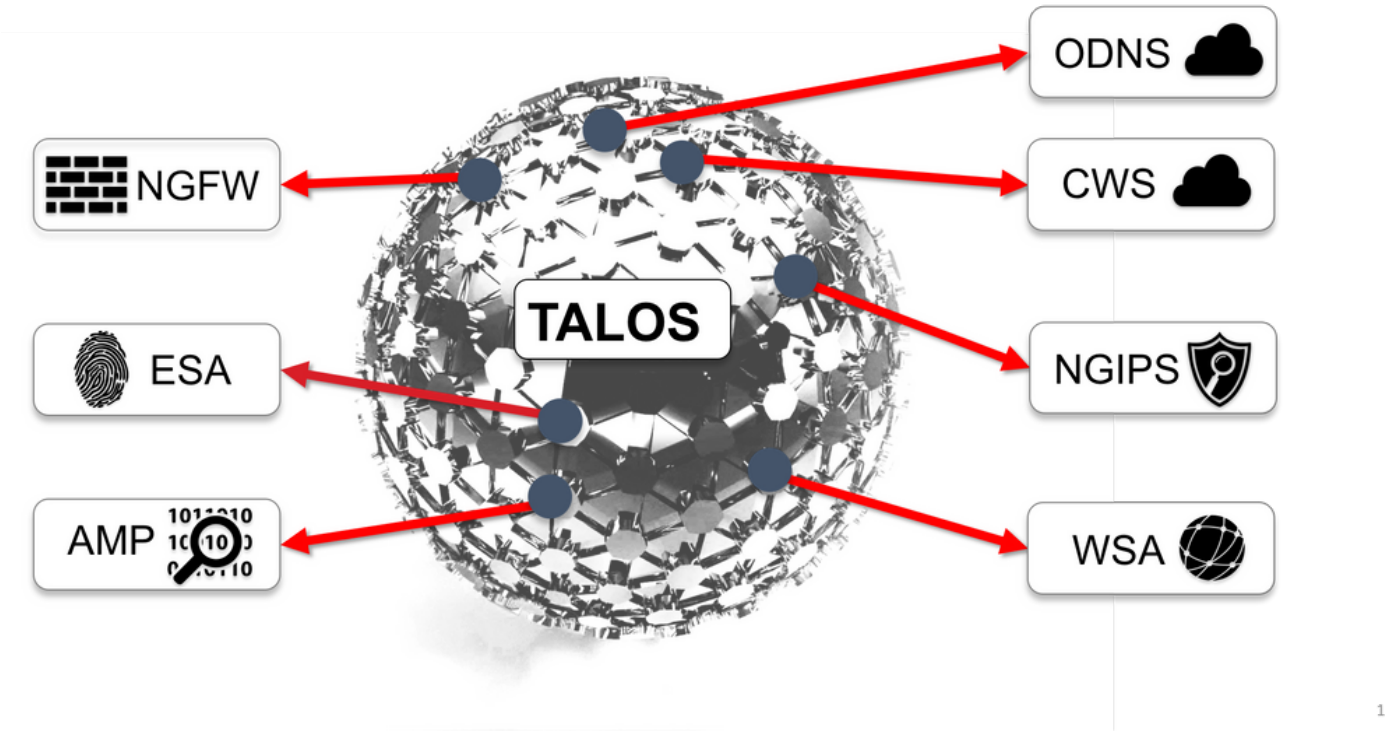
판정 - AMP 평판 쿼리	악성/정상/알 수 없음
Spyname - 탐지된 악성코드의 이름	[트로이 목마-테스트]
점수 - AMP에서 할당한 평판 점수	[1-100]
업로드 - 파일 업로드에 표시된 AMP 클라우드	1
파일 이름 - 파일 첨부 파일의 이름	abcd.pdf

최종 사용자 피드백 통계 피드

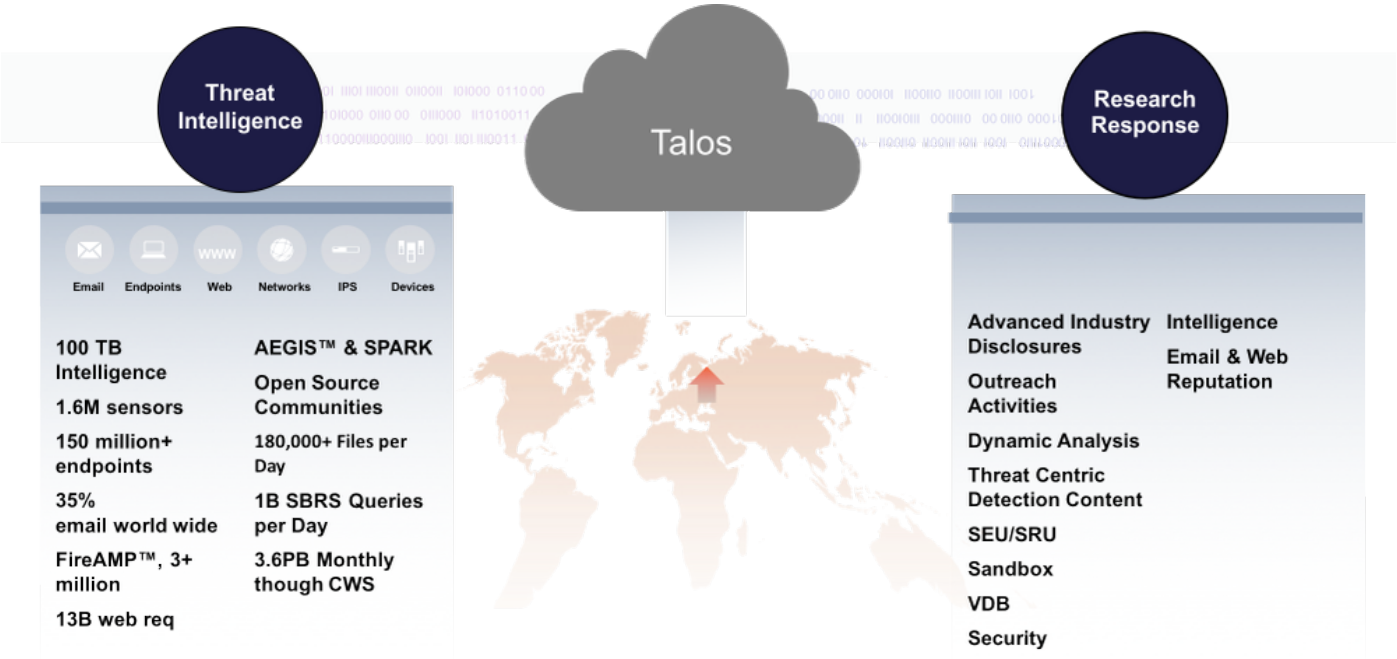
최종 사용자당 공유 통계 잘못된 분류 피드백

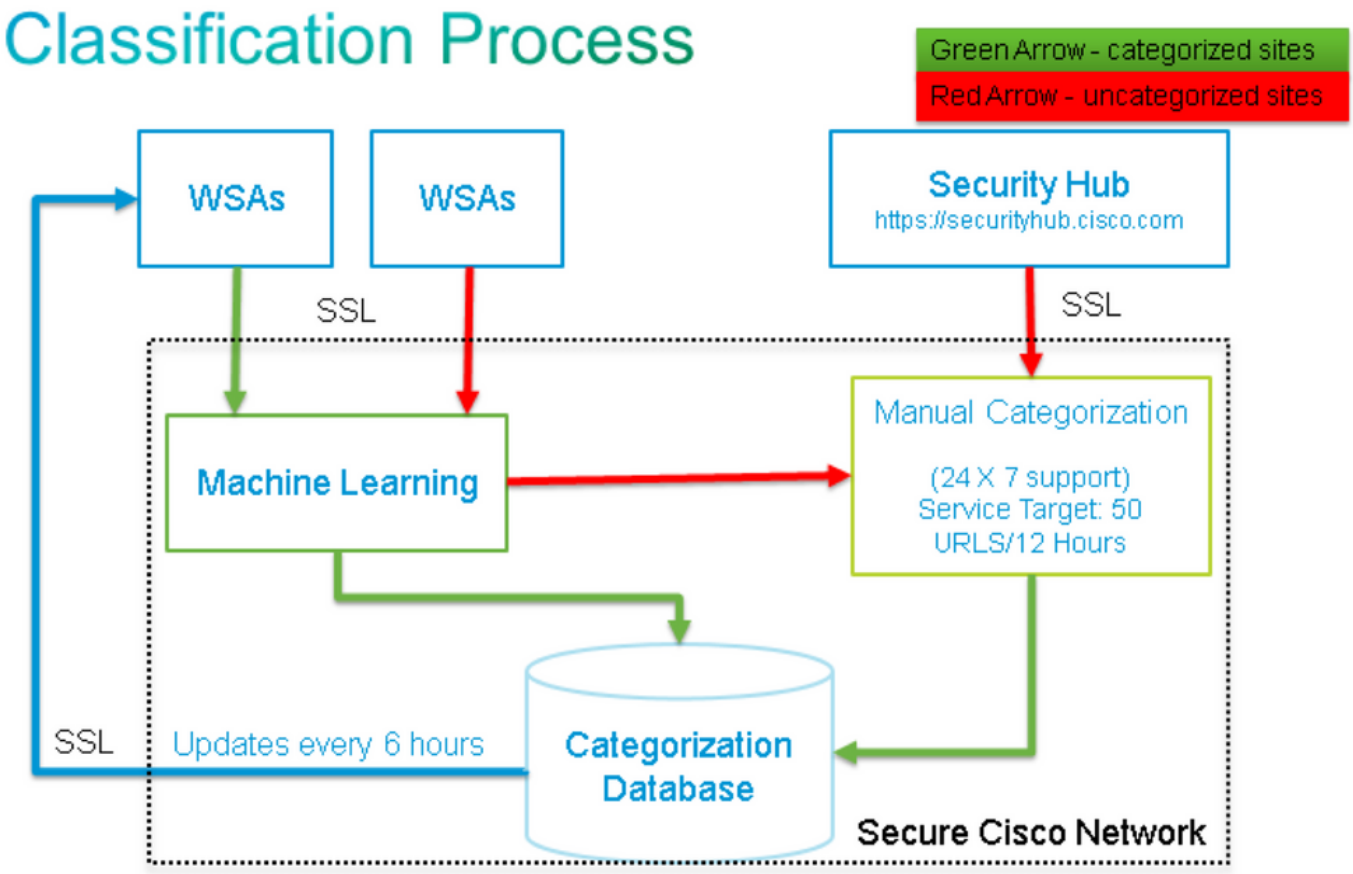
항목	샘플 데이터
엔진 ID(숫자)	0
레거시 웹 분류 코드	
CIWUC 웹 분류 소스	'resp' / 'req'
CIWUC 웹 범주	1026

Talos 탐지 콘텐츠



위협 중심





관련 정보

- Cisco Web Security Appliance - 제품 페이지
- Cisco Email Security Appliance - 제품 페이지
- 기술 지원 및 문서 – Cisco Systems