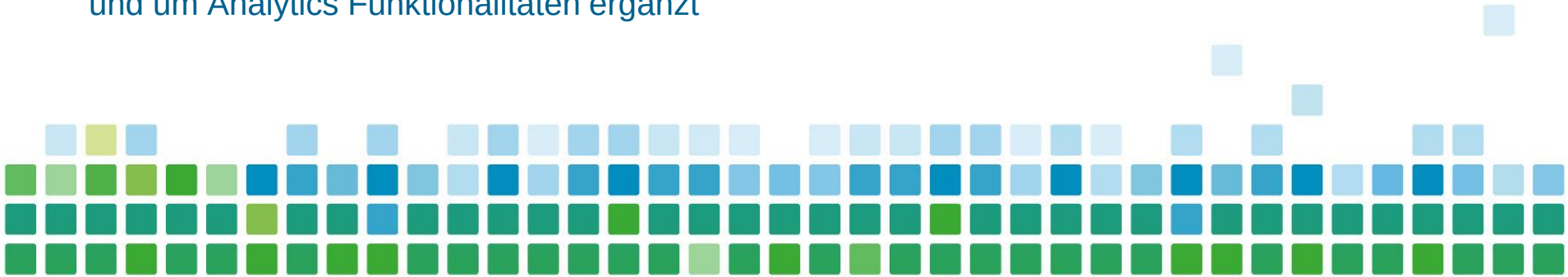
Von Netzwerk-Management zu Netzwerk-Analytics

Wie man mit Splunk die Netzwerkmanagementlösung StableNet integriert

und um Analytics Funktionalitäten ergänzt



Roland Kaiser
Senior Consultant & Teamlead ITM Integration

www.controlware.de

Zürich, 29.10.2019

Agenda Network Analytics

controlware

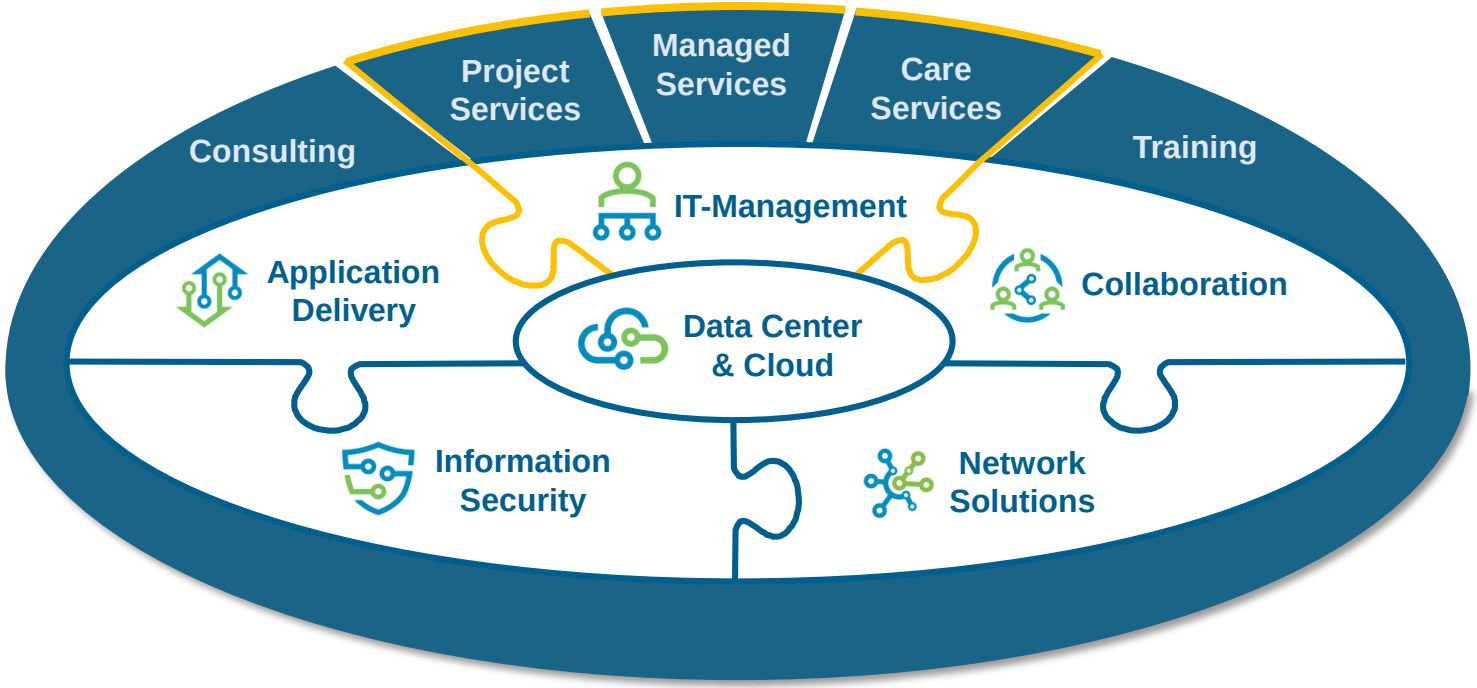
1	Controlware
2	splunk> kurz erklärt
3	Integration StableNet – splunk>
4	Analytics

Marcom V1.0 2018

Controlware GmbH

- **Hersteller unabhängiger Berater, Systemintegrator und Betreiber von IT-Lösungen.**
- **16 Standorte – Deutschland, Österreich und Schweiz**
- **840 Mitarbeiter**
- **Eigenständiges Familienunternehmen**

Controlware GmbH



splunk> kurz erklärt

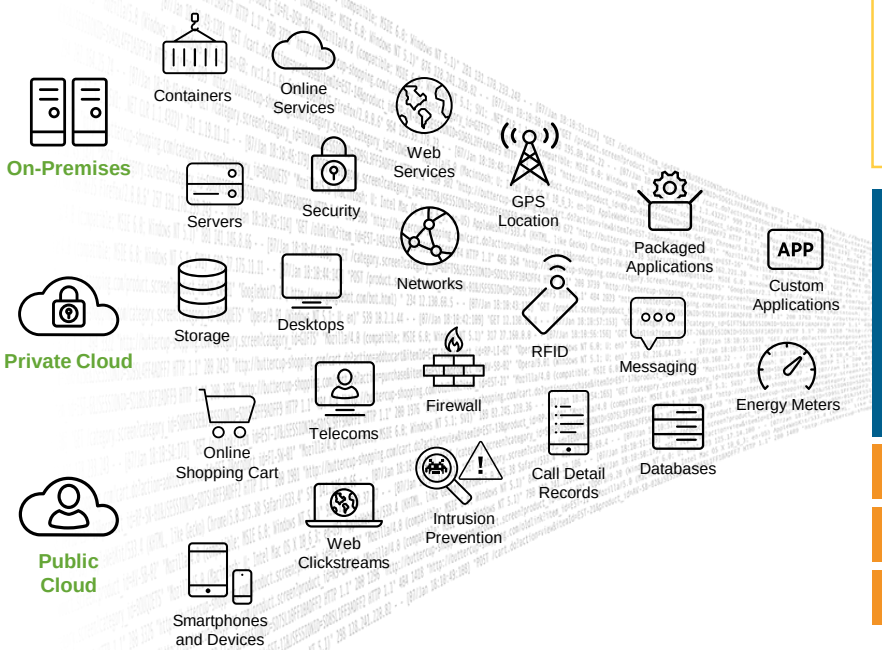
controlware

- Big Data Engine
- Schweizer Taschenmesser für Maschinendaten
- Google für die IT
- Es gibt fast nichts was man nicht abbilden kann – sofern es einen Zeitstempel hat
- Egal welches Format – Hauptsache Text

Industry Leading Platform For Machine Data

controlware

Machine Data: Any Location, Type, Volume



Answer Any Question

Ad hoc search | Monitor and alert | Report and analyze | Custom dashboards | Developer Platform

splunk>enterprise

splunk>cloud

Platform Support (Apps / API / SDKs)

Enterprise Scalability

Universal Indexing

Industry Leading Platform For Machine Data

controlware

Machine Data: Any Location, Type, Volume

On-Premises

Private Cloud

Public Cloud

Smartphones and Devices

Web Clickstreams

Prevention

Answer Any Question

Developer Platform

Enterprise Scalability

Universal Indexing

Any Amount, Any Location, Any Source

Schema on-the-fly	Universal indexing	No back-end RDBMS	No need to filter data

What Does Machine Data Look Like?

Sources

Order Processing

```
ORDER,2014-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100
```

Middleware Error

```
May 21 14:04:12.996  wl-01.acme.com Order 569281734 failed for customer 10098213.
Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:
weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused
```

Care IVR

```
05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type
0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-
13ae51a6d092, Trunk T451.16
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
```

Twitter

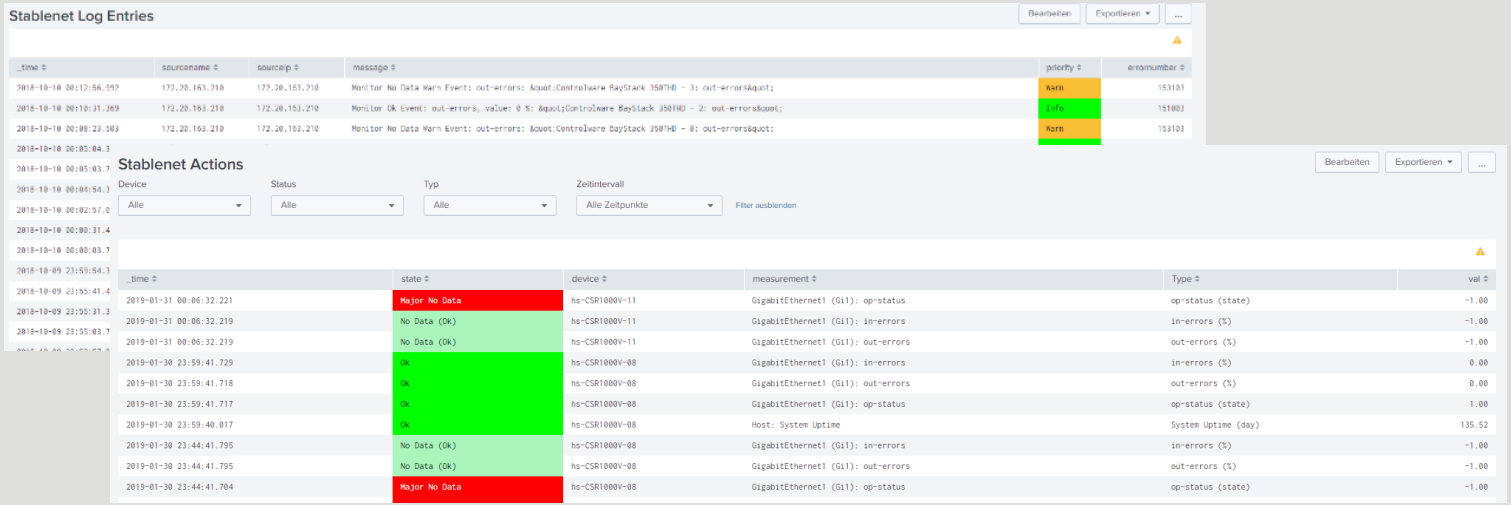
```
{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:
"http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place”},
objectType:"person”,preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Can't buy
this device from @ACME. Site doesn't work! Called, gave up on waiting for them to answer!  RT if
you hate @ACME!!”,objectType:"activity”,postedTime:"2014-05-21T16:39:40.647-0600”}
```

Warum StableNet mit Splunk?

- StableNet liefert das ‚Unified Network & Service Management‘
- Splunk erlaubt es Daten aus **weiteren Datenquellen** zu konsolidieren und zu korrelieren und bringt erweiterte Analysemöglichkeiten
- **Keine Einschränkung** auf klassische Netzwerk Daten! Dies können von Servern, Anwendungen, Security, IoT, …. kommen – eben Maschinen Daten

StableNet Alarme

- Events, Actions und Open Alarms sind über Rest API als XML abfragbar



Stablenet Log Entries

Bearbeiten | Exportieren | ...

_time	sourcename	sourceip	message	priority	errornumber
2018-10-10 00:12:56.992	172.20.163.210	172.20.163.210	Monitor No Data Warn Event: out-errors: "Controlware BayStack 350THD - 3: out-errors"	Warn	153103
2018-10-10 00:10:31.369	172.20.163.210	172.20.163.210	Monitor Ok Event: out-errors, value: 0 %: "Controlware BayStack 350THD - 2: out-errors"	Info	151003
2018-10-10 00:08:23.503	172.20.163.210	172.20.163.210	Monitor No Data Warn Event: out-errors: "Controlware BayStack 350THD - 0: out-errors"	Warn	153103
2018-10-10 00:05:04.3					
2018-10-10 00:05:03.7					
2018-10-10 00:04:54.3					
2018-10-10 00:02:57.0					
2018-10-10 00:00:31.4					
2018-10-10 00:00:03.7					
2018-10-09 23:59:54.3					
2018-10-09 23:55:41.4					
2018-10-09 23:55:31.3					
2018-10-09 23:55:03.7					

Stablenet Actions

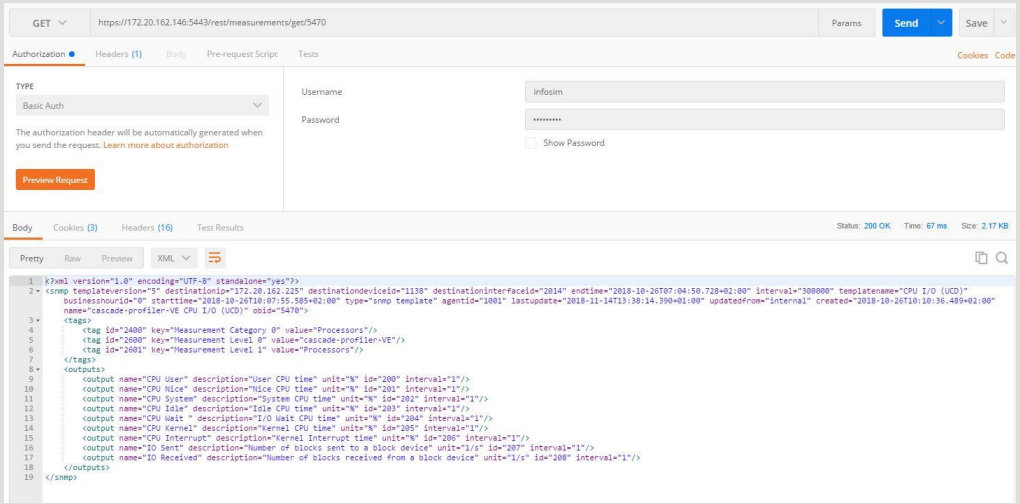
Bearbeiten | Exportieren | ...

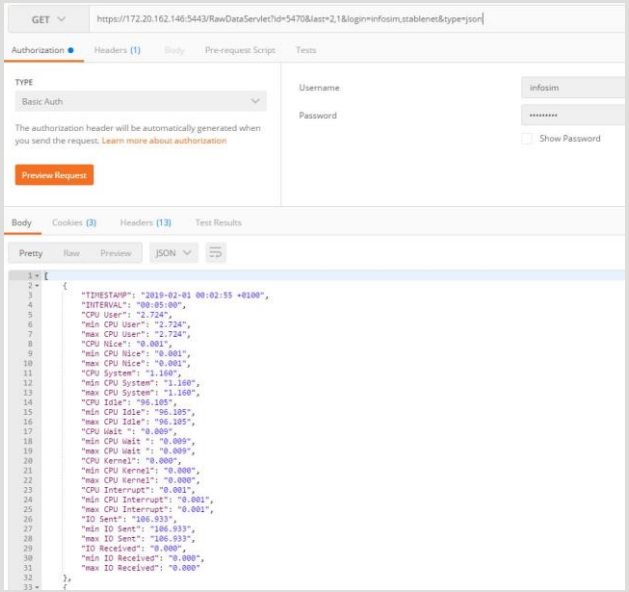
Device: Alle | Status: Alle | Typ: Alle | Zeitintervall: Alle Zeitpunkte | Filter ausblenden

_time	state	device	measurement	Type	val
2019-01-31 00:06:32.221	Major No Data	hs-CSR1000V-11	GigabitEthernet1 (Gi1): op-status	op-status (state)	-1.00
2019-01-31 00:06:32.219	No Data (Ok)	hs-CSR1000V-11	GigabitEthernet1 (Gi1): in-errors	in-errors (%)	-1.00
2019-01-31 00:06:32.219	No Data (Ok)	hs-CSR1000V-11	GigabitEthernet1 (Gi1): out-errors	out-errors (%)	-1.00
2019-01-30 23:59:41.729	Ok	hs-CSR1000V-08	GigabitEthernet1 (Gi1): in-errors	in-errors (%)	0.00
2019-01-30 23:59:41.718	Ok	hs-CSR1000V-08	GigabitEthernet1 (Gi1): out-errors	out-errors (%)	0.00
2019-01-30 23:59:41.717	Ok	hs-CSR1000V-08	GigabitEthernet1 (Gi1): op-status	op-status (state)	1.00
2019-01-30 23:59:40.017	Ok	hs-CSR1000V-08	Host: System Uptime	System Uptime (day)	135.52
2019-01-30 23:44:41.795	No Data (Ok)	hs-CSR1000V-08	GigabitEthernet1 (Gi1): in-errors	in-errors (%)	-1.00
2019-01-30 23:44:41.795	No Data (Ok)	hs-CSR1000V-08	GigabitEthernet1 (Gi1): out-errors	out-errors (%)	-1.00
2019-01-30 23:44:41.704	Major No Data	hs-CSR1000V-08	GigabitEthernet1 (Gi1): op-status	op-status (state)	-1.00

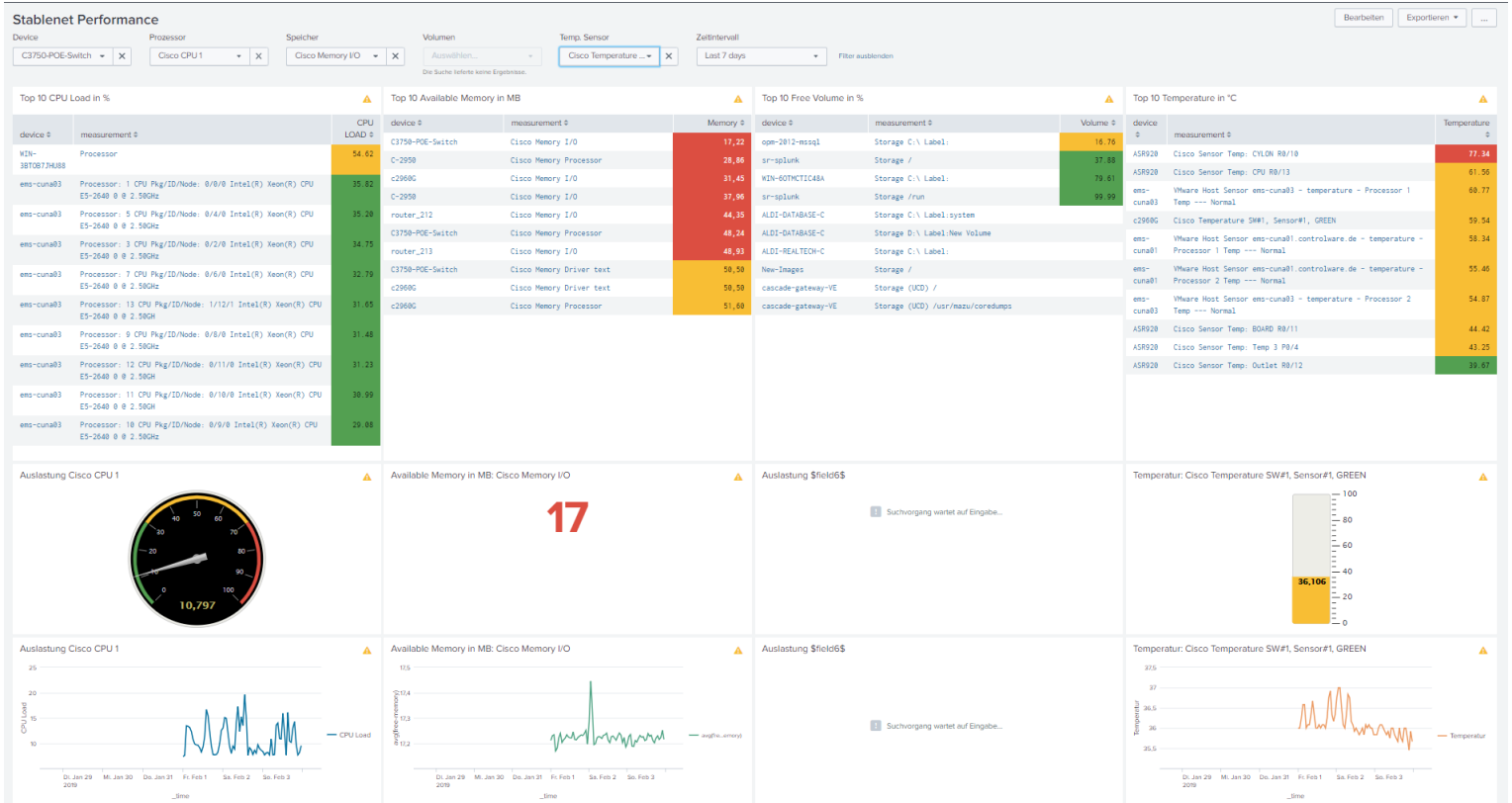
StableNet Performance Daten

- Daten über eingerichtete Performance Messungen über Rest API abfragbar
- Werte der Performance Messungen werden über Servlets abgerufen





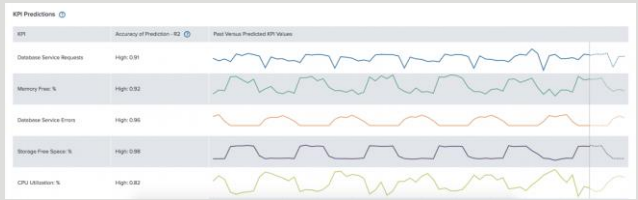
Splunk Performance Dashboard – mit StableNet Daten

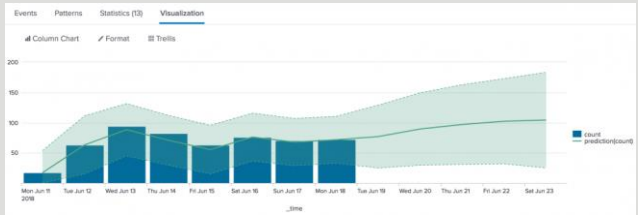


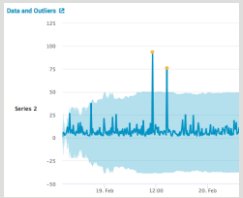
Advanced Analytics

- Data Mining
  - Erkennen von Muster und Beziehungen (e.g. to user behavior)
- Machine Learning
  - Verknüpfung von strukurierten Daten und Maschinen Daten
  - Trends erkennen und Vorhersagen treffen
  - Auswirkungen auf Geschäftsprozesse frühzeitig vermeiden

  → Predictive Maintenance, Failure, ….







controlware

Vielen Dank für Ihre Aufmerksamkeit!
Thank you very much for your attention!

controlware