Stand der CERT-Dienste im D-Grid

Security Workshop Göttingen

27.-28. März 2007

Aufgaben des Grid-CERT

- Praktische Hilfe (Beratung) und Unterstützung bei Angriffen (Reaktion)
- Verhinderung von Angriffen und frühe Erkennung möglicher Probleme (Prävention)
- Nationale / Internationale Zusammenarbeit

Praktische Hilfe

- Grid-CERT Hotline (seit November 2006)
  - Beantwortung von Sicherheitsfragen aus den Communities
  - Hilfe bei Sicherheitsvorfällen

Hotline 040-808077-999

Reaktion - Was war neu?

- Bisher sehr wenige Vorfälle
- Meist entwendete X.509 Zertifikate
  - soweit bekannt: noch nicht im DFN-Bereich !
- Quasi keine praktischen Erfahrungen mit Grid-Vorfällen
  - Lernen von anderen CERTs scheidet aus
- Extrapolation bekannter Angriffe – brauchbar ?
- Selber mögliche Wege finden

Angriffstests

- Host Enumeration
  - Finden aktiver Systeme in einem Teilnetz
- Portscans
  - Herausfinden angebotener Dienste eines Systems, bzw.offene TCP und UDP Ports
- Portscans bestimmen nur, ob ein Dienst läuft
  - Nicht ob der Dienst eine Schwachstelle aufweist
  - Wissen um die Version eines Dienstes kann ausreichen
    - Banner Grabbing
    - Direktes Abfragen der Version von Anwendungen
  - Verschiedene Ansätze für verschiedene Dienste

Angriffstests - Ergebnisse

- SSL Zertifikat verrät Grid-Site
  - Evtl. auch durch Besonderheiten der SSLImplementierung (nur SSLv3, keine Auto-Negotiation, Ciphersuites)
- Dto. für nicht SSL-Dienste (SSH, FTP)
  - Ausgangspunkt für bekannte Angriffe
  - z.B. SSH Paßwortraten
- Bisher unbekannte Dienste lassen sich bestimmen
  - Über nmap Service Signaturen
  - z.B. TORQUE, LEMON

Angriffstests - Fazit

- Es ist Angreifern möglich, mit Standard-Werkzeugen
  - Grid-Sites zu finden
  - und spezifischen Grids zuzuordnen (SSL)
- Grid-Dienste können auch auf anderen Portnummern als den Defaults gefunden werden
- Wenig bekannte Protokolle können unbekannte Schwachstellen beinhalten
  - Strikte Firewall-Konfiguration ist ein Muß
  - Zusätzliche Sicherheitsmaßnahmen für den Fall eines Einbruchs sind (immer) empfehlenswert

Zusammenarbeit

In Deutschland, Europa und weltweit

- Sensibilisierung für Grid-spezifische Sicherheitsthemen in nationalen und internationalen Gremien (z.B. CERT-Verbund, TERENA TF-CSIRT, FIRST)
- Einrichtung von Grid-Arbeitsgruppen in den Gremien
- Vorträge auf diversen Veranstaltungen

Zukünftiger Schwerpunkt im Grid-CERT:

Frühe Warnung im D-Grid

Möglichkeiten und Systemkomponenten

Sinnvolle Definition

Definition “Frühwarnung”:

- Aufgrund eindeutiger Erkenntnisse,
- die noch möglichst wenige betreffen,
- sind Informationen zu verteilen,
- die vielen (noch nicht Betroffenen) helfen,
- und (insgesamt) schlimmeres vermeiden!

➲ *Andere können sich noch retten!*

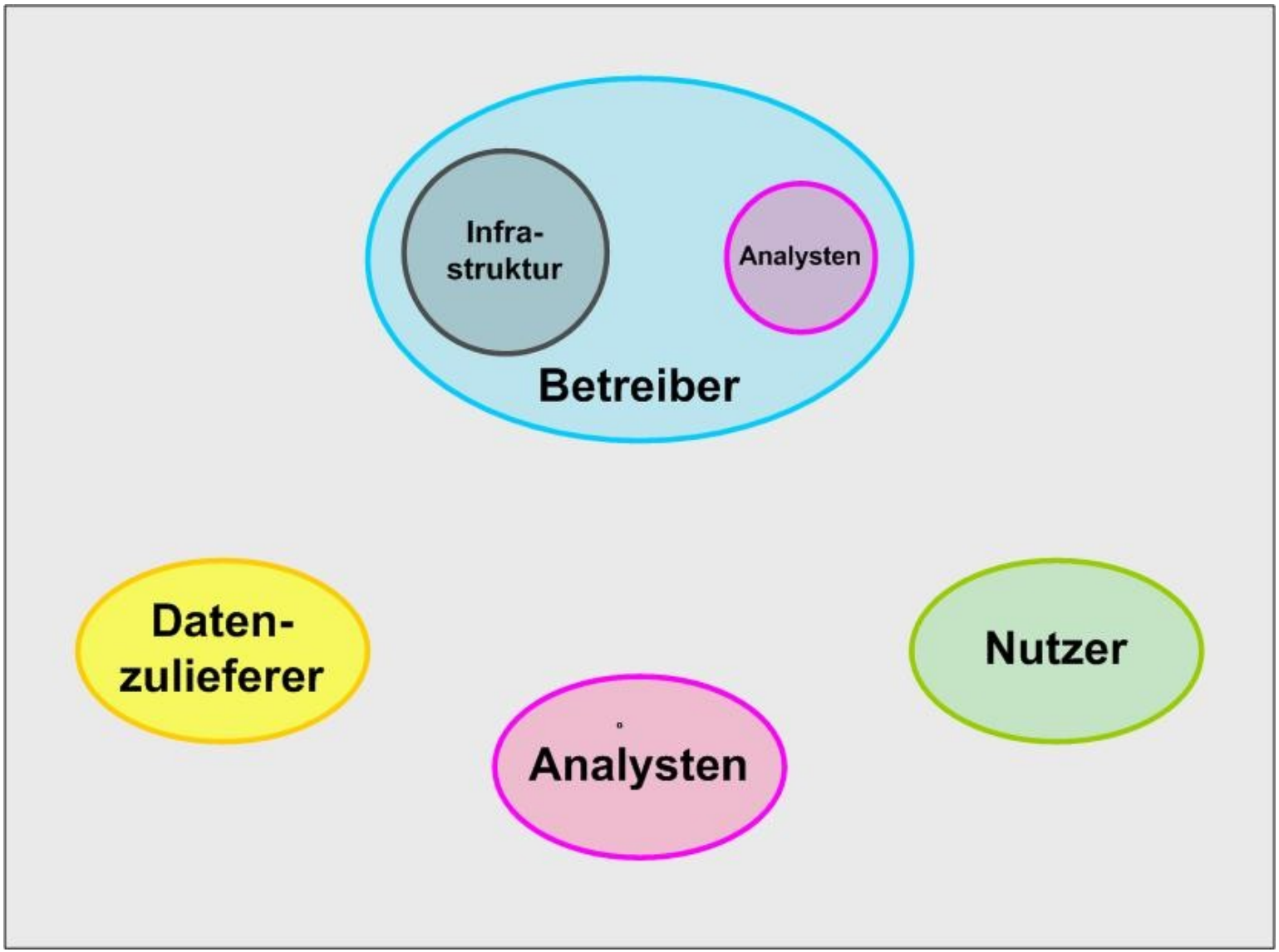
Zielvorgaben

- Angriffe im System / Netzwerk / Grid möglichst früh erkennen, um
  - zu warnen und
  - Unterstützung Betroffener zu koordinieren
- Lagebild zur aktuellen Bedrohung inkl.
  - Trendanalyse
  - Statistik
- Entlastung des Systemadministrators
  - Aufbereitung der verfügbaren Informationen

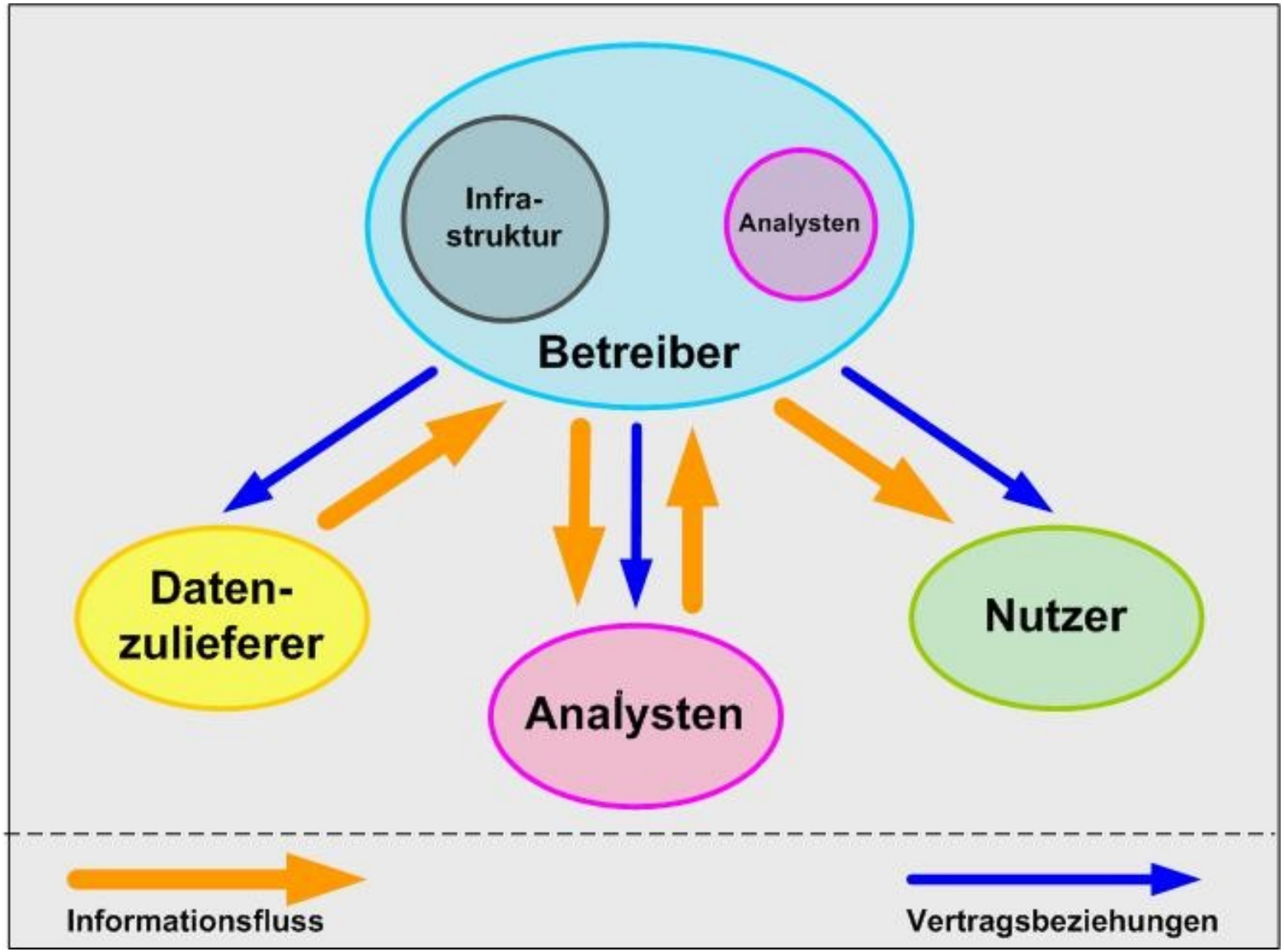
Ebenen der Kooperation

- Nutzer
  - Profitiert von den Erkenntnissen und Information
  - Steigert eigene Sicherheit
- Analysten
  - Stellen ihre Expertise bereit
  - Bieten Dienstleistung für Nutzergemeinschaft an
- Datenzulieferer
  - Liefern eigene Daten mit eigener Sensorik
  - Erhalten Zusatznutzen durch Vergleich mit Gesamtlage

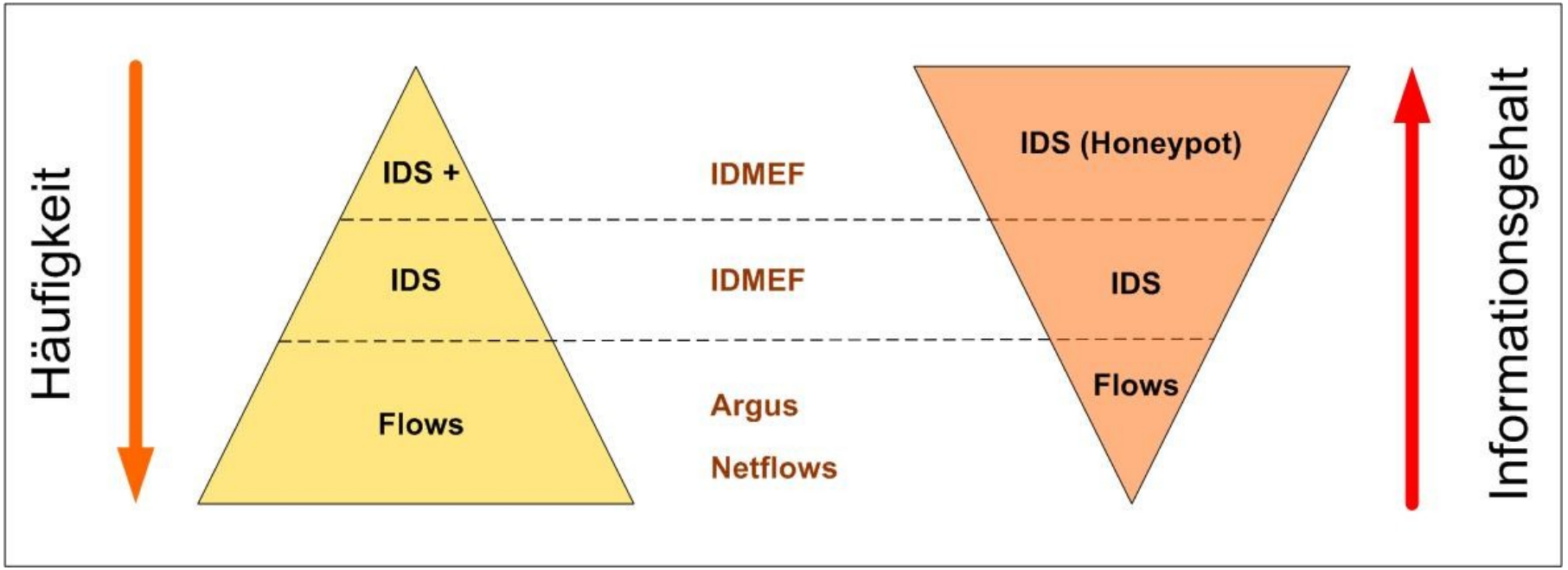
Mitarbeit / Beteiligung



Organisatorische Schnittstellen

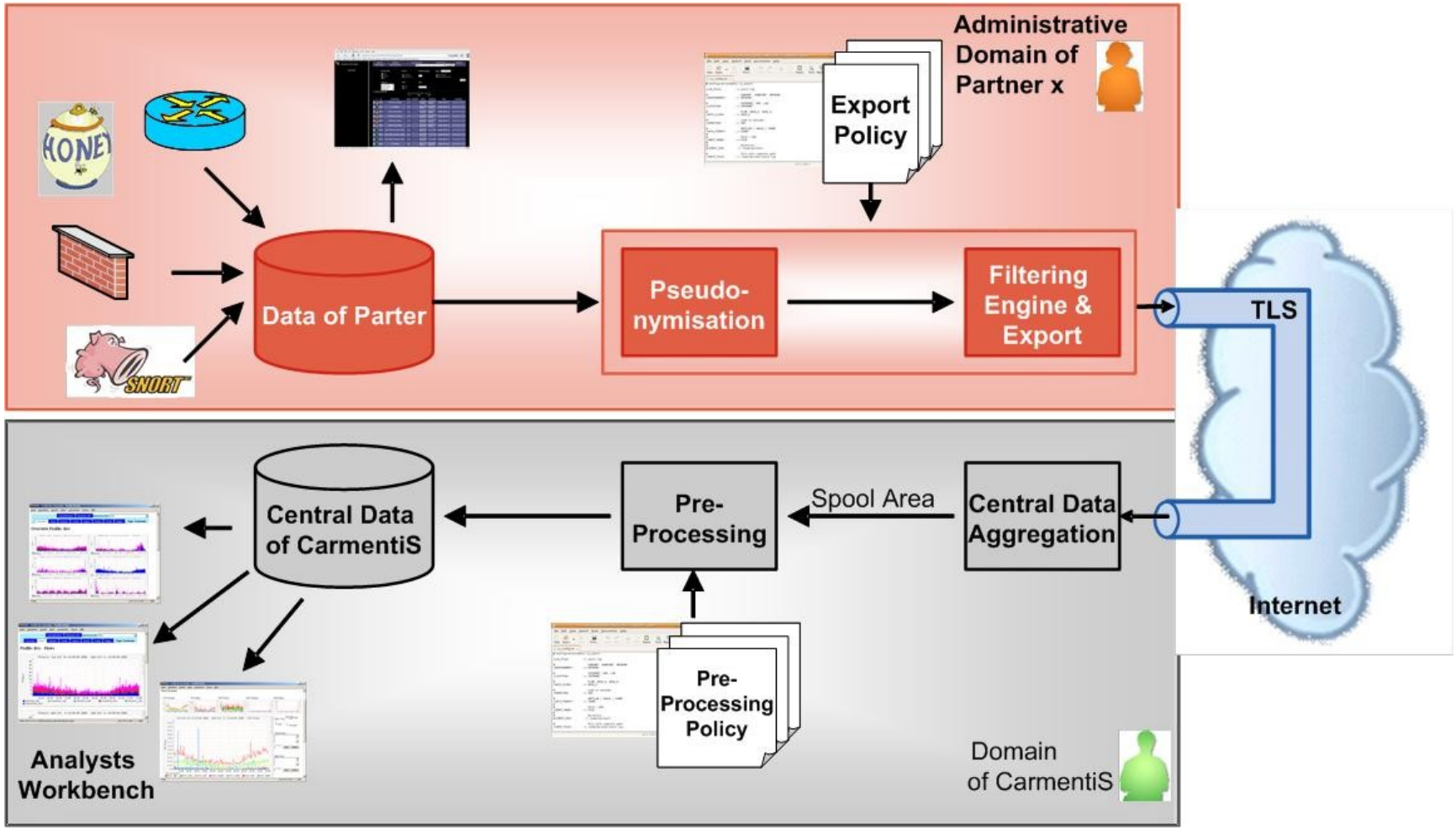


Bewertung der Eigenschaften

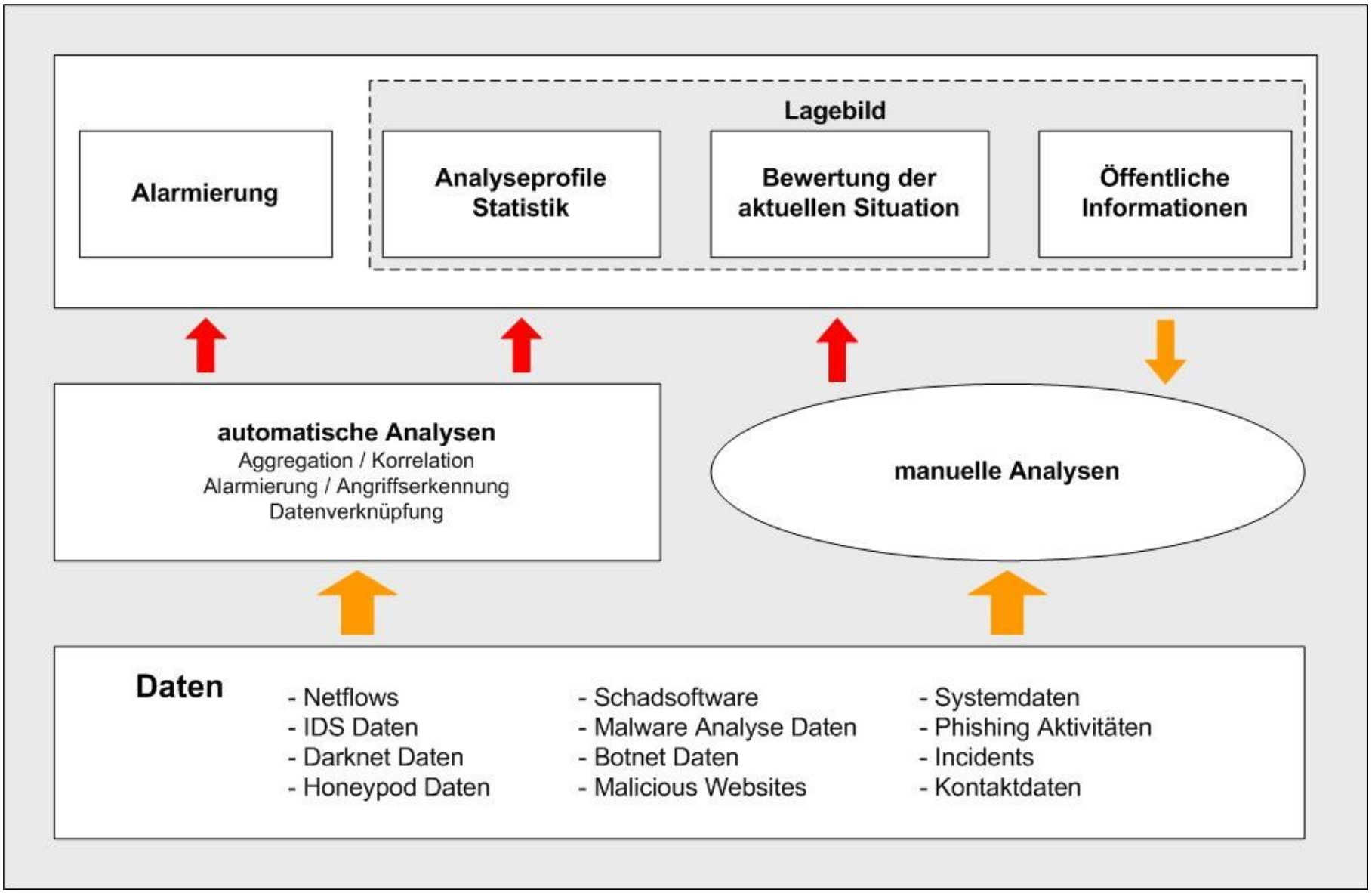


➲ *Je mehr, desto besser!*

Datenfluss bei der Übergabe



Schnittstelle für Analysten



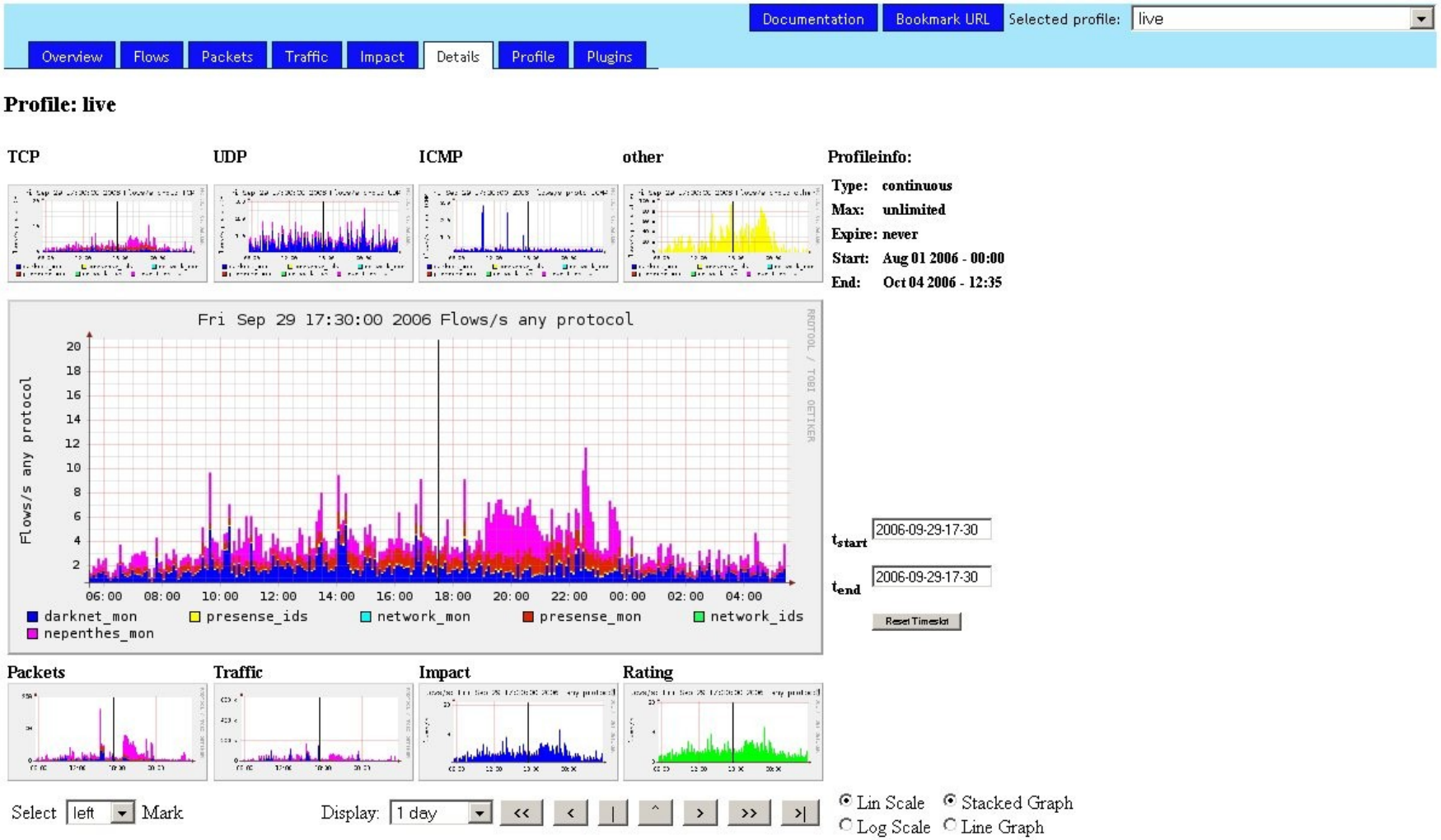
Analysts Workbench (1)

Documentation | Bookmark URL | Selected profile: live

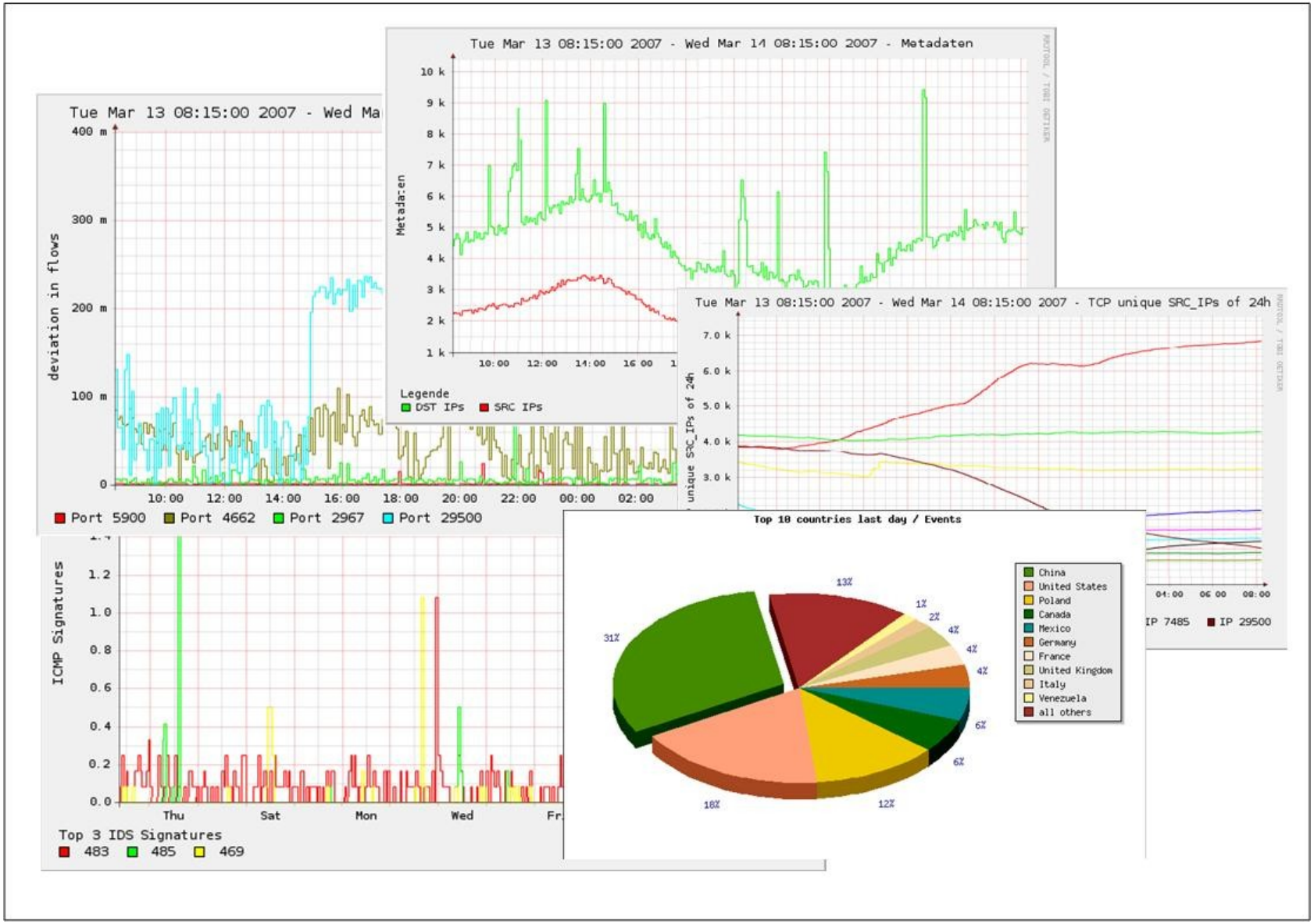
Overview | Flows | Packets | Traffic | Impact | Details | Profile | Plugins | **Type: Continues**

Overview Profile: live

Analysts Workbench (2)



Analysts Workbench (3)



Nutzerschnittstelle

Energie | FE | Finanz | Gefahrenstoffe | Gesamt | IT | Justiz | Sonstiges | Verkehr | Versorgung

Index

- Allgemein
- Hilfe

CarmentiS Partner

- CarmentiS
- BSI
- CERT Verbund
- DFN-CERT
- PRESECURE
- RUS-CERT

Links

- ISC
- NetWatchman
- IWR
- IP-DIGGER
- CERT/CC
- Atlas
- mwcollect

Lagebild: Gesamt

Bewertung

Zusammenfassung

Seit Fr (9.3.2007) ist in den Daten ein signifikanter Anstieg der ICMP-Flows zu sehen (Typ 8:0). Der Anstieg wird in der Mehrzahl vermutlich durch dial-in erzeugt, die bestimmte Netzwerke scannen, wobei die IP Adresse zufällig gewählt wird. Der Anstieg der ICMP-Pakete ist nicht in allen Netzwerken zu beobachten. Die Sensoren des DFN-CERTs zeigen keine Auffälligkeiten. Allerdings wird der Anstieg beispielsweise vom Switch-CERT mit sehr ähnlicher Charakteristik bestätigt. Die Quelle / Malware ist bislang noch unbekannt. Aufgrund der Vielzahl der scannenden Rechner und der bislang noch unbekannten Quellen vermuten wir im Moment ein höheres Risiko für Angriffe im Internet.

Historie

Stand: **2007-03-13 13:24**

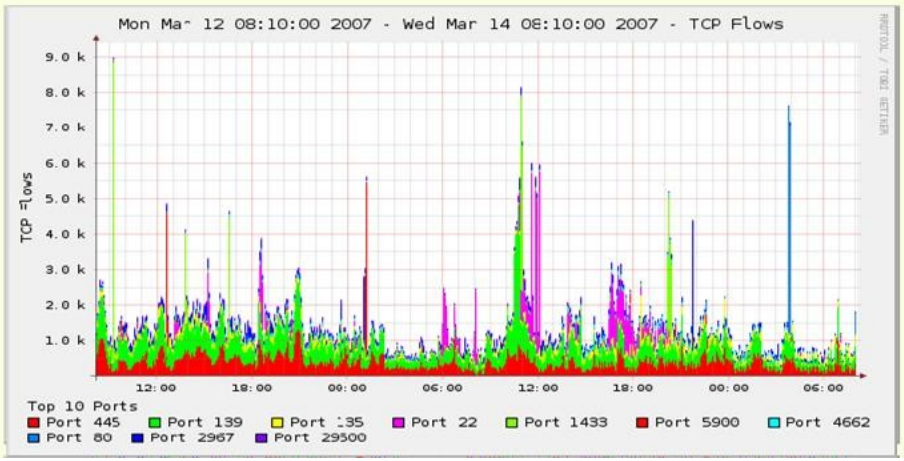
Analysen ausblenden

Angreifer | Ereignisse | Portstatistik

Analyse: Portstatistik

Auswertung nach Ziel-Ports

TCP



Öffentliche Quellen

DFN-CERT Ticker

- 2007-03-13 - Mehrere Schwachstellen in OpenSLP
- 2007-03-13 - Schwachstelle in HP-UX Implementierung des Service Locator Protocol (SLP)
- 2007-03-13 - Schwachstelle in HP-UX Java
- 2007-03-12 - Schwachstellen in Mozilla
- 2007-03-12 - Schwachstellen im Linux Kernel

RUS-CERT Ticker

- [MS/Windows] Malware in vorgeblichen Quelle- und single.de-Rechnungen
- [Cisco/IOS, CatOS] Schwachstelle in der SNMP-Verarbeitung
- [Generic/SNORT] Puffer?berlaufschwachstelle in SNORT
- [MS/Windows] MicrosoftSecurity Bulletin f?r Februar 2007 behebt 20 Schwachstellen
- [Sun/SunOS] telnetd Schwachstelle in SunOS 5.10/5.11

Bisherige Erkenntnisse

Architektur ist operabel und skaliert

- für Massendaten
- Netzwerk-, IDS-Daten und Honeypots
- Policy-gestützter Export / Pseudonymisierung

Kontakte

- Ansprechpartner zum Teilprojekt DGI FG3-6:

  Gerti Foest, Marcus Pattloch

  cert@d-grid.de

- Liste für Sicherheits-Ansprechpartner in Communities und DGI

  dgi-cert@d-grid.de