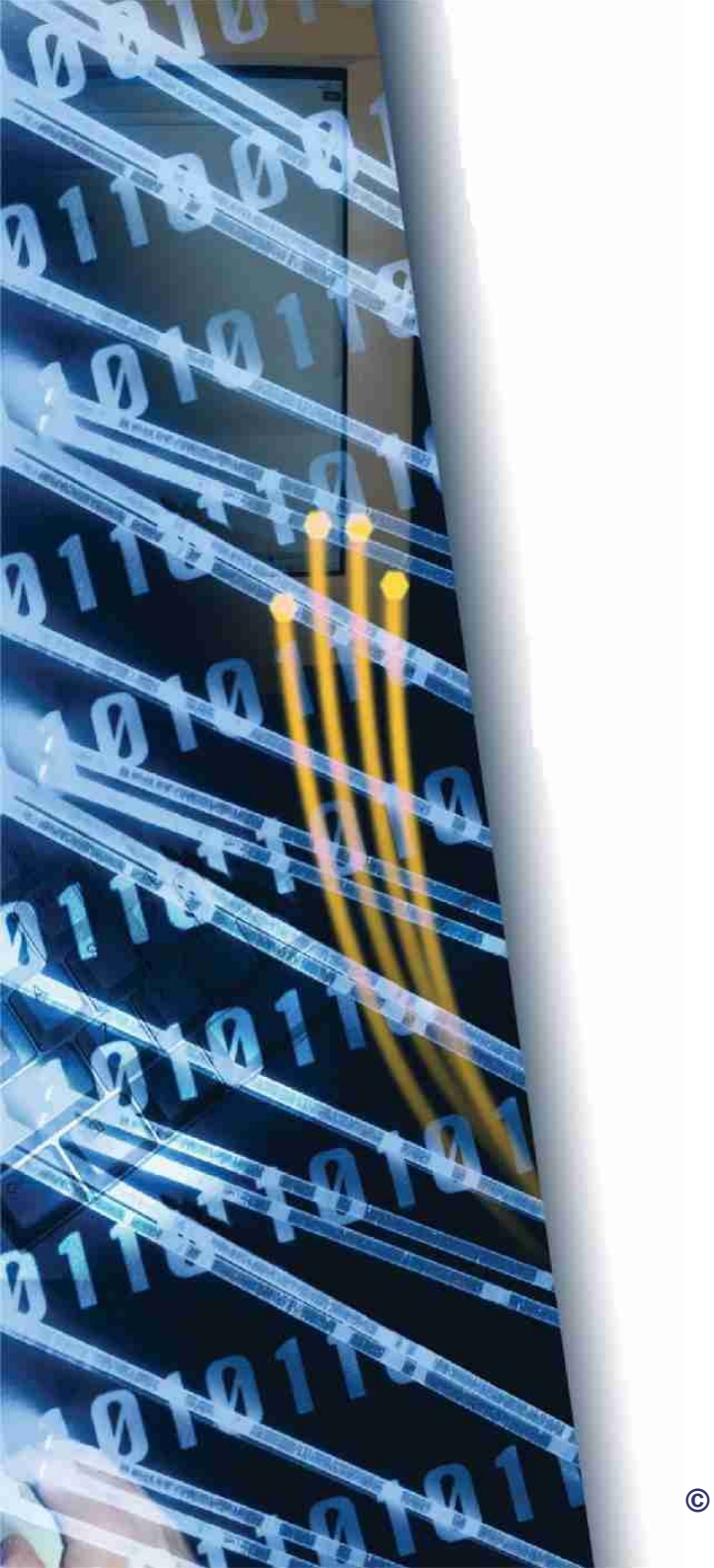


Event Aggregation for Early Warning Systems

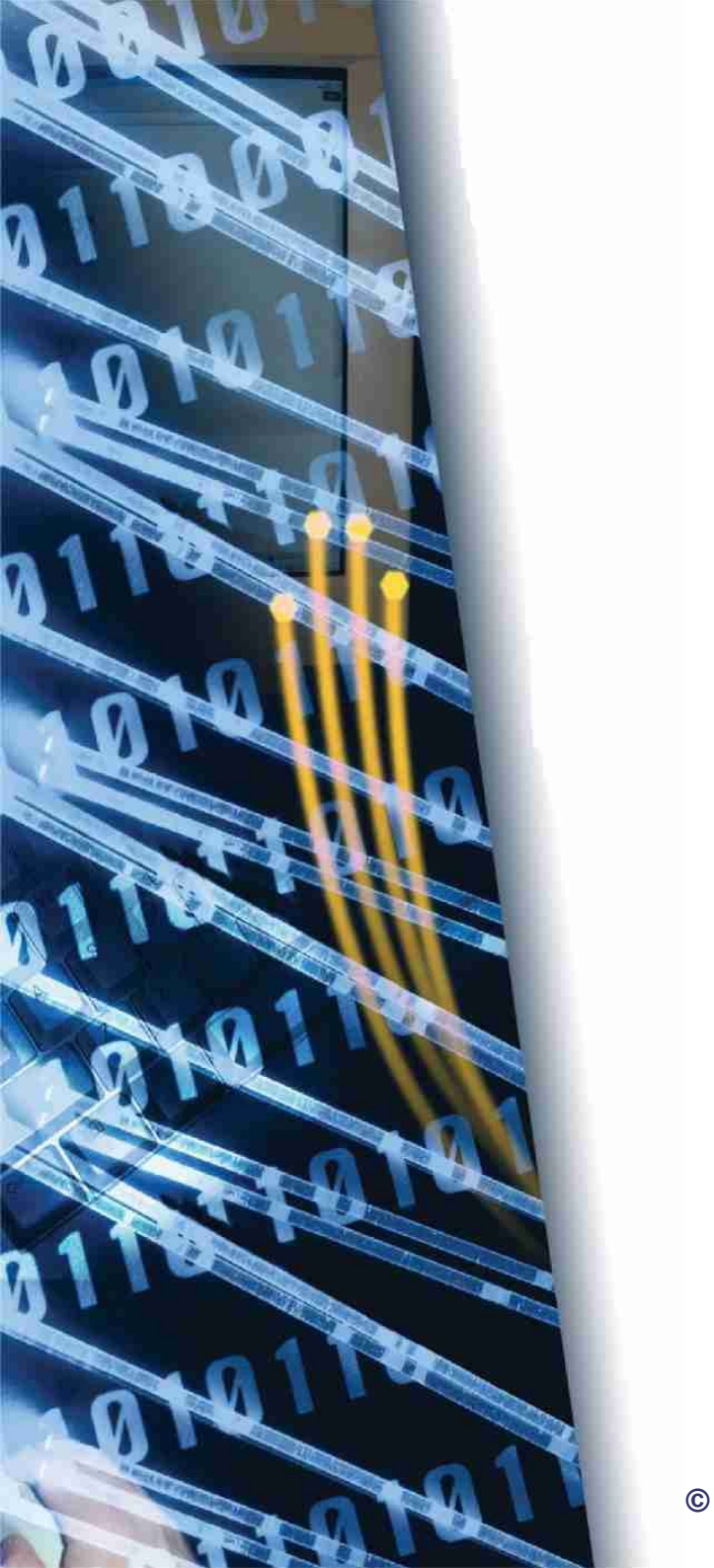
Till Dörges

PRESECURE® Consulting GmbH

Outline / ToC

- Motivation
- Definitions
- CarmentiS
- Aggregation for CarmentiS
- Implementation
- First Results / Outlook

PRESECURE® Consulting GmbH



Motivation

PRESECURE®
Consulting GmbH

Motivation / Problem statement

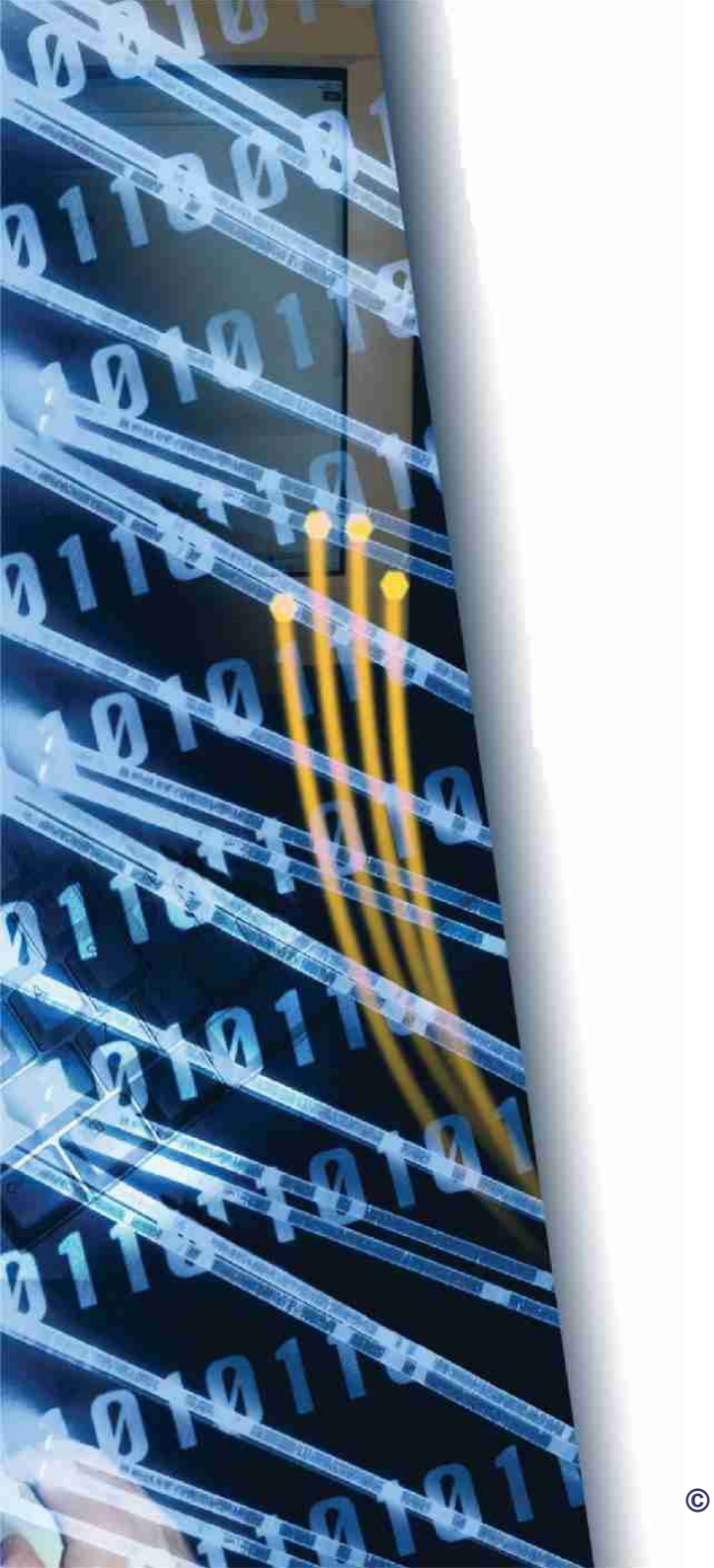
- **Networks are critical resources**
  - Certain things are nice to know in advance
  - Monitoring important & necessary
- **“Bad” traffic possibly hard to spot**
  - base-rate fallacy
  - unknown malicious activity
- **Process large amounts of data / events**
- **More than just Network Information for EW**
- **How to determine (Network) status**
- **When to warn?**

PRESECURE® Consulting GmbH

Towards solution(s)

- Monitoring
- Pre-classify traffic (Honeypots etc.)
- Better representation of data
- Reduce data to by analyzed by Humans
  - Aggregation
  - Correlation
- ...

PRESECURE® Consulting GmbH



Definitions

PRESECURE®
Consulting GmbH

Definitions

- **Early Warning**

  "In case of perceptible indicators and (still) a low number of victims, or none, information must be distributed to help others – not yet victims – including response organisations in order to avoid a major crisis!"

  (Kossakowski, 2005)

- **More "intuitive" definition problematic**

PRESECURE® Consulting GmbH

Definitions

- **Situational Awareness**
  - Provide enough Information
  - For given environment / scenario
  - Enable informed decisions
  - Basis for Early Warning

PRESECURE® Consulting GmbH

Definitions

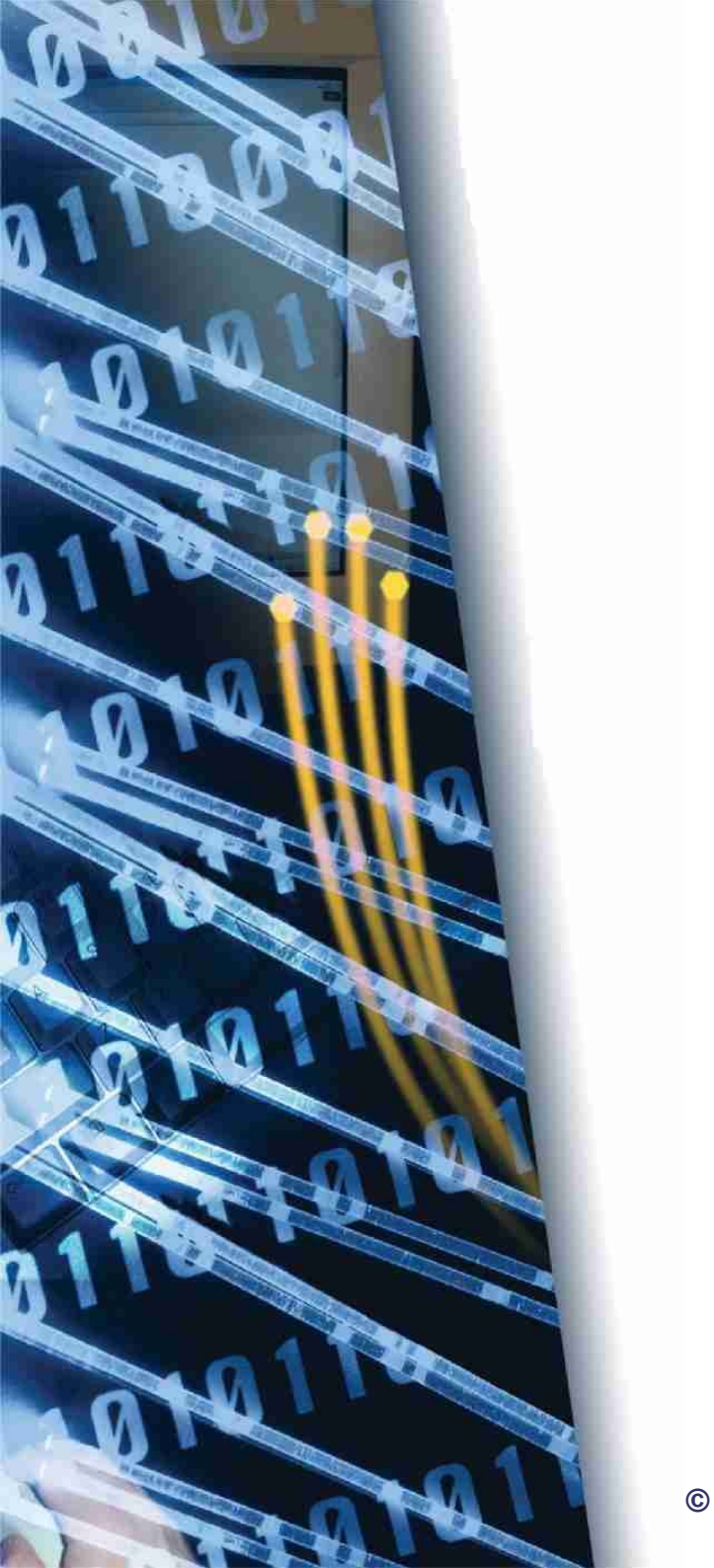
- **Correlation**
  - Statistics / probability theory
  - Relationships (correlation coefficients) between different variables
- **Aggregation**
  - Combine single events
  - Meta events
- **Sometimes confused**

PRESECURE® Consulting GmbH

Existing Tools / Solutions

- **Different Types**
  - Enterprise (Tivoli, ...)
  - Specialized (Arbor, ArcSight, ...)
  - Open Source (OSSIM, SEC, ...)
  - Custom (CarmentiS, ...)
  - Dashboards
- **Not a complete overview!**

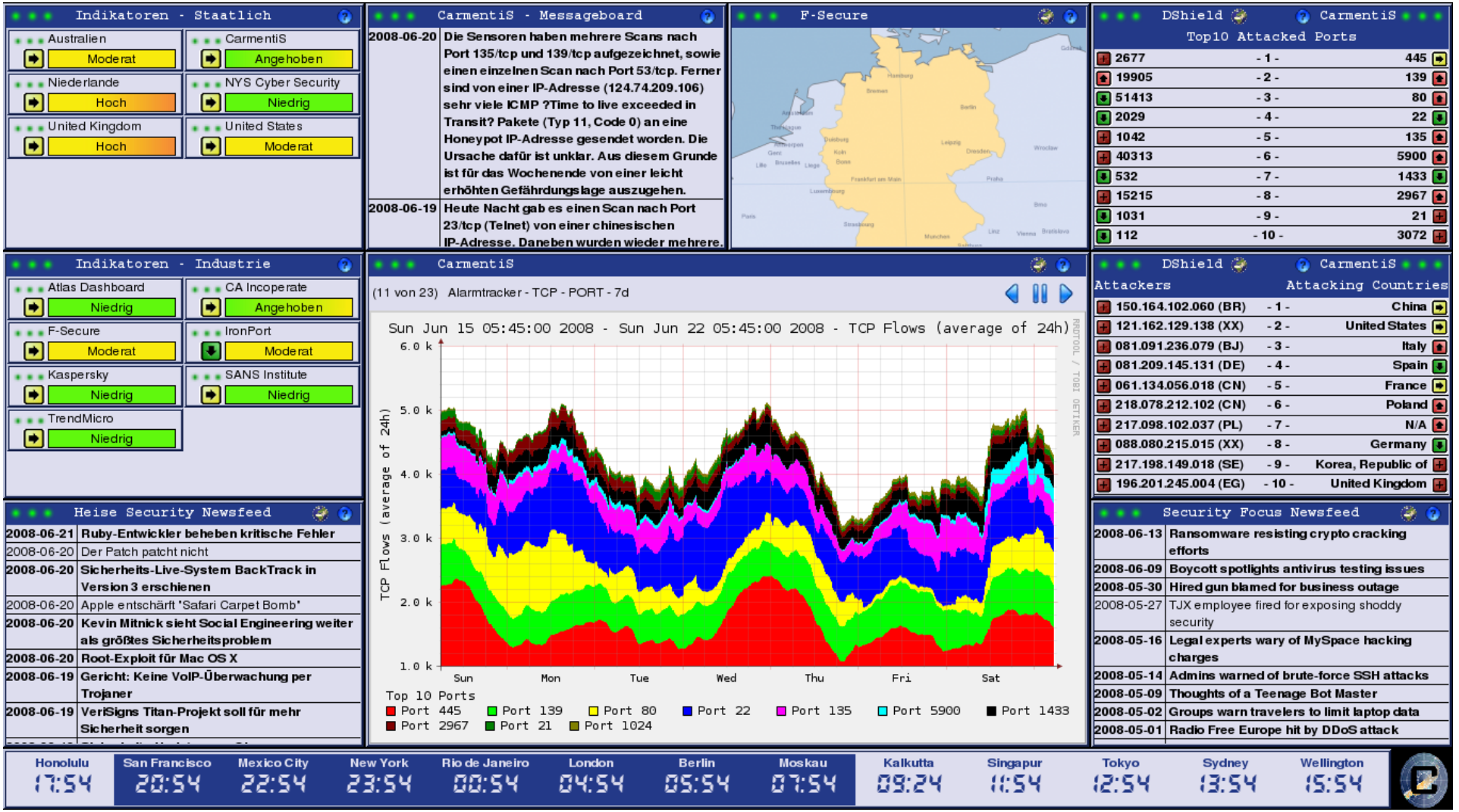
PRESECURE® Consulting GmbH



CarmentiS

PRESECURE®
Consulting GmbH

CarmentiS Security Dashboard

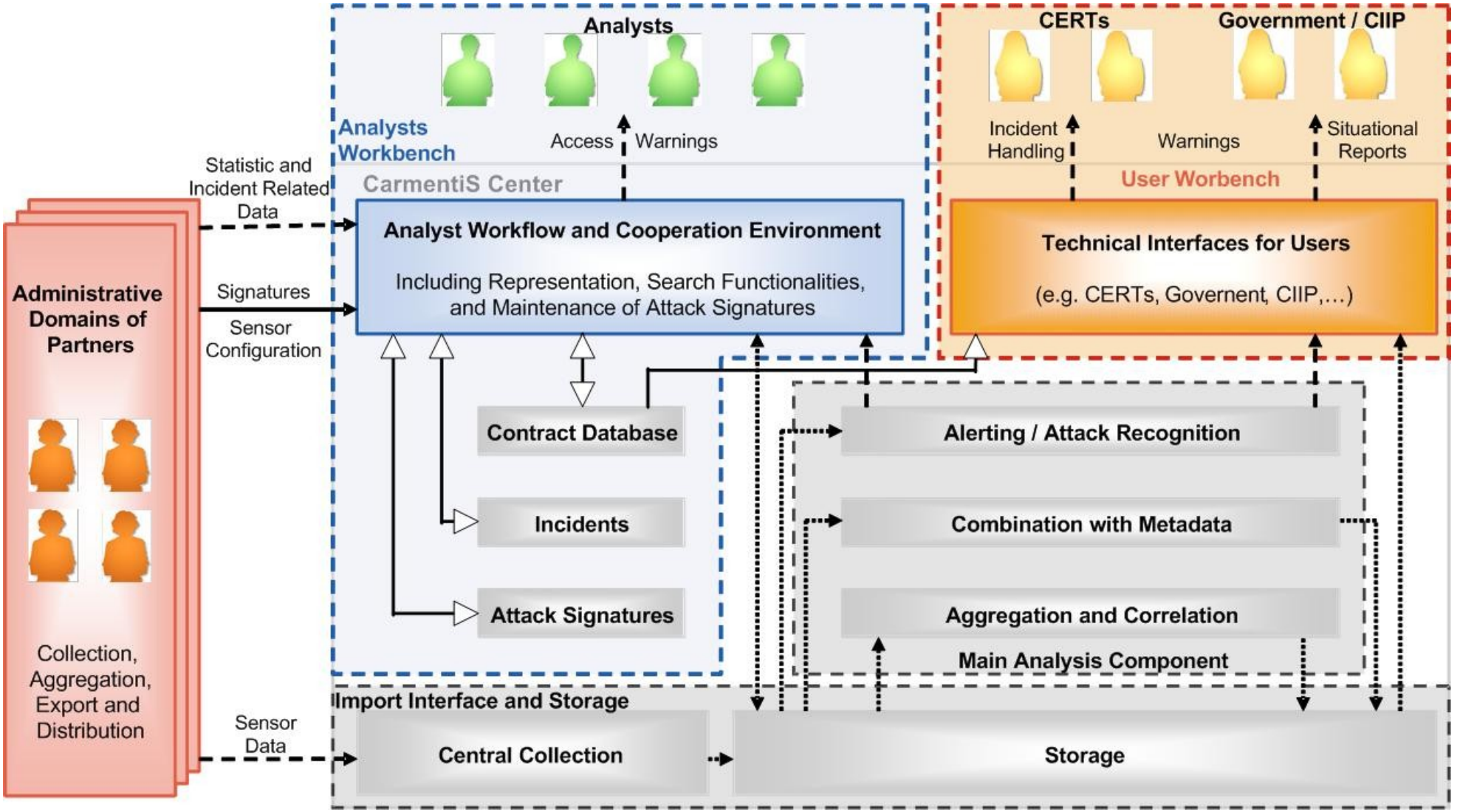


CarmentiS at a glance

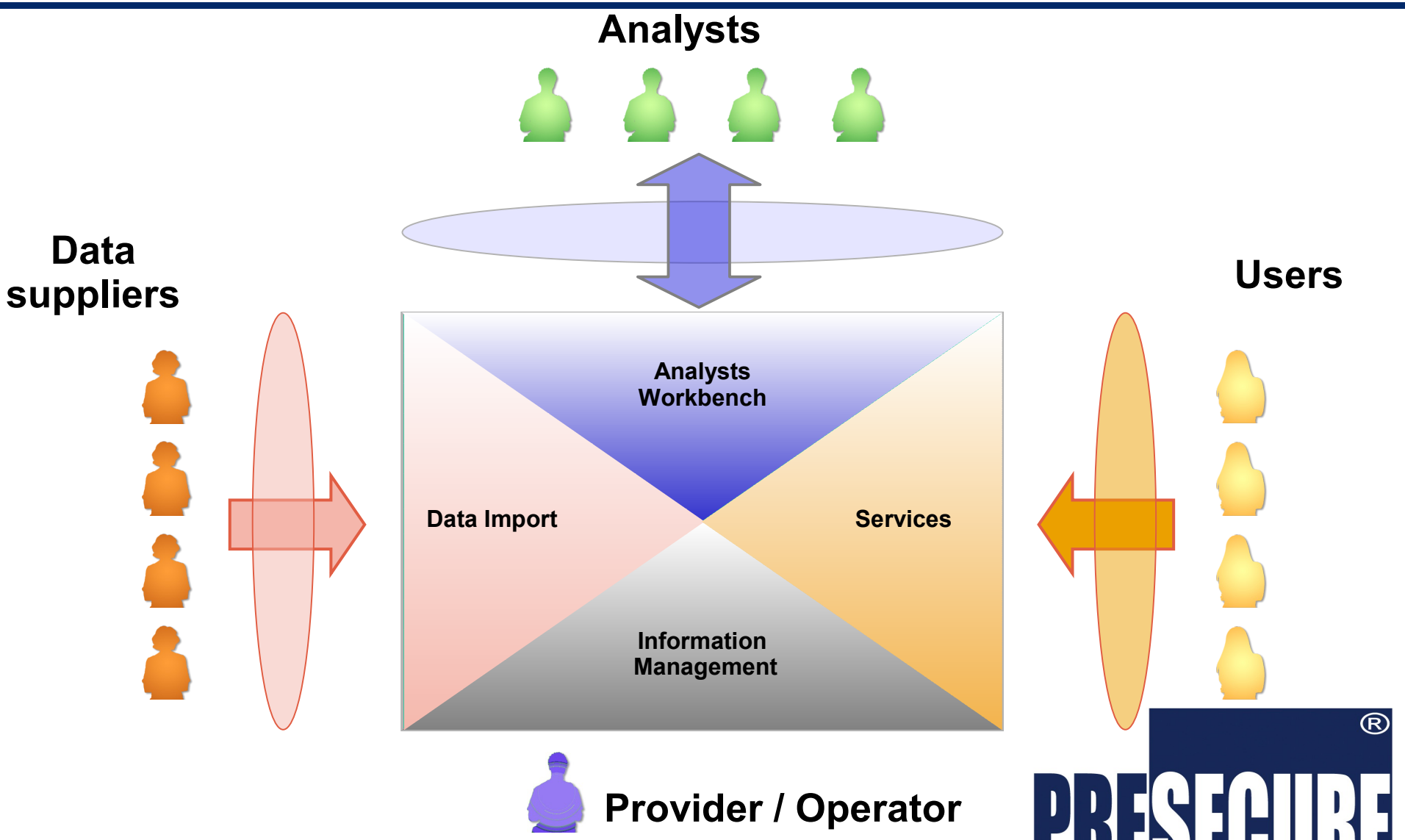
- **Project by BSI and CERT-Verbund**
- **Early Warning**
- **Situational Awareness**
- **Open Source based**
  - NfSen/Nfdump
  - Snort, Argus, ...
- **Cooperative approach**
  - Collaboration / Exchange
  - Autonomous data suppliers (trust)
- **Quick results wanted**

PRESECURE® Consulting GmbH

Architecture

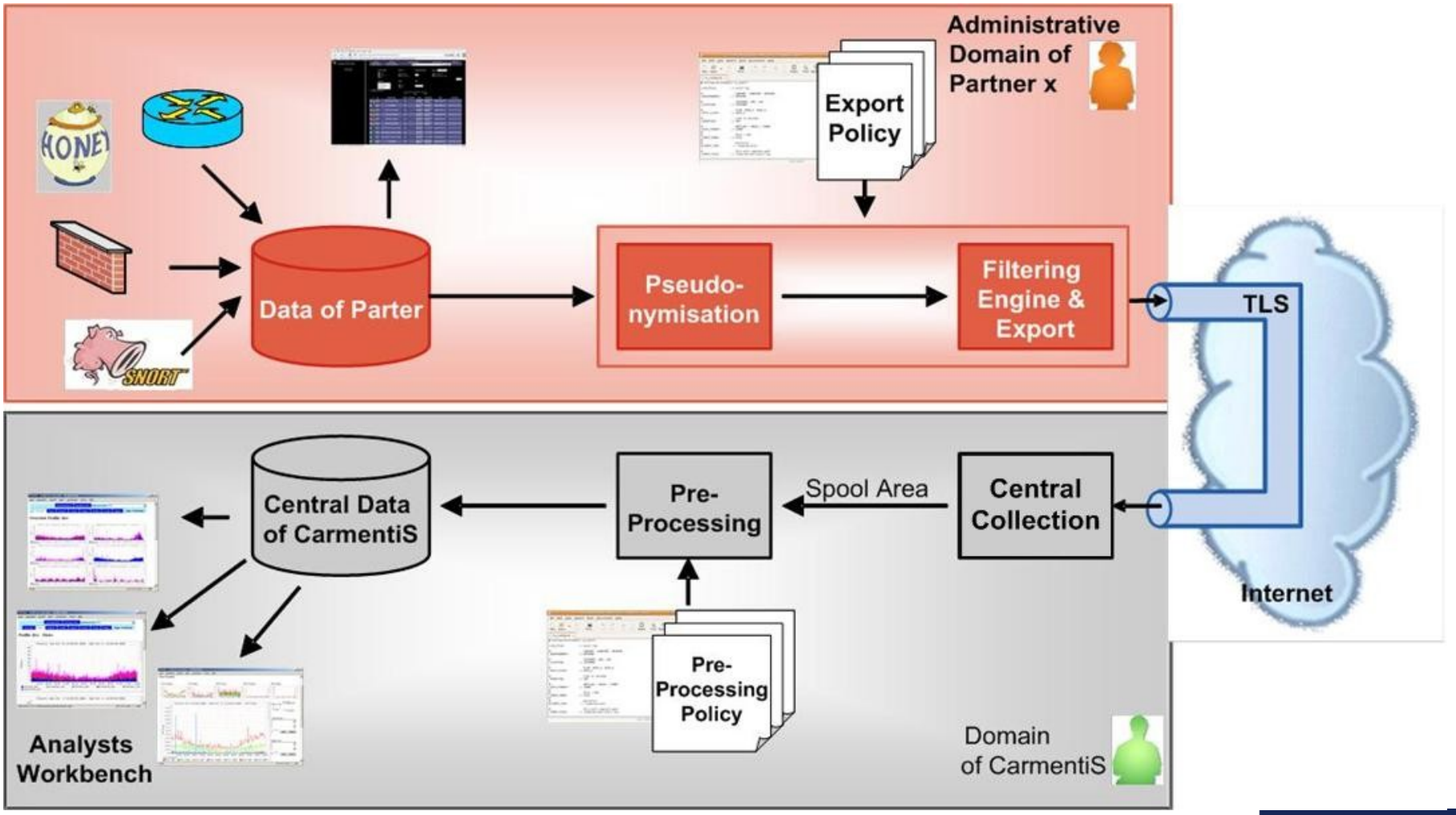


Framework and Roles



PRESECURE Consulting GmbH

Data collection



PRESECURE Consulting GmbH

Data collection

- **Data suppliers fully control their data**
  - Filtering
  - Pseudonymization / Anonymization
- **Data origins**
  - Dark nets
  - Production networks
  - Honeypots
- **Sensors**
  - Software
  - Appliance

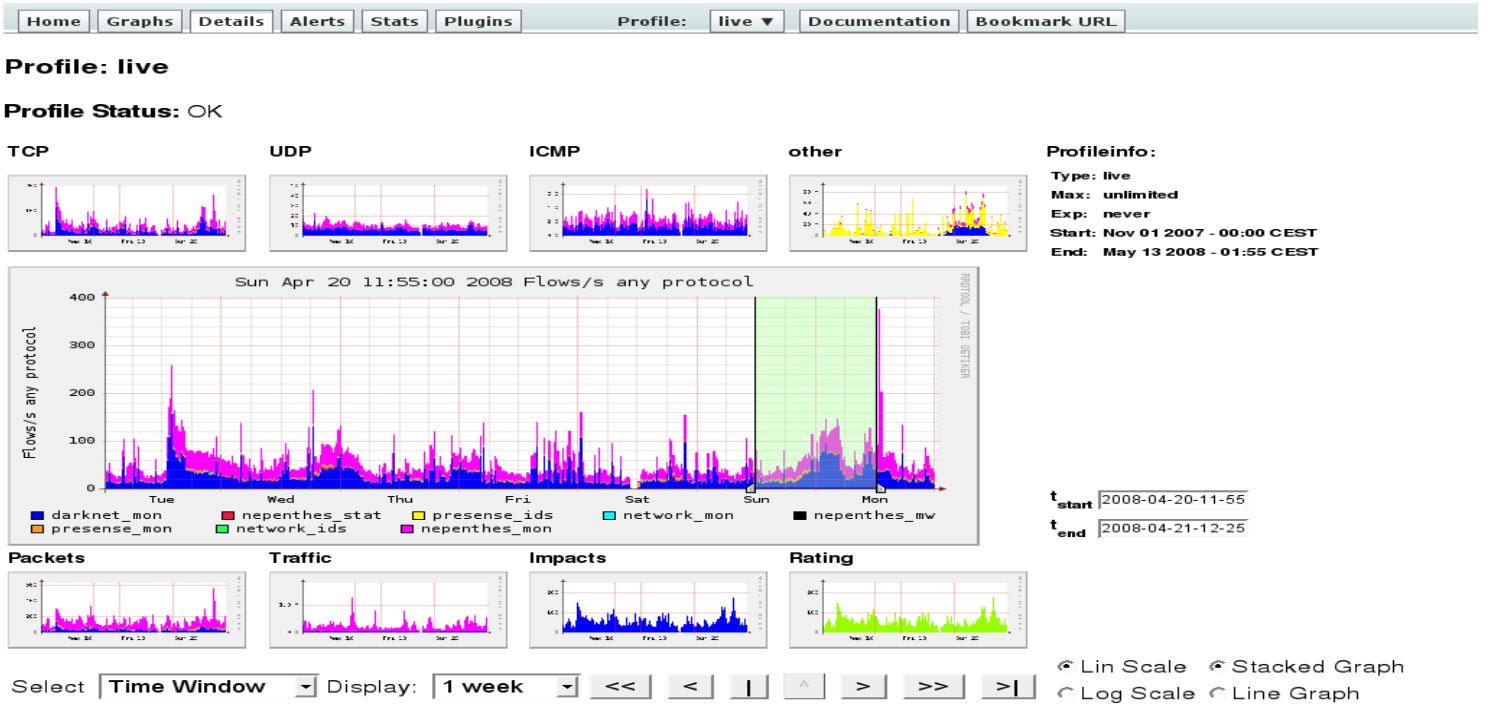
PRESECURE® Consulting GmbH

Data types

- **Data types**
  - Netflows (v5, v7)
  - Argus
  - IDS (Snort)
  - Malware (Nepenthes)
  - Exploits (Argos)
  - Meta events (Aggregation)
  - ...

PRESECURE® Consulting GmbH

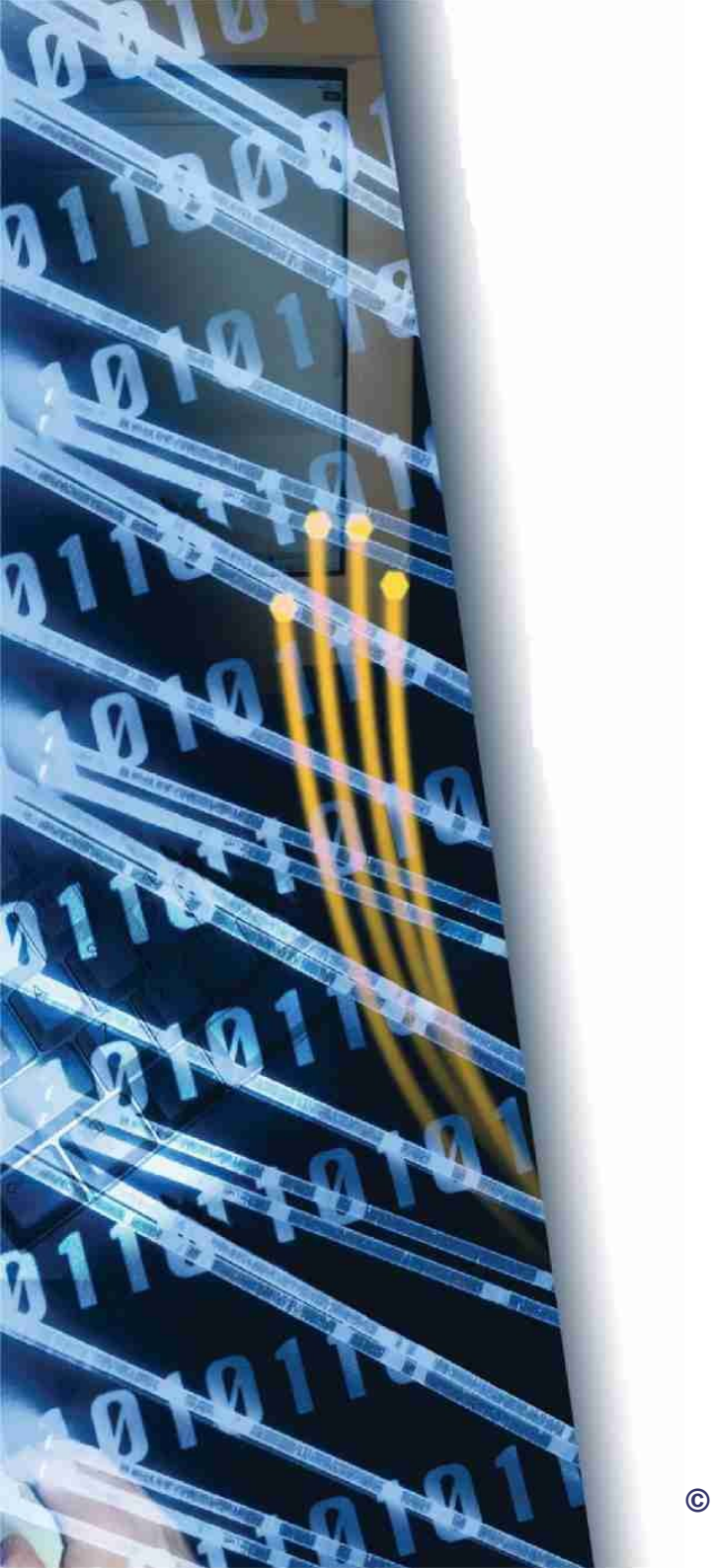
Analysts' Interface



Statistics timeslot Apr 20 2008 - 11:55 - Apr 21 2008 - 12:25

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
nepenthes_mon	2.6 M	2.1 M	346.1 k	86.6 k	438.0	9.2 M	8.7 M	353.8 k	86.8 k	462.0	3.1 GB	3.0 GB	126.5 MB	5.7 MB	273.1 kB
network_ids	9.1 k	7.5 k	1.4 k	145.0	0	0	0	0	0	0	0 B	0 B	0 B	0 B	0 B
presense_mon	204.9 k	204.3 k	586.0	27.0	0	1.3 M	1.3 M	614.0	27.0	0	74.0 MB	73.7 MB	295.4 kB	2.0 kB	0 B
nepenthes_mw	1.3 k	1.3 k	0	0	0	0	0	0	0	0	0 B	0 B	0 B	0 B	0 B
network_mon	56.3 k	54.4 k	767.0	1.1 k	0	79.3 k	77.3 k	844.0	1.1 k	0	5.5 MB	5.0 MB	396.7 kB	86.1 kB	0 B
presense_ids	4.4 k	1.9 k	826.0	44.0	1.7 k	0	0	0	0	0	0 B	0 B	0 B	0 B	0 B
nepenthes_stat	115.5 k	115.5 k	0	0	0	0	0	0	0	0	0 B	0 B	0 B	0 B	0 B
darknet_mon	3.1 M	2.4 M	586.9 k	102.5 k	961.0	3.6 M	2.9 M	596.4 k	103.1 k	961.0	341.0 MB	137.6 MB	195.9 MB	6.9 MB	610.1 kB

PRESECURE Consulting GmbH



Aggregation for CarmentiS

PRESECURE®
Consulting GmbH

Extend / enhance existing EW system

- **Different types of aggregation**
  - Data mining
  - Clustering
  - Rule based
  - ...
  - Hybrid approaches
- **Several approaches evaluated**

PRESECURE® Consulting GmbH

Requirements

- Flexibility
- Performance
- Scalability
- Quality of Results
- Integratable
- Availability
- Support for different data types

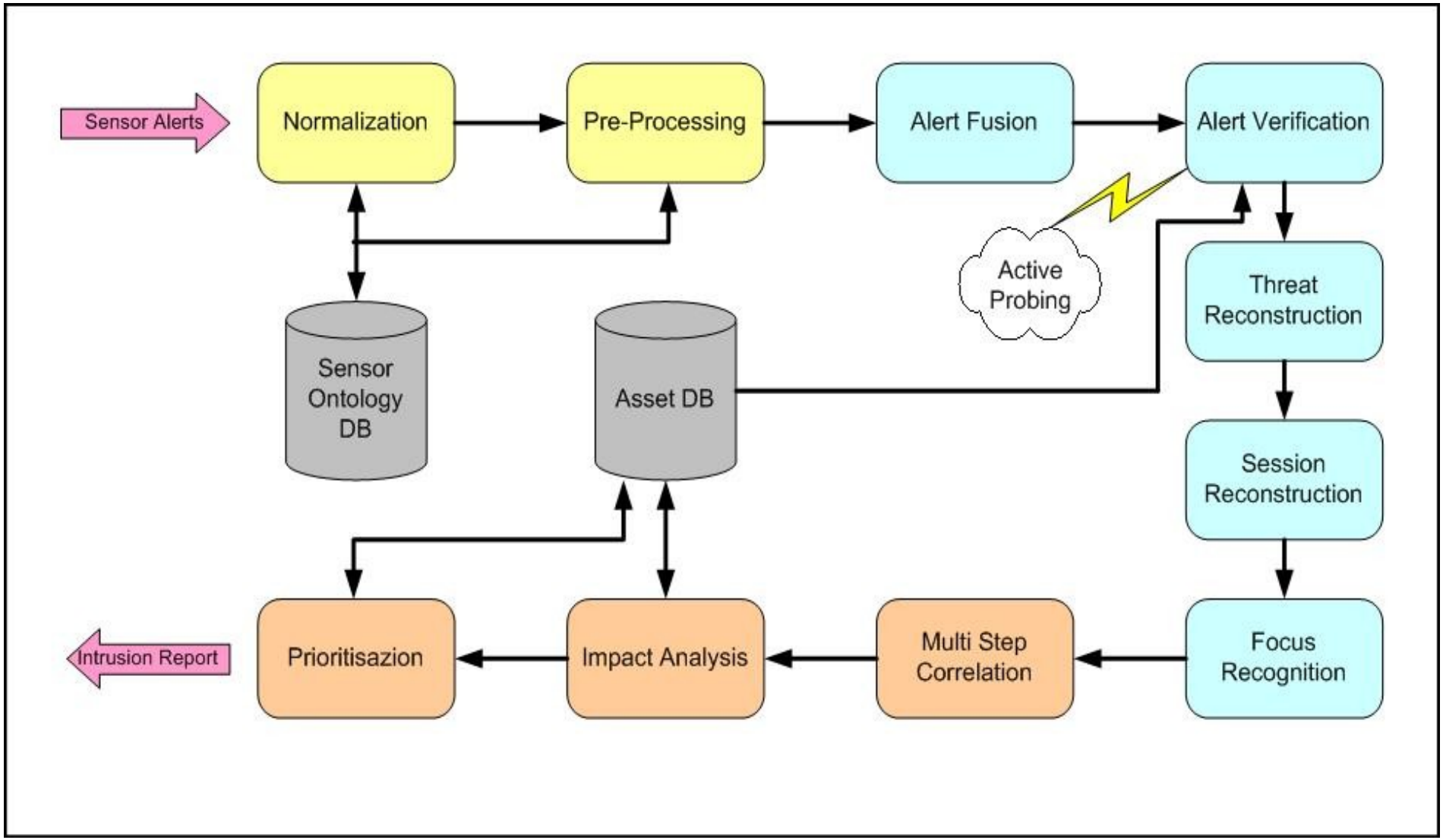
PRESECURE® Consulting GmbH

Chosen approaches

- 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

PRESECURE® Consulting GmbH

Chosen approach (Valeur)



Chosen approach (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**

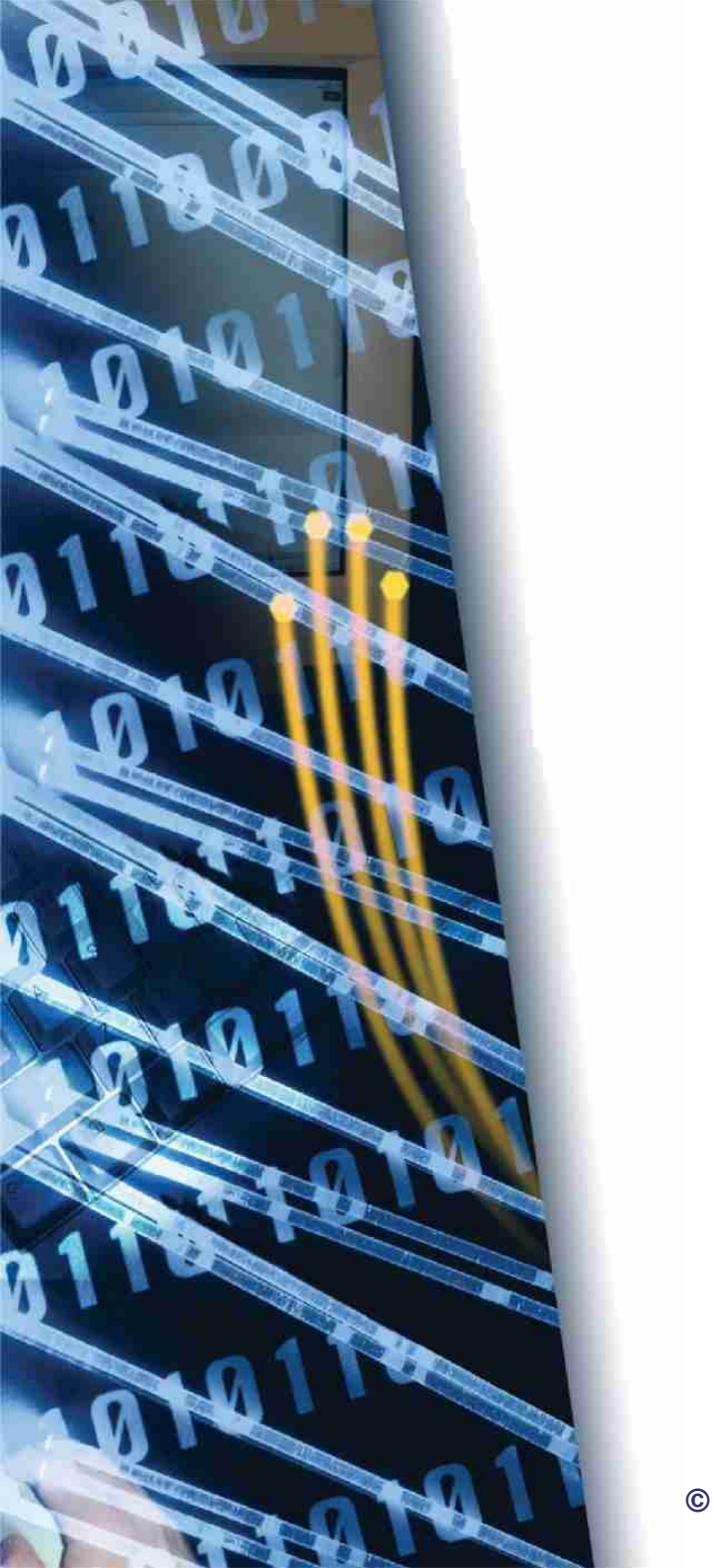
PRESECURE® Consulting GmbH

Chosen approach (Panjwani)

- No. Packets — Classification

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

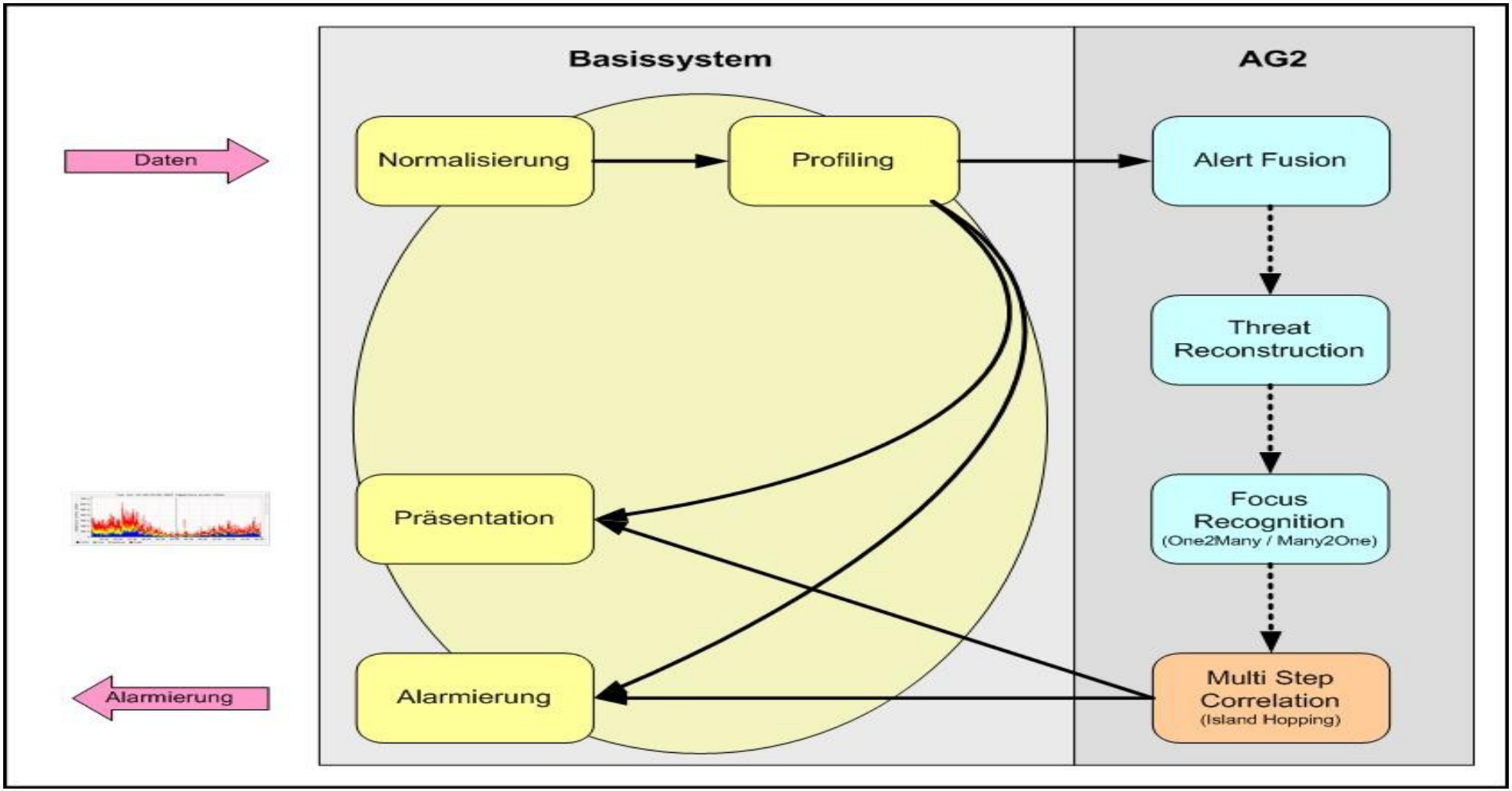
PRESECURE® Consulting GmbH



Implementation

PRESECURE®
Consulting GmbH

Integration into CarmentiS



Algorithm Alert Fusion

E1 E2

src_ip/port = src_ip/port

dst_ip/port = dst_ip/port

starttime + duration <= starttime(detectiontime)

PRESECURE® Consulting GmbH

Algorithm 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)
- Further classification (password guessing, exploit, ...)

PRESECURE® Consulting GmbH

Algorithm 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)
- Further classification (scanning, ...)

PRESECURE® Consulting GmbH

Algorithm 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)
- Further classification (scanning, ...)

PRESECURE® Consulting GmbH

Problems

- Introduction of meta events
- Biflows needed
- Extension of the representation layer
- Integration with other events / information
- Status information from previous time slice needed

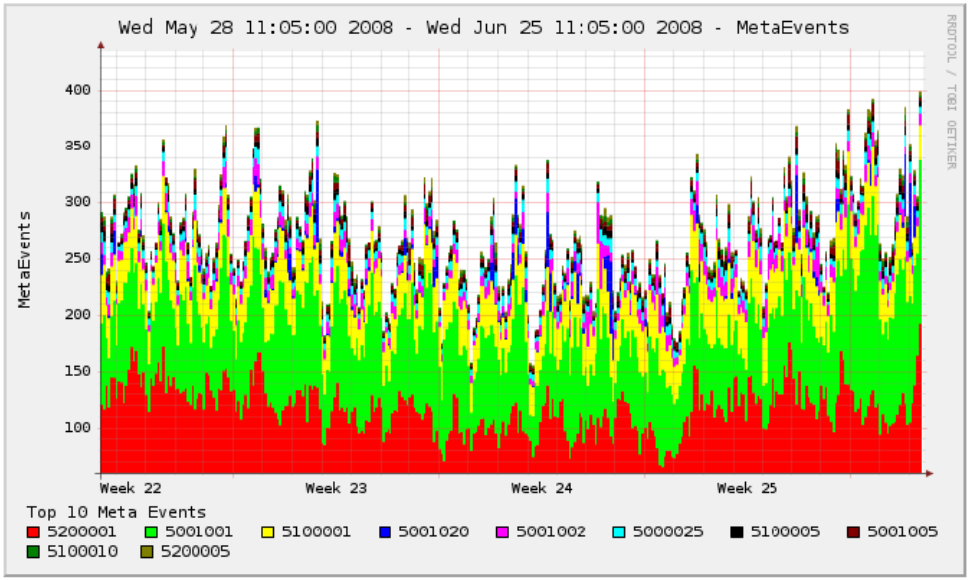
PRESECURE® Consulting GmbH

Detailed analysis

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 Overview



Show Top 10 MetaEvents

now 24 hours

Track MetaEvent:

Add Delete

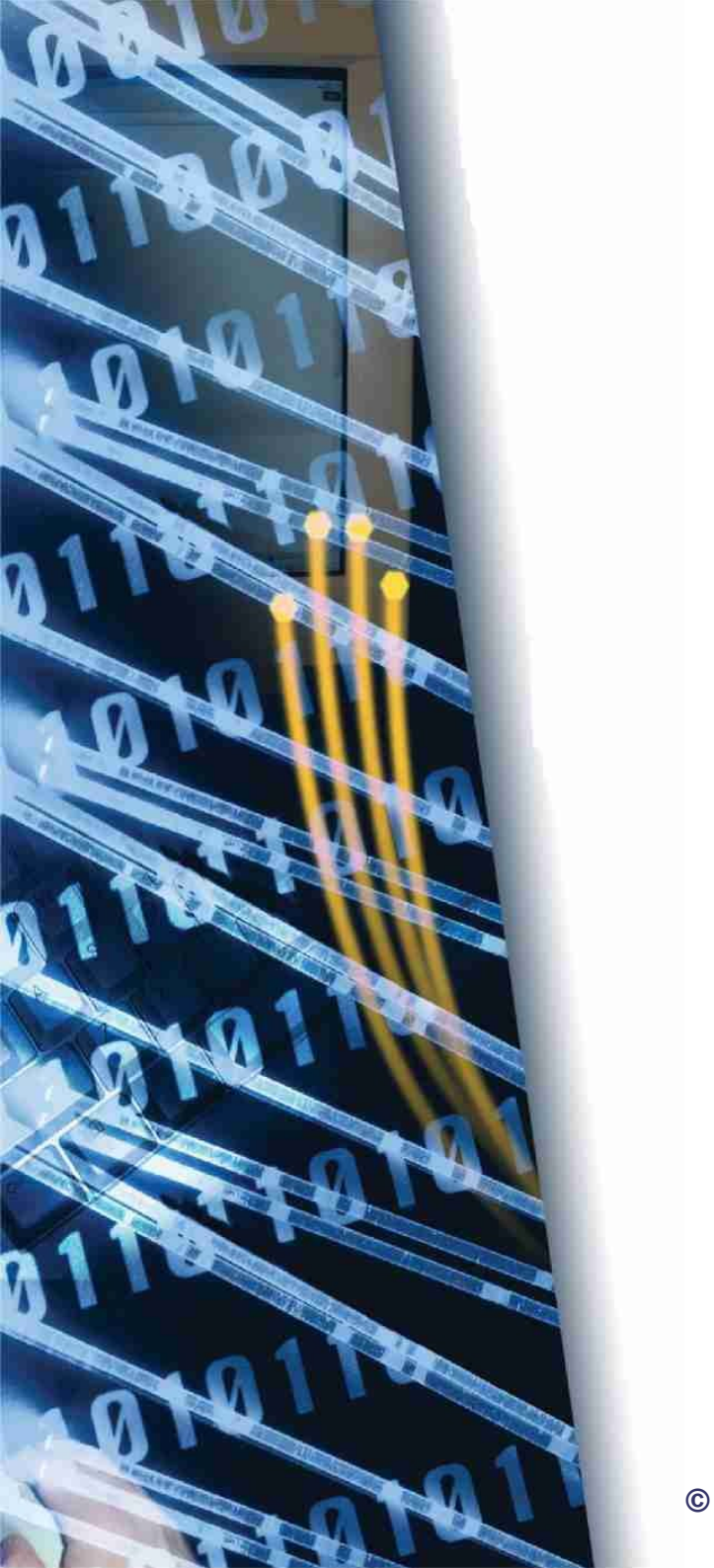
Skip MetaEvent:

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"



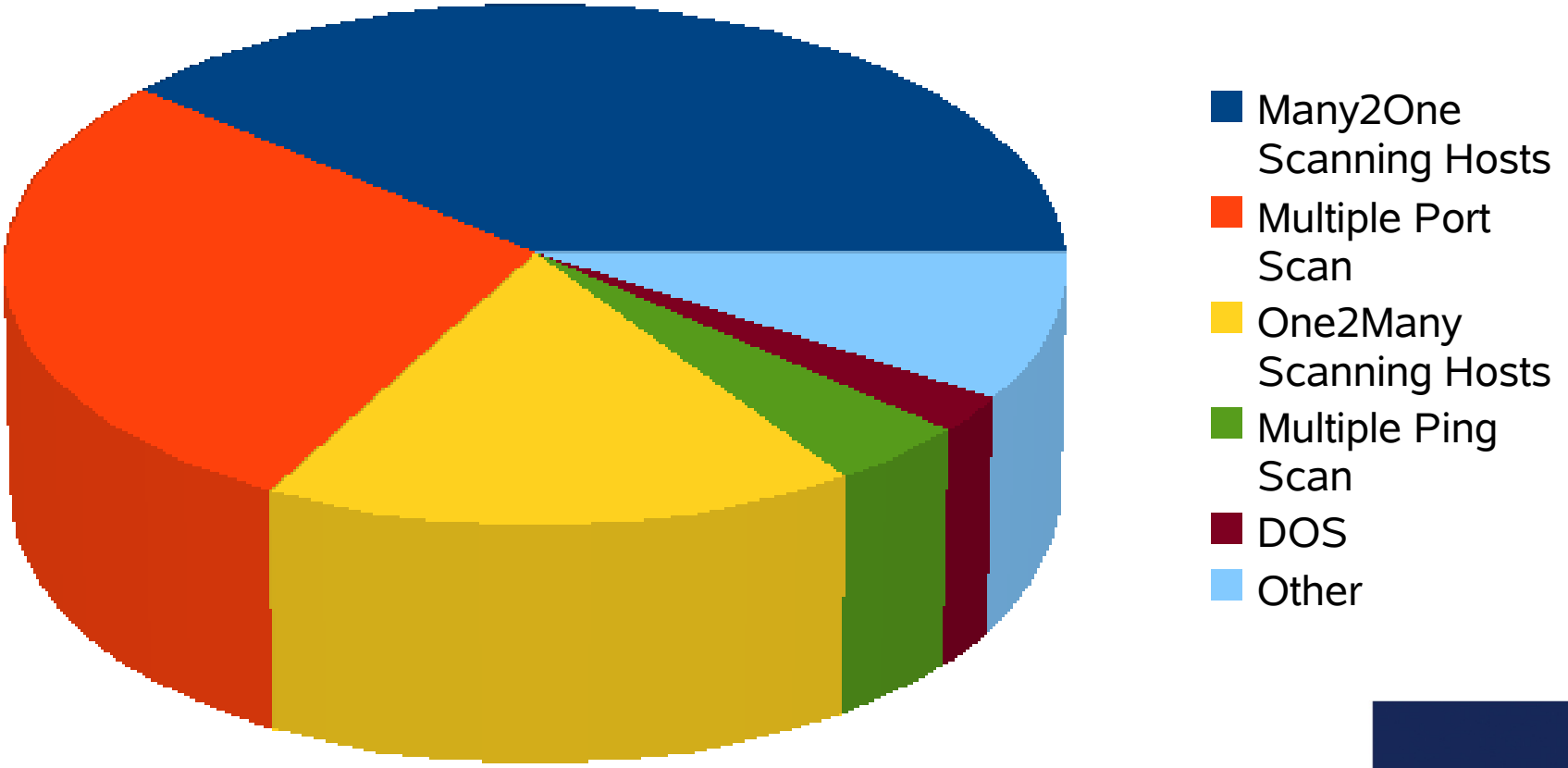
First Results

PRESECURE®
Consulting GmbH

First results

Aggregated Events

2008-05-08 - 2008-06-04



PRESECURE® Consulting GmbH

First results

- **A few months in production**
- **Reduction ratio**
  - ~ 11,87 %
- **Mostly scanning aggregated into meta events**
  - Many2One Scanning Hosts
  - Multiple Port Scan
  - One2Many Scanning Hosts

PRESECURE® Consulting GmbH

Outlook

- “Drilling” into the data
- Better GUI integration
- Tweak existing algorithms
- New algorithms

PRESECURE® Consulting GmbH

Contact

Till Dörges

td@pre-secure.de

- GnuPG
- 2048R / 0x22A13E69
- 2226 8447 3251 F6BE F8DC 6D4D 2F54 E55F

PRE-CERT

PRESECURE Consulting GmbH

https://www.pre-secure.com/

The End

Thanks!

Questions?

PRESECURE® Consulting GmbH