



Cisco Web Security App for IBM QRadar

Version Number: 1.4

Date: August 05, 2019

Contents

1.	Introduction.....	3
1.1.	Overview	3
1.2.	About this Document	3
1.3.	About the app	3
1.4.	Prerequisites	3
1.5.	Custom Field Properties of DSM.....	3
2.	General.....	6
2.1	Installation.....	6
2.2	Configuring Log Source	7
3.	Cisco Web Security App.....	8
3.1.	General	8
3.1.1.	Time Range Selector.....	9
3.1.2.	Reset.....	9
3.2.	Overview Tab.....	9
3.3.	User Analysis Tab	10
3.4.	Browsing Analysis Tab	11
3.5.	Application Analysis Tab	12
3.6.	Security Analysis Tab.....	12
3.6.1	Advance Malware Protection	12
3.6.2	Anti - Malware	13
3.6.3	L4 - Traffic Monitor.....	14
3.6.4	Web Reputation Filter.....	15
3.7	Web Tracking Tab	16
4.	Legal Notice.....	17
4.1.	Confidentiality Notice	17

1. Introduction

1.1. Overview

The Cisco Web Security App for IBM QRadar provide insight from multiple security products and integrates them with QRadar. The Cisco Web 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 Web 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 Web Security app for QRadar, it integrates all the data from Cisco Web 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.
- Analyzes and categorizes unknown URLs.

1.4. Prerequisites

- IBM QRadar version 7.2.8 patched to 20170105231716 and above.
- Administration privileges

1.5. Custom Field Properties of DSM

Screenshot for Custom field property

- Regex Properties (57)
 - URL Category Verdict
 - Response Body MIME type
 - SHA256 Hash
 - Sophos Scan Return Code
 - Client IP Address
 - Application name
 - Malware Scanning Verdict
 - Data Security Scan Verdict(Cisco)
 - WSA Username
 - Server Code
 - Threat Identifier Value
 - Safe Browsing Scanning Verdict
 - Malware Scanning Verdict Value
 - UserType
 - Threat Name(AMP)
 - Spyware Name
 - Application Behaviour
 - Disposition
 - Data Source
 - ACL Decision Tag
 - Reputation Score
 - WSA URL

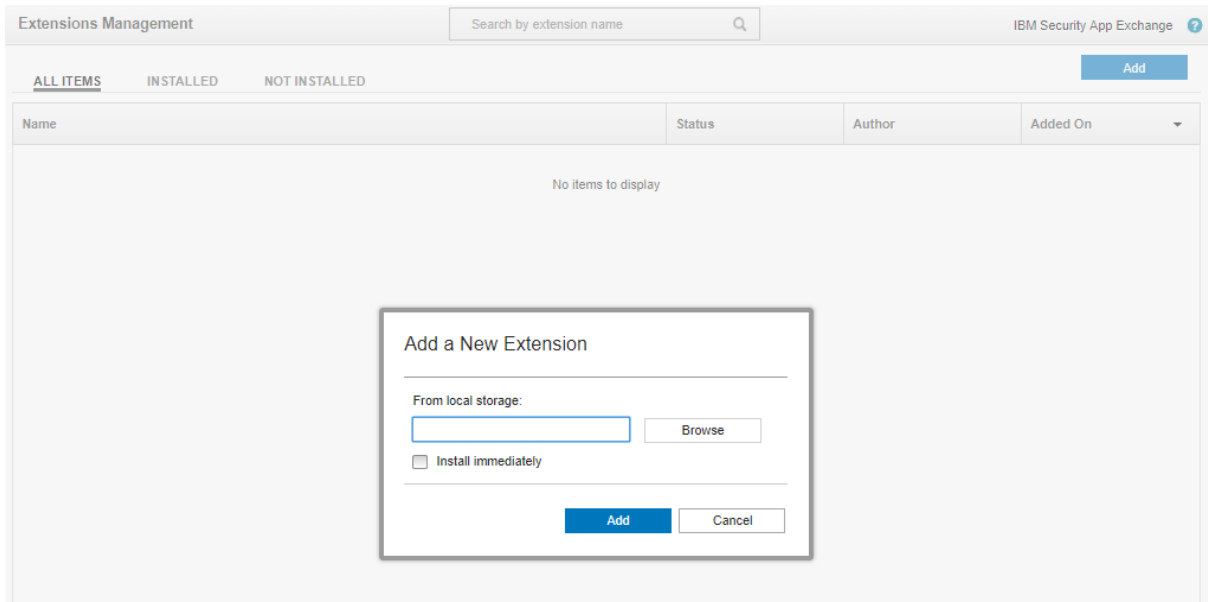
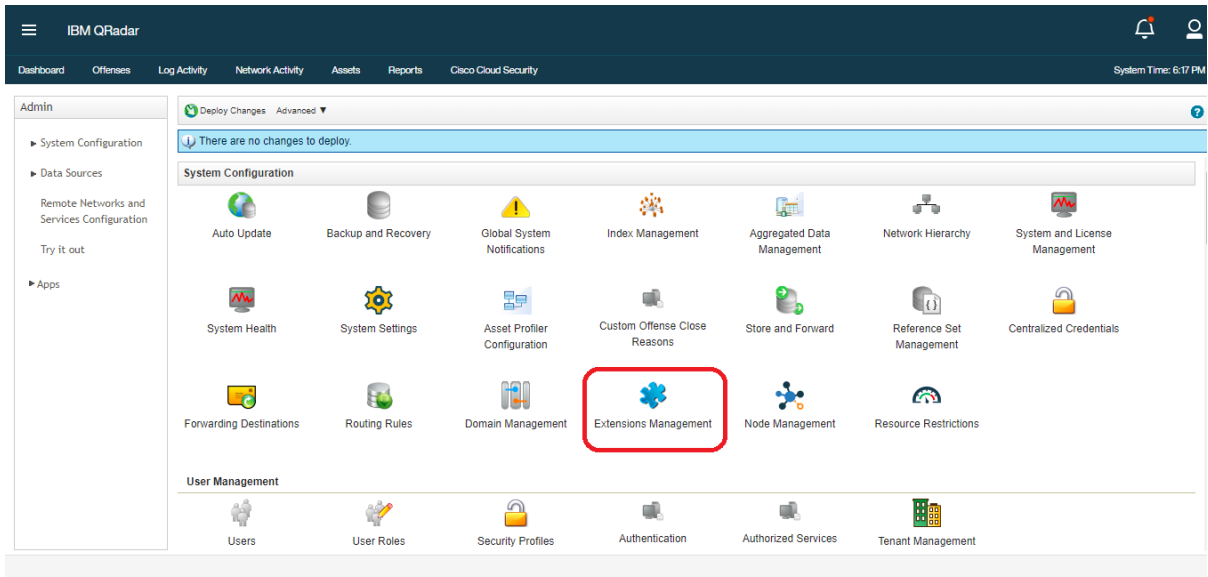
- Custom URL Category
- File Name (Downloaded)
- Detection Type Value
- Archive Scan Verdict Detail
- Malware Scanning Verdict (Sophos)
- Malware Category
- Verdict for File(AMP)
- Transaction Result Code
- Response Code
- Archive Scan Verdict
- Web Reputation Filter Score
- URL Category Verdict (Dynamic Conte
- File Name (Objectionable Content)
- Scanning Verdict Information
- Response Size
- File Name
- File Type
- Threat Type
- Unified Anti Malware Scanning Verdict
- AMP Verdict
- Indicator of Upload and Analysis Requ
- Suspect User Agent

- Threat Name Value (Sophos)
- Transaction Time
- Average Bandwidth Consumed
- Elapsed Time(Latency)
- Trace Identifier Value
- 50...99
 - External DLP Scan Verdict
 - Scan Error Value
 - Probability(Malware Exists or Not)
 - Request Throttled or Not
 - Virus Type Value
 - VirusName
 - WSA Port
 - Application Type

2. General

2.1 Installation

1. Login to QRadar and go to Admin tab
2. Select Extension Management Services
3. Install the application as a QRadar Plugin (For more details plugin installation, click [here](#))
4. After the installation, deploy changes in QRadar



Extensions Management Search by extension name IBM Security App Exchange ?

ALL ITEMS INSTALLED NOT INSTALLED Add

Name	Status	Author	Added On
<div style="border: 1px dashed blue; padding: 5px;"> <p>Cisco Web Security Appliance(WSA)</p> <p>This IBM QRadar App for Cisco Web Security Appliance(WSA).</p> <p><input type="button" value="Install"/> <input type="button" value="Delete"/></p> <p style="text-align: right;">(More Details...)</p> </div>	⚠ Not Installed	Cisco	March 18, 2019

Extensions Management Search by extension name IBM Security App Exchange ?

ALL ITEMS INSTALLED NOT INSTALLED Add

Cisco Web Security Appliance(WSA)

By: Cisco

⚠ The extension contains 8 items which are already on the system and marked with REPLACE. You can replace these items with the versions in the extension that you are about to install, or you can preserve existing items as-is and add only new items. Application items that are marked with REPLACE are upgraded but internal data and configuration is preserved. Any other item types marked with REPLACE will be replaced and customizations will be lost. How would you like to proceed?

Replace existing items. (Application data is preserved)
 Preserve existing items. (Not recommended for applications)

By installing this extension, the following changes will occur in the system:

Log Source Extensions (1)	
CiscoWebSecurityAppliancesWSACustom_ext	ADD

Regex Properties (56)

File Name (Downloaded)	ADD
Threat Name Value (Sophos)	ADD
Elapsed Time(Latency)	ADD
Archive Scan Verdict Detail	ADD
Suspect User Agent	ADD
Malware Scanning Verdict Value	ADD
Application Type	ADD
User Type	ADD

⚠ Not secure | https://192.168.0.226/console/plugins/1710/app_proxy/app_settings

From 192.168.0.226

Successfully updated application settings

Api Settings

2.2 Configuring Log Source

1. From the Admin tab on the QRadar navigation bar, scroll down to Log Sources
2. Click on Add to create a new log source
3. Enter the required parameters for creating log source:
 - a. Enter a Log Source Name
 - b. Use Host Name for Log Source Identifier
 - c. Select Cisco Web Security Appliances (WSA) as Log Source Type
 - d. Select CiscoWebSecurityAppliancesWSACustom_ext in Log Source extension

Add a log source	
Log Source Name	<input type="text"/>
Log Source Description	<input type="text"/>
Log Source Type	Cisco Web Security Appliances (WSA) ▼
Protocol Configuration	Syslog ▼
Log Source Identifier	<input type="text"/>
Enabled	<input checked="" type="checkbox"/>
Credibility	5 ▼
Target Event Collector	eventcollector0 :: qradar732 ▼
Coalescing Events	<input checked="" type="checkbox"/>
Incoming Payload Encoding	UTF-8 ▼
Store Event Payload	<input checked="" type="checkbox"/>
Log Source Language	▼
Log Source Extension	CiscoWebSecurityAppliancesWSACustom_ext ▼

4. Save and Deploy the changes.

3. Cisco Web Security App

3.1. General

Information displayed in Cisco Web Security App for Syslog.

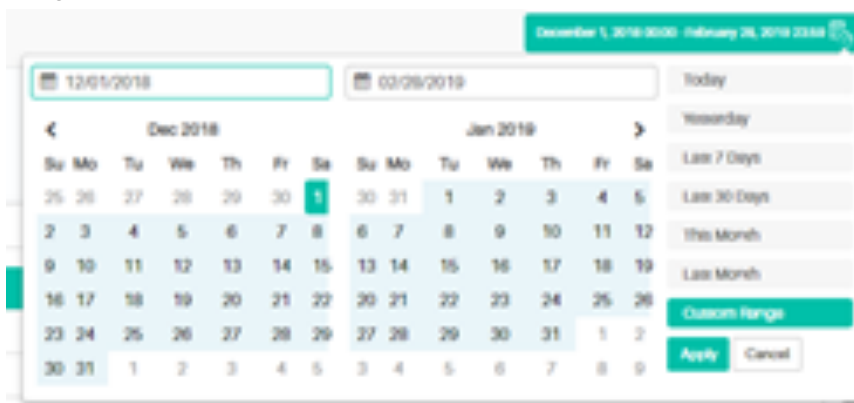
To navigate to the Cisco Web Security app, in IBM QRadar:

1. From the QRadar Homepage, click the Cisco WSA 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.

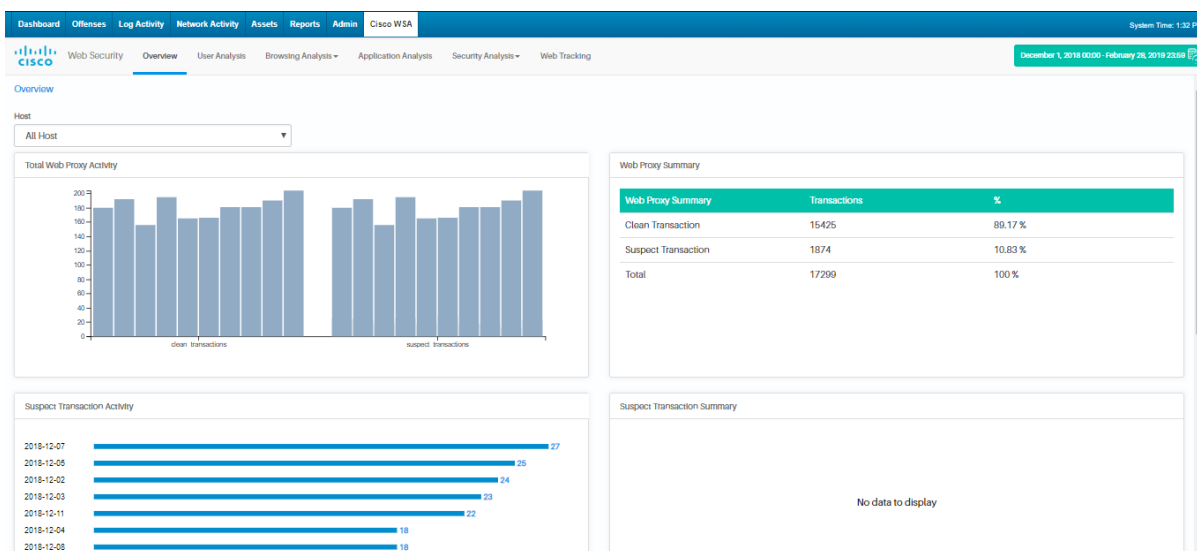


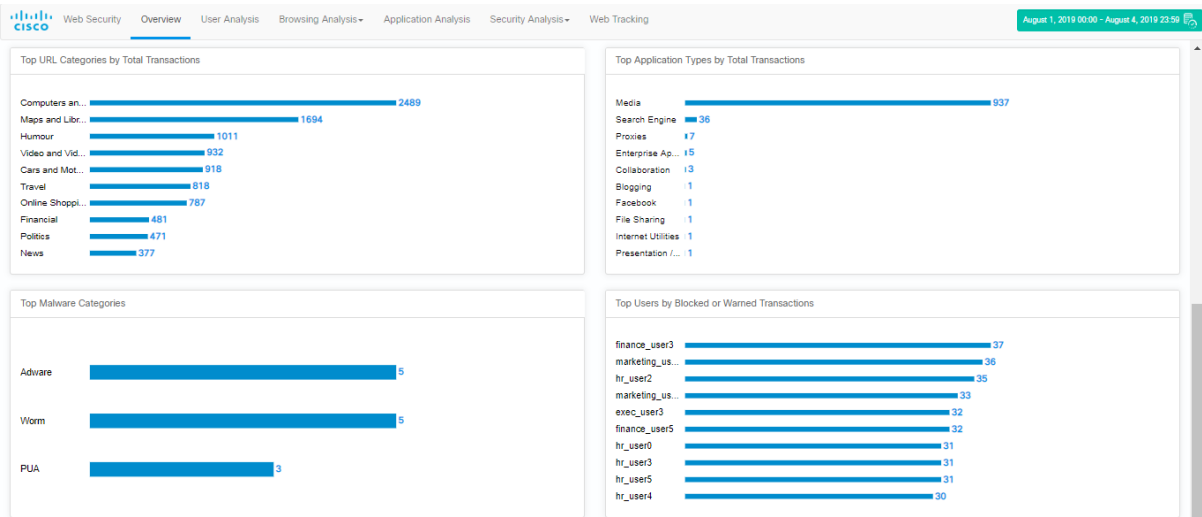
3.1.2. Reset

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

3.2. Overview Tab

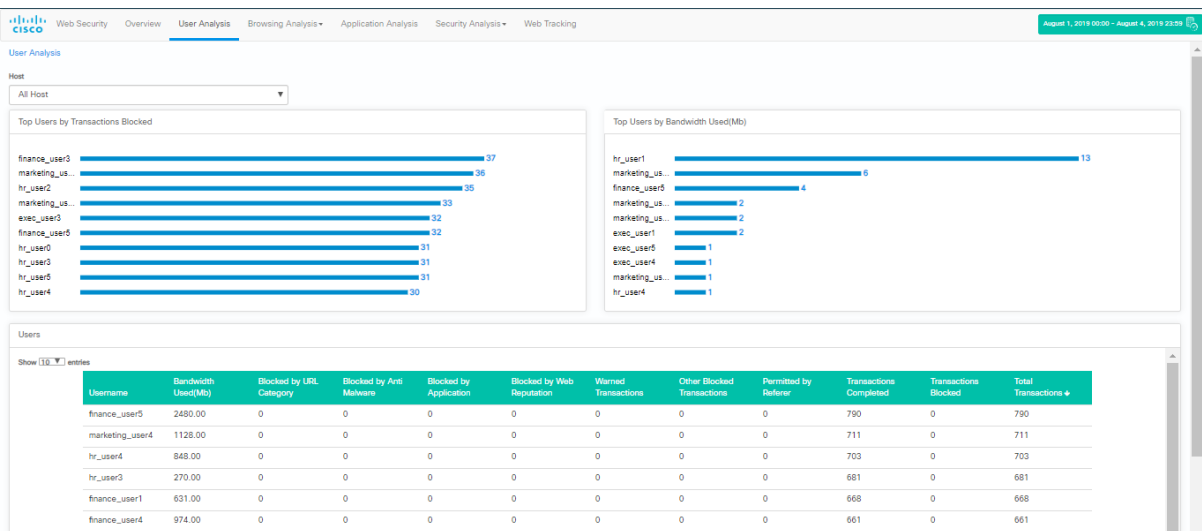
1. Overview Tab enables the user to search the information related to hostname.
2. Overview tab gives the information such as Web Proxy Activity & respective summary, Suspect Transaction Activity and respective summary, URL categories and Malware categories etc.



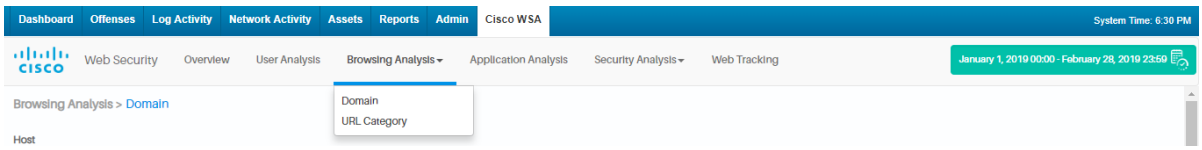


3.3. User Analysis Tab

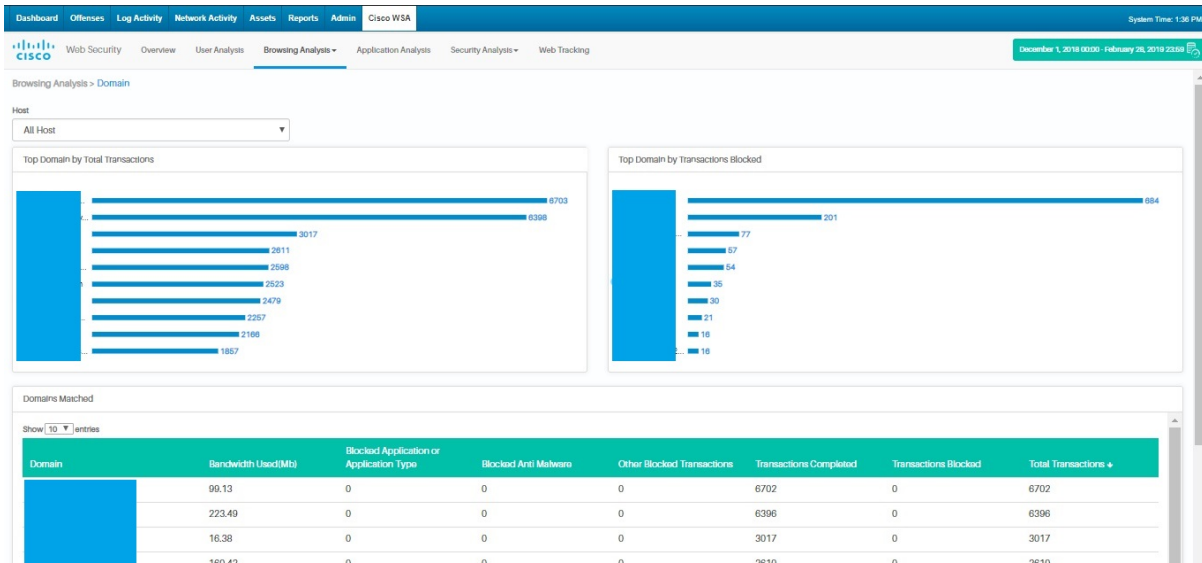
1. Overview Tab enables the user to search the information related to hostname
2. Overview tab gives the information such as Top users by transactions blocked, Top users by Bandwidth used etc.



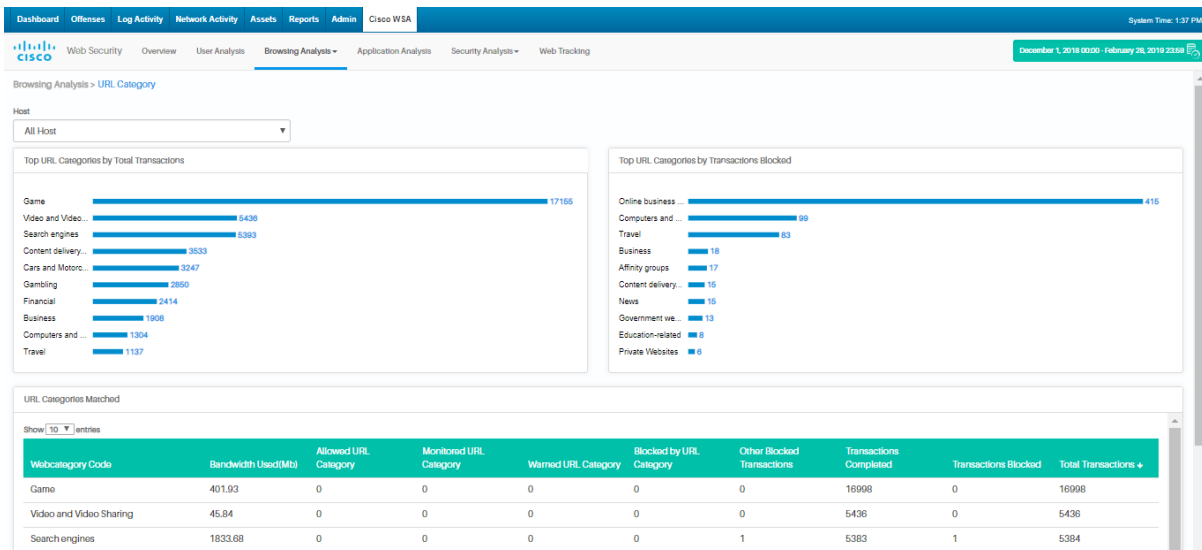
3.4. Browsing Analysis Tab



1. The Domain Menu displays the information such as Top Domain by Total Transactions, Top Domain by transactions Blocked and Domain matching information.

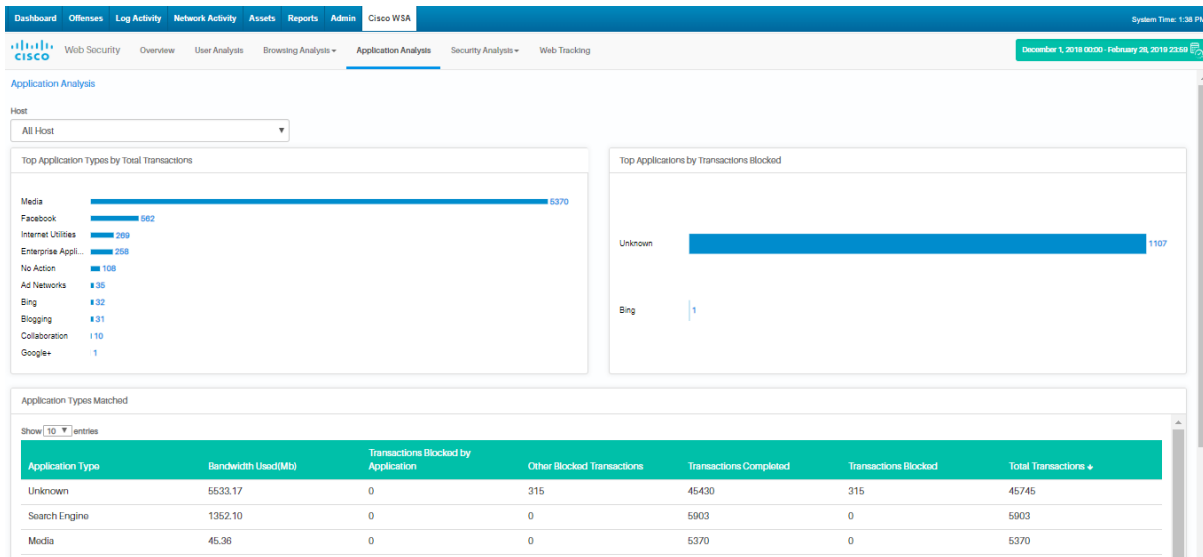


2. The URL category displays the information such as Top URL categories by Total Transactions, Top URL Categories by transactions Blocked and URL matching information.

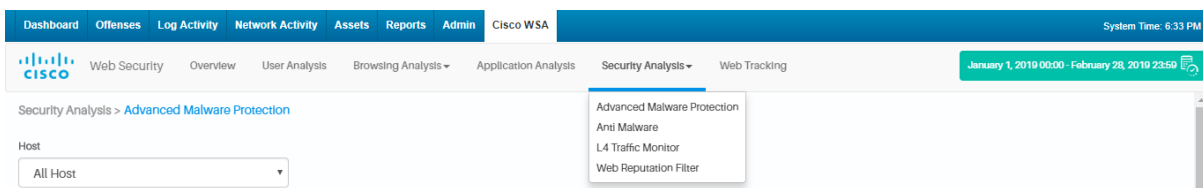


3.5. Application Analysis Tab

The Application Analysis Menu displays the information such as Top Application Types by Total Transactions, Top Applications by Transactions Blocked and Application Types matching information.



3.6. Security Analysis Tab

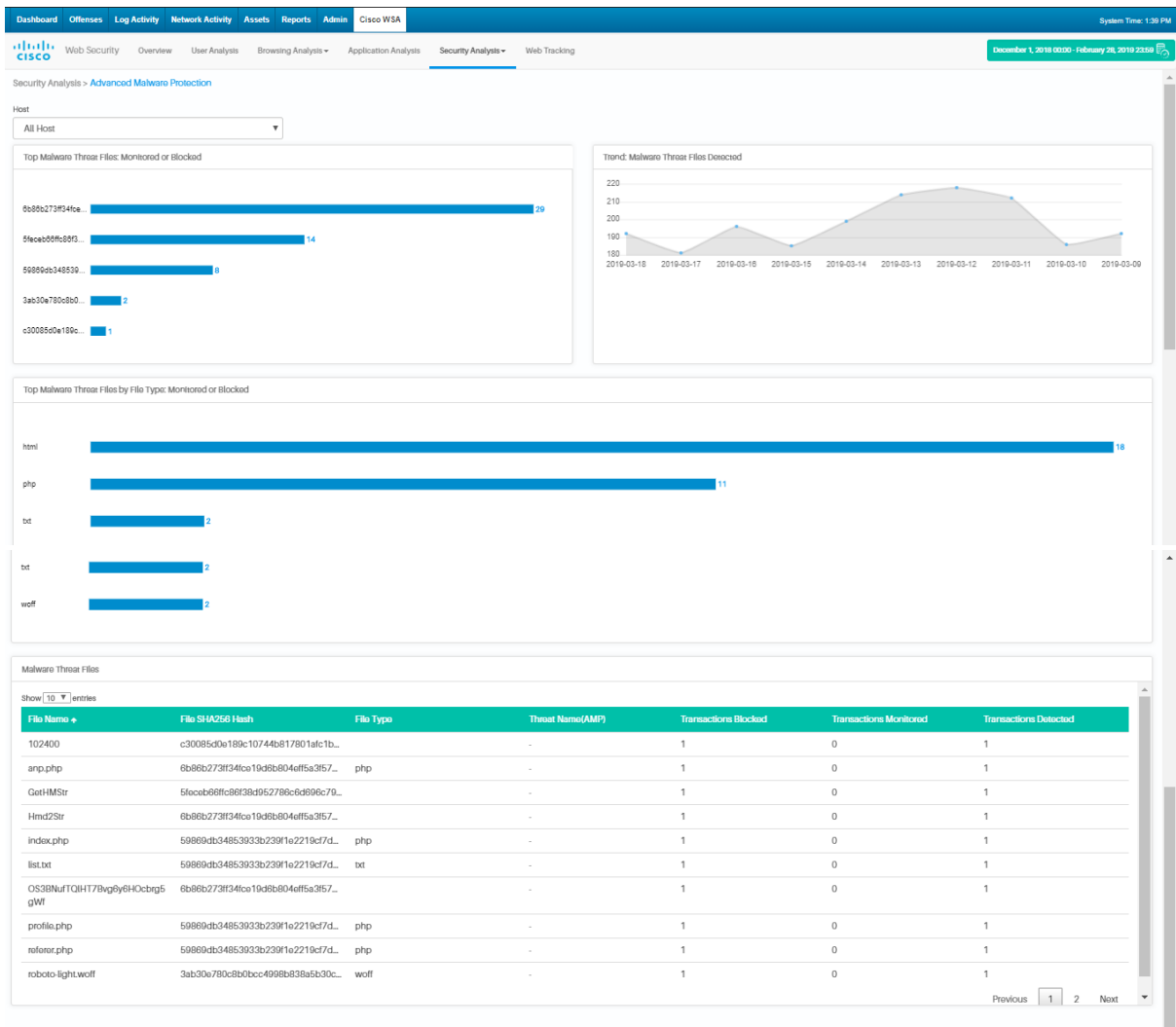


The Security Analysis Menu contains the below sub menus:

1. Advance Malware Protection
2. Anti - Malware
3. L4 Traffic Monitor
4. Web Reputation Filter

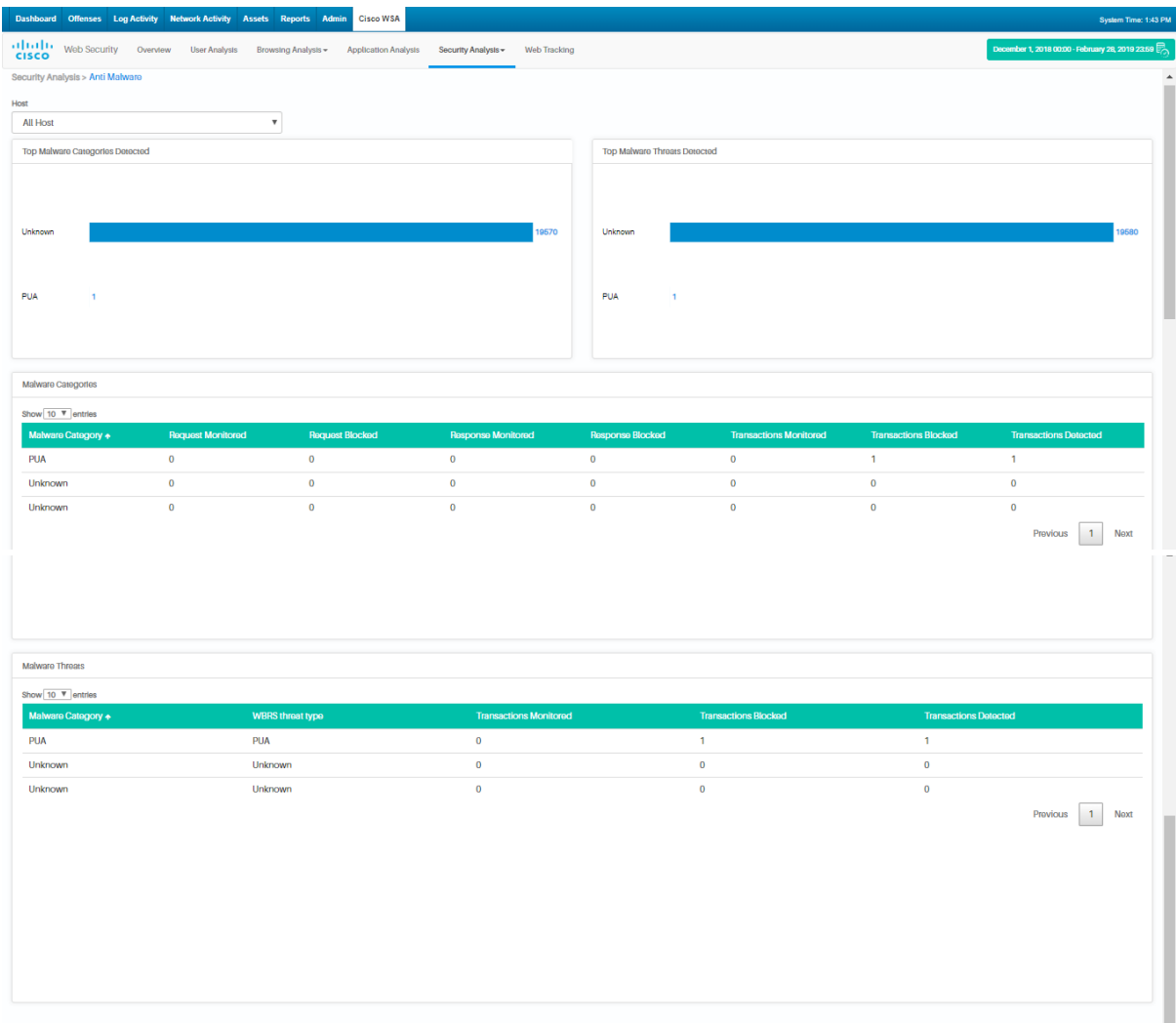
3.6.1 Advance Malware Protection

The Advance Malware Protection displays the information such as Top Malware Threat files for Malware or Blocked, Trend chart which show total number of Malware reported for a specific period, Top Malware Threat files by File and respective Malware Threat files information.



3.6.2 Anti - Malware

The Anti - Malware displays the information such as Top Malware categories detected, Top Malware threat detected and displays Malware categories and Malware threat information.



3.6.3 L4 - Traffic Monitor

The L4 - Traffic Monitor displays the information such as Top Malware Hosts detected, Top Malware ports detected, Top Malware sites detected and associate user details.

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco WSA System Time: 1:44 PM

Web Security Overview User Analysis Browsing Analysis Application Analysis Security Analysis Web Tracking December 1, 2018 00:00 - February 28, 2019 23:59

Security Analysts > L4 Traffic Monitor

Host: All Host

Top Malware Hosts Detected

No data to display

Top Malware Ports Detected

No data to display

Top Malware Sites Detected

No data to display

Malware Hosts Detected

Show 10 entries

Hosts Detected	Transactions Monitor	Transactions Blocked	Transactions Completed
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	3

Previous 1 2 3 4 5 ... 55 Next

Associated Users

Client IP Address

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

Previous 1 2 3 4 5 ... 55 Next

Malware Ports Detected

Show 10 entries

Ports Detected	Transactions Monitor	Transactions Blocked	Transactions Completed
80	0	297	0
443	0	0	28
3128	0	56	0

Previous 1 Next

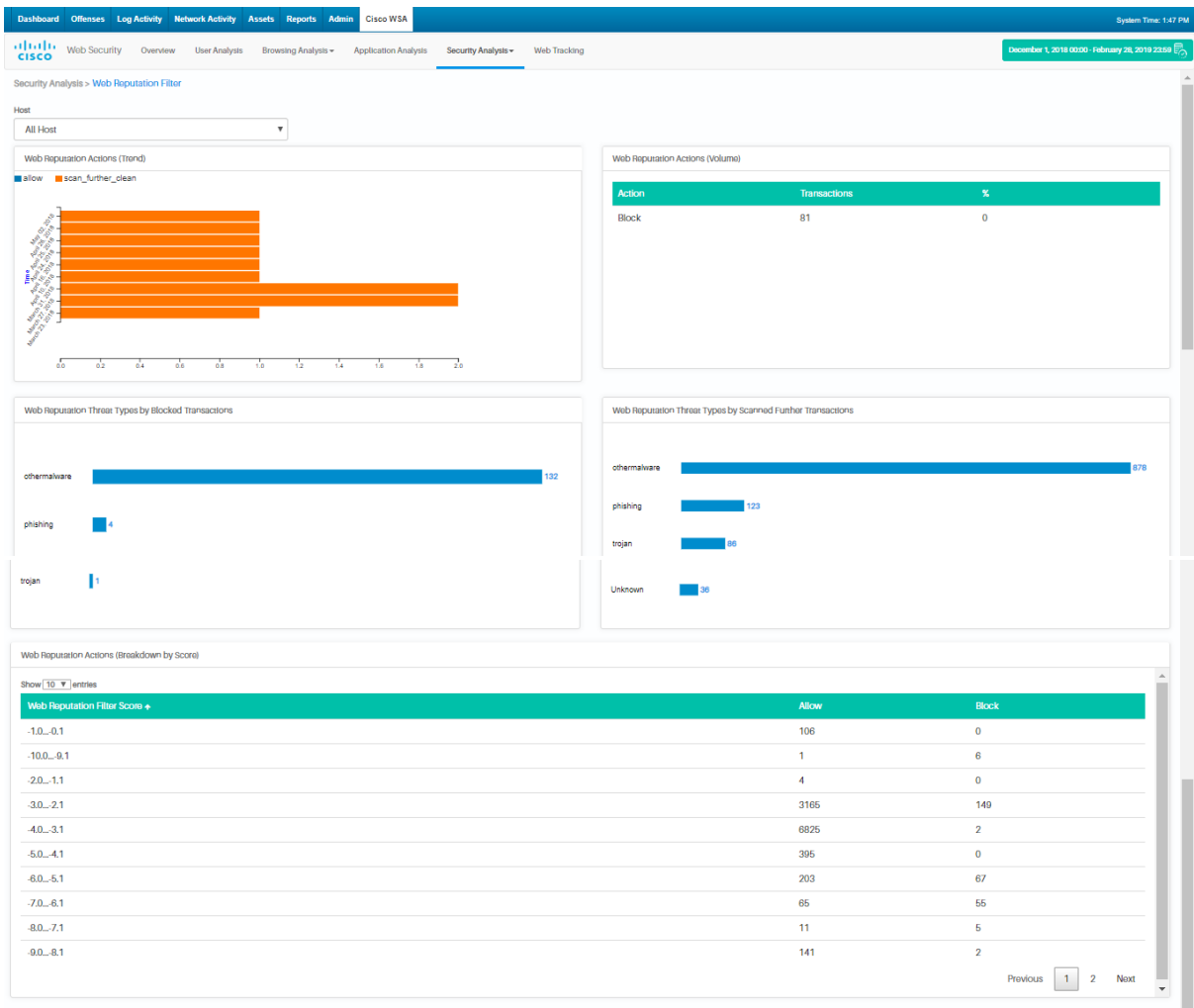
Malware Sites Detected

Show 10 entries

WSA URL	Transactions Monitor	Transactions Blocked	Transactions Completed
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	0	1
[Redacted]	0	1	0

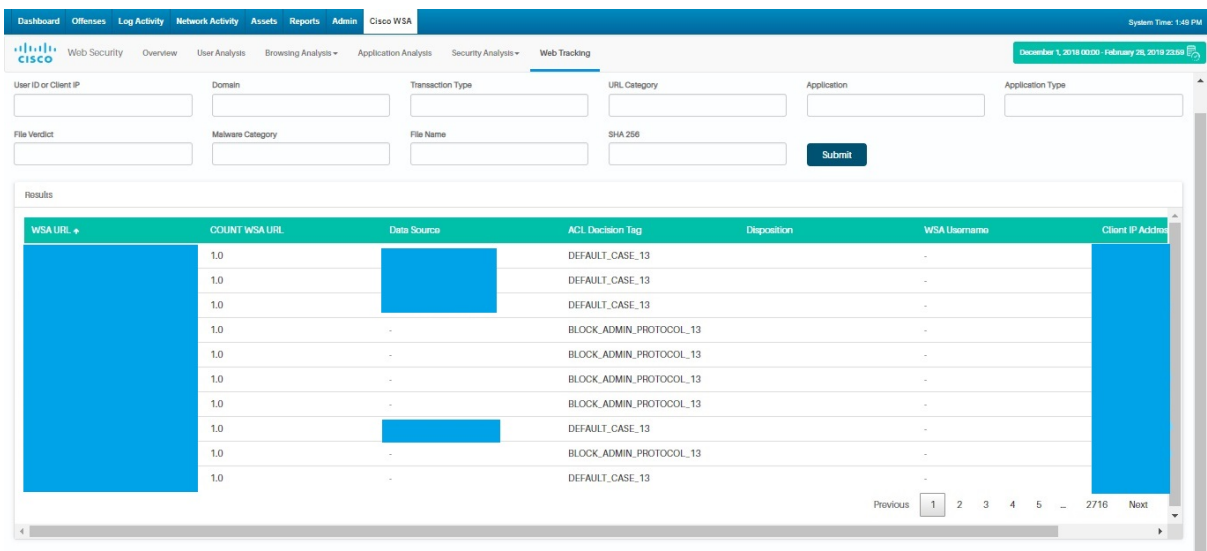
3.6.4 Web Reputation Filter

The Web Reputation Filter details displayed as Trend, as Volume and as Breakdown score. It also displays information such as Top Malware Hosts detected, Top Malware ports detected, Top Malware sites detected and associate user details.



3.7 Web Tracking Tab

Admin can search for any web transactions from Web Tracking tab.



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.