

Gestione la aplicación Cloud Security App para IBM QRadar

Contenido

[Introducción](#)

[Overview](#)

[Acceso a la aplicación Cisco Cloud Security](#)

[Componentes de la aplicación Cisco Cloud Security](#)

[Descripción general de nube](#)

[Umbrella](#)

[Investigar](#)

[CloudLock](#)

[Ficha Aplicación](#)

Introducción

Este documento describe cómo administrar la aplicación Cisco Cloud Security para IBM QRadar.

Overview

QRadar de IBM es un popular SIEM para el análisis de registros. Proporciona una interfaz potente para analizar grandes fragmentos de datos, como los registros proporcionados por Cisco Umbrella para el tráfico DNS de su organización. La información que se muestra en la aplicación Cisco Cloud Security App para IBM QRadar proviene de las API de Cisco Umbrella, CloudLock, Investigate and Enforcement.

Al configurar la aplicación Cisco Cloud Security para QRadar, integra todos los datos de la plataforma Cisco Cloud Security y le permite ver los datos en forma gráfica en la consola de QRadar. Desde la aplicación, los analistas pueden:

- Investigue dominios, direcciones IP y direcciones de correo electrónico
- Bloquear y desbloquear dominios (aplicación)
- Ver la información de todos los incidentes de la red.

En este artículo se explica cómo navegar por la aplicación Cisco Cloud Security. Puede encontrar instrucciones sobre cómo configurar la aplicación aquí: [Configuración de Cisco Cloud Security App para IBM QRadar](#)

Acceso a la aplicación Cisco Cloud Security

Para navegar hasta la aplicación Cisco Cloud Security en IBM QRadar, vaya a la página de inicio

y haga clic en la pestaña Cisco Cloud Security. Aparece la pestaña Descripción general de la nube y el panel. A continuación, puede acceder a las pestañas Umbrella, Investigate, CloudLock y Enforcement para ver sus registros.

La aplicación Cloud Security está configurada para mostrar los datos de los últimos 7 días de forma predeterminada. Puede cambiar el intervalo de tiempo haciendo clic en el intervalo de fechas de la parte superior derecha:

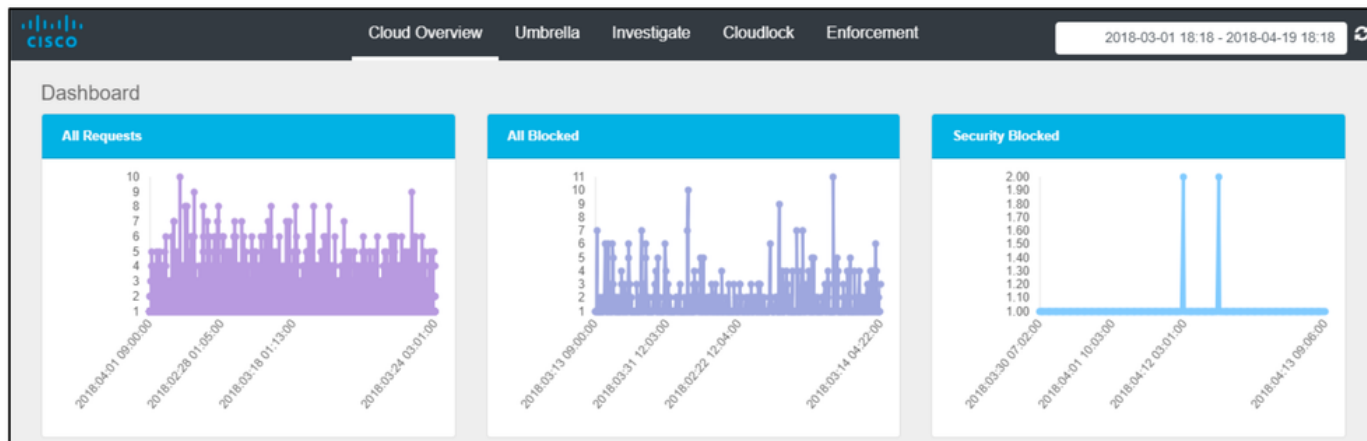
The screenshot shows the Cisco Cloud Security interface with the 'Enforcement' tab selected. The date range is set to '2018-04-13 18:18 - 2018-04-19 18:18'. Below this, there are two calendar views: 'Apr 2018' and 'May 2018'. The 'Apr 2018' calendar shows dates from 25 to 31, with the 13th and 19th highlighted. The 'May 2018' calendar shows dates from 29 to 9, with the 1st and 2nd highlighted. To the right of the calendars, there 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 are 'Apply' and 'Cancel' buttons.

360072030052

Componentes de la aplicación Cisco Cloud Security

Descripción general de nube

La pestaña Descripción general de la nube muestra información como Todas las solicitudes, Todas las bloqueadas, Seguridad bloqueada, DGA probables, Clasificación segura sospechosa, Incidentes de bloqueo de nube, CloudLock en general, Principales políticas y Principales infractores en una representación visual basada en gráficos.



Likely DGA's		Suspicious Secure Rank ⓘ			
Destination	Last Queried	Destination	Securerank	Status Label	Last Queried
example.com	2018-06-05 01:11	example.com	5.64000	safe	2018-06-05 04:16
example.com	2018-06-02 09:01	example.com	-0.03000	malicious	2018-06-01 01:06
example.com	2018-06-05 01:15	example.com	-0.01000	malicious	2018-06-04 09:20
example.com	2018-06-02 11:04	example.com	-18.92000	malicious	2018-06-03 12:03
example.com	2018-06-08 11:05	example.com	-0.01000	malicious	2018-06-05 01:10
example.com	2018-06-02 01:09				
example.com	2018-06-06 03:20				
example.com	2018-06-04 01:07				
example.com	2018-06-08 12:05				

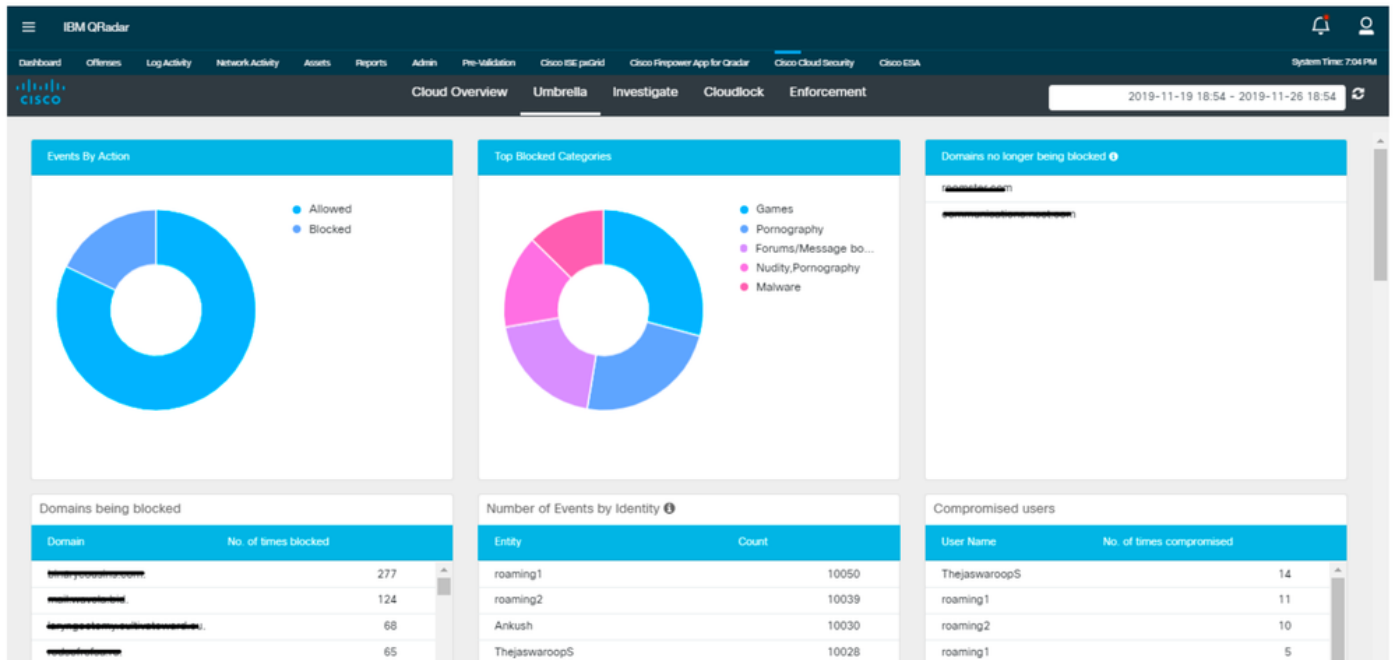
360072257631

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

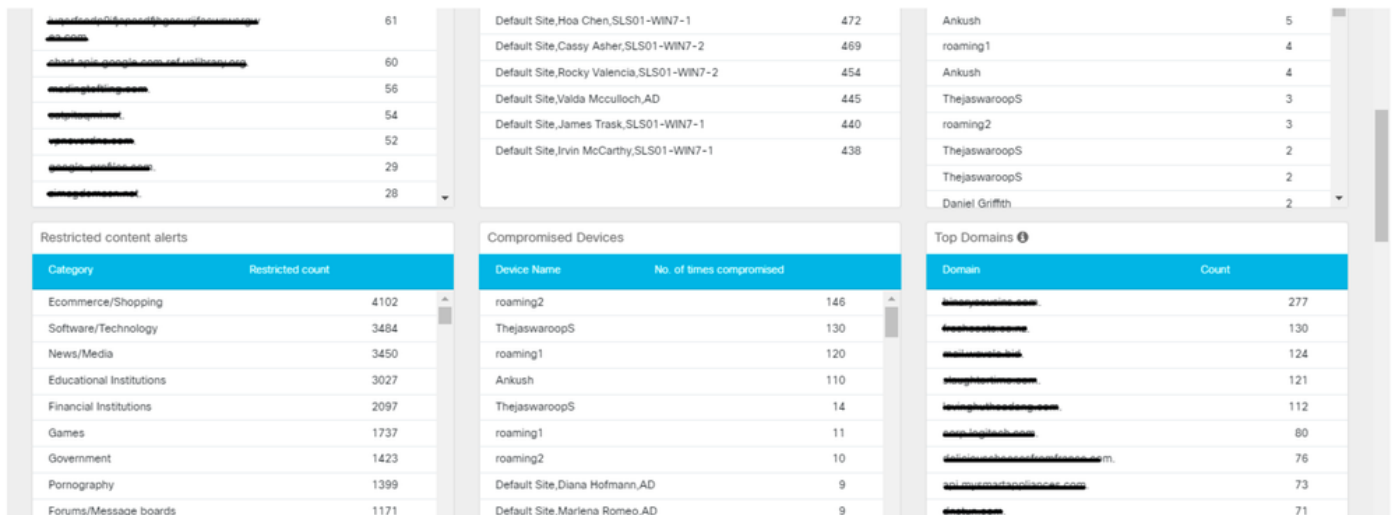
360072257611

Umbrella

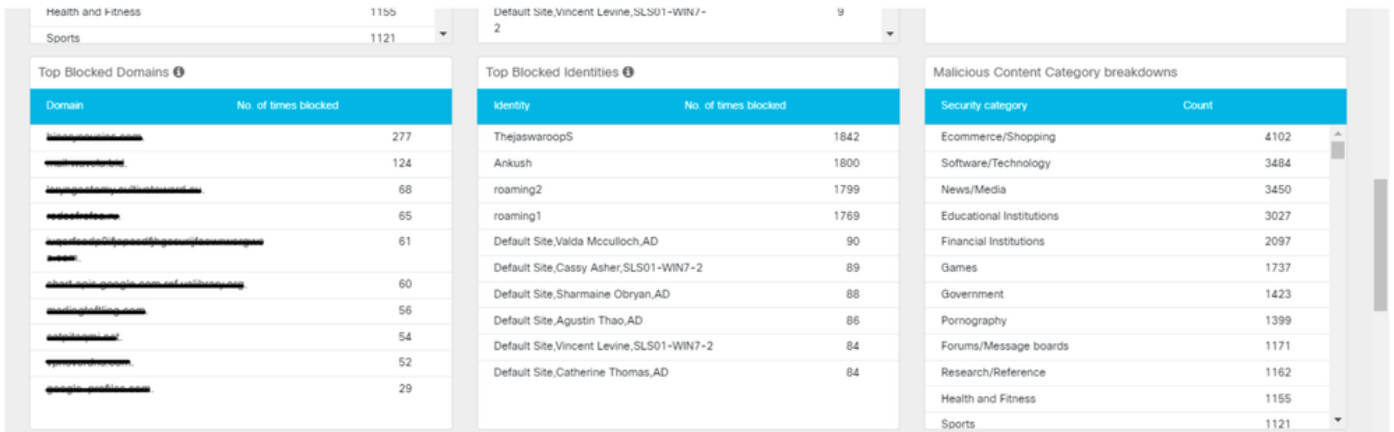
La pestaña Paraguas muestra información como eventos por acción, categorías principales bloqueadas, número de eventos por identidad, dominios que se están bloqueando, dominios que ya no se están bloqueando, usuarios en riesgo, alertas de contenido restringido, dispositivos en riesgo, dominios principales, dominios principales bloqueados, identidades principales bloqueadas, desgloses de categorías de contenido malintencionado, categorías principales, actividad y tendencia de acceso de usuario en una representación visual basada en gráficos.



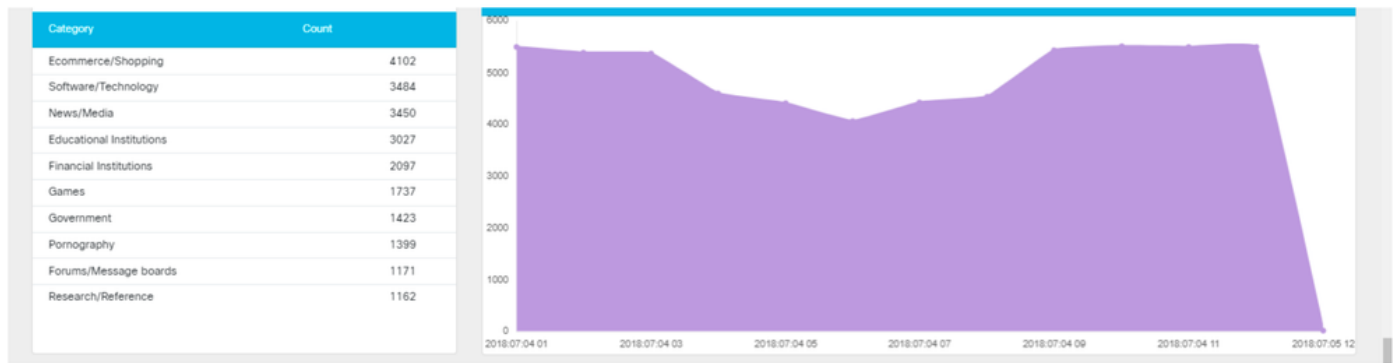
360072263411



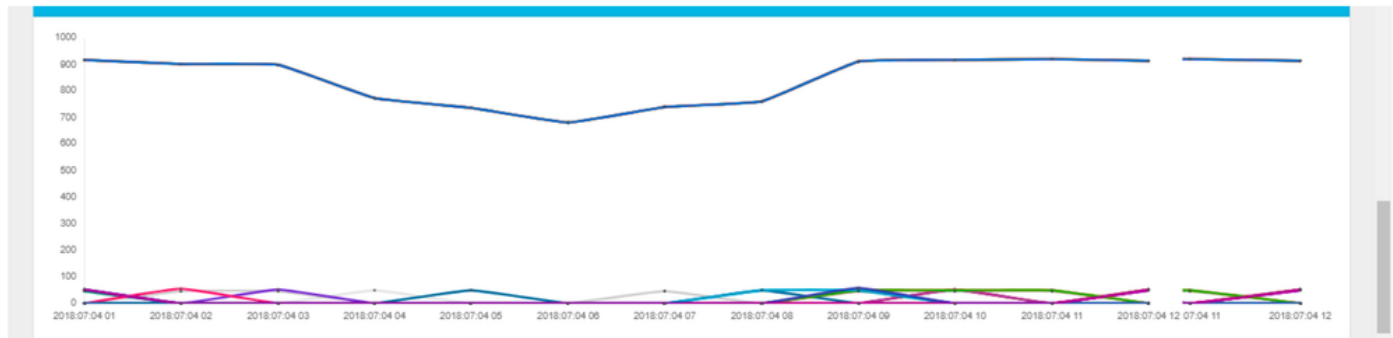
360072263391



360072037372



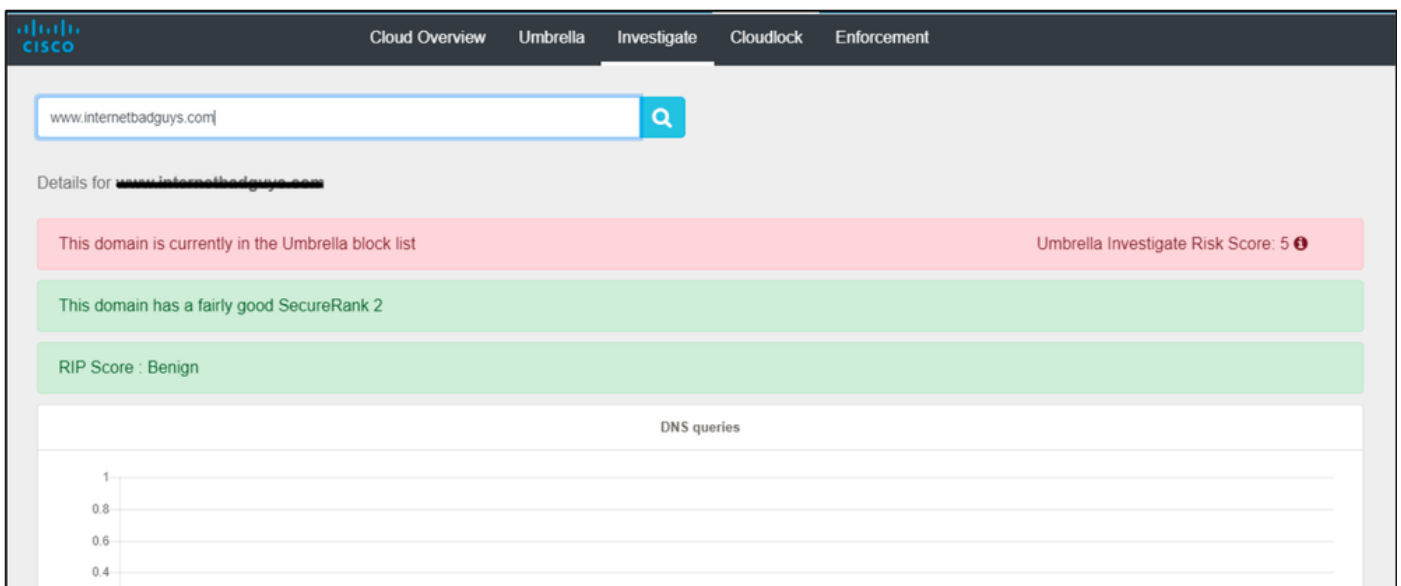
360072263331



360072263351

Investigar

La ficha Investigar permite al usuario buscar la información relacionada con el nombre de host, URL, ASN, IP, Hash o dirección de correo electrónico. También tiene información como el registro WHOIS, información DGA, etc.



360072263511

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

Ficha Aplicación

La ficha Aplicación muestra información sobre los dominios que están bloqueados. Los usuarios también pueden seleccionar dominios bloqueados y desbloquearlos de esta interfaz.

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).