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

Inhoud

Inleiding

De producten van Cisco Web en Email Content Security kunnen telemetrie-gegevens teruggeven aan Cisco en Talos om de effectiviteit van webcategorisatie in Web Security Appliance (WSA) en de IP-reputatie aansluiten voor de e-mail security applicatie (ESA).

De telemetrie-gegevens voor de WSA en het ESA worden op "opt-in"-basis verstrekt.

De gegevens worden verzonden via binaire gecodeerde SSL gecodeerde pakketten. De onderstaande bijlagen bieden inzicht in de gegevens, de specifieke opmaak en beschrijvingen van de gegevens die worden doorgegeven. WebeBase Network Participation (WBNP) en SenderBase Network Participation (SBNP) gegevens zijn niet zichtbaar in een direct logbestand of bestandsindeling. Deze gegevens worden in gecodeerde vorm verzonden. Deze gegevens zijn nooit "in rust".

WSA - WebeBase Network Participation

Cisco erkent het belang om uw privacy te bewaren, en verzamelt of gebruikt geen persoonlijke of vertrouwelijke informatie zoals gebruikersnamen en pasgrepen. Daarnaast worden de bestands namen en URL eigenschappen die de hostname volgen, verduisterd om vertrouwelijkheid te garanderen.

Wanneer het op gedecrypteerde HTTPS transacties aankomt, ontvangt het SensorBase Network slechts het IP adres, de score van de web reputatie, en de URL categorie van de servernaam in het certificaat.

Raadpleeg de WSA User Guide voor meer informatie over de versie van AsyncOS voor webbeveiliging die momenteel op uw apparaat actief is. Zie "Het Cisco SensorBase Network" in de gebruikershandleiding.

ESA - SenderBase Network Participation

Klanten die aan het SenderBase Network deelnemen staan Cisco toe om geaggregeerde e-mailverkeersstatistieken over hun organisatie te verzamelen, waardoor het nut van de service voor iedereen die het gebruikt wordt wordt uitgebreid. Deelname is vrijwillig. Cisco verzamelt alleen summiere gegevens over berichteigenschappen en informatie over hoe verschillende typen berichten door Cisco apparaten werden verwerkt. Bijvoorbeeld, Cisco verzamelt de berichttekst of de berichtonderwerp niet. Persoonlijk identificeerbare informatie en informatie die uw organisatie identificeert, wordt vertrouwelijk gehouden.

Voor volledige informatie: pLees de ESA-gebruikershandleiding voor de versie van AsyncOS voor ESA security die momenteel op uw apparaat actief is. Zie het hoofdstuk "Deelname in netwerk SenderBase" in de gebruikershandleiding.

Algemene veiligheidsproblemen

Vraag:	Waar worden de verzamelde gegevens opgeslagen?
Antwoord:	De applicatie telemetrie wordt opgeslagen in Cisco Amerika-gebaseerde datacenters.
Vraag:	Wie heeft toegang tot de verzamelde en opgeslagen gegevens?
Antwoord:	De toegang is beperkt tot het personeel van Cisco SBG dat de gegevens analyseert/gebruikt o actieve intelligentie te creëren.
Vraag:	Wat is de bewaartijd van de verzamelde gegevens?
Antwoord:	Er bestaat geen beleid voor het bewaren en het verstrijken van gegevens met betrekking tot de telemetrie van het apparaat. Gegevens kunnen om verschillende redenen voor onbepaalde tijd worden bewaard of kunnen worden gewist, onder meer om niet te worden beperkt tot het neme van monsters/aggregatie, opslagbeheer, leeftijd, relevantie voor huidige/toekomstige bedreigin enz.
Vraag:	Zijn de klant serienummer(s) of het (de) openbare IP-adres(en) opgeslagen in de talencategorieën
Antwoord:	Nee, alleen URL en categorieën blijven behouden. Het WBNP-pakket bevat geen bron-IP-informa

Bediening

Hieronder, het soort gegevens (naar beschrijving) en een steekproefgegevens om de te verstrekken informatie aan te tonen:

- SBNP - Specifieke gegevenstypen (velden) en steekproefgegevens met betrekking tot e-mail security
- WBNP - Specifieke gegevenstypen (velden) en voorbeeldgegevens met betrekking tot Web Security
- Handeling voor detectie van bedreigingen - Algemeen overzicht van detectie van bedreigingen vanuit een operationeel perspectief

Deelname aan netwerk SenderBase (e-mail)

Statistieken per e-mail gedeeldapparaat

Item	Gegevens
MGA-identificatie	MGA 10012
Tijdstempel	Gegevens van 8.00 tot 8.05 uur op 1 juli 200
Softwareversienummers	MGA versie 4.7.0
Regelset versienummers	Anti-Spam Regel 102
Interval met anti-virusupdate	updates om de 10 minuten
Quarantine Size	500 MB
Quarantine Berichtenaantal	50 berichten in quarantaine
Drempel voor Virus Score	Bericht naar quarantaine op bedreigingsnivea of hoger
Aantal virusscores voor berichten die in quarantaine worden geplaatst	120
Aantal berichten dat in quarantaine wordt ingevoerd	30 (geeft een gemiddelde score van 4)
Maximale quarantainetijd	12 uur
Aantal quarantaineberichten van de uitbraak uitgesplitst naar de reden waarom zij in quarantaine zijn binnengebracht en zijn uitgezet, gecorreleerd met het resultaat van het antivirus	50 die in quarantaine werden geplaatst vanw .exe regel 30, die quarantaine verlaat door handmatige introductie, en alle 30 waren pos voor het virus
Aantal quarantaineberichten van de buitenwereld, uitgesplitst naar maatregelen bij het verlaten van de quarantaine	Na het verlaten van de quarantaine zijn er 10 berichten verschoven
In quarantaine werden meerdere tijdberichten gehouden	20 uur

Statistieken gedeeld per IP-adres

Item	Gegevens	Standaarddeel name	Beperkte deelname
Berichtenaantal in verschillende fasen van het apparaat	Gezien door een antivirusmotor: 100 Gezien door een anti-spammotor: 80		
Aantal scores en vonnissen tegen het sep en het antivirus	2.000 (som van anti-spamscores voor alle bekeken berichten)		
Aantal berichten dat verschillende combinaties van antisemiddelen en antivirale middelen bevat	100 berichten met de regels A en B 50 berichten worden alleen op regel A geplaatst		
Aantal verbindingen	20 MGT-verbindingen		
Aantal totale en ongeldige ontvangers	50 totale begunstigden 10 ongeldige ontvangers		
Bestandsnaam(en) hashed: a)	Een bestand <one-way-hash>.pif is	Niet-geharde	Bestandsna

	gevonden in een archiefbijlage met de naam <one-way-hash>.zip.	bestandsnaam hashed	
Verduisterde bestandsnaam(s): b)	Een bestand aaa0.aaa.pif is gevonden in een bestand aaa.zip.	Niet-geharde bestandsnaam	Verduisterde bestandsnaa
URL Hostname (c)	Er is een link gevonden in een bericht naar www.domain.com	Verbonden URL naam	Verouderde URL-naam
Verouderde URL (d)	Er werd een link gevonden in een bericht naar hostname www.domain.com, en het pad aaa000aa/aa00aaa.	Verbonden URL-pad	Verwante UI pad
Aantal berichten per spam en via het virus scannen	10 spam-positief 10 spam-negatief 5 spam verdachte 4 viruspositief 16 Virus-negatief 5 Virus onscannbaar		
Aantal berichten door verschillende vonnissen tegen spam en tegen het virus	500 spam, 300 ham		
Aantal berichten in groottebereiken	125 in 30K-35K bereik		
Aantal verschillende extensietypen	300 bijlagen ".exe"		
Correlatie van bijlagetypen, echt bestandstype en containertype	100 bijlagen met een ".doc"-extensie maar die in werkelijkheid ".exe" zijn 50 bijlagen zijn ".exe" extensies binnen een zip		
Correlatie van uitbreiding en reëel bestandstype met bijlagegrootte	30 bijlagen waren ".exe" binnen het bereik van 50-55K		
Aantal berichten door de Stochastische Steekproeven	14 berichten overgeslagen tot bemonstering 25 in de wachtrij voor steekproeven 50 gescande berichten uit de steekproef		
Aantal berichten dat de DMARC-verificatie heeft mislukt	34 berichten zijn niet geverifieerd door de DMARC		

Opmerkingen:

a) Bestandsnaam wordt in een hash (MD5) met 1 ingang gecodeerd.

b) De bestandsnamen worden in verduisterde vorm verstuurd, waarbij alle ASCII-letters in kleine letters ([a-z]) worden vervangen door "a", alle ASCII-letters ([A-Z]) worden vervangen door "A", alle UTF-8-tekens in meerdere letters worden vervangen door "x" (om privacy te bieden voor andere tekensets), alle ASCII-tekens ([0-9]) worden vervangen.

(c) URL hostname wijst naar een webserver die inhoud biedt, net zoals een IP-adres doet. Er is geen vertrouwelijke informatie, zoals gebruikersnamen en wachtwoorden, inbegrepen.

d) URL-informatie na de hostname wordt verduisterd om ervoor te zorgen dat geen persoonlijke informatie van de gebruiker wordt bekendgemaakt.

Statistieken gedeeld per SDS-client

Item	Gegevens
TimeStamp	
Clientversie	
Aantal aan de klant gedane verzoeken	
Aantal verzoeken van de SDS-client	
Tijdresultaten voor DNS-links	
Resultaten van de responsietijd van de server	
Tijd om verbinding met server te maken	
Aantal aangelegde verbindingen	
Aantal gelijktijdige open verbindingen met de server	
Aantal serviceaanvragen bij WBRS	
Aantal verzoeken dat betrekking heeft op de lokale WBRS-cache	
Grootte van lokale WBRS-cache	
Resultaten van de responsietijd van externe WBRS	

AMP SBNP-telemetingsgegevens

Notatie	Gegevens
amp_vonnissen": { ("vonnis", "spyname", "score", "geüpload", "file_name"), ("vonnis", "spyname", "score", "geüpload", "file_name"), ("vonnis", "spyname", "score", "geüpload", "file_name"), ... ("vonnis", "spyname", "score", "geüpload", "file_name"), >	

Beschrijving	
Veroordeling - van de reputatie van de AMP-partij	kwaadaardig/schoon/onbekend
Spyname - Naam van de gedetecteerde malware	[Trojan-test]
Score - AMP toegewezen reputatiescore	[1-100]
Upload - AMP-cloud aangegeven om het bestand te uploaden	1
Bestandsnaam - Naam van de bestandsbijlage	abcd.pdf

Webex-netwerkdeelname (WebBase)

Statistieken gedeeld per webverzoek

Item	Gegevens	Standaarddeelname	Beperkte deelname
Versie	reus 7.7.0-608		
Serienummer			
SBNP-bemonsteringsfactor (volume)			
SBNP-bemonsteringsfactor (snelheid)	1		
IP en poort op bestemming		niet-verduisterde URL-segmenten	hashed URL-padsegmenten
Voor anti-spyware-malware categorie	Geskipt		
WBRS Score	4.7		
Uitspraak in categorie McAfee malware			
URL		niet-verduisterde URL-segmenten	hashed URL-padsegmenten

Content Type-id	
ACL-beslissingslabel	0
Verouderde webclassificatie	
CIWUC-webcategorie en -besluitvormingsbron	{'src': 'req', 'kat': "1026"}
AVC-toepassingsnaam	Bestanden en tracering
AVC-app	Ad-netwerken
AVC-toepassingsgedrag	onveilig
Interne AVC-resultaattracering	[0,1,1,1]
Volgorde gebruikersagent via geïndexeerde gegevensstructuur	3

Geavanceerde Malware Statistieken per webverzoek

AMP-statistieken

Veroordeling - van de reputatie van de AMP-partij	kwaadaardig/schoon/onbekend
Spyname - Naam van de gedetecteerde malware	[Trojan-test]
Score - AMP toegewezen reputatiescore	[1-100]
Upload - AMP-cloud aangegeven om het bestand te uploaden	1
Bestandsnaam - Naam van de bestandsbijlage	abcd.pdf

Feedback van eindgebruiker

Statistieken gedeeld per eindgebruiker categorisering Feedback

Item	Gegevens
Engine-id (numeriek)	0
Verouderde webcategoriseringscode	
CIWUC-bron voor webcategorieën	‘resp’ / ‘req’
CIWUC-webcategorie	1026

Verstrekking van voorbeeldgegevens - Standaarddeelname

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

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

Verstrekking van voorbeeldgegevens - Beperkte deelneming

- Oorspronkelijk verzoek van de cliënt: www.gunexams.com/Non-Restricted-FREE-Practice-Exams

- Bericht ingelogd (in telemetrieserver): http://www.gunexams.com/76bd845388e0

Volledig WBNP-decoder

Statistieken gedeeld per Cisco-applicatie

Item	Gegevens
Versie	reus 7.7.0-608
Serienummer	0022190B6ED5-XYZ1YZ2
Model	S660-software
Webroot ingeschakeld	1
AVC ingeschakeld	1
Soob ingeschakeld	0
Activering van responscategorie	1
Anti-spyware Engine ingeschakeld	standaard-2001005008
Anti-Spyware SSE-versie	standaard-2001005008
Antispyware Spycat-versie	standaard 8640
Anti-spyware URL Blocklist DAT-versie	
Anti-spyware URL phishing DAT-versie	
DAT-versie van anti-spyware Cookies	
Anti-spyware-domeinblokkering ingeschakeld	0
Drempel voor risico's tegen spyware	90
McAfee ingeschakeld	0
Versie McAfee Engine	
McAfee DAT-versie	standaard 5688
WBNP-Detail-niveau	2
WBRS Engine versie	vrieskist6-i386-30036
WBRS-componentversies	categorieën=v2-1337979188,ip=default-1379460997,sleutelwoord=v2-1312487822,prefixcat=v2-1379460670 regel=standaard-1358979215
Drempel WBRS-Blocklist	-6
Drempel voor WBRS-Allowlist	6
WBRS ingeschakeld	1
Secure Mobility ingeschakeld	0
L4 Traffic Monitor ingeschakeld	0
L4 Traffic Monitor Blocklist versie	standaard-0
L4 Traffic Monitor Admin-blokkeringslijst	
L4 Traffic Monitor Admin Blocklist poorten	
L4-controlelijst voor verkeer	
L4-poorten voor controllering van verkeer	
SBNP-bemonsteringsfactor	0.25
SBNP-bemonsteringsfactor (volume)	0.1
SurfControl SDK-versie (verleden)	standaard-0
SurfControl Full Database-versie (nalatenschap)	standaard-0
SurfControl lokale stapeling (nalatenschap)	standaard-0
Firestone Engine versie	standaard 210016
Firestone DAT-versie	v2-310003
AVC Engine versie	standaard-10076
AVC DAT-versie	standaard-137556980
Sofos Engine versie	standaard-1310963572
Sfos DAT-versie	standaard-0

Adaptieve scannen ingeschakeld	0
Drempel voor adaptieve scans	[10, 6, 3]
Drempel voor adaptieve scanfactor	[5, 3, 2]
SOCKS ingeschakeld	0
Totale transacties	
Totale transacties	
Totale toegestane transacties	
Totale aantal herkende Malware-transacties	
Totale transacties geblokkeerd door Admin-beleid	
Totale transacties geblokkeerd door WBRS-score	
Totale transacties met hoog risico	
Totale door Traffic Monitor gedetecteerde transacties	
Totale transacties met IPv6-clients	
Totale transacties met IPv6-servers	
Totale transacties met SOCKS-proxy	
Totale transacties van externe gebruikers	
Totale transacties van lokale gebruikers	
Totale toegestane transacties met SOCKS-proxy	
Totale transacties van lokale gebruikers toegestaan met behulp van SOCKS-proxy	
Totale transacties van externe gebruikers toegestaan met behulp van SOCKS-proxy	
Totale transacties geblokkeerd met behulp van SOCKS-proxy	
Totale transacties van lokale gebruikers die worden geblokkeerd via SOCKS-proxy	
Totale transacties van externe gebruikers geblokkeerd via SOCKS-proxy	
seconden sinds laatste herstart	2843349
CPU-gebruik (%)	9.9
RAM-benutting (%)	55.6
Gebruik vaste schijf (%)	57.5
Bandbreedtesysteem (/sec)	15307
TCP-verbindingen openen	2721
Transacties per seconde	264
Clientmelding	163
Snelheid cache	21
Gebruik van Proxy-CPU’s	17
Gebruik van WBRS WUC CPU’s	2.5
Gebruik van opslagCPU’s	3.4
Gebruik van CPU’s	3.9
Gebruik van Webex CPU’s	0
Gebruik van Sfos CPU	0
Gebruik van McAfee CPU’s	0
vmstat bruikbaarheidsoutput (vmstat -z, vmstat -m)	
Aantal ingesteld toegangsbeleid	32
Aantal geconfigureerde aangepaste webcategorieën	32

Verificatieprovider	Basis, NTLMSSP
Verificatieresultaten	Hostnaam voor verificatieproviders, Protocol en andere configuratieelementen

Statistieken gedeeld per webverzoek

Item	Gegevens	Standaarddeelname	Beperkte deelname
Versie	reus 7.7.0-608		
Serienummer			
SBNP-bemonsteringsfactor (volume)			
SBNP-bemonsteringsfactor (snelheid)	1		
IP en poort op bestemming		niet-verduisterde URL-segmenten	hashed URL-padsegmenten
Voor anti-spyware-malware categorie	Geskipt		
WBRS Score	4.7		
Uitspraak in categorie McAfee malware			
URL		niet-verduisterde URL-segmenten	hashed URL-padsegmenten
Content Type-id			
ACL-beslissingslabel	0		
Verouderde webclassificatie			
CIWUC-webcategorie en -besluitvormingsbron	{'src': 'req', 'kat': "1026"}		
AVC-toepassingsnaam	Bestanden en tracering		
AVC-app	Ad-netwerken		
AVC-toepassingsgedrag	onveilig		
Interne AVC-resultaattracering	[0,1,1,1]		
Volgorde gebruikersagent via geïndexeerde gegevensstructuur	3		

Geavanceerde Malware Statistieken per webverzoek

AMP-statistieken

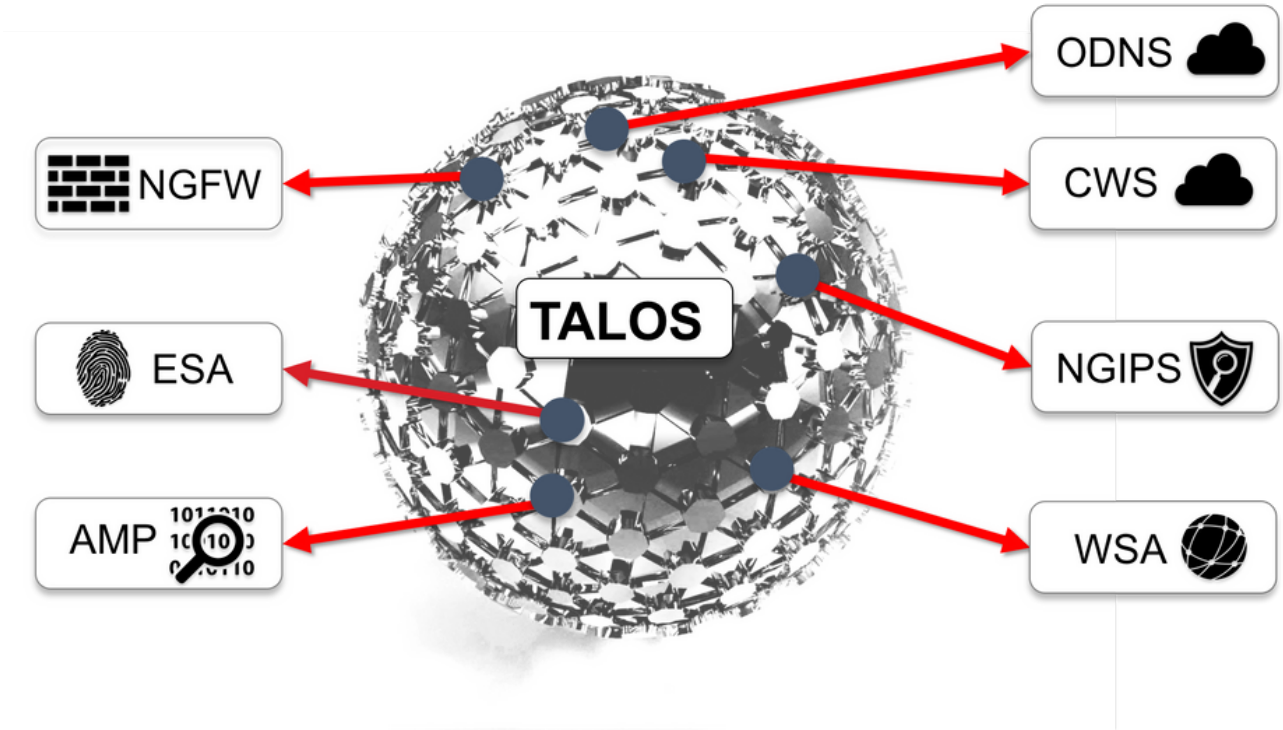
Veroordeling - van de reputatie van de AMP-partij	kwaadaardig/schoon/onbekend
Spyname - Naam van de gedetecteerde malware	[Trojan-test]
Score - AMP toegewezen reputatiescore	[1-100]
Upload - AMP-cloud aangegeven om het bestand te uploaden	1
Bestandsnaam - Naam van de bestandsbijlage	abcd.pdf

Feedback van eindgebruiker

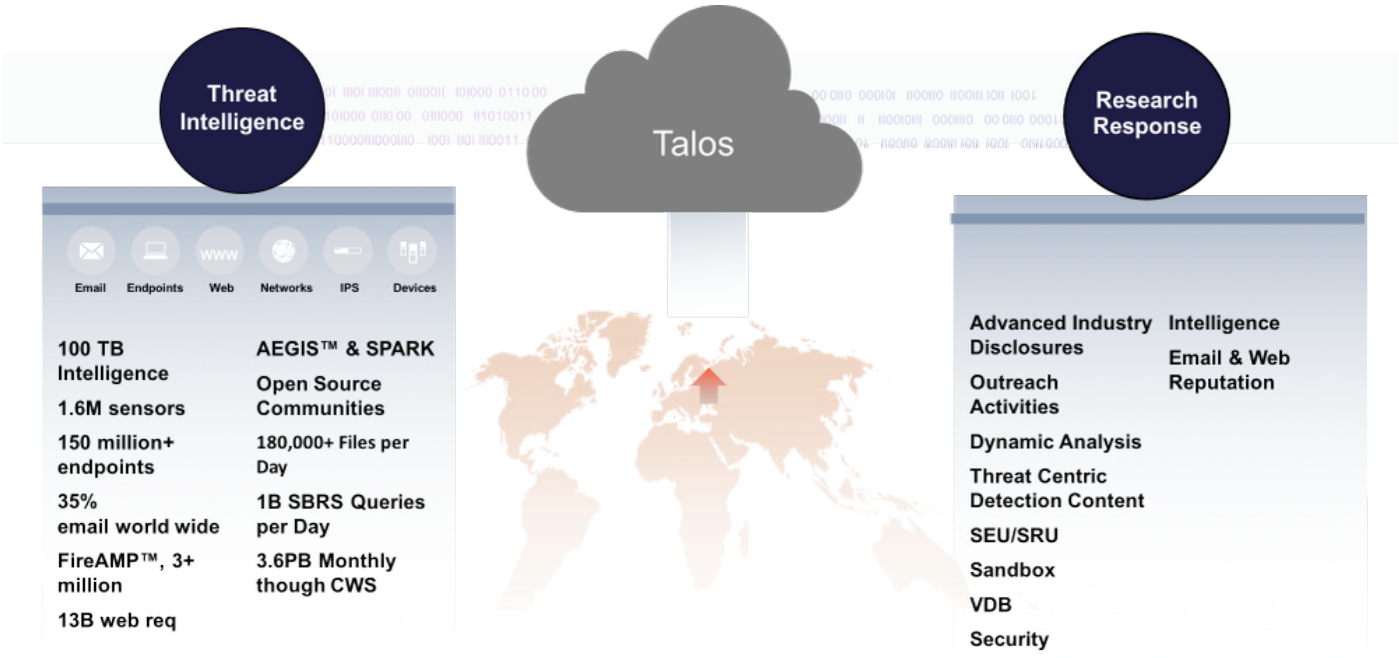
Statistieken gedeeld per eindgebruiker categorisering Feedback

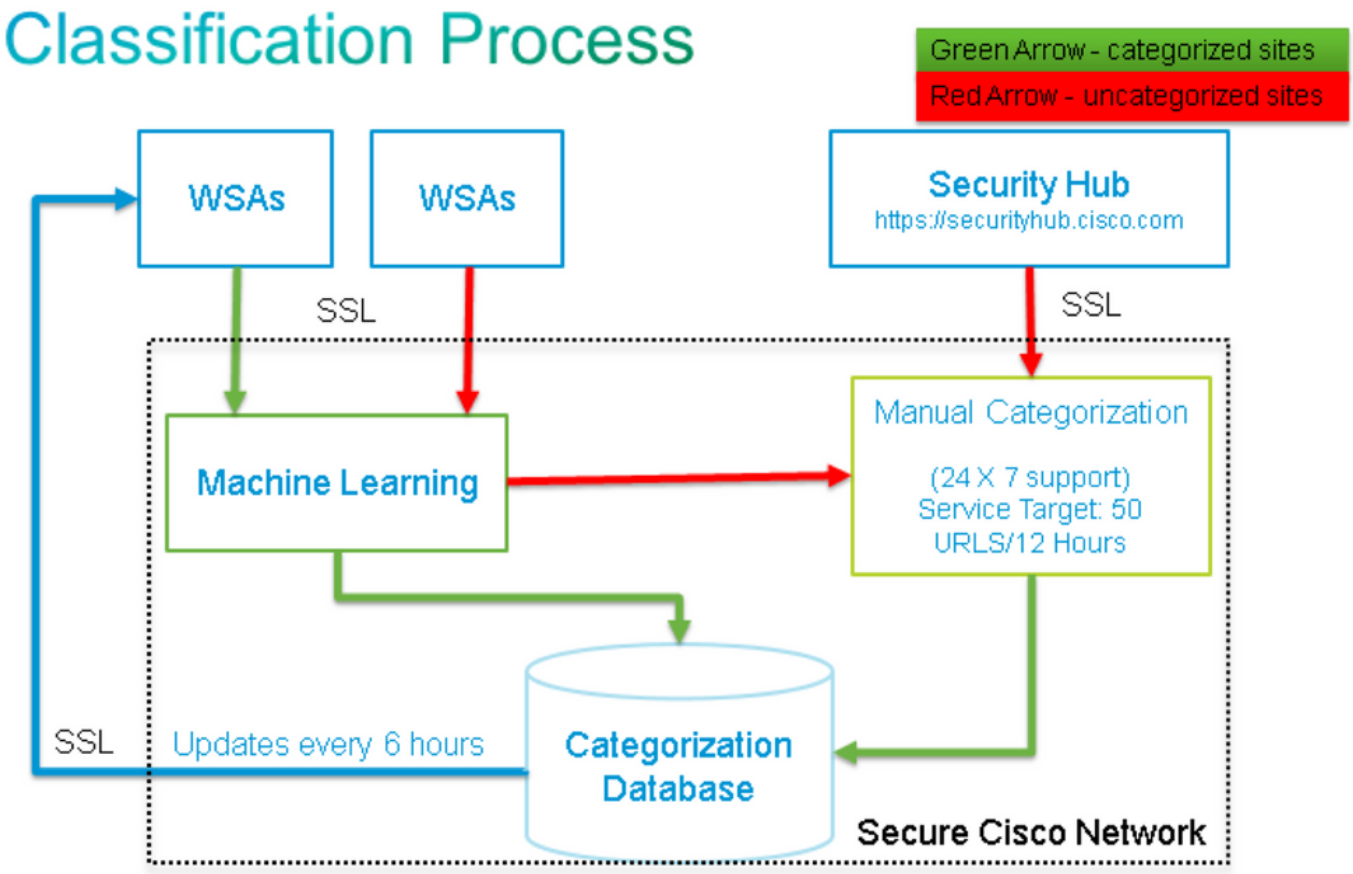
Item	Gegevens
Engine-id (numeriek)	0
Verouderde webcategoriseringscode	
CIWUC-bron voor webcategorieën	‘resp’ / ‘req’
CIWUC-webcategorie	1026

Inhoud voor talendetectie



Bedreigingsgerichte





Gerelateerde informatie

- [Cisco web security applicatie - productpagina]
- [Cisco e-mail security applicatie - productpagina]
- [Technische ondersteuning en documentatie – Cisco Systems]