Partecipazione alla rete di base Web (WBNP) e partecipazione alla rete di base mittente (SBNP)

Sommario

[Introduzione](#)
[WSA - Partecipazione alla rete WebBase](#)
[ESA - Partecipazione rete SenderBase](#)
[Domande frequenti (FAQ)](#)
[Operazione](#)
[Partecipazione alla rete SenderBase (e-mail)](#)
[Statistiche condivise per appliance di posta elettronica](#)
[Statistiche condivise per indirizzo IP](#)
[Statistiche condivise per client SDS](#)
[Dati di telemetria SBNP AMP](#)
[Partecipazione alla rete WebBase (Web)](#)
[Statistiche condivise per richiesta Web](#)
[Statistiche malware avanzate per richiesta Web](#)
[Feedback statistiche feedback utente finale](#)
[Dati di esempio forniti - Partecipazione standard](#)
[Dati di esempio forniti - Partecipazione limitata](#)
[Decodifica WBNP completa](#)
[Statistiche condivise per richiesta Web](#)
[Statistiche malware avanzate per richiesta Web](#)
[Feedback statistiche feedback utente finale](#)
[Contenuto rilevamento talos](#)
[Focalizzato sulle minacce](#)
[Informazioni correlate](#)

Introduzione

I prodotti Cisco Web and Email Content Security possono restituire dati di telemetria a Cisco e Talos per aumentare l'efficacia della categorizzazione Web in Web Security Appliance (WSA) e collegare la reputazione IP di Email Security Appliance (ESA).

I dati di telemetria sono forniti per il WSA e l'ESA su base "opt-in".

I dati vengono trasmessi tramite pacchetti crittografati SSL con codifica binaria. Gli allegati forniti di seguito forniscono informazioni dettagliate sui dati, sulla formattazione specifica e sulle descrizioni dei dati trasmessi. I dati WBNP (WebBase Network Participation) e SBNP (SenderBase Network Participation) non sono visualizzabili in un registro diretto o in un formato di file. Questi dati vengono trasmessi in forma crittografata. In nessun momento questi dati sono "inattivi".

WSA - Partecipazione alla rete WebBase

Cisco riconosce l'importanza di mantenere la privacy degli utenti e non raccoglie né utilizza informazioni personali o riservate, quali nomi utente e passphrase. Inoltre, i nomi dei file e gli attributi URL che seguono il nome host vengono celati per garantire la riservatezza.

Quando si tratta di transazioni HTTPS decrittografate, la rete SensorBase riceve solo l'indirizzo IP, il punteggio della reputazione Web e la categoria URL del nome server nel certificato.

Per informazioni complete, consultare la Guida dell'utente di WSA per la versione di AsyncOS for Web Security attualmente in esecuzione sull'accessorio. Consultare "Cisco SensorBase Network" nel Manuale dell'utente.

ESA - Partecipazione rete SenderBase

I clienti che partecipano alla rete SenderBase consentono a Cisco di raccogliere statistiche aggregate sul traffico e-mail relativo alla propria organizzazione, aumentando l'utilità del servizio per tutti gli utenti che lo utilizzano. La partecipazione è volontaria. Cisco raccoglie solo dati di riepilogo sugli attributi dei messaggi e informazioni su come i diversi tipi di messaggi sono stati gestiti dalle appliance Cisco. Ad esempio, Cisco non raccoglie il corpo del messaggio o l'oggetto del messaggio. Le informazioni personali e quelle che identificano la tua azienda rimangono confidenziali.

Per informazioni complete, pEsaminare la EGuida per l'utente SA per la versione di AsyncOS for ESA Security attualmente in esecuzione sull'accessorio. Consultare il capitolo "SenderBase Network Participation" del Manuale dell'utente.

Domande frequenti (FAQ)

Domanda:	Dove vengono memorizzati i dati raccolti?
Risposta.	La telemetria delle appliance è memorizzata nei centri dati Cisco negli Stati Uniti.
Domanda:	Chi ha accesso ai dati raccolti e memorizzati?
Risposta.	L'accesso è limitato al personale Cisco SBG che analizza/utilizza i dati per creare informazioni pratiche.
Domanda:	Qual è il tempo di conservazione dei dati raccolti?
Risposta.	Non esistono regole di conservazione/scadenza dei dati relative alla telemetria dell'accessorio dati possono essere conservati per un periodo di tempo indefinito o possono essere eliminati p vari motivi, tra cui il sottocampionamento/aggregazione, la gestione dello storage, l'età, la rilev per le minacce attuali e future, ecc.
Domanda:	I numeri di serie o gli indirizzi IP pubblici dei clienti sono memorizzati nel database di classifica Talos?
Risposta.	No, vengono mantenute solo le categorie e gli URL. Il pacchetto WBNP non contiene informaz sull'IP di origine.

Operazione

Di seguito è riportata l'operazione dettagliata, il tipo di dati (per descrizione) e un campione di dati per dimostrare le informazioni da trasmettere:

- SBNP - Tipi di dati specifici (campi) e dati di esempio relativi a Email Security

- WBNP - Tipi di dati specifici (campi) e dati di esempio correlati alla sicurezza Web
- Operazione di rilevamento delle minacce: panoramica generale del rilevamento delle minacce da un punto di vista operativo

Partecipazione alla rete SenderBase (e-mail)

Statistiche condivise per e-mailapparecchiatura

Articolo	Dati di esempio
Identificatore MGA	MGA 10012
Timestamp	Dati dalle 8.00 alle 8.05 del 1 luglio 2005
Numeri di versione del software	MGA versione 4.7.0
Numeri di versione set di regole	Set di regole antispam 102
Intervallo di aggiornamento antivirus	Aggiornamenti ogni 10 minuti
Dimensioni quarantena	500 MB
Conteggio messaggi quarantena	50 messaggi attualmente in quarantena
Soglia punteggio virus	Invia messaggi in quarantena al livello di ris 3 o superiore
Somma dei punteggi dei virus per i messaggi in quarantena	120
Numero di messaggi in quarantena	30 (rendimento punteggio medio di 4)
Durata massima quarantena	12 ore
Numero di messaggi di quarantena relativi a focolai, suddivisi in base al motivo per cui sono entrati e sono usciti dalla quarantena, in correlazione con il risultato dell'antivirus	50 entra in quarantena a causa della regola 30 esce dalla quarantena a causa del rilasc manuale, e tutti e 30 sono stati virus positiv
Numero di messaggi di quarantena di focolai suddivisi in base all'azione intrapresa all'uscita dalla quarantena	In 10 messaggi gli allegati sono stati rimoss dopo aver lasciato la quarantena
Somma dei messaggi di ora in quarantena	20 ore

Statistiche condivise per indirizzo IP

Articolo	Dati di esempio	Partecipazione standard	Partecipazio limitata
Conteggio dei messaggi nelle varie fasi dell'accessorio	Visto dal motore antivirus: 100 Visualizzato dal motore antispam: 80		
Somma dei punteggi e dei verdetti relativi a protezione da posta indesiderata e antivirus	2.000 (somma dei punteggi anti-spam per tutti i messaggi visualizzati)		
Numero di messaggi che hanno raggiunto diverse combinazioni di regole antispam e antivirus	100 messaggi rispettano le regole A e B 50 messaggi raggiungono solo la regola A		
Numero di connessioni	20 connessioni SMTP		
Numero di destinatari totali e non validi	50 destinatari totali 10 destinatari non validi		
Nomi file con hash: (a)	Èstato trovato un file <one-way-hash>.pif in un allegato di archivio denominato <one-way-hash>.zip.	Nome file non disattivato	Nome file co hash
Nomi file offuscati: (b)	Èstato trovato un file aaaaaa0.aaa.pif all'interno di un file aaaaaa.zip.	Nome file non disattivato	Nome file offuscato
URL Nome host (c)	Èstato trovato un collegamento in un messaggio a www.domain.com	Nome host URL non crittografato	Nome host U offuscato

Percorso URL offuscato (d)	Èstato trovato un collegamento in un messaggio al nome host www.domain.com, con il percorso aaa000aa/aa00aaa.	Percorso URL non nascosto	Percorso UR offuscato
Numero di messaggi per posta indesiderata e risultati della ricerca virus	10 Posta indesiderata positiva 10 Posta indesiderata negativa 5 sospetto di posta indesiderata 4 Virus positivi 16 Virus Negativo 5 Virus non analizzabile		
Numero di messaggi inviati da diversi verdetti antispam e antivirus	500 spam, 300 ham		
Numero di messaggi in intervalli di dimensioni	Range 30K-35K da 125 pollici		
Numero di tipi di estensione diversi	300 allegati ".exe"		
Correlazione tra tipi di allegato, tipo di file true e tipo di contenitore	100 allegati con estensione ".doc" ma che in realtà sono ".exe" 50 allegati sono estensioni ".exe" all'interno di un file zip		
Correlazione tra estensione e tipo di file true e dimensioni dell'allegato	30 allegati erano ".exe" nell'intervallo 50-55K		
Numero di messaggi per risultati del campionamento stocastico	14 messaggi senza campionamento 25 messaggi in coda per il campionamento 50 messaggi analizzati dal campionamento		
Numero di messaggi per i quali la verifica DMARC non è riuscita	34 messaggi non hanno superato la verifica DMARC		

Note:

(a) I nomi file verranno codificati in un hash a una via (MD5).

(b) I nomi dei file vengono inviati in forma offuscata, con tutte le lettere ASCII minuscole ([a-z]) sostituite da "a", tutte le lettere ASCII maiuscole ([A-Z]) sostituite da "A", tutti i caratteri UTF-8 multibyte sostituiti da "x" (per garantire la privacy per altri set di caratteri) e tutte le cifre ASCII ([0-9]) sostituite.

(c) I nomi host degli URL puntano a un server Web che fornisce contenuti, proprio come un indirizzo IP. Non sono incluse informazioni riservate, come nomi utente e password.

d) Le informazioni URL che seguono il nome dell'host sono celate per evitare che vengano rivelate informazioni personali dell'utente.

Statistiche condivise per client SDS

Articolo	Dati di esempio
Timestamp	
Versione client	
Numero di richieste effettuate al client	
Numero di richieste effettuate dal client SDS	

Risultati temporali per le ricerche DNS	
Risultati tempo di risposta server	
Tempo per stabilire la connessione al server	
Numero di connessioni stabilite	
Numero di connessioni aperte simultanee al server	
Numero di richieste di servizio a WBRS	
Numero di richieste che hanno raggiunto la cache WBRS locale	
Dimensioni della cache WBRS locale	
Risultati dei tempi di risposta da WBRS remoto	

Dati di telemetria SBNP AMP

Formato	Dati di esempio
amp_verdicts': { ("verdict", "spyname", "score", "uploaded", "nome_file"), ("verdict", "spyname", "score", "uploaded", "file_name"), ("verdict", "spyname", "score", "uploaded", "file_name"), ... ("verdict", "spyname", "score", "uploaded", "file_name"), }	
Descrizione	
Verdetto - della query sulla reputazione AMP	dannoso/pulito/sconosciuto
Spyname: nome del malware rilevato	[Trojan test]
Punteggio - Punteggio reputazione assegnato da AMP	[1-100]
Upload - cloud AMP indicato per caricare il file	1
Nome file - Nome del file allegato	abcd.pdf

Partecipazione alla rete WebBase (Web)

Statistiche condivise per richiesta Web

Articolo	Dati di esempio	Partecipazione standard	Partecipazione limita
Version	coeus 7.7.0-608		
Numero di serie			
Fattore di campionamento SBNP (volume)			
Fattore di campionamento SBNP (frequenza)	1		
IP e porta di destinazione		segmenti di percorso URL non offuscati	segmenti di percorso con hash
Categoria di malware scelta per l'antispyware	Ignorato		
Punteggio WBRS	4.7		
Verdetto categoria malware McAfee			
URL riferimento		segmenti di percorso URL non offuscati	segmenti di percorso con hash
ID tipo di contenuto			

Tag di decisione ACL	0
Categorizzazione Web legacy	
Categoria Web e origine decisione CIWUC	{'src': "req", "cat": '1026'}
Nome app AVC	Annunci e rilevamento
Tipo di app AVC	Reti pubblicitarie
Comportamento app AVC	Non sicuro
Tracciamento risultati AVC interno	[0,1,1,1]
Tracciamento agente utente tramite struttura di dati indicizzata	3

Statistiche malware avanzate per richiesta Web

Statistiche AMP

Verdetto - della query sulla reputazione AMP	dannoso/pulito/sconosciuto
Spyname: nome del malware rilevato	[Trojan test]
Punteggio - Punteggio reputazione assegnato da AMP	[1-100]
Upload - cloud AMP indicato per caricare il file	1
Nome file - Nome del file allegato	abcd.pdf

Feedback statistiche feedback utente finale

Statistiche condivise per utente finale
Classificazione errata Feedback

Articolo	Dati di esempio
ID motore (numerico)	0
Codice di categorizzazione Web legacy	
Origine classificazione Web CIWUC	"resp" / "req"
Categoria Web CIWUC	1026

Dati di esempio forniti - Partecipazione standard

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

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

Dati di esempio forniti - Partecipazione limitata

- Richiesta originale dal client: www.gunexams.com/Non-Restricted-FREE-Practice-Exams
- Messaggio registrato (nel server di telemetria): http://www.gunexams.com/76bd845388e0

Decodifica WBNP completa

Statistiche condivise per appliance Cisco

Articolo	Dati di esempio
Version	coeus 7.7.0-608
Numero di serie	0022190B6ED5-XYZ1YZ2
Modello	S660
Webroot abilitata	1
AVC abilitato	1
Sophos abilitato	0
Categorizzazione lato risposta abilitata	1
Motore antispyware abilitato	default-2001005008
Versione SSE antispyware	default-2001005008
Versione definizioni antispyware	default-8640
Versione DAT elenco di blocco URL antispyware	
Versione DAT di phishing URL antispyware	
Versione DAT cookie antispyware	
Blocco del dominio antispyware abilitato	0
Soglia di rischio di minaccia antispyware	90
McAfee abilitato	0
Versione McAfee Engine	
Versione McAfee DAT	default-5688
Livello dettagli WBNP	2
Versione motore WBRS	freebsd6-i386-300036
Versioni componente WBRS	categories=v2-1337979188,ip=default-1379460997,keyword=v2-1312487822,prefix=v2-1379460670,rule=default-1358979215
Soglia elenco di blocco WBRS	-6
Soglia elenco consentito WBRS	6
WBRS abilitato	1
Mobilità protetta abilitata	0
Monitoraggio traffico L4 abilitato	0
Versione L4 Traffic Monitor Blocklist	predefinito-0
Blocco amministratore L4 Traffic Monitor	
Porte L4 Traffic Monitor Admin Blocklist	
L4 Traffic Monitor Allowlist	
Porte consentite L4 Traffic Monitor	
Fattore di campionamento SBNP	0.25
Fattore di campionamento SBNP (volume)	0.1
Versione di SurfControl SDK (legacy)	predefinito-0
Versione completa del database di SurfControl (legacy)	predefinito-0
Versione del file di accumulazione incrementale locale di SurfControl (legacy)	predefinito-0
Versione di Firestone Engine	default-210016
Versione Firestone DAT	v2-310003
Versione motore AVC	default-110076
Versione AVC DAT	default-137756980
Versione Sophos Engine	default-1310963572
Versione Sophos DAT	predefinito-0

Scansione adattiva abilitata	0
Soglia punteggio rischio scansione adattiva	[10, 6, 3]
Soglia fattore di carico scansione adattiva	[5, 3, 2]
SOCKS abilitato	0
Totale transazioni	
Totale transazioni	
Totale transazioni consentite	
Totale transazioni rilevate da malware	
Totale transazioni bloccate dai criteri di amministrazione	
Totale transazioni bloccate dal punteggio WBRS	
Totale transazioni ad alto rischio	
Totale transazioni rilevate da Monitoraggio traffico	
Totale transazioni con client IPv6	
Totale transazioni con server IPv6	
Totale transazioni che utilizzano il proxy SOCKS	
Totale transazioni da utenti remoti	
Totale transazioni da utenti locali	
Totale transazioni consentite tramite proxy SOCKS	
Totale transazioni dagli utenti locali consentite tramite il proxy SOCKS	
Totale transazioni da utenti remoti consentite tramite il proxy SOCKS	
Totale transazioni bloccate tramite proxy SOCKS	
Totale transazioni da utenti locali bloccati tramite proxy SOCKS	
Totale transazioni da utenti remoti bloccati tramite proxy SOCKS	
Secondi dall'ultimo riavvio	2843349
Utilizzo CPU (%)	9.9
Utilizzo RAM (%)	55.6
Utilizzo disco rigido (%)	57.5
Utilizzo larghezza di banda (/sec)	15307
Apri connessioni TCP	2721
Transazioni al secondo	264
Latenza client	163
Frequenza riscontri nella cache	21
Utilizzo CPU proxy	17
Utilizzo CPU WBRS WUC	2.5
Registrazione utilizzo CPU	3.4
Report utilizzo CPU	3.9
Utilizzo CPU Webroot	0
Utilizzo CPU Sophos	0
Utilizzo CPU McAfee	0
output utilità vmstat (vmstat -z, vmstat -m)	
Numero di criteri di accesso configurati	32
Numero di categorie Web personalizzate configurate	32

Provider di autenticazione	Base, NTLMSSP
Realm di autenticazione	Nome host, protocollo e altri elementi di configurazione del provider di autenticazione

Statistiche condivise per richiesta Web

Articolo	Dati di esempio	Partecipazione standard	Partecipazione limita
Version	coeus 7.7.0-608		
Numero di serie			
Fattore di campionamento SBNP (volume)			
Fattore di campionamento SBNP (frequenza)	1		
IP e porta di destinazione		segmenti di percorso URL non offuscati	segmenti di percorso con hash
Categoria di malware scelta per l'antispyware	Ignorato		
Punteggio WBRS	4.7		
Verdetto categoria malware McAfee			
URL riferimento		segmenti di percorso URL non offuscati	segmenti di percorso con hash
ID tipo di contenuto			
Tag di decisione ACL	0		
Categorizzazione Web legacy			
Categoria Web e origine decisione			
CIWUC	{'src': "req", "cat": '1026'}		
Nome app AVC	Annunci e rilevamento		
Tipo di app AVC	Reti pubblicitarie		
Comportamento app AVC	Non sicuro		
Tracciamento risultati AVC interno	[0,1,1,1]		
Tracciamento agente utente tramite struttura di dati indicizzata	3		

Statistiche malware avanzate per richiesta Web

Statistiche AMP

Verdetto - della query sulla reputazione AMP	dannoso/pulito/sconosciuto
Spyname: nome del malware rilevato	[Trojan test]
Punteggio - Punteggio reputazione assegnato da AMP	[1-100]
Upload - cloud AMP indicato per caricare il file	1
Nome file - Nome del file allegato	abcd.pdf

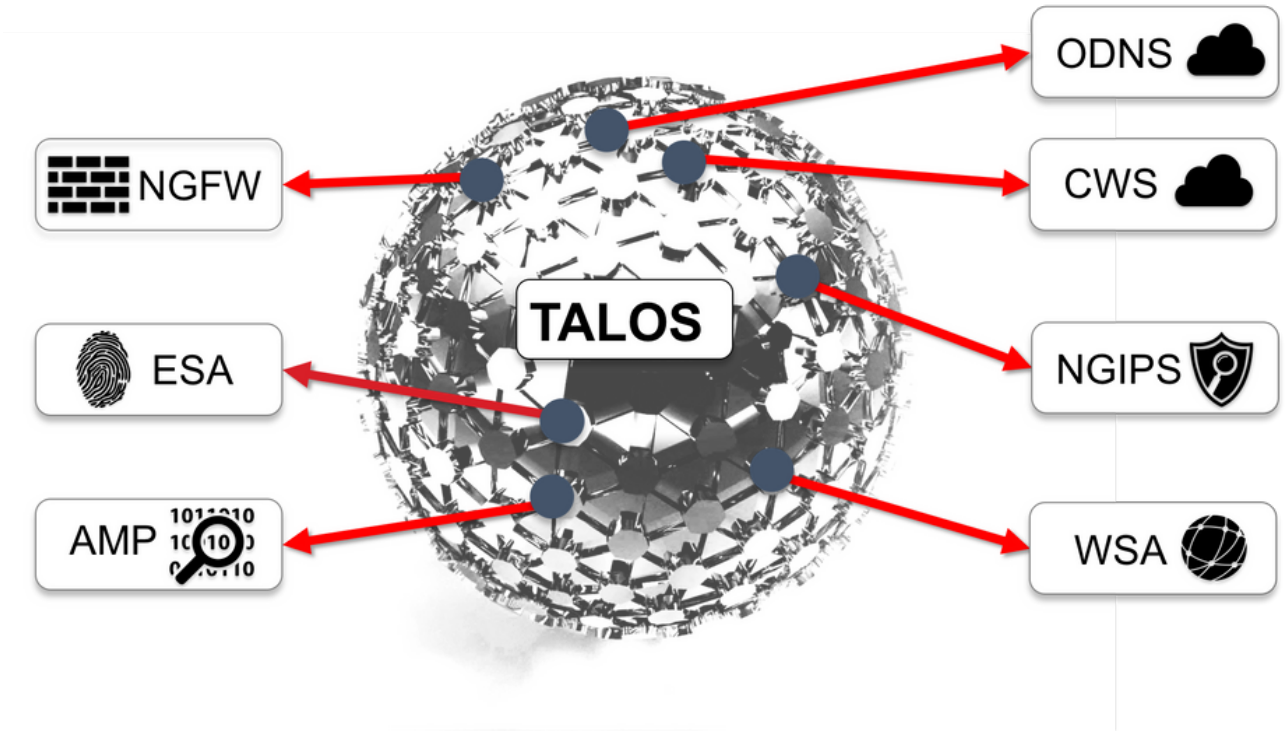
Feedback statistiche feedback utente finale

Statistiche condivise per utente finale Classificazione errata Feedback

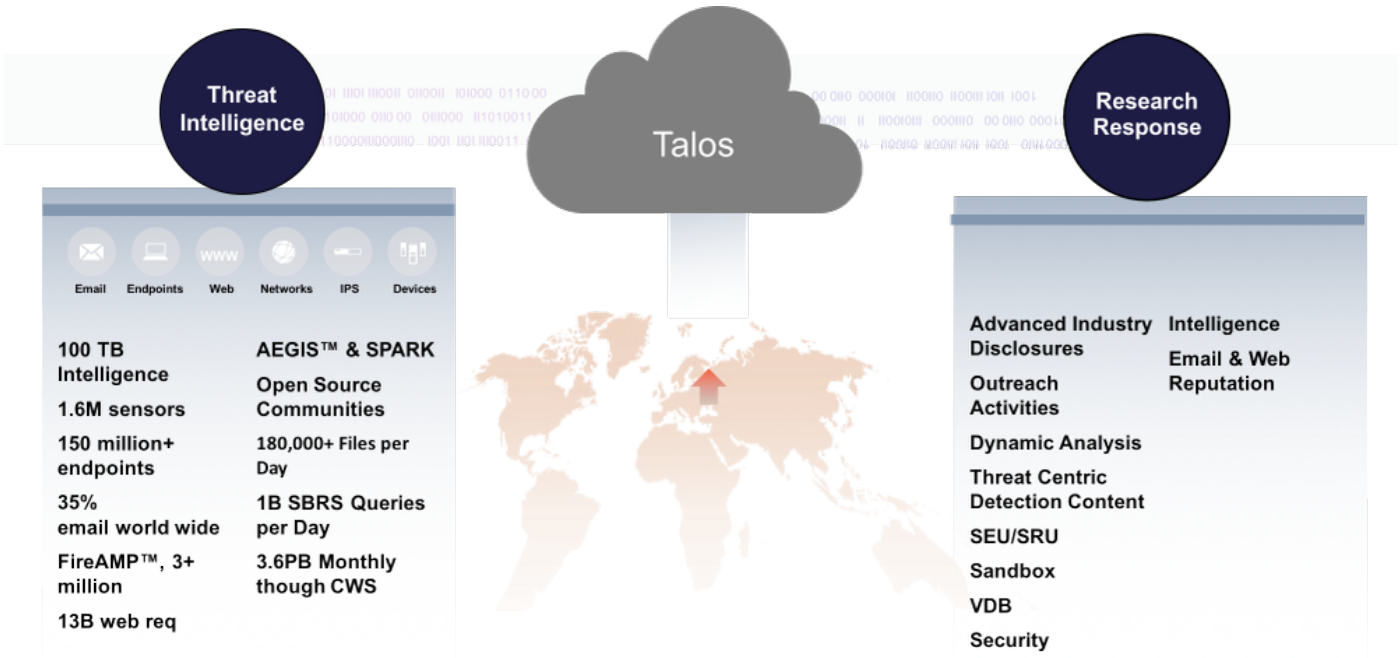
Articolo	Dati di esempio
ID motore (numerico)	0
Codice di categorizzazione Web legacy	

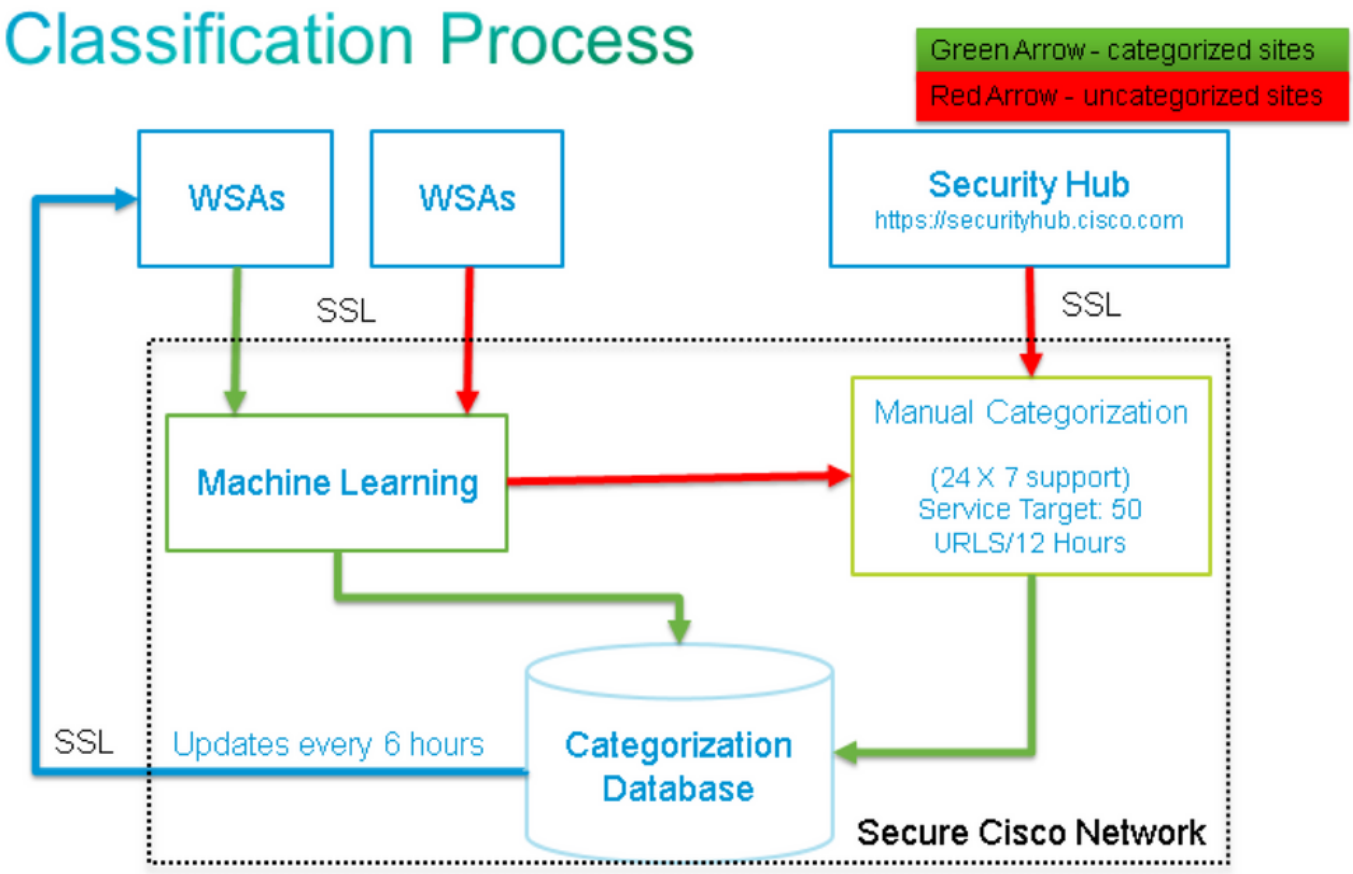
Origine classificazione Web CIWUC "resp" / "req"
Categoria Web CIWUC 1026

Contenuto rilevamento talos



Focalizzato sulle minacce





Informazioni correlate

- [Cisco Web Security Appliance - Pagina del prodotto]
- [Cisco Email Security Appliance - Pagina del prodotto]
- [Documentazione e supporto tecnico – Cisco Systems]