Splunk for Cisco IronPort WSA: User Guide

Table of Contents

Introduction:	
Supplement to Existing Splunk Documentation:	3
Logging In:	3
Report Usage:	3
Choosing a Time Range:	3
Find Data:	3
Export Data	3
Option 1	3
Option 2	3
Tables:	4
Sorting Columns	4
Choosing Fields	4
Report Descriptions:	4
Overview	4
Users	5
Web Sites	6
URL Categories	7
Application Visibility	7
Anti-Malware	8
Client Malware Risk	9
Web Reputation Filters	10
L4 Traffic Monitor	11
Reports by Drilldown	
Malware Category Drilldown	
Malware Threat Drilldown	
Application Drilldown	12
Application Type Drilldown	
Domain Drilldown	
URL Category Drilldown	
User Drilldown	
Reports by Location	
Overview by Location	
URL Categories by Location	
Anti-Malware by Location	

Web Reputation Filters by Location	12
Application Visibility by Location	12
Users by Location	12
Websites by Location	12
Web Tracking (form based search) Simple	13
Advanced	14
Sample Usage Scenarios	15
FAQ	16
Why does the overview report show more events than are in Splunk?	16
How may I improve performance when I perform ad hoc queries?	16
Why am I missing hosts? Why do I see extra hosts? How do I change the label of hosts?	16
How do I change the dropdown options on the web tracking report?	16
Why do I not see trafmon (L4TM) logs? Why do I only see data for specific departments?	17

Introduction:

This manual covers the Splunk Cisco IronPort WSA Reporting Application for users of the application. This application provides reports and dashboards that can give you insight into data from the IronPort Web Security Appliance (WSA).

Supplement to Existing Splunk Documentation:

This guide serves a supplement to the existing body of documentation existing at http://docs.splunk.com.

It is not intended to replace existing Splunk materials or techniques regarding user experience. This guide will serve as a supplement by reviewing functionality as it relates to this application.

Logging In:

Information regarding login credentials and URL should be procured from the Splunk administrator(s). The credential should be entered at the Splunk Login page to access the SplunkforCiscoIronportWSA application.

Report Usage:

Choosing a Time Range:

Each report contains a Time Range Picker. This dropdown box (located in the report's upper left hand corner) allows you to specify the time range from which to pull reports. You may choose from pre-defined ranges or select a custom range. Smaller time range are generally more preferred – especially on the Web Tracking (ad hoc search) and L4TM reports which do not leverage summarized data optimization and report directly against raw data.

Find Data:

There are many pre-defined reports (described in below "Report Descriptions" section).

Additionally, the drilldown reports will allow you to specify specific information. For example, the User Drilldown report allows you to type the name of a specific user and re-run the report. Alternatively, this may be accomplished by clicking on a user ID wherever it is displayed in a table on any report. This is true of all drilldown reports.

Another way to search data is to navigate to the Web Tracking report. The advanced link will present more options narrow the scope of your search compared to the *simple* version which contains fewer options

Export Data

There are two options for manually exporting data.

Option 1

You may go to the Web Tracking form, search for desired data, and click the Export button in the upper right hand corner.

Option 2

If your Splunk administrator enabled PDF you may save any report as a PDF by choosing that option in the upper left corner of the report.



Tables:

Sorting Columns

You may click on any column header to sort by that column. Clicking on a column header again will reverse the order of the sort.

Choosing Fields

You may use the *Pick fields* link anywhere it exists to choose the columns displayed in a report's table. This is especially useful on the web tracking report to display individual URLs visited for specific domains and other information that is initially hidden to make the layout easier to navigate.

Drilling In

All tables that contain hyperlinked data may be clicked on to drilldown further. The target page will vary based on which column in the table was clicked (e.g. clicking on a user will take you to the user drilldown).

Report Descriptions:

Overview

The Overview report contains a high level view of appliances reporting to Splunk. The top of the report contains graphs and tables aggregating information received from access logs and L4TM logs. The bottom portion of the report details usage by user ID or IP address.



Users

The Users report shows usage information about all users. The drilldown report may be used to report on individuals.

unk> ' + + cisco. ni for Claco ironport WSA . Searches .		•]								
								Logged in as admi	in App - Managa	Aleris Jobs
								_		a Help
Actions +	_									
ays -										
Users by Transactions Blocked				Top Users by Bandwidth Used						
mfg_user2 finance_user2 192.168.240.101 end_user3 end_user3 end_user3 contract_user5 eng_user5				mig usert mig usert finance usert inance usert mig usert end usert end usert end usert guest user6	2510		0510	0510	-	1.051
-	1,000,000 2,000	,000 3,000,000	4,000,000		2E12	4E12	6E12	8E12	10E12	1.2E13
	T	ransactions					KByt	es		
rs uts per page 10_+										
ala per paga 10 -	Bandwidth Used I	Tima Saert 8	Transactions Compl	elect 1	Transactions Blocked			Total Transact	Som)	
its per page 10_+	Bandwidth_Usad 1 10700.71 TS	Time_Specf. # 2+0521:27.00	Transactions_Compl 784254459	eted 1	Transactions_Biocked			Total_Transact 754055495	Sons)	
fa per page 10 + 1 feids sec_JD_or_Client_JP 1				alaced 3		E 0			dons I	
In per page IC_+ Initia Ini	10709.71 TB	2+08:21:27.00	784958489	efed 3	8	1.0		784958495	Sens I	
In per page IC +	10700.71 TB 8460.00 TB 7902.25 TB 9799.34 TB	2+0821:27.00 3+0421:32.00 1+21:03:10.00 3+08:07:55.00	784958489 619576873 578854018 422107708	eted 1	6 4 1 8	**		784058495 610576877 578864019 422107716	dons 8	
Is per page IC Is before, IP 1 g_ser/1 g_ser/1 g_ser/1 sam7 man_user/2 man_user/	10700.71 TB 8400.00 TB 7902.25 TB 5759.34 TB 5621.13 TB	2+08.21:27.00 3+04.21:22.00 1+21:53.10.00 3+08.07:55.00 3+08.27:55.00	784958489 619576873 578894018 422107708 412215349	alad 1	6 4 1 8 13	••		784058495 610576877 578864019 422107716 412215362	dons (
is per page [[] bits m.r.(D.p.r.(Elem.)P) g_amer1 g_amer1 same1 same1 g_amer3 same3 same3 sames3 sam	80708.71 TS 8480.00 TS 7002.25 TS 5789.34 TIS 5621.13 TS 4081.12 TIS	2+08.21:27.00 3+04.21:32.00 1+21:53.10.00 3+08.07:55.00 3+08.26:58.00 3+08.26:718.00	784258459 619576873 578854015 422107706 412215349 364038006	elod 1	6 4 1 8 13 2471787	* *		784058498 810578877 578864019 422107716 412215382 366500833	áons I	
ام به به به ال عن ال عن المالية المالي المالية المالية المالية المالية المالية المالية المالية المالية	10700 /1 13 8460.00 T0 7960 23 10 9758 24 10 9621 13 T0 4661 12 T0 4425 32 T0	2+0821:27.00 3+0421:32.00 1+21:53.10.00 3+0827:55.00 3+082555.00 3+02257.10.00 4+01:53.35.00	78495489 619578673 578864018 422107708 4122105708 384038088 324807341	eled)	6 4 5 5 13 2471787 28			784958495 611676677 578864019 422107716 412215362 366509633 324617367	Sona I	
ta per paga IC fields aer_JD_er_Client_JP 8 Ig_user1	80708.71 TS 8480.00 TS 7002.25 TS 5789.34 TIS 5621.13 TS 4081.12 TIS	2+08.21:27.00 3+04.21:32.00 1+21:53.10.00 3+08.07:55.00 3+08.26:58.00 3+08.26:718.00	784258459 619576873 578854015 422107706 412215349 364038006	ned 1	6 4 1 8 13 2471787			784058498 810578877 578864019 422107716 412215382 366500833	Sona 9	

Web Sites





URL Categories

unk> 'lliili' secuerty cisco. Searches -				Logged in as admin App - Manager Alerts Jobs I
Categories Actions -				- net
categories Actors -				
Days -				
URL Categories by Total Transactions			Top URL Categories by Blocked and Warned Transaction	ons
Computers and Internet Shopping Transportation Health and Nutrition Travel News Business and Industry Afts and Entertainment Sports and Recreation Government and Law	600,000,000	10E8 1.4E9	Pom Computers and Internet Filter Avoidance Instant Messaging Search Engines and Portals Gambing Aduit Weapons Arts and Entertainment. Hacking	3,000,000 5,000,000 7,000,000
	Transactio	ons		Transactions
		ons		
IL Categories Matches		ns		
-		ins		
LL Categories Matches suits par page 10 -		ins		
sults per page 10 -		ins blocked webcat :	allowed transactions s	
sults per page 10 • fields k_webcat_code_full #	Transactio		allowed_transactions # 120503155	Transactions
tulls per page 10 • k fields k webcat_code_full : Computers and Internet	Transactio	blocked_webcat #		Transactions count_transactions 1
telis per page 10	Transactic bytes_allowed : 17508.37 TB	blocked_webcat ¢ 0	1283638155	count_transactions :
k felds k felds k webcat_code_full E Computers and Internet Mapping Transportation	bytes_allowed : 17006.37 TB 16563.09 TB	blocked_webcat † 0 0	1283638155 1214109172	Count_transactions : 128496970 1214109172
k feids k feids k webcat_code_full t Computers and Internet Shopping Imagination Health and Nutrition	bytes_allowed s 17506.37 TB 16062.05 TB 16047.17 TB	blocked_webcat # 0 0 0	1283638165 1214169172 758381282	Count, transactions 2 1284949570 1214169172 755381282
sulls per page 10 • • • • • • • • • • • • • • • • • •	bytes_allowed : 17506.37 TB 16553.09 TB 10347.17 TB 6994.29 TB	blocked_webcat t 0 0 0 0	1285030155 1214109172 758391282 658640173	Count_transactions 1 128499570 1214109172 759391292 60840181
sults per page 10 🔹	bytes_allowed : 1750e.37 TB 16955.00 TB 10347.17 TB 8984.29 TB 7606.40 TB	bicked_webcat ¢ 0 0 0 0 0	1283638165 1214169172 756381282 665640173 5569642820	Count_transactions # 128484670 1274109172 756381282 668464181 509642820
k fields k fields k mekset, code, full 1 Computers and Internet Messith and Notifion Transportation Health and Notifion Transel News	bytes_allowed : 170063.7 TB 16053.09 TB 10347.17 TB 8984.29 TB 7006.46 TB 7205.05 TB	blocked_webcat # 0 0 0 0 0 0 0	1289638195 1214109172 758915282 658940173 566942820 527853237	Count_transactions : 128494970 121409172 756381282 658642181 555642820 627853237
k fields k fields k webcat_code_full t Computers and Internet Bhopping Transportation Transel News Business and Industry	bytes_allowed s 17506.37 TB 16565.09 TB 10347.17 TB 8894.29 TB 7050.40 TB 6899.70 TB	blocked_webcat t 0 0 0 0 0 0 0 0 0 0	1283638165 121469172 756381282 658840173 555642820 52785237 505557300	Count_transactions : 1284948970 1224168172 796381282 665840181 566942820 52785327 605857301

Application Visibility

	App	lication Visibility - Splu	nkforCiscolronportWSA – Splur	nk 4.2.1 (98164)			_		1
Application Visibility - Splur	nkforC +									
unks thethe source							Ligger(11 ex	istrin (Allo -	Meraper An	na Jaka
CISCO. R for Class Irongont WSA . Searches .					_					
eation Valibility Actors -						_	_	_		• mp
cation Visibility Actions -										
Days -										
Applications Types by Total Transactions			Top Applications by Blocked Transactions							
			154130, 12							
YouJube			GenericSearchEngi	ineTraffic						
GenericSearchEngine (raffic)										
Pandora Ly e365			Facebo	pok Chat						
Facebook General										
Blogger			u	uickTime						
YouTube GenericSearchErprite Vario Hardon Lyests Facebook General Booger Cragsist	400,000	800,000 1,	200,000	20	40 60	80	100	120	140	160
	400,000	800,000 1,	200,000	20	40 00	80	100	120	140	100
		1223				<u>11</u>				
	Tra	insactions				Transact	ions			
plication Types Matched										
nuts per page 10										
A Fields										
K_HVS_hpe I Media	bytes_slowed 8	allowed_transaction	e e biocked	d_application #		court_transa	ctiona I			
Search Engine	198.30 MB	9135	9			10152				
Facatoria.	1.12.508	112	0			129				
Biogging	813.71 KB	73	0			73				
		48	0			48				
Social Networking	2.29 MB					21				
Enkadir	454.00 K2	21	0							
Linkadir Presentation / Contenencing	454.00 KB 614.82 KB	21 21	0			21				
Linkadir Presentation / Contenencing	454.00 K2	21	0							
Linkadir Presentation / Contenencing	454.00 KB 614.82 KB	21 21	0			21				
Enhade Presentation / Conferencing Waterset	454.00 KB 614.82 KB	21 21	0			21				
Sout Anexating Chardon Phanetasian (Contenency Webmill Splication Matched	454.00 KB 614.82 KB	21 21	0			21			_	
Unado Preventaria i Contenenza Volkonal gelaction Matched mala perpage K	454.00 KB 614.82 KB	21 21	0			21				
Dandin Mandalah Cahamatag Waknak Waknak mala ser paga K	404 00 100 6 44 52 46 6 53 46	21 21 8	0 0 8			21 R				
Landon Phenetation Contenents Potential piloation Mitched with prepare K	44(0)00 64(0)00 600(0)	21 21 2 Sythe_Jilowst 5	0 0 0 8 Jourse Journeton 1	Viocked, application 8		21 8 00000000000000000000000000000000000	unt, fransactions			
Sando- Mandan (Sandanag Rabadan Kahada Anda ya ya <u>v</u> <u>v</u> <u>v</u> <u>v</u> Anda ya ya <u>v</u> <u>v</u> <u>v</u>	64(202) 61/220 633/6 433/6 433/6 433/6	21 22 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0		21 8 000 100 100 100	53655	*		
sado Manatari (chanang Manatari Alakina Alakin	44(0)00 64(0)00 600(0)	21 21 2 Sythe_Jilowst 5	0 0 0 8 Jourse Journeton 1	0		21 8 00000000000000000000000000000000000	45	•		
landin Restant (Schennung Restant) Ander Aufer (Schennung Ander Schennung) State Careves Schennung Restant Re	esta to to esta to to esta to esta to esta to sent topine	21 21 8 8 9406, Slowed 8 36, 10 TH 10, 10 TH 10, 10 TH	2 2 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	0		21 8 50 50 50 50 50 50 50 50 50 50 50 50 50	52655 45 24	*:		
sado Mandal Colomany Mandal Salari Mandal S	esta to to 6 A Kato Sta 6 E Sta 7 E St	27 27 6 5 5 5 5 5 5 5 5 5 7 5 6 6 7 7 7 7 7	e 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	0		21 8 60 10 10 42	53655 45 24 8	8		
zestő meterelete / cohoreneg meterelet del ner ange (K) del ner ange (K) Asate Les yest (K) Ander Del ner del ner generalistic meterelete (K) Ander Del ner del ner generalistic meterelete (K) Ander	440.0000 440.000 4.0040 4.0040 4.0040 Mark Saturbury Mark Saturbury Mark	21 21 6 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	2 2 3 4045,0005019 1 10205 000 000 000 000 000 000 000 000 000	0 0 0		21 8 00 10 55 42 45	53555 45 24 8 8	•		
saado mantari (clamang mantari (clamang altalitar Malaha) da lar page status concept 1 concept 1	esta to to esta to to esta to esta to esta to base bas	21 22 23 24 24 24 24 24 24 24 24 24 24 24 24 24	2 2 3 40xet junction 1 0030 400 40 40 40	0 0 10 0		21 8 00 10 10 10 10 10 10 10 10 10 10 10 10	53555 45 24 5 5 5	•		
Sando Televanov Televanov Antaria antaria Anta	44204 14209 4009 4009 4009 4009 4009 400 400 400	20 20 30 6 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	0 0 0 0 0 0 0 0 0 0 0 0 0		21 8 6 6 7 7 7 7 7 7	52055 40 24 5 5 5 5 9	•		
Stade Mandari Colomati Rabard Mahard	482.06 492.06 552.05 5555.05 5555.05 555.05 555.05 555.05 555.05 555.05 555.05 555.055	27 27 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	8 8 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	0 0 0 0 0 8 0		21 8 00 10 10 10 10 10 10 10 10 10 10 10 10	52555 45 24 8 5 5 9			

die 1

Anti-Malware

	re - SplunkforCis	scolro	+							
unk's alualu							Logged	in as admin App -	Manager Alerts	Jobs Logo
nk for Cisco Ironport										Help Abo
Malware Actions		_	_						_	
Days	•									
p Malware Categori	es Detected					Top Malware Threats Detected				
Adware	i i			- i - i	1	Blackhole DNS URLs	ĺ.		ľ ľ	-
						Drive By Website URLs			1	-
						· · · · · · · · · · · · · · · · · · ·				
Phishing						Ultimate Cleaner				
						EICAR-AV-Test	12			
						EICAH-AV-Test				
	10 20	30	40	50 60	70		40	80 120) 160	200
		Trans	actions					Transactio	ons	
lalware Categories										
	-1									
esults per page 10 _	<u>.</u>									
esults per page 10 _		monitore	d_transaction			detected_transactions #	block	ked_transactions #		
esults per page 10 _		monitore	d_transaction			detected_transactions #	block	ked_transactions #		
icsults per page 10 _ lick fields x_wbrs_threat_type 1		1000	d_transaction					ked_transactions #		
Adware		69	d_transaction			69	0	ked_transactions {		
Results per page 10 Pick fields x_wbrs_threat_type 1 Adware		69	d_transaction			69	0	ked_transactions ‡		
lesults per page 10 lick fields x_wbrs_threat_type 1 Adware Phishing		69	d_transaction			69	0	ked_transactions #	_	
lesults per page 10_ lick fields x_wbrs_threat_type t Adware Phishing	2 2	69	d_transaction			69	0	ked_transactions {		
esuits per page 10_ inck fields x_wbrs_threat_type it Adware Phishing Islaware Threats esuits per page 10_	2 2	69	id_transaction		_	69	0	ked_transactions (
esults per page 10 ick fields x_whrs_threat_type 1 Advan Phishing lalware Threats esults per page 10 ick fields		69 20				69 20	0		tions #	
esuits per page 10		69 20 			ransactions #	69	0	detected_transac	tions 8	
tesults per page 10		69 20 		monitored_s	ransactions 8	69 20 blockd_transactions t	0	detected_transac	tions \$	

Client Malware Risk

	2		circine man	10 million 10 million	c opran	RIDICISC	olronportWSA	- Spiulik	7.2.1 (90	104)		_	_	
Clien	t Malwar	e Risk - Sp	lunkforCi	+										
nk> ala	the secure									Logged in	es estrein Ac	co - Mana	ger Alerk	Jobe Log
		rches .												🔹 Help Ab
talware Hisk	Actions -													
yt														
Proxy - Top C	Clients by Malware	Risk.					L4 Traffic Monitor - Top Cli	ents by Malware Risk						
		craete												
QU	est_user2						192.168.2	40.88						
-	mkt user1		100				182:168:2	48.82					-	
conti	ract user5						182-168-3	40.74		1				
conti	ract user1		-				182 188 2	40.83 48.93						
final	mkt usera mkt usera ract usera ract usera ract usera hr usera mkt usera						192 168 2	40.76						
gu	nce user4 est user6		40 0		400	400	195:188:5	48:44		400	500		-	
		20	40 60	0 80	100	120		100	200 300	400	500	600	700	800
			Trans	sactions						Transac	tions			
	ta by Malware Risk		664 (52) (64)			_								
a per paga 🗍 er jid k	IC_+	bytes_blocked i			ed_tesporaes I	blocked_request				locked_transact	tions 1		_transactio	a 1
a per paga [] er_id 1 er_uaer2	10 user_domain # AD	bytes_blocked (100	D	nd_maporaes I	B	0	109		Ŕ	tions 8	108	transactio	na 8
a per paga [] er_jd 1 es_coor2 t_coor1	tt_+ user_domain # AD AD	bytes_blocked (Dis Dis	100 75	0	ed_responses i	0	0	109 79			tiona a	928 79	_transactio	na 8
a per page [] e, jd 1 et juser2 t juser1 t juser3	tr_+ user_domain # AD AD AD	bytes_blocked (Db Db Db	100 75 48	0 0	id_maporaes I	0 0	0 0 11	105 79 43			flora 8	108 79 48	transactio	na 1
s per paga [] er jid 8 est user2 User1 User3 fract_user3	K view domain # AD AD AD AD	bytes_blocked (Dis Dis Dis Dis Dis	100 73 48 45	0 0 0	sd_tesporaes I	0 0 0 0 0	0 0 11 0	109 79 45 45			tions #	109 79 48 45	_transactio	na †
s per page [] rc.jd i rst_user2 t_user3 fract_user3 fract_user3 rst_user3	tr_+ user_domain # AD AD AD	bytes_blocked (DS DS DS DS DS DS	100 75 48	0 0	sd_tesporaes I	0 0	0 0 11	105 79 43			Bors I	108 79 48	tanastio	na 8
r, jd i r, jd i useri useri useri useri useri useri useri useri useri	K view domain # AC AC AC AC AC	bytes_blocked (Dis Dis Dis Dis Dis	108 75 48 45 42	0 0 0 0	Nd_Tesporses	0 0 0 0	0 0 11 0 0	109 79 48 45 42			tions I	109 79 48 45 42	_ transactio	na 8
a per page [] r_id 8 ret_user2 t_user1 t_user3 rtsct_user3 rtsct_user3 rtsct_user3 rtsct_user1 user2 user2	K user_domain # AD AD AD AD AD AD AD	bytes_blocked (DS DS DS DS DS DS DS DS DS	100 79 48 45 42 42 41	8 9 9 9 9	kd_responses I	0 0 0 0 0	D 0 11 0 0 11	109 79 48 45 45 42 41			tions 1	109 79 48 45 42 41	_transctio	na 8
a per page [rg (d 1 rd, use? g, use? g, use? rtract, use? rtract, use? rtract, use? use? use? rtract, use? rtract, u	10 x x x x x x x x x x x x x x x x x x x	bytes_blocked of Dis Dis Dis Dis Dis Dis Dis Dis Dis Dis	100 75 45 45 42 41 40	0 0 0 0 0 0	id_responses I	0 0 0 0 0 0	0 0 0 0 0 0 11 0	109 79 48 45 42 41 40		0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	lions I	109 79 48 45 42 41 40		ne 8
s per page [] signals () signals () sig	10 + user_domain II A0 A0 A0 A0 A0 A0 A0 A0 A0 A0	bytes_blocked (Ds Ds Ds Ds Ds Ds Ds Ds Ds Ds Ds Ds	100 73 48 45 45 42 41 40 40	0 0 0 0 0 0 0 0	nd_responses I		0 0 0 0 0 11 0 0	109 79 48 45 42 41 40 40			lians I	108 75 48 45 42 41 40 40		na 8
s per page [] signals () signals () sig	11. + user_domain I A3 A3 A3 A3 A3 A3 A3 A3 A3 A3	bytes_blocked (Dis Dis Dis Dis Dis Dis Dis Dis Dis Dis	100 73 48 45 42 41 40 40 38	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nd_responses 1		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39			tions I	108 79 48 45 42 41 40 40 39	t_transactio	na 8
s per page [] signals () signals () sig	11. + user_domain I A3 A3 A3 A3 A3 A3 A3 A3 A3 A3	bytes_blocked (Dis Dis Dis Dis Dis Dis Dis Dis Dis Dis	100 73 48 45 42 41 40 40 38	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nd_responses I		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39			tions I	108 79 48 45 42 41 40 40 39	t_transactio	na ð
a per page m, id a rel use? use? use? use? rect use? rect use?	11. + user_domain I A3 A3 A3 A3 A3 A3 A3 A3 A3 A3	bytes_blocked (DB DB DB DB DB DB DB DB DB DB DB DB DB	100 73 48 45 42 41 40 40 38	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ed_responses i		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39			tions I	108 79 48 45 42 41 40 40 39	transactio	ne 8
a perpage [ar, ja t tel, use? L, use? L, use? L, use? tel,	IC user_donaln. 8 AD AD	bytes_blocked (DB DB DB DB DB DB DB DB DB DB DB DB DB	100 73 48 45 42 41 40 40 38	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	et_responses I		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39			tions #	108 79 48 45 42 41 40 40 39		ne 8
a per page [rr_j d 1 rr_j d 2 rr_j d 2 rr	tc - user_stands 4 AD -	bytes_blocked (DB DB DB DB DB DB DB DB DB DB DB DB DB	100 75 45 45 45 40 40 50 50	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39				108 79 48 45 42 41 40 40 39	, transaction	na ð
a per page [r_jd i r_jd i (_useri (_useri (_useri rrsc(_useri	tc - user_stands 4 AD -	Bytes_blocked (Ds Ds Ds Ds Ds Ds Ds Ds Ds Ds Ds Ds Ds	100 75 45 45 45 40 40 50 50	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39				108 79 48 45 42 41 40 40 39	<u>panastis</u>	na 3
a per page [r_jd 1 (_user1 (_user3 (_user3 trac1_user3 rtrac1_user3 rtrac1_user3 rtrac1_user4 user4 rtrac1_user3 rtr	It • user_domain # AD AD AD	Nytes_blocked (100 75 45 45 45 40 40 50 50	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	5485		0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39	Total, Malware			108 79 48 45 42 41 40 40 39	, Panastie	ne 8
a per page [er, juit 1 er, juart 1, uaert 1, ua	It - AD - <tr td=""></tr>	bytes_blocked (100 75 45 45 45 40 40 50 50	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	5×83 001		0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39	Total, Malware 723			108 79 48 45 42 41 40 40 39	, transectio	58 8
a per page [] r, jd i at_user2 Laser1 Laser1 tuser2 rect_user3 rect_user3 rect_user4 rect_us	tc - user_stands 4 AD - AD - <	bytes_blocker (100 75 45 45 45 40 40 50 50	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	5049 500 500		0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39	Tota (Meleare 72) 559			108 79 48 45 42 41 40 40 39	, transactio	NK 9
a per page [r, jd i ist_user5 i_user6 i_user6 ist	It - AD - <tr td=""></tr>	Nytes_blocked (100 75 45 45 45 40 40 50 50	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	5485 001 573 401 332 225		0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39	Total Melean 723 859 830 400 230			108 79 48 45 42 41 40 40 39		na ()
a per page [[] (r, j, k, j, k,	tc	bytes, blocked (100 75 45 45 45 40 40 50 50	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	5485 001 379 459 332 225 275		0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39	Total_Maleant 723 859 850 920 233			108 79 48 45 42 41 40 40 39	Panaactio	na J
a per page [r, jd i el, user? Laert Laert el, user? el, use	tc	bytes_blocker (100 75 45 45 45 40 40 50 50	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	5485 001 573 401 332 225		0 0 0 0 0 0 0 0 0 0	109 79 48 45 42 41 40 40 40 39	Total Melean 723 859 830 400 230			108 79 48 45 42 41 40 40 39	varaectie	na 9

Web Reputation Filters





L4 Traffic Monitor

The L4 Traffic Monitor report is a aggregate and drilldown report in one. Drilldowns from this page will refresh this page with the targeted drilldown information loaded. This report has tips for more powerful uses (i.e. correlating L4TM data using accesslog data using this report).

<form>Arring INote that is the control of the contro</form>	L4 Traffic Monitor		or - SplunkforCiscolronportW	- Spiulik 4.2.1 (
		- SplunkforCisc +			
	nk5 altalla sesere				Lagged in as admin App - Manager Aleria Joba
					· Heg (
	Clear Form				
	•				
	Search Host				
	+				
	o rocus results: ech for a Host, Malwars Port, or Malware Sit x or the Top Malware Hosts Detected bar or	In the search boxes (above) to focus this reports results (with Owlow) to search accessions for a user ID associated.	(wildcards may also be used) with the boat IP address		
	k on any now in a results table to apply the ass	incluted Nost, Malware Port, or Malware Site as a litter fo	r this reports results		
Weblewick	laiware Hosts Detected	Тор	Malware Porta Detected	Top Malware Sites	Defected
Weblewick			0.0		
Weblewick	192 188 240 41		443		www148.mysearch.com
1922.163.240.34 200 400 600 800 2000 3,000 5,000 7,000 Connections	192.168.240.82		-25	w	ebig005.webigonline.com
1922.163.240.34 200 400 600 800 2000 3,000 5,000 7,000 Connections	192.168.240.83		7777		neededware.com
1922.163.240.34 200 400 600 800 2000 3,000 5,000 7,000 Connections	192 188 248 98			SI	IV ey 2.securestudies.com www.adacuity.com
No. N	192 168 240 34	2 10220 202 10220	20000		onesteosearch.net
	20	0 400 600 800	3,000 5,000	7,000	700
		10 10 11 11 11 10 20 10 10 10 10 10			1. 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.
<form>Arring INote that is the control of the contro</form>		Connections	Connections		Conons
<form>Norman in the second with the sec</form>					
<form>ArriteNore, Concent of the encoded of th</form>	are Hosta Detected		Click on IP to report o	n associated users	
Marka and a part of the M	ta per page tC - 1				
Name Name <th< td=""><td></td><td>tions Blocked I Malware Connections Monitored I</td><td></td><td></td><td></td></th<>		tions Blocked I Malware Connections Monitored I			
M3244MMMMMM3247MMMMMMMM3248MMMMMMMM3241MMMMMMMM3241MMMMMMMM3241MMMMMMMM3241MMMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMMM3241MMMMMM					
minimummin<		575			
100 000 010200010100 000 12021101010100 000 1202020201010100 000 120202020101010100 000 120202020101010100 000 120202020101010100 000 120202020101010100 000 120202020101010100 000 120202010101010100 000 120202020101010100 000 120202020101010100 000 120202020202020100 000 120202020202020100 000 1202020202020100 000 1202020202020100 000 1202020202020100 000 1202020202020100 000 1202020202020100 000 1202020202020100 000 1202020202020100 000 1202020202020 <td< td=""><td></td><td></td><td></td><td></td><td></td></td<>					
148.2431 19 271 30 148.2431 12 272 37 148.2431 12 273 37 148.2431 12 273 37 148.2431 12 273 37 149.2431 12 273 37 Server Problem International problem		1.92	101 (101 SMC/171)		
101 40 1 20					
193 0 23 23 23 27 100 2017 193 0 23 24 29 100 2013 100 2013 Image: Second Secon					
NNB 2013 2 21 21 21 21 NNB 2013 2 21 10 10 10 NNB 2014 2 10 10 10 10 None Conscione Discist 3 Name Conscione Discist 3 Name Conscione Discist 3 10 10 None Conscione Discist 3 Name Conscione Discist 3 Name Conscione Discist 3 10 10 So 44 10 Name Conscione Discist 3 10 10 10 So 44 10 Name Conscione Discist 3 10					
Server Port Detected Server Consistent, Detected Serve	2 168.240.75 52				
Service Service service <	a sea alla set	229	257 112.308.2481.31		
Number of the second	2 158 240 31 23				
Number of the second	2 158,240,31 23	*******			
Number of the second	2 188 240 31 23)4+>		
NameNameNameNameNameIndextor	2.188.240.31 23				
101 172 172 172 132 172 172 172 13 19 172 172 140 19 172 172 140 12 12 12 120 2 2 12 12 177 2 2 2 12 12 177 2 2 2 12 12 170 2 2 2 12 12 171 2 12 2 12 12 172 2 12 12 12 12 172 2 12 12 12 12 172 2 12 12 12 12 172 1 12 12 12 12 173 1 12 12 12 12 174 1 12 12 12 12 174	2 108 240 31 23				
DMaMaMaMaD2266772224022370123701222011220112201122011110111101111011110111101111011110111101111011110111101111011110111101111011110111011101110111011101110111011101110111011101) 4 +		
interm join join join 200 2 201 2 201 2 201 2 201 2 201 2 201 2 201 2 201 3 201	ware Ports Detected de per page IC.+ alleven, Ports, Descad 9		Malware, Connectione, Nontornal I		ware, Connectione, Delected 1
M22 9 1 6 777 2 2 4 777 2 2 3 80 1 2 3 80 1 3 3 80 1 3 3 80 1 3 3 80 1 3 3 80 1 3 3 80 1 3 3 80 1 3 3 80 1 1 1 80 1 1 1 80 1 1 1 80 1 1 1 80 1 1 1 80 1 1 1 80 1 1 1 80 1 1 1 80 1 1 1 80 1 1 1	ware Ports Detected dis propage 15.4. Ports_Detected 9 0	1212	Nation_Correction_Netword 1 2723	1943	ven_Convetion_Detroted 1
Y7 2 2 1 2 2 3 500 3 10 10 11 10 12 1 12 1 12 1 13 1 14 1 15 1 15 1 16 1 17 1 18 1 19 1 10 1	wire Ports Detected ds ser page <u>K_+</u> wiren_Ports_Detected #	992 54	Malwary_Connections_Ventored I 9723 711	6945 765	win_Convetions_Detected 1
SODE 1 2 15 1 1 2 16 1 1 2 start 1 1 start 1 <td>www.Ports Outocted ans per page 10 Network, Ports, Johnsond 9 </td> <td>1212 54 20</td> <td>Walkaw, Connection, Violatoret 8 973 70 28</td> <td>6945 785 86</td> <td>way, Convectory, Delected 1</td>	www.Ports Outocted ans per page 10 Network, Ports, Johnsond 9 	1212 54 20	Walkaw, Connection, Violatoret 8 973 70 28	6945 785 86	way, Convectory, Delected 1
NY I I 2 Normalization I International Status International Status Normalization Normalizational Status Normalizational Status International Status Normalizational Normalizational Status Normalizational Status International Status Normalizational Advancementational Status Normalizational Status International Status Normalizational Advancementational Status International Status International Status Normalizational International Status International Status International Status	wire Ports Detected de ser page <u>K_+</u> 13 5220 777	94 30 3	Nations_Corrections_Nectional 1 0703 711 30 3	1045 785 88	wars_Connections_Detected
Stars Betcket Stars Betcket Interpart [1] Mawa, Sonstein, Bucket I Make, Sonstein, Bucket I Make, Sonstein, Bucket I March Stars, Bucket I Make, Sonstein, Bucket I Make, Sonstein, Bucket I Make, Sonstein, Bucket I March Stars, Bucket I Make, Sonstein, Bucket I Make, Sonstein, Bucket I Make, Sonstein, Bucket I March Stars, Bucket I Make, Sonstein, Bucket I Make, Sonstein, S	www.Ports.Detected Its per page K Microw_Ports_Detected # 13 14 15 15 15 15 15 15 15 15 15 15	1912 64 20 3 2 5	Markurn, Connectorn, Mantanned I 1773 711 32 3 3 2 2 2	1945 705 60 6 4 3	ware, Connectione, Defected 1
Annu Construction Maximum Cons	wire Ports Detected wire ports Detected this propage K • 1 0 40 5 5 5 5 5 5 5 5 5 5 5 5 5	1212 54 30 3 2 1 1	Nations, Connections, Machined 1 8723 78 39 3 2 2 2 3 1	1943 705 00 0 4 2 2	way, Convertione, Deladed 1
Annu Construction Maximum Cons	wire Ports Detected wire ports Detected this propage K • 1 0 40 5 5 5 5 5 5 5 5 5 5 5 5 5	1212 54 30 3 2 1 1	Nations, Connections, Machined 1 8723 78 39 3 2 2 2 3 1	1943 705 00 0 4 2 2	win_Convetions_Detected 1
Jackson Jackson <t< td=""><td>www.Ports Detected to the per page K.+ therees, Ports, Detected 9 5 5 5 5 5 5 5 5</td><td>1212 54 30 3 2 1 1</td><td>Nations, Connections, Machined 1 8723 78 39 3 2 2 2 3 1</td><td>1943 705 00 0 4 2 2</td><td>wars_Connections_Delected 1</td></t<>	www.Ports Detected to the per page K.+ therees, Ports, Detected 9 5 5 5 5 5 5 5 5	1212 54 30 3 2 1 1	Nations, Connections, Machined 1 8723 78 39 3 2 2 2 3 1	1943 705 00 0 4 2 2	wars_Connections_Delected 1
Jackson Jackson <t< td=""><td>wire Ports Detected wire ports Detected this propage K • 1 0 40 5 5 5 5 5 5 5 5 5 5 5 5 5</td><td>1212 54 30 3 2 1 1</td><td>Nations, Connections, Machined 1 8723 78 39 3 2 2 2 3 1</td><td>1943 705 00 0 4 2 2</td><td>wan, Connections, Defector I</td></t<>	wire Ports Detected wire ports Detected this propage K • 1 0 40 5 5 5 5 5 5 5 5 5 5 5 5 5	1212 54 30 3 2 1 1	Nations, Connections, Machined 1 8723 78 39 3 2 2 2 3 1	1943 705 00 0 4 2 2	wan, Connections, Defector I
tadjifum 20 20 20 ad garidocaram 5 27 27 adqu00 cm 27 20 20 adqu00 cm 20 20 20 adqu00 cm 2 20 20 adqu00 cm 2 20 20 adqu00 cm 2 20 20 adqu00 cm 20 20 20	were Parts Detected Interest Parts De De De De De De De De De De	1212 54 30 3 2 1 1	Nations, Connections, Machined 1 8723 78 39 3 2 2 2 3 1	1943 705 00 0 4 2 2	war_Connettors_Datected
adgrinheencamin 272 277 app000 270 260 app0000 270 260 app00000 270 260 app00000 270 260 app000000 270 260 app00000000000000000000000000000000000	www.Ports Detected fits are page 10	00 94 33 3 2 1 1 1 1 1 1	Nations, Corrections, Ventioner I 973 713 30 3 2 3 3 3 4 3 4 3	1943 785 6 4 3 2 2 2	
app001sm 20 207 440 app001sm 20 20 20 applo1se 20 20 20 applo1se 20 20 20 applo1se 20 17 20 applo1se 20 15 17 applo1se 12 12 12	errs Parts Detected It me page K www.parts_Detected I 	UD 64 22 2 1 1 1 1 1 1 1 1 2 1 1 2 1 1 1 1 2 1	Manue, Correction, Notional 1 073 70 20 2 2 2 3 3 3 3 3 4 3 5 5 5 5 5 5 5 5 5 5 5 5 5	1043 705 60 4 2 2 2 2 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	
Josephane J25 J26 Analyhourn 2 217 218 Elakairankourn 2 717 718 Analyhourn 2 717 719 Analyhourn 2 717 719 Analyhourn 1 719 719 Analyhourn 2 719 719 Analyhourn 1 710 710	www.Ports Detected this per page (t_) www.Ports_Detected * 13 13 13 13 14 15 15 15 15 15 15 15 15 15 15	UIQ 5 64 90 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Maleur, Correction, Vicitaria I 973 791 30 3 3 2 3 3 3 3 3 3 4 3 3 3 3 3 3 3 3 3 3	004 705 60 8 3 2 2 2 2 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	
2 20 20 20 Else Arekeans 2 77 77 Schelagnet List 2 75 77 Schelagnet List 10 10 10	www.Forts.Detected als tor page K - bitmans.Prot.Solution 8 0 12 13 14 15 15 15 15 15 15 15 15 15 15	US2 64 53 2 3 3 1 1 1 1 Kennen, Connections, Blacked 1 8 3 5 5	Maleur, Correction, Markand I 572 78 39 3 2 2 3 3 3 4 3 5 4 5 5 6 7 7 1 3 5 5 7 7 1 3 5 7 7 1 3 5 7 7 7 7 7 7 7 7 7 7 7 7 7	8943 785 60 4 3 2 2 2 2 7 5 5 5 6 6 6 6 6 6 6 2 77 27	
Backbackson 2 17 17 Schappedall 175 17 17 objassif 15 17 17	ware Forth Detected the serves to the servest binary State of the servest to the	UD 64 2 2 1 1 1 1 1 1 1 1 1 1 1 2 1 2 3 3 3 3 3 3 3 3 3 5 5 5 5 5 5 5 5 5 5 5 5 5	Malware, Connectione, Manternet 8 973 791 28 2 2 2 2 3 3 2 2 4 4 4 5 4 5 4 5 4 5 4 5 4 5 4 7 2 3 2 2 2 2 3 3 2 2 3 3 3 3 3 3 3 3 3	1043 705 00 4 2 2 2 2 7 7 5 5 5 5 5 5 5 5 5 5 5 5 5 5	
1 114 112	www.Ports.Detected who per page 10 0 10	UC2	Malware, Corrections, Notional 1 0773 70 30 3 2 3 3 2 3 3 4 4 4 4 6 6 6 7 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	894 705 6 6 7 2 2 2 7 7 7 8 6 8 6 20 7 7 7 20 20 227 20 228	
	www.Ports Detected white program to an	UC2	Maleon, Corrections, Manternet 8 973 719 30 3 3 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	8943 705 60 8 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
	ware Forts Ordected arb per page (C+) Second 9 Second	UQ 54 53 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1	Mahan, Correction, Notional 1	894 705 6 6 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	
	www.Ports.Detected who pro page (too) thereary.Ports_Detected # 0 43 5 5 5 5 5 5 5 5 5 5 5 5 5	U(2) 64 20 3 2 1 1 1 1 1 1 1 1 1 1 1 1 1	Maken, Correction, National 1 973 78 28 2 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	894 705 90 4 3 2 2 2 3 7 2 4 4 4 4 5 4 6 4 5 2 7 7 2 0 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 27 20 27 20 27 27 27 20 27 27 27 27 27 27 27 27 27 27 27 27 27	
	ere Ports Ordented and pre page (*) bitevers, Ports, Ordented # 5 5 5 5 5 5 5 5 5 5 5 5 5	U(2) 64 20 3 2 1 1 1 1 1 1 1 1 1 1 1 1 1	Maken, Correction, National 1 973 78 28 2 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	894 705 90 4 3 2 2 2 3 7 2 4 4 4 4 5 4 6 4 5 2 7 7 2 0 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 20 27 27 20 27 20 27 27 27 20 27 27 27 27 27 27 27 27 27 27 27 27 27	



Reports by Drilldown

Below is a list of the drilldown reports available. They have detailed information compared to the aggregate parent reports from which they came. In addition to accessing them by clicking into them from parent reports – they may also be accessed via the menu system and manual searches may be done for individual components...

Malware Category Drilldown Malware Threat Drilldown Application Drilldown Application Type Drilldown Domain Drilldown URL Category Drilldown User Drilldown

Reports by Location

These reports are available via the menu and are similar to their parent reports PLUS they contain information as broken down by location of user...

Overview by Location

URL Categories by Location

Anti-Malware by Location

Web Reputation Filters by Location

Application Visibility by Location

Users by Location

Websites by Location

Web Tracking (form based search)

Simple

O O Web Tracking - SplunkforCiscolro +		Web Tracki	ng – SplunkforCisc	olronpor	tWSA – Splunk 4.2.1	(98164)	_	_	_	0
Search finalized.	_		_	_	_	_	_			
splunk> 'llull' security								Logged in as adn	nin App - Manager A	Nerts Jobs Logo
Splunk for Cisco Ironport WSA 🗸 Searches 🗸										🕜 Help Abc
Actions -										
Week -										
Oliver From									refreshed: to	oday at 11:12:55 AM
Clear Form	Result	s per page 10 🗾								Export
Simple Advanced										
Search	Pick fie	lds								
User ID or Client IP hr. user1	« pre	/ 🚺 2 3 4 next	»							
User ID or Client IP hr_user1	« pre	/ 1 2 3 4 next _time ≑	» Website ≎	host ‡	Disposition +	Bandwidth ≎	user_id ‡	dvc_ip ≎	x_webcat_code_full ≎	x_wbrs_score ≎
User ID or Client IP hr_user1	« pre [,]	-	Website ÷		Disposition ÷	Bandwidth + 26.97 GB		dvc_ip +		x_wbrs_score ≎ 4.9
Website •	« pre [,] 1 2	_time ÷	Website +	prepeat	-		hr_user1		Education	
	1	_time + 6/20/11 12:15:28.029 PM	Website indiana.edu digitalcorvettes.com	prepeat prepeat	DEFAULT - CASE	26.97 GB	hr_user1	192.168.245.101	Education Transportation	4.9
Website •	1 2	_time \$ 6/20/11 12:15:28.029 PM 6/20/11 12:15:28.028 PM	Website ÷ indiana.edu digitalcorvettes.com taylor.edu	prepeat prepeat prepeat	DEFAULT - CASE DEFAULT - CASE	26.97 GB 56.78 GB	hr_user1 hr_user1 hr_user1	192.168.245.101 192.168.245.101	Education Transportation Education	4.9 0.0
Website •	1 2 3	_time \$ 6/20/11 12:15:28.029 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.028 PM	Website ÷ indiana.edu digitalcorvettes.com taylor.edu ued.net	prepeat prepeat prepeat prepeat	DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE	26.97 GB 56.78 GB 31.11 GB	hr_user1 hr_user1 hr_user1	192.168.245.101 192.168.245.101 192.168.245.101	Education Transportation Education Shopping	4.9 0.0 0.0
Website •	1 2 3 4	_time \$ 6/20/11 12:15:28.029 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.028 PM	Website indiana.edu digitalcorvettes.com taylor.edu ued.net dallasnews.com	prepeat prepeat prepeat prepeat prepeat	DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE	26.97 GB 56.78 GB 31.11 GB 40.44 GB	hr_user1 hr_user1 hr_user1 hr_user1	192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101	Education Transportation Education Shopping News	4.9 0.0 0.0 0.0
Website *	1 2 3 4 5	_time = 6/20/11 12:15:28.029 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.027 PM	Website indiana.edu digitalcorvettes.com taylor.edu ued.net dallasnews.com islandrental.com	prepeat prepeat prepeat prepeat prepeat	DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE	26.97 GB 56.78 GB 31.11 GB 40.44 GB 75.85 GB	hr_user1 hr_user1 hr_user1 hr_user1 hr_user1 hr_user1 hr_user1	192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101	Education Transportation Education Shopping News	4.9 0.0 0.0 0.0 5.3
Website •	1 2 3 4 5	_time ≎ 6/20/11 12:15:28.029 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.027 PM 6/20/11 12:15:28.027 PM	Website indiana.edu digitalcorvettes.com taylor.edu ued.net dallasnews.com islandrental.com 456bereastreet.com	prepeat prepeat prepeat prepeat prepeat prepeat	DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE	26.97 GB 56.78 GB 31.11 GB 40.44 GB 75.85 GB 38.97 GB 8.20 GB	hr_user1 hr_user1 hr_user1 hr_user1 hr_user1 hr_user1 hr_user1 hr_user1	192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101	Education Transportation Education Shopping News Travel	4.9 0.0 0.0 0.0 5.3 0.0
Website •	1 2 3 4 5 6 7	_time ÷ 6/20/11 12:15:28.029 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.028 PM 6/20/11 12:15:28.027 PM 6/20/11 12:15:28.027 PM 6/20/11 12:15:28.026 PM	Website ÷ indiana.edu digitalcorvettes.com taylor.edu ued.net dallasnews.com islandrental.com 456bereastreet.com dol.gov	prepeat prepeat prepeat prepeat prepeat prepeat prepeat	DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE DEFAULT - CASE	26.97 GB 56.78 GB 31.11 GB 40.44 GB 75.85 GB 38.97 GB 8.20 GB	hr_user1 hr_user1 hr_user1 hr_user1 hr_user1 hr_user1 hr_user1 hr_user1	192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101 192.168.245.101	Education Transportation Education Shopping News Travel Computers and Internet Government and Law	4.9 0.0 0.0 0.0 5.3 0.0 4.7



Advanced

Web Tracking - Splunkfor	rCiscolro	+							
unk's vilivilia securry							Logged in as adm	in App - Manag	er Alerts Jobs I
k for Cisco Ironport WSA + Searches									🕐 Help
ins •									
sk -									
ar Form	2 105	6 complete 1 result							
pie Advanced	Results pe	r page 10 💌						1	Export
Search									
r ID ar Client IP	Pick fields								
		time #	Website ‡ host	Disposition 4	Bandwidth	t user_id t	dvc_ip #	x_webcat_code_fu	ill t x_wbrs_score
site *	1 6	/14/11 12:25:04.353 AM	toolator.com prepe	at BLOCK - WEBCAT	1.05 TB	mfg_user5	192.168.246.105	Filter Avoidance	0.0
saction Type Blocked -									
Category									
ter Avoidance									
lication •									
lication Type *									
ay •									
ware Threat *									
ware Category *									
RS from -10 •									
10 •									
utation Threat *									
r Location Any									
Appliance * [all hosts]									

Sample Usage Scenarios

Finding information

The following usage scenarios illustrate how to use Splunk to find information.

Example 1: Investigating a User

This example demonstrates how a system administrator would investigate a particular user at a company. In this scenario, a manager has gotten a complaint that an employee is visiting inappropriate web sites at work. To investigate this, the system administrator now needs to look at the employee's web usage trends and transaction history. The administrator generates reports about the employee's browsing history.

- Choose Users from the Splunk for Cisco IronPort WSA dropdown menu (click on Splunk for Cisco IronPort WSA at the top left corner of the page to get the drop down menu). The Users page appears.
- 2. In the **Users** table, click on the User ID or Client IP address you want to investigate. The **User Drilldown** page appears for the User ID or Client IP.

If you cannot see the User ID or Client IP address you want to investigate in the Users table, click on any User ID or Client IP to be led to the **User Drilldown** page. Enter in all or part of the User ID or Client IP address in the text box and click **Search**.

3. From the **User Drilldown** page you can determine the URL Categories by Total Transactions, Trend by Total Transaction, URL Categories Matched, Domains Matched, Applications Matched, Malware Threats Detected, and Policies Matched for a particular User ID or Client IP.

These categories allow you to find out if, for example, user "johndoe" was trying to access blocked URLs, which could be viewed in the Transactions Blocked column under the Domains section on the page.

4. If you want to print the data, click on **Actions** next to the User Drilldown title. Select **Print** from the dropdown menu.

The administrator now wants to see the user's transaction history. They follow the steps below:

- 5. Click on Splunk for Cisco IronPort WSA at the top of the page to access the dropdown menu. Select **Web Tracking** at the bottom of the menu.
- 6. In the User/Client IP Address text field type in the user name or IP address, then click Search.

The users transaction history appears. Click on "Pick fields" above the transaction list to change the information displayed for each transaction.

7. Export the data to a CSV file by clicking Export at the top right corner.

Example 2: Tracking a URL

In this scenario, a Sales manager wants to find out what the top five visited web sites are at their company are for the last week. Additionally, the manager wants to know which users are going to those websites.

- On the Splunk application, choose Web Sites from the Splunk for Cisco IronPort WSA dropdown menu (click on Splunk for Cisco IronPort WSA at the top left corner of the page to get the drop down menu). The Web Sites page appears.
- 2. From the Time Range drop-down list, choose Week.
- Scroll down to the **Domains Matched** table to view the top 25 domains that have been visited. Click on a domain you want to investigate. This leads to the **Domain Drilldown** page, which shows the users who have visited that domain in order of frequency.

Example 3: Investigating Top URL Categories Visited

In this scenario, the Human Resources manager wants to know what the top three URL categories her employees are visiting over the 30 days. Additionally, a network manager wants to get this information to monitor bandwidth



usage, to find out what URLs are taking up the most bandwidth on her network. The example below is to show how you can gather data for several people covering several points of interest, while only having to generate one report.

 On the Splunk application, choose URL Categories from the Splunk for Cisco IronPort WSA dropdown menu (click on Splunk for Cisco IronPort WSA at the top left corner of the page to get the drop down menu). The URL Categories page appears.

From the **URL Categories** page, you can see the top 10 URL Categories by Total Transactions graph.

At this point you can export this report to PDF, by clicking **Actions** (next to the URL Categories title at the top of the page) and selecting **Schedule for PDF Delivery**. This file can be sent to the Human Resources manager. But remember, your network manager wants to know the bandwidth usage by each URL.

 Scroll down to the URL Categories Matches table to view the Bytes Allowed column. This shows the bandwidth usage for each URL Category. You can select Schedule for PDF Delivery to send this file to the Network Manager.

For finer granularity, click on a specific URL Category. You will be led to a **URL Category Drilldown** page that shows which users have the most transactions in a category. Scroll down to see the **Web Users** table. The **Bytes Allowed** column shows you which users have used the most bandwidth.

FAQ

Why does the overview report show more events than are in Splunk?

The summary information exists in a separate index. Information in the summary index is a condensed version of the raw data where superfluous data (i.e. data not needed to present reports) has been quelled. This allows reports to load quicker. As this information is stored in a separate index – the raw data may 'roll off' per the settings configured by the Splunk administrator(s) but its aggregated information may still exist in the summary index and therefore be available for reports.

How may I improve performance when I perform ad hoc queries?

Craft your ad hoc searches to be as specific as possible so that they return only information needed. Returning superfluous event data is more costly in terms of searching and retrieving all the rows. Searching for a specific user will be quicker than searching for all users. Searching for a specific user who visited a specific domain will be quicker still

Narrow your time range to an appropriate window. Do not select 90 days when 30 days will meet the reporting need

Why am I missing hosts?

Why do I see extra hosts?

How do I change the label of hosts?

Only Splunk administrators are able to control the hosts you see on the Overview report and Web Tracking report. Contact your Splunk administrator with details of host you would like to add, remove, or rename.

How do I change the dropdown options on the web tracking report?

Only Splunk administrators are able to control the options you see in the dropdown fields in the Web Tracking form. Contact your Splunk administrator with details of changes you would like to make regarding hosts, malware categories, transaction types, and URL categories



Why do I not see trafmon (L4TM) logs?

Why do I only see data for specific departments?

The SplunkforCiscoIronportWSA application may be configured for role-based access. In this configuration users may be restricted to viewing data from specific departments (or groups). If this configuration is enabled L4TM data will only be available to administrators (as L4TM data is not linked to a department or role). Please contact your Splunk administrator for additional details.