

Beheer de Cloud Security App voor IBM QRadar

Inhoud

[Inleiding](#)

[Overzicht](#)

[Toegang tot de Cisco Cloud Security App](#)

[Onderdelen van Cisco Cloud Security App](#)

[Overzicht van de cloud](#)

[Umbrella](#)

[onderzoeken](#)

[CloudLock](#)

[Tabblad Handhaving](#)

Inleiding

In dit document wordt beschreven hoe u de Cisco Cloud Security-app voor IBM QRadar kunt beheren.

Overzicht

QRadar van IBM is een populaire SIEM voor log-analyse. Het biedt een krachtige interface voor het analyseren van grote hoeveelheden gegevens, zoals de logs die door Cisco Umbrella worden geleverd voor het DNS-verkeer van uw organisatie. Informatie die wordt weergegeven in de Cisco Cloud Security App voor IBM QRadar wordt geleverd via de API's van Cisco Umbrella, CloudLock, Investigate en Enforcement.

Wanneer u de Cisco Cloud Security-app voor QRadar instelt, worden alle gegevens van het Cisco Cloud Security-platform geïntegreerd en kunt u de gegevens in grafische vorm bekijken in de QRadar-console. Vanuit de applicatie kunnen analisten:

- Domeinen, IP-adressen, e-mailadressen onderzoeken
- Domeinen blokkeren en deblokkeren (handhaving)
- Bekijk de informatie over alle incidenten van het netwerk.

In dit artikel wordt uitgelegd hoe u door de Cisco Cloud Security-app kunt navigeren. Instructies voor het instellen van de toepassing vindt u hier: [De Cisco Cloud Security App configureren voor IBM QRadar](#)

Toegang tot de Cisco Cloud Security App

Om naar de Cisco Cloud Security App in IBM QRadar te navigeren, gaat u naar de startpagina en klikt u op het tabblad Cisco Cloud Security. Het tabblad Cloud Overview en het Dashboard worden

weergegeven. U kunt vervolgens toegang krijgen tot de tabbladen Umbrella, Investigate, CloudLock en Enforcement om uw logs te bekijken.

De Cloud Security App is standaard ingesteld om de gegevens van de afgelopen 7 dagen weer te geven. U kunt het tijdsbestek wijzigen door rechtsboven op het datumbereik te klikken:

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

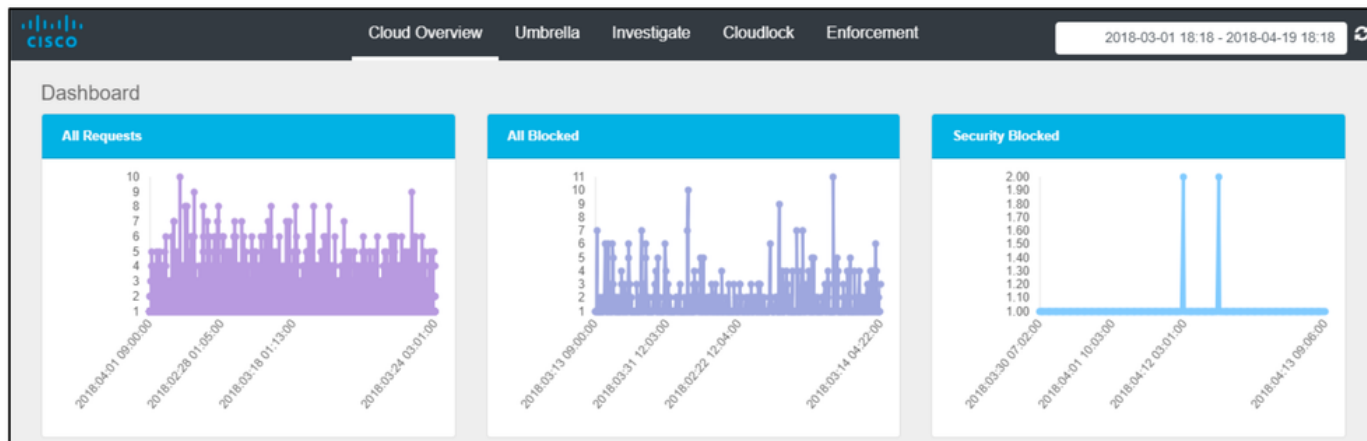
Last 1 Day
Last 2 Days
Last 7 Days
Last 30 Days
This Month
Last Month
Custom Range
Apply Cancel

360072030052

Onderdelen van Cisco Cloud Security App

Overzicht van de cloud

Op het tabblad Cloud Overview wordt informatie weergegeven zoals Alle aanvragen, Alle geblokkeerde aanvragen, Beveiliging geblokkeerd, Waarschijnlijk DGA's, Verdachte veilige rang, Cloudlock-incidenten, CloudLock Overall, Top Policies en Top Offenders in een op diagrammen gebaseerde visuele weergave.



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				

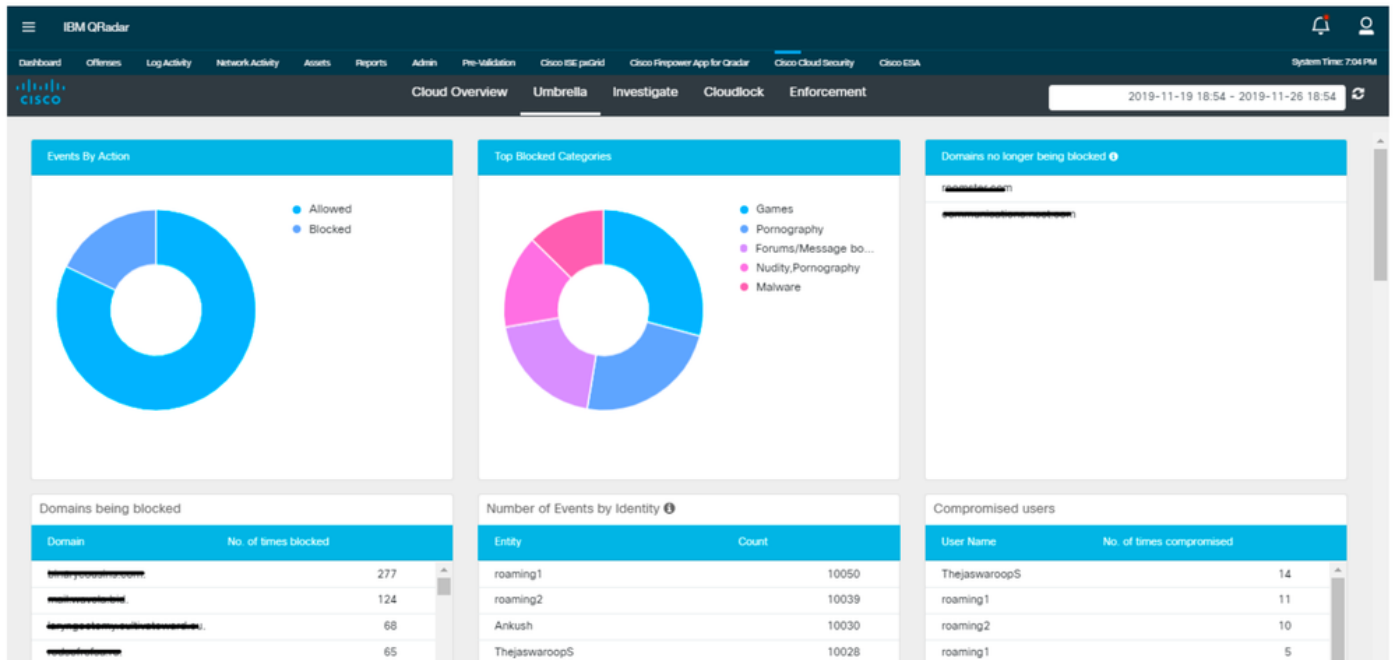
360072257631

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

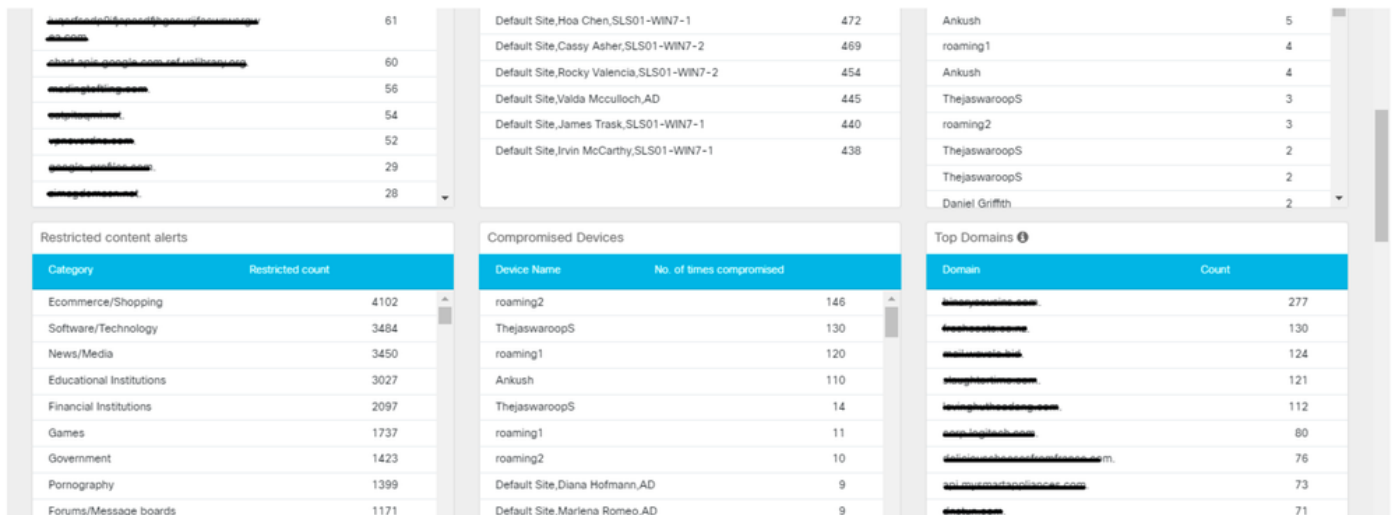
360072257611

Umbrella

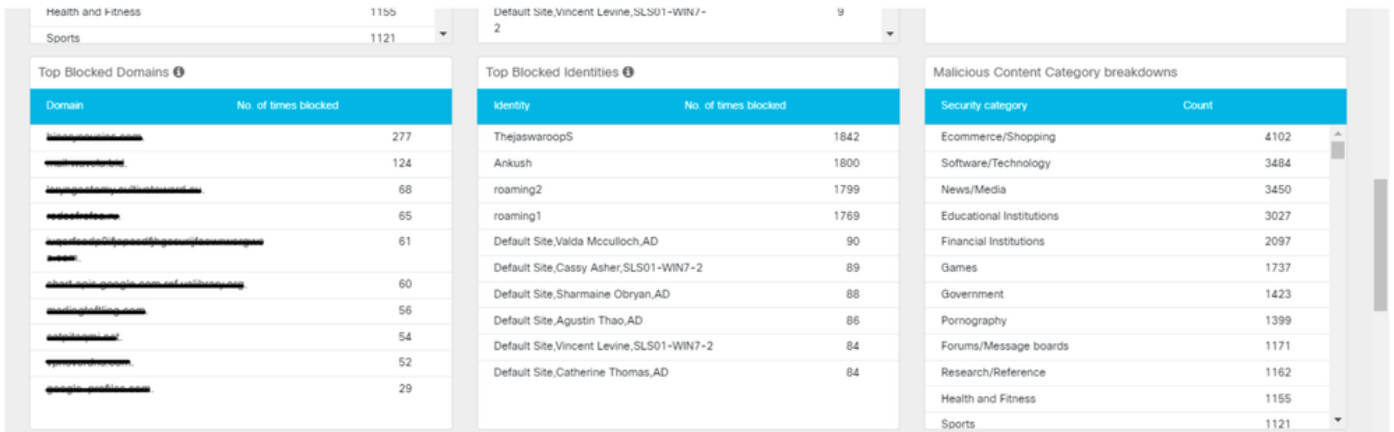
Op het tabblad Umbrella wordt informatie weergegeven zoals Gebeurtenissen op actie, Bovenste geblokkeerde categorieën, Aantal gebeurtenissen op identiteit, Geblokkeerde domeinen, Geblokkeerde domeinen, Gevaarlijke gebruikers, Gevaarlijke inhoudswaarschuwingen, Gevaarlijke apparaten, Bovenste domeinen, Bovenste geblokkeerde domeinen, Bovenste geblokkeerde identiteiten, Uitsplitsingen van kwaadwillige inhoudscategorieën, Bovenste categorieën, Activiteit en Trend gebruikerstoegang in een grafische visuele weergave.



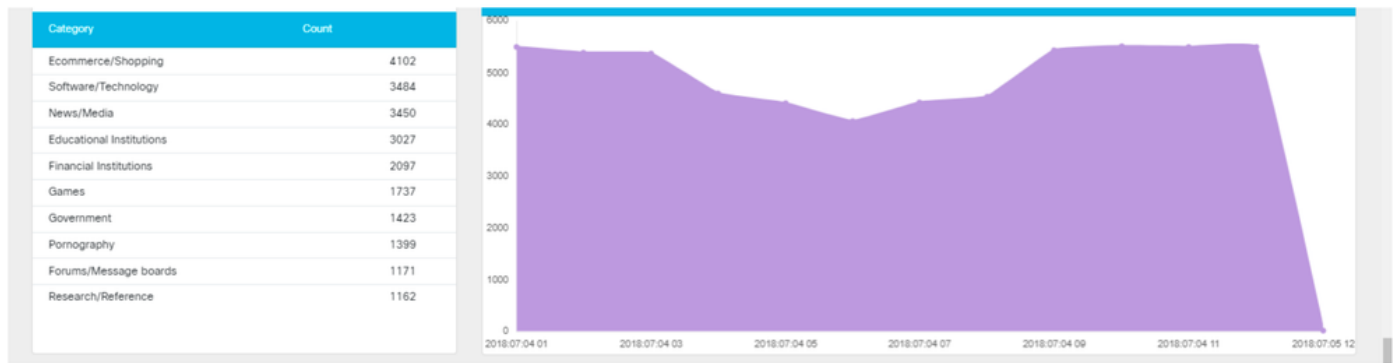
360072263411



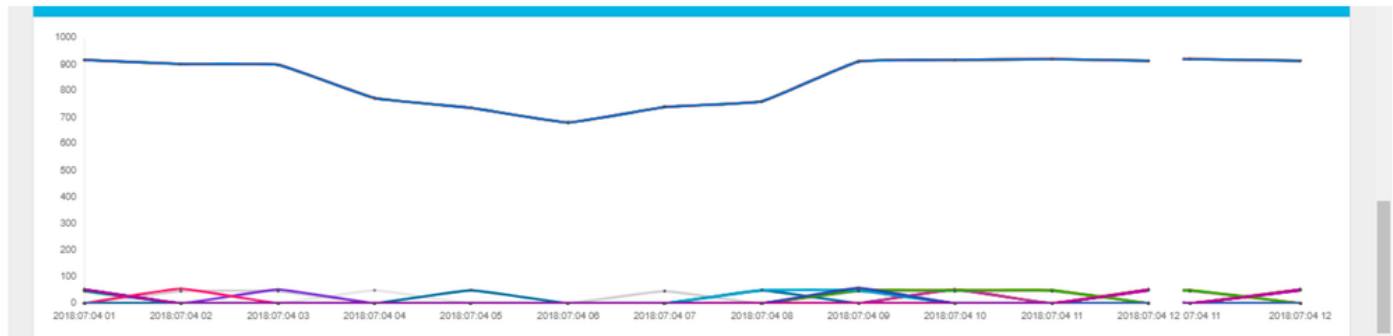
360072263391



360072037372



360072263331



360072263351

onderzoeken

Op het tabblad Onderzoeken kan de gebruiker zoeken naar de informatie met betrekking tot hostnaam, URL, ASN, IP, Hash of e-mailadres. Het heeft ook informatie zoals WHOIS-record, DGA-informatie enzovoort.

Cloud Overview
Umbrella
Investigate
Cloudlock
Enforcement

Details for www.internetbadguys.com

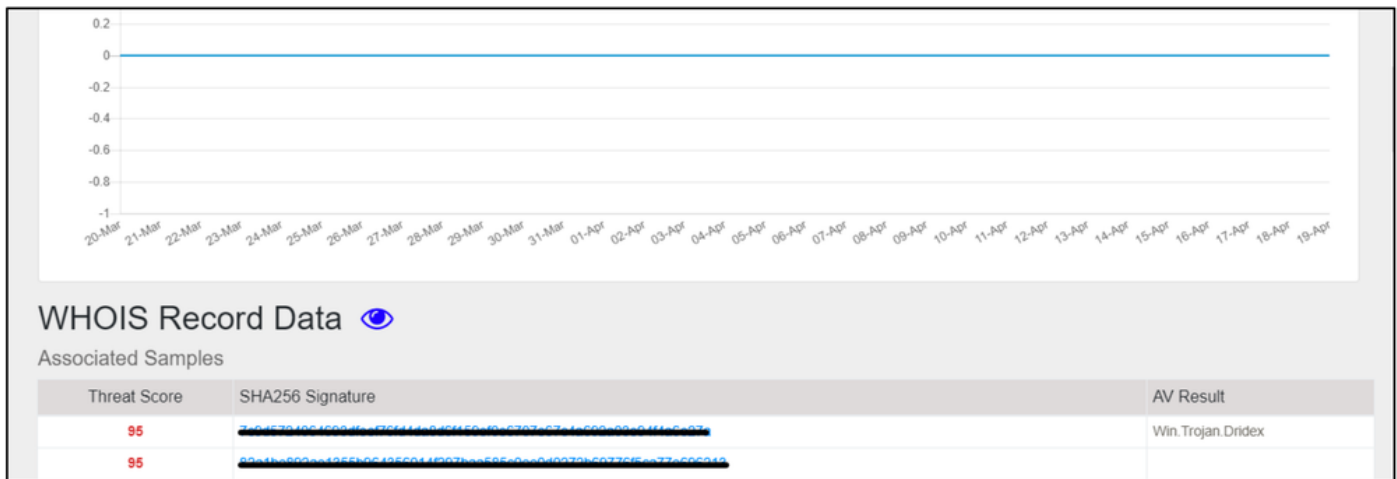
This domain is currently in the Umbrella block list
 Umbrella Investigate Risk Score: 5

This domain has a fairly good SecureRank 2

RIP Score : Benign

DNS queries

360072263511

WHOIS Record Data

Threat Score	SHA256 Signature	AV Result
95	7e04f7b19516994ba376141e0d6c55e0e3707c371e609e8b044e9c937	Win. Trojan.Dridex
95	89e4be809ee0355b0c4956044607bae585e0ae0d0070b60736fe973e66949	

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

Op het tabblad CloudLock kunnen gebruikers informatie bekijken over alle gedetecteerde incidenten. Gebruikers kunnen ook de ernst en status van het incident bijwerken door de waarden in het vervolgkeuzemenu te selecteren en op "Bijwerken" te klikken.

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 v	IN PRO v	Update
132352852	office365	1	AppTest	Jun 03, 2018 5:24:23 pm	AzureActiveDirectory User Login Failed	Mohit Vaish	CRITIC v	--Select-- NEW IN PROGRESS RESOLVED DISMISSED	Update
132352856	office365	1	AppTest	Jun 03, 2018 5:24:39 pm	AzureActiveDirectory User Logg ed In	Khiladi Bayal	CRITIC v	RESOL	Update
132490696	office365	1	AppTest	Jun 04, 2018 4:39:22 pm	AzureActiveDirectory User Logg ed In	Anil Kumar Yari apalli	CRITIC v	IN PRO v	Update

360072268311

Gebruikers kunnen op elk van de gebeurtenissen klikken om meer details over het incident te

bekijken.

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

Tabblad Handhaving

Op het tabblad Handhaving wordt informatie weergegeven over welke domeinen worden geblokkeerd. Gebruikers kunnen ook geblokkeerde domeinen selecteren en deblokkeren vanuit deze interface.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.