

Homeland Security

Minimizing the Gaps with Bro, GRR, and Elk (Brogrrelk)

David Zito Northrop Grumman Information Systems

Outline

- 1. Goal of SATR
- 2. Overview of SATR
- 3. Components of SATR
- 4. Accomplishments of SATR
- 5. Standardized Reporting
- 6. Conclusion



2

Introduction

<Insert "Who I am" bullets>



What is the gap?





What are these gaps? - EVT

Vent Viewer (Local) Custom Views Vindows Logs Application Security Setup Setup Forwarded Events Applications and Services Lo Saved Logs Subscriptions	Security Number of e	Actions					
	Keywords Audit Success Audit Success	Date and Time 1/4/2016 1:25:44 PM 1/4/2016 1:25:44 PM	Source Microsoft Windows security Microsoft Windows security	Event ID 4622 4622		Security Open Saved Log Create Custom View	
	Audit Success Audit Success Audit Success Audit Success	1/4/2016 1:25:44 PM 1/4/2016 1:25:44 PM 1/4/2016 1:25:44 PM 1/4/2016 1:25:44 PM	Microsoft Windows security Microsoft Windows security Microsoft Windows security Microsoft Windows security	4622 4622 4622 4622	Security System Extension Security System Extension Security System Extension Security System Extension	Import Custom View Clear Log	
	Audit Success Audit Success Audit Success Audit Success Audit Success	1/4/2016 1:25:44 PM 1/4/2016 1:25:44 PM 1/4/2016 1:25:44 PM 1/4/2016 1:25:44 PM	Microsoft Windows security Microsoft Windows security Microsoft Windows security Microsoft Windows security	4622 4622 4622 4622 4624	Security System Extension Security System Extension Security System Extension Logon	Properties	
	Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success	1/4/2016 1:25:44 PM 12/30/2015 10:40:26 AM 12/30/2015 10:40:25 AM 12/30/2015 10:40:25 AM 12/30/2015 10:40:25 AM	Microsoft Windows security Eventlog Microsoft Windows security Microsoft Windows security Microsoft Windows security	4608 Security State Chan 1100 Service shutdown 4688 Process Creation 4672 Special Logon 4624 Logon	Process Creation Special Logon	Attach a Task To this Log View Refresh	
	Audit Success Audit Success Audit Success Audit Success	12/30/2015 10:40:25 AM 12/30/2015 10:40:24 AM 12/30/2015 10:40:21 AM 12/30/2015 10:40:21 AM	Microsoft Windows security Microsoft Windows security Microsoft Windows security Microsoft Windows security	4688 4647 4688 4688	Process Creation Logoff Process Creation Process Creation Process Creation	Event 5152, Microsoft Windows securit Event Properties Attach Task To This Event	ty
	Audit Success Audit Success Audit Success Audit Success	12/30/2015 10:39:49 AM 12/30/2015 10:39:49 AM 12/30/2015 10:39:49 AM 12/30/2015 10:39:36 AM	Microsoft Windows security Microsoft Windows security Microsoft Windows security Microsoft Windows security	4688 4688 4688 5157	Process Creation Process Creation Process Creation Filtering Platform Connection -	Copy Green Save Selected Events Refresh	
	Event 5152, Microsoft W General Details	- Help					
	The Windows Filteri Application Informa Log Name: 5 Source: 1 Event ID: 5						
	Usen M	nformation Keywords: / I/A Computer: nfo	Audit Failure				



P

1--/

E.

67

National Cybersecurity and Communications Integration Center

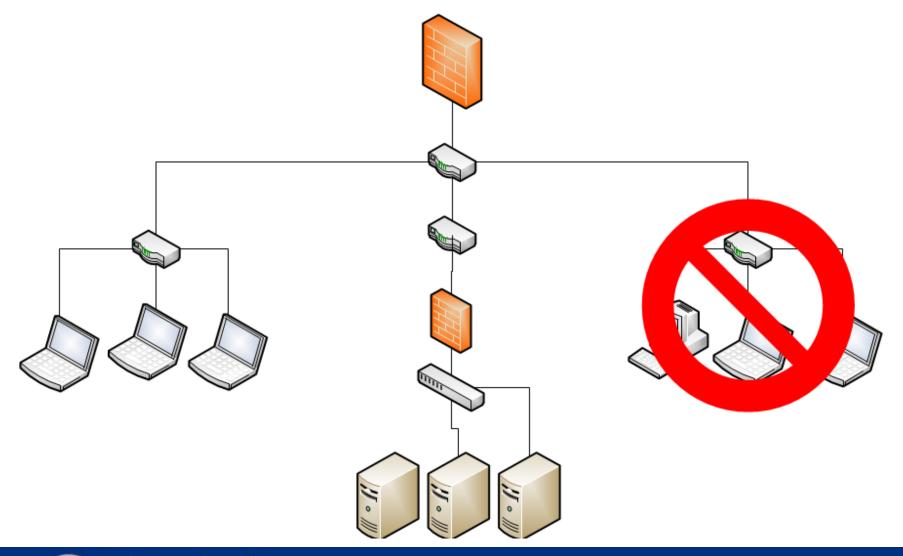
▲ 1:37 PM 1/4/2016

What are these gaps?Apache/IIS

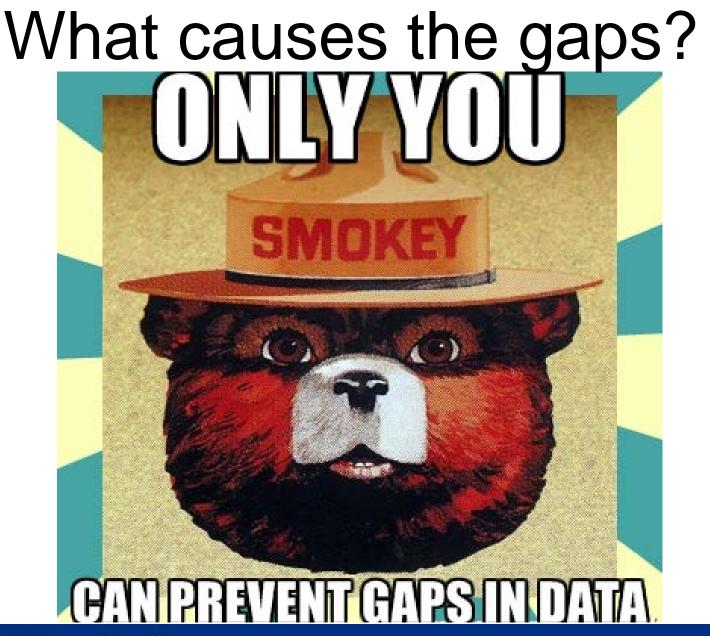
: 📄 u_ex	151208.log 🗵
1	#Software: Microsoft Internet Information Services 8.5
2	#Version: 1.0
3	#Date: 2015-12-08 18:47:44
4	#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-stat
5	2015-12-08 18:47:44 127.0.0.1 OPTIONS / - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 - 200 0 0 93
6	2015-12-08 18:47:49 127.0.0.1 OFTIONS /share\$ - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 - 200 0 0 46
7	2015-12-08 18:47:51 127.0.0.1 PROPFIND /share\$ - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 - 404 0 2 46
8	2015-12-08 18:47:51 127.0.0.1 PROPFIND /share\$ = 80 = = Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 = 404 0 2 62
9	2015-12-08 19:01:02 127.0.0.1 OPTIONS /Applications - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 - 200 0 0 62
10	2015-12-08 19:01:04 127.0.0.1 PROPFIND /Applications - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 - 404 0 2 4
11	2015-12-08 19:01:06 127.0.0.1 PROPFIND /Applications - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 - 404 0 2 4
12	2015-12-08 19:01:06 127.0.0.1 PROPFIND /Applications - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 - 404 0 2 6
13	2015-12-08 19:01:06 127.0.0.1 PROPFIND /Applications = 80 = - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 = 404 0 2 6
14	2015-12-08 19:04:35 127.0.0.1 OPTIONS /Applications/Workstation/VMwareWorkstation.msi - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/
15	2015-12-08 19:04:38 127.0.0.1 PROPFIND /Applications/Workstation/VMwareWorkstation.msi - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko
16	2015-12-08 19:04:40 127.0.0.1 PROPFIND /Applications/Workstation - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
17	2015-12-08 19:04:42 127.0.0.1 PROPFIND /Applications/Workstation/VMwareWorkstation.msi - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko
18	2015-12-08 19:04:44 127.0.0.1 PROPFIND /Applications/Workstation = 80 = - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
19	2015-12-08 19:04:47 127.0.0.1 PROPFIND /Applications/Workstation/VMwareWorkstation.msi - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko
20	2015-12-08 19:04:49 127.0.0.1 PROPFIND /Applications/Workstation - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
21	2015-12-08 19:07:00 127.0.0.1 OPTIONS /share\$/Applications/Workstation/VMwareWorkstation.msi = 80 = - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0)
22	2015-12-08 19:07:02 127.0.0.1 PROPFIND /share\$/Applications/Workstation/VMwareWorkstation.msi - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0
23	2015-12-08 19:07:04 127.0.0.1 PROPFIND /share\$/Applications/Workstation - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firef
24	2015-12-08 19:07:06 127.0.0.1 PROPFIND /share\$/Applications/Workstation/VMwareWorkstation.msi - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0
25	2015-12-08 19:07:09 127.0.0.1 PROPFIND /share\$/Applications/Workstation - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firef
26	2015-12-08 19:07:11 127.0.0.1 PROPFIND /share\$/Applications/Workstation/VMwareWorkstation.msi = 80 = - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0
27	2015-12-08 19:07:13 127.0.0.1 PROPFIND /share\$/Applications/Workstation - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firef
28	2015-12-08 19:08:36 127.0.0.1 OPTIONS /Applications/Workstation/ - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
29	2015-12-08 19:08:38 127.0.0.1 PROPFIND /Applications/Workstation/ - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43. 2015-12-08 19:08:40 127.0.0.1 PROPFIND /Applications - 80 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 - 404 0 2 4
31	2013-12-08 19:08:40 12/.0.0.1 PROFFIND / Applications - 60 Mozilia/3.0 (Windows N1 6.1; Wow64; PV:43.0) Geck0/20100101 FifeFox/43.0 - 404 0 2 4
:: 3T	



What are these gaps? - Netflow











What causes the gap?

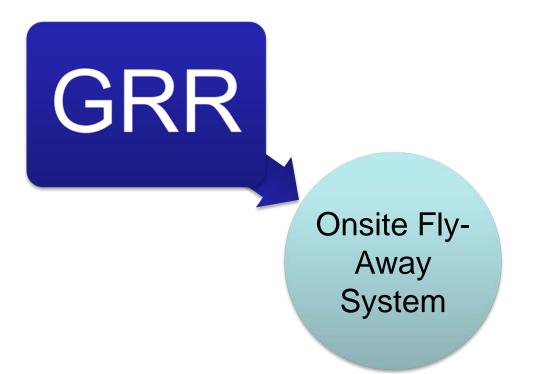
- Low fidelity logs
- Short shelf life of data
- Missing/destruction data



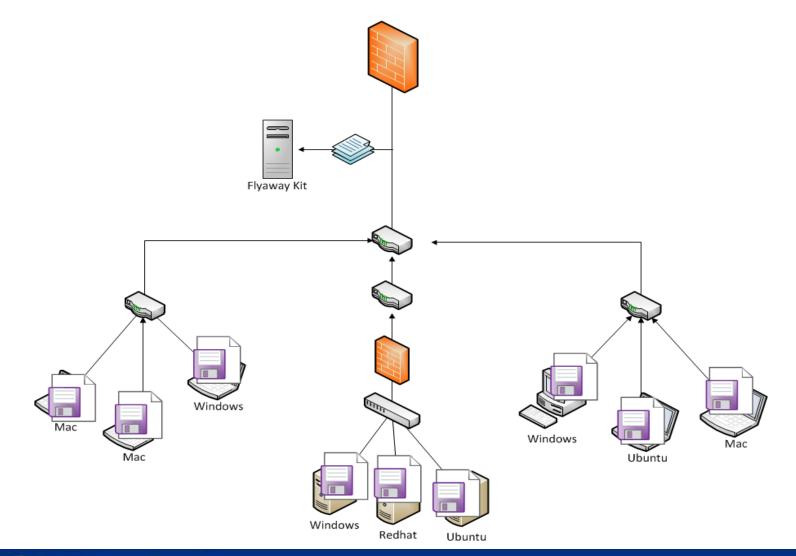
How do you fill the gaps?



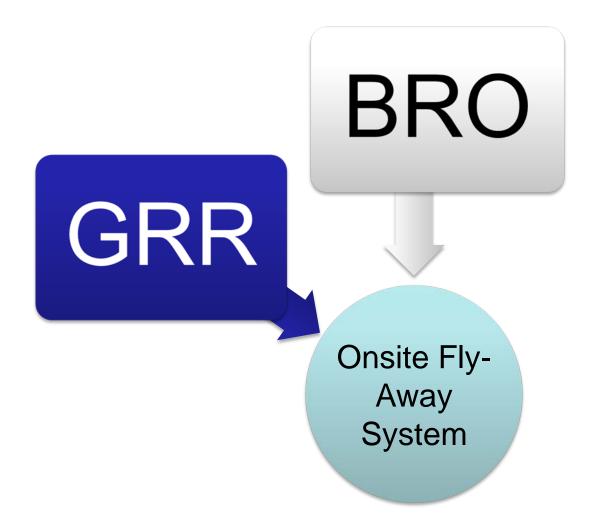




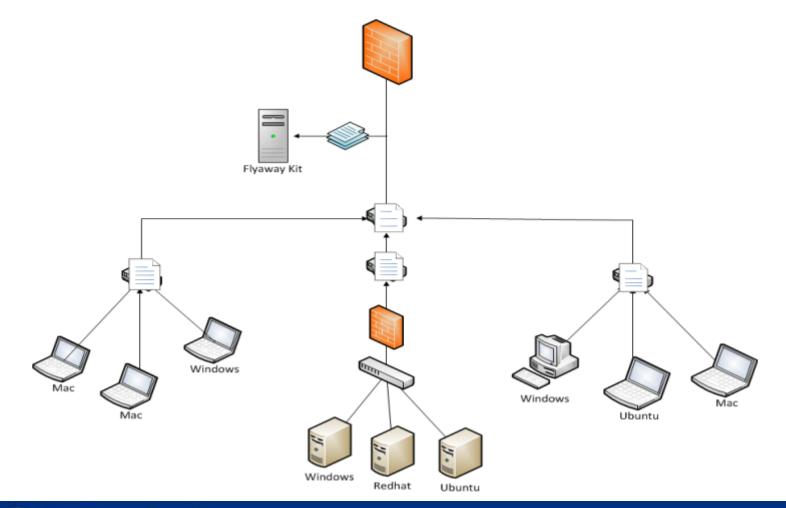




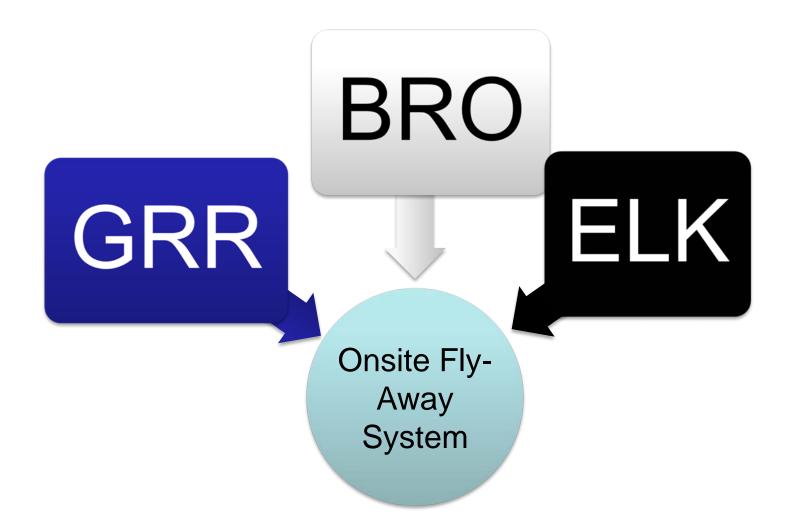














Visualize

							rs ago to 3 minutes ago. +	0 4	
Approx 2									
O Dynes (0 TO 400000	0) AND @tags.success								٩+
TYPING +									
EVENTS OVER TIME				0 0 + ×	мар				0 0 ÷ ×
View + 0 2000 Dir 0 50 50 50 50 50 50 50 50 50 50 50 50 50	1411 (and) (686) © phy junt) (656) © phy		21) GUARTERS 2000 (2274 HHG) 04.00 08.00 12.00 02-25 02-25 02-25	1400 2000 02-25 2000					
	0 0 + x VOLUME	(1)	Differentiations 0	• + x TOP SOURCES					• • + ×
(2	o o + x VOLUME	0 0 + x	-	Offer salar		00 00 00 00			0 0 + x
ALL EVENTS	0 0 + x		-			00 00 00 00	· phymemory -		
ALL EMENTS Relids Q		05	Churchen	Of the values and the second s	traging		, bytamentory i		0 0 + x
ALL EVENTS Paids Q Ally:// Exercit (M)	eners.	9 5	Chine salars	0 to 100 of 500 ansister + clientip +	kr piging • bytes =		<pre>c phonemory ;</pre>		0 0 + x
ALL EVENUE ALL EVENTS Fields O Major/former IBC Type for filter	Otoga - Recommendation	9%	Chier solars State (extension) Teni	© Torretues 825 0 to 100 of 500 available + clientip + 167,15,22,360	kr suging s bytes a 8540	00 42 20 10 10 10 10 10 10 10 10	: pigmemory :	-	0 0 + x



Homeland Security



<Insert contact info>

