Visualizing your security posture from link, to gateway, and beyond.

.ca

BERNETIO



Joe Cummins CTO / Founder



Cyber Security is a series of interconnected & complex challenges





#thechallenge

01 CURRENT

02

FUTURE



dbort("The Rails environment is remained and a second part"
require "spec_helper"
require "repoined"

require "coptors/repo!" require "coptors/relis"

Capybors. javascript. brier + Category. delete..all; Calegors Sheelds: Skitchers.col carfig.integrate with, test..fro with, test..fro





















#thechallenge **SITUATION CURRENT Business Objectives** Political/Regulatory **Business Layer Function Layer** Outline of Use Cases **Information Layer** Interoperability Subfunctions ata Model **Communication Layer** rotocol **Component Layer** Market Generation Enterprise Transmission Station Distribution Field DER Zones Domains Customer Process Premise









Typical SIEM interfaces when they're being marketed. "Pretty screens" appear to make cyber security simple. These are great for executive summaries and seeing trends.



Datibut / Security (AWE D									id Save Share	4 0 La	Contribute							Complants	Service Data Searched		😳 Help Desk
men Security (MAS) - Lacation	. 8		an B	ANS perce	rigi-Non-US	Countries 0 = 0 = 0	anti a	Security (XWI) - D	ata Source Distrib	ofian official offici	LDW Hi Hal				Dashboard Deshboards > Execu	ds live	Vuene autors	outpearte N	Lans creption Plan		Manage labs 1 🐟 1 🧿
										• Court	hard.				- 005 evenes (-) 1)			runy.			300 * 11 = 17 ± C / 15501000
- C.S.		1													Events (803)	Patterns S	tatistics Visu	alization			
Dashboards						Concert And In		_							210112 (000)	- recents - s	1000				
🛃 Incidents	Class		Type	Search text	in all feids	raters fearen is	in charge		Status	Pr	iority	Actors			Format Timeline 🗸	- Zoom Out	+ Zoom to Selection	× Deselect			1 day per colu
» Alarms	ALL	•	ALL					Oper	9 Q	• ALL	•	learch Close sele	lected							_	
> Tickets																					
Knowledge DB	- 111 - 11	an can	- March -	Dom							*	Apply tags to selecte	ed tickets				List v Form	at 🗸 🛛 20 Pe	r Page V		<pre> 1 2 3 4 5 6 7 8 9 Next</pre>
jį Analysis	E1 10	CKIPT TI	i me his is a test ticket for events generated	by FLWARE	nonty	Created	Life Life	e in chi SE	nde and	enviceer	type fearl	status extra te	roc regel				d Time	French	1.0.0.000 (C)		
Reports		A172	GE coming from SENSOR his is a test ticket for events generated	t by FI-WARE	-	2014-04-03 19:19	S4 S Cays I	Admini	strator as	oren	Generic	open			< Hide Fields	i≡ All Fields	1 Time	80 144 1	102 54 [20/Apr/20	13-22-15-14 +02001	"GET /tamplatas/ sustam/css/manaral css WTTD/1 1" 404 230 "http://www.a
Assets		A109	GE coming from SENSOR his is a test ticket for events generated	by FI-WARE		2014-04-03 19.10	32 5 Days 11	Adminia SE	strator di M	oniko	Generic	Open			Solostad Eields		1:15:14.000 F	M huette-r	raith.at/" "Mozilla/5	.0 (iPad; CPU OS 6_	_0_1 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 M
		A100	GE coming from SENSOR his is a test ticket for events generated	by FI-WARE		2014-04-03 19:03		Adminis	strator ^{ex}	omen	Generic	Open			a host 1			ile/10A5	523 Safari/8536.25" "		reversions - seaseds stade lies
Intelligence		A100	GE coming from SENSOR			2014-04-03 10:55	02 5 Days 17	Adminia	strator ^{as} M	omen	Generic	Open			a source 1		> 4/30/13	178 115	249 93 130/Apr/2	013:20:34:49 +02001	sourcecype = genenc_single_une 1 "GET /templates/ system/css/general css HTTP/1 1" 404 239 "http://www
Situational Awareness	E 4	A159	Check a potential port-scanning atte	tempt		2014-04-03 10:41	47 5 Days 17	54 Admini SE	strator al	5min	Generic	Open			a sourcetype 1		11:34:49.000	AM mhuette-	-raith.at/" "Mozilla/	5.0 (compatible; MS	SIE 10.0; Windows NT 6.1; Trident/6.0; MAMD)" "-"
Coployment	A	A156	GE coming from SENSOR	by FLWARF	5	2014-04-03 18:41	38 5 Days 17	54 Admini	strator ^{do}	dmin .	Generic	Open			Interesting Fields			host = mit	zkowitz-mbp.sv.splunk.com	n source = log.txt s	sourcetype = generic_single_line
	E A	A153	GE coming from SENSOR			2014-04-03 10:36 43 2014-04-03 18:19:44	43 5 Days 17	57 Admini	strator ex	șeniis	Generic	Open			a index 1		> 4/30/13	178.115.	178.115.249.93 - [30/Apr/2013:20:34:34 +0200] "GET /templates/_system/css/general.css HTTP/1.1" 404 239 "http://www./		
	E 64	E174	[interface_name:source_addressisource_port] [(idfw_user)] [FQ0II_string] dst interface_name:dest_addressidest_p	rce_port) it st_p	٥		44 5 Days 10	16 SE Admini	M. strator av	dmin	Generic	Open			# linecount 1 a splunk_server 1		11:34:34:000	NT 6.1; host = mit	; Trident/6.0; MAMD)" zkowitz-mbp.sv.splunk.com	source = log.txt is	sourcetype = generic_single_line
	E 6	E173	[interface_name:source_addressisour [interface_name:source_addressisour [(idfw_user)] [/GON_string] dst interface_name:dest_addressides	rce_port) it st_p	١	2014-04-03 18 19	42 5 Days 10	:16 SE Admini	M strator ac	dmin	Generic	Open		sts	G Extract New P	Hosts with Mul	tiple Threats	8	Total Threats		GET /favicon.ico HTTP/1.1" 404 217 "-" "Mozilla/5.0 (compatible; MSIE
	E N	£171	Deny protocol src [interface_name:source_address/sour [(idfw_user)] (FQ0I_string) dst interface_namedeat_address/idea	rce_port] it	8	2014-04-03 18:10	40 S Days 18	125 St Admin	strator et	dmin.	Generic	Open		g one or moi	e active threats	Hosts containing m	ultiple active threats	0	Total threat instances across	the enviroment	<pre>vetype = generic_single_line</pre>
	E 6	E170	Deny protocol src (interface_namecsource_address/sour ((idtw_user)) (rGDN_string) dat interface_namedest_address/des	rce_port] it \$1_p	8	2014-04-03 18:10	38 5 Days 18	125 SE Admini	M ec	dmin	Generic	Open		ſ	1		Ο		58	26	
	E E	E168	Demy protocol src [interface_name:source_addressisour [(idfw_user)] [FQ0N_string] dst interface_name:dest_addressides	rce_port] it st.p	8	2014-04-03 18:03	56 5 Days 18	131 SE Admini	M strator as	ónin	Generic	Open					U				Actual care and SOC analysts
	E 6	E167	Deny protocol arc (interface_name:source_address/sour ((idfw_user)) [FGON_string] dat interface_namerical_address/idea	rce_port]	2	2014-04-03 18:03	48 5 Døys 18	132 SE Admini	ti strator at	dmin	Generic	Open			Threat Activity By Cla	ssification					do their daily job
Cotres tie 🛋		E165	Deny protocol src (interface_name:source_address/sour [(idfw_user)] [/QDN_string] dst	rce_port] it	8	2014-04-03 17:58	23 5 Days 18	1.37 SE Admini	M strator at	dmin 🛛	Generic	Open			600						do then daily job.
User session: 23 minutes (3.35) 4 active users			Deny protocol src	ng porti	_										400 ₩				/	Malware - Backdoor	
1	17 10	2164	C Halvare - Ba	ackdoor		2014-04-03 17:58	22 5 Qays 18	37		5min	Generic	Open	37		Cour			/	/	- Idalware - Infostealer	THE GAP: Current products o
			So Malware - Down	nloader									qu	arantined ived	200			/		- Malware - Ransom Malware - Trojan	roport throats based on food
			Ulahvare - Info	ostealer														/		Malware - Virus	report tilleats based on leed
			Malware - R	Ransom											Librah	And	Unu	luna	10.	PUP - Adware PUP - Keygen	AI applied to those feeds Th
			Maluare	- Virus O	50	100 15	50 200	250	300	350	400	450 500			2016	Ара	Time	June	July		don't take into account netw
			Threat Activi	Threat Activity By Device											New Threats - Last 30	design flaws, policy changes.					
			600												SHA256 0				File Status 🗧 Classific	ation a AV Industry a	
											1				1 5C2A85FB56DE2E0	A1A1D260EF2177E020	9477586C8A6740494	BBAF40A9785F4	7 quarantined N/A	Threat	organizational complexity, an
			400								/				2 D90376CD498C5A0	E396FC3A824B8159FF	AE50D5DFD0BE51943	6BC33B228F4A4	9 quarantined N/A	Threat	doop communication path is
			count							/			CYL CYLFIXE	FUNCTIO	3 E20760572137FFA3	34D15E717F39E63F0BE	5C61B09C12F125A4	D8366AFCE84E9	guarantined N/A	Threat	a ueep communication path is
			200						,	/			DESKTO	P-02HGFLJ	4 CBF516FEA95A7C9	6E96AD9C392783B966	5CA866247F5B94C0	CE9B9A89FD8F7	74 quarantined N/A	Threat	Most AI is really algorithms
									/				WIN-6SL	4J65SKF	5 A5837302D24D7D0	D24C3D05DF2F7B3A0	SCF8F87B2E8E9B15	4BEC92B6FC745	54 quarantined N/A	Threat	
			_		-				1		_		— user's Ma		6 EAFD6E79D96E125	F2AD888CBDA1E4BA8	EC04B7E870E6B3F46	ACB6AC26F0479	95 quarantined N/A	Threat	applied to specific use cases.
			March		April		May		June		July				7 E2A7E2596857EBC	F22E8238CEF91F4BA1	CE05619D3589C1AE6	3319BA6D88D02	7 guarantined N/A	Threat	C

Stream CYBERNETIQ

	ţ	<u>.</u>	Sun B	ANS per		0.00			N I	eta VPC_FLDBW SSAccessi Cloudthall Cloudthant			Dashboard Dashboards > Executiv	ls •						Managetabs 💠 🧿
		o	° 2008 -										Events (803)	Patterns St	atistics	Visualization				300 * 11 10 // 2 O / Factoride *
Dashboards					Simple	Filters (switch to	Advanced) 🖭						Formal Timeline	7		Colordina y Douglas				1 day per colur
 Incidents 	0	lass	Туре	Search tex	d in all field	s 1	n charge	Stat	15	Priority	Actors		Formac Timetine 🗸	-200m Ouc	- 200m i	to selection in A Deselec	λ.			
» Alarma	ALL	•	ALL	•				Open	()	ALL -	Search Close selected	4			_					
Tickets Knowledge D6											Apply tags to selected ticke	· .								_
i. Analusia	12	Ticket	Title		Priority	Created	Life Time	In charge	Submitter	Type (Edd)	Status Extra (Edit Tags)				List	✓ Format ✓ 20) Per Page 🗸			<pre> 1 2 3 4 5 6 7 8 9 Next:</pre>
, readjuit	10	ALA172	This is a test ticket for events gen GE coming from SEN	nerated by FI-WARE ISOR		2014-04-03 19:19:	5 Oays 17:1	SIEM Administrator	admin	Generic	Open		< Hide Fields	I All Fields	1 1	lime Event				
Reports	13	ALA169	This is a test ticket for events gen GE coming from SEN	verated by FI-WARE ISOR	5	2014-04-03 19:10	32 5 Days 17.2	SEM Administrator	admin	Generic	Open				> 4	4/30/13 89.14	4.192.54 [30/Apr/201	3:22:15:14 +0200] 0 (iPad: CPU 05 6	"GET /templates/_sys	tem/css/general.css HTTP/1.1" 404 239 "http://www.al
Assets	10	ALA 166	This is a test ticket for events gen GE coming from SEN	rerated by FI-WARE	5	2014-04-03 19:03:	5 5 Days 17.3	SEM Administrator	admin	Generic	Open		Selected Fields		2	ile/1	0A523 Safari/8536.25" "-		_0_1 11KC BUC 05 K) K	ppreneokie/330/20 (kinac, 12ke decko) fersion 0.0 mo
Intelligence	1	ALA 160	This is a test ticket for events gen GE coming from SEN	serated by FI-WARE	5	2014-04-03 18:55	22 5 Days 17:4	SEM Administrator	admin	Generic	Open		a host 1 a source 1			host =	mitzkowitz-mbp.sv.splunk.com	source = log.txt s	sourcetype = generic_single	_line
Situational Awareness	13	ALA159	Check a potential port-scane	ning attempt		2014-04-03 10:41	67 S Days 17:5	SEM Administrator	admin	Generic	Open		a sourcetype 1		> 4	4/30/13 178.1	15.249.93 [30/Apr/20 te-raith.at/" "Mozilla/5	13:20:34:49 +0200] "GET /templates/_sy SIE 10.0: Windows NT	stem/css/general.css HTTP/1.1" 404 239 "http://www.a 6.1: Trident/6.0: MAMD)" "-"
P Deployment	13	ALA156	This is a test ticket for events gen GE coming from SEN	verated by FI-WARE ISOR	5	2014-04-03 18:41:	5 Days 17.5	SEN Administrator	admin	Generic	Open					host =	mitzkowitz-mbp.sv.splunk.com	source = log.txt s	sourcetype = generic_single	_line
Colorina	•	ALA153	This is a test ticket for events gen GE coming from SEN	erated by FI-WARE ISOR	5	2014-04-03 18:36	43 SDays 17.5	SEM Administrator	admin	Generic	Open		a index 1		> 4	¥/30/13 178.1	15.249.93 [30/Apr/20	13:20:34:34 +0200] "GET /templates/_sy	stem/css/general.css HTTP/1.1" 404 239 "http://www.al
	83	EVE174	Deny protocol src [interface_namecsource_address/source_port] [(idtw_user) [(FGDB_string) dst interface_namecdest_address/dest_p	c ssisource_port) ling) dist essidest_p	Ð	2014-04-03 18 19 1	14 S Days 18:16	SEM Administrator	admin	Generic	Open		<pre># linecount 1 a splunk_server 1</pre>		1	11:34:34.000 AM mhuet NT 6 host =	<pre>te-raith.at/index.php?op .1; Trident/6.0; MAMD)" mitzkowitz.mbo.sv.solunk.com</pre>	"_"	view=article&id=49&It	emid=55" " <mark>Mozilla</mark> /5.0 (compatible; MSIE 10.0; Window:
	в	EVE173	Deny protocol sin [interface_name:source_addren [(idfw_user)] [/'GDN_str interface_name:dest_addre	c ssisource_port] ing] dst essidest_p	2	2014-04-03 18 19	12 5 Days 18:1	SEM Administrator	admin	Generic	Open	sts	O Extract New Fie	Hosts with Mult	iple Th	reats	Total Threats	, searce together a	GET /favicon.ico H	TTP/1.1" 404 217 "-" "Mozilla/5.0 (compatible; MSIE
		EVE171	Deny protocol sn [interface_name:source_addres [(idfw_user)] [FGDN_str	e ssisource_port] leg] dst	Ð	2014-04-03 18:10	40 5 Days 18:2	SEM Administrator	admin	Generic	Open	g one or more	active threats	Hosts containing multip		ive threats	Total threat instances across th	Total threat instances across the enviroment		_line
		EVE170	(interface_name:dest_addre Deny protocol sn (interface_name:source_addres ((idfw_user)) (FQDN_str	ess/dest_p c ss/source_port] ing] dst	Ð	2014-04-03 18:10:	38 5 Days 18.2	SEM Administrator	edmin	Generic	Open	0			0		EO	6		
	13	EVE168	interface_name:dest_addro Demy protocol sin (interface_name:source_addres (iddfw_user)) (FQ0N_str	essidest_p c ssisource_port] ing] dst	8	2014-04-03 18:03 1	56 5 Days 18.3	SEM Administrator	edmin	Generic	Open	U			U		50	U		FALSE POSITIVES are
		EVE167	interface_name:dest_addressidest_p Deny protocol src [interface_name:source_addressisource_port [interface_name:source_sidessisource] dist		Ð	2014-04-03 18:03 -	48 5 Døys 18 3	32 SEV Administrator	admin	Generic	Open		Threat Activity By Class	lassification						hreaking our
			interface_name:dest_addre Deny protocol sn	essidest_p c									600							Dicaking our
-Castren ille 🗮	13	EVE165	[interface_name:source_addree [(idfw_user)] [/GDN_str interface_name:dest_addre	ssisource_port] leg] dst essidest_p	B	2014-04-03 17:58:2	3 5 Days 18:37	SEM Administrator	admin	Generic	Open		400				/	- Nalware - Backdoor		organizations.
active users	12	EVE164	[interface_name:source_addres	c ssisource_port)	12	2014-04-03 17:58:	22 5 Days 18:3	SEM	admin	Generic	Open		int					- Malware - Bactooor - Malwarewnloader		
			ukil si jiga	vare - Backdoor								guarantined	200			,	/	- Malware - Parasitic Malware - Ransom		
			C Halva	re - Downloader ure - Infostealer								waived				/				SOC analysts have becor
			Mab	ware - Parasitic											_			PUP - Adware		
			Mal	ware - Ransom Walware - Vinus									March 2016	April	May	June	July	- PUP - Keygen		"ticket responders"
				0	50	100 15	0 200	250 3	00 350	400	450 500					Time				answering alert tickets
			Threat	Activity By Devic	ce								New Threats - Last 30 D	Days						rather than investigating
			600										SHA256 0				File Status 🗧 Classifica	tion a AV Industry a	F	wooknossos in our
										1			1 5C2A85FB56DE2E0A	1A1D260EF2177E020	477586	C8A6740494BBAF40A978	5F47 quarantined N/A	Threat	c	weaknesses in our
			400 Ĕ							/		-	2 D90376CD498C5A0E	396FC3A824B8159FF	E50D5D	FD0BE519436BC33B228F	4A49 quarantined N/A	Threat	C	networks.
			Cou						/	1		LFIXEDFUNCTIO	3 E20760572137FFA34	E06AD0C202702D066	CA8641	3C12F125A4CD8366AFCE8	VALUE quarantined N/A	Threat	C	
			200 -	200 - PM01 - PM01 - Wil45L								01 N-6SL04J65SKF	5 A5837302D24D7D0D	24C3D05DF2F7B3A01	5CF8F87	B2E8E9B1574BEC92B6FC	7454 guarantined N/A	Threat	c	
					~			/	/		W	N-UOHEHM2HG	6 EAFD6E79D96E125F	2AD888CBDA1E4BARF	C04B7F	870E6B3F461ACB6AC26F0	04795 guarantined N/A	Threat	C	



#reports **PSC CCRR**

01

Objective

02

Findings

Public Safety Sécurité publique Canada Canada



Regional Resilience Assessment Program and Critical Infrastructure Assessments Tools

Canada

G CYBERNETIQ





Universal Information Security Challenges

- Performance of IT Assessments of Enterprise and Automation networks is unpredictable, delicate, and risky!
- Requires in-depth understandings of:
 - Protocols, Devices, and entire Systems
- Existing tools:
 - bulky, costly, do not meet baselines
 - Generic Standards
 - Generate too many false positives
- Needed:
 - Lightweight, Risk Analysis Framework
 - Repeatable (Trending / Metrics)
 - Gap / Overlap analysis (Functionality / Optimization)
 - Identify exposures (Security / Awareness)
 - Business Value Proposition / Procurement
- <u>Simple</u> unified solution for mapping Resilience!



Universal Information Security Outcomes

•Contain, Identify, Control – 100% of Client network Ecosystem through "multiple source" inclusion

•Overlap / Overlay

•Network Architecture, Network Configuration Vulnerability data / Network Mapping Traffic / Syslogs / Netmon / Netflow Integrate existing security appliances •Network Traffic / System Applications •Network Vulnerability Management •Network Architecture / Endpoint Instantly Locate system / network gaps Remediate weaknesses Isolate Segmentation gaps Define actionable mitigations •Build / Change / Expand / Evaluate Network Infrastructure modifications •Network Segmentations failures

•Effective Network Security Posture

#thechallenge FUTURE- is NOW!

01

Problem Analysis

02

CLAW - a 3D Virtual Cyber Solution



dbort("The Rolls environment to remain a require "spec_belger" require "spec_belger"

require "coptors/rept" require "coptors/relis"

Capybors, jonescript, Arier e Category, daleta, alli, Calegore Secolds: Hetchers, col config.integrate inth, test. Arie with, library cruite

#thechallenge **FUTURE-** is NOW! **Problem Analysis**

"We treat security as device-centric weaknesses"



• Where is this device in my network?

- Howe is the computing ting to a the devices?
- Is in functioning about imabae the managed of source ty."
- • How in the watching public way fire wall rules?
- • What no motobolising three theorise cusiing Pool, EVER!"
- Arévilyeseurliendendetifsenenoftbamtother similar devices?
- • Wheren's know devaliging proving ity to my sensitive data?
- "I just need to meet compliance."









#reports **Discoveries**

D1 Problem Analysis

02 CLAW - a 3D Virtual Cyber Solution



require "coptors/non" require "coptors/noils"

Copybors.jonscript.driver = Cotogory.delete.oli; Cologors Seculdo:::Hetchark.col config.integrate elith.test.dru elith.test.dru elith.library.colis

Select from multiple "lenses" and Models to animate the dataset

Tree View Org, Location, Netblock, Subnet, Device





3

Ĉ

Q 7 💠

ð

Sun, 13 Jun 2010 12:05:38

01 - Remote

al BlackLis

0









CLAW-CE cybernetiq.ca/register

cybernetIQ.ca

info@CybernetIQ.ca

(877) 236-6996