Host-Intrustion Detection based on OSSEC

Theresa Meiksner

3. 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
- 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?

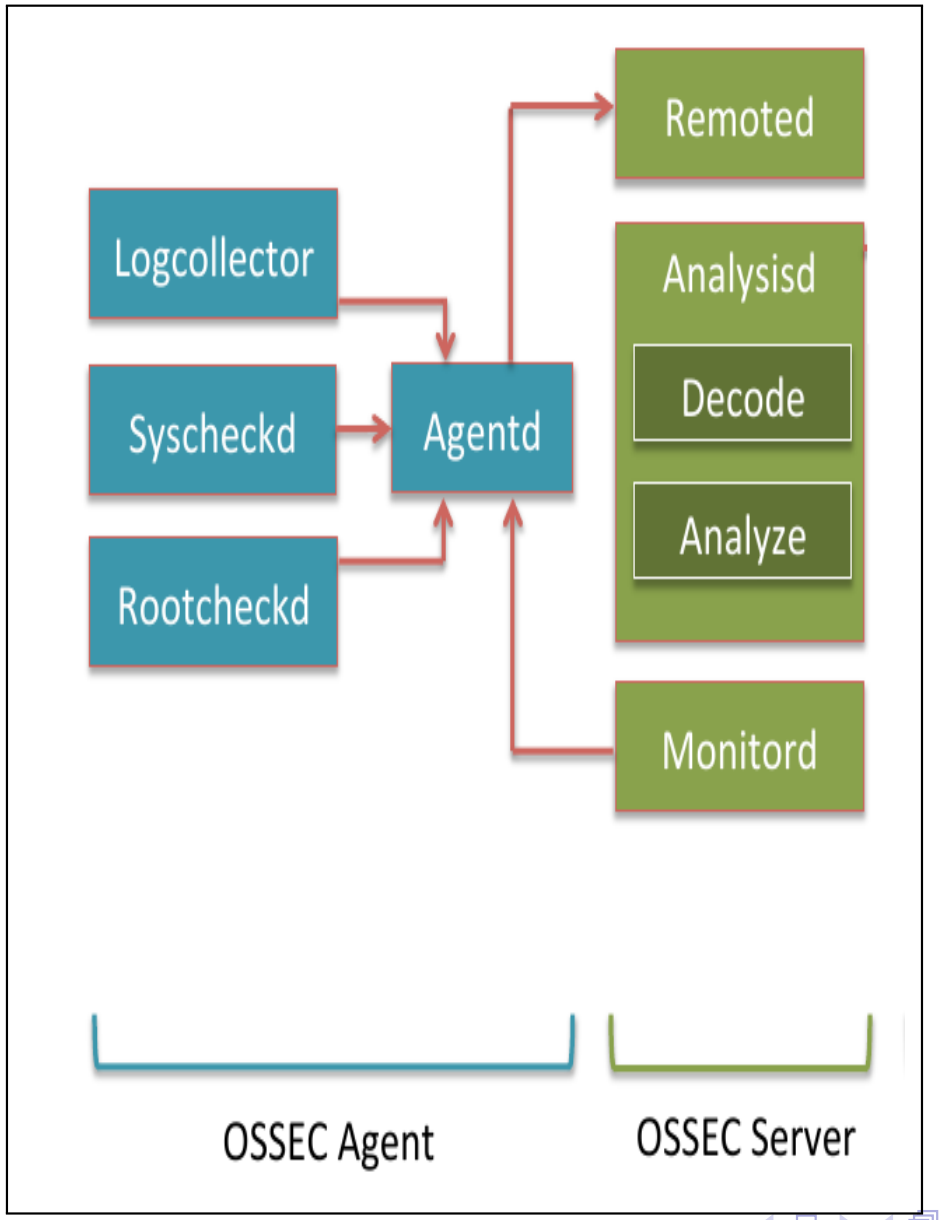
Wozu Log Analyse?

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

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

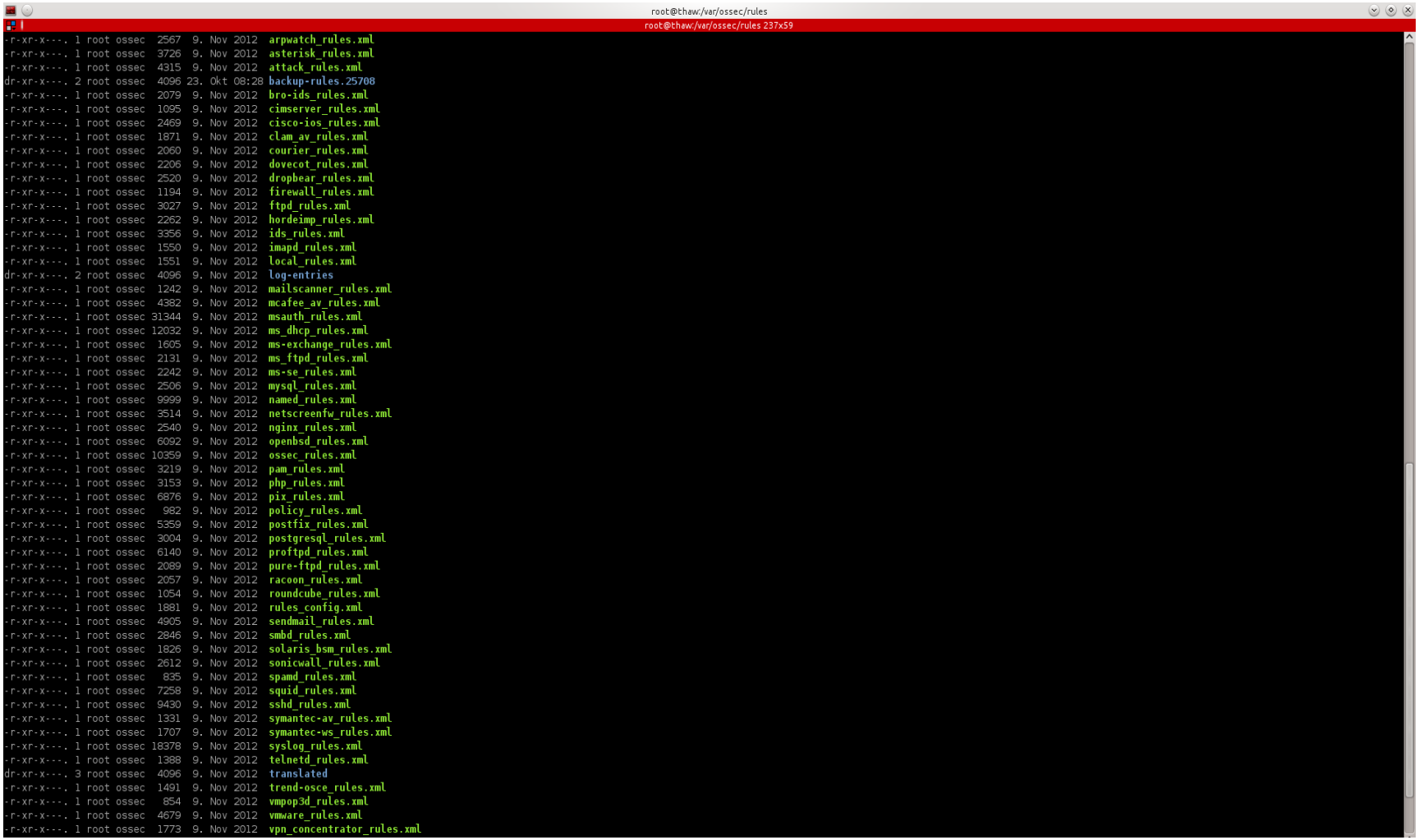
- Analysisd - Hauptprozess, ist hauptverantwortlich für die Analyse von Logs
- Remoted – Empfängt und leitet die remote logs an analysisd weiter
- Logcollector – lesen und weiterleiten der Logs an analysisd
- Agentd – leitet die Logs an den Server (master) weiter
- Maild – verschickt die e-mail alerts
- 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) 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.



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

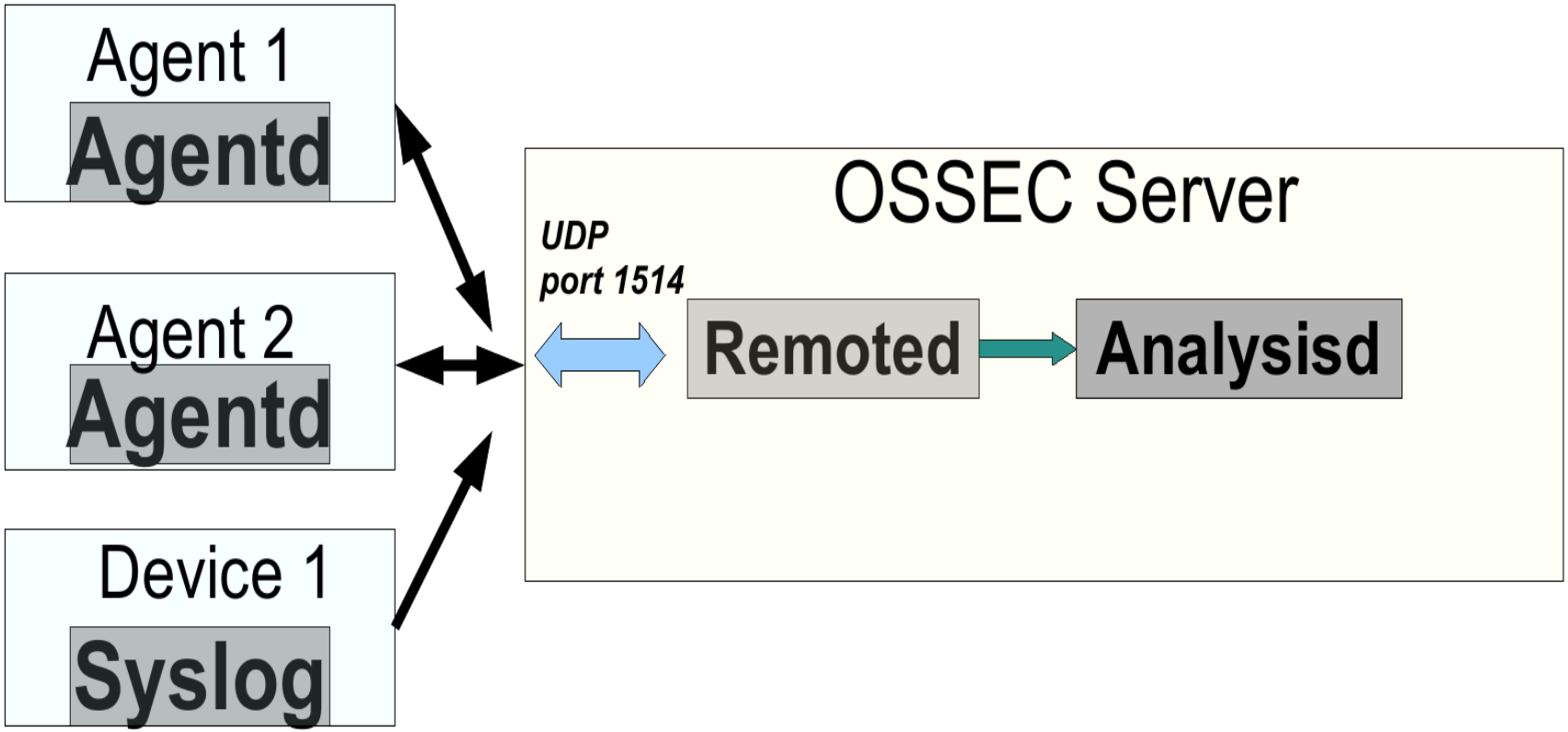
Example

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

Example

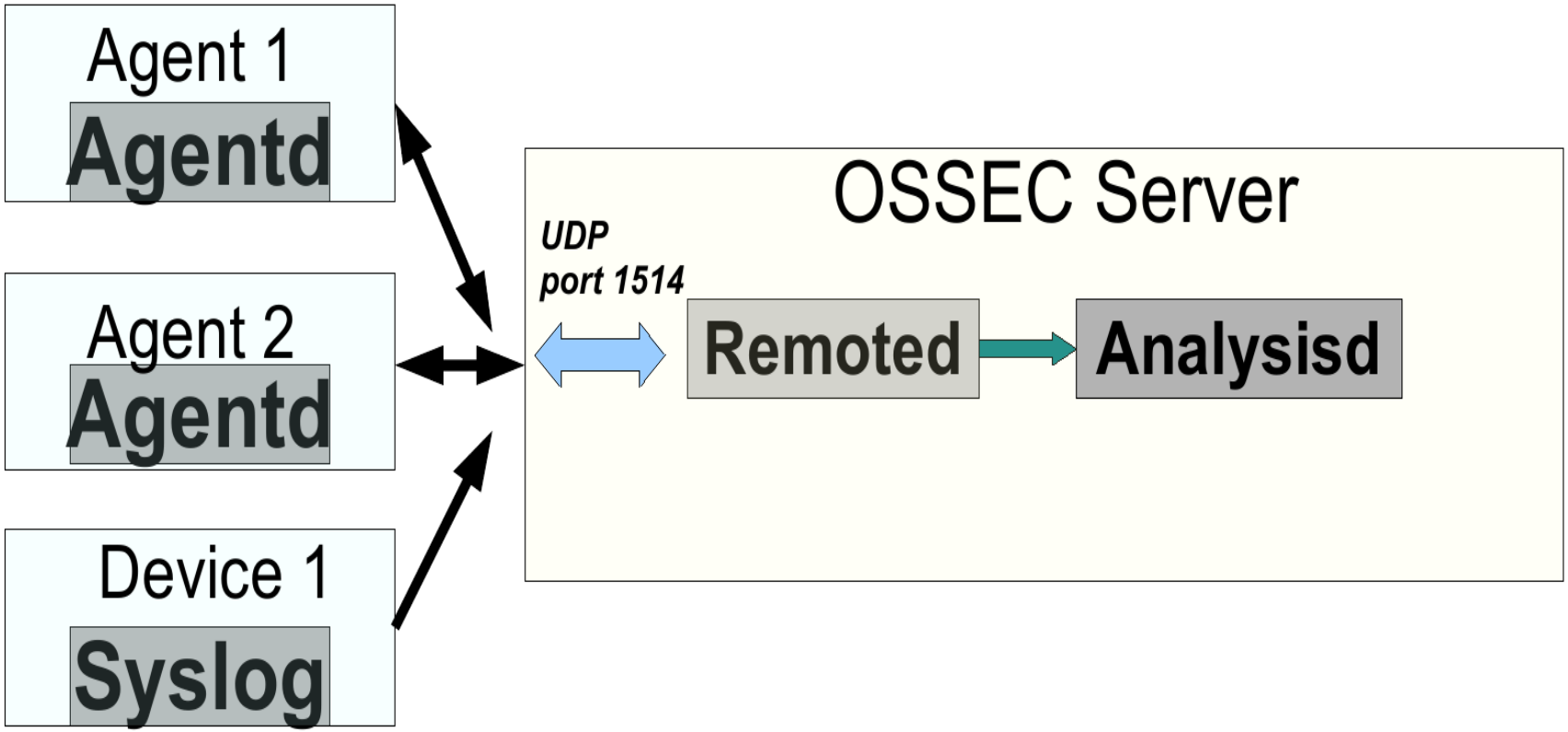
```
<rule id="35052" level="10" frequency="$SQUID_FREQ" timeframe="120">
    <if_matched_sid>35007</if_matched_sid>
    <same_source_ip />
    <description>Multiple unauthorized attempts to use proxy.</description>
  </rule>
```

Network Communication



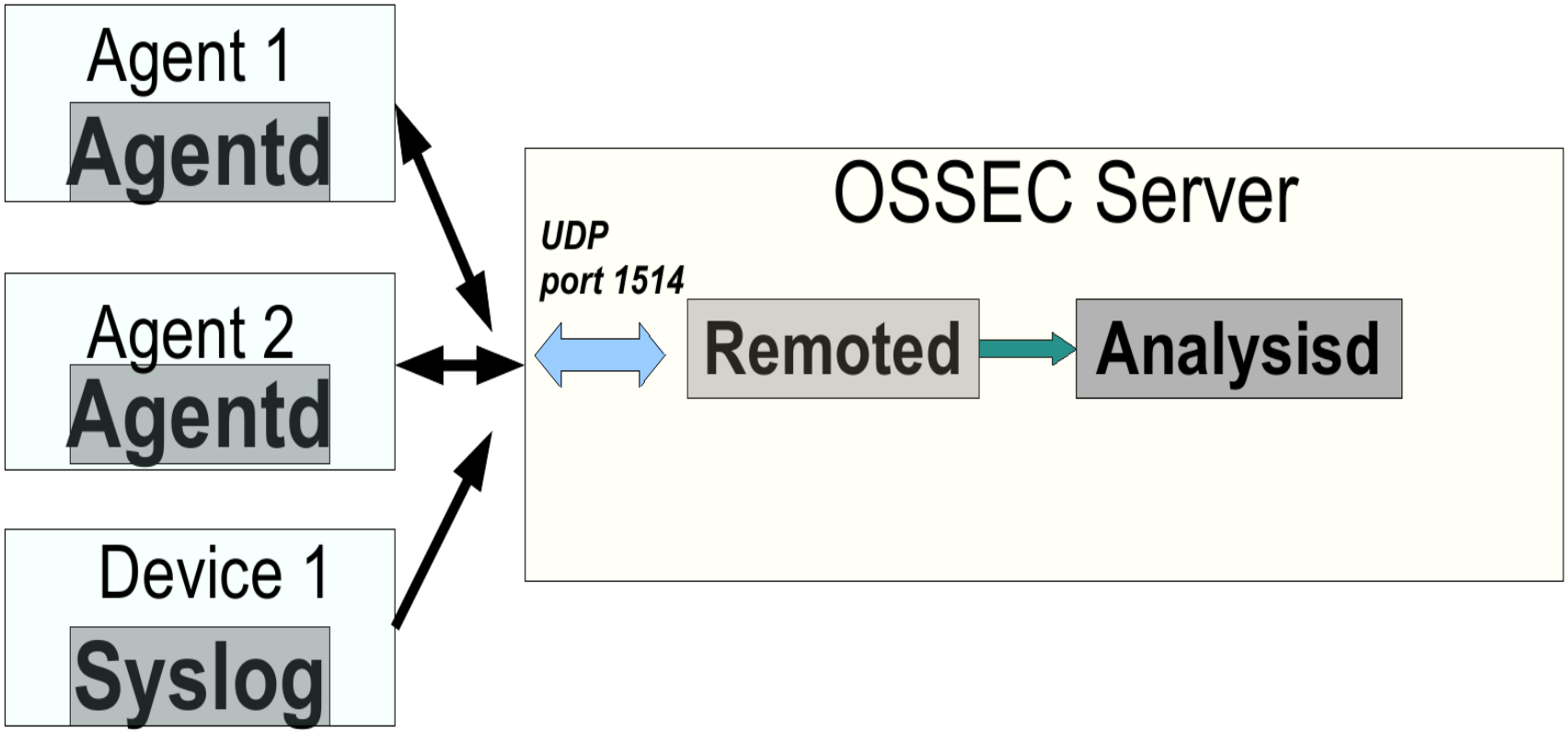
- komprimiert (zlib)

Network Communication



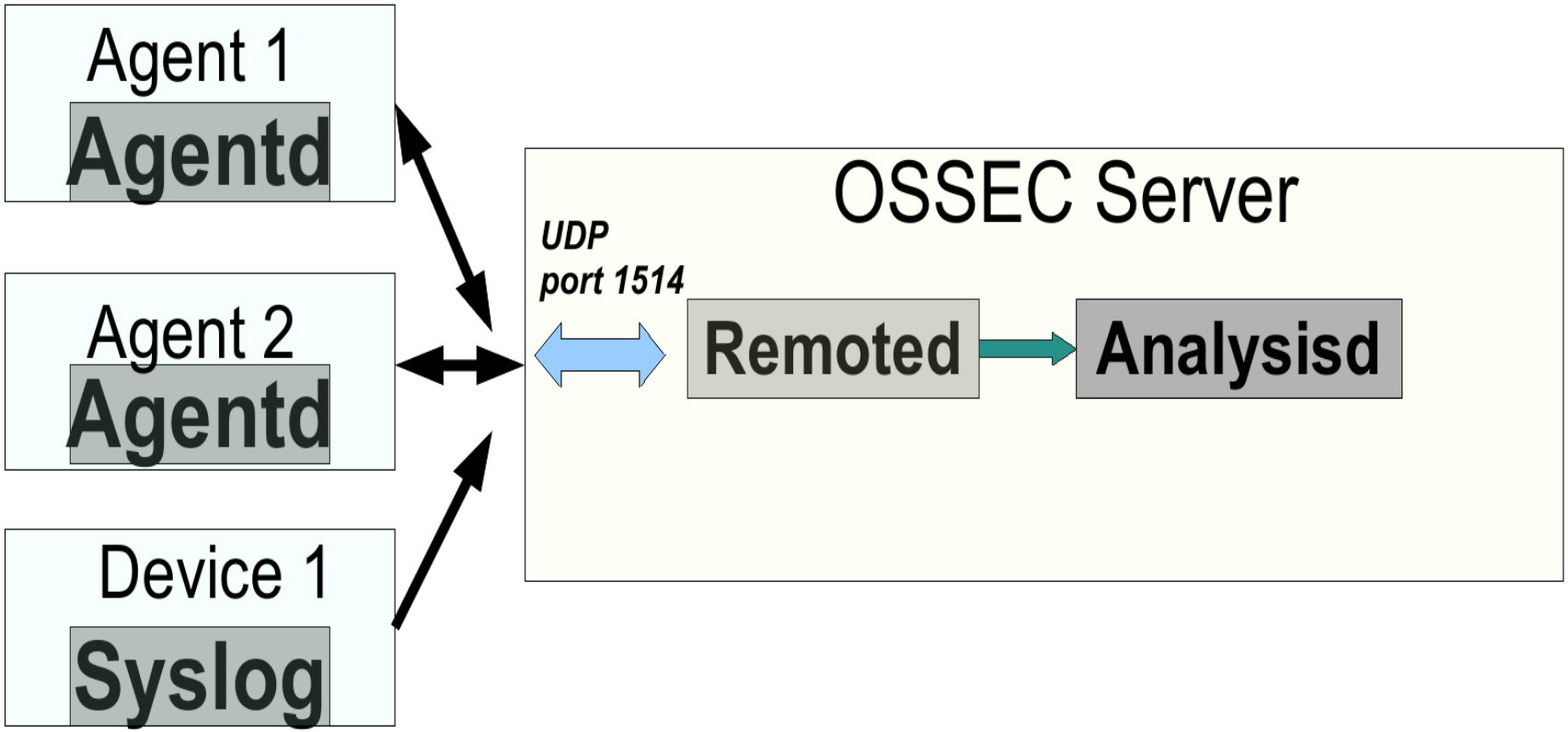
- komprimiert (zlib)
- verschlüsselt mit pre-shared keys

Network Communication



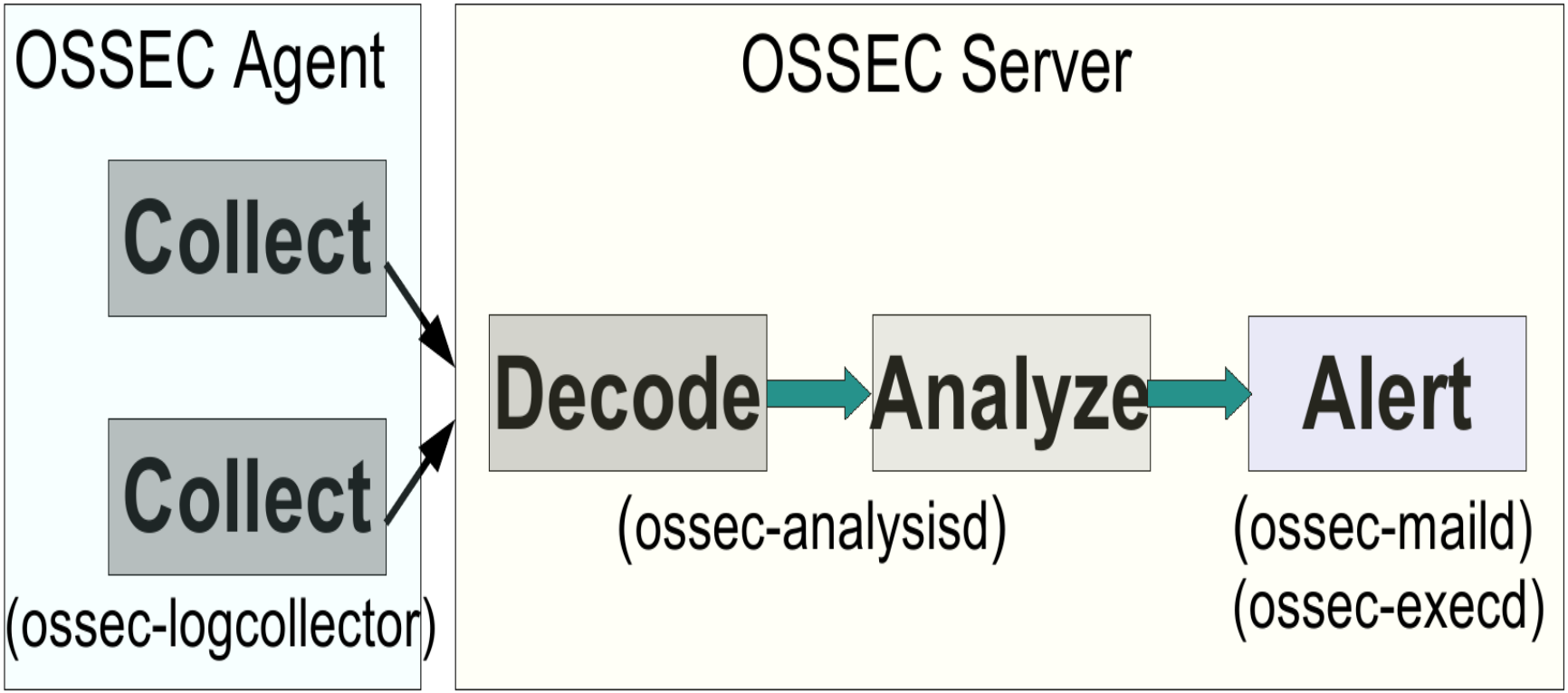
- komprimiert (zlib)
- verschlüsselt mit pre-shared keys
- verwendet per default UDP port 1514 (FW Freischaltung!)

Network Communication



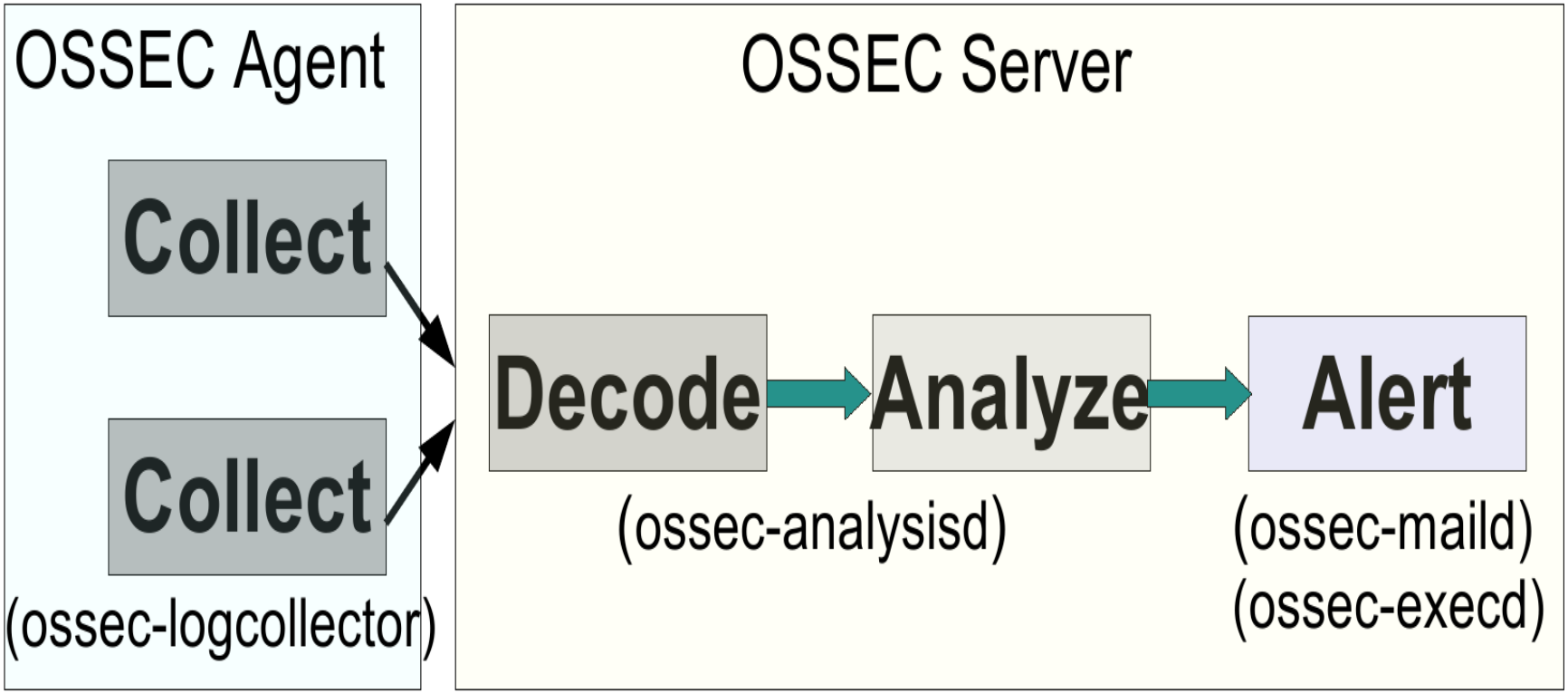
- komprimiert (zlib)
- verschlüsselt mit pre-shared keys
- verwendet per default UDP port 1514 (FW Freischaltung!)
- Multi-platform (Windows, Solaris, Linux, etc)

Log Flow (agent/server)



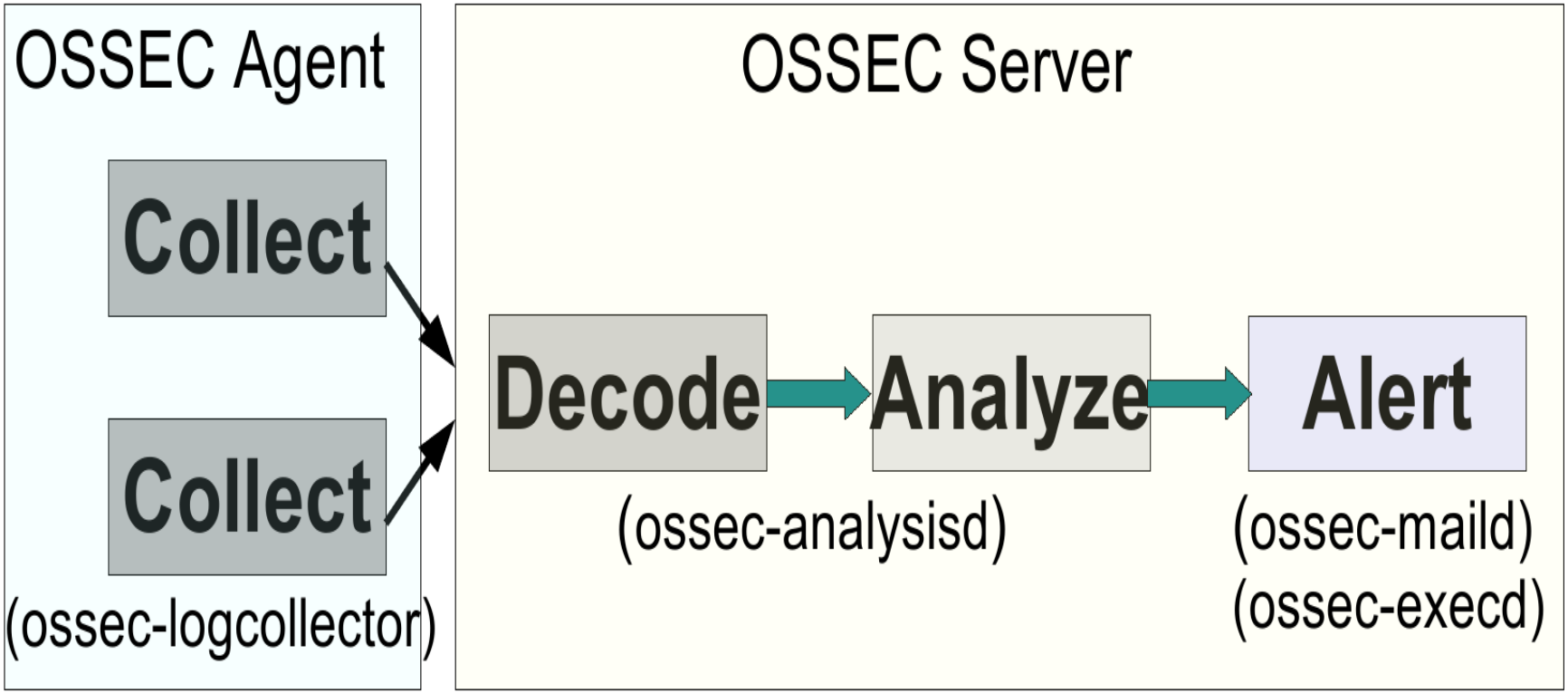
- ossec-logcollector sammelt die Logs

Log Flow (agent/server)



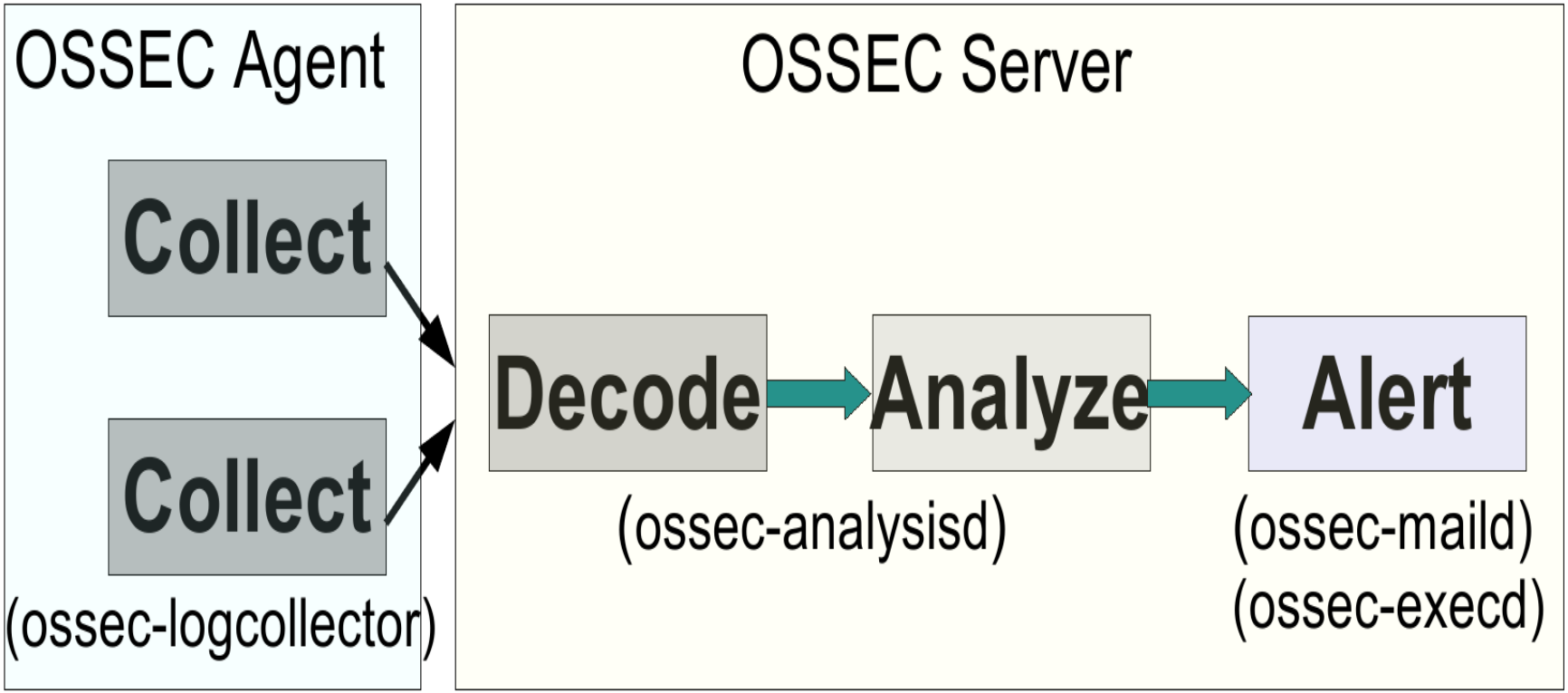
- ossec-logcollector sammelt die Logs
- ossec-analysisd analysiert und decoded Logs

Log Flow (agent/server)



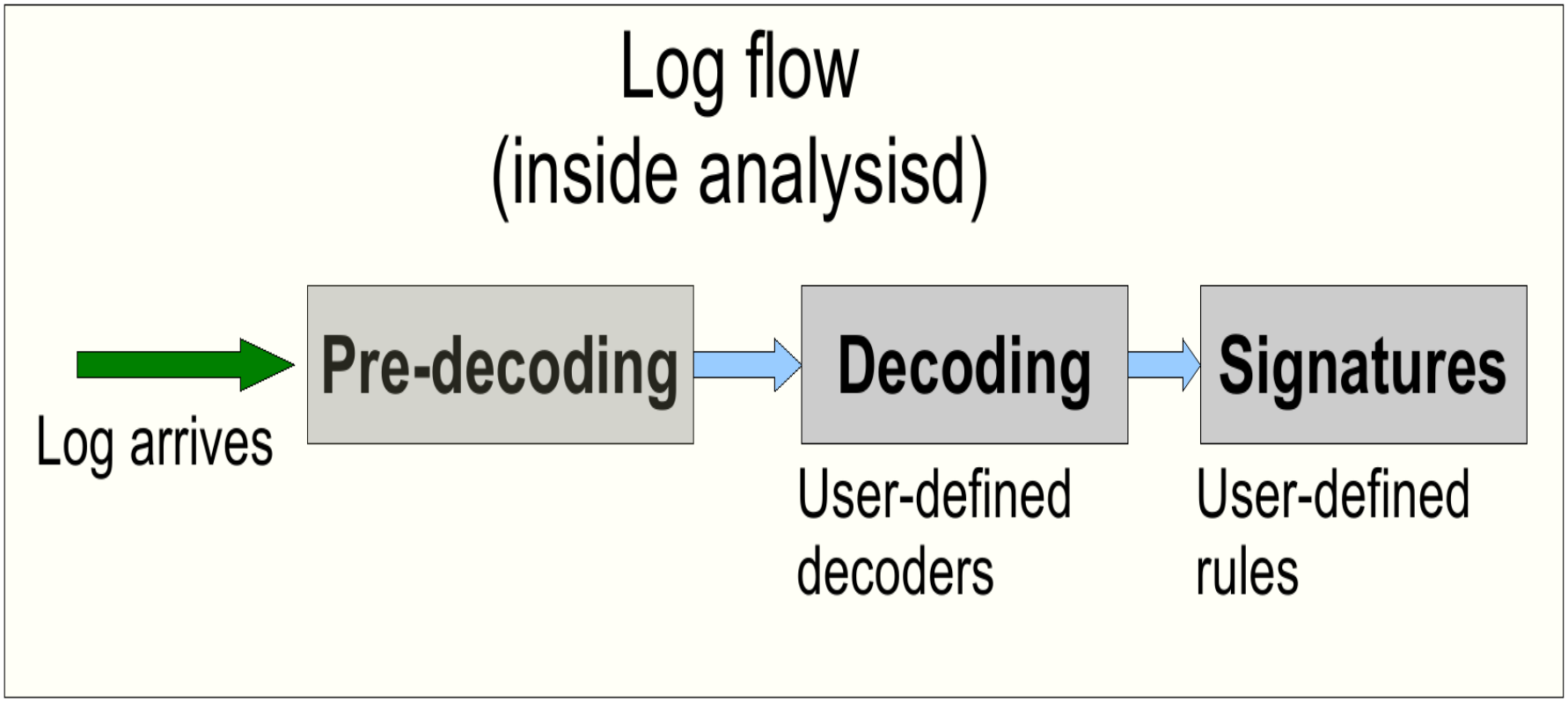
- ossec-logcollector sammelt die Logs
- ossec-analysisd analysiert und decoded Logs
- ossec-maild verschickt die Meldungen

Log Flow (agent/server)



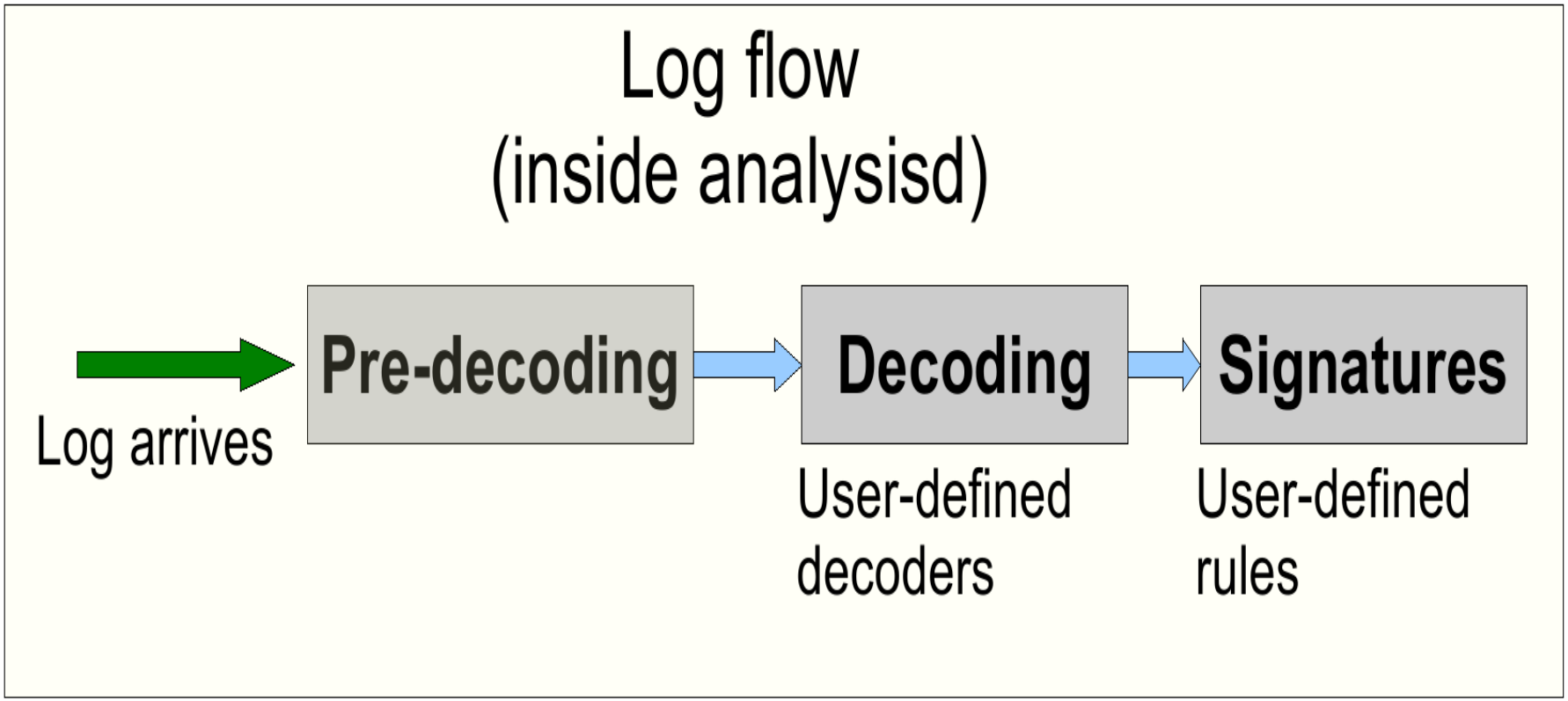
- ossec-logcollector sammelt die Logs
- ossec-analysisd analysiert und decoded Logs
- ossec-maild verschickt die Meldungen
- ossec-execd

Internal Log Flow



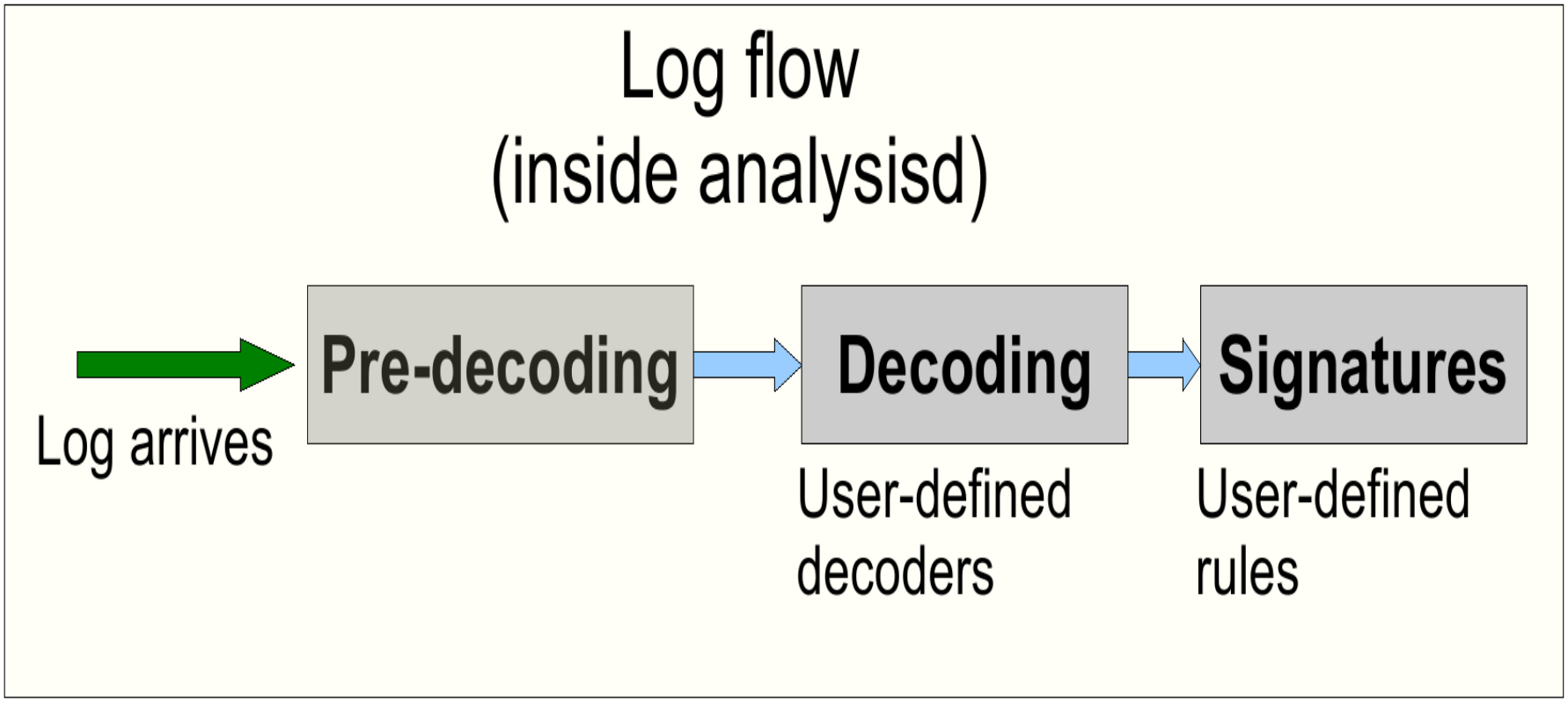
- 3 Hauptteile:
  - Pre-decoding (extrahiert bekannte Bereiche, wie Datum/Zeit, etc)

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:

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
```

Decoding

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
```

Decoding 2/2

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
```

Alerts

- 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...

Log / Data Processing

- 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.aremai.net/files/ossec_summary.pdf