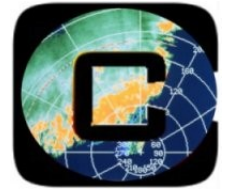


# Event-Aggregation in Frühwarnsystemen

Till Dörges



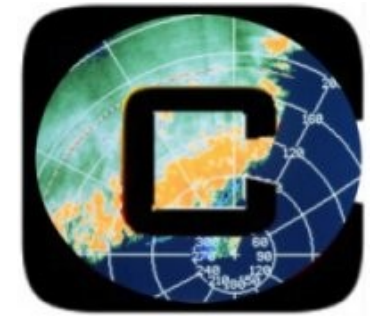
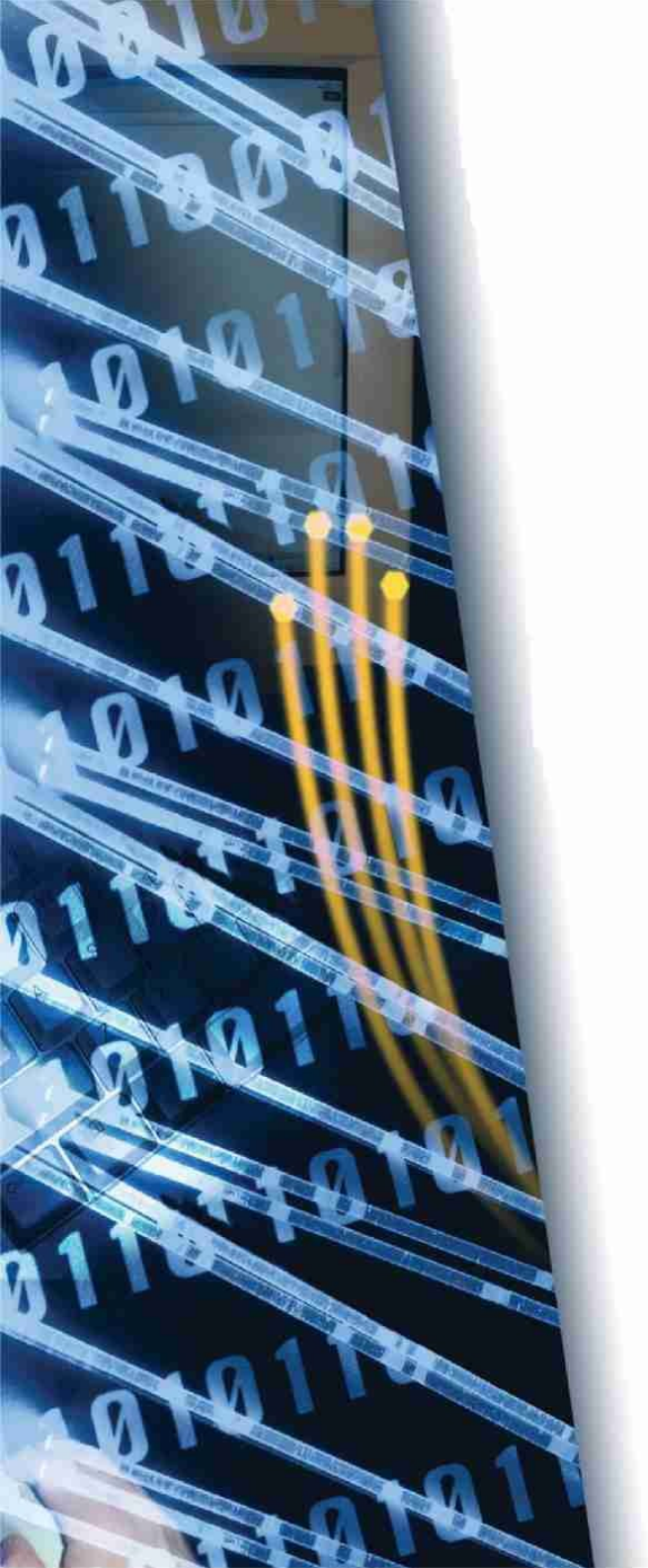


# Gliederung

---

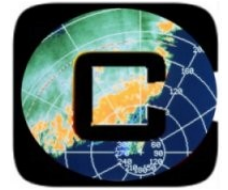
- Motivation
- Definitionen
- Aggregationsverfahren
- Implementierung
- Ergebnisse / Ausblick





# Motivation / Fragestellungen

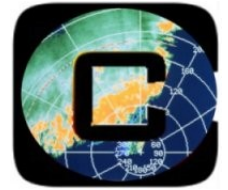




# Motivation / Fragestellungen

- **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?**

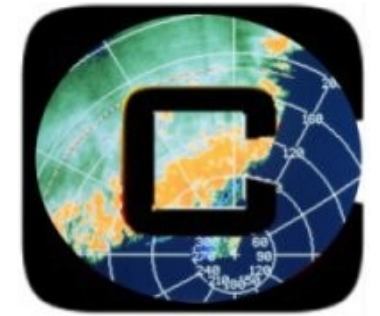




# Lösungsansätze

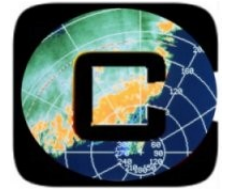
- Monitoring
- Vorklassifizierung von Traffic (z.B. Honeypots)
- Bessere Datenrepräsentation / -visualisierung
- Datenmenge reduzieren
  - Aggregation
  - Korrelation
- ...





# Definitionen





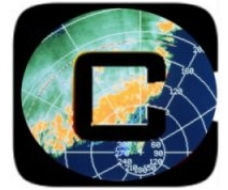
# Definitionen

## ■ 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)



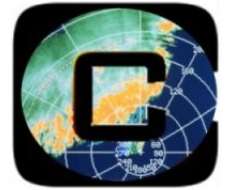


# Definitionen

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







# Definitionen

## ■ Korrelation

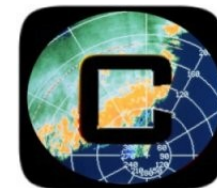
- Statistik / Wahrscheinlichkeitstheorie
- Beziehung („Korrelationskoeffizienten“) zwischen unterschiedlichen Variablen

## ■ Aggregation

- Zusammenfassung einzelner Ereignisse / Informationen
- Metaereignisse

## ■ Nicht immer saubere Trennung



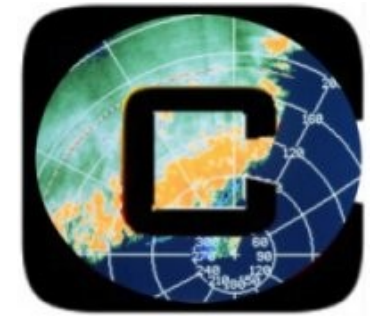
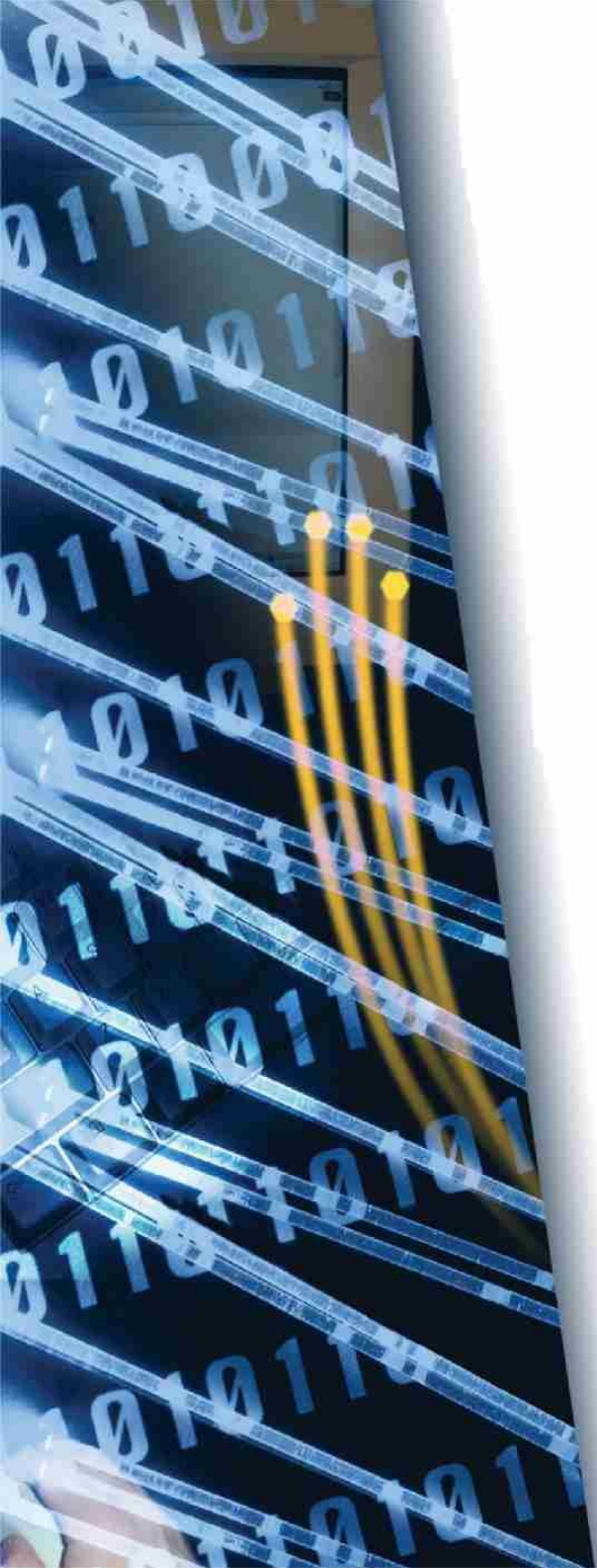


# Carmentis Security Dashboard

## ■ Beispiel für Aggregation

The dashboard is divided into several sections:

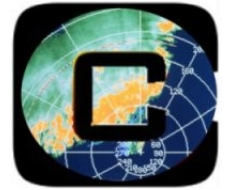
- Indikatoren - Staatlich:** Shows security levels for Australia (Moderat), Netherlands (Hoch), United Kingdom (Hoch), Carmentis (Angehoben), NYS Cyber Security (Niedrig), and United States (Moderat).
- Carmentis - Messageboard:** Contains two entries from 2008-06-20 and 2008-06-19 regarding port scans and ICMP traffic.
- F-Secure:** A map of Germany showing sensor locations.
- DSshield / Carmentis:** A table of Top10 Attacked Ports.
- Indikatoren - Industrie:** Shows security levels for Atlas Dashboard (Niedrig), CA Incooperate (Angehoben), F-Secure (Moderat), IronPort (Moderat), Kaspersky (Niedrig), SANS Institute (Niedrig), and TrendMicro (Niedrig).
- Carmentis Alarmtracker:** A line graph showing TCP Flows (average of 24h) from Sun Jun 15 to Sun Jun 22, 2008. The graph shows multiple colored lines representing different ports, with a legend for Top 10 Ports: 445, 139, 80, 22, 135, 5900, 1433, 2967, 21, 1024.
- DSshield / Carmentis:** A table of Attackers and Attacking Countries.
- Heise Security Newsfeed:** A list of security news items from 2008-06-21 to 2008-06-19.
- Security Focus Newsfeed:** A list of security news items from 2008-06-13 to 2008-05-01.
- Global Time:** A row of digital clocks for various cities: Honolulu (17:54), San Francisco (20:54), Mexico City (22:54), New York (23:54), Rio de Janeiro (00:54), London (04:54), Berlin (05:54), Moskau (07:54), Kalkutta (09:24), Singapur (11:54), Tokyo (12:54), Sydney (13:54), Wellington (15:54).



# Aggregationsverfahren



# Erweiterung eines bestehend. FWS

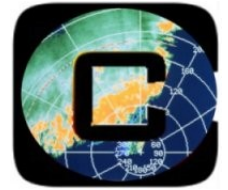


## ■ Ansätze für Aggregation

- Angriffsgraphen
- Clustering
- Regelbasierte Verfahren
- ...
- Hybride Ansätze

## ■ Untersuchung verschiedener Ansätze





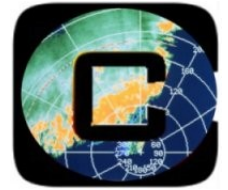
# Angriffsgraphen

## ■ Modellierung

- Netzwerkzustände
- (Erfolgreiche) Angriffsversuche
- Angreiferverhalten
- Aufdeckung von Schwachstellen

→ **Erstellung sehr aufwändig**

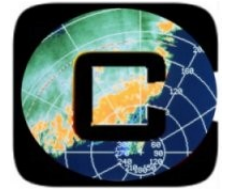




# Clustering

- Zusammenfassung ähnlicher Ereignisse zu Clustern
- Merkmale
- Ähnlichkeitsmaß / Klassifikator
- Ggf. Trainingsphase nötig
- Aufwändig oder „unsensibel“ für Neues



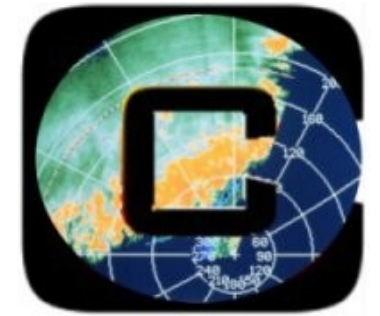
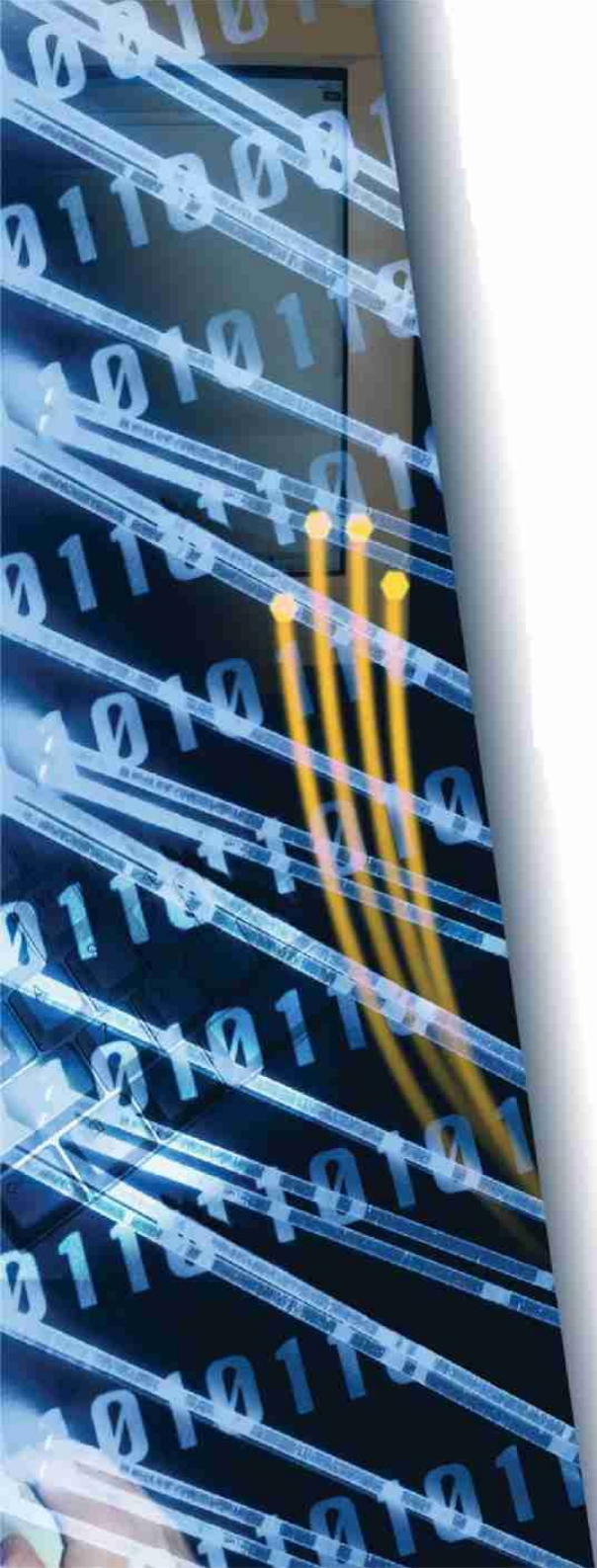


# Regelbasierte Verfahren

---

- Inferenzkomponente
- Wissensbasis
- Laufzeit akzeptabel

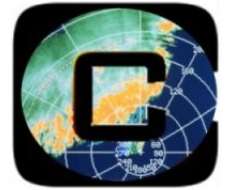




# Implementierung



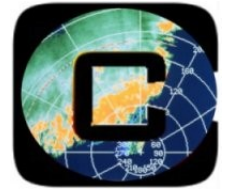




# Anforderungen

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

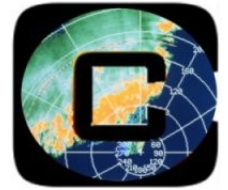




# Implementierungshürden

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

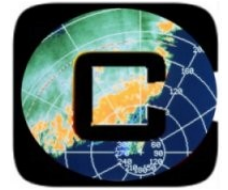




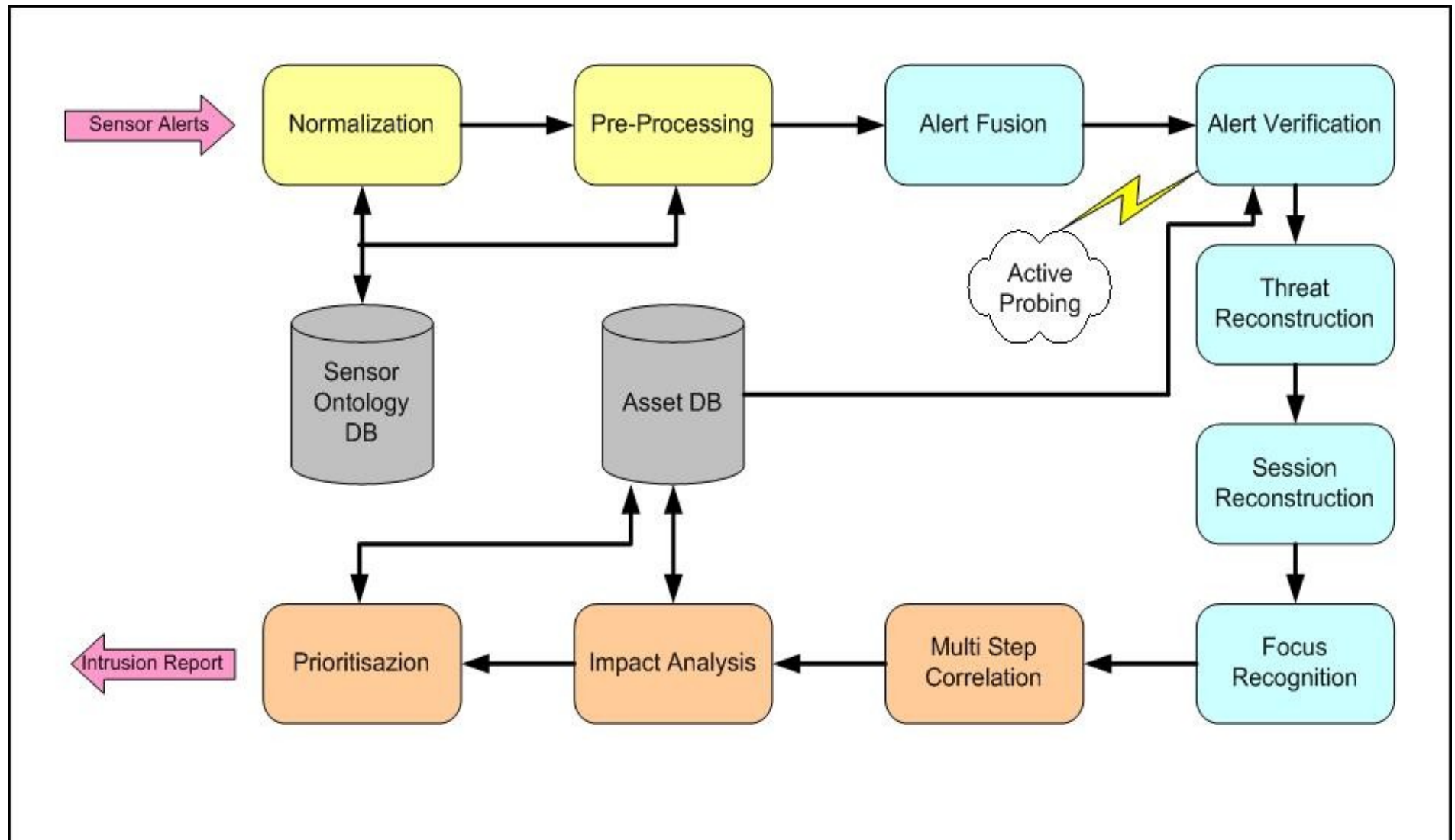
# Ausgewählte Verfahren

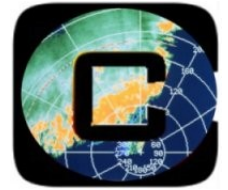
- **Valeur, F.; Vigna, G.; Krügel, C. & Kemmerer, R. A**  
**Comprehensive Approach to Intrusion Detection**  
**Alert Correlation**  
**IEEE, 2004**
- **Panjwani; Tan; Jarrin; Cukier**  
**Experimental Evaluation to Determine if Port**  
**Scans are Precursors to an Attack**  
**International Conference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





# Ausgewählte Verfahren (Valeur)



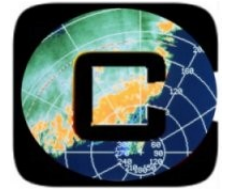


# Ausgewählte Verfahren (Valeur)

- 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



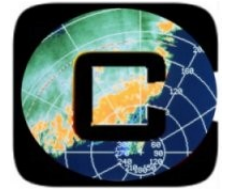
# Ausgewählte Verfahren (Panjwani)



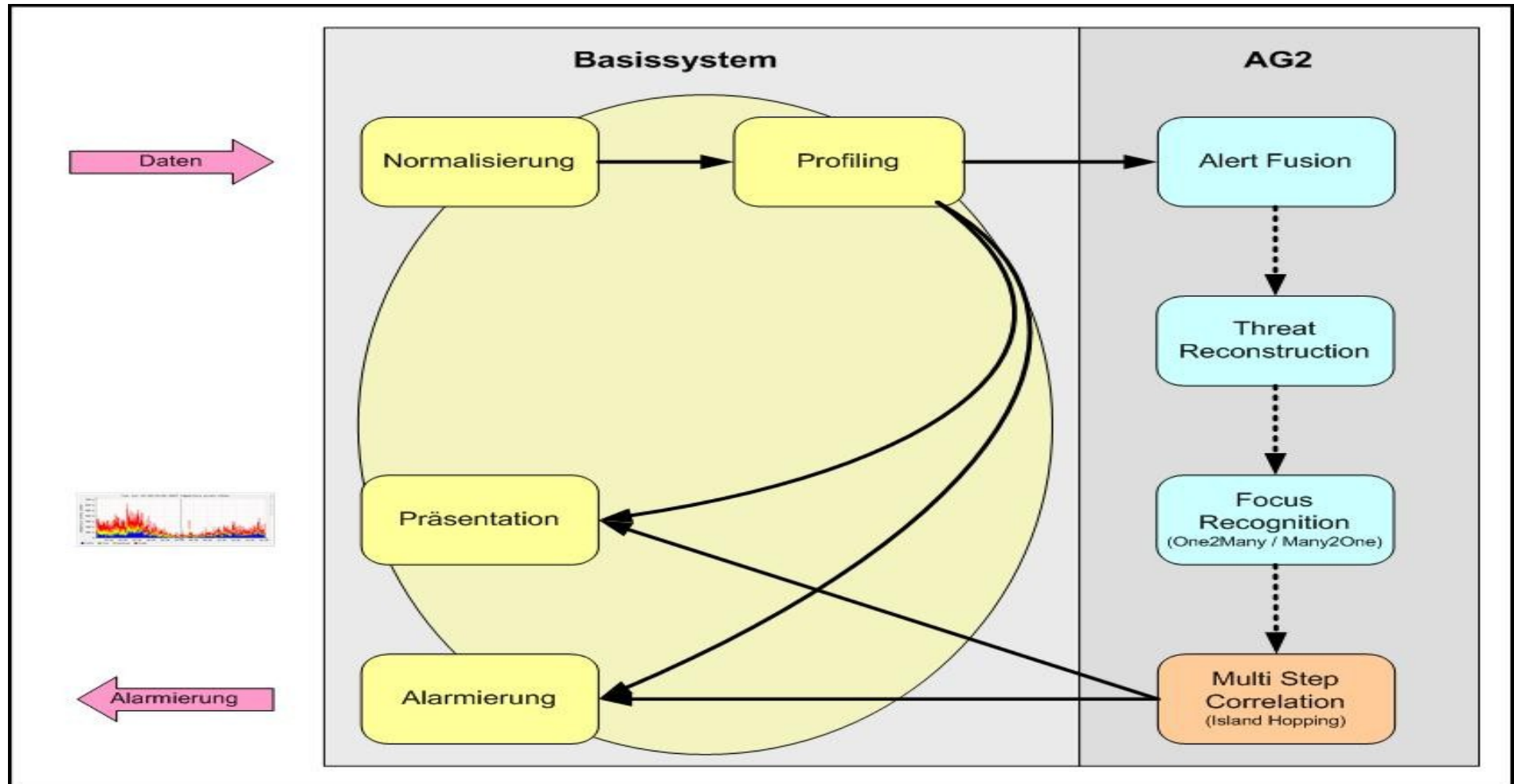
<b>■ Anz. Pakete</b>	<b>Klassifikation</b>
$0 \leq n < 5$	<b>Port Scan / Ping Scan (ICMP)</b>
$5 \leq n \leq 12$	<b>Probe</b>
$12 < n$	<b>Attack</b>

→ Einsatz zur Grobklassifikation





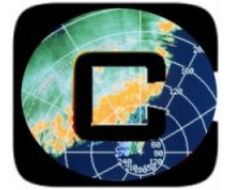
# Integration in Carmentis







# Algorithmus Thread Reconstruction

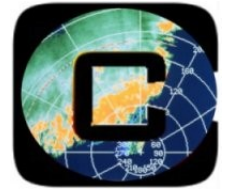


## ■ One2One

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, ...)





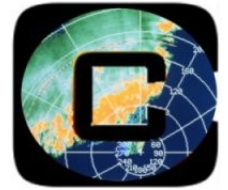
# Algorithmus Focus Recognition

## ■ One2Many

<b>E1</b>		<b>E2</b>		<b>...</b>		<b>En</b>
<b>src_ip</b>	<b>=</b>	<b>src_ip</b>	<b>=</b>	<b>...</b>	<b>=</b>	<b>src_ip</b>

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





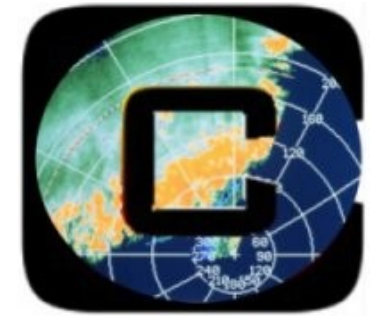
# Algorithmus Focus Recognition

## ■ Many2One

<b>E1</b>		<b>E2</b>		<b>...</b>		<b>En</b>
<b>dst_ip</b>	<b>=</b>	<b>dst_ip</b>	<b>=</b>	<b>...</b>	<b>=</b>	<b>dst_ip</b>

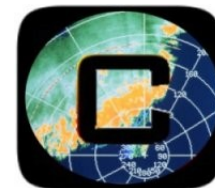
- Time window      120 seconds
- Threshold        configurable
- Start time         $\text{Min}(e1.st, en.st)$
- End time           $\text{Max}(e1.et, en.et)$
- Weitere Klassifikation  
(scanning, ...)





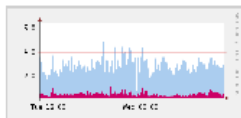
# Ergebnisse



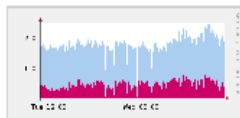


# Detaillierte Analyse

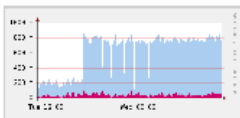
TCP



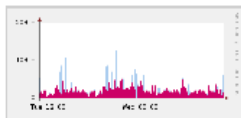
UDP



ICMP

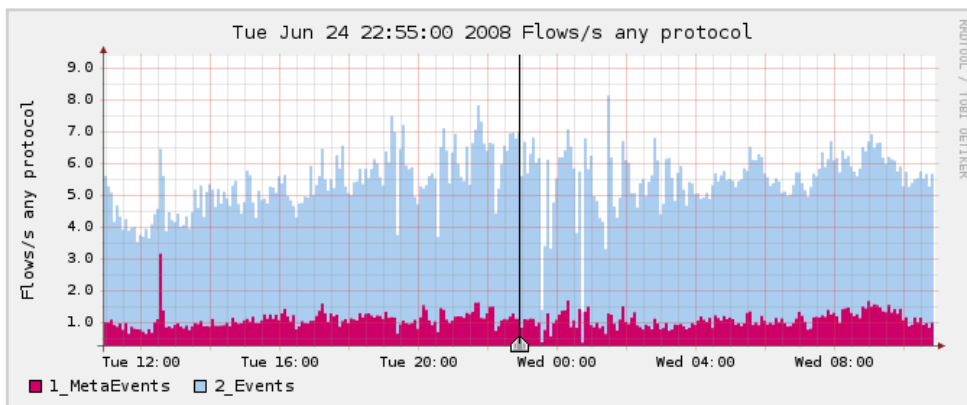


other



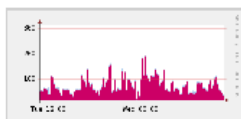
Profileinfo:

Type: continuous  
 Max: unlimited  
 Exp: never  
 Start: May 07 2008 - 12:00 CEST  
 End: Jun 25 2008 - 10:55 CEST

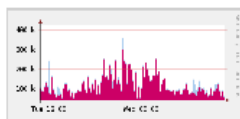


t\_start: 2008-06-24-22-55  
 t\_end: 2008-06-24-22-55

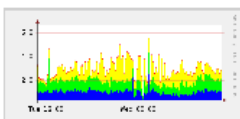
Packets



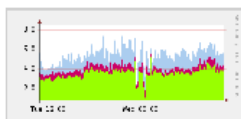
Traffic



Impacts



Rating



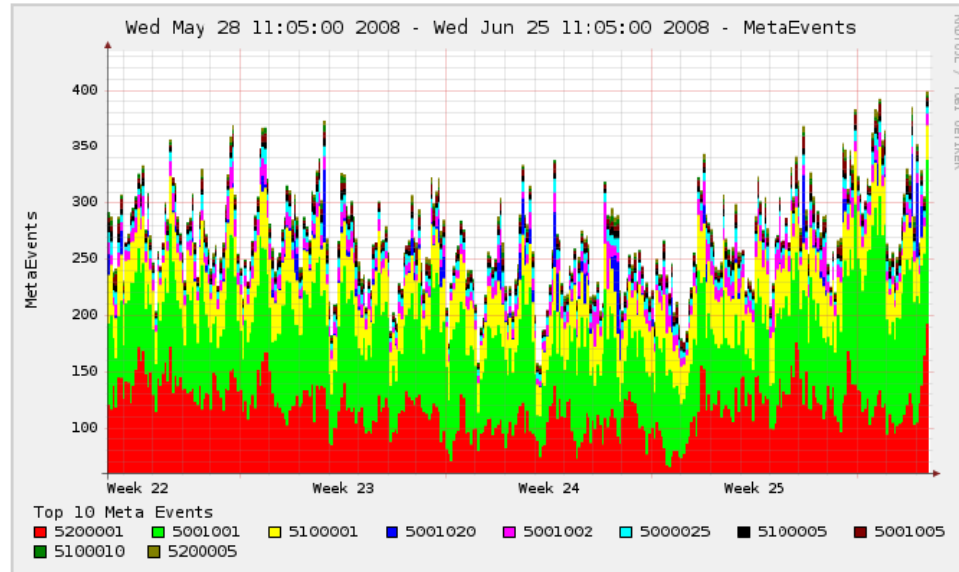
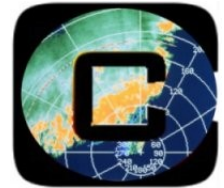
Select  Display:  << < | ^ > >> >|

Lin Scale  Stacked Graph  
 Log Scale  Line Graph

## 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:
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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  MetaEvents

now  24 hours

Track MetaEvent:

Skip MetaEvent:

Display

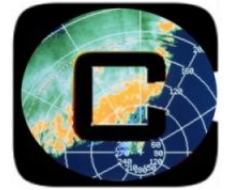
Y-axis:  Linear  Log

Type:  Stacked  Line

## Top 10 Statistics

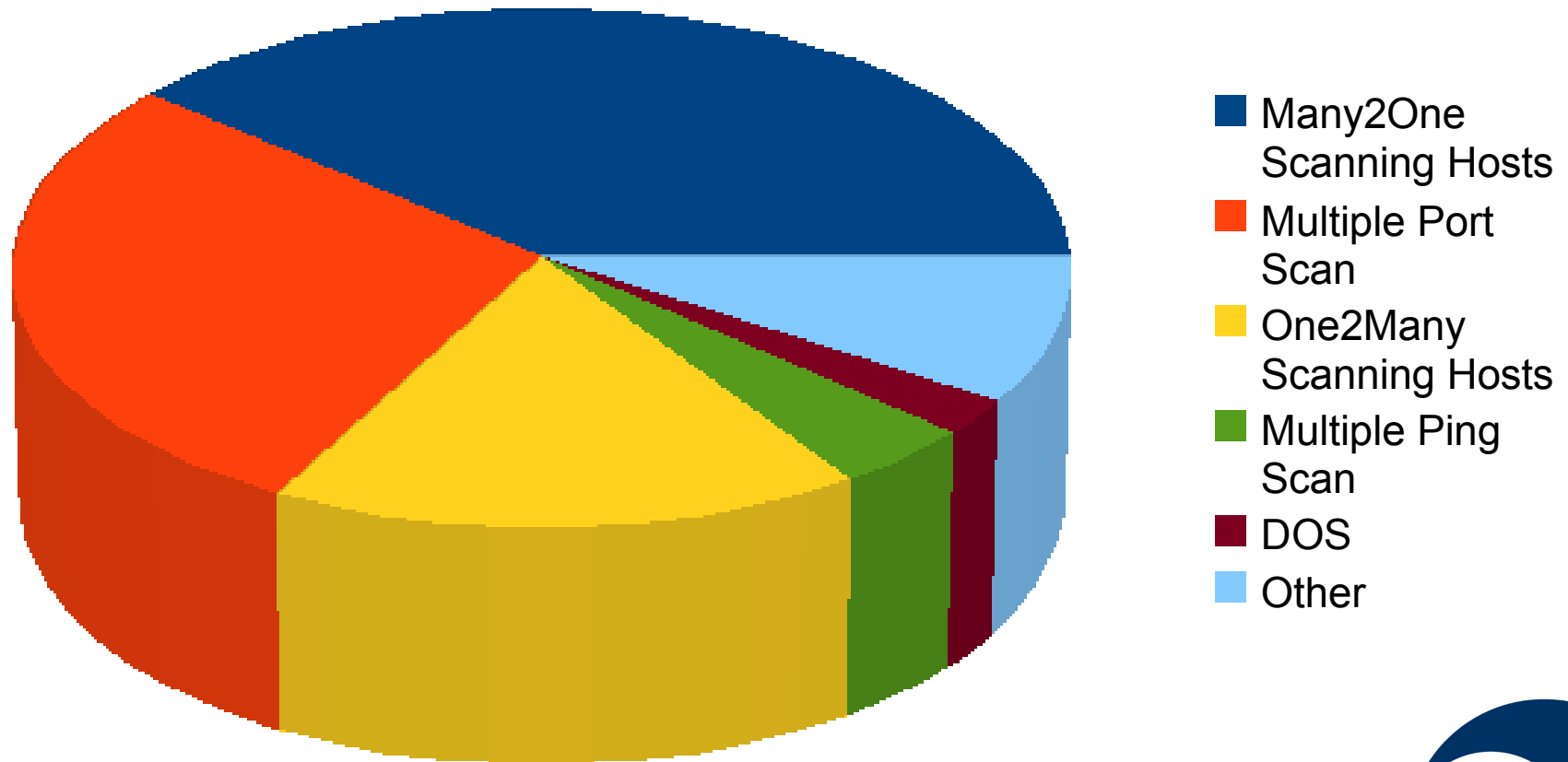
Rank	ID	Count	Info
1	5200001	35822	"Many2One Scanning Hosts"
2	5001001	31860	"Multiple Port Scan"
3	5100001	9198	"One2Many Scanning Hosts"
4	5001020	2751	"Multiple Malware Download"
5	5001002	2583	"Multiple Ping Scan"

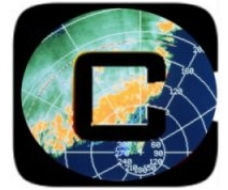
# Erste Ergebnisse



## Aggregated Events

2008-05-08 - 2008-06-04



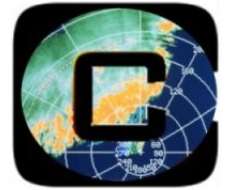


# Erste Ergebnisse

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





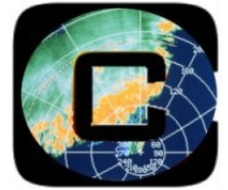


# Ausblick

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



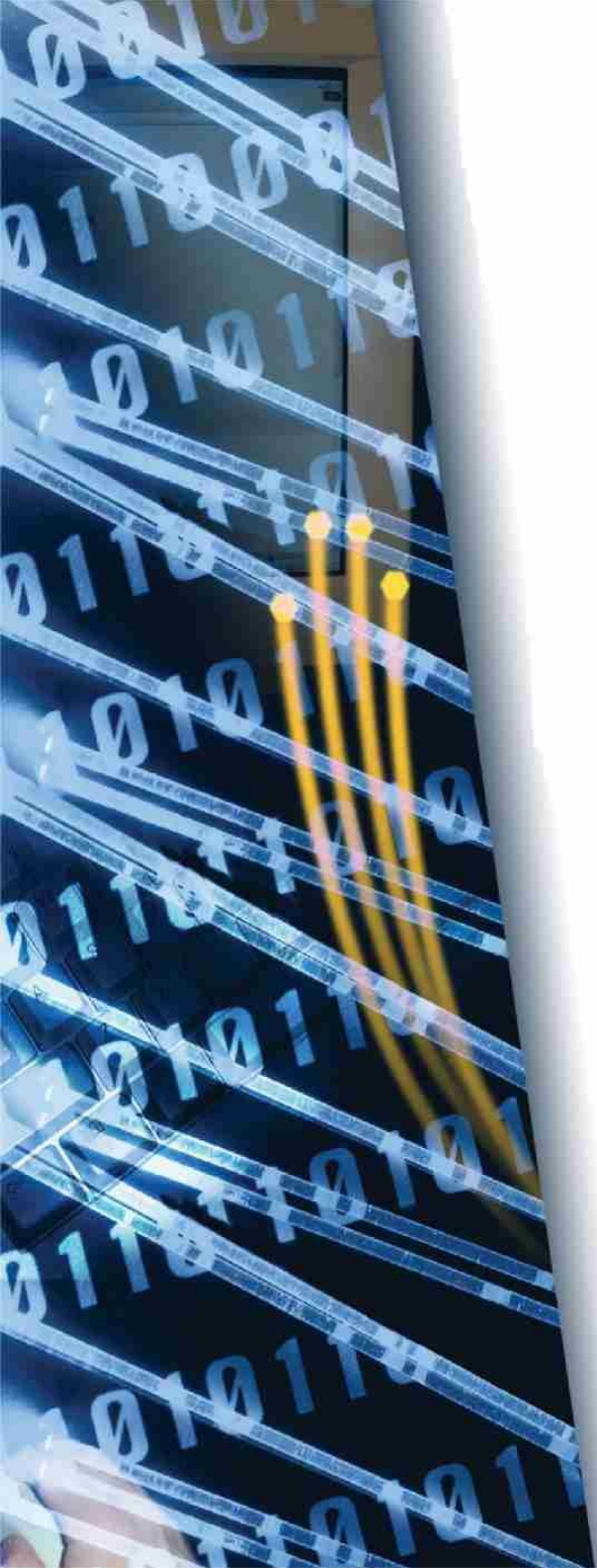
# Kontakt



**Till Döriges <[doerges@pre-sense.de](mailto:doerges@pre-sense.de)>**

**PRESENSE Technologies GmbH**

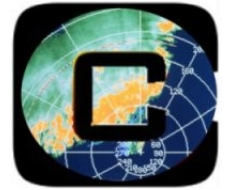




# Anhang



# Conficker-Wurm



## ■ Entdeckt durch einfache Aggregationsverfahren

