

IBM QRadar向けクラウドセキュリティアプリの管理

内容

[はじめに](#)

[概要](#)

[Cisco Cloud Securityアプリケーションへのアクセス](#)

[Cisco Cloud Securityアプリケーションコンポーネント](#)

[クラウドの概要](#)

[Umbrella](#)

[調査](#)

[Cloudlock](#)

[「強制」タブ](#)

はじめに

このドキュメントでは、IBM QRadar向けCisco Cloud Securityアプリの管理方法について説明します。

概要

IBMのQRadarは、ログ分析用の一般的なSIEMです。Cisco Umbrellaが組織のDNSトラフィック用に提供するログなど、大量のデータを分析するための強力なインターフェイスを提供します。IBM QRadar向けCisco Cloud Security Appに表示される情報は、Cisco Umbrella、CloudLock、Investigate、およびEnforcementのAPIを通じて提供されます。

QRadar用のCisco Cloud Securityアプリをセットアップすると、Cisco Cloud Securityプラットフォームからのすべてのデータが統合され、QRadarコンソールにグラフィカルな形式でデータを表示できるようになります。アナリストはアプリケーションから次の操作を実行できます。

- ドメイン、IPアドレス、電子メールアドレスの調査
- ドメインのブロックとブロック解除（適用）
- ネットワークのすべてのインシデントに関する情報を表示します。

この記事では、Cisco Cloud Securityアプリケーションのナビゲート方法について説明します。アプリケーションをセットアップする方法については、次のサイトを参照してください。

[Configuring the Cisco Cloud Security App for IBM QRadar](#)

Cisco Cloud Securityアプリケーションへのアクセス

IBM QRadarでCisco Cloud Securityアプリケーションに移動するには、ホームページに移動して

Cisco Cloud Securityタブをクリックします。クラウドの概要タブとダッシュボードが表示されます。その後、Umbrella、Investigate、CloudLock、およびEnforcementの各タブにアクセスして、ログを表示できます。

デフォルトでは、クラウドセキュリティアプリケーションは過去7日間のデータを表示するように設定されています。時間枠を変更するには、右上の日付範囲をクリックします。

ite Cloudlock Enforcement 2018-04-13 18:18 - 2018-04-19 18:18

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

18 : 18 18 : 18

< Apr 2018 > May 2018

Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

Su	Mo	Tu	We	Th	Fr	Sa
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

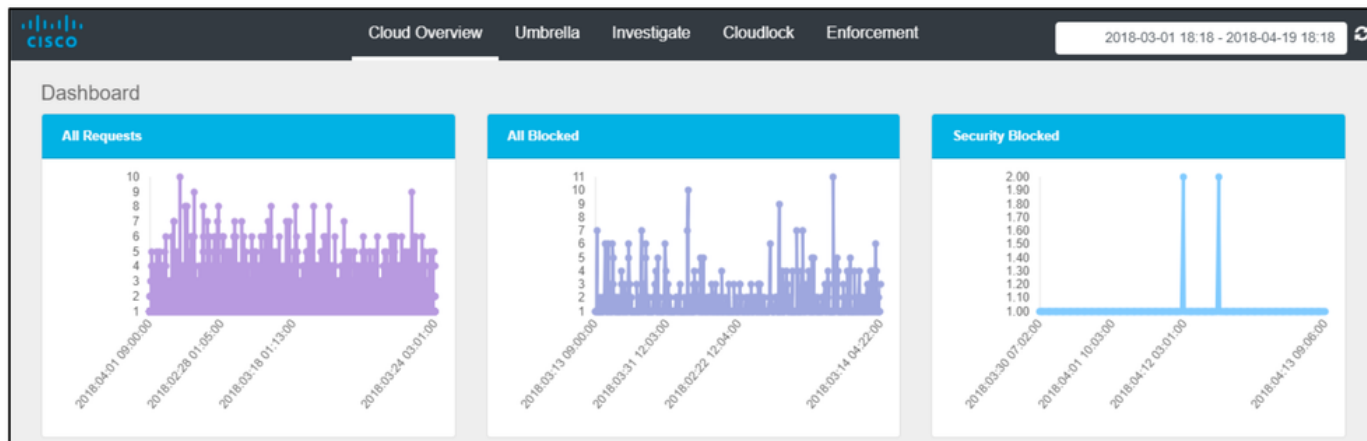
Last 1 Day
Last 2 Days
Last 7 Days
Last 30 Days
This Month
Last Month
Custom Range
Apply Cancel

360072030052

Cisco Cloud Securityアプリケーションコンポーネント

クラウドの概要

Cloud Overviewタブには、All Requests、All Blocked、Security Blocked、Possible DGA's、Suspicious Secure Rank、Cloudlock Incidents、CloudLock Overall、Top Policies、Top Severorなどの情報がグラフ形式で表示されます。



Likely DGA's		Suspicious Secure Rank ⓘ			
Destination	Last Queried	Destination	Securerank	Status Label	Last Queried
104.154.142.100	2018.06.05 01:11	cloudflare.com	5.64000	safe	2018.06.05 04:16
104.154.142.100	2018.06.02 09:01	cloudflare.com	-0.03000	malicious	2018.06.01 01:06
104.154.142.100	2018.06.05 01:15	cloudflare.com	-0.01000	malicious	2018.06.04 09:20
104.154.142.100	2018.06.02 11:04	cloudflare.com	-18.92000	malicious	2018.06.03 12:03
104.154.142.100	2018.06.08 11:05	cloudflare.com	-0.01000	malicious	2018.06.05 01:10
104.154.142.100	2018.06.02 01:09	cloudflare.com	-0.03000	safe	2018.06.05 01:10
104.154.142.100	2018.06.06 03:20				
104.154.142.100	2018.06.04 01:07				
104.154.142.100	2018.06.08 12:05				

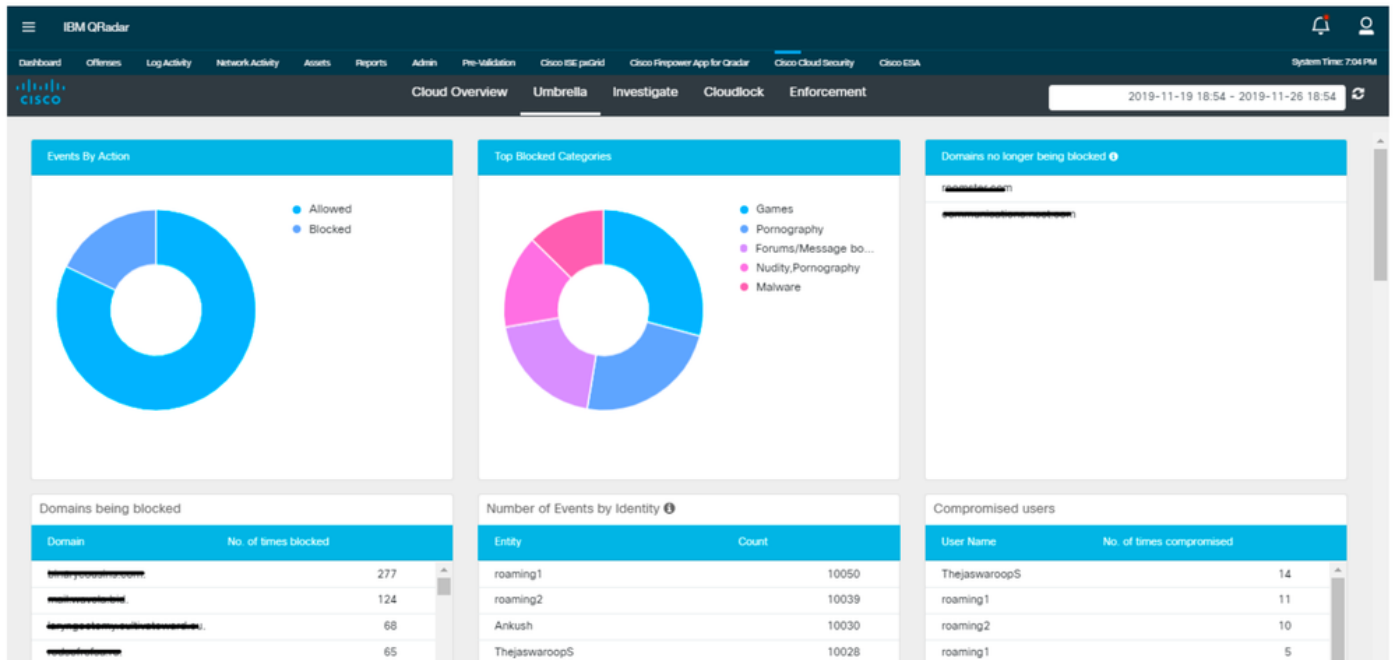
360072257631

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

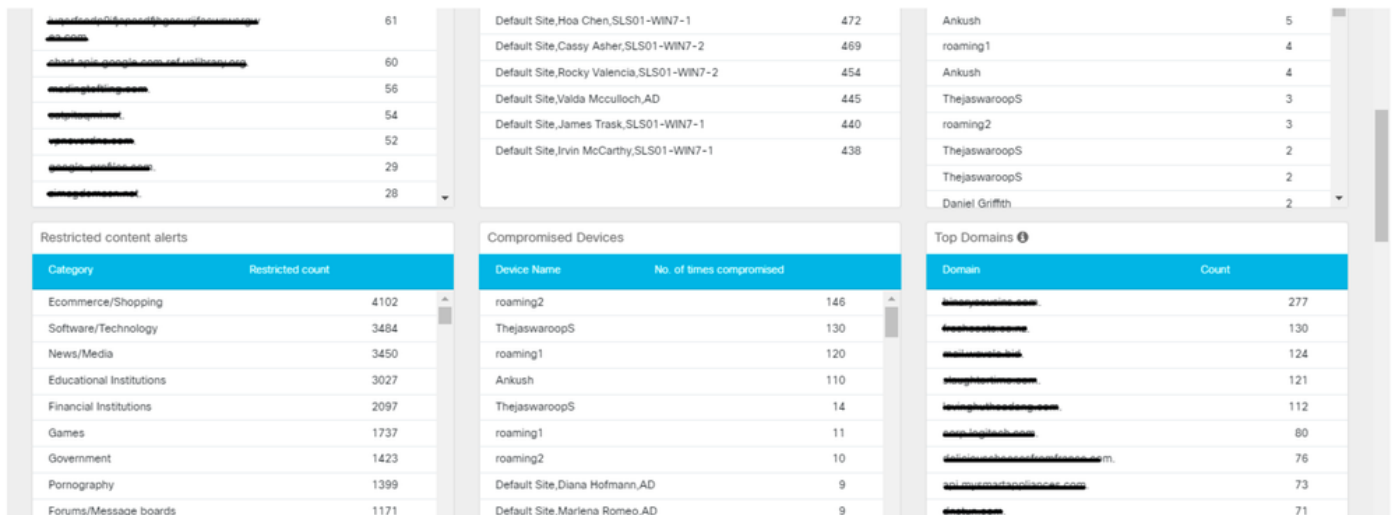
360072257611

Umbrella

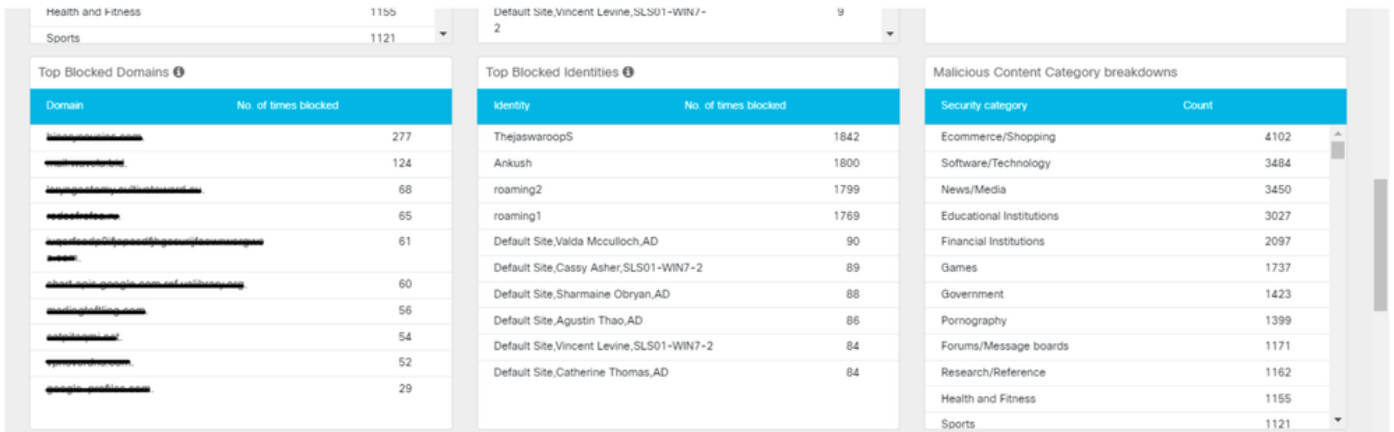
Umbrellaタブには、アクション別イベント、ブロックされた上位カテゴリ、ID別イベントの数、ブロックされているドメイン、ブロックされていないドメイン、侵害されたユーザ、制限されたコンテンツアラート、侵害されたデバイス、上位ドメイン、ブロックされた上位ドメイン、ブロックされた上位ID、悪意のあるコンテンツカテゴリの内訳、上位カテゴリ、アクティビティ、およびユーザアクセスの傾向などの情報が、グラフベースの視覚表現で表示されます。



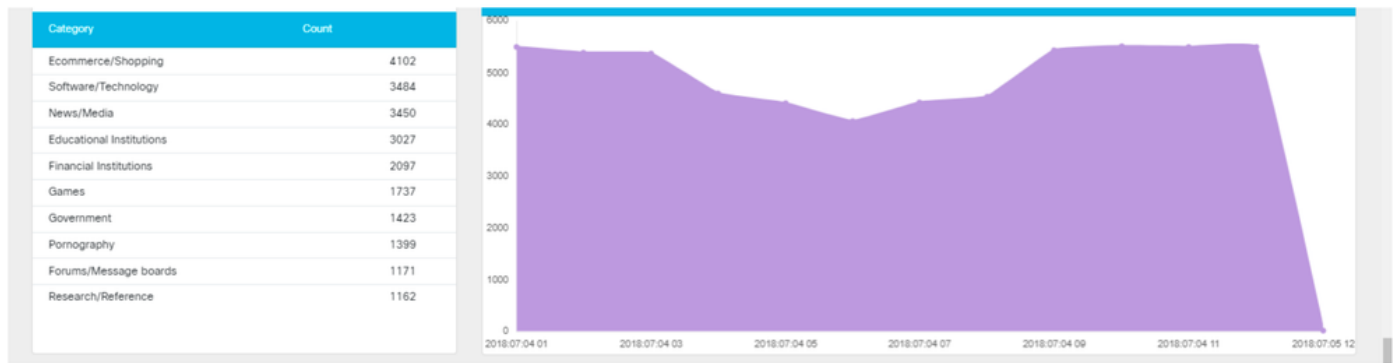
360072263411



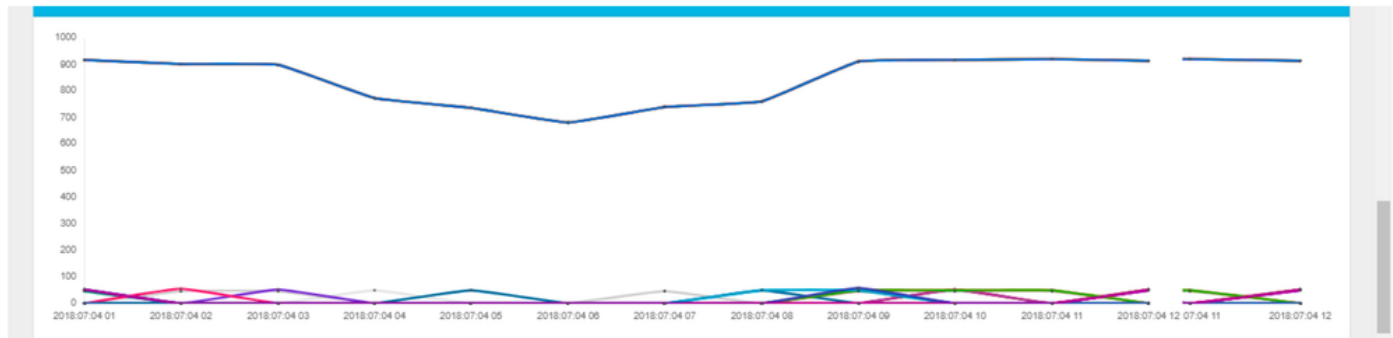
360072263391



360072037372



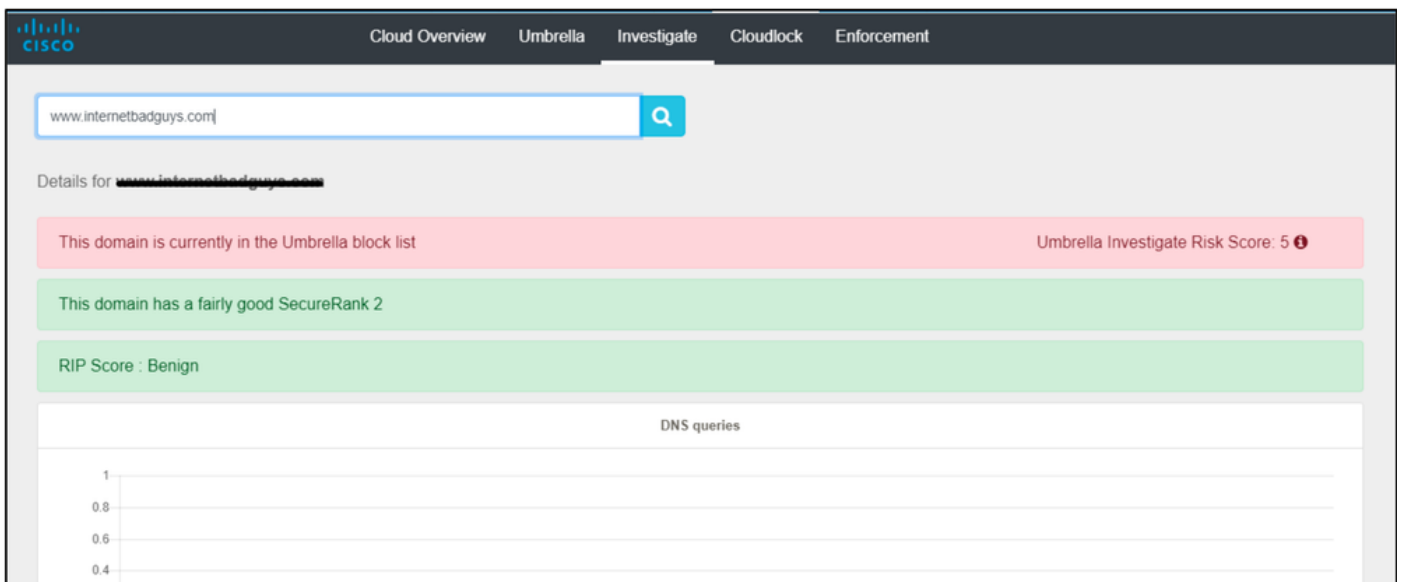
360072263331



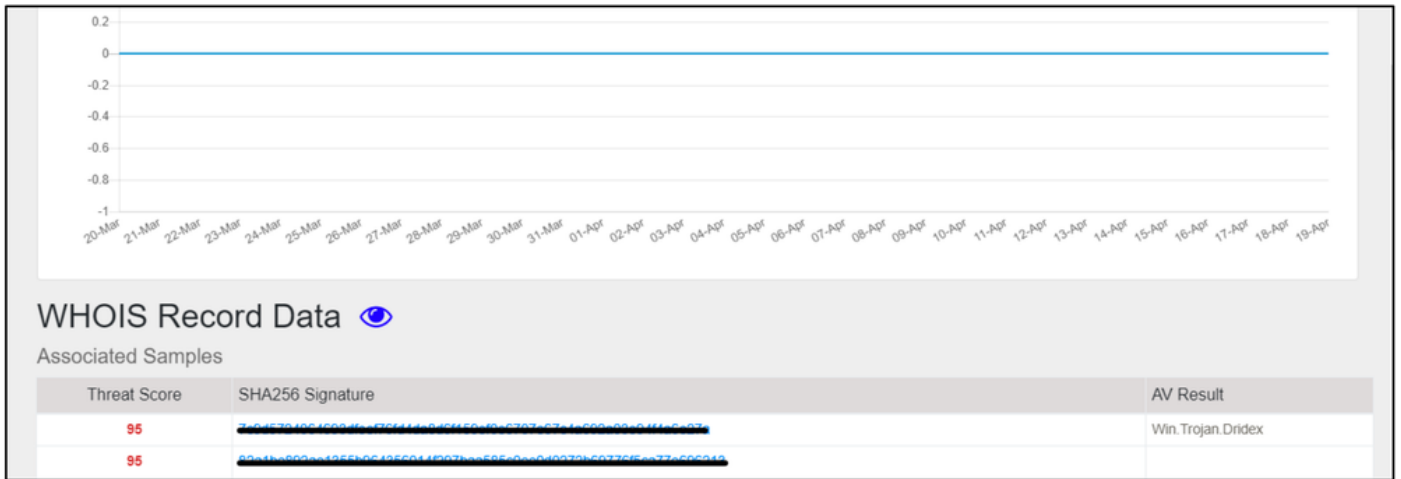
360072263351

調査

「Investigate」タブでは、ホスト名、URL、ASN、IP、ハッシュ、またはメール・アドレスに関連する情報を検索できます。また、WHOISレコード、DGA情報などの情報もあります。



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

CloudLockタブでは、検出されたすべてのインシデントに関する情報を表示できます。また、ドロップダウンメニューから値を選択して[更新]をクリックすることで、インシデントの重大度とステータスを更新することもできます。

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

ユーザは、インシデントに関する詳細を表示するために、任意のイベントにクロックを合わせる

ことができます。

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

「強制」タブ

[強制]タブには、ブロックされているドメインに関する情報が表示されます。ユーザは、ブロックされたドメインを選択し、このインターフェイスからブロックを解除することもできます。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。