

Gestisci l'app Cloud Security per IBM QRadar

Sommario

[Introduzione](#)

[Panoramica](#)

[Accesso all'app Cisco Cloud Security](#)

[Componenti dell'app Cisco Cloud Security](#)

[Panoramica del cloud](#)

[Umbrella](#)

[Indaga](#)

[CloudLock](#)

[Scheda Imposizione](#)

Introduzione

Questo documento descrive come gestire l'app Cisco Cloud Security per IBM QRadar.

Panoramica

QRadar di IBM è un popolare SIEM per l'analisi dei log. Fornisce una potente interfaccia per l'analisi di grandi blocchi di dati, ad esempio i registri forniti da Cisco Umbrella per il traffico DNS della tua organizzazione. Le informazioni visualizzate in Cisco Cloud Security App per IBM QRadar sono disponibili tramite le API di Cisco Umbrella, CloudLock, Investigate and Enforcement.

Quando si configura l'app Cisco Cloud Security per QRadar, integra tutti i dati della piattaforma Cisco Cloud Security e consente di visualizzare i dati in formato grafico nella console QRadar. Dall'applicazione, gli analisti possono:

- Analizza domini, indirizzi IP, indirizzi e-mail
- Bloccare e sbloccare i domini (imposizione)
- Visualizzare le informazioni di tutti gli incidenti della rete.

In questo articolo viene illustrato come esplorare Cisco Cloud Security App. Le istruzioni su come configurare l'applicazione sono disponibili qui: [Configurazione dell'app Cisco Cloud Security per IBM QRadar](#)

Accesso all'app Cisco Cloud Security

Per passare all'app Cisco Cloud Security in IBM QRadar, vai alla home page e fai clic sulla scheda Cisco Cloud Security. Vengono visualizzate la scheda Panoramica cloud e il dashboard. È quindi possibile accedere alle schede Umbrella, Investigate, CloudLock e Enforcement per

visualizzare i log.

Per impostazione predefinita, l'app Cloud Security è impostata per visualizzare i dati degli ultimi 7 giorni. È possibile modificare l'intervallo di tempo facendo clic sull'intervallo di date in alto a destra:

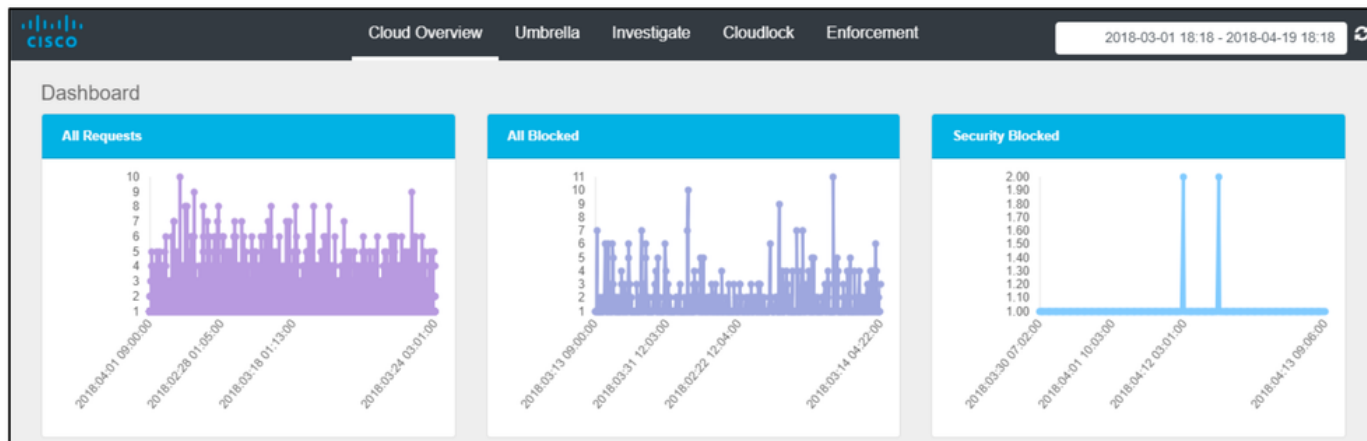
The screenshot shows the 'Enforcement' tab in the Cisco Cloudlock interface. At the top, a date range '2018-04-13 18:18 - 2018-04-19 18:18' is displayed. Below this, there are two date pickers for the start and end dates, each with a time selector set to 18:18. To the right of these pickers is a vertical list of preset time range buttons: 'Last 1 Day', 'Last 2 Days', 'Last 7 Days', 'Last 30 Days', 'This Month', and 'Last Month'. Below the date pickers are two calendar views for April and May 2018. In the April calendar, the 13th and 19th are highlighted. At the bottom right, there is a 'Custom Range' button, an 'Apply' button, and a 'Cancel' button.

360072030052

Componenti dell'app Cisco Cloud Security

Panoramica del cloud

Nella scheda Panoramica cloud vengono visualizzate informazioni quali Tutte le richieste, Tutte le richieste bloccate, Sicurezza bloccata, DGA probabile, Classificazione sicura sospetta, Incidenti di blocco cloud, Blocco cloud complessivo, Primi criteri e Primi offensori in una rappresentazione grafica basata su grafico.



Likely DGA's		Suspicious Secure Rank ⓘ			
Destination	Last Queried	Destination	Securerank	Status Label	Last Queried
104.154.100.100	2018.06.05 01:11	104.154.100.100	5.64000	safe	2018.06.05 04:16
104.154.100.100	2018.06.02 09:01	104.154.100.100	-0.03000	malicious	2018.06.01 01:06
104.154.100.100	2018.06.05 01:15	104.154.100.100	-0.01000	malicious	2018.06.04 09:20
104.154.100.100	2018.06.02 11:04	104.154.100.100	-18.92000	malicious	2018.06.03 12:03
104.154.100.100	2018.06.08 11:05	104.154.100.100	-0.01000	malicious	2018.06.05 01:10
104.154.100.100	2018.06.02 01:09				
104.154.100.100	2018.06.06 03:20				
104.154.100.100	2018.06.04 01:07				
104.154.100.100	2018.06.08 12:05				

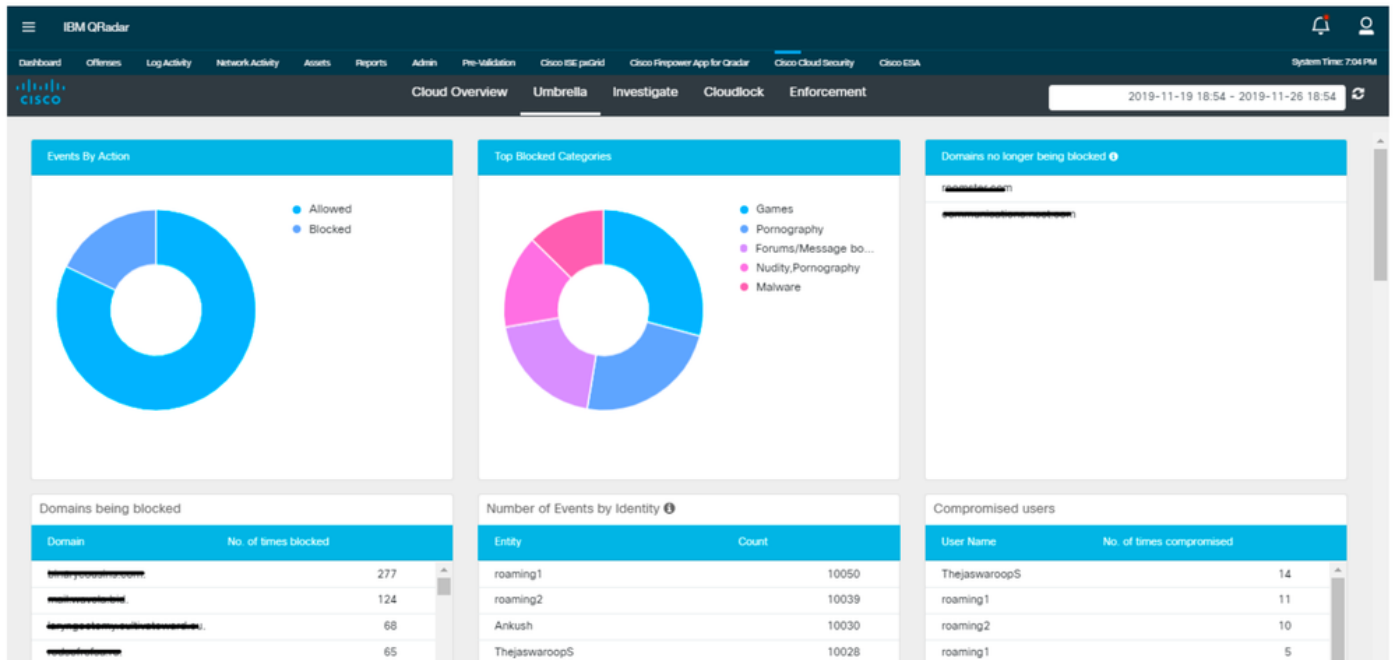
360072257631

Cloudlock Incidents		Cloudlock Top Policies		Cloudlock Top Offenders	
Status	Count	Policy	Count	User Name	Count
New	102548	Social Security Number	1	unknown user	3549
In Progress	12	New Unclassified App Installs	120	Sarat Kumar	3061
Dismissed	3	AppTest	102441	Anuraj C	2205
Resolved	2			Mohit Vaish	2002
				Kedar Bhat	1937
				Touseef Jagirdar	1893
				Rajeev Menon	1818
				Sameer Shelke	1814

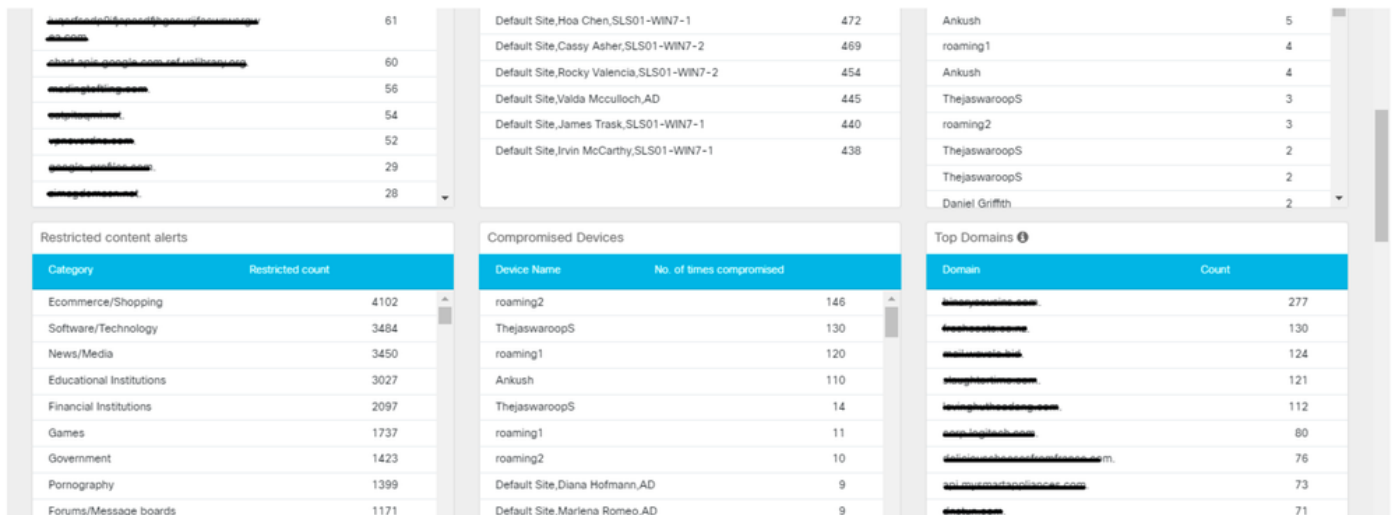
360072257611

Umbrella

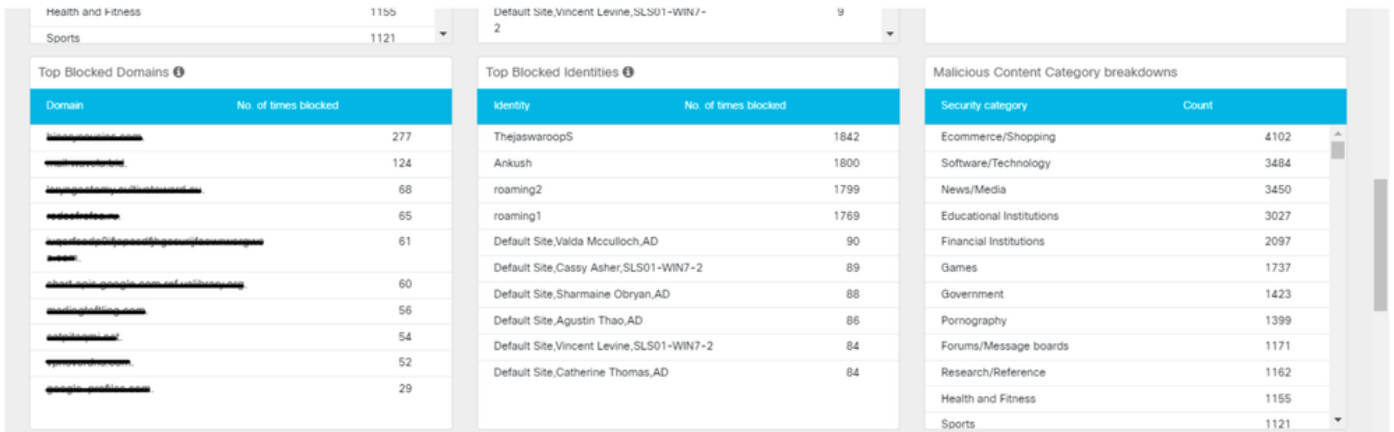
Nella scheda Umbrella vengono visualizzate informazioni quali Eventi per azione, Categorie bloccate principali, Numero di eventi per identità, Domini bloccati, Domini non più bloccati, Utenti compromessi, Avvisi di contenuto con restrizioni, Dispositivi compromessi, Primi domini, Primi domini bloccati, Primi identità bloccate, Suddivisioni categorie di contenuto dannoso, Principali categorie, Attività e Tendenza accesso utente in una rappresentazione grafica basata su grafico.



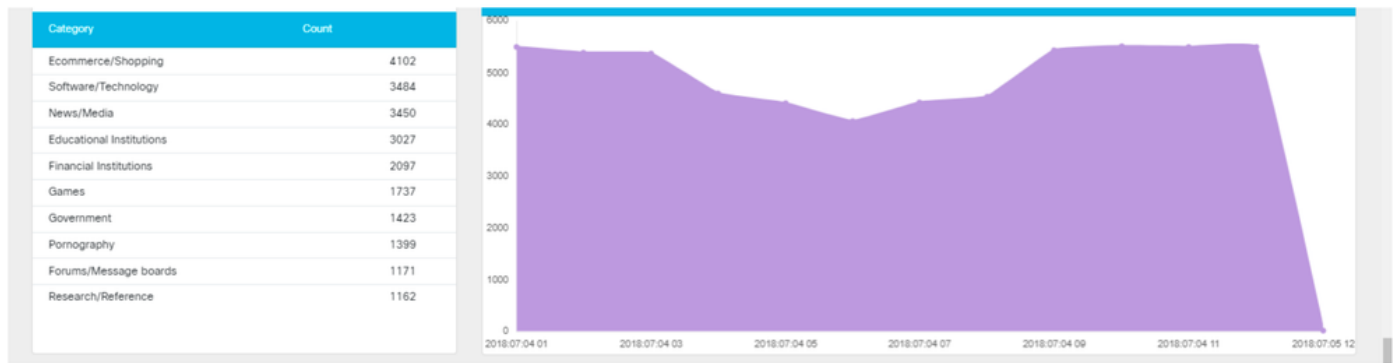
360072263411



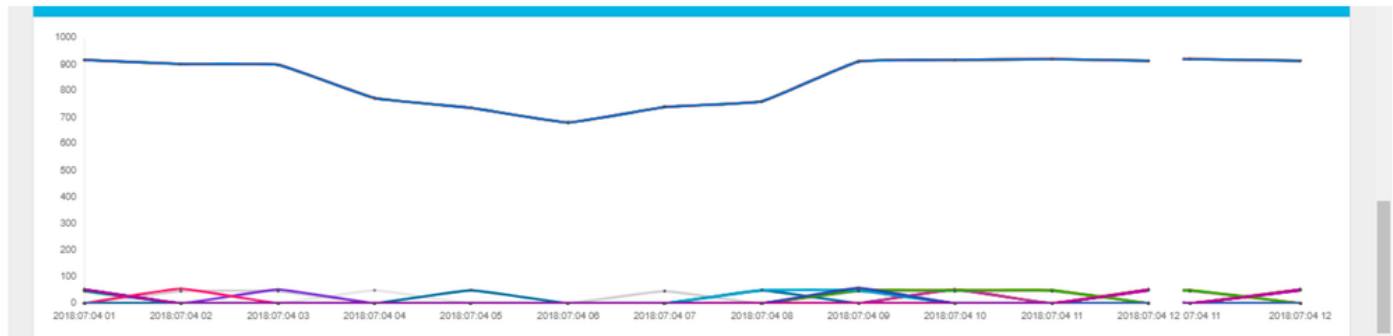
360072263391



360072037372



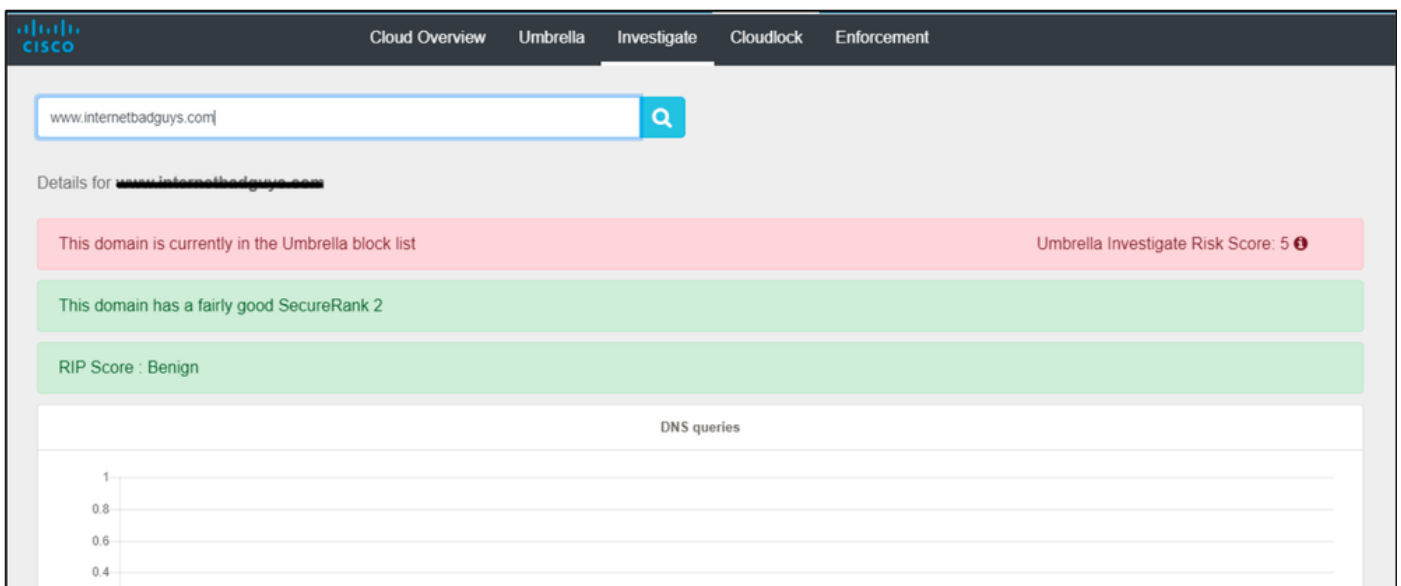
360072263331



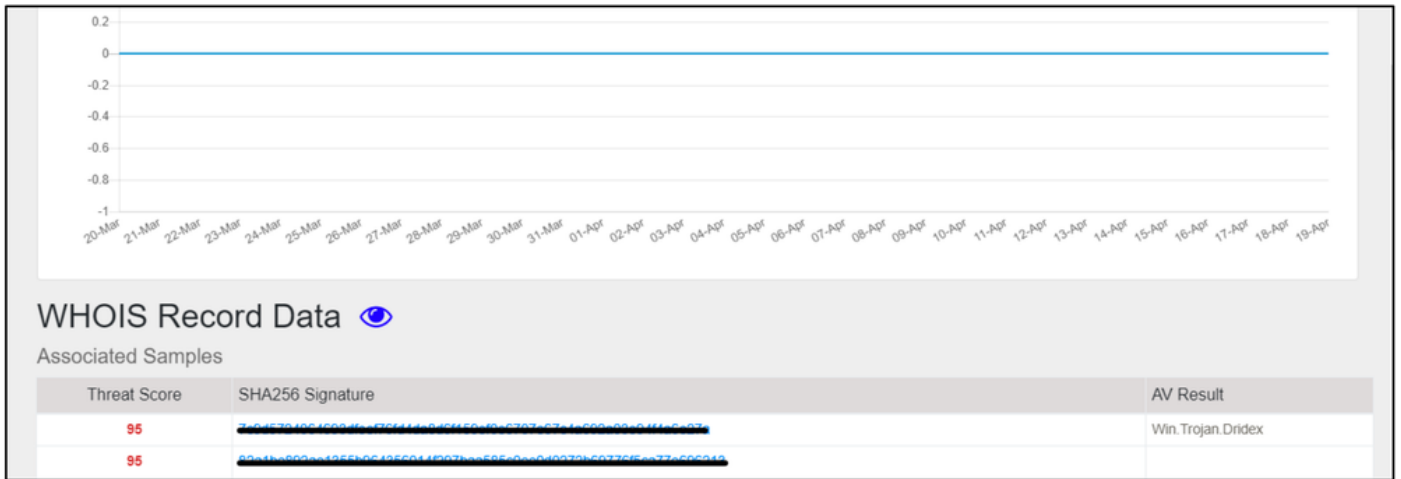
360072263351

Indaga

La scheda Indaga consente all'utente di cercare le informazioni relative a nome host, URL, ASN, IP, hash o indirizzo e-mail. Contiene inoltre informazioni quali record WHOIS, informazioni DGA e così via.



360072263511



360072037472

Features	
TTLs min	1
TTLs max	1
TTLs mean	1
TTLs median	1
TTLs standard deviation	0
Country codes	US
Country count	1
ASNs	AS 36692
ASNs count	1
Prefixes	67.215.88.0
Prefixes count	1

360072037452

CloudLock

La scheda CloudLock consente agli utenti di visualizzare informazioni su tutti gli incidenti rilevati. Gli utenti possono anche aggiornare la gravità e lo stato dell'incidente selezionando i valori dal menu a discesa e facendo clic su "Aggiorna".

Incidents									
Incident ID									
Id	Platform	Matches	Policy	Detected	Source	Owner	Severity	Status	Actions
132352847	office365	1	AppTest	Jun 03, 2018 5:20:13 pm	AzureActiveDirectory User Login Failed	unknown user	CRITIC	IN PRO	Update
132352852	office365	1	AppTest	Jun 03, 2018 5:24:23 pm	AzureActiveDirectory User Login Failed	Mohit Vaish	CRITIC	NEW	Update
132352856	office365	1	AppTest	Jun 03, 2018 5:24:39 pm	AzureActiveDirectory User Logg ed In	Khiladi Bayal	CRITIC	IN PROGRESS	Update
132490696	office365	1	AppTest	Jun 04, 2018 4:39:22 pm	AzureActiveDirectory User Logg ed In	Anil Kumar Yarl apalli	CRITIC	RESOLVED	Update
								DISMISSED	

360072268311

Gli utenti possono registrare gli eventi per visualizzare ulteriori dettagli sull'incidente.

Incident Details

Objective Type

Name

CodeSign Production

Platform

office365

Owner

██████████@aujas.com

Policy

New Unclassified App Installs

Time

IP Address

Status

NEW

Severity

ALERT

Detected

Match Type

Match

New Unclassified App Install

s

360072042332

Scheda Imposizione

Nella scheda Imposizione vengono visualizzate informazioni sui domini bloccati. Gli utenti possono anche selezionare i domini bloccati e sbloccarli da questa interfaccia.

cloud

CISCO

Cloud Overview

Umbrella

Investigate

Cloudlock

Enforcement

2018-04-13 18:18 - 2018-04-19 18:18

Blocked Domains

☐

Domain

Last Seen

☐

aujasdigital.com

Mar 16, 2018 9:46 AM

☐

havanacubanrealestate.co

Mar 28, 2018 11:47 AM

1 - 2 < >

Unblock

360072038472

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).