



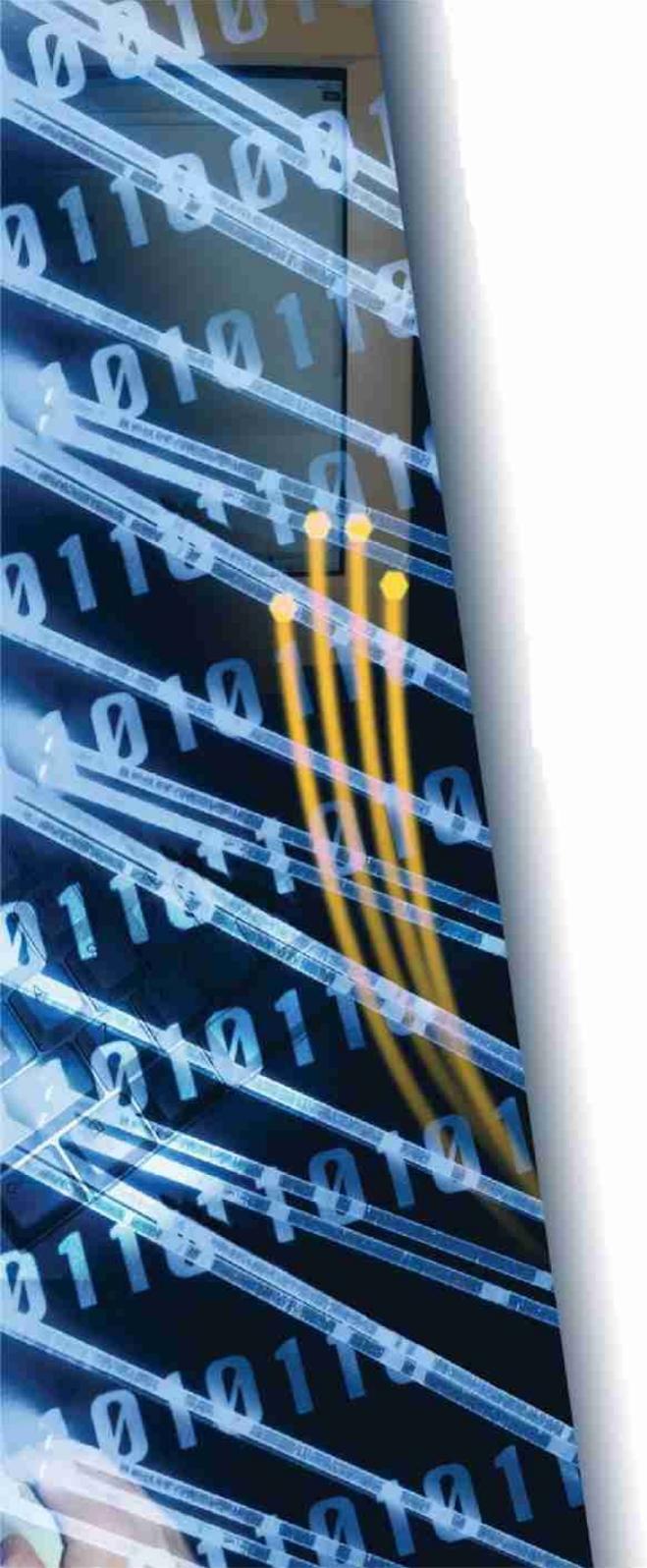
Event Aggregation for Early Warning Systems

Till Döriges



Outline / ToC

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



Motivation



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?**

Towards solution(s)

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





Definitions

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



Definitions

■ Situational Awareness

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

Definitions

■ Correlation

- Statistics / probability theory
- Relationships (correlation coefficients) between different variables

■ Aggregation

- Combine single events
- Meta events

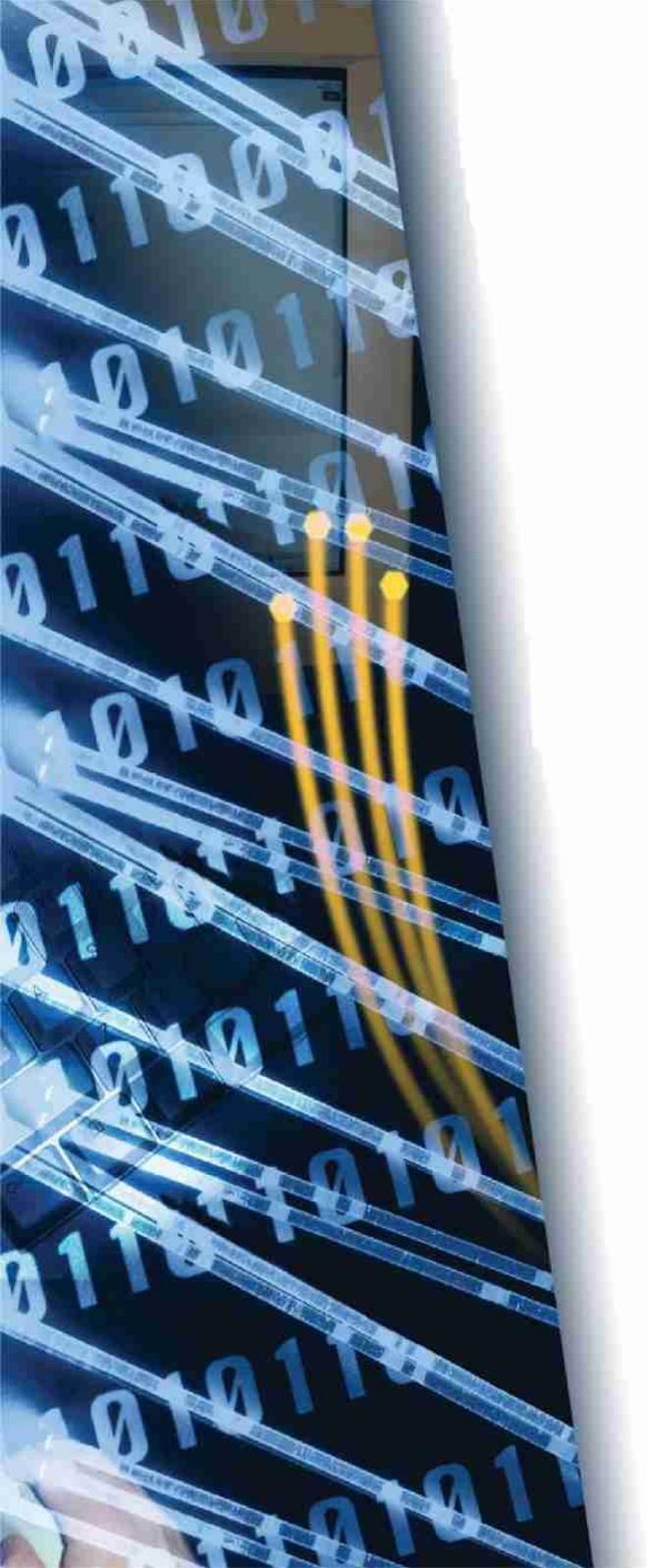
■ Sometimes confused

Existing Tools / Solutions

■ Different Types

- Enterprise (Tivoli, ...)
- Specialized (Arbor, ArcSight, ...)
- Open Source (OSSIM, SEC, ...)
- Custom (CarmentiS, ...)
- Dashboards

■ Not a complete overview!



CarmentiS

© 2000-2008 by PRESECURE Consulting GmbH

PRESECURE[®]
Consulting GmbH

CarmentiS Security Dashboard

Indikatoren - Staatlich

Australien	CarmentiS
Moderat	Angehoben
Niederlande	NYS Cyber Security
Hoch	Niedrig
United Kingdom	United States
Hoch	Moderat

CarmentiS - Messageboard

2008-06-20 Die Sensoren haben mehrere Scans nach Port 135/tcp und 139/tcp aufgezeichnet, sowie einen einzelnen Scan nach Port 53/tcp. Ferner sind von einer IP-Adresse (124.74.209.106) sehr viele ICMP ?Time to live exceeded in Transit? Pakete (Typ 11, Code 0) an eine Honeypot IP-Adresse gesendet worden. Die Ursache dafür ist unklar. Aus diesem Grunde ist für das Wochenende von einer leicht erhöhten Gefährdungslage auszugehen.

2008-06-19 Heute Nacht gab es einen Scan nach Port 23/tcp (Telnet) von einer chinesischen IP-Adresse. Daneben wurden wieder mehrere.

F-Secure

DShield CarmentiS

Top10 Attacked Ports

2677	- 1 -	445
19905	- 2 -	139
51413	- 3 -	80
2029	- 4 -	22
1042	- 5 -	135
40313	- 6 -	5900
532	- 7 -	1433
15215	- 8 -	2967
1031	- 9 -	21
112	- 10 -	3072

Indikatoren - Industrie

Atlas Dashboard	CA Incooperate
Niedrig	Angehoben
F-Secure	IronPort
Moderat	Moderat
Kaspersky	SANS Institute
Niedrig	Niedrig
TrendMicro	
Niedrig	

CarmentiS

(11 von 23) Alarmtracker - TCP - PORT - 7d

Sun Jun 15 05:45:00 2008 - Sun Jun 22 05:45:00 2008 - TCP Flows (average of 24h)

Top 10 Ports

- Port 445
- Port 139
- Port 80
- Port 22
- Port 135
- Port 5900
- Port 1433
- Port 2967
- Port 21
- Port 1024

DShield CarmentiS

Attackers Attacking Countries

150.164.102.060 (BR)	- 1 -	China
121.162.129.138 (XX)	- 2 -	United States
081.091.236.079 (BJ)	- 3 -	Italy
081.209.145.131 (DE)	- 4 -	Spain
061.134.056.018 (CN)	- 5 -	France
218.078.212.102 (CN)	- 6 -	Poland
217.098.102.037 (PL)	- 7 -	N/A
088.080.215.015 (XX)	- 8 -	Germany
217.198.149.018 (SE)	- 9 -	Korea, Republic of
196.201.245.004 (EG)	- 10 -	United Kingdom

Security Focus Newsfeed

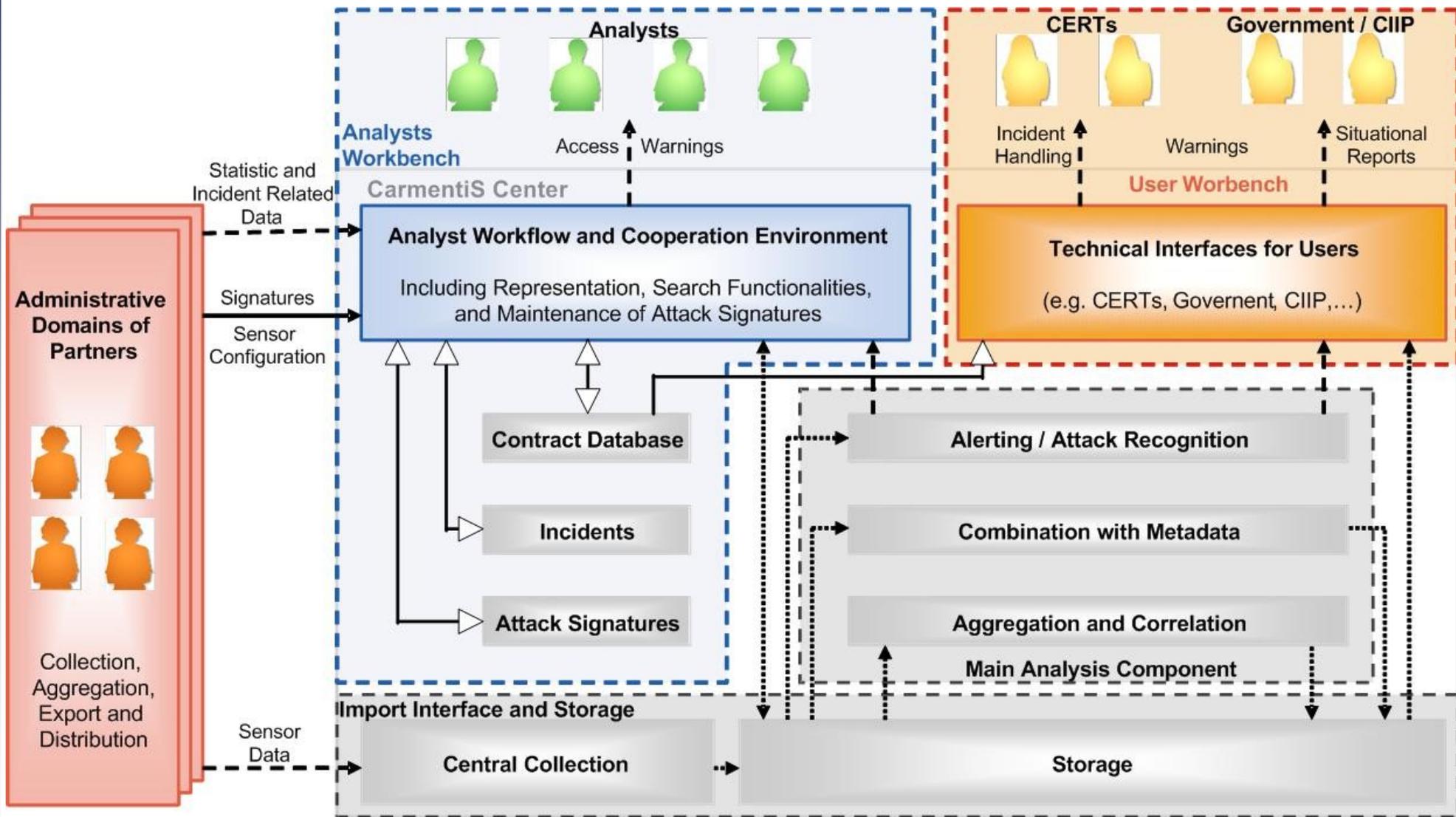
- 2008-06-13 Ransomware resisting crypto cracking efforts
- 2008-06-09 Boycott spotlights antivirus testing issues
- 2008-05-30 Hired gun blamed for business outage
- 2008-05-27 TJX employee fired for exposing shoddy security
- 2008-05-16 Legal experts wary of MySpace hacking charges
- 2008-05-14 Admins warned of brute-force SSH attacks
- 2008-05-09 Thoughts of a Teenage Bot Master
- 2008-05-02 Groups warn travelers to limit laptop data
- 2008-05-01 Radio Free Europe hit by DDoS attack

Honolulu	San Francisco	Mexico City	New York	Rio de Janeiro	London	Berlin	Moskau	Kalkutta	Singapur	Tokyo	Sydney	Wellington
17:54	20:54	22:54	23:54	00:54	04:54	05:54	07:54	09:24	11:54	12:54	13:54	15:54

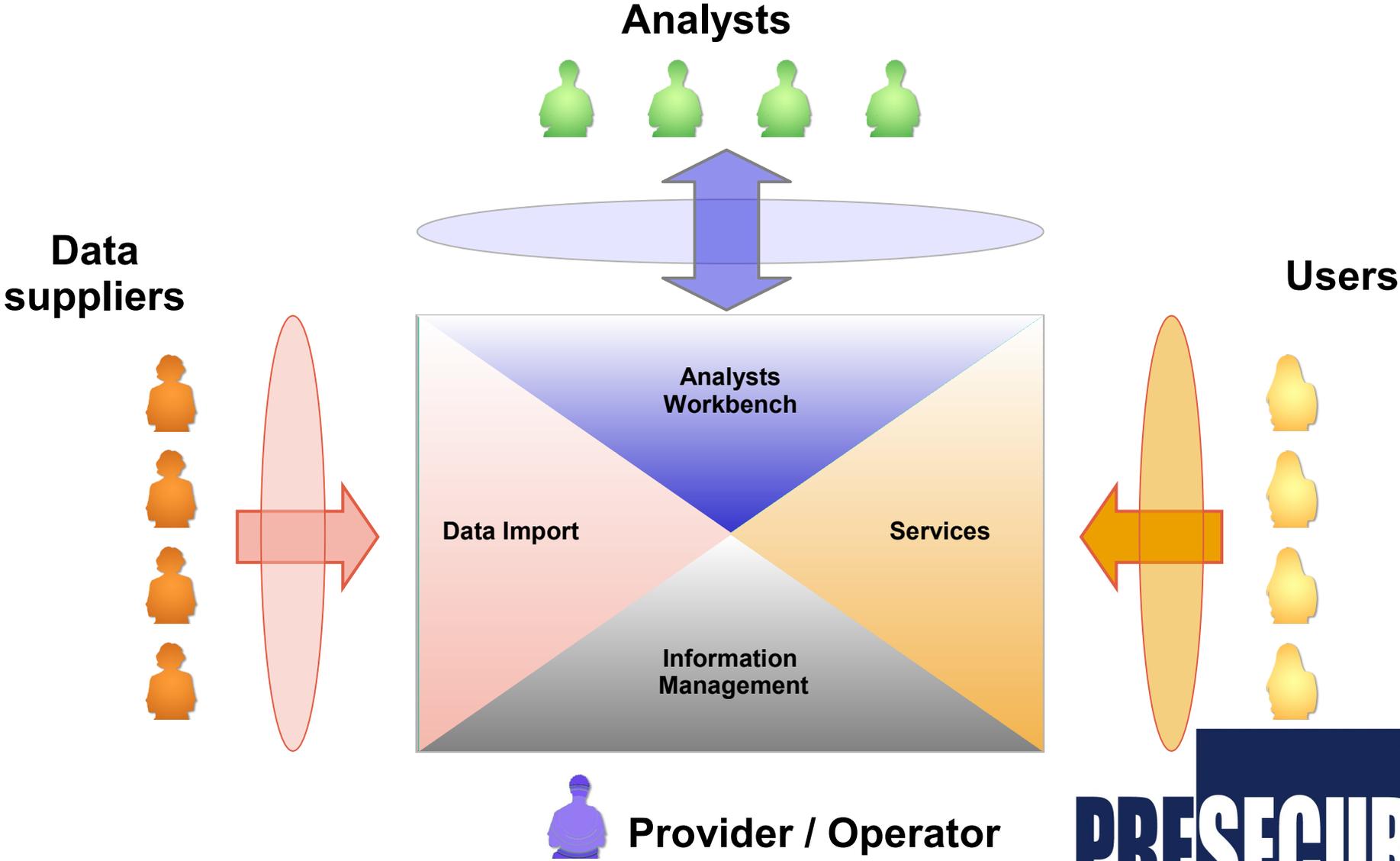
Carmentis at a glance

- **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**

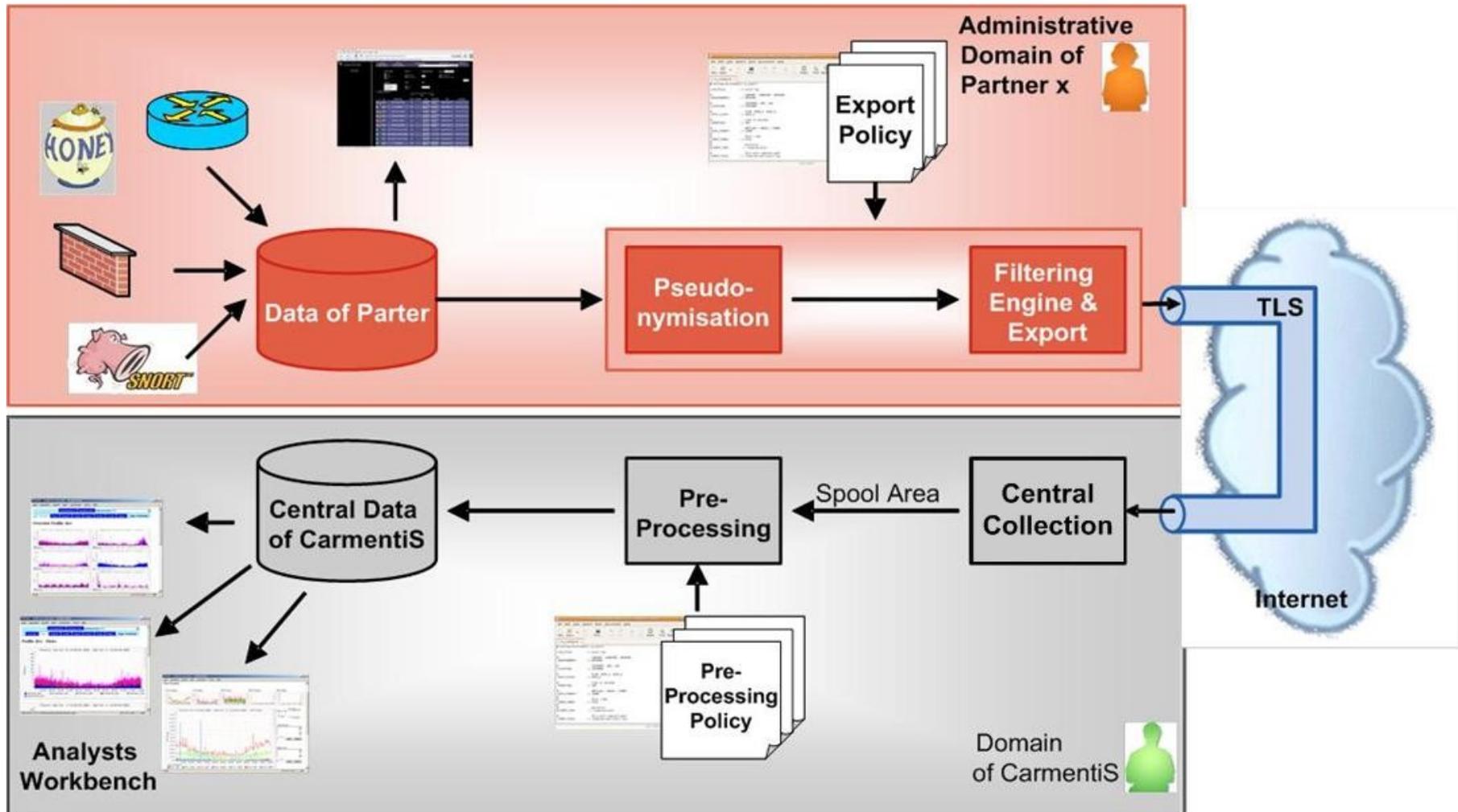
Architecture



Framework and Roles



Data collection



Data collection

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

Data types

■ Data types

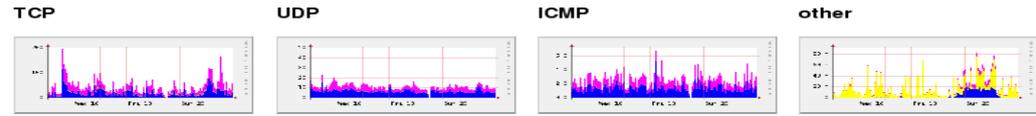
- Netflows (v5, v7)
- Argus
- IDS (Snort)
- Malware (Nepenthes)
- Exploits (Argos)
- Meta events (Aggregation)
- ...

Analysts' Interface

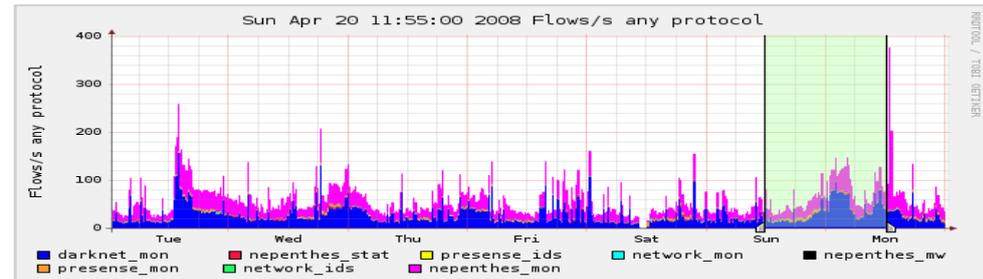
Home | Graphs | Details | Alerts | Stats | Plugins | Profile: live | Documentation | Bookmark URL

Profile: live

Profile Status: OK



Profileinfo:
 Type: live
 Max: unlimited
 Exp: never
 Start: Nov 01 2007 - 00:00 CEST
 End: May 13 2008 - 01:55 CEST



t_start | 2008-04-20-11-55
 t_end | 2008-04-21-12-25



Select [Time Window] Display: [1 week] [Navigation icons] [Lin Scale] [Stacked Graph] [Log Scale] [Line Graph]

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





Aggregation for CarmentiS

© 2000-2008 by PRESECURE Consulting GmbH

PRESECURE[®]
Consulting GmbH

Extend / enhance existing EW system

■ Different types of aggregation

- Data mining
- Clustering
- Rule based
- ...
- Hybrid approaches

■ Several approaches evaluated

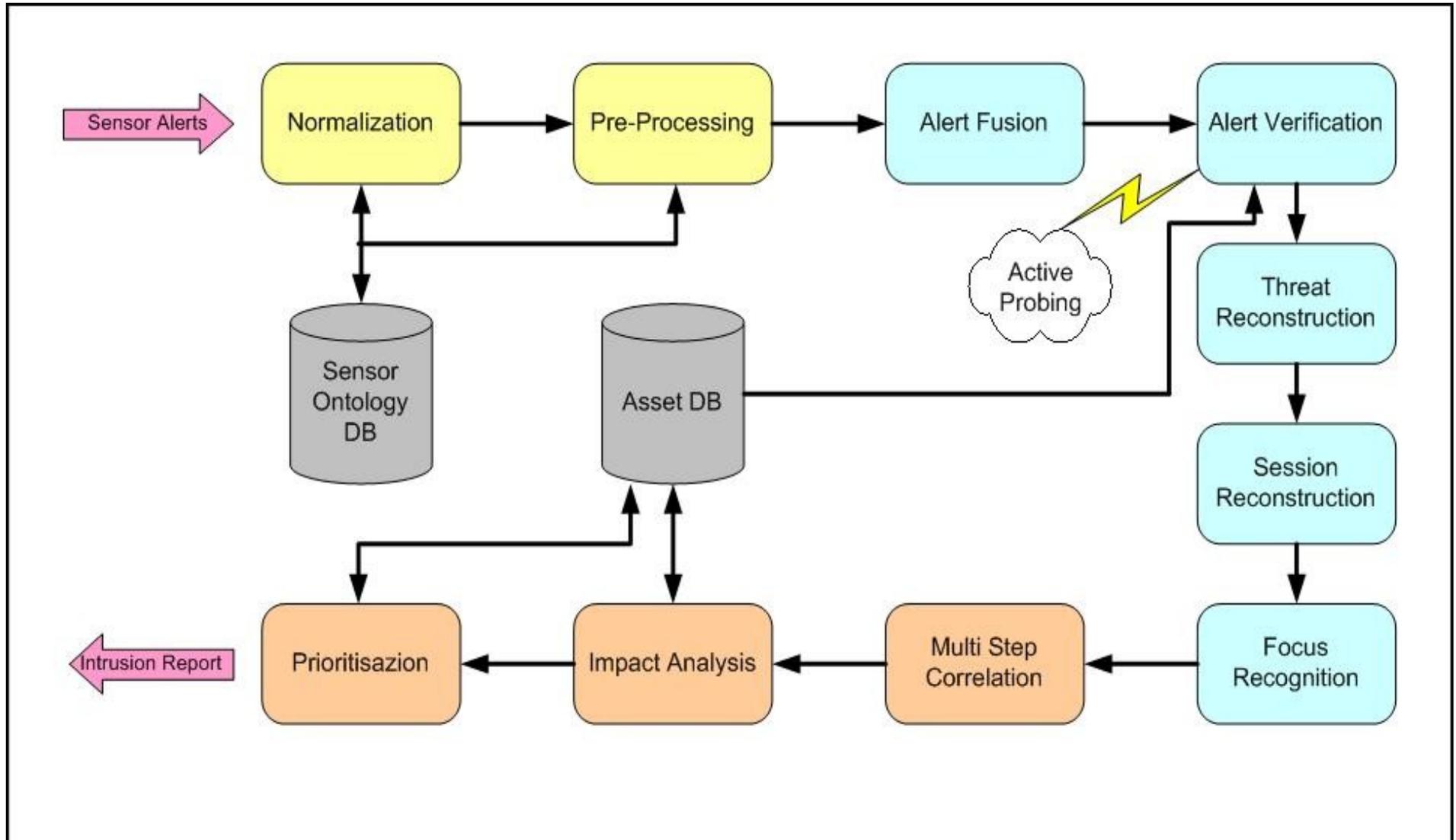
Requirements

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

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

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

Chosen approach (Panjwani)

■ No. Packets	Classification
$0 \leq n < 5$	Port Scan / Ping Scan (ICMP)
$5 \leq n \leq 12$	Probe
$12 < n$	Attack

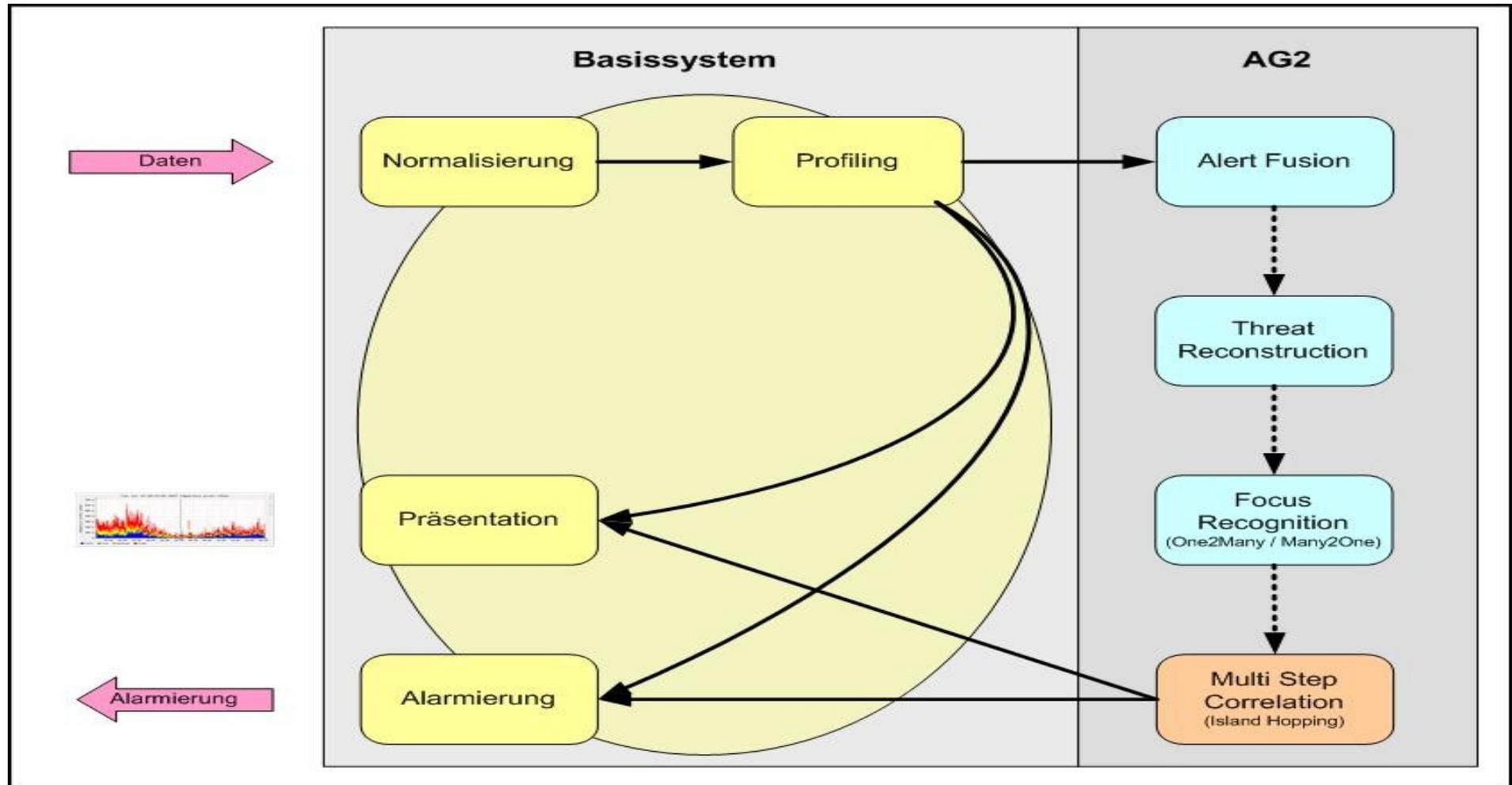


Implementation

© 2000-2008 by PRESECURE Consulting GmbH

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)

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, ...)

Algorithm Focus Recognition

■ One2Many

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

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

Algorithm Focus Recognition

■ Many2One

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

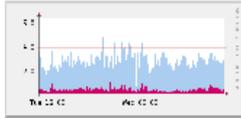
- Time window 120 seconds
- Threshold configurable
- Start time $\text{Min}(e1.st, en.st)$
- End time $\text{Max}(e1.et, en.et)$
- Further classification
(scanning, ...)

Problems

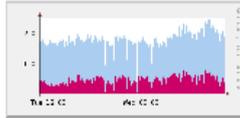
- Introduction of meta events
- Biflows needed
- Extension of the representation layer
- Integration with other events / information
- Status information from previous time slice needed

Detailed analysis

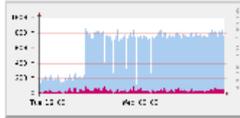
TCP



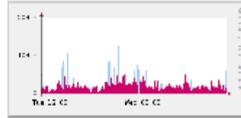
UDP



ICMP

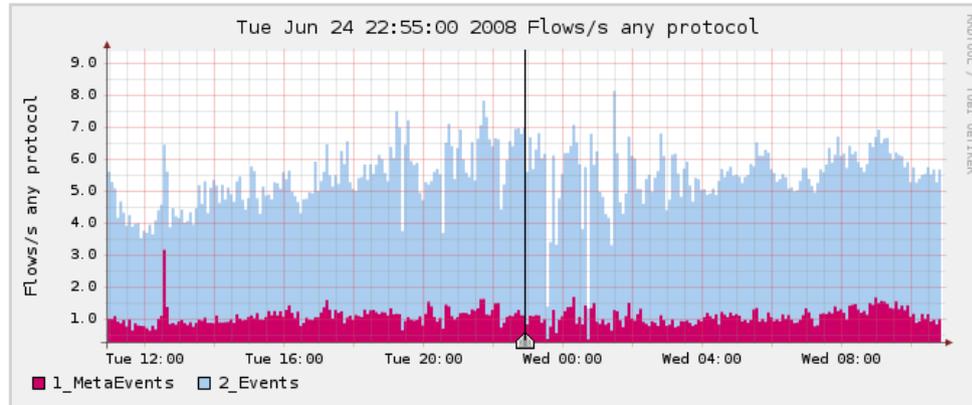


other



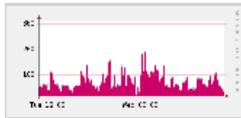
Profileinfo:

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

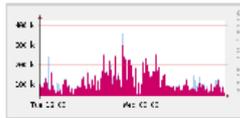


t_start: 2008-06-24-22-55
 t_end: 2008-06-24-22-55

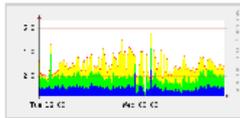
Packets



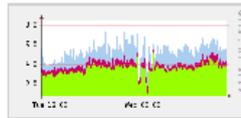
Traffic



Impacts



Rating



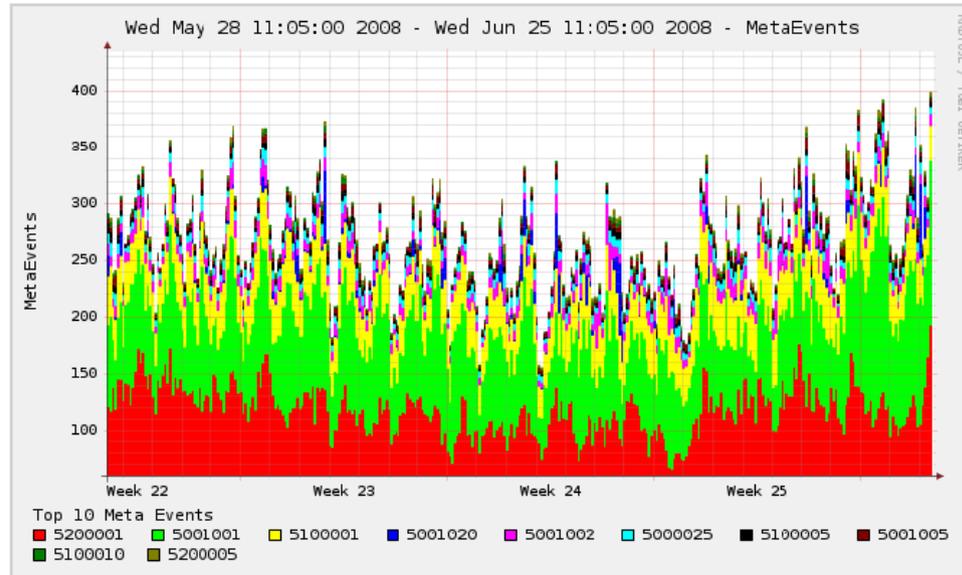
Select Display: << < | ^ > >> >|

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 Overview



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"



First Results

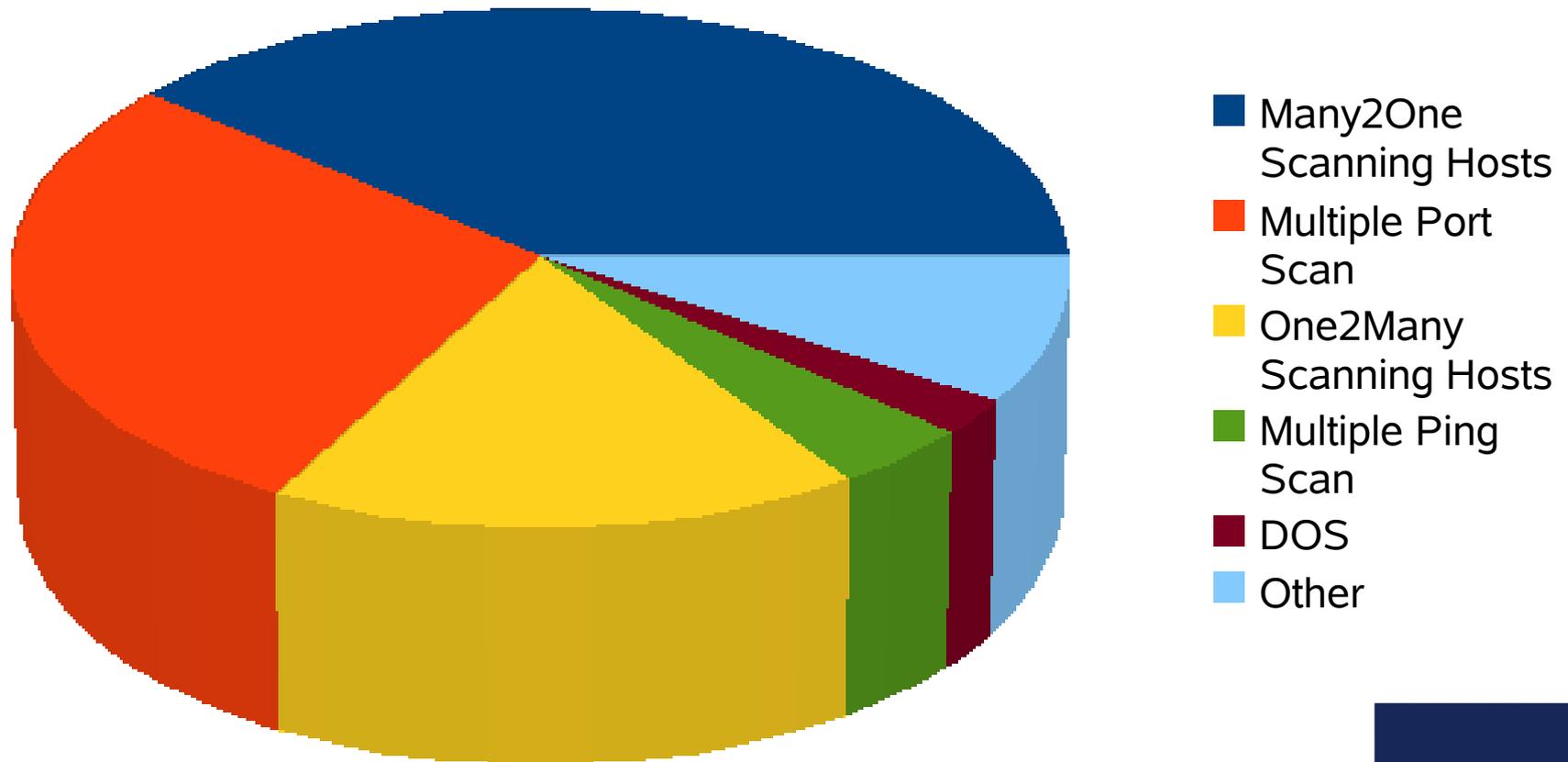
© 2000-2008 by PRESECURE Consulting GmbH

PRESECURE[®]
Consulting GmbH

First results

Aggregated Events

2008-05-08 - 2008-06-04



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

Outlook

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

Contact

Till Döriges

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?