



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



Introduction

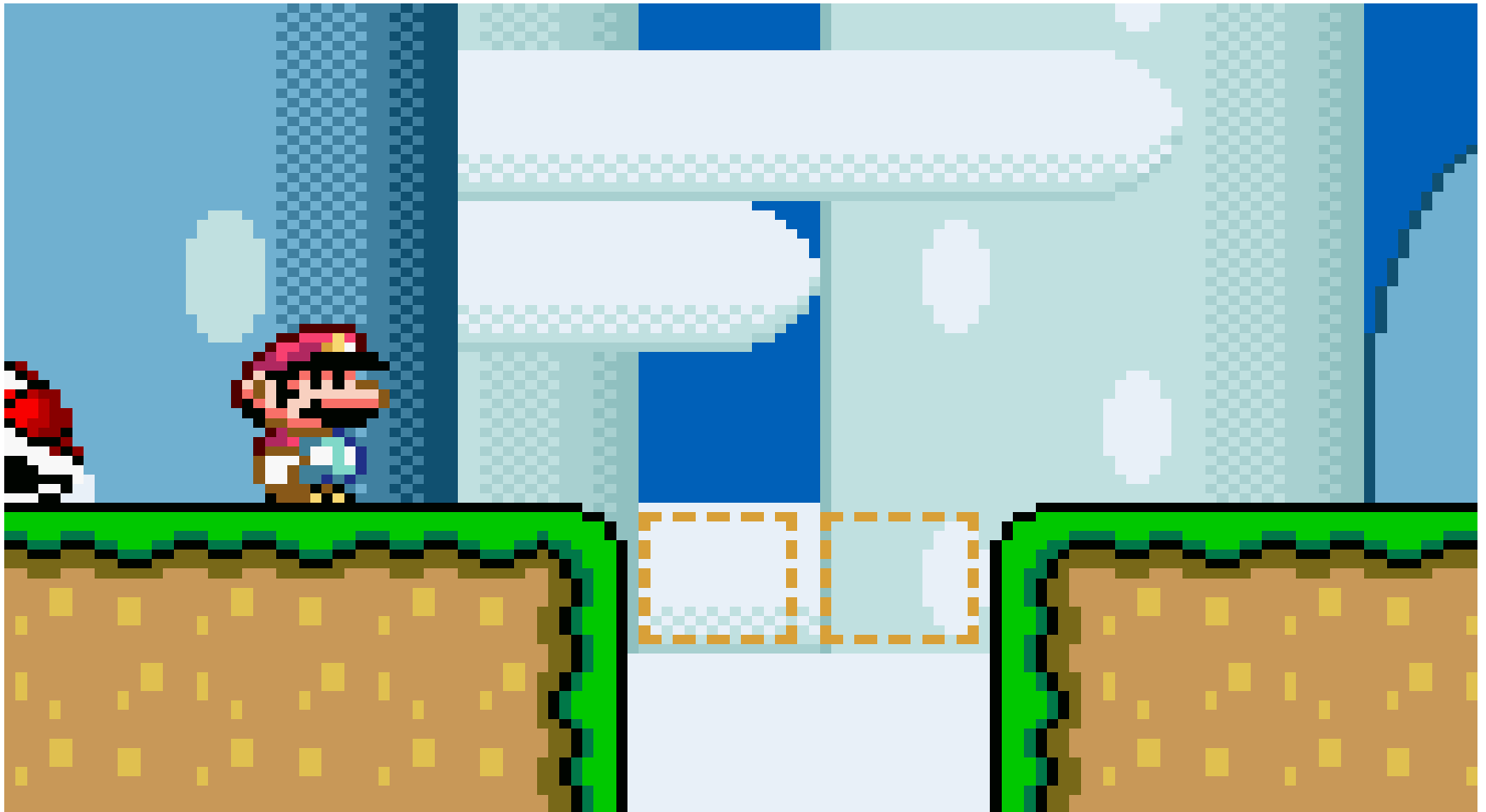
<Insert “Who I am” bullets>



Homeland
Security

National Cybersecurity and
Communications Integration Center

What is the gap?



Homeland
Security

National Cybersecurity and
Communications Integration Center

What are these gaps? - EVT

The screenshot displays the Windows Event Viewer interface. The main pane shows a list of security events with the following columns: Keywords, Date and Time, Source, Event ID, and Task Category. The list includes multiple 'Audit Success' events from 1/4/2016 and 'Audit Failure' events from 12/30/2015. The 'Event 5152, Microsoft Windows security auditing' window is open, showing the following details:

Field	Value
Log Name:	Security
Source:	Microsoft Windows security
Event ID:	5152
Level:	Information
User:	N/A
OpCode:	Info
Logged:	1/4/2016 1:36:01 PM
Task Category:	Filtering Platform Packet Drop
Keywords:	Audit Failure
Computer:	

The event description reads: "The Windows Filtering Platform has blocked a packet." The 'Details' tab is active, and the 'General' tab is also visible.

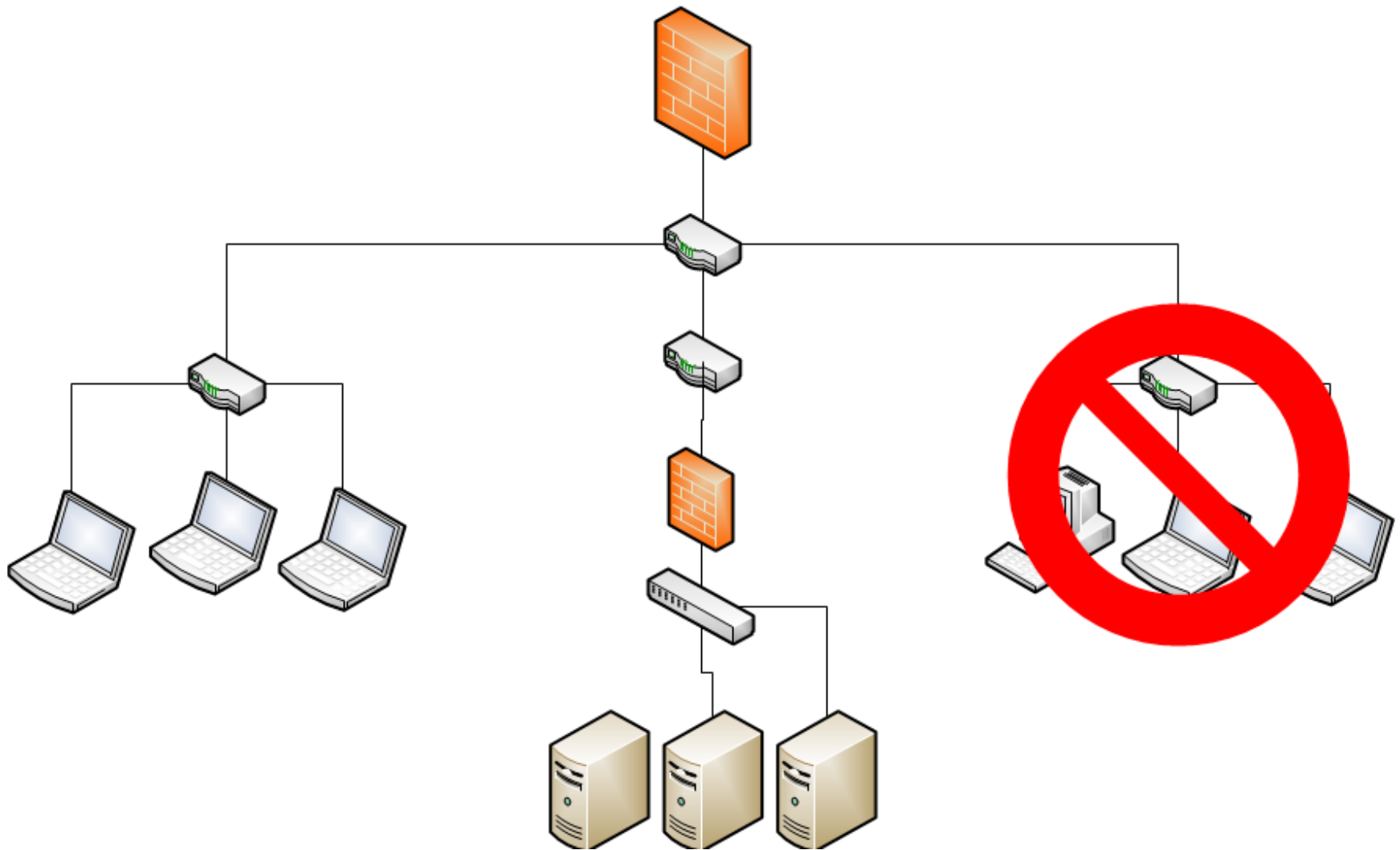


What are these gaps?Apache/IIS

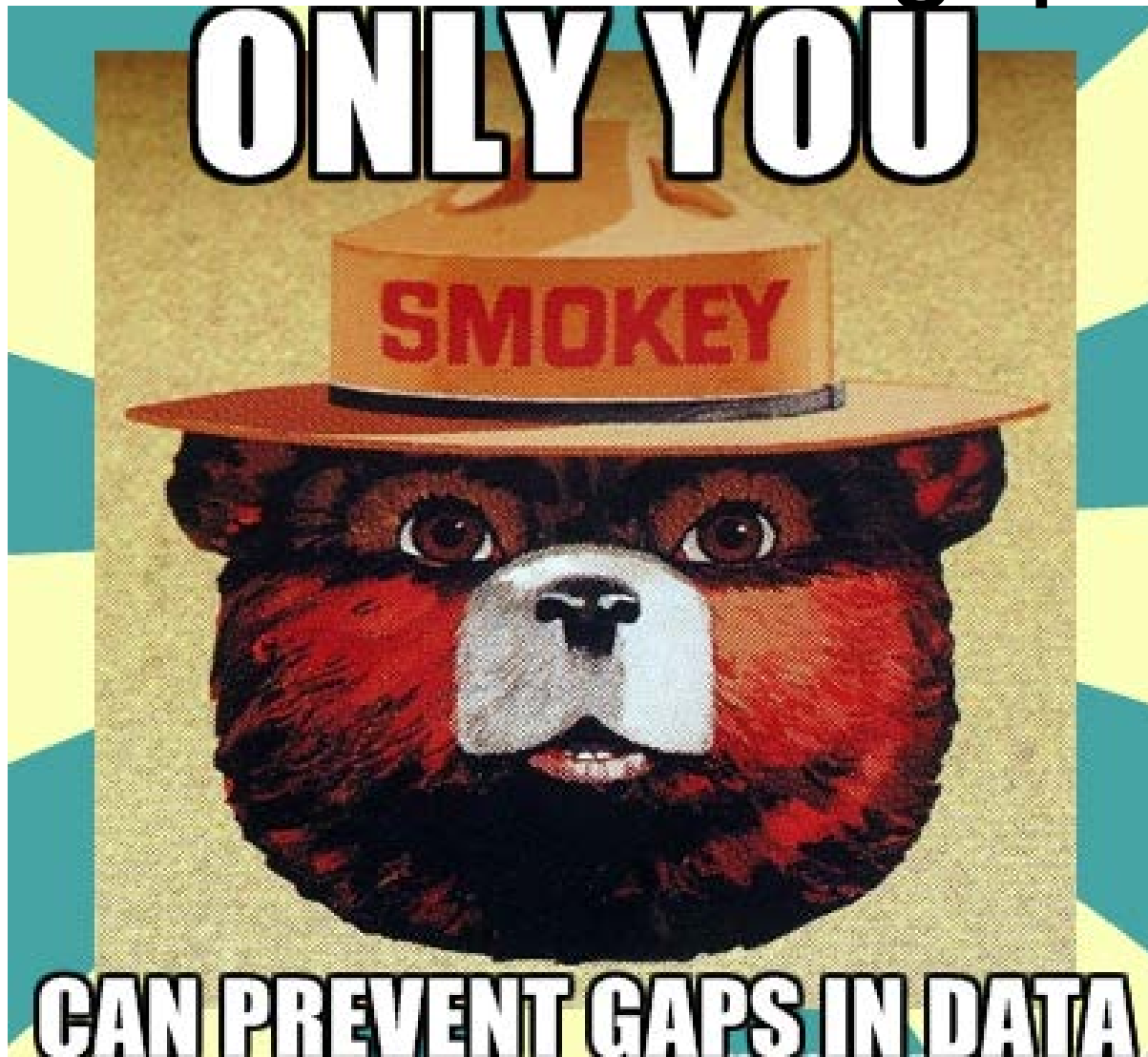
```
u_ex151208.log x
1 #Software: Microsoft Internet Information Services 8.5
2 #Version: 1.0
3 #Date: 2015-12-08 18:47:44
4 #Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-stat
5 2015-12-08 18:47:44 127.0.0.1 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 OPTIONS /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/43.0
30 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
```



What are these gaps? – Netflow



What causes the gaps?



Homeland
Security

National Cybersecurity and
Communications Integration Center

What causes the gap?

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



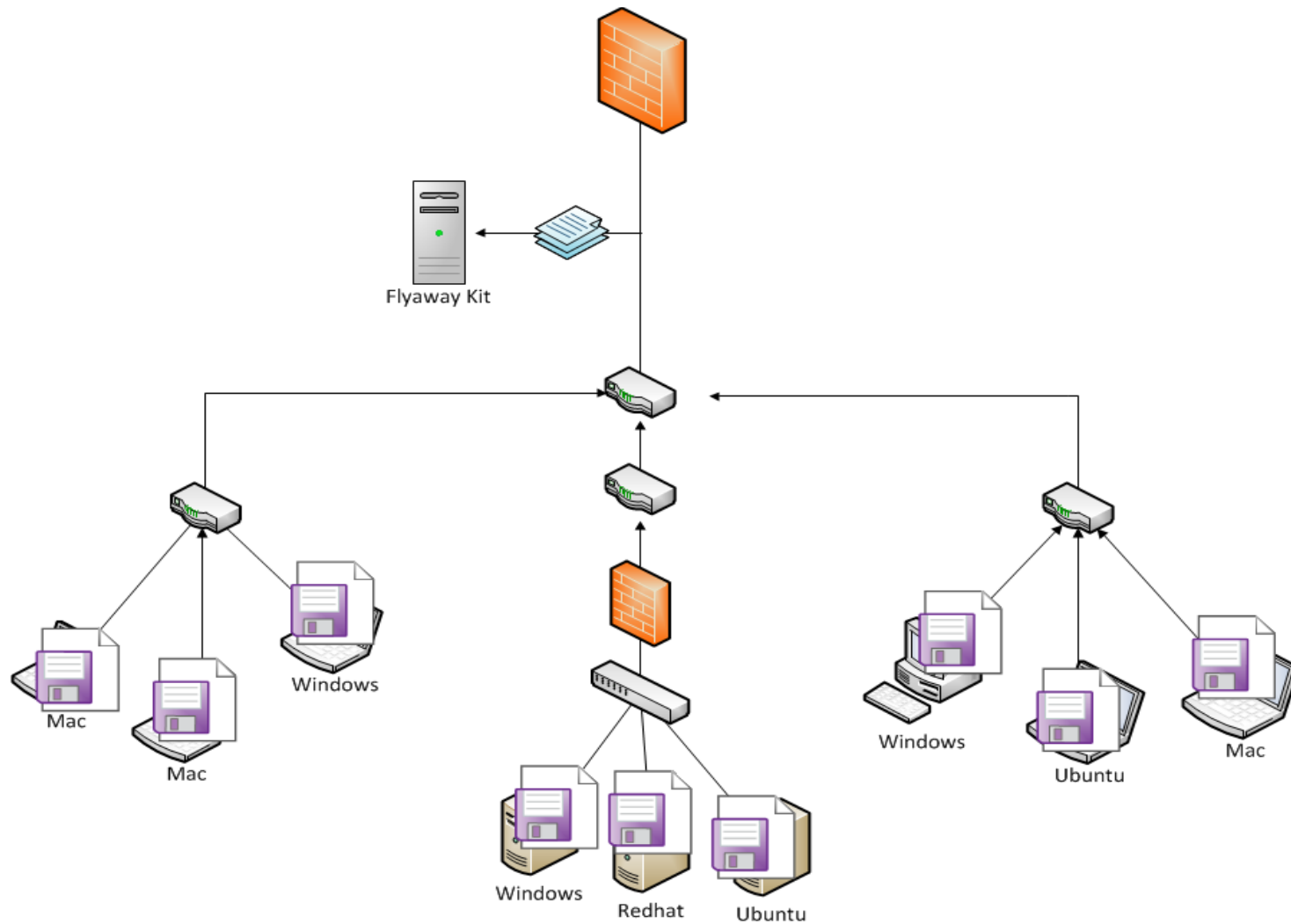
How do you fill the gaps?



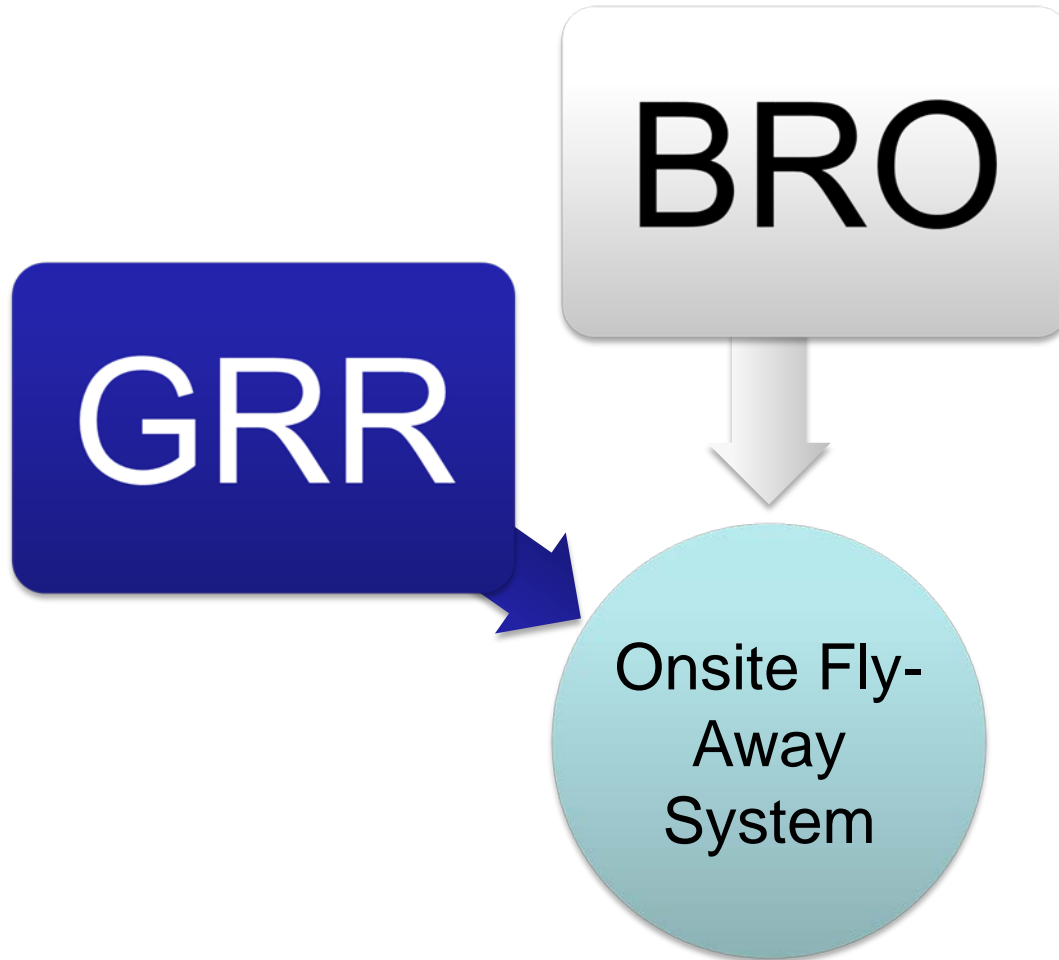
Bringing it all together



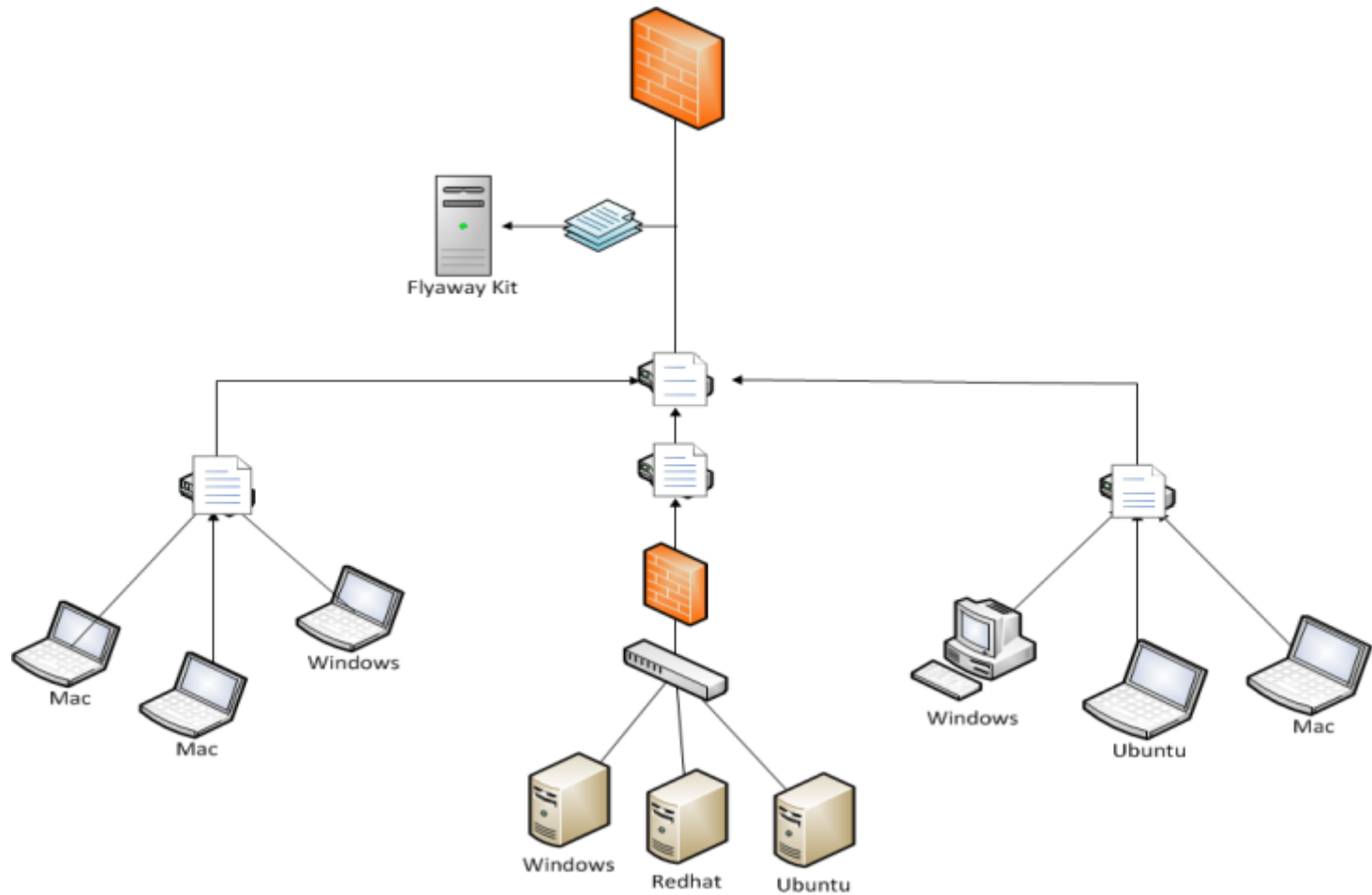
Bringing it all together



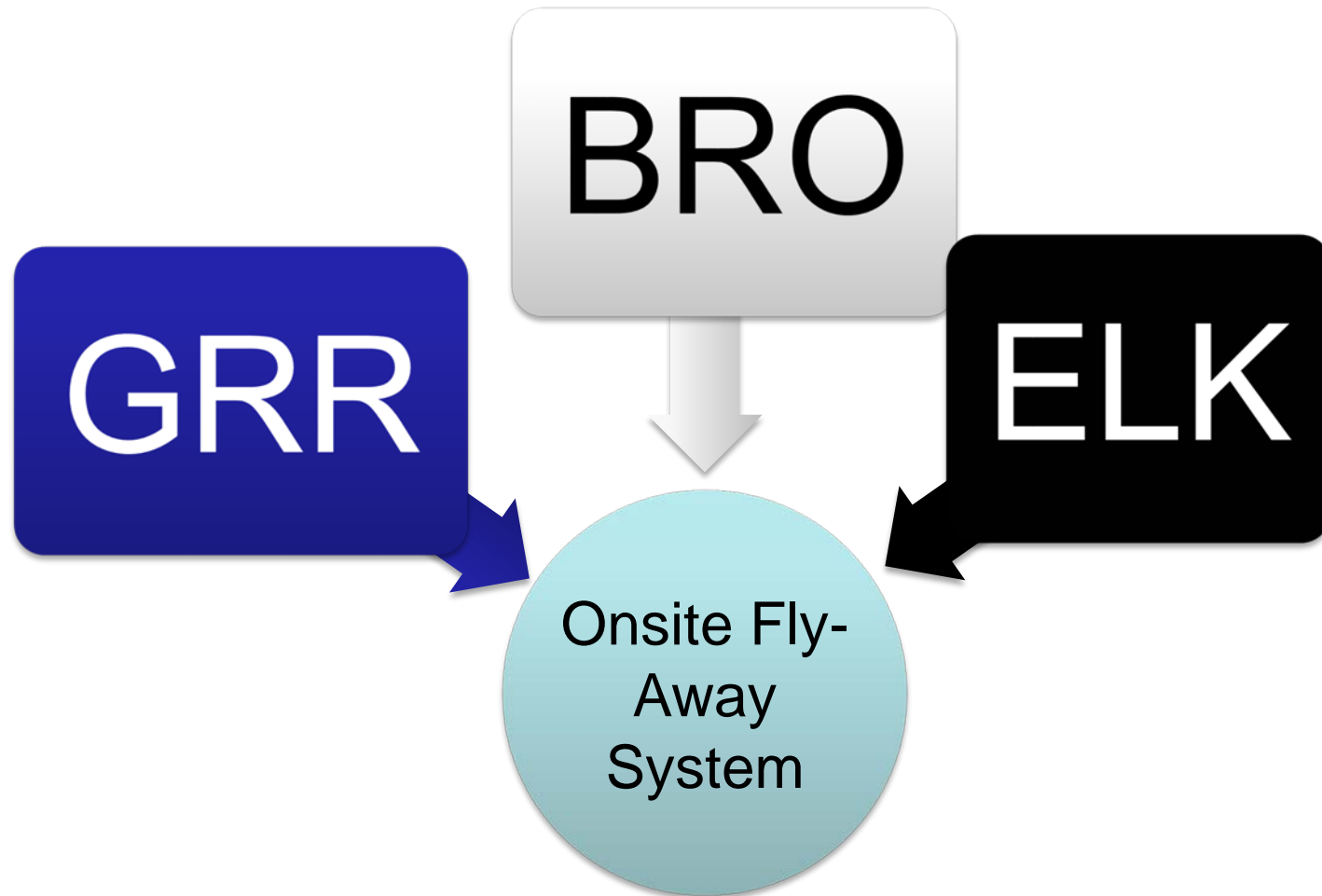
Bringing it all together



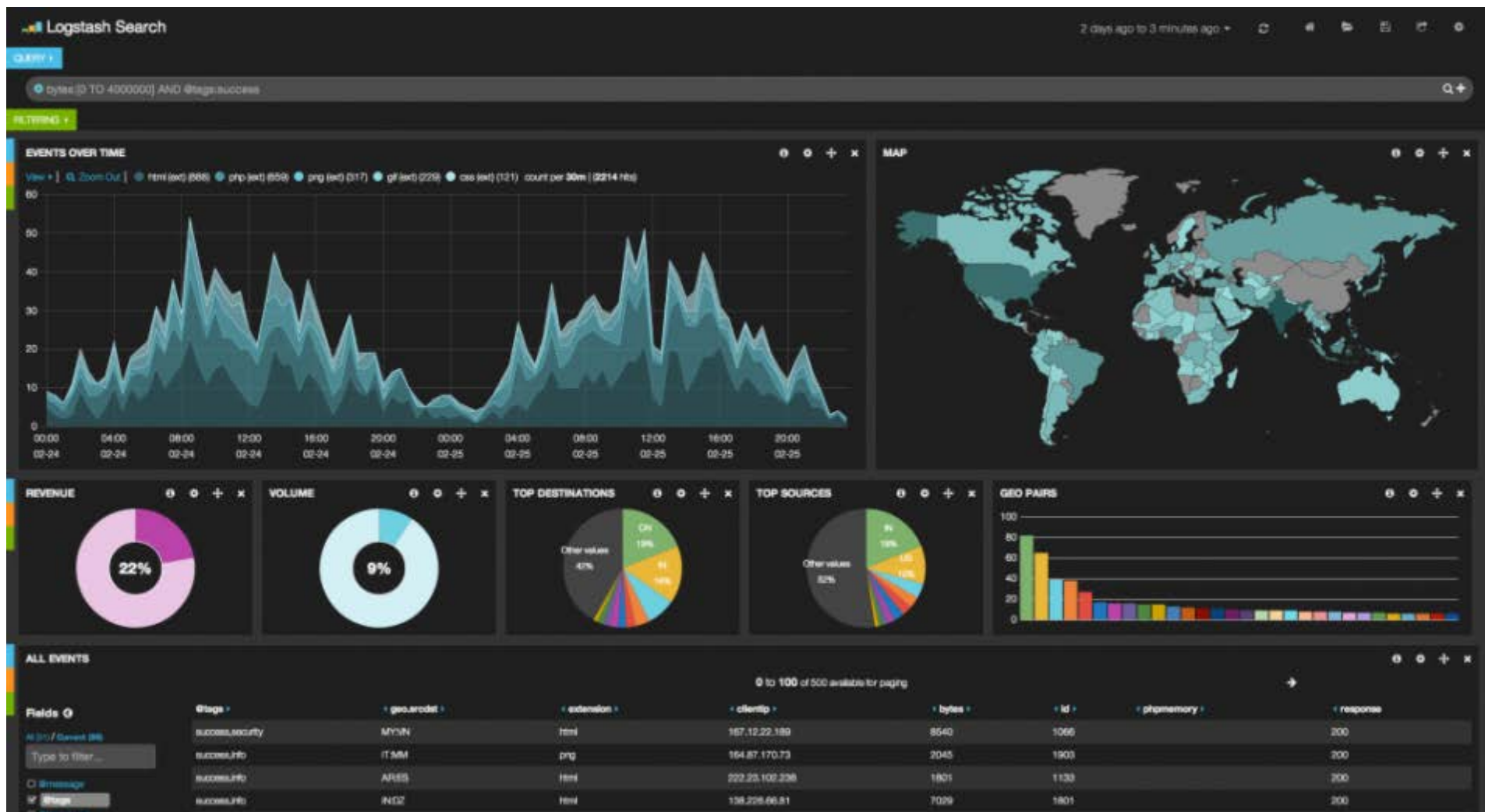
Bringing it all together



Bringing it all together



Visualize



Homeland Security

National Cybersecurity and Communications Integration Center

Contact info

<Insert contact info>



Homeland
Security

National Cybersecurity and
Communications Integration Center