FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IT-Forensik eines Edge Systems

Vinh Tran

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Agenda

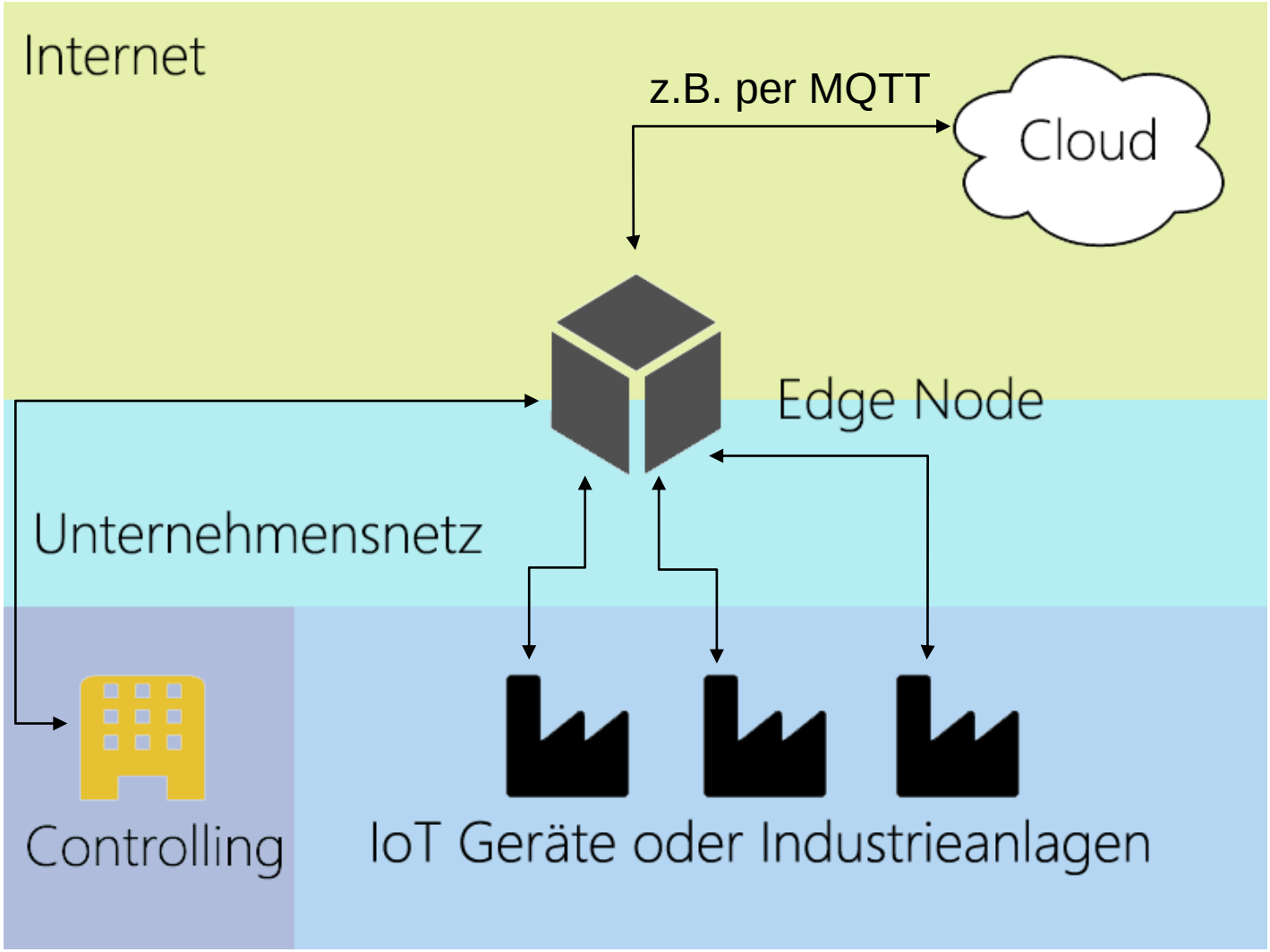
- Vorstellung ProCom GmbH
- Edge Computing?
  - ClouverEdge
- Edge Computing und IT-Forensik?
- IT-Forensik und ClouverEdge
- Ausblick
- Fazit

Vorstellung ProCom GmbH

ProCom

- Business Units
  - Automation
  - Energy Production Planning
- ca. 120 Mitarbeiter
- Standorte
  - Aachen
  - Köln
  - Berlin

Was ist Edge Computing?

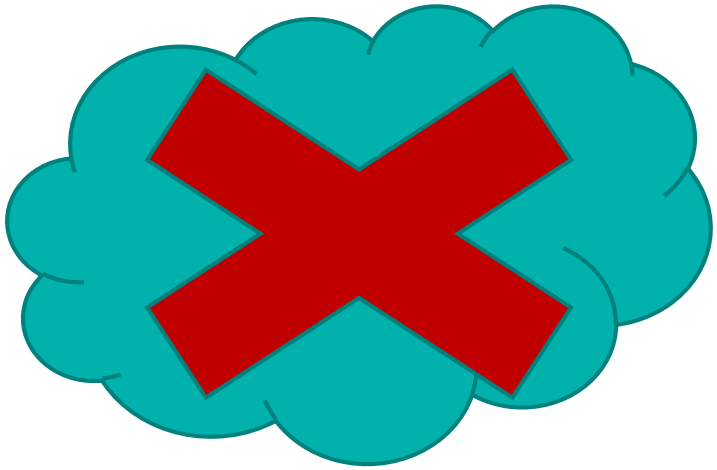


Was bietet Edge Computing?

- Fast Echtzeit Verarbeitung von Daten
- Filterung von Daten
- Validierung von Daten
- Weiterleitung von Daten
- Datenspeicherung
- Verbinden von ERP/CRM Systemen mit Maschinendaten

Was bietet Edge Computing?

- Ersatz für die Cloud?

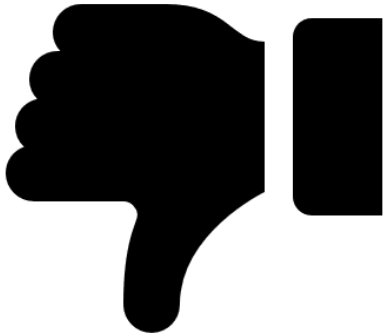


Warum Edge Computing?

- Verbesserung der Verarbeitungszeit
- Geringere Latenz
- Senkung des Traffics ins Internet
- Eigenverwaltung der Daten
- Sensible Informationen im Firmennetz halten
- Unabhängigkeit vom Internet/der Cloud

Edge Computing Nachteile

- Selbstverwaltung der Daten
- Kapazitätsengpässe
- Anfällig für DDoS
- Guter Angriffspunkt



Was ist ClouverEdge?

- Edge Version der Clouver I4.0 Cloud Plattform
- Zielgruppe: Schneidende Industrie
- Funktionen:
  - Filterung
  - Visualisierung von Daten
  - Streaming Analytics von Daten
  - Reporting etc.

Edge Forensik

- Kombination aus:
  - Digitaler Forensik
  - Cloud Forensik
  - IoT Forensik

Herausforderungen

- Dynamisches Joinen und Leaven von Edge Nodes möglich
- Grenzüberschreitende Geräte (z.B. autonome Fahrzeuge)
- Datenaustausch zwischen den Knoten
- Viele flüchtige Daten
- Unübersichtliche und große Datenmengen

Beispiel Edge Forensik ClouverEdge

- Im Kern:
  - CentOS System
  - Java Anwendung
    - Verwendet Apache Karaf
  - Nginx Webserver
  - PostgreSQL und mongoDB

Beispiel Edge Forensik ClouverEdge

- Was sollte auf jeden Fall untersucht werden?
  - Server (z.B. Logs)
  - Datenbanken
  - Webapplikation

Herangehensweise bei ClouverEdge

- Gerätetyp erkennen
  - Server
  - Gateway Device
  - IoT Gerät oder Betrieb auf der Maschine?
- Anzahl der Nodes

Herangehensweise bei ClouverEdge

- SSH vorhanden und aktiviert?
- Imaging z.B. mit „dd“
- Loglösch Script stoppen
  - /etc/cron.daily/delete-logs.sh

Welche Ordner sind relevant?

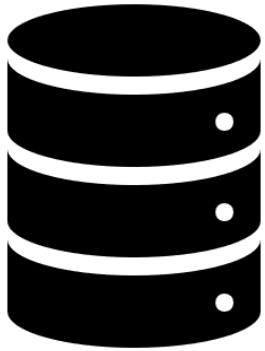
- /etc
  - Enthält Anwendungen bzw. deren Config
    - z.B. /etc/clouver/clouver-core.properties
- /var/log
  - Enthält verschiedene Logdateien
- /home/$USER
  - Benutzerspezifische Daten und Konfigurationen

Logs? Aber welche?

- Audit Trails - /var/log/audit/audit.log
- Secure Log - /var/log/secure
- Benutzerhistory - /home/$USER/.bash_history
- Webanwendunglogs
  - Zugriffslogs - /var/log/clouver/access.log
  - MQTT Logs - /var/log/clouver/mqtt.log
- Messagelog - /var/log/messages

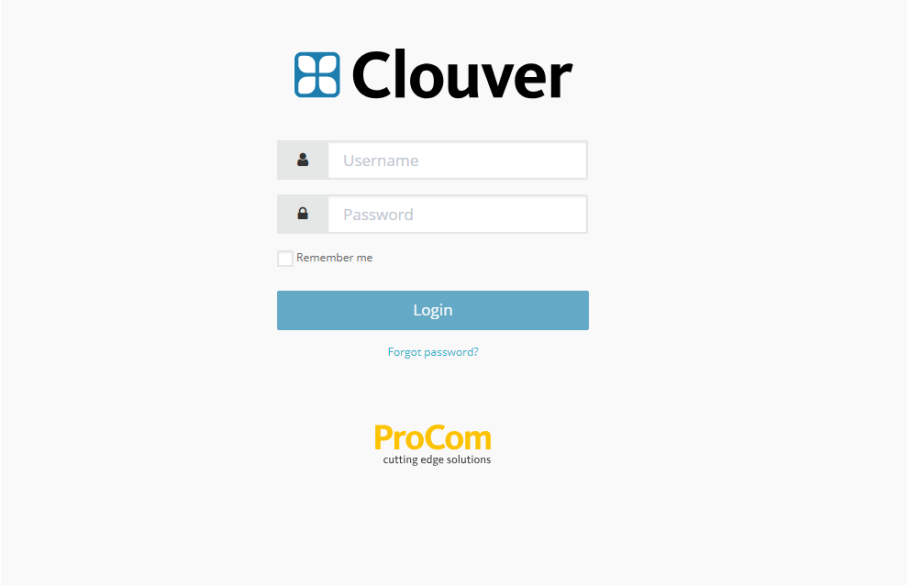
Datenbankuntersuchung

- Hinweise auf Manipulation der Datenbanken?
- Benutzerverwaltung etc. in PostgreSQL Datenbank
- Interessante Tabellen in „clouver“ Datenbank:
  - New_device_request
  - Users
  - Cep_module
- Maschinendaten in MongoDB

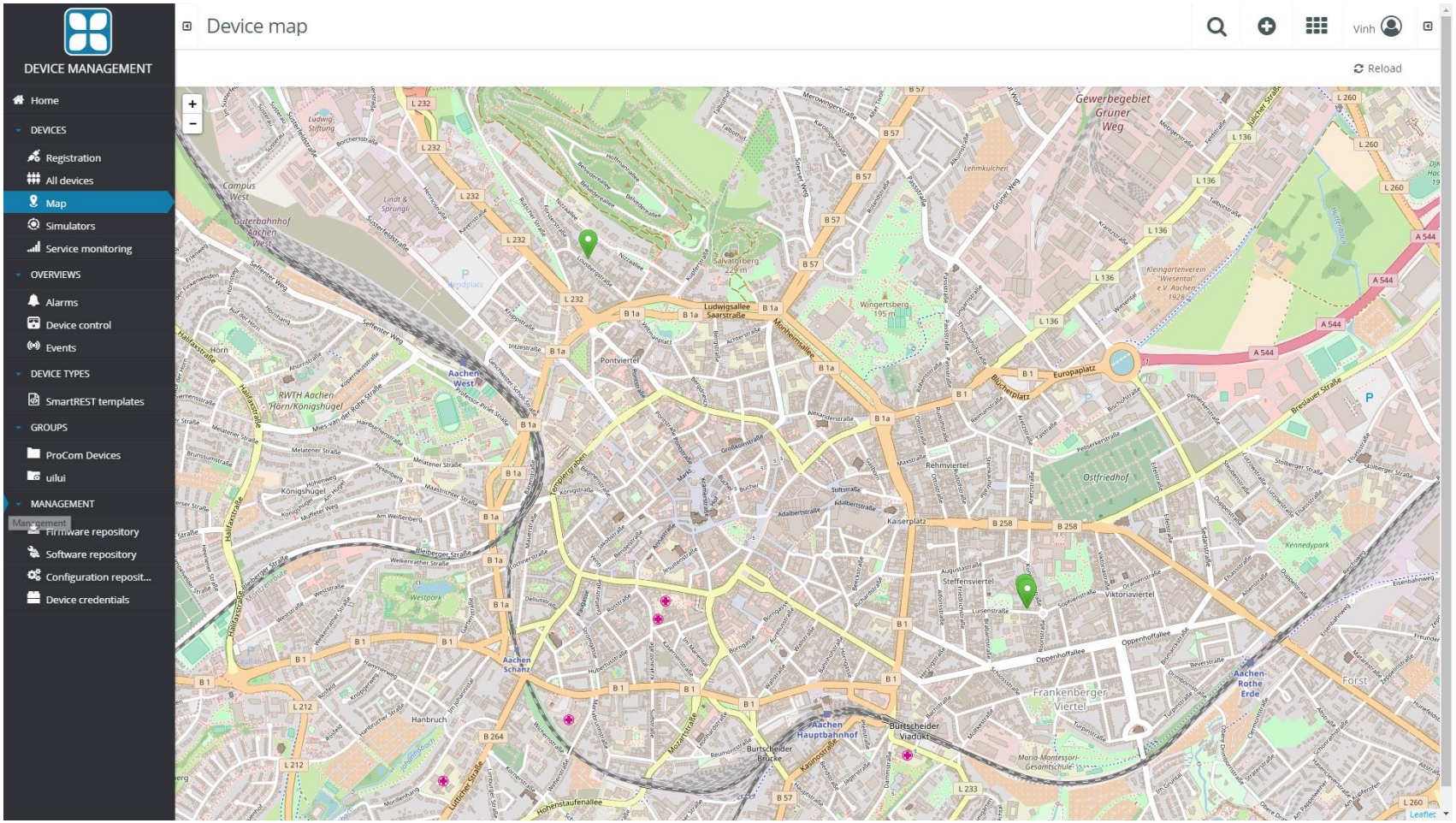


Möglichkeiten der Plattform nutzen

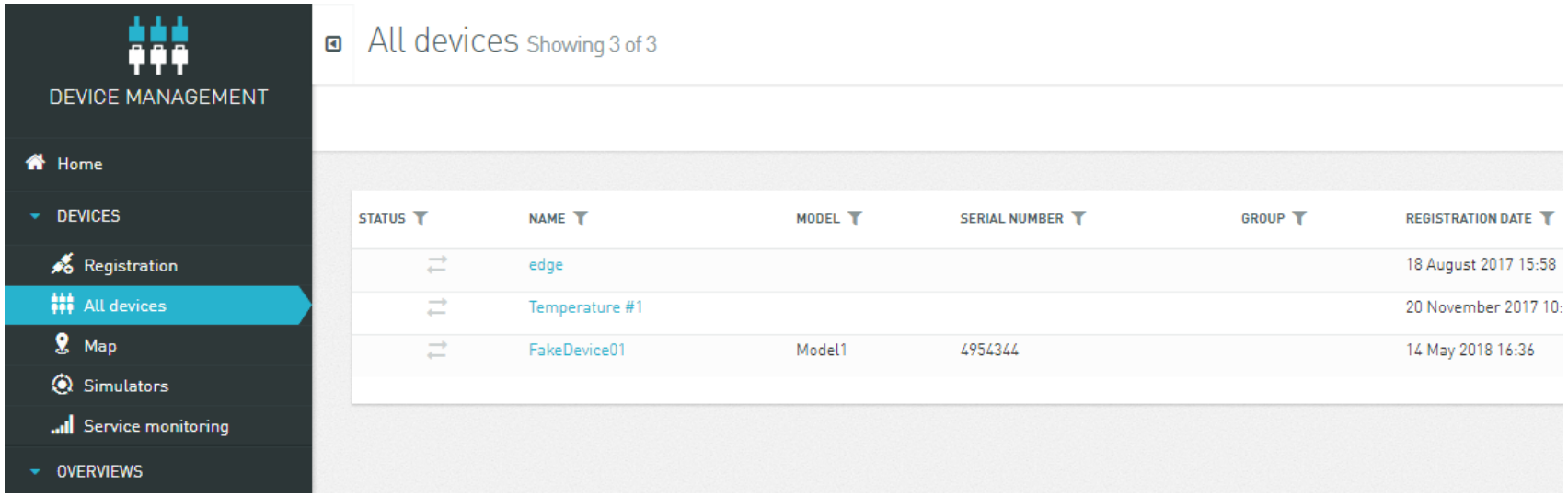
- Visualisierung & Aufbereitung der Daten aus der Datenbank
  - Vereinfachung der Analyse



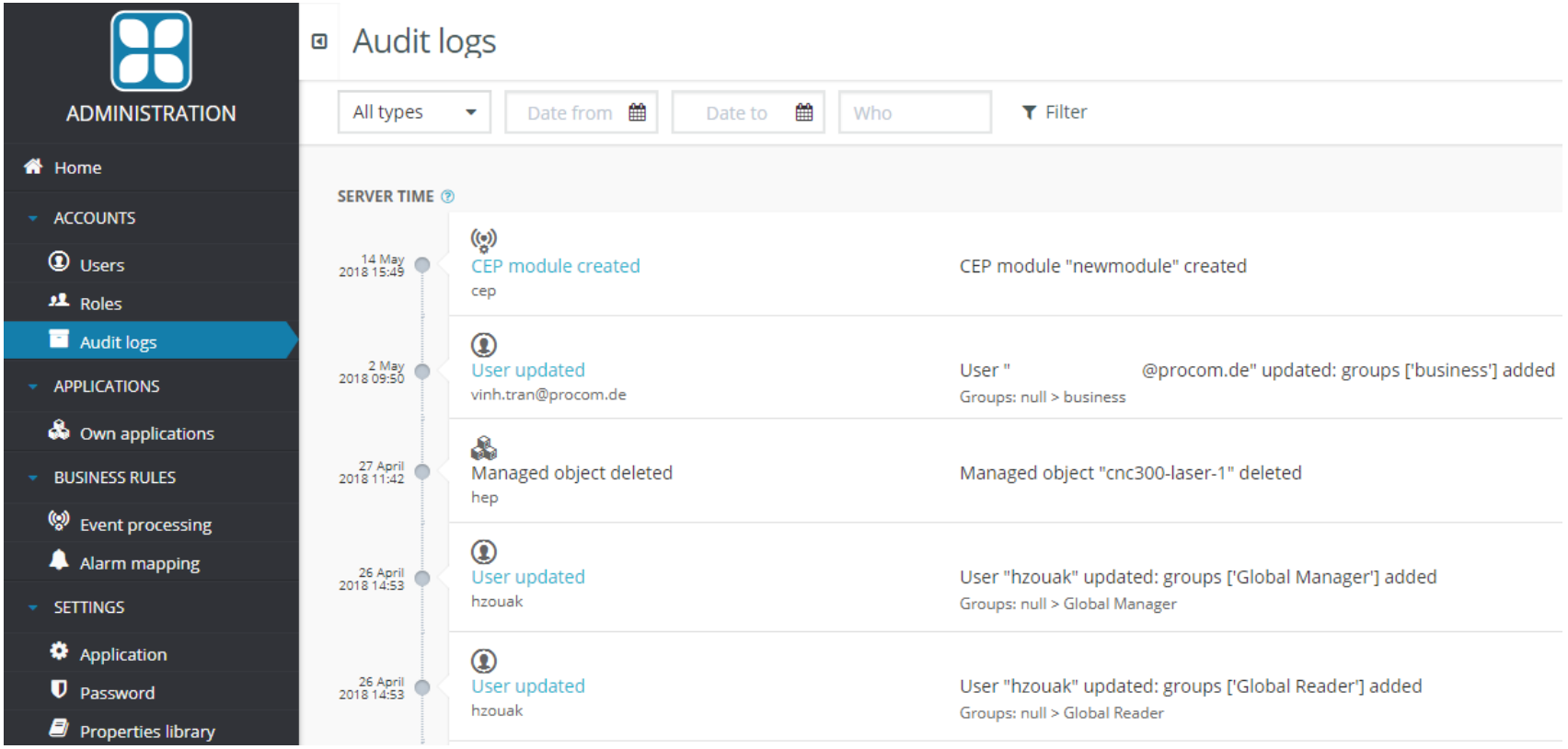
GPS Daten


DEVICE MANAGEMENT
Home
DEVICES
Registration
All devices
Map
Simulators
Service monitoring
OVERVIEWS
Alarms
Device control
Events
DEVICE TYPES
SmartREST templates
GROUPS
ProCom Devices
uilui
MANAGEMENT
Management
Firmware repository
Software repository
Configuration reposit...
Device credentials
Device map
Vinh
Reload
Leaflet

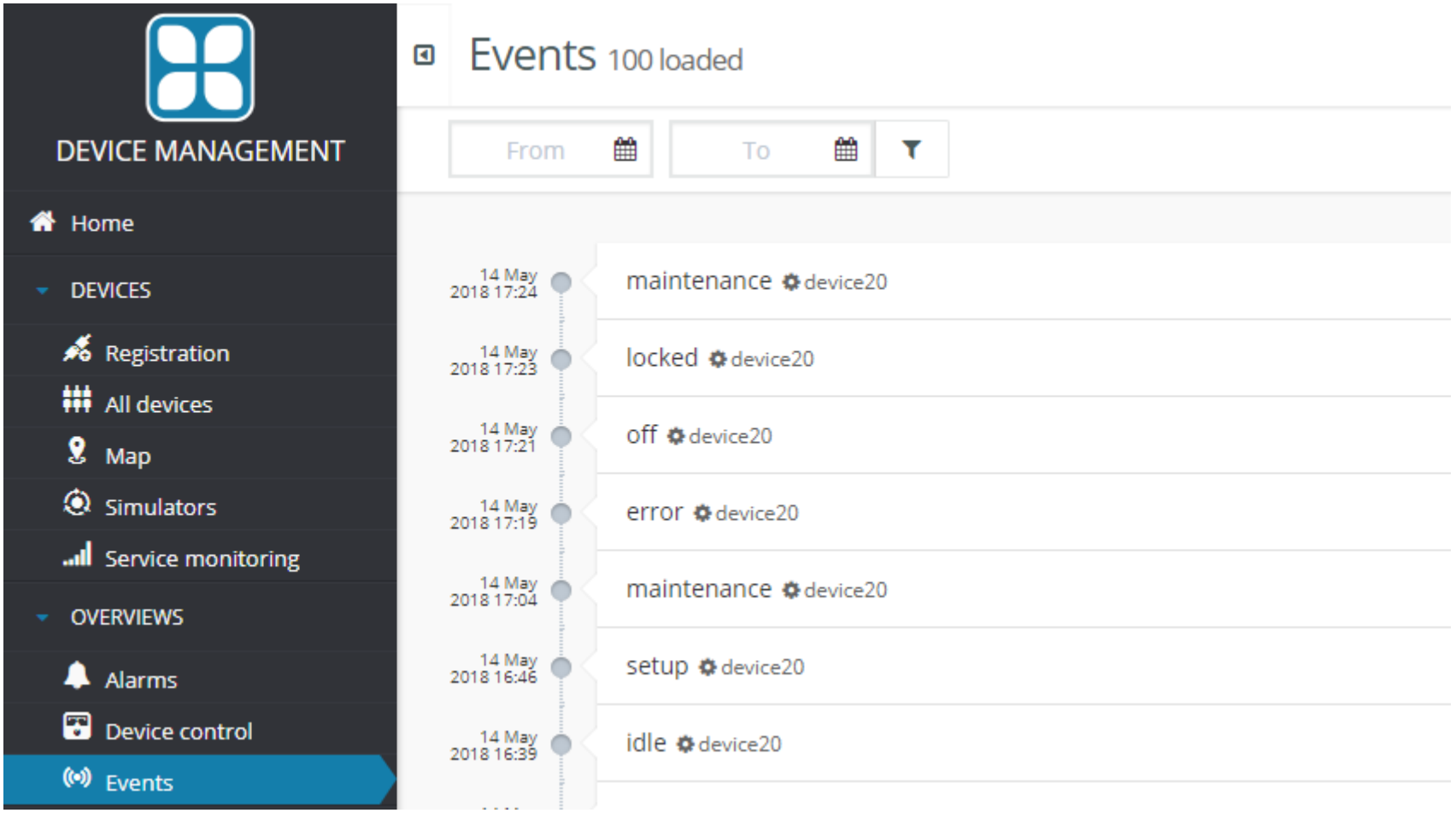
Geräteverwaltung



Audit Trail

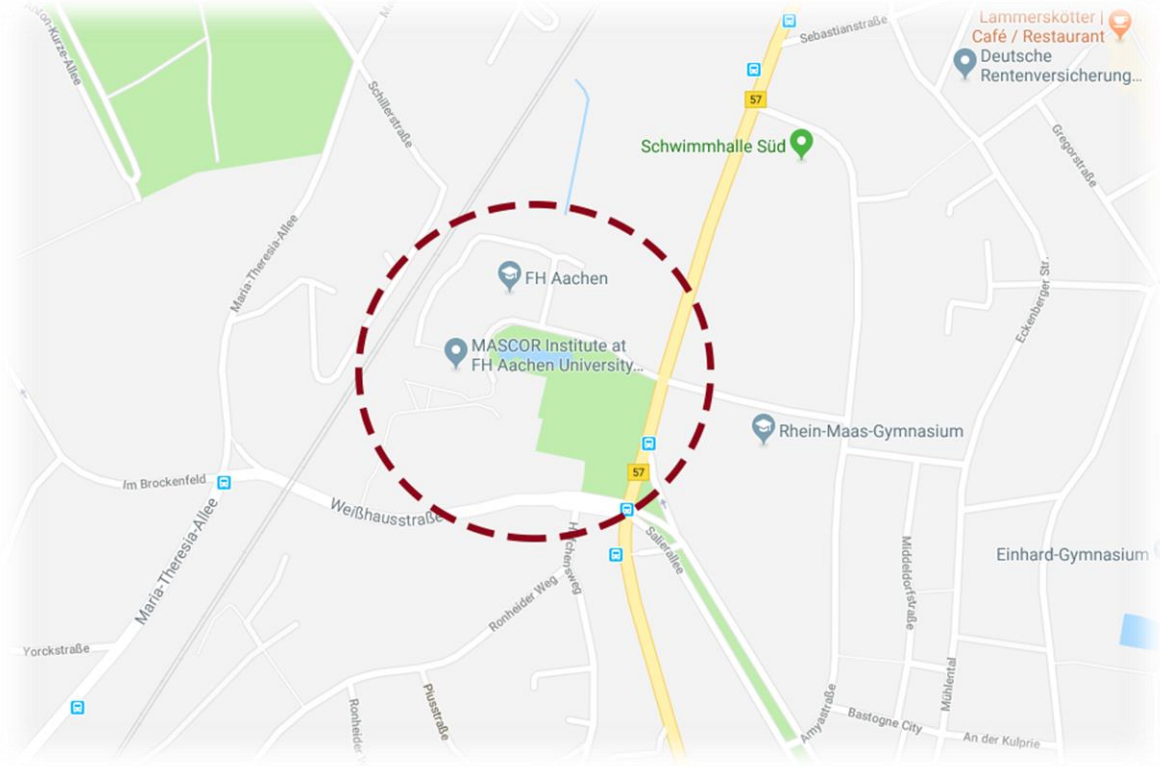

ADMINISTRATION
Home
ACCOUNTS
Users
Roles
Audit logs
APPLICATIONS
Own applications
BUSINESS RULES
Event processing
Alarm mapping
SETTINGS
Application
Password
Properties library
Audit logs
All types
Date from
Date to
Who
Filter
SERVER TIME
14 May 2018 15:49
CEP module created
cep
CEP module "newmodule" created
2 May 2018 09:50
User updated
vinh.tran@procom.de
User " @procom.de" updated: groups ['business'] added
Groups: null > business
27 April 2018 11:42
Managed object deleted
hep
Managed object "cnc300-laser-1" deleted
26 April 2018 14:53
User updated
hzouak
User "hzouak" updated: groups ['Global Manager'] added
Groups: null > Global Manager
26 April 2018 14:53
User updated
hzouak
User "hzouak" updated: groups ['Global Reader'] added
Groups: null > Global Reader

Eventlog


DEVICE MANAGEMENT
Home
DEVICES
Registration
All devices
Map
Simulators
Service monitoring
OVERVIEWS
Alarms
Device control
Events
Events 100 loaded
From
To
14 May 2018 17:24
maintenance device20
14 May 2018 17:23
locked device20
14 May 2018 17:21
off device20
14 May 2018 17:19
error device20
14 May 2018 17:04
maintenance device20
14 May 2018 16:46
setup device20
14 May 2018 16:39
idle device20

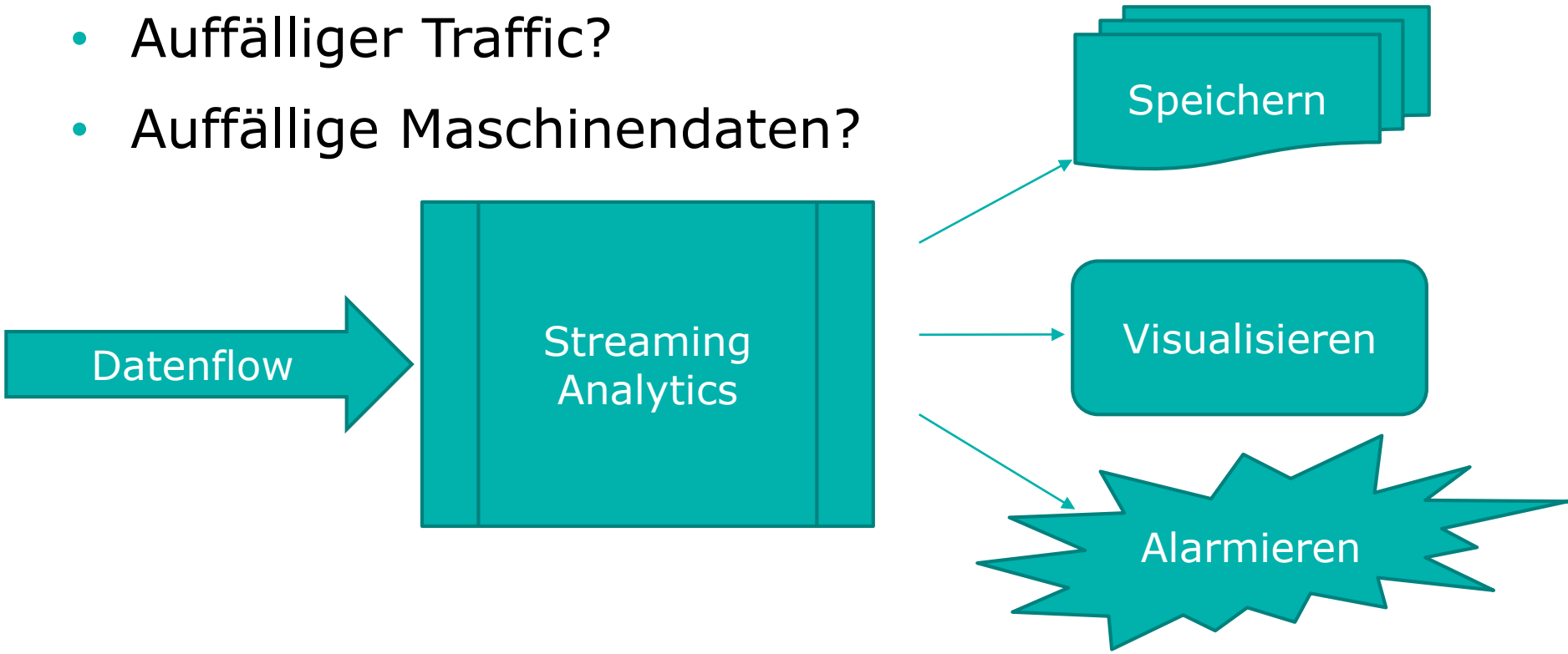
Ausblick – Was geht noch?

- Geofencing
- Streaming Analytics verwenden um alarmiert zu werden



Streaming Analytics

- Live Daten Analyse
- Anomalie Detection
  - Temperaturspikes?
  - Auffälliger Traffic?
  - Auffällige Maschinendaten?



Fazit

- Neue Herausforderung
  - Kombination von Forensik auf verschiedenen Ebenen
  - Große Datenmengen
  - Verteilt auf vielen Knoten
- Aber auch:
  - Neue Möglichkeiten
  - Liefert Hinweise auf Angriffe auf angeschlossenen IoT Geräten

Ende