



# Setting up a Security Team

► The CERN CERT as an example

**Dr. Stefan Lüders**  
(CERN Computer Security Officer)  
Openlab Summer Student Lectures, July 3<sup>rd</sup> 2012



# Attackers vs. Defense

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

- ▶ There is no 100% security.
- ▶ **Security is as good as weakest link:**  
Attacker chooses time, place, method  
Defender needs to protect against all...



theguardian

## PlayStation Network hack: why it took Sony seven days to tell the world

Sony's company blog says forensic analysis of the PlayStation Network hack took 'several days' to complete and extent of intrusion wasn't understood until Tuesday



THE DAILY  
BEAST  
READ THIS SKIP THAT

HOME POLITICS BUSINESS INNOVATION ENTERTAINMENT BEAST TV BOOKS ART WOMEN IN T

Featured: ELECTION • FASHION • ANDREW SULLIVAN • HOWARD KURTZ • DAVID FRUM

## CHEAT SHEET

MUST READS FROM ALL OVER

WE DID IT

### Anonymous Hacked Justice Dept., FBI Sites



Frederic J. Brown / AFP-Getty Images

So much for staying Anonymous. The hacking group has admitted to crashing the Justice Department and FBI websites, after federal officials took down the popular file-sharing site Megaupload. Seven executives from Megaupload were indicted Thursday for disobeying copyright laws and protection, though the site's attorney denied the charges. Hours later, the websites of the Justice Department and Universal Music and the FBI's homepage all malfunctioned. Anonymous didn't steal any information from the sites—the attacks were meant to flood the pages with more traffic than they could handle and were targeted at the Stop Online Piracy Act. The founder of an online think tank that works in tandem with the hacking site said Anonymous might



# Attackers vs. Defense

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

- ▶ There is no 100% security.
- ▶ **Security is as good as weakest link:**  
Attacker chooses time, place, method  
Defender needs to protect against all...



- ▶ Targeted attackers (→ APTs) are **focused and keen**,  
have **better skills/networks**, are **better financed/resourced**
- ▶ The untargeted/stupid  
attackers might be caught...
- ▶ Automatism, at least, can be fought.

“Anonymous is a handful of geniuses  
surrounded by a legion of idiots.”

Cole Stryker

- ▶ Defense usually lacks money/resources/networks.
- ▶ (International) **Law is always a step behind.**

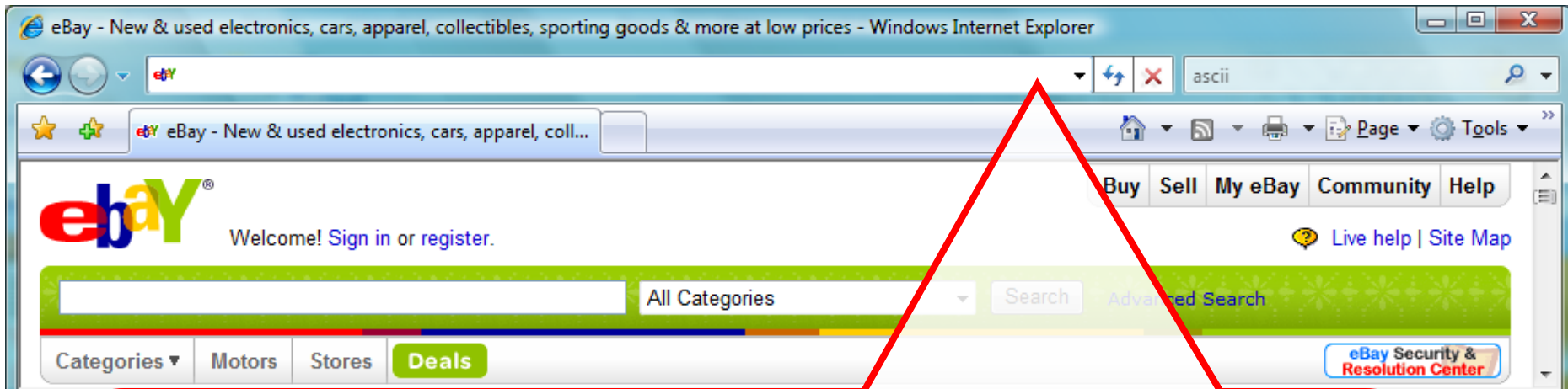
# Attackers vs. Defense

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



# A small quiz.

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



## Quiz: Which URL leads you to [www.ebay.com](http://www.ebay.com) ?

- ✗ <http://www.ebay.com/cgi-bin/login?ds=1%204324@%31%33%37%2e%31%33%38%2e%31%33%37%2e%31%37%37/p?uh3f223d>
- ✗ <http://www.ebay.com/ws/eBayISAPI.dll?SignIn>
- ✓ [http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co\\_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&raflid=0&encRaflid=default](http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&raflid=0&encRaflid=default)
- ✗ <http://secure-ebay.com>





**1. Understand your environment  
& security footprint.**



**2. Assess your threats!**



**3. Develop your security paradigm.**



**4. The Permanent Mitigation Cycle**



**5. Set up your Team**



# **1. Understand your environment & security footprint.**

# Do you know your environment?

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012





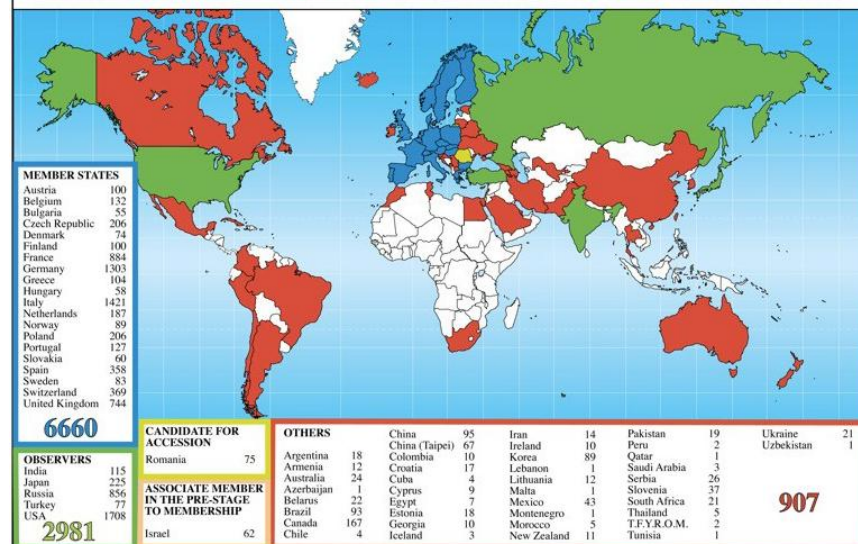
# Academic Freedom at CERN

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

## CERN's Users:

- ▶ ...from 100s of universities worldwide
- ▶ Pupils, students, post-docs, professors, technicians, engineers, physicists, ...
- ▶ **High turn-over** (~10k per year)
- ▶ **Merge of professional and private life:** Social Networks, Dropbox, Gmail, LinkedIn, ...

Distribution of All CERN Users by Nation of Institute on 9 January 2012



## Academic Freedom in Research:

- ▶ **No limitations** and boundaries if possible
- ▶ **Free** communication & **freedom** to publish
- ▶ Difficult to change people, impossible to force them
- ▶ Trial of the new, no/very fast life-cycles, all-time prototypes
- ▶ **Open campus attitude:** I consider CERN being an ISP!

# Academic Freedom at CERN

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

## CERN's Users:

- ▶ ...from 100s of universities worldwide
  - ▶ Pupils, students, post-docs, professors, technicians, engineers, physicists, ...
  - ▶ High turn-over (~10k per year)
  - ▶ Merge of professional and private life: Social Networks, Dropbox, Gmail, LinkedIn, ...
- The threshold**



The threat is already inside.

A good security paradigm must balance this “Academic Freedom”

m in Research:  
foundations possible  
freedom to publish



**A9**

**balance this**

**Academic freedom is Research:**

**and bounded as far as possible**

**freedom to publish**

- ▶ **Open campus attitude:** I consider CERN being an ISP!

# Do you know your security foot-print?

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012





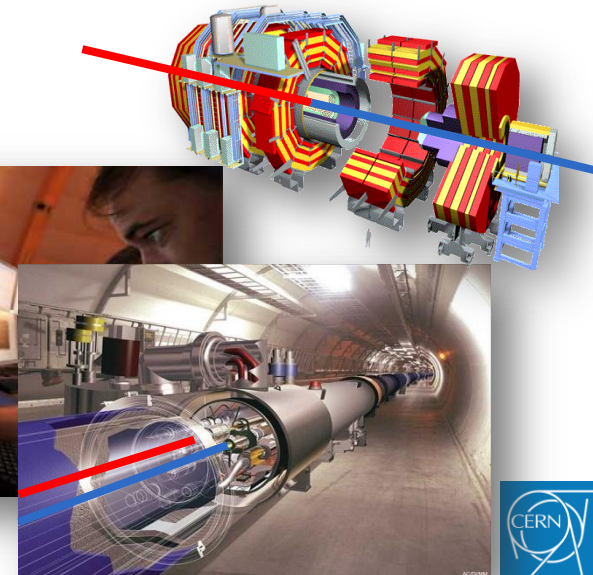
# CERN Sectors of Operations

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



Office Computing Security  
Computing Services Security

Grid Computing Security  
Control Systems Security





**1. Understand your environment  
& security footprint.**



**2. Assess your threats!**



# Do you know your threats?

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012





# Under Permanent Attack

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

**CERN is under permanent attack... even now.**

**Servers accessible from Internet are permanently probed:**

- ▶ ...attackers trying to brute-force passwords;
- ▶ ...attackers trying to break Web applications;
- ▶ ...attackers trying to break-in servers and obtain administrator rights.

**Users are not always aware/cautious/proactive enough:**

- ▶ ...attackers trying to harvest credentials outside CERN;
- ▶ ...attackers trying to “phish” user passwords.

**Security events happen:**

- ▶ Web sites & web servers, data-base interfaces, computing nodes, mail accounts, ...
- ▶ The office network is very liberal: free connection policy and lots of visitors. Thus, there are always devices being infected/compromised.



# Under Permanent Attack

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

**CERN is under permanent attack... even now.**

**Servers accessible from Internet are permanently probed:**

- ▶ ...attackers trying to brute-force passwords;
- ▶ ...attackers trying to break Web applications;
- ▶ ...attackers trying to break-in servers and obtain administrator rights.

**Users are not always aware/cautious/proactive enough:**

- ▶ ...attackers trying to harvest credentials outside CERN;
- ▶ ...attackers trying to “phish” user passwords.

**Coming up:  
My top-12 security events of the last 5yrs  
(There weren't much more)**

- ▶ Web sites & web servers, data-base interfaces, computing nodes, mail accounts, ...

- ▶ The CERN network is very liberal: free connection policy and lots of visitors. Thus, there are always devices being infected/compromised.



# Phishing (1)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

Date: Fri, 5 Sep 2008 15:53:42 -0700  
From: Webmail IT Service <sandraward@charterinternet.com>  
Reply-To: webITService@live.com

Targeted and untargeted  
“Phishing” attacks in  
English & French...



To: CERN Authentication v2  
Subject: webusadlq2.appspot.com/WkVoa2NHRXlhM1ZaTWxaNVltazFhbUZET1RCa01teHlZVk01YVdGWESiWmtiV3hzWkhrNVFtUkhIR2hqTVVKNVlqTUNl...

Dear

This mail is a spoofed login page for CERN authentication.

ver

In c

Full

Use

Pass

Dom

\*Im

Pla

We

Web

Reg

We

Web

Reg

Sign in with your CERN account

>>>Help Desk Error>>> Respond - Message (HTML)

File Message

Delete Reply Reply All Forward Service Accounts To Manager Team E-mail Mark Unread

Delete Respond Quick Steps Move Tags

From: Kim Thomas <kthomas@bbisd.org>  
To: it@helpdesk.org  
Cc:  
Subject: >>>Help Desk Error>>> Respond

Sent: Mon 05/12/2011 01:40

Dear User,

You have exceeded the limit for the number of new emails and sent size (10 MB). You have exceeded the limit for the number of KB, You have exceeded the limit for the number of KB.

<https://docs.google.com/spreadsheet/viewform?formkey=dfphslvithy5dmuws3zmotdxqvjrvee6ma>  
Click to follow link

To prevent this, please click to reset your account. [CLICK HERE](#)

Thanks  
Administrator.

Spoofed login pages...



...on “trusted” hoster!





# Data Leakage (1)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

The screenshot shows a Windows Internet Explorer browser window. The address bar displays a Google search URL: `http://www.google.com/search?q=samfox+site%3Acern.ch&rls=com.microsoft:*&ie=UTF-8&oe=UTF-8`. The search results show a link to 'samfox site:cern.ch - Google Search'. Below this, the browser displays a forum page from the 'CERN LHC portal'. The forum topic is 'What is where in LHC sectors?'. The post is by 'Harbles' and is dated 'Sun Mar 07, 2010 5:03 pm'. The post content includes a greeting to 'Serych' and a list of links to PDF documents: 'Atlas http://cdsweb.cern.ch/record/1129811/...', 'Alice http://cdsweb.cern.ch/record/1129812/...', 'CMS http://cdsweb.cern.ch/record/1129810/...', and 'LHCb http://cdsweb.cern.ch/record/1129809/...'. Below the post, there is a profile section for 'serych' with a photo and a response dated 'Sun Mar 07, 2010 5:03 pm'. The response thanks 'Harbles' and mentions that a password is required for some documents. At the bottom, there is another post by 'Harbles' dated 'Mon Mar 08, 2010 1:33 am' which provides an alternate source for the Atlas document: `http://docs.google.com/fileview?id=0B-oldYyTyx9CZmNmMjZOTQTMWZhOS00YzYwLThhNmMtZGNjM2Q4YTcwMDYx&hl=en`.

Confidential data on Wikis, Webs, CVS...



Sensitivity levels are user dependent!



# Data Leakage (2)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

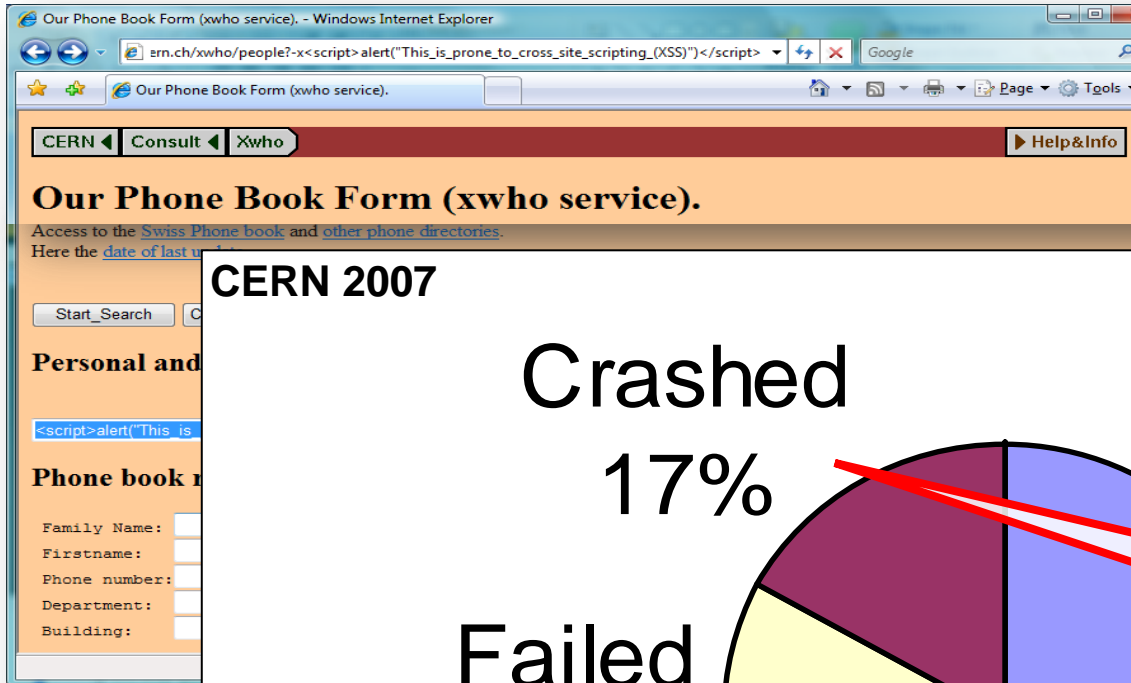
A month earlier, he reported to the U.S. Department of Homeland Security who informed us plus SWITCH and MELANI.

PVSS  
Graphical Editor

- Exécuter « Remote Desktop Connection »
  - Se connecter sur Cerntsab06
  - User name : atlassecr
  - Password : Operateur1
- Ouvrir C:\Dev\_Disk\PVSS\_Projects\unicos\_pvss\_OWS
  - Exemple : BTPCS
  - Exécuter « Atlas\_Cryo\_Unity.Editeur.bat »
- Ouvrir Panel Editor

# Suboptimal configuration (1)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



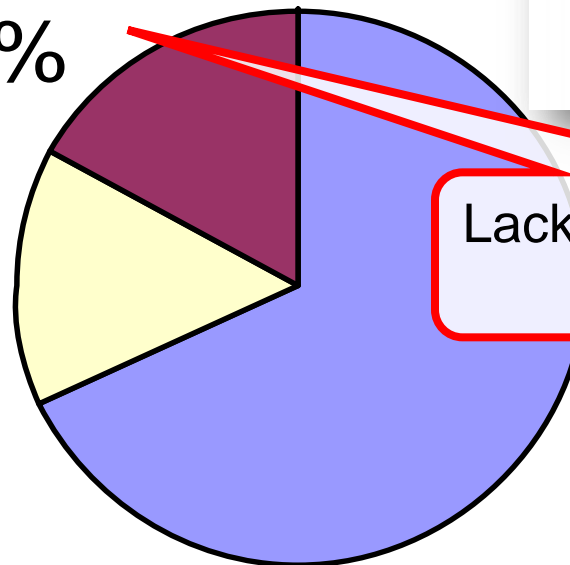
Lack of input validation/sanitization



CERN 2007

Crashed  
17%

Failed  
15%



Lack of robustness ☹️



Passed  
68%





# Suboptimal configuration (2)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

Mozilla Firefox

Αρχείο Επεξεργασία Προβολή Ιστορικό Σελιδοδείκτες Εργαλεία Βοήθεια

http://[redacted].cern.ch/[redacted]/apanthsh.html

Proxy: None Apply Edit Remove Add Status: Using None Preferences

Post a new topic http://[redacted].anthsh.html

## GST

GREEK SECURITY TEAM

10/09/08 03:00

Αυτήν την ώρα γίνεται η απόπειρα πειράματος στο CERN.

Ο λόγος που διαλέξαμε αυτή τη σελίδα είναι για να σας θυμίζουμε μερικά πράγματα. Δεν έγινε βάση κάποιας προσωπικής μας αντιπαράθεσης με την ομάδα διαχείρισης του CERN αλλά με βάση την μεγάλη επισκεψιμότητα που θα αποκτήσει τα επόμενα 24ωρα ο συγκεκριμένος διαδικτυακός τόπος λόγω του πειράματος.

Μερικά στοιχεία απ' τη βάση :

| USERNAME        | USER_ID | CREATED               |
|-----------------|---------|-----------------------|
| SYS             | 0       | 2008-02-18 16:19:25.0 |
| SYSTEM          | 5       | 2008-02-18 16:19:25.0 |
| OUTLN           | 11      | 2008-02-18 16:19:28.0 |
| DIP             | 19      | 2008-02-18 16:21:17.0 |
| TSMSYS          | 21      | 2008-02-18 16:23:27.0 |
| DBSNMP          | 24      | 2008-02-18 16:24:25.0 |
| WMSYS           | 25      | 2008-02-18 16:24:53.0 |
| EXFSYS          | 34      | 2008-02-18 16:27:55.0 |
| XDB             | 35      | 2008-02-18 16:28:04.0 |
| PDB_ADMIN       | 46      | 2008-02-18 17:26:32.0 |
| GLEGE           | 49      | 2008-02-19 10:13:07.0 |
| PDBMON          | 45      | 2008-02-18 17:25:24.0 |
| BALYS           | 44      | 2008-02-18 17:25:24.0 |
| USERMON         | 48      | 2008-02-18 17:59:26.0 |
| ..etc...etc.... |         |                       |

A defaced  
(added)  
web-page...

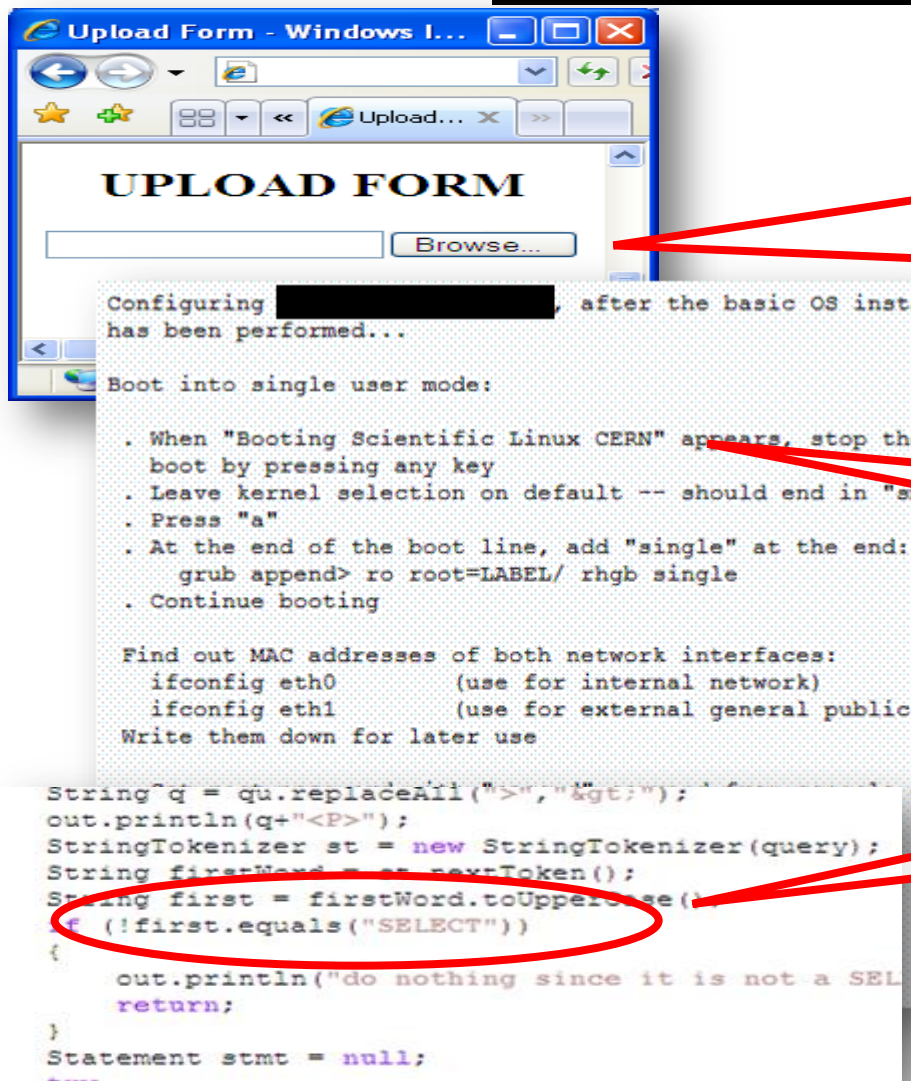


Oops !!???  
...a user listing



# Suboptimal configuration (3)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



The screenshot shows a web browser window titled 'Upload Form - Windows I...' with a 'Browse...' button. Below it is a terminal window with the following content:

Configuring [REDACTED], after the basic OS installation has been performed...

Boot into single user mode:

- . When "Booting Scientific Linux CERN" appears, stop the boot by pressing any key
- . Leave kernel selection on default -- should end in "s"
- . Press "a"
- . At the end of the boot line, add "single" at the end:  
grub append> ro root=LABEL/ rhgb single
- . Continue booting

Find out MAC addresses of both network interfaces:

```
ifconfig eth0      (use for internal network)
ifconfig eth1      (use for external general public)
Write them down for later use
```

```
String q = qu.replaceAll(">", "&gt;");
out.println(q+"<P>");
StringTokenizer st = new StringTokenizer(query);
String firstWord = st.nextToken();
String first = firstWord.toUpperCase();
if (!first.equals("SELECT"))
{
    out.println("do nothing since it is not a SELECT");
    return;
}
Statement stmt = null;
try
```

***Neglected*** "Rule of Least Privileges":  
Everyone could upload whatever he/she wants...



Configuration well documented in Google...



Lack of input validation & sanitization



# Break-Ins (1)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

```
220-<<<<<<==< Haxed by A|0n3 >==<>>>>>
220- ,,øx°°^°°xø, ,,øx°°^°°xø, ,,øx°°^°°xø, ,,øx°°^°°xø
220-/
```

```
220-| Welcome to this fine str0
```

```
220-| Today is: Thursday 12 January, 2006
```

```
220-| "In March .... Windows computers were compromised..."
```

```
220-| Current throughput: 0.000 Kb/sec
```

```
220-| ...The initial compromised host was scanning the ... network
220-| and several compromise attempts succeeded due to
220-| MS-SQL servers (port 1433/tcp) with no password for the
220-| 'sa' account...
```

```
220-| ...Analysis indicated that the [THIRD PARTY SOFTWARE]
220-| installation left the password empty by default..."
```

Unpatched oscilloscope  
(running Win XP SP2)



Undocumented feature  
in SCADA application





# Break-Ins (2)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

Lack of input  
validation & sanitization



Unpatched web server  
(running LX)



The screenshot shows a web browser window with a URL bar containing a long, complex URL. Below the browser, a terminal window titled "Terminal — ssh — ttys000 — 80x24" displays the output of an exploit. The terminal shows a list of files being transferred, followed by a successful execution of an exploit script. The user's identity is shown as "uid=48(apache) gid=48(apache) groups=48(apache),50004(ticketgroup),1100241092 context=root:system\_r:system\_mail\_t". The user then runs a shell command "sh-3.00# id" and the output shows "uid=0(root) gid=0(root) groups=48(apache),50004(ticketgroup),1100241092 context=root:system\_r:system\_mail\_t", indicating a successful root shell.

```
3200K ..... 95% 10.85 MB/s
3250K ..... 96% 11.49 MB/s
3300K ..... 98% 10.99 MB/s
3350K ..... 99% 11.24 MB/s
3400K ..... 100% 10.83 MB/s

15:03:29 (11.18 MB/s) - 'exploit2.tgz' saved [3492005/3492005]

tar -zxvf exploit2.tgz && cd wunderbar_emporium
wunderbar_emporium/
wunderbar_emporium/pwnkernel.c
wunderbar_emporium/tzameti.avi
wunderbar_emporium/wunderbar_emporium.sh
wunderbar_emporium/exploit.c
id
uid=48(apache) gid=48(apache) groups=48(apache),50004(ticketgroup),1100241092 context=root:system_r:system_mail_t
./wunderbar_emporium.sh
sh: mplayer: command not found
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache),50004(ticketgroup),1100241092 context=root:system_r:system_mail_t
sh-3.00#
```

One error in opening the page. For more information, choose Window > Activity.



**1. Understand your environment  
& security footprint.**



**2. Assess your threats!**



**3. Develop your security paradigm.**

# What would be your strategy?

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012





# CERN Security Paradigm

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

**Find balance** between “Academic Freedom”,  
“Operations” and “Computer Security”

“Academic Freedom” means “Responsibility”

- ▶ (I, as Security Officer, **decline** to accept that responsibility)
- ▶ Instead, **computer security at CERN is delegated** to all users of computing resources.
- ▶ If they don't feel ready, they can pass that responsibility to the IT department using central services.



**Change of culture & a new mind set:**

- ▶ Enable users to fully assume this responsibility.
- ▶ Make security integral part of the overall.

(Plus a **Defense-In-Depth** approach, still.)



# CERN Security Paradigm

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

**Find balance** between “Academic Freedom”,  
“Operations” and “Computer Security”

“Academic Freedom” means “Responsibility”

- ▶ (I, as Security Officer, decline to accept that responsibility)
- ▶ Instead, computer security at CERN is delegated to all users of computing resources
- ▶ If they don't feel ready, they can pass that responsibility to the IT department using central services.

**This is a “people” problem!**  
**A good Security Team becomes**  
**facilitator and enabler!**

**Change of culture? New mind set:**

- ▶ Enable users to fully assume this responsibility.
- ▶ Make security integral part of the overall.

**(Plus a Defense-In-Depth approach, still.)**





**1. Understand your environment  
& security footprint.**



**2. Assess your threats!**



**3. Develop your security paradigm.**



**4. The Permanent Mitigation Cycle**



# Permanent Mitigation Cycle

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



# Examples for “Prevention”?





Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



# Permanent Mitigation Cycle (1)

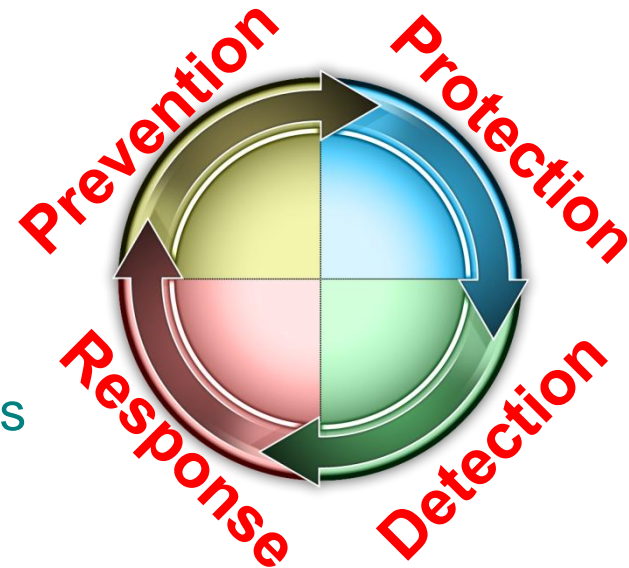
Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

## Prevention:

- ▶ Definition and communication of security policies
- ▶ **Security Baseline**ing for systems & services:  
Contract between owner & Security Officer
- ▶ **Assessments & reviews**
- ▶ **Training** for secure coding & configuration practices
- ▶ Provisioning of **static code analyzers**
- ▶ **Vulnerability scanning:**      
w3af/Wapiti/Skipfish (Web apps), Nessus/nmap (hosts), John the Ripper (passwords), “Prodder”-scans (e.g. for Open Shares, MyPhpAdmin)...
- ▶ **“Credential hunts”** (e.g. unprotected clear text passwords on AFS)

## Plus:

- ▶ Deployment of an integrated identity management system, AuthZ & AuthN
- ▶ Central PC management & immediate patching
- ▶ Active research (e.g. Siemens/CERN openlab collaboration)





# Examples for “Protection“?

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



# Permanent Mitigation Cycle (2)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

## Protection:

- ▶ “Defense-in-Depth”, in particular for control systems
- ▶ Tightened outer perimeter firewall with life-cycle, scanning & opening approval
- ▶ Awareness raising:  
Dedicated awareness sessions,  
Introduction sessions for newcomers,  
Leaf sheets & posters

## Plus:

- ▶ Segregated networks for dedicated purposes
- ▶ Inter-network filtering and access control
- ▶ Deployment of local firewalls
- ▶ Centralized anti-virus software (on IT managed Windows PCs & servers)

**SECURITY is not complete without U**

**Quelques astuces pour protéger votre ordinateur et vos données**

- Utilisez les systèmes d'exploitation fournis par le département IT du CERN : ils sont configurés de manière sûre et mis à jour automatiquement pour vous.
- Protégez votre ordinateur privé : utilisez l'antivirus du CERN; appliquez les mises à jour logicielles; n'installez pas de logiciels douteux.
- Protégez vos fichiers et données : limitez l'accès à vos documents et répertoires; appliquez le principe du droit d'accès minimal.
- Soyez prudent lorsque vous naviguez sur le Web : ne cliquez pas sur des liens suspects et n'installez pas de plug-in douteux.
- Suivez les règles informatiques du CERN : respectez le droit d'auteur; n'utilisez pas de logiciels non-autorisés; consultez <http://cern.ch/ComputingRules>.
- Protégez vos mots de passe : ne les partagez jamais; prenez garde au phishing (technique qu'utilisent les escrocs en ligne pour voler votre mot de passe); ne les réutilisez pas (utilisez des mots de passe différents pour des applications différentes); ne les tapez pas sur des ordinateurs ou des sites Web suspects.
- Demandez conseil : l'équipe de sécurité informatique vous propose des cours de formation, des analyses de codes logiciels, des balayages Web ou serveur etc., et est là pour vous aider : contactez [Computer.Security@cern.ch](mailto:Computer.Security@cern.ch) ou consultez <http://cern.ch/Computer.Security>.

**Be careful with e-mail & Web**

Cybercriminals are trying to trick you!

# Examples for “Detection”?

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



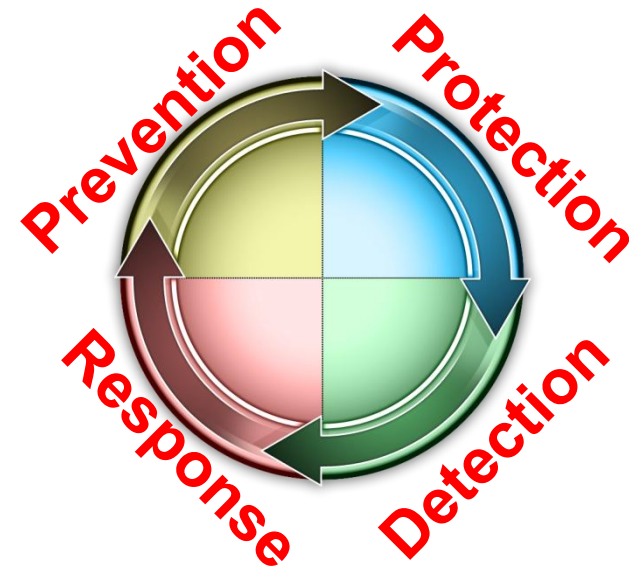


# Permanent Mitigation Cycle (3)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

## Detection:

- ▶ **Statistical analysis** of network flows:  
e.g. number of peers (→ P2P),  
multiple SSH/SNMP/Web connections,  
infected devices (ports 137/tcp, 139/tcp, 445/tcp)
- ▶ **Analysis of DNS queries** (→ Conficker worm)
- ▶ **Packet inspection IDS:**  
~12k rules from VRT and ET for  
detection of e.g. IRC, ...
- ▶ **Automatic log analysis:**  
logins, kernel panic, critical commands (“uname -a; id”), ...
- ▶ **“SSH receipts”** for remote connections from “strange” locations
- ▶ Training of users to report phishing emails



## Plus:

- ▶ Centralized anti-virus software (on IT managed Windows PCs & servers)

# How to do “Response”?

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

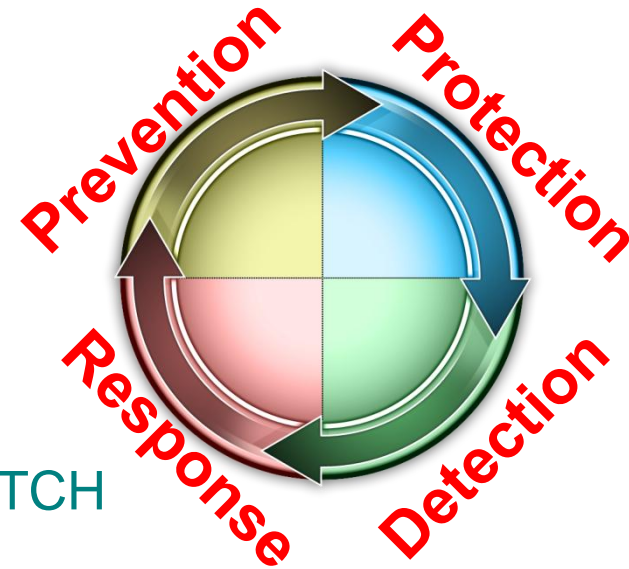


# Permanent Mitigation Cycle (4)

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

## Response:

- ▶ Provisioning of CSIRT/CERT, and WLCG Grid Security Officer
- ▶ Containment
- ▶ Impact analysis / classification / prioritization
- ▶ Incident forensics (above a certain impact)
- ▶ Interaction with third parties: e.g. universities, SWITCH
- ▶ Recovery (i.e. usually reinstallation)
- ▶ Application of lessons learned
- ▶ Costing



## Plus:

- ▶ Business continuity planning / Disaster recovery planning
- ▶ Verification: Annual Security Challenges inside the WLCG Grid





**1. Understand your environment  
& security footprint.**



**2. Assess your threats!**



**3. Develop your security paradigm.**



**4. The Permanent Mitigation Cycle**



**5. Set up your Team**

# What makes a good Security Team?

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



# A good Security Team

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

A good Security Team is **mainly facilitator and enabler**, sometime enforcer, and (hopefully) rarely punisher.

Members of the Team **cover all social and technical aspects**: (see Belbin Team Role Inventory)

- ▶ “Resource Investigator” to reach out into the environment;
- ▶ “Co-ordinator” to manage the Team and its priorities;
- ▶ “Evaluator” to develop and deploy security policies;
- ▶ “Team Worker” to run security audits and provide consulting;
- ▶ “Implementer” to maintain the infrastructure;
- ▶ “Specialist” to dig into the forensics and deal with challenging technicalities.

**Of course,  
any key function can be assumed by anyone anytime!**



# CERN Computer Security Team

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

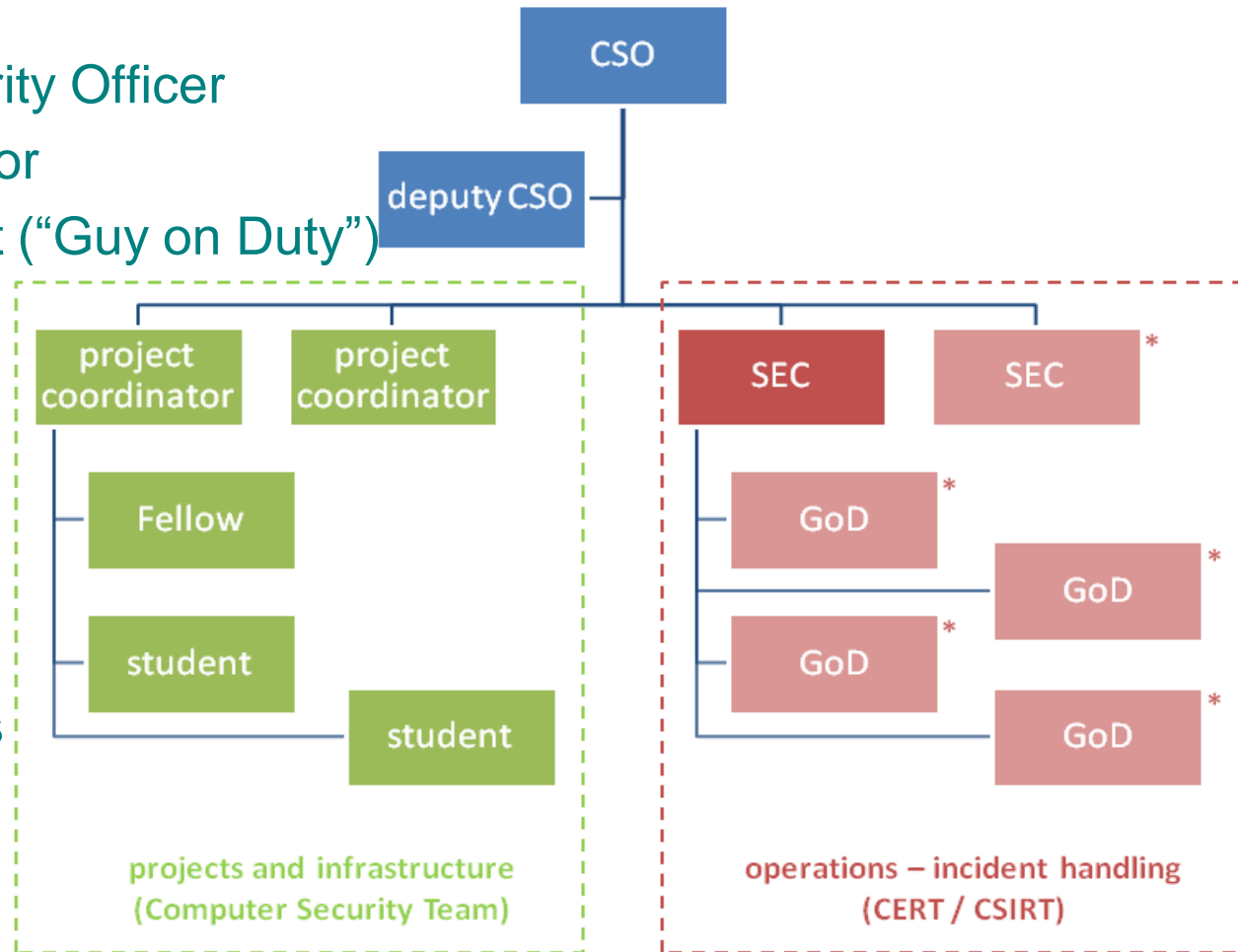
- ▶ **CSO:** Computer Security Officer
- ▶ **SEC:** Security Escalator
- ▶ **GoD:** first line support (“Guy on Duty”)

## ▶ Manpower:

- ▶ 4 staff  
i.e. CSO and SEC
- ▶ 1 fellow
- ▶ 2-3 students
- ▶ 5 external contributions  
of 10% for first line

## ▶ Pipeline:

- ▶ About 40 different on-going and pending projects
- ▶ incl. coordination of external efforts (Web services, comp’g clusters, ...)



# CERN Computer Security Team

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012

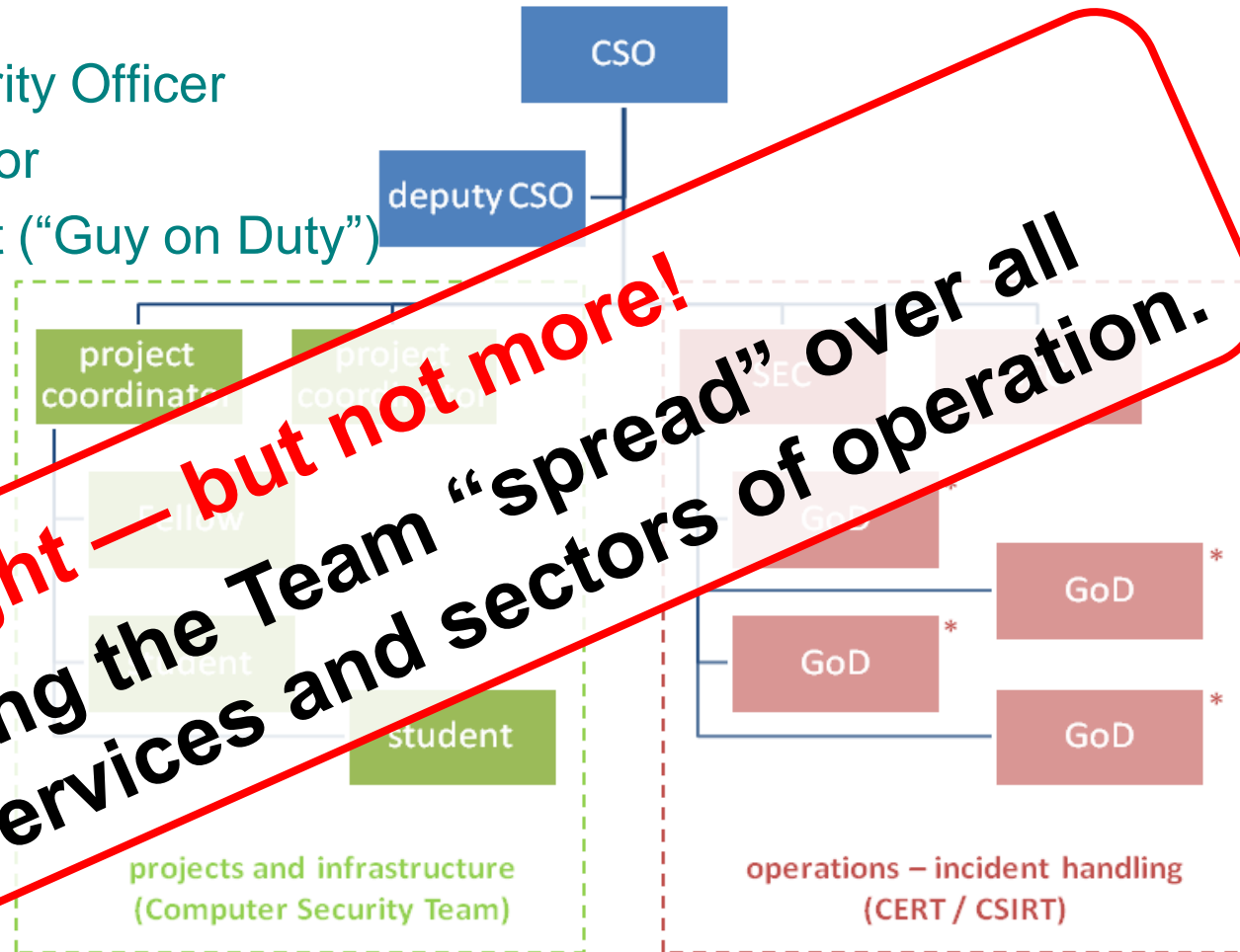
- ▶ **CSO:** Computer Security Officer
- ▶ **SEC:** Security Escalator
- ▶ **GoD:** first line support (“Guy on Duty”)

## ▶ Manpower:

- ▶ 4 staff  
i.e. CSO and SEC
- ▶ 1 fellow
- ▶ 2-3 students
- ▶ 5 external contributors  
of 10% for first line

## ▶ Pipeline:

- ▶ About 10 different on-going and pending projects
- ▶ incl. coordination of external efforts (Web services, comp’g clusters, ...)





**CERN's Security Footprint**  
is **heterogeneous and vast**



However, **security events** happen  
and **will continue** to happen



Iterate on the **right balance**:  
**Academic Freedom vs. Operation vs. Security**



Lot's of **efforts on prevention & protection**  
while maintaining good **detection & response**



**Enable users assuming responsibility.**  
**Provoke a Change-of-Mind!!!**



# Summary

Computer.Security@cern.ch — Openlab Summer Student Lectures — July 3rd 2012



CERN's Security Footprint  
is **heterogeneous and vast**



However, **security events** happen  
and **will continue** to happen



Academic

**right balance:**  
Operation vs. Security

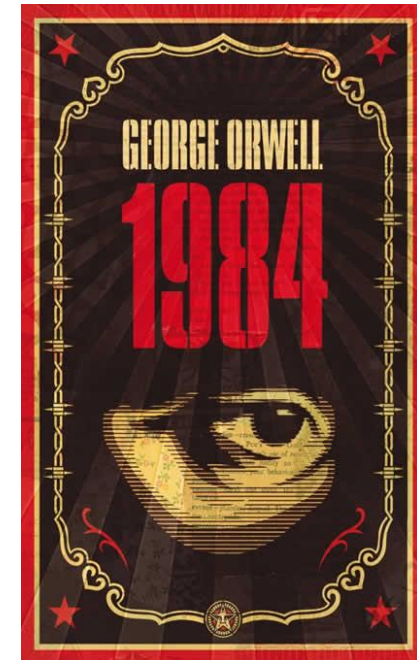
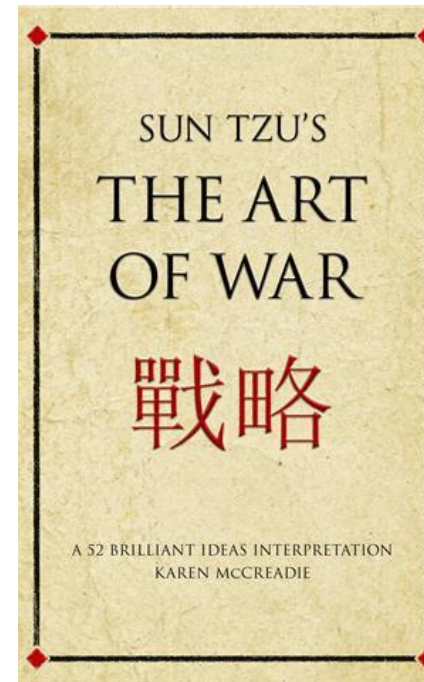
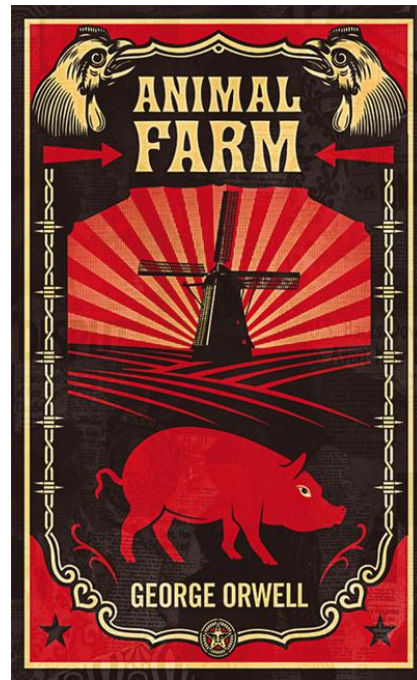
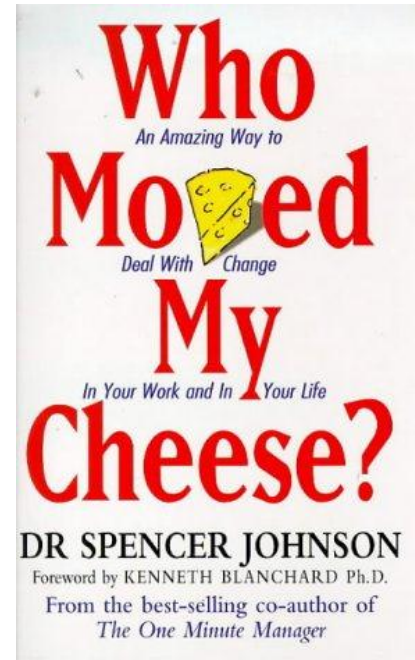


“Computer Security” is rather a  
**sociological problem**, less a technical one!  
Lot's of efforts on **prevention & protection**  
While maintaining good **detection & response**



**Enable users assuming responsibility.**  
**Provoke a Change-of-Mind!!!**





...and, of course,  
there are plenty of (good) books on computer security!!!