

Gérer l'application de sécurité cloud pour IBM QRadar

Table des matières

[Introduction](#)

[Aperçu](#)

[Accès à l'application Cisco Cloud Security](#)

[Composants de l'application Cisco Cloud Security](#)

[Présentation du cloud](#)

[Umbrella](#)

[Enquêteur](#)

[CloudLock](#)

[Onglet Application](#)

Introduction

Ce document décrit comment gérer l'application Cisco Cloud Security pour IBM QRadar.

Aperçu

QRadar d'IBM est un SIEM populaire pour l'analyse des journaux. Il fournit une interface puissante pour analyser de grandes quantités de données, telles que les journaux fournis par Cisco Umbrella pour le trafic DNS de votre entreprise. Les informations affichées dans l'application de sécurité cloud Cisco pour IBM QRadar proviennent des API de Cisco Umbrella, CloudLock, Investigate et Enforcement.

Lorsque vous configurez l'application Cisco Cloud Security pour QRadar, elle intègre toutes les données de la plate-forme Cisco Cloud Security et vous permet de visualiser les données sous forme graphique dans la console QRadar. À partir de l'application, les analystes peuvent :

- Étudier les domaines, les adresses IP et les adresses e-mail
- Bloquer et débloquer des domaines (application)
- Affichez les informations de tous les incidents du réseau.

Cet article vous explique comment naviguer dans l'application Cisco Cloud Security. Les instructions relatives à la configuration de l'application sont disponibles ici : [Configuration de l'application de sécurité cloud Cisco pour IBM QRadar](#)

Accès à l'application Cisco Cloud Security

Pour accéder à l'application Cisco Cloud Security dans IBM QRadar, accédez à la page d'accueil

et cliquez sur l'onglet Cisco Cloud Security. L'onglet Cloud Overview et le tableau de bord s'affichent. Vous pouvez ensuite accéder aux onglets Umbrella, Investigate, CloudLock et Enforcement pour afficher vos journaux.

Par défaut, l'application de sécurité du cloud est configurée pour afficher les données des 7 derniers jours. Vous pouvez modifier la période en cliquant sur la plage de dates en haut à droite :

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

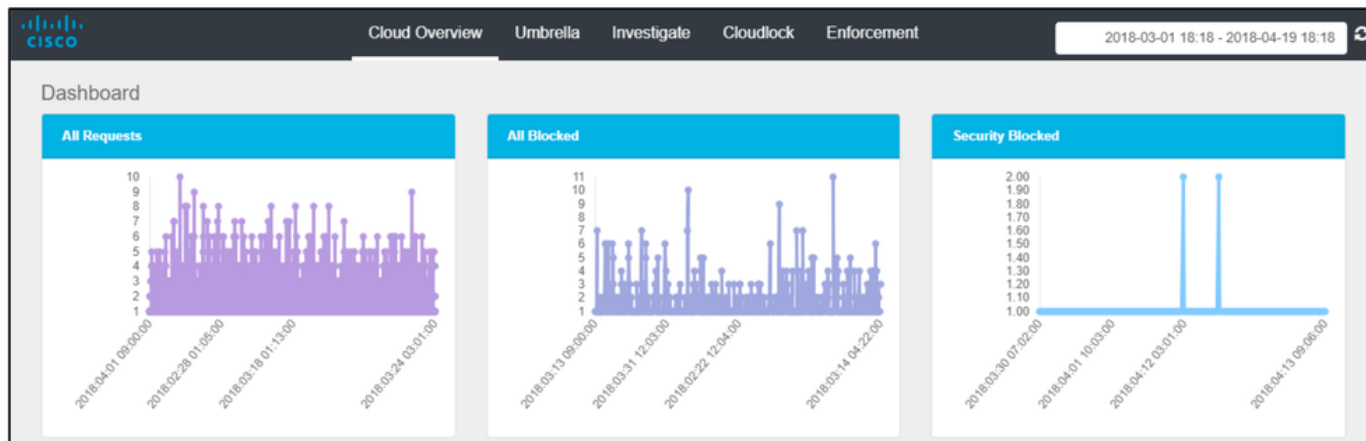
Last 1 Day
Last 2 Days
Last 7 Days
Last 30 Days
This Month
Last Month
Custom Range
Apply Cancel

360072030052

Composants de l'application Cisco Cloud Security

Présentation du cloud

L'onglet Cloud Overview affiche des informations telles que All Requests, All Blocked, Security Blocked, Likely DGA's, Suspicious Secure Rank, Cloudlock Incidents, CloudLock Overall, Top Policies et Top Offenders dans une représentation visuelle basée sur un tableau.



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				

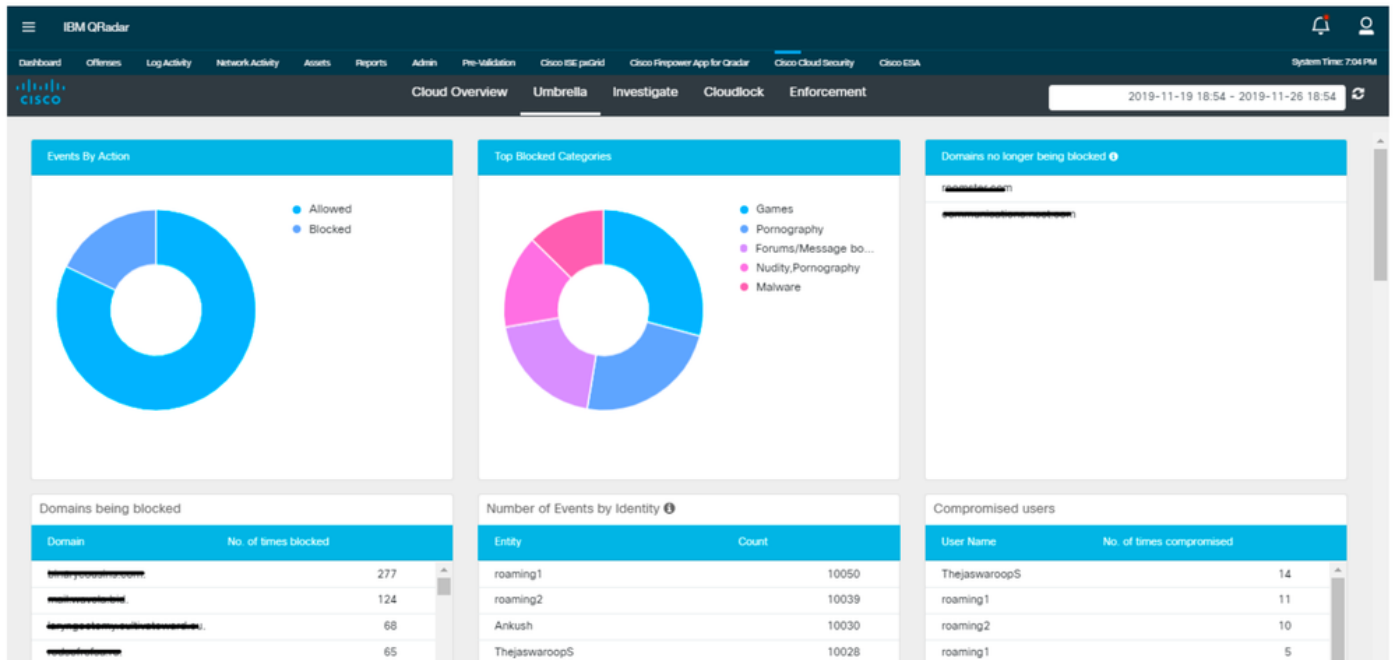
360072257631

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

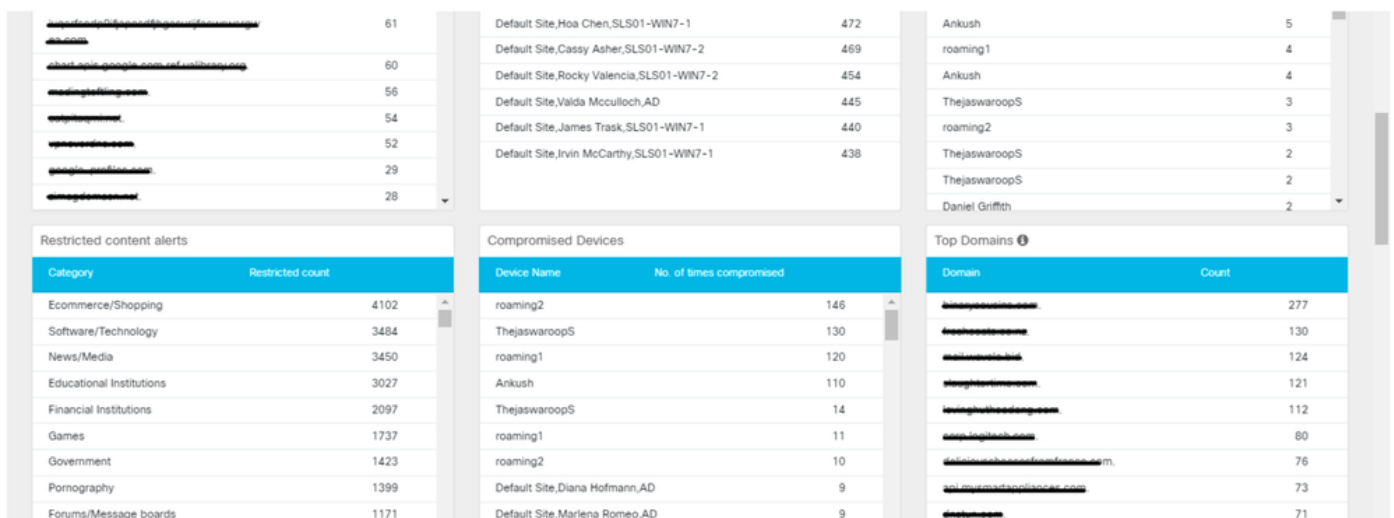
360072257611

Umbrella

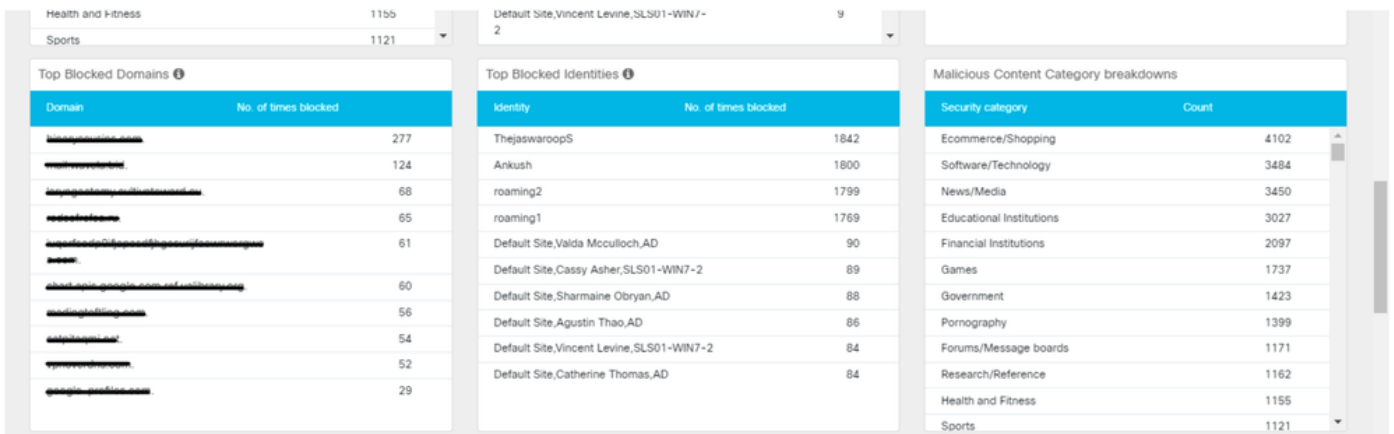
L'onglet Umbrella affiche des informations telles que Événements par action, Principales catégories bloquées, Nombre d'événements par identité, Domaines bloqués, Domaines qui ne sont plus bloqués, Utilisateurs compromis, Alertes de contenu limité, Périphériques compromis, Principaux domaines, Principaux domaines bloqués, Principales identités bloquées, Ventilations des catégories de contenu malveillant, Principales catégories, Tendence de l'activité et de l'accès utilisateur dans une représentation visuelle basée sur un graphique.



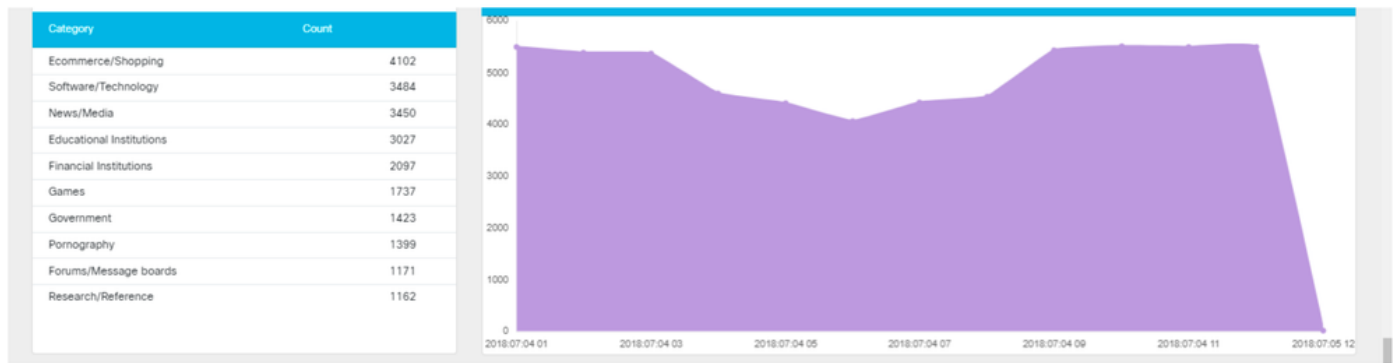
360072263411



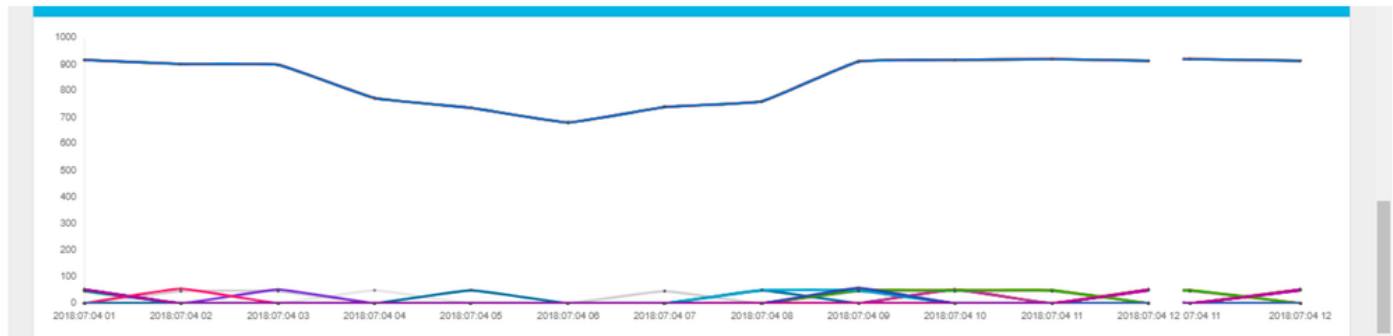
360072263391



360072037372



360072263331



360072263351

Enquêteur

L'onglet Enquêteur permet à l'utilisateur d'effectuer une recherche dans les informations relatives au nom d'hôte, à l'URL, au numéro de système autonome, à l'IP, au hachage ou à l'adresse électronique. Il contient également des informations telles que les enregistrements WHOIS, les informations DGA, etc.

Cloud Overview
Umbrella
Investigate
Cloudlock
Enforcement

Details for ~~www.internetbadguys.com~~

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 5

This domain has a fairly good SecureRank 2

RIP Score : Benign

DNS queries

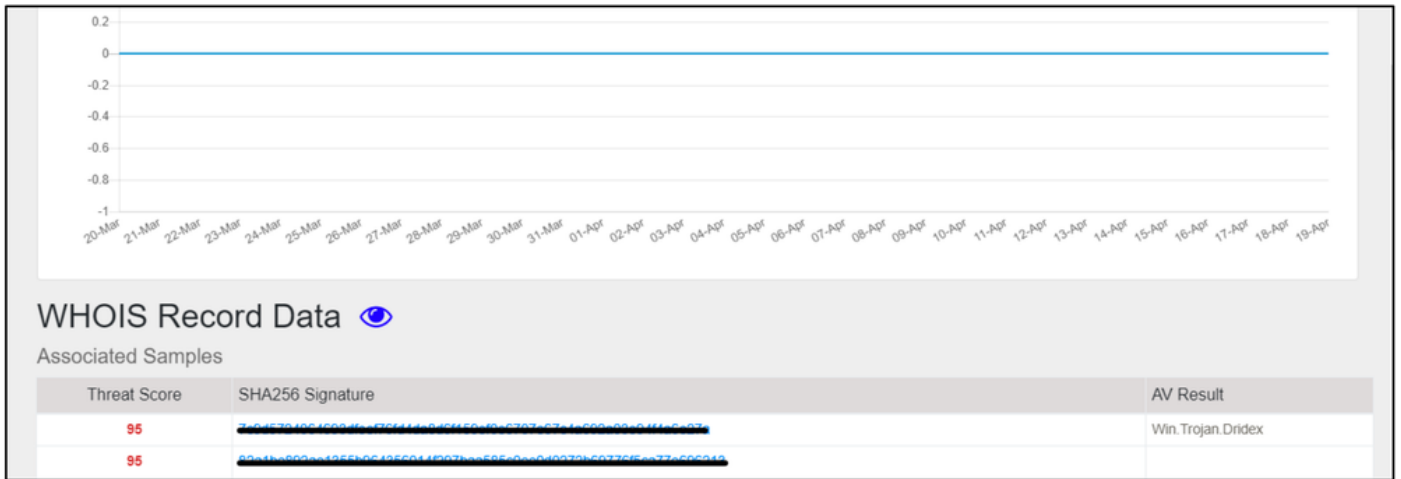
1

0.8

0.6

0.4

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

L'onglet CloudLock permet aux utilisateurs d'afficher des informations sur tous les incidents détectés. Les utilisateurs peuvent également mettre à jour la gravité et l'état de l'incident en sélectionnant les valeurs dans le menu déroulant et en cliquant sur « Mettre à jour ».

Cisco CloudLock									
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	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

Les utilisateurs peuvent surveiller n'importe quel événement pour afficher plus de détails sur

l'incident.

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

Onglet Application

L'onglet Application affiche des informations sur les domaines bloqués. Les utilisateurs peuvent également sélectionner des domaines bloqués et les débloquer de cette 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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.