Implementando o OSSEC HIDS

Jerônimo Zucco

/me

- Security guy
- blog: http://jczucco.blogspot.com
- Twitter: @jczucco
- zucco on freenode
- http://www.linkedin.com/in/jeronimozucco

Agenda

- Introduction
- Arquiteture
- Log Analysis
- Integrity Monitoring
- Rootkit Detection
- Policy audit

Agenda

- Alerts
- Active Response
- Server and Agents Instalations
- Configuration Files
- Rule Files
- Customize Rules

Security Terminology

LIDS

Integrity Checking

Rootkit Detecion

HIDS ?

Log Management

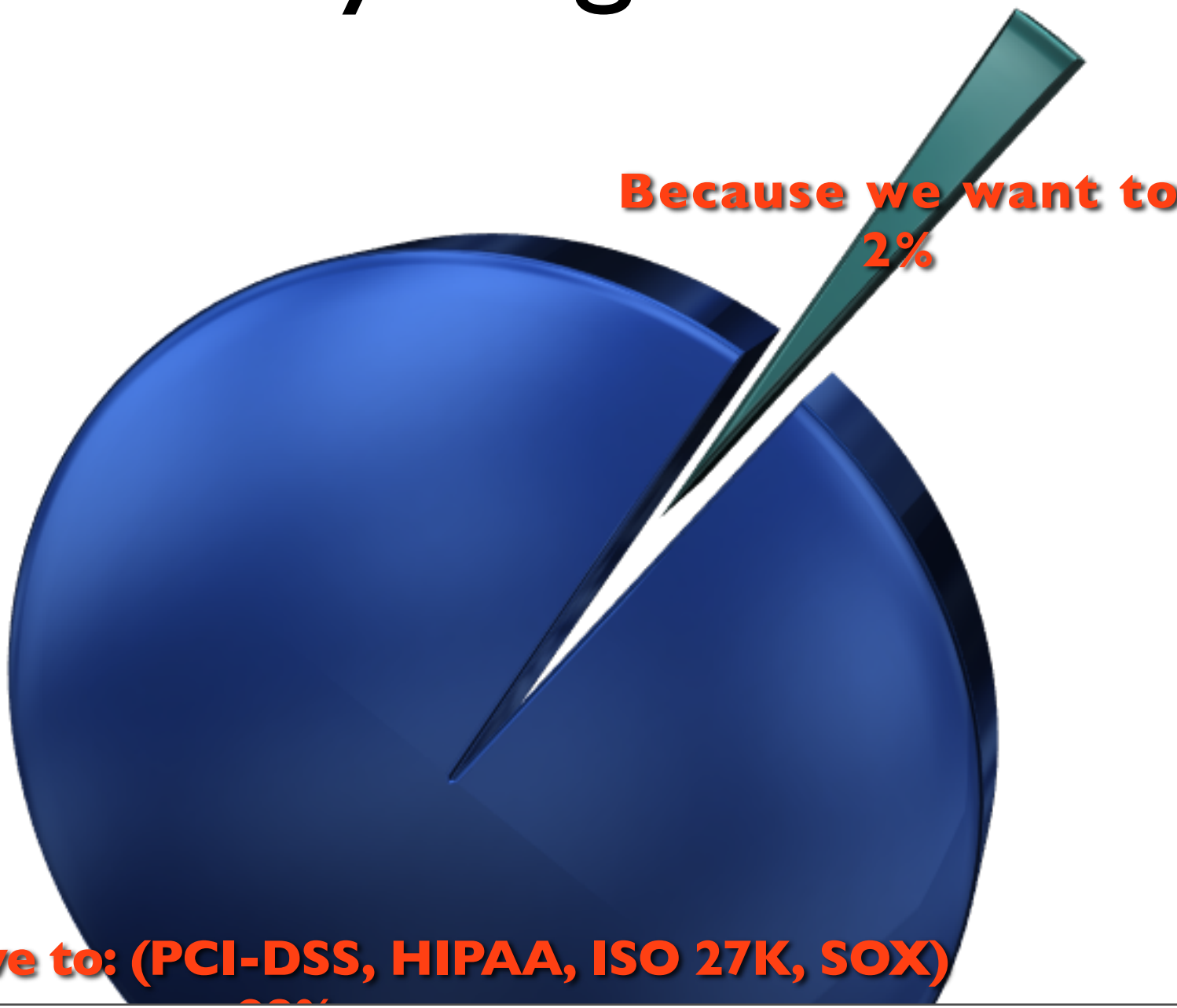
Why Log ?

System monitoring

Compliance

Forensics

Why Log ?

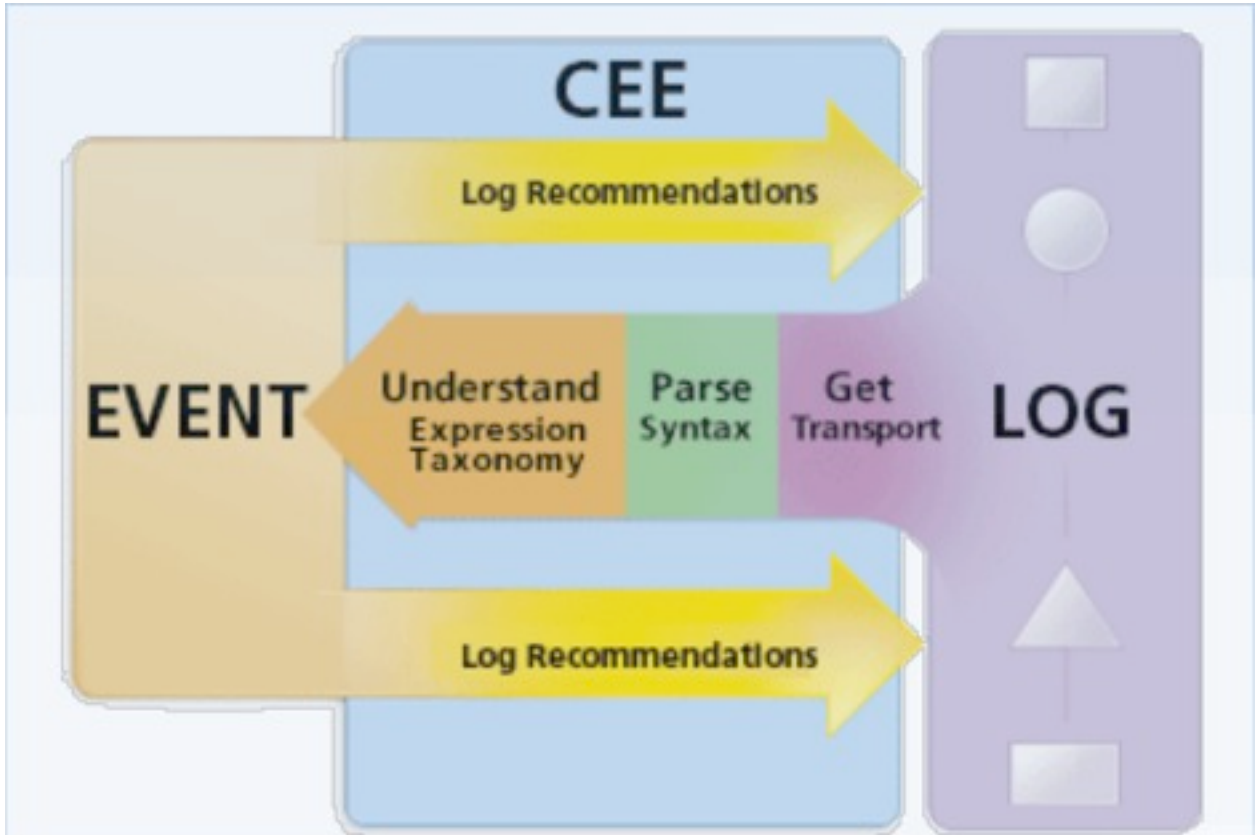

Because we want to
2%
Because we have to: (PCI-DSS, HIPAA, ISO 27K, SOX)

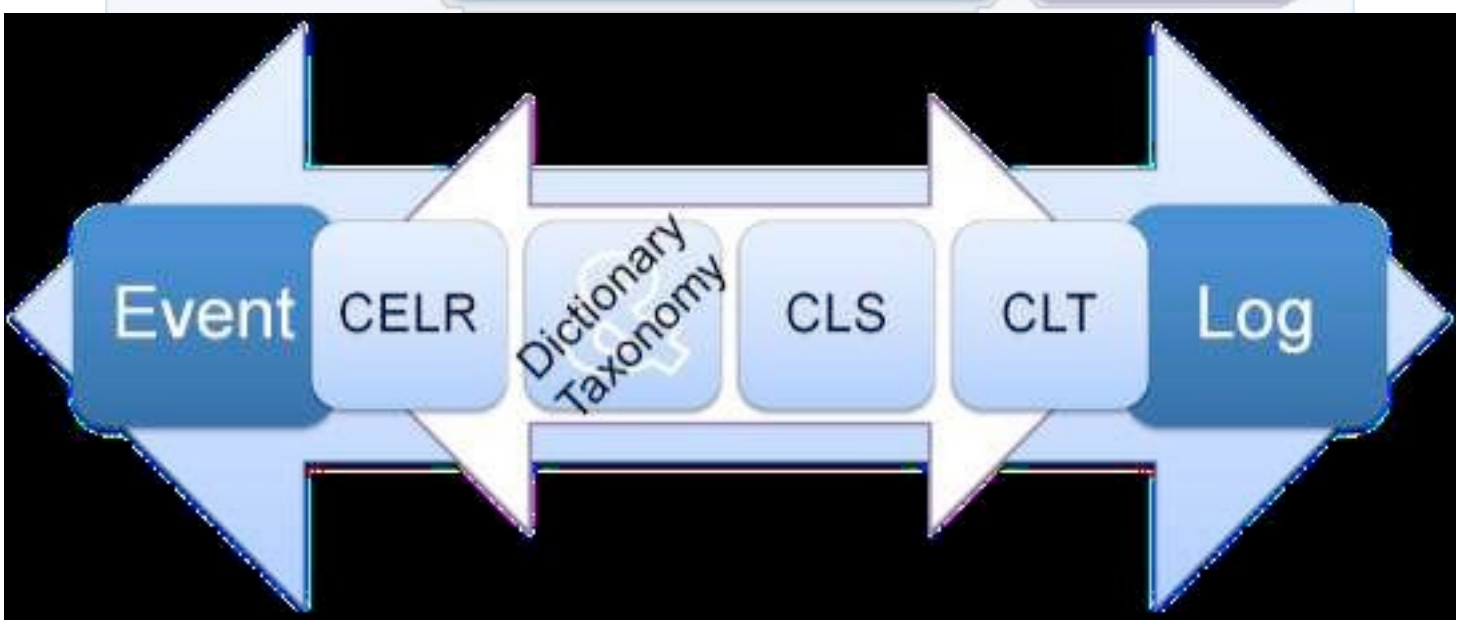
Standards

Syslog: RFC 3164

WELF, CBE, CEF, IDMF

CEE
Common
Event Expression
http://cee.mitre.org


CEE
Log Recommendations
EVENT
Understand
Expression
Taxonomy
Parse
Syntax
Get
Transport
LOG
Log Recommendations


Event
CELR
Dictionary
Taxonomy
CLS
CLT
Log

What is OSSEC?

Daniel Cid

@danielcid

Third Brigade, Trend Micro

- Open Source Host-based IDS (HIDS)
- File Integrity checking
- Registry Integrity checking
- Host-based anomaly detection
- Policy monitoring/enforcement
- Active response

OSSEC HIDS complements a SIEM

OSSEC in the News

- OSSEC #1 open source security tool in the enterprise http://www.linuxworld.com/news/2007/031207-top-5-security.html
- OSSEC #2 IDS tool in the security tools survey. http://sectools.org/ids.html
- More: http://www.ossec.net/wiki/IntheNews

OSSEC Agents

- GNU/Linux (all distributions, including RHEL, Ubuntu, Slackware, Debian, etc)
- Windows XP,2000,2003,Vista,2008,Seven
- VMWare ESX 3.0,3.5 (including CIS checks)
- *BSD
- Solaris 2.7,2.8,2.9 and 10
- AIX 5.3 and 5.3
- HP-UX 10, 11, 11i
- MacOSX 10

Support via Syslog

- Cisco PIX, ASA and FWSM (all versions)
- Cisco IOS routers (all versions)
- Juniper Netscreen (all versions)
- SonicWall firewall (all versions)
- Checkpoint firewall (all versions)
- Cisco IOS IDS/IPS module (all versions)
- Sourcefire (Snort) IDS/IPS (all versions)

Support via Syslog

- Dragon NIDS
- Checkpoint Smart Defense (all versions)
- McAfee VirusScan Enterprise (v8 and v8.5)
- Bluecoat proxy (all versions)
- Cisco VPN concentrators (all versions)

Agentless

- Cisco PIX, ASA and FWSM (all versions)
- Cisco IOS routers (all versions)
- Juniper Netscreen (all versions)
- SonicWall firewall (all versions)
- Checkpoint firewall (all versions)
- All operating systems specified in the “operating systems” section

Supportted Log Formats

- DB Logs (Mysql, PostgreSQL)
- Unix like logs (dpkg, yum, su, sudo)
- Mail Server, FTP, SSH, Xinetd logs
- Web Server logs (apache, IIS, Zeus)
- Web Apps (Horde, ModSecurity)
- NIDS (Snort, Cisco IOS/IPS, Checkpoint)
- Sec.Tools (Symantec and McAfee AV, nmap)
- Windows Events

Secure by Default

- Installation script does the chroot, user creation, permissions, etc
- User has no choice to run it “less secure”
- Each process with limited privileges and tasks

DOCS

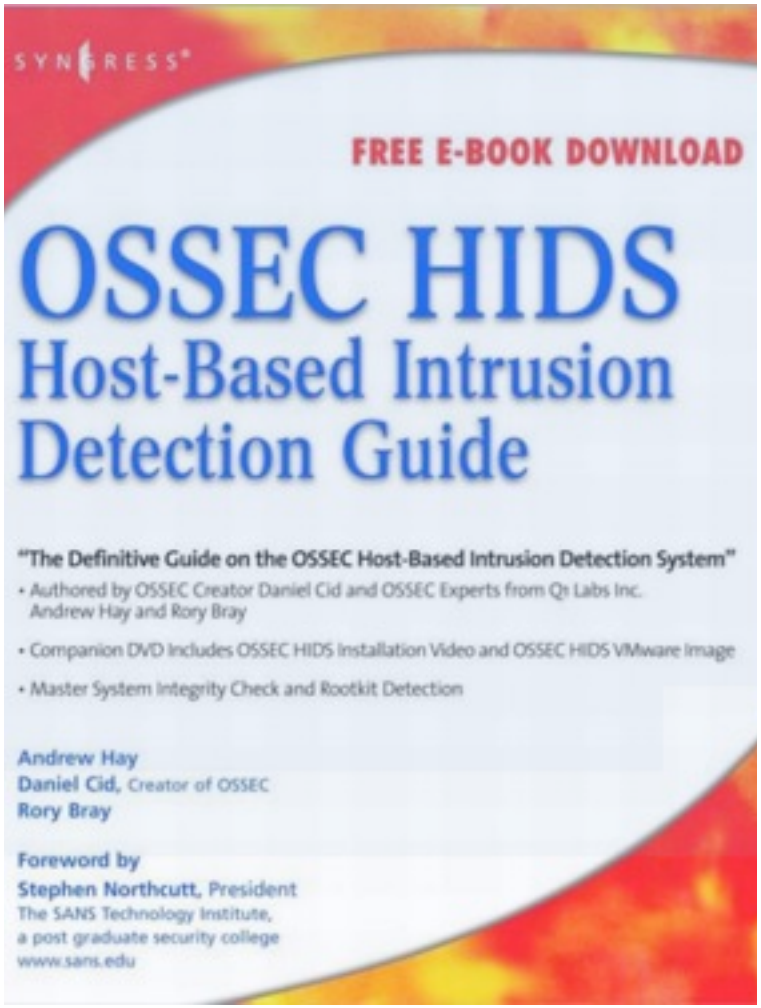
http://www.ossec.net

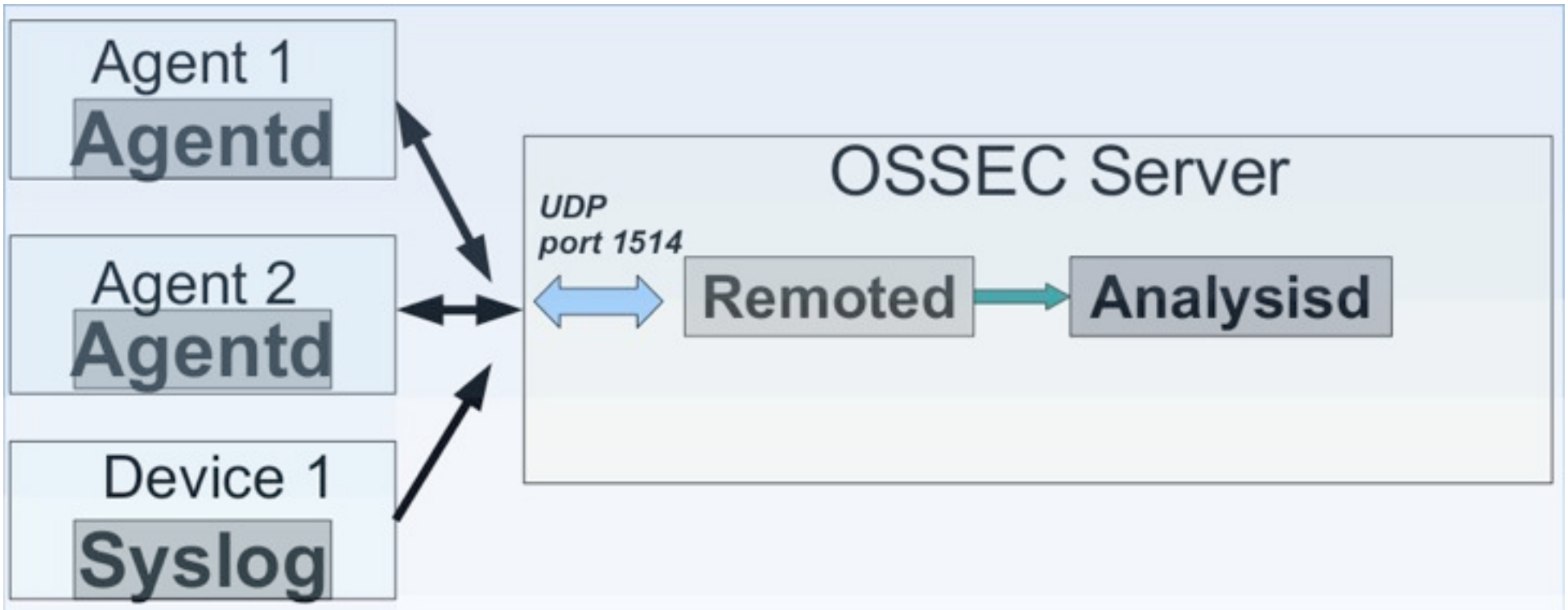
#ossec on freenode

- mailing lists

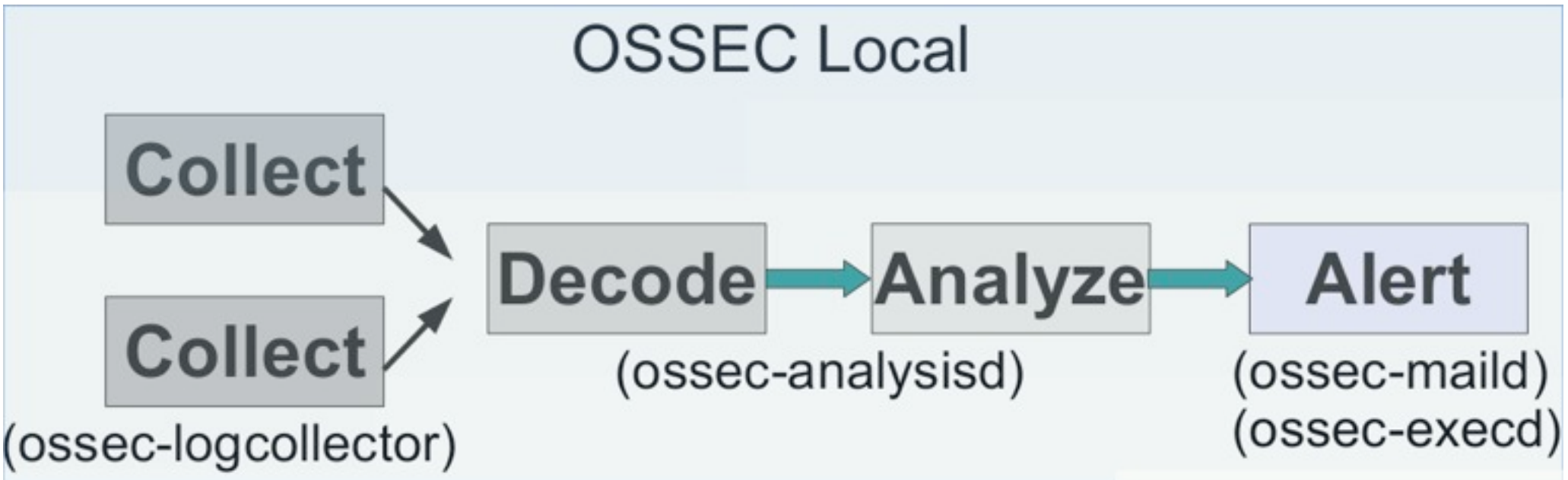
- wiki, manuals, etc

- source :-)

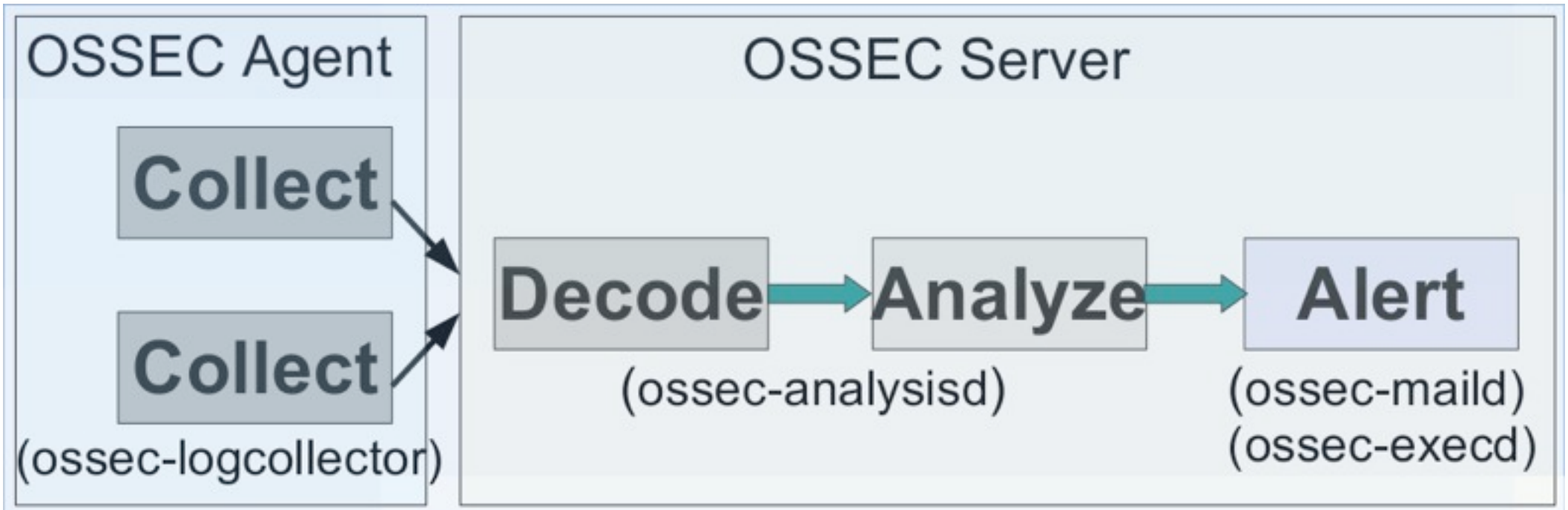




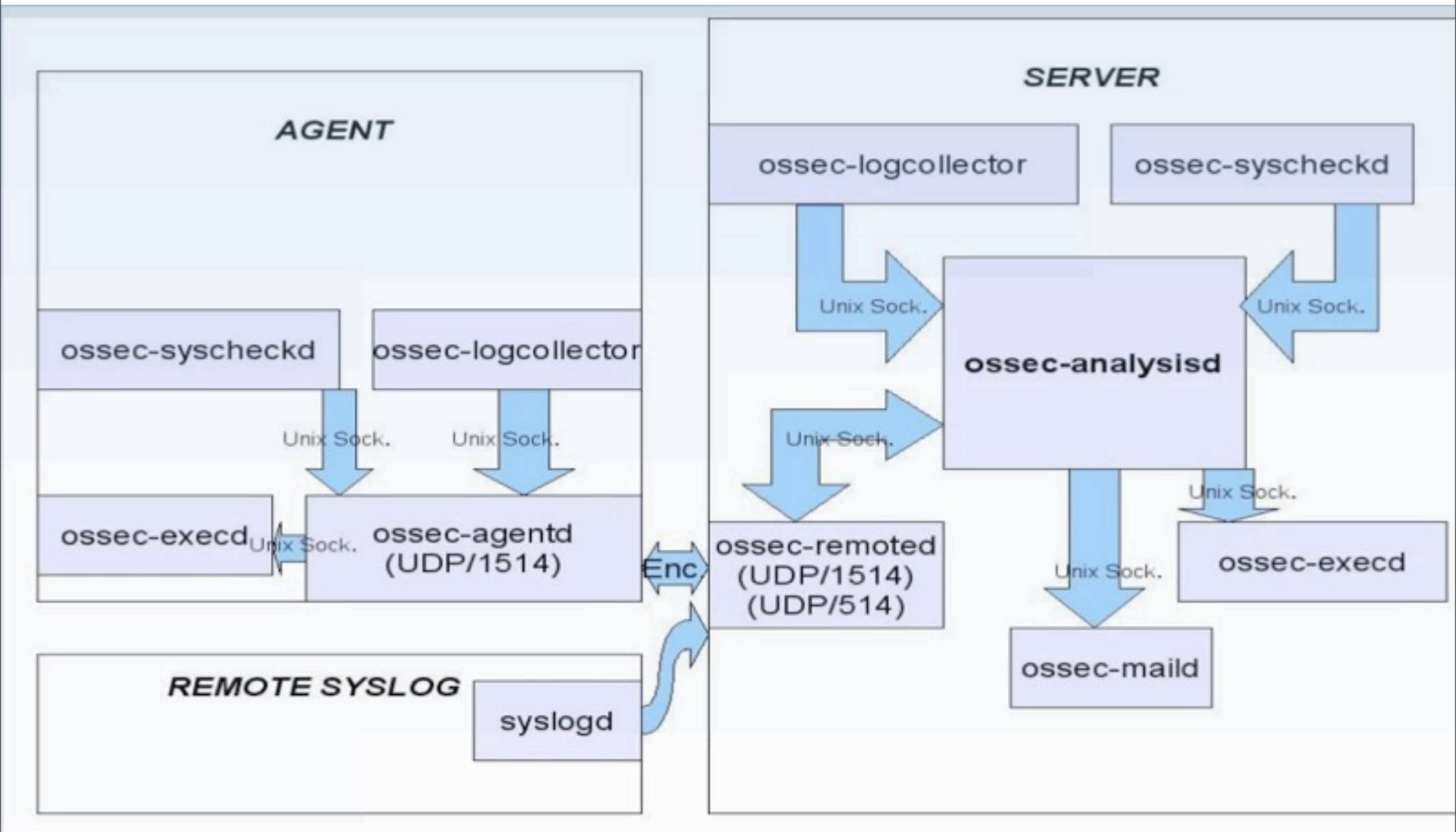
Network Communication



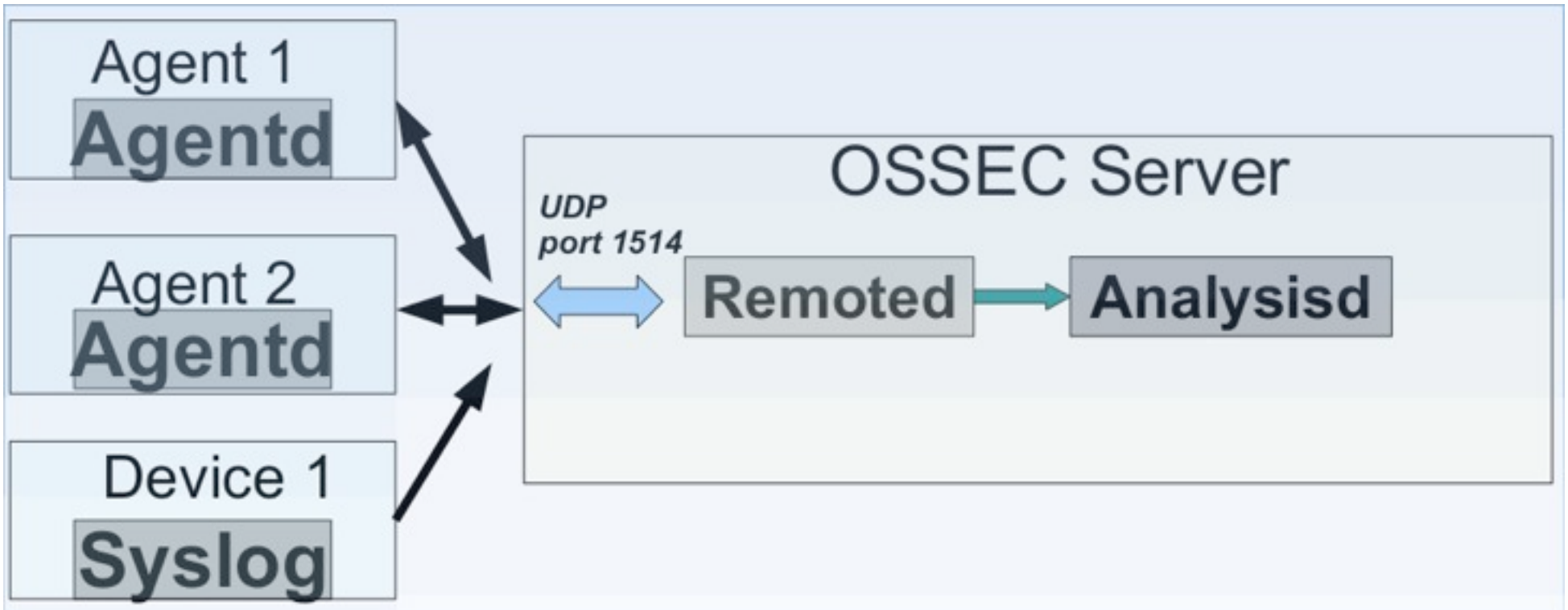
OSSEC Log Flow



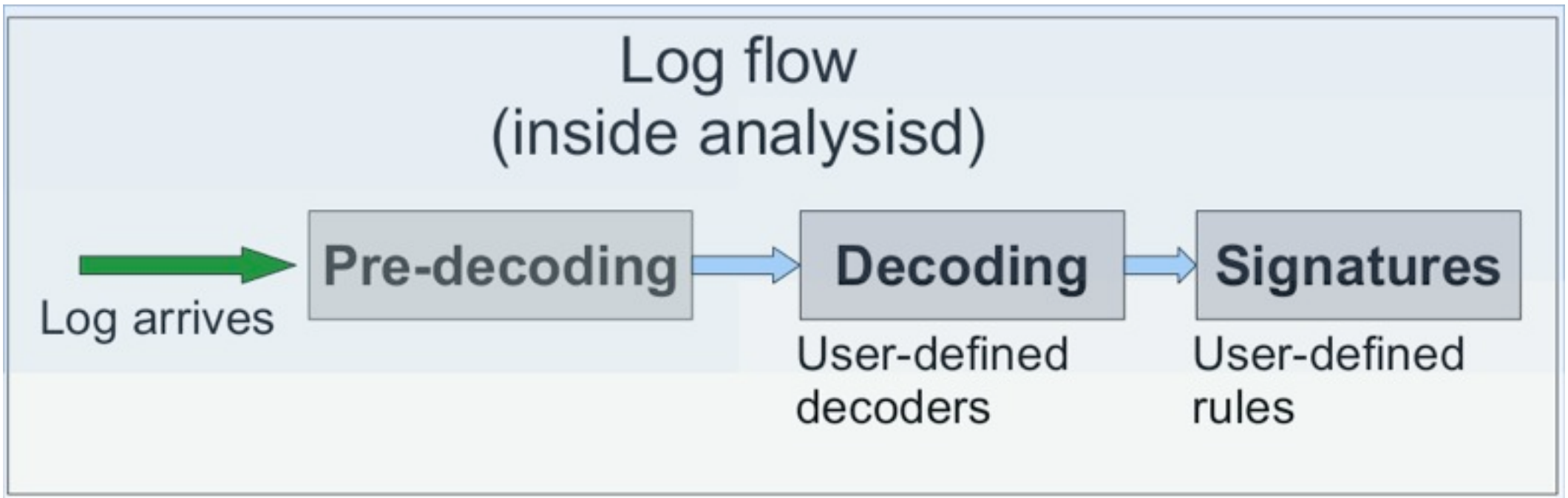
OSSEC Log Flow
Agent -> Server



Arquitetura OSSEC



Network Communication



Internal Log Flow

Agent -> Server

- Zlib Compressed
- Blowfish Encrypted
- udp 1514
- Centralized Management

Integrity Check

- each X time, or realtime
- File / Directory Properties
- Permissions
- Size
- Ownership
- sha1sum
- md5sum

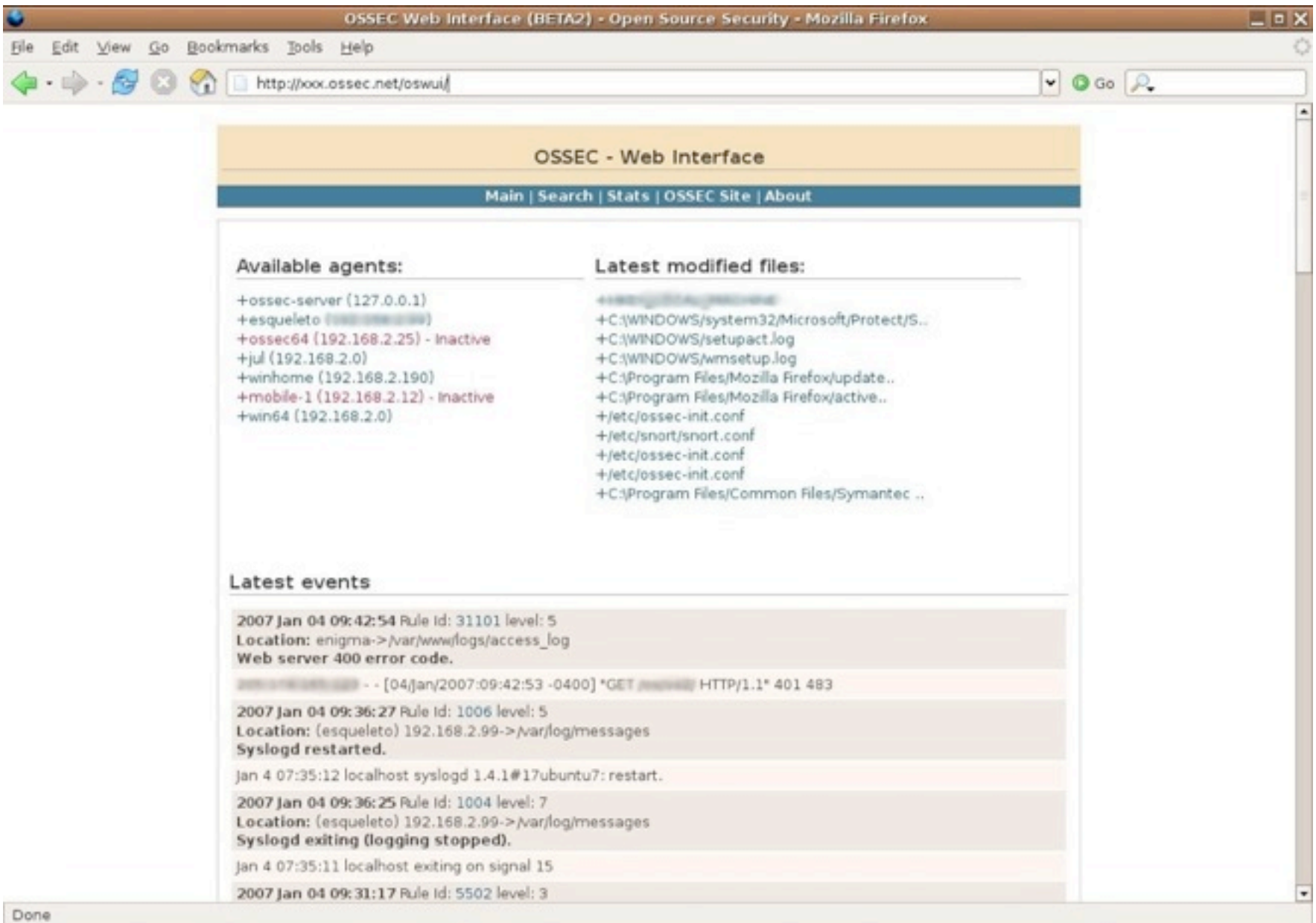
Rootkit Checks

- Signature (Adore, Knark, LOC) and anomaly-based
- Files in /dev which aren't device files
- Hidden directories
- SUID files
- Files owned by root world-writable
- Running processes hidden from “ps”
- Listening ports hidden from “netstat”
- Promiscuous interfaces

Policy Monitoring

- Identify situation which can lead to a breach
- Benchmark system against CIS standard (http://cisecurity.org) or create your own
- File, registry setting, or process exists or does not exist (win_audit_rcl.txt, win_applications_rcl.txt)
- Is anti-virus installed but not running?
- Has the host firewall been disabled?
- How do you know your systems are still hardened?

OSSEC WebUI


OSSEC Web Interface (BETA2) - Open Source Security - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://xxx.ossec.net/oswui/
Go
OSSEC - Web Interface
Main | Search | Stats | OSSEC Site | About
Available agents:
+ossec-server (127.0.0.1)
+esqueleto
+ossec64 (192.168.2.25) - Inactive
+jul (192.168.2.0)
+winhome (192.168.2.190)
+mobile-1 (192.168.2.12) - Inactive
+win64 (192.168.2.0)
Latest modified files:
+C:\WINDOWS/system32/Microsoft/Protect/S..
+C:\WINDOWS/setupact.log
+C:\WINDOWS/wmsetup.log
+C:\Program Files/Mozilla Firefox/update..
+C:\Program Files/Mozilla Firefox/active..
+/etc/ossec-init.conf
+/etc/snort/snort.conf
+/etc/ossec-init.conf
+/etc/ossec-init.conf
+C:\Program Files/Common Files/Symantec ..
Latest events
2007 Jan 04 09:42:54 Rule Id: 31101 level: 5
Location: enigma->/var/www/logs/access_log
Web server 400 error code.
- - [04/Jan/2007:09:42:53 -0400] "GET HTTP/1.1" 401 483
2007 Jan 04 09:36:27 Rule Id: 1006 level: 5
Location: (esqueleto) 192.168.2.99->/var/log/messages
Syslogd restarted.
Jan 4 07:35:12 localhost syslogd 1.4.1#17ubuntu7: restart.
2007 Jan 04 09:36:25 Rule Id: 1004 level: 7
Location: (esqueleto) 192.168.2.99->/var/log/messages
Syslogd exiting (logging stopped).
Jan 4 07:35:11 localhost exiting on signal 15
2007 Jan 04 09:31:17 Rule Id: 5502 level: 3
Done

Rules

- XML Files
- Levels -> 0 to 15

Rules

- Atomic
- Composite

Rule Sample

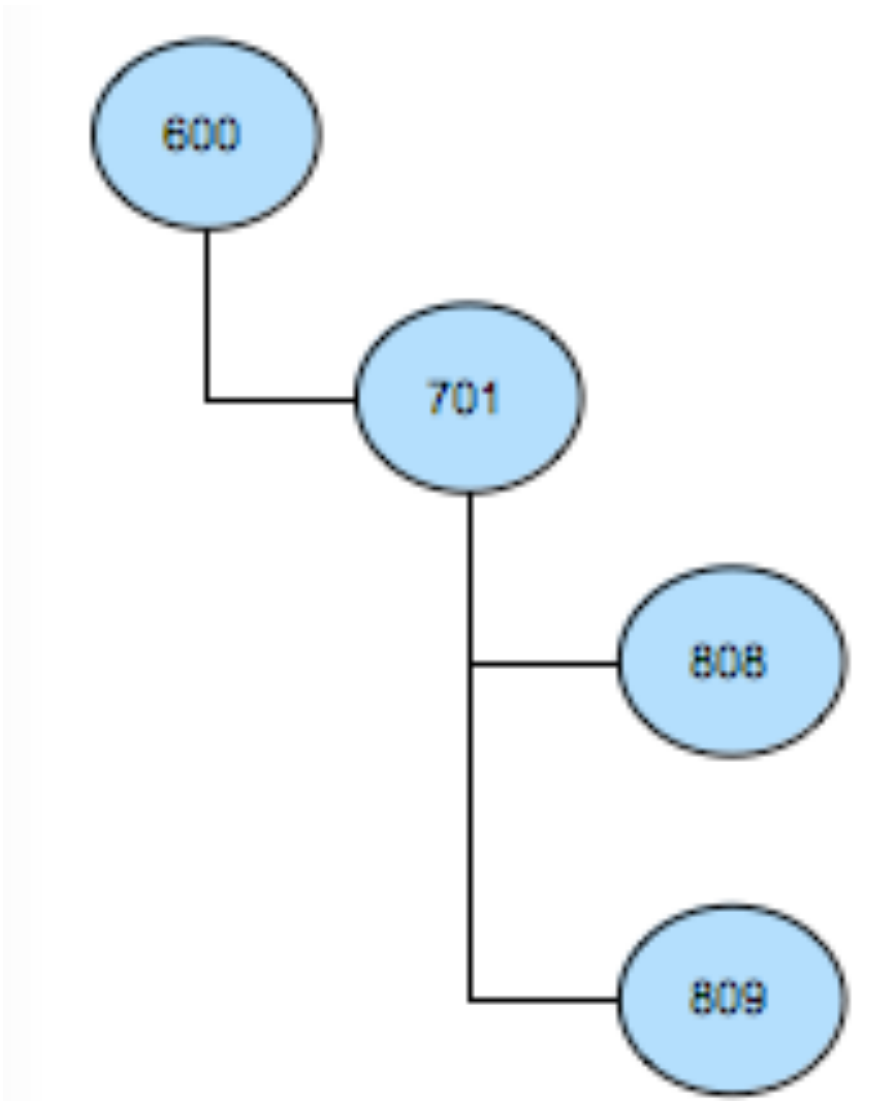
```
<!-- SSHD messages -->
<group name="syslog,sshd,">
  <rule id="5700" level="0" noalert="1">
    <decoded_as>sshd</decoded_as>
    <description>SSHD messages grouped.</description>
  </rule>
```

Rule Sample

```
<rule id="5704" level="4">
  <if_sid>5700</if_sid>
  <match>fatal: Timeout before authentication for</match>
  <description>Timeout while logging in (sshd).</description>
</rule>

<rule id="5705" level="10" frequency="4" timeframe="360">
  <if_matched_sid>5704</if_matched_sid>
  <description>Possible scan or breakin attempt </description>
  <description>(high number of login timeouts).</description>
</rule>
```

Analysys Tree



OSSEC in the real world

- Authentication control
- MSN usage
- Integrity checking
- Authentication logs

Authentication control

- Alerting on every authentication success outside business hours → Every authentication event is classified as "authentication success" (that's why we use if_group
- Added to local_rules.xml:

```
<rule id="100101" level="10">
    <if_group>authentication_success</if_group>
    <time>7 pm - 6:30 am</time>
    <description>Login during non-business hours.</
    description>
</rule>
```

Authentication control 2

- Alerting on first time logins outside business hours
- We have some FTS (first time seen) rules
- Increased severity when a user logs in for the first time on a specific system outside business hours → Added to **local_rules.xml**:

```
<rule id="100101" level="13">
    <if_sid>18119, 10100</if_sid>
    <time>7 pm - 6:30 am</time>
     <description>First time Login during non-bus. hours.<description>
</rule>
```

MSN Usage

- Alerting on new MSN users → MSN logs to the event log (with the email address) every time it starts

```
<rule id="100213" level="7">
      <if_sid>18101</if_sid>
      <id>102</id>
      <match>The database engine started a new instance</match>
       <description>MSN login.</description>
</rule>
```

2008 Apr 17 20:02:16 (xx) 192.168.2.190->WinEvtLog WinEvtLog: Application: INFORMATION(102): ESENT: (no user): no domain: OSSEC-HM: msnmsgr (1240) \\.\C:\Documents and Settings\xyz\Local Settings\Application Data\Microsoft\Messenger\xyz@hotmail.com\SharingMetadata\Working\database_F218_E 79B_18E7_5CDB\dfsr.db: The database engine started a new instance (0)

Integrity Checking

- Alerting with high severity on changes to /var/www/htdocs

```
<rule id="100345" level="12">
    <if_matched_group>syscheck</if_matched_group>
    <description>Changes to /var/www/htdocs – Critical file!</description>
    <match>/var/www/htdocs</match>
</rule>
```

Auth Logs

- Brute force attempts followed by a success

Rule: 5720 (level 10) -> 'Multiple SSHD authentication failures.' Src IP: 125.192.xx.xx Feb 11 09:31:58 wpor sshd[4565]: Failed password for root from 125.192.xx.xx port 42976 ssh2
Feb 11 09:31:58 wpor sshd[4565]: Failed password for admin from 125.192.xx.xx port 42976 ssh2

Feb 11 09:31:58 wpor sshd[4565]: Failed password for admin from 125.192.xx.xx port 42976 ssh2 Rule: 40112 (level 12) -> **'Multiple authentication failures followed by a success.'** Src IP: 125.192.67.136
User: admin Feb 11 09:31:58 wpor sshd[7235]: Accepted password for admin from 125.192.xx.xx port 42198 ssh2

And many more !

"Nobody knows your environment/applications as you"

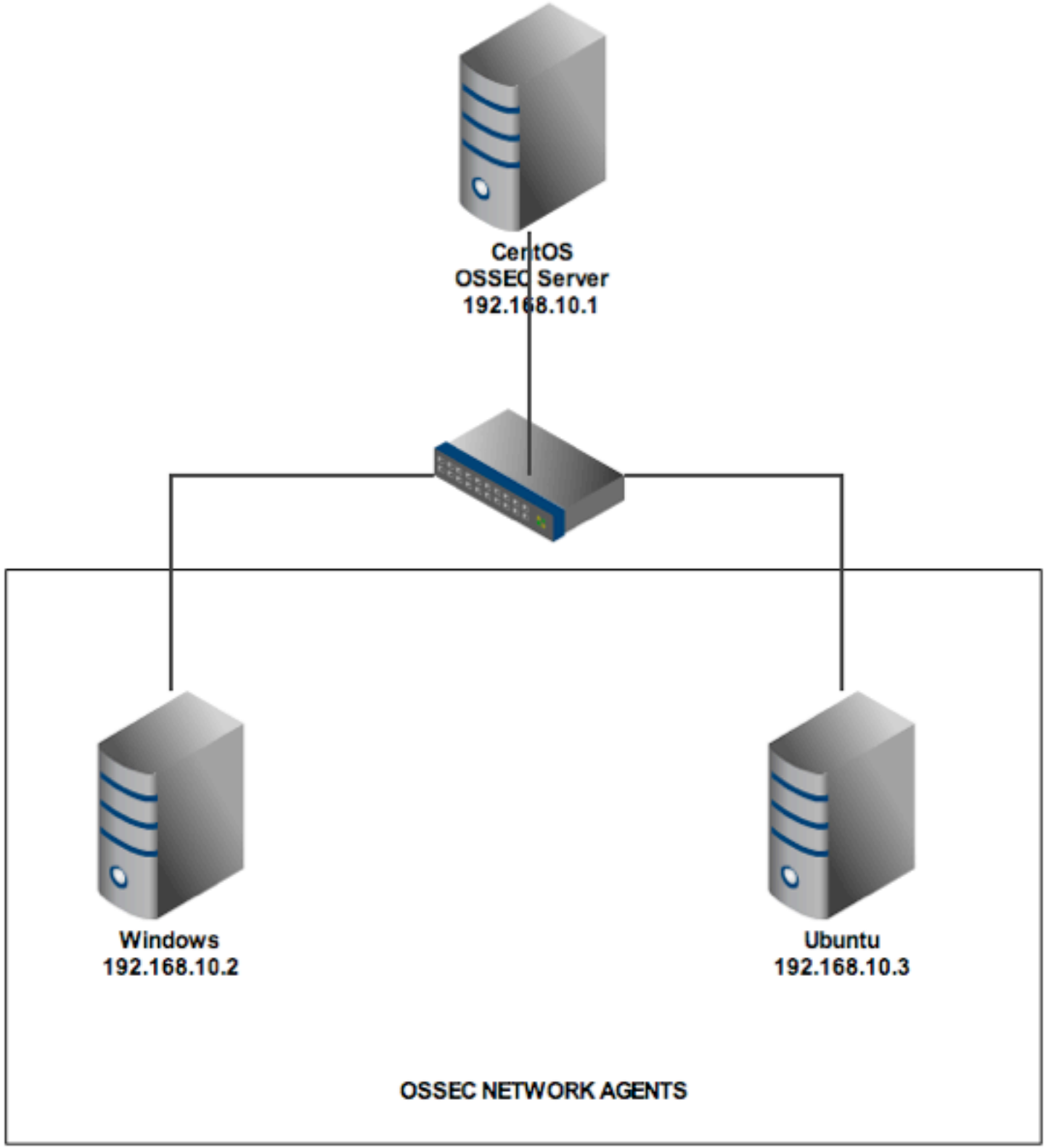
The “OSSEC Efect”

Challenges

- Deploying large amounts of agents
- Attackers who know Active Response is in use may try to use that to their advantage
- IPs can be spoofed, thereby triggering an incorrect response (whitelists, response timeouts)
- Alert Flooding - By default, OSSEC will only send 12 alerts per hour
- Log Injection
- - Tuning rules never stops !


OSSEC
OSSEC HIDS Notification.
2010 Oct 20 15:10:04
Received From: ossec-community->/var/log/communitylog
Rule: 100000 fired (level 15) -> "A Sincere Thanks"
Portion of the log(s):
Oct 20 15:10:04 allhosts ossec-awardd[423]: To: Daniel Cid. From: the OSSEC Community. Thank you for your tireless devotion to making our digital world a safer place.
--END OF NOTIFICATION

Let`s do it !



quinta-feira, 25 de novembro de 2010