OSSIM

Open Source SIEM
KNF Kongress, 25.11.2012

SIEM

- Wikipedia

Create account Log in

Article Talk Read Edit View history Search

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

Toolbox

Print/export

Languages
Česky
Italiano

Security information and event management

From Wikipedia, the free encyclopedia

This article **has been nominated to be checked for its neutrality.** Discussion of this nomination can be found on the talk page. *(September 2012)*

Security Information and Event Management (SIEM) solutions are a combination of the formerly disparate product categories of SIM (security information management) and SEM (security event manager). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes.[1]

The acronyms SEM, SIM and SIEM have been used interchangeably, though there are differences in meaning and product capabilities. The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is commonly known as Security Event Management (SEM). The second area provides long-term storage, analysis and reporting of log data and is known as Security Information Management (SIM).[2] As with many meanings and definitions of capabilities evolving requirements continually shape derivatives of SIEM product categories. The need for voice centric visibility or vSIEM (voice security information and event management) is a recent example of this evolution.

The term Security Information Event Management (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005,[3] describes the product capabilities of gathering, analyzing and presenting information from network and security devices; identity and access management applications; vulnerability management and policy compliance tools; operating system, database and application logs; and external threat data. A key focus is to monitor and help manage user and service privileges, directory services and other system configuration changes; as well as providing log auditing and review and incident response.[2]

As of January 2012, [4] Mosaic Security Research identified 85 unique SIEM products.

ANFORDERUNGEN

- **S**ecurity **I**nformation and **E**vent **M**anagement
- Anforderungen
  - Aggregierung von Daten
  - Korrelation
  - Alarmierung
  - Dashboards
  - Compliance
  - Langzeitarchivierung
  - Echtzeit oder zumindest beinahe Echtzeit

OSSIM

- Open Source SIEM
  - aktuelle Version 4.1
  - basiert auf Debian (aktuell Squeeze)
  - Entwicklung in Madrid
- AlienVault
  - vertreibt kommerzielle Version
  - entwickelt OSS und Pro Version

GESCHICHTE

2003
Eine kleine Gruppe von "Hackern" beschliesst das Datenchaos zu beenden. OSSIM wird geboren

2007
OSSIM ist kampferprobt. AlienVault wird gegründet. Die Firma wird zu einer Softwarefirma

2011
Umzug der Firma ins Silicon Valley. OSSIM mittlerweile ca. 160.000x heruntergeladen
OSSIM 3.0 erscheint

2012
OSSIM 4.0 und 4.1 erscheinen. Viele neue Features.

WIE SEHE ICH MEHR?

- Logs
- Monitoring
- Schwachstellen kennen
- Paketanalyse
- File Integrity Monitoring
- Anomalien erkennen
- Korrelation
- Aktuelles Netz möglichst genau kennen

WAS IST DRIN

- IDS
  - Snort, Suricata
- WIDS (Wireless IDS)
  - Kismet
- HIDS (Host-Based IDS)
  - Ossec
- NetFlow collection
  - NFsen
- Availability Monitoring
  - Nagios
- Scannen
  - aktiv: nmap
  - passiv: p0f, prads
- Vulnerability Scanner
  - OpenVAS
  - optional Nessus
- Inventarisierung
  - OCS Inventory NG
- OSVDB

WAS IST DRIN?

Detection Tools

EMERGING THREATS

SNORT

OSSEC

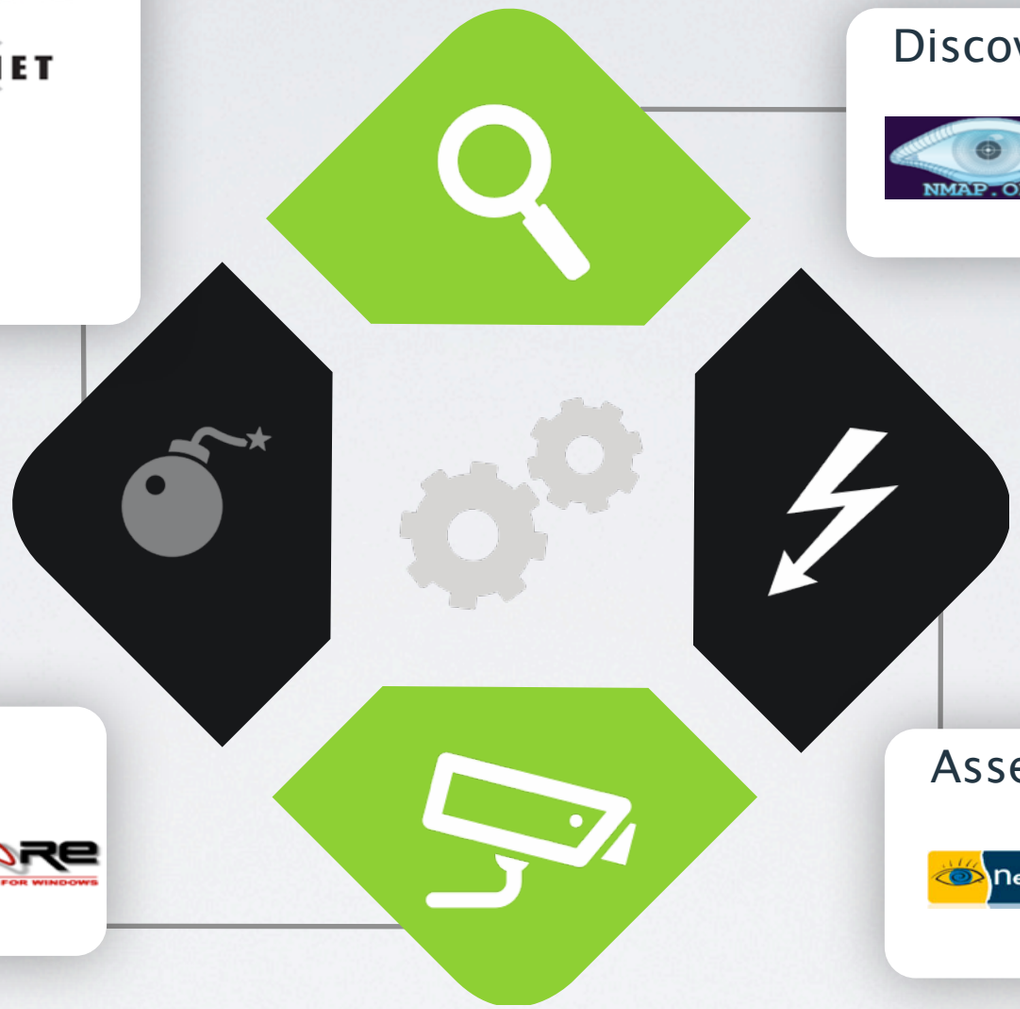
KISMET

SURICATA

Discovery Tools

NMAP.ORG

OCS inventory



debian

Monitoring Tools

ntop

Nagios

SNARE AGENT FOR WINDOWS

Assessment Tools

Nessus

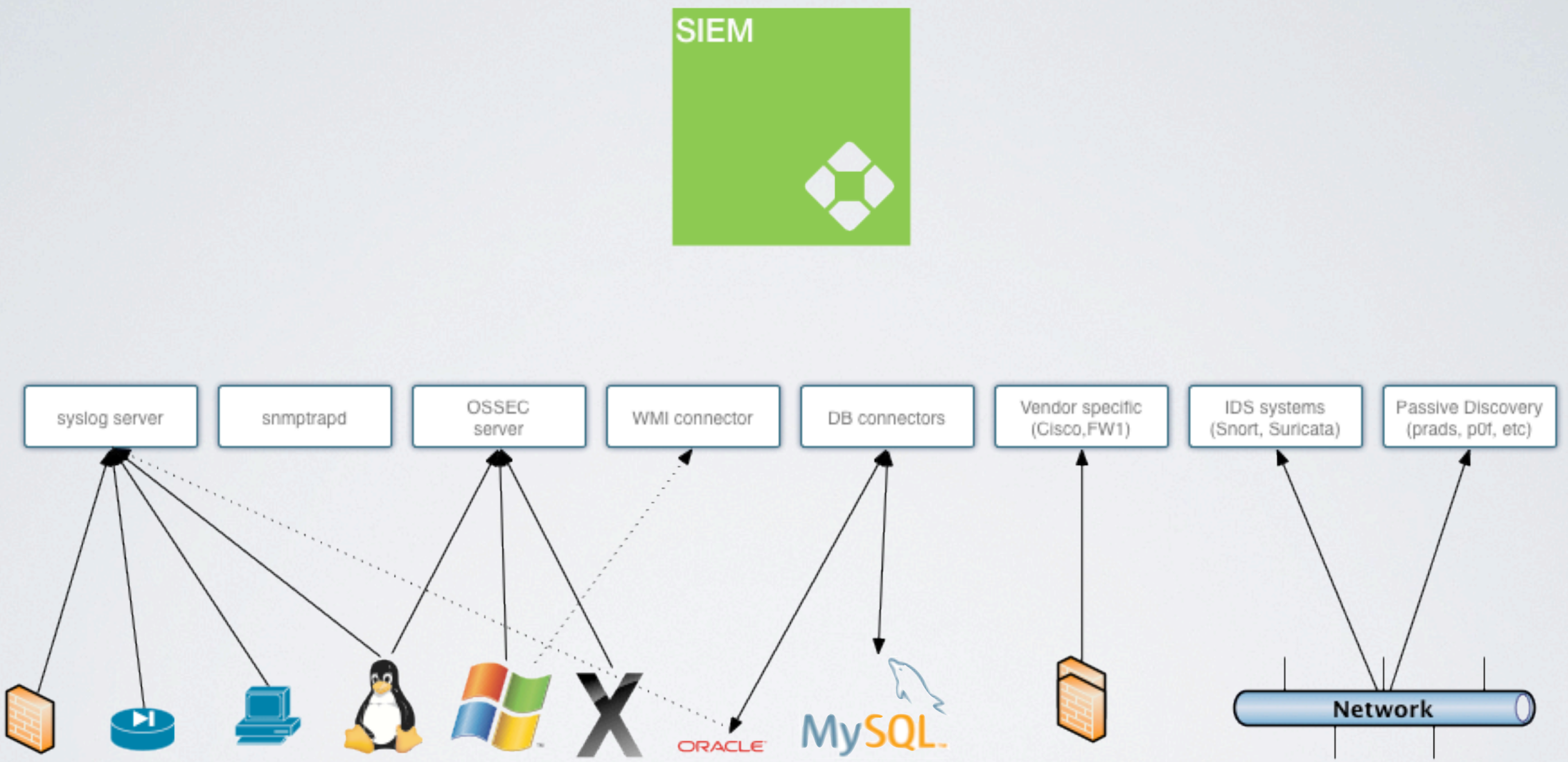
OSVDB

OpenVAS

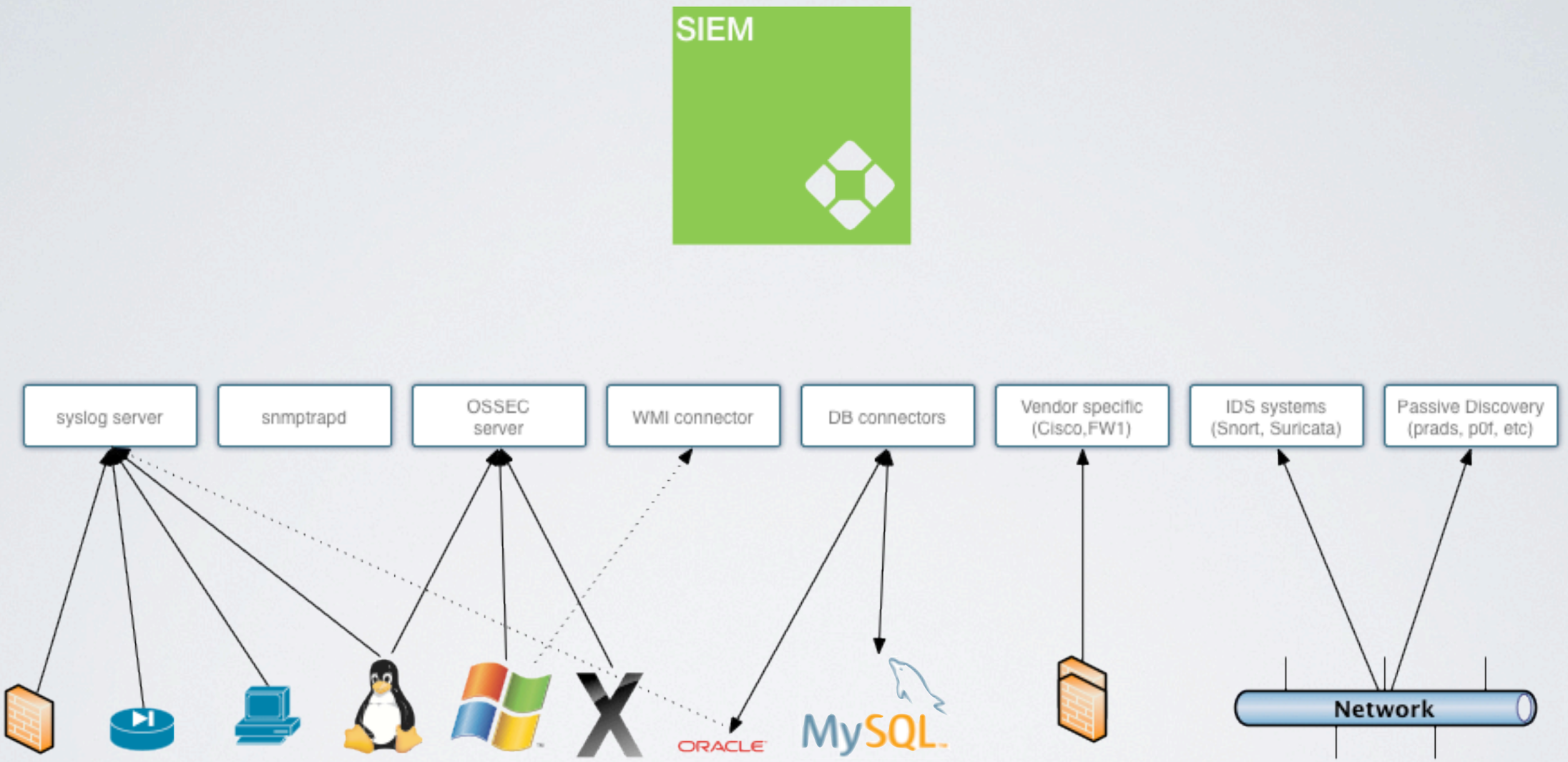
WARUM SO VIELE TOOLS?

- Sicherheit durch Sichtbarkeit
- Bei einem Vorfall ist man über jede Zusatzinfo dankbar
- Man möchte im Idealfall alle Infos zentral haben
- Man hat oder wird ähnliche Tools eh im Einsatz haben

OSSIM DATENQUELLEN

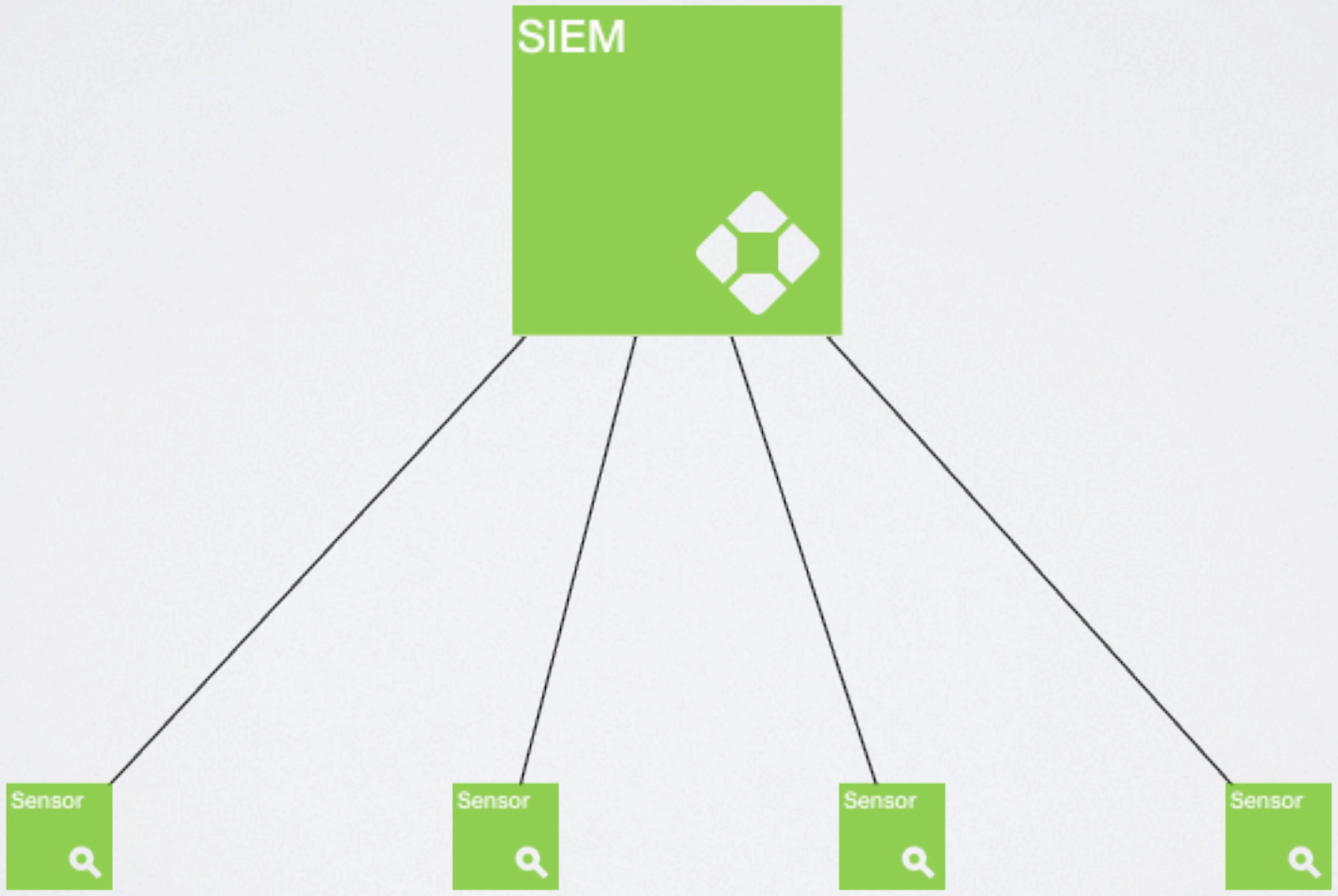


MÖGLICHE SETUPS



MÖGLICHE SETUPS

- Verteilte Architektur
  - zentrales SIEM (UI, Korrelation, SQL)
  - verteilte Sensoren
    - z.B Erlangen, Nürnberg, Regensburg, Würzburg



NORMALISIERUNG

```
Nov 24 17:47:36 alienvault sshd[12888]: Accepted
password for root from 192.168.3.100 port 61582 ssh2
```

```
Nov 24 17:47:36
```

Date	24.11.2012 17:47:36

```
alienvault
```

Destination IP	alienvault (192.168.3.222)

```
sshd
```

Data Source	sshd

```
Accepted password for
```

Event Type	Successful Login (password)

```
root
```

Username	root

```
from 192.168.3.100
```

Source IP	192.168.3.100

```
port 61582
```

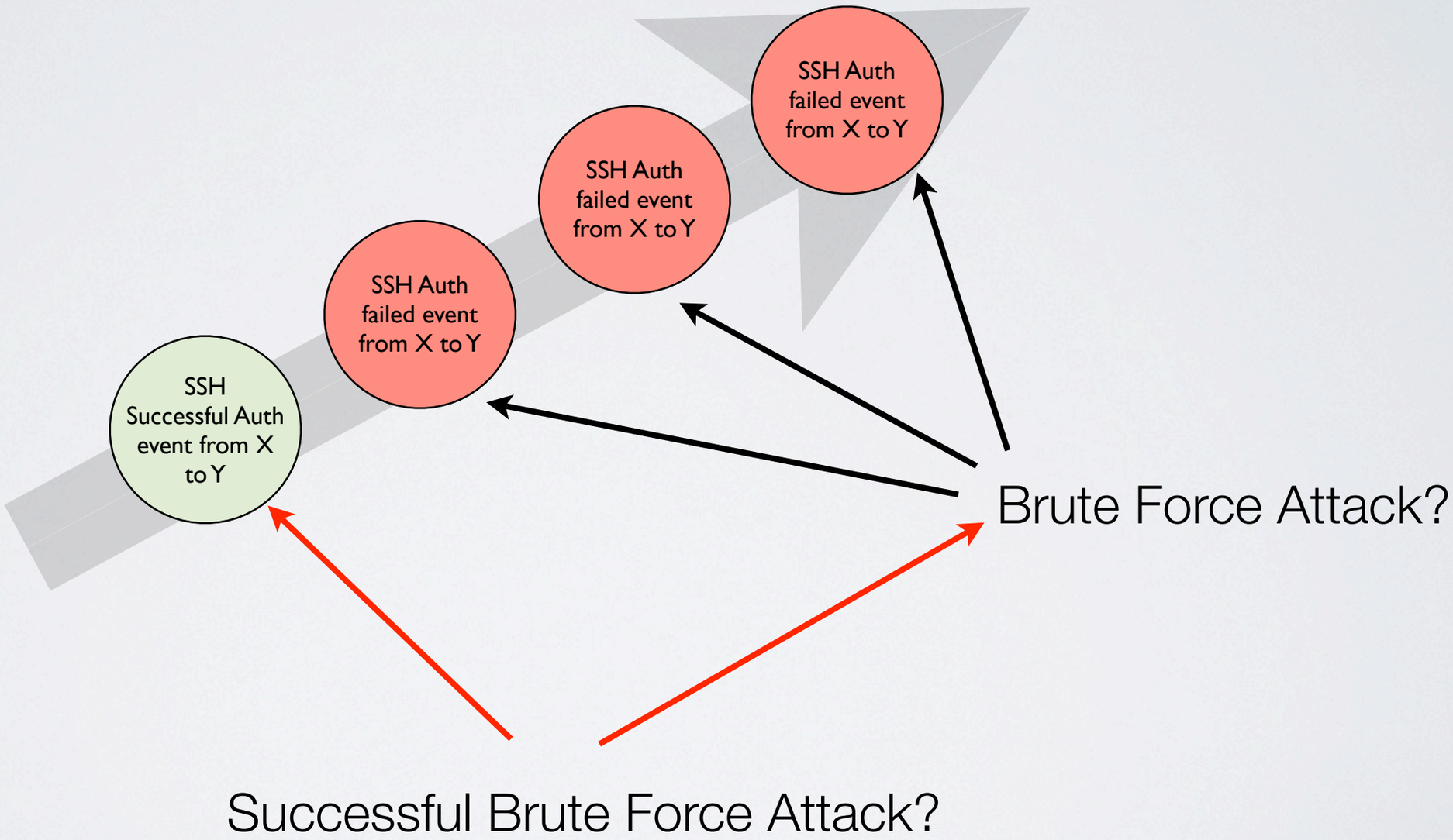
Source Port	61582

Destination Port	22

- Lesen der Logzeile(n)
- Parsen der interessanten Infos
  - Datum laut Syslog
  - Destination IP
    - alienvault
  - Datenquelle
    - sshd
  - Event innerhalb der Quelle
    - Login mit Passwort
  - Username
    - root
  - Source IP
    - 192.168.3.100
  - Source Port
    - 61582
  - Destination Port
    - in diesem Fall default (22)

KORRELATION

- Bringt viele Events in Beziehung

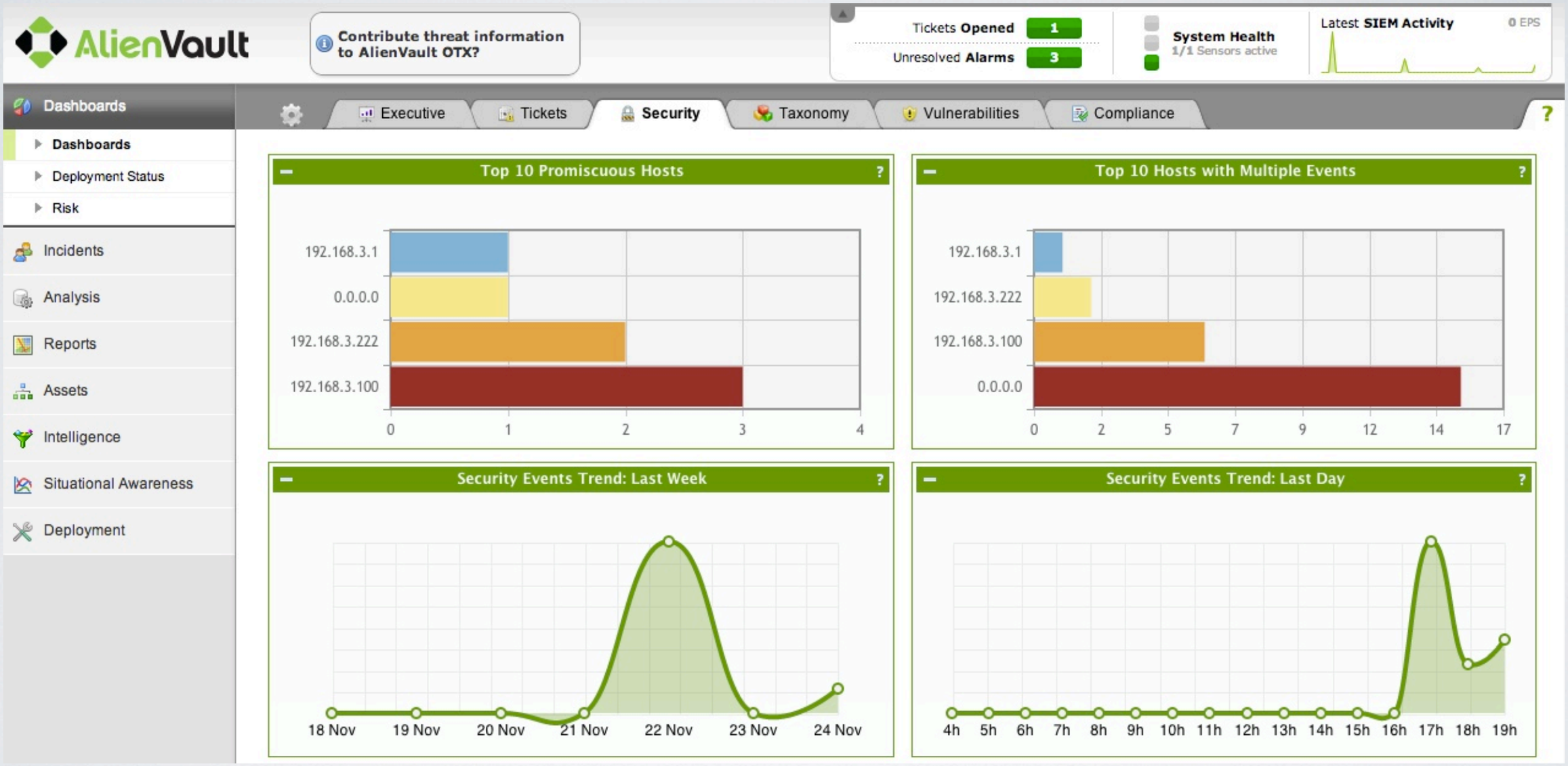


ALARMIERUNG

- Internes Alarm-Panel
- Internes Ticketing
- Aktionen auf alle Event-Arten
  - Email wenn jemand von ausserhalb sich erfolgreich auf einem internen Server einloggt
- Schicke SMS wenn ein Account als “locked out” gemeldet wird
- Beliebige Kommandos ausführbar

DASHBOARDS

- Frei anpassbar



COMPLIANCE

- Freies Mapping von Events auf die jeweiligen Regeln in
  - ISO 27001
  - PCI DSS
- Compliance Reporting

OSSIM INTERN

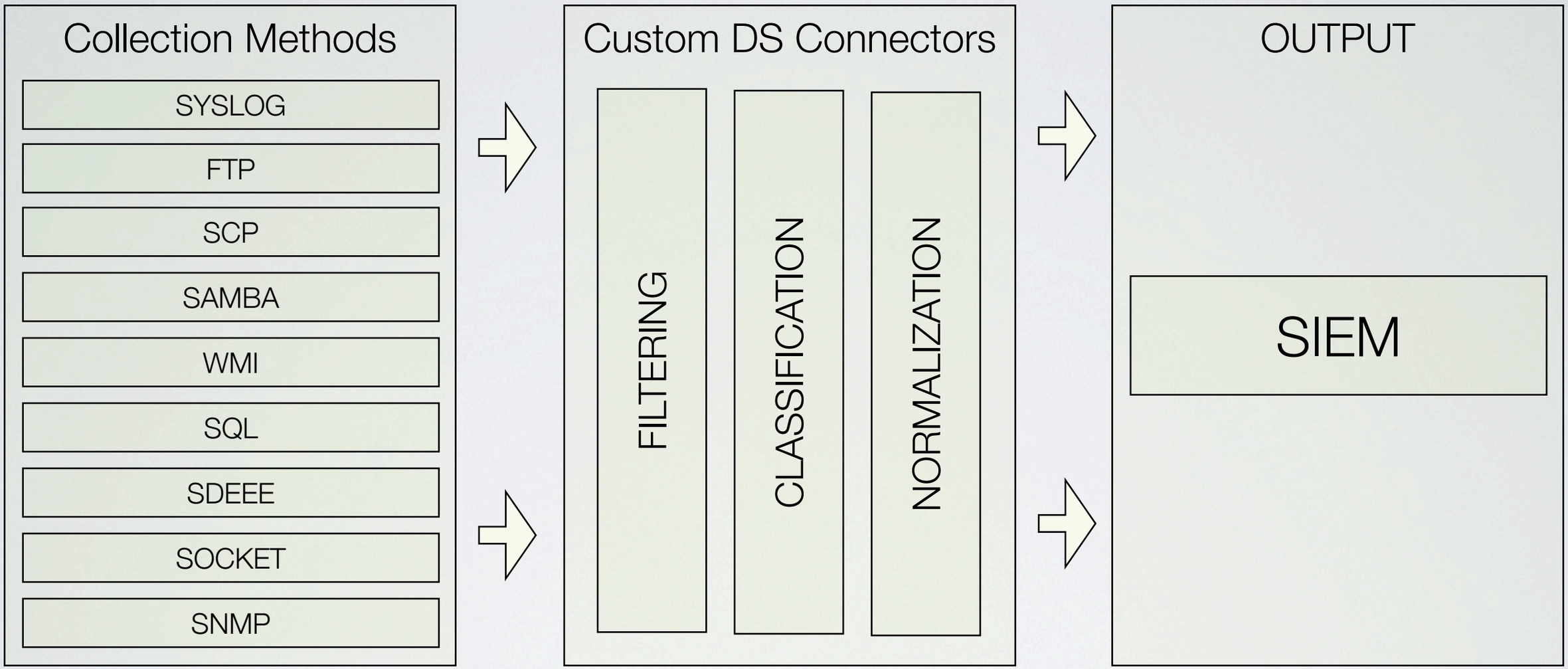
EVENT WORKFLOW

- Einsammeln der Events
- Auswerten und Parsen der Events
- Auswerten der Policy für den Event
  - Beispiele
    - zur Korrelation nutzen, aber nicht speichern
    - Priorität erhöhen
    - verwerfen
- Kalkulation eines Risikos für diesen Event
- Korrelation
- Speichern (optional)
- Bearbeiten, Suche, Reporting, Alarmierung, Ticketing

LOGS EINSAMMELN: OSSIM-AGENT

- ossim-agent sammelt Logs ein
  - Syslog
  - DB
  - Herstellerspezifische Protokolle
- Analysiert Logs
- Normalisiert
- Verschickt Events an ossim-server

OSSIM-AGENT


Collection Methods
SYSLOG
FTP
SCP
SAMBA
WMI
SQL
SDEEE
SOCKET
SNMP
Custom DS Connectors
FILTERING
CLASSIFICATION
NORMALIZATION
OUTPUT
SIEM

AGENT:WIE FUNKTIONIERTS?

- Plugins
  - definiert Datenquelle (File, DB, etc.)
  - definiert Datentyp (sshd, Cisco ASA, etc.)
  - enthält vernünftige Defaults
    - Beispiel: Destination Port 22 im Falle von SSH
- enthält beliebig viele Parsingregeln

BEISPIEL SSHD

```
[DEFAULT]
plugin_id=4003

# default values for dst_ip and dst_port
# they can be overwritten in each rule
dst_ip=\_CFG(plugin-defaults,sensor)
dst_port=22

[config]
type=detector
enable=yes

source=log
location=/var/log/auth.log

# create log file if it does not exists,
# otherwise stop processing this plugin
create_file=false

process=sshd
start=no
stop=no
startup=/etc/init.d/ssh start
shutdown=/etc/init.d/ssh stop

exclude_sids=98

[translation]
Version=22
Throughput=23
password=1
none=1
publickey=2
opened=25
closed=26
```

BEISPIEL SSHD

```
[08 - Login sucessful (Accepted password)]
# Sep  6 10:51:04 alienvault sshd[6379]: Accepted password for dgil from 10.222.14.12
port 33232 ssh2
event_type=event
regexp="(?P<date>\SYSLOG_DATE)\s+(?P<dst>\S+)\s.*ssh.*Accepted password for (?P<user>
\S+)\s.*from\s+(?P<src>\IPV4)\s.*port\s+(?P<sport>\d{1,5})"
plugin_sid=7
date={normalize_date($date)}
src_ip={resolv($src)}
dst_ip={resolv($dst)}
src_port={$sport}
username={$user}
```

RULES: REGEX

- Reguläre Ausdrücke (Python)
  - Unterstützung von Named Patterns
    - (?P<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
  - Eingebaute, erweiterbare Aliases
    - (?P<src_ip>\IPV4)
    - Verfügbar: Datum, IP Ausdrücke, etc.
- Flexibel
- relativ effizient

RULES: ZUORDNUNG

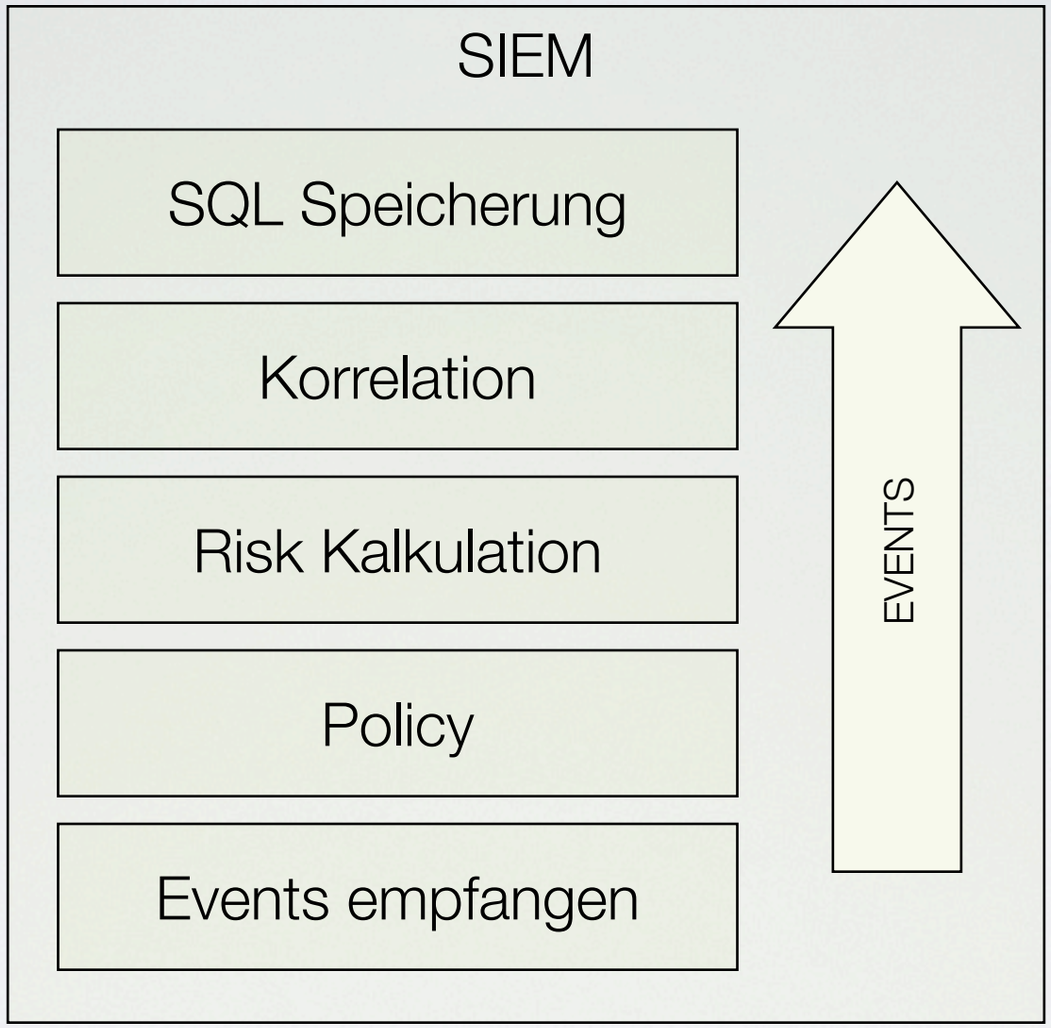
- Jede Capture-Group steht in der Zuordnung von Event-Attributen zur Verfügung
  - Beispiel
    - src_ip={$3}
    - src_ip={$src_ip}
- Erweiterbare Funktionen zur Transformation von Attributen
  - z.B. Namen auflösen
    - dst_ip={resolv($sensor)}
  - Verfügbar
    - translate(), resolv(), normalize_date(), etc.

RESULTAT: OSSIM EVENT

- Standardisiertes Event Format
  - Rot: Pflichtfelder
  - Grün: Pflichtfelder
    - werden mit vernünftigen Standardwerten gefüllt wenn nicht vorhanden
  - Grau: frei verfügbare Felder

plugin_id **Datentyp**	**plugin_sid** **Event innerhalb dieses Datentyps**	**date**	**sensor**	**interface**	**protocol** **TCP**
src_ip **192.168.3.100**	**src_port** **61582**	**dst_ip** **alienvault (192.168.3.222)**	**dst_port** **22**	**username** root	password
filename	userdata1	userdata2	userdata3	userdata4	userdata5
userdata6	userdata7	userdata8	userdata9		

WIE GEHTS WEITER? OSSIM-SERVER



RISIKO KALKULIEREN

- Asset Value (0-5)
  - Drucker: 0
  - Firewall: 4
  - Internes Netz: 2 (default)
  - DMZ: 4

Asset Value Source 2	**Asset Value Dest 3**				
plugin_id Datentyp	**plugin_sid Event innerhalb**	**date**	**sensor**	**interface**	**protocol TCP**
src_ip 192.168.3.100	**src_port 61582**	**dst_ip alienvault**	**dst_port 22**	**username** root	password
filename	userdata1	userdata2	userdata3	userdata4	userdata5
userdata6	userdata7	userdata8	userdata9		

RISIKO KALKULIEREN

- Event Priorität (0-5)
  - 0 - unwichtig
  - 5 - sehr wichtig
- Beispiel
  - Interface up/down auf Switch: 1
  - IDS event für bekannte Lücke: 5

Asset Value Source **2**	**Asset Value Dest** **3**	**Priorität** **2**			
plugin_id **Datentyp**	**plugin_sid** **Event innerhalb**	**date**	**sensor**	**interface**	**protocol** **TCP**
src_ip **192.168.3.100**	**src_port** **61582**	**dst_ip** **alienvault**	**dst_port** **22**	**username** root	password
filename	userdata1	userdata2	userdata3	userdata4	userdata5
userdata6	userdata7	userdata8	userdata9		

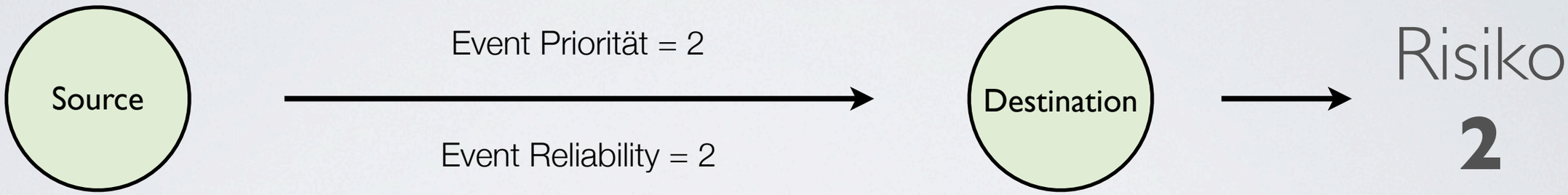
RISIKO KALKULIEREN

- Event Wahrscheinlichkeit (0-10)
  - 0 - sehr wahrscheinlich false-positive
  - 10 - 100% sicherer Event, gefährlich

Asset Value Source **2**	**Asset Value Dest** **3**	**Priorität** **2**	**Reliabilty** **2**	**Risk** **?**	
plugin_id **Datentyp**	**plugin_sid** **Event innerhalb**	**date**	**sensor**	**interface**	**protocol** **TCP**
src_ip **192.168.3.100**	**src_port** **61582**	**dst_ip** **alienvault**	**dst_port** **22**	**username** root	password
filename	userdata1	userdata2	userdata3	userdata4	userdata5
userdata6	userdata7	userdata8	userdata9		

RISIKO KALKULIEREN

- Für jeden eintreffenden Event wird ein Risiko kalkuliert
- Risiko kann zwischen 0 und 10 liegen



Source Asset Value = 2

Destination Asset Value = 3

RISK = (ASSET VALUE * EVENT PRIORITY * EVENT RELIABILITY)/25
RISK = (3 * 2 * 2)/25

Haben die beiden beteiligten Assets verschiedene Werte, wird der höhere verwendet

Asset Value = 0-5
Priority = 0-5
Reliability = 0-10
Event Risk = 0-10

RISIKO KALKULIEREN

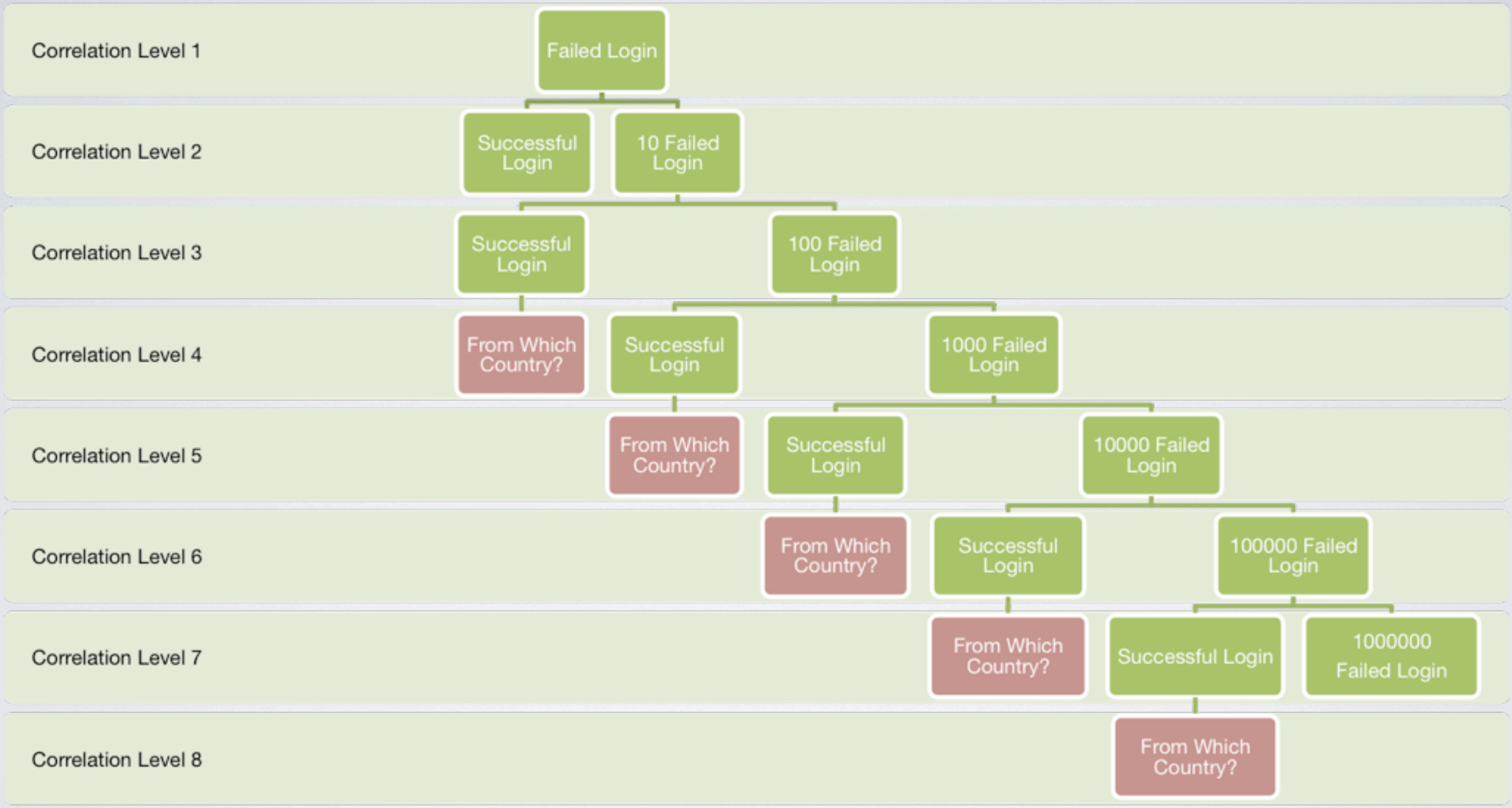
- Event nach der Risikoevaluierung

Asset Value Source **2**	**Asset Value Dest** **3**	**Priorität** **2**	**Reliabilty** **2**	**Risk** **0.48 (=0)**	
plugin_id **Datentyp**	**plugin_sid** **Event innerhalb**	**date**	**sensor**	**interface**	**protocol** **TCP**
src_ip **192.168.3.100**	**src_port** **61582**	**dst_ip** **alienvault**	**dst_port** **22**	**username** root	password
filename	userdata1	userdata2	userdata3	userdata4	userdata5
userdata6	userdata7	userdata8	userdata9		

RISIKO KALKULIEREN

- Event mit Risiko > 1
  - wird per Konvention automatisch zu
    - Alarm
  - optional auch zu einem Ticket

KORRELATION



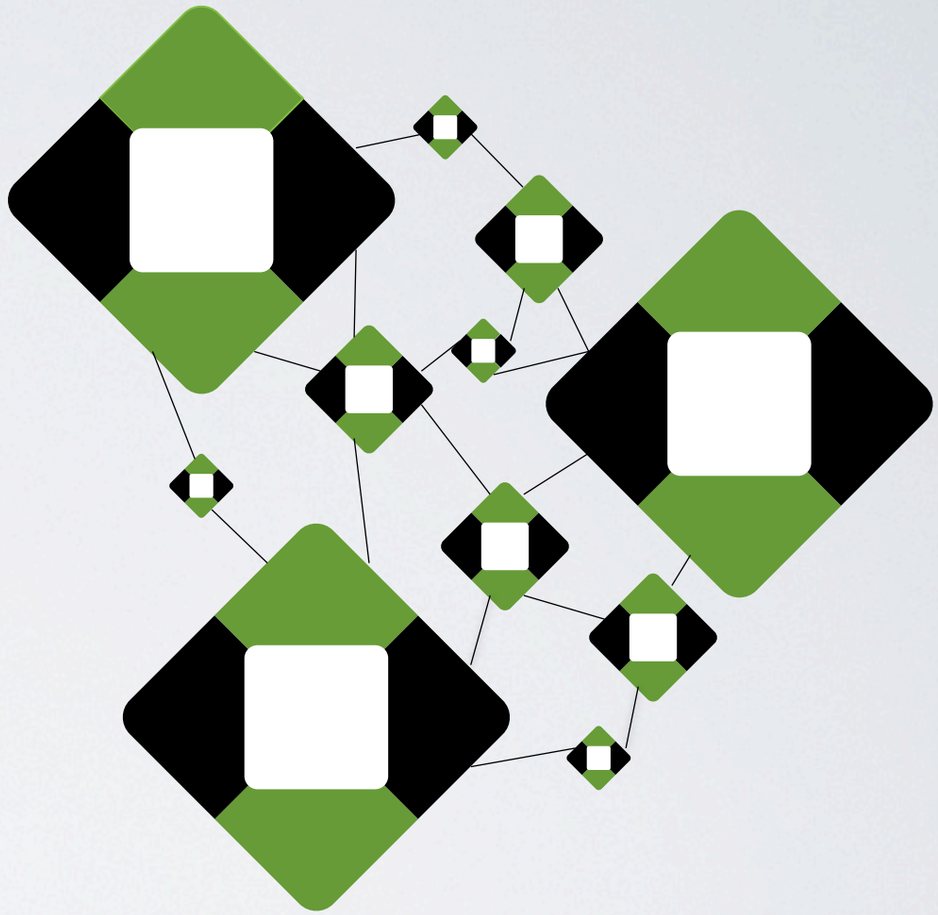
KORRELATION

- Zusätzlich: Cross Correlation
- Event geht ein
  - Ist der Host, der an diesem Event beteiligt ist gegen den eingehenden Event verwundbar?
    - Ja? Reliabilty erhöhen, Priorität erhöhen
    - Nein? Keine Aktion

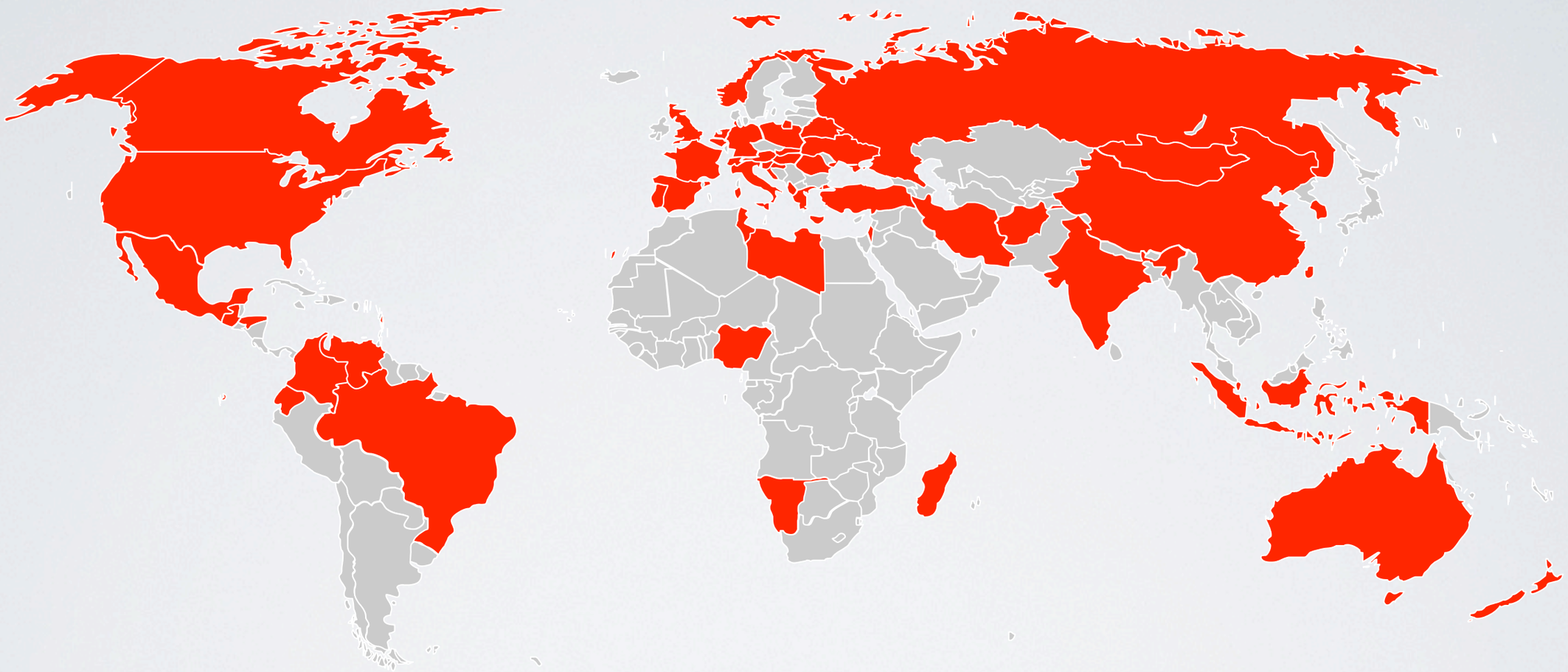
OPEN THREAT EXCHANGE

OPEN THREATEXCHANGE

- Offene Plattform zur Kollaboration
- Opt-In für jede Installation



OTX TEILNEHMER



WIE FUNKTIONIERT

- Attacke wird irgendwo auf der Welt gesehen
- Anonymisierte Informationen werden an OTX gesendet
- Analyse
  - automatisch
  - manuell (ca. 5 Personen)
- Feedback der Informationen in IP-Reputations DB
- Erhältlich über Updates
  - momentan wöchentlich, geplant Realtime

DOWNLOAD & SUPPORT

- Download: http://alienvault.com
- Support: http://forums.alienvault.com
- Source Repo: https://www.assembla.com/spaces/os-sim/

- weiterführende Dokumentation:
  - http://alienvault.bloomfire.com

FRAGEN? ANTWORTEN!