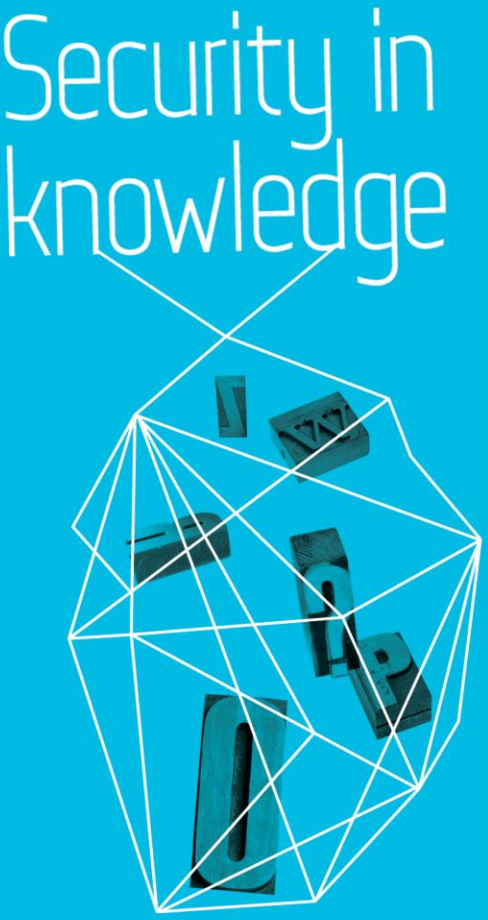
BUILDING YOUR OWN CENTRAL INTELLIGENCE SYSTEM IN THE REAL WORLD



Jan Hertsens
LiveOps

Ryan Barrett
Intermedia

Session ID: END-F42

Session Classification: Intermediate

INTERMEDIA

liveops

What is this session about?

- Building your own security geek system that can automate a broad range of security tasks including:
  - ✓ Logical/Physical access monitoring
  - ✓ Google earth data visualization (and Geo-IP)
  - ✓ XSS face-palm generator
  - ✓ Custom "lock your screen" shamer
  - ✓ Compliance nagging tool

Different Backgrounds

Jan

- Came from business consulting
- Started own malware analysis firm

Ryan

- Operations, security and compliance background

The problem:

so many boxes,
so little time

You’re doing it wrong

- Making manual requests for information from system owners
- Manually using excel spreadsheets, vlookups to organize the data
- Time consuming and boring
- Dangerous? Maybe.
- Definitely a misuse of time.

Your doing in right!

- Build a repeatable, automated system
- Connect and gather data centrally
- Create web based reports dynamically
- Use open source software
- Use spare hardware

Principles

1. Suck up all the data you can find
2. Consolidate & Cross-reference
3. … Find nuggets
4. Profit!

Getting started

What you need:

- Box (or VM instance)
- Database
- Web server
- Scripting language

What we did:

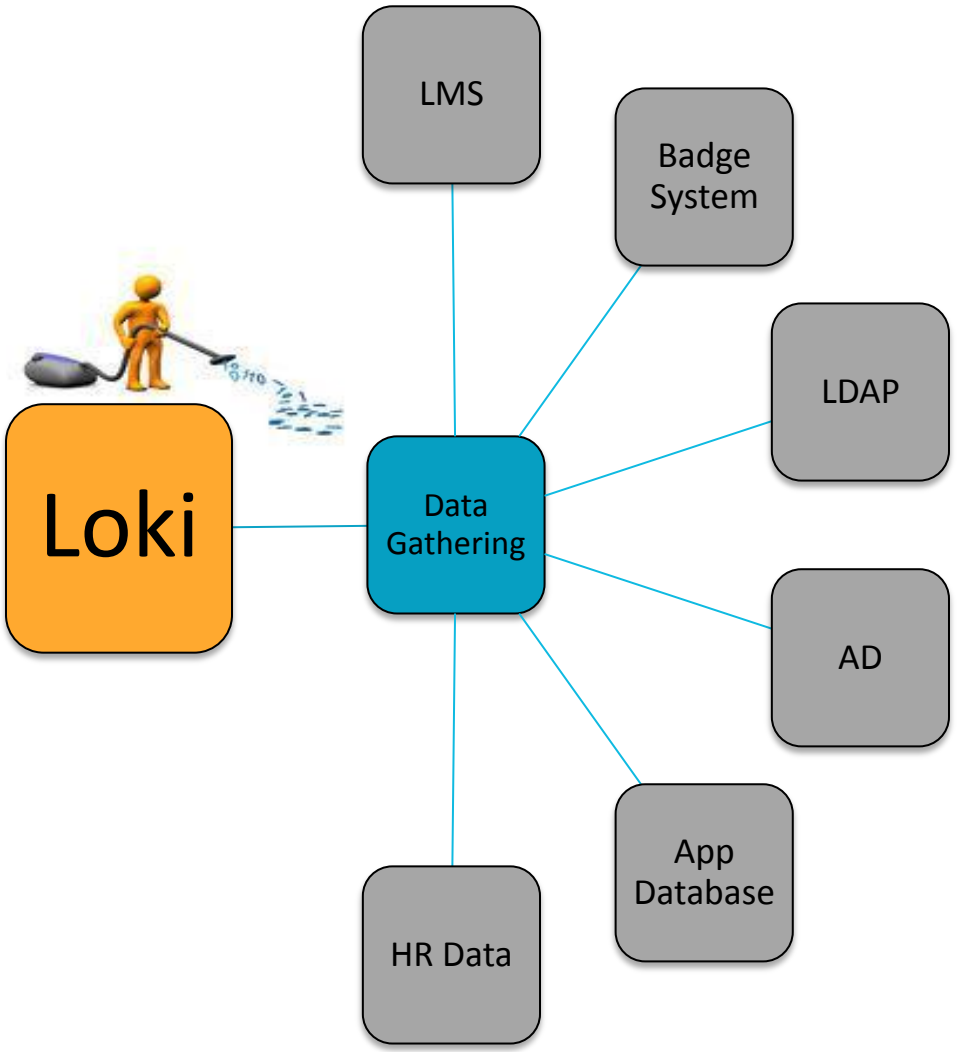
- Basic LAMP (Linux/Apache/MySQL/PHP)

You can make this in Perl, Ruby, ASP, Java

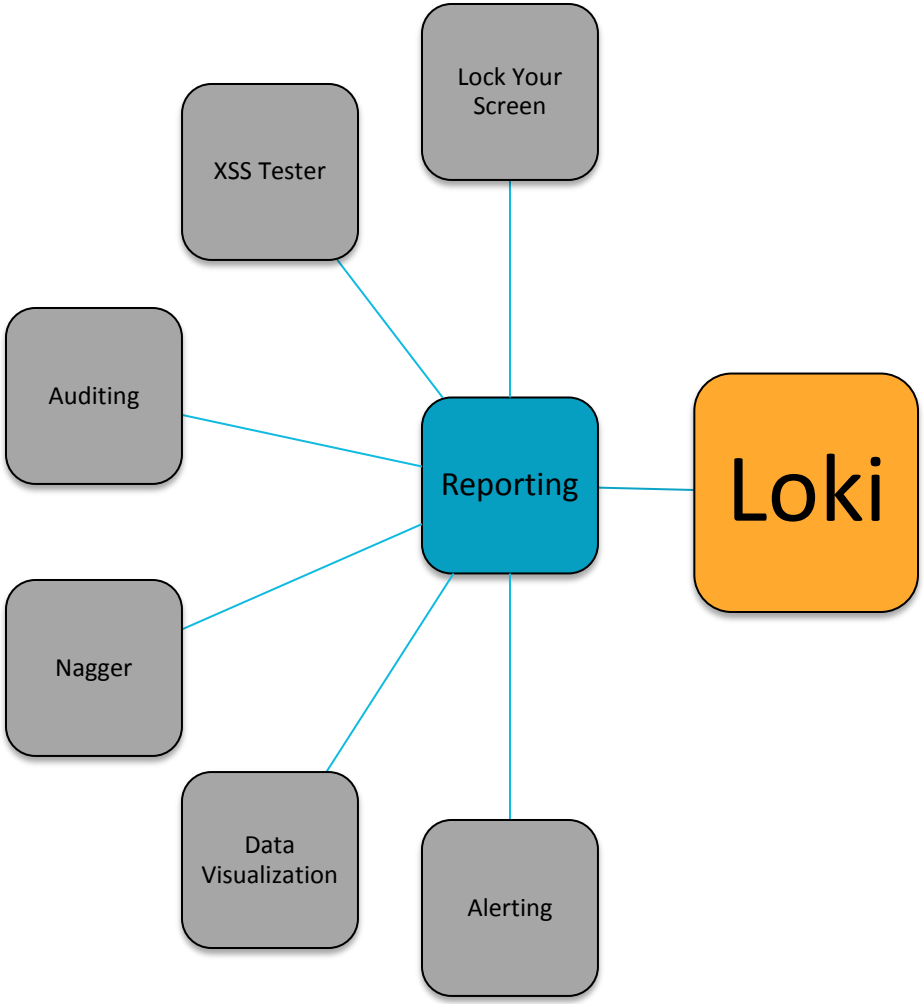
Isn’t this some sort of SIEM?

- No
- SIEM’s typically focus on an IP address as the central data point
- Our system focused mainly on employee data, application and system data, and source code.
- Your system can pivot on anything you want; you decide.

Logical view- Data Gathering



Logical view- Reporting



How do we cross-reference users across various systems?

INTERMEDIA

liveops

Problem

- Disparate systems (each with their owner) that have different naming conventions for users
  - E.g. JoeSmith@corp.com, jsmith, jacks, U3110, nibbler
- The Hertsens theorem:
  "Over time, the accuracy of any reference data source will exponentially approach zero unless it is directly linked to a financial consequence."
- "Follow the money" rule leads us to HR
  - Payroll list is managed very accurately!
  - Contractors & contract pay is audited closely!

Solution: HRID

- HR now assigns a unique numerical “HRID” to each employee, vendor or contractor when they are hired.
- One time effort to retrofit existing user accounts
- Integrate into process
  - Work with HR, Finance and Sys Admins
  - Mandatory field on “new hire” forms
  - Stored in every system at account provision time
    - LDAP, AD : Unused attribute field
    - Badge system: Found an unused field
    - SAP: Found an unused field

HRID : Paydirt!

- Physical and logical access reviews are now automated, and instantaneous
- Instead of weeks of manual work every quarter:
  - Cross-referencing happens automagically
  - Review runs every night
- White-list approach instead of blacklist of “terminated users”
  - Answers the question “who has an account on my system who doesn’t have a business relationship with the company?”

Connectors

INTERMEDIA

liveops

Find your data sources

- SAP (HTTP post)
- HR upload (HTTP post, manual)
- Application database (DB connection)
- Active Directory
- LDAP
- CVS Code Repository
- Learning Management System Badge system (MS SQL)
- Badge system (via undocumented API)
- …

Connector Example: App Database

Simplest case: We need some information from an database that we have native support for.

```
$res=db_select_array("
        SELECT  DISTINCT
        r.rep_id, username, `name`,firstname, lastname,
        email, ra.last_login_success
        ,(SELECT GROUP_CONCAT(p2.name) FROM ccconf.rep_permission rp2, ccconf.permission p2
        WHERE rp2.rep_id=r.rep_id AND p2.permission_id =rp2.permission_id ) Perms
        ,(SELECT rv.value FROM rep_value rv WHERE r.rep_id = rv.rep_id  AND rv.attribute_id = 8315 ) `HRID`
        FROM ccconf.rep r, ccconf.rep_activity ra
        JOIN ccconf.rep_permission rp ON (rp.permission_id IN (15,16,18,728,729,879) AND rp.rep_id=r.rep_id  )
        WHERE callcenter_id=1 AND r.disabled=0
        AND ra.rep_id=r.rep_id
        AND NOT EXISTS (
        SELECT 1
        FROM ccconf.rep_permission rp2
        WHERE rp2.rep_id = r.rep_id AND rp2.permission_id ir
        ORDER BY 1
        ",$m);

$vals='';  $groups=$groupsraw='';
echo "<table>";
foreach ($res as $user)
{
    $empid=$user['HRID']+0;  if (!($empid)) {
        $empid='NULL';
    }

    echo  "<tr><td>". $user['username']                                    . $empid . "</td></tr>\n" ;

    $sql="insert into lo_ccusers
    (rep_id,username,lastname,firstname
    ,groups,last_use
    ,active,employee_id,firstseen,lastseen,created,updated
    ) values
    (" .$user['rep_id'] .", '" . db_escape($user['username']) ."', '" . db_escape($user['lastname']) ."', '" . db_escape($user['fi
    , '" . db_escape($user['Perms']) ."', '" . db_escape($user['last_login_success']) ."'
    ,1,$empid,now(),now(),now(),now() \n )
    ON DUPLICATE KEY UPDATE active=values(active), lastseen=now(), employee_id=values(employee_id)
```

Grab data from the remote datasource

Massage it a bit, then insert into our database

Connector Example: LDAP/AD

- Luckily, we have a LDAP interface we can load

```
$LDAP_SERVER    =GetConfig('ADSERVER');
$LDAP_U         =GetConfig('ADUSERNAME');
$LDAP_P         =GetConfig('ADPASSWORD');
$LDAP_BASE      ='OU=LiveOpsUsers,DC=Corp,DC=liveops,DC=com';

if (!$LDAP_SERVER or !$LDAP_U or !$LDAP_P) { die ('Missing configuration

// ---- Get full LDAP list

//  Pull it from the LDAP
?><h2>Full List</h2><?php


echo "\n<h3>Employees</h3>\n\n\n";

$LDAPUserquery='(&(objectClass=person)(objectClass=user))';
$res=GetLDAP_List($LDAP_SERVER,$LDAP_U,$LDAP_P,$LDAPUserquery ,$LDAP_BASE
$res=LDAPArrayCleg    ($res);
```

Grab list of users from correct tree and class

```
foreach ($res as $user)
{
 if (String_Begins_With('z - ',$user['cn'])) { continue; }
 if (String_Begins_With('aaa - ',$user['cn'])) { continue; }
 $empid=$user['extensionattribute10'];
  $uid=$user['samaccountname'];
 if (!$uid)
  {  $uid=$user['mailnickname'];   }
 if (!($empid)) { $empid='NULL'; }
 $has_vpn=0;
 if (is_array($user['memberof']) and in_array($vpngroup,$user['memberof']))
        { $has_vpn=1; }

 $myexpire=$user['accountexpires'];
 if ((!$myexpire) or ($myexpire==9223372036854775807))
  {  $myexpire='NULL';  }
  else
    {  $myexpire= win_time_to_unix_time($my      e) ;
       $myexpire=" FROM_UNIXTIME($myexpire)";
     }


 if ($vals) { $vals .= ','; }
 $vals .= "('". db_escape($uid)."','". db_escape($user['cn'])."',$empid,$has_vpn,$myexpire
 ,now(),now(),now(),now()) \n  ";

 echo  "<tr><td>". $uid . "</td><td nowrap>" . $user['cn'] . "</td><td>" . $empid . "</td></

 }
echo "</table>";
if ($vals)
 {
$sql="insert into lo_aduser
    (uid, fullname, employee_id,has_vpn, accountexpires, firstseen, lastseen,created, update
    values $vals
     ON DUPLICATE KEY UPDATE lastseen=now(),active=1
            , employee_id=values(employee_id) , has_vpn=values(has_vpn)
```

Our business logic

Work around MS specific weirdness

Pump it into our database

Connector Example: Learning Mmgt System (MSSQL)

- It has a database, but we had NO native drivers!

```
-rwxr-xr-x 1 jhertsens eng    454 Nov  5 20:18 lms_export.sh
-rwxr-xr-x 1 jhertsens eng    302 Jan 27  2012 lms_import.sh
-rwxr-xr-x 1 jhertsens eng    282 Jun 14  2012 lms_parse.sh
-rwxr-xr-x 1 jhertsens eng     48 Jan 12  2012 lms_run.sh
-rw-r--r-- 1 jhertsens eng     40 Jan 11  2012 lmscommands.sql
-rw-r--r-- 1 jhertsens eng 490440 Jan 25 14:37 lmsout.txt
-rw-r--r-- 1 jhertsens eng  32411 Jan 25 14:37 lo_lmsusers_import.t
[jhertsens@loki-master1.lab lms]$ cat lmscommands.sql
select * from vw_LO_SecurityCourse
GO
```

- So we hacked together a bunch of scripts

```
# Because lab dns is f-ed, we need to hack the ip in there
bsqldb -S 10.32.54.555  -U mulder -P  trustno1  -D inquisiqEX  -i lmscommands.sql -o lmsout.txt > /dev/null 2> /dev/null
```

Call an (experimental) binary that can access the db, grab output

```
sed 's/\s\s\s*/\t/g' lmsout.txt > lms_out2.txt
#tail  lms_out2.txt
# rm  lmsout.txt
```

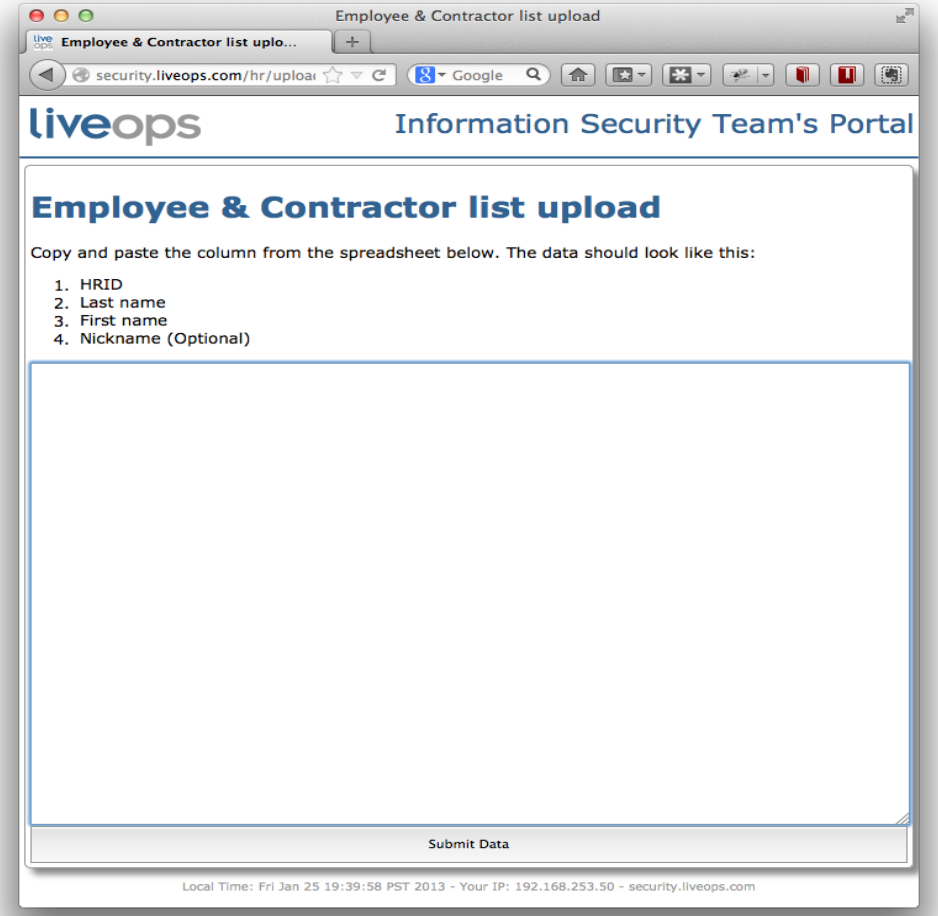
Use file massaging to turn it into a reasonable format

```
mv lms_out2.txt lo_lmsusers_import.txt

echo Importing...
mysqlimport $creds -f  --delete    secteam  $curdir/lo_lmsusers_import.txt

#rm lo_juniperlog_import.csv

echo Processing...
mysql  $creds -v  -e "CALL secteam.sp_process_lms();"
echo Done.
```

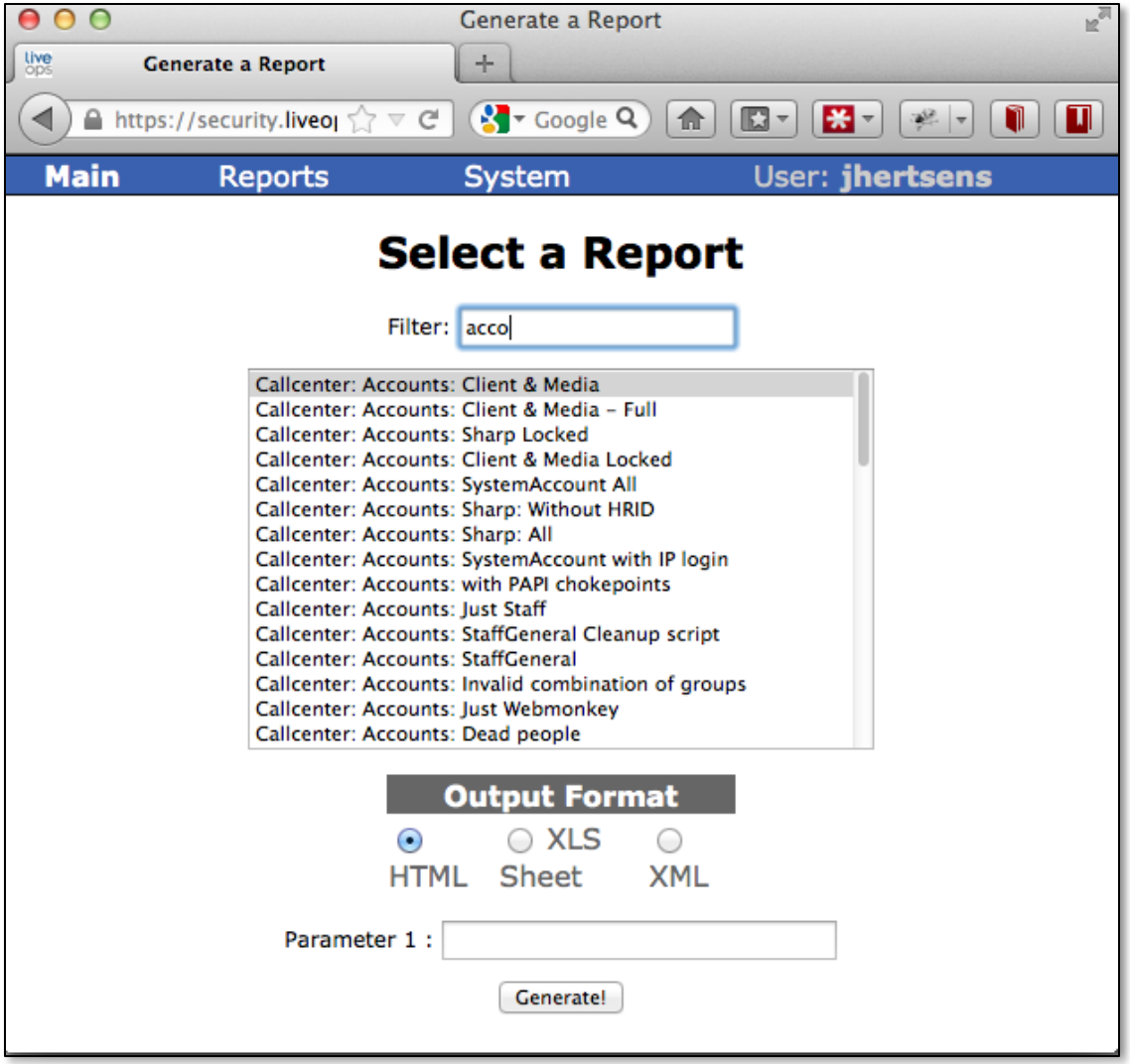
Bulk process the raw results into the database, then clean up

Do all the connectors have to be scripted and automated?

- No
- The company had a small HR system that could not be connected programmatically.
- The HR person manually uploaded (copy/paste) from their excel spreadsheet into an http form we created for them.



Report Generator



Behind the scenes...

id	descr	descr_long	weight	qry	mailcompat	public	alerting	entity_id	connection	alert_email
152	Bugzilla: Rowobject fixes patches (Overview)	NULL	77	SELECT b.bug_id `ID`, b.bug_stat...	0	0	0	6	bugzilla	NULL
154	Network: Machine classes and permissions	NULL	61	SELECT class `Machine Class`, c.a...	0	0	0	NULL	NULL	NULL
155	Bugzilla: Reviewbot recent usage	List of bugs that have reviewbot fl...	70	SELECT b.bug_id ID, b.bug_status...	0	0	0	6	zilla	NULL
156	Callcenter: Accounts: Sharp Locked	All LOCKED users with any of Shar...	2	SELECT r.r id AS ID, username,...	0	0	1	1	onf_dev	NULL
157	Callcenter: Accounts: Systemaccount with password changes	All active users without password...	3	SELECT	0	0	0			NULL
158	Network: List of visible machines with web ports	NULL	67	SELECT NCT(IP)	0	0	0			NULL
159	Network: Systems not in KPPs	List of machines detected during s...	69	SEL stactive...	0	0	0			NULL
160	Bugzilla: Reviewbot passed : Checklist	List of bugs that have	71	SEL _status...	0	0	0			NULL
163	LDAP Accounts: with HRID anomalies	Active users in LDAP that do not h...	57	SEL name, s....	0	1	1	3	NULL	azahabi@lived
164	Network: Machine list with Redzone info	NULL	68	SEL	0	0	0	NULL	NULL	NUL
165	AD: Accounts with HRID anomalies	NULL	93	SELECT	0	1	1	NULL	NULL	it-s port@liv
166	Callcenter: Callcenters and encryption key names	Reference list to verify that encryp...	39	SELECT c.callcenter_id `ID` , NAM...	0	1	0	NULL	ccconf_dev	NUL
167	Users with HRID	Reference list of know active empl...	109	select *, HRID `ID` from vw_hrlist...	0	1	0	13	NULL	NUL
168	Callcenter: Accounts: SystemAccount All	NULL	4	SELECT DISTINCT r.rep_id AS ID, u...			0	1	ccconf_dev	NUL
169	Callcenter: Accounts: SystemAccount with IP login		7	SELECT DISTINCT r.rep_id AS ID, u...			0	1	ccconf	
170	Callcenter: Accounts: StaffGeneral	Accounts with "StaffGeneral" rights.	11	select r.rep_id as ID, username, `...			0	1	ccconf	
171	Callcenter: Accounts: StaffGeneral Cleanup script	This is a list of accounts that have...	10	select group_concat(username or...			0	1	ccconf	
172	AD: All accounts	NULL	92	SELECT uid, fullname, employee_i...	0	0	0	NULL	NULL	
173	Callcenter: IP's of logins by REPID	Given a rep_id, show recent login l...	35	SELECT DATE(logtime) `Date`, INE...	0	0	0	NULL	ccconf_dev	NULL
174	Accounts: Production database users	Users who have mysql access on a...	95	SELECT	0	0	0	NULL	ccconf_dev	NULL
177	AD: No HRID for a week	Active Directory : Users created m...	94	SELECT uid, fullname, DATE(firstse...	0	1	0	NULL	NULL	NULL
178	Bugzilla: Reviewbot passed with QA flag	List of bugs that have	72	SELECT b.bug_id ID, b.bug_status...	0	0	0	6	bugzilla	NULL
179	S2: Accounts with HRID anomalies	NULL	90	SELECT	0	1	1	NULL	NULL	it-support@liv
180	Accounts: Terminated by HR, still have access	People who are terminated accordi...	96	SELECT h.lastname, h.firstname, h...	0	0	1	NULL	NULL	jhertsens@live
181	Callcenter: Groups and usage	NULL	41	SELECT pr.permission_id, pr.ide...	0	0	0	NULL	ccconf_dev	NULL
182	Callcenter: Anomaly: Duplicate rep emails	A list of duplicate email addresses...	42	SELECT email, COUNT(email) AS o...	0	0	0	NULL	ccconf_dev	NULL
183	Callcenter: Accounts: Invalid combination of groups	Accounts with "contradicting" gro...	12	SELECT DISTINCT r.rep_id AS ID, u...	0	0	0	1	ccconf_dev	NULL
184	Callcenter: Accounts with HRID anomalies	NULL	46	SELECT s.rep_id `ID`,	0	0	1	1	NULL	it-support@liv

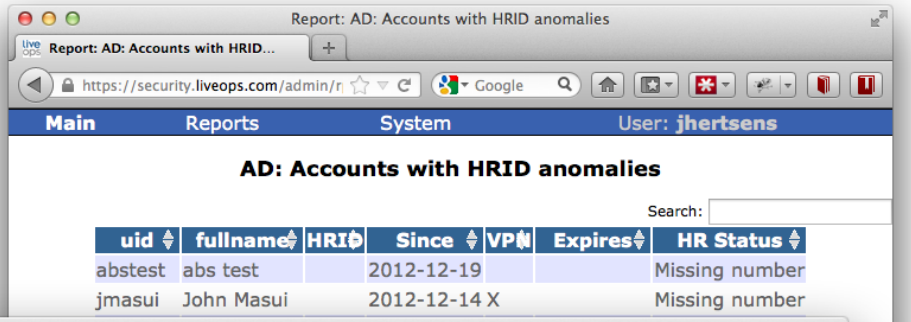
SQL for reports

Database

Enable for mailings

Email for alerting

Report Examples



Report: Callcenter: Accounts: Suspected Active Mailboxes

Report: Callcenter: Accounts: Su...

https://security.liveops.com/admin/rpt/report_main.php?reportnum=93&do_xls=0&p1=&submit=Generate!

Google

Main | Reports | System | User: jhertsens

Callcenter: Accounts: Suspected Active Mailboxes

Callcenter accounts that have the "All send" flag turned on

Search:

ID	username	name	firstname	lastname	email	phonenum	comment	last_login_success	
99053	LOUSupport	LOUSupport (LOU)	LOU	Support				0000-00-00 00:00:00	StaffGenera
94117	LiveOps Advocacy	LiveOps Advocacy (LiveOps Advocacy)	LiveOps Advocacy				account set up for a PB account as per Regan (Marcia)	2009-05-29 18:13:40	StaffGenera
93037	Bilingual Referral	Bilingual Referral	Bilingual Referral					2009-06-02 02:09:23	Mailbox
78216	Spanish Script Suggestions	Spanish Script Suggestions (Spanish Script)	Spanish Script	Suggestions				2009-05-31 22:33:20	Mailbox
69219	Agent License Administration	Agent License Administration	Agent License Administration		pneblock@liveops.com			2009-06-02 12:32:10	Staff
							Support account for ProFlowers program. PM: Adam		

How do we get those darn **users** to behave (in compliance with company procedures)?

INTERMEDIA

liveops

Reminder Mailing System

- Problem: Users “forget” to ..
  - Complete trainings
  - Keep data up to date
  - Login and change their password
- Solution: Automated Reminder system
  - Automates the "reminding" of required (compliance) activities
  - Existing Report + Template + Timing = Reminder

Overview

List of Templates

Description	Mailing Title
Callcenter: Stale accounts warning	FYA: Your Callcenter account "<# username #>" is about to be disabled.
LMS: First Course Nag : Never taken	FYA Reminder: "LiveOps Security Awareness" course
LMS: Re-Take course after 1 year	FYA Reminder: Please re-take "LiveOps Security Awareness" course

Records 1 to 3 of 3

[Create New Template]

List of Jobs

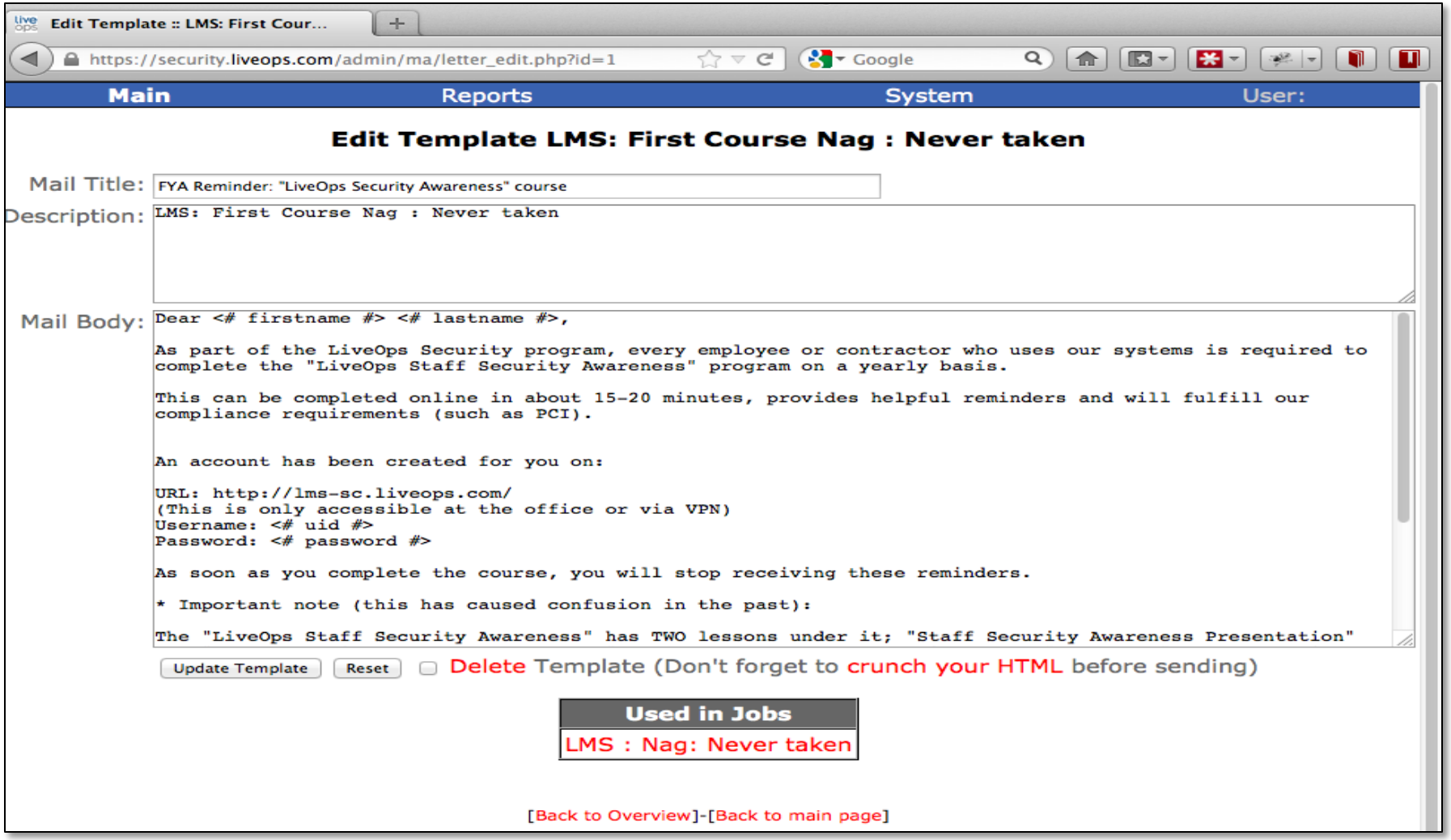
Name	Last Run	Freq.	Enabled
Callcenter: Accounts: Staff gone stale	2012-12-04 05:23:57	7	Yes
LMS : Nag: Never taken	2012-12-01 05:24:07	5	Yes
LMS: Retake after 1 year	2012-12-04 05:23:35	7	Yes

[Create New Job]

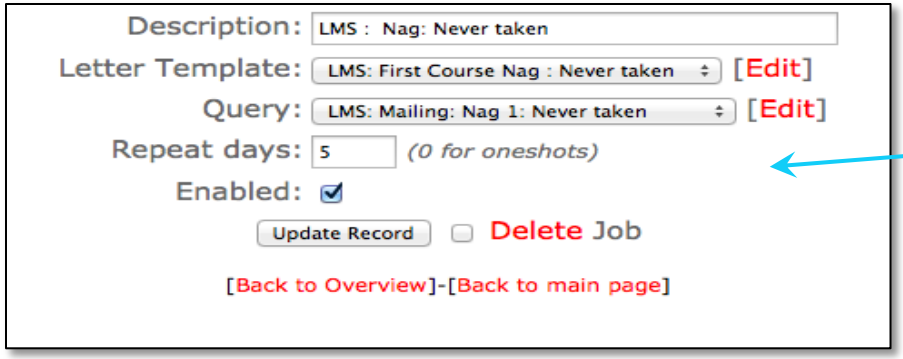
Run batch now

[Back to main page]

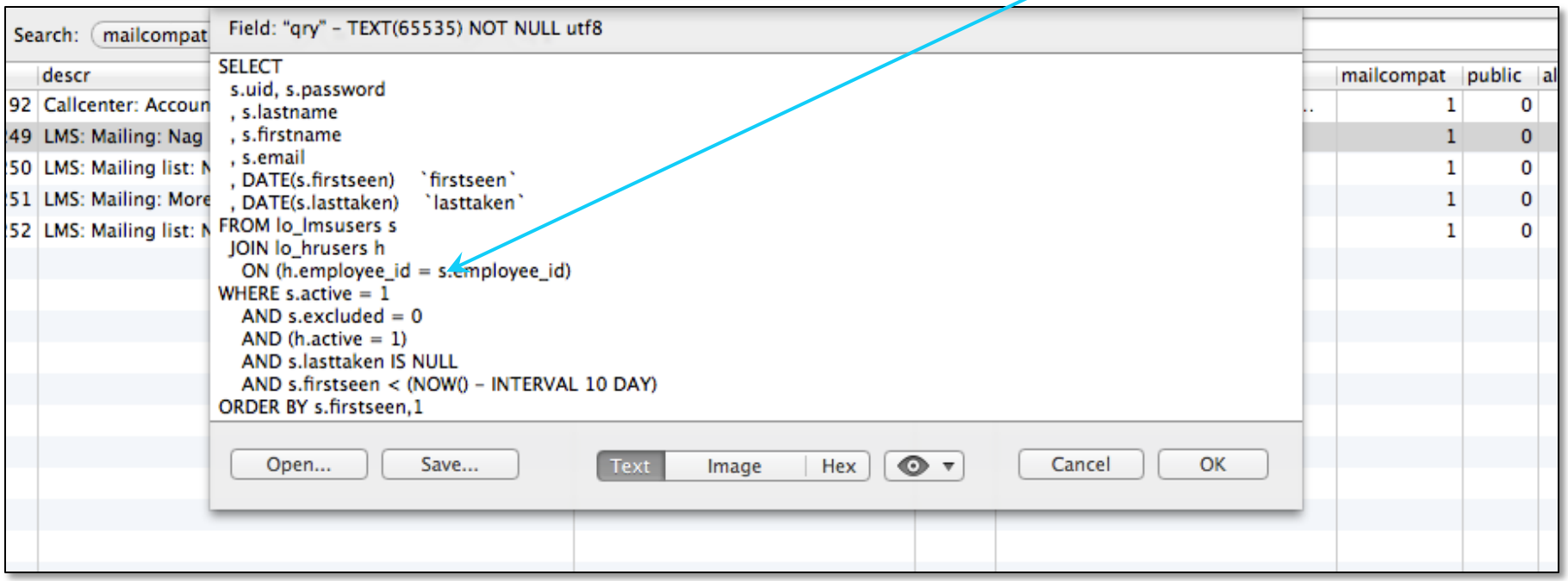
Making it happen



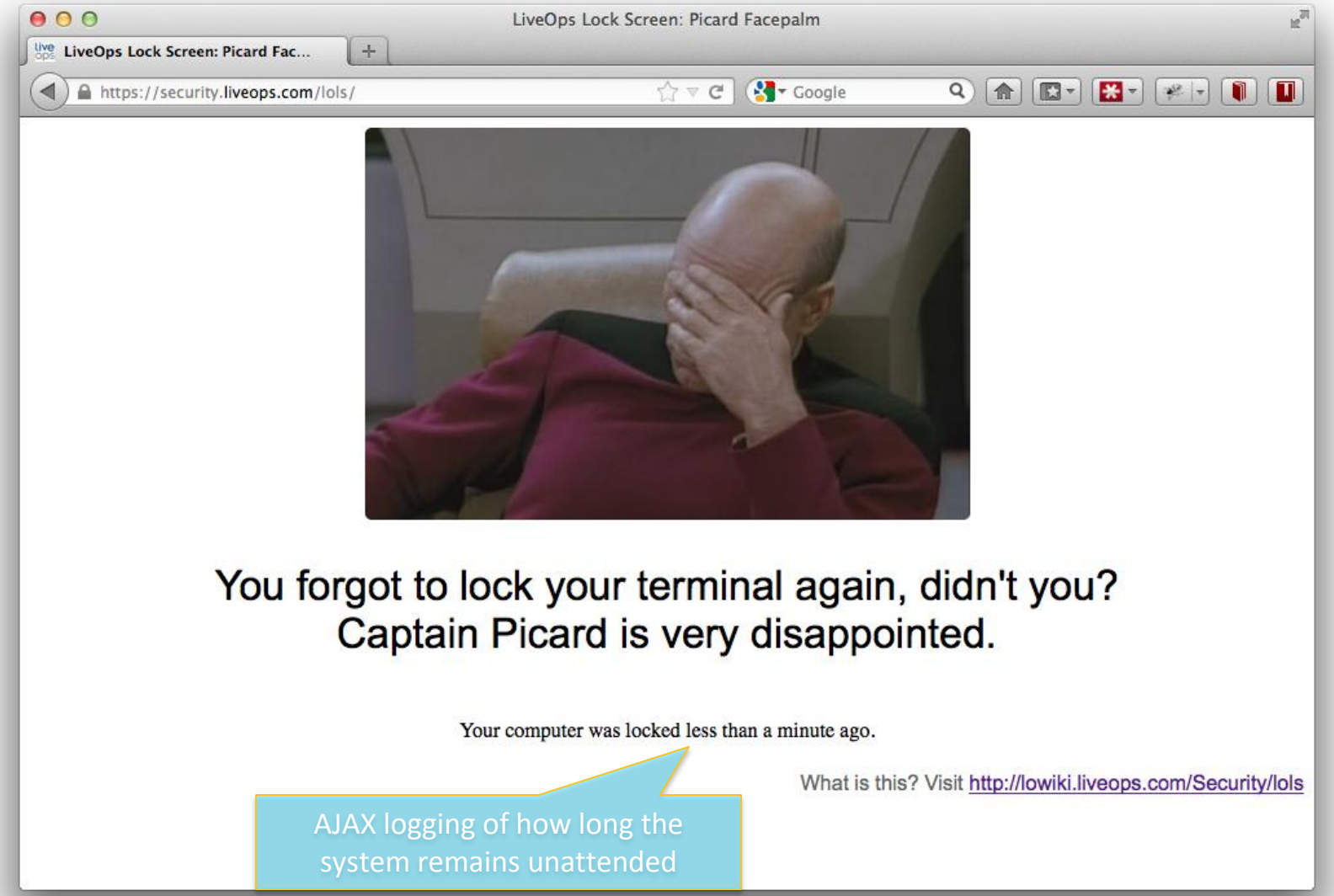
Making it happen (SQL'ness)



Pick what report to run. SQL gets executed when needed, recordset date gets merged into template



“Lock your Screen” system



“Lock your Screen” system

- Problem: Users leave their systems unlocked
  - Closing the gap on screensavers
- Solution: “Lock your screen” shaming system
  - Provide a gamification system
  - Let users “pwn” each other
  - Keep track of the usage stats
  - Publish “top offenders” for extra humiliation

How do we get those darn **developers** to behave (in compliance with company procedures)?

Fighting XSS with face-palms

- Problem:
  Having developers and QA do tests for XSS is boring, repetitive

- Solution:
  Facepalm image generator

Facepalms (Cont.)

- For testers and QA:
  - Fill fields with:
    Test <img src="http://site/fp.php?testcase167"> Test
  - Check if you see a facepalm, yell
- What we log:
  - All parameters supplied
  - Referral URL
  - Time & Date
  - Request IP

Crazy products for fun & profit

INTERMEDIA

liveops

Geolocate everything

- Get the tools:
  - An IP-to-location database
    http://www.maxmind.com
  - An address-to-location API (e.g. Google maps)
    https://developers.google.com/maps/documentation/geocoding/
- Run it on all your data
- Make reports!
  - Visual reports google earth map
  - Transactions per region
  - People logging in from multiple countries
  - Etc…

Make it look interesting

Demo Time!

Conclusion

Lesson Learned

- Think outside the boxes & shelves
- Nobody understands your business but you
- Involve other departments
  - Make their life easier
  - Make allies, get funding & resources

Lesson Learned

- Hire / borrow / cajole a developer!
- Don't be afraid to start. Jump in and build.
- It costs nearly nothing to start.
- Find some extra hardware, prove value, then move up!

Q&A

Source & supporting materials

http://g.obijan.com/LokiSR