Nicolas Prigent, Équipe CIDRE, Supélec Campus de Rennes

Visualisation d'Évènements de Sécurité

Contexte

Sécurité préventive
Confidentialité, Intégrité, Disponibilité

- **Objectifs**
  - Contrôler l'accès aux services et aux données.
  - Contrôler la modification des données et des services.
  - Maintenir l'accès aux services et aux données même en cas d'attaque.
- **Outils**
  - Cryptographie.
  - Mécanismes de contrôle d'accès.
  - Programmation sécurisée…

Sécurité réactive
Traçabilité, détection et réaction

- **Objectifs**
  - Détecter une compromission.
  - Comprendre ce qui s'est passé.
  - Corriger.
- **Outils**
  - Générer et stocker un historique le plus complet possible.
  - Protéger cet historique, avec toutes les contraintes précédentes.
  - Exploiter cet historique.

Traitement manuel des données

- Inspecter et traiter les données avec des outils de base (grep, sed, awk, etc.).
- Liberté totale d'exploration.
- Lent, obscur, humain.

Traitement automatique

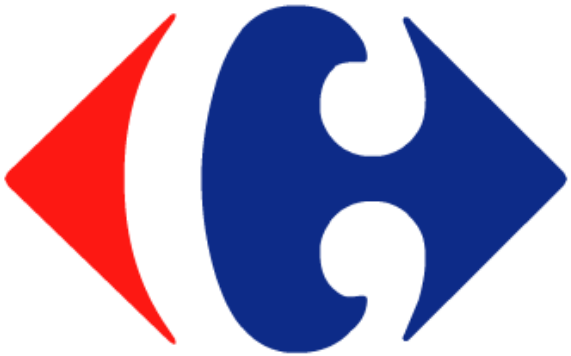
- Laisser des moteurs d'agrégation/corrélation agir.
- Rapide, autonome, automatique.
- Statique , intermédiaire et parfois inefficace face à la quantité de données.

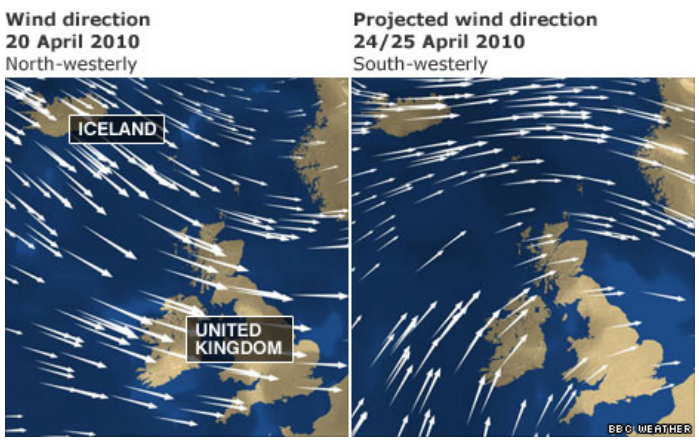
Visualisation

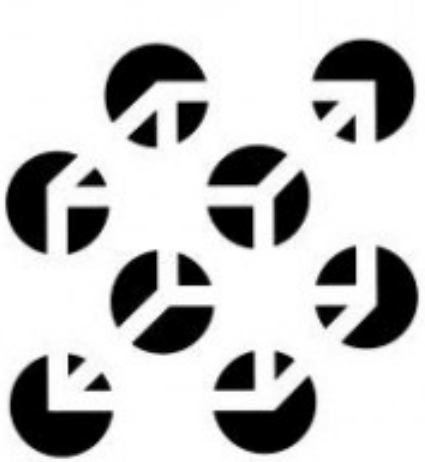
Visualiser ?

- Se servir des capacités de la vision humaine pour faire de la corrélation et de la détection.
- Représenter les informations de manière adéquate afin d'en faciliter la compréhension.
- Prendre en compte les données, le domaine, l'utilisateur et les objectifs.

Gestalt (*proudly not sponsored*)

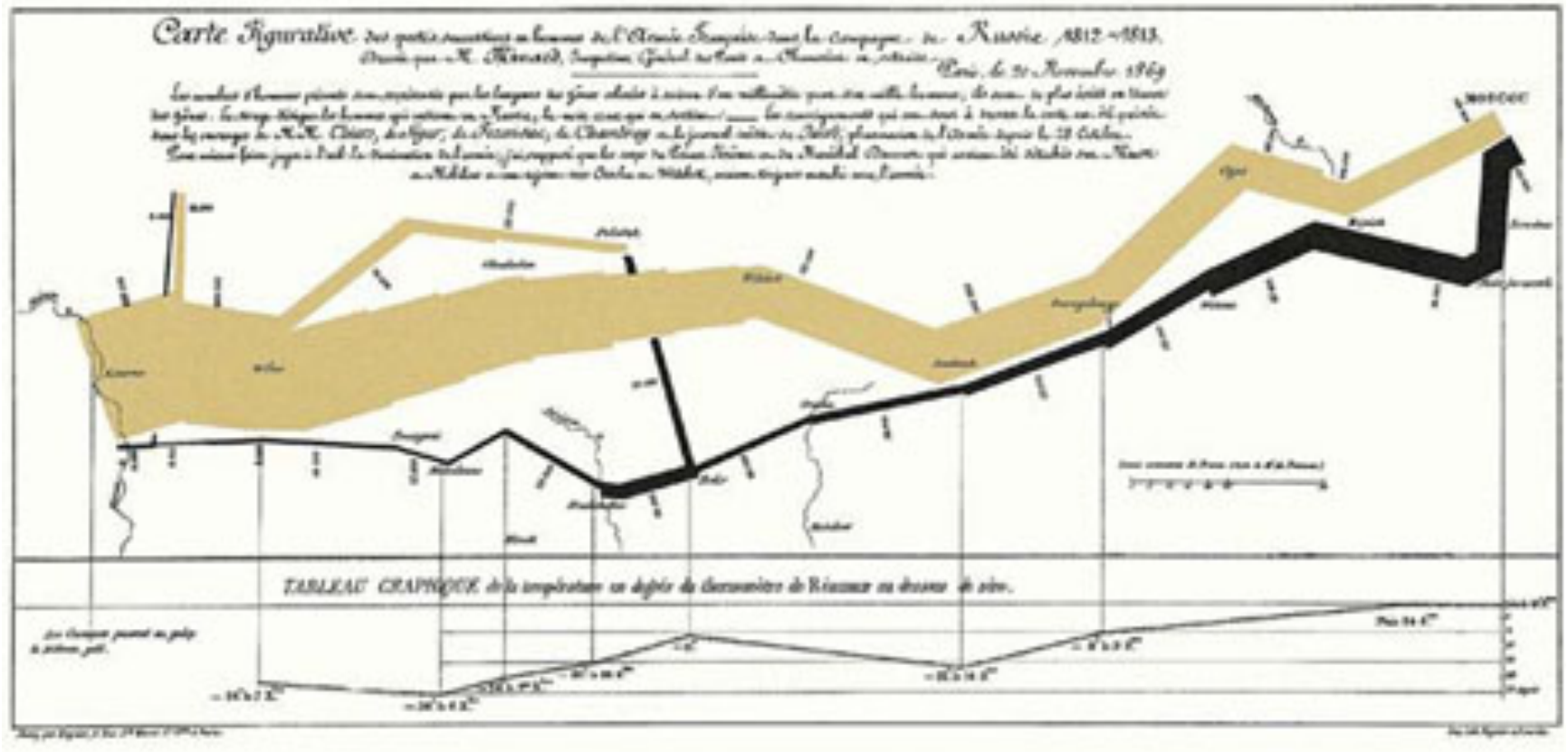






L'Important selon Porsche

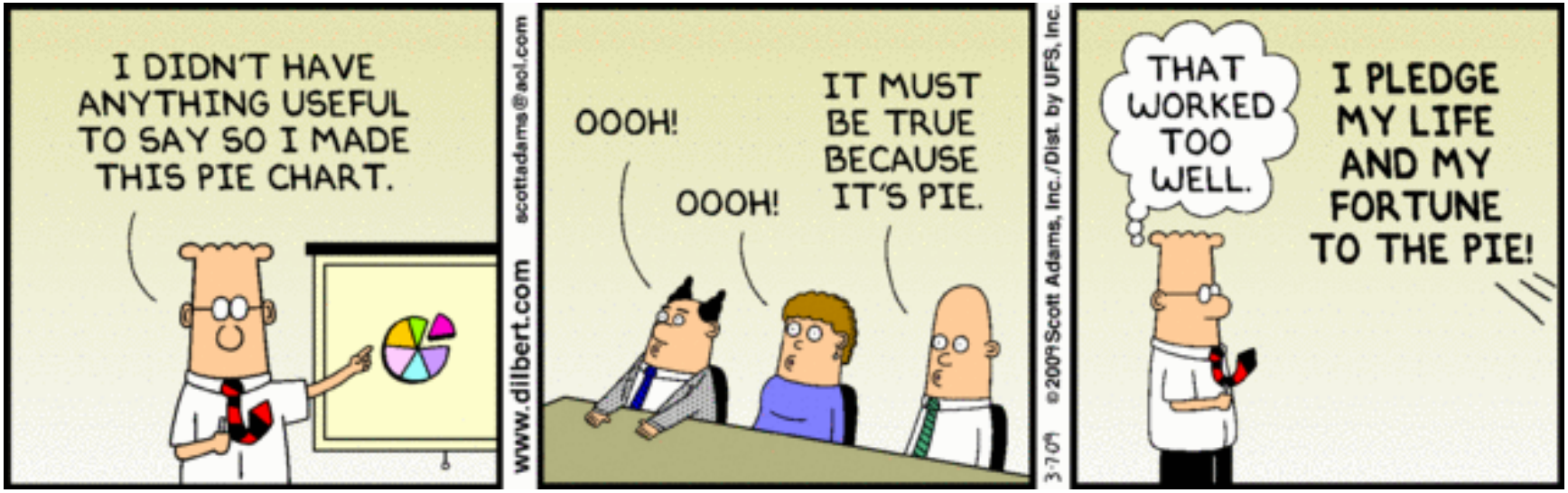
La Bérézina selon Minard



Le Choléra selon John Snow

Ceci n'est pas une carte…

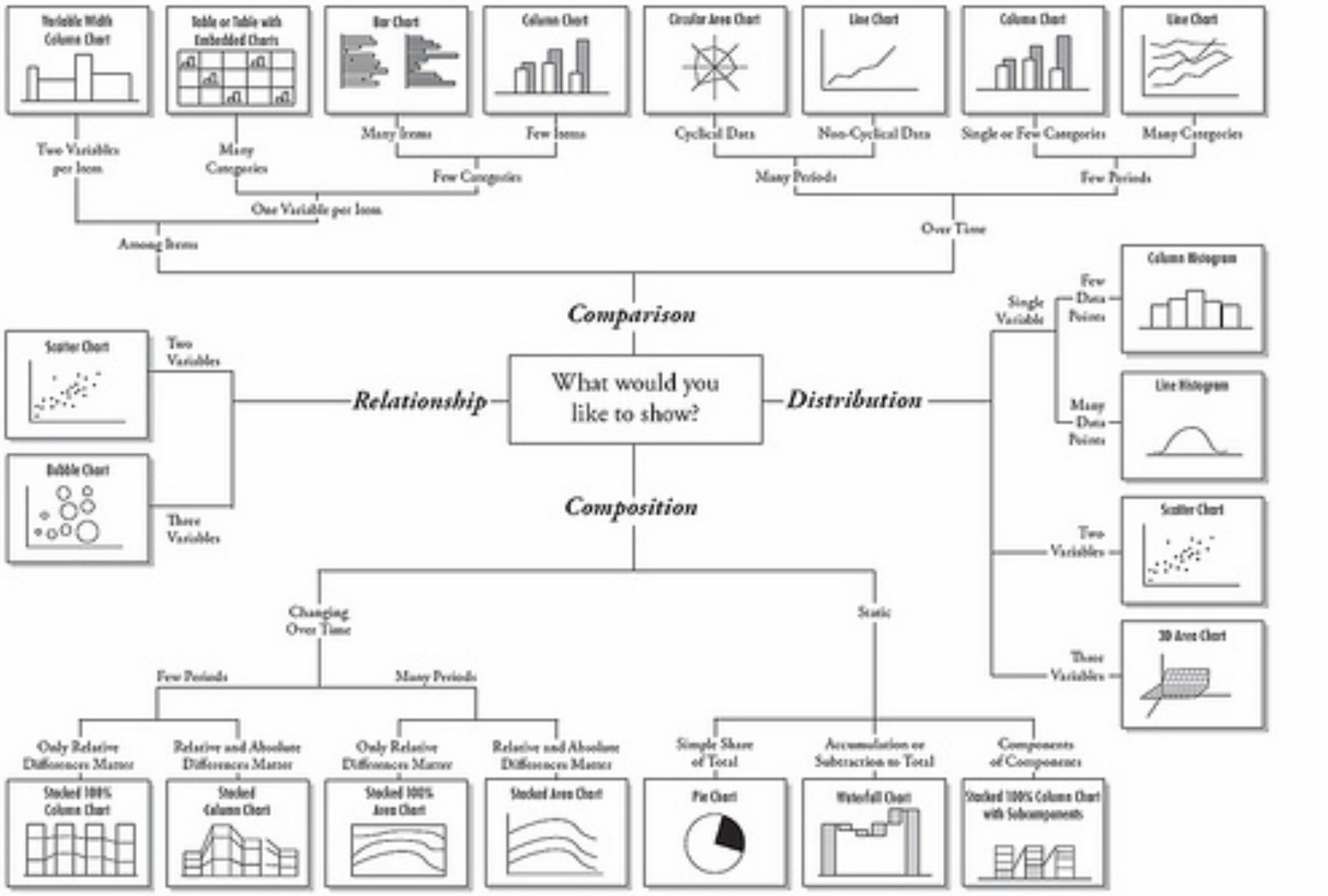
Convaincus ?


I DIDN'T HAVE ANYTHING USEFUL TO SAY SO I MADE THIS PIE CHART.
www.dilbert.com scottadams@aol.com
OOOH!
OOOH!
IT MUST BE TRUE BECAUSE IT'S PIE.
3-7-09 ©2009 Scott Adams, Inc./Dist. by UFS, Inc.
THAT WORKED TOO WELL.
I PLEDGE MY LIFE AND MY FORTUNE TO THE PIE!

Designer et Spécialiste Sécu ?

- Créer des représentations pertinentes est un travail à temps complet.
- Connaissances en design, en statistiques, en psychologie, en sociologie, en esthétique.
- Veille régulière sur l'évolution des techniques.

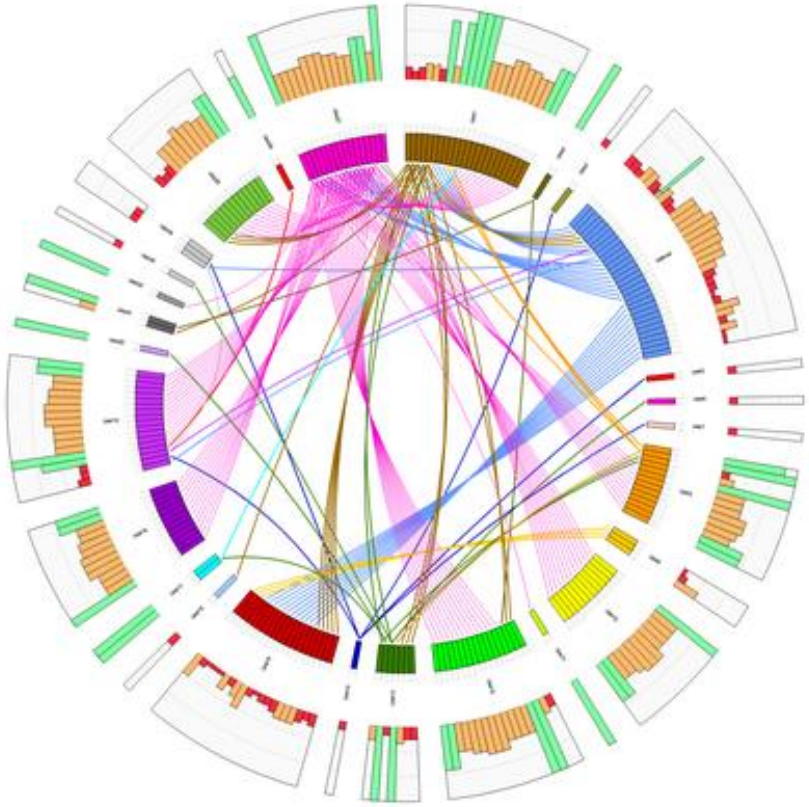
Chart Suggestions—A Thought-Starter



Yeah, Piece o' Cake…

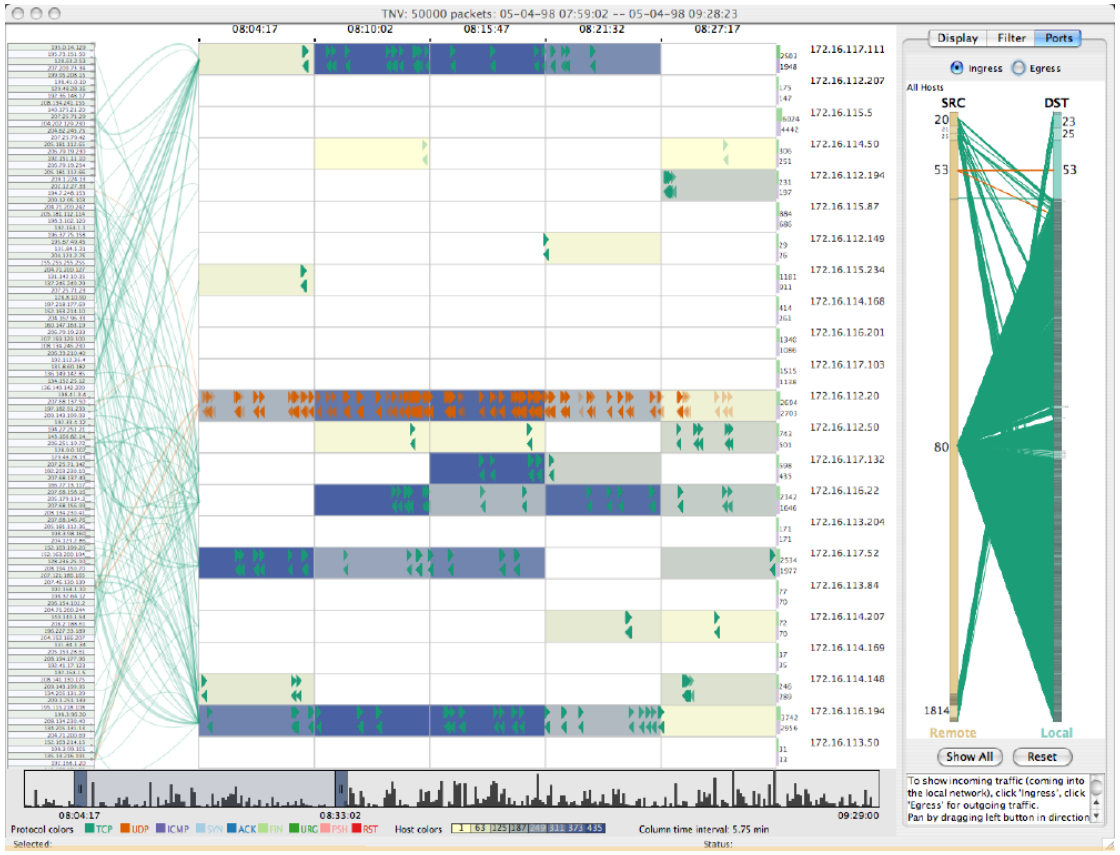
Ou pas…

Ce que font les designers…



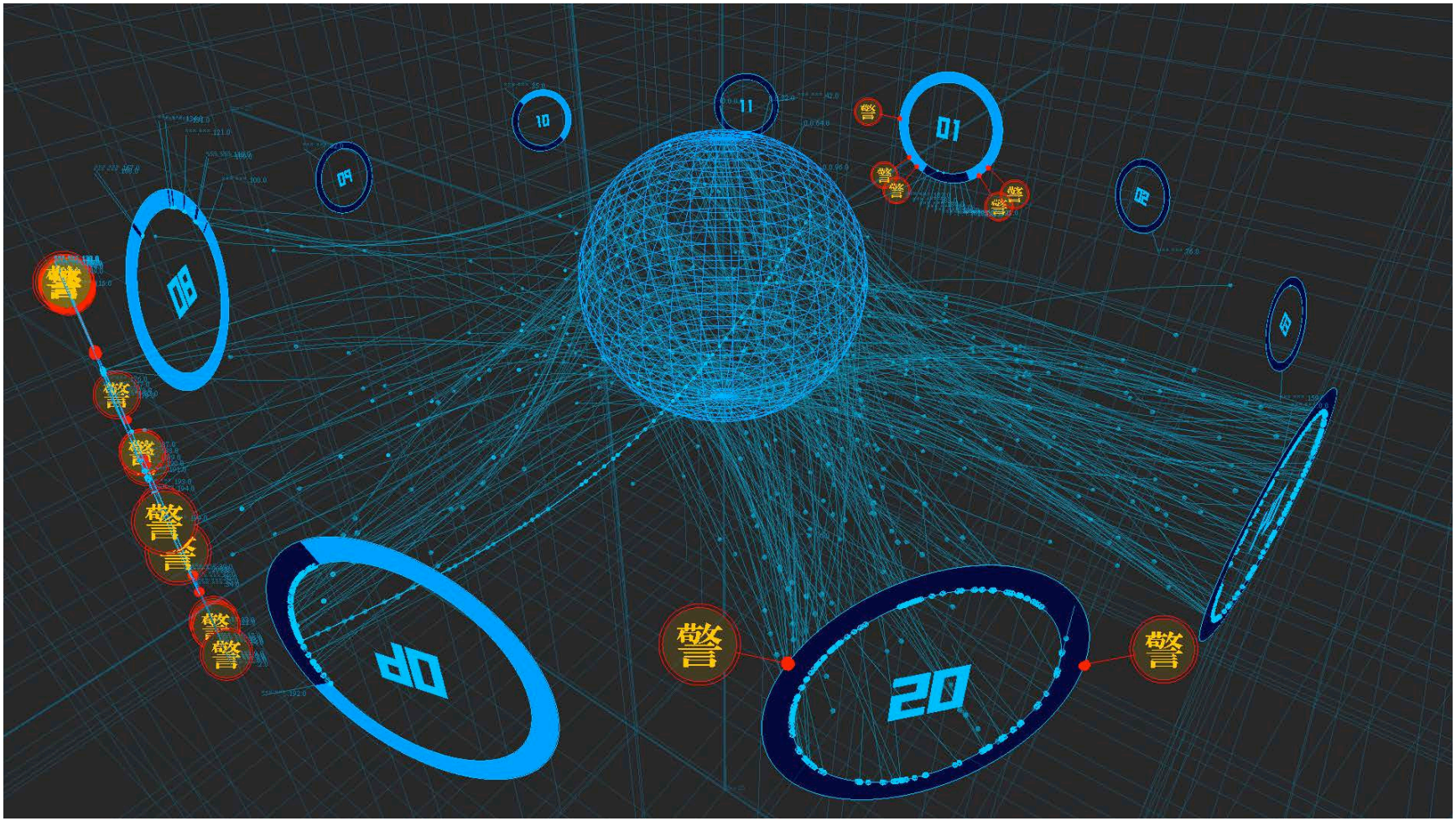
Circos pour la détection des individus impliqués dans la diffusion d'e-mail inappropriés

Ce que font les spécialistes sécu…



TNV et la représentations de pcap

Ce que font les fans de SF



~~Ghost in the Shell~~ Daedalus-VIZ (vs. Darknet)

Évaluer une représentation ?

- Critique par les pairs.
- Tests utilisateurs et questionnaires.
- Approche psycho-cognitive.
- Est-ce que les gens s'en servent ?

Les dimensions cognitives

- Proximité mentale.
- Opérations difficiles.
- Évaluation progressive.
- Viscosité.
- *Et d'autres…*

Green, T. R. G.; Petre, M. (1996). "Usability analysis of visual programming environments: A 'cognitive dimensions' framework".

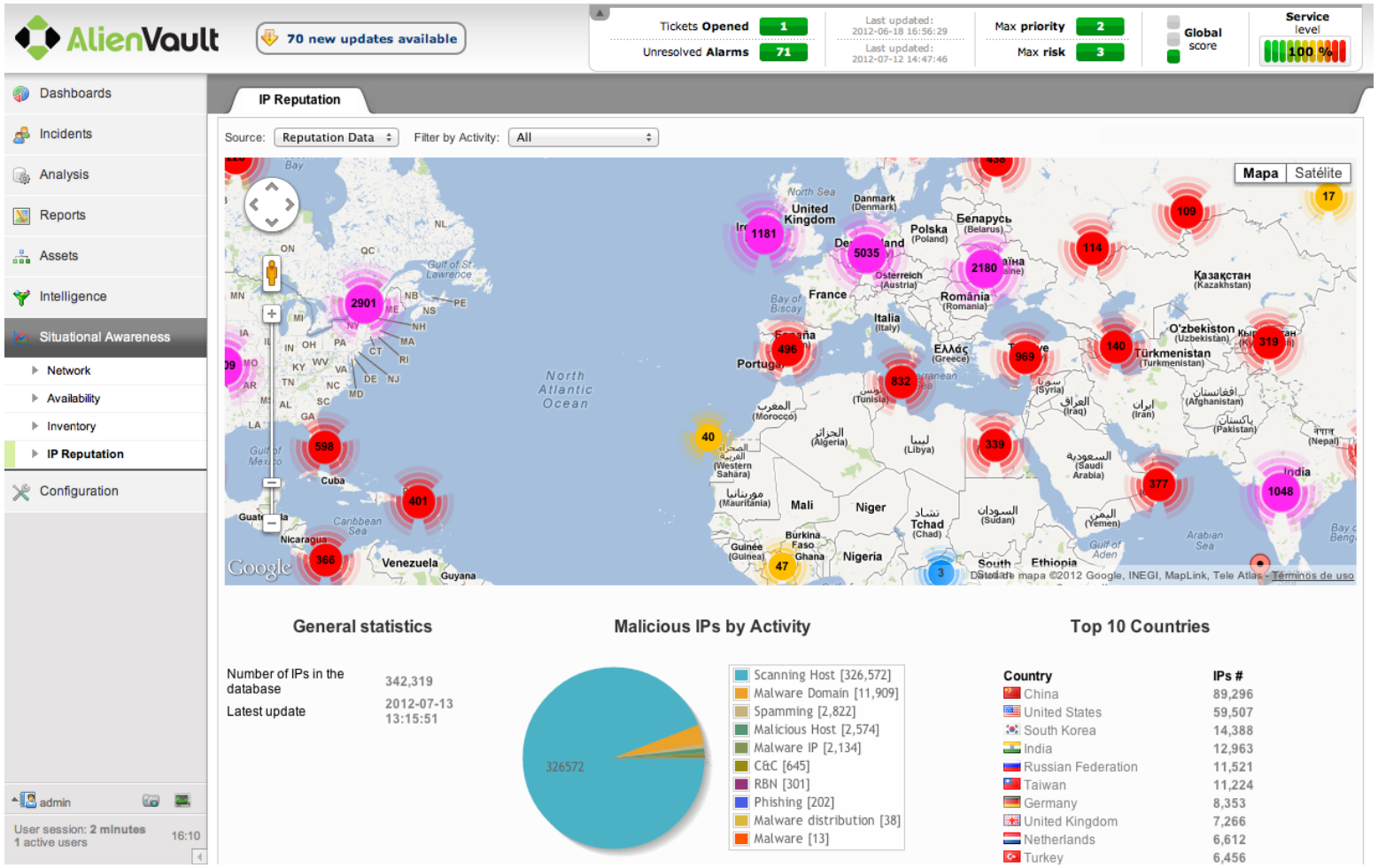
Objectifs de la Visu en Sécu
Une tentative de classification

- Rapporter des informations (*reporting*).
- Surveillance des systèmes (*monitoring*).
- Fouille des données (*forensics*).

Principes du *reporting*

- Communiquer les informations pertinentes sur une situation ou sur son analyse.
- Représenter l'état de la situation.
- Les sujets d'observation sont à peu près figés.
- Peut précéder l'analyse, ou la suivre.

Tableaux de bord

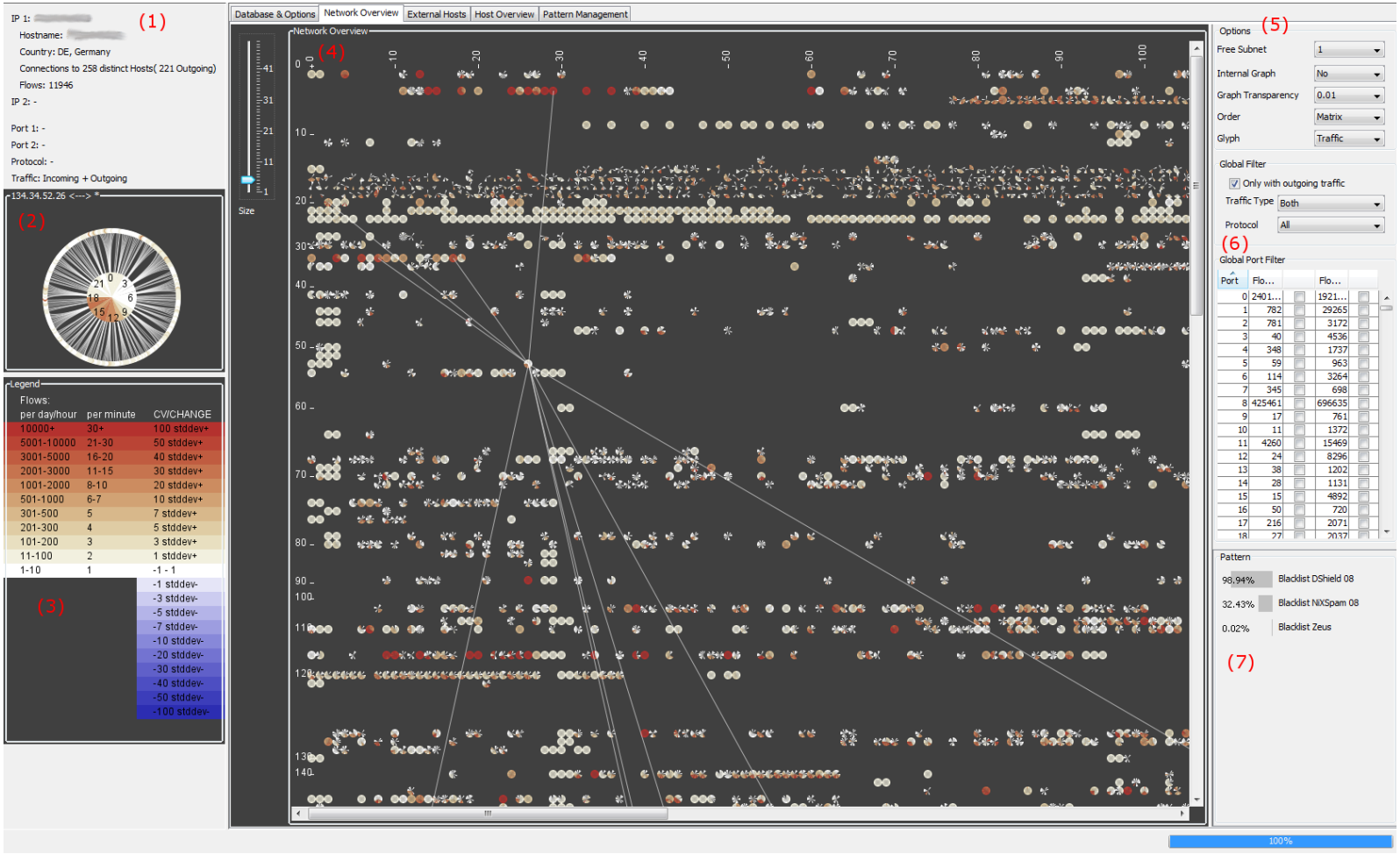


Dashboard AlienVault

Principes du *monitoring*

- Représenter des faits connus en temps réel
- Représentations synthétiques juxtaposées
- Utilisation de codes couleur
- Accès aux détails à la demande

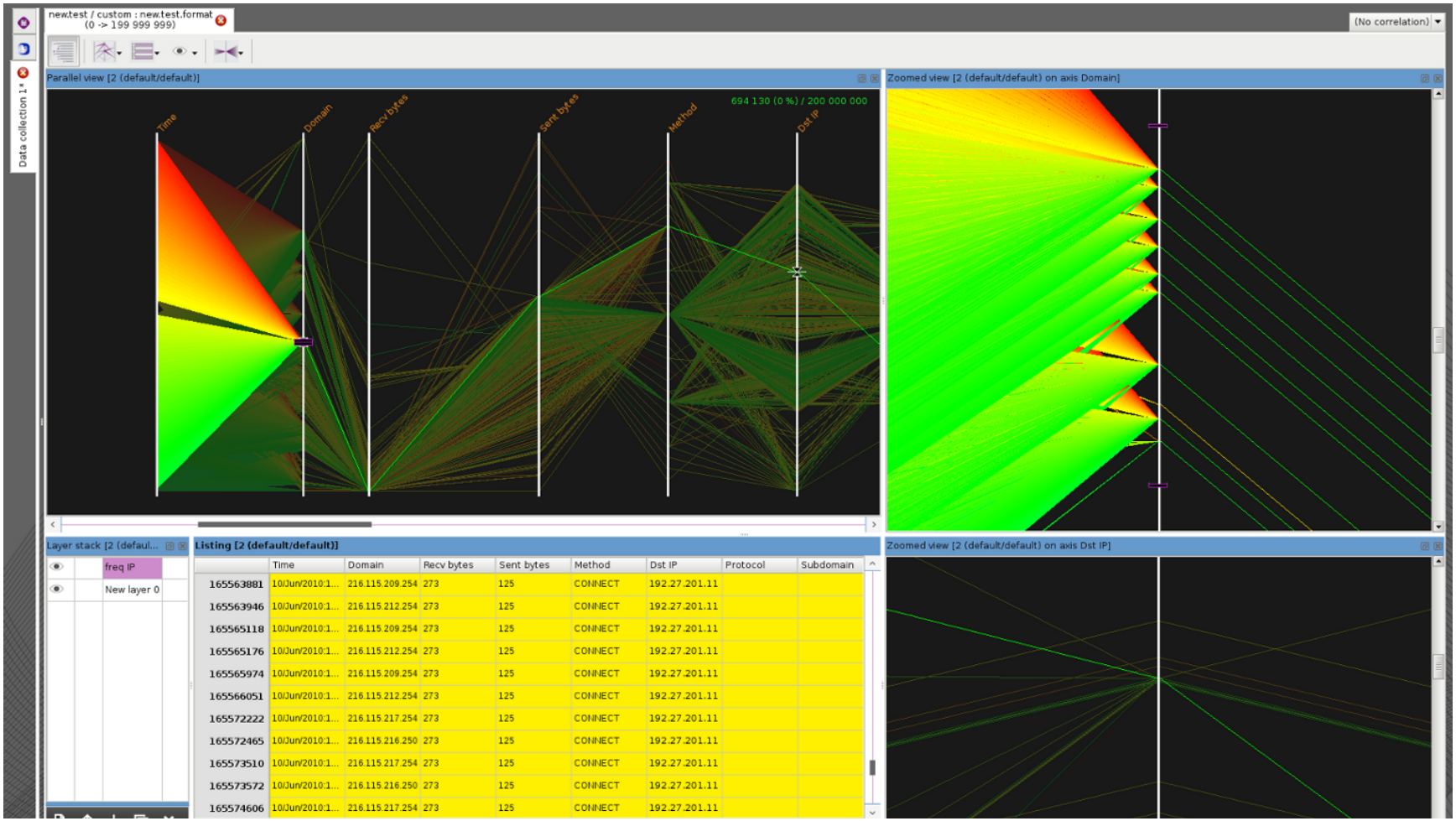
ClockView et la surveillance d'IP



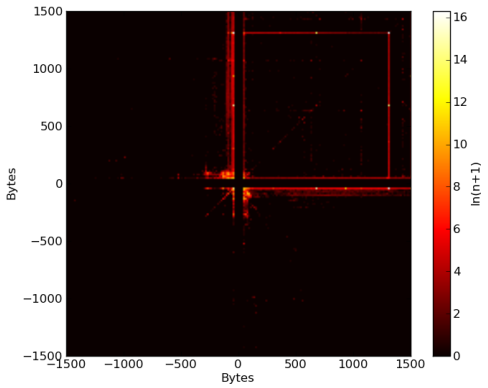
Principes de la fouille

- Représenter *a posteriori* des quantités importantes de données
- Faciliter leur compréhension et leur manipulation
- Pas de connaissance *a priori* de ce qui est recherché par l'analyste

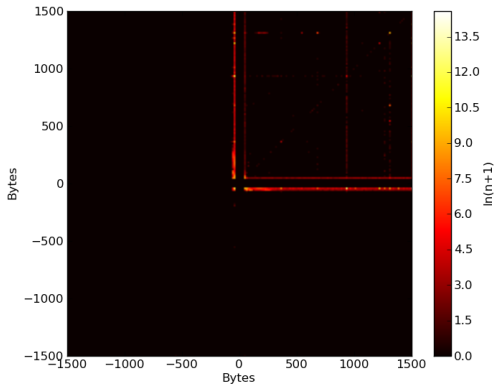
PicViz


new.test / custom : new.test.format
(0 -> 199 999 999)
(No correlation)
Parallel view [2 (default/default)]
694 130 (0 %) / 200 000 000
Time
Domain
Recv bytes
Sent bytes
Method
Dst IP
Zoomed view [2 (default/default) on axis Domain]
Zoomed view [2 (default/default) on axis Dst IP]
Layer stack [2 (defaul...
freq IP
New layer 0
Listing [2 (default/default)]
Time Domain Recv bytes Sent bytes Method Dst IP Protocol Subdomain
165563881 10/Jun/2010:1... 216.115.209.254 273 125 CONNECT 192.27.201.11
165563946 10/Jun/2010:1... 216.115.212.254 273 125 CONNECT 192.27.201.11
165565118 10/Jun/2010:1... 216.115.209.254 273 125 CONNECT 192.27.201.11
165565176 10/Jun/2010:1... 216.115.212.254 273 125 CONNECT 192.27.201.11
165565974 10/Jun/2010:1... 216.115.209.254 273 125 CONNECT 192.27.201.11
165566051 10/Jun/2010:1... 216.115.212.254 273 125 CONNECT 192.27.201.11
165572222 10/Jun/2010:1... 216.115.217.254 273 125 CONNECT 192.27.201.11
165572465 10/Jun/2010:1... 216.115.216.250 273 125 CONNECT 192.27.201.11
165573510 10/Jun/2010:1... 216.115.217.254 273 125 CONNECT 192.27.201.11
165573572 10/Jun/2010:1... 216.115.216.250 273 125 CONNECT 192.27.201.11
165574606 10/Jun/2010:1... 216.115.217.254 273 125 CONNECT 192.27.201.11

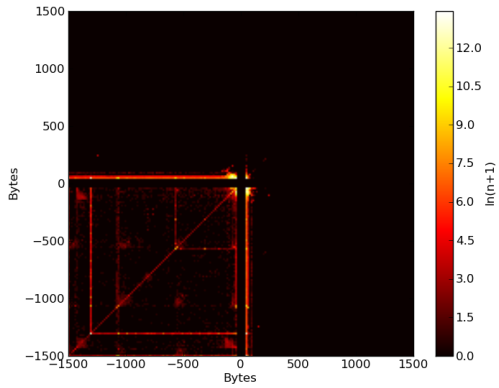
Voir plus loin que le port...



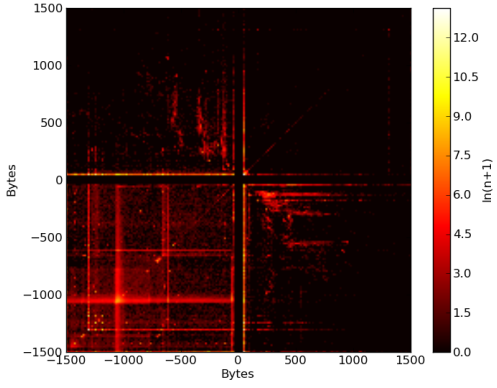
(a) SMTP



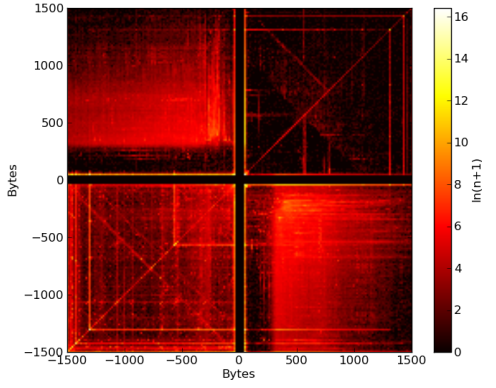
(b) LPD



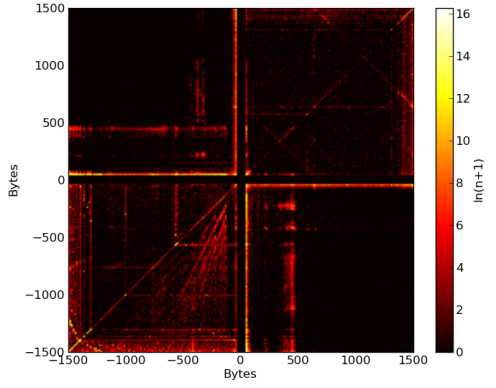
(c) POP



(d) RTSP

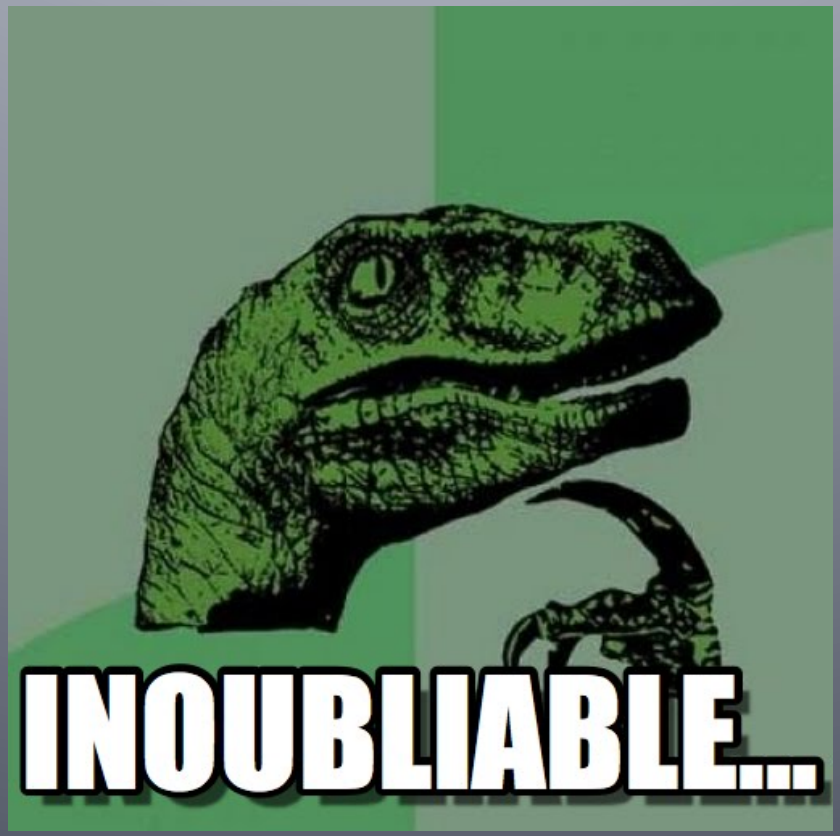


(e) HTTP



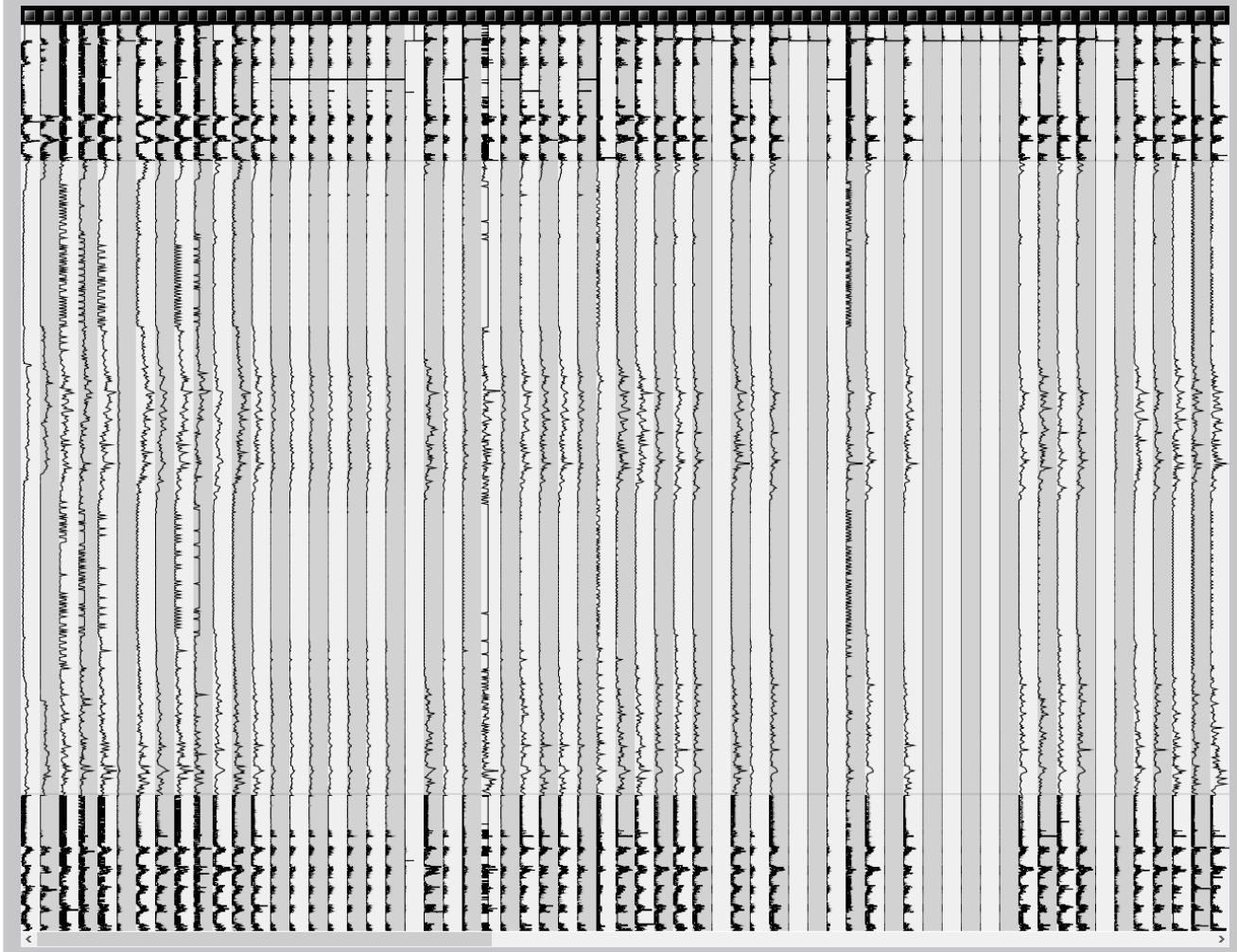
(f) Kazaa

Vu à VizSec 2013



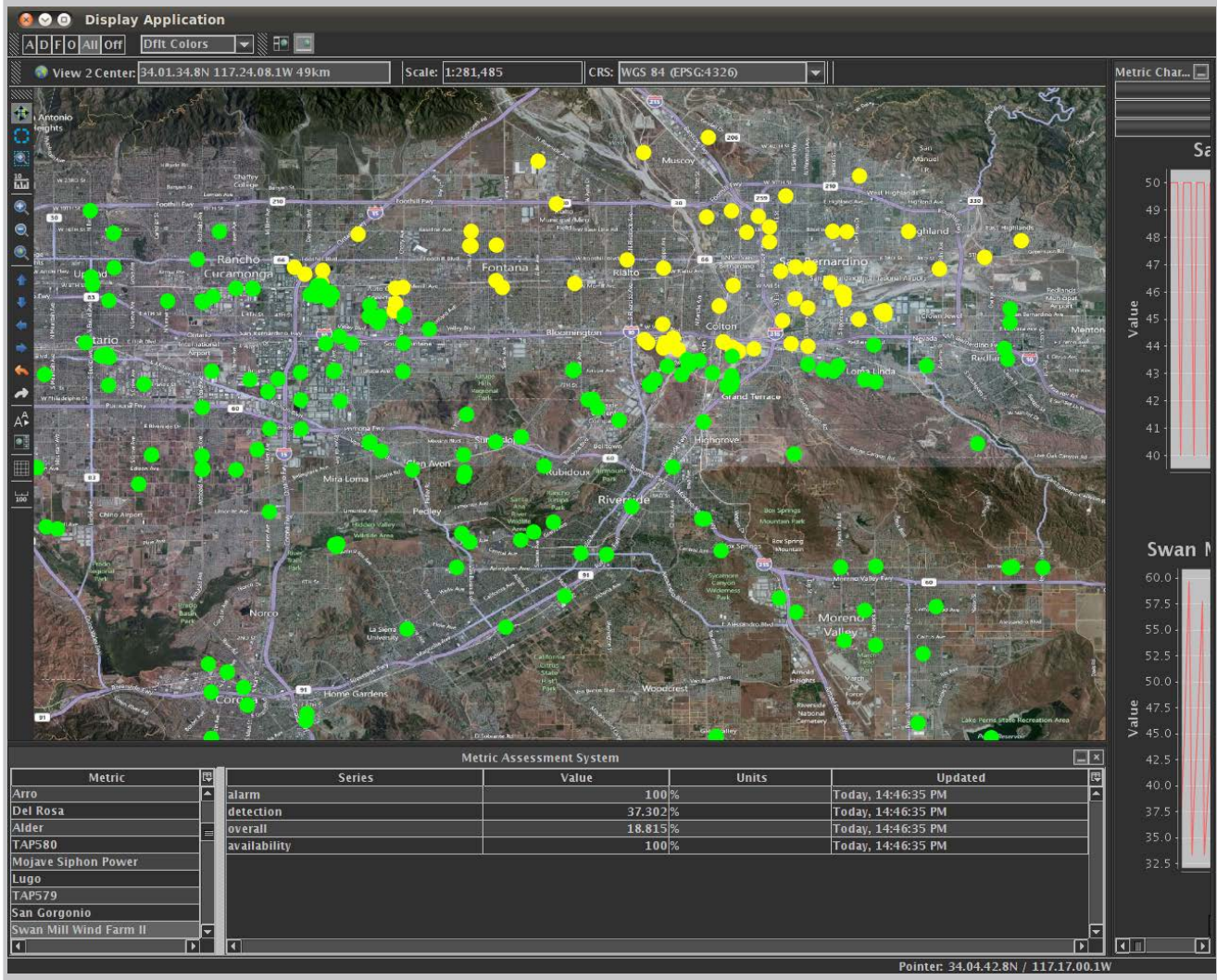
Finding Anomalies in Time-Series using Visual Correlation for Interactive Root Cause Analysis

Florian Stoffel, Fabian Fischer, Daniel Keim



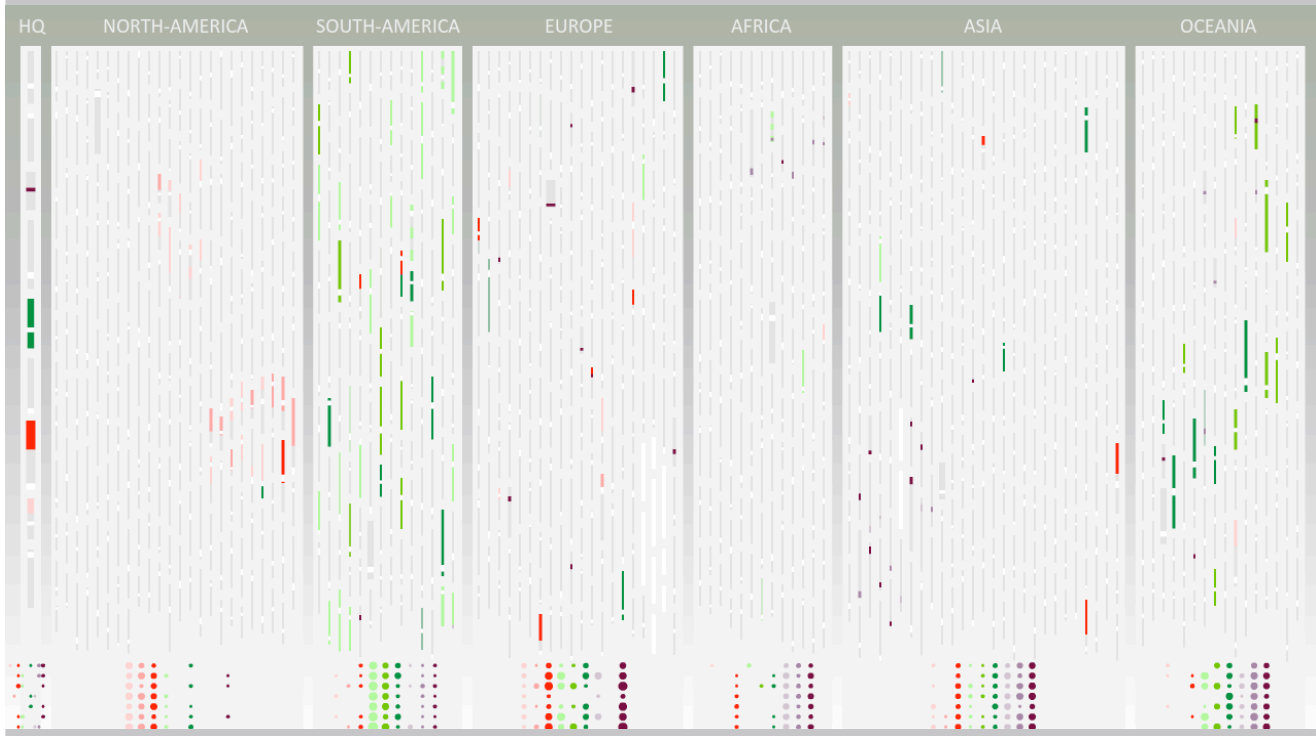
CyberSAVe - Situational Awareness Visualization for Cyber Security of Smart Grid Systems

Lisa Dipippo, William Matuszak, Yan Lindsay Sun



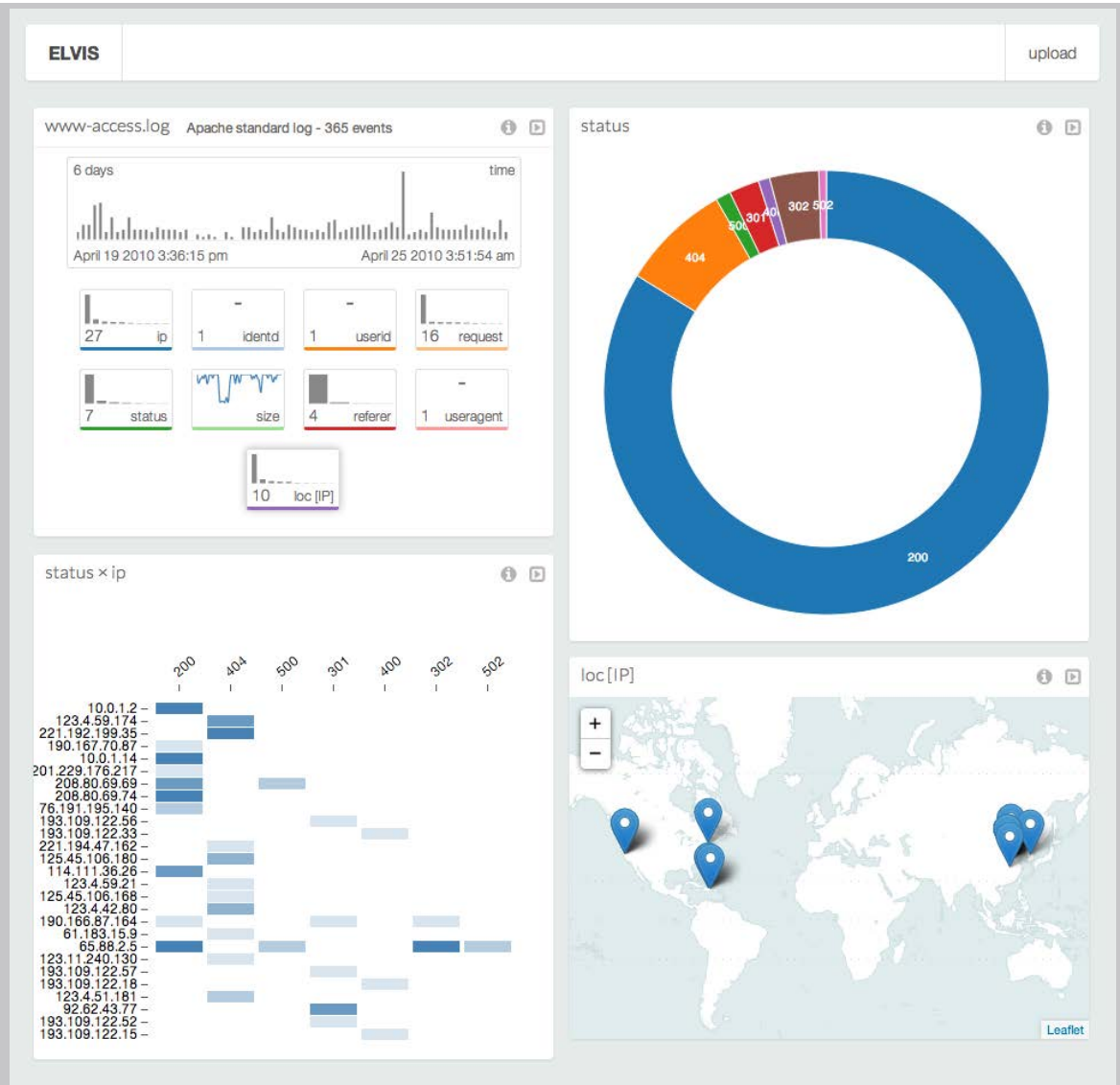
SpringRain: An Ambient Information Display

Marlen Promann, Yue (Aaron) Ma, Shuang Wei, Weiran (Tyki) Lei, Jack Shen-Kuen Chang, Zhenyu Cheryl Qian, Yingjie Victor Chen



Elvis: Extensible Log VISualization

C. Humphries, N. Prigent, C. Bidan, F. Majorczyk



Nous contacter

@neekop

@egleek