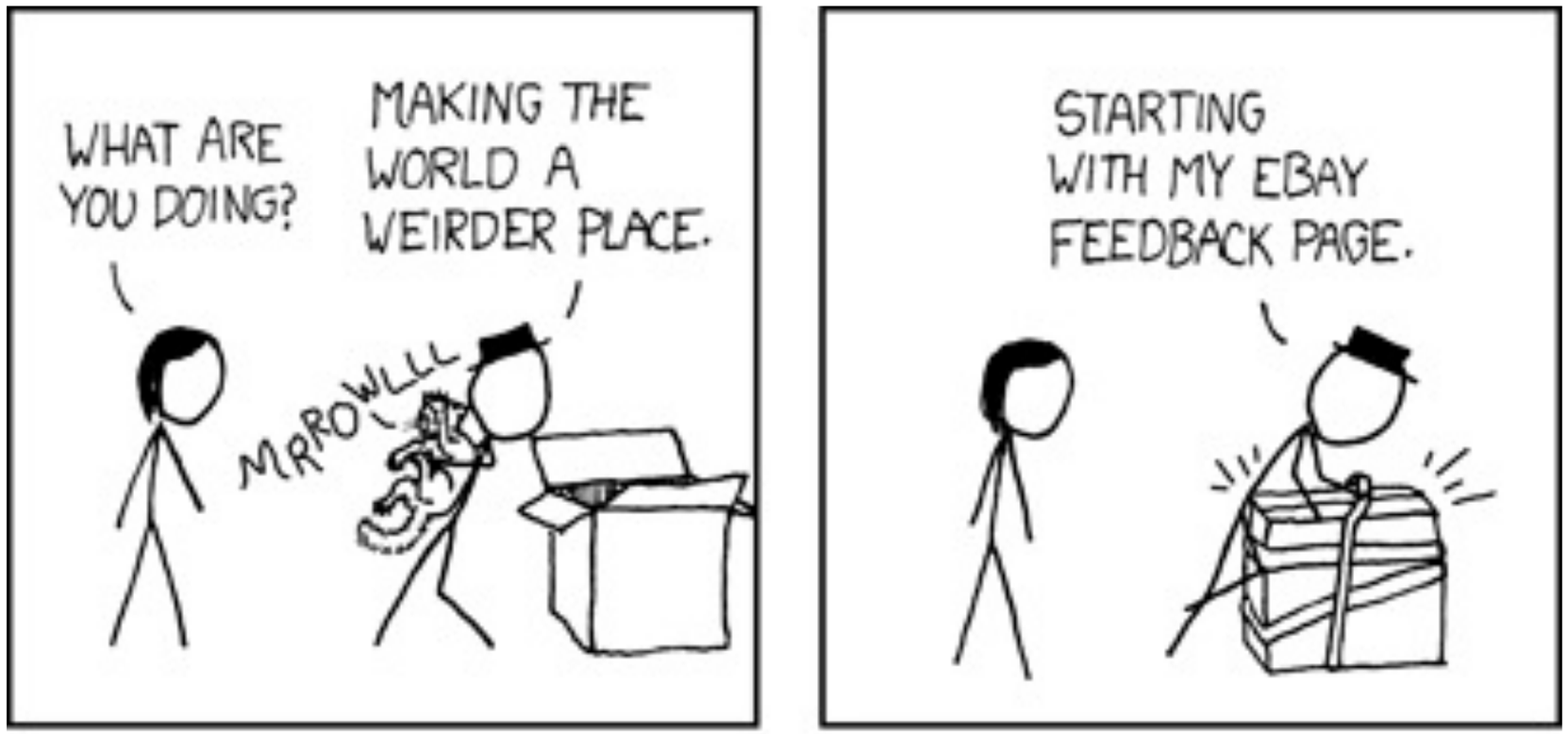


http://xkcd.com/325

Building Useful Security Infrastructure for Free

Now with more Madness!!

Who am I?

- Brad Lhotsky, Recovering Perl Programmer
  - "Information Security Manager"
  - System Administrator
  - Database Administrator
  - Keeper of the Codes
  - Raptor Herder

Who are YOU?

Where I work ..

Disclaimer: *The views presented here are almost certainly do* ***not*** *reflect the views of my Employer.*

S·E·C·U·R·I·T·Y

I've Locked Down My Host to the Point Where It'sUnusable

“I don’t care about security and never will. So do whatever you want, but make sure I know I’m better off with you employed”

What is “Useful Security” ?

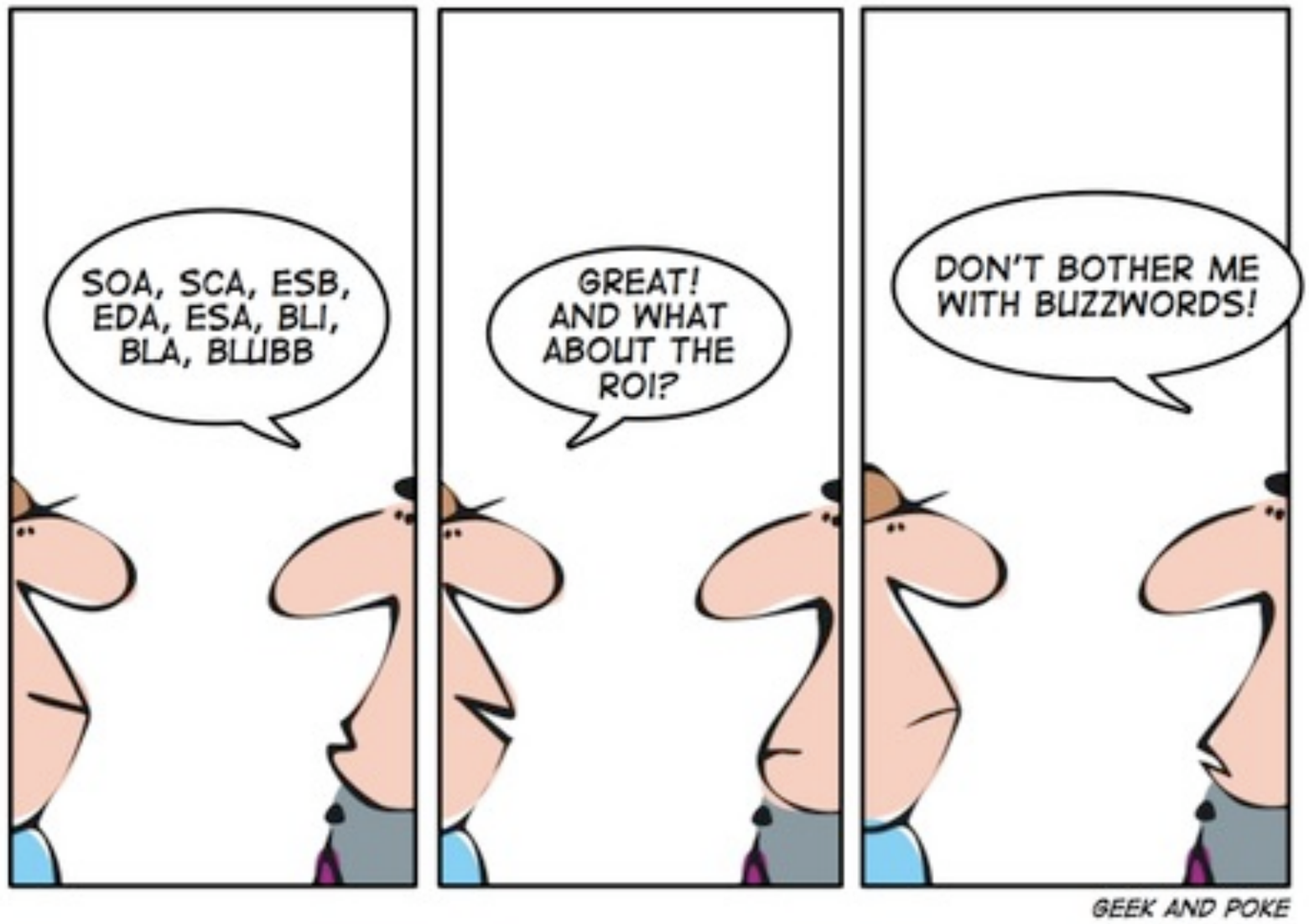
- Not security for the sake of security
- Solves Operations problems
- Makes business more efficient
- Meets requirements for Compliance to legislation:
  - PCI-DSS, SOX, HIPAA, FISMA

Why "Build" It?

Invest in Your Team

- Open Source encourages you to get into the nuts and bolts
- You learn more than just the software
  - Networking
  - Protocols
  - Operating Systems
- Promotes Cross Training

CEO & CFO want ROI



(Comic: Bill Hood)

Part Duex; Duexing It!

Complying, like a boss.

- Systems and Network Inventory
- Systems and Network Monitoring
- Accountability
  - Who is where, when, why, and how?

Paying Attention

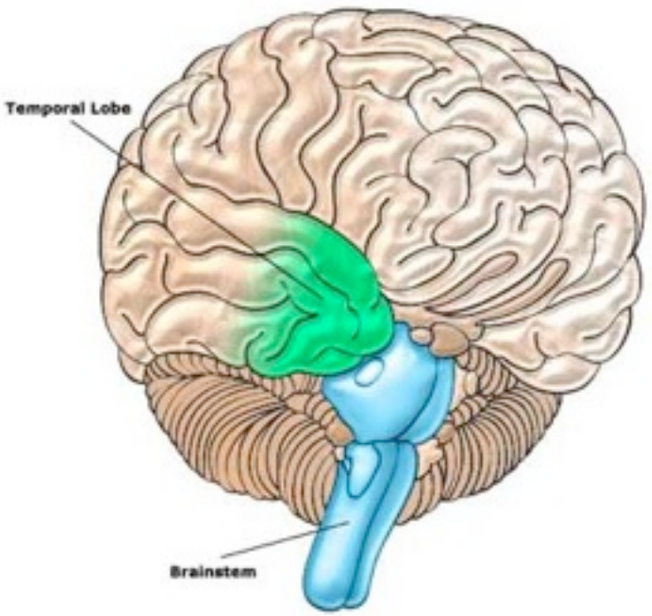
- Already have a great deal of information
- Just need to get into one Place
- Central Logging

syslog-ng

- Program destination
  - Started with syslog-ng daemon
  - Messages passed in to that program's STDIN
  - Allows Dynamic Programming Languages with high startup costs to be really quick
- Configuration syntax makes sense
- Caveat: Some features are not free

rsyslog

- All Open Source
- Supports Native Encryption via TLS
- Supports on-disk queueing for remote destinations
- Caveat: Configuration syntax is ugly



Long Term Memory

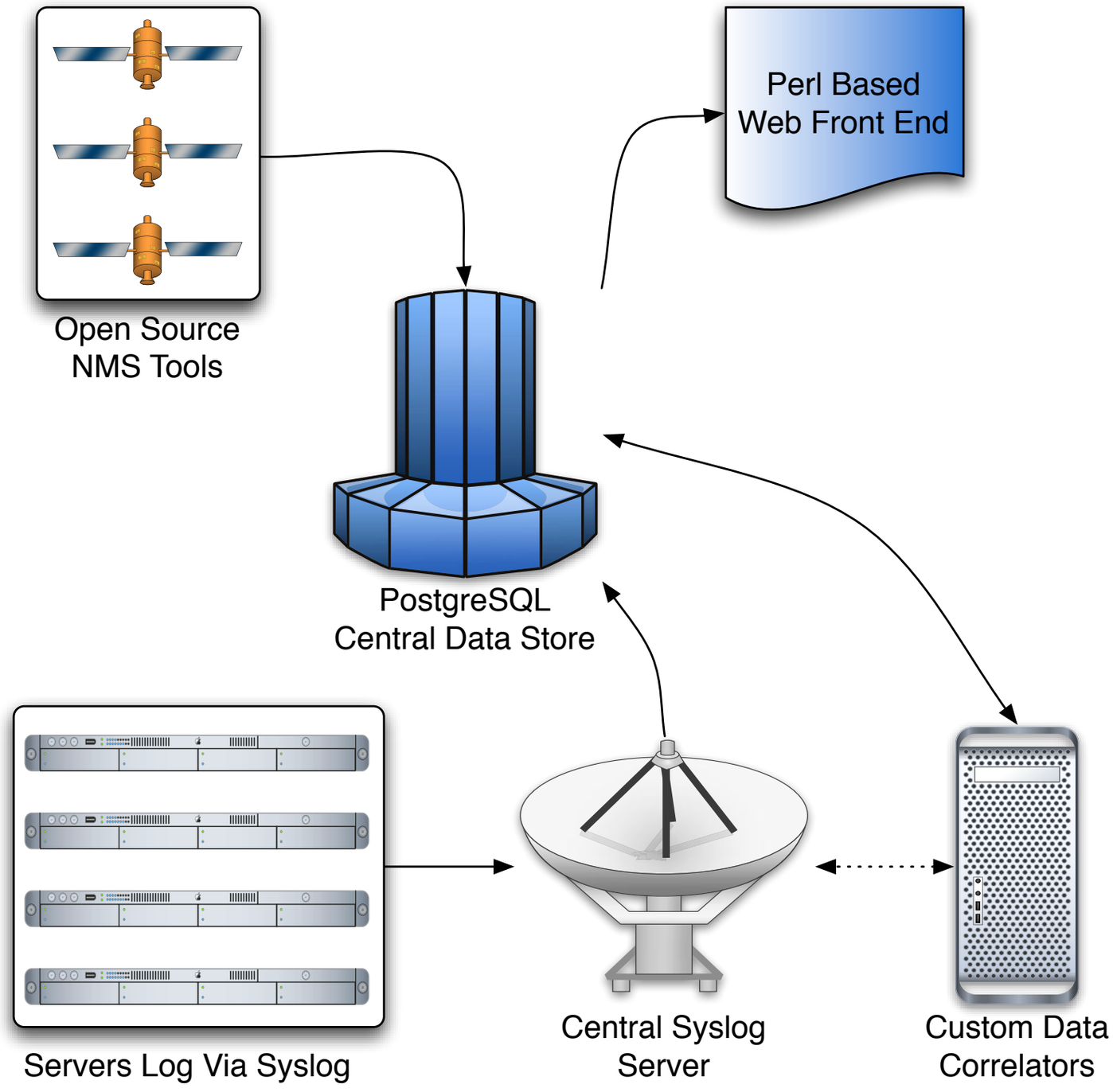
- Store our relational data with PostgreSQL
- ACID Compliant for Standards Compliance
- Support for Stored Procedures, Triggers, and Views
- Extensible via pgFoundry and PGXN
  - PL/R, PostGIS, ltree, etc ..

PostgreSQL : inet

Allows us to ask if an IP address in a certain range

```
SELECT * FROM node_history
 WHERE
   ip_address << inet ‘192.168.1.0/24’
```

Information Flow



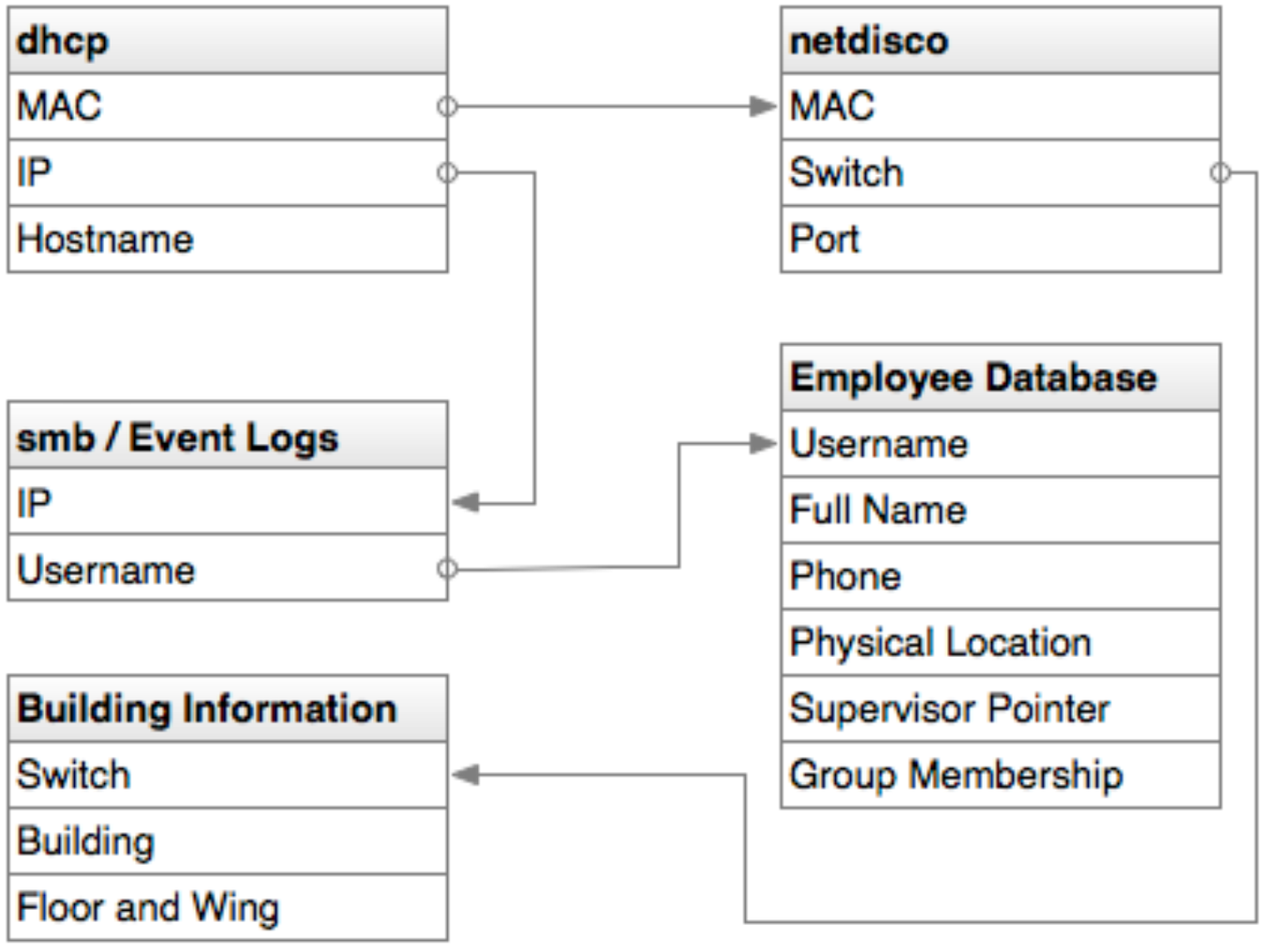
Getting Useful Data

- DHCP logs to syslog
  - MAC, IP, and Hostname
- Arpwatch logs to syslog
  - MAC, IP, and Hostname
- Netdisco stores data in PgSQL
  - MAC, Switch, and Port

Getting Useful Data

- Samba logs via syslog
  - IP and Username
- ActiveDirectory and LDAP for users
  - Username, Email, Phone #
- Custom Built App track Employee Data
  - Supervisor, Manager, Contractor POC

Data Relationships



Now it's easy to solve Operations Problems

Security Under the Veil of Utility

eris :: user list

main | dnsmgr | security | nodes | logout

network : search

filtered on 'lhotsky'

Show 10 entries Search:

First Name	Last Name	Username	Email	Last Login
April	Lhotsky	lhotskya	lhotskya@mail.nih.gov	2010-10-06
Brad	Lhotsky	lhotskyb	lhotskyb@mail.nih.gov	2010-10-06

Showing 1 to 2 of 2 entries

[nodes] Recently Discovered

- puje-pc
- niaosd-01626204
- niacrb-01742245
- nialcs-00000000
- nia-pc

Identify and Locate Users

eris :: network console

main | dnsmgr | security | nodes | logout

network :

User Details

Status : Active
Full Name : Brad Lhotsky
Email : lhotskyb@mail.nih.gov
Lab : IRP RRB
AD Last Logon : 2010-10-06T16:04:31
eris Roles : eris::admin, eris::login

Authentication History | User's Devices

Show 10 entries Search:

Device	Type	Last Seen	By
nia-syslog	Server	2010-10-07T18:10:04	netdisco
aphrodite	Workstation	2010-10-07T13:14:28	dhcpack
niancts-01778011	Workstation	2010-10-07T07:45:08	dhcpack
niancts-1743178	Laptop	2010-09-01T16:53:21	dhcpack
testing512	iPad	2010-08-20T14:19:37	manual
irpdns	Server	2010-07-30T20:49:26	arpwatch
niaunixcm	Server	2010-07-30T20:49:08	arpwatch
beholder	Server	2010-03-30T12:35:26	netdisco
handlsmrv	Server	2010-03-30T12:35:26	netdisco
oldhandlsdb	Server	2010-03-30T12:35:26	netdisco

Showing 1 to 10 of 16 entries

Get useful information on our users

eris :: view device overview

main | dnsmgr | security | nodes | logout

network : search

Device Details

Machine Name : niaunixcm
MAC : 00:15:60:0c:30:5c
Current IP : [redacted]
Switch Port : C2 @ BRCSHP541
Decal # :
Primary User : Brad Lhotsky
Discovered User : unknown
Functions : Edit Details

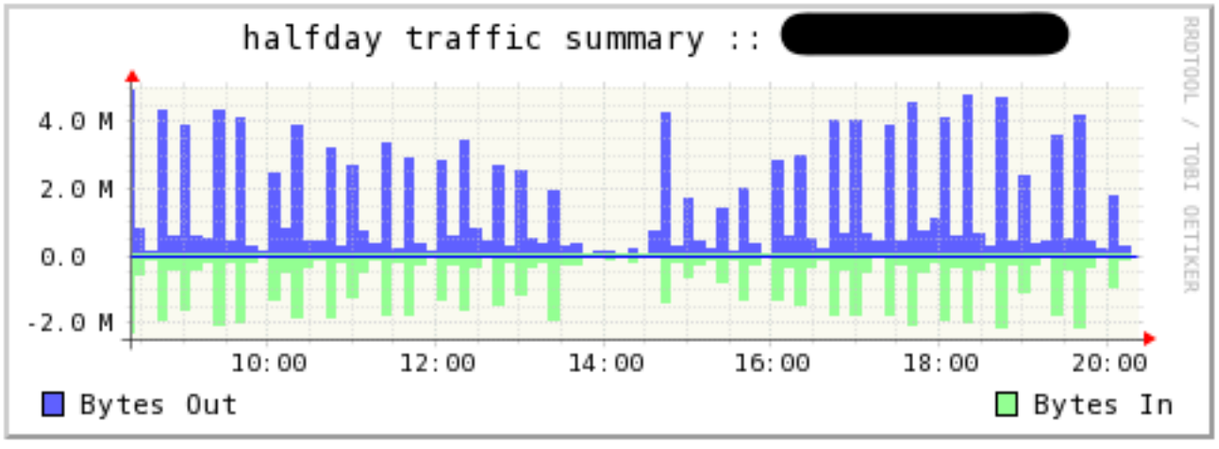
Services Active Recently

- tcp:22 @ external
- tcp:80 @ external
- tcp:443 @ external

[nodes] Recently Discovered

- puje-pc
- niaosd-01626204
- niacrb-01742245
- nialcs-00000000
- nia-pc

Network Traffic | Network History | Authentication History | Security Events



eris :: network console

main | dnsmgr | security | nodes | logout

network :

Show 25 entries Search:

Host	Start	End	Violations
niairpfiler1	2010-09-08 12:01:09	2010-10-08 11:16:00	169087
nialci-01068973	2010-09-09 13:03:42	2010-10-06 11:58:11	99705
securityrecorder	2010-09-10 13:23:49	2010-09-30 10:48:04	98697
niaosd-01577764	2010-09-08 11:50:34	2010-10-08 11:19:58	68875
lci-0028521288	2010-09-09 17:42:30	2010-10-01 18:30:42	66499
mousedbdev	2010-09-08 11:20:07	2010-10-08 11:17:20	62333
nialci-01541080	2010-10-01 21:36:30	2010-10-06 11:33:19	62049

Past 30 Days Events for niaunixcm

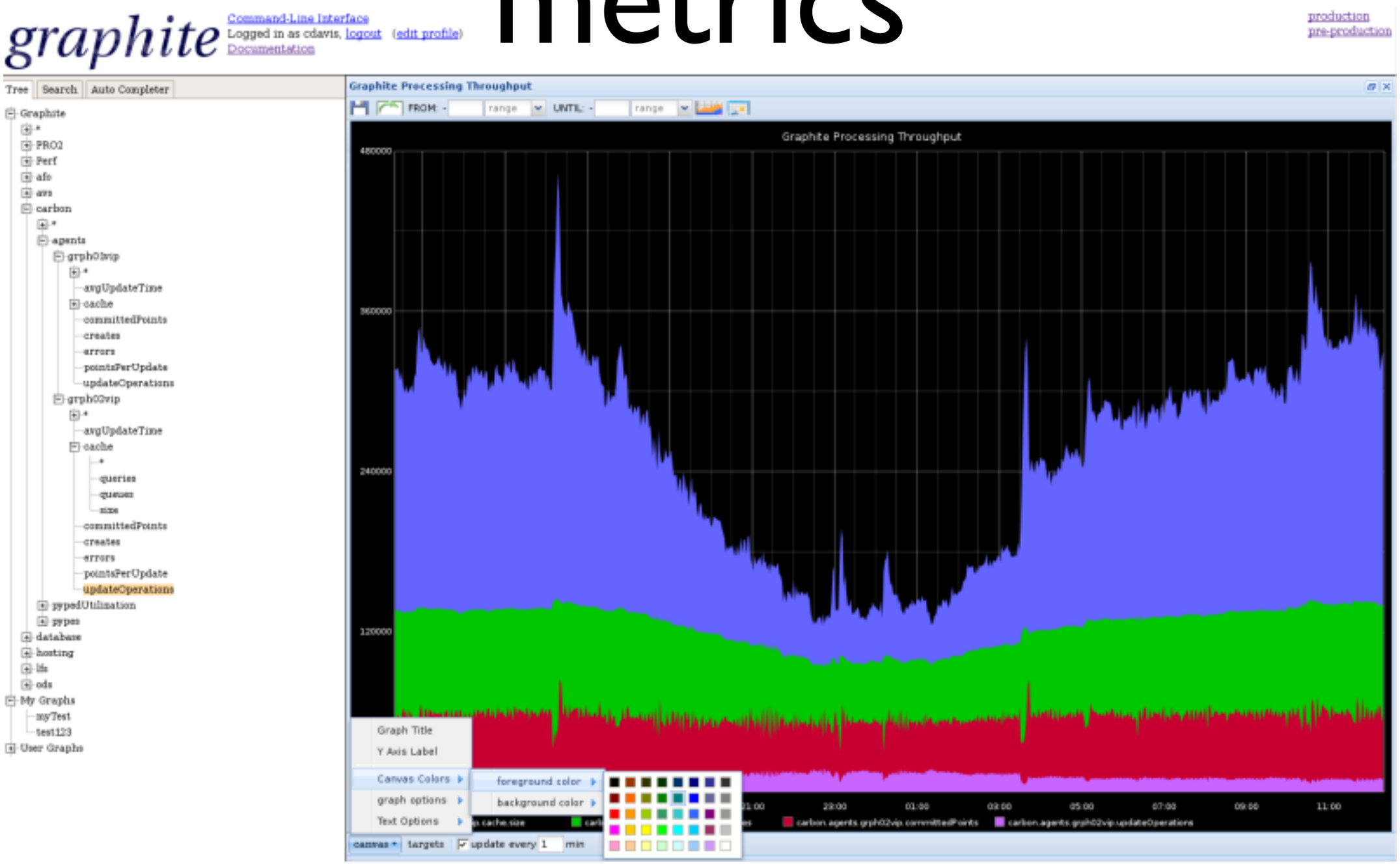
Signature Description	Violations
ET POLICY TLS/SSL Encrypted Application Data on Unusual Port	14700
ET POLICY Unusual number of DNS No Such Name Responses	4216
ET POLICY Outbound TFTP Read Request	190
DNS SPOOF query response with TTL of 1 min. and no authority	22
ET ATTACK_RESPONSE HTTP 401 Unauthorized	1

nialci-2762181	2010-09-20 10:59:24	2010-10-07 15:39:17	30209
niairpfiler1	2010-09-28 06:23:07	2010-10-07 05:10:40	26896
niamds-01566197	2010-09-09 15:49:33	2010-10-07 14:37:19	26496
vnetmon	2010-09-08 11:26:28	2010-10-08 11:12:20	22638
niaunixcm	2010-09-08 11:20:07	2010-10-08 11:10:55	19106
niairphome	2010-09-14 16:00:47	2010-10-08 10:59:08	15213
cvpm167	2010-09-08 11:26:19	2010-10-08 10:45:33	12784

Showing 1 to 25 of 346 entries

a few other tricks ..

do something cool w/ metrics



cool deploy macros via Puppet

```
subversion::deploy { 'project':
  owner => apache,  group => apache,
  svnurl => 'svn+ssh://svn/repo/project',
  target => '/var/www/project',
  notify => Service['httpd']
}
```

This satisfies "Change Management" Requirements

https://github.com/reyjrar/svnutils

http://ossec.net

"OSSEC is a scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS). It has a powerful correlation and analysis engine, integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response.

It runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows."

- Policy Compliance
  - Exceeds current logging recommendations
- Open Source Software
  - #ossec on irc.freenode.net
- Great functionality
  - Distributed Active Response
  - WebUI

Thank you!

brad.lhotsky@gmail.com
https://twitter.com/reyjrar
https://github.com/reyjrar