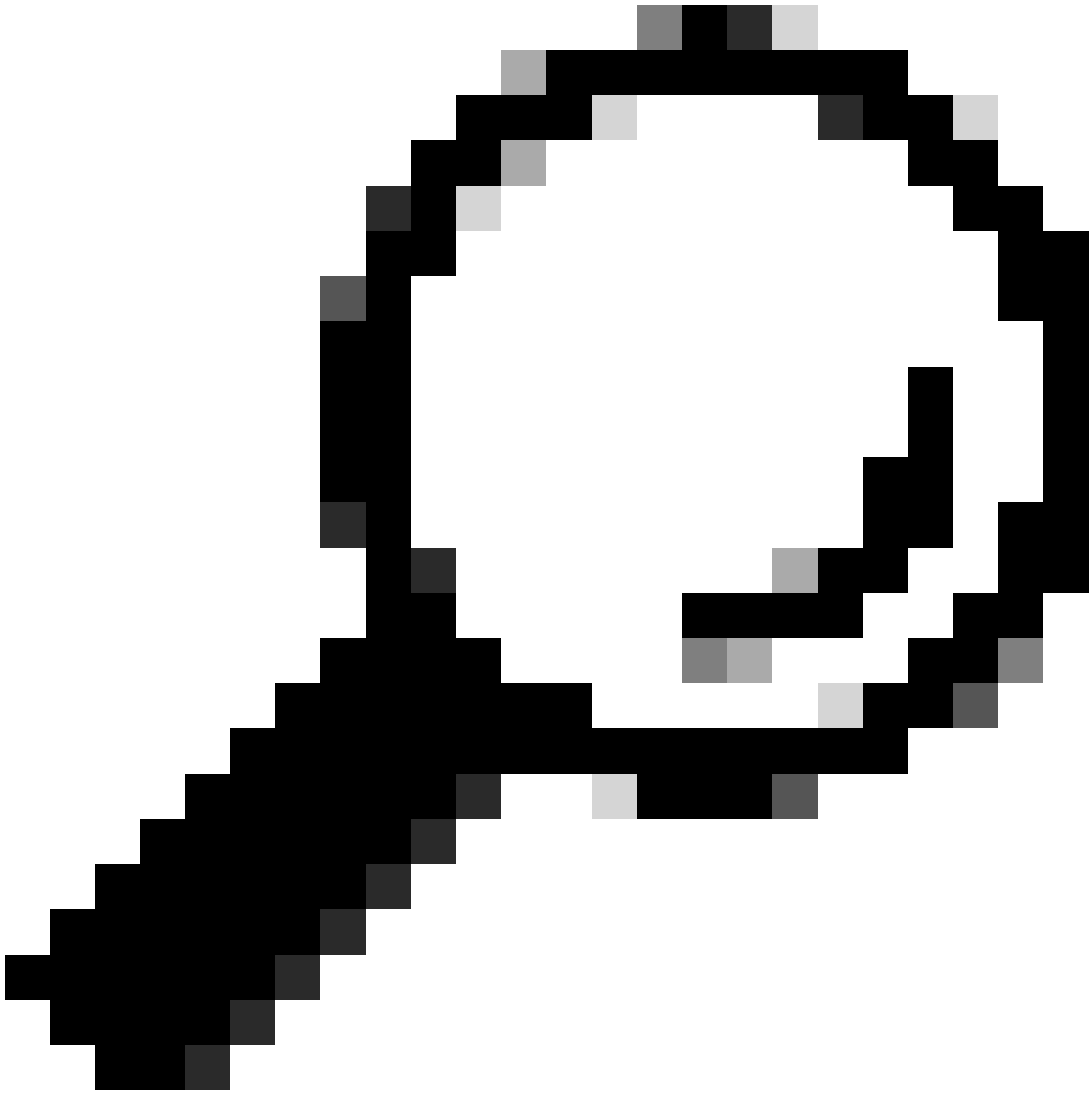
Analisi della rete sicura Informazioni sulle connessioni esterne Guida

Sommario

Introduzione

Utilizzare questa guida per esaminare le connessioni esterne necessarie per il rapido funzionamento di alcune funzionalità di Analisi rete sicura. Queste connessioni esterne possono essere domini o endpoint. I domini sono nomi utilizzati per identificare le risorse su Internet, di solito siti web o servizi; e gli endpoint sono dispositivi o nodi reali che comunicano attraverso una rete. Poiché l'elemento attivo di questa guida sono i servizi Web, questi verranno visualizzati come URL. Nella tabella sono elencati in ordine alfabetico gli URL delle connessioni esterne.



Suggerimento: Nella tabella sono elencati in ordine alfabetico gli URL delle connessioni esterne.

Connessioni esterne

URL connessione esterna	Scopo
https://analytics.int.obsrvbl.com	Utilizzato da Secure Network Analytics per lo scambio di dati di telemetria con i servizi Secure Cloud Analytics.
https://api.apj.sse.itd.cisco.com	Richiesto da Cisco per il transito dei dati verso

	Amazon Web Services (AWS) per l'area Asia Pacifico, Giappone e Cina (APJC). Utilizzato per l'inoltro di avvisi a Cisco XDR e per le metriche del servizio clienti.
https://api.eu.sse.itd.cisco.com	Richiesto da Cisco per il transito di dati verso Amazon Web Services (AWS) per l'area Europa (EU). Utilizzato per l'inoltro di avvisi a Cisco XDR e per le metriche del servizio clienti.
https://api-sse.cisco.com	Richiesto da Cisco per il transito dei dati verso Amazon Web Services (AWS) per l'area degli Stati Uniti. Utilizzato per l'inoltro di avvisi a Cisco XDR e per le metriche relative all'assistenza clienti e al successo.
https://apix.cisco.com	Utilizzato da Secure Network Analytics per la funzionalità Download diretti di software.
https://dex.sse.itd.cisco.com	Obbligatorio per l'invio e la raccolta di metriche di successo cliente
https://est.sco.cisco.com	Obbligatorio per l'invio e la raccolta di metriche di successo cliente
https://eventing-ingest.sse.itd.cisco.com	Obbligatorio per l'invio e la raccolta di metriche di successo cliente
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	Richiesto da Threat Feed, utilizzato per gli avvisi e le osservazioni di Secure Network Analytics, quando Analytics è abilitato.
https://id.cisco.com	Utilizzato da Secure Network Analytics per la funzionalità Download diretti di software.

https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	Richiesto da Threat Feed, utilizzato per gli avvisi e le osservazioni di Secure Network Analytics, quando Analytics è abilitato.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	Richiesto da Threat Feed, utilizzato per gli avvisi e le osservazioni di Secure Network Analytics, quando Analytics è abilitato.
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	Richiesto dal feed di analisi della rete sicura Threat Intelligence, utilizzato per gli avvisi e gli eventi di sicurezza di analisi della rete sicura. È necessario disporre della licenza Secure Network Analytics Threat Intelligence Feed.
https://mx*.sse.itd.cisco.com	Obbligatorio per l'invio e la raccolta di metriche di successo cliente
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	Consente di accedere alle informazioni MITER per gli avvisi quando Analytics è abilitato.
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	Consente di accedere alle informazioni MITER per gli avvisi quando Analytics è abilitato.
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	Consente di accedere alle informazioni MITER per gli avvisi quando Analytics è abilitato.
https://s3.amazonaws.com/onconfig/global-blacklist	Feed minacce obbligatorio, utilizzato per gli avvisi e le osservazioni di Analisi di rete sicura, quando l'analisi è abilitata.
https://sensor.anz-prod.obsrvbl.com	Richiesto da Cisco per il transito dei dati verso Amazon Web Services (AWS) per l'area Asia Pacifico, Giappone e Cina (APJC). Utilizzato per l'inoltro di avvisi a Cisco

	XDR e per le metriche del servizio clienti.
https://sensor.eu-prod.obsrvbl.com	Richiesto da Cisco per il transito di dati verso Amazon Web Services (AWS) per l'area Europa (EU). Utilizzato per l'inoltro di avvisi a Cisco XDR e per le metriche del servizio clienti.
https://sensor.ext.obsrvbl.com	Richiesto da Cisco per il transito dei dati verso Amazon Web Services (AWS) per l'area degli Stati Uniti. Utilizzato per l'inoltro di avvisi a Cisco XDR e per le metriche del servizio clienti.
smartreceiver.cisco.com	Consente di accedere a Cisco Smart Software Licensing. Per ulteriori informazioni, consultare la Smart Licensing Guide. Se si preferisce, è disponibile una licenza non in linea alternativa. Per ulteriori informazioni, consultare le note sulla versione.
https://software.cisco.com	Utilizzato da Secure Network Analytics per la funzionalità Download diretti di software.
https://www.cisco.com	Obbligatorio per il dominio Cisco, utilizzato per i test delle licenze Smart, del proxy cloud e della connessione firewall.

Ulteriori informazioni

Per ulteriori informazioni su come e perché vengono utilizzate connessioni a domini ed endpoint specifiche, fare riferimento agli argomenti seguenti:

- Cisco Secure Service Exchange (SSE)
- Download diretti di software (Beta)
- MITER ATT&CK® Framework
- Feed minaccia

Cisco Secure Service Exchange (SSE)

Gli endpoint SSE vengono utilizzati per il transito dei dati verso Amazon Web Services (AWS), da Cisco per le metriche del servizio clienti e anche per l'inoltro di avvisi a Cisco XDR. Questi variano in base all'area e agli host. Questi endpoint vengono individuati in modo dinamico utilizzando un meccanismo di individuazione dei servizi fornito dal connettore SSE. Durante la pubblicazione dei rilevamenti in Cisco XDR, Secure Network Analytics cerca di individuare un servizio denominato "xdr-data-platform" e il relativo endpoint API "Events".

Area geografica e host

A seconda della regione degli ambienti di produzione, gli host sono i seguenti.

STATI UNITI:

- https://api-sse.cisco.com
- https://sensor.ext.obsrvbl.com

UE:

- https://api.eu.sse.itd.cisco.com
- https://sensor.eu-prod.obsrvbl.com

APJC:

- https://api.apj.sse.itd.cisco.com
- https://sensor.anz-prod.obsrvbl.com

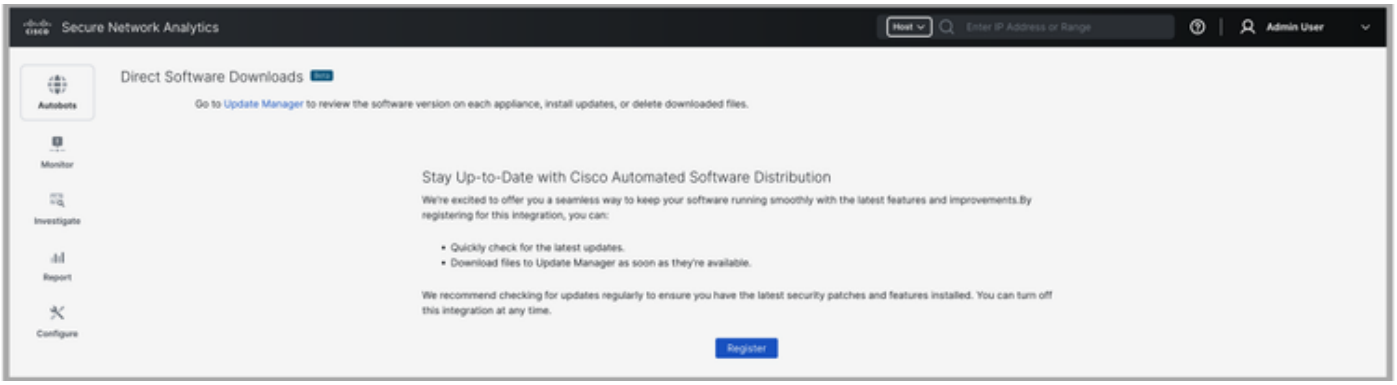
Download diretti di software (Beta)

La funzionalità Download diretti di software utilizza le connessioni seguenti:

- https://apix.cisco.com
- https://software.cisco.com
- https://id.cisco.com

Per utilizzare questa nuova funzionalità per scaricare software e file di aggiornamento delle patch direttamente in Update Manager, assicurarsi di aver effettuato la registrazione utilizzando il proprio cisco.com ID utente (CCOID).
1. Accedere al Manager.
2. Dal menu principale, scegliere Configura > Globale > Gestione centrale.

3. Fare clic sulla scheda Gestione aggiornamenti.
4. Fare clic sul collegamento Download diretti di software per aprire la pagina di registrazione.
5. Fare clic sul pulsante Registra per avviare il processo di registrazione.

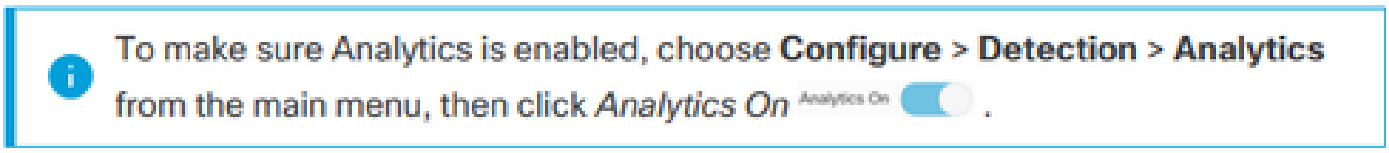


6. Fare clic sul collegamento fornito.
7. Viene visualizzata la pagina Attiva dispositivo. Fare clic su Avanti per continuare.
8. Accedere con il proprio cisco.com ID utente (CCOID).
9. Al termine dell'attivazione, verrà visualizzato il messaggio "Dispositivo attivato".
10. Tornare alla pagina Download diretti di software sul proprio Manager e fare clic su Continua.
11. Fare clic sui collegamenti per leggere e accettare i termini dell'EULA e degli accordi K9. Una volta accettati i termini, fare clic su Continue (Continua).

Per ulteriori informazioni sui download diretti di software, contattare il supporto Cisco

MITER ATT&CK® Framework

Il framework MITER ATT&CK® è una base di conoscenze pubblicamente disponibile di tattiche e tecniche avversarie basate su osservazioni del mondo reale. Dopo aver abilitato Analytics all'interno di Secure Network Analytics, le tattiche e le tecniche MITER forniscono assistenza con l'intelligence, il rilevamento e la risposta alle minacce di cibersicurezza.



Le connessioni seguenti consentono a Secure Network Analytics di accedere alle informazioni MITER
per gli avvisi:

- https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
- https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobileattack.json
- https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterpriseattack.json

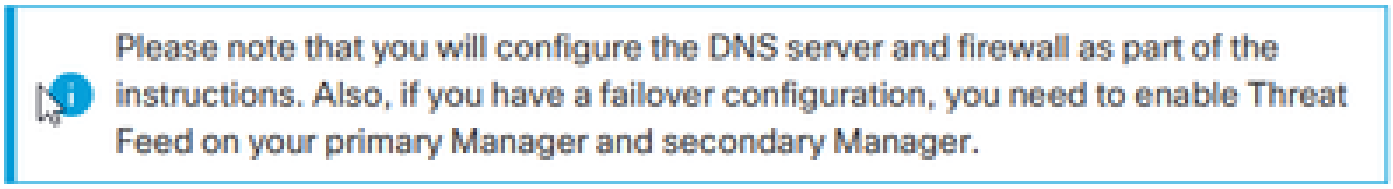
Feed minaccia

Il feed delle minacce di Cisco Secure Network Analytics (in precedenza feed Stealthwatch Threat

Intelligence) fornisce i dati del feed delle minacce globali sulle minacce alla rete. Il feed viene aggiornato di frequente e include indirizzi IP, numeri di porta, protocolli, nomi host e URL noti per essere utilizzati per attività dannose. I seguenti gruppi host sono inclusi nel feed: server di comando e controllo, bogon e Tor.

Per abilitare il feed di minacce in Gestione centrale, seguire le istruzioni visualizzate nella Guida.

1. Accedere al proprio responsabile principale.
2. Selezionare Configura > Globale > Gestione centrale.
3. Fare clic sull'icona (Guida). Selezionare ?.
4. Selezionare Configurazione accessorio > Avanzamento minaccia.



Per ulteriori informazioni sull'alimentazione a rischio, consultare la Guida alla configurazione del sistema.

Come contattare il supporto tecnico

Se hai bisogno di supporto tecnico, effettua una delle seguenti operazioni:

- Contatta il tuo partner Cisco locale
- Contatta il supporto Cisco
- Per aprire una richiesta tramite Web: http://www.cisco.com/c/en/us/support/index.html
- Per il supporto telefonico: 1-800-553-2447 (Stati Uniti)
- Per i numeri del supporto mondiale: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).