



Host-Intrusion Detection based on OSSEC

Theresa Meiksner

3. Oktober 2014

- 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
- Configuring Alerts

Agenda

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

Agenda

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

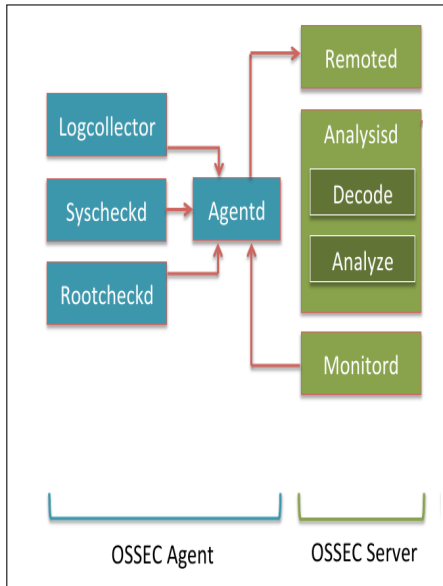
Wozu Log Analyse?

- 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) Usern 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@shaw:/etc/ossec/rules
root@shaw:/etc/ossec/rules 23:53

root@shaw:~# ls -la /etc/ossec/rules/
total 1008
-rw-r--r-- 1 root ossec 2567  9. Nov 2012 arpsploit.rules.nal
-rw-r--r-- 1 root ossec 3726  9. Nov 2012 asterisk.rules.nal
-rw-r--r-- 1 root ossec 4315  9. Nov 2012 attack.rules.nal
-rw-r--r-- 2 root ossec 4366 23. Okt 08:28 backup.rules.25708
-rw-r--r-- 1 root ossec 2079  9. Nov 2012 bkr-ids.rules.nal
-rw-r--r-- 1 root ossec 1095  9. Nov 2012 ciscoerror.rules.nal
-rw-r--r-- 1 root ossec 2469  9. Nov 2012 cisco-ios.rules.nal
-rw-r--r-- 1 root ossec 1871  9. Nov 2012 clam_av.rules.nal
-rw-r--r-- 1 root ossec 2060  9. Nov 2012 courier.rules.nal
-rw-r--r-- 1 root ossec 2205  9. Nov 2012 dnetsec.rules.nal
-rw-r--r-- 1 root ossec 2320  9. Nov 2012 dropbear.rules.nal
-rw-r--r-- 1 root ossec 1194  9. Nov 2012 firewall.rules.nal
-rw-r--r-- 1 root ossec 3027  9. Nov 2012 ftpd.rules.nal
-rw-r--r-- 1 root ossec 2362  9. Nov 2012 hardening.rules.nal
-rw-r--r-- 1 root ossec 3590  9. Nov 2012 ids.rules.nal
-rw-r--r-- 1 root ossec 1550  9. Nov 2012 imapd.rules.nal
-rw-r--r-- 1 root ossec 1551  9. Nov 2012 local.rules.nal
-rw-r--r-- 2 root ossec 4086  9. Nov 2012 log-entries
-rw-r--r-- 1 root ossec 1242  9. Nov 2012 mailscanner.rules.nal
-rw-r--r-- 1 root ossec 4362  9. Nov 2012 mcafee_av.rules.nal
-rw-r--r-- 1 root ossec 8184  9. Nov 2012 month.rules.nal
-rw-r--r-- 1 root ossec 12002  9. Nov 2012 ms_dhcc.rules.nal
-rw-r--r-- 1 root ossec 1605  9. Nov 2012 ms-exchange.rules.nal
-rw-r--r-- 1 root ossec 2131  9. Nov 2012 ms_ftpd.rules.nal
-rw-r--r-- 1 root ossec 2242  9. Nov 2012 msn.rules.nal
-rw-r--r-- 1 root ossec 2506  9. Nov 2012 mysql.rules.nal
-rw-r--r-- 1 root ossec 9999  9. Nov 2012 named.rules.nal
-rw-r--r-- 1 root ossec 9514  9. Nov 2012 netstrenfnd.rules.nal
-rw-r--r-- 1 root ossec 2640  9. Nov 2012 nginx.rules.nal
-rw-r--r-- 1 root ossec 6092  9. Nov 2012 openbsd.rules.nal
-rw-r--r-- 1 root ossec 10359  9. Nov 2012 ossec.rules.nal
-rw-r--r-- 1 root ossec 3219  9. Nov 2012 pcr.rules.nal
-rw-r--r-- 1 root ossec 3153  9. Nov 2012 php.rules.nal
-rw-r--r-- 1 root ossec 6876  9. Nov 2012 pix.rules.nal
-rw-r--r-- 1 root ossec 962  9. Nov 2012 policy.rules.nal
-rw-r--r-- 1 root ossec 5259  9. Nov 2012 postfix.rules.nal
-rw-r--r-- 1 root ossec 3004  9. Nov 2012 postgresql.rules.nal
-rw-r--r-- 1 root ossec 6140  9. Nov 2012 proftpd.rules.nal
-rw-r--r-- 1 root ossec 2069  9. Nov 2012 pure-ftpd.rules.nal
-rw-r--r-- 1 root ossec 2567  9. Nov 2012 racoon.rules.nal
-rw-r--r-- 1 root ossec 1054  9. Nov 2012 roundcube.rules.nal
-rw-r--r-- 1 root ossec 1881  9. Nov 2012 rules.config.nal
-rw-r--r-- 1 root ossec 4705  9. Nov 2012 sendmail.rules.nal
-rw-r--r-- 1 root ossec 2846  9. Nov 2012 smbd.rules.nal
-rw-r--r-- 1 root ossec 1826  9. Nov 2012 solaris_bon.rules.nal
-rw-r--r-- 1 root ossec 2611  9. Nov 2012 sshnail.rules.nal
-rw-r--r-- 1 root ossec 839  9. Nov 2012 squid.rules.nal
-rw-r--r-- 1 root ossec 7258  9. Nov 2012 squid.rules.nal
-rw-r--r-- 1 root ossec 9430  9. Nov 2012 squid.rules.nal
-rw-r--r-- 1 root ossec 1331  9. Nov 2012 symantec.rules.nal
-rw-r--r-- 1 root ossec 1707  9. Nov 2012 symantec-os.rules.nal
-rw-r--r-- 1 root ossec 18378  9. Nov 2012 syslog.rules.nal
-rw-r--r-- 1 root ossec 1388  9. Nov 2012 telnetd.rules.nal
-rw-r--r-- 2 root ossec 4096  9. Nov 2012 translated
-rw-r--r-- 1 root ossec 1491  9. Nov 2012 trend-mce.rules.nal
-rw-r--r-- 1 root ossec 854  9. Nov 2012 vmop3d.rules.nal
-rw-r--r-- 1 root ossec 4679  9. Nov 2012 vmware.rules.nal
-rw-r--r-- 1 root ossec 1772  9. Nov 2012 vpn concentrator.rules.nal
```


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

Example

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

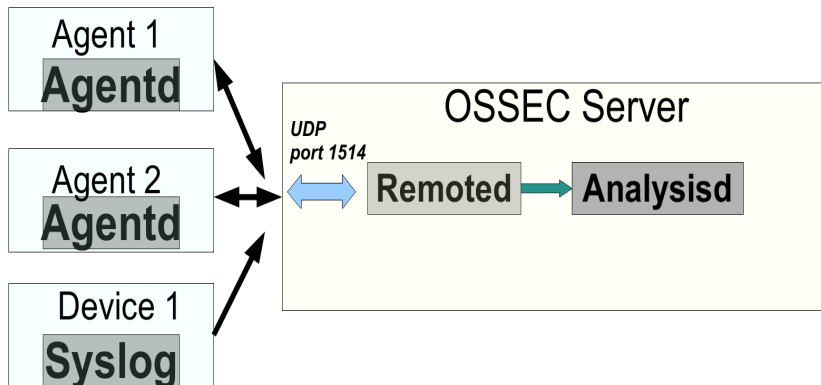
Example

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

Example

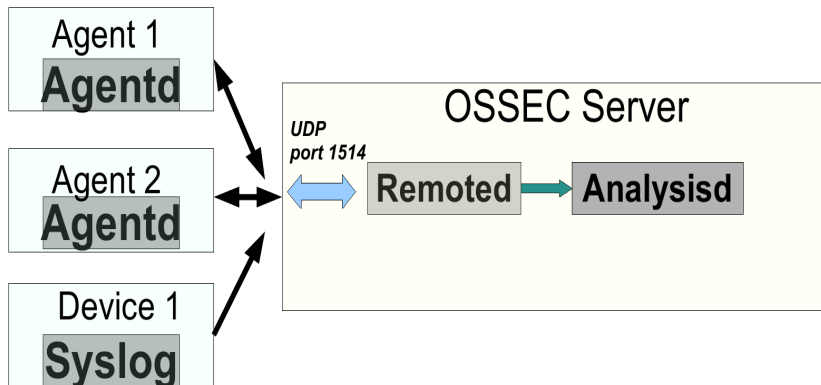
```
<rule id="35052" level="10" frequency="$SQUID_FREQ" timeframe="120">
  <if_matched_sid>35007</if_matched_sid>
  <same_source_ip />
  <description>Multiple unauthorized attempts to use proxy.</description>
</rule>
```

Network Communication



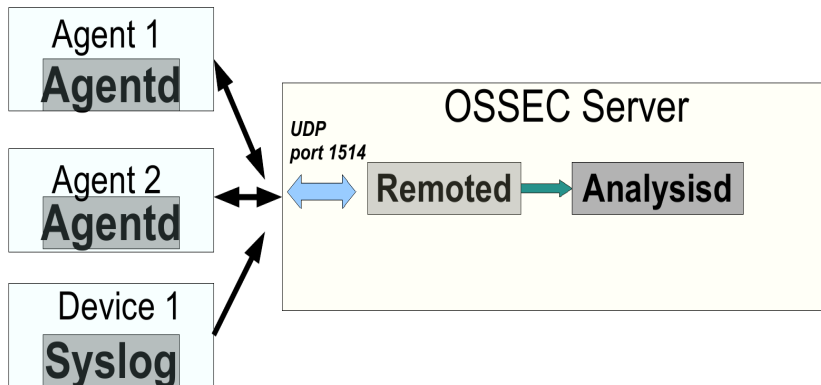
- komprimiert (zlib)

Network Communication



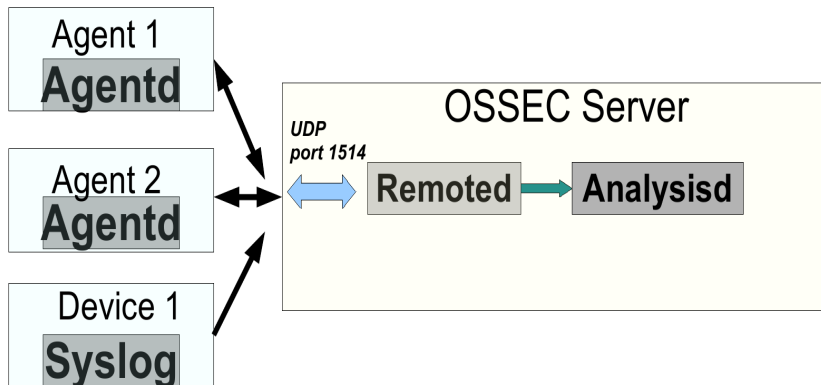
- komprimiert (zlib)
- verschlüsselt mit pre-shared keys

Network Communication



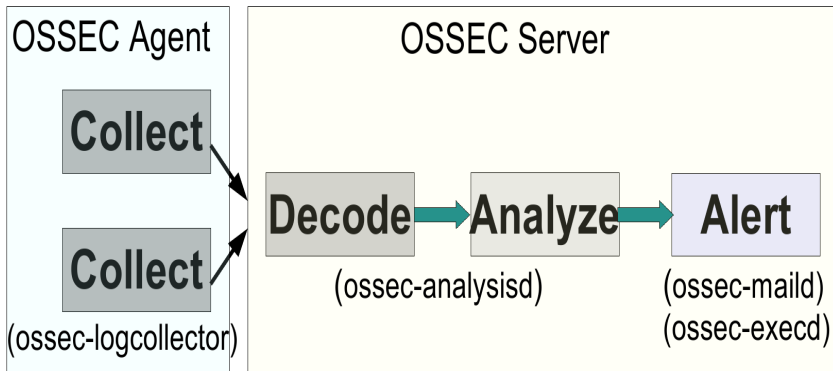
- komprimiert (zlib)
- verschlüsselt mit pre-shared keys
- verwendet per default UDP port 1514 (FW Freischaltung!)

Network Communication



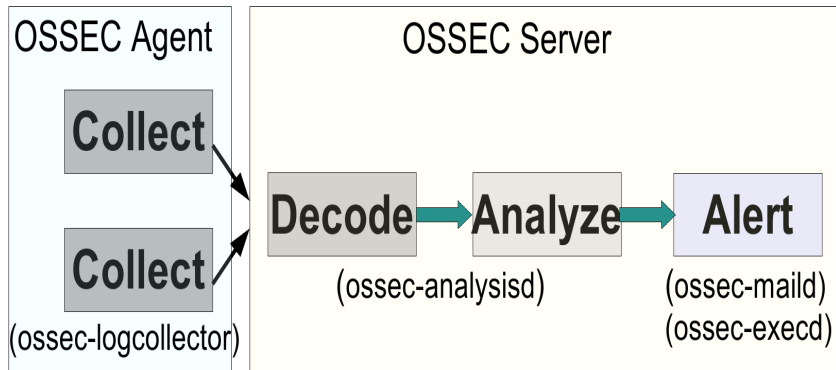
- komprimiert (zlib)
- verschlüsselt mit pre-shared keys
- verwendet per default UDP port 1514 (FW Freischaltung!)
- Multi-platform (Windows, Solaris, Linux, etc)

Log Flow (agent/server)



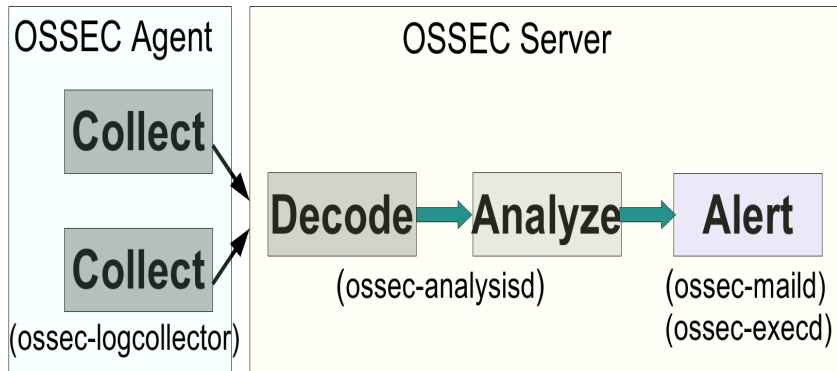
- ossec-logcollector sammelt die Logs

Log Flow (agent/server)



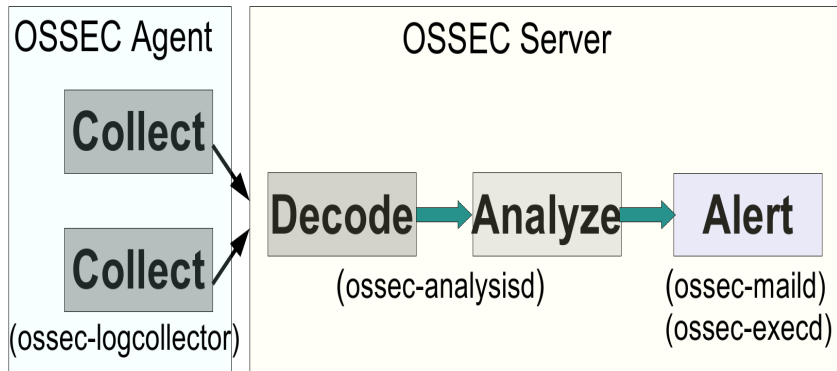
- ossec-logcollector sammelt die Logs
- ossec-analysisd analysiert und decoded Logs

Log Flow (agent/server)



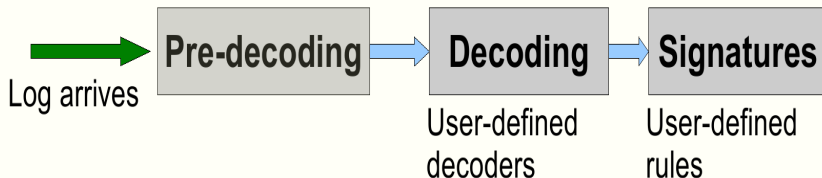
- ossec-logcollector sammelt die Logs
- ossec-analysisd analysiert und decoded Logs
- ossec-maild verschickt die Meldungen

Log Flow (agent/server)



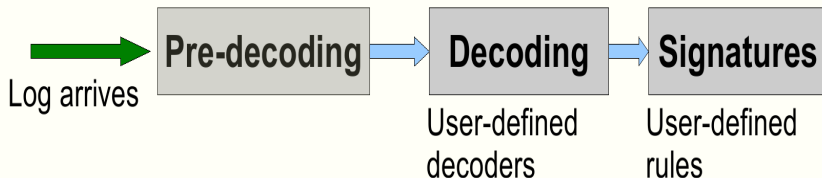
- ossec-logcollector sammelt die Logs
- ossec-analysisd analysiert und decoded Logs
- ossec-maild verschickt die Meldungen
- ossec-execd

Log flow (inside analysisd)



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

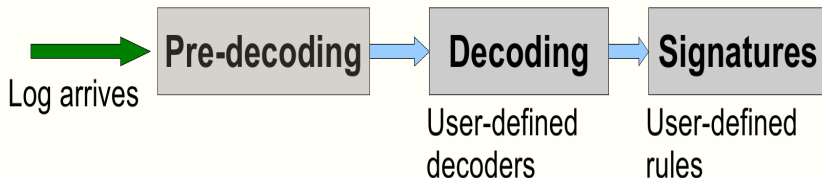
Log flow (inside analysisd)



- 3 Hauptteile:

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

Log flow (inside analysisd)



- 3 Hauptteile:

- ▶ Pre-decoding (extrahiert bekannte Bereiche, wie Datum/Zeit, etc)
- ▶ Decoding
- ▶ Signatures (können eigene user-defined rules sein)

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:

Example

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

Wie formatiert OSSEC den Output?

Example

```
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  
Hostname -> gruenberg  
Prozess_name -> yum  
log -> Installed: hp-health -9.40-1602.44.rhel6.x86_64  
Alert -> Rule: 2932 fired (level 7) -> "New Yum package installed."  
user -> root
```

Log kommt rein als:

Example

```
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?

Example

```
Datum/Zeit -> Oct 28 12:41:01  
Hostname -> gruenberg  
Prozess_name -> yum  
log -> Installed: hp-health -9.40-1602.44.rhel6.x86_64
```


Wie schaut ein Log nach dem es decoded wurde aus?

Example

```
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  
Hostname -> gruenberg  
Prozess_name -> yum  
log -> Installed: hp-health-9.40-1602.44.rhel6.x86_64  
Alert -> Rule: 2932 fired (level 7) -> "New Yum package installed."  
user -> root
```

- verschiedene Alert-Levels von 0-15
- OSSEC loggt jeden Alert von 1-15
- ab Alert Level 7 werden per default Alert Emails erstellt (anpassbar!)
- if alert_severity > log_level_alert send email.
- es gibt für PCI DSS bestimmte Requirements in Bezug auf log collection und retention.
- usw...

- kostenpflichtig (aber gut):
 - ▶ USM von AlienVault
 - ▶ Splunk OSSEC App
- Open-Source:
 - ▶ OSSIM von AlienVault
 - ▶ Logstash+ElasticSearch+Kibana (Nachteil: Bastelarbeit)

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/files/ossec_summary.pdf