Devops, Secops, Opsec, DevSec *ops *.* ?

Kris Buytaert
OWASP Belgium

Kris Buytaert

- I used to be a Dev,
- Then Became an Op
- Even did Security (OSSTM etc)
- Chief Trolling Officer and Open Source Consultant @inuits.eu
- Everything is an effing DNS Problem
- Building Clouds since before the bookstore
- Some books, some papers, some blogs
- But mostly, trying to be good at my job

Devop, definition

- 30 something
- Senior Infrastructure guy
- Development background
- Open Source Expcerience
- Mostly European (.be / .uk)
- Likes Belgian Beer
- Likes Sushi

What's this Devops thing really about ?

World , 200X-2009

Patrick Debois, Gildas Le Nadan, Andrew Clay Shafer, Kris Buytaert, Jezz Humble, Lindsay Holmwood, John Willis, Chris Read, Julian Simpson, and lots of others ..

Gent , October 2009

Mountain View , June 2010

Hamburg , October 2010

Boston, March 2011

Mountain View, June 2011

Bangalore, Melbourne,

Goteborg , October 2011

- Devops is a growing movement
- We don't have all the answers yet
- We are reaching out to different communities
- We will point out problems we see..
- Only the name is new

While we are still working out the solutions

What's the problem ?

The community of developers whose work you see on the Web, who probably don’t know what ADO or UML or JPA even stand for, deploy better systems at less cost in less time at lower risk than we see in the Enterprise. This is true even when you factor in the greater flexibility and velocity of startups.

Tim Bray , on his blog January 2010

- Adopt the new philosophy. We are in a new economic age. Western management must awaken to the challenge, must learn their responsibilities, and take on leadership for change.
- Cease dependence on inspection to achieve quality. Eliminate the need for massive inspection by building quality into the product in the first place.
- Improve constantly and forever the system of production and service, to improve quality and productivity, and thus constantly decrease costs.
- Institute training on the job.
- Institute leadership The aim of supervision should be to help people and machines and gadgets do a better job.
- Drive out fear, so that everyone may work effectively for the company.
- Break down barriers between departments. People in research, design, sales, and production must work as a team, in order to foresee problems of production and usage that may be encountered with the product or service.
- Eliminate slogans, exhortations, and targets for the work force asking for zero defects and new levels of productivity. Such exhortations only create adversarial relationships, as the bulk of the causes of low quality and low productivity belong to the system and thus lie beyond the power of the work force.
- Eliminate management by objective. Eliminate management by numbers and numerical goals. Instead substitute with leadership.
- Remove barriers that rob the hourly worker of his right to pride of workmanship. The responsibility of supervisors must be changed from sheer numbers to quality.
- Remove barriers that rob people in management and in engineering of their right to pride of workmanship.
- Institute a vigorous program of education and self-improvement.
- Put everybody in the company to work to accomplish the transformation. The transformation is everybody's job.

William Edwards Deming

1986, Out of the Crisis.

http://en.wikipedia.org/wiki/W._Edwards_Deming

CAMS

- Culture
- Automation
- Measurement
- Sharing

Damon Edwards and John Willis

“DevOps is a cultural and professional movement”

Adam Jacob

How did we get here ?

The Old Days

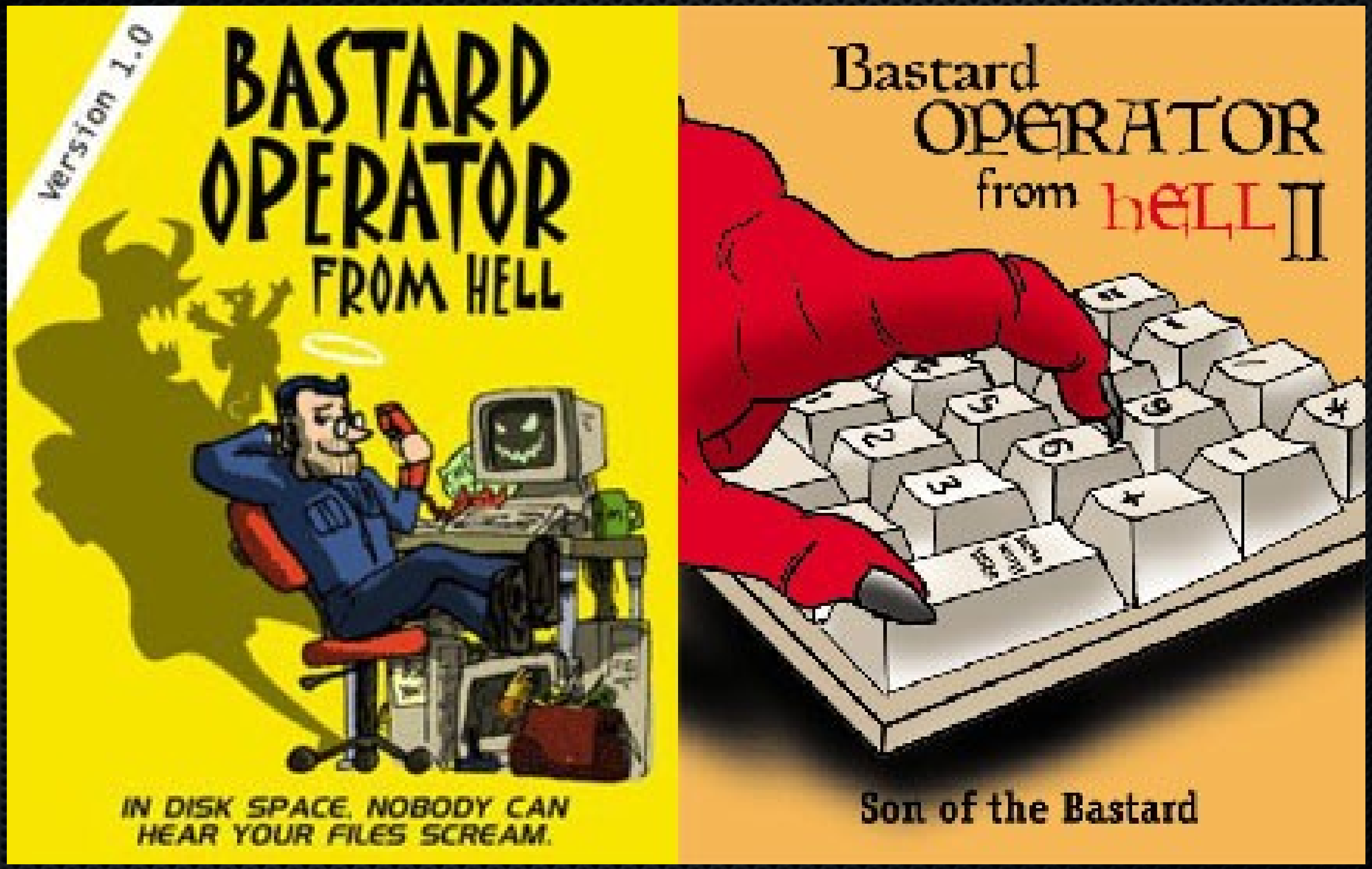
- “Put this Code Live, here's a tarball” NOW!
- What dependencies ?
- No machines available ?
- What database ?
- Security ?
- High Availability ?
- Scalability ?
- My computer can't install this ?

Devs vs Ops

People hate Sysadmins

Because

- They slow stuff down
- The say no
- They say no again
- They refuse to break stuff
- They care about uptime
- They don't care about fancy new features


version 1.0
BASTARD OPERATOR FROM HELL
IN DISK SPACE, NOBODY CAN HEAR YOUR FILES SCREAM.
Bastard OPERATOR from hELL II
Son of the Bastard

People hate Security Officers

Because

- They slow stuff down
- The say no
- They say no again
- They refuse to leave holes open
- They care about security
- They don't care about fancy new features
- Security Officers have an expiry date


BSOFH

10 days into operation

- What High Load ? What Memory usage ?
- Are these Logs ? Or this is actualy customer data ?
- How many users are there , should they launch 100 queries each ?? Oh we're having 10K users
- Why is debugging enabled ?
- Who wrote this ?

11 days into operations

12 days into operations

13 days into operations

We can solve this !

- We are not here to block
- Some people think the Security / Operations work starts on deployment
- It starts much earlier
- Start talking asap

Talk about Non functional Reqs NOW!

- Security
- Backups
- High Availability
- Upgradability
- Deployment
- Monitoring
- Scale

Breaking the Silos

Devs Ops Getting Along

Nirvana

An “ecosystem” that supports continuous delivery, from infrastructure, data and configuration management to business.

Through automation of the build, deployment, and testing process, and improved collaboration between developers, testers, and operations, delivery teams can get changes released in a matter of hours — sometimes even minutes–no matter what the size of a project or the complexity of its code base.

Continuous Delivery , Jez Humble

How many times a day ?

- 10 @ Flickr
- Deployments used to be pain
- Nobody dared to deploy a site
- Practice makes perfect
- Knowing you can vs constantly doing it

" Our job as engineers (and ops, dev-ops, QA, support, everyone in the company actually) is to enable the business goals. We strongly feel that in order to do that you must have the ability to deploy code quickly and safely. Even if the business goals are to deploy strongly QA'd code once a month at 3am (it's not for us, we push all the time), having a reliable and easy deployment should be non-negotiable."

Etsy Blog upon releasing Deployinator

http://codeascraft.etsy.com/2010/05/20/quantum-of-deployment/

How do we get there ?

Continuous Integration

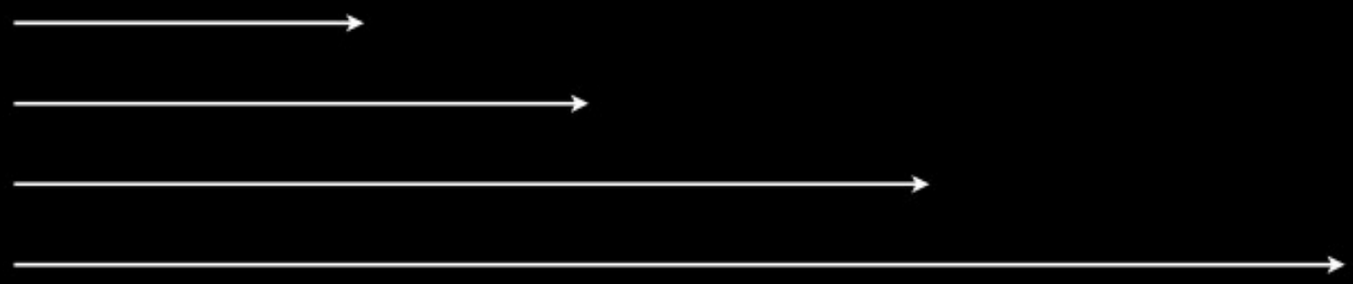
- If it's hard do it more often

CI Tools

- ~~Hudson~~
- Jenkins
- A zillion plugins
- Make your builds reproducible !
- Test your (Puppet/Chef/CFengine)

Build Pipelines

DEV TEST UAT PREPROD PROD

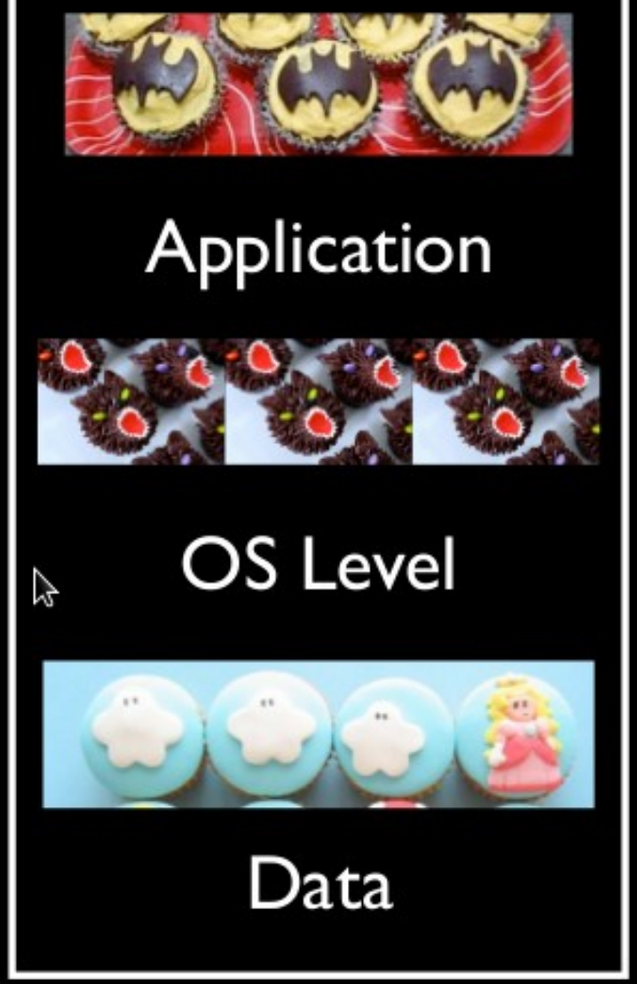


Parallel Build Pipelines

Software Build & Test

Infrastructure Build & Test

Data Build & Test



Make all environments the same

DEV TEST PROD

Todays Enviroments

For Devs

- Scrum
- Version Control
- Automated Build
- Bugtracking
- Continous integration
- Integrated testing
- Automated deployment

For Ops

- Kanban
- Version Control
- Automated Build
- Bugtracking
- Continous integration
- Integrated testing
- Automated deployment

Everybody is a developer

- Yes we write code also
- Httpd.conf, squid.conf, my.cnf
- Just crappy languages :)
- Shell, perl, ruby, python, puppet
- Everyone is a developer these days
- Automate your infrastructure !
- So those rules apply for Everyone

Deploying

- Automated Deployments
- “If my computer can't install it , the installer is borken” Luke at Fosdem (200X)
- Reproducable
- Think:
- Kickstart, FAI, Preseeding, SystemImager Suite

Looking for ?

“As a system administrator, I can tell when software vendors hate me. It shows in their products.”

“DON'T make the administrative interface a GUI. System administrators need a command-line tool for constructing repeatable processes. Procedures are best documented by providing commands that we can copy and paste from the procedure document to the command line. We cannot achieve the same repeatability when the instructions are: "Checkmark the 3rd and 5th options, but not the 2nd option, then click OK." Sysadmins do not want a GUI that requires 25 clicks for each new user.”

Thomas A. Limoncelli in ACM Queue December 2010

http://queue.acm.org/detail.cfm?id=1921361

How do security tools score ?

- Very little (security) vendors succeed at this
- Automation is key
- Plenty of #Fail

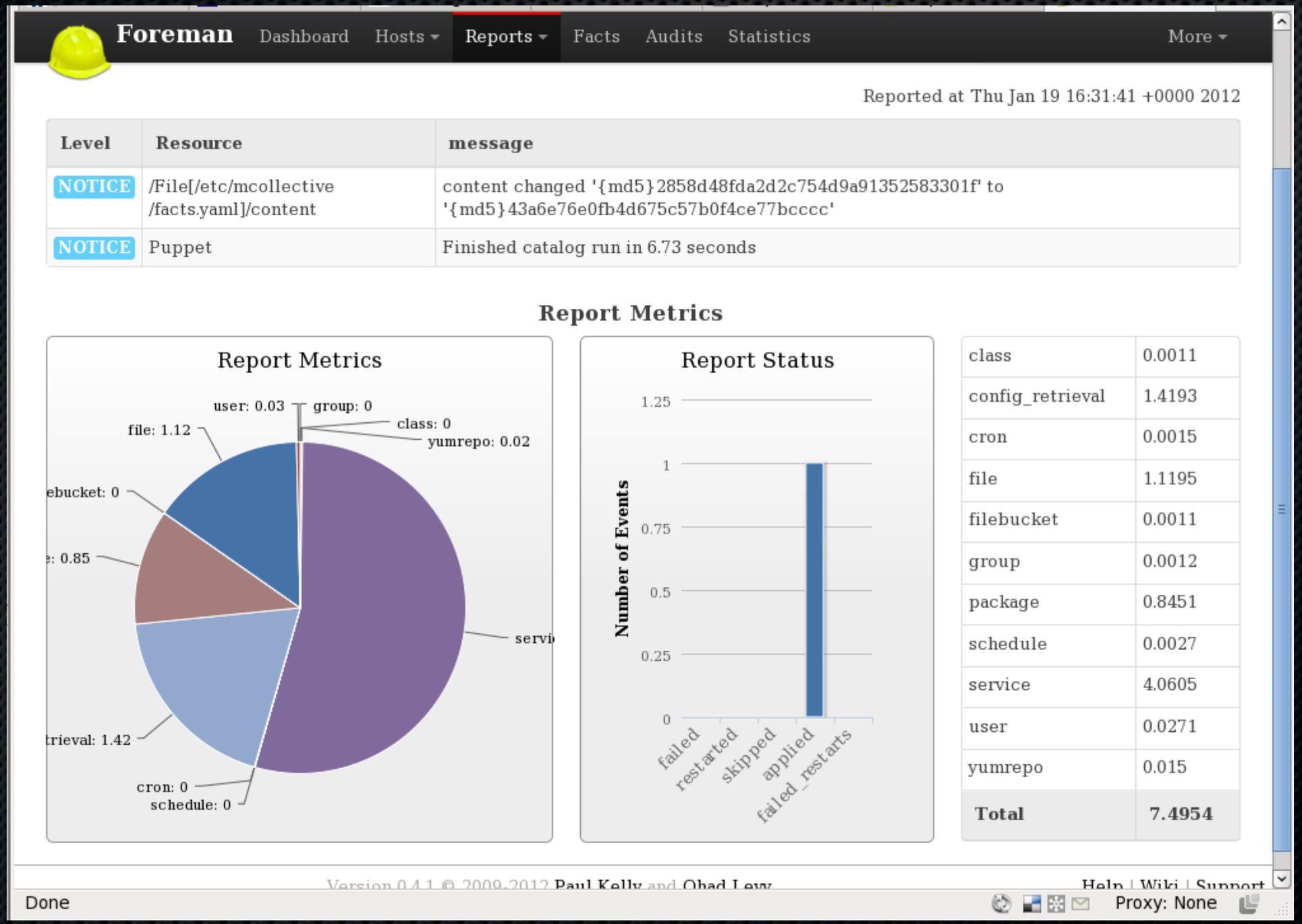
Configuration Mgmt

- Configure 1000 nodes,
- Modify 2000 files,
- Together
- Think :
- Cfengine,Puppet, Chef
- Put configs under version control
- Please don't roll your own ...

So eh .. Security ?

- Version control => Auditing
- CI => Add security IN the pipeline
- Configuration Mgmt
- Policy Definition
- Auditing & Enforcing
- Monitoring

Puppet in Action



Deployment isn't the End

Orchestration

- Manage 1000 nodes,
- Trigger
  - Upgrades
  - Config Runs
  - Service Changes
- Think :
  - Mcollective
  - Noah
  - Rundeck

High Availabilty

Scalability

Monitor

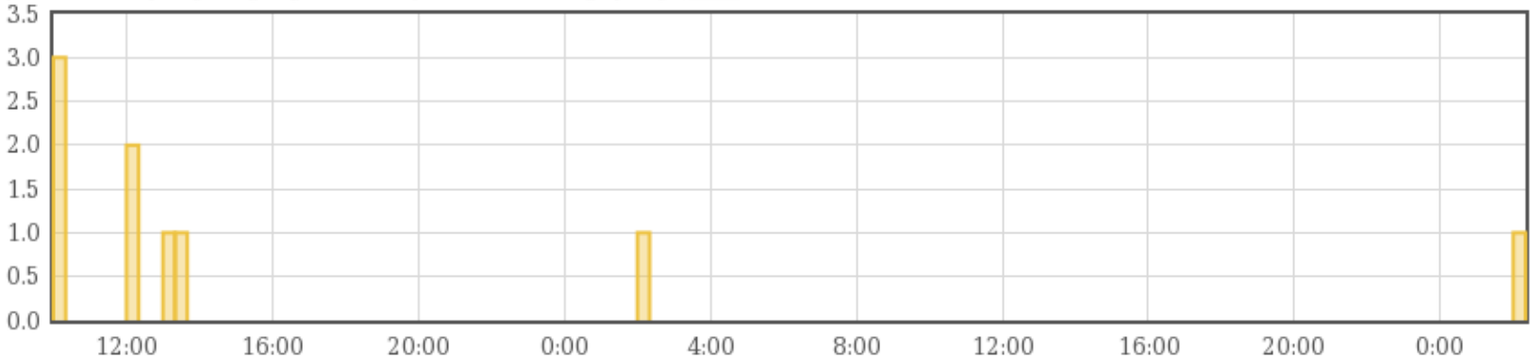
But Monitoring Stinks !

- #monitoringsucks trending
- https://github.com/monitoringsucks/
- 2008 Study :Nagios + Friends
- 2011 Conclusion : Nagios/Icinga are the only automatable alternatives
- Monitoring and trending at Scale , new kids Graphite, flapjack, etc
- What about Logging ? : Logstash, Graylog2

Logstash in Action

Query: login Search Clear **logstash.**

You can click on any search result to see what kind of fields we know about for that event. You can also click on the graph to zoom to that time period. The query language is that of Lucene's string query (docs).



Search results for 'login'

Results 0 - 9 of 9 | first | prev | next | last | refresh | (0.221 seconds)

timestamp	event
2012-01-13T10:10:47.000Z	Jan 13 10:10:47 vu02vx01.dc01.unifiedpost.local local7: [2012-01-13 10:10:47,213,accounting] "login","admin"
2012-01-13T10:15:55.000Z	Jan 13 10:15:55 vu02vx01.dc01.unifiedpost.local local7: [2012-01-13 10:15:55,471,accounting] "login","admin"
2012-01-13T10:19:24.000Z	Jan 13 10:19:24 vu02vx01.dc01.unifiedpost.local local7: [2012-01-13 10:19:24,817,accounting] "login","exception.handler"
2012-01-13T12:12:29.000Z	Jan 13 12:12:29 vu02vx01.dc01.unifiedpost.local local7: [2012-01-13 12:12:29,787,accounting] "login","exception.handler"
2012-01-13T12:18:11.000Z	Jan 13 12:18:11 vu02vx01.dc01.unifiedpost.local local7: [2012-01-13 12:18:11,264,accounting] "login","exception.handler"
2012-01-13T13:12:46.000Z	Jan 13 13:12:46 vu02vx01.dc01.unifiedpost.local local7: [2012-01-13 13:12:46,080,accounting] "login","exception.handler"
2012-01-13T13:32:44.000Z	Jan 13 13:32:44 vu02vx01.dc01.unifiedpost.local local7: [2012-01-13 13:32:44,610,accounting] "login","exception.handler"
2012-01-14T02:00:22.000Z	Jan 14 02:00:22 myup02 local7: [2012-01-14 02:00:22,408,BasicAuthenticator] Login succeded for user imqueryr
2012-01-15T02:00:24.000Z	Jan 15 02:00:24 myup02 local7: [2012-01-15 02:00:24,829,BasicAuthenticator] Login succeded for user imqueryr

Done Proxy: None

All this automation will only help against some local pain

Devop, definition

- There is no definition
- It certainly isn't a person
- No strict rules
- No strict tools
- It's not even new
- If you aren't doing it already ...

  ... you are doing it wrong

Debunking the Critics

Security not included ?

Everyone is Included:
security, dba, devs,
ops, designer, analysts,

We are solving a busines problem,

Not a technology problem

*ops

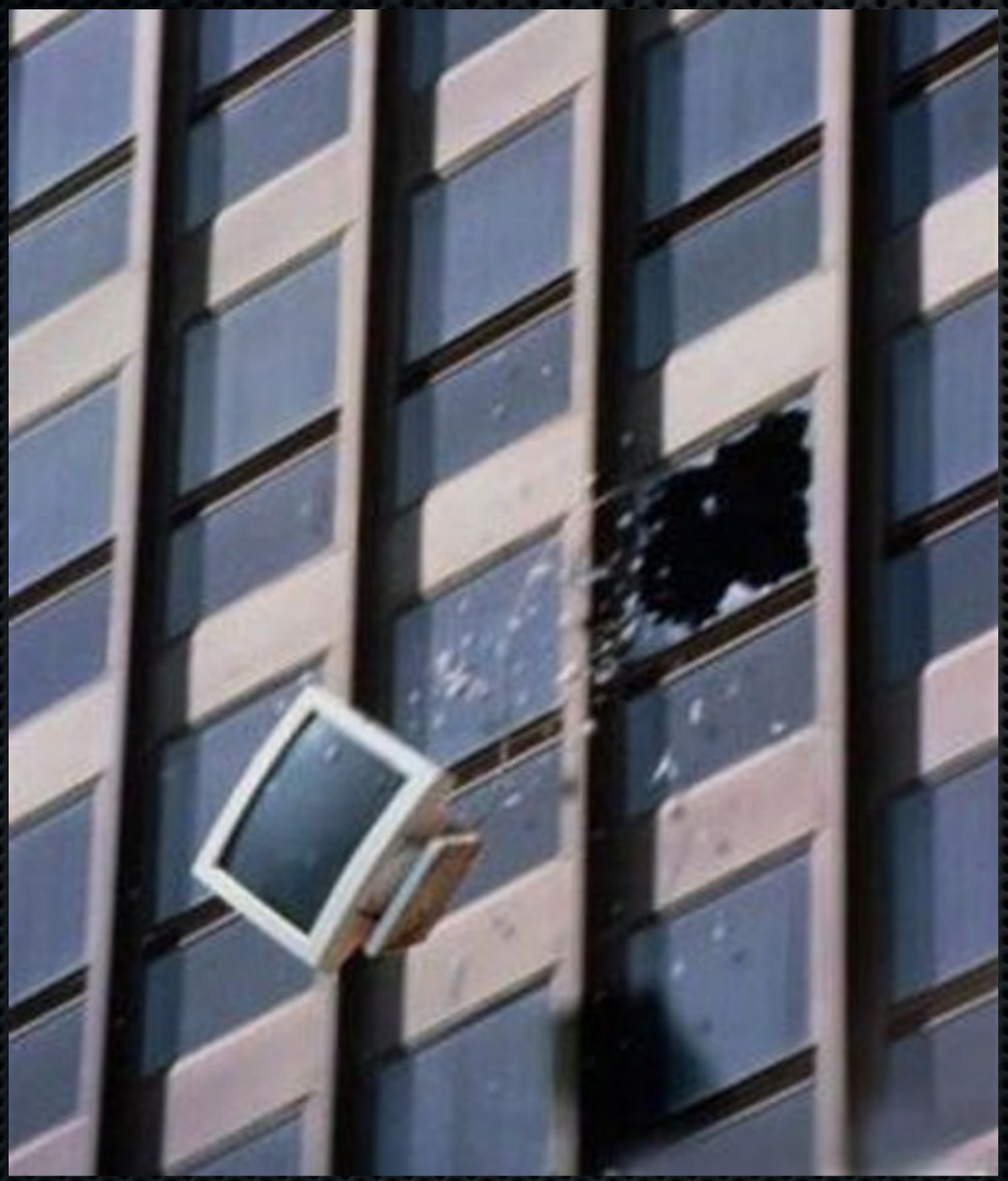
.

It's not about the tools

It's about change

It's about the people

Surviving the test !



- After 7+ years of preaching I`m not alone anymore
- Devops, a new Movement !
- Join the movement !
- Devopsdays.org
- Agile System Adminstration GoogleGroups

Contact

Kris Buytaert
Kris.Buytaert@inuits.be

Further Reading
@krisbuytaert
http://www.krisbuytaert.be/blog/
http://www.inuits.be/

Inuits
't Hemeltje
Duboistraat 50
2060 Antwerpen
Belgium
891.514.231

+32 475 961221