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

Inhalt

Einführung
WSA = WebBase Network Participation
ESA = SenderBase Network Participation
Häufig gestellte Fragen zu allgemeinen Sicherheitsbedenken
Betrieb
Teilnahme am SenderBase-Netzwerk (E-Mail)
Freigegebene Statistiken pro E-Mail-Appliance
Pro IP-Adresse freigegebene Statistiken
Pro SDS-Client freigegebene Statistiken
Telemetriedaten zu AMP SBNP
WebBase (Web)-Netzwerkteilnahme
Statistiken werden pro Webanfrage freigegeben
Erweiterte Malware-Statistiken pro Webanfrage
Feedback-Feed für Endbenutzer
Bereitgestellte Beispieldaten - Standardbeteiligung
Bereitgestellte Beispieldaten - Eingeschränkte Beteiligung
Vollständige WBNP-Dekodierung
Statistiken werden pro Webanfrage freigegeben
Erweiterte Malware-Statistiken pro Webanfrage
Feedback-Feed für Endbenutzer
Talos Detection-Inhalte
Bedrohungsorientiert
Zugehörige Informationen

Einführung

Die Cisco Web- und E-Mail Content Security-Produkte können Cisco und Talos Telemetriedaten übermitteln, um die Effizienz der Webkategorisierung in der Web Security Appliance (WSA) zu erhöhen und die Verbindung der IP-Reputation der E-Mail Security Appliance (ESA) zu verbessern.

Die Telemetriedaten werden für die WSA und die ESA auf "Opt-in"-Basis bereitgestellt.

Die Daten werden mittels binär verschlüsselter SSL-verschlüsselter Pakete übertragen. Die unten angegebenen Anhänge bieten einen Einblick in die Daten, die spezifische Formatierung und Beschreibungen der übertragenen Daten. Die Daten für WebBase Network Participation (WBNP) und SenderBase Network Participation (SBNP) können nicht in einem direkten Protokoll- oder Dateiformat angezeigt werden. Diese Daten werden verschlüsselt übertragen. Diese Daten sind zu keinem Zeitpunkt "ruhend".

WSA = WebBase Network Participation

Cisco ist sich der Wichtigkeit der Wahrung Ihrer Privatsphäre bewusst und sammelt und verwendet keine persönlichen oder vertraulichen Informationen wie Benutzernamen und Passphrasen. Darüber hinaus werden die Dateinamen und URL-Attribute, die dem Hostnamen folgen, verschleiert, um Vertraulichkeit zu gewährleisten.

Bei entschlüsselten HTTPS-Transaktionen empfängt das SensorBase-Netzwerk nur die IP-Adresse, den Web-Reputationswert und die URL-Kategorie des Servernamens im Zertifikat.

Vollständige Informationen finden Sie im WSA-Benutzerhandbuch für die derzeit auf Ihrer Appliance ausgeführte Version von AsyncOS für Web Security. Weitere Informationen finden Sie im Benutzerhandbuch unter "Das Cisco SensorBase-Netzwerk".

ESA = SenderBase Network Participation

Kunden, die am SenderBase-Netzwerk teilnehmen, ermöglichen es Cisco, aggregierte Statistiken zum E-Mail-Datenverkehr über ihre Organisation zu sammeln, wodurch der Nutzen des Services für alle Benutzer erhöht wird. Die Teilnahme ist freiwillig. Cisco sammelt nur zusammengefasste Daten zu Nachrichtenattributen und Informationen darüber, wie verschiedene Arten von Nachrichten von Cisco Appliances behandelt wurden. Beispielsweise erfasst Cisco nicht den Nachrichtentext oder den Betreff der Nachricht. Persönlich identifizierbare Informationen und Informationen zur Identifizierung Ihres Unternehmens werden vertraulich behandelt.

Vollständige Informationen finden Sie hier: pBitte überprüfen Sie die ESA-Benutzerhandbuch für die derzeit auf Ihrer Appliance ausgeführte Version von AsyncOS für ESA Security. Siehe "SenderBase-Netzwerkteilnahme" im Benutzerhandbuch.

Häufig gestellte Fragen zu allgemeinen Sicherheitsbedenken

Frage:	Wo werden die gesammelten Daten gespeichert?
Antwort:	Die Appliance-Telemetrie wird in Cisco Rechenzentren in den USA gespeichert.
Frage:	Wer hat Zugriff auf die gesammelten und gespeicherten Daten?
Antwort:	Der Zugriff ist auf Mitarbeiter der Cisco SBG beschränkt, die die Daten analysieren/verwenden, u aussagekräftige Informationen zu erstellen.
Frage:	Wie lange dauert die Aufbewahrung der erfassten Daten?
Antwort:	Es gibt keine Richtlinien zur Datenspeicherung/zum Ablauf von Appliance-Telemetrie. Die Daten können unbegrenzt gespeichert oder aus verschiedenen Gründen gelöscht werden, u. a. aus de folgenden Gründen: Down-Sampling/Aggregation, Speichermanagement, Alter, Relevanz für aktuelle/zukünftige Bedrohungen usw.
Frage:	Werden in der Kategorisierungsdatenbank von Talos Seriennummern oder öffentliche IP-Adress gespeichert?
Antwort:	Nein, nur URLs und Kategorien werden beibehalten. Das WBNP-Paket enthält keine Quell-IP-Informationen.

Betrieb

Im Folgenden werden der Vorgang, der Datentyp (nach Beschreibung) und eine Beispieldaten zum Demonstrieren der zu übertragenden Informationen beschrieben:

- SBNP - Spezifische Datentypen (Felder) und Beispieldaten für E-Mail-Sicherheit
- WBNP - Spezifische Datentypen (Felder) und Beispieldaten für Web Security
- Bedrohungserkennungsvorgang - Allgemeiner Überblick über die Bedrohungserkennung aus betrieblicher Sicht

Teilnahme am SenderBase-Netzwerk (E-Mail)

Pro E-Mail freigegebene StatistikenEinheit

Element	Beispieldaten
MGA-Kennung	MGA 10012
Zeitstempel	Daten von 08:05 bis 08:05 Uhr am 1. Jul 2005
Software-Versionsnummern	MGA-Version 4.7.0
Regelsatz-Versionsnummern	Anti-Spam-Regelsatz 102
Anti-Virus-Aktualisierungsintervall	Aktualisierung alle 10 Minuten
Quarantänegröße	500 MB
Anzahl der Quarantänemeldungen	Aktuell befinden sich 50 Nachrichten in Quarantäne
Virus-Punktwert	Nachrichten bei Bedrohungsstufe 3 oder höher an Quarantäne senden
Summe der Virusbewertungen für Nachrichten, die in den Quarantänebereich eingegeben werden	120
Anzahl der Nachrichten, die in Quarantäne eingegeben werden	30 (ergibt einen Durchschnittswert von 4
Maximale Quarantänezeit	12 Stunden
Anzahl der Outbreak-Quarantänenachrichten, aufgeschlüsselt nach dem Grund, warum sie in den Quarantänebereich eingedrungen und aus diesem entfernt wurden, korreliert mit dem Anti-Virus-Ergebnis	50 wurden in Quarantäne gesetzt, weil d .exe-Regel 30 aufgrund einer manuellen Freigabe die Quarantäne verlässt, und a waren viruspositiv
Anzahl der Outbreak-Quarantänenachrichten, aufgeschlüsselt nach den Maßnahmen, die beim Verlassen der Quarantäne ergriffen wurden	Bei 10 Nachrichten wurden Anhänge na dem Verlassen des Quarantänebereichs entfernt.
Anzahl der Nachrichten, die in Quarantäne gehalten wurden	20 Stunden

Pro IP-Adresse freigegebene Statistiken

Element	Beispieldaten	Standardbeteiligung	Eingeschränkte Beteiligung
Nachrichtenanzahl in verschiedenen Phasen innerhalb der Appliance	Gesichtet von der Anti-Virus-Engine: 100 Nach Anti-Spam-Engine gesehen: 80		
Summe der Anti-Spam- und Anti-Virus-Bewertungen und Verdicts	2.000 (Summe der Anti-Spam-Bewertungen für alle erkannten Nachrichten)		
Anzahl der Nachrichten, die von verschiedenen Anti-Spam- und Anti-Virus-Regelkombinationen empfangen werden	100 Nachrichten werden von den Regeln A und B empfangen Nur 50 Nachrichten werden von Regel A empfangen		
Anzahl der Verbindungen	20 SMTP-Verbindungen		
Anzahl der Empfänger insgesamt und ungültig	Insgesamt 50 Empfänger 10 ungültige Empfänger		

Dateinamen mit Hashfunktion: a)	Eine Datei <unidirektionaler Hash>.pif wurde in einem Archivanhang mit der Bezeichnung <unidirektionaler Hash>.zip gefunden.	Unbekannter Dateiname	Hashed-Dateiname
Verdeckte Dateinamen: b)	Eine Datei aaaaaa0.aaa.pif wurde in einer Datei aaaaa.zip gefunden.	Unbekannter Dateiname	Verdeckter Dateiname
URL-Hostname (c)	Es wurde ein Link in einer Nachricht an www.domain.com gefunden.	Unbekannter URL-Hostname	Verdeckter U Hostname
Verdeckter URL-Pfad (d)	In einer Nachricht wurde ein Link zum Hostnamen www.domain.com gefunden, und der Pfad aaa000aa/aa00aaa.	Nicht verwendeter URL-Pfad	Verdeckter U Pfad
Anzahl der Nachrichten nach Spam- und Virenscanning-Ergebnissen	10 Spam-positiv 10 Spam negativ 5 Spam-verdächtig 4 Virus-positiv 16 Virus negativ 5 Virus nicht scanbar		
Anzahl der Nachrichten nach verschiedenen Anti-Spam- und Anti-Virus-Verdicts	500 Spam, 300 Schinken		
Anzahl der Nachrichten in Größenbereichen	125 im Bereich 30.000-35.000		
Anzahl verschiedener Erweiterungstypen	300 ".exe"-Anhänge		
Korrelation von Anlagentypen, echtem Dateityp und Containertyp	100 Anhänge mit der Erweiterung ".doc", die aber tatsächlich ".exe" sind 50 Anhänge sind ".exe"-Erweiterungen innerhalb eines Zip-Archivs.		
Korrelation von Erweiterung und echtem Dateityp mit der Größe des Anhangs	30 Anhänge waren ".exe" im Bereich von 50-55 K.		
Anzahl der Nachrichten nach Stochastic Sampling-Ergebnissen	14 Nachrichten wurden per Sampling übersprungen 25 Nachrichten in Warteschlange für Stichproben 50 aus Stichproben gescannte Nachrichten		
Anzahl der Nachrichten, die die DMARC-Überprüfung nicht bestanden haben	34 Nachrichten haben die DMARC-Überprüfung nicht bestanden.		

Hinweise:

(a) Dateinamen werden in einem einseitigen Hash (MD5) kodiert.

(b) Dateinamen werden verdeckt gesendet, wobei alle ASCII-Kleinbuchstaben ([a-z]) durch "a" ersetzt werden, alle ASCII-Großbuchstaben ([A-Z]) durch "A" ersetzt werden, alle UTF-8-Multi-Byte-Zeichen, die durch "x" ersetzt werden (um den Datenschutz für andere Zeichensätze zu gewährleisten), alle ASCII-Ziffern ([0-9]).

(c) URL-Hostnamen verweisen auf einen Webserver, der Inhalte bereitstellt, ähnlich wie eine IP-Adresse. Es werden keine vertraulichen Informationen wie Benutzernamen und Kennwörter eingegeben.

(d) URL-Informationen, die auf den Hostnamen folgen, werden verschleiert, um sicherzustellen, dass keine persönlichen Informationen des Benutzers weitergegeben werden.

Pro SDS-Client freigegebene Statistiken

Element	Beispieldaten
TimeStamp	
Client-Version	
Anzahl der an den Kunden gestellten Anfragen	
Anzahl der vom SDS-Client gestellten Anforderungen	
Zeitergebnisse für DNS-Suchvorgänge	
Server-Reaktionszeit-Ergebnisse	
Zeit zum Herstellen der Verbindung zum Server	
Anzahl der Verbindungen	
Anzahl gleichzeitiger offener Verbindungen zum Server	
Anzahl der Serviceanfragen an WBRS	
Anzahl der Anforderungen, die den lokalen WBRS-Cache treffen	
Größe des lokalen WBRS-Cache	
Reaktionszeit durch Remote-WBRS	

Telemetriedaten zu AMP SBNP

Format	Beispieldaten
AMP_VERdicts': { ("Verdict", "spyname", "score", "hochgeladen", "file_name"), ("Verdict", "spyname", "score", "hochgeladen", "file_name"), ("Verdict", "spyname", "score", "hochgeladen", "file_name"), ... ("Verdict", "spyname", "score", "hochgeladen", "file_name"), }	
Beschreibung	
Verdict - der AMP-Reputationsabfrage	schädlich/sauber/unbekannt
Spyname - Name der erkannten Malware	[Trojaner-Test]
Bewertung - AMP zugewiesene Reputationsbewertung	[1-100]
Upload - Die AMP-Cloud hat angegeben, die Datei hochzuladen.	1
Dateiname - Name der Dateianlage	abcd.pdf

WebBase (Web)-Netzwerkteilnahme

Statistiken werden pro Webanfrage freigegeben

Element	Beispieldaten	Standardbeteiligung	Eingeschränkte Beteiligung
Version	coeus 7.7.0-608		
Seriennummer			
SBNP-Samplingfaktor (Volumen)			

SBNP-Stichprobenfaktor (Rate)	1		
Ziel-IP und -Port		unverschleierte URL-Pfadsegmente	Hash-URL-Pfadsegr
Für Anti-Spyware ausgewählte Malware-Kategorie	Übersprungen		
WBRS-Bewertung	4,7		
Kategorie-Verdict für McAfee-Malware			
Referer-URL		unverschleierte URL-Pfadsegmente	Hash-URL-Pfadsegr
Inhaltstyp-ID			
ACL-Entscheidungstag	0		
Ältere Web-Kategorisierung			
CIWUC-Webkategorie und Entscheidungsquelle	{'src': 'req', 'cat': '1026'}		
AVC-Anwendungsname	Anzeigen und Nachverfolgen		
AVC-Anwendungstyp	Ad-Netzwerke		
AVC-Anwendungsverhalten	Unsicher		
Interne AVC-Ergebnisverfolgung	[0,1,1,1]		
Nachverfolgung von Benutzeragenten über indizierte Datenstruktur	1		

Erweiterte Malware-Statistiken pro Webanfrage

AMP-Statistiken

Verdict - der AMP-Reputationsabfrage	schädlich/sauber/unbekannt
Spyname - Name der erkannten Malware	[Trojaner-Test]
Bewertung - AMP zugewiesene Reputationsbewertung	[1-100]
Upload - Die AMP-Cloud hat angegeben, die Datei hochzuladen.	1
Dateiname - Name der Dateianlage	abcd.pdf

Feedback-Feed für Endbenutzer

Freigegebene Statistiken pro Endbenutzer
Fehlkategorisierung Feedback

Element	Beispieldaten
Engine-ID (numerisch)	0
Legacy-Webkategorisierungscode	
CIWUC-Webkategorisierungsquelle	"resp"/"req"
CIWUC-Webkategorie	1026

Bereitgestellte Beispieldaten - Standardbeteiligung

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

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

Bereitgestellte Beispieldaten - Eingeschränkte Beteiligung

- Ursprüngliche Anfrage vom Client: www.gunexams.com/Non-Restricted-FREE-Practice-Exams
- Protokollierung der Nachricht (auf dem Telemetrieserver): http://www.gunexams.com/76bd845388e0

Vollständige WBNP-Dekodierung

Auf Cisco Appliance freigegebene Statistiken

Element	Beispieldaten
Version	coeus 7.7.0-608
Seriennummer	0022190B6ED5-XYZ1YZ2
Modell	S660
Webroot aktiviert	1
AVC aktiviert	1
Sophos aktiviert	0
Kategorisierung auf der Antwortseite aktiviert	1
Anti-Spyware-Engine aktiviert	default-2001005008
Anti-Spyware SSE-Version	default-2001005008
Anti-Spyware Spycat Definitions-Version	default-8640
DAT-Version der Anti-Spyware-URL-Blocklist	
Anti-Spyware URL Phishing-DAT-Version	
DAT-Version für Anti-Spyware-Cookies	
Blockierung von Anti-Spyware-Domänen aktiviert	0
Schwellenwert für Anti-Spyware-Bedrohungsrisiko	90
McAfee aktiviert	0
McAfee-Modulversion	
McAfee DAT-Version	default-5688
WBNP-Detailstufe	2
WBRS-Modulversion	freebsd6-i386-300036
WBRS-Komponentenversionen	categories=v2-1337979188,ip=default-1379460997,keyword=v2-1312487822,prefixcat=v2-1379460670,Rule=default-1358979215
Schwellenwert der WBRS-Sperrliste	6
Zulässiger WBRS-Grenzwert	6
WBRS aktiviert	1
Sichere Mobilität	0
L4-Datenverkehrsüberwachung aktiviert	0
Version der L4-Datenverkehrsüberwachungs-Sperrliste	default-0
Administrator-Sperrliste der L4-Datenverkehrsüberwachung	

Admin-Sperrlisten-Ports der L4-Datenverkehrsüberwachung	
L4-Datenverkehrsüberwachung zulässig	
Zulässige Ports der L4-Datenverkehrsüberwachung	
SBNP-Stichprobenfaktor	0,25
SBNP-Samplingfaktor (Volumen)	0,1
SurfControl SDK-Version (Legacy)	default-0
SurfControl Vollständige Datenbankversion (Legacy)	default-0
SurfControl Local Incremental Accumulation file version (Legacy)	default-0
Firestone-Engine-Version	default-210016
Firestone DAT-Version	V2-310003
AVC-Modul-Version	default-110076
AVC-DAT-Version	default-1377556980
Sophos-Modulversion	default-1310963572
Sophos-DAT-Version	default-0
Adaptives Scanning möglich	0
Adaptive Scanning Risk Score-Grenzwert	[10, 6, 3]
Grenzwert für adaptiven Scanfaktor	[5, 3, 2]
SOCKS aktiviert	0
Transaktionen gesamt	
Transaktionen gesamt	
Zulässige Transaktionen gesamt	
Gesamtzahl erkannter Malware-Transaktionen	
Gesamtzahl der durch die Admin-Richtlinie blockierten Transaktionen	
Gesamtzahl der durch WBRS-Bewertung blockierten Transaktionen	
Transaktionen mit hohem Risiko gesamt	
Von der Datenverkehrsüberwachung erkannte Transaktionen gesamt	
Gesamttransaktionen mit IPv6-Clients	
Gesamttransaktionen mit IPv6-Servern	
Gesamtanzahl an Transaktionen mit dem SOCKS-Proxy	
Gesamtanzahl an Transaktionen von Remote-Benutzern	
Gesamtanzahl an Transaktionen von lokalen Benutzern	
Gesamtzahl der zulässigen Transaktionen mit dem SOCKS-Proxy	
Gesamtanzahl an Transaktionen von lokalen Benutzern, die mit dem SOCKS-Proxy zulässig sind	
Gesamtzahl der Transaktionen von Remote-Benutzern, die mit dem SOCKS-Proxy zugelassen sind	
Gesamtzahl der blockierten Transaktionen über SOCKS-Proxy	
Gesamtzahl der Transaktionen lokaler	

Benutzer, die mit dem SOCKS-Proxy blockiert wurden	
Gesamtzahl der Transaktionen von Remote-Benutzern, die mit dem SOCKS-Proxy blockiert wurden	
Sekunden seit dem letzten Neustart	2843349
CPU-Auslastung (%)	9,9
RAM-Auslastung (%)	55,6
Festplattenauslastung (%)	57,5
Bandbreitennutzung (/Sek.)	15307
TCP-Verbindungen öffnen	2721
Transaktionen pro Sekunde	264
Client-Latenz	163
Cache-Trefferrate	21
Proxy-CPU-Auslastung	17
WBRS-WUC-CPU-Auslastung	2,5
Protokollieren der CPU-Auslastung	3,4
Reporting-CPU-Auslastung	3,9
Webroot-CPU-Auslastung	0
Sophos-CPU-Auslastung	0
McAfee CPU-Auslastung	0
Ausgabe des VMSTAT-Dienstprogramms (vmstat -z, vmstat -m)	
Anzahl der konfigurierten Zugriffsrichtlinien	32
Anzahl der konfigurierten benutzerdefinierten Webkategorien	32
Authentifizierungsanbieter	Einfach, NTLMSSP
Authentifizierungsbereiche	Hostname des Authentifizierungsanbieters, Protokoll und andere Konfigurationselemente

Statistiken werden pro Webanfrage freigegeben

Element	Beispieldaten	Standardbeteiligung	Eingeschränkte Beteiligung
Version	coeus 7.7.0-608		
Seriennummer			
SBNP-Samplingfaktor (Volumen)			
SBNP-Stichprobenfaktor (Rate)	1		
Ziel-IP und -Port		unverschleierte URL-Pfadsegmente	Hash-URL-Pfadsegr
Für Anti-Spyware ausgewählte Malware-Kategorie	Übersprungen		
WBRS-Bewertung	4,7		
Kategorie-Verdict für McAfee-Malware			
Referer-URL		unverschleierte URL-Pfadsegmente	Hash-URL-Pfadsegr
Inhaltstyp-ID			
ACL-Entscheidungstag	0		
Ältere Web-Kategorisierung			
CIWUC-Webkategorie und Entscheidungsquelle	{'src': 'req', 'cat': '1026'}		
AVC-Anwendungsname	Anzeigen und		

	Nachverfolgen
AVC-Anwendungstyp	Ad-Netzwerke
AVC-Anwendungsverhalten	Unsicher
Interne AVC-Ergebnisverfolgung	[0,1,1,1]
Nachverfolgung von Benutzeragenten über indizierte Datenstruktur	1

Erweiterte Malware-Statistiken pro Webanfrage

AMP-Statistiken

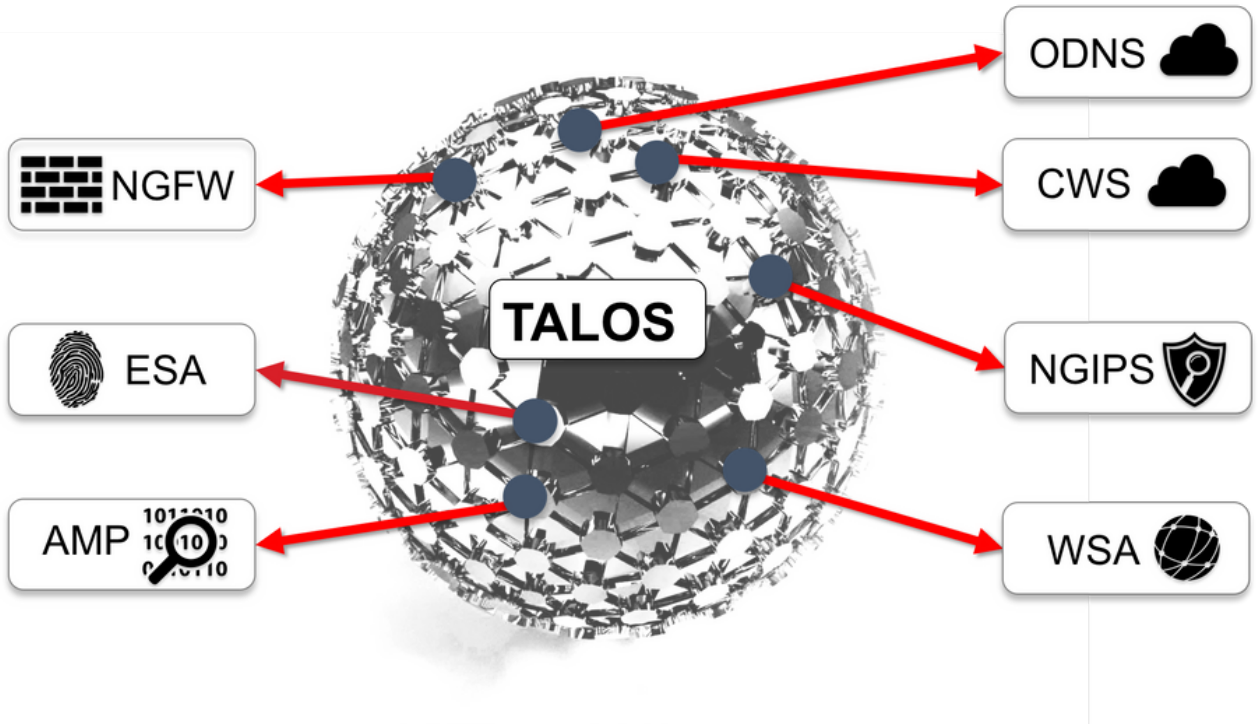
Verdict - der AMP-Reputationsabfrage	schädlich/sauber/unbekannt
Spyname - Name der erkannten Malware	[Trojaner-Test]
Bewertung - AMP zugewiesene Reputationsbewertung	[1-100]
Upload - Die AMP-Cloud hat angegeben, die Datei hochzuladen.	1
Dateiname - Name der Dateianlage	abcd.pdf

Feedback-Feed für Endbenutzer

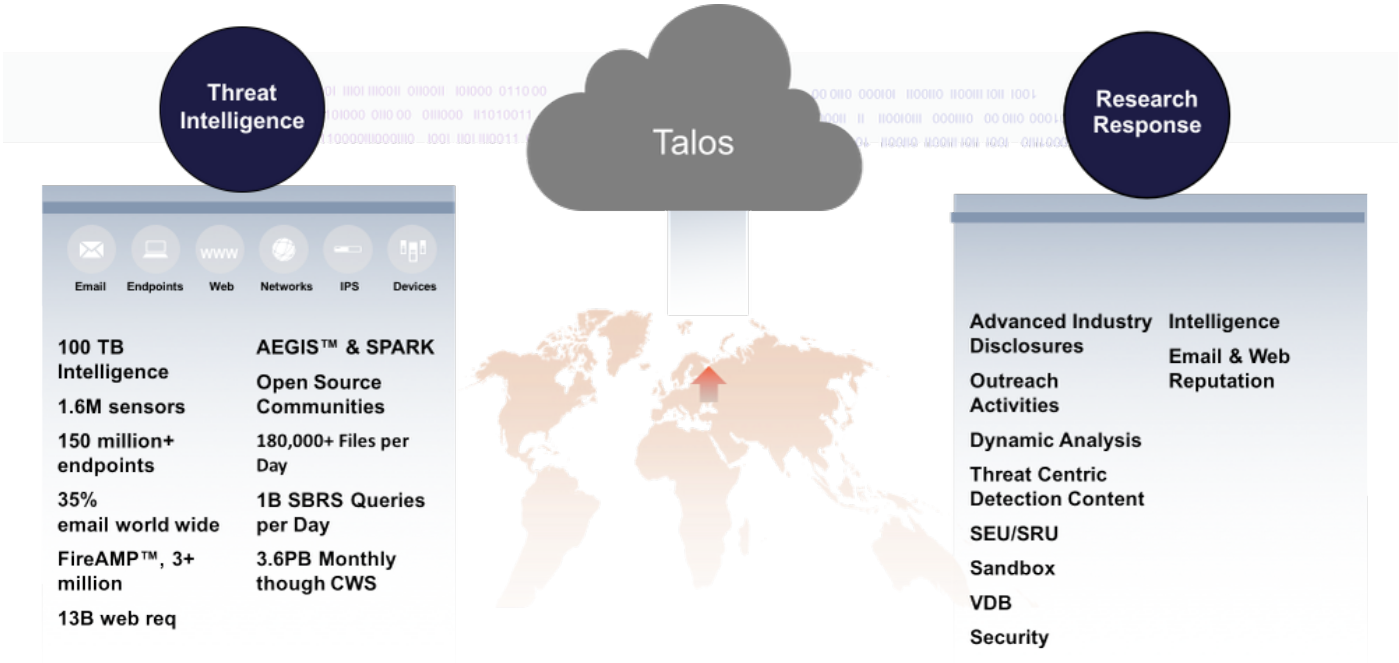
Freigegebene Statistiken pro Endbenutzer
Fehlkategorisierung Feedback

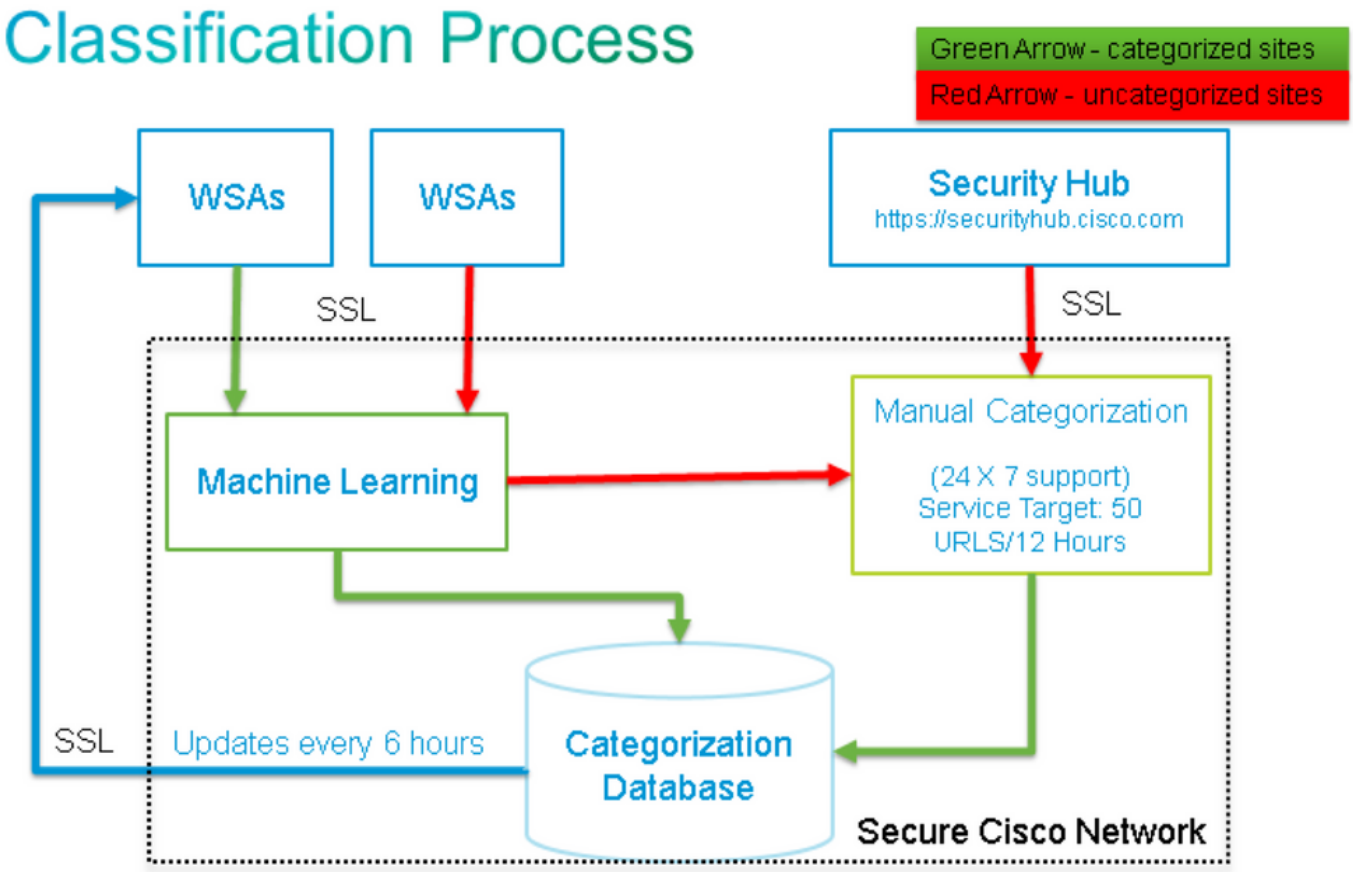
Element	Beispieldaten
Engine-ID (numerisch)	0
Legacy-Webkategorisierungscode	
CIWUC-Webkategorisierungsquelle	"resp"/"req"
CIWUC-Webkategorie	1026

Talos Detection-Inhalte



Bedrohungsorientiert





Zugehörige Informationen

- [Cisco Web Security Appliance - Produktseite]
- [Cisco Email Security Appliance - Produktseite]
- [Technischer Support und Dokumentation - Cisco Systems]