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.

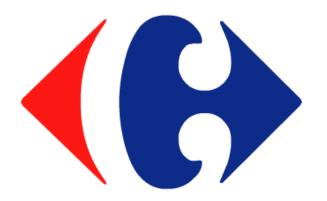
Visualisation



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)

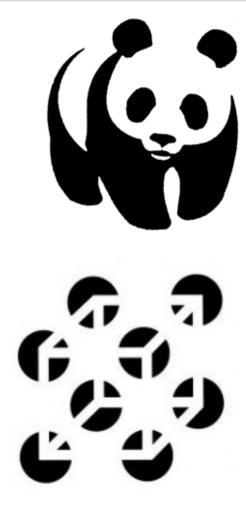


Wind direction 20 April 2010 North-westerly



Projected wind direction 24/25 April 2010 South-westerly

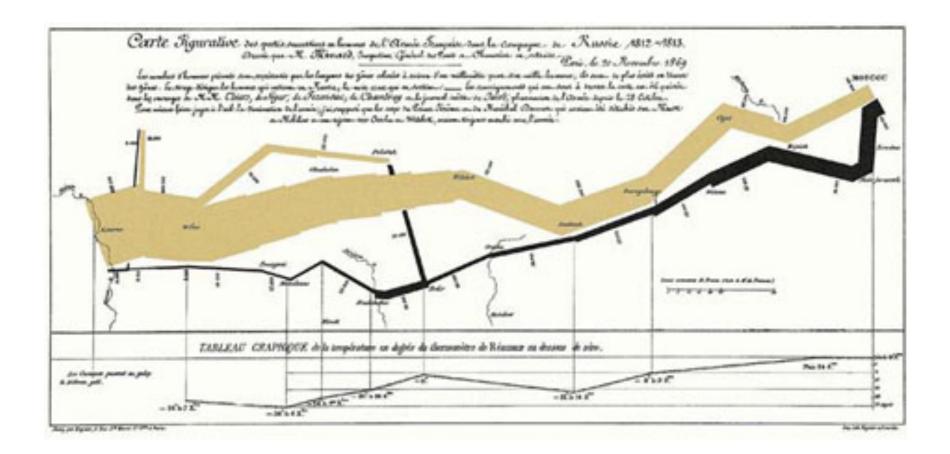




L'Important selon Porsche



La Bérézina selon Minard



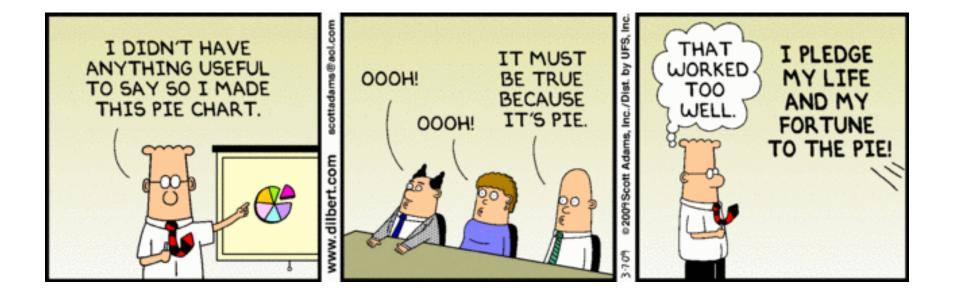
Le Choléra selon John Snow



Ceci n'est pas une carte...



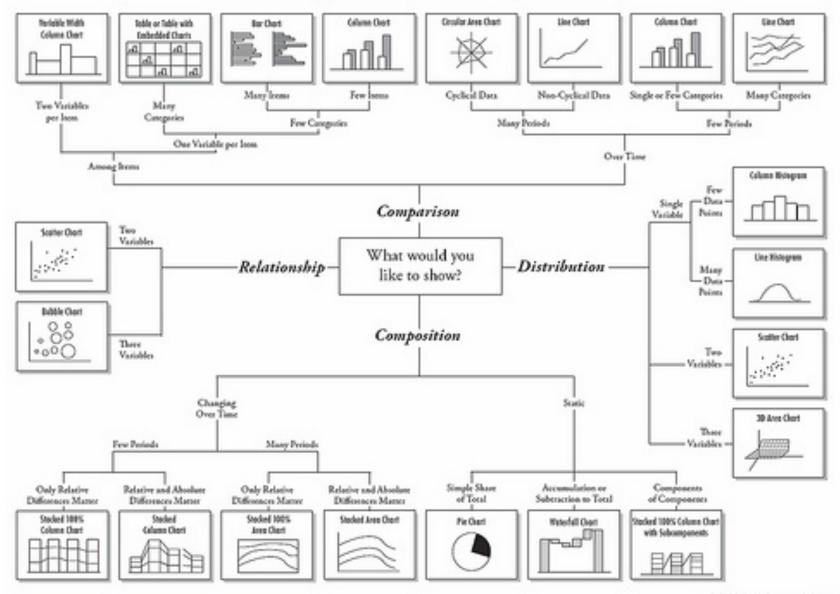
Convaincus?



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.

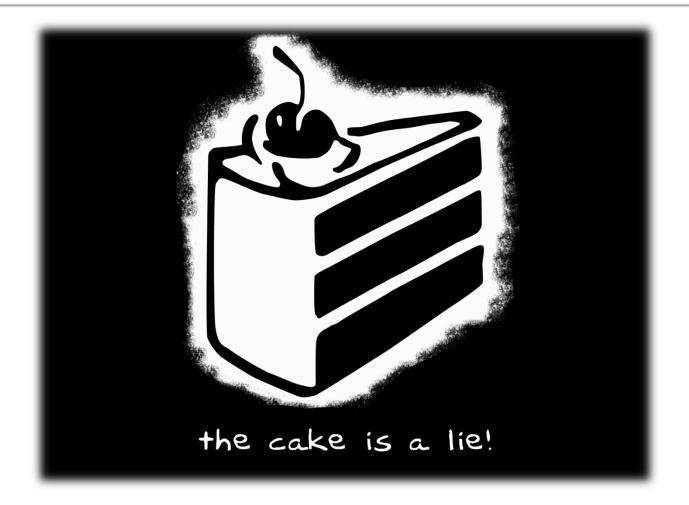
Chart Suggestions—A Thought-Starter



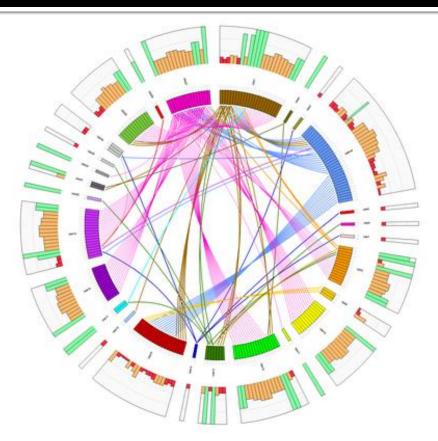
Yeah, Piece o' Cake...



Ou pas...

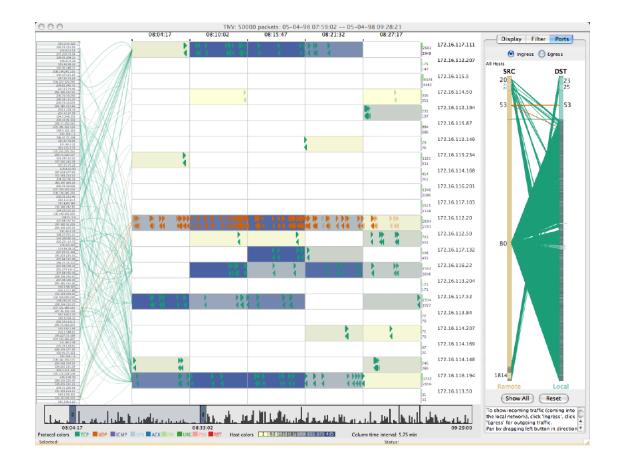


Ce que font les designers...



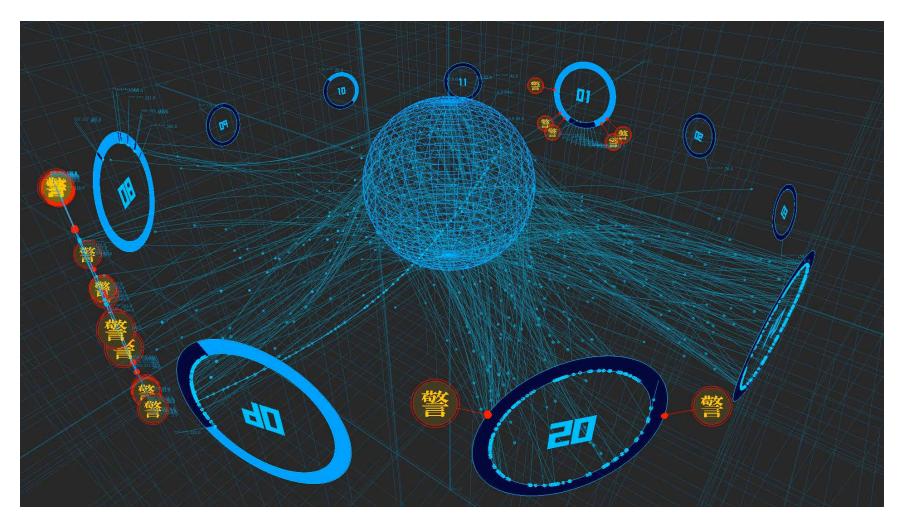
Circos pour la détection des individus impliqués dans la diffusion d'e-mail inappropriés

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*).

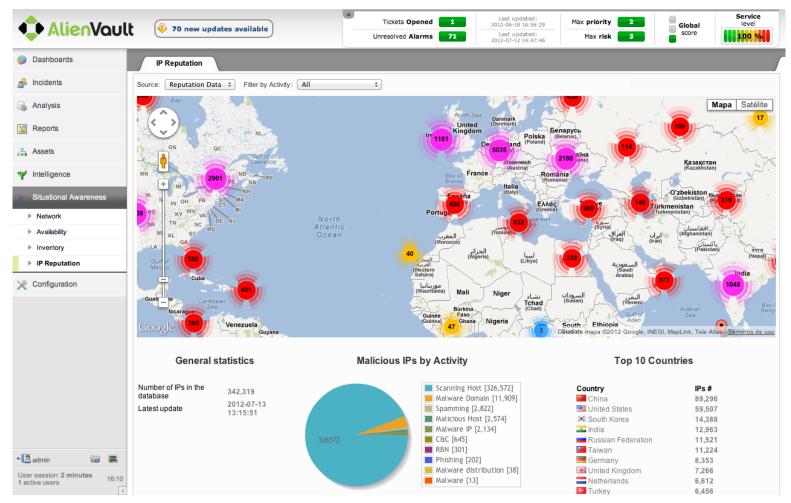
Surveillance des systèmes (*monitoring*).

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

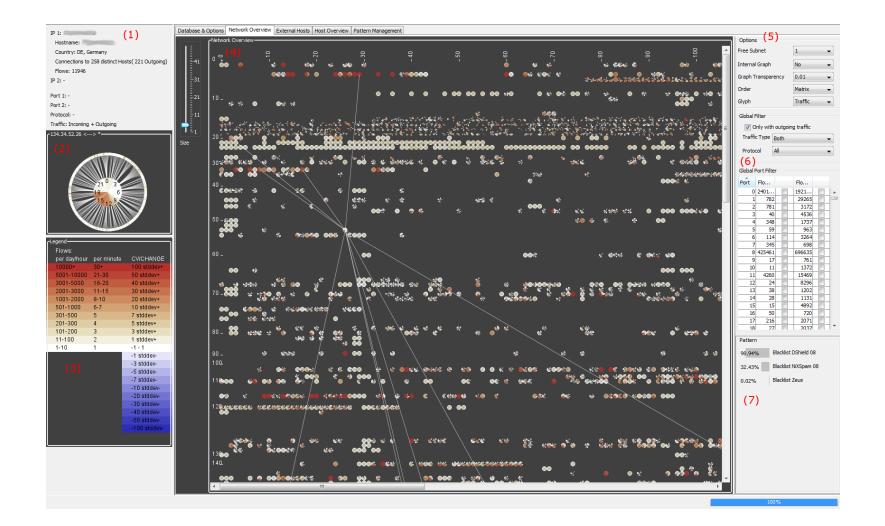


Dashboard AlienVault

Principes du *monitoring*

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

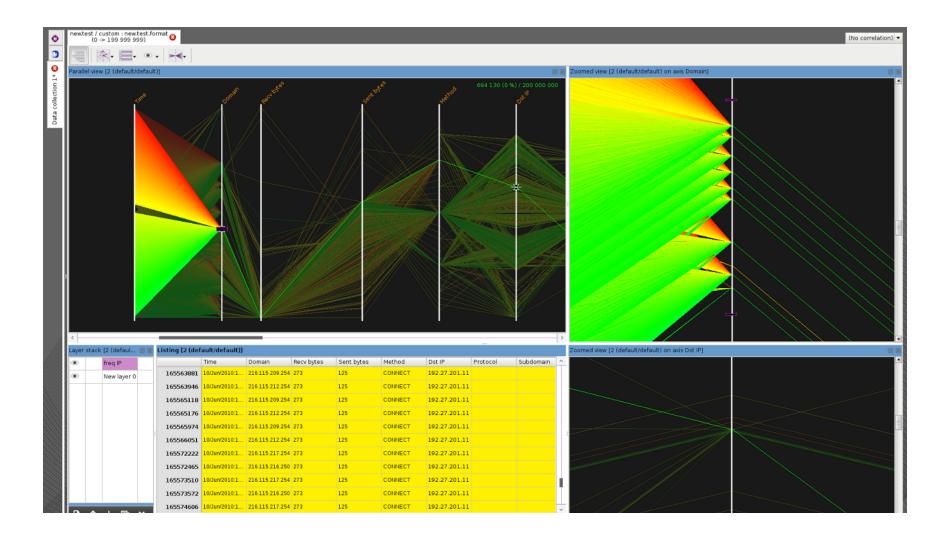
ClockView et la surveillance d'IP



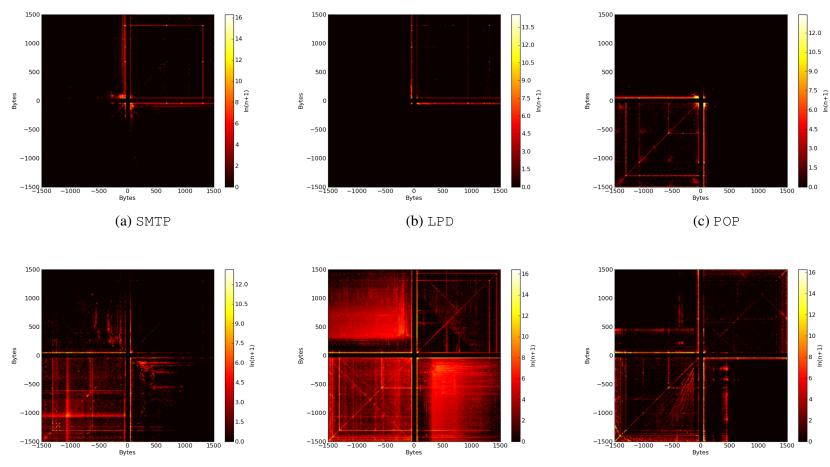
Principes de la fouille

- 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



Voir plus loin que le port...

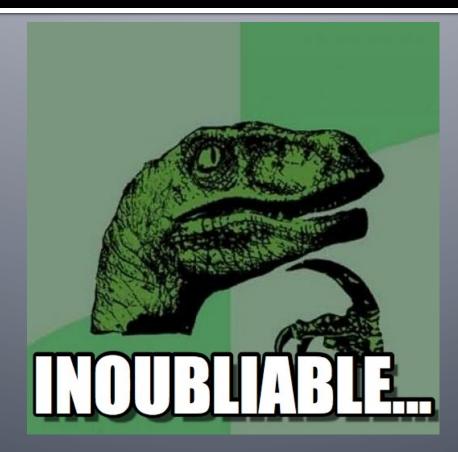


(d) RTSP



(f) Kazaa

Vu à VizSec 2013



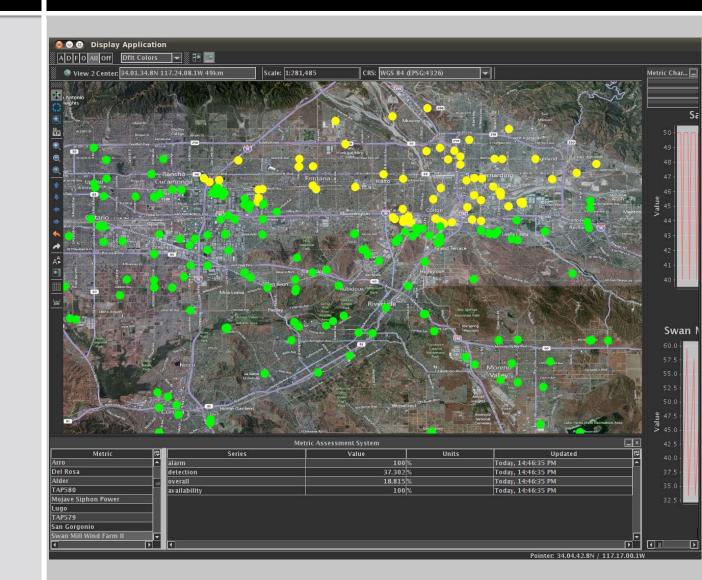
Finding Anomalies in Time-Series using Visual Correlation for Interactive Root Cause Analysis

Florian Stoffel, Fabian Fischer, Daniel Keim

		and the second se	1 martin and the second se	
			WINNING ALLINGUNUNANGALALAAAAAAAAAAAAAAAAAAAAAAAAAAA	
		~~~Mukhanahahahahahahan	[ [	
		-		
			Mary and	
		A AL MA MA MA MA MA MANNA	ALIANDAL ALIANDALIANANA	
	The second se	w v v v v v	man man man	
				Junior States
	No. of Lot of Lo	Anna management and the second s	Lanna and and and and and and and and and	Contraction of the second second
		~~~~~~~~		
			A	
	and the state are			the state of the s
		and the second s		Land Land Market
	and the state of the	and a superior and the second s		in the second
	-			-
			and and the second and the second and the	
	al da ann can			
		have a second and the second	and the manufacture of the second sec	A
	n mit bie ficherneber	4 Y Y	Y W 4	
	and the state state			the second s
			the second secon	
			when the second when the second	
			- address and the second s	
	and a state of the	man have been a have been a have been and been a	m &	المراقع المحلوم المراقع والمحال
		and an	- WOWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW	-
		A second s	and a new production of the second seco	
		and the second	and the second	A COLORED AND A
	A AL	m		and the second second
		man man man and and and and and and and and and a		
	-			
		and and a second s	- Algert and the for the second s	
	A A A	An and a summer show have been and a second se	and the second	
	-	-	-	
	-			
			and the second s	
	A A A	have been a second	- Marine	
اف الالانجيب من ال مدارعة من المستقدمة من المن المحالية المحالية من الانتخابية المحالية المحالية المحالية المح وفي الانتخابية المحالية المحالي ومحالية المحالية المح ومحالية المحالية الم المحالية المحالية المح والمحالية المحالية المح والمحالية المحالية ا والمحالية المحالية ا والمحالية المحا				
لف الالانويوس الإسدانية من المستقدين المستقد العامل من المانويون المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستقد المستق والمستقد المستقد المستق والمستقد المستقد المستق				
Image: State				
الله الإسراح المارية ال المارية المارية ال المارية المارية ا المارية المارية الم				
bis Methodowerski served server s	L.A.A.	- An and the second sec		
in solutions in the solution of the solution o				
in second s			to shark when h	
bis Shirker on the second s bis second se bis second s bis second sec	and the second	And the second sec	Į	
bi Shikana sa		Same and the second sec	- Address and many and many and	
bis sectors and sectors sectors sectors and sectors se				
ki Shikawan Sana Sana Sana Sana Sana Sana Sana	بالمحادين المحاجبين المراجع			and the second
bi Shikawa sa				
La	-			
لىلىىلەنچەر مەرىكى، مەرىپىلەر مەرىپى مەرىپىيەت مەرىپىيەت مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر م لىلىىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپىيەر مەرىپى			and the second s	
La Martine management and a second	11 A. A. 11	man market and the second and the se		
have a man and a second a second and a second a		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	monorman was a second and an adapted	
M. M. Martin and M. Land			and the second s	
			And Marthank	

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

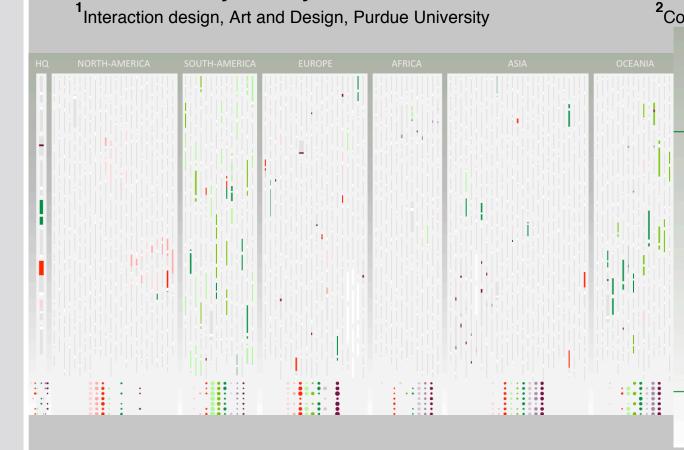
Lisa Dipippo, William Matuszak, Yan Lindsay Sun



SpringRain: An Ambient Information Display

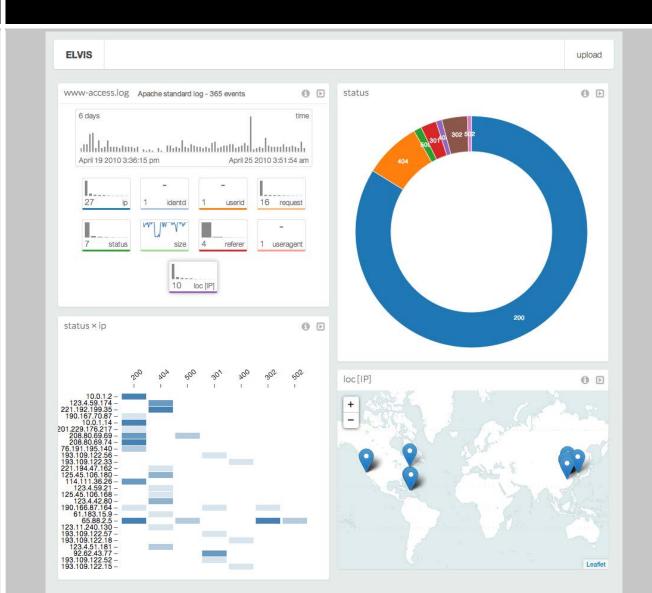
Marlen Promann, Yue (Aaron) Ma, Shuang Wei, Weiran (Tyki) Lei, Jack Shen-Kuen Chang, Zhenyu Cheryl Qian, Yingjie Victor Chen

Zhenyu Cheryl Qian¹



Elvis: Extensible Log VISualization

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



Nous contacter

