

Fraud Detection 2.0 – Real Time SIP Analytics mithilfe von Complex Event Processing

Stuttgart, 09.03.2017

Markus Schneider
toplink GmbH

Darmstadt

Agenda

- **Vorstellung toplinek**
- **Das toplinek Produktportfolio**
- **Fraud – wie alles begann**
- **Fraud-Methoden und Muster**
- **Fraud Detection -Tools heute**
- **Fraud Detection 2.0 - TrustCom**
- **Systemübersicht**
- **APAMA**



LOEWE

Exzellente Forschung für
Hessens Zukunft

Agenda

- **Vorstellung toplinek**
- Das toplinek Produktportfolio
- Fraud – wie alles begann
- Fraud – Methoden und Muster
- Fraud Detection -Tools heute
- Fraud Detection 2.0 – TrustCom
- Systemübersicht
- APAMA



LOEWE

Exzellente Forschung für
Hessens Zukunft

toplink GmbH: Cloud-basierte Telekommunikation

- Sitz in Darmstadt, gegründet im Jahr 1995
- toplink GmbH ist der Betreiber eines der größten Cloud-Telefonsysteme in Deutschland (Telefonieren über das Internet)
- Pionier für SIP-Trunking-Technologie (IP-Telefonanschluss) auf dem deutschen Markt
- toplink ist ein von der Bundesnetzagentur zugelassener Teilnehmer-netzbetreiber mit einem Next-Generation-Network (NGN), über das Telefonanschlüsse in über 50 Ländern bereitgestellt werden
- alle Dienste werden ausschließlich in deutschen Rechenzentren betrieben und unterliegen den deutschen Datenschutzbestimmungen
- toplink ist einer der wenigen Anbieter in Deutschland, der alle Kunden-anschlüsse automatisch und permanent vor Gebührenmissbrauch (Fraud Detection) schützt

Agenda

- Vorstellung toplinek
- **Das toplinek Produktportfolio**
- Fraud – wie alles begann
- Fraud – Methoden und Muster
- Fraud Detection -Tools heute
- Fraud Detection 2.0 – TrustCom
- Systemübersicht
- APAMA



LOEWE

Exzellente Forschung für
Hessens Zukunft

Das topline-Portfolio

Breitband-Internetanschluss

Hochperformante und ausfallsichere Highspeed-Internetanschlüsse mit bundesweiter Verfügbarkeit

SIP-Trunking

Nahezu unbegrenzt skalierbare, flexible, durchwahl-fähige und VoIP-basierte Telefonanschlüsse mit Top-Sprachqualität

Cloud-Telefonanlage

Virtuelle Telefonanlage mit über 160 Funktionen, umfangreiche Individualisierungs- und Integrationsmöglichkeiten.

LUCA hosted Skype for Business

Innovative cloud-basierte UCC-Lösung. Interaktive, virtuelle und standortübergreifende Zusammenarbeit in ihrem Unternehmen

System- & Call-Center-Lösungen

Die modernsten IP-basierten Kommunikationslösungen und Cloud Services: CAESAR CASERIS und UNIFY Xpressions für Contact Centers und UNIFY Messaging



Agenda

- Vorstellung toplink
- Das toplink Produktportfolio
- **Fraud – wie alles begann**
- Fraud – Methoden und Muster
- Fraud Detection -Tools heute
- Fraud Detection 2.0 – TrustCom
- Systemübersicht
- APAMA

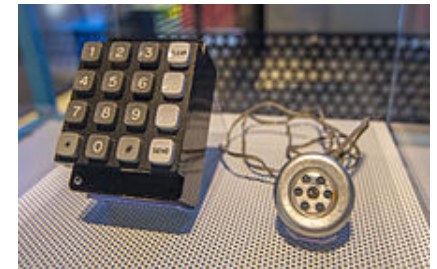


LOEWE

Exzellente Forschung für
Hessens Zukunft

Fraud – wie alles begann

- Switch Hook Fraud
 - Pulssimulation durch Tippen der Hörergabel
- Captain Crunch
 - John Draper
 - Spielzeugpfeife
 - 2600 Hz Ton – Simulation „Long Distance Call“
- Blue Box (Phreaking)
 - Multifrequenz Tongenerator
 - Simulation von Frequenzen zum Steuern von Calls



„If it hadn't been for the BLUE BOX, there would have been no APPLE“

Steve Jobs 1994



Agenda

- Vorstellung toplink
- Das toplink Produktportfolio
- Fraud – wie alles begann
- **Fraud – Methoden und Muster**
- Fraud Detection -Tools heute
- Fraud Detection 2.0 – TrustCom
- Systemübersicht
- APAMA



LOEWE

Exzellente Forschung für
Hessens Zukunft



Fraud - Methoden

- PBX Hacking bzw. IP-PBX Hacking
- Subscription Fraud (Anmeldung mit gefälschten Daten, keine Zahlungsabsicht)
- Dealer Fraud (interner Fraud, Reaktivierung alter Accounts...)
- Account/Identity Übernahme
- VoIP Hacking (Caller-ID Manipulation)

Fraud – Muster

- International Revenue Share Fraud (IRSF)
- Premium Rate Services (0900...)
- Interconnect Bypass (z.B. SIM Box)
- Massenanrufe auf gezielte B-Rufnummer (z.B. Blocken einer Hotline)





Agenda

- Vorstellung toplinek
- Das toplinek Produktportfolio
- Fraud – wie alles begann
- Fraud – Methoden und Muster
- **Fraud Detection -Tools heute**
- Fraud Detection 2.0 – TrustCom
- Systemübersicht
- APAMA



LOEWE

Exzellente Forschung für
Hessens Zukunft



Fraud Detection-Tools heute

- Blacklisten
- PrePaid Module
- Limitierung der Gesprächsdauer
- CDR-Statistiken
- Operator
- IN Lösung
- Fraud-Detection-System

Es gibt eine große Herausforderung....der überwiegende Teil dieser Systeme basiert auf „**Schadensminimierung**“ und nicht auf „**Schadensvermeidung**“

=> Erkennung und Vermeidung von schadhaften Calls bevor Kosten entstehen



Agenda

- Vorstellung toplinek
- Das toplinek Produktportfolio
- Fraud – wie alles begann
- Fraud – Methoden und Muster
- Fraud Detection -Tools heute
- **Fraud Detection 2.0 – TrustCom**
- Systemübersicht
- APAMA



LOEWE

Exzellente Forschung für
Hessens Zukunft



Fraud Detection 2.0 -TrustCom

- Ausleitung der SIP-Daten aus Produktivsystemen (SIP-Server, SBC, Softswitch)
- PCAP (packet capture)
- Konsistenzprüfung der SIP-Nachrichten
- Echtzeitverarbeitung mittels APAMA der Software AG
 - SIP Flooding (INVITE)
 - Syntaxfehler
 - Semantikfehler
 - SIP DoS
 - A-Nummer Anomalie (große Anzahl an parallelen Calls)
 - B-Nummer Anomalie (Ziele, die vorher nie angewählt wurden)
- Ausgabe an Zielsysteme (Softswitch, Registrar,...)
- Verhinderung bzw. Unterbrechung des Anrufs



Agenda

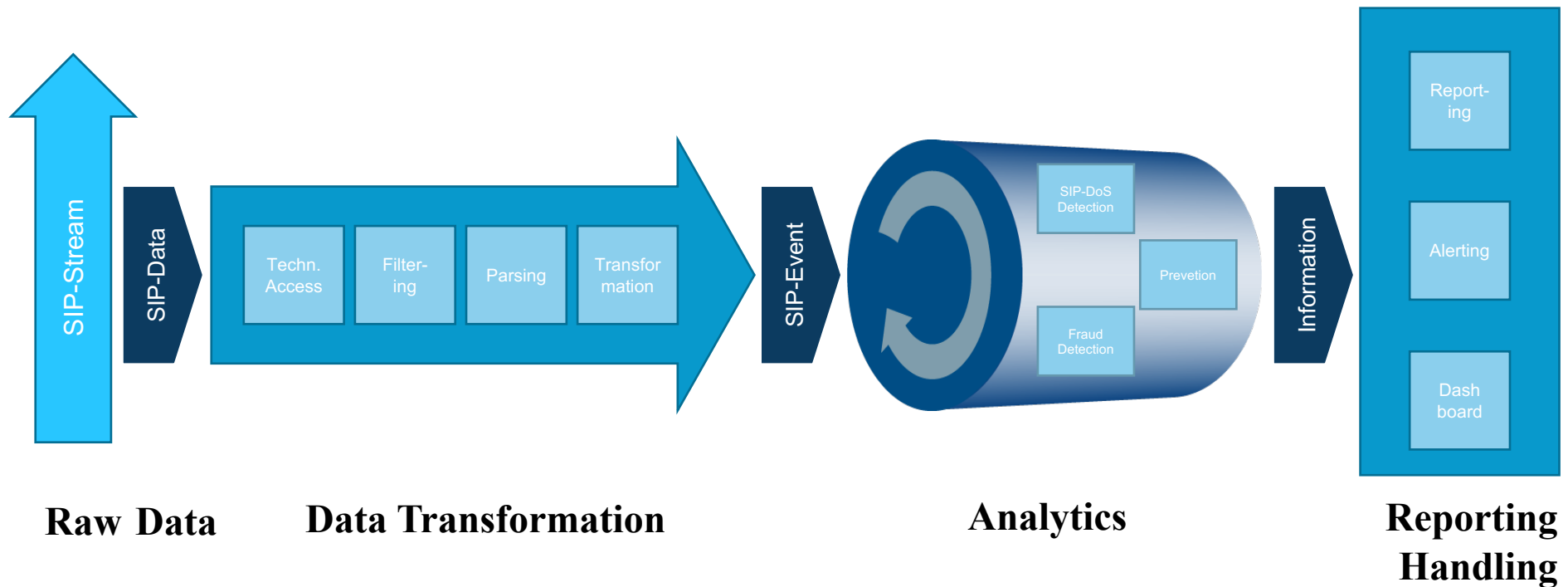
- Vorstellung toplinek
- Das toplinek Produktportfolio
- Fraud – wie alles begann
- Fraud – Methoden und Muster
- Fraud Detection -Tools heute
- Fraud Detection 2.0 - TrustCom
- **Systemübersicht**
- APAMA



LOEWE

Exzellente Forschung für
Hessens Zukunft

Apama – Funktionale Architektur





Agenda

- Vorstellung toplinek
- Das toplinek Produktportfolio
- Fraud – wie alles begann
- Fraud – Methoden und Muster
- Fraud Detection -Tools heute
- Fraud Detection 2.0 – TrustCom
- Systemübersicht
- **APAMA**



LOEWE

Exzellente Forschung für
Hessens Zukunft

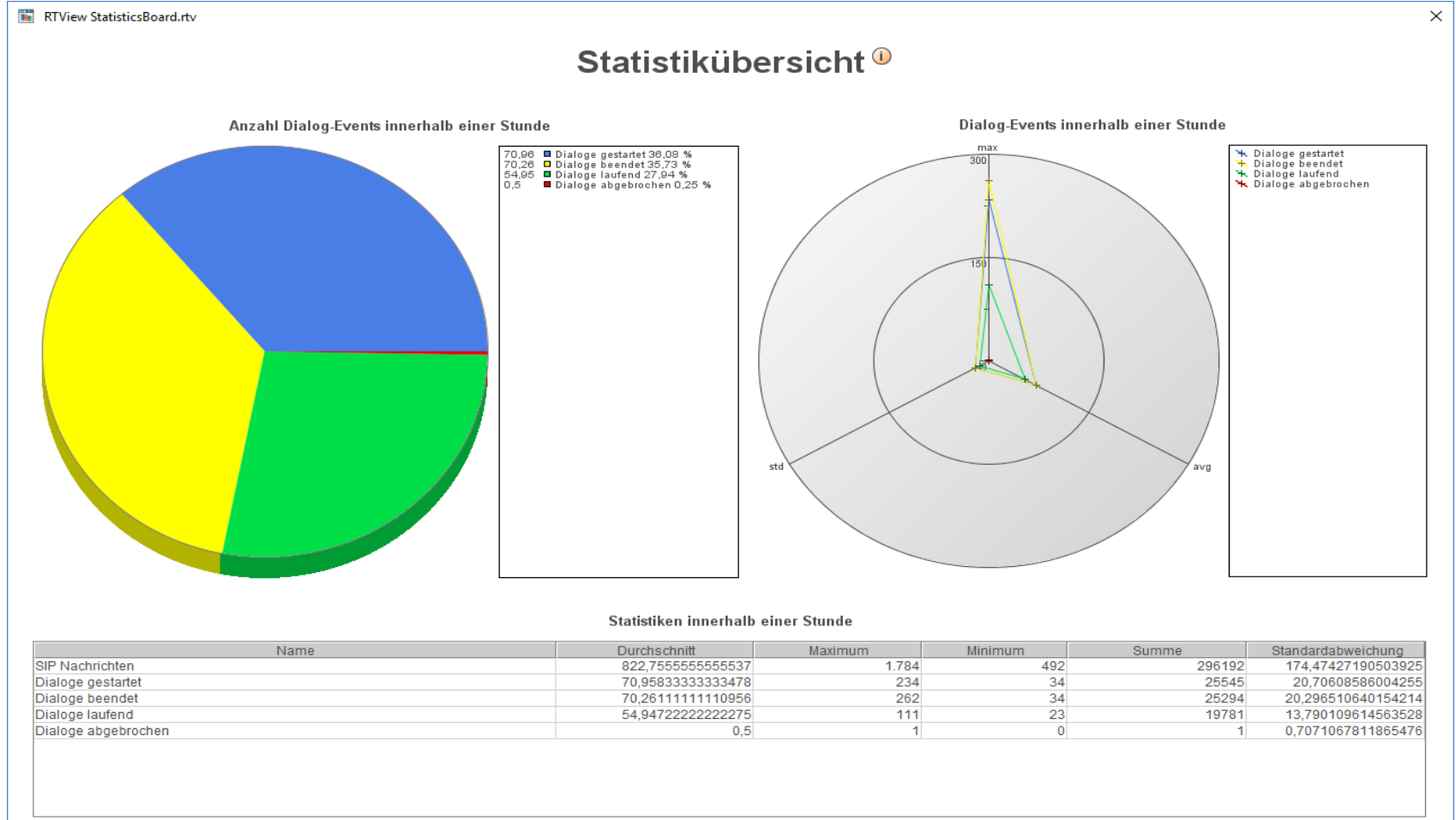
APAMA



software AG

- **Complex-Event-Processing (CEP) Plattform**
- **Analyse von Datenströme in „Echtzeit“**
- **Aggregation, zeitbezogene Analysen, Filterung und Korrelation**
- **Automatisches Auslösen (ohne manuelle Eingriffe) von Aktionen mit geringer Latenz**
- **Anreicherung von Datenströmen mit statischen Daten**
- **Verfügbarkeit von Hunderten von Adaptern**
- **Erstellung von Monitoring-Dashboards für Endanwender**
- **APAMA ist ein führendes System bei der Erkennung von Kreditkartenbetrug**

Dashboards



Filter

Benutzersuche

Anz. angezeigter Ben. 200

Benutzer - Score-Heatmap



RTView ValuePerIdHistory.rtv

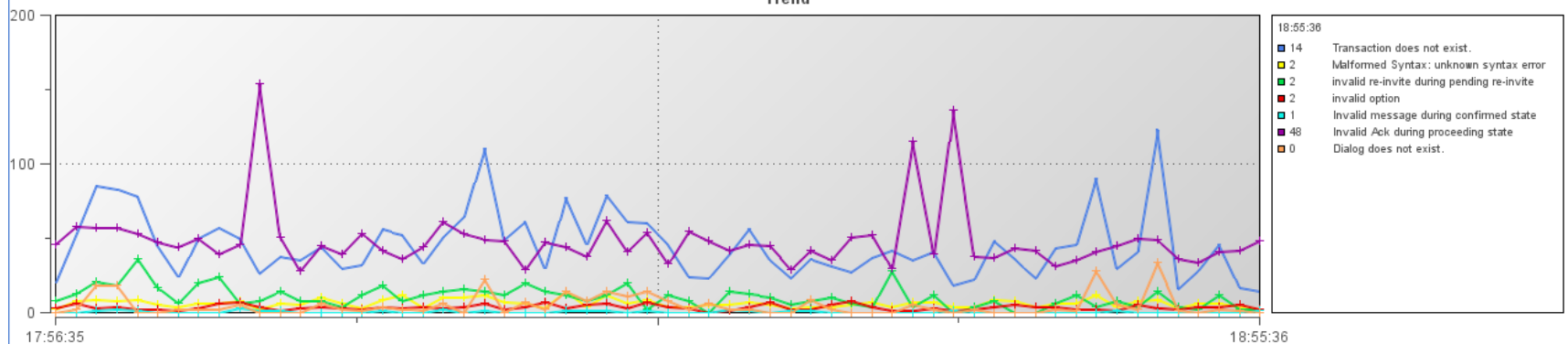
Ansicht: Ungültige Pakete pro Grund

Einstellungen

Wertetabelle

Zeitstempel ▾	Transaction does not exist	Malformed Syntax: unkno...	invalid re-invoke during pen...	invalid option	Invalid message during c...	Invalid Ack during proceedi...	Dialog does not exist.
14.12.2016 18:55:35	14	2	2	2	1	48	0
14.12.2016 18:54:35	17	4	2	5	0	42	1
14.12.2016 18:53:35	46	6	12	4	0	41	2
14.12.2016 18:52:35	28	6	2	4	0	34	0
14.12.2016 18:51:35	16	3	4	2	0	36	1
14.12.2016 18:50:35	123	9	14	3	0	49	34
14.12.2016 18:49:35	41	8	4	5	0	50	2
14.12.2016 18:48:35	30	4	8	1	1	45	5
14.12.2016 18:47:35	90	12	4	2	0	41	28
14.12.2016 18:46:35	46	6	12	2	0	35	1
14.12.2016 18:45:35	43	6	6	4	0	31	2
14.12.2016 18:44:35	23	4	0	4	0	42	0
14.12.2016 18:43:35	36	8	0	5	0	43	0
14.12.2016 18:42:35	48	9	8	4	0	37	0
14.12.2016 18:41:35	22	4	4	2	0	38	2
14.12.2016 18:40:35	18	4	0	1	1	136	0
14.12.2016 18:39:35	41	7	12	3	0	39	2
14.12.2016 18:38:35	35	7	4	1	0	115	5
14.12.2016 18:37:35	42	4	28	1	0	30	0

Trend



toplink

Happy to help

Markus Schneider

Director Operations
Robert-Bosch-Straße 20
64293 Darmstadt

markus.schneider@toplink.de
+49 6151 6275-570

