SIEMENS

Corporate Technology

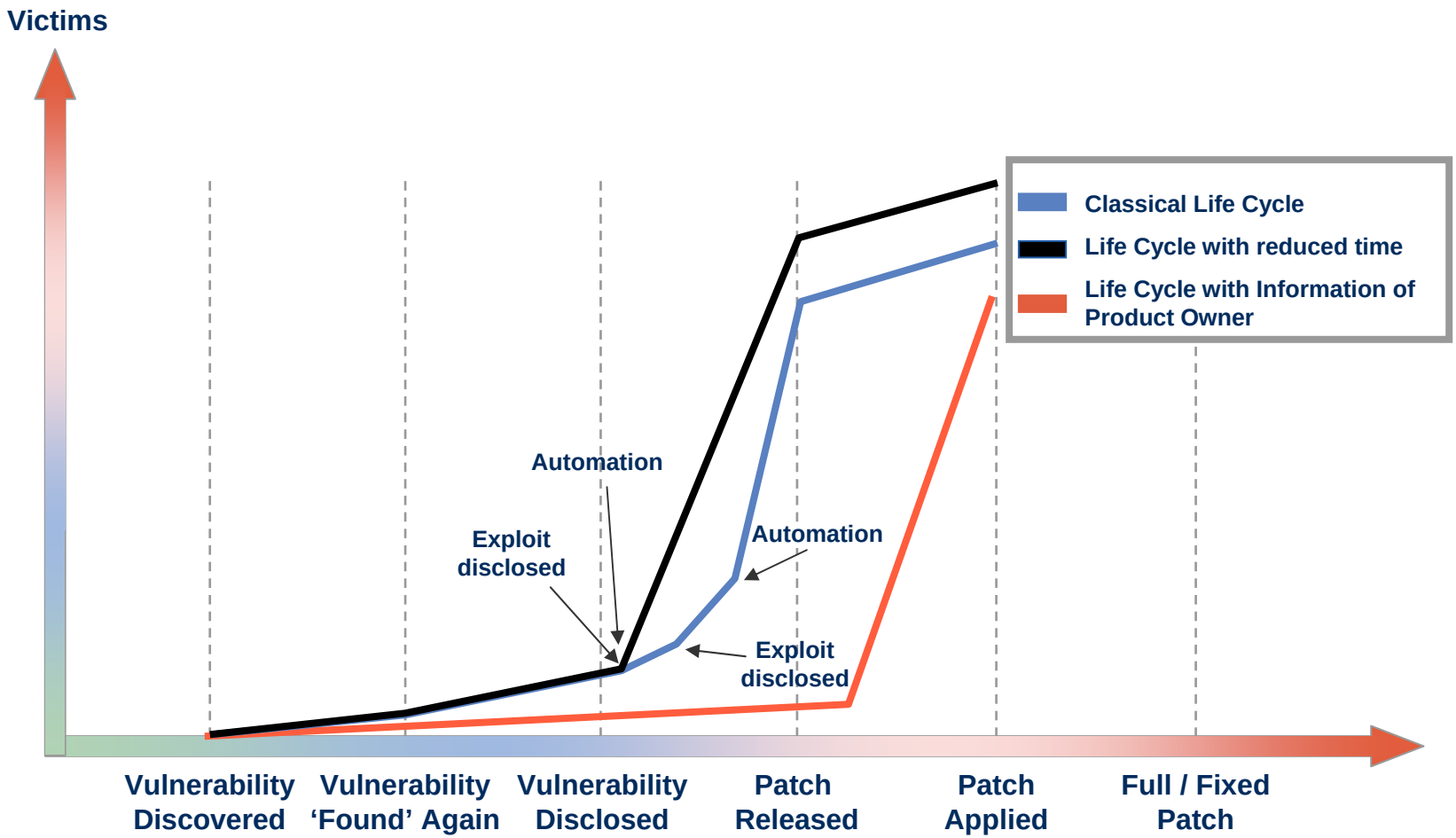
CarmentiS

A Co-Operative Approach Towards Situation Awareness and Early Warning for the Internet

Contents

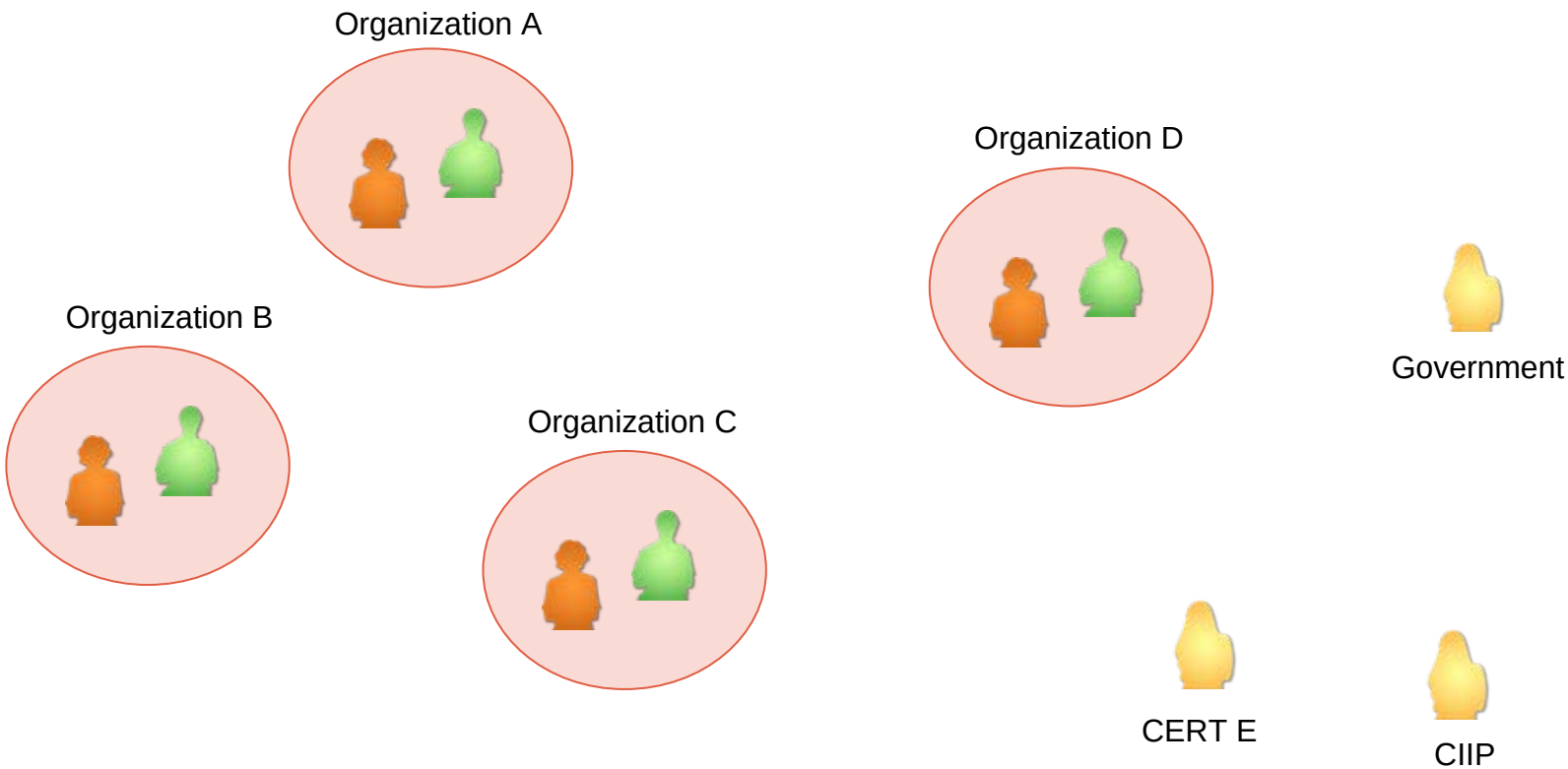
I Motivation

Vulnerability Life Cycle

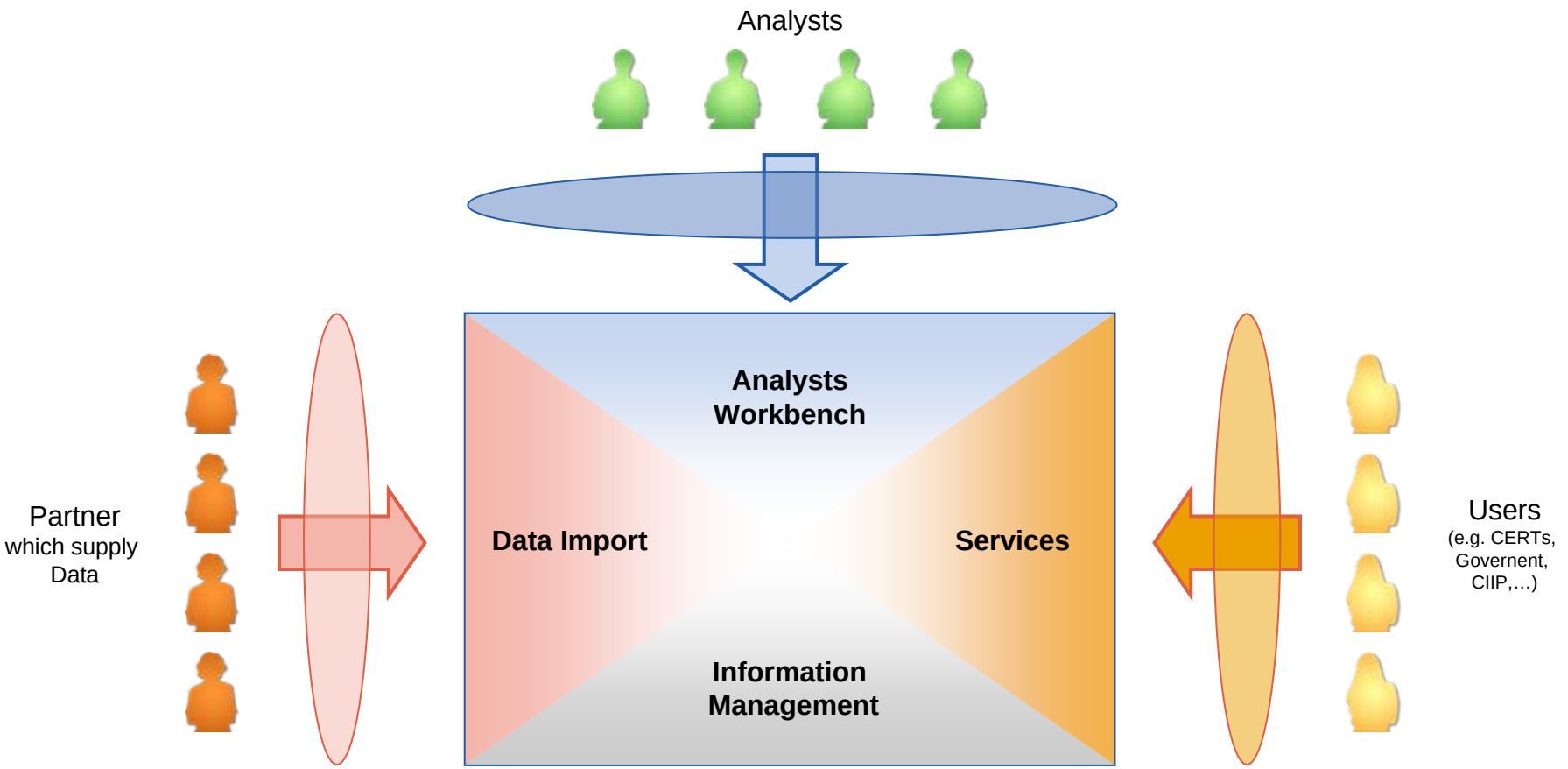


II CarmentiS Approach

Status Quo

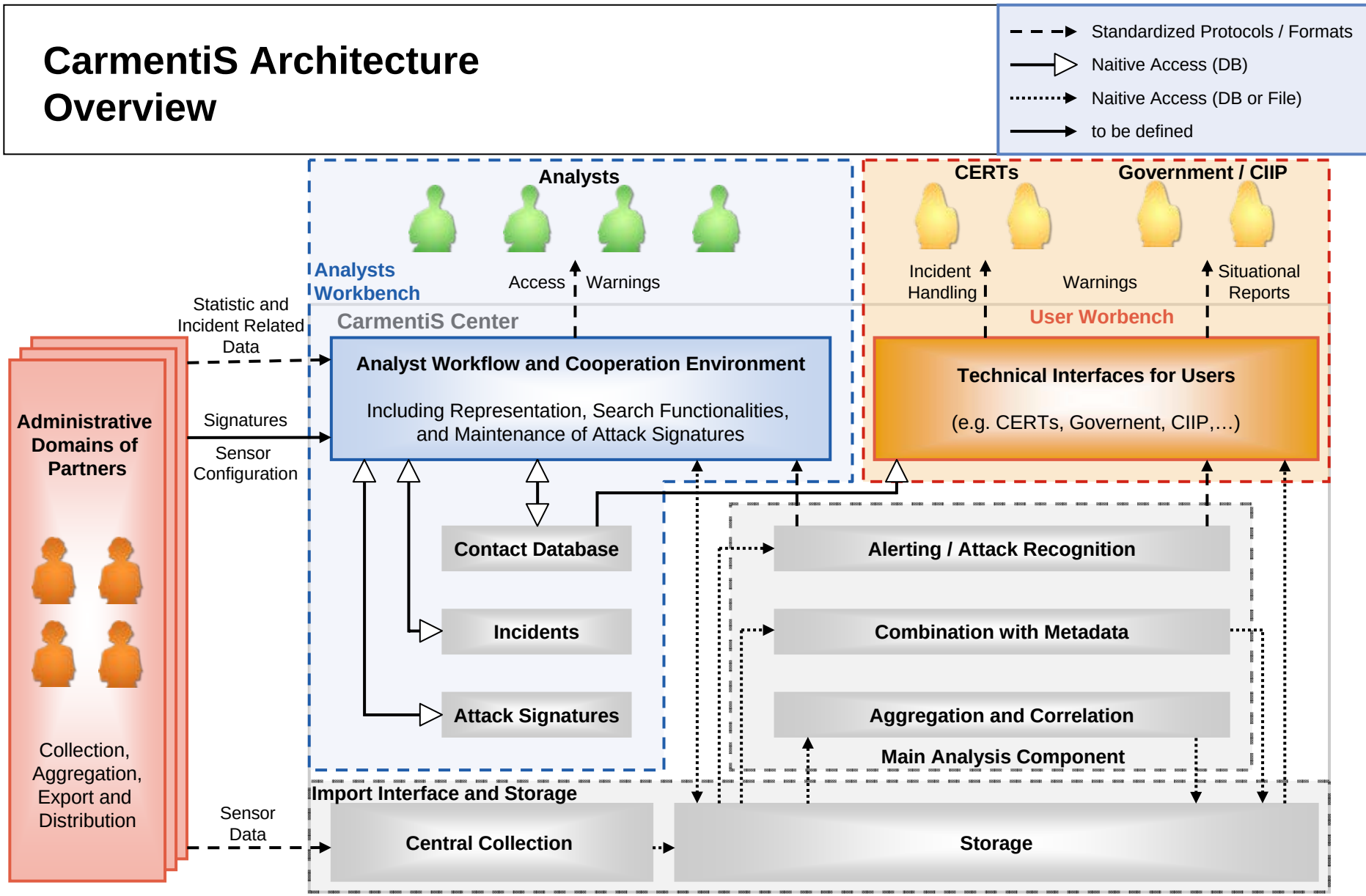

Organization A
Organization B
Organization C
Organization D
Government
CERT E
CIIP

Approach - Participants

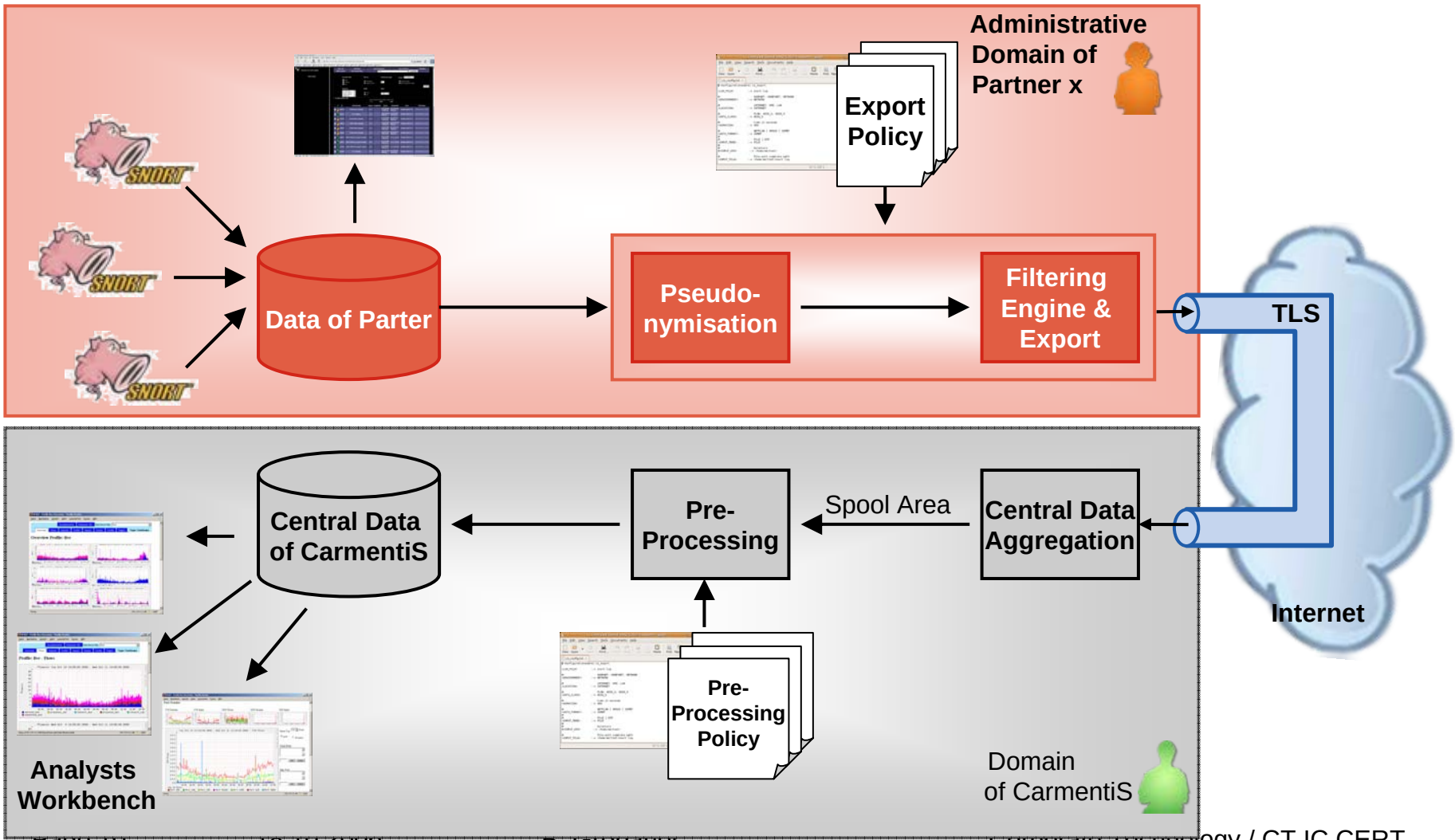


CarmentiS - Architecture

CarmentiS Architecture Overview



Import


Administrative Domain of Partner x
Export Policy
SNORT
SNORT
SNORT
Data of Parter
Pseudo-nymisation
Filtering Engine & Export
TLS
Internet
Central Data of CarmentiS
Pre-Processing
Spool Area
Central Data Aggregation
Pre-Processing Policy
Analysts Workbench
Domain of CarmentiS

CS-Container

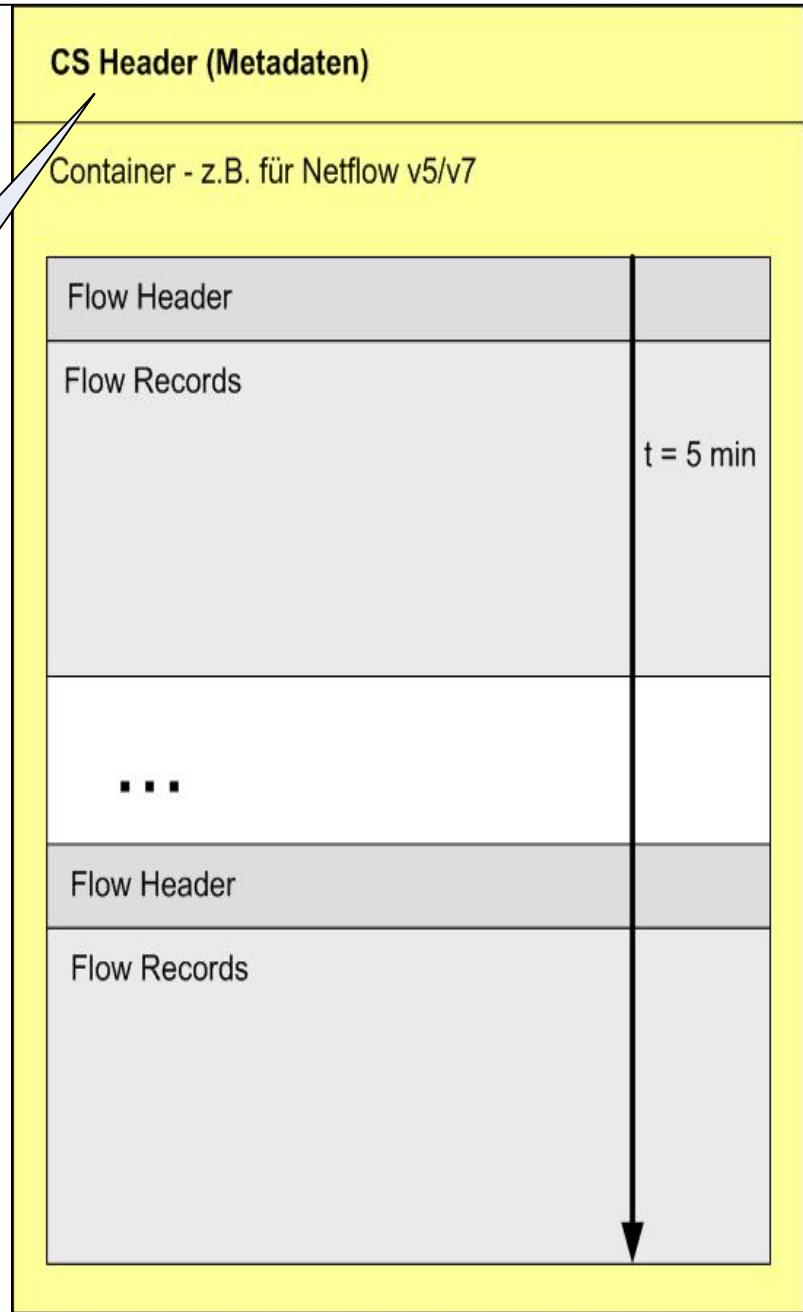
Requirements for the Data Export

- Meta-Data
- Data Compression
- Protection of Sensitive Information
- Capabilities for Configuration th
  Data Export

Developed CS-export mechanism support these features.

Metadata Examples:

- Identity of a Domain
- Environment of Sensor
- Data Format
- Business Sector belonging to Data
- Anonymizing Method



Example Export Policy

```
# Konfigurationsdatei cs_export

<LOG_FILE>          ::= /var/log/cs_export.log

#                       DARKNET, HONEYNET, NETWORK
<ENVIRONMENT>       ::= HONEYNET

#                       INTERNET, DMZ, LAN
<LOCATION>          ::= INTERNET

#                       FLOW, NIDS_S, NIDS_A
<DATA_CLASS>        ::= NIDS_S

#                       time in seconds
<DURATION>          ::= 300

#                       NETFLOW | ARGUS | IDMEF
<DATA_FORMAT>       ::= IDMEF

...
```

Example CS-Container

```
Show cs file: /carmentis/cs_spool/darknet_mon/CS-200610031610-030288

Version:          1
organisation_id: 123217736
environment:      DARKNET
location:         INTERNET
data_class:       FLOW
data_format:      NETFLOWS
src_mode:         PLAIN
dst_mode:         PSEUDO
creation_time:    2006-10-03 13:10:00
duration:         300
flags:            0

 ...
```

Pseudonymization (1/2)

```
Time      Prot      SRC IP           Port      DST IP           Port      Pks    Bytes
---

13:07:54 TCP      219. 27.152. 26:1603 -> 159.157.137.218:135      1        40
13:08:02 TCP       70. 52.131.111:3075 -> 159.157.107.247:139      2        96
13:08:04 TCP       62.178. 39.234:1517 -> 159.157. 86.163:445      4       305
13:08:06 ICMP     219. 27.152. 26:0    -> 159.157.137.218:771      1        56
13:08:06 TCP       70. 52.131.111:3077 -> 159.157.107.244:139      2        96
13:08:07 TCP       62.178. 39.234:1520 -> 159.157. 86.174:445      4       305
13:08:10 TCP      219. 27.152. 26:1603 -> 159.157.137.218:135      4      1936
13:08:10 TCP      195.174. 71. 95:4020 -> 134. 51.211.229:445      1        40
13:08:10 TCP      219. 27.152. 26:2159 -> 159.157.137.218:4444     7       356
13:08:11 TCP       70. 52.131.111:3079 -> 159.157.107.246:139      2        96
13:08:12 TCP      195.174. 71. 95:4020 -> 134. 51.211.229:5000     4       168
13:08:12 TCP       72. 20. 33. 75:3773 -> 134. 49.  5. 67:135      6      1928
13:08:12 TCP      195.174. 71. 95:4020 -> 134. 51.211.229:139      2        88
13:08:13 TCP       72. 20. 33. 75:3773 -> 134. 49.  5. 67:33568   32     30056
13:08:14 TCP       62.178. 39.234:1522 -> 159.157. 86.172:445      4       305
13:08:16 UDP      219. 27.152. 26:69   -> 159.157.137.218:37355   13      6592
13:08:18 ICMP     219. 27.152. 26:0    -> 159.157.137.218:771      1        56
---
```

Pseudonymization (2/2)
Example Cryptography-based Prefix-preserving Anonymization

Time	Prot	SRC IP	Port	DST IP			
13:07:54	TCP	219. 27.152. 26:1603	->	200.118.139.			
13:08:02	TCP	70. 52.131.111:3075	->	200.118.227.2			
13:08:04	TCP	62.178. 39.234:1517	->	200.118.193.			
13:08:06	ICMP	219. 27.152. 26:0	->	200.118.139. 27			
13:08:06	TCP	70. 52.131.111:3077	->	200.118.227.230:1		2	96
13:08:07	TCP	62.178. 39.234:1520	->	200.118.193. 85:	45	4	305
13:08:10	TCP	219. 27.152. 26:1603	->	200.118.139. 27:135		4	1936
13:08:10	TCP	195.174. 71. 95:4020	->	222. 63.132. 43:445		1	40
13:08:10	TCP	219. 27.152. 26:2159	->	200.118.139. 27:4444		7	356
13:08:11	TCP	70. 52.131.111:3079	->	200.118.227.229:139		2	96
13:08:12	TCP	195.174. 71. 95:4020	->	222. 63.132. 43:5000		4	168
13:08:12	TCP	72. 20. 33. 75:3773	->	222. 61.185. 34:135		6	1928
13:08:12	TCP	195.174. 71. 95:4020	->	222. 63.132. 43:139		2	88
13:08:13	TCP	72. 20. 33. 75:3773	->	222. 61.185. 34:33568		32	30056
13:08:14	TCP	62.178. 39.234:1522	->	200.118.193. 87:445		4	305
13:08:16	UDP	219. 27.152. 26:69	->	200.118.139. 27:37355		13	6592
13:08:18	ICMP	219. 27.152. 26:0	->	200.118.139. 27:771		1	56

Problem:

Partner uses different Key for Pseudonymization

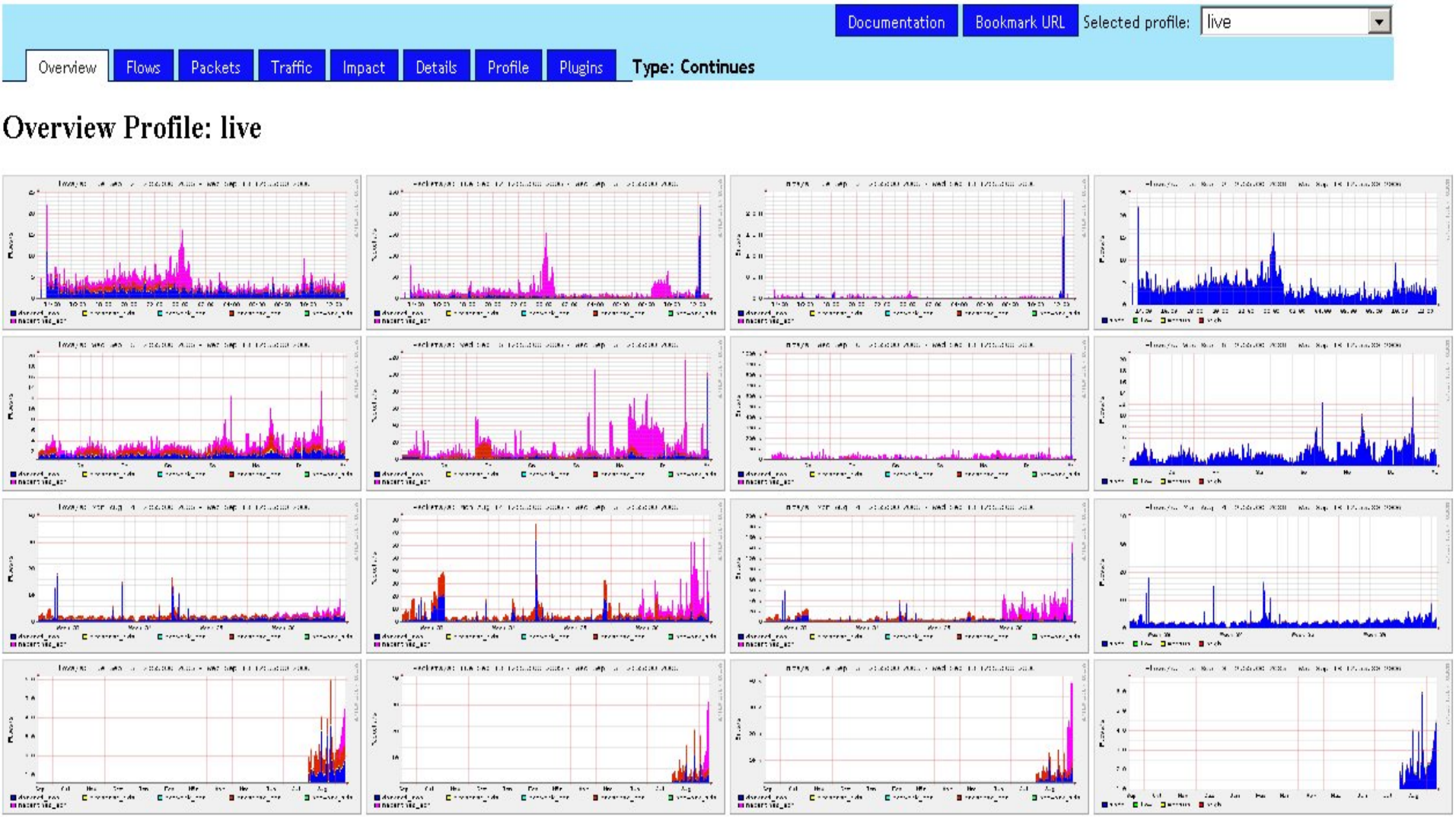
Correlation of IP-Addresses between Partner is impossible!

SIEMENS

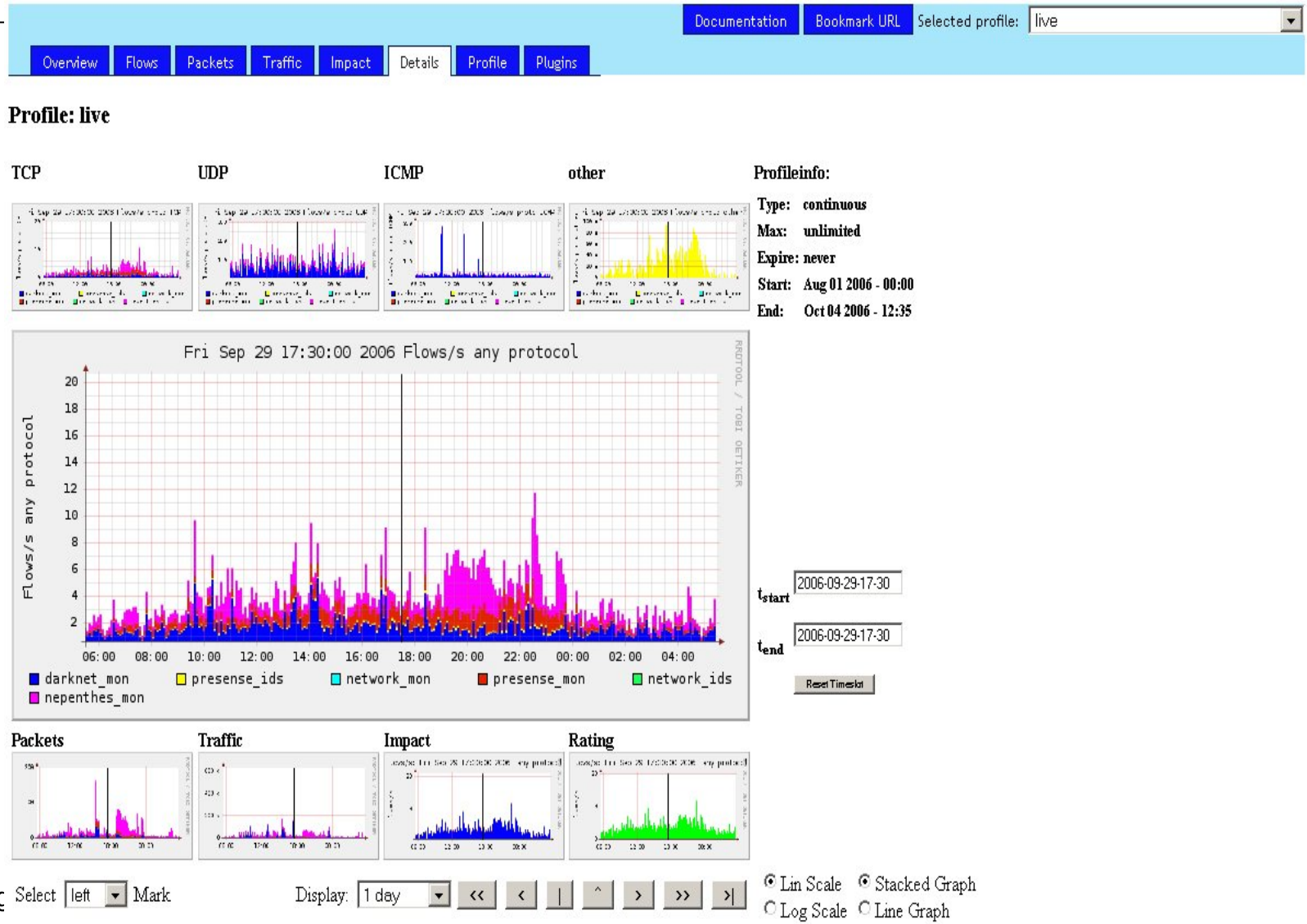
Corporate Technology

CarmentiS System

CarmentiS Analysts Workbench Overview



CarmentiS Analysts Workbench View with Details



CarmentiS Analysts Workbench
Creating Individual Queries

Statistics Timeslot Sep 29 2006 - 17:30

Source:	Flows:	Packets:					Traffic:					Impact:				
		all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
☑ darknet_mon	2.0 /s	17.5 /s	1.5 /s	15.7 /s	0.3 /s	0 /s	144.4 Kb/s	601.1 b/s	143.6 Kb/s	163.4 b/s	0 b/s	0 /s	0 /s	0 /s	0 /s	0 /s
☑ presense_ids	0.1 /s	0.1 /s	0.0 /s	0 /s	0 /s	0.0 /s	0.4 b/s	0.3 b/s	0 b/s	0 b/s	0.1 b/s	0 /s	0 /s	0.0 /s	0 /s	0 /s
☑ network_mon	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s	0 /s	0 /s	0 /s	0 /s	0 /s
☑ presense_mon	1.0 /s	2.8 /s	2.7 /s	0.1 /s	0 /s	0 /s	2.5 Kb/s	2.5 Kb/s	44.2 b/s	0 b/s	0 b/s	0 /s	0 /s	0 /s	0 /s	0 /s
☑ network_ids	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s	0 /s	0 /s	0 /s	0 /s	0 /s
☑ nepenthes_mon	0.5 /s	0.8 /s	0.5 /s	0.3 /s	0.0 /s	0 /s	1.3 Kb/s	185.8 b/s	1.1 Kb/s	3.0 b/s	0 b/s	0 /s	0 /s	0 /s	0 /s	0 /s

All None

Display: ○ Sum ◉ Rate

Details

Source:
darknet_mon
presense_ids
network_mon
presense_mon
network_ids
nepenthes_mon

Filter:
host 200.118.193.80

and <none>

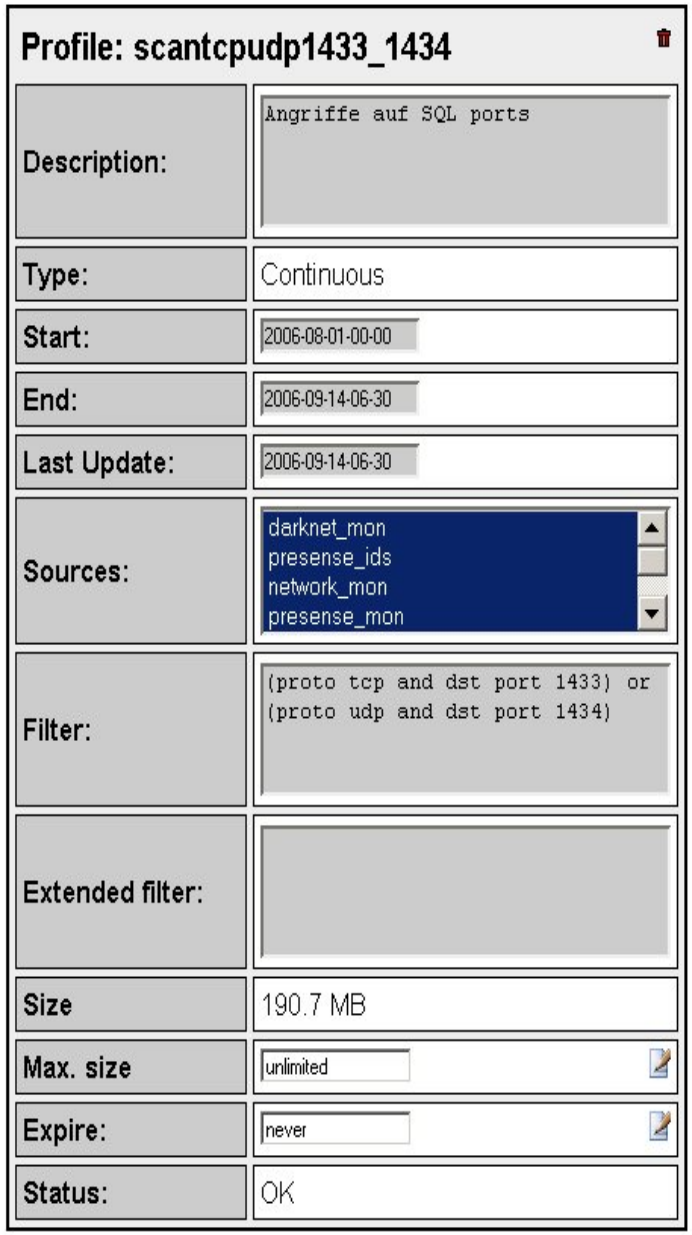
Show:

List: First 1000 Flows
☐ aggregated.
☐ sort desc.
Output format ◉ line ○ long ○ extended
Refresh

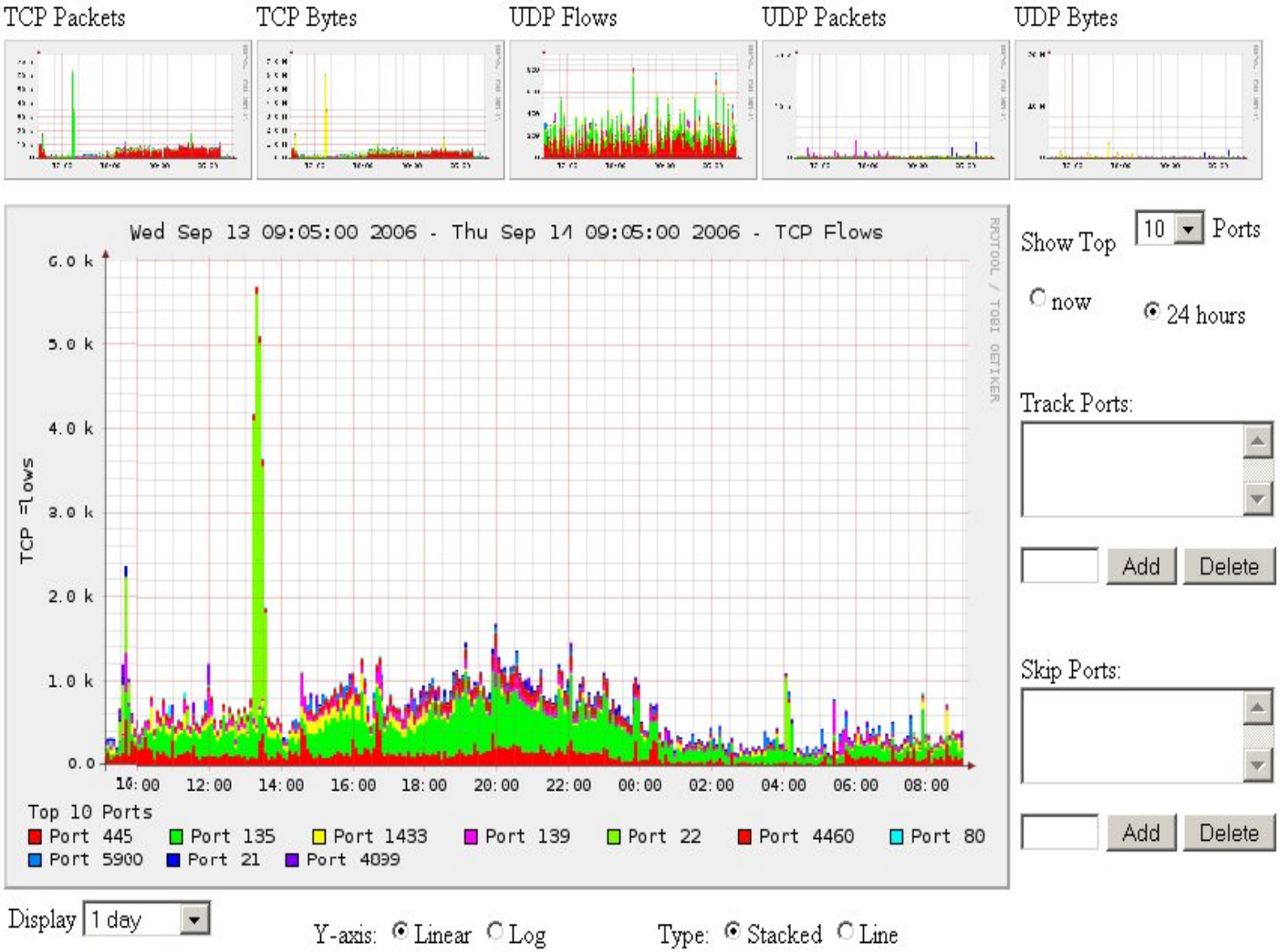
Stat: Top 50
☐ Limit Packets > 0 -
☐ Flow sorted flows
Output format ◉ line ○ long ○ extended

☐ DST Port sorted flows
Refresh

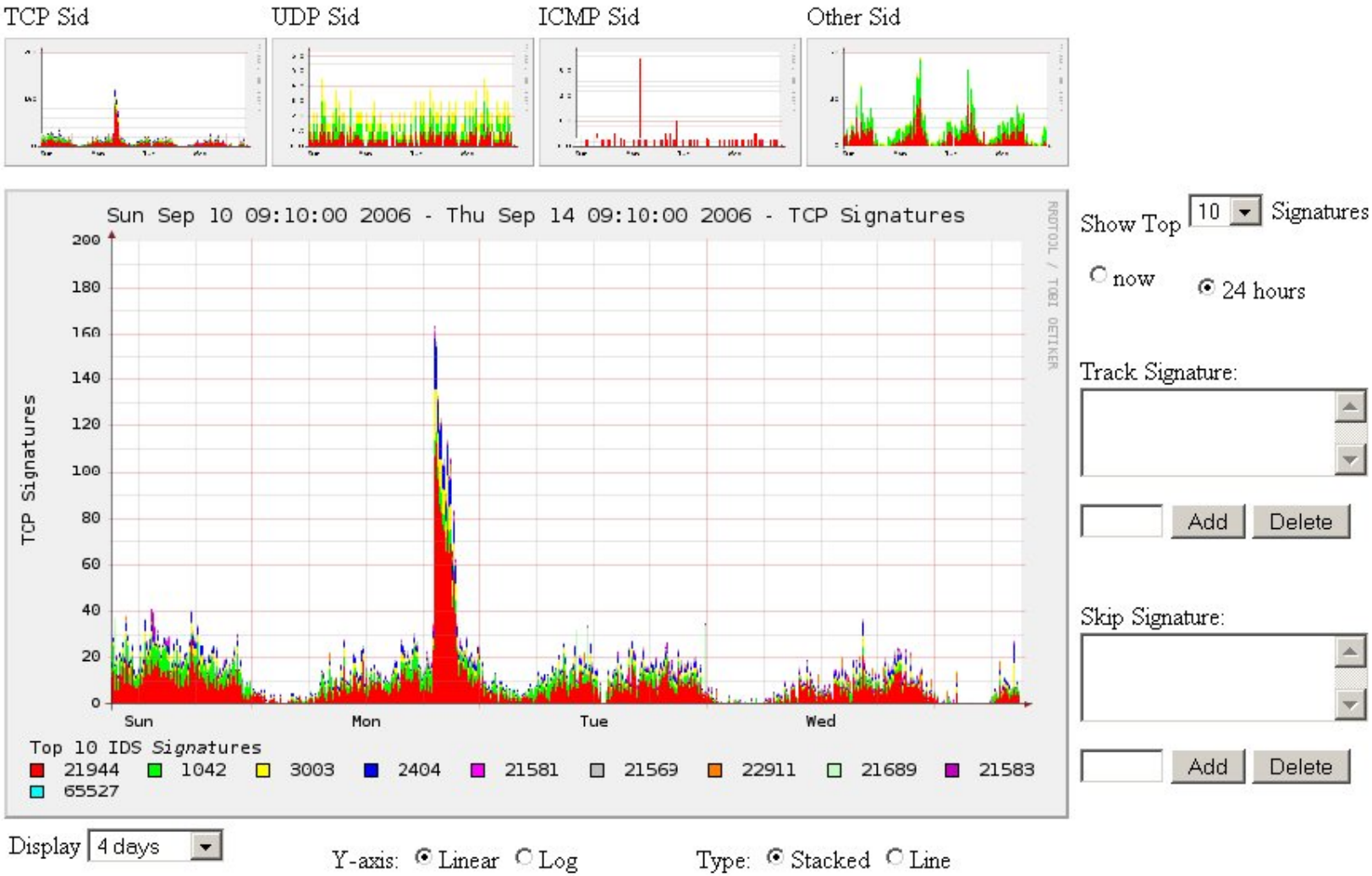
CarmentiS Analysts Workbench
Editing Profiles for CarmentiS



CarmentiS Analysts Workbench Extensions with PlugIns: Port Statistic



CarmentiS Analysts Workbench
Extensions with PlugIns: TOP IDS Signatures



Outlook

Conclusion and Outlook – Experimenting with Correlation and Co-Operative Analysis

In conclusion CarmentiS provides a co-operative approach towards situation awareness and early warning in the Internet.

Further experiments in collecting sensor data from several institutions, correlating and co-operatively analyzing this data can begin.

Further research topics may be:

- Analyzing Consequences of Pseudonymization
- Analyzing the proper use of Sensor Meta Data

Contact

Dr. Bernd Grobauer

Siemens AG
Corporate Technology
Information & Communications
Siemens CERT
Otto-Hahn-Ring 6
D-81730 Munich
Germany
E-Mail: bernd.grobauer@siemens.com
Phone: +49 89 636 – 40016