



Host-Intrusion Detection based on OSSEC

Theresa Meiksner

1. Oktober 2014

Agenda

- ▶ Was ist OSSEC?

Agenda

- ▶ Was ist OSSEC?
- ▶ OSSEC @ s-IT Solutions

Agenda

- ▶ Was ist OSSEC?
- ▶ OSSEC @ s-IT Solutions
- ▶ Rules

Agenda

- ▶ Was ist OSSEC?
- ▶ OSSEC @ s-IT Solutions
- ▶ Rules
- ▶ OSSEC Prozesse

Agenda

- ▶ Was ist OSSEC?
- ▶ OSSEC @ s-IT Solutions
- ▶ Rules
- ▶ OSSEC Prozesse
- ▶ Network Communication

Agenda

- ▶ Was ist OSSEC?
- ▶ OSSEC @ s-IT Solutions
- ▶ Rules
- ▶ OSSEC Prozesse
- ▶ Network Communication
- ▶ Log Flow

Agenda

- ▶ Was ist OSSEC?
- ▶ OSSEC @ s-IT Solutions
- ▶ Rules
- ▶ OSSEC Prozesse
- ▶ Network Communication
- ▶ Log Flow
- ▶ Internal Log Flow

Agenda

- ▶ Was ist OSSEC?
- ▶ OSSEC @ s-IT Solutions
- ▶ Rules
- ▶ OSSEC Prozesse
- ▶ Network Communication
- ▶ Log Flow
- ▶ Internal Log Flow
- ▶ Log (Pre) Decoding

Agenda

- ▶ Was ist OSSEC?
- ▶ OSSEC @ s-IT Solutions
- ▶ Rules
- ▶ OSSEC Prozesse
- ▶ Network Communication
- ▶ Log Flow
- ▶ Internal Log Flow
- ▶ Log (Pre) Decoding
- ▶ Log/Data Processing

Agenda

- ▶ Was ist OSSEC?
- ▶ OSSEC @ s-IT Solutions
- ▶ Rules
- ▶ OSSEC Prozesse
- ▶ Network Communication
- ▶ Log Flow
- ▶ Internal Log Flow
- ▶ Log (Pre) Decoding
- ▶ Log/Data Processing

Was ist OSSEC?

- ▶ ein Open Source Host-based IDS (HIDS)
- ▶ <http://www.ossec.net>
- ▶ Main tasks
 - ▶ Log analysis

Was ist OSSEC?

- ▶ ein Open Source Host-based IDS (HIDS)
- ▶ <http://www.ossec.net>
- ▶ Main tasks
 - ▶ Log analysis
 - ▶ File Integrity Monitoring (UNIX & Windows)

Was ist OSSEC?

- ▶ ein Open Source Host-based IDS (HIDS)
- ▶ <http://www.ossec.net>
- ▶ Main tasks
 - ▶ Log analysis
 - ▶ File Integrity Monitoring (UNIX & Windows)
 - ▶ Host-based anomaly detection (rootkit detection)

Was ist OSSEC?

- ▶ ein Open Source Host-based IDS (HIDS)
- ▶ <http://www.ossec.net>
- ▶ Main tasks
 - ▶ Log analysis
 - ▶ File Integrity Monitoring (UNIX & Windows)
 - ▶ Host-based anomaly detection (rootkit detection)
 - ▶ Real time alerting & Active Response

Was ist OSSEC?

- ▶ ein Open Source Host-based IDS (HIDS)
- ▶ <http://www.ossec.net>
- ▶ Main tasks
 - ▶ Log analysis
 - ▶ File Integrity Monitoring (UNIX & Windows)
 - ▶ Host-based anomaly detection (rootkit detection)
 - ▶ Real time alerting & Active Response

Wozu braucht man Logfile Analyse?

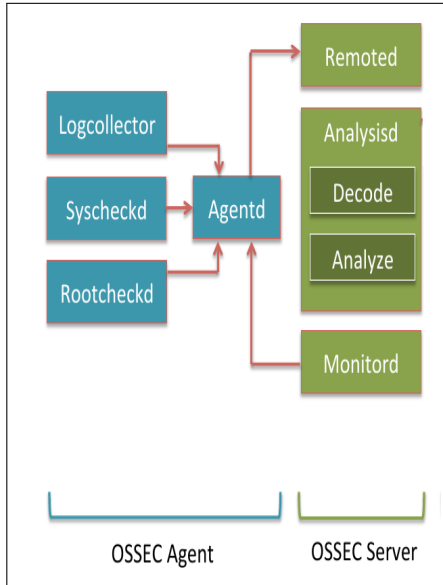
Wozu Log Analyse?

- ▶ Log Analyse u.a ist eine Voraussetzung für
- ▶ PCI DSS Compliance
- ▶ HIPAA Compliance
- ▶ FISMA Compliance
- ▶ SOX Compliance
- ▶ usw...



- ▶ Syslog Server = OSSEC Master VM auf RHEL 6.8
- ▶ OSSEC Clients verfügbar für alle Plattformen (Linux, Solaris, AIX, Windows)
- ▶ etliche vorgefertigte Rules/Decoder
sshd (Open-SSH), Samba, Su, Sudo, Squid, Postfix, Sendmail, Named, Apache, etc. . . .
- ▶ Rules Config im xml Format (RegEx Know-How von Vorteil)

OSSEC Prozesse Übersicht



- ▶ Analysisd - Hauptprozess, ist hauptverantwortlich für die Analyse von Logs
- ▶ Remoted – Empfängt und leitet die remote logs an analysisd weiter
- ▶ Logcollector – lesen und weiterleiten der Logs an analysisd
- ▶ Agentd – leitet die Logs an den Server (master) weiter
- ▶ Maild – verschickt die e-mail alerts
- ▶ Execd – ist für die active responses verantwortlich
- ▶ Monitord – überwacht den agent status, komprimiert und signiert die Logs

- ▶ Jeder dieser Prozesse wird mit stark eingeschränkten Rechten und Tasks ausgeführt
 - ▶ die meisten laufen in einer chroot Umgebung
 - ▶ die meisten werden unter separaten (unprivileged) User ausgeführt
- ▶ `/var/ossec/bin/ossec-control` führt die oben genannten Prozesse in der richtigen Reihenfolge aus.

Rules 1/2

Rules, die bei der Installation dabei sind.

```
root@chaw:/var/ossec/rules
root@chaw:/var/ossec/rules/17009
1
----- 1 root ossec 2567 9. Nov 2012 arpmatch_rules.xml
----- 1 root ossec 7226 9. Nov 2012 asterisk_rules.xml
----- 1 root ossec 4315 9. Nov 2012 attack_rules.xml
----- 2 root ossec 4096 23. Okt 08:28 backup-rules.25700
----- 1 root ossec 2079 9. Nov 2012 brca-ids_rules.xml
----- 1 root ossec 1905 9. Nov 2012 ciscoerror_rules.xml
----- 1 root ossec 2469 9. Nov 2012 cisco-ios_rules.xml
----- 1 root ossec 1871 9. Nov 2012 clam_av_rules.xml
----- 1 root ossec 2300 9. Nov 2012 courier_rules.xml
----- 1 root ossec 2205 9. Nov 2012 daverat_rules.xml
----- 1 root ossec 2520 9. Nov 2012 dropbear_rules.xml
----- 1 root ossec 1194 9. Nov 2012 firewall_rules.xml
----- 1 root ossec 3027 9. Nov 2012 ftpd_rules.xml
----- 1 root ossec 2262 9. Nov 2012 hardmap_rules.xml
----- 1 root ossec 3906 9. Nov 2012 ids_rules.xml
----- 1 root ossec 1850 9. Nov 2012 imaps_rules.xml
----- 1 root ossec 1551 9. Nov 2012 local_rules.xml
----- 2 root ossec 4096 9. Nov 2012 log-entries
----- 1 root ossec 1242 9. Nov 2012 mailscanner_rules.xml
----- 1 root ossec 4382 9. Nov 2012 maweg_wg_rules.xml
----- 1 root ossec 31344 9. Nov 2012 smouth_rules.xml
----- 1 root ossec 12032 9. Nov 2012 ms_dhcp_rules.xml
----- 1 root ossec 1805 9. Nov 2012 ms-exchange_rules.xml
----- 1 root ossec 2131 9. Nov 2012 ms_ftpd_rules.xml
----- 1 root ossec 2242 9. Nov 2012 ms-ss_rules.xml
----- 1 root ossec 2508 9. Nov 2012 mysql_rules.xml
----- 1 root ossec 9669 9. Nov 2012 nandl_rules.xml
----- 1 root ossec 3514 9. Nov 2012 netacronb_rules.xml
----- 1 root ossec 2540 9. Nov 2012 nginx_rules.xml
----- 1 root ossec 6902 9. Nov 2012 openbsd_rules.xml
----- 1 root ossec 10959 9. Nov 2012 ossec_rules.xml
----- 1 root ossec 3219 9. Nov 2012 pam_rules.xml
----- 1 root ossec 3153 9. Nov 2012 php_rules.xml
----- 1 root ossec 6876 9. Nov 2012 pir_rules.xml
----- 1 root ossec 982 9. Nov 2012 policy_rules.xml
----- 1 root ossec 5269 9. Nov 2012 postfix_rules.xml
----- 1 root ossec 3004 9. Nov 2012 postgres_rules.xml
----- 1 root ossec 6140 9. Nov 2012 proftpd_rules.xml
----- 1 root ossec 2080 9. Nov 2012 pure-ftpd_rules.xml
----- 1 root ossec 2057 9. Nov 2012 racoon_rules.xml
----- 1 root ossec 1854 9. Nov 2012 randomize_rules.xml
----- 1 root ossec 1881 9. Nov 2012 rules.config.xml
----- 1 root ossec 4905 9. Nov 2012 sendmail_rules.xml
----- 1 root ossec 2846 9. Nov 2012 send_rules.xml
----- 1 root ossec 1826 9. Nov 2012 solaris_bon_rules.xml
----- 1 root ossec 2612 9. Nov 2012 sonicwall_rules.xml
----- 1 root ossec 835 9. Nov 2012 spamd_rules.xml
----- 1 root ossec 7299 9. Nov 2012 squid_rules.xml
----- 1 root ossec 6430 9. Nov 2012 sshd_rules.xml
----- 1 root ossec 1331 9. Nov 2012 symantec-ar_rules.xml
----- 1 root ossec 1707 9. Nov 2012 symantec-av_rules.xml
----- 1 root ossec 18378 9. Nov 2012 syslog_rules.xml
----- 1 root ossec 1388 9. Nov 2012 telnetd_rules.xml
----- 3 root ossec 4096 9. Nov 2012 translated
----- 1 root ossec 1401 9. Nov 2012 trend-secure_rules.xml
----- 1 root ossec 854 9. Nov 2012 vncppd_rules.xml
----- 1 root ossec 4679 9. Nov 2012 vmware_rules.xml
----- 1 root ossec 1773 9. Nov 2012 vpn-concentrator_rules.xml
```

Rules 2/2

- ▶ zu finden unter: `/var/ossec/rules`
- ▶ `local_rules.xml` (für `syslog/messages.log`) und eigene Rules
- ▶ Auszug aus dem `squid_rules.xml`

Rules 2/2

- ▶ zu finden unter: /var/ossec/rules
- ▶ local_rules.xml (für syslog/messages.log) und eigene Rules
- ▶ Auszug aus dem squid_rules.xml

```
1 <group name="squid," >
  <rule id="35000" level="0">
3   <category>squid</category>
   <description>Squid messages grouped.</description>
5 </rule>
```

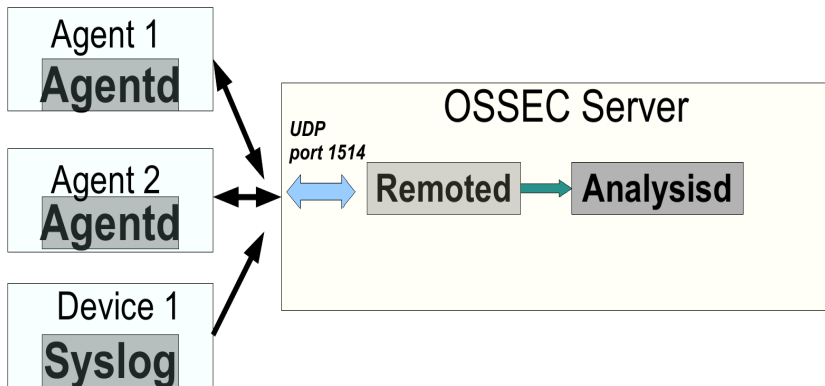
Rules 2/2

- ▶ zu finden unter: /var/ossec/rules
- ▶ local_rules.xml (für syslog/messages.log) und eigene Rules
- ▶ Auszug aus dem squid_rules.xml

```
1 <group name="squid,">  
  <rule id="35000" level="0">  
3    <category>squid</category>  
    <description>Squid messages grouped.</description>  
5  </rule>
```

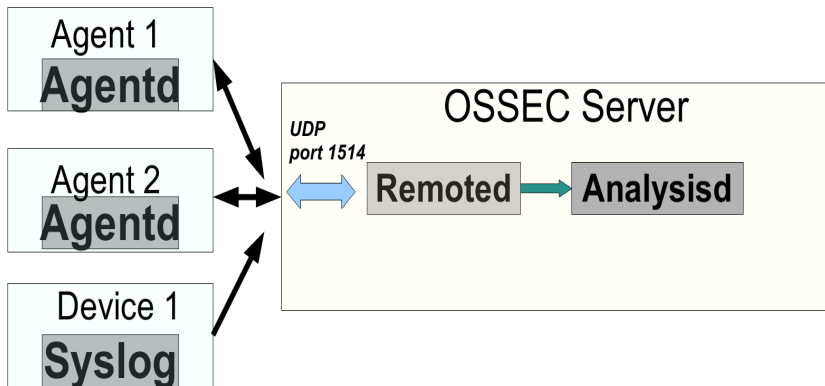
```
1 <rule id="35052" level="10" frequency="$SQUID_FREQ" timeframe="120">  
  <if_matched_sid>35007</if_matched_sid>  
3  <same_source_ip />  
  <description>Multiple unauthorized attempts to use proxy.</description>  
5 </rule>
```

Network Communication



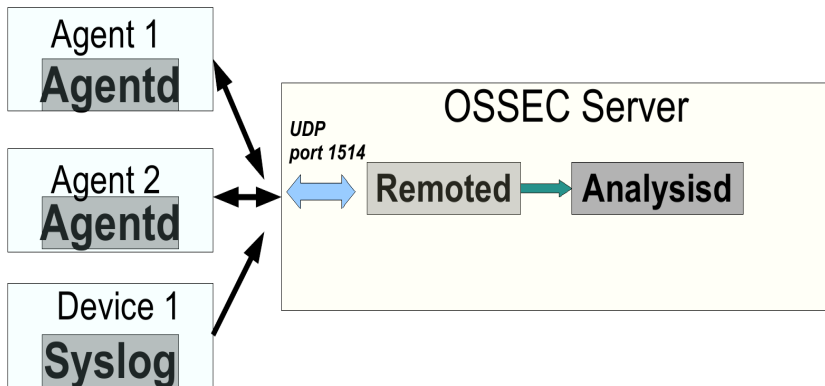
- komprimiert (zlib)

Network Communication



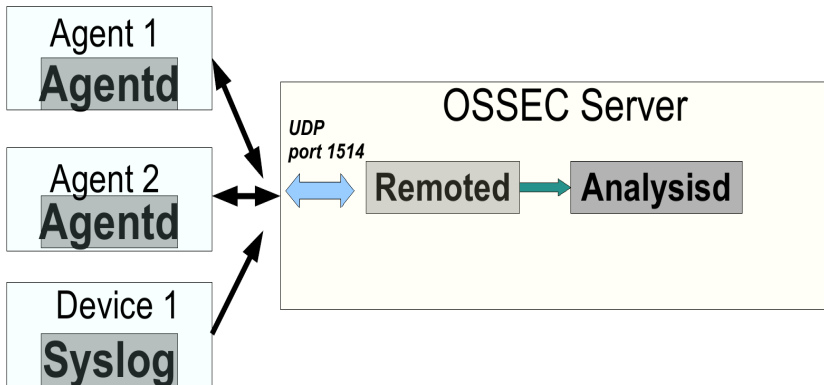
- ▶ komprimiert (zlib)
- ▶ verschlüsselt mit pre-shared keys

Network Communication



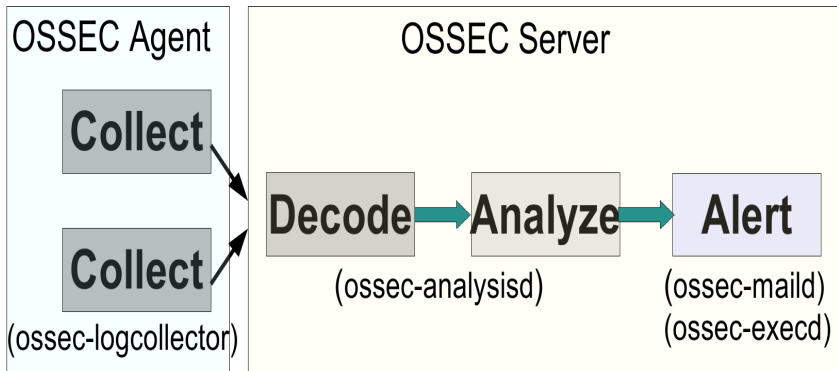
- ▶ komprimiert (zlib)
- ▶ verschlüsselt mit pre-shared keys
- ▶ verwendet per default UDP port 1514 (FW Freischaltung!)

Network Communication



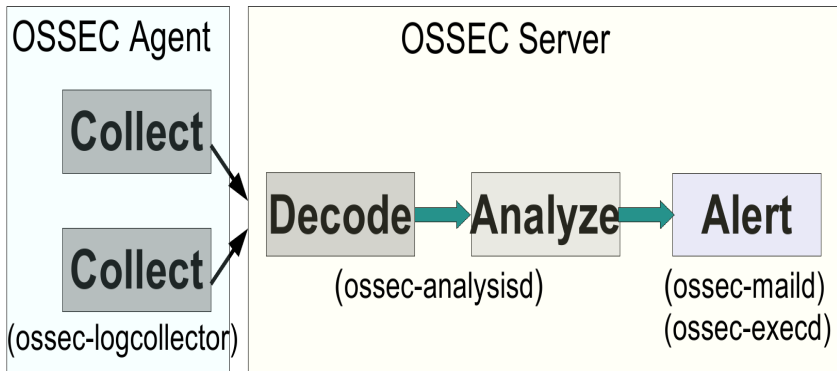
- ▶ komprimiert (zlib)
- ▶ verschlüsselt mit pre-shared keys
- ▶ verwendet per default UDP port 1514 (FW Freischaltung!)
- ▶ Multi-platform (Windows, Solaris, Linux, etc)

Log Flow (agent/server)



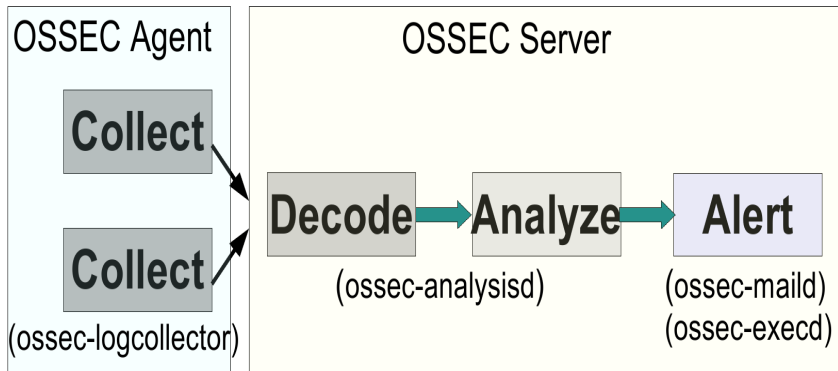
- ▶ ossec-logcollector sammelt die Logs

Log Flow (agent/server)



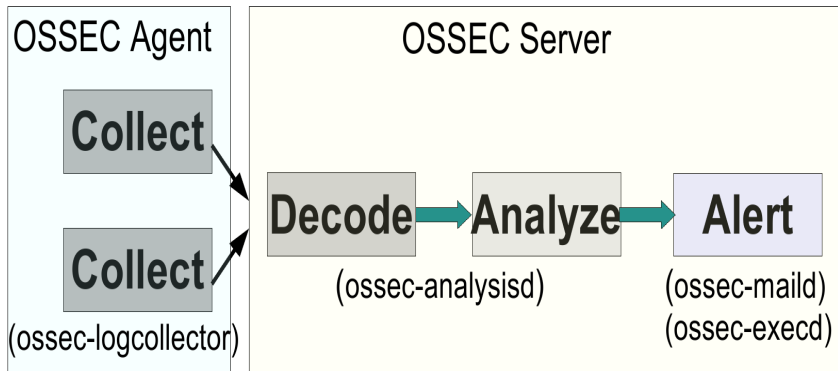
- ▶ ossec-logcollector sammelt die Logs
- ▶ ossec-analysisd analysiert und decoded Logs

Log Flow (agent/server)



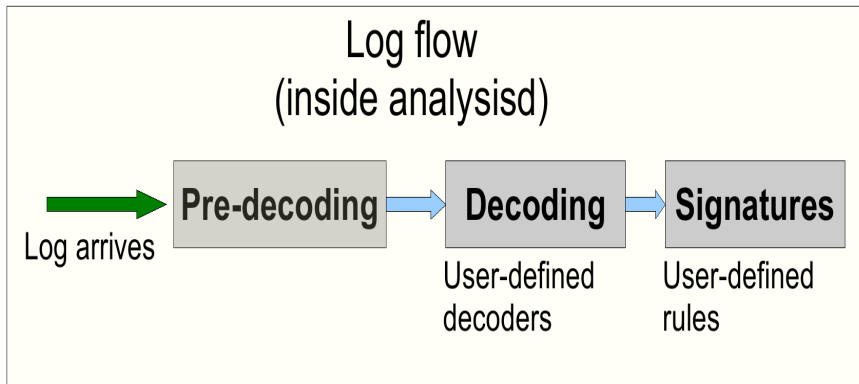
- ▶ ossec-logcollector sammelt die Logs
- ▶ ossec-analysisd analysiert und decoded Logs
- ▶ ossec-maild verschickt die Meldungen

Log Flow (agent/server)



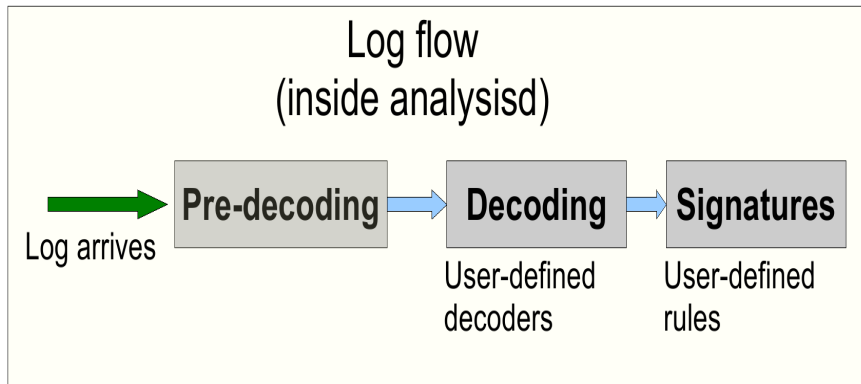
- ▶ ossec-logcollector sammelt die Logs
- ▶ ossec-analysisd analysiert und decoded Logs
- ▶ ossec-maild verschickt die Meldungen
- ▶ ossec-execd

Internal Log Flow



- ▶ 3 Hauptteile:
 - ▶ Pre-decoding (extrahiert bekannte Bereiche, wie Datum/Zeit, etc)

Internal Log Flow



- ▶ 3 Hauptteile:
 - ▶ Pre-decoding (extrahiert bekannte Bereiche, wie Datum/Zeit, etc)
 - ▶ Decoding

Log pre-decoding

Extrahiert allgemeine Informationen aus den Logs

- ▶ Hostname, Name der Applikation und Zeit aus dem syslog header
- ▶ Logs sollten einheitlich formatiert sein

Log kommt rein als:

```
1 2013-10-25T16:36:37.610526+02:00 gruenberg rsyslogd:  
[origin software="rsyslogd" swVersion="5.8.10" x-pid="53802"  
3 x-info="http://www.rsyslog.com"] start
```

Wie formatiert OSSEC den Output?

```
1 2013-10-28T12:41:01.840351+01:00 gruenberg yum[53258]:  
Installed: hp-health-9.40-1602.44.rhel6.x86_64  
3 Datum/Zeit -> Oct 28 12:41:01  
Hostname -> gruenberg  
5 Prozess.name -> yum  
log -> Installed: hp-health-9.40-1602.44.rhel6.x86_64  
7 Alert -> Rule: 2932 fired (level 7) -> "New Yum package installed."  
user -> root
```

Log kommt rein als:

2

```
2013-10-28T12:41:01.840351+01:00 gruenberg yum[53258]:  
Installed: hp-health-9.40-1602.44.rhel6.x86_64
```

Wie schaut ein Log nach dem es decoded wurde aus?

2

```
Datum/Zeit -> Oct 28 12:41:01
```

```
Hostname -> gruenberg
```

```
Prozess_name -> yum
```

4

```
log -> Installed: hp-health-9.40-1602.44.rhel6.x86_64
```

Wie schaut ein Log nach dem es decoded wurde aus?

```
2 2013-10-28T12:41:01.840351+01:00 gruenberg yum[53258]:  
   Installed: hp-health-9.40-1602.44.rhel6.x86_64  
   Datum/Zeit -> Oct 28 12:41:01  
4  Hostname -> gruenberg  
   Prozess.name -> yum  
6  log -> Installed: hp-health-9.40-1602.44.rhel6.x86_64  
   Alert -> Rule: 2932 fired (level 7) -> "New Yum package installed."  
8  user -> root
```


- ▶ Splunk
- ▶ OSSIM von Alienvault
- ▶ Open-Source: Logstash, ElasticSearch, Kibana usw...

To Do's

- ▶ Alert Configuration and Management (individual alert categories)
- ▶ Real-time alerting
- ▶ Rootkit-Detection
- ▶ Agent/Agentless
usw...

Danke für eure Aufmerksamkeit!

http://www.arei.net/ossec_summary.pdf