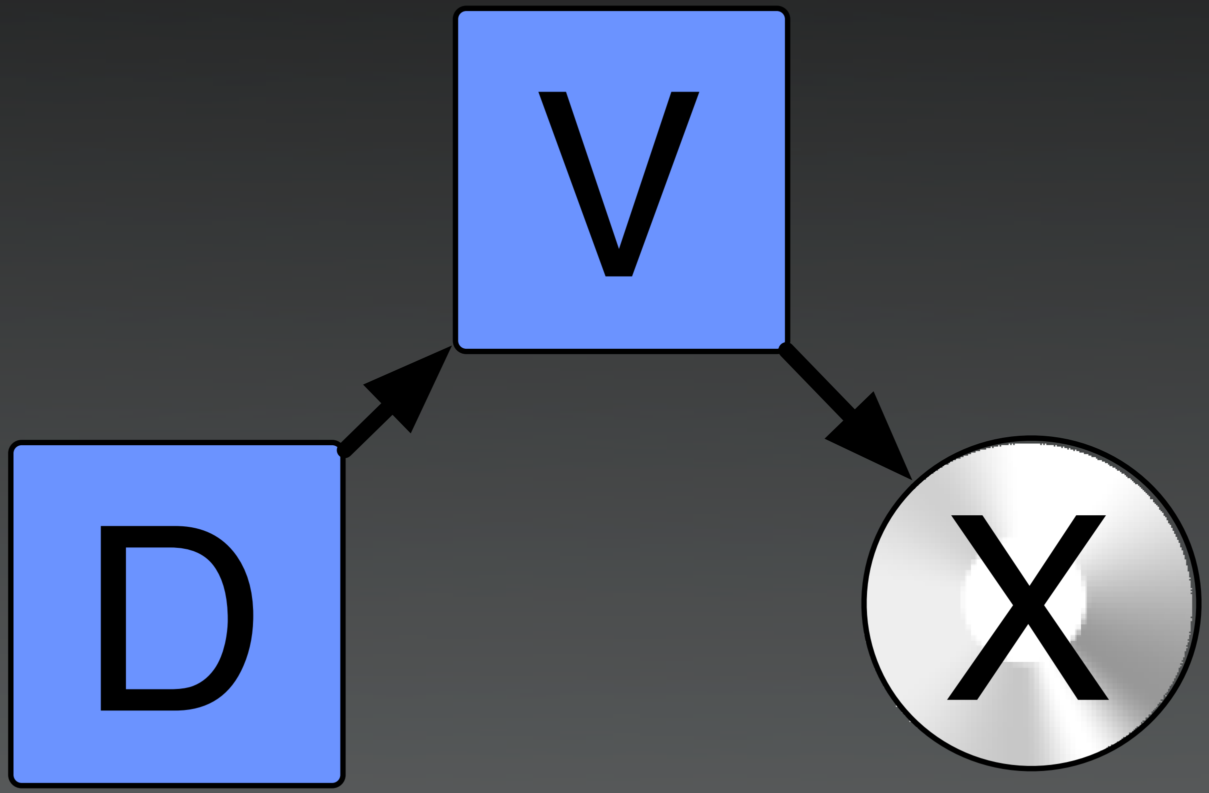


Data Analysis and Visualization Linux

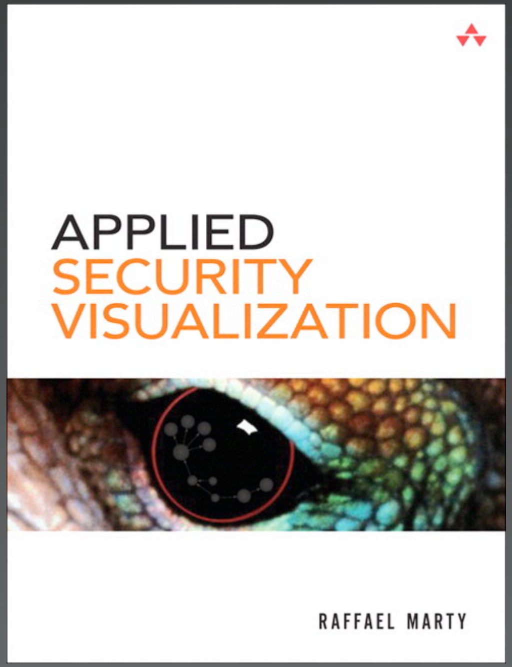
Jan . Monsch at iplosion . com
Raffael . Marty at secviz . org

Raffael Marty

- Chief Security Strategist @ Splunk>
- Passion for Visualization
  - http://secviz.org
  - http://afterglow.sourceforge.net

Jan P. Monsch

- Senior Security Analyst
- Post-Graduate Student DCU Ireland
- DAVIX initiator and engineer
  - http://davix.secviz.org
  - http://www.iplosion.com



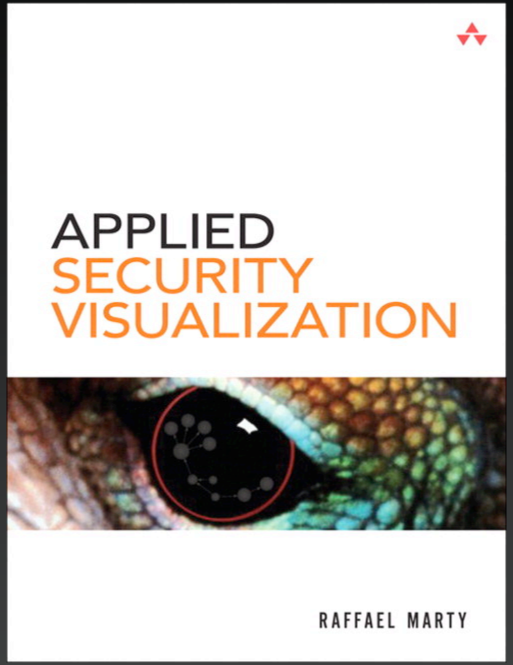
Applied Security Visualization

Paperback: 552 pages
Publisher: Addison Wesley (August, 2008)
ISBN: 0321510100

Security Visualization

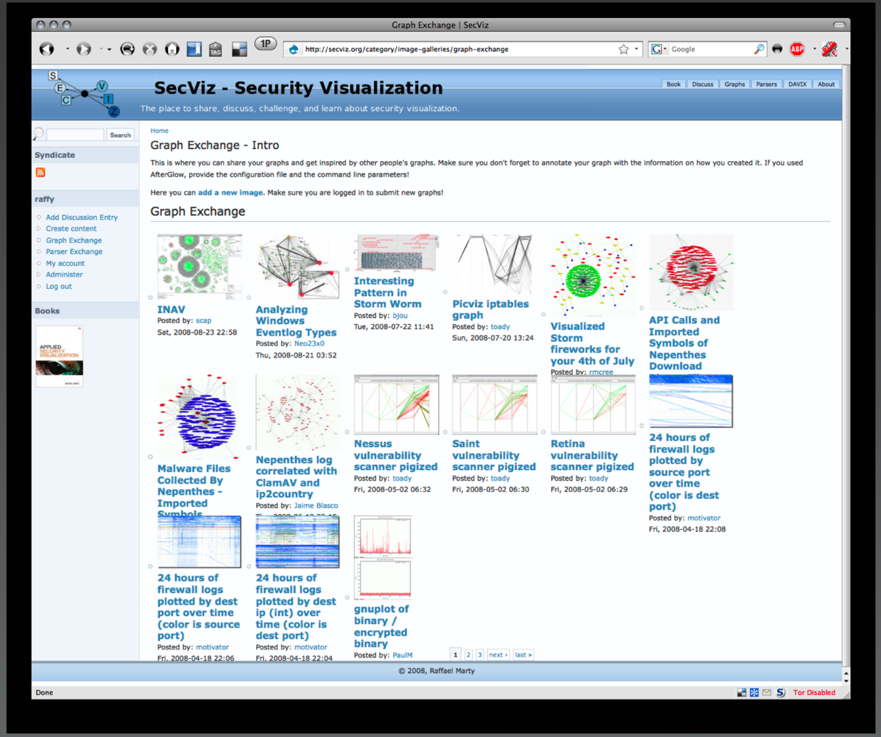
- Security visualization is a new field
- Lack of security visualization tools
- Lack of security visualization best practices and approaches
- Lack of understanding
- SecViz upfront investment high

www.SecViz.org



APPLIED
SECURITY
VISUALIZATION

RAFFAEL MARTY



Graph Exchange | SecViz

http://secviz.org/category/image-galleries/graph-exchange

SecViz - Security Visualization

The place to share, discuss, challenge, and learn about security visualization.

Home

Graph Exchange - Intro

This is where you can share your graphs and get inspired by other people's graphs. Make sure you don't forget to annotate your graph with the information on how you created it. If you used AfterGlow, provide the configuration file and the command line parameters!

Here you can add a new image. Make sure you are logged in to submit new graphs!

Graph Exchange

INAV
Posted by: scap
Sat, 2008-08-23 22:58

Analyzing Windows Eventlog Types
Posted by: Neo23x0
Thu, 2008-08-21 03:52

Interesting Pattern in Storm Worm
Posted by: bjou
Tue, 2008-07-22 11:41

Picviz iptables graph
Posted by: toady
Sun, 2008-07-20 13:24

Visualized Storm fireworks for your 4th of July
Posted by: rmcree

API Calls and Imported Symbols of Nepenthes Download

Malware Files Collected By Nepenthes - Imported Symbols

Nepenthes log correlated with ClamAV and ip2country
Posted by: Jaime Blasco

Nessus vulnerability scanner pigized
Posted by: toady
Fri, 2008-05-02 06:32

Saint vulnerability scanner pigized
Posted by: toady
Fri, 2008-05-02 06:30

Retina vulnerability scanner pigized
Posted by: toady
Fri, 2008-05-02 06:29

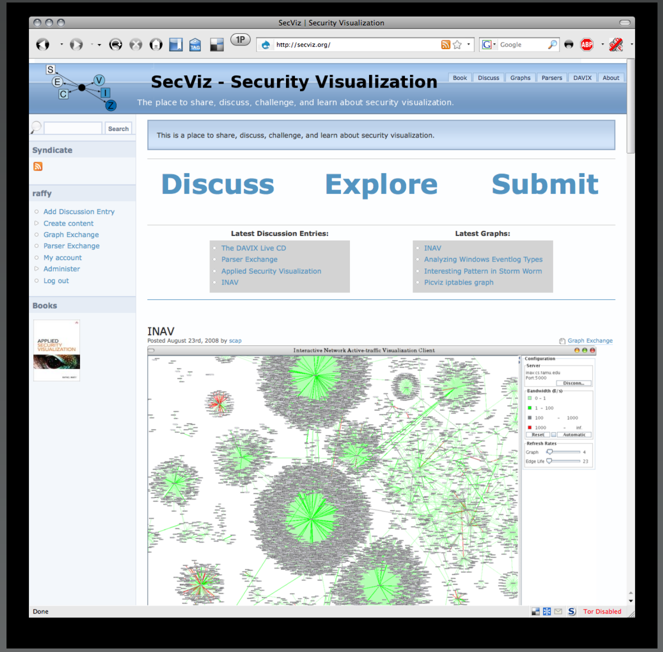
24 hours of firewall logs plotted by source port over time (color is dest port)
Posted by: motivator
Fri, 2008-04-18 22:08

24 hours of firewall logs plotted by dest port over time (color is source port)
Posted by: motivator
Fri, 2008-04-18 22:06

24 hours of firewall logs plotted by dest ip (int) over time (color is dest port)
Posted by: motivator
Fri, 2008-04-18 22:04

gnuplot of binary / encrypted binary
Posted by: PaulM

© 2008, Raffael Marty



SecViz | Security Visualization

http://secviz.org/

SecViz - Security Visualization

The place to share, discuss, challenge, and learn about security visualization.

This is a place to share, discuss, challenge, and learn about security visualization.

Discuss Explore Submit

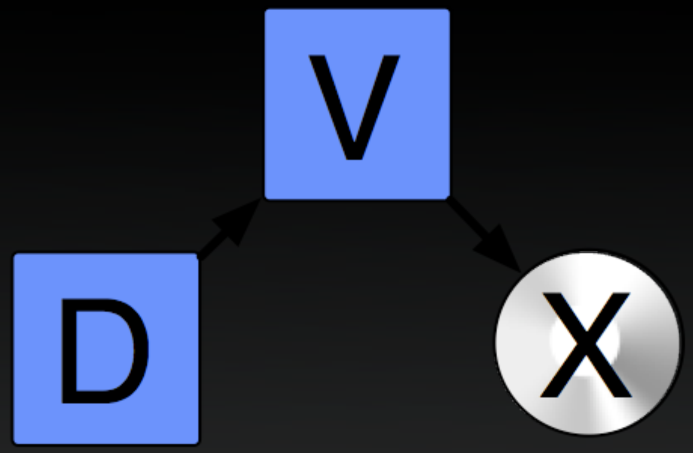
Latest Discussion Entries:
- The DAVIX Live CD
- Parser Exchange
- Applied Security Visualization
- INAV

Latest Graphs:
- INAV
- Analyzing Windows Eventlog Types
- Interesting Pattern in Storm Worm
- Picviz iptables graph

INAV

Posted August 23rd, 2008 by scap

Initial Situation



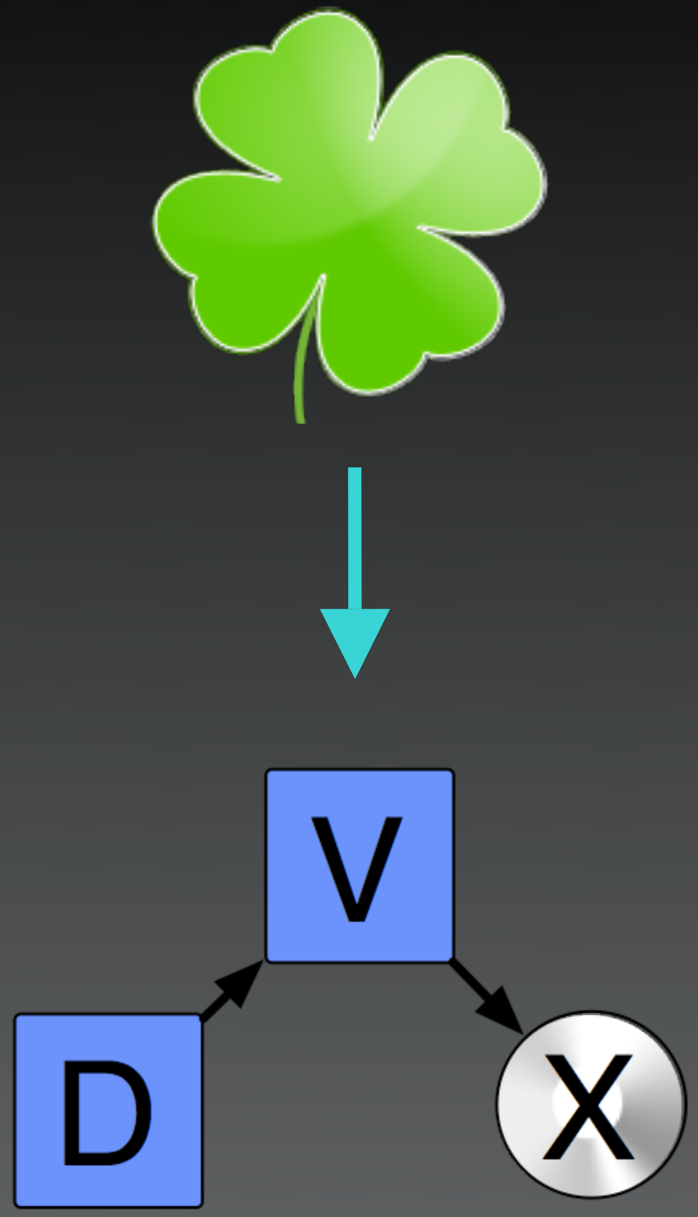
- Many free visualization tools available
- No free solution offering wide range of processing and visualization tools
- Cumbersome to get tools running and installed
  - Compiler issues, e.g. gcc 3 vs. gcc 4
  - Dependencies with uncommon and old libraries
  - Different runtime environments

DAVIX Mission Statement

- Provide the audience with a workable and integrated tool set,
- enable them to immediately start with security visualization and
- motivate them to contribute to the security visualization community.

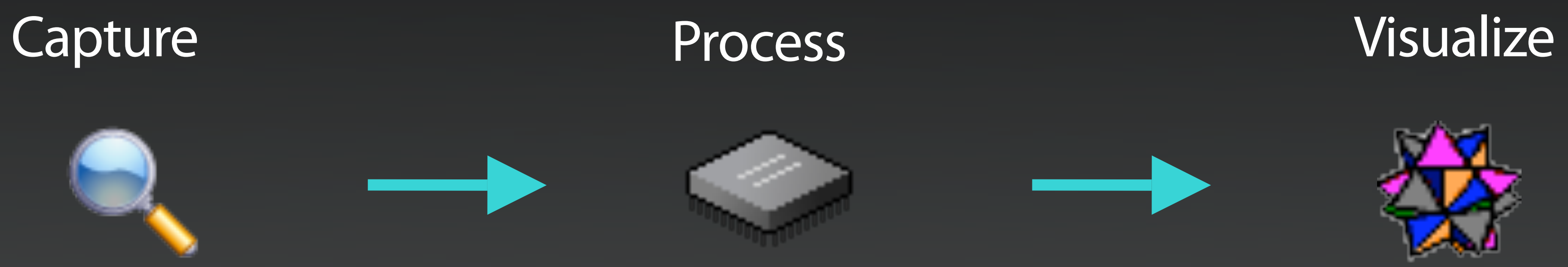
Inside the CD

- Live Linux CD system based on SLAX 6
  - Software packages are modularized
  - Easy customizable
  - Runs from CD/DVD, USB stick or hard drive
- Collection of free tools for data processing & visualization
  - Tools work out of the box
  - No compilation or installation of tools required
- Comes with documentation
  - Quick start description for the most important tools
  - Links to manuals and tutorials



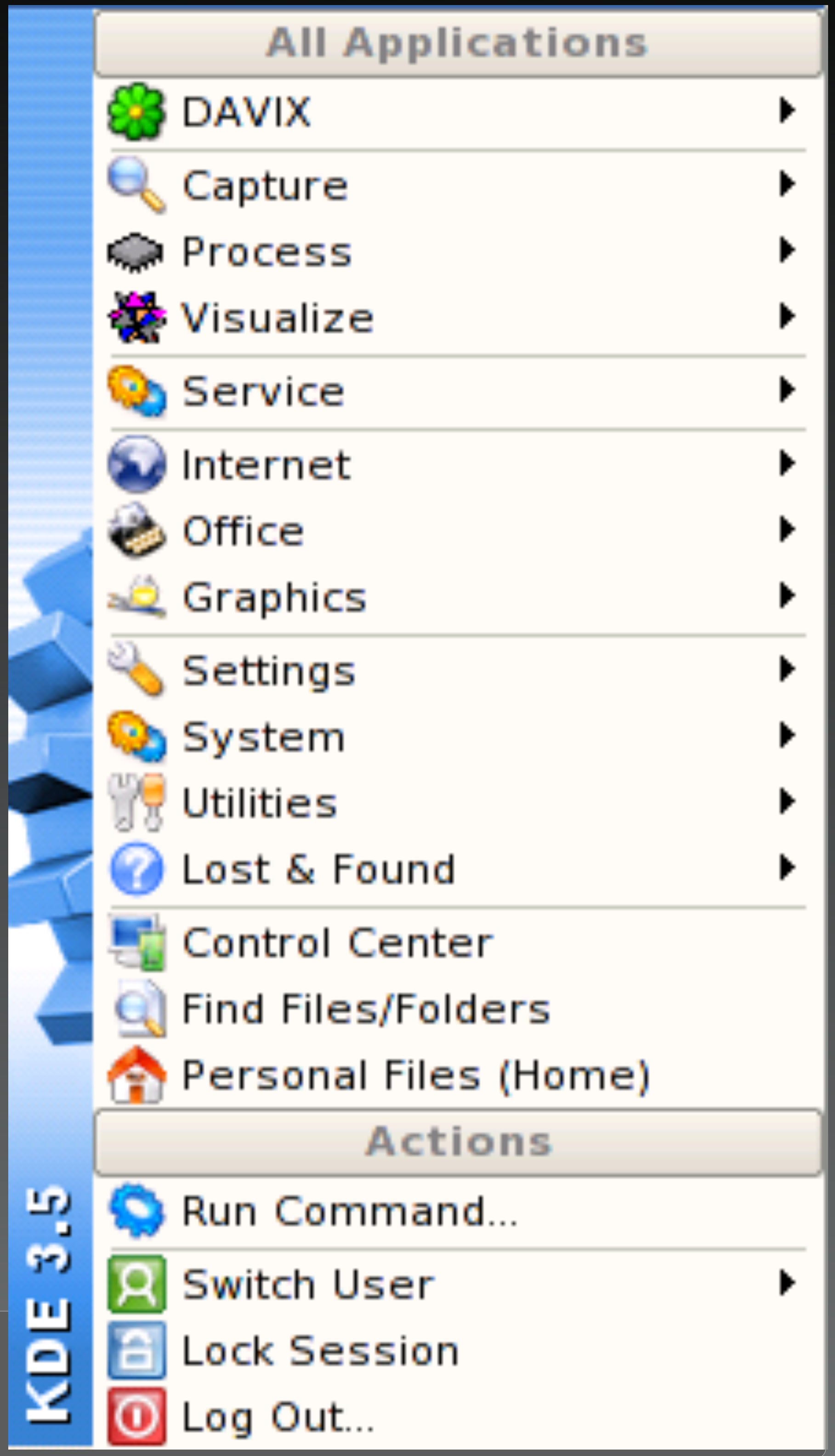
User Interface - Menu Organization

- Menu organized around the information visualization process



Capture → Process → Visualize

- Tools often cover more than one category
  - Afterglow → Process, Visualize
- Additional tools/services:
  - Apache, MySQL, NTP
- Documentation built-in



Tools

Capture

- *Network tools*
  - Argus
  - Snort
  - Wireshark
- *Logging*
  - syslog-ng
- *Fetching data*
  - wget
  - ftp
  - scp

Processing

- *Shell tools*
  - awk, grep, sed
- *Graphic preprocessing*
  - Afterglow
  - LGL
- *Data enrichment*
  - geoiplookup
  - whois/gwhois

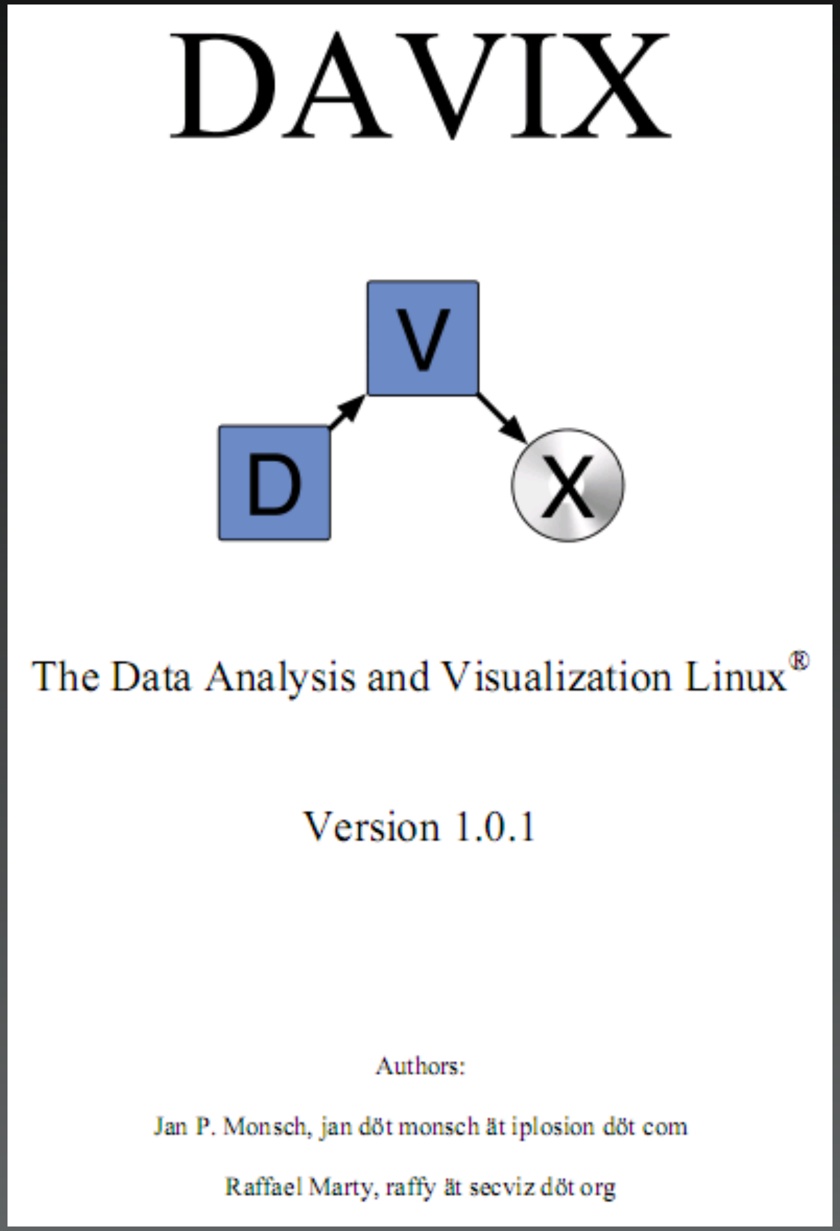
Visualization

- *Network Traffic*
  - EtherApe
  - InetVis
  - tnv
- *Generic*
  - Afterglow
  - LGL Viewer
  - Mondrian
  - R Project

* Non-concluding list of tools

PDF User Manual

- Quick start guide
- Network setup information
- Tool usage examples
- Links to online resource: Tool home pages, manuals, tutorials
- Customizing DAVIX
  - Customizing ISO image
  - Creating new modules
  - Installation on USB stick or hard drive



DAVIX

The Data Analysis and Visualization Linux®

Version 1.0.1

Authors:

Jan P. Monsch, jan döt monsch ät iplosion döt com

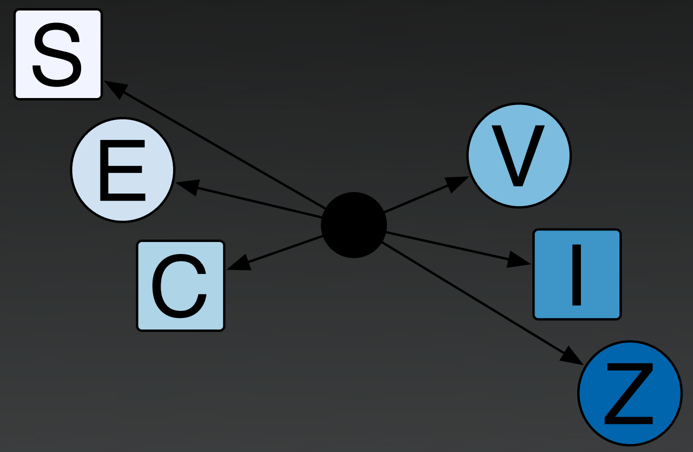
Raffael Marty, raffy ät secviz döt org

DAVIX Roadmap

- **Short-Term**
  - Integrated UI that allow easy orchestration of the different tools
    - Afterglow, NSM Console, Splunk
  - More visualization tools
  - Improve manual by adding use-cases
- **Mid-Term**
  - Data format converters for the visualization tools
  - Sample data sets and tutorials
- **Long-Term**
  - Support for distributed processing

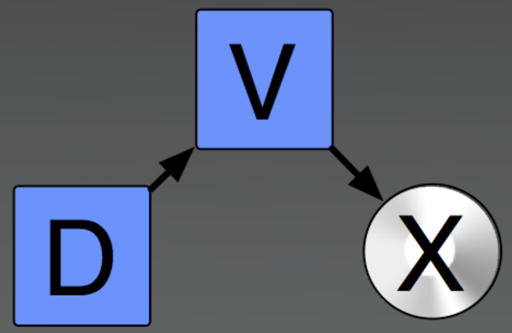
Call for Action

Submit on www.secviz.org



- Visualization Tools
- Use-cases
- Security data

Post to mailing list or email the authors

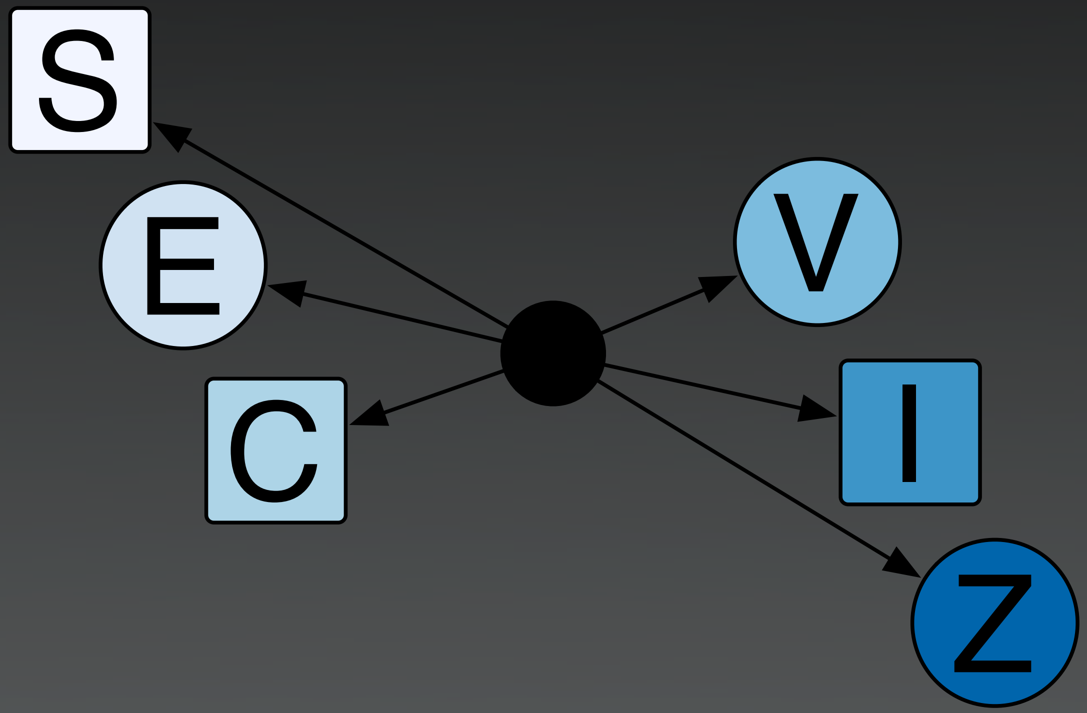


- Feedback
- Testing

http://groups.google.com/group/davix-support

Jan . Monsch at iplosion . com
Raffael . Marty at secviz . org

Thank You



secviz . org

davix . secviz . org

Visit us during the demos tonight!