Homeland Security

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

David Zito

Northrop Grumman
Information Systems

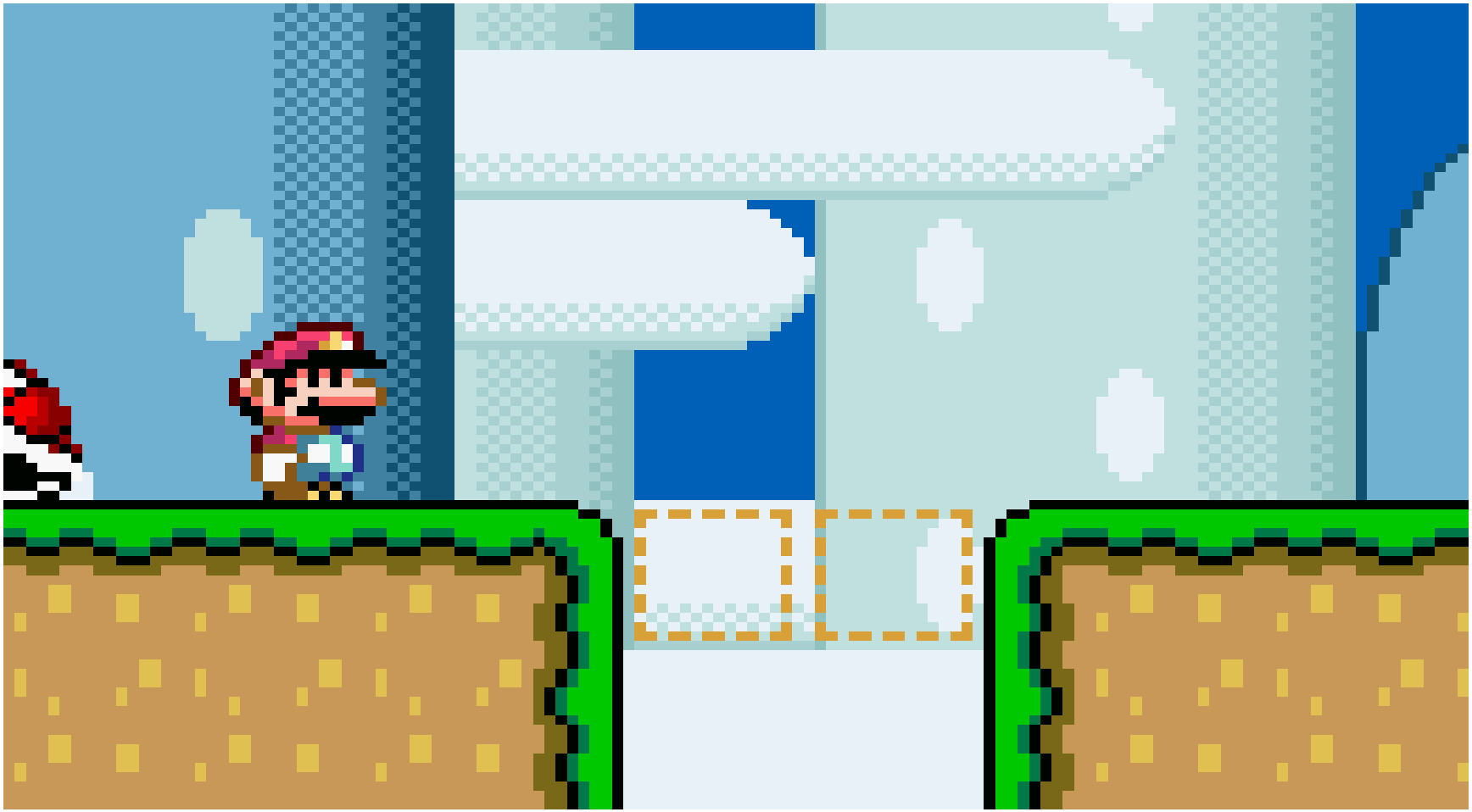
Outline

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

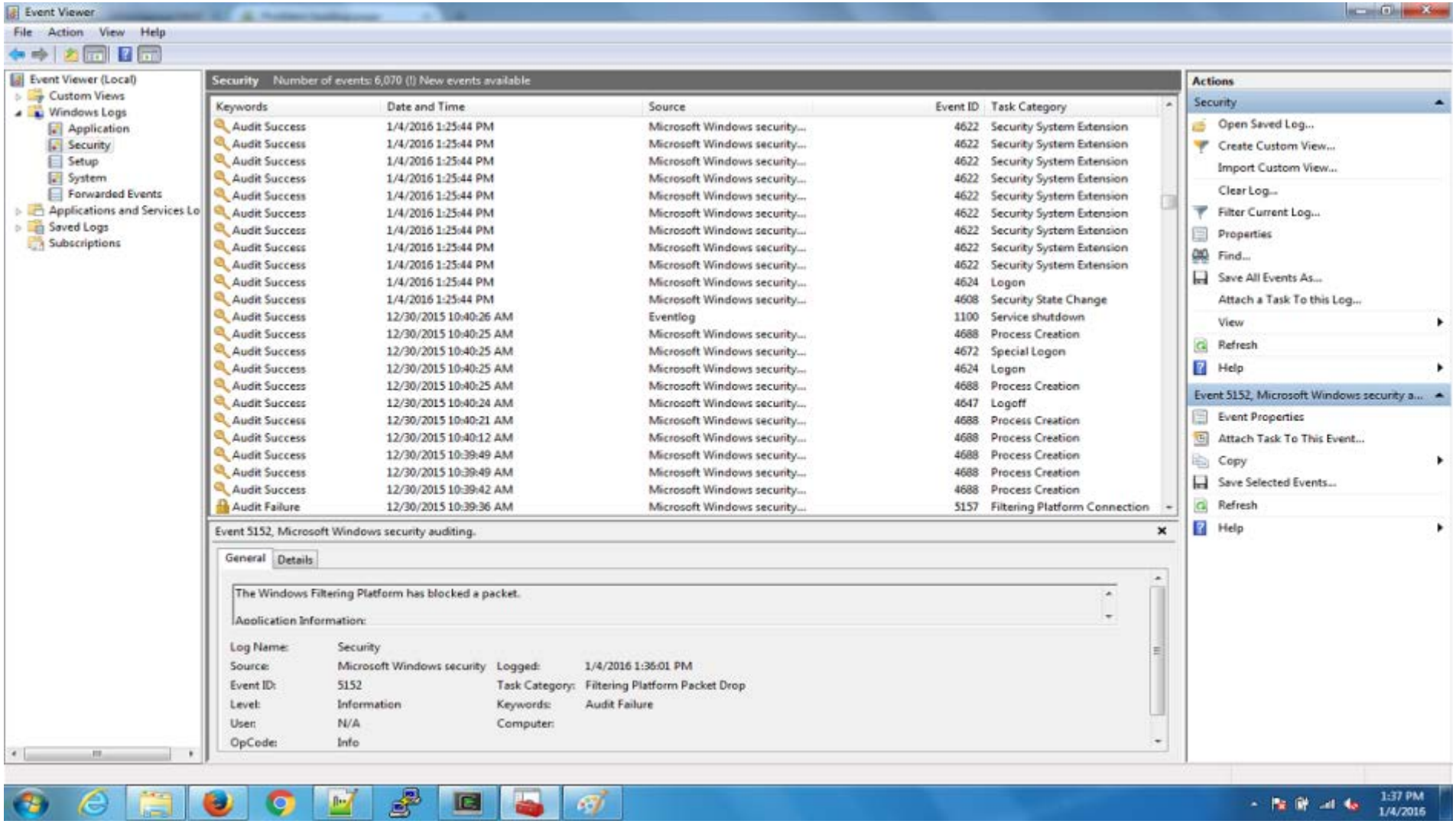
Introduction

<Insert “Who I am” bullets>

What is the gap?



What are these gaps? - EVT

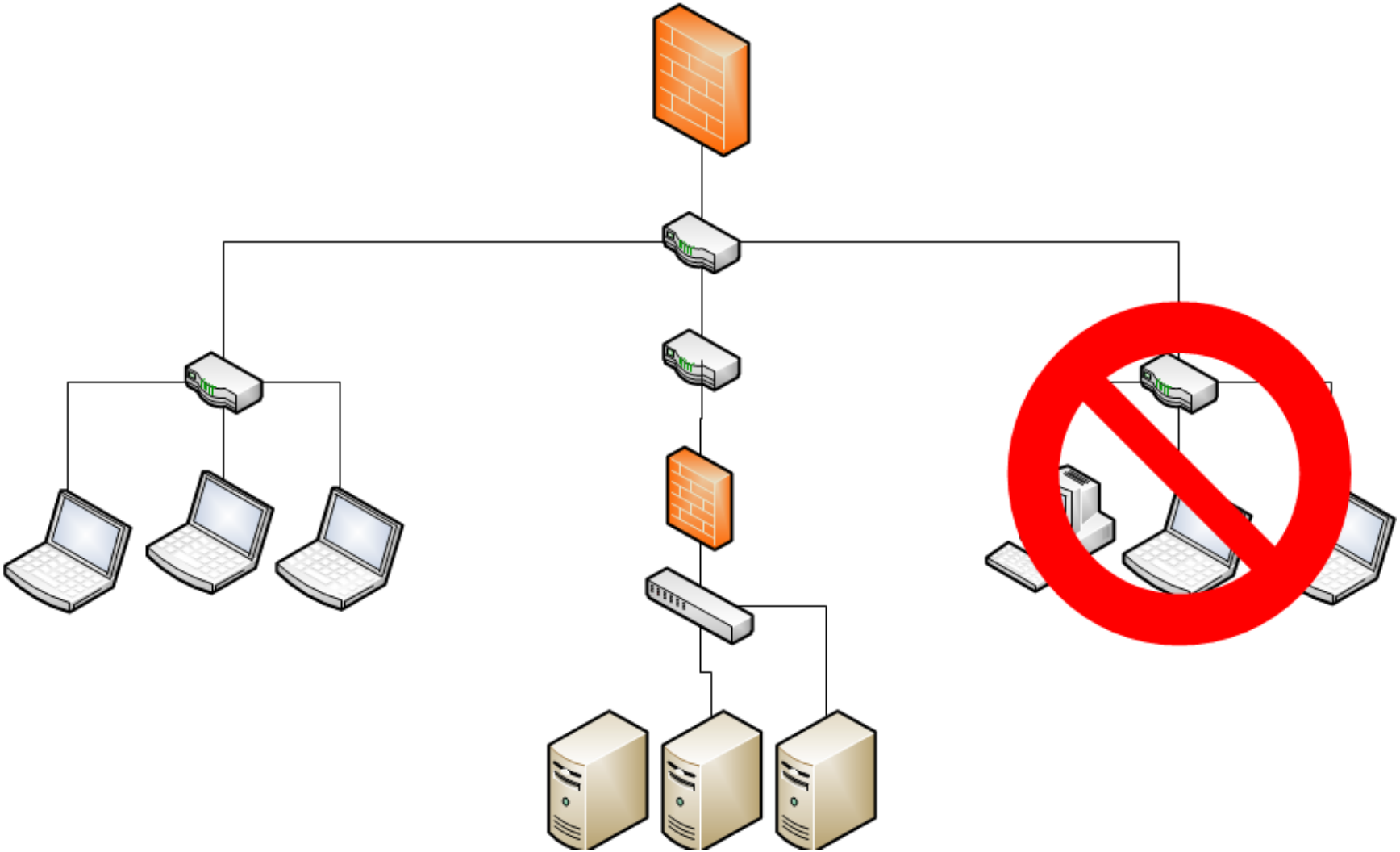


What are these gaps?Apache/IIS

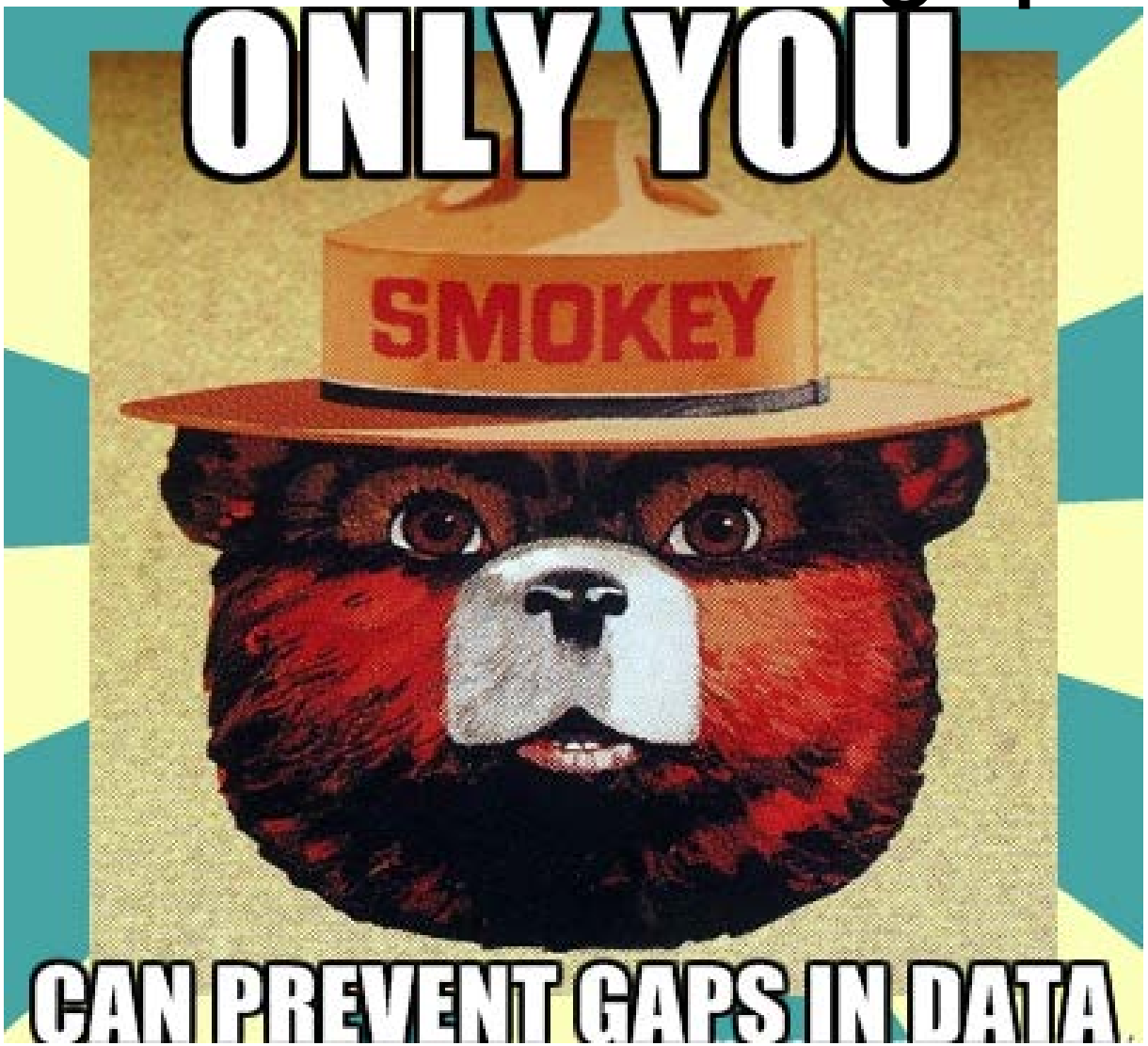
u_ex151208.log

```
#Software: Microsoft Internet Information Services 8.5
#Version: 1.0
#Date: 2015-12-08 18:47:44
#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
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
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
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
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
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
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
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
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
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
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/
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
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
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
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
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
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
2015-12-08 19:07:00 127.0.0.1 OPTIONS /share$/Applications/Workstation/VMwareWorkstation.msi - 80 - - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0)
2015-12-08 19:07:02 127.0.0.1 PROPFIND /share$/Applications/Workstation/VMwareWorkstation.msi - 80 - - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0
2015-12-08 19:07:04 127.0.0.1 PROPFIND /share$/Applications/Workstation - 80 - - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firef
2015-12-08 19:07:06 127.0.0.1 PROPFIND /share$/Applications/Workstation/VMwareWorkstation.msi - 80 - - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0
2015-12-08 19:07:09 127.0.0.1 PROPFIND /share$/Applications/Workstation - 80 - - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firef
2015-12-08 19:07:11 127.0.0.1 PROPFIND /share$/Applications/Workstation/VMwareWorkstation.msi - 80 - - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0
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
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
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
```

What are these gaps? – Netflow



What causes the gaps?



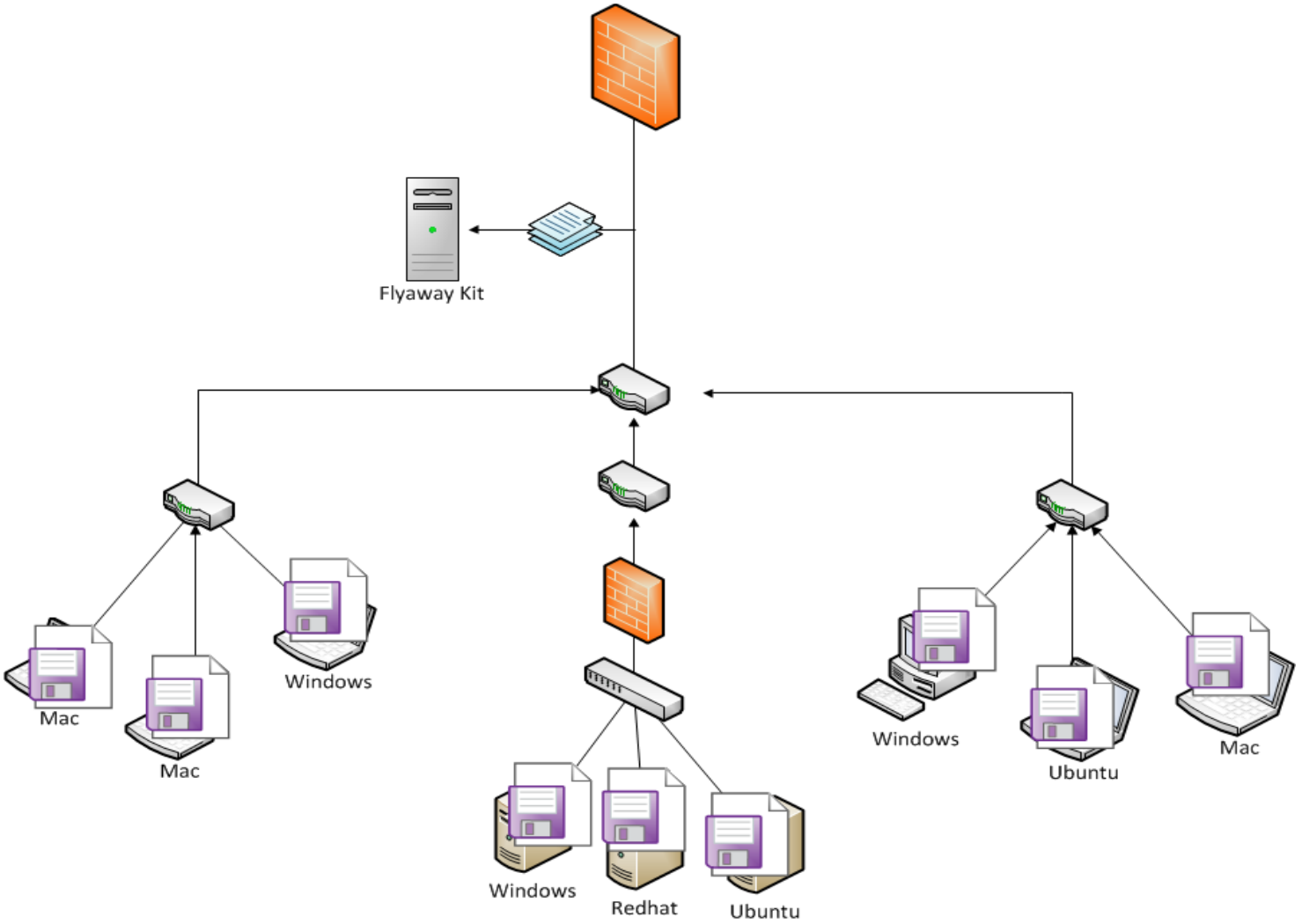
What causes the gap?

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

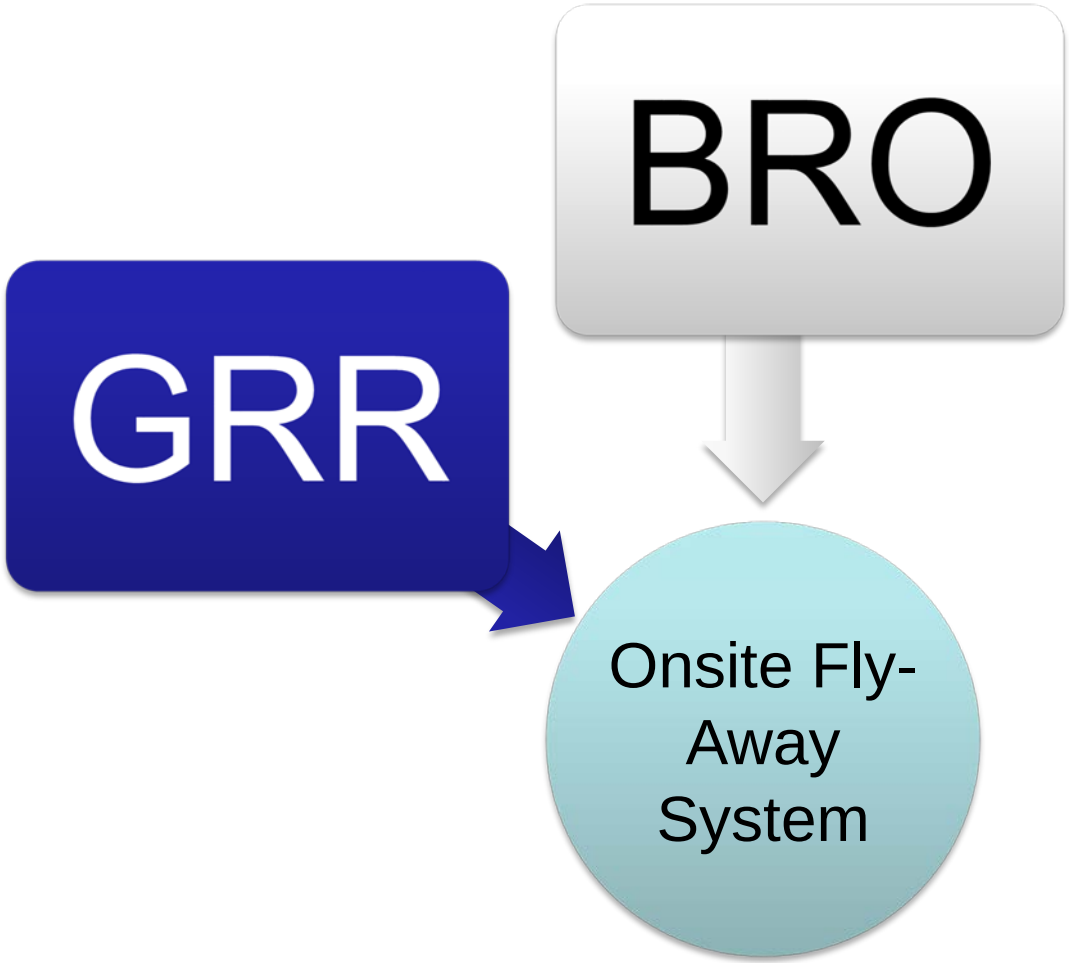
How do you fill the gaps?

Bringing it all together

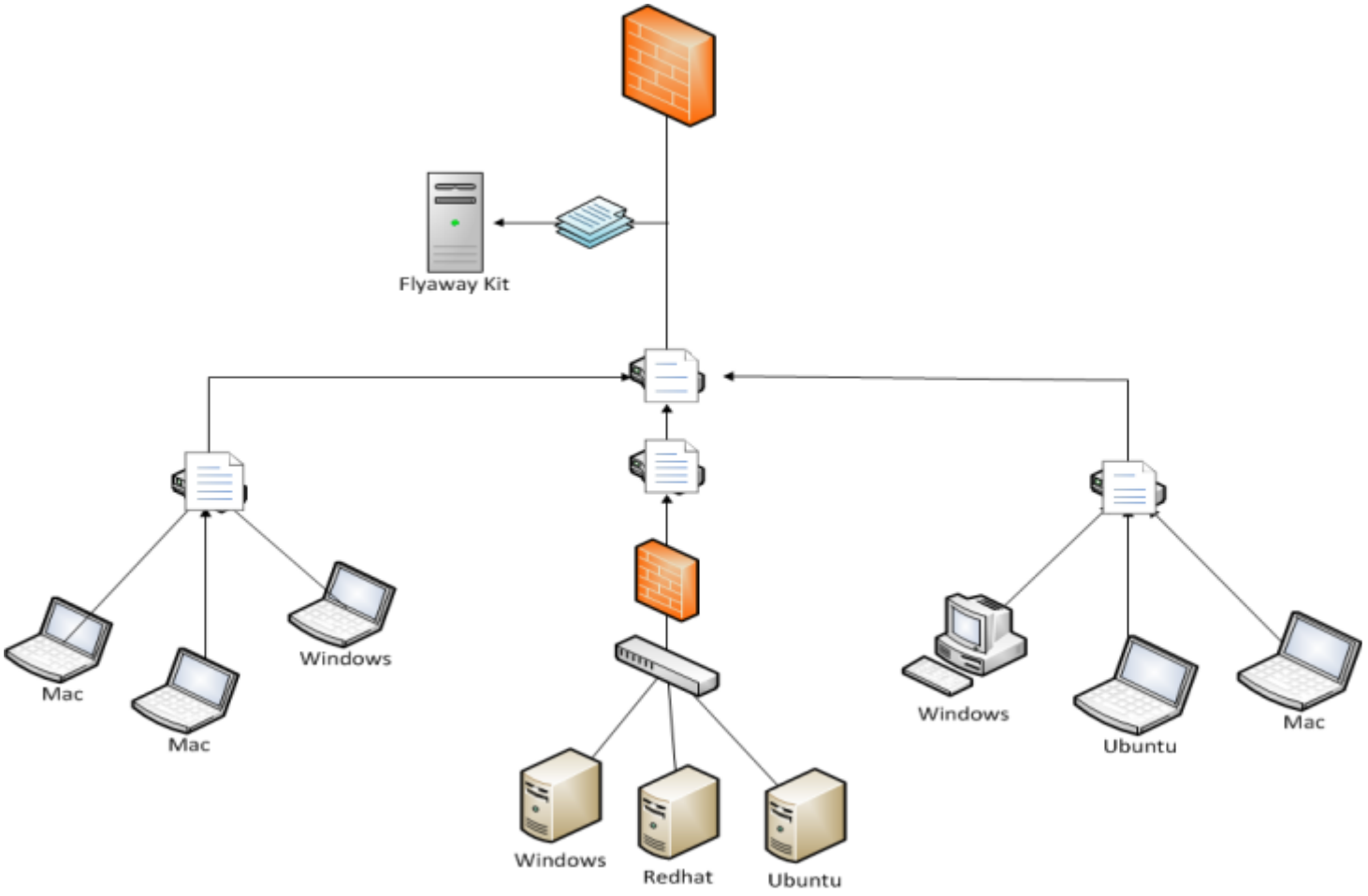
Bringing it all together



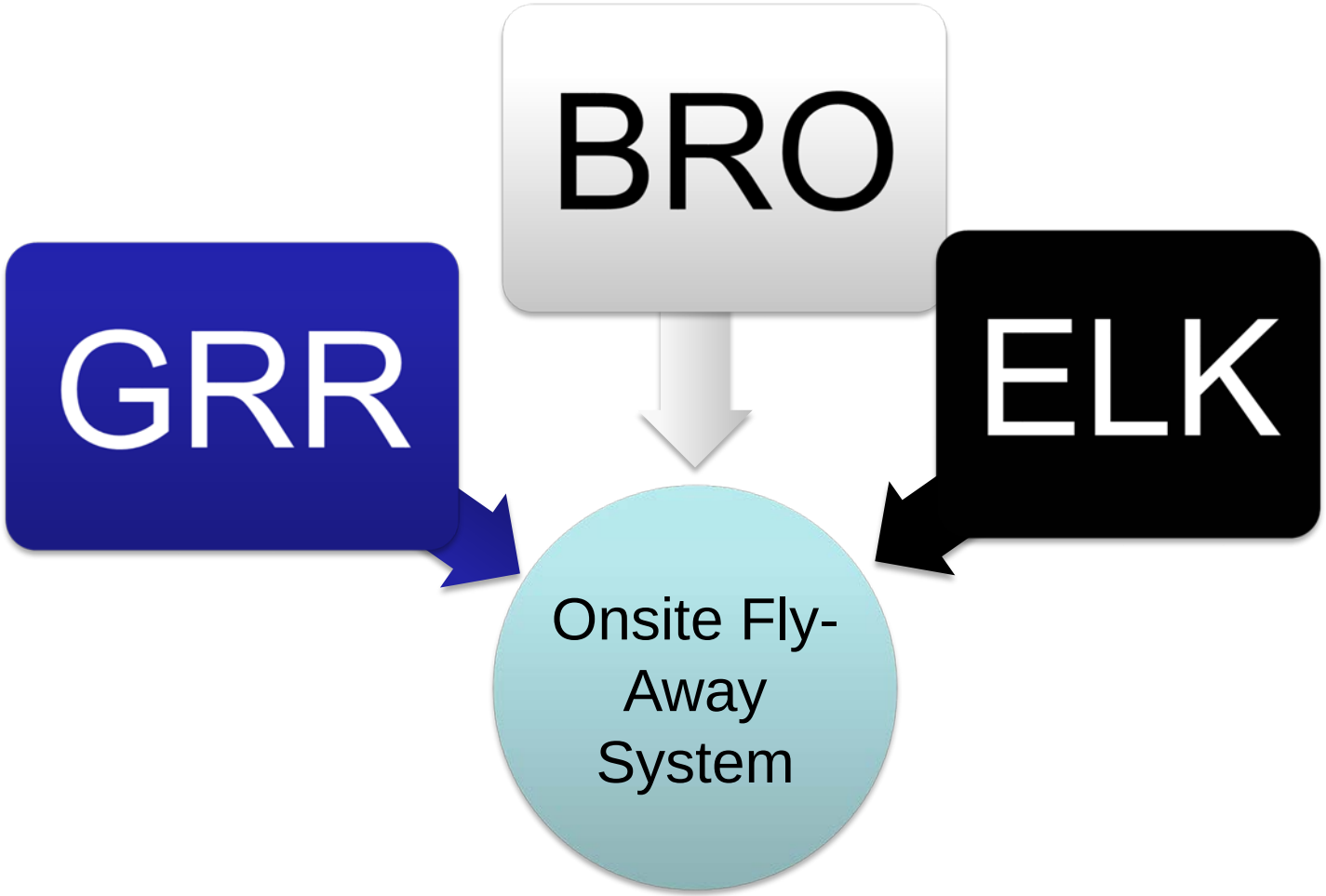
Bringing it all together



Bringing it all together



Bringing it all together



Visualize


Logstash Search
EVENTS OVER TIME
MAP
REVENUE
22%
VOLUME
9%
TOP DESTINATIONS
TOP SOURCES
GEO PAIRS
ALL EVENTS
Fields

Contact info

<Insert contact info>