

Cybersecurity und IOT in Schulen?



Prof. DI Christian Schöndorfer
HTL Wien 3 Rennweg
christian@schoendorfer.cc



Der Fortschritt geschieht heute so schnell, dass, während jemand eine Sache für gänzlich undurchführbar erklärt, er von einem anderen unterbrochen wird, der sie schon realisiert hat.“

[Albert Einstein](#) († [18. April 1955](#))

DIGITALISIERUNG

2010



12.5 bn

2015



25 bn

2020



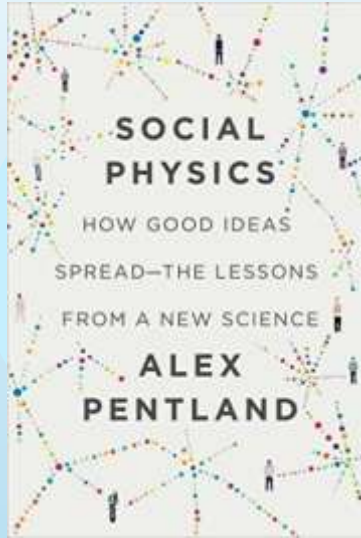
50 bn





Software + Hardware + Daten + Ecosystem

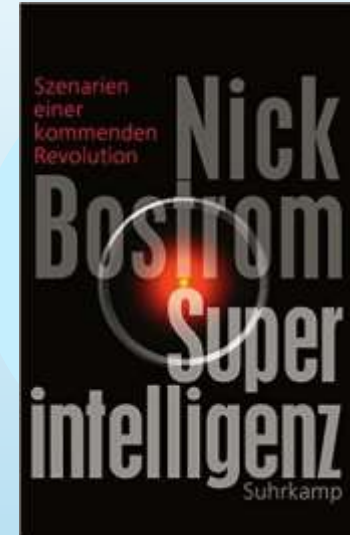
TRENDS



BigData

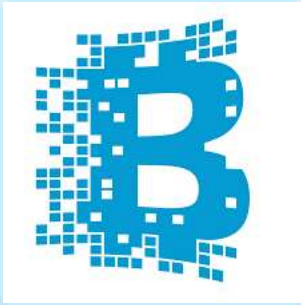


Automation



Artificial Intelligence

TECHNOLOGIE



STOP: Wir sprechen doch über Schule?

BlockChaining

Software Defined Network
Compute / Storage

Fog Computing



WOULD YOU FLY IN A PLANE
MADE OUT OF 50 PLANES?
*There's never been a better time
for security that works together.*

Von der Vision zur Projektidee

- Fakten:
 - 80 k SchülerInnen als „Zielgruppe“ im Fokus
 - Davon ca. 70% mit (zumindest teilweise) Internetzugang
 - ca 35 Wochenstunden „Zeit“ vor Ort
 - Am Schulstandort
 - 1200 SchülerInnen
 - Etwa 3.800 Mobile Geräte pro Sekunde im WLAN
 - 2 GB Internetanbindung zum Desktop
 - Internetauslastung...

Von der Vision zur Projektidee

- Problemfelder
 - Datenschutz
 - Privatsphäre versus Bildungsauftrag
 - Strafrechtsrelevante Delikte!
 - Wie soll ein Internetzugang „gestaltet“ werden?
 - Das Prinzip des Verbotens - und die Sache mit dem Aufwand!
 - Keine zentralen Vorgaben / Richtlinien?
 - Fachwissen?
 - Motivation der MitarbeiterInnen?

Von der Vision zur Projektidee

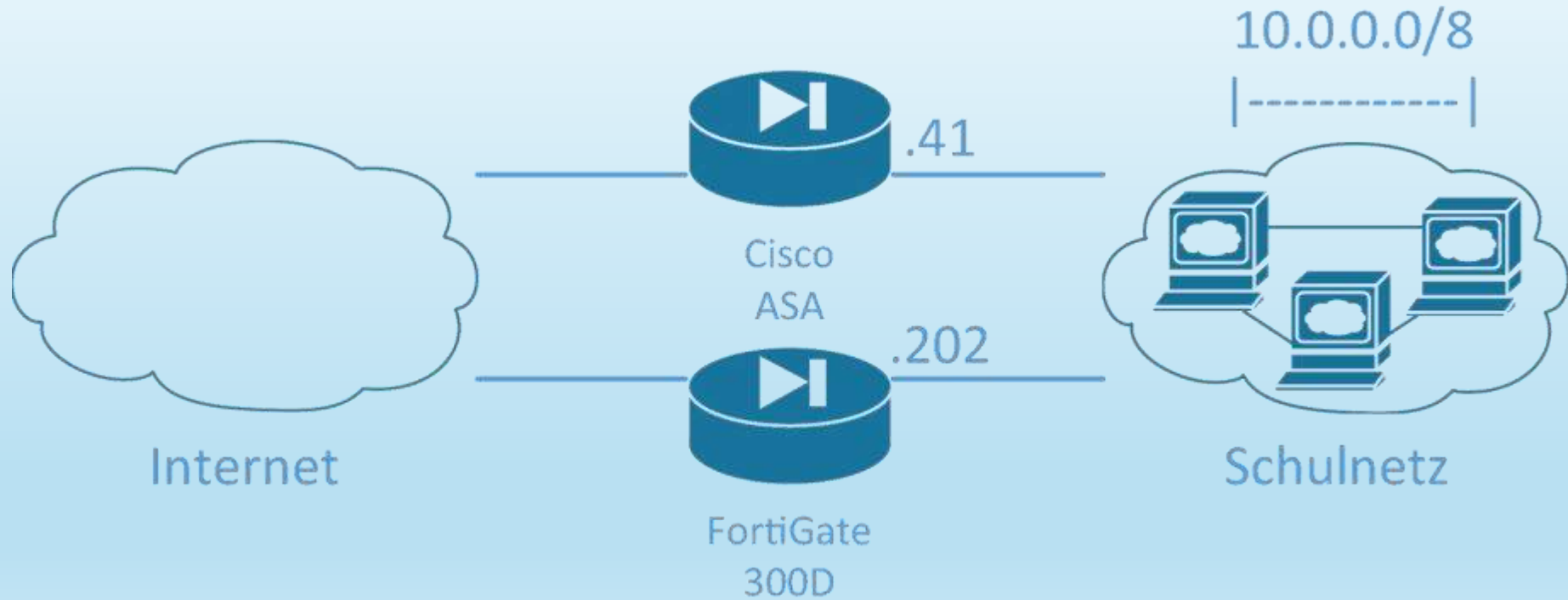
- Conclusio:
 - Wir benötigen Fakten und Zahlen!
 - Woher sollen die Daten kommen?
 - Ach ja: und der Datenschutz!
 - Mitarbeit von SchülerInnen!
 - Erster Ansatz: Syslog

Die Projektidee :: Schritt 1

- Zentrale Auswertung von Syslogging
 - Dazu einmal Syslog „aktivieren“
 - Aber welcher Level / Intensität?
 - Auf welchen Geräten sollen Syslog betrieben werden?

- Ergebnis: Daten, Daten, Daten,...
- Welche Hardware schafft das?
- Datenschutz – Auftrag zur Datenverwaltung!?

Erster Ansatz



Von Logfiles zur Auswertung



Von Logfiles zur Auswertung

- Welche Geräte „verursachen“ Traffic:
 - Cisco ASA
 - Serverlandschaft
 - Logumfang: 1.111.317 Zeilen; 659.163.564 Bytes (Stand: 09.01.2017)
 - FortiGate 300D
 - WLAN, Serverraum 078, verkabelte Klassen
 - Logumfang: 3.313.207 Zeilen; 1.926.514.346 Bytes (Stand: 09.01.2017)
 - 3 x Catalyst 4600
 - Schulnetz-Core
 - Logumfang: 37.317.209 Zeilen; 17.246.324.322 Bytes (Stand: 10.01.2017)

Von Logfiles zur Auswertung

1

Beispiel-Logentry: *date=2017-01-13 time=10:43:14
srcip=10.14.81.11 srcport=53404 dstip=65.52.108.136
dstport=443 ...*

2

date	time	srcip	srcport	dstip	dstport
13.01.2017	10:43.14	10.14.81.11	53404	65.52.108.136	443

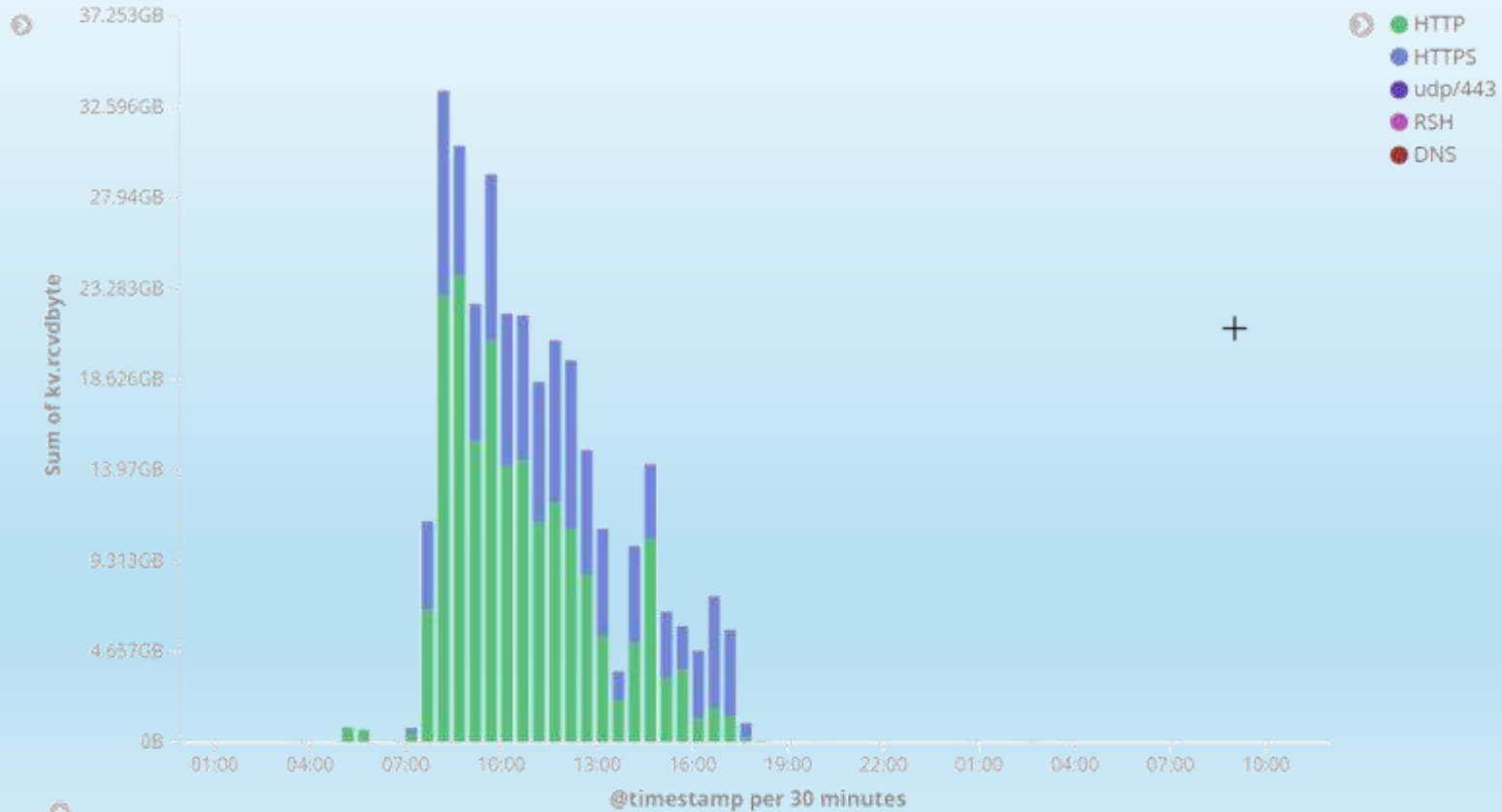
3

date	time	srcip	srcport	dstip	dstport
13.01.2017	10:43.14	WLAN Schulnetz	53404	United States	HTTPS

4

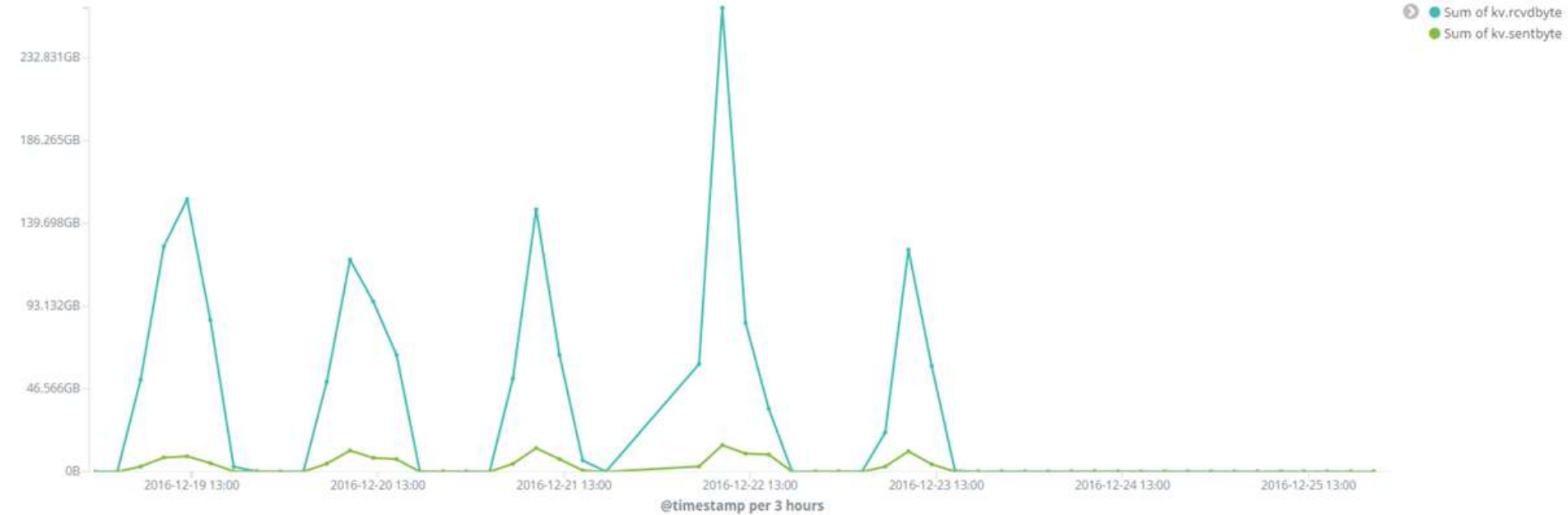
An die Datenbank senden

Ein erstes Ergebnis?



Ein erstes Ergebnis

FortiGate: Network utilization



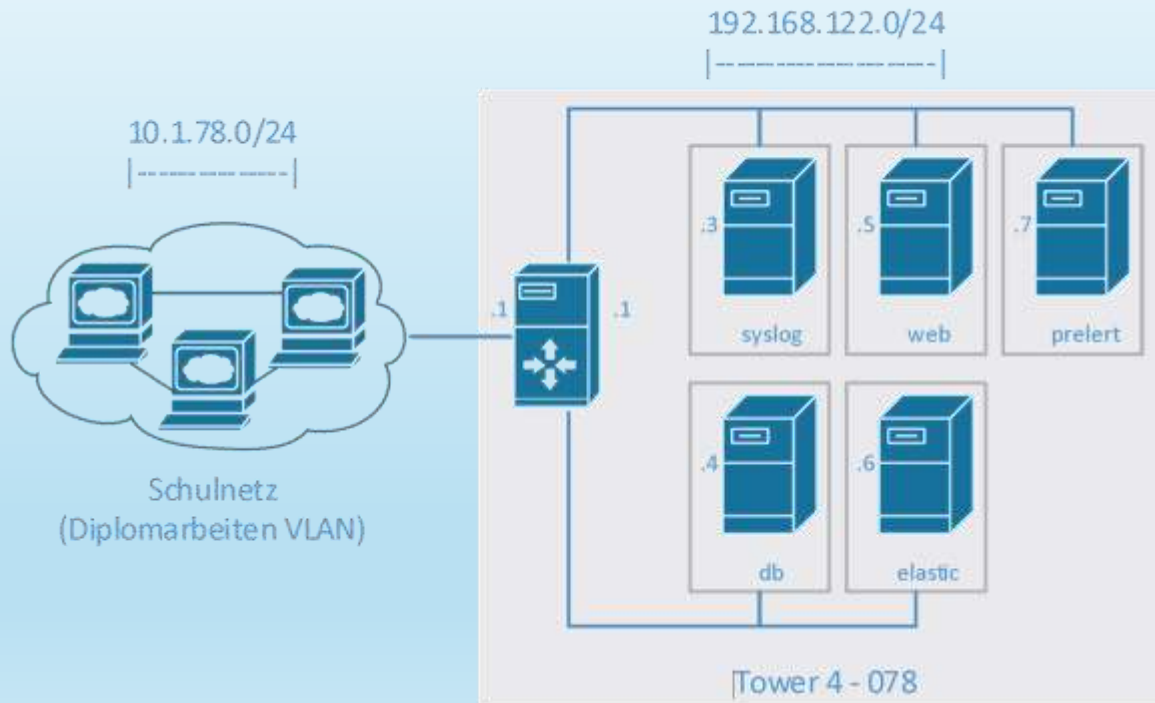
Ein erstes Ergebnis

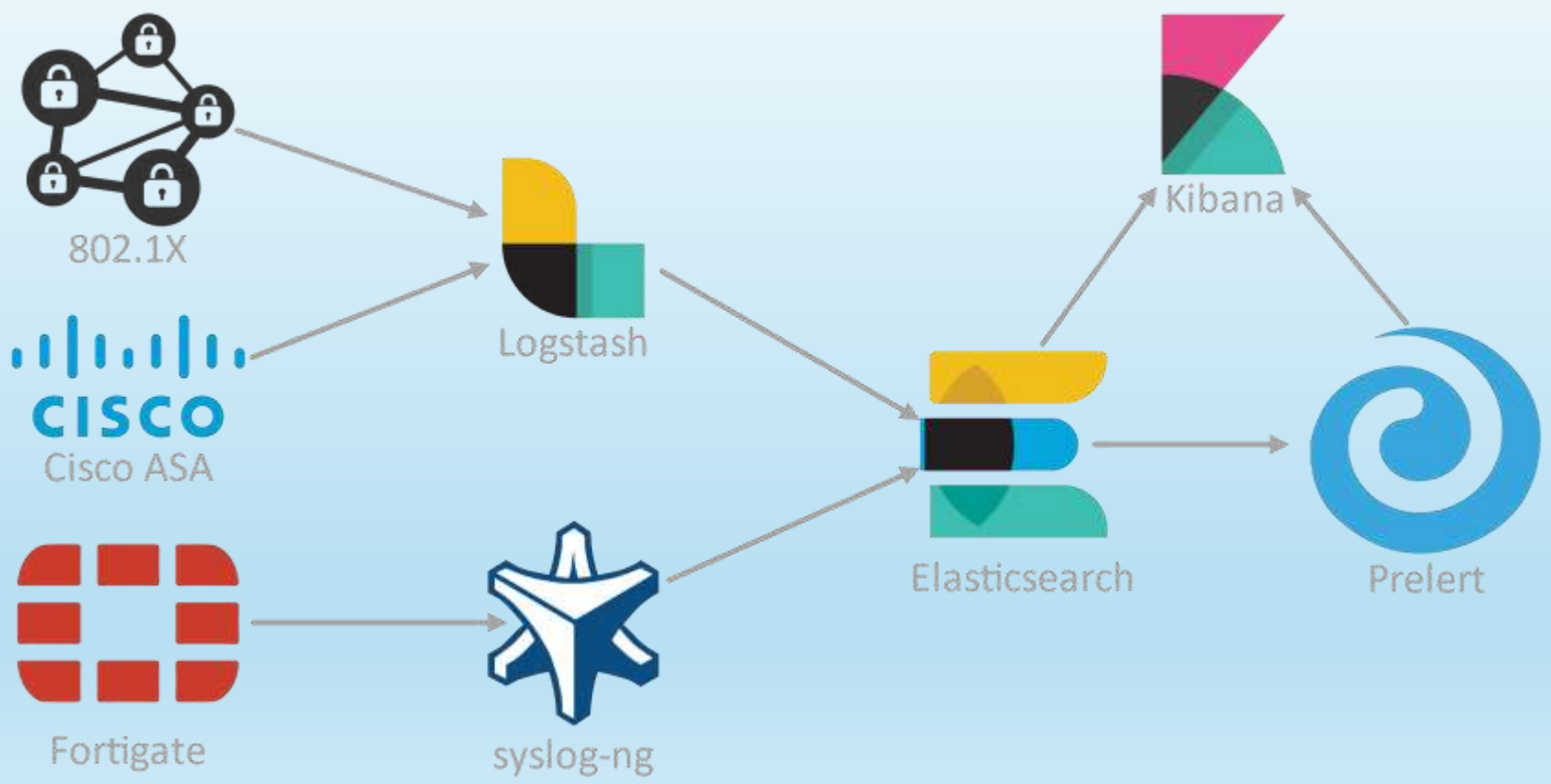
kv.srcip: Descending ↕ Q	Sum of kv.rcvdbyte ↕	Sum of kv.sentbyte ↕
10.14.75.189	48.315GB	890.355MB
10.2.45.30	26.802GB	489.322MB
10.14.79.185	24.569GB	293.154MB
10.0.0.114	24.09GB	1.397GB
10.14.78.229	22.071GB	419.981MB
10.2.45.28	16.889GB	318.188MB
10.14.82.208	15.785GB	303.934MB
10.2.61.59	14.892GB	57.95MB
10.14.76.31	11.962GB	240.256MB
10.14.80.182	11.764GB	252.867MB

Die Projektidee :: Schritt 1

- Typische Fragestellungen
 - Surferguy des Tages?
 - Top IP-Adressen
 - Top Google-Suchwörter?
 - Anzahl von gleichzeitigen Sessions
 - „Lasterverteilung“ WLAN – „Festnetz“
 - Social Media Traffic

Send in more servers...





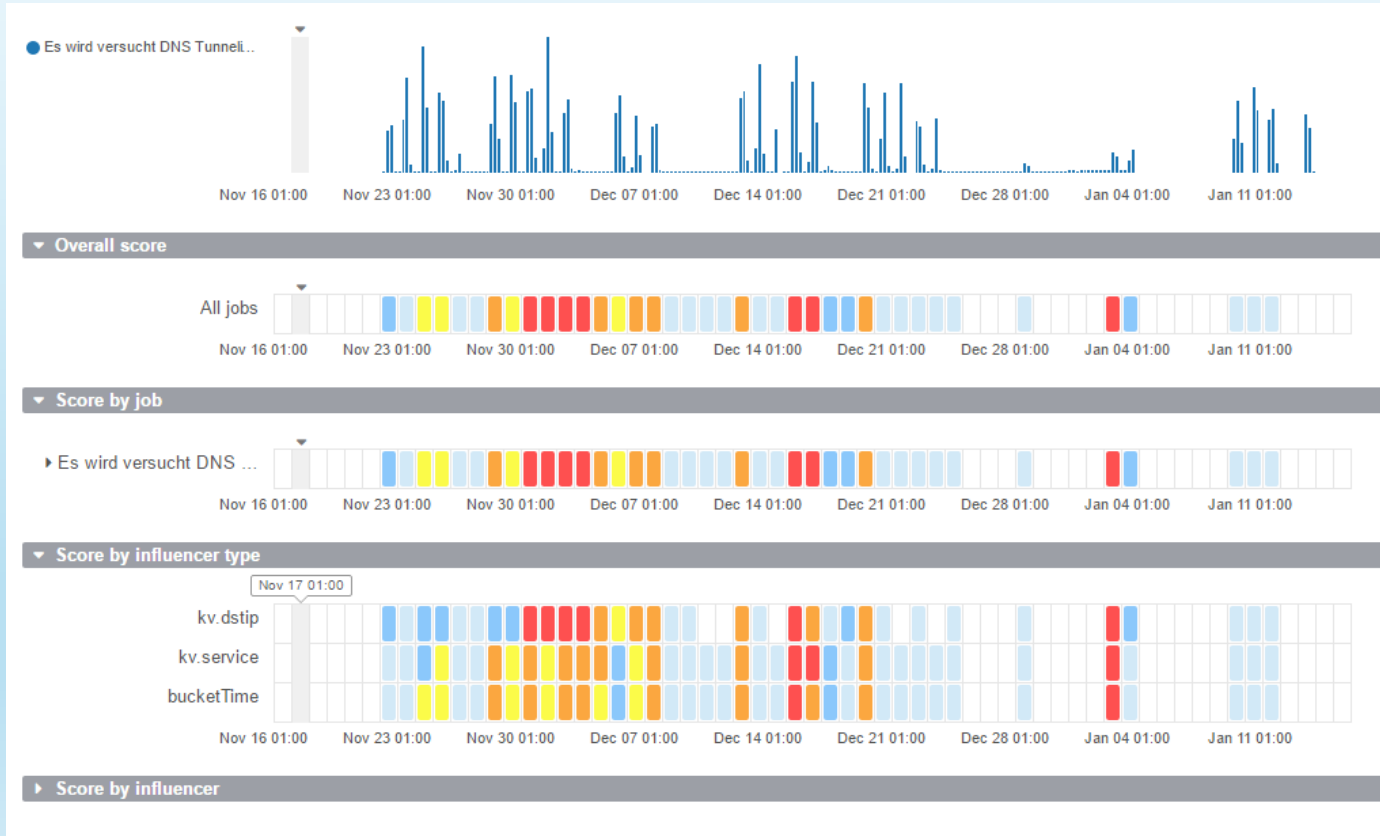
Die Projektidee :: Schritt 2

- Suchen wir Signaturen
 - Die Nadel im Heuhaufen!
 - Noch mehr syslogging

Die Projektidee :: Schritt 2

- Typische Fragestellungen
 - DNS Tunneling
 - Browsergames
 - Verschlüsselter Traffic?
 - Torrents?

Deep Learning



Ausblick

- Erweiterung auf weitere Standorte
- Suche nach leistungsfähiger Serverinfrastruktur
- Partnerschaft mit Herstellern
 - Know How Transfer
- IOT Security
 - KMX Bussysteme