# OSQuery

Eine Sprache alles
zu erfahren.

oder

SQL anstat grep, awk & sed

# Wer bin ich?

Oliver Fischer

Software-Entwickler

E-Post Development GmbH

# Was tue ich?

Meine Tochter dachte lange, dass ich Briefe austrage.

Was tue ich
wirklich?

Mit Leuten reden.

In Meetings sitzen.

Mit Leuten reden.

Bugs analysieren.

Software schreiben.

Welche
IP-Adressen
hat das System?

# „ifconfig" oder „ip"

```
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::5054:ff:fe47:4652  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:47:46:52  txqueuelen 1000  (Ethernet)
        RX packets 123188  bytes 150011831 (143.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22983  bytes 1538218 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.10  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::a00:27ff:fecf:f3d6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cf:f3:d6  txqueuelen 1000  (Ethernet)
        RX packets 13  bytes 3016 (2.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 2790 (2.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

# Und jetzt für Profis

```
$ ifconfig | awk -F "[: ]+" '/inet addr:/ { if ($4 != "127.0.0.1") print $4 }'
10.186.0.229
10.187.1.50
10.178.76.19
```

# Was ist anders?

```
$ ifconfig | awk -F "[: ]+" '/inet addr:/
{ if ($4 != "127.0.0.1") print $4 }'
$
```

macOS

```
$ ifconfig | awk -F "[: ]+" '/inet addr:/
{ if ($4 != "127.0.0.1") print $4 }'
10.186.0.229
10.187.1.50
10.178.76.19
$
```

Linux

Undjctzt elegant

```
$ osqueryi
osquery> select address as ip from interface_addresses;
   ip = 127.0.0.1

   ip = 10.0.2.15

   ip = 192.168.10.10

   ip = ::1

   ip = fe80::5054:ff:fe47:4652

   ip = fe80::a00:27ff:fecf:f3d6
osquery>
```

# Auftritt osquery

- bei facebook entstanden
- geschrieben in C++
- SQL als Abfragesprache
- auf verschiedenen Plattformen verfügbar

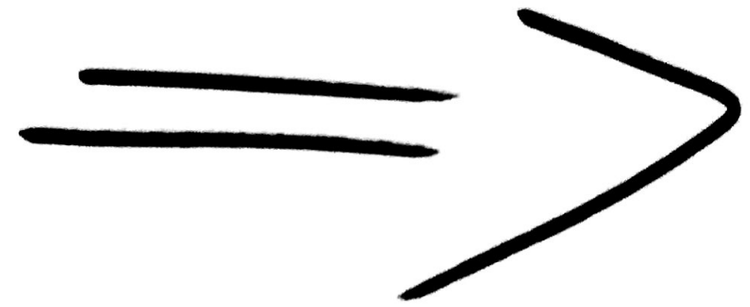
S tructured
Q uery
L anguage

```
select ...
from   ...
where  ...
order by ...
```

# Vorteile?

- Weit verbreitet
- ein Standard (mit Erweiterungen)
- viele Beispiele
- relationale Algebra um Informationen zu verknüpfen

# Beispiele ...



# Welche IPs gibt es?

```
$ osqueryi
osquery> select interface as inf, address as addr, mask from
interface_addresses;
+------+---------------------------+-----------------------------------------+
| inf  | addr                      | mask                                    |
+------+---------------------------+-----------------------------------------+
| lo   | 127.0.0.1                 | 255.0.0.0                               |
| eth0 | 10.0.2.15                 | 255.255.255.0                           |
| eth1 | 192.168.10.10             | 255.255.255.0                           |
| lo   | ::1                       | ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff |
| eth0 | fe80::5054:ff:fe47:4652   | ffff:ffff:ffff:ffff::                   |
| eth1 | fe80::a00:27ff:fecf:f3d6  | ffff:ffff:ffff:ffff::                   |
+------+---------------------------+-----------------------------------------+
osquery>
```

# Welche Benutzer sind in Gruppe root?

```
osquery> select  *
    ...> from    users u
    ...> where   u.gid = 0;
+-----+-----+------------+------------+----------+-------------+-----------+---
| uid | gid | uid_signed | gid_signed | username | description | directory | sh
+-----+-----+------------+------------+----------+-------------+-----------+---
| 0   | 0   | 0          | 0          | root     | root        | /root     | /b
| 5   | 0   | 5          | 0          | sync     | sync        | /sbin     | /b
| 6   | 0   | 6          | 0          | shutdown | shutdown    | /sbin     | /s
| 7   | 0   | 7          | 0          | halt     | halt        | /sbin     | /s
| 11  | 0   | 11         | 0          | operator | operator    | /root     | /s
+-----+-----+------------+------------+----------+-------------+-----------+---
osquery>
```

# Wie viele Daten gingen über den Draht?

```
osquery> select  d.interface, d.ipackets, d.opackets,
    ...>         d.ibytes/1024 as 'kB in', d.ibytes/1024/1024 as 'MB in',
    ...>         d.obytes/1024 as 'kB out', d.obytes/1024/1024 as 'MB out'
    ...> from    interface_details d
    ...> where   d.interface not in ('lo');
+-----------+----------+----------+--------+-------+--------+--------+
| interface | ipackets | opackets | kB in  | MB in | kB out | MB out |
+-----------+----------+----------+--------+-------+--------+--------+
| eth0      | 123969   | 23428    | 146554 | 143   | 1543   | 1      |
| eth1      | 71       | 23       | 16     | 0     | 2      | 0      |
+-----------+----------+----------+--------+-------+--------+--------+
osquery>
```

# Welche Daten, äh Tabellen gibt es?

- ports
- processes
- yara related
- docker related
- ...
- ...
- osqueryi> .tables

# Einsatzgebiete...

- Monitoring
- Security
- Diagnose

Was wurde
ausgelassen?

-Daemon-Modus