cisco

Cisco Web Security App for IBM QRadar

Version Number: 1.4

Date: August 05, 2019

Contents

1. Intr	oduction
1.1.	Overview
1.2.	About this Document
1.3.	About the app
1.4.	Prerequisites
1.5.	Custom Field Properties of DSM
2. Ger	neral6
2.1	Installation6
2.2	Configuring Log Source7
3. Cise	co Web Security App8
3.1.	General
3.1	.1. Time Range Selector9
3.1	.2. Reset9
3.2.	Overview Tab9
3.3.	User Analysis Tab
3.4.	Browsing Analysis Tab
3.5.	Application Analysis Tab12
3.6.	Security Analysis Tab12
3.6	.1 Advance Malware Protection12
3.6	.2 Anti - Malware
3.6	.3 L4 – Traffic Monitor14
3.6	.4 Web Reputation Filter15
3.7 W	/eb Tracking Tab16
4. Leg	al Notice17
4.1. C	Confidentiality Notice17

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

<u>c</u> _	P	0	ne	ν.	P	or	20	rtia	(57)	٦
	•	×.	3.	····		~	~~		(o .,	1

- 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

≡ IBM QRadar								Ĺ	<u>i c</u>
Dashboard Offenses I	Log Activity Network Activity	Assets Reports	Cisco Cloud Security					System	Time: 6:17 P
Admin	O Deploy Changes Advance	ad 🔻							
 System Configuration 	There are no changes	to deploy.							
 Data Sources 	System Configuration								
Remote Networks and Services Configuration			1	<u>.</u>		C.	σ ⁴ 0	M	
Try it out	Auto Update	Backup and Recovery	Global System Notifications	Index Mana	jement	Aggregated Data Management	Network Hierarchy	System and License Management	
▶ Apps	~~	1	코무	ul,		2	G	9	
	System Health	System Settings	Asset Profiler Configuration	Custom Offen Reaso	se Close	Store and Forward	Reference Set Management	Centralized Credentials	
		E		*		*	6		
	Forwarding Destinations	Routing Rules	Domain Management	Extensions Ma	nagement	Node Management	Resource Restrictions		
	User Management	a če	9	mil		- mil	Ha		
	Users	User Roles	Security Profiles	Authentic	ation	Authorized Services	Tenant Management		
Extensions Manager	ment		Search by extension	n name		Q		IBM Security App Excha	ange 🕜
ALL ITEMS IN	ISTALLED NOT IN	STALLED						Add	
Name					Status		Author	Added On	-
			No it	ems to display					
		Add	a New Extension	n					
		From	local storage:						
			nstall immediately		Browse				
				Add	Ci	ancel			

Extensions Management	Search by extension name	Q	I	BM Security App Exchange 🛛 🥑
ALL ITEMS IN STALLED NOT IN STALLED				Add
Name		Status	Author	Added On 👻
Cisco Web Security Appliance(WSA) This IBM QRadar App for Cisco Web Security Appliance(WSA).	×	A Not Installed	Cisco	March 18, 2019
Install Delete	(More Details)			

Extensions Management	Search by extension name Q		IBM Security App Exchange 💡
ALLITEMS INSTALLED NOT INSTALLED Name Cisco Web Security Appliance(WSA) This IBM ORadar App for Cisco Web Security Appliance(Install Delete	Cisco Web Security Appliance(WSA) By: Cisco	CE. You can replace these items with ns as-is and add only new items. guration is preserved. Any other item you like to proceed?	Add Added On March 18, 2019
	Log Source Extensions (1) CiscoWebSecurtlyAppliancesWSACustom_ext Regex Properties (56) File Name (Downloaded) Threat Name Value (Sophos) Elapsed Time(Latency) Archive Scan Verdict Detail Suspect User Agent Malware Scanning Verdict Value Application Type Lines Time	ADD ADD ADD ADD ADD ADD ADD ADD ADD ADD	
Total: 1	< 1 >		10 25 50 All +
A Not secure https://192.168.0.226/	console/plugins/1710/app_proxy/app_settings		

After how many cycles the settir to be refreshed	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	
Log Source Description	
Log Source Type	Cisco Web Security Appliances (WSA)
Protocol Configuration	Syslog •
Log Source Identifier	
Enabled	×.
Credibility	5 🔻
Target Event Collector	eventcollector0 :: gradar732 ▼
Coalescing Events	
Incoming Payload Encoding	UTF-8 V
Store Event Payload	
Log Source Language	T
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

IBM QRad	dar Security	Intelligence)							ad	min 🔻	Help 🔻	Messages ⁸ v	IBM.
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Admin	Cisco WSA						System 1	ime: 6:27 PM
ahaha cisco	Web Securi	ty Overvie	w User Analysis	Brows	sing Analys	ls∓ A	pplication Analysis	Security Analysis -	Web Tracking		Febru	ary 1, 2019 00:	00 - February 28, 201	19 23:59 🖏

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.

	12/01	2018						02/28	2019					Today
¢		6	No 201							ien 201			>	woorday
hr	Mo	Tv	We	Th	Fr	54	54	мо	Tu	We	Th	Ft	54	Late 7 Days
25	28	27	28	29	30	1	30	31	1	2	з	4	5	Later 30 Days
2	3	4	5	6	7		6	7		9	10	11	12	The Month
9	10	11	12	13	14	15	13	14	15	16	17	18	19	Las Month
16	17	18	19	20	21	22	20	21	22	23	24	25	26	Conception Review
23	24	25	26	27	28	29	27	28	29	30	31	1	2	
30	31	1	2	3	4	5		4	5		7		0	Acety Carcel

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.



User Analysis Browsing Analysis - Application Analysis Security Analysis -	Web Tracking August 1, 2019 00:00 - August 4, 2019 23:59 🖏
Top URL Categories by Total Transactions	Top Application Types by Total Transactions
Computers an 2489 Maps and Lbr 1694 Humour 1011 Video and Vid 932 Cars and Met 933 Travel 818 Online ShoppI 787 Prinarcial 481 Politics 4/71 Nexe 377	Media 537 Sarah Engine 36 Fronias 17 Enterprise Ap., 15 Collaboration 13 Blogging 1 Froeseook 1 File Shamig 1 Internet URIties 1 Presentation / 1
Top Malware Categories	Top Users by Blocked or Warned Transactions
Advare 5	finance_user3 37 marketing_us 36 hr_user2 35 marketing_us 33
Worm 5	exec_user3 32 finance_user5 32
PUA 3	hr_user0 31 hr_user3 31 hr_user5 31 hr_user4 30

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.

	oser Analysis	Browsing Analysis -	Application Analys	is Security Analy	sis - Web Tracking						August 1, 20
nalysis											
lost		Ŧ									
Users by Transactions Blocked						Top Users by	Bandwidth Used(Mb)				
ice_user3				3	87	hr_user1					
ser2				36		marketing_us.		4	6		
keting_us				33		marketing_us.	2				
_user3				32		marketing_us.	2				
ice_userð				32		exec_user1	2				
-				31		exec_user5					
ser0				31		ever user4	1				
serð serð				31 31		exec_user4 marketing_us.	1				
serð serð ser4			8	31 31 30		exec_user4 marketing_us. hr_user4	1				
ser0 ser3 ser5 ser4				■ 31 ■ 31 30		exec_user4 marketing_us. hr_user4	1				
ser0 ser3 ser5 ser4				31 31 30		exec_user4 marketing_us. hr_user4	1				
5670 5673 5675 75 (10)) entries				31 31 30		exec_user4 marketing_us. hr_user4					
5470 5473 5475 5474 75 75 75 75 75 75 75 75 75 75 75 75 75	Bandwidth Used(Mb)	Blocked by URL Category	Blocked by Anti Malware	31 31 30 Blocked by Application	Blocked by Web Reputation	exec_user4 marketing_us. hr_user4 Warned Transactions	Other Blocked Transactions	Permitted by Referer	Transactions Completed	Transactions Blockad	Total Transactions +
Ser0 Ser0 Ser0 Ser0 (IC T) entries Username finance_user0	Bandwidth Used(Mb) 2480.00	Blocked by URL Category 0	Blocked by Anti Malware 0	31 31 30 Blocked by Application 0	Blocked by Web Reputation 0	exec_user4 marketing_us. hr_user4 Warned Transactions 0	Other Blocked Transactions 0	Permitted by Referer 0	Transactions Completed 790	Transactions Blocked 0	Total Transactions + 790
ser) ser3 ser3 (10) entries Unermanne fnance_user3 marketing_user4	Bandwidth Used(Mb) 2480.00 1128.00	Eliocked by URL Category 0 0	Blocked by Anti Malware 0 0	a 31 a 31 30 Ellocked by Application 0 0	Blocked by Web Reputation 0	exec_user4 marketing_us. hr_user4 Warmed Transactions 0 0	Cther Blocked Transactions 0 0	Permitted by Referer 0	Transactions Completed 790 711	Transactions Blockod 0 0	Total Transactions + 790 711
ser) ser3 ser4 TS Username france_user5 marketing_user4 Ivr_user4	Bendwidth Used(Mb) 2480.00 1128.00 848.00	Biostead by URL Category 0 0 0	Biocked by Anti Malware 0 0	31 33 50 Ellocked by Application 0 0 0	Blocked by Web Reputation 0 0	exec_user4 marketing_us. hr_user4 Warmed Transactions 0 0 0	Other Blocked Transactions 0 0 0	Permitted by Parlerer 0 0	Transactions Completed 790 711 703	Transactions Blocked 0 0	Total Transactionsi ↓ 730 711 703
ser) ser3 ser4 rs rs tigentes thereare finance_user3 marketing_user4 hr_user4 hr_user3	Bendwidth Used(Mb) 2480.00 1128.00 848.00 270.00	Blocked by URL Category 0 0 0 0	Elocked by Anti Malvastre 0 0 0 0	31 33 80 Blocked by Application 0 0 0 0 0	Biochead by Web Reputation 0 0 0	exec_user4 marketing_us. hr_user4 Warmed Transactions 0 0 0 0 0	Cither Blocked Transactions 0 0 0 0	Permitted by Parlerer 0 0 0 0	Transactions Completed 790 711 703 681	Transactions Blocked 0 0 0 0	Total Transactione • 790 711 703 681
ser0 ser3 ser4 (10 T) ensites Username finance_user15 marketing_user4 hr_user3 finance_user11	Bendwicth Used(Mb) 2480.00 1128.00 848.00 270.00 631.00	Blocked by URL Category 0 0 0 0 0	Blocked by Anti Malware 0 0 0 0 0 0	31 31 30 Ellocked by Application 0 0 0 0 0	Blocked by Web Reputation 0 0 0 0 0	exec_user4 marketing_us. hr_user4 Warmsd Transactions 0 0 0 0 0 0 0 0	1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Permitted by Referent 0 0 0 0 0	Transactions Completed 790 711 703 681 668	Transactions Bioclard 0 0 0 0 0 0	Total Transactiona • 790 711 703 681 668

3.4. Browsing Analysis Tab

Dashboard	Offenses	Log Activity	Network Activity	Assets Repor	ts Admir	Cisco WSA			System Time: 6:30 PM
ahaha cisco	Web Secu	ity Overvie	w User Analysis	Browsing An	alysis -	Application Analysis	Security Analysis -	Web Tracking	January 1, 2019 00:00 - February 28, 2019 23:59 🗒
Browsing Ar	nalysis > Do	main		Domain URL Category					
Host									

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

Dashboard Offenses Log Activ	vity Network Activity Assets Reports	Admin Cisco WSA					System Time: 1:	36 PM
Web Security Ow	erview User Analysis Browsing Analy	sis - Application Analysis Se	curity Analysis - Web Tracking				December 1, 2018 00:00 - February 28, 2019 23:55	5
Browsing Analysis > Domain								-
Host								
All Host	٣							
Top Domain by Total Transactions	8			Top Domain by Transactions Blo	cked			
			6703				684	
	3017		6398		201			
	2611			57				
	2598			54				
	2479			30				
	2257			= 21				
	1857			16				
								1
Domains Matched								
Show 10 V entries								
		Blocked Application or						
Domain	Bandwidth Used(Mb)	Application Type	Blocked Anti Malware	Other Blocked Transactions	Transactions Completed	Transactions Blocked	Total Transactions +	
	99.13	0	0	0	6702	0	6702	
	223.49	0	0	0	6396	0	6396	
	16.38	0	0	0	3017	0	3017	
	100.42	٥	0	0	0010	0	2010	

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.

Dashboard Offenses Log Activity Network Activity Assets	Reports Admin Cisco WSA	A						System Tim	e: 1:37 PM
CISCO Web Security Overview User Analysis Brow	Ing Analysis - Application Ar	nalysis Security Analysis +	Web Tracking				Decembe	er 1, 2018 00:00 - February 28, 2019 :	
Browning Analysis > URL Category Heat All Host Top URL Categories by Total Transactores Game Vela and Velac. Search engine Search engine Contrant delivery. Status Cara and Motor. Stat]		17185 C C T T B A C C T T B A C C C T T B A C C C T T B A C C C T T B A C C C T T B A C C C C T T T C C C C C C C C C C C C	Top URL Categories by Trans Drine business - fravel - Miney proves - Miney proves - Miney proves - Miney proves - Miney proves - Sovernment Westers - O Privets Websters - 0	actions Blocked			415	
URL Categories Matched Show 10 T entries Webcategory Code Bandwidth UsedR	Allowed URL (b) Category	Monitored URL Category	Warned URL Category	Blocked by URL Category	Other Blocked Transactions	Transactions Completed	Transactions Blocked	Total Transactions +	
Game 401.93	0	0	0	0	0	16998	0	16998	
Video and Video Sharing 45.84	0	0	0	0	0	5436	0	5436	
Search engines 1833.68	0	0	0	0	1	5383	1	5384	

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.

Dashboard Offenses Log Activity Netwo	ork Activity Assets Reports Admin	Cisco WSA					System Time: 1:38 F
CISCO Web Security Overview I	User Analysis Browsing Analysis -	Application Analysis Security Analysis -	Web Tracking				December 1, 2018 00:00 - February 28, 2019 23:59
Application Analysis Host All Host	¥						
Top Application Types by Total Transactions Media Facabook 662 Internet Utilities 200 No Action 100 Ad Newrons 135 Bing 132 Biogring 131 Collaboration 110 Google+ 1			5370	Top Application	n by Transactions Blocked		1107
Application Types Matched							A
Application Type	Bandwidth Used (Mb)	Transactions Blocked by Application	Other Blocked Tra	nsactions	Transactions Completed	Transactions Blocked	Total Transactions +
Unknown	5533.17	0	315		45430	315	45745
Search Engine	1352.10	0	0		5903	0	5903
Modia	45.36	0	0		5370	0	5370

3.6. Security Analysis Tab

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco WSA	System Time: 6:33 PM
CISCO Web Security Overview User Analysis Browsing Analysis - Application Analysis	Security Analysis - Web Tracking January 1, 2019 00:00 - February 28, 2019 23:59
Security Analysis > Advanced Malware Protection	Advanced Malware Protection Anti Malware
Host	L4 Traffic Monitor
All Host 🔹	Web Reputation Filter

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.

Dashboard Offenses Log Activity	Network Activity Assets Reports Admir	Cisco WSA				System Time: 1:39 F	РМ
CISCO Web Security Overview	User Analysis Browsing Analysis +	Application Analysis Security Analysis -	Web Tracking			December 1, 2018 00:00 - February 28, 2019 23:59	9
Security Analysis > Advanced Malware R	Protection						Â
Host							
All Host	Ŧ						l
Top Malware Threat Files: Monitored or I	Blocked			Trend: Malware Threat Files Detected			l
				220			l
6b86b273#34fce			29	210			l
5feceb60ffc88f3	14			190			l
59889db348539	8			180 2019-03-18 2019-03-17 2019-03-18 2019-03-1	5 2019-03-14 2019-03-13 2019	03-12 2019-03-11 2019-03-10 2019-03-09	l
2=520=720=250							l
2 2 Contract (200000							1
c30085dDe189c 🚺 1							
Top Malware Threat Files by File Type: N	tonitored or Blocked						
html						18	
php				11			
bd	2						
bd	2						*
wom	2						
Malware Threat Files							
Show 10 Tentries						A	
File Name +	File SHA256 Hash	File Type	Threat Name(/	MP) Transactions Blocked	Transactions Monitored	Transactions Detected	
102400	c30085d0e189c10744b817801afc1b		-	1	0	1	
anp.php	6b86b273tf34fce19d6b804eff5a3t57	php		1	0	1	
GotHMStr	5feceb66ffc86f38d952786c6d696c79			1	0	1	į,
Hmd2Str	6b86b273ff34fce19d6b804eff5a3f57_			1	0	1	I
index.php	59869db34853933b239f1e2219cf7d	php		1	0	1	I
list.txt	59869db34853933b239f1e2219cf7d	txt		1	0	1	I
OS3BNufTQIHT7Bvg6y6HOcbrg5 gWf	6b86b273ff34fce19d6b804eff5a3f57			1	0	1	
profile.php	59869db34853933b239f1e2219cf7d	php		1	0	1	
referer.php	59869db34853933b239f1e2219cf7d	php		1	0	1	
roboto-light.woff	3ab30e780c8b0bcc4998b838a5b30c	woff		1	0	1	I
						Previous 1 2 Next *	

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 L	Log Activity Network Activity	Assets Reports Admin Cisco	WSA		System	Time: 1:44 Pi
Web Security	/ Overview User Analysis	Browsing Analysis - Application	on Analysis Security Analysis - Web Track	Ing	December 1, 2018 00:00 - February 28, 20	019 2369 🗒
Security Analysis > L4 Traf	ffic Monitor					
Host						
All Host		*				
Top Malware Hosts Detec	ned		Top Malware Ports Detected		Top Malware Stees Detected	
	No data to display		No.d	ata to display	No data to display	
	no one to cropiny			and to aniphay		
Malware Hosts Detected				Associated Users		_
Show 10 T entries	Transactions Monitor	r Transactions Disclored	Transactions Completed	Client IP Address 🛧		
			1			
	0	0	1			
	0	0	1			
	0	0	1			
	0	0	1			- 11
	0	0	1			
	0	0	1			
	0	0	1			
	0	0	3		Provinus 1 2 3 4 5 55 No	ant
		Previous 1 2	3 4 5 55 Noxt			
						=1
Malware Ports Detected						_
Show 10 V entries		Transactions Mon	itor	Transactions Blockod	Transactions Completed	- 1
80		0	104	297		- 1
443		0		0	28	- 1
3128		0		56	0	
					Provious 1 Ne	axt
Malware Sites Detected						
Show 10 Tentries						^
WSA URL 🛧		Transactions Monit	or	Transactions Blockod	Transactions Completed	
		0		0	1	
		0		0	1	
		0		0	1	
		0		0	1	
		0		1	0	-
		Ŭ			U	-
						1

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.

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Cisco WSA		System Time: 1:47 PM
CISCO Web Security Overview User Analysis Browsing Analysis • Application Analysis Security Analysis • Web Tracking		December 1, 2018 00:00 - February 28, 2019 22:59 🛱
Security Analysis > Web Reputation Filter		
Host		
All Host V		
Web Reputation Actions (Trend)	Web Reputation Actions (Volume)	
alow scan_further_clean	Action Transactione	
	Block 81	0
Web Reputation Threat Types by Blocked Transactions	Web Reputation Threat Types by Scanned Further Transactions	
othermalware 132	othermalware	878
	phishing 123	
phishing 4		
	trojan 86	
trojan I	Unknown 36	
Wich Danusesion Antions (Broakdown by Score)		
		*
Snow 10 V jennes	Alkow	Block
10.01	106	0
-1000.1	1	6
20-11	4	-
-30_21	3165	149
-403.1	6825	2
-5.04.1	395	0
-6.05.1	203	67
-7.06.1	65	55
-8.07.1	11	5
-9.08.1	141	2
		Previous 1 2 Next v

3.7 Web Tracking Tab

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

Web Security Ove	erview User Analysis Browsing Analysis •	Application Analysis Security Analysis	is - Web Tracking		Decembr	er 1, 2018 00:00 - February 28, 2019
or Client IP	Domain	Transaction Type	URL Category	Application	Application 1	Туре
let	Malware Category	File Name	SHA 256	Submit		
				300111		
S						
A URL 🕈	COUNT WSA URL	Data Source	ACL Decision Tag	Disposition	WSA Usomamo	Client IP Addr
	1.0		DEFAULT_CASE_13			
	1.0		DEFAULT_CASE_13			
	1.0		DEFAULT_CASE_13			
	1.0		BLOCK_ADMIN_PROTOCOL_13			
	1.0		BLOCK_ADMIN_PROTOCOL_13			
	1.0		BLOCK_ADMIN_PROTOCOL_13			
	1.0		BLOCK_ADMIN_PROTOCOL_13			
	1.0		DEFAULT_CASE_13			
	1.0		BLOCK_ADMIN_PROTOCOL_13			
	1.0		DEFAULT_CASE_13			

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.