

Gerencie o aplicativo Cloud Security para IBM QRadar

Contents

[Introdução](#)

[Overview](#)

[Como acessar o aplicativo Cisco Cloud Security](#)

[Componentes do aplicativo Cisco Cloud Security](#)

[Visão geral da nuvem](#)

[Umbrella](#)

[Investigar](#)

[CloudLock](#)

[Guia Aplicação](#)

Introdução

Este documento descreve como gerenciar o aplicativo Cisco Cloud Security para IBM QRadar.

Overview

O QRadar da IBM é um SIEM popular para análise de registros. Ele fornece uma interface eficiente para analisar grandes blocos de dados, como os logs fornecidos pelo Cisco Umbrella para o tráfego DNS da sua organização. As informações exibidas no Cisco Cloud Security App para IBM QRadar são fornecidas através das APIs do Cisco Umbrella, CloudLock, Investigate e Enforcement.

Quando você configura o aplicativo Cisco Cloud Security para QRadar, ele integra todos os dados da plataforma Cisco Cloud Security e permite que você visualize os dados em forma gráfica no console QRadar. No aplicativo, os analistas podem:

- Investigar domínios, endereços IP, endereços de e-mail
- Bloquear e desbloquear domínios (imposição)
- Exibir as informações de todos os incidentes da rede.

Este artigo mostra como navegar no aplicativo Cisco Cloud Security. As instruções sobre como configurar o aplicativo podem ser encontradas aqui: [Configurando o aplicativo Cisco Cloud Security para IBM QRadar](#)

Como acessar o aplicativo Cisco Cloud Security

Para navegar para o aplicativo Cisco Cloud Security no IBM QRadar, vá para a página inicial e

clique na guia Cisco Cloud Security. A guia Visão geral da nuvem e o Painel são exibidos. Você pode acessar as guias Umbrella, Investigate, CloudLock e Enforcement para exibir seus logs.

O aplicativo Cloud Security está configurado para mostrar os dados dos últimos 7 dias por padrão. Você pode alterar o período clicando no intervalo de datas no canto superior direito:

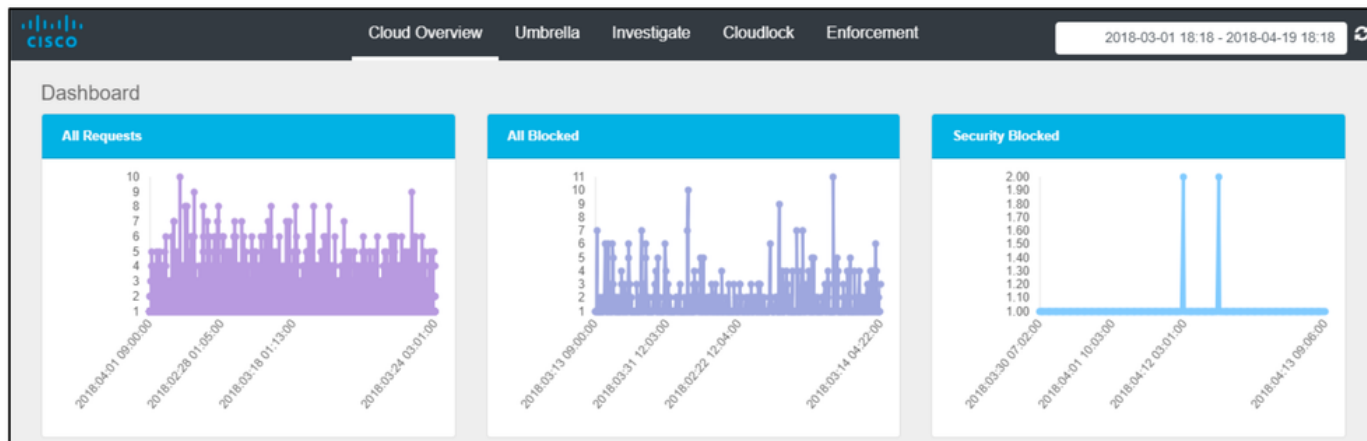
The screenshot shows the date range selection interface in the Cisco Cloud Security application. At the top, there are tabs for 'ite', 'Cloudlock', and 'Enforcement'. A date range '2018-04-13 18:18 - 2018-04-19 18:18' is displayed. Below this, there are two date pickers. The left one is set to '2018-04-13 18:18' and the right one to '2018-04-19 18:18'. Each picker has a clock icon and a time selector set to '18 : 18'. Below the date pickers are two calendar views. The left calendar is for 'Apr 2018' and the right is for 'May 2018'. In the April calendar, the 13th and 19th are highlighted. In the May calendar, the 1st through 9th are visible. To the right of the calendars are buttons for 'Last 1 Day', 'Last 2 Days', 'Last 7 Days', 'Last 30 Days', 'This Month', and 'Last Month'. At the bottom right, there is a 'Custom Range' button, an 'Apply' button, and a 'Cancel' button.

360072030052

Componentes do aplicativo Cisco Cloud Security

Visão geral da nuvem

A guia Visão geral da nuvem exibe informações como Todas as solicitações, Todas bloqueadas, Segurança bloqueada, DGAs prováveis, Classificação segura suspeita, Incidentes de Cloudlock, CloudLock Geral, Principais políticas e Principais infratores em uma representação visual baseada em gráfico.



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				

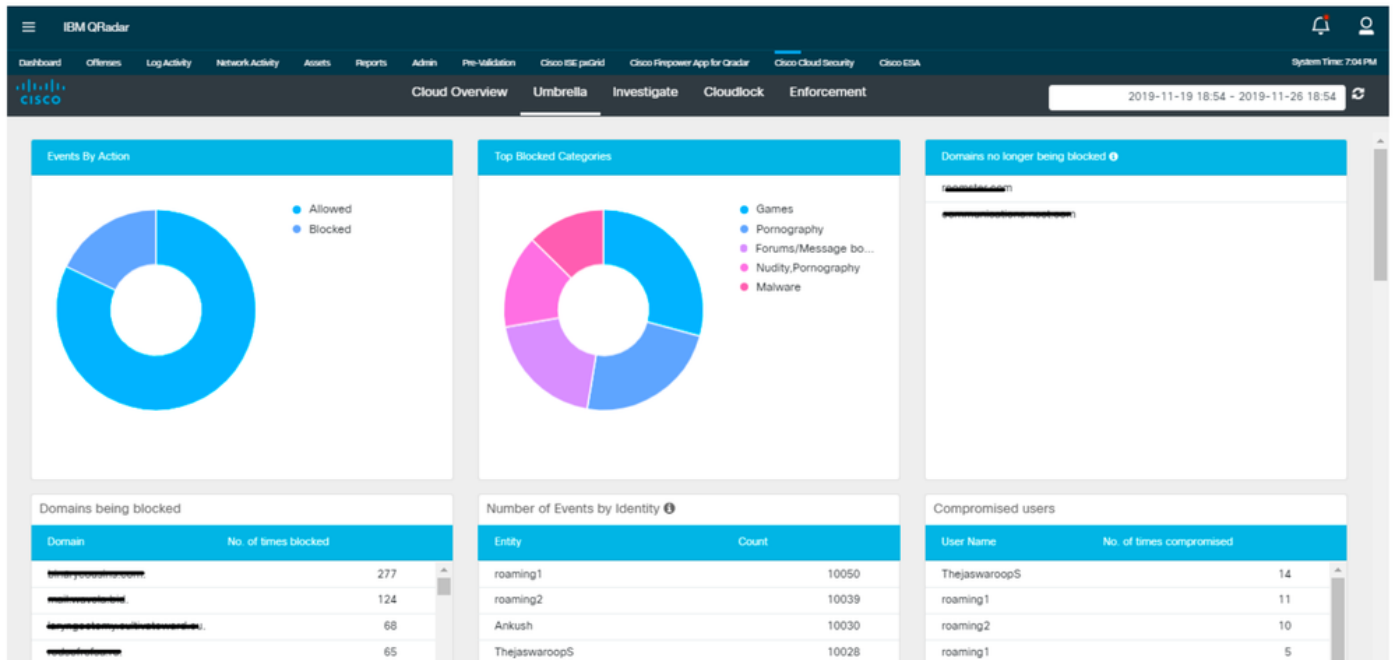
360072257631

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

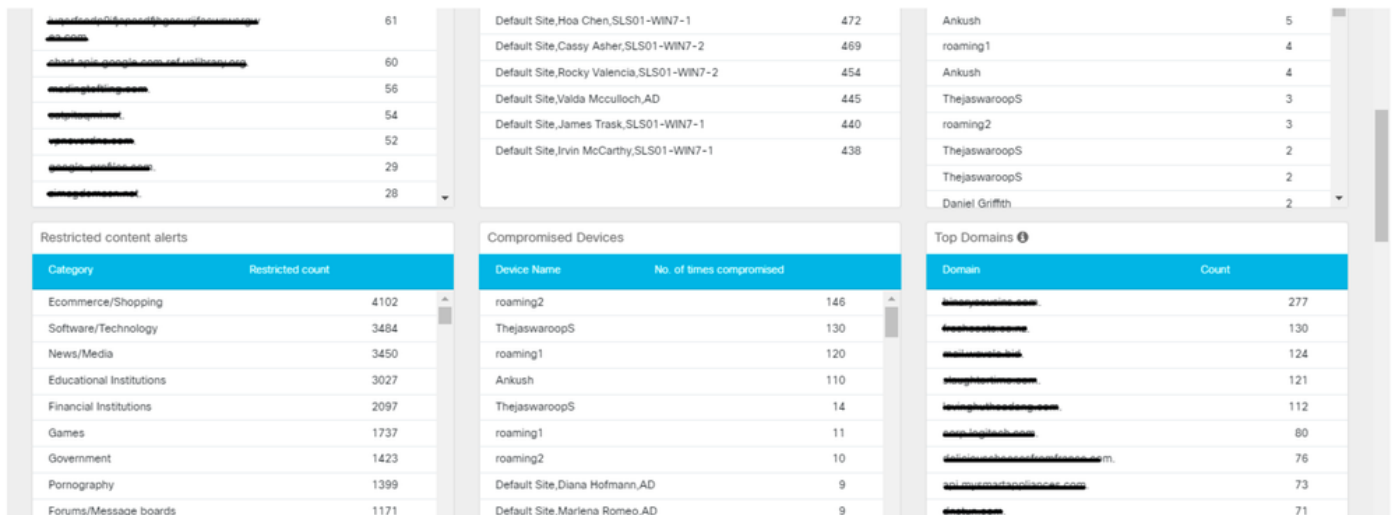
360072257611

Umbrella

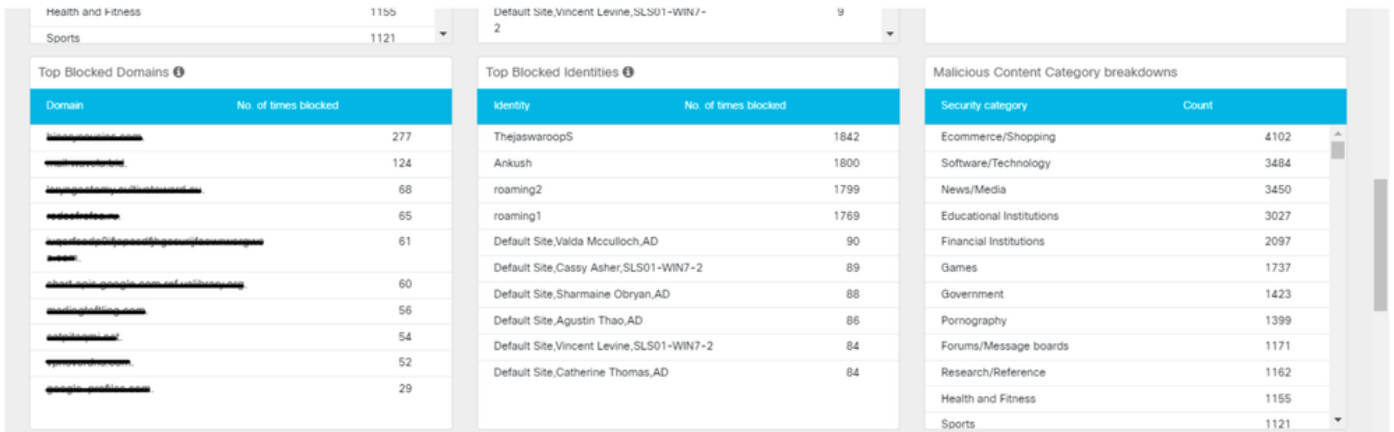
A guia Guarda-chuva exibe informações como Eventos por ação, Principais categorias bloqueadas, Número de eventos por identidade, Domínios que estão sendo bloqueados, Domínios que não estão mais sendo bloqueados, Usuários comprometidos, Alertas de conteúdo restrito, Dispositivos comprometidos, Principais domínios, Principais domínios bloqueados, Principais identidades bloqueadas, Desagregações de categorias de conteúdo mal-intencionado, Principais categorias, Tendência de atividade e acesso do usuário em uma representação visual baseada em gráfico.



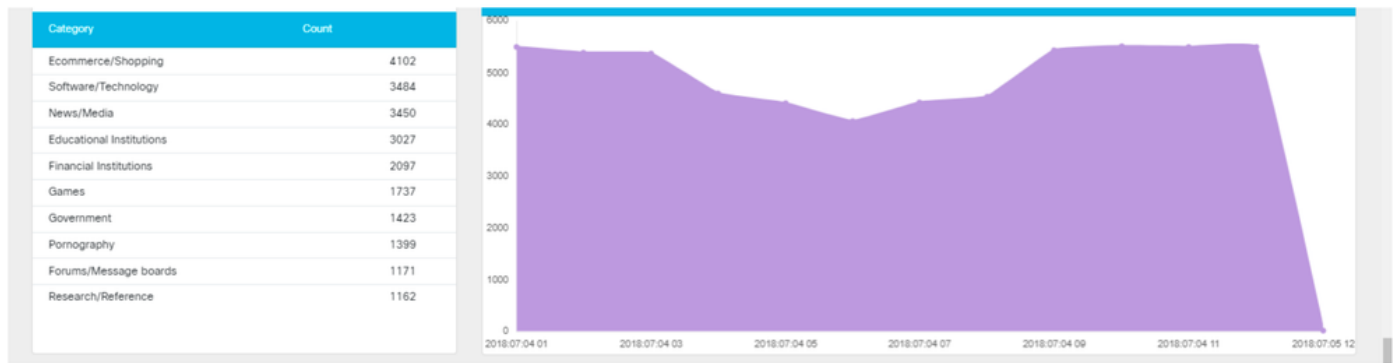
360072263411



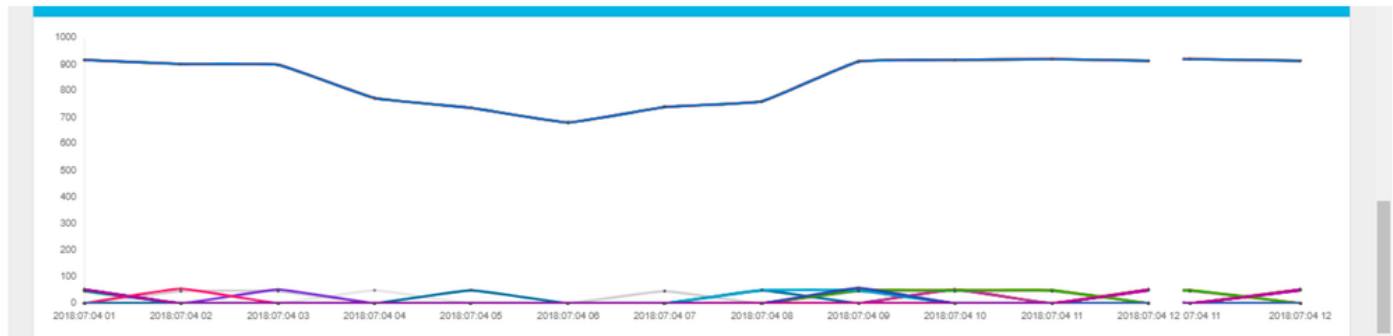
360072263391



360072037372



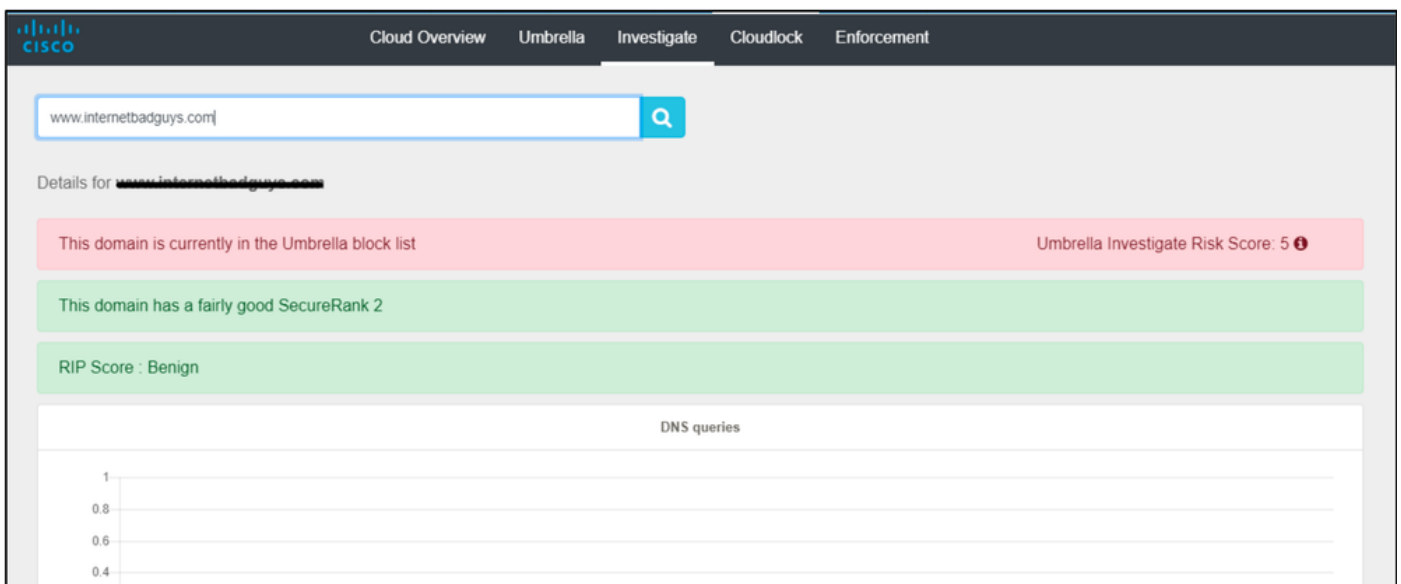
360072263331



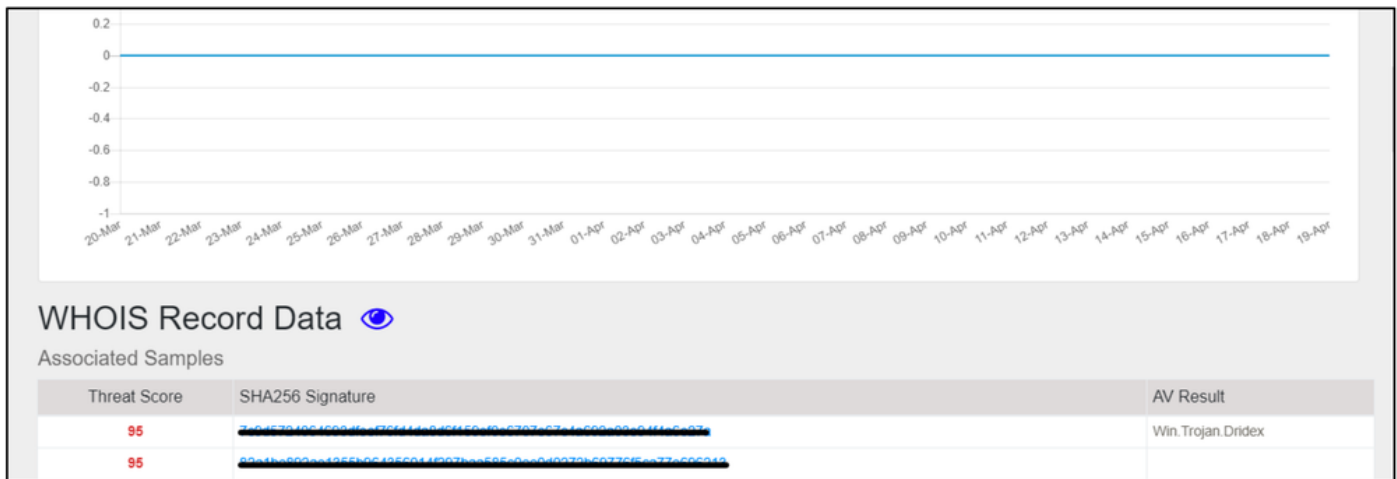
360072263351

Investigar

A guia Investigar permite que o usuário pesquise as informações relacionadas ao nome do host, URL, ASN, IP, Hash ou endereço de e-mail. Ele também tem informações como registro WHOIS, informações DGA e assim por diante.



360072263511

WHOIS Record Data

Threat Score	SHA256 Signature	AV Result
95	7e04f7b19516994ba376141e0d6c55e0e3707c371e609e8b044e9c937	Win. Trojan.Dridex
95	89e4be893ee4355fb0c4956044f607bae585e0ae0d0070bc0736fe973e566949	

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

A guia CloudLock permite que os usuários exibam informações sobre todos os incidentes detectados. Os usuários também podem atualizar a gravidade e o status do incidente selecionando os valores no menu suspenso e clicando em "Atualizar".

Cloud Overview

Umbrella

Investigate

Cloudlock

Enforcement

2018-06-01 18:06 - 2018-06-08 18:06

Incidents

Incident ID

Q

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	RESOLVED	Update
132490696	office365	1	AppTest	Jun 04, 2018 4:39:22 pm	AzureActiveDirectory User Logg ed In	Anil Kumar Yari apalli	CRITIC	IN PRO	Update

360072268311

Os usuários podem monitorar a hora em qualquer um dos eventos para visualizar mais detalhes

sobre o 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

Guia Aplicação

A guia Aplicação exibe informações sobre quais domínios estão bloqueados. Os usuários também podem selecionar domínios bloqueados e desbloqueá-los nessa interface.

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.