PV210 Bezpečnostní analýza síťového provozu

Automatické systémy detekce a vizualizace toků

Pavel Čeleda

29. 10. 2014

Opakování

Systémy pro detekci útoků/anomálií

Vizualizace a toky

Co již znáte

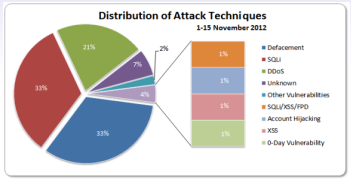
Proč?

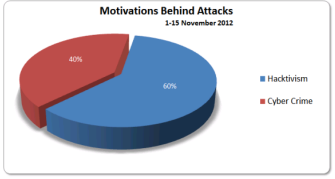
Network Flow 2012: Year in Review

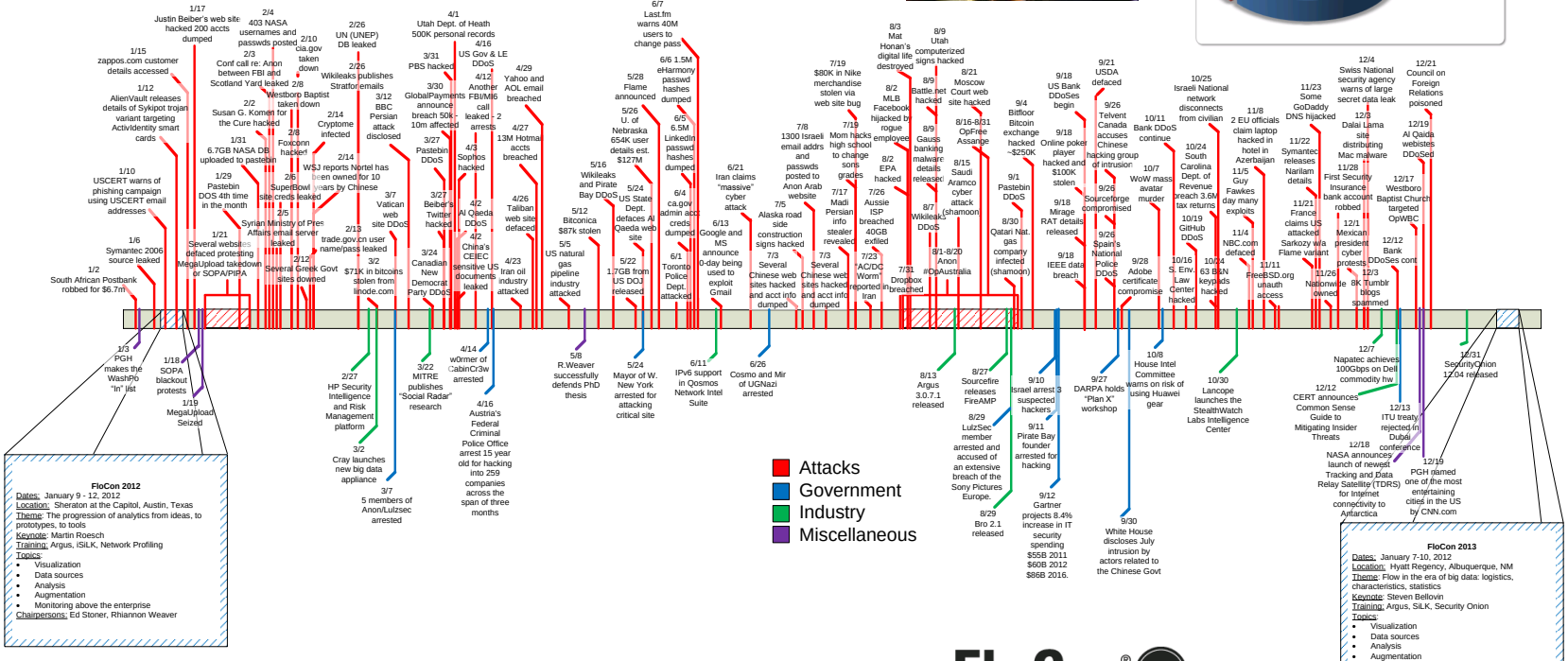
CERT
@GeoWarnagiris
gwarnagi@cert.org

Software Engineering Institute | Carnegie Mellon

- Attacks
- Government
- Industry
- Miscellaneous







FloCon 2012

Dates: January 9 - 12, 2012
Location: Sheraton at the Capitol, Austin, Texas
Theme: The progression of analytics from ideas, to prototypes, to tools
Keynote: Martin Roesch
Training: Argus, SiLK, Network Profiling
Topics:
- Visualization
- Data sources
- Analysis
- Augmentation
- Monitoring above the enterprise

Chairpersons: Ed Stoner, Rhiannon Weaver

- Attacks
- Government
- Industry
- Miscellaneous

FloCon 2013

Dates: January 7-10, 2012
Location: Hyatt Regency, Albuquerque, NM
Theme: Flow in the era of big data: logistics, characteristics, statistics
Keynote: Steven Bellovin
Training: Argus, SiLK, Security Onion
Topics:
- Visualization
- Data sources
- Analysis
- Augmentation
- Signature vs. anomaly detection
- Real time vs. near real time

Chairpersons: Rhiannon Weaver, George Jones, Donovan Truitt

FloCon®

Network Flow 2012: Year in Review

CERT
@GeoWarnagiris
gwarnagi@cert.org

Software Engineering Institute | Carnegie Mellon

Credit to:
http://hackmageddon.com
@paulsparrows

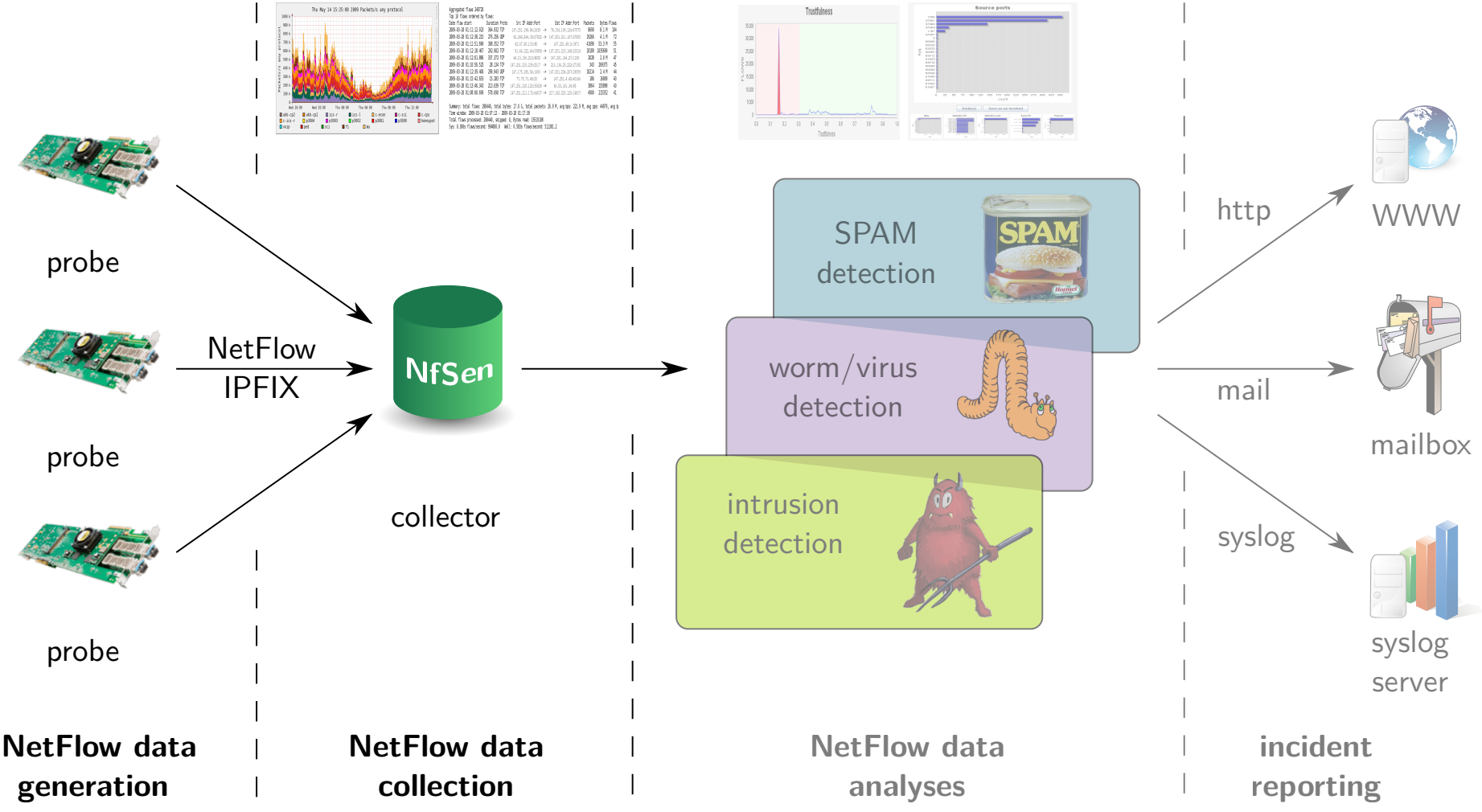
Co již znáte

- Schopnost zachytávat velké množství dat z celé sítě
- V datech mohou být obsaženy nové informace o bezpečnostních událostech

Co již znáte

Jak?

Co již znáte


probe
probe
probe
NetFlow
IPFIX
NfSen
collector
SPAM
detection
SPAM
worm/virus
detection
intrusion
detection
http
mail
syslog
WWW
mailbox
syslog
server
NetFlow data
generation
NetFlow data
collection
NetFlow data
analyses
incident
reporting

Co již znáte

Co?

Co již znáte

Charakteristika naměřených dat

- **Základní charakteristiky provozu:** časová značka, zdrojová/cílová IP, číslo zdrojového/cílového portu, typ protokolu, objem provozu, TCP příznaky ...
- **Rozšiřující charakteristiky:** zeměpisná poloha, HTTP doména, user agent, typ aplikace ...
- **Odvozené charakteristiky:** počet toků do destinací z dané IP, počet toků do cílové IP využívající stejný zdrojový port ...

Jak cennou informaci tyto data nesou, jak ji získat?

Co ještě neznáte

Co s tím?

Co ještě neznáte

IDS

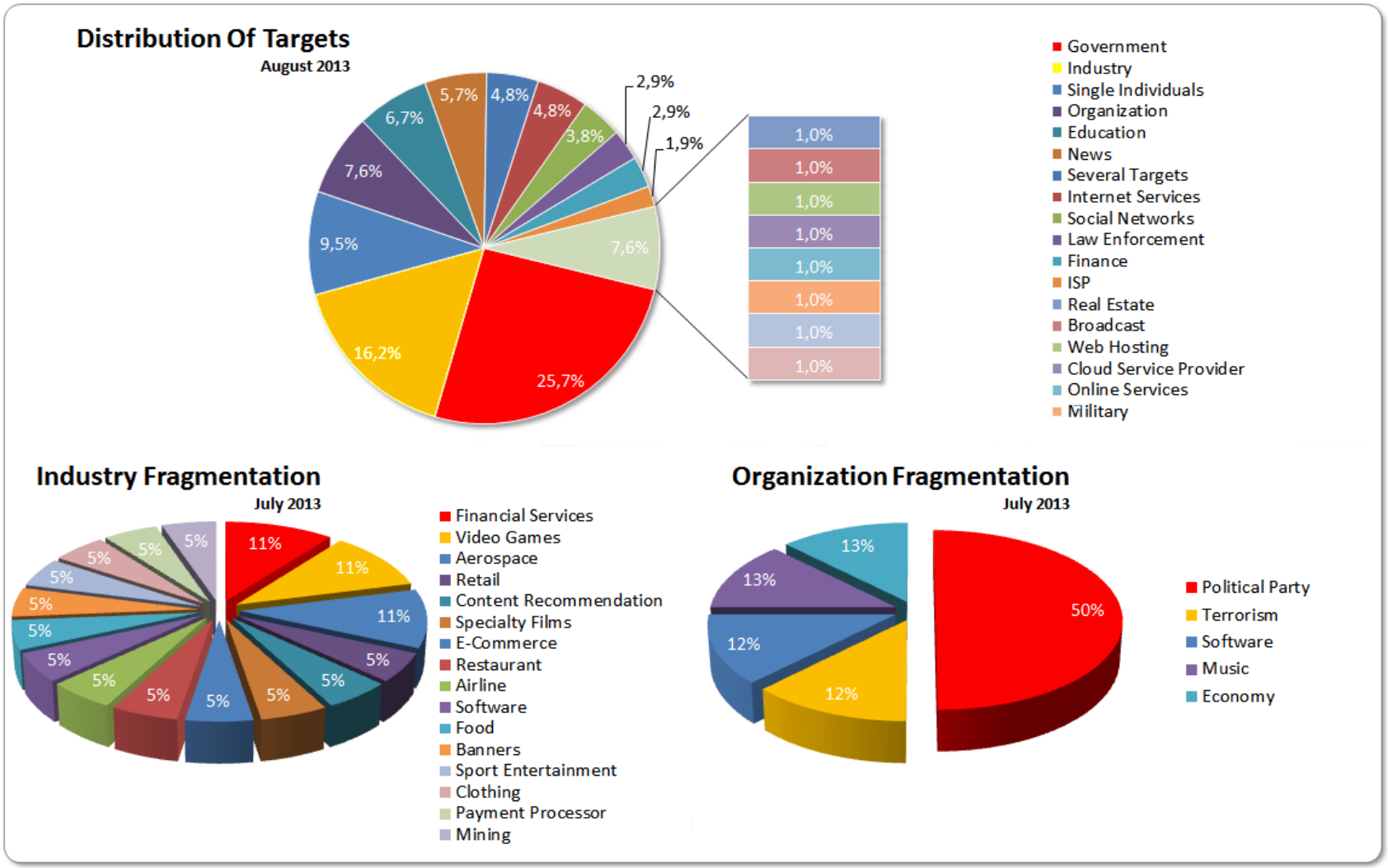
ADS

IPS

Systémy pro detekci útoků/anomálií

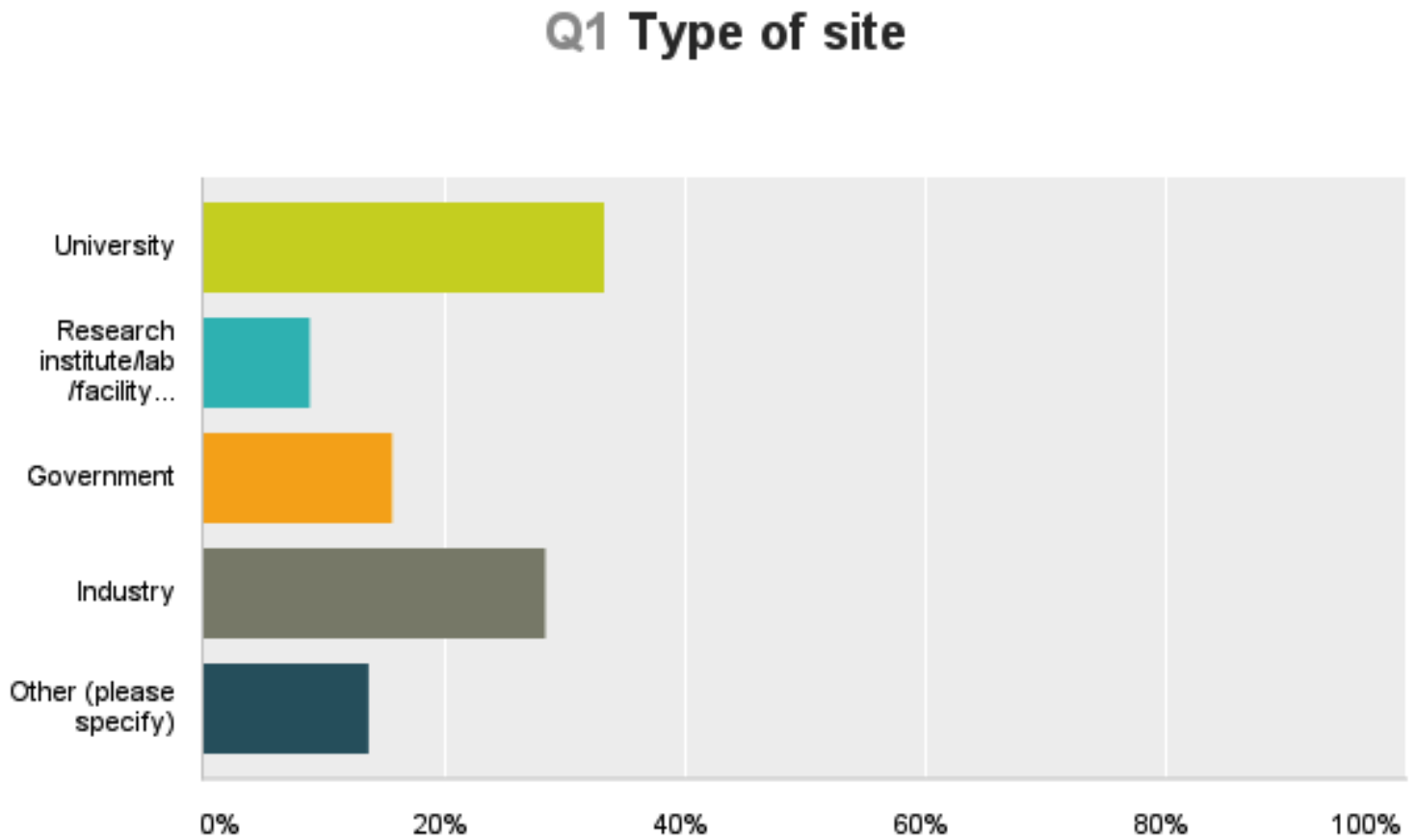
- umožňuje získat informace o síťovém provozu => možnost správy, možnost optimalizace
- umožňuje vyhodnotit informace ze síťového provozu => detekce útoků/anomálií
- umožňuje použít získané informace ze síťového provozu => možnost automatizace, kooperace

Cílový zákazník



Zdroj:http://hackmageddon.com/

Cílový zákazník



Zdroj: http://blog.bro.org/2013/07/results-from-our-deployment-survey.html

Co Systémy pro detekci přináší?

Dobrý detekční systém

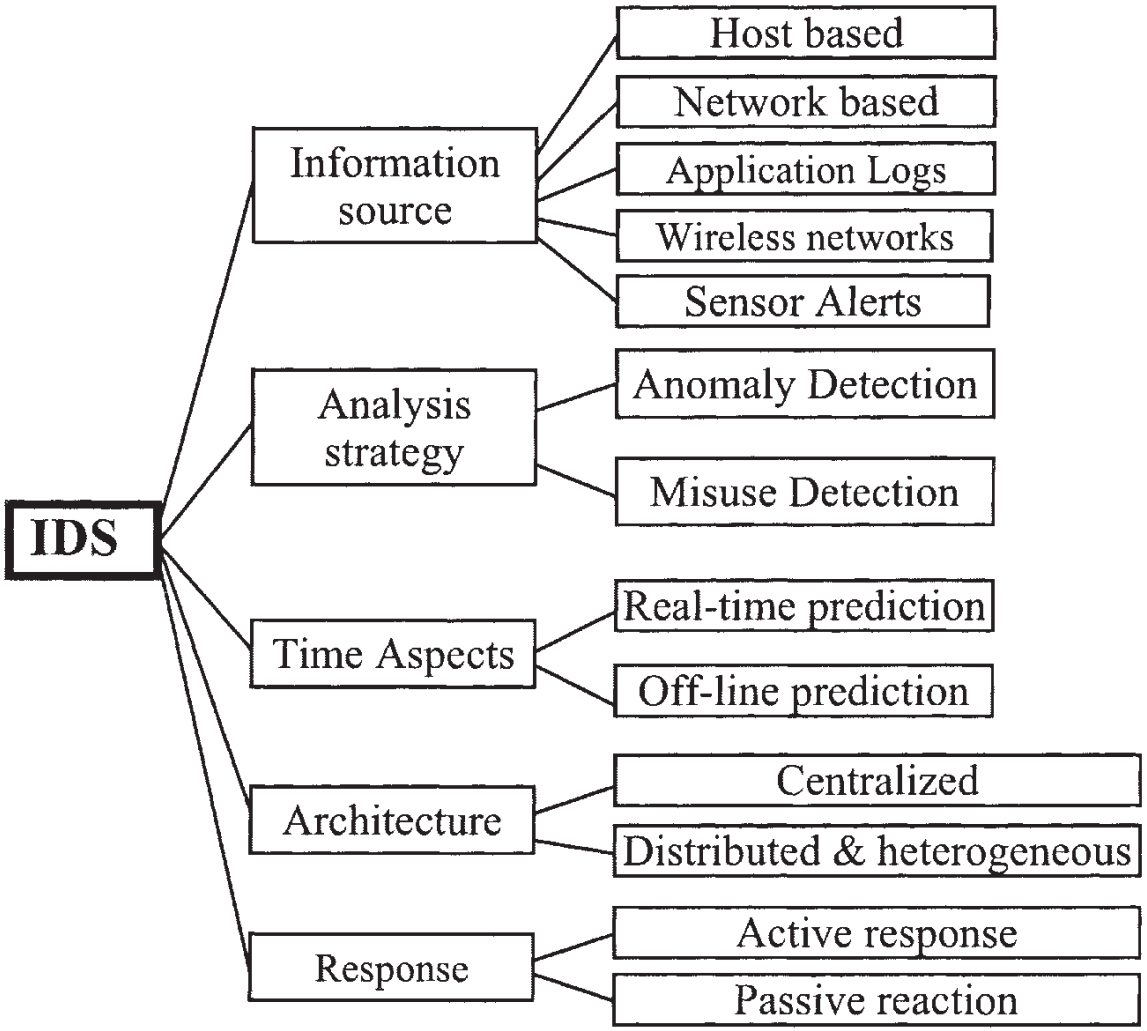
- Zachycuje tzv. *zero-day* útoky
- Možnost definice nových analýz
- Umožní získat porozumění síťovému prostředí
- Iniciativní přístup k síťové bezpečnosti
- Malá míra falešných poplachů
- Schopnost integrace a spolupráce se stávajícími řešeními

Co Systémy pro detekci přináší?

Špatný detekční systém

- Výkonnostní nedostatky
- Zahlcení informacemi
- Nevhodné využití modelů (*Intrusion Detection has been shown to have fundamental differences from other areas where machine learning has been applied (Sommer & Paxson, 2010).*)
- Vysoký počet falešných poplachů
- Náročný handling událostí

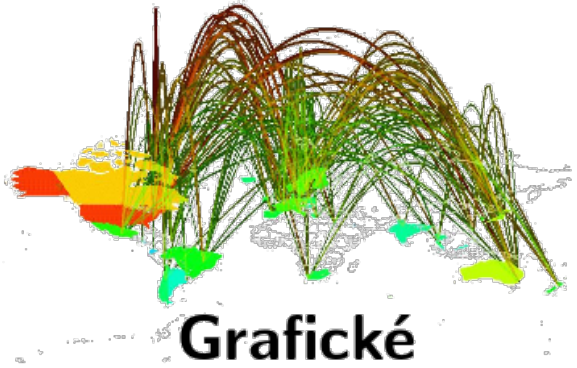
Taxonomie systémů



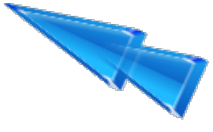
Aleksandar Lazarevic, Vipin Kumar, and Jaideep Srivastava: INTRUSION DETECTION: A SURVEY

Workflow

Upozornění



Grafické znázornění

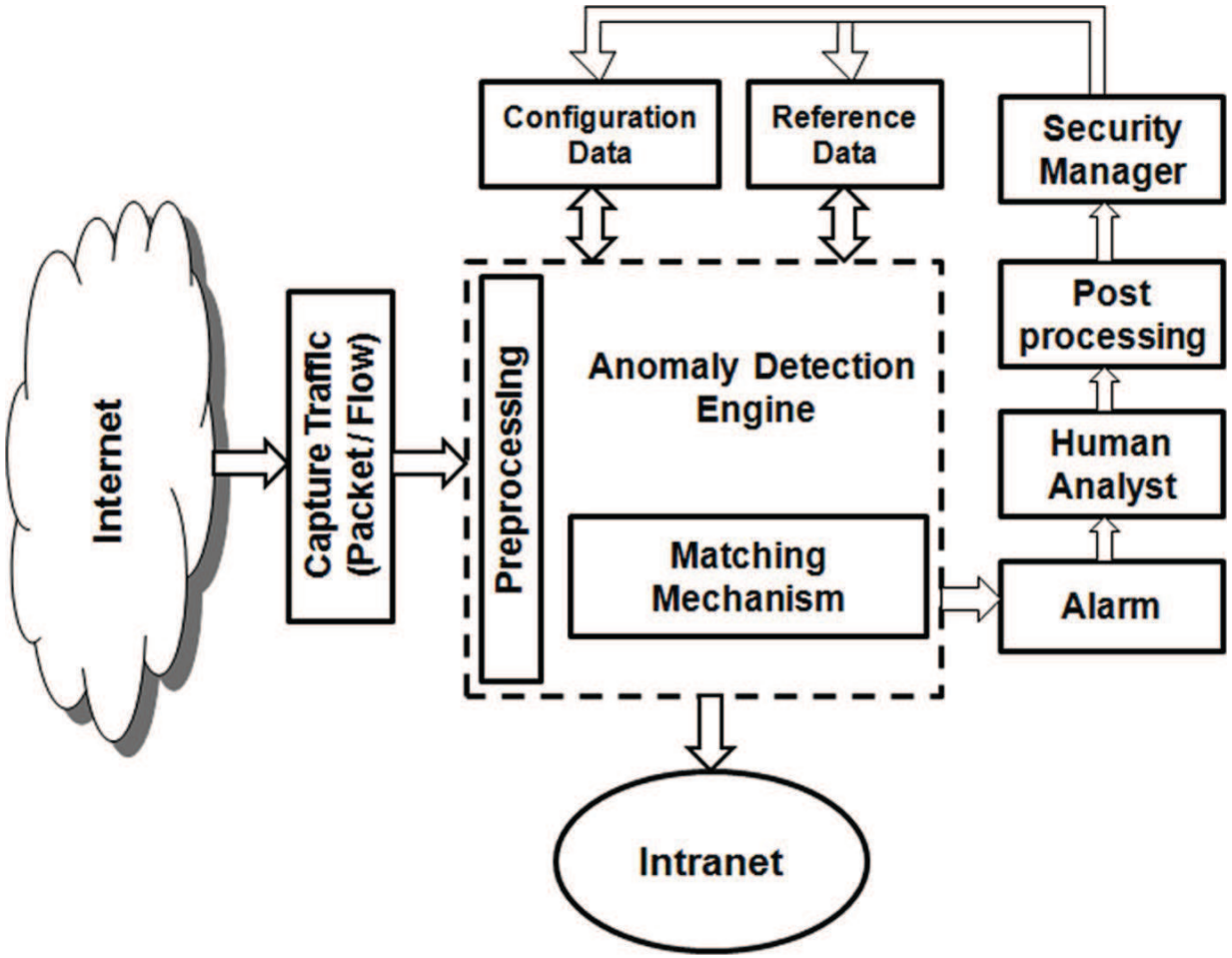


Detekce

Akce

Vyhodnocení

Architektura systémů



Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita: Network Anomaly Detection: Methods, Systems and Tools

Praktická ukázka IDS

- NfSen - open-source nástroj
  `http://nfsen.sourceforge.net/`
- FlowMon INVEA-TECH - komerční nástroj
  `https://www.invea.com/`

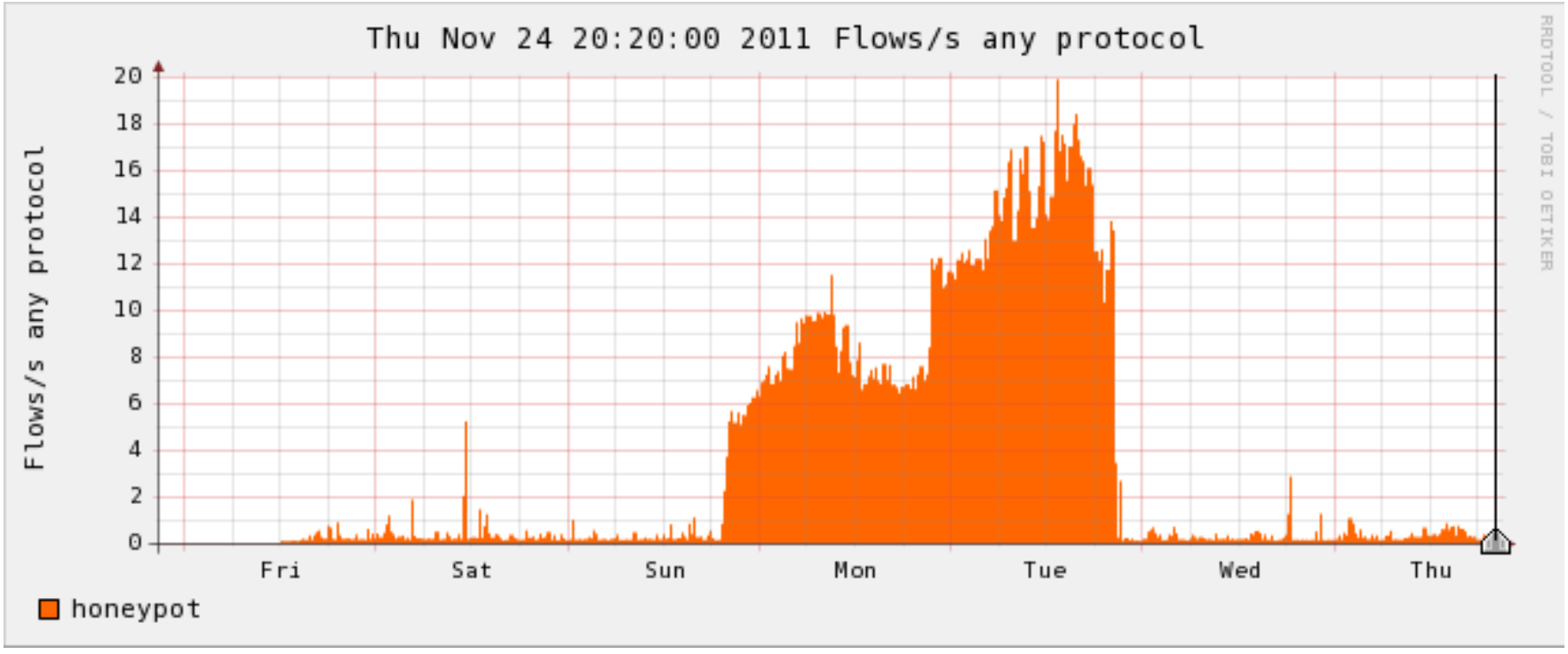
Vizualizace a toky

Proč?

Grafy (diagramy)

- Přirozená metoda vizualizace.
- Na osu x nanášíme většinou čas a na osu y sledovanou veličinu.
- Vhodně vybrané veličiny a podsítě mohou pomoci s odhalením anomálie pouhým okem.
- Ukázka grafů různých veličin univerzitní sítě v nástroji *NfSen*.

2D graf počtu toků v čase

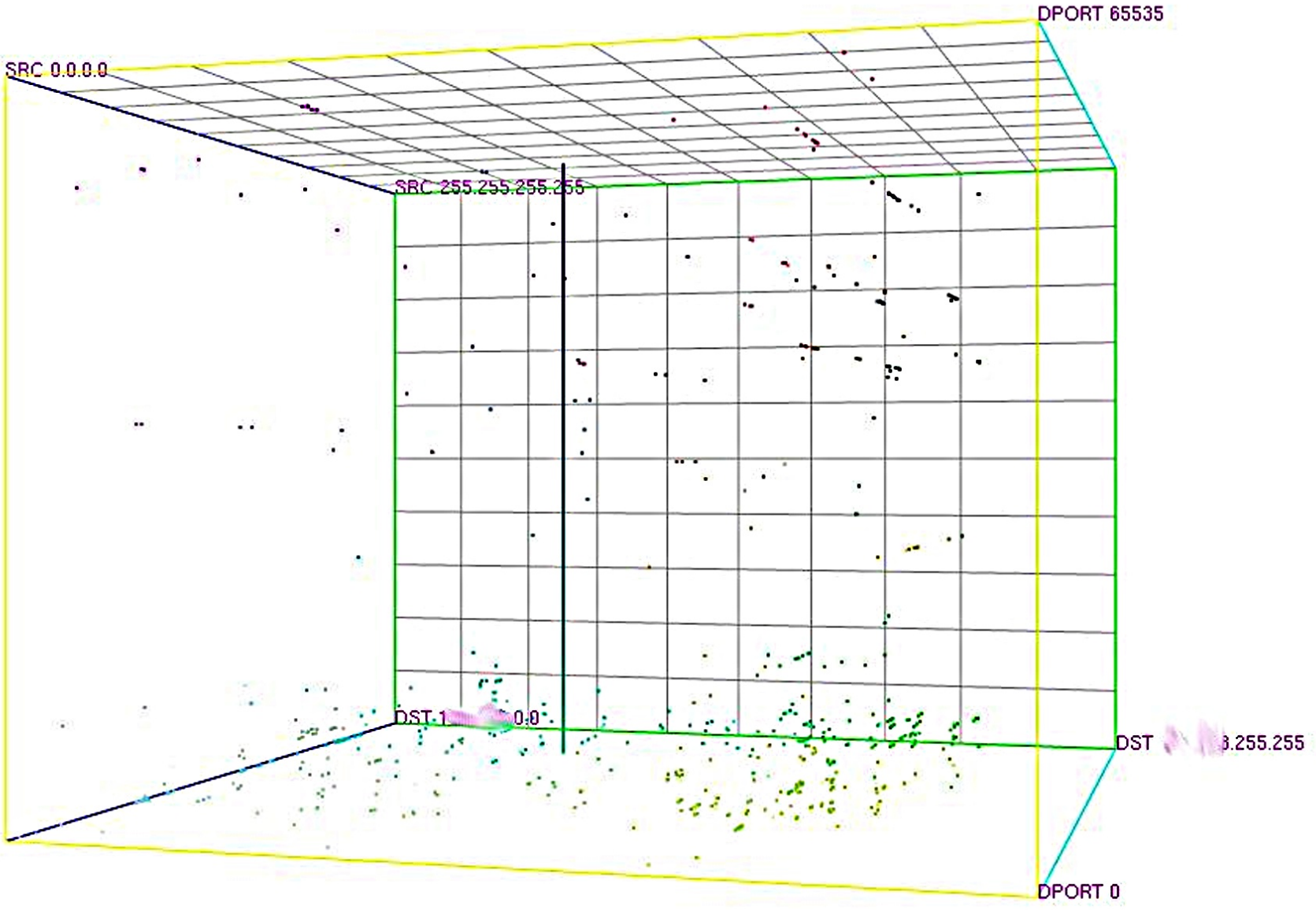


Využití stereoskopického vnímání

- „Převádí” vzory provozu na grafické vzory a útvary.
- *The Spinning Cube of Potential Doom*
  - osa x: lokální adresový prostor,
  - osa z: globální adresový prostor,
  - osa y: čísla cílových portů.
  - Úspěšná TCP spojení bíle, neúspěšná v barvě duhy.
- Ukázka vizualizací pomocí nástroje *Flamingo*[5].

[5] `http://flamingo.merit.edu/gallery.html`

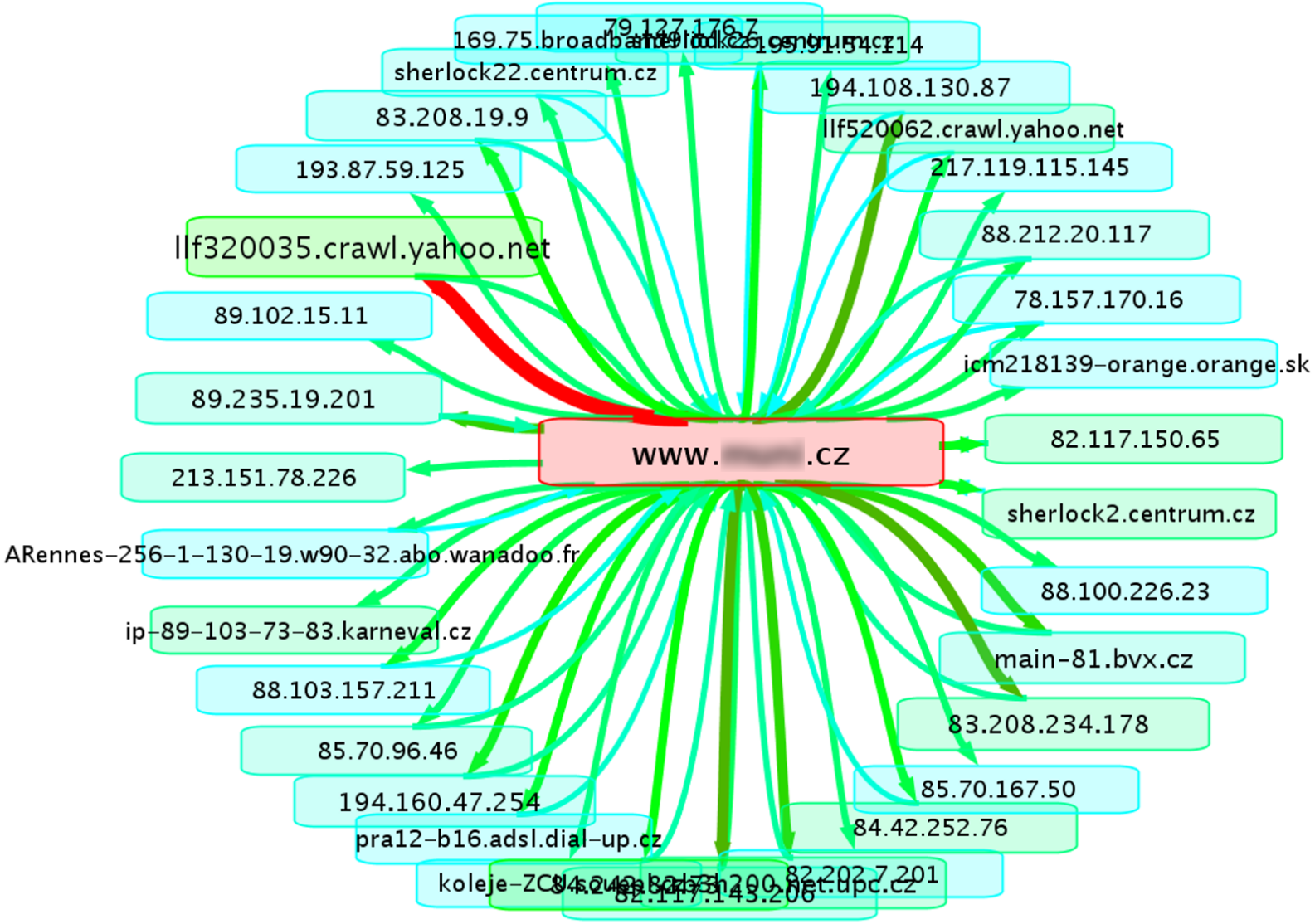
Skenování portů v kostce



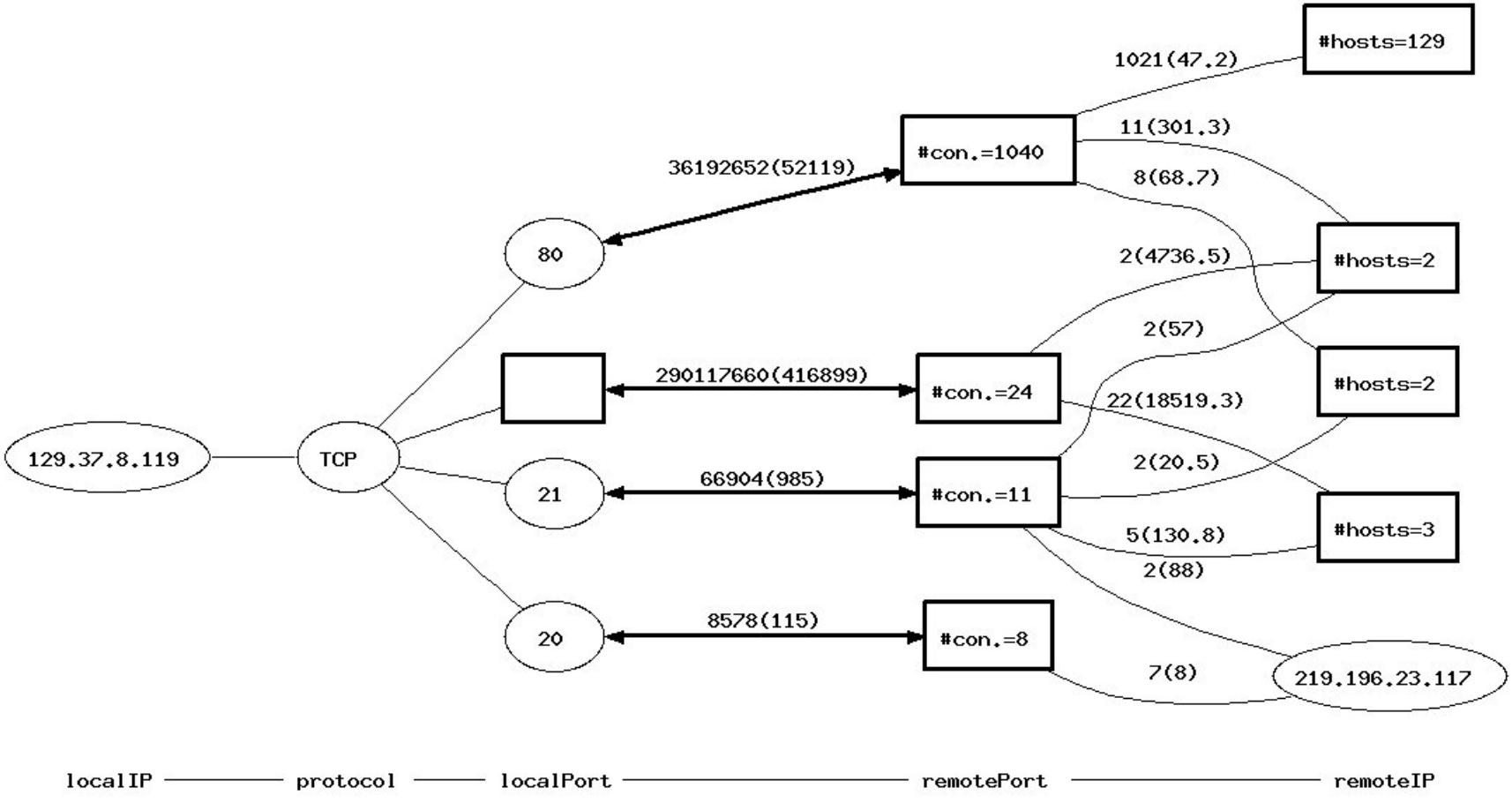
Stroje a toky jako orientovaný graf

- Vrcholy grafu tvoří stroje (IP adresy).
- Hrany zobrazují jednotlivé toky nebo jejich agregace.
- Velikost, zabarvení. . . vrcholu/hrany odráží nějakou jeho/její charakteristiku (např. počet přenesených bajtů).
- Pohled na to, ***kdo*** *kolik čeho* ***kam*** *přenášel*.

Orientovaný graf zobrazující síťový provoz

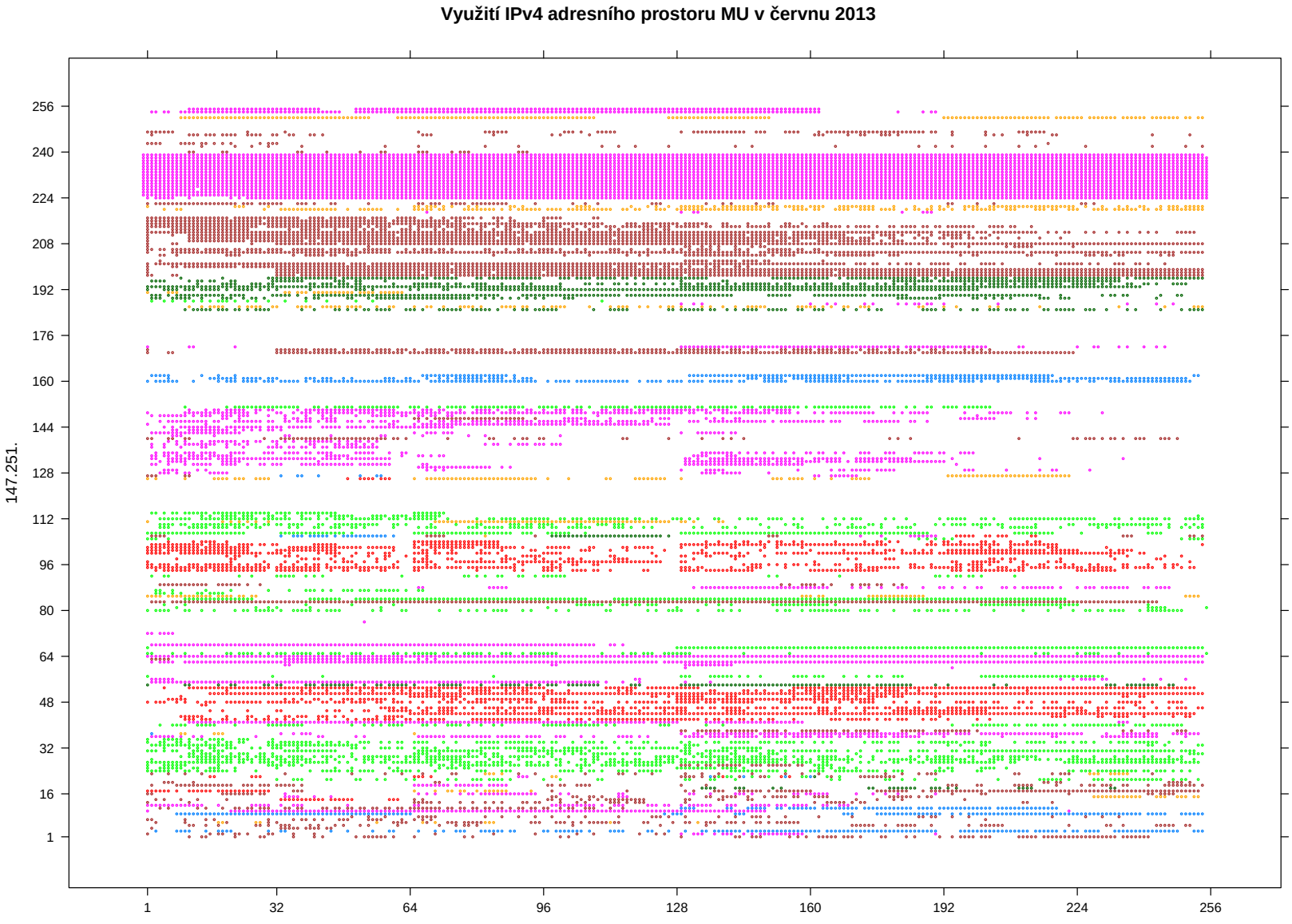


Další příklad grafu



Výstup z nástroje HAPviewer – `http://hapviewer.sourceforge.net/`

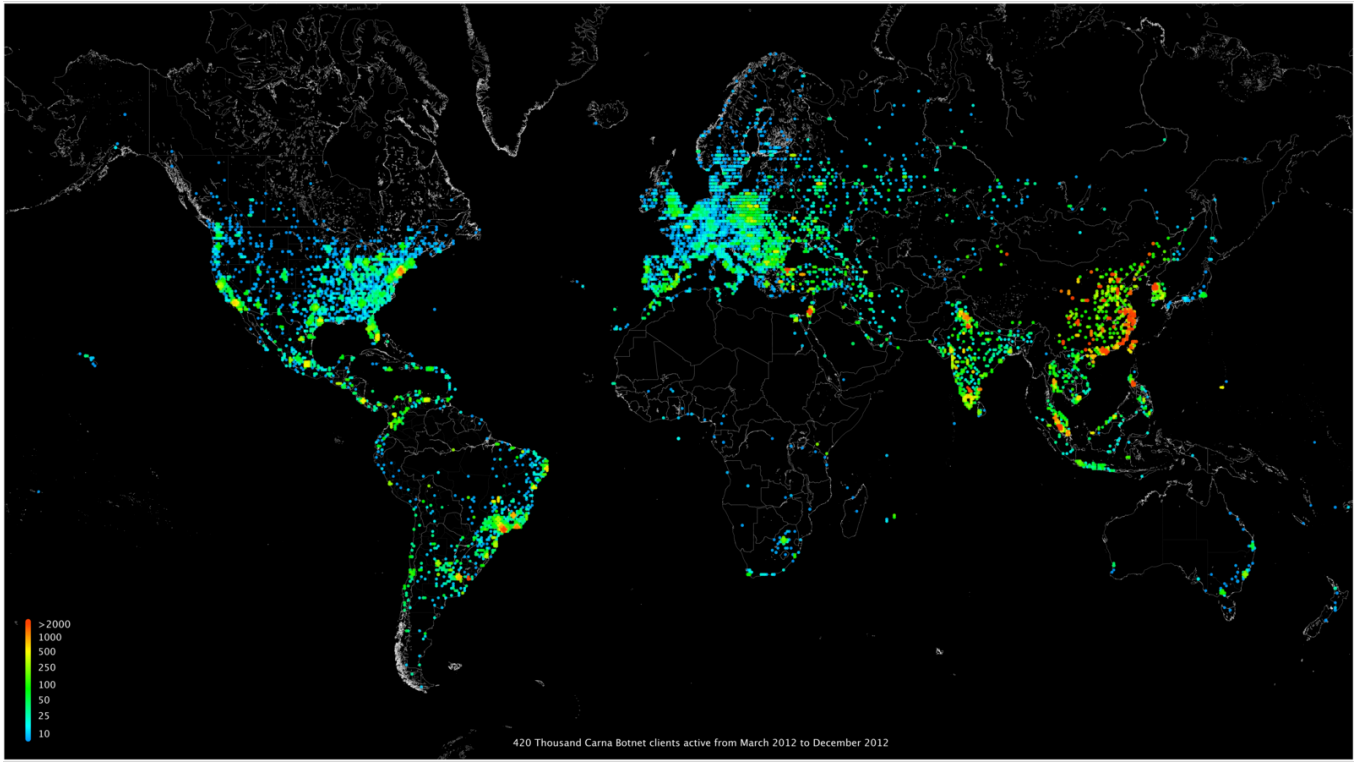
Vizualizace IPv4 adresního prostoru



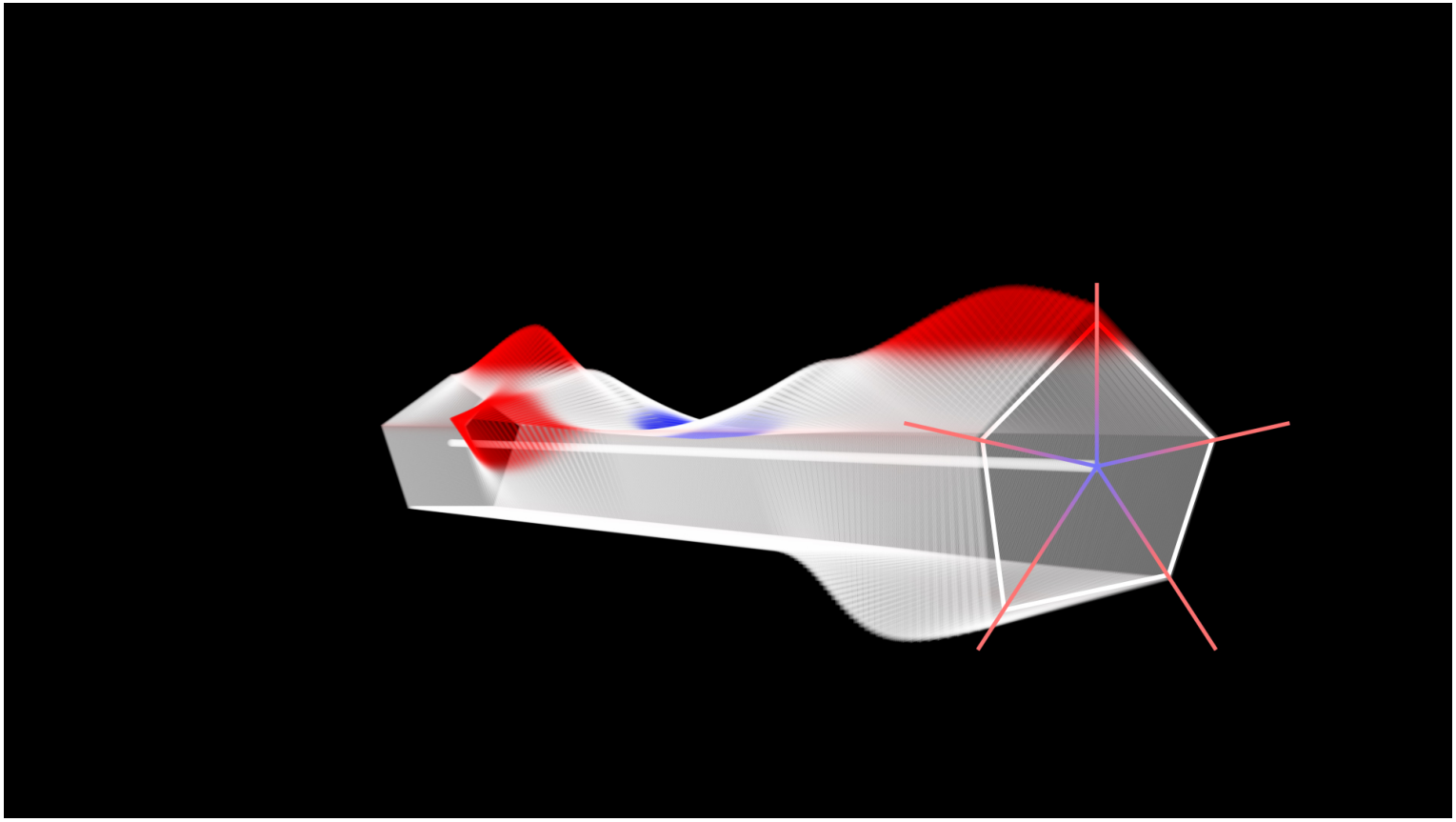
Vizualizace IPv4 adresního prostoru

Internet Census 2012

http://internetcensus2012.bitbucket.org/paper.html



Spider



- umožňuje zobrazit vztah více veličin v průběhu času

Pokročilé vizualizace DDoS útoků

- Real-time vizualizace DDoS útoků po celém světě (Google Ideas & Arbor Networks)
  `http://www.digitalattackmap.com/`
- Ukázka pokročilých vizualizací
  `http://infosthetics.com/archives/2012/06/nict_daedalus_3d_real-time_cyber-attack_alert_visualization.html`

Další literatura

- *InetVis, a Visual Tool for Network Telescope Traffic Analysis*
  `http://www.cs.ru.ac.za/research/g02v2468/publications/vanRiel-Afrigraph2006.pdf`
- *WireViz (plugin do Wiresharku) – screencast*
  `http://www.youtube.com/watch?v=fU8w0jooIwE`
- *Manidant APT1 Report*
  `http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf`