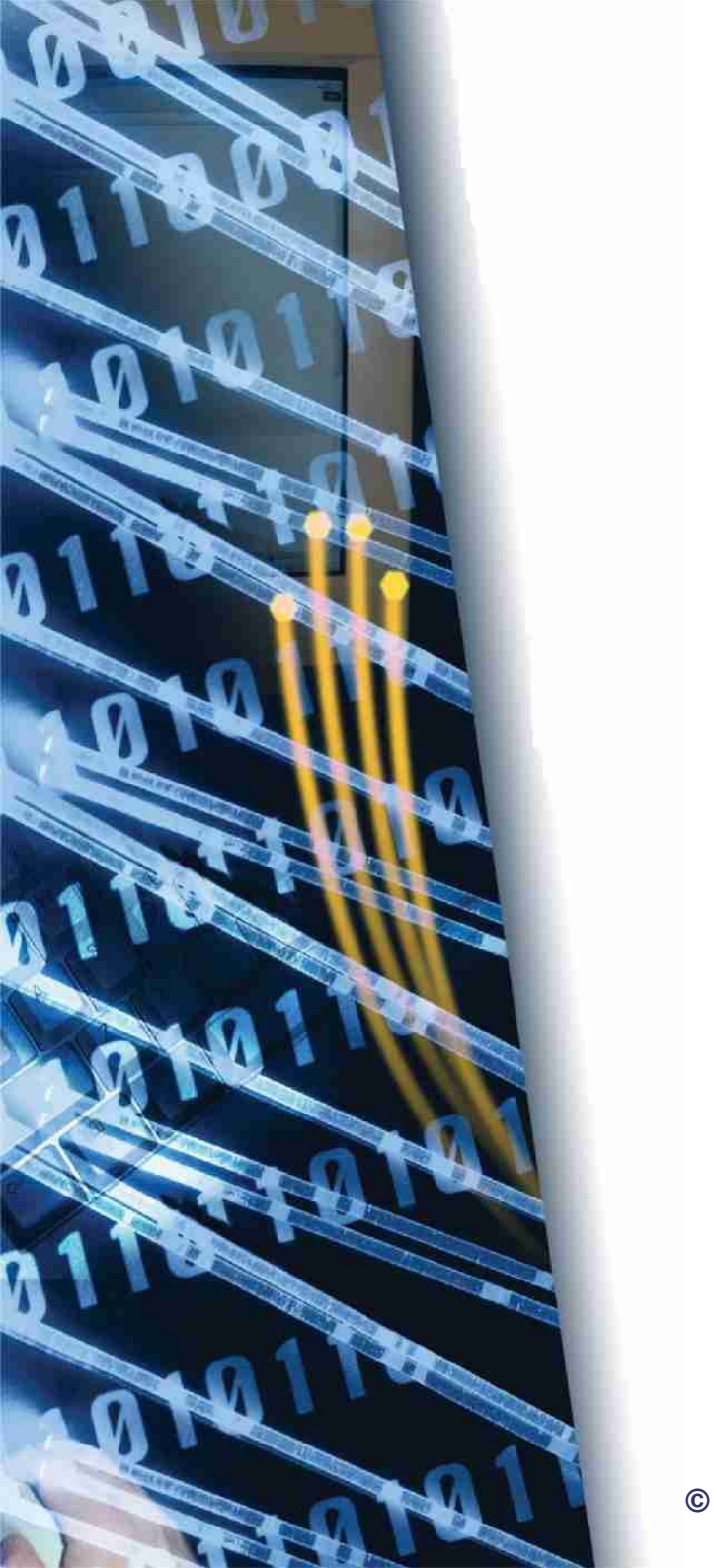
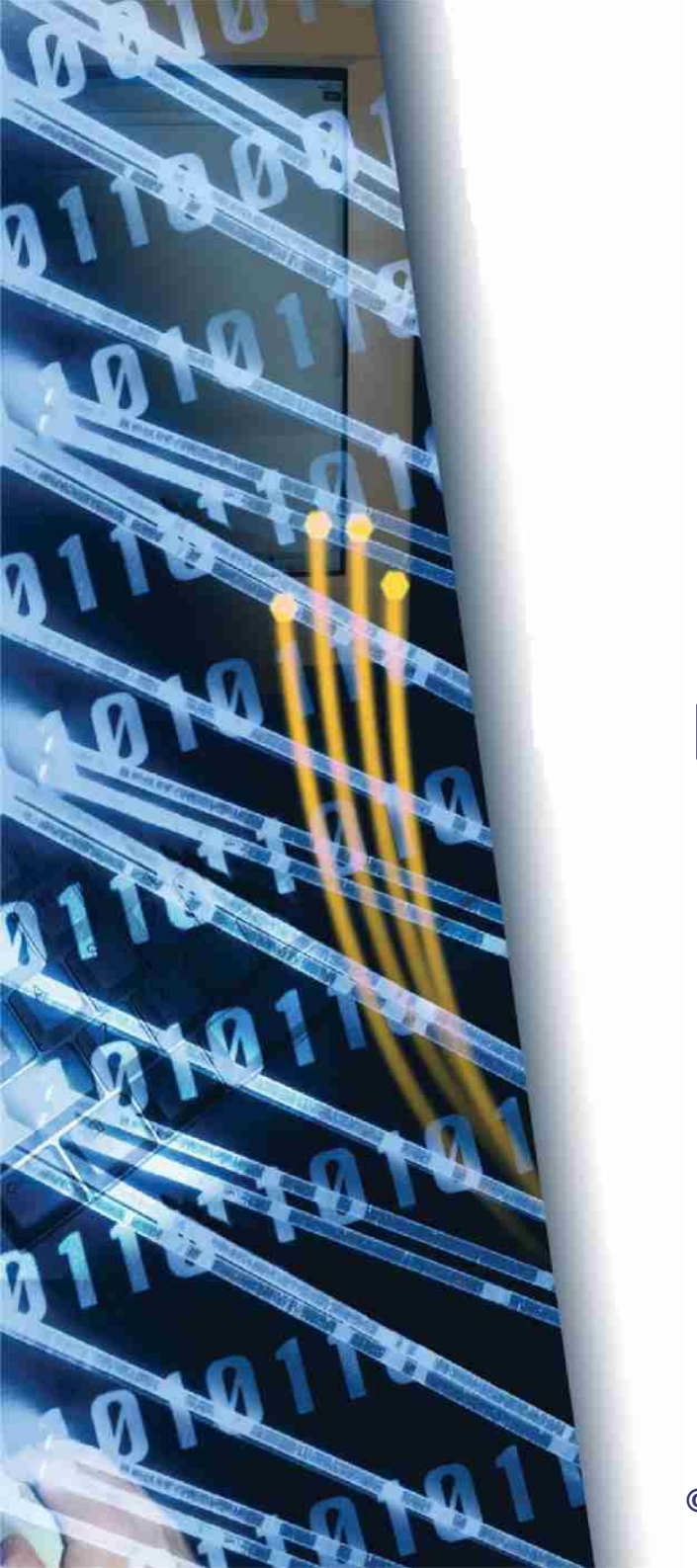


Event-Aggregation in Frühwarnsystemen

Till Dörges

Gliederung

- Motivation
- Definitionen
- Aggregationsverfahren
- Implementierung
- Ergebnisse / Ausblick



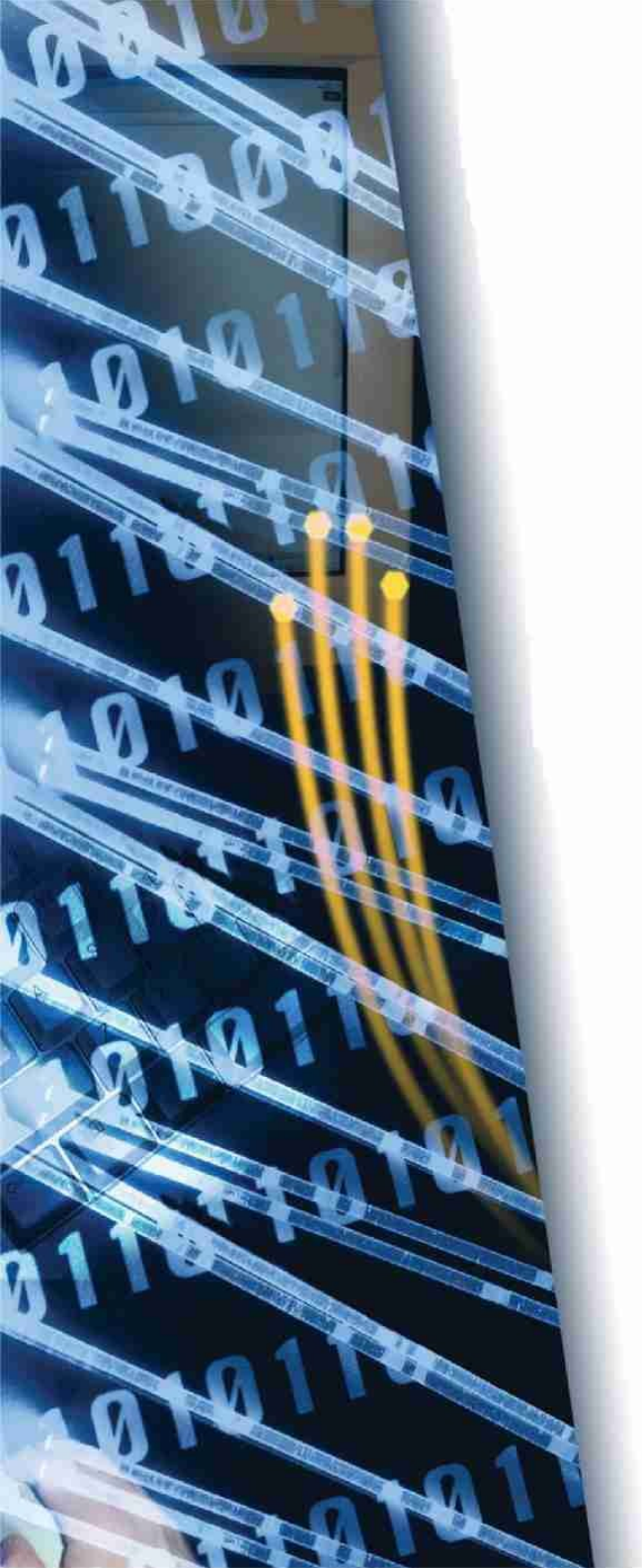
Motivation / Fragestellungen

Motivation / Fragestellungen

- **Netzwerke sind kritische Ressourcen**
  - Bestimmte Dinge weiß man gerne vorher (oder so früh wie möglich)
  - ➔ Monitoring unumgänglich
- **Monitoring erzeugt u.U. große Datenmengen**
- **Bösartiger Traffic nicht immer leicht zu entdecken**
- **Definition von „Netzwerkstatus“?**
- **Definition von „Lagebild“?**
- **Wann wen alarmieren?**

Lösungsansätze

- **Monitoring**
- **Vorklassifizierung von Traffic (z.B. Honeypots)**
- **Bessere Datenrepräsentation / -visualisierung**
- **Datenmenge reduzieren**
  - Aggregation
  - Korrelation
- **...**



Definitionen

Definitionen

- **Frühe Warnung / Frühwarnung**

„Aufgrund eindeutiger Erkenntnisse, die noch möglichst Wenige betreffen, sind Informationen zu verteilen, die vielen (noch nicht) Betroffenen helfen, und insgesamt Schlimmeres vermeiden!“

(Kossakowski, 2005)

Definitionen

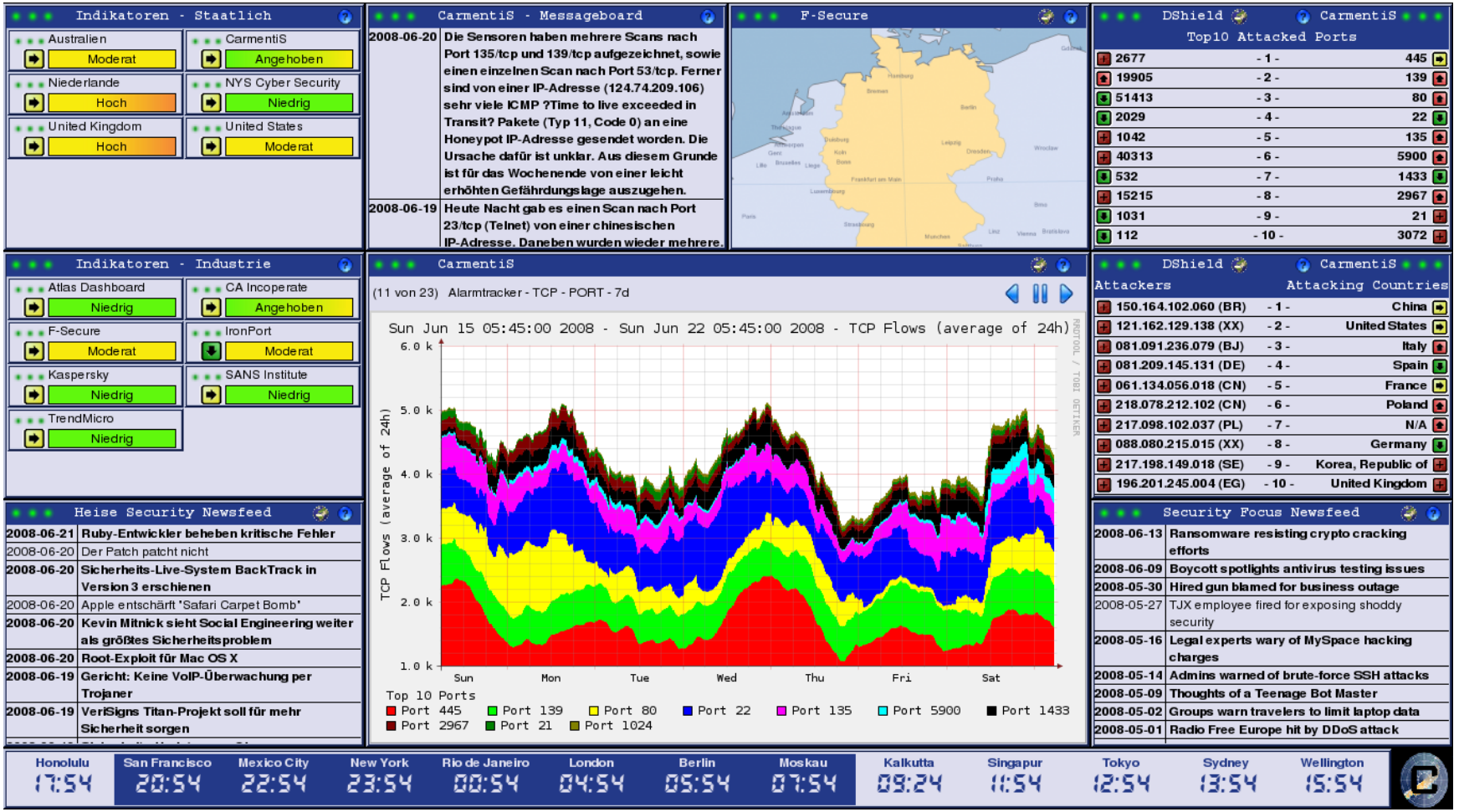
- **Lagebild (“Situational Awareness”)**
  - Benötigt ausreichend Informationen
  - Spezifisch für jeweiliges Szenario
  - Ermöglicht Entscheidungen
  - Basis für Frühwarnung

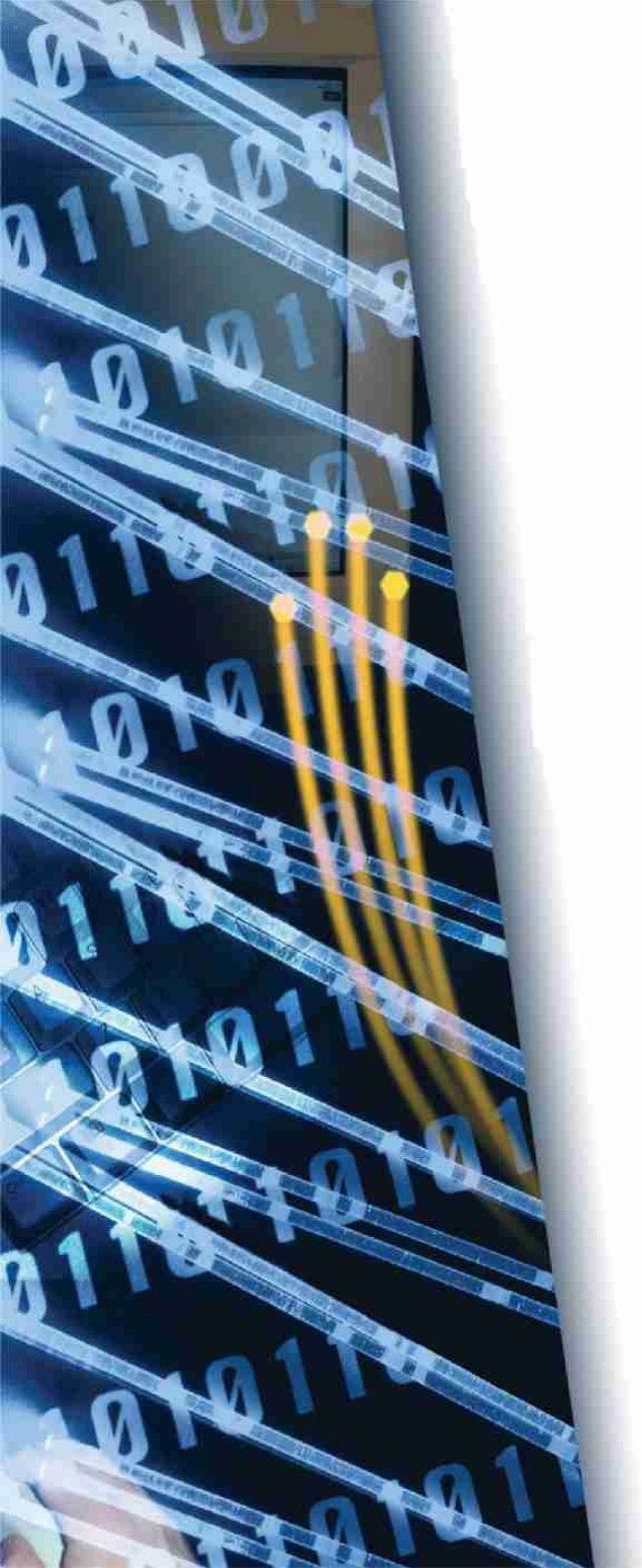
Definitionen

- **Korrelation**
  - Statistik / Wahrscheinlichkeitstheorie
  - Beziehung („Korrelationskoeffizienten“) zwischen unterschiedlichen Variablen
- **Aggregation**
  - Zusammenfassung einzelner Ereignisse / Informationen
  - Metaereignisse
- **Nicht immer saubere Trennung**

CarmentiS Security Dashboard

■ Beispiel für Aggregation





Aggregationsverfahren

Erweiterung eines bestehend. FWS

- **Ansätze für Aggregation**
  - Angriffsgraphen
  - Clustering
  - Regelbasierte Verfahren
  - ...
  - Hybride Ansätze
- **Untersuchung verschiedener Ansätze**

Angriffsgraphen

- **Modellierung**
  - Netzwerkzustände
  - (Erfolgreiche) Angriffsversuche
  - Angreiferverhalten
  - Aufdeckung von Schwachstellen
- → **Erstellung sehr aufwändig**

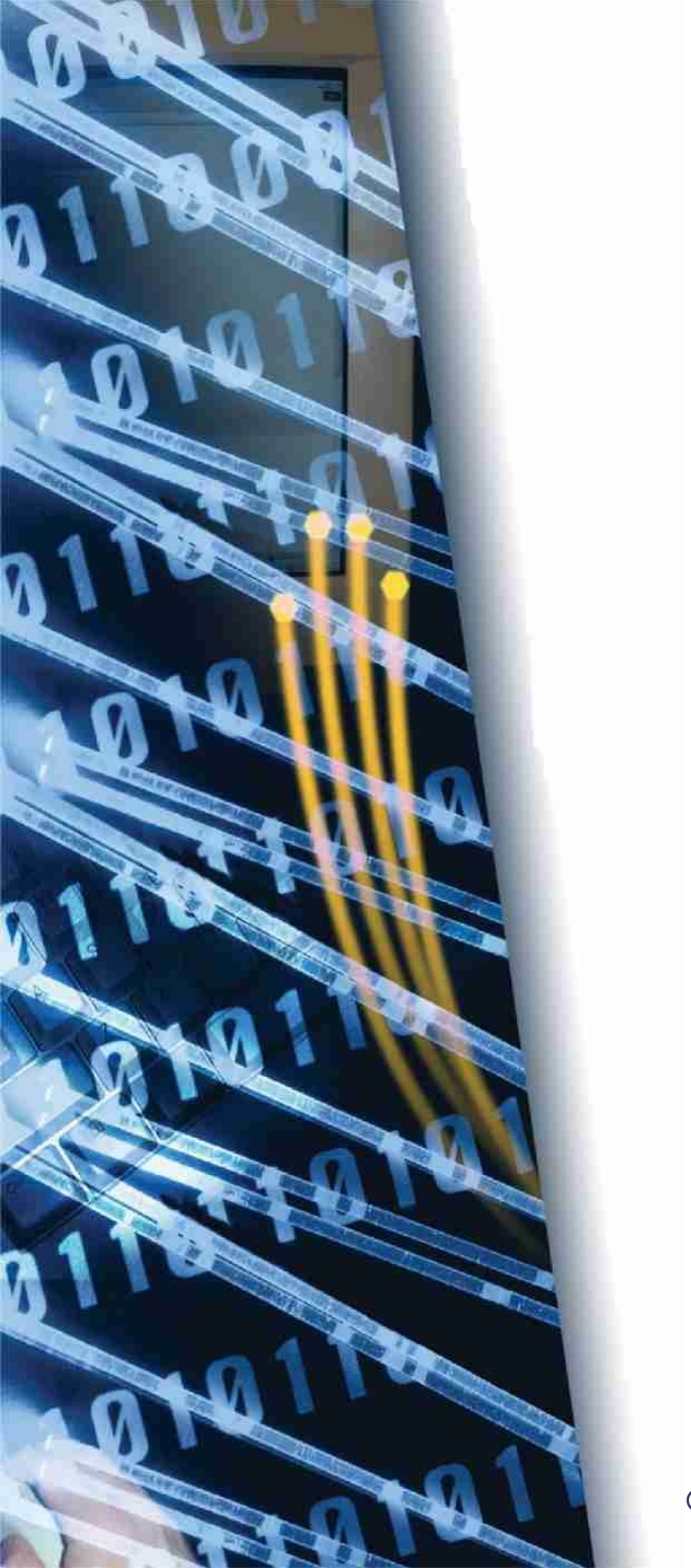
Clustering

- Zusammenfassung ähnlicher Ereignisse zu Clustern
- Merkmale
- Ähnlichkeitsmaß / Klassifikator
- Ggf. Trainingsphase nötig

→ Aufwändig oder „unsensibel“ für Neues

Regelbasierte Verfahren

- Inferenzkomponente
- Wissensbasis
- Laufzeit akzeptabel



Implementierung

Anforderungen

- Flexibilität
- Performanz
- Skalierbarkeit
- Qualität der Ergebnisse
- Integrierbarkeit
- Verfügbarkeit
- Unterstützung für unterschiedliche Datenarten

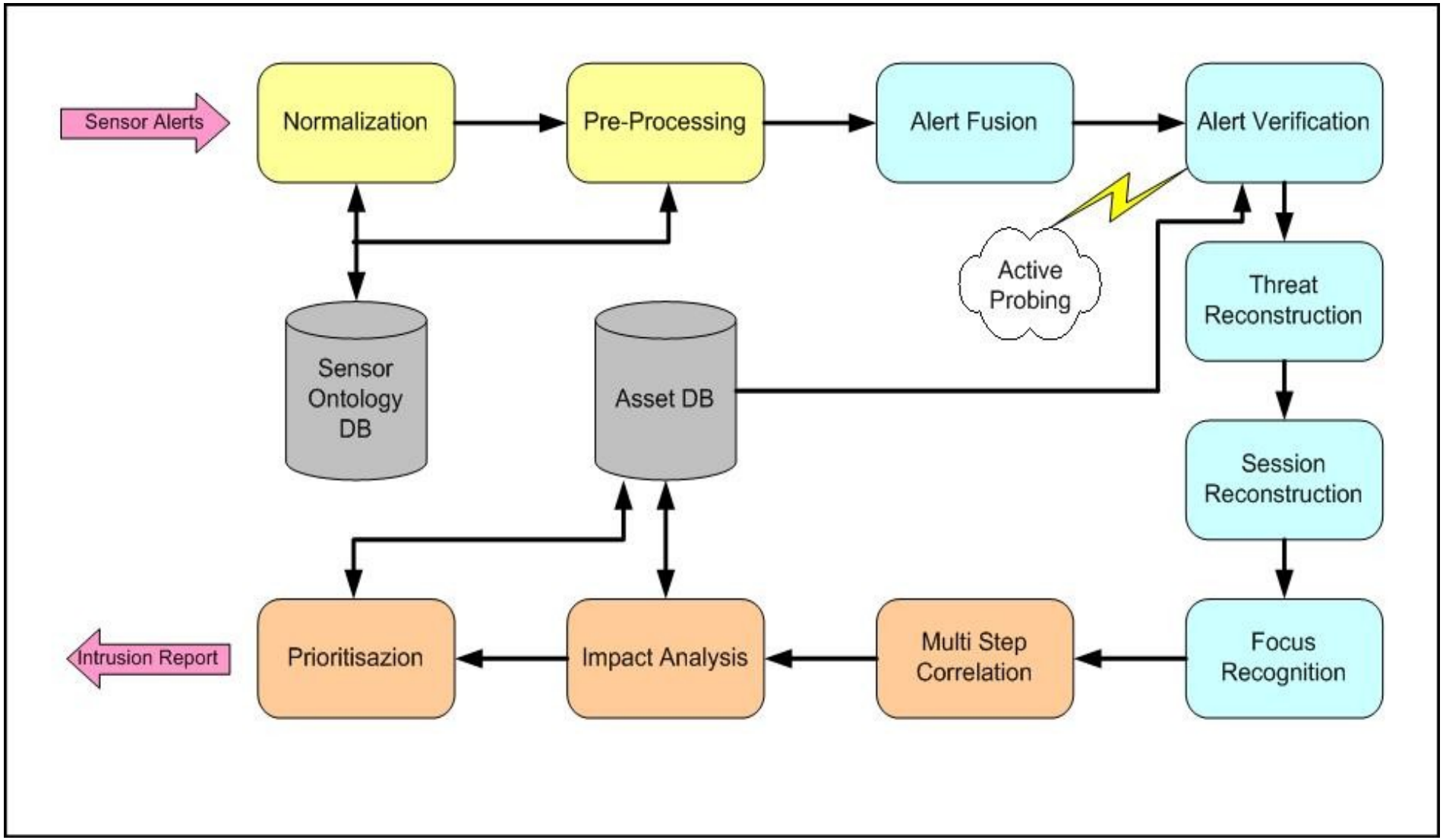
Implementierungshürden

- Einführung von Metaereignissen
- Biflows benötigt
- Erweiterung der Darstellungsschicht
- Statusinformationen aus voriger Zeitscheibe benötigt

Ausgewählte Verfahren

- Valeur, F.; Vigna, G.; Krügel, C. & Kemmerer, R. A Comprehensive Approach to Intrusion Detection Alert Correlation
  IEEE, 2004
- Panjwani; Tan; Jarrin; Cukier
  Experimental Evaluation to Determine if Port Scans are Precursors to an Attack
  International Conference on Dependable Systems and Networks, 2005

Ausgewählte Verfahren (Valeur)



Ausgewählte Verfahren (Valeur)

- **Normalization / Pre-Processing**
- **Alert Fusion (remove duplicates)**
- **Alert Verification (no false positives)**
- **Thread Reconstruction (one attacker)**
- **Session Reconstruction (net / host based)**
- **Focus Recognition**
  - Many2One (DDos)
  - One2Many (horizontal port scans)
- **Multi-Step Correlation (island hopping)**
- **Impact Analysis / Alert Prioritization**

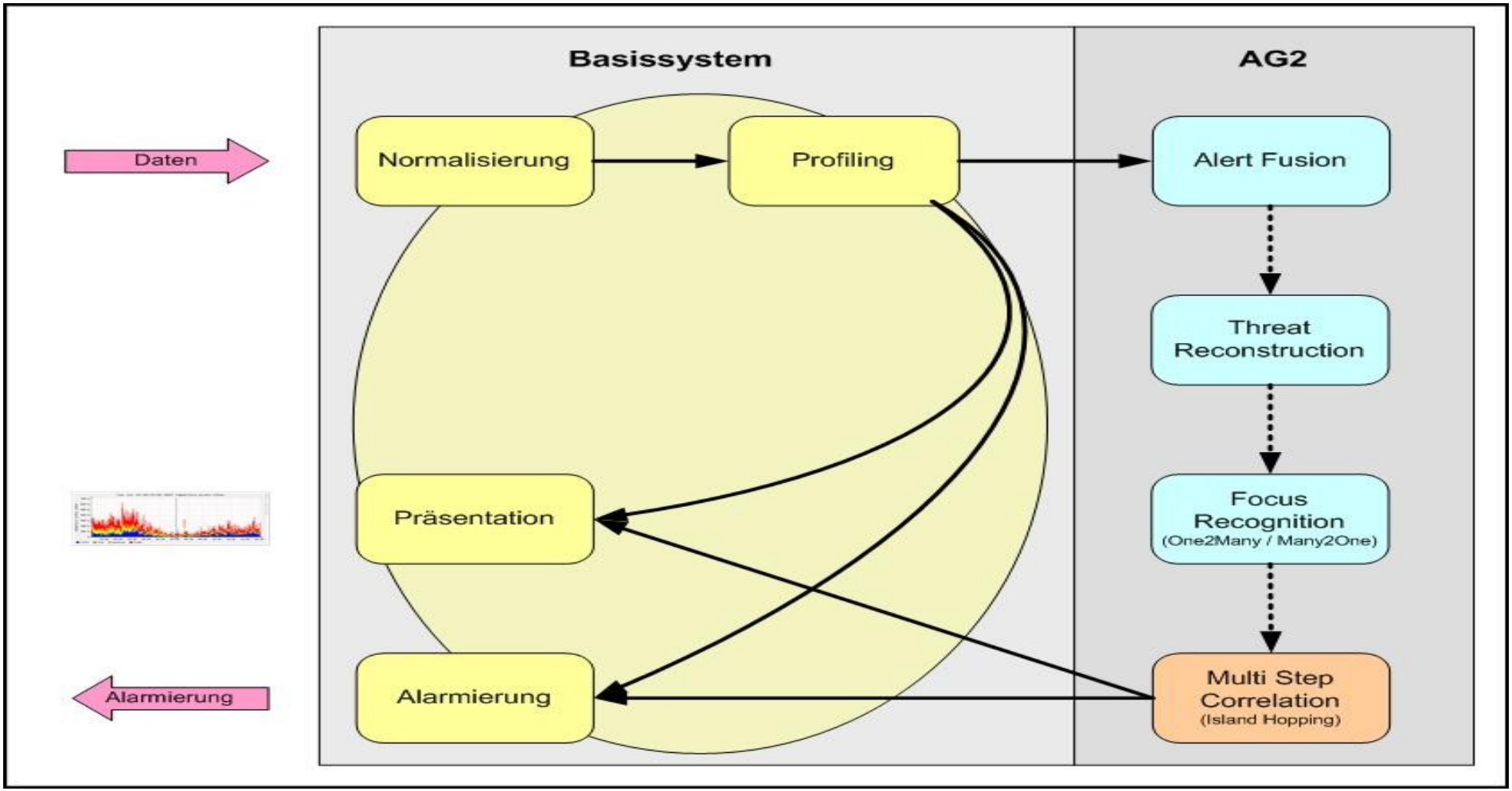
Ausgewählte Verfahren (Panjwani)

- Anz. Pakete — Klassifikation

0 <= n < 5	Port Scan / Ping Scan (ICMP)
5 <= n <= 12	Probe
12 < n	Attack

→ Einsatz zur Grobklassifikation

Integration in CarmentiS



Algorithmus Alert Fusion

E1 E2

src_ip/port = src_ip/port

dst_ip/port = dst_ip/port

starttime + duration <= starttime(detectiontime)

Algorithmus Thread Reconstruction

- One2One

E1		E2
src_ip	=	src_ip
dst_ip	=	dst_ip

- Time window 120 seconds
- Start time Min(e1.st, e2.st)
- End time Max(e1.et, e2.et)
- Weitere Klassifikation (password guessing, exploit, ...)

Algorithmus Focus Recognition

- One2Many

E1	E2	...	En
src_ip	= src_ip	...	= src_ip

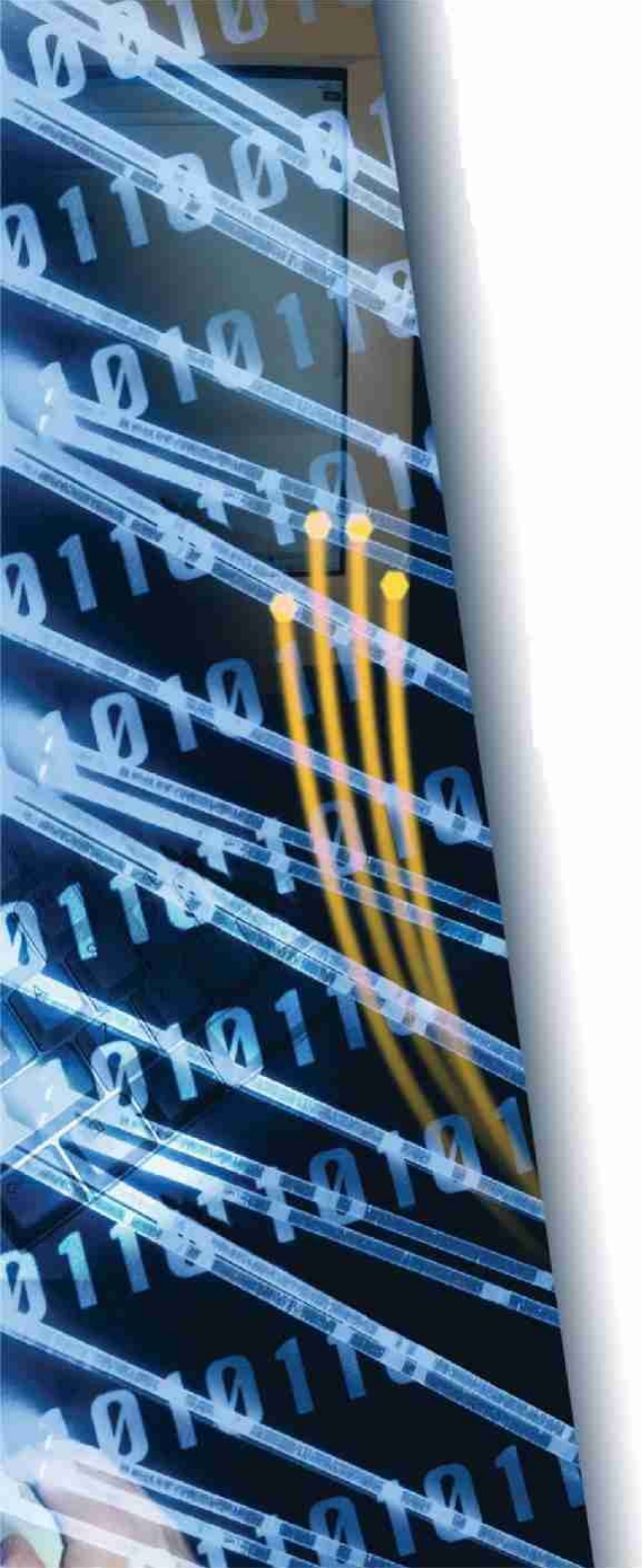
- Time window 120 seconds
- Threshold configurable
- Start time Min(e1.st, en.st)
- End time Max(e1.et, en.et)
- Weitere Klassifikation (scanning, ...)

Algorithmus Focus Recognition

- Many2One

E1	E2	...	En
dst_ip	= dst_ip	...	= dst_ip

- Time window 120 seconds
- Threshold configurable
- Start time Min(e1.st, en.st)
- End time Max(e1.et, en.et)
- Weitere Klassifikation (scanning, ...)



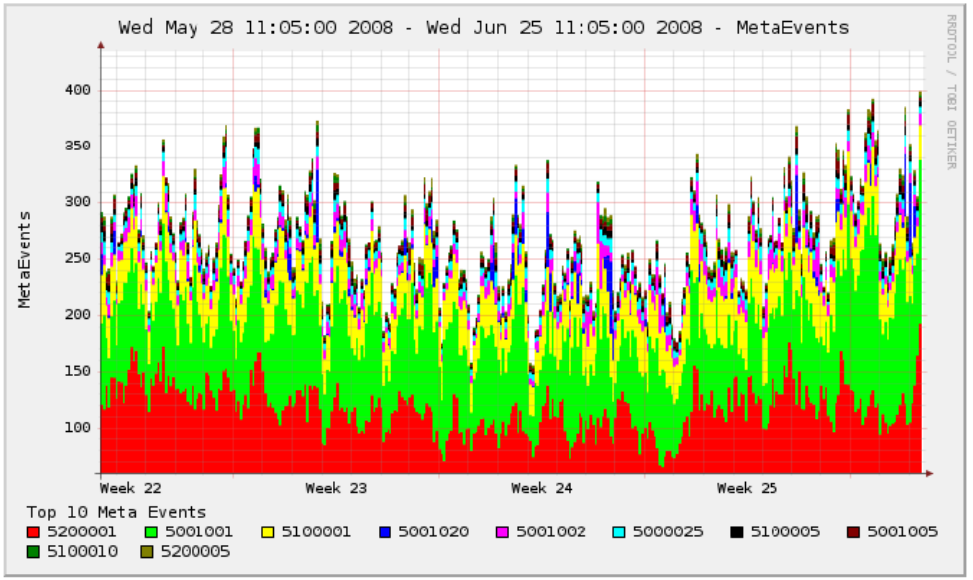
Ergebnisse

Detaillierte Analyse

Statistics timeslot Jun 24 2008 - 22:55

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
2_Events	5.9 /s	3.7 /s	1.4 /s	0.8 /s	0 /s	3.2 /s	1.9 /s	0.5 /s	0.8 /s	0 /s	4.9 kb/s	3.3 kb/s	1.3 kb/s	347.0 b/s	0 b/s
1_MetaEvents	1.1 /s	0.6 /s	0.5 /s	0.1 /s	0.0 /s	91.8 /s	75.5 /s	2.9 /s	1.5 /s	11.9 /s	184.6 kb/s	170.9 kb/s	6.5 kb/s	705.7 b/s	6.5 kb/s

TopN-Statistiken



Show Top 10 MetaEvents

now 24 hours

Track MetaEvent:

Add Delete

Skip MetaEvent:

Add Delete

Display 4 weeks Y-axis: Linear Log Type: Stacked Line

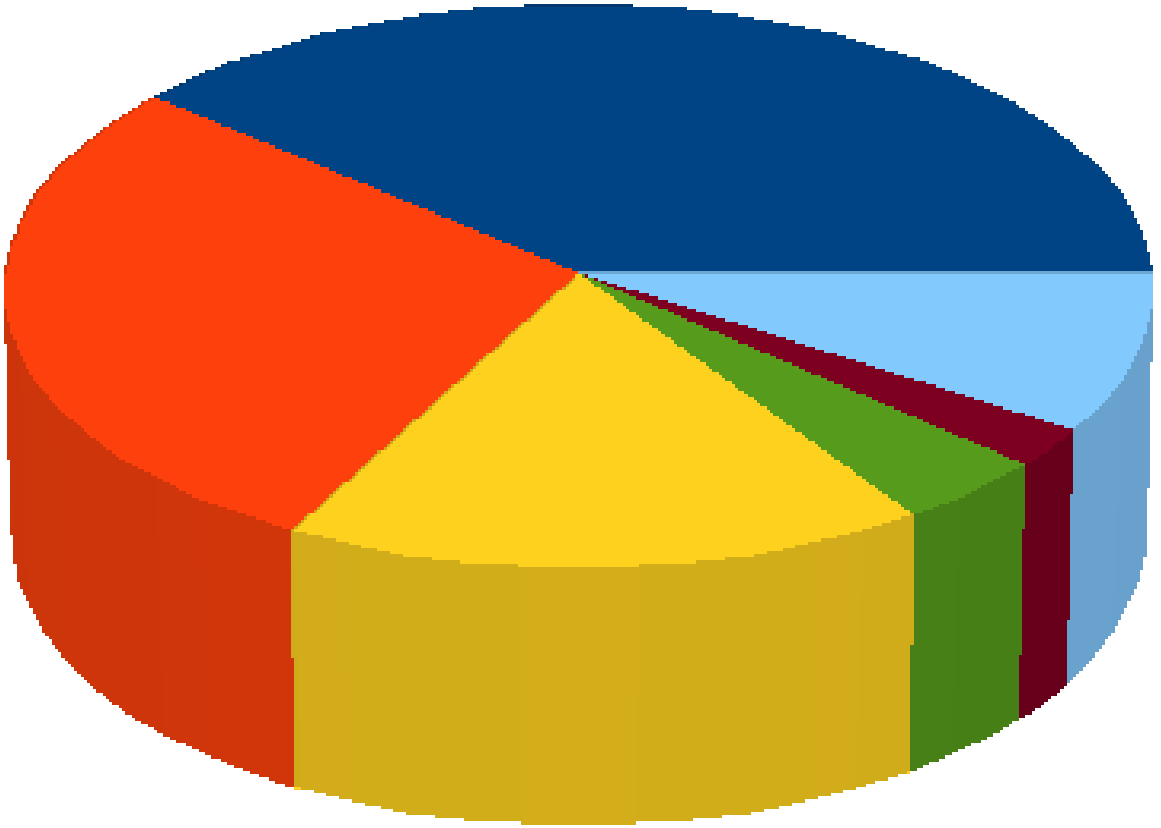
Top 10 Statistics

Rank	ID	Count	Info
1	5200001	35822	"Many2One Scanning Hosts"
2	5001001	31860	"Multiple Port Scan"
3	5100001	9198	"One2Many Scanning Hosts"
4	5001020	2751	"Multiple Malware Download"
5	5001002	2583	"Multiple Ping Scan"

Erste Ergebnisse

Aggregated Events

2008-05-08 - 2008-06-04



Erste Ergebnisse

- **Wirkbetrieb**
- **Reduction ratio**
  - 10-12 %
- **Scanning-Ereignisse dominieren**
  - Many2One Scanning Hosts
  - Multiple Port Scan
  - One2Many Scanning Hosts

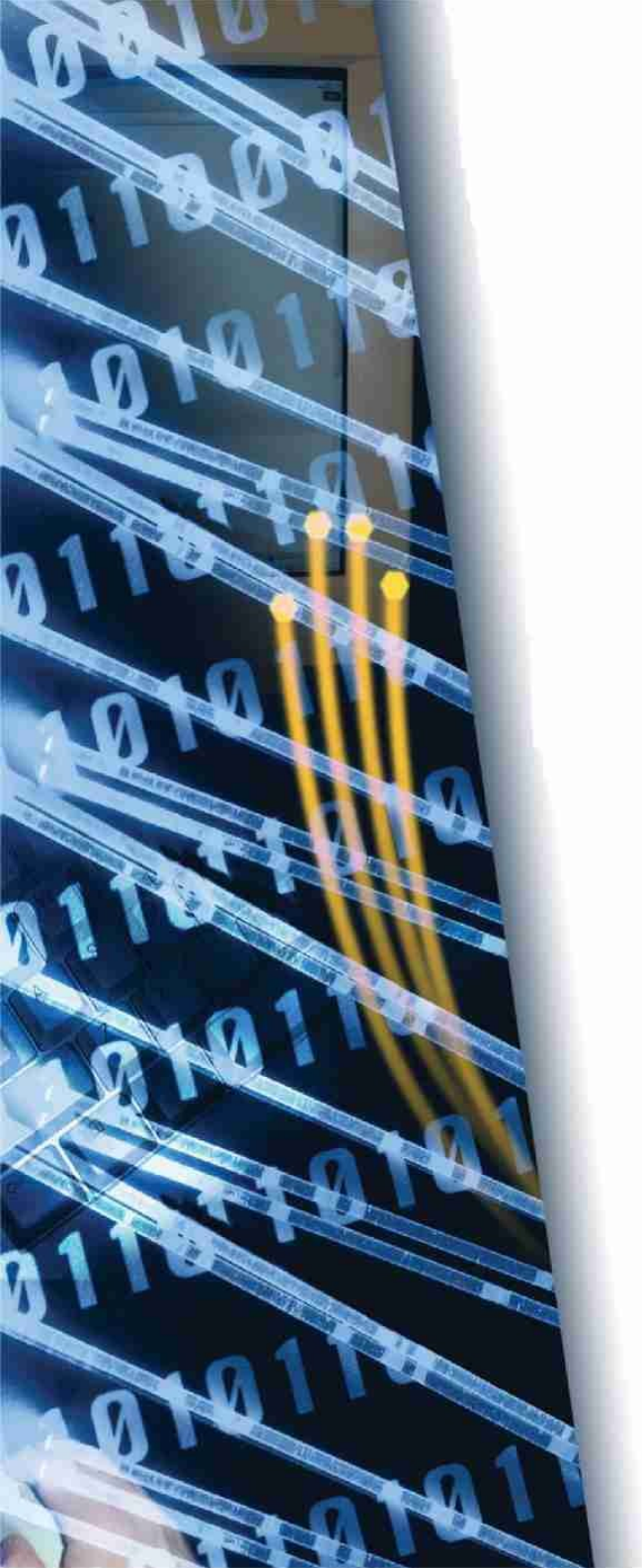
Ausblick

- „Drilldown“ in Metaereignisse
- Verbesserungen Visualisierung
- Bestehende Algorithmen tunen
- Neue Algorithmen ausprobieren

Kontakt

Till Dörges <doerges@pre-sense.de>

PRESENSE Technologies GmbH



Anhang

Conficker-Wurm

- Entdeckt durch einfache Aggregationsverfahren