



Host-Intrusion Detection based on OSSEC

Theresa Meiksner

30. September 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?

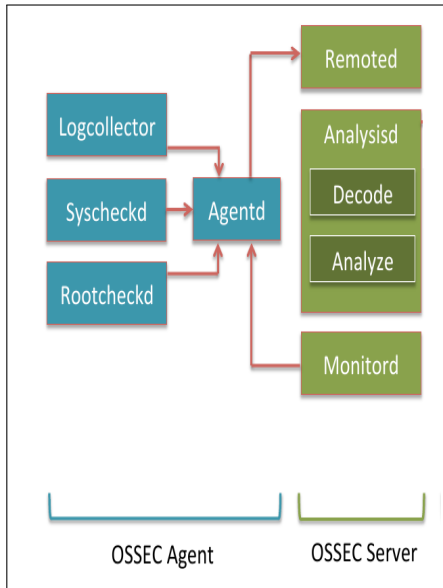
- ▶ Log Analyse u.a ist eine Voraussetzung für
- ▶ PCI DSS Compliance
- ▶ HIPAA Compliance
- ▶ FISMA Compliance
- ▶ SOX Compliance
- ▶ usw...



OSSEC @ s-IT Solutions

- ▶ 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



OSSEC Prozesse

- ▶ 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

OSSEC Prozesse

- ▶ 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@thau:~/fw/iptables/rules
root@thau:~/fw/iptables/rules 2376a
iptables -I root ostate 2567 9. Nov 2012 aspothich_rules.m
iptables -I root ostate 3726 9. Nov 2012 asterisk_rules.m
iptables -I root ostate 4315 9. Nov 2012 attack_rules.m
iptables -I root ostate 4096 23. Oct 08:28 backup_rules_25700
iptables -I root ostate 2099 9. Nov 2012 brw-ids_rules.m
iptables -I root ostate 1095 9. Nov 2012 clamserver_rules.m
iptables -I root ostate 2469 9. Nov 2012 cisco-ids_rules.m
iptables -I root ostate 1891 9. Nov 2012 clam-av_rules.m
iptables -I root ostate 2000 9. Nov 2012 courier_rules.m
iptables -I root ostate 2206 9. Nov 2012 dmsccat_rules.m
iptables -I root ostate 2520 9. Nov 2012 dropbear_rules.m
iptables -I root ostate 1184 9. Nov 2012 firewall_rules.m
iptables -I root ostate 3027 9. Nov 2012 ftpt_rules.m
iptables -I root ostate 2282 9. Nov 2012 hardening_rules.m
iptables -I root ostate 3396 9. Nov 2012 ids_rules.m
iptables -I root ostate 1550 9. Nov 2012 ismpd_rules.m
iptables -I root ostate 1551 9. Nov 2012 local_rules.m
iptables -I root ostate 4096 9. Nov 2012 log-entries
iptables -I root ostate 1242 9. Nov 2012 mailscanner_rules.m
iptables -I root ostate 4382 9. Nov 2012 mcafee-av_rules.m
iptables -I root ostate 3184 9. Nov 2012 month_rules.m
iptables -I root ostate 12032 9. Nov 2012 ms_dhcp_rules.m
iptables -I root ostate 1800 9. Nov 2012 ms-exchange_rules.m
iptables -I root ostate 2131 9. Nov 2012 ms_ftpt_rules.m
iptables -I root ostate 2242 9. Nov 2012 msrpc_rules.m
iptables -I root ostate 2508 9. Nov 2012 mysql_rules.m
iptables -I root ostate 9989 9. Nov 2012 nand_rules.m
iptables -I root ostate 3514 9. Nov 2012 netbiosfw_rules.m
iptables -I root ostate 2540 9. Nov 2012 nginx_rules.m
iptables -I root ostate 6992 9. Nov 2012 openbsd_rules.m
iptables -I root ostate 31059 9. Nov 2012 ossec_rules.m
iptables -I root ostate 3219 9. Nov 2012 pam_rules.m
iptables -I root ostate 3153 9. Nov 2012 php_rules.m
iptables -I root ostate 6896 9. Nov 2012 pix_rules.m
iptables -I root ostate 582 9. Nov 2012 policy_rules.m
iptables -I root ostate 5369 9. Nov 2012 postfix_rules.m
iptables -I root ostate 6104 9. Nov 2012 postgrey_rules.m
iptables -I root ostate 6140 9. Nov 2012 profpd_rules.m
iptables -I root ostate 2589 9. Nov 2012 pure-ftpt_rules.m
iptables -I root ostate 2007 9. Nov 2012 racoon_rules.m
iptables -I root ostate 1004 9. Nov 2012 rundecke_rules.m
iptables -I root ostate 1581 9. Nov 2012 rules_config.m
iptables -I root ostate 4905 9. Nov 2012 sendmail_rules.m
iptables -I root ostate 2846 9. Nov 2012 snmp_rules.m
iptables -I root ostate 1805 9. Nov 2012 solaris-bm_rules.m
iptables -I root ostate 2612 9. Nov 2012 sshd_rules.m
iptables -I root ostate 895 9. Nov 2012 squid_rules.m
iptables -I root ostate 7258 9. Nov 2012 squid_rules.m
iptables -I root ostate 9480 9. Nov 2012 snmp_rules.m
iptables -I root ostate 1531 9. Nov 2012 symantec-av_rules.m
iptables -I root ostate 1707 9. Nov 2012 symantec-av_rules.m
iptables -I root ostate 18378 9. Nov 2012 syslog_rules.m
iptables -I root ostate 1388 9. Nov 2012 telnetd_rules.m
iptables -I root ostate 4096 9. Nov 2012 translated
iptables -I root ostate 1491 9. Nov 2012 trend-micro_rules.m
iptables -I root ostate 854 9. Nov 2012 vsnpd_rules.m
iptables -I root ostate 4829 9. Nov 2012 vmware_rules.m
iptables -I root ostate 1773 9. Nov 2012 vpn-concentrator_rules.m

```

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>
```

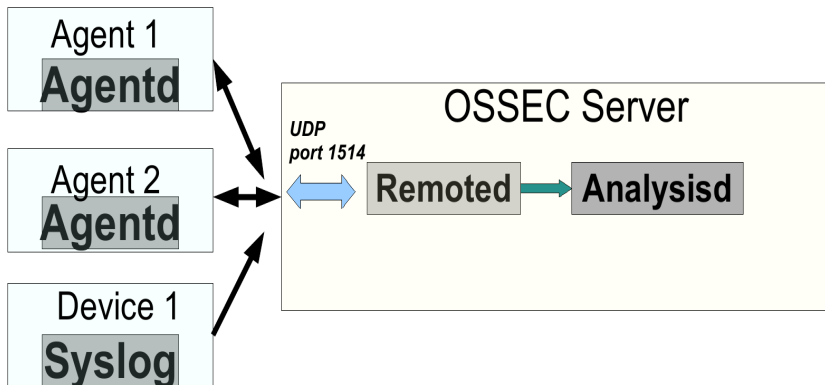
Rules 2/2

- ▶ 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>
```

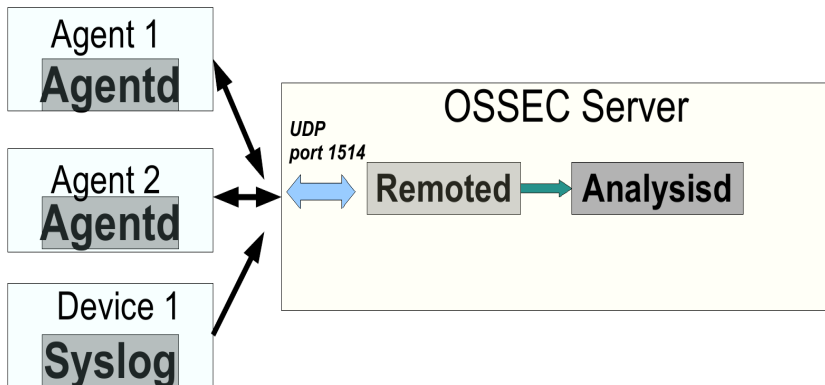
```
1 <rule id="35052" level="10" frequency="$SQUID_FREQ" timeframe="120">
  <if_matched_sid>35007</if_matched_sid>
3   <same_source_ip />
  <description>Multiple unauthorized attempts to use proxy.</description>
5 </rule>
```

Network Communication



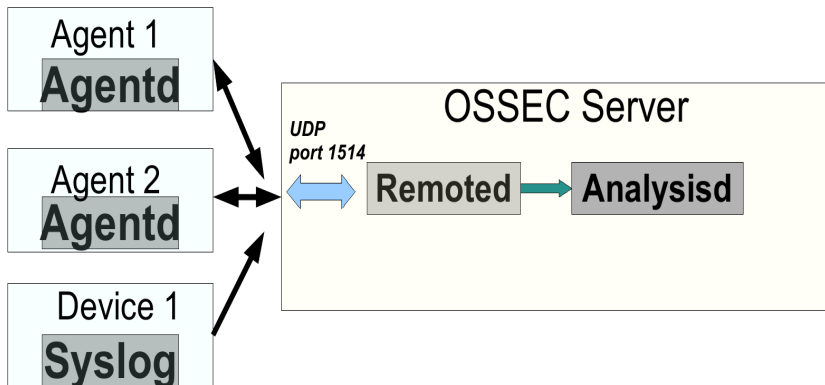
- komprimiert (zlib)

Network Communication



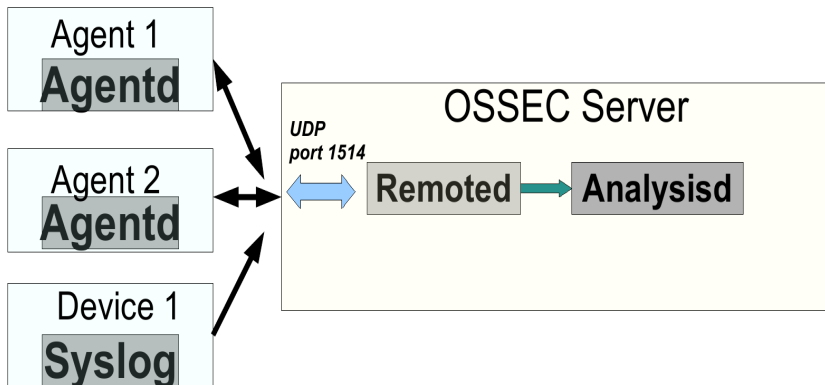
- ▶ komprimiert (zlib)
- ▶ verschlüsselt mit pre-shared keys

Network Communication



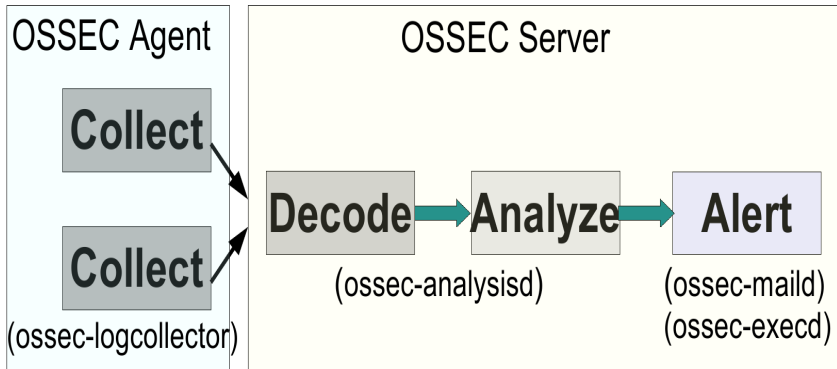
- ▶ komprimiert (zlib)
- ▶ verschlüsselt mit pre-shared keys
- ▶ verwendet per default UDP port 1514 (FW Freischaltung!)

Network Communication



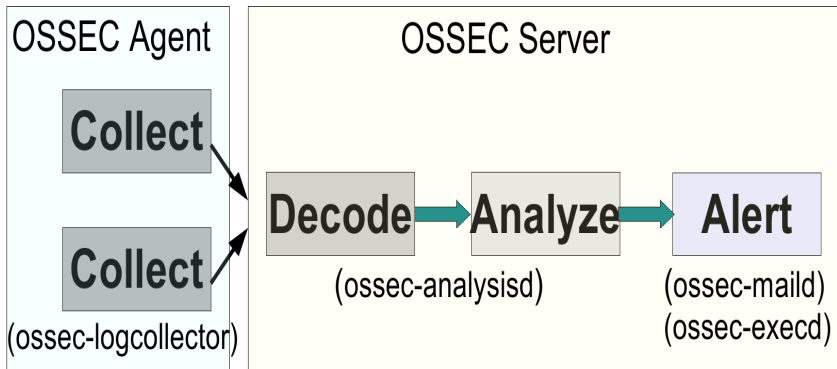
- ▶ komprimiert (zlib)
- ▶ verschlüsselt mit pre-shared keys
- ▶ verwendet per default UDP port 1514 (FW Freischaltung!)
- ▶ Multi-platform (Windows, Solaris, Linux, etc)

Log Flow (agent/server)



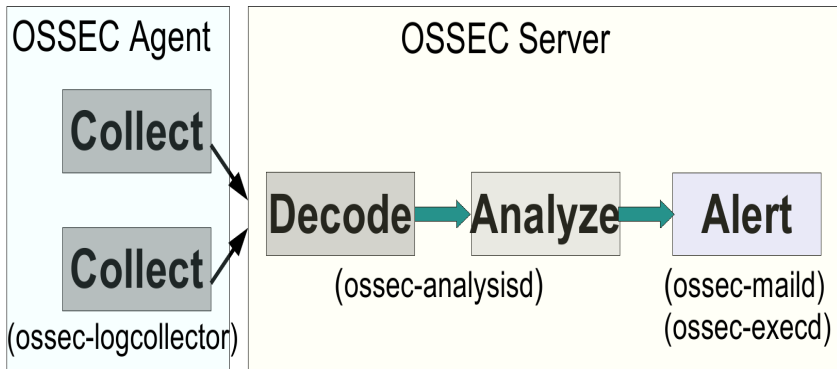
- ▶ ossec-logcollector sammelt die Logs

Log Flow (agent/server)



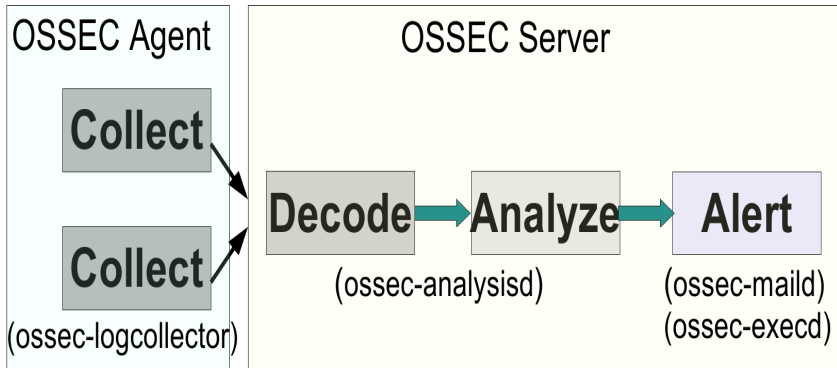
- ▶ ossec-logcollector sammelt die Logs
- ▶ ossec-analysisd analysiert und decoded Logs

Log Flow (agent/server)



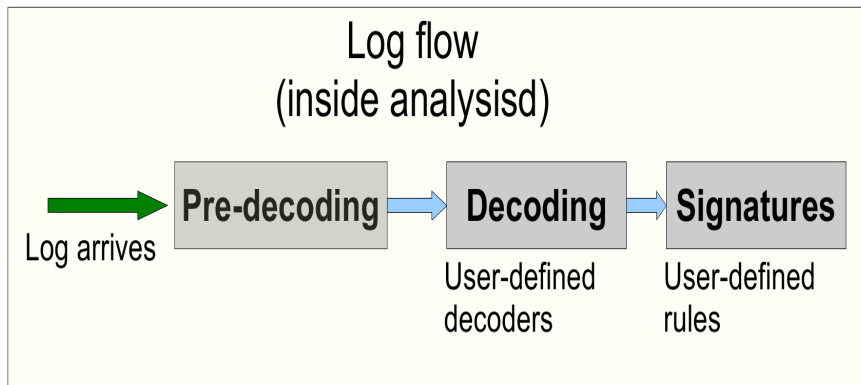
- ▶ ossec-logcollector sammelt die Logs
- ▶ ossec-analysisd analysiert und decoded Logs
- ▶ ossec-maild verschickt die Meldungen

Log Flow (agent/server)



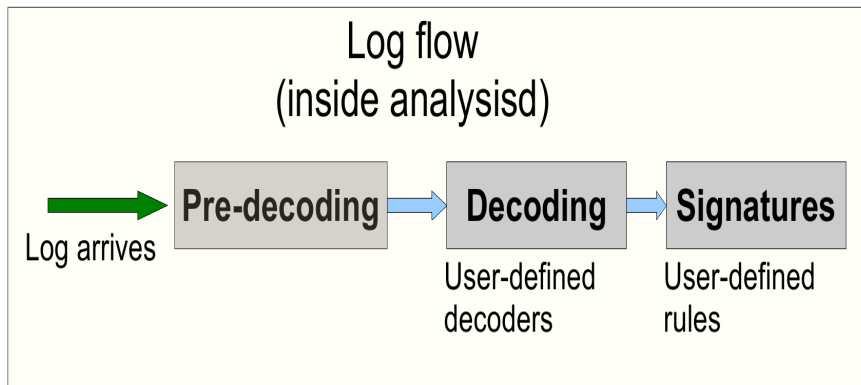
- ▶ ossec-logcollector sammelt die Logs
- ▶ ossec-analysisd analysiert und decoded Logs
- ▶ ossec-maild verschickt die Meldungen
- ▶ ossec-execd

Internal Log Flow



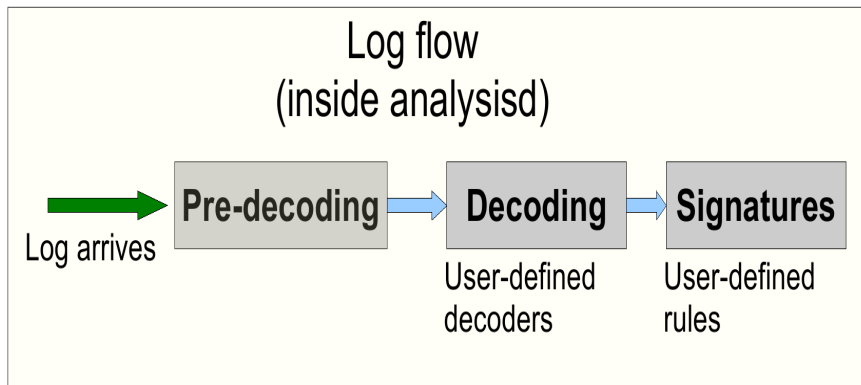
- ▶ 3 Hauptteile:
 - ▶ Pre-decoding (extrahiert bekannte Bereiche, wie Datum/Zeit, etc)

Internal Log Flow



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

Internal Log Flow



- ▶ 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:

```
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
```

Decoding

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
```

Decoding 2/2

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
```


Log / Data Processing

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

Danke für eure Aufmerksamkeit!

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