



Use Case:

Commercieel gaan met je open source project,
hoe doe je dat?

Michael Boelen

- Security
- Open source
 - [Rootkit Hunter](#) (malware)
 - [Lynis](#) (security)
- Blog: linux-audit.com



Arnoud Engelfriet

- IT lawyer
- Open source specialist
- blog.iusmentis.com



Use Case: Lynis

Lynis

- 2007
- Security scanner
- Linux / Unix

```
[+] Users, Groups and Authentication
-----
- Search administrator accounts... [ OK ]
- Checking UIDs... [ OK ]
- Checking chkgrp tool... [ FOUND ]
- Consistency check /etc/group file... [ OK ]
- Test group files (grpck)... [ OK ]
- Checking login shells... [ WARNING ]
- Checking non unique group ID's... [ OK ]
- Checking non unique group names... [ OK ]
- Checking LDAP authentication support [ NOT ENABLED ]
- Check /etc/sudoers file [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Shells
-----
- Checking console TTYS... [ WARNING ]
- Checking shells from /etc/shells...
  Result: found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] File systems
-----
- [FreeBSD] Querying UFS mount points (fstab)... [ OK ]
- Query swap partitions (fstab)... [ OK ]
- Testing swap partitions... [ OK ]
- Checking for old files in /tmp... [ WARNING ]
- Checking /tmp sticky bit... [ OK ]
```

The Idea: Lynis++

Start

- 2013
- Community
- Business

Build a Business

Easy!

- CoC/VAT
- Website
- Get customers



Belastingdienst

Build a Business

Reality...

- Customers
- Time
- Responsibilities

Customer Segments

Small companies:

- Detection
- Guidance
- Good feeling

Customer Segments

Big companies:

- Reporting
- Save time
- Compliance

Bonus Challenge: Community

- Usage
- Nessus / Tripwire
- Features

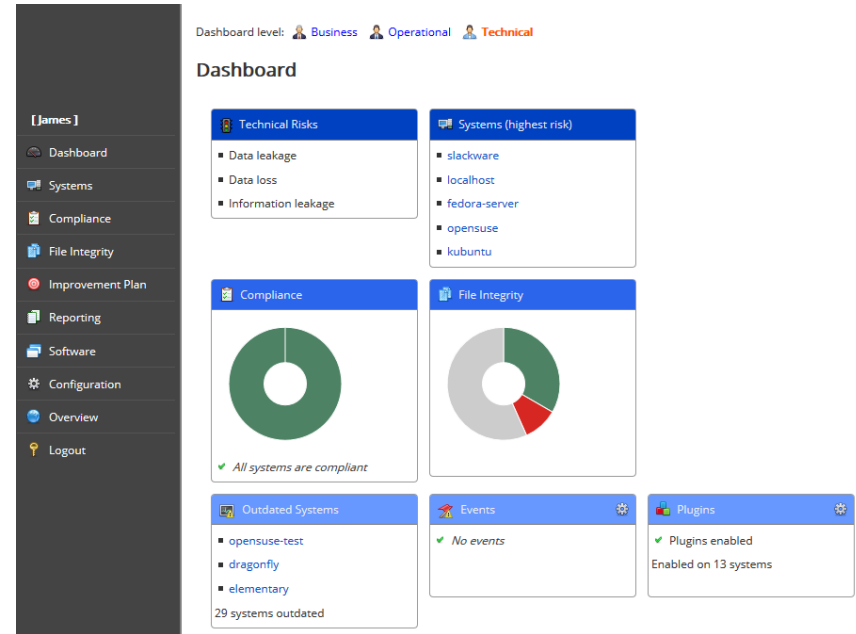
Solution

Community	Customers
Lynis	Lynis
	Central management
(data export)	Reporting / Compliance
(some plugins)	Additional plugins
(basic help)	Hardening snippets
(best effort support)	Support

Lynis Enterprise

- Happy community
- Business value

1 + 1 = 3!



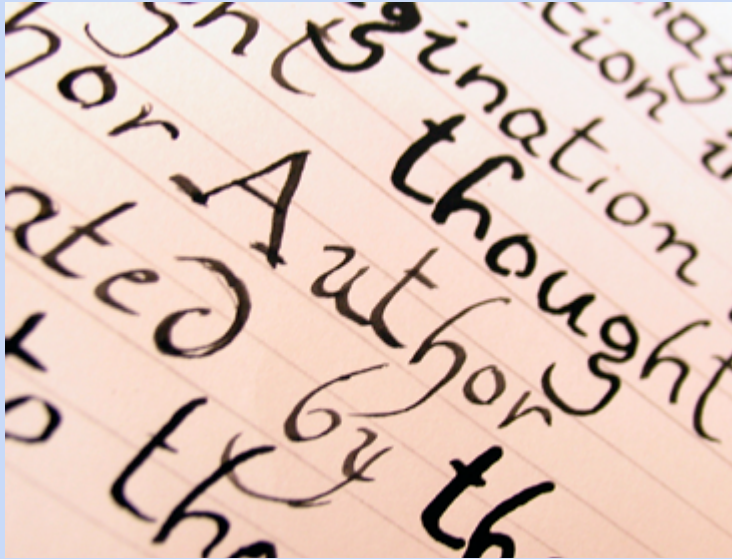
Examples

Example

Ownership

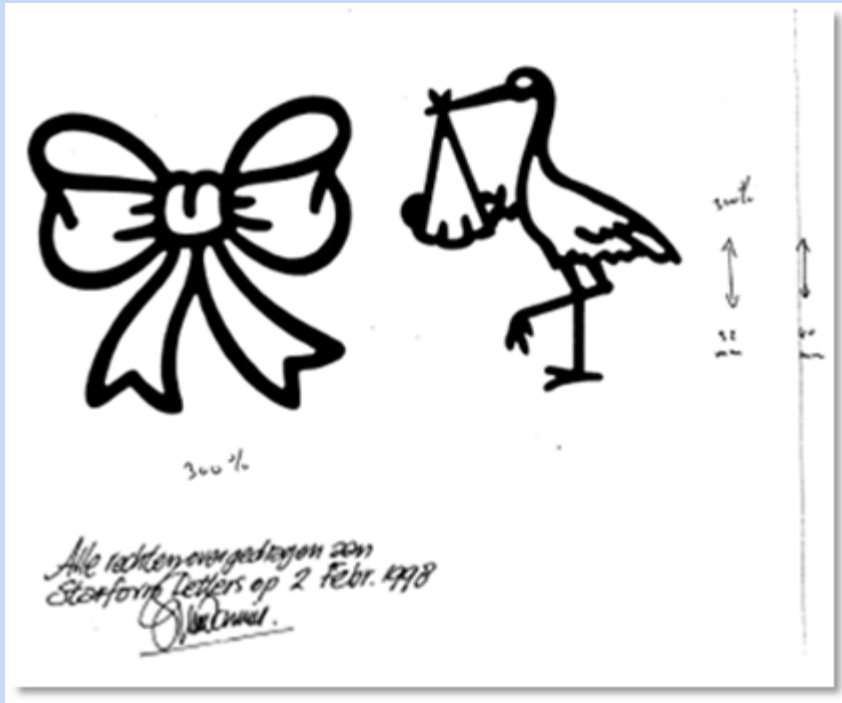
- My name or company?
- Contributors?

Copyright Owner



- Actual creator
- Employer
- Freelancer
- Assignment only by written and signed instrument

Copyright Assignment



```
$ cat hash.md5
595f44fecle92a71d3e9e77456ba80d1 filetohashA.txt
71f920fa275127a7b60fa4d4d41432a3 filetohashB.txt
43c191bf6d6c3f263a8cd0efd4a058ab filetohashC.txt
```

```
dboth: bash
File Edit View Scrollback Bookmarks Settings Help
root root dboth: bash
[dboth@david1 ~]$ ls -l
total 2096
-rw-rw-r-- 1 dboth dboth 7740 2008-06-26 16:49 alice.txt
dneaxr-x-x 2 dboth dboth 4096 2009-10-28 17:55 bla
-rw-r----- 1 dboth dboth 421246 2009-07-30 07:02 bookmarks.html
-rw-rw-r-- 1 dboth dboth 76467 2009-01-05 16:39 DavidAddresses.ldif
-rw-rw-r-- 1 dboth dboth 50 2006-02-26 20:55 dboth.sig
dneaxr-x-x 2 dboth dboth 4096 2009-08-11 11:11 Desktop
dneaxr-x-x 26 dboth dboth 4096 2009-11-05 11:27 Documents
dneaxr-x-x 2 dboth dboth 4096 2009-06-17 15:00 Download
-rw-rw-r-- 1 dboth dboth 1319809 2009-10-06 17:24 Firefox_wallpaper.png
dneaxr-x-x 2 dboth dboth 32768 2009-11-13 16:36 GnuCash
dneaxr-x-x 6 dboth dboth 4096 2009-08-30 09:04 Graphics
dneaxr-x-x 2 dboth dboth 4096 2006-11-16 11:02 Intel
-rw-rw-r-- 1 dboth dboth 196576 2009-10-23 14:28 Kaddressbook.ldif
dneaxr-x-x 2 dboth dboth 4096 2006-07-23 08:00 ksysguard
dneaxr-x-x 2 dboth dboth 4096 2009-09-09 07:38 logs
dneaxr-x-x 15 dboth dboth 4096 2009-09-01 15:21 Music
-rw-rw-r-- 1 dboth dboth 131 2003-04-03 17:37 Peace.SIG
dneaxr-x-x 104 dboth dboth 4096 2009-11-06 17:42 Pictures
dneaxr-x-x 2 dboth dboth 4096 2009-06-17 15:00 Public
-rw-rw-r-- 1 dboth dboth 1852 2009-06-17 15:01 screen-configurations.xml
-rw-rw-r-- 1 dboth dboth 362 2008-04-05 09:17 Short.SIG
-rw-rw-r-- 1 dboth dboth 294 2009-03-27 06:44 ShortTech.SIG
-rw-rw-r-- 1 dboth dboth 174 2007-03-26 16:24 SourceForge.SIG
dneaxr-x-x 2 dboth dboth 4096 2009-06-17 15:00 Templates
dneaxr-x-x 3 dboth dboth 4096 2009-10-07 07:25 top
dneaxr-x-x 2 dboth dboth 4096 2009-02-20 12:41 vboxshared
dneaxr-x-x 3 dboth dboth 4096 2009-08-24 08:11 Videos
[dboth@david1 ~]$
```

Rb. Den Haag 27 juni 2007, IEF 4262

Assignment or Contributor License?

Assignment:

- All in one hand
- Easy to relicense
- Requires trust from contributors
- Requires managing paper with signatures

Contributor license:

- Contributor retains ownership
- No relicensing without permission
- Easier to contribute

Example

Liability

- Snippet
- Bad advice
- Internationally

Liability

- OSS license protects you
- Negotiate limitation in commercial license
- Consider liability insurance
- Use GTC for professional advice

Example

EULA / license

- Lynis: GPL
- Enterprise: SaaS solution
- Enterprise: On-premise version

Example

Service providers

- White label
- Dual licensing?

Proprietary License

- **EULA:** Standard license for end users, support maybe/maybe not included
 - **TOS:** Standard license for SaaS
 - **Enterprise license:** large corporations, includes support & service levels
- Why is paid license more attractive?

Proprietary License

- License scope: per user, per company?
- Payment structure
- Audit rights
- Limitation of liability
- Indemnification
- Term & termination

OSS License Choices

Open source can be used commercially!

Goal:

Make closed version more attractive for businesses than open version

OSS License Choices

- GPLv3: the Big Bad, full copyleft
- AGPLv3: the SaaS Big Bad
- LGPL/Mozilla: limited copyleft
- BSD: no copyleft, free reuse

Example

NDA signing

- Financial company in US
- Sign their NDA
- No NDA = No Business

NDA Signing

- Single- or double-sided?
- Definition of Authorized Purpose
- Definition of Confidential Information
- Ownership of IP
- Obligation to negotiate?

Always review!



Example

Partnerships

- Company in different country
- Wants to be a partner
- How to define contracts?

Partner Agreement

Affiliate

- Brings in leads for a fee
- You own the customer
- How to handle lead quality?

Reseller

- Sells licenses, pays a fee/percentage
- Who handles support?
- What if customer does not pay to reseller?

Example

Investors

- What to share?
- What if they offer €10M?

Investors

- Signing NDA or not?
- Due diligence
- Letter of intent

(this is where you really need a lawyer)



Questions?

More Information

Arnoud Engelfriet

blog.iusmentis.com

arnoud@engelfriet.net

@ictrecht

Michael Boelen

linux-audit.com

michael@cisofy.com

@mboelen