Cisco Cloud Security App for IBM QRadar

Version Number: 0.4

Date: Oct 10, 2018

Contents

1. Introduction

1.1. Overview

The Cisco Cloud Security App for IBM QRadar provide insight from multiple security products (Investigate, Enforcement and CloudLock) and integrates them with QRadar. The Cisco Cloud Security platform helps the user to automate security and contain threats faster and directly from QRadar.

1.2. About this Document

This document explains how to deploy and use the Cisco Cloud Security App for IBM QRadar.

1.3. About the app

QRadar provides a robust solution for Security Information and Event Management (SIEM), anomaly detection, incident forensics, and vulnerability management.

When you set up Cisco Cloud Security app for QRadar, it integrates all the data from Cisco Cloud Security platform and allows you to view the data in graphical form in the QRadar console. From the application, analysts can:

- Investigate the domains, ip addresses, email addresses.
- Block and Unblock domains(Enforcement).
- View the information of all the incidents of the network.

1.4. Prerequisites

- IBM QRadar version 7.2.8 patched to 20170726184122 and above.
- Cisco Cloud Security
- Administration privileges

2. General

2.2. Installation

1. Download and install the Cisco Cloud Security App for IBM QRadar:
2. Navigate to the IBM X-Force Exchange console:
   https://exchange.xforce.ibmcloud.com/hub
3. Search for ‘Cisco Cloud Security’
4. Download and install the application as a QRadar Plugin (For more details plugin installation, click here)
5. After the installation, deploy changes in QRadar.

2.3. Configuration

2.3.1. IBM QRadar AWS Protocol Fix (Only for beta users)

Current AWS protocol used by IBM has connection issue for which temporary fix can be used until a fix is released by IBM. Following are the steps for applying the temporary fix:

1. Download and SCP the attached jar file onto the QRadar System.

2. Disable the Log Source ---> To be able to make changes to it
3. # mkdir /store/IBMSupport/aws_jar_backup ---> Make a directory to back up the existing JAR file
4. #mv/opt/qradar/jars/q1labs_semsources_protocol_amazonawsrest.jar /store/IBMSupport/aws_jar_backup ---> Move the existing JAR into the backup folder
5. Unzip the attachment in the email on your Windows System and SCP the resulting file q1labs_semsources_protocol_amazonawsrest.jar onto the QRadar Console and place it in the home directory of the root user. ---> To make the jar available on the QRadar Console
6. # cp ~/q1labs_semsources_protocol_amazonawsrest.jar /opt/qradar/jars/ ---> To copy the modified JAR in folder from where the QRadar System will use it.
7. # systemctl restart ecs-ecs ---> To restart the event collection services
8. Enable the Log Source in the QRadar Console

2.3.2. Log Source

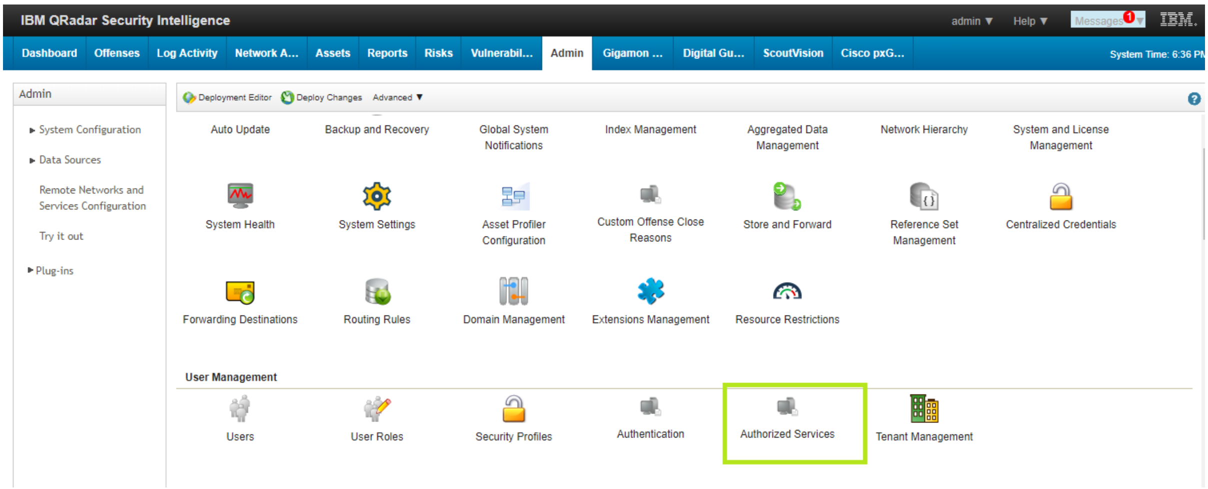
1. From the **Admin** tab on the QRadar navigation bar, scroll down to Log Sources.
2. Search the cisco_umbrella_dns_logs, cisco_umbrella_ip_logs, cisco_umbrella_proxy_logs and configure the log sources with correct fields.

Note: User can also create the log source manually, but the log source name must be cisco_umbrella_dns_logs, cisco_umbrella_ip_logs, cisco_umbrella_proxy_logs.

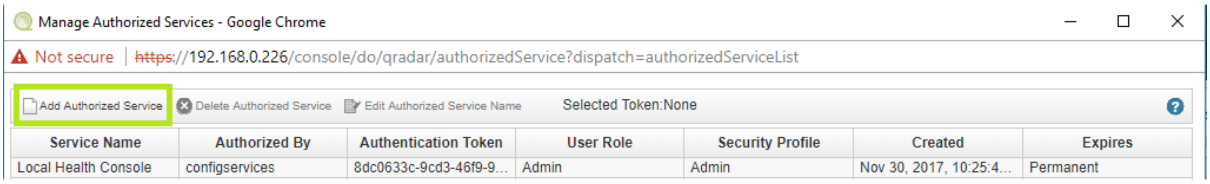
2.3.3. Generation of Authentication Token

1. Login to QRadar and go to Admin tab.

2. Select Authorized Services.



3. Click on Add Authorized Service


Manage Authorized Services - Google Chrome
Not secure
Add Authorized Service
Delete Authorized Service
Edit Authorized Service Name

https://192.168.0.226/console/do/qradar/authorizedService?dispatch=authorizedServiceList

Selected Token:None

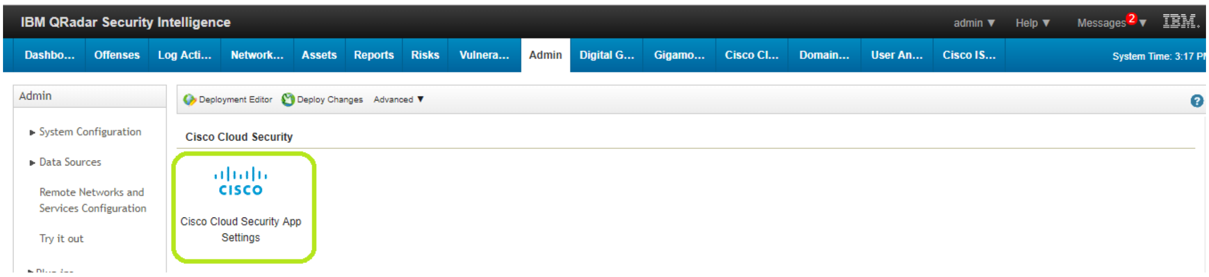
Service Name	Authorized By	Authentication Token	User Role	Security Profile	Created	Expires
Local Health Console	configservices	8dc0633c-9cd3-46f9-9...	Admin	Admin	Nov 30, 2017, 10:25:4...	Permanent

4. Enter the details and generate the authentication token.

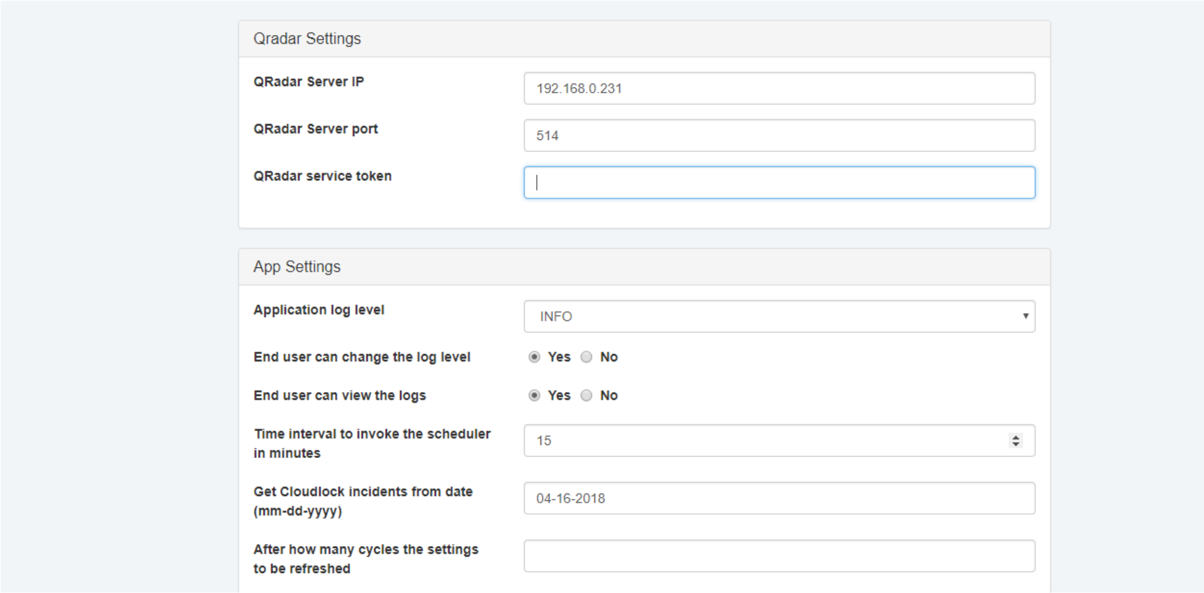
5. After generating the token Deploy Changes.

2.3.4. Configuring the Cisco Cloud Security App

1. From the **Admin** tab on the QRadar navigation bar, scroll down and open Cisco Cloud Security App Settings.



2. Enter the Authentication Token generated in previous step and other details and click on Submit.



Qradar Settings

QRadar Server IP: 192.168.0.231

QRadar Server port: 514

QRadar service token:

App Settings

Application log level: INFO

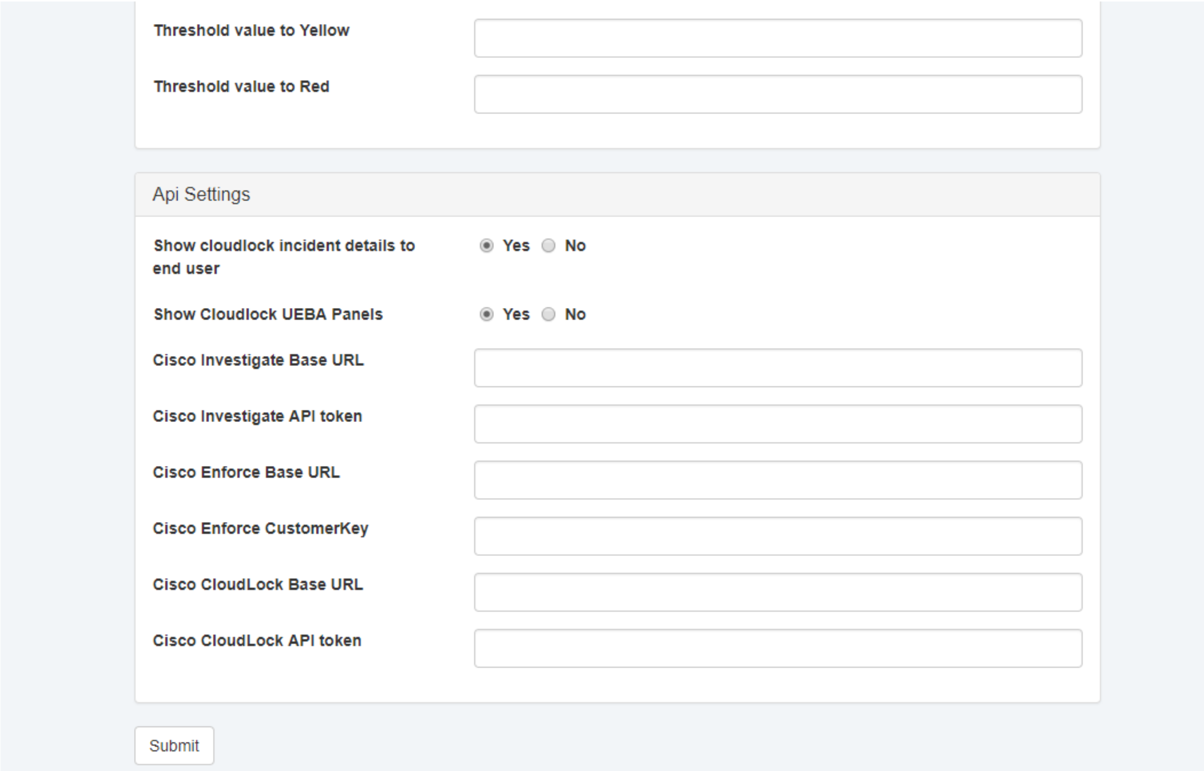
End user can change the log level: ● Yes ○ No

End user can view the logs: ● Yes ○ No

Time interval to invoke the scheduler in minutes: 15

Get Cloudlock incidents from date (mm-dd-yyyy): 04-16-2018

After how many cycles the settings to be refreshed:



Threshold value to Yellow:

Threshold value to Red:

Api Settings

Show cloudlock incident details to end user: ● Yes ○ No

Show Cloudlock UEBA Panels: ● Yes ○ No

Cisco Investigate Base URL:

Cisco Investigate API token:

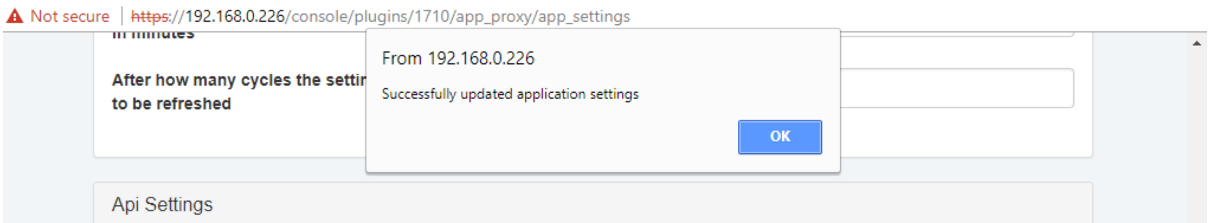
Cisco Enforce Base URL:

Cisco Enforce CustomerKey:

Cisco CloudLock Base URL:

Cisco CloudLock API token:

3. After click on Submit, a popup will appear displaying Successfully updated application settings.



Not secure
~~https~~://192.168.0.226/console/plugins/1710/app_proxy/app_settings
in minutes
After how many cycles the settir
to be refreshed

From 192.168.0.226

Successfully updated application settings

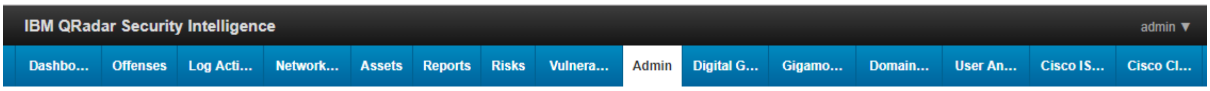
3. Cisco Cloud Security App

3.1. General

Information displayed in Cisco Cloud Security App for IBM QRadar comes through the API's of Cisco CloudLock, Investigate and Enforcement.

To navigate to the Cisco Cloud Security app, in IBM QRadar:

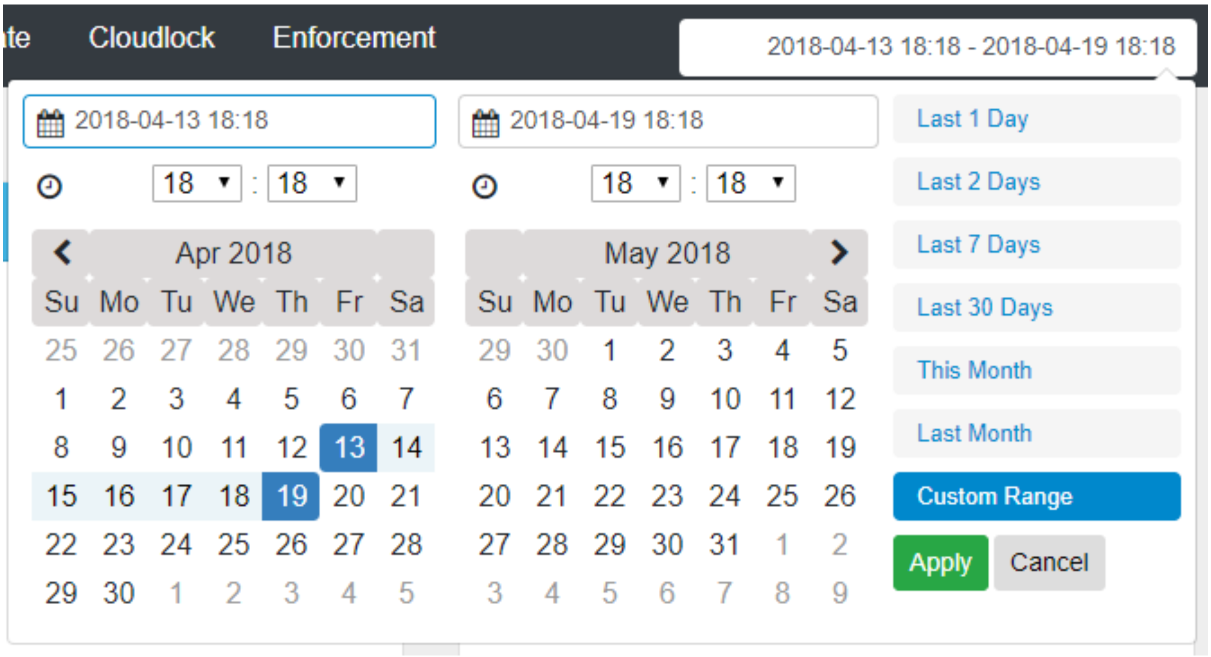
1. From the QRadar Homepage, click the **Cisco Cloud Security** tab.



2. **Cloud Overview tab** and dashboard will appear.
3. **Umbrella, Investigate, CloudLock and Enforcement tab** can be accessed in one click to the right of Investigate tab.

3.1.1. Time Range Selector

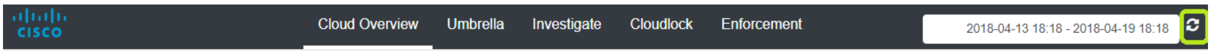
1. The time range selector tool can be used by the user to display information for a certain timeframe. By default, the application shows the data of Last 7 Days.
2. User can select the predefined date ranges as well as can click on the Custom and select Custom Date Ranges.



Note: Time Range selector is available in Enforcement, CloudLock, Dashboard and Umbrella tab only

3.1.2. Reset

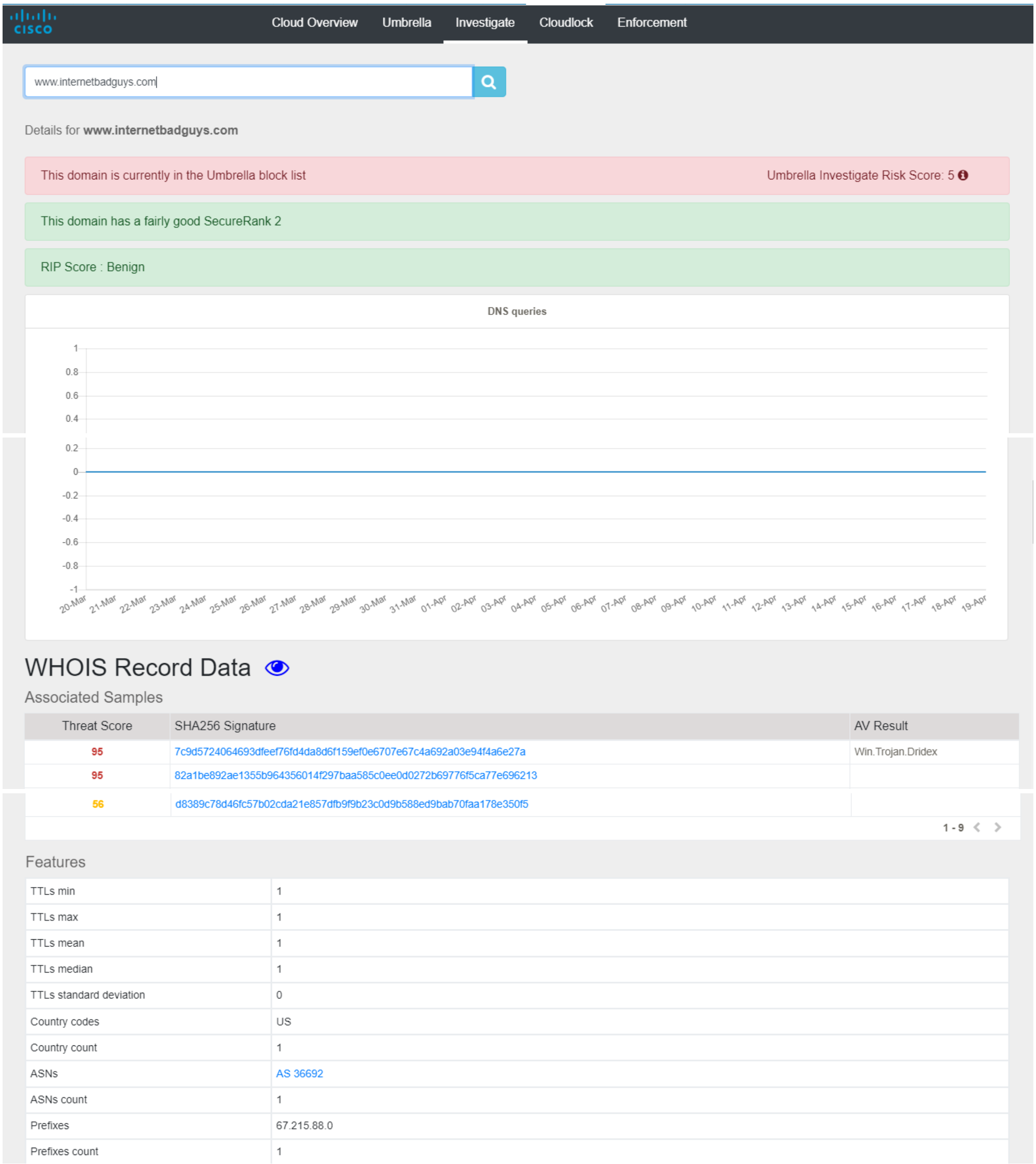
1. The user can click on the Reset button to reset the Date range to default Date range i.e. Last 7 Days.



3.2. Investigate Tab

1. The Investigate Tab enables the user to search the information related to hostname, URL, ASN, IP, Hash or email address.

2. The investigate tab gives the information such as WHOIS record, DGA information etc.



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

WHOIS Record Data

Associated Samples

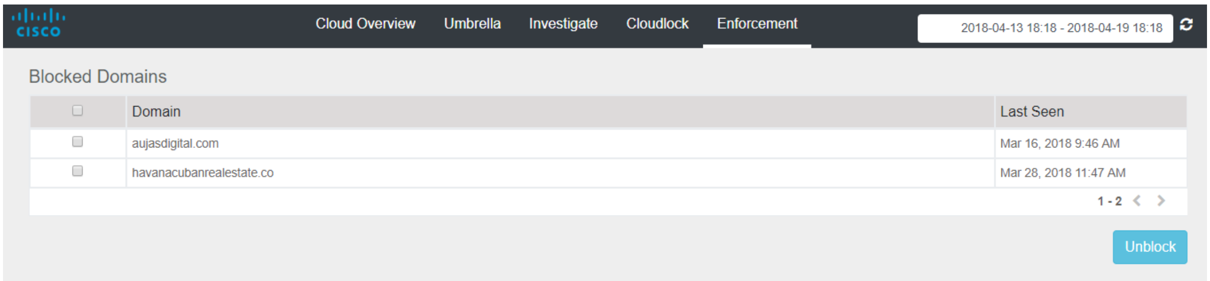
Threat Score	SHA256 Signature	AV Result
95	7c9d5724064693dfeef76fd4da8d6f159ef0e6707e67c4a692a03e94f4a6e27a	Win.Trojan.Dridex
95	82a1be892ae1355b964356014f297baa585c0ee0d0272b69776f5ca77e696213	
56	d8389c78d46fc57b02cda21e857dfb9f9b23c0d9b588ed9bab70faa178e350f5	

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

2.3. Enforcement Tab

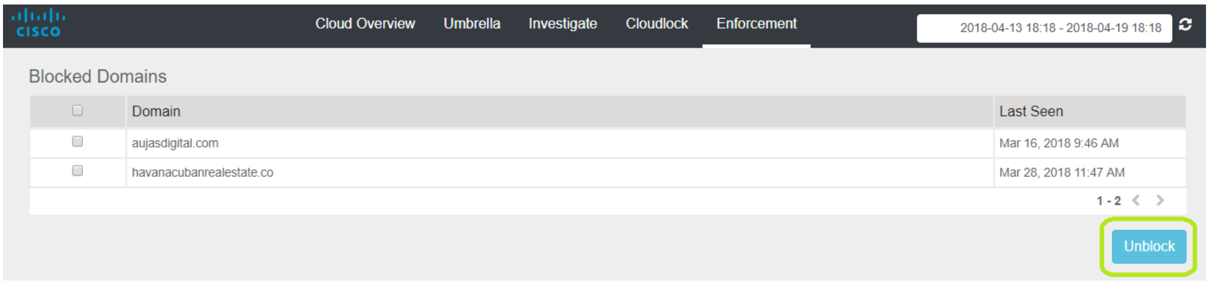
1. The Enforcement Tab displays the information related to the Blocked Domains.



Blocked Domains

□	Domain	Last Seen
□	aujasdigital.com	Mar 16, 2018 9:46 AM
□	havanacubanrealestate.co	Mar 28, 2018 11:47 AM

2. User can select the domain and can unblock the domains which are currently blocked.



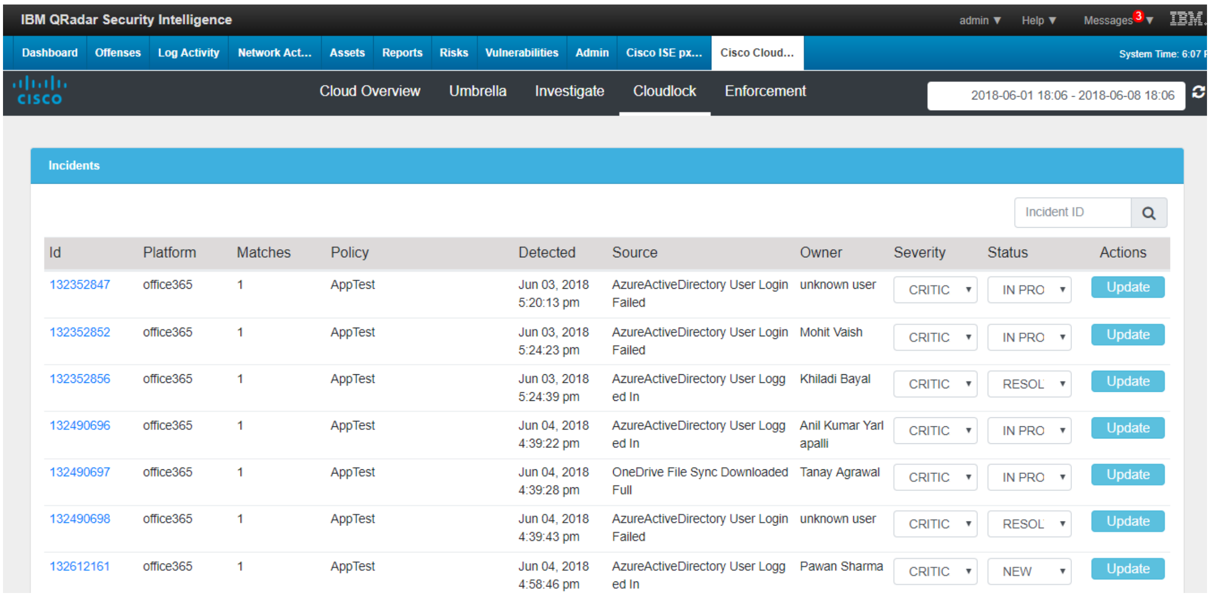
Blocked Domains

□	Domain	Last Seen
□	aujasdigital.com	Mar 16, 2018 9:46 AM
□	havanacubanrealestate.co	Mar 28, 2018 11:47 AM

1 - 2

2.4. CloudLock Tab

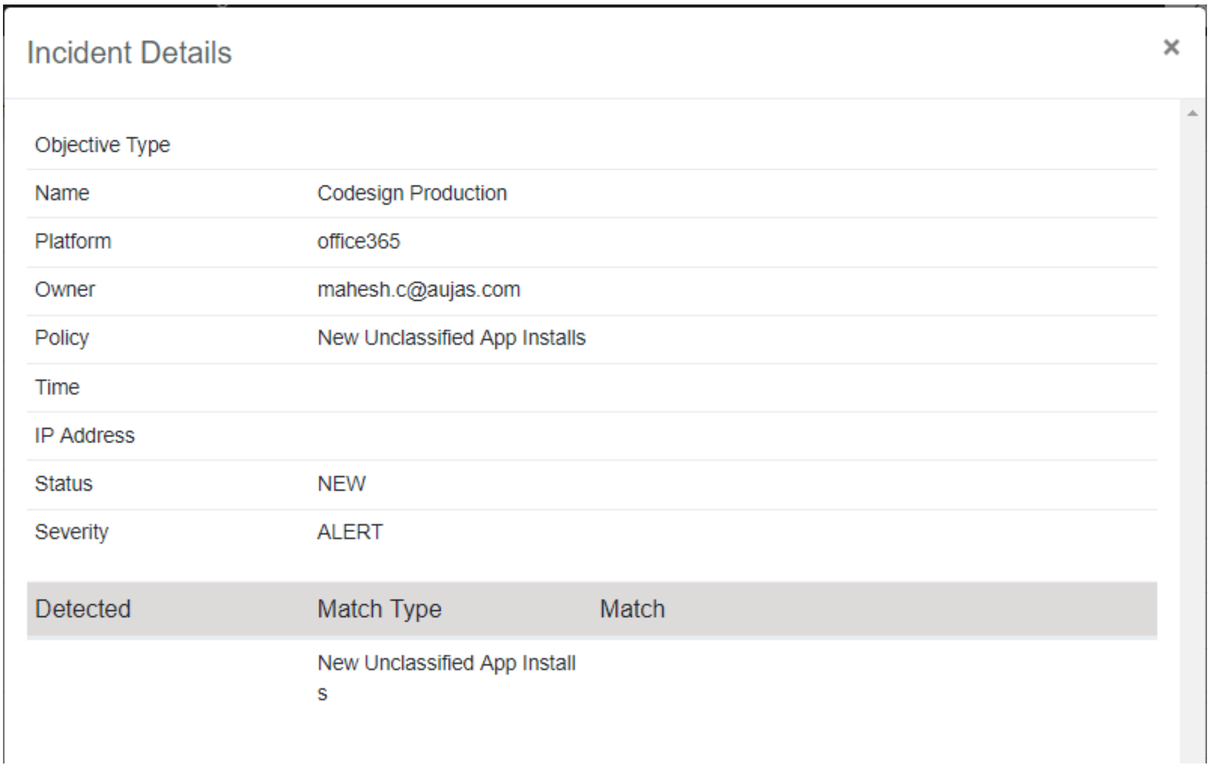
1. The CloudLock Tab displays the information related to all the incidents in a table based visual representation.



Incidents

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 ▾	IN PRO ▾	Update
132352856	office365	1	AppTest	Jun 03, 2018 5:24:39 pm	AzureActiveDirectory User Logged In	Khiladi Bayal	CRITIC ▾	RESOL ▾	Update
132490696	office365	1	AppTest	Jun 04, 2018 4:39:22 pm	AzureActiveDirectory User Logged In	Anil Kumar Yarlapalli	CRITIC ▾	IN PRO ▾	Update
132490697	office365	1	AppTest	Jun 04, 2018 4:39:28 pm	OneDrive File Sync Downloaded Full	Tanay Agrawal	CRITIC ▾	IN PRO ▾	Update
132490698	office365	1	AppTest	Jun 04, 2018 4:39:43 pm	AzureActiveDirectory User Login Failed	unknown user	CRITIC ▾	RESOL ▾	Update
132612161	office365	1	AppTest	Jun 04, 2018 4:58:46 pm	AzureActiveDirectory User Logged In	Pawan Sharma	CRITIC ▾	NEW ▾	Update

2. User can click on any of the id to view the details about the incident.

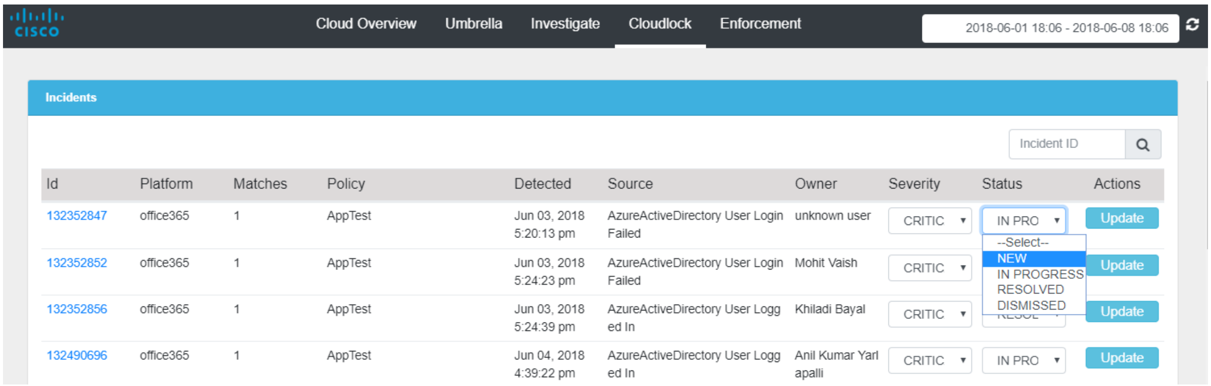


Incident Details

Objective Type	
Name	Codesign Production
Platform	office365
Owner	mahesh.c@aujas.com
Policy	New Unclassified App Installs
Time	
IP Address	
Status	NEW
Severity	ALERT

Detected	Match Type	Match
	New Unclassified App Installs	

3. User can also update the severity and status of the incidents by selecting the values from the drop-down list and clicking on update.

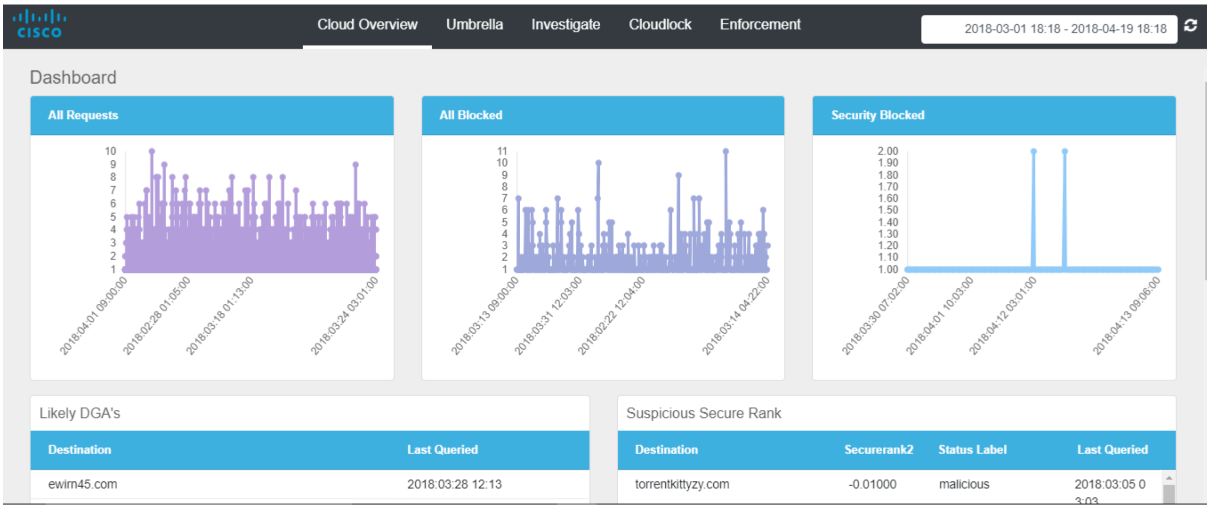


Incidents

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		Update
132352856	office365	1	AppTest	Jun 03, 2018 5:24:39 pm	AzureActiveDirectory User Logged In	Khiladi Bayal	CRITIC	RESOL	Update
132490696	office365	1	AppTest	Jun 04, 2018 4:39:22 pm	AzureActiveDirectory User Logged In	Anil Kumar Yarlapalli	CRITIC	IN PRO	Update

3.5. Cloud Overview Tab

The Cloud Overview Tab displays the information such as All Requests, All Blocked, Security Blocked, Likely DGA's, Suspicious Secure Rank, Cloudlock Incidents, CloudLock Overall, Top Policies, Top Offenders and Where in a chart based visual representation.

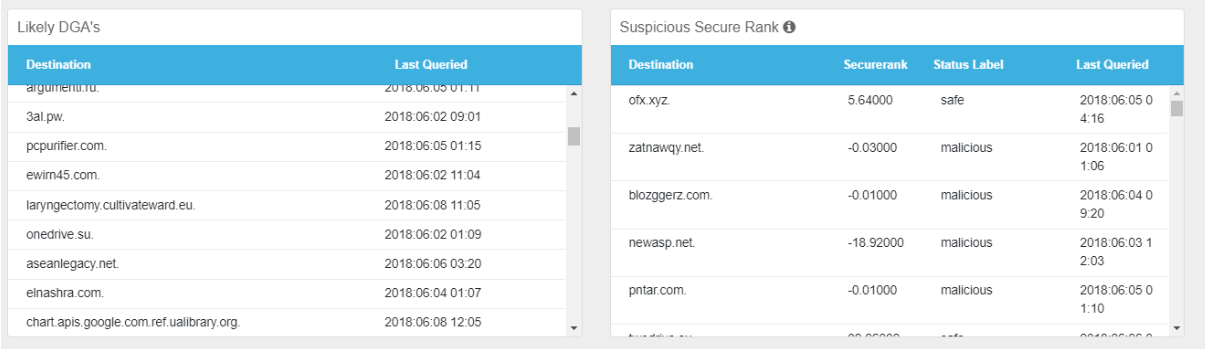


Likely DGA's

Destination	Last Queried
ewirn45.com	2018:03:28 12:13

Suspicious Secure Rank

Destination	Securerank2	Status Label	Last Queried
torrentkittyzy.com	-0.01000	malicious	2018:03:05 0 3:03

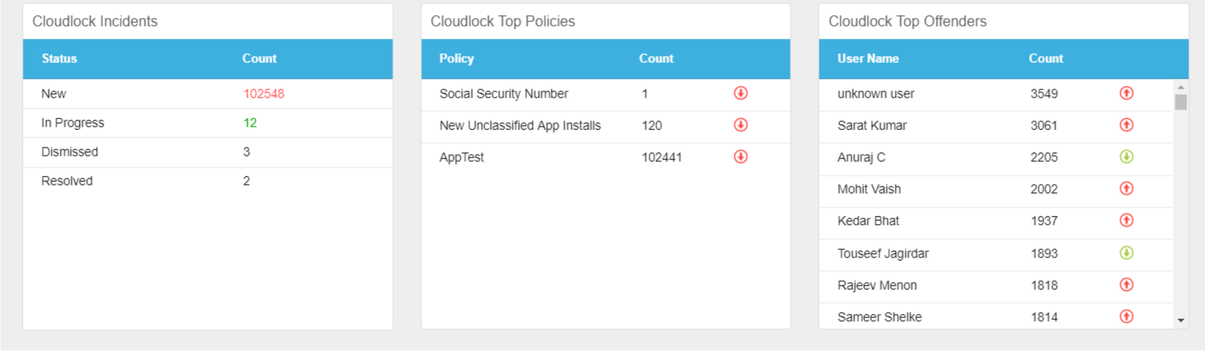


Likely DGA's

Destination	Last Queried
argumenti.ru.	2018:06:05 01:11
3al.pw.	2018:06:02 09:01
pcpurifier.com.	2018:06:05 01:15
ewirn45.com.	2018:06:02 11:04
laryngectomy.cultivateward.eu.	2018:06:08 11:05
onedrive.su.	2018:06:02 01:09
aseanlegacy.net.	2018:06:06 03:20
elnashra.com.	2018:06:04 01:07
chart.apis.google.com.ref.ualibrary.org.	2018:06:08 12:05

Suspicious Secure Rank

Destination	Securerank	Status Label	Last Queried
ofx.xyz.	5.64000	safe	2018:06:05 0 4:16
zatnawqy.net.	-0.03000	malicious	2018:06:01 0 1:06
blozggerz.com.	-0.01000	malicious	2018:06:04 0 9:20
newasp.net.	-18.92000	malicious	2018:06:03 1 2:03
pntar.com.	-0.01000	malicious	2018:06:05 0 1:10



Cloudlock Incidents

Status	Count
New	102548
In Progress	12
Dismissed	3
Resolved	2

Cloudlock Top Policies

Policy	Count	
Social Security Number	1	↓
New Unclassified App Installs	120	↓
AppTest	102441	↓

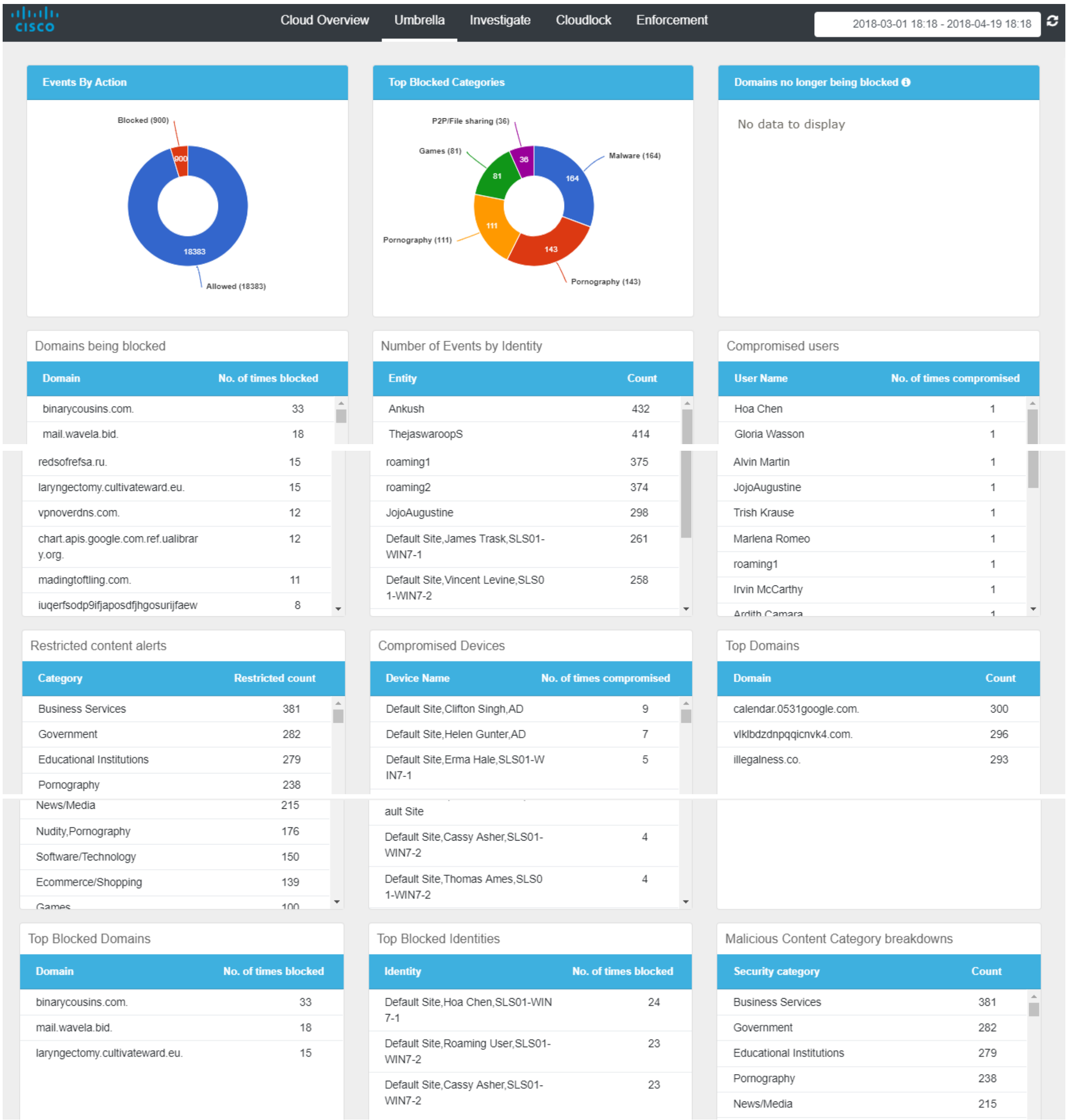
Cloudlock Top Offenders

User Name	Count	
unknown user	3549	↑
Sarat Kumar	3061	↑
Anuraj C	2205	↓
Mohit Vaish	2002	↑
Kedar Bhat	1937	↑
Touseef Jagirdar	1893	↓
Rajeev Menon	1818	↑
Sameer Shelke	1814	↑

3.6. Umbrella Tab

1. The Umbrella Tab displays the information such as Events By Action, Top Blocked Categories, Number of Events by Identity, Domains Being Blocked, Domains No longer being blocked, Compromised Users, Restricted content alerts, Compromised Devices, Top Domains, Top Blocked Domains, Top Blocked Identities, Malicious

Content Category breakdowns, Top Categories, Activity and User Access Trend in a chart based visual representation.



No data to display

Domains being blocked

Domain	No. of times blocked
binarycousins.com.	33
mail.wavela.bid.	18
redsofrefsa.ru.	15
laryngectomy.cultivateward.eu.	15
vpnoverdns.com.	12
chart.apis.google.com.ref.ualibrary.org.	12
madingtoftling.com.	11
iuqerfsodp9ifjaposdfjhgosurijfaew	8

Number of Events by Identity

Entity	Count
Ankush	432
ThejaswaroopS	414
roaming1	375
roaming2	374
JojoAugustine	298
Default Site,James Trask,SLS01-WIN7-1	261
Default Site,Vincent Levine,SLS01-WIN7-2	258

Compromised users

User Name	No. of times compromised
Hoa Chen	1
Gloria Wasson	1
Alvin Martin	1
JojoAugustine	1
Trish Krause	1
Marlena Romeo	1
roaming1	1
Irvin McCarthy	1
Ardith Camara	1

Restricted content alerts

Category	Restricted count
Business Services	381
Government	282
Educational Institutions	279
Pornography	238
News/Media	215
Nudity,Pornography	176
Software/Technology	150
Ecommerce/Shopping	139
Games	100

Compromised Devices

Device Name	No. of times compromised
Default Site,Clifton Singh,AD	9
Default Site,Helen Gunter,AD	7
Default Site,Erma Hale,SLS01-WIN7-1	5
ault Site	
Default Site,Cassy Asher,SLS01-WIN7-2	4
Default Site,Thomas Ames,SLS01-WIN7-2	4

Top Domains

Domain	Count
calendar.0531google.com.	300
vlklbdzdnpqqicnvk4.com.	296
illegalness.co.	293

Top Blocked Domains

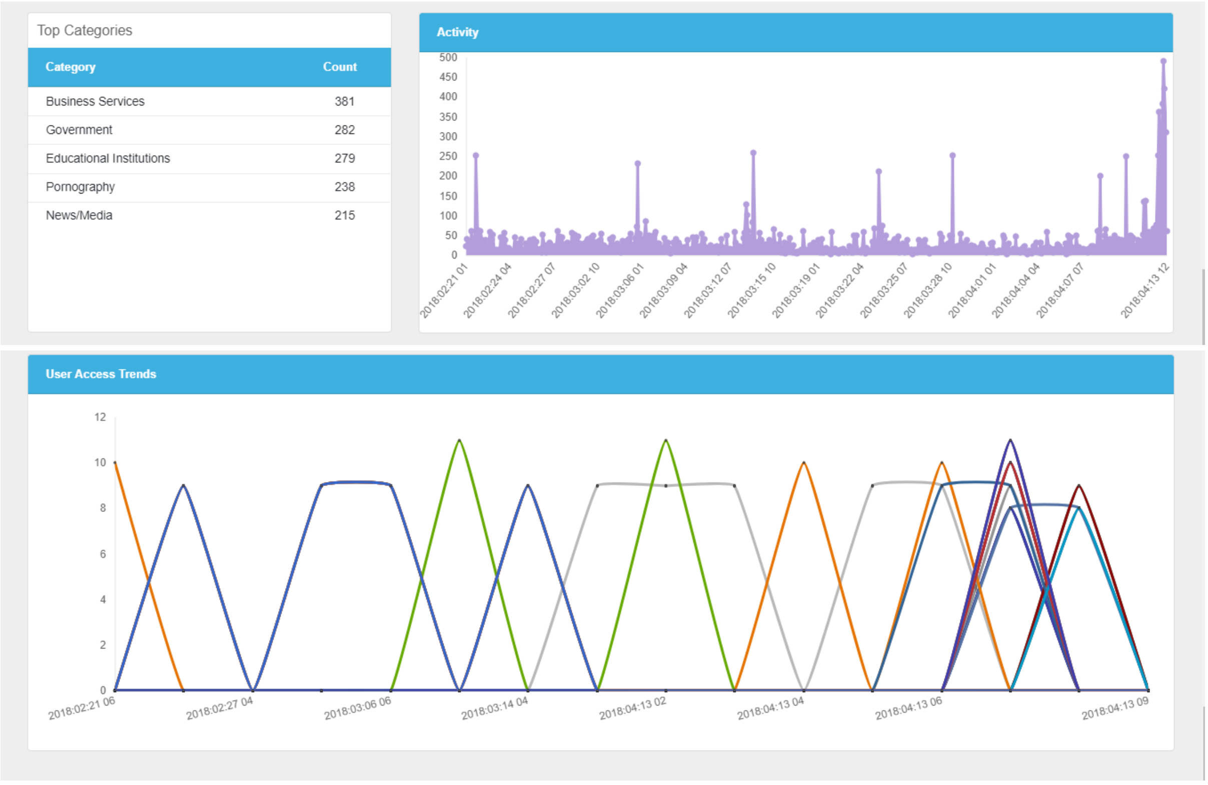
Domain	No. of times blocked
binarycousins.com.	33
mail.wavela.bid.	18
laryngectomy.cultivateward.eu.	15

Top Blocked Identities

Identity	No. of times blocked
Default Site,Hoa Chen,SLS01-WIN7-1	24
Default Site,Roaming User,SLS01-WIN7-2	23
Default Site,Cassy Asher,SLS01-WIN7-2	23

Malicious Content Category breakdowns

Security category	Count
Business Services	381
Government	282
Educational Institutions	279
Pornography	238
News/Media	215



Top Categories

Category	Count
Business Services	381
Government	282
Educational Institutions	279
Pornography	238
News/Media	215

Activity

User Access Trends

4. Legal Notice

4.1. Confidentiality Notice

This document transmission (and/or the documents accompanying it) is for the sole use of the intended recipient(s) and may contain information protected by the attorney-client privilege, the attorney-work-product doctrine or other applicable privileges or confidentiality laws or regulations. If you are not an intended recipient, you may not review, use, copy, disclose or distribute this message or any of the information contained in this message to anyone. If you are not the intended recipient, contact the sender by reply e-mail and destroy all copies of this message and attachments.