Cisco Web Security App for IBM QRadar

Version Number: 1.4

Date: August 05, 2019

Contents

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:

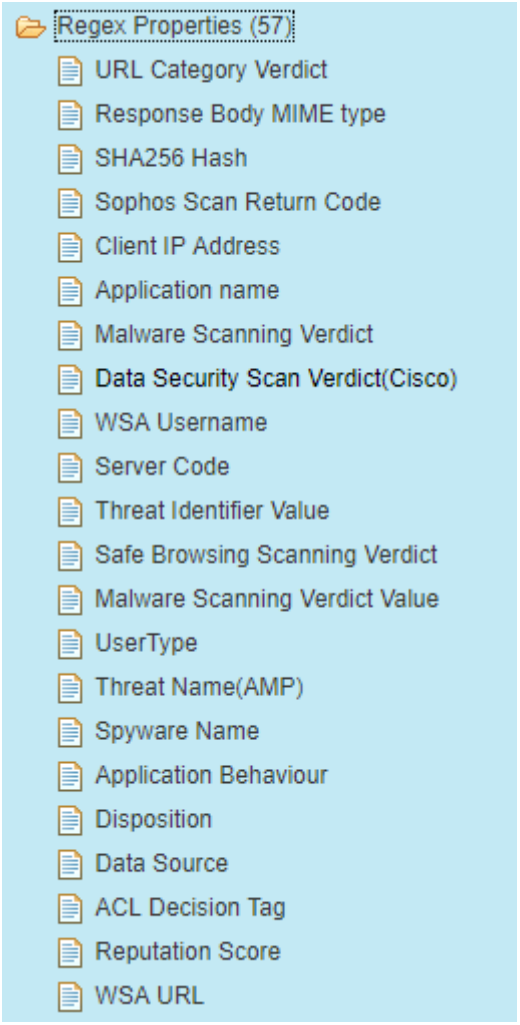
- Investigate the domains, IP addresses, email addresses.
- Block and Unblock domains (Enforcement).
- View the information of all the incidents of the network.
- Analyzes and categorizes unknown URLs.

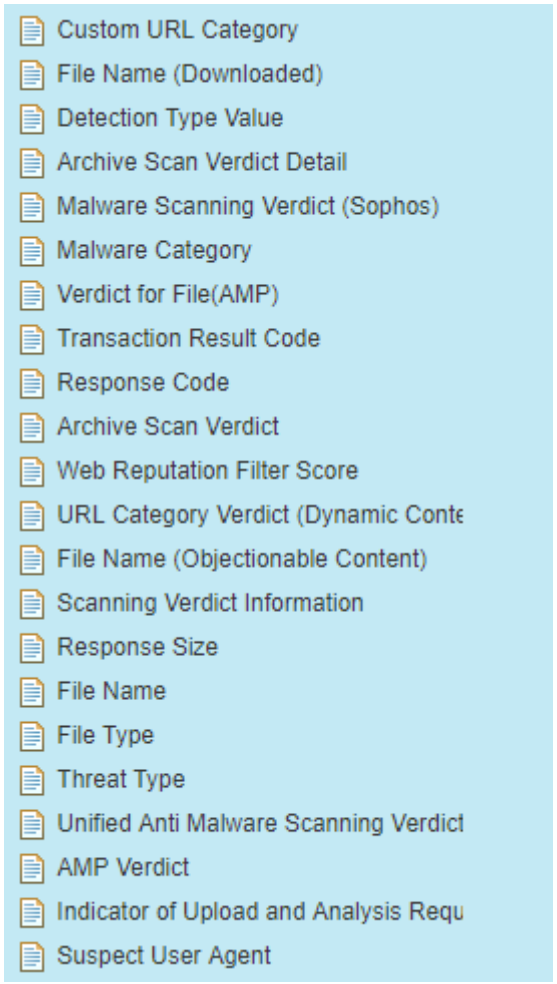
1.4. Prerequisites

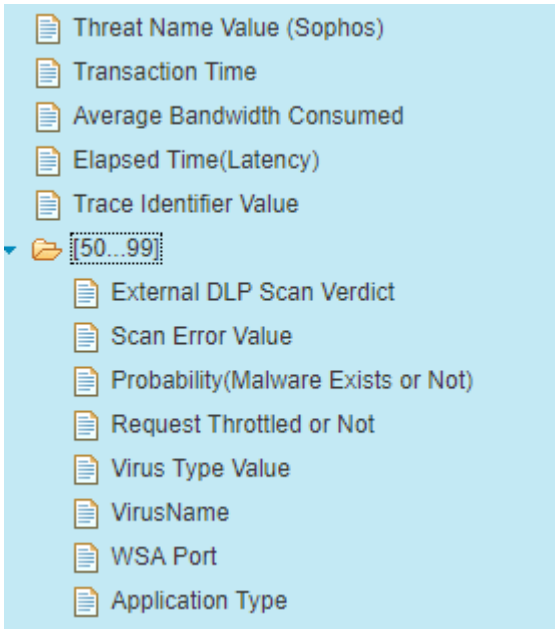
- IBM QRadar version 7.2.8 patched to 20170105231716 and above.
- Administration privileges

1.5. Custom Field Properties of DSM

Screenshot for Custom field property



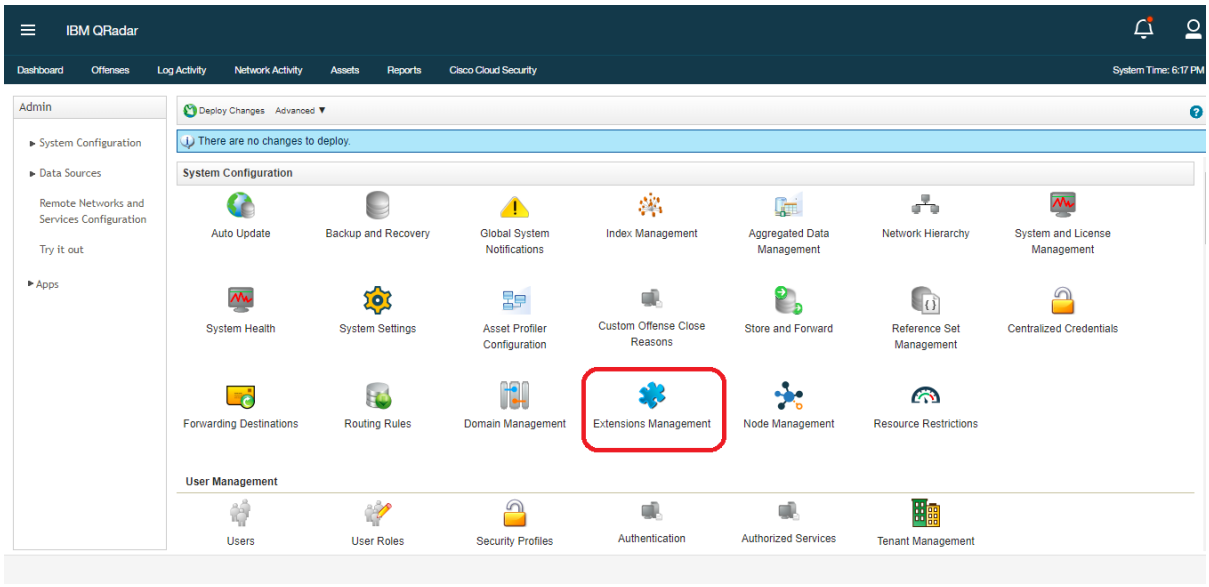


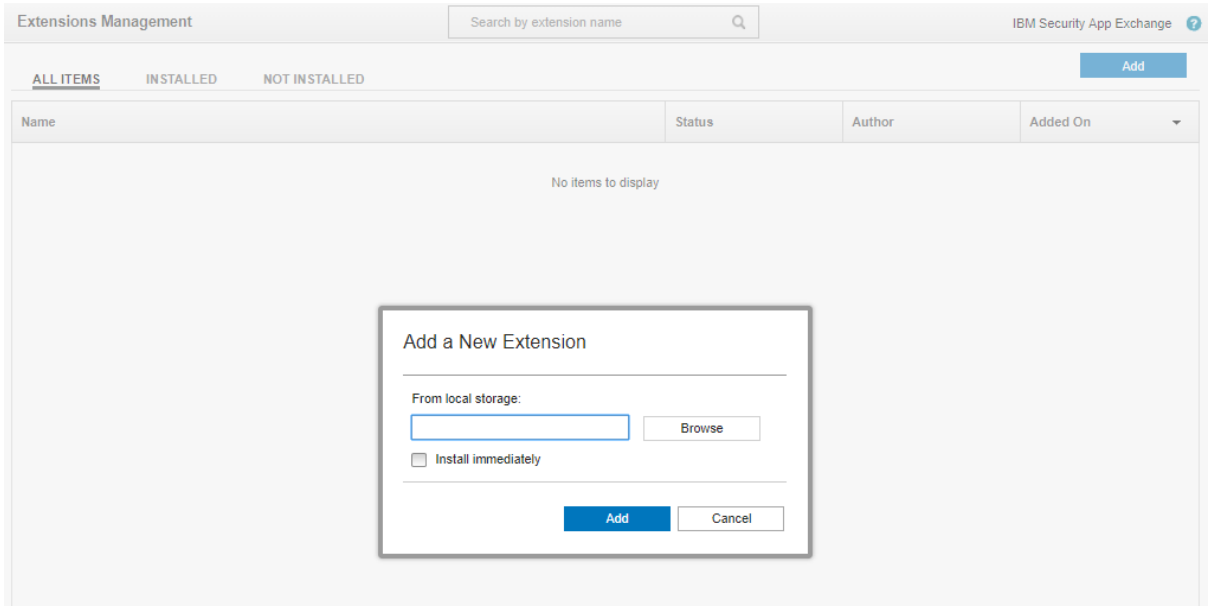


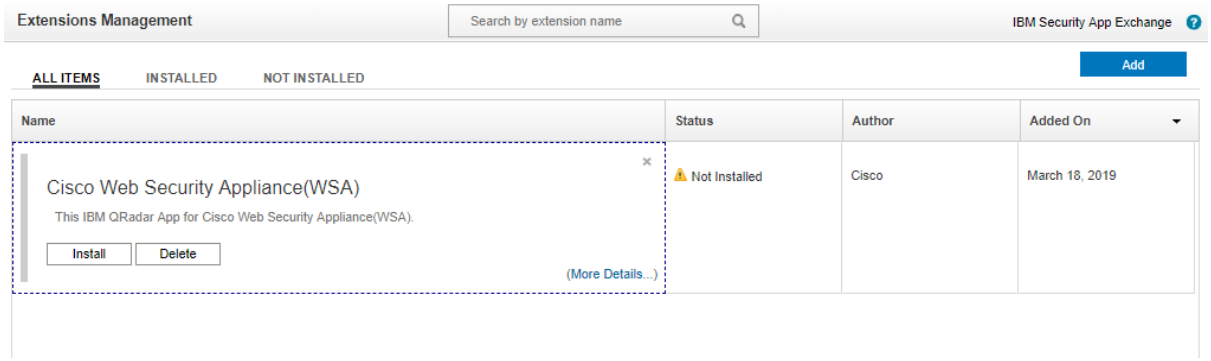
2. General

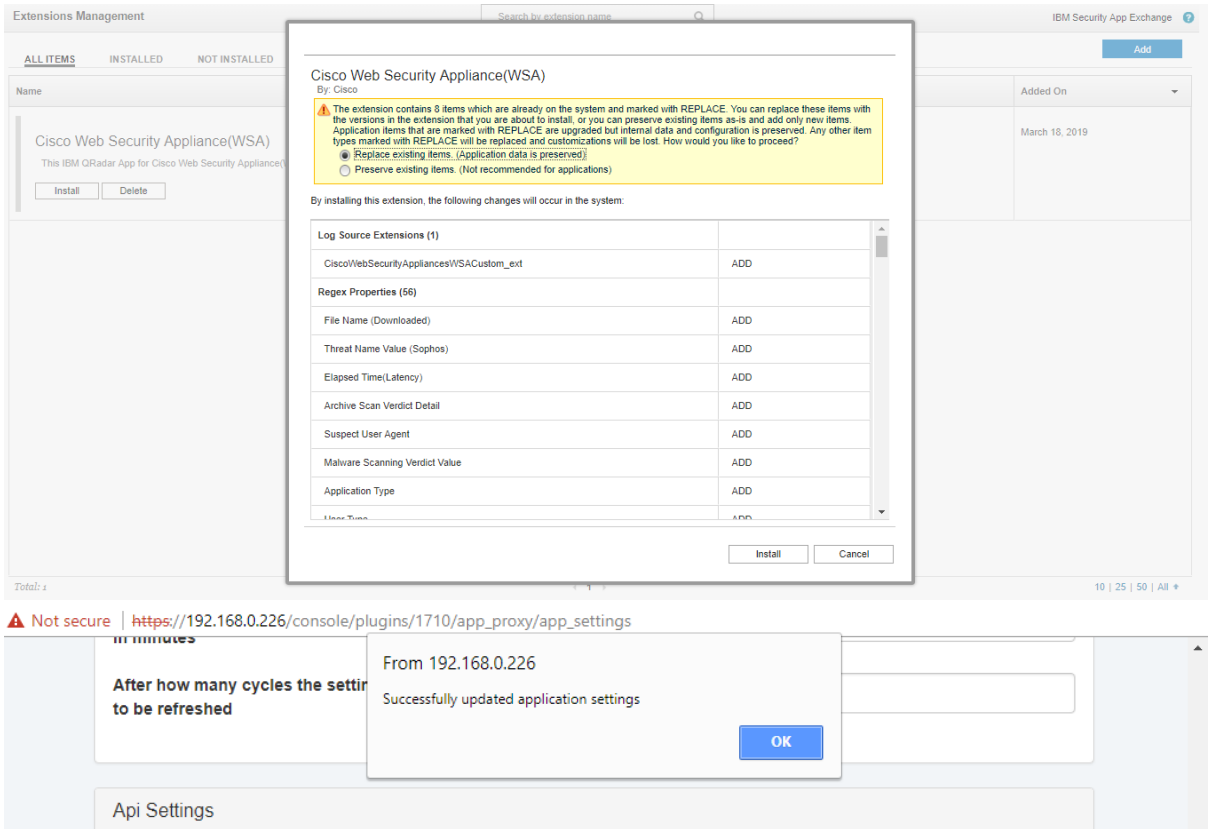
2.1 Installation

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



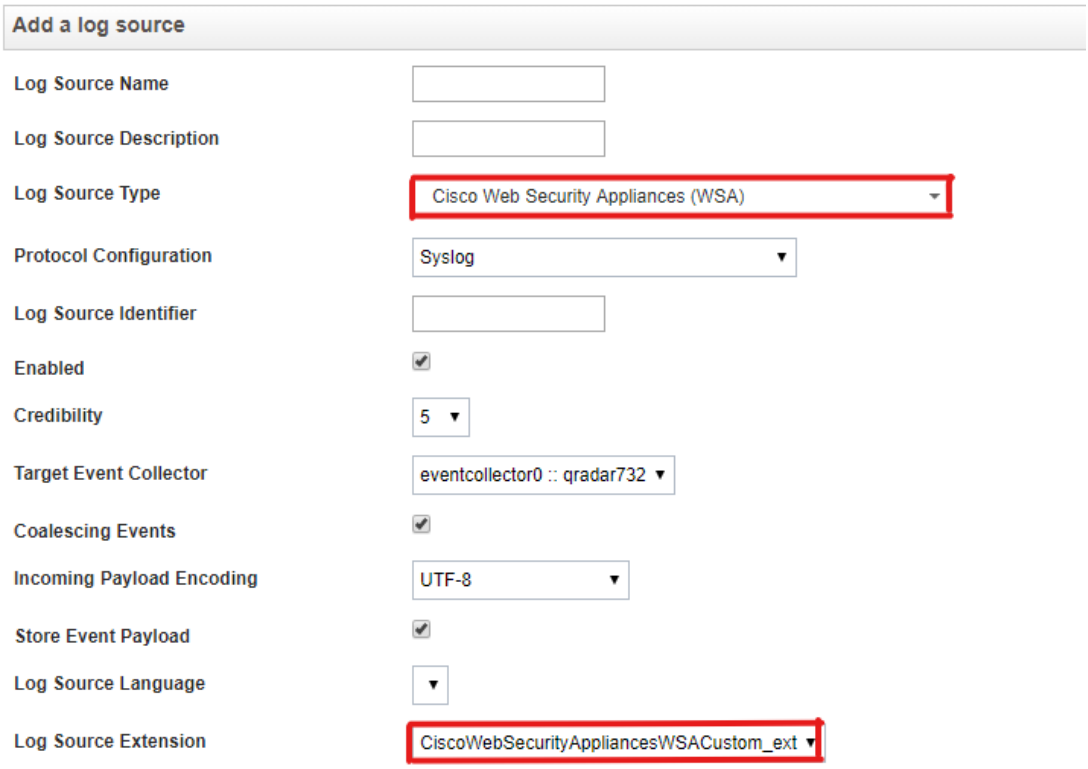






2.2 Configuring Log Source

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



4. Save and Deploy the changes.

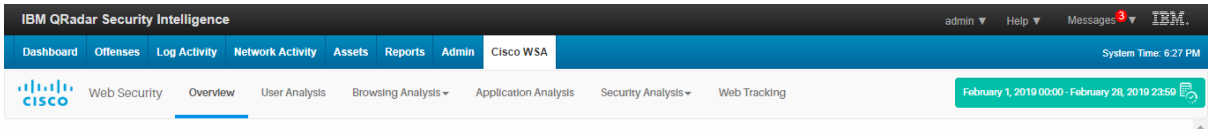
3. Cisco Web Security App

3.1. General

Information displayed in Cisco Web Security App for Syslog.

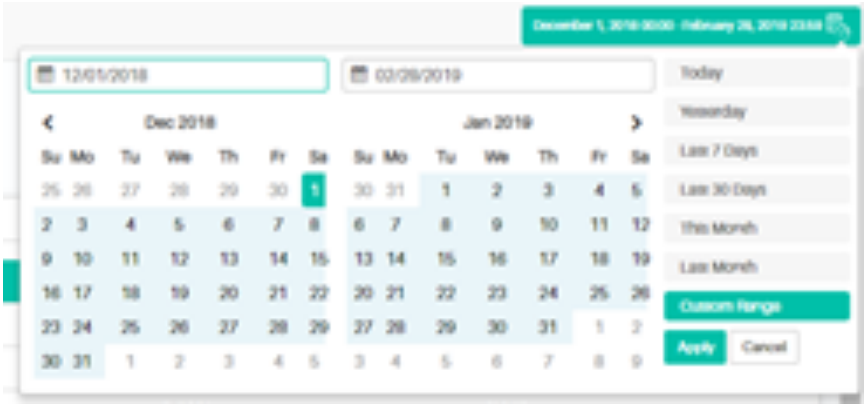
To navigate to the Cisco Web Security app, in IBM QRadar:

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.

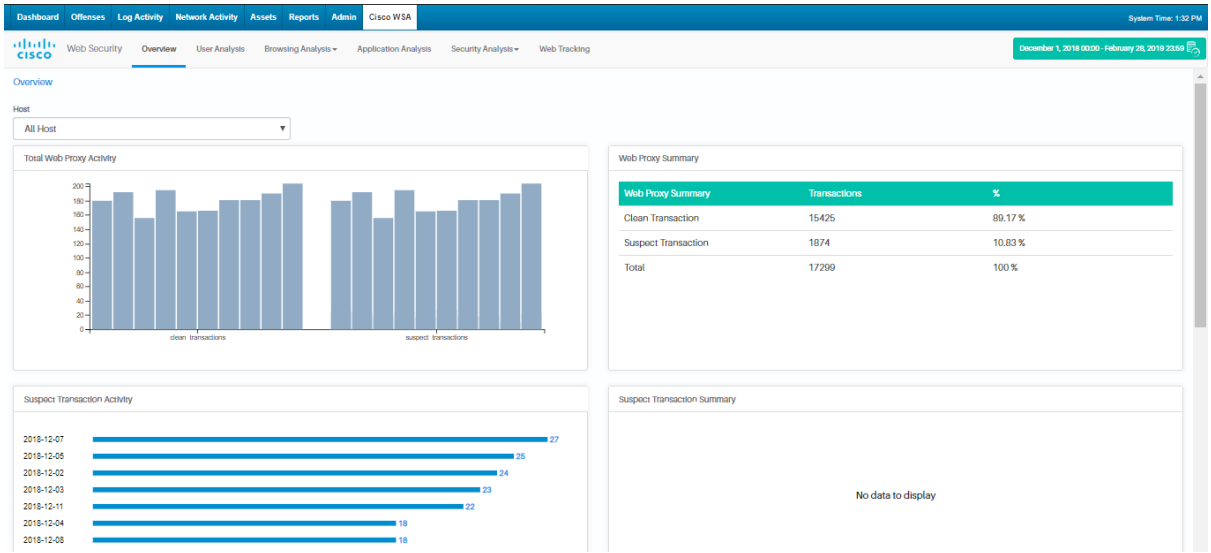


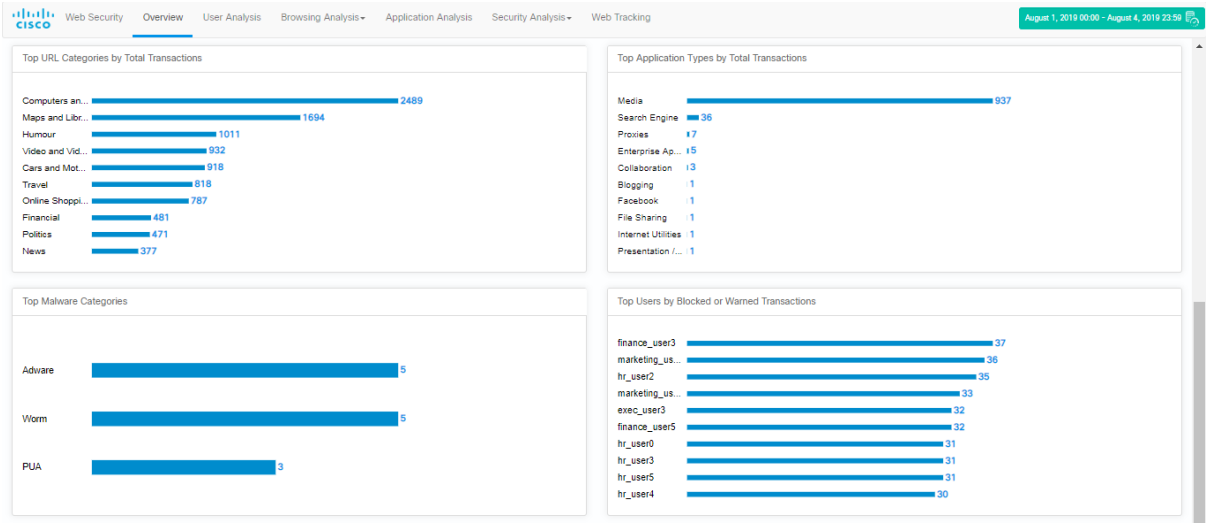
3.1.2. Reset

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

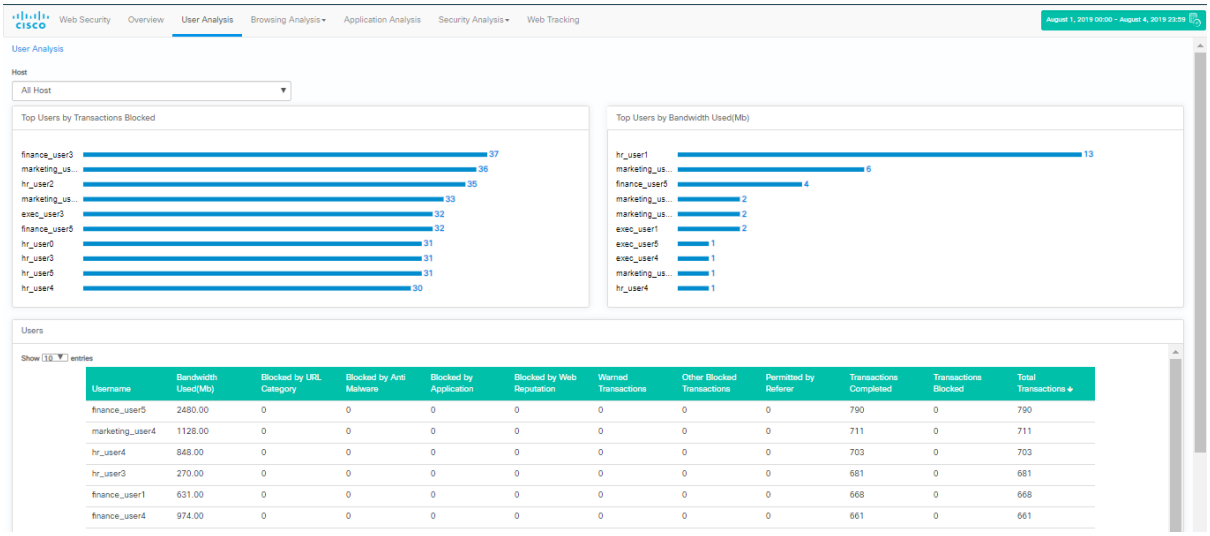
1. Overview Tab enables the user to search the information related to hostname.
2. Overview tab gives the information such as Web Proxy Activity & respective summary, Suspect Transaction Activity and respective summary, URL categories and Malware categories etc.



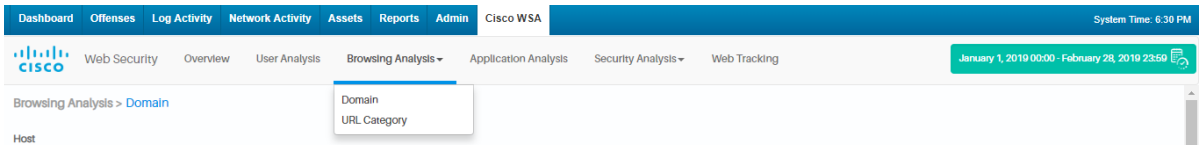


3.3. User Analysis Tab

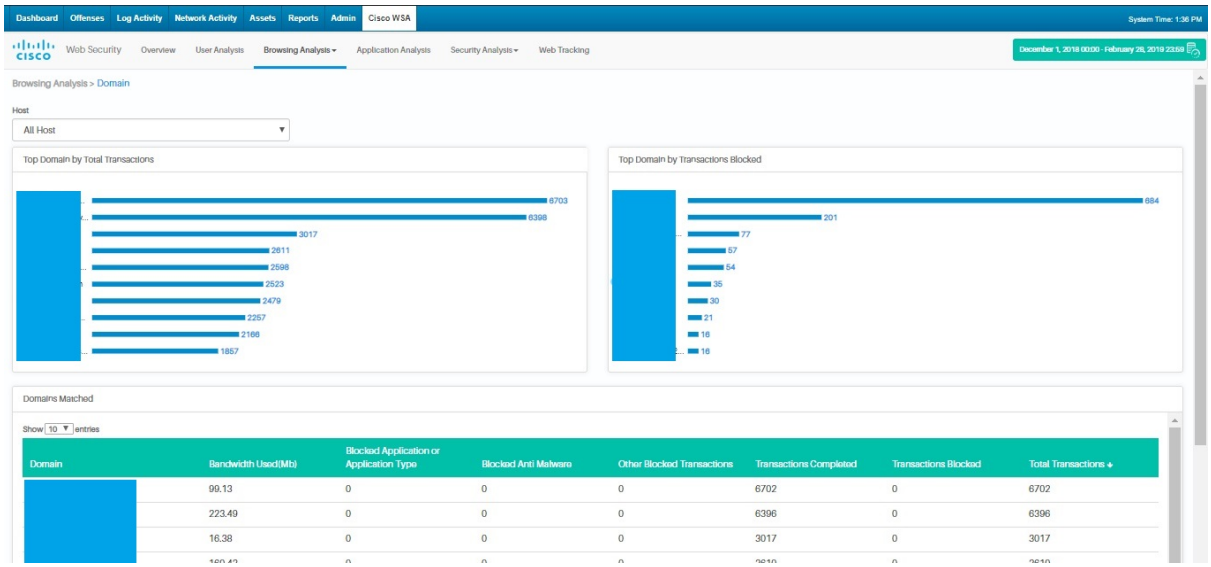
1. Overview Tab enables the user to search the information related to hostname
2. Overview tab gives the information such as Top users by transactions blocked, Top users by Bandwidth used etc.



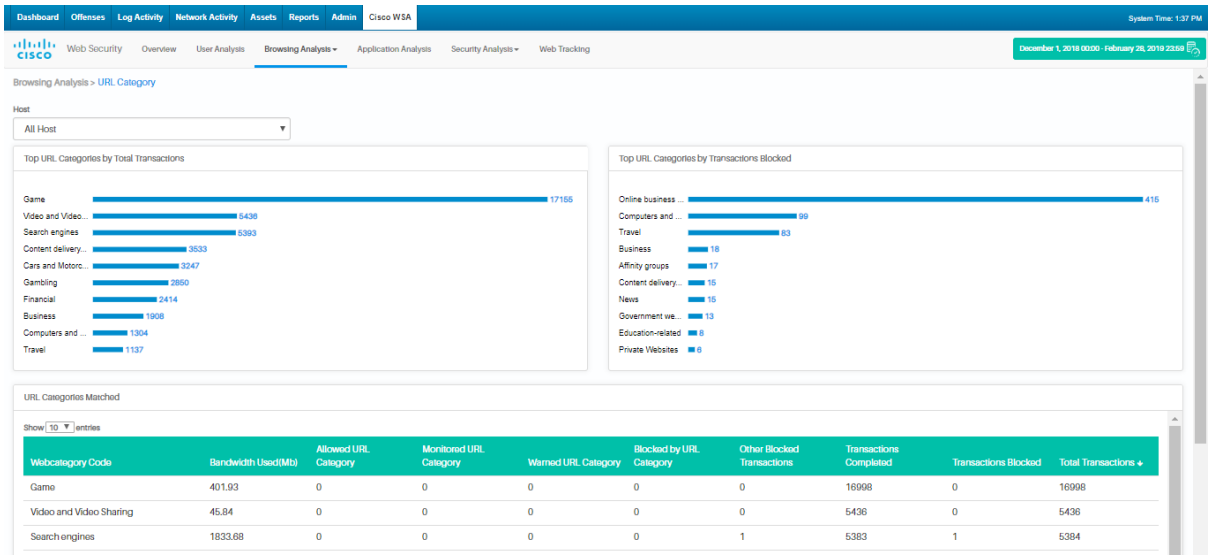
3.4. Browsing Analysis Tab



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

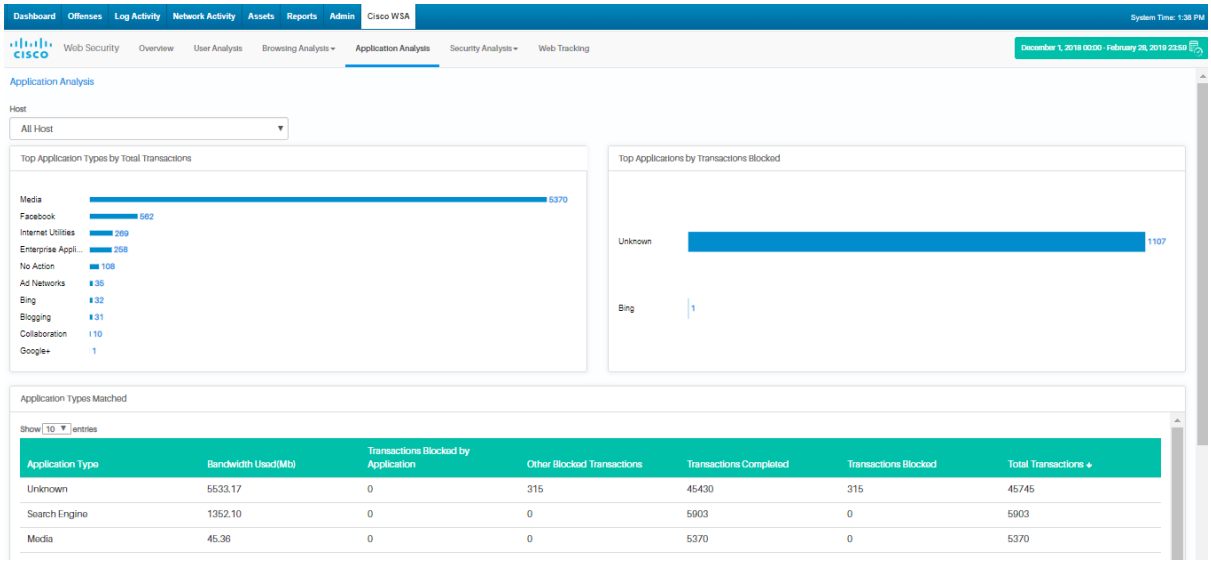


2. The URL category displays the information such as Top URL categories by Total Transactions, Top URL Categories by transactions Blocked and URL matching information.

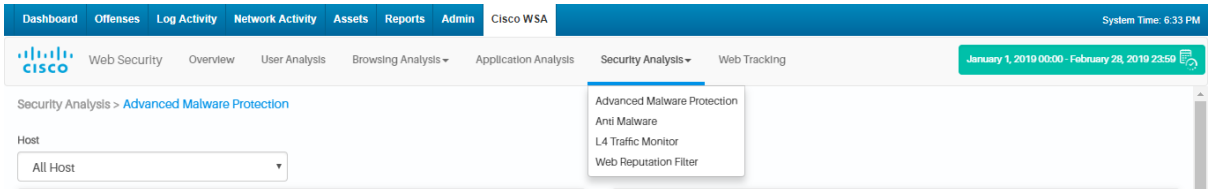


3.5. Application Analysis Tab

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

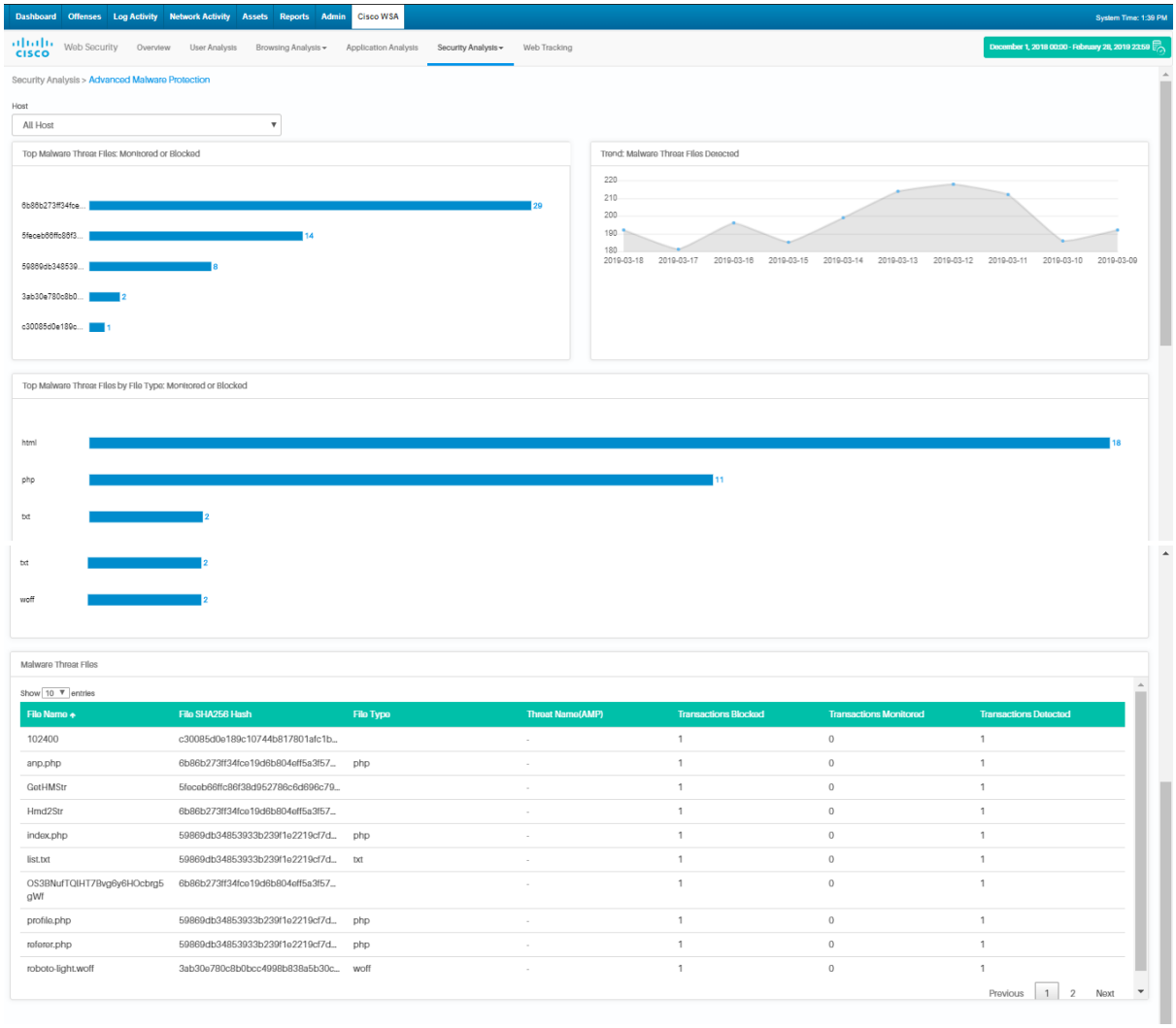


The Security Analysis Menu contains the below sub menus:

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

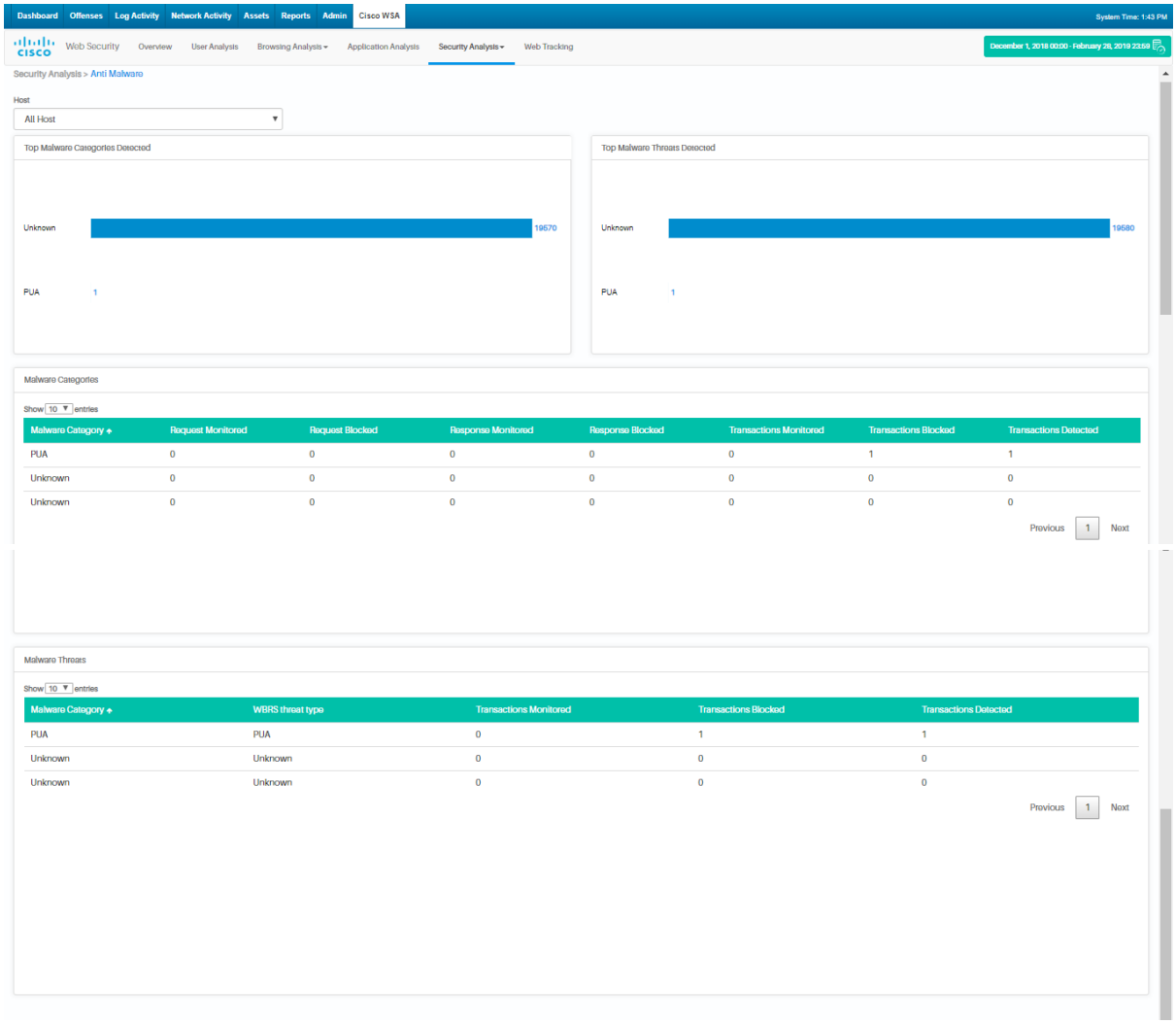
3.6.1 Advance Malware Protection

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.



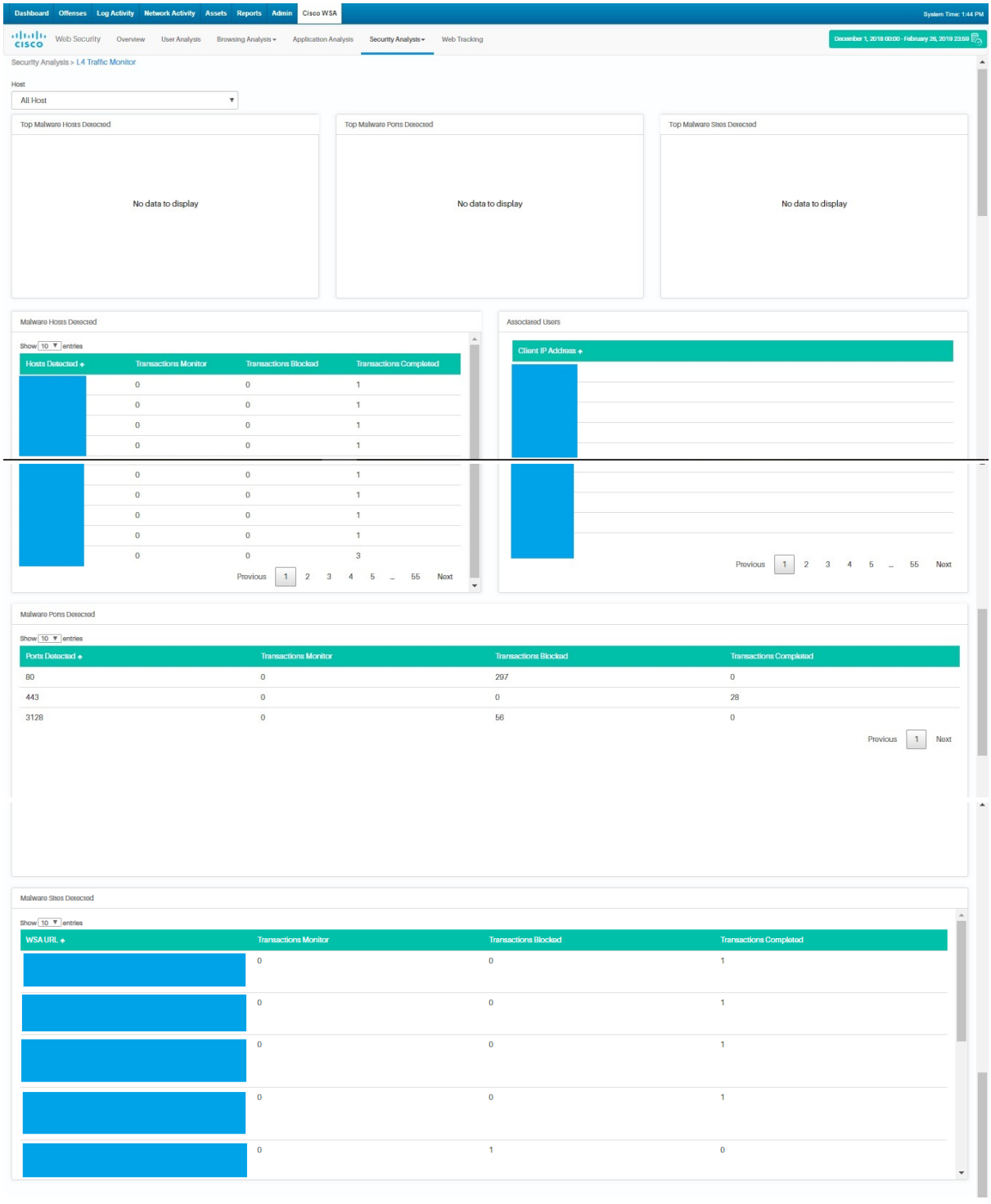
3.6.2 Anti – Malware

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



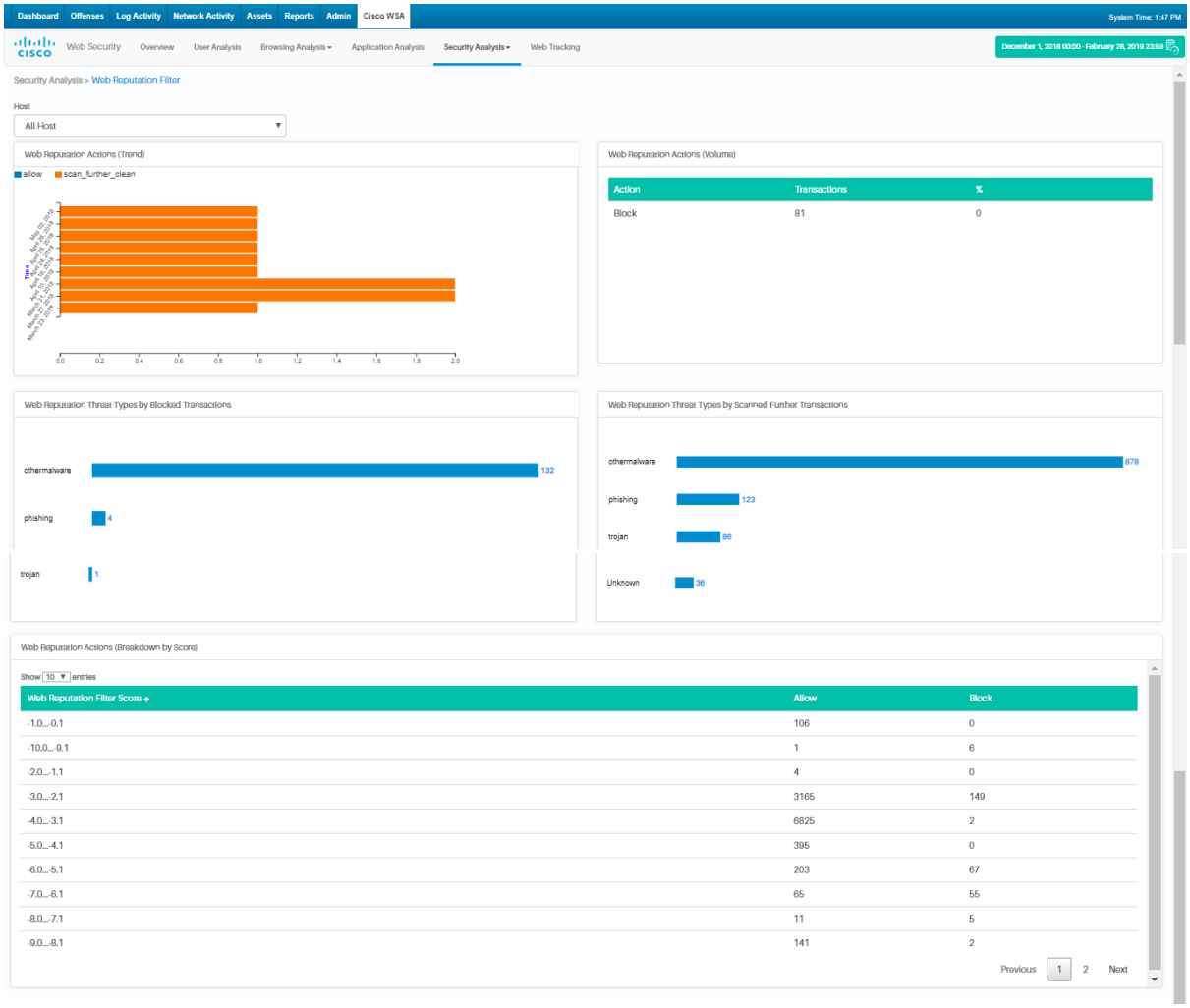
3.6.3 L4 – Traffic Monitor

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.



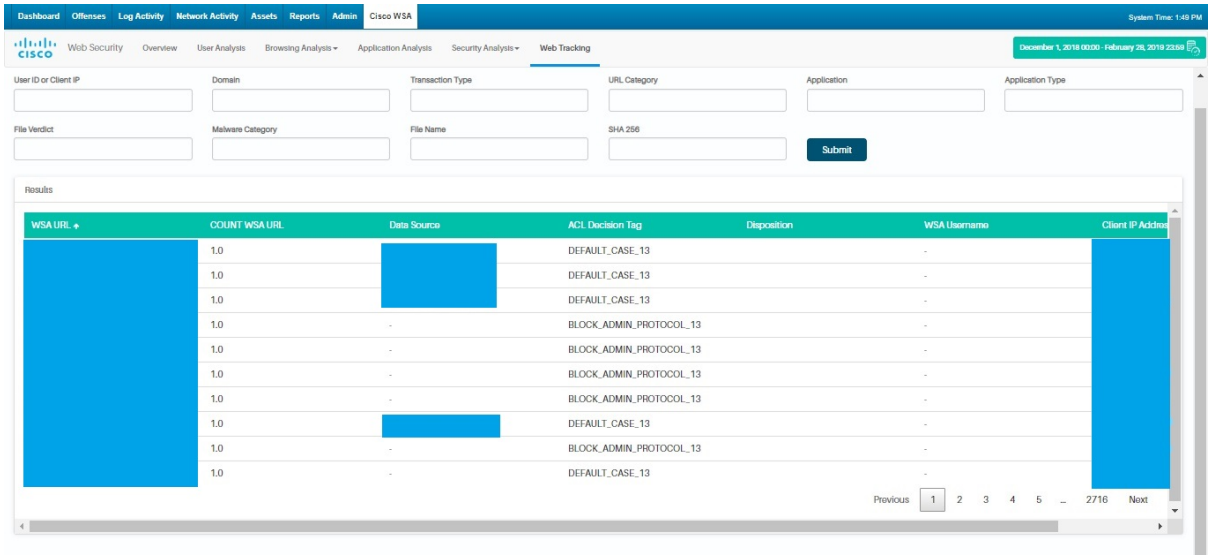
3.6.4 Web Reputation Filter

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.