

管理適用於IBM QRadar的雲安全應用

目錄

[簡介](#)

[概觀](#)

[訪問思科雲安全應用](#)

[思科雲端安全應用程式元件](#)

[雲概述](#)

[Umbrella](#)

[調查](#)

[CloudLock](#)

[「實施」頁籤](#)

簡介

本文說明如何管理適用於IBM QRadar的思科雲安全應用。

概觀

來自IBM的QRadar是日誌分析的常用的SIEM。它提供強大的介面來分析大量資料，例如Cisco Umbrella為您的組織的DNS流量提供的日誌。Cisco Cloud Security App for IBM QRadar中顯示的資訊通過Cisco Umbrella、CloudLock、Investigate and Enforcement的API獲得。

當您為QRadar設定思科雲安全應用時，它整合了思科雲安全平台的所有資料，並允許您在QRadar控制檯中以圖形形式檢視資料。從應用程式中，分析師可以：

- 調查域、IP地址、電子郵件地址
- 阻止和取消阻止域（實施）
- 檢視網路所有事件的資訊。

本文會指導您如何導航思科雲安全應用。有關如何設定應用程式的說明，請訪問以下網站：[為IBM QRadar配置思科雲安全應用](#)

訪問思科雲安全應用

要在IBM QRadar中導航到Cisco Cloud Security App，請轉至首頁，然後按一下Cisco Cloud Security頁籤。系統將顯示Cloud Overview頁籤和控制面板。然後，您可以訪問Umbrella、Investigate、CloudLock和Enforcement頁籤以檢視日誌。

預設情況下，雲安全應用設定為顯示最近7天的資料。您可以通過按一下右上方的日期範圍來更改時間範圍：

ite

Cloudlock Enforcement

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

2018-04-13 18:18

18

:

18

2018-04-19 18:18

18

:

18

Last 1 Day

Last 2 Days

Last 7 Days

Last 30 Days

This Month

Last Month

Custom Range

Apply

Cancel

<

Apr 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

<

May 2018

>

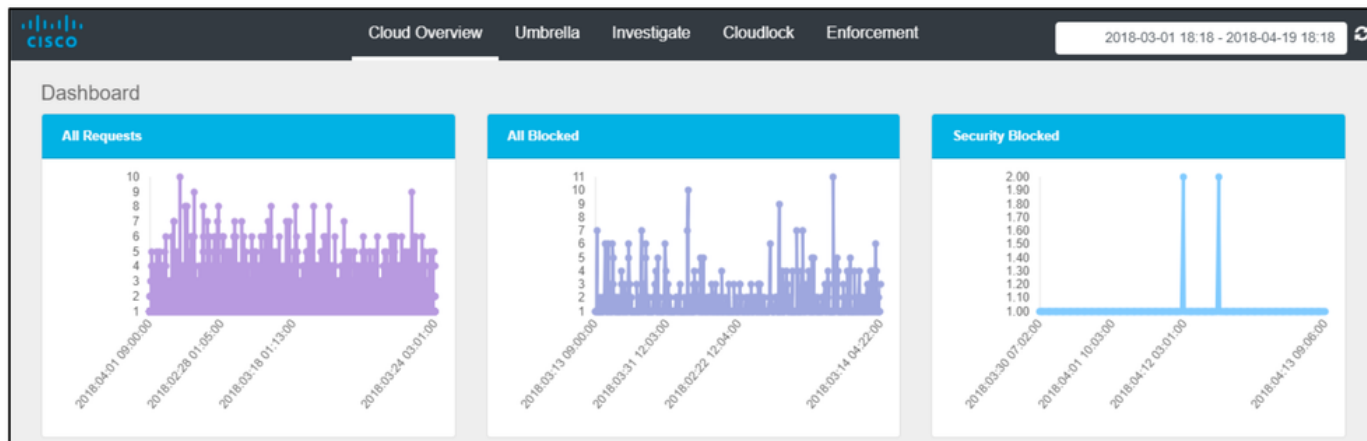
Su	Mo	Tu	We	Th	Fr	Sa
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

360072030052

思科雲端安全應用程式元件

雲概述

Cloud Overview 頁籤以基於圖表的視覺表示方式顯示所有請求、所有被阻止、安全被阻止、可能為 DGA 的、可疑安全排名、Cloudlock 事件、CloudLock Overall、Top Policies 和頂級違規者等資訊。



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

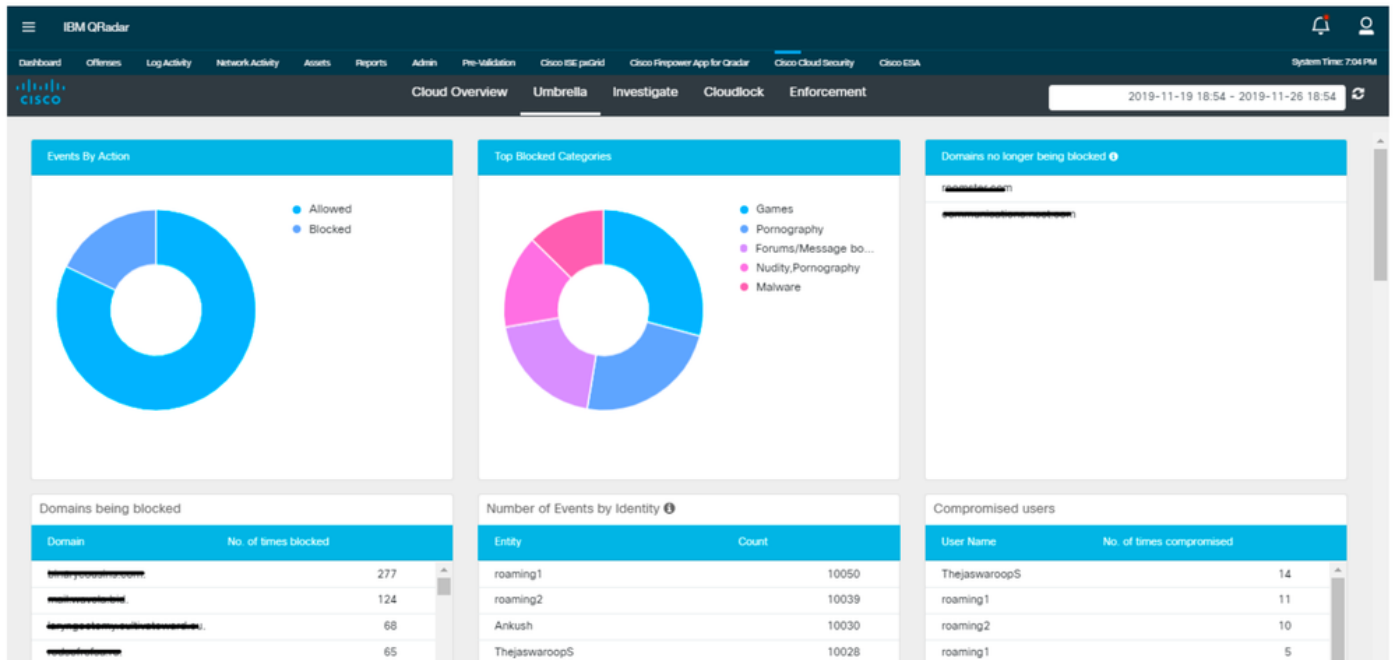
360072257631

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

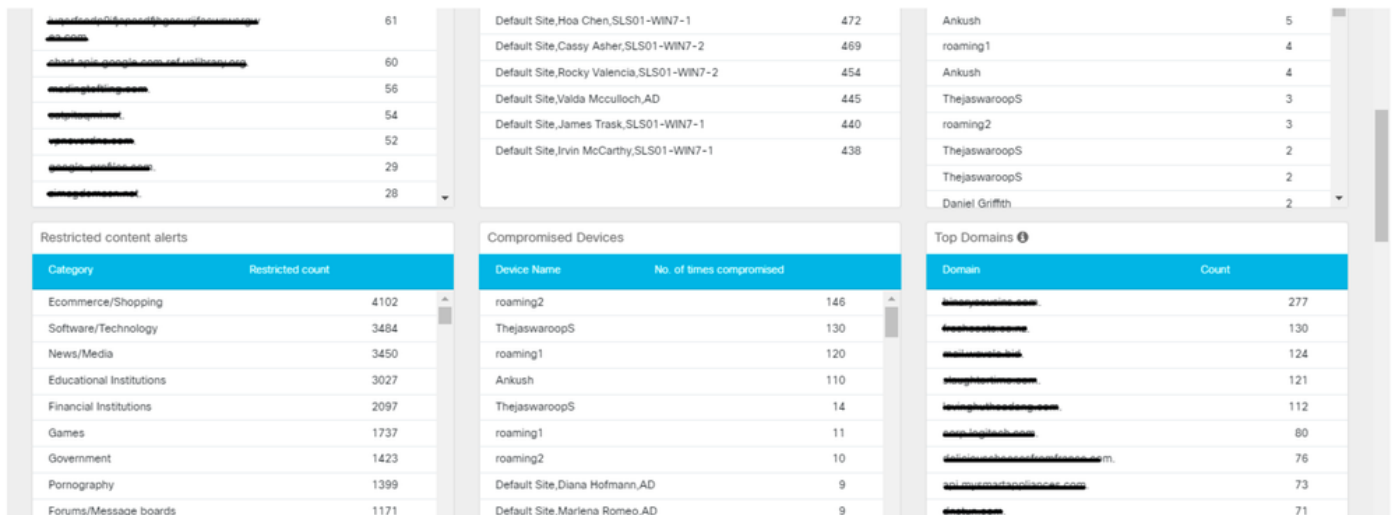
360072257611

Umbrella

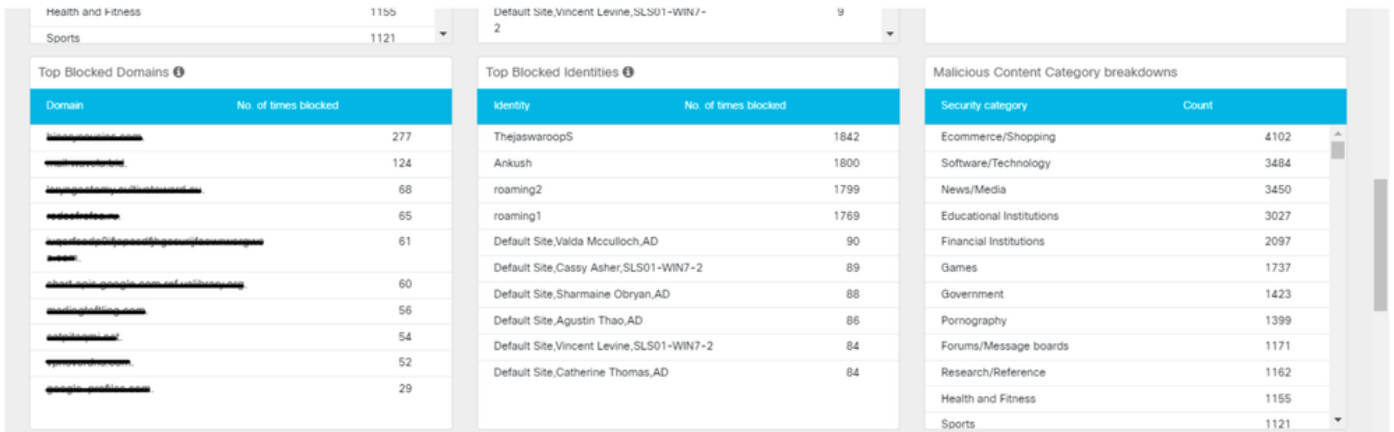
Umbrella頁籤以基於圖表的視覺呈現方式顯示按操作顯示的事件、排名靠前的阻止類別、按標識顯示事件數、正在阻止的域、不再阻止的域、受危害的使用者、受限制的內容警報、受危害的裝置、排名靠前的域、排名靠前的阻止的域、排名靠前的阻止的標識、惡意內容類別細分、排名靠前的類別、活動和使用者訪問趨勢。



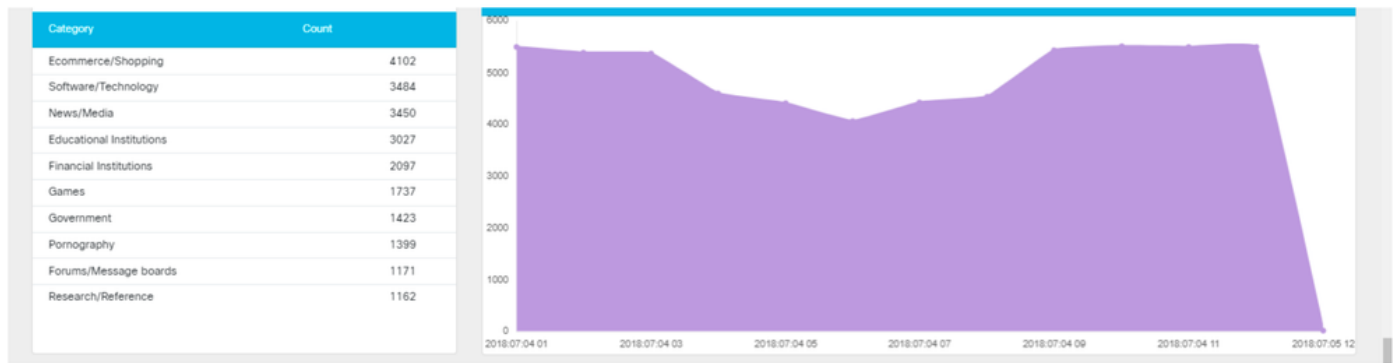
360072263411



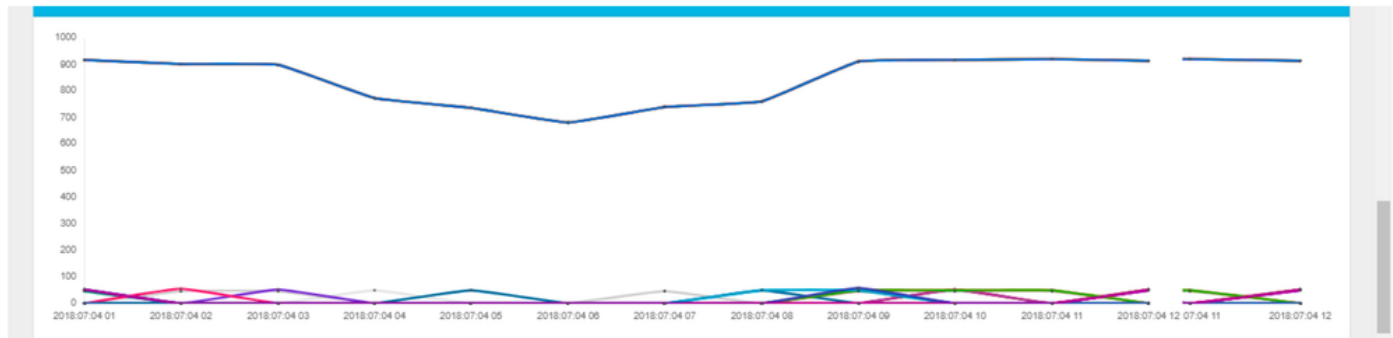
360072263391



360072037372



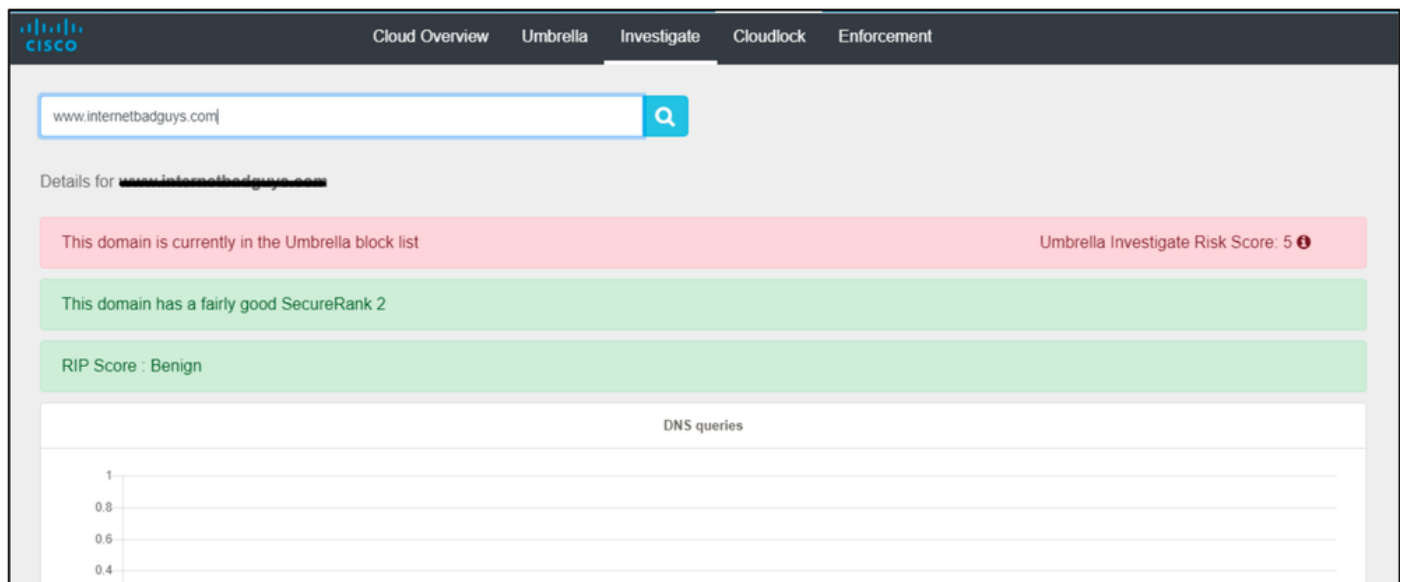
360072263331



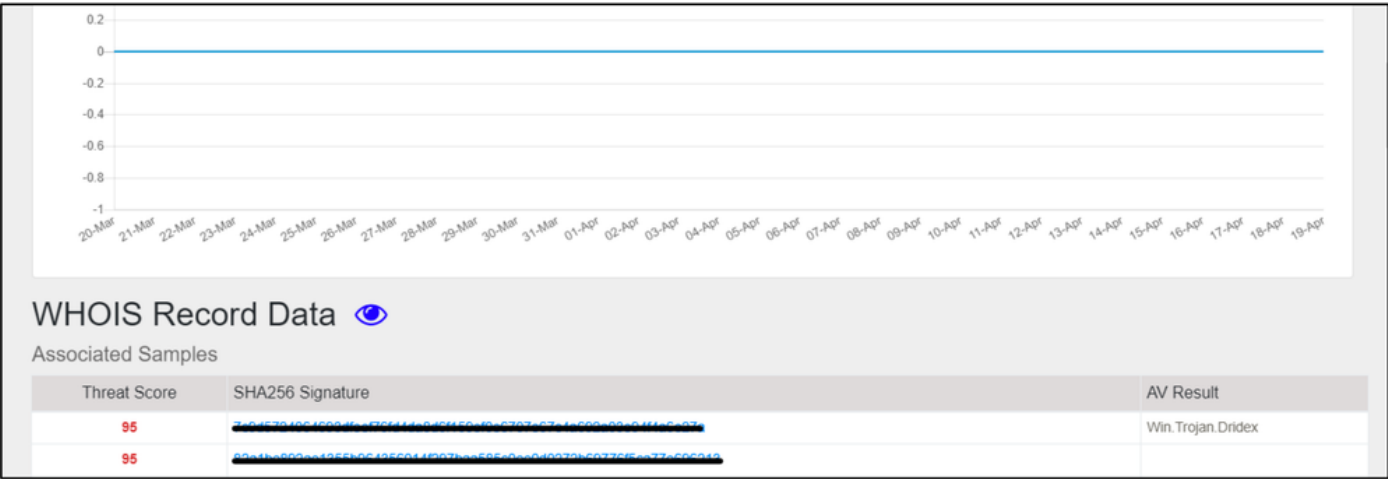
360072263351

調查

Investigate頁籤使使用者可以搜尋與主機名、URL、ASN、IP、雜湊或電子郵件地址相關的資訊。它還有WHOIS記錄、DGA資訊等。



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頁籤允許使用者檢視有關檢測到的所有事件的資訊。使用者還可以通過從下拉選單中選擇值並按一下「更新」來更新事件的嚴重性和狀態。

Cloud Overview Umbrella Investigate Cloudlock Enforcement									
2018-06-01 18:06 - 2018-06-08 18:06									
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	Update
								IN PRO	Update

360072268311

使用者可以鎖定任何事件以檢視有關該事件的更多詳細資訊。

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

「實施」頁籤

Enforcement頁籤顯示有關哪些域被阻止的資訊。使用者還可以選擇阻止的域並從此介面中取消阻止它們。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。