Re-writing the CSIRT Playbook



Jeff Bollinger – Infosec Investigator Matt Valites - Infosec Investigator



54 CSIRT members



19 Data Sources

splunk > 1TB Data Indexed / Day



NetFlow: 15.6 Billion flows / day

;; QUESTION SECTION: ;first.org. IN A

2.5 Trillion DNS lookups / Day



Passive DNS Lancope.

dce-cli - CLI for the Device Context Engine





Multiple Data Repositories

Our Mission

Mission:

- Protect Cisco by developing security monitoring architecture and strategy
- Respond to security threats using ad-hoc and prescribed methods of incident detection and response

How did we get here?

Effective CIRTs **must** evolve with changes in the cyber threat landscape to remain relevant.

Over the last 11 years:

- Organic evolution
- Team growth
- Dramatic increase in value and scope of service offering

More information, more problems

My Data is Bigger

Index	Total Count (24 hours)
syslog	2,196,902,891
ad	1,054,349,972
wsa	426,229,009
acns	228,283,446
esa	49,836,291
dhcp	20,734,821
vpn	17,340,902
acs	15,785,442
ids	2,907,842
csa	682,527
edcs	549,044
sinkhole	282,399
dns	168,460
еро	42,775
fireeye	4,797
altiris	349



Query Time vs. Indexed Data

My Data is Bigger

The old way:

- Buy and trust a SIEM to run canned reports
- Wait for updates from the vendor

Scaling Problems

Secretes and reports			ep034_s1	_t00_	inv-m	fe-out	-to-in				
Searches and reports New Showing 1-100 of 483 items 1 2 3 4 5	next »	1_1	rep034_s1	_t01_	inv-m	fe-dc-	to-dmz-dn	s)	Results per page	100 🛊
Search name \$	RSS feed 🗧 Schedu	d time							ons		
1_rep002_s1_t23_hlth-mfe-cips	2013-03	24 07:0 1_1	'ep034_s1	_t01_	inv-m	te-dc-	to-out		v recent Run	Clone Move	Delete
1_rep003_s1_t23_trnd-device-event-count	2013-03	24 07:0							v recent Run	Clone Move	Delete
1_rep007_s1_t23_trnd-top-firing-sigs	2013-03	24 07:0	ep034 s1	t01	inv-m	fe-in-t	o-dc		v recent Run	Clone Move	Delete
1_rep009_s1_t13_trgt-crdc-to-not-out	2013-03	24 21:0							v recent Run	Clone Move	Delete
1_rep009_s1_t13_trgt-crdc-to-out	2013-03	24 21:0	00034 c1	+0.1	inv.m	fo in t	o out		v recent Run	Clone Move	Delete
1_rep009_s1_t13_trgt-not-out-to-crdc	2013-03	24 21:0	epus4_si	_101_	v-m	10-111-L	0-0ut		v recent Run	Clone Move	Delete
1_rep009_s1_t13_trgt-out-to-crdc	2013-03	24 21:0							v recent Run	Clone Move	Delete
1_rep015_s2_t03_mal-infect-bundle	2013-03	24 11:0 1_1	'ep034_s1	_t02_	inv-m	fe-dc-	to-in		v recent Run	Clone Move	Delete
1_rep016_s2_t03_mal-64005-dmz	2013-03	24 11:0							v recent Run	Clone Move	Delete
1_rep017_s2_t03_mal-60001-60111	2013-03	24 11:0 1	ep034 s1	t02	inv-m	fe-dm	z-dns-to-d	С	v recent Run	Clone Move	Delete
1_rep021_s1_t03_mal-60007-temp-kb-query	2013-03	24 11:0						-	v recent Run	Clone Move	Delete
1_rep021_s1_t04_mal-60007	2013-03	24 12:0	op034_e1	+0.2	inv-m	fo_dm	z_dne_to_d	mz_dne	v recent Run	Clone Move	Delete
1_rep021_s1_t09_monthly-60007	2013-04	01 17:0	ep034_31	_102_		ie-uiii	2-0113-10-01	nz-una	v recent Run	Clone Move	Delete
1_rep024_s1_t03_mai-irc-to-external	2013-03	24 11:0		10.4					v recent Run	Clone Move	Delete
1_rep024_s1_t03_mal-irc-to-internal	2013-03	24 11:0	ep034_s2	_t01_	inv-m	te-in-t	o-dmz-dns	i	v recent Run	Clone Move	Delete
1_rep027_s1_t02_inv-64003	2013-03	24 10:0							v recent Run	Clone Move	Delete
1_rep029_s1_t03_mal-64000	2013-03	24 11:0 1	ep034 s2	t01	inv-m	fe-out	-to-dc		v recent Run	Clone Move	Delete
1_rep034_s1_t00_inv-mfe-out-to-in	2013-03	24 08:0	. –						v recent Run	Clone Move	Delete
1_rep034_s1_t01_inv-mfe-dc-to-dmz-dns	2013-03	24 09:0	on034 e2	t02	inv-m	fe-de-	to-de		v recent Run	Clone Move	Delete
1_rep034_s1_t01_inv-mfe-dc-to-out	2013-03	24 09:0	CP004_32	_102_		10-u0-	10-00		v recent Run	Clone Move	Delete
1_rep034_s1_t01_inv-mfe-in-to-dc	2013-03	24 09:00							w recent Run	Clone Move	Delete
1_rep034_s1_t01_inv-mfe-in-to-out	2013-03	24 09:00:0	epu34_s2	_t02_	inv-m	re-am	z-ans-to-in	l le	ew recent Run	Clone Move	Delete
1_rep034_s1_t02_inv-mfe-dc-to-in	2013-03	24 10:00:00 0						Vie	ew recent Run	Clone Move	Delete
1_rep034_s1_t02_inv-mfe-dmz-dns-to-dc	2013-03	24 10:00:00 UTC	<u>0034 c2</u>	t02	inv-m	fe-dm	z-dns-to-o	Ut vie	ew recent Run	Clone Move	Delete
1_rep034_s1_t02_inv-mfe-dmz-dns-to-dmz-dns	2013-03	24 10:00:00 UTC	None	CSOC	search	1	App Permissions	Enabled Vie	ew recent Run	Clone Move	Delete
1_rep034_s2_t01_inv-mfe-in-to-dmz-dns	2013-03	24 09:00:00 UTC	None	CSOC	search	1	App Permissions	Enabled Vie	ew recent Run	Clone Move	Delete
1_rep034_s2_t01_inv-mfe-out-to-dc	2013-03	24 09:00:00 UTC	None	CSOC	search	0	App Permissions	Enabled Vie	ew recent Run	Clone Move	Delete
1_rep034_s2_t02_inv-mfe-dc-to-dc	2013-03	24 10:00.00 UTC	None	CSOC	search	1	App Permissions	Enabled Vie	ew recent Run	Clone Move	Delete
rep034_s2_t02_inv-mfe-dmz-dns-to-in	2013-03	24 10:00:00 UTC	None	CSOC	search	1	App Permissions	Enabled Vie	ew recent Run	Clone Move	Delete
1_rep034_s2_i02_inv-mie-dmz-dms-io-out	2013-03	24 10:00:00 UTC	None	CSOC	search	1	App Permissions	Enabled Vie	ew recent Run	Clone Move	Delete
1_rep034_s2_t02_inv-mfe-in-to-in	2013-03	24 10:00:00 UTC	None	CSOC	search	1	App Permissions	Enabled Vie	ew recent Run	Clone Move	Delete

- SEIM unable to process reports during an analyst's shift
- Reports broken into multiple smaller 'directional based reports'
- based reports'
 Inefficient way to process data
- Led to inefficiency

v 💼 9	-13-11	Aug 27, 2012 3:40 PM		Folder
	DS_Store	Today 10:37 AM	6 KB	Document
t	all_sources.txt	Sep 13, 2011 10:59 AM	1 KB	Plain Text File
	check event	Sep 13, 2011 11:54 AM		Folder
	daily_sources.csv	Sep 13, 2011 3:21 PM	6 KB	commvalues
	a daily_sources.txt	Sep 13, 2011 11:19 AM	284 bytes	Plain Text File
	daily_sources.xlsx	Sep 13, 2011 4:17 PM	57 KB	Microrkbook
1	Daily-virus-track-active.xls	Sep 13, 2011 2:49 PM	216 KB	Microrkbook
t	a dhcp.txt	Sep 13, 2011 4:13 PM	54 bytes	Plain Text File
1	Infection_Tracking.xls	Sep 13, 2011 3:07 PM	143 KB	Microrkbook
1	IPsxis	Dec 7, 2010 10:42 AM	15 KB	Microrkbook
T	irc	Sep 13, 2011 11:49 AM		Folder
	.DS_Store	Sep 13, 2011 11:48 AM	6 KB	Document
	1_rep024_s2_t03_mal-irc-to-external-CheckEvent-1315909826069.csv	Sep 13, 2011 11:23 AM	930 KB	commvalues
	1_rep024_s2_t03_mal-irc-to-external-EventSummary-1315909826069.csv	Sep 13, 2011 6:30 AM	33 KB	commvalues
	hl_results.csv	Sep 13, 2011 11:29 AM	12 KB	commvalues
	🖬 hl.txt	Sep 13, 2011 11:25 AM	722 bytes	Plain Text File
	🖹 irc.zip	Sep 13, 2011 11:48 AM	300 KB	ZIP archive
	🖬 message_decoded.txt	Sep 13, 2011 11:28 AM	589 KB	Plain Text File
	message_decoded.xlsx	Sep 13, 2011 11:36 AM	75 KB	Microrkbook
	🖙 message.txt	Sep 13, 2011 11:26 AM	623 KB	Plain Text File
▼ 🗋	Malware	Sep 13, 2011 10:06 AM		Folder
	DS_Store	Sep 13, 2011 10:06 AM	6 KB	Document
	Malware.zip	Sep 13, 2011 10:04 AM	8.3 MB	ZIP archive
t	a nachi.txt	Sep 13, 2011 10:18 AM	2 KB	Plain Text File
t	notes.txt	Sep 13, 2011 4:19 PM	2 KB	Plain Text File
5	e rep054.txt	Sep 13, 2011 10:19 AM	4 KB	Plain Text File
▼ 🗋	summaries	Sep 13, 2011 11:54 AM		Folder
	DS_Store	Sep 13, 2011 11:53 AM	6 KB	Document
	1_rep015_s2_t03_mal-infect-bundle-EventSummary-1315908367680.csv	Sep 13, 2011 6:06 AM	7 KB	commvalues
	1_rep016_s2_t03_mal-64005-dmz-EventSummary-1315908737428.csv	Sep 13, 2011 6:12 AM	20 KB	commvalues
	1_rep017_s2_t03_mal-60001-60111-EventSummary-1315908565190.csv	Sep 13, 2011 6:09 AM	7 KB	commvalues
	1_rep021_s2_t03_mal-60007-temventSummary-1315909264283.csv	Sep 13, 2011 6:21 AM	3 KB	commvalues
	1_rep024_s2_t03_mal-irc-to-external-EventSummary-1315909826069.csv	Sep 13, 2011 6:30 AM	33 KB	commvalues
	1_rep029_s2_t03_mal-64000-EventSummary-1315909553321.csv	Sep 13, 2011 6:25 AM	6 KB	commvalues
	1_rep054_s2_t03_mal-medium-fidventSummary-1315908893391.csv	Sep 13, 2011 6:14 AM	34 KB	commvalues
	🖬 csa_scan_summary.txt	Sep 13, 2011 11:22 AM	3 KB	Plain Text File
	🝸 summaries.zip	Sep 13, 2011 11:54 AM	15 KB	ZIP archive
▼ [Total Files	Sep 13, 2011 8:58 AM		Folder
	Totalxls	Sep 13, 2011 4:47 AM	817 KB	Microrkbook
	Toto Americans	Sep 13, 2011 4:20 AM	1.1 MB	Microrkbook
	Virus_Total_May_FY011Q1.xls	Sep 13, 2011 4:21 AM	6 MB	Microrkbook
ſ	Total_Alliance_FY11Q1.xls	Sep 8, 2011 7:49 AM	1.3 MB	Microrkbook
t	a vpn.txt	Sep 13, 2011 4:10 PM	218 bytes	Plain Text File
		Sep 5, 2011 9:24 PM	70 KB	Microrkbook
P Q	-13-11 zin	Sep 13 2011 4:25 PM	21 7 MB	7IP archive

Static and inflexible

- Performance
- Expensive
- Limited

 \bullet

ullet

- Compatibility
- Retention

13

My Data is Bigger

The new way:

- Build your own collection infrastructure
- Build your own reports
- Research your own intelligence
- Operationalize and optimize

Dependencies

- Requires good architecture and a plan
- Requires smart people
- Scale and efficacy
- Data management

The New Way

Previously

)						PKI	as source 24 h	ours.csv									\bigcirc
1 🏛	in 🖬 i	a 📈 🗈 I	🖒 🎸 🗈		2 . 2		🕼 🛅 🚮 100	x = 0						Q.+ (50	arch in She	et		
A Hor	ne Layo	ut Tables	Charts	SmartAr	t Form	nulas E	Data Review										^	۰.
	61		Ford			Alg	rment	N/	viber		Format			Cells		The	965	
8 .	🕹 Fil 💌	Calibri (Body)	* 12	• A• A•		= _ ab	кс 🐐 🔜 Wrap Text -	General			Normal		-	. 📷	· III.	Aa .		
Parte	Clear •	BIU		4 · A			4 Merge	- 😇 - %	· % 🛷	Conditiona	Bad	۲	loter	Delet	e Ecomat	Thomas	Aa-	
A	1 1	0.00	fx run							Formatting					e rema			
			D	r	E	C	M I		×	1	M N			P	0		. c	
	hostid	Date1	signature	subSigid	description	attacker	attacker_por attacke	r_locitarget	target_port tar	get_locali pro	tocol trigger_paci	trigge	pack fro	mAttacke	fromTarget	sig_type	tag:host	
13640	86927 mtv5-	ski-nm 03/24/2013	81 60503	ι ο	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	OTHER (top			A	4440444	ApAAAnAC	Aother		
13640	(86927) mtv5-	oki-nm 03/24/2013	3 60501	L 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	OTHER_(tcp			(A)	4440444	ABAAANACI	A other		
13640	(86927) mtvS-	oki nm 03/24/2013	3 (60501	L 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	_OTHER_(top			A	4AAQAAA	ABAAANACI	A other		
13640	(86927) mtv5-p	ski-nm 03/24/2013	31 60503	L 0	Established	1171.68.34.1	5 9465 Pi0	173.37.163.2	1524 DC	OTHER_(top			A	чаасаал	AgAAAwAC	Aother		_1
13640	(86927) mtv5-	ski-nm 03/24/2013	3 (60503	ι ο	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	OTHER_(top			A	4440444	AgAAAMAAC	Aother		_
13640	(86927) mtv5-	oki-nm 03/24/2013	3 60501	ι Ο	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	_OTHER_(top			A	4AAQAAA	AGAAANACI	A other		_
13640	86927) mtv5-j	oki nm 03/24/2013	3 60501	L 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	OTHER_(top			A	4AAQAAA	AgAAAwAC	A other		-1
13640	(86927) mtv5-p	ski-nm 03/24/2013	31 60503	L 0	Established	1171.68.34.1	5 9465 Pi0	173.37.163.2	1524 DC	OTHER_(top			A	чаасаал	AgAAAwAC	A other		_1
0 13640	(86927) mtv5-	ski-nm 03/24/2013	3 (60503	ι ο	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	OTHER_(top			A	4440444	AgAAAMAAC	Aother		_
1 13640	86927) mtv5-	oki-nm 03/24/2013	3 60501	L 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	_OTHER_(top			A	4440444	AGAAAWAC	A other		-1
2 13640	86927) mtv5 (oki nm 03/24/2013	3 60501	L 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	OTHER_(top			A	4AAQAAA	AgAAAwAC	A other		_
3 13640	(86927) mtv5-j	ski-nm 03/24/2013	3 60503	L 0	Established	1171.68.34.1	5 9465 PH0	173.37.163.2	1524 DC	_OTHER_(top			A	чаасаал	AgAAAwAC	Aother		_
4 13640	186927) mtx5-	ski-nm 03/24/2013	3 60503	ι 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	OTHER_(top			10	SOMEAN	ADAMANACI	Aother		-1
5 13640	86927) mtv5-	oki-nm 03/24/2013	3 60501	L 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	_OTHER_(top			10	SOAAEAA	AGAAAWAC	A other		-1
6 13640	(86927) mtv5-	oki nm 03/24/2013	3 60501	1 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.1	1524 DC	_OTHER_(tcp			10	SOAAEAA	ABAAANACI	Aother		-1
7 13640	(86927) mtv5-j	ski-nm 03/24/2013	3 60503	L 0	Established	1171.68.34.1	5 9465 PH0	173.37.163.2	1524 DC	_OTHER_(top			10	SOAAEAA	AgaaawaCi	Aother		_
8 13640	186927) mtx5-	ski-nm 03/24/2013	3 60503	ι 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	OTHER_(top			10	SOMEAN	ADAMANACI	Aother		_
9 13640	(86927) mtv5-	oki-nm 03/24/2013	3 60501	L 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	_OTHER_(tcp			10	SOAAEAA	AGAAANACI	Aother		-1
0 13640	86927) mtv5 (oki nm 03/24/2013	3 60505	L 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.1	1524 DC	_OTHER_(tcp			10	SOAAEAA	ABAAANAC	A other		-1
1 13640	186927) mtv5-j	skinm 03/24/2013	51 60503	. 0	Established	1171.68.34.1	5 9465 PHD	173.37.163.3	1524 DC	OTHER_(top			10	SOAAEAA	ARAAAAAA	Aother		-1
2 13640	186927) mtv5-j	ski-nm 03/24/2013	60503	ι ο	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	OTHER_(top			10	SOAAEAA	A BANKWAC	Aother		-1
3 13540	(86927) mtv5-	oki-nm 03/24/2013	3 60503	L 0	Established	1171.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	_OTHER_(tcp			6	SOAAEAA	AGAAAWAC	A other		-1
4 13640	istory mitris	pto nm 03/24/2013	si 60503	. 0	Established	11/1.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	_OTHER_(top			10	JUAAEAA	ABAAANACI	A other		-1
3 13640	186927) mtv5-	ski-nm 03/24/2013	51 60503	0	Established	1171.68.34.1	5 9465 Pi0	173.37.163.3	1524 DC	OTHER_(tep			10	SOAAEAA	AgAAAwAC	Aother		-1
0 13640	acez / mtv5-	se-nm u3/24/2013	60501	. 0	established	11/1.68.34.1	3 9465 PR	178.37.163.2	1524 DC	_OTHER_(tep				JUMEAA	NEW WINK	n other		-1
/ 13640	seez / mtv5-	pip-nm/03/24/2013	51 60503	. 0	established	11/1.68.34.1	5 9465 PKI	1/5.37.163.2	1524 DC	_OTHER_(top				JUAAEAA	A BAAANACI	A other		-1
8 13640	istory metals	ato nm 03/24/2013	51 60503	0	established	11/1.68.34.1	5 9465 PKI	173.37.163.2	1524 DC	_OTHER_(top			10	JUAAEAA	AGAAANACI	A other		-1
13640	acout in mtv5-	se-nm us/24/2013	60503		established	11/1.68.34.1	s 9465 PR	175.37.163.2	1524 DC	_OTHER_ETEP				JUNALAA	ADVIANACI	N OTHER		-1
0 13640	acez / mtv5-	se-nm u3/24/2013	60501	. 0	established	11/1.68.34.1	3 9465 PR	178.37.163.2	1524 DC	_OTHER_(tep				JUMEAA	NEW WINK	n other		-1
13640	istez // mtx5-	ato-nm 03/24/2013	51 60503	. 0	established	11/1.68.34.1	5 9465 PKI	175.37.163.2	1524 DC	_OTHER_(top				JUAAEAA	AGAAANACI	A other		-1
13540	acoz // mtv5 /	serm 03/24/2013	60503		escapished	11/1.68.34.1	2 9465 PKI	1/5.37.163.2	1524 00	_OTHER_LITEP				JURALAA	ADVANAC.	H OLINEY		-1
3 13640	acout in mbs5-	se-nm u3/24/2013	80503		catablahed	11/1.68.34.1	5 9465 PKI	173.37.163.2	1524 00	OTHER (tep				JURALAA	Agan An AC	N OTHER		-1
1,3940	evel // mtx5-	Arnim 03/24/2013	s 60501		escopested	1171.08.94.1	a 9460 MG	178.87.163.2	1524 00	OTHER_LITED					- CONNIACO	other		-1
3 13940	soone / mtv5	okrmm 03/24/2013	60500		cscool/sted	11/1.08.34.1	2 2465 PN	175.57.165.2	1524 00	_OTHER_LITEP				COMMERA	- NOVANAL)	H OLINE!		-1
2 13640	86037 mb/5	binn 03/24/2013	51 60503	. 0	escapished fatablished	1171.68.34.1	2 9465 PKI	173.37.163.2	1524 00	OTHER LINE				JUNNEAA	ADDAMAC	A other		-1
13040	100271 mts5-1	mu3/24/2013	60503		Locatement of	171.08.04.1	9465 96	173.37.163.2	1524 00	COTHER_LEEP			A1	-JgADA	- CONNAC	other .		-1
0 12640	260371 mtv5-	kion 03/24/2013	60501		Established	1171 69 34 1	a 9400 PN	172 27 163 1	1524 00	OTHER (100			-	ADDARDAR	Achter Achter	A other		-1
7 13940 0 13640	0002/11005	ki om 03/24/2013	60503	. 0	Couplished Couplished	1171.08.34.1	2 2460 PN	173.37.163.2	1524 00	OTHER (NO			A	ADDADAR	ADDADAD C	A other		-1
1 19640	REGION MENDI	bi am 03/24/2013	60501		fatablished	1171 69 34 1		172.37.103.1	1524 00	OTHER (Area			A1	10,04040	And Advertige	Anthor		-1
2 13640	86027) mt	klop 01/24/2013	1 60503		Established	1171 68 34 1	5 0445 PT	173 17 143 3	1524 00	OTHER (THEP			-	40.040	Arabbu C	A other		
3 12640	260371 mtv5-	kiom 03/24/2013	60501		Established	1171 69 34 1	a 9400 PN	172 27 163 1	1524 00	OTHER (100			-	ADDADAU	Acht hat C	A other		-1
1 12640	26037 mt 5	ki om 03/24/2013	2 60503 21 60504		Compromed Completioned	1171 69 34 1	2 0460 FK	173.37.165.2	1524 00	OTHER (NO			A	ADDADAR	And A Amaton	A other		-1
13040	REGION MENDI	bi am 03/24/2013	60501		fatablished	1171 69 34 1		172.37.103.1	1524 00	OTHER (Area			A1	10,04040	And A fund (Anthor		-1
11540	86027) mtv5.	klop 01/24/2013	1 60501		Established	1171 68 34 1	5 0445 001	173 37 163 2	1524 00	OTHER LINE			41	401040040	Arabahus Co	A other		-1
7 12640	26037 mtv 5	kion 03/24/2013	a 60501		Ertablished	1171 69 34 1	2 0465 241	172 27 163 1	1524 00	OTHER (no			-	ADMARA PAR	Achahant Co	Acther		-1
0 10640	26027 mt-5	ki om 03/24/2013	60501		Crahiched	1171 69 24 1	C 0465 841	172 27 162 1	1524 00	OTHER (tree			A1	10 0 0 A P	Act Actual Co	Active		-0
9 13540	86927i mts5.	kine 03/24/2013	L 60501	0	Established	1171 68 34 1	5 9465 PM	173 37 163 1	1524 00	OTHER (Inco			41	48103848	Aria and	A other		-17
	14 4 5 51	PKI as source	e 24 hours.cs	w + 1										- Sector			Date	n l'
BB	Macroal Mar	Ready							Suma 0	-		_						1
-	monthal vice	. Actor							2011-0			_				_		_

- 112,374 results 0
- Analyzed in Excel \bullet

10.28.21.229 171.70.145.234 64.100.18.131 64.100.23.14 64.102.120.6 64.102.17.55 DC_NETAPP_FILER DC_NIS_SERVERS DC_RTP_DC_NETS 171.68.34 171.68.34 171.68.34 71.68.34.158 71.68.34.170 71.68.34.171 64.102.106.27 64.102.106.40 64.102.106.48 64.102.106.50 64.102.106.89 171.68.34.158 DC_ALL_DC_NET 171.68.34.159 171.68.34.154 171.68.34.158 171.68.34.159 171.68.34.170 171.68.34.171 DC_SJ 1234 171.70.145.23 173.36.129.23 171.68.34.13 DC_OTHER_DC_NET 171.68.34.153 171.68.34.155 171.68.38.36 171.68.38.38 DC ALL DC NETS 71.68.34.13 DC_AD_SERVER 171.68.34.141 171.68.34.153 171.68.34.153 171.68.34.155 64.102.106.55 64.102.106.80 64.102.106.81 DC_OTHER_DC_NET DC_NETAPP_FILER: DC_SJ

Currently

16 results 0

171.68.34.15

Analyzed in Splunk Formats data

10.28.21.229 171.70.145.234 64.100.23.14

during search

16

The Playbook



What is a playbook?

playbook |'plā,bŏk|

noun

A prescriptive collection of repeatable queries (reports) against security event data sources that lead to incident detection and response.

0100003-HF-IDS-MALWARE:BOT-C2

Objective:

Discover and report botnet infected hosts for remediation and enhance future detection.

Working:

index="ids" earliest=-10m tag=**HF-IDS** NOT (tag=**IN_DNS** OR tag=**DC_MBOX** | stats count by host | sort -count limit=50 | rename attacker AS C2 | <u>`csirtTable`</u> | <u>`makeAcaseHF`</u> | <u>`botSquash(</u>C2)`

Action:

Case generated into auto-remediation queue: CSIRT-Analysts-HF

Analysis: The generated report is high fidelity – if an IRC Join is detected, verify the NICK is computer generated. These events require the reimage malware remediation process. If the bot matches the <u>Infostealer List</u>, email client <u>password update instructions</u>. If a the client address matches the <u>VIP list</u>, those hosts must be escalated to the <u>on-duty investigator</u>.

Reference: wiki/<u>10012</u>, bugzilla:<u>576</u>, GIR: n/a

Where do I Begin?

- What am I trying to protect?
- What are the threats?
- How do I detect them?
- How do we respond?

IR Fundamentals

- Develop requirements on frequency, priority, and scope
- Ensure basic requirements:
 - Solid systems of record
 - Complete traffic inspection coverage
 - Proper communication channels
 - Ensure proper remediation controls
 - Enforceable policies
- If you can build a good query, you can find malware, infected systems, and dedicated attackers
- If you can't automate, investigate

The Playbook MUST:

- Detect malware infected machines
- Detect suspicious network activity
- Detect anomalous authentication attempts
- Describe and understand inbound AND outbound traffic
- Provide custom views into certain environments

Additionally:

- Provide summary information including trends, statistics, counts
- Provide usable and quick access to statistics and metrics
- Correlate events across all relevant data sources

Correlation



CSA
timestamp (date)
source IP
source port
destination IP
destination port(s)
hostname
nbtname
sourcetype
eventsource
alerttype

Why?

- Áttribution \bullet
- \bullet
- \bullet
- Confirmation Temporal correlation Concurrent multi-index search \bullet ("sub-search")
- Homś Union \bullet Join \bullet

0800001-INV-MULTI-MALWARE:WSA validation of attempted CSA network connections

Objective:

Searches HIDS for outgoing tcp/80 connections and uses those IPs to find corresponding WSA logs to determine if the HIDS detected connection was malicious or not.

Working:

```
index="wsa" x wbrs_threat_type="*" (NOT (cs_referer="*")) [search
index="csa" "attempted to initiate a connection as a client on TCP port 80" "allowed"
rex "on TCP port 80 to (?<csa_dst_ip>\d+\.\d+\.\d+\.\d+\.\d+) using" |
dedup csa_dst_ip |
rename csa_dst_ip AS s_ip |
fields s_ip] |
rex field=cs_url "http:\//(?<domain>[^\/]+)" |
rex field=cs_url "\/(?<script_name>[^\/\?]+) (?=$|\?)" |
dedup script_name |
dedup domain |
dedup c_ip |
dedup cs_url
```

Action: Manual investigation. Analysis may result in submitting a host for remediation.

Analysis: Investigate whether HIDS detected connections may be a sign of an infected host by reviewing the WSA SIO data and any additional event indicators.

Reference: wiki/10103, bugzilla:6742, GIR: n/a

How do we know you're working?

METRICS!

- Top events fired per event source
- Top malicious domain
- Total infected hosts
- Top malware type/family
- Highest areas of infection (lab, DC, DMZ, etc.)
- Infections by theatre
- Infection by role/org (sales, engineering, marketing, etc.)
- Event rates and collection stats (total volume of alarms, then alarms by source, index/filesize avg/day)
- Unique user counts avg/day
- Total attacks blocked by CSIRT
- Top infections by event source (event source detection ranking)

Yeah, but how exactly do we do it?

Malware/Advanced Detection e.g. Phishing URLs in email

Anomaly Detection e.g. Two VPN logins from a single user

Policy-driven monitoring: e.g. Flows from datacenter to Internet

Operational intelligence: e.g. Malware analysis for indicator discovery

You can help!

- FIRST standard
- Information sharing how do YOU detect threats?
- Strategy sessions (network agnostic)



Q/A

jeff.bollinger@cisco.com matthew.valites@cisco.com