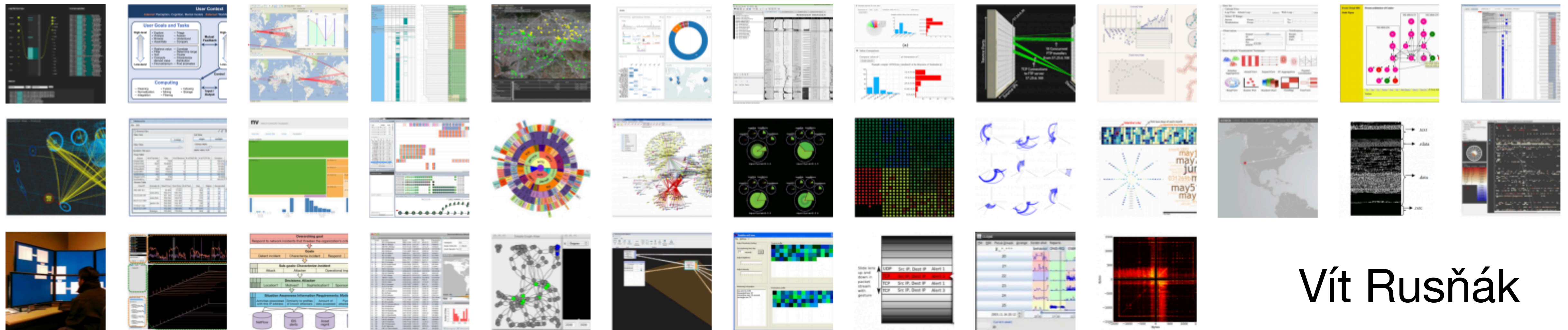# Visualizations for Cybersecurity

PA214 — Visualization II

Vít Rusňák

Protect Yourself

Share

DEMO
ON

https://cybermap.kaspersky.com
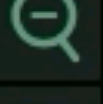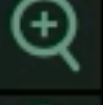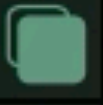
# Talk Overview

- Users and Data

- Visualization Categories

- Trends in Cybersecurity Visualization Research

# Typical Users

**Cybersecurity operations** (L1)

- monitoring, countermeasures

- CSIRT, Incident handlers
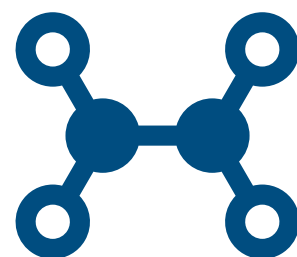
**Cybersecurity Analysts** (L2)

- network traffic anomalies, malware analysts, penetration testing

**Management** (both IT and non-IT background)

- Chief information security officer (CISO), policy makers, lawyers

**Cybersecurity Researchers**

- simulations, process automation, application of ML/AI

# Data Sources

**Applications**

**Network Services**

**Proxies**
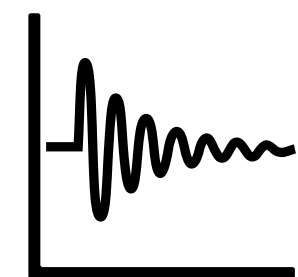
**Operating System**

**Intrusion Detection Systems**

**Firewalls**

**Passive Network Analysis**

**Traffic Flows**

**Packet Captures**

**Logs**

**Time-series**

*Adapted from [1]*

# Complexity of Visualizations

**Visualizations**

**Complexity**

**Monitoring** — Dashboards

Low

**Analysis** — VA Visualizations

**Simulations and Predictions** — Modeling, Explainable AI

High

# Monitoring

Image source: https://www.logpoint.com/en/
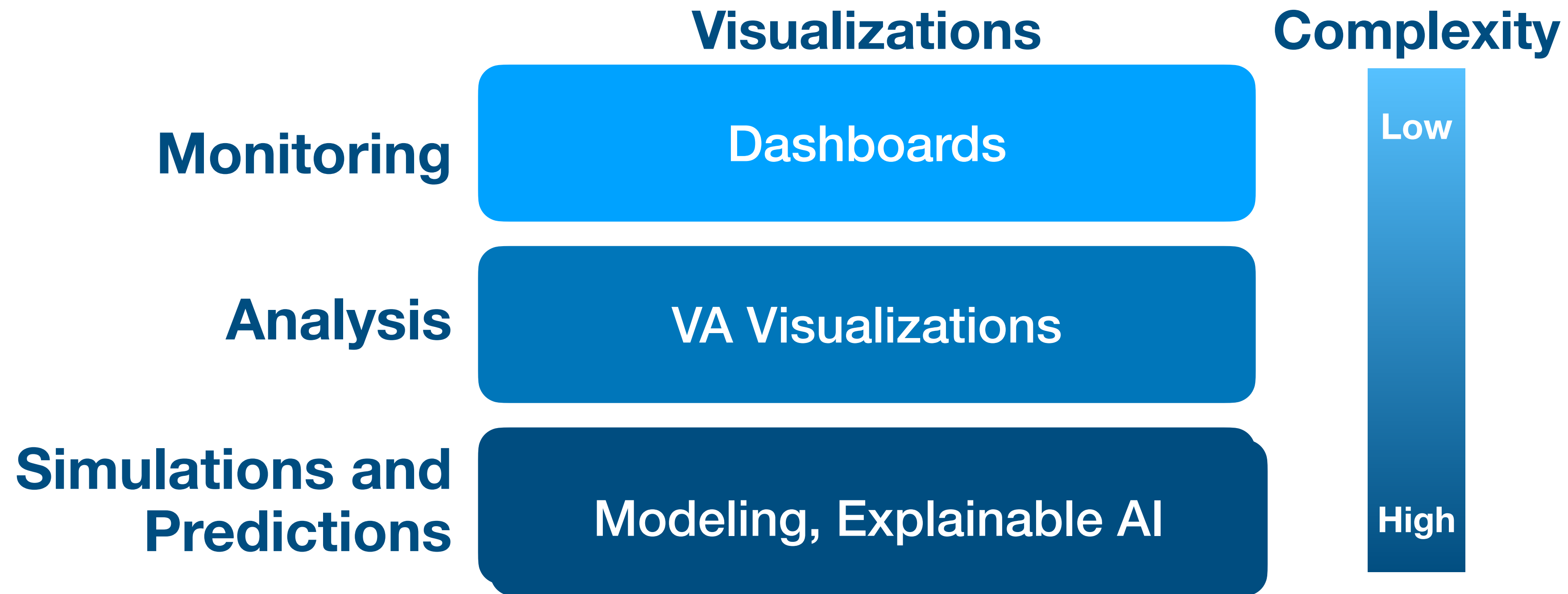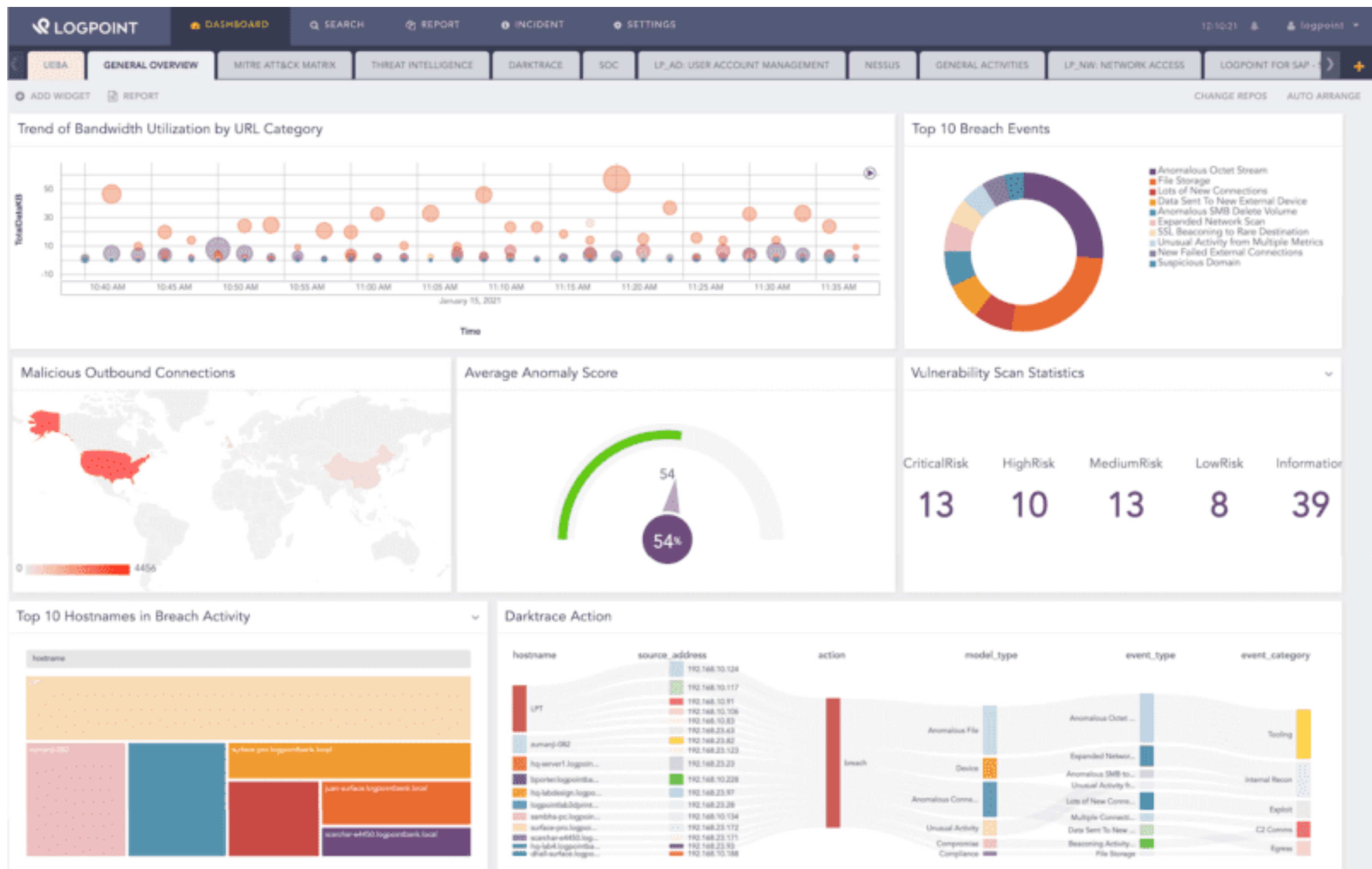
# Characteristics

- **Dashboards are prevalent**

  - Typically easy to read, decode and understand, multiple views (panels)

- **Goal(s):** situational awareness, trends, outliers and anomalies (e.g., peaks)

- **Typical visualizations:** tables, line/area charts, sparklines (microvisualizations), basic 2D charts (bar charts, heatmaps), basic geovisualizations (choropleth, links)

- **Shortcuts** and **click-throughs** allowing **drill-down** in analytical tools

# Dashboards

*"A dashboard is a visual display of the most important information needed to achieve one or more objectives that has been consolidated in a single computer screen so it can be monitored at a glance."*
— **Stephen Few**, Information Dashboard Design

## Provide

- current value of key measures (KPI, number of detected events, blocked IP addresses, …)

- comparison to target measures (difference, trend)

- a range of possible values of the measures with a qualitative association (semaphore, warnings)

## Types

- Operational (monitoring, single source of information)

- Tactical (planning)

- Strategic (management)

# Examples: Commercial Tools



Source: https://demo.flowmon.com

# Examples: Commercial Tools

# Examples: Commercial Tools

tenable.sc — Dashboard ▾  Analysis ▾  Scans ▾  Reporting ▾  Assets  Workflow ▾  Users ▾

## Understanding Risk

⊞ Switch Dashboard ▾   ⚙ Options ▾

### Understanding Risk - Vulnerability Severity Summary

■ Low  ■ Medium  ■ High  ■ Critical

Last Updated: 18 minutes ago

### Understanding Risk - Details by Severity

|  | Total | Exploitable | Vuln Publ >90d | Patch Avail >30d | Hosts |
|---|---|---|---|---|---|
| All Severities | 1204157 | 2% | 3% | 6% | 1356 |
| Critical | 7025 | 32% | 31% | 91% | 765 |
| High | 198029 | 8% | 10% | 17% | 962 |
| Medium | 118985 | 6% | 7% | 20% | 1008 |
| Low | 4957 | 7% | 35% | 47% | 974 |
| Info | 875161 | 0% | 0% | 0% | 1352 |

Last Updated: 5 hours ago

### Understanding Risk - Details by Vulnerability Grouping

|  | Total | Exploitable | Vuln Publ >90d | Patch Avail >30d | Hosts |
|---|---|---|---|---|---|
| Default Cred. | 10199 | 1% | 0% | 0% | 495 |
| OS | 39974 | 48% | 52% | 94% | 573 |
| Web Tech. | 2434 | 47% | 88% | 91% | 233 |
| Web Browser | 6162 | 73% | 93% | 93% | 210 |
| Office Suite | 809 | 73% | 83% | 83% | 162 |

Last Updated: 5 hours ago

### Understanding Risk - CVSS Scores by Severity ⚙▾

|  | Total | CVSS 10.0 | CVSS 7.0 - 9.9 | CVSS 4.0 - 6.9 | CVSS 0.0 - 3.9 |
|---|---|---|---|---|---|
| Critical | 7025 | 100% | 0% | 0% | 0% |
| High | 198029 | 0% | 16% | 0% | 0% |
| Medium | 118985 | 0% | 0% | 24% | 0% |
| Low | 4957 | 0% | 0% | 0% | 87% |
| Info | 875161 | 0% | 0% | 0% | 0% |

Last Updated: 5 hours ago

### Understanding Risk - Remediation Opportunities

| Solution | Risk Reduction | Host Total |
|---|---|---|
| Apply MS16-106: Security Update for Microsoft Graphics Component (3185848) | 3.36% | 185 |
| Apply MS16-111: Security Update for Windows Kernel (3186973) | 3.16% | 187 |
| Apply MS16-097: Security Update for Microsoft Graphics Component (3177393) | 3.13% | 179 |

Last Updated: 5 hours ago

### Understanding Risk - Most Severe

| Plugin ID | Name | Severity | Host Total |
|---|---|---|---|
| 9309 | OpenSSH < 7.0 Multiple Vulnerabilities | Critical | 393 |
| 91786 | CentOS 6 / 7 : libxml2 (CESA-2016:1292) | Critical | 144 |
| 91605 | MS16-077: Security Update for WPAD (3165191) | Critical | 131 |
| 89059 | CentOS 6 / 7 : openssl (CESA-2016:0301) (DROWN) | Critical | 98 |

Last Updated: 5 hours ago

### Understanding Risk - Most Prevalent

| Plugin ID | Name | Severity | Host Total |
|---|---|---|---|
| 51192 | SSL Certificate Cannot Be Trusted | Medium | 468 |
| 9312 | OpenSSH < 7.2p2 X11Forwarding xauth Command Injection | Medium | 406 |
| 7200 | TLS Certificate Signed Using Weak Hashing Algorithm - SHA-1 | Low | 401 |

Last Updated: 5 hours ago

### Understanding Risk - By Asset Group

| Asset | Total | Vulnerabilities |
|---|---|---|
| Exploitable (Generic) | 319161 | |
| Exploited by Malware | 303460 | |

# Examples: Research
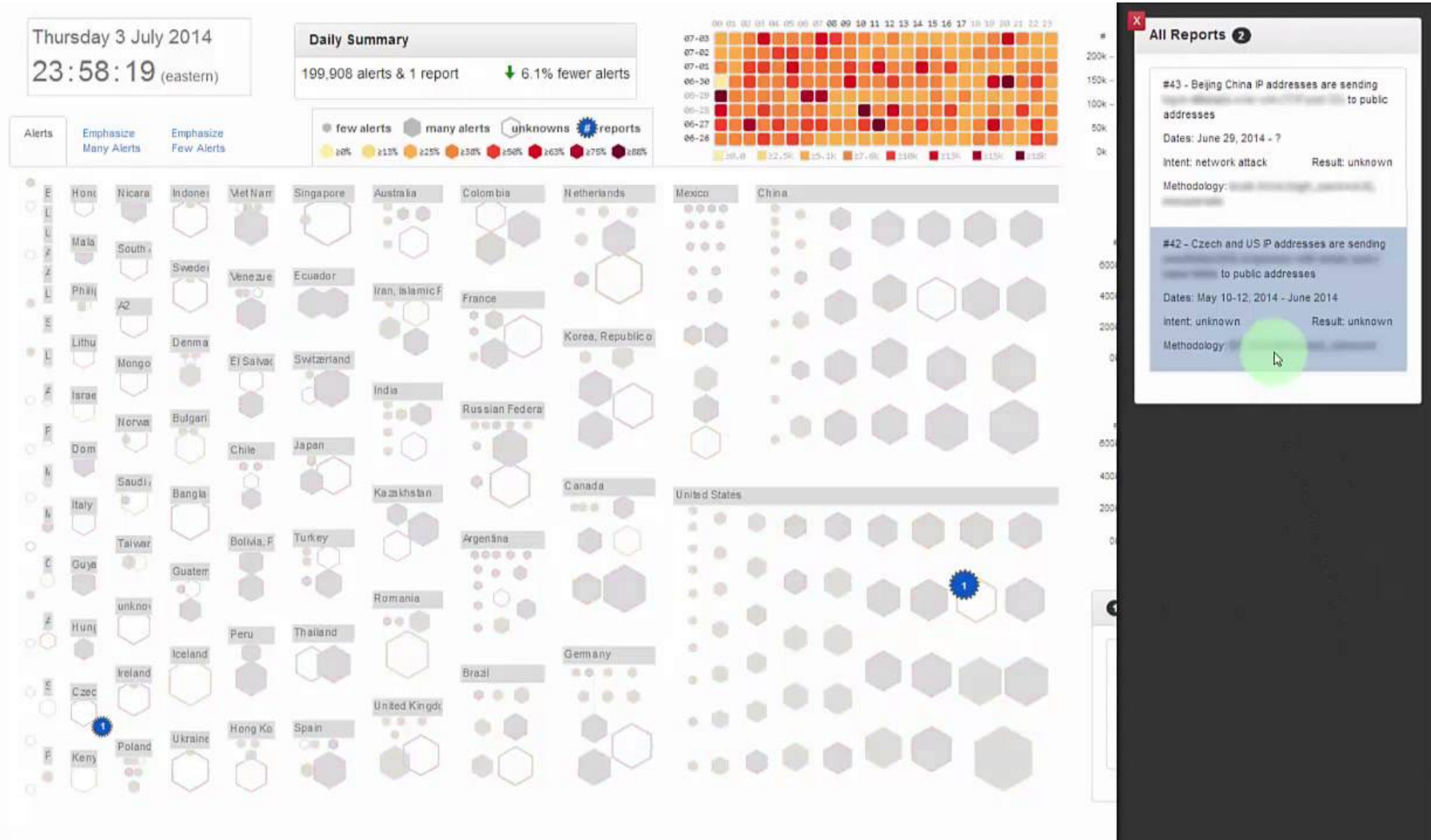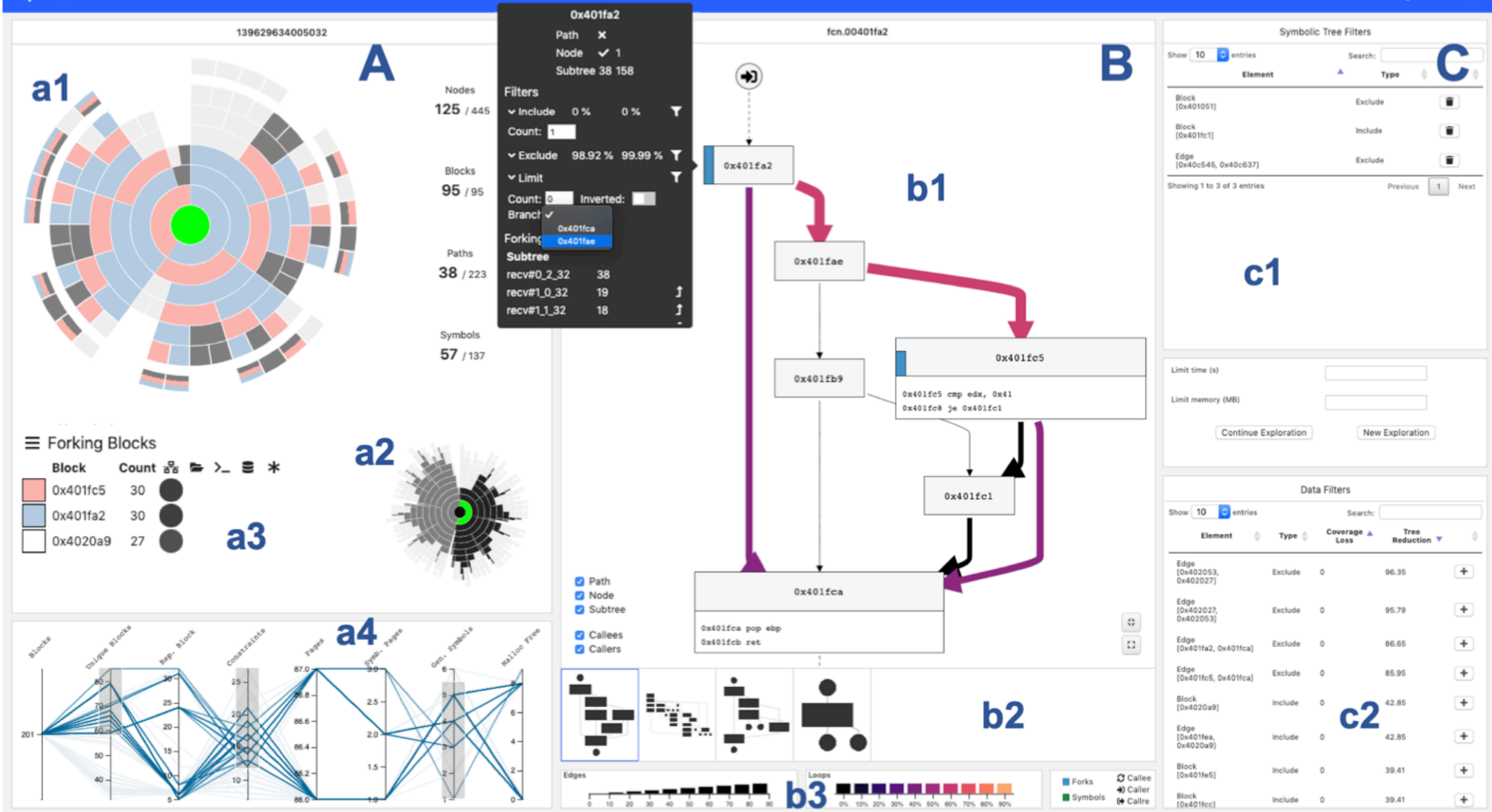
# Analysis

# Characteristics

- Drill-down **Visual Analytics Tools**

  - Usually designed for particular use-case (e.g., malware vs. network analysis)

- **Goal(s):** Reduce "time-to-insight", automate repetitive tasks, help to identify anomalies in data

- **Typical visualizations:** linked views, basic but also novel visualization types

- Extend command line interface, use of APIs

  - Supported in existing systems (e.g, Splunk, Flowmon ADS) vs. custom-made tools

- Computational notebooks (e.g., Jupyter) are also in this category

# Example: File System Analysis



Source: [6]

# Example: Traffic Analysis
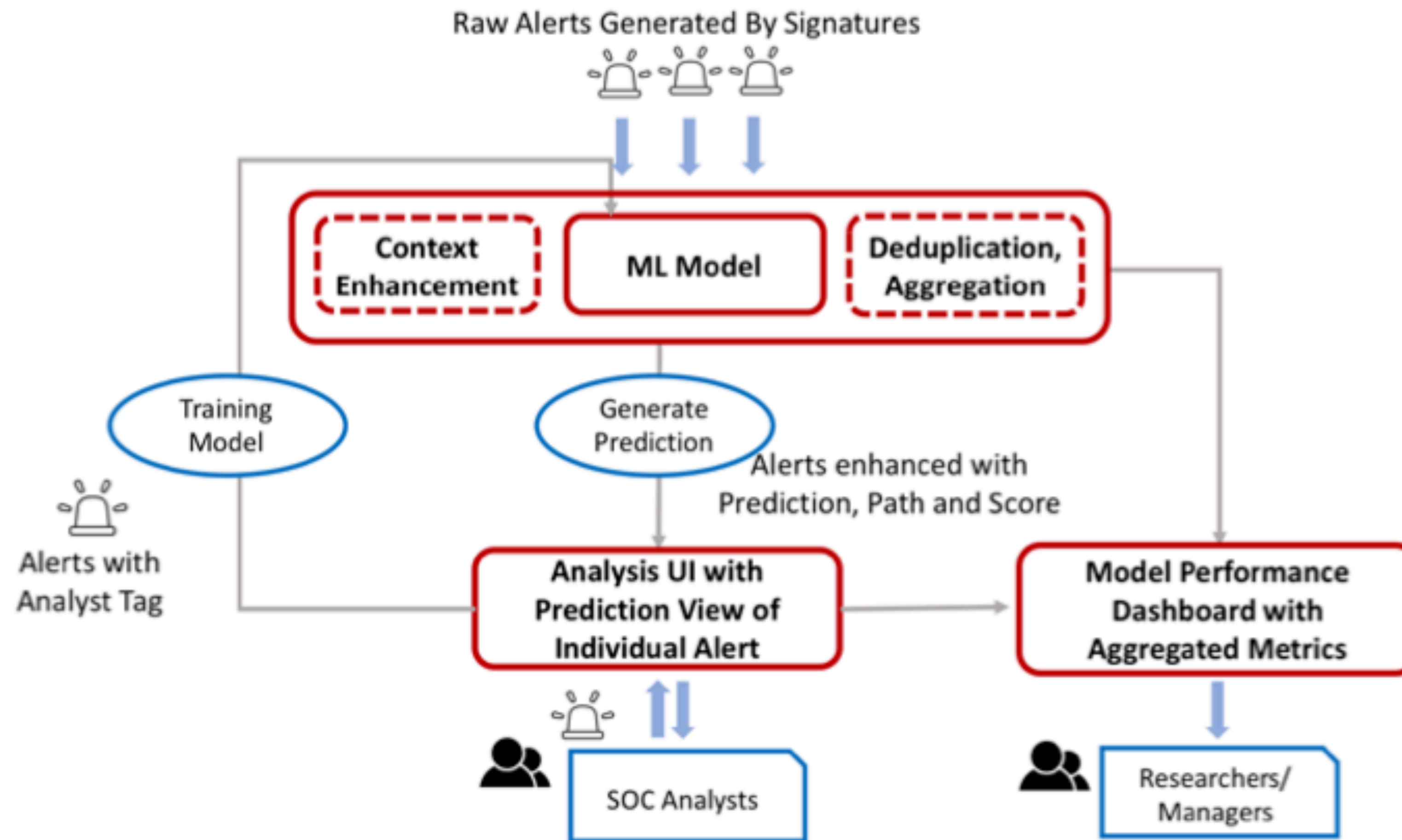
# Predictions and Simulations

# Characteristics

- Visual support for understanding **ML/AI** techniques, visualizations for explainability (**XAI = eXplainable AI**)

- **Goal(s):** understanding ML/AI techniques, behavior explanation, trust building

- **Typical visualizations:** clustering visualizations (for dimensionality reduction methods), linked views, basic visualizations

- Rise on popularity correlates with growing application of ML/AI in cybersecurity.

- Explainability approaches are transferable between different domains

# AI in Cybersecurity

- Application of AI in cybersecurity is substantially difficult comparing to domains such as image recognition

- Three main areas:

  - **Insights Generation:** analyze the data to discover hidden patterns which can be used by decision-makers in order to react to anomalies.

  - **Recommendations:** the model discovers patterns in the data and provides recommendations on what should be best to do to a security specialist.

  - **Autonomous mitigation:** the model discovers patterns and tries to automatically solve problems without needing user input (e.g., approvals).

# Example: Alert Predictions
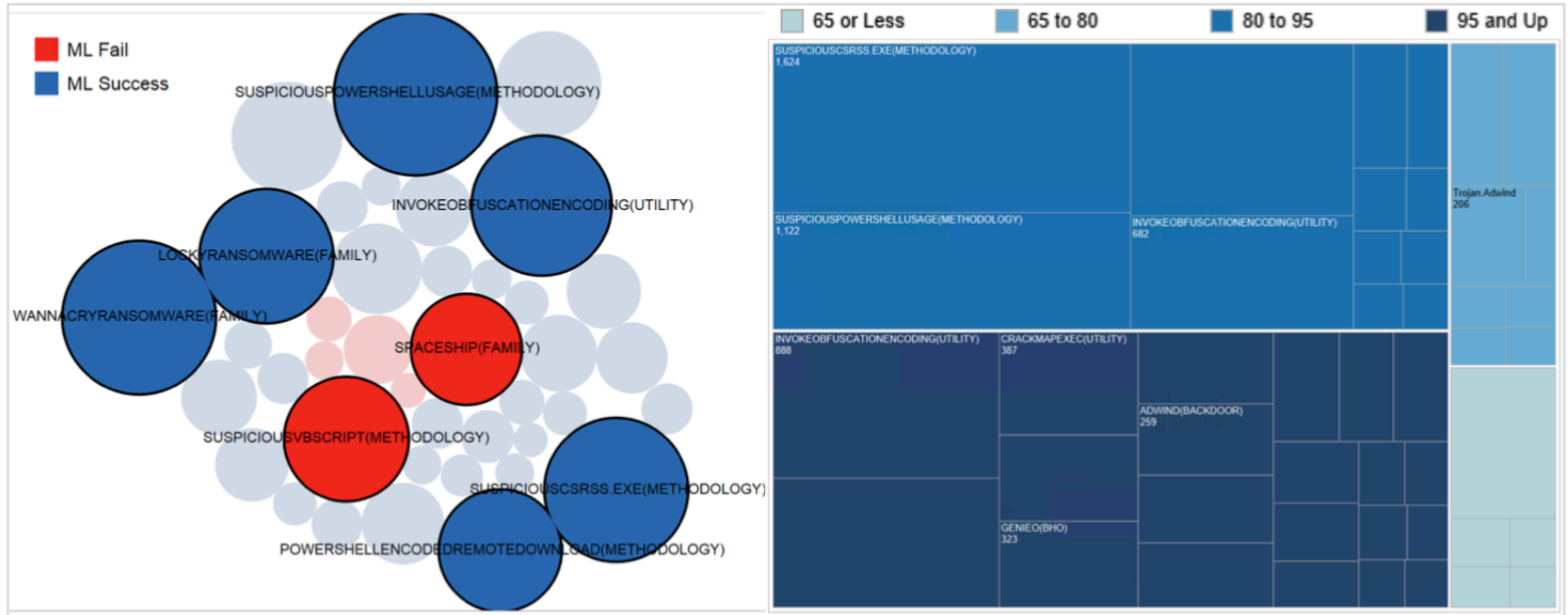


Figure 7: Left: Circle pack visualization showing alerts by signatures. Each circle represents alerts from a particular signature. Circles are sized by the total alerts of that signature and color coded by the ML Model success of ML failure. Right: A Treemap visualization showing only alerts that are correctly labeled by the model, grouped by signatures. Color coded by prediction Score range, sized by total number of alerts in that signature group. It shows which signatures are more common and how the model is performing to classify alerts triggered by those signatures.

# Simulations

- Largely unexplored

- Areas:

  - Attack surface and attack vectors

  - Scenario modelling tool

  - Autonomous agents (attackres) behavior

  - Comparison and explanation of their decisions

# CyberSecVis Research

## VizSec papers 2004—2015



**Top 5 Words in Cluster**
- 🔴 malware, sample, execution, imaging, virus
- 🔺 ip, ported, hosts, traffic, packet
- 🟢 analysts, task, models, cyber, alerts
- 🟣 attacks, graph, node, vulnerabilities, exploit
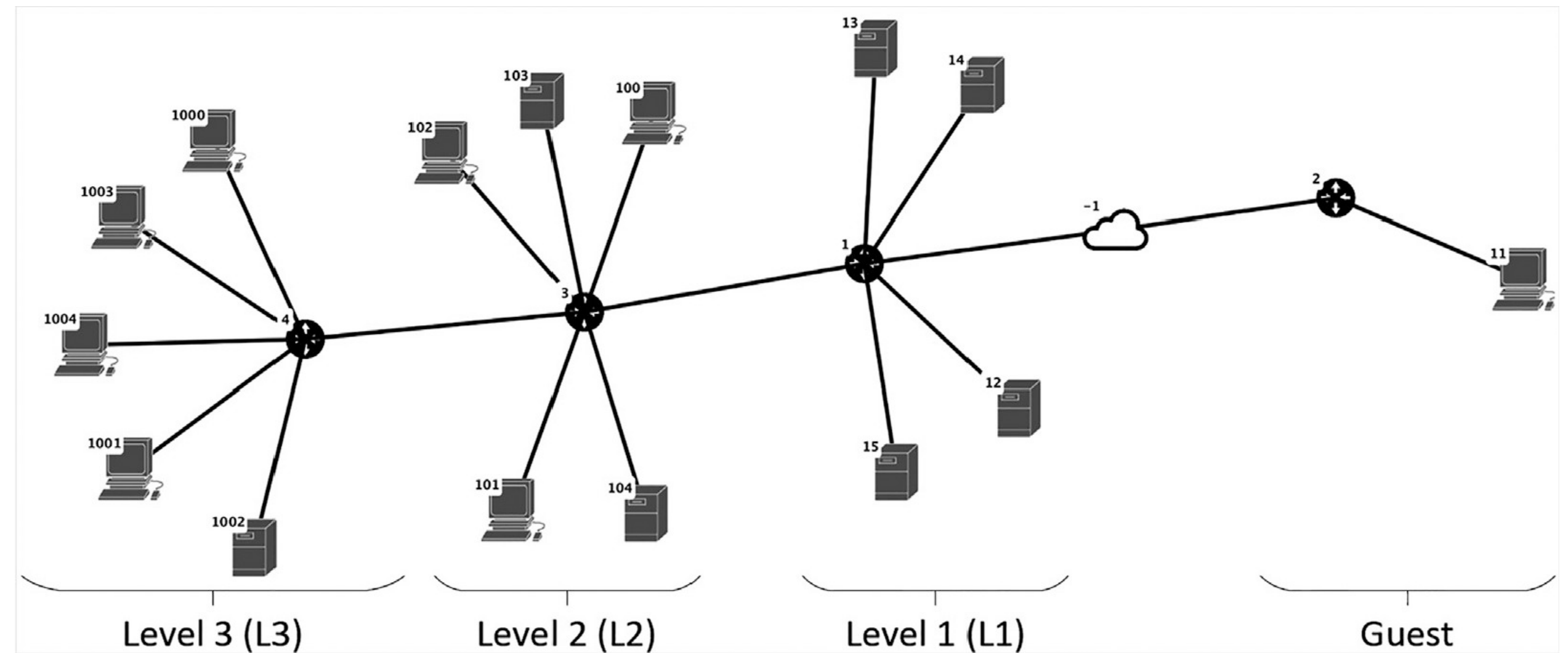
# Utilization of Visualizations

**VizSec papers 2004—2015**
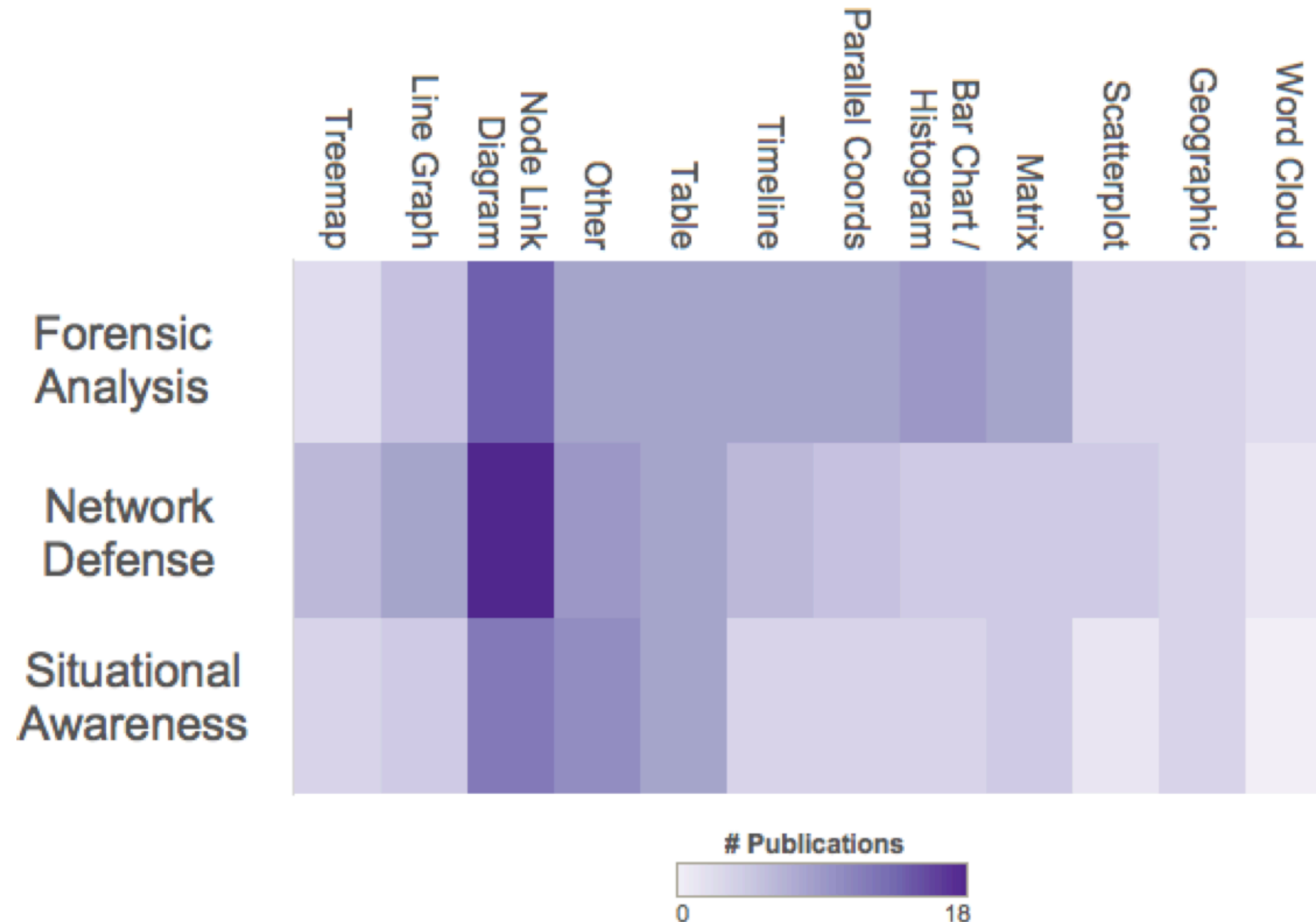
# Utilization of Visual Metaphors

**VizSec papers 2004—2015**
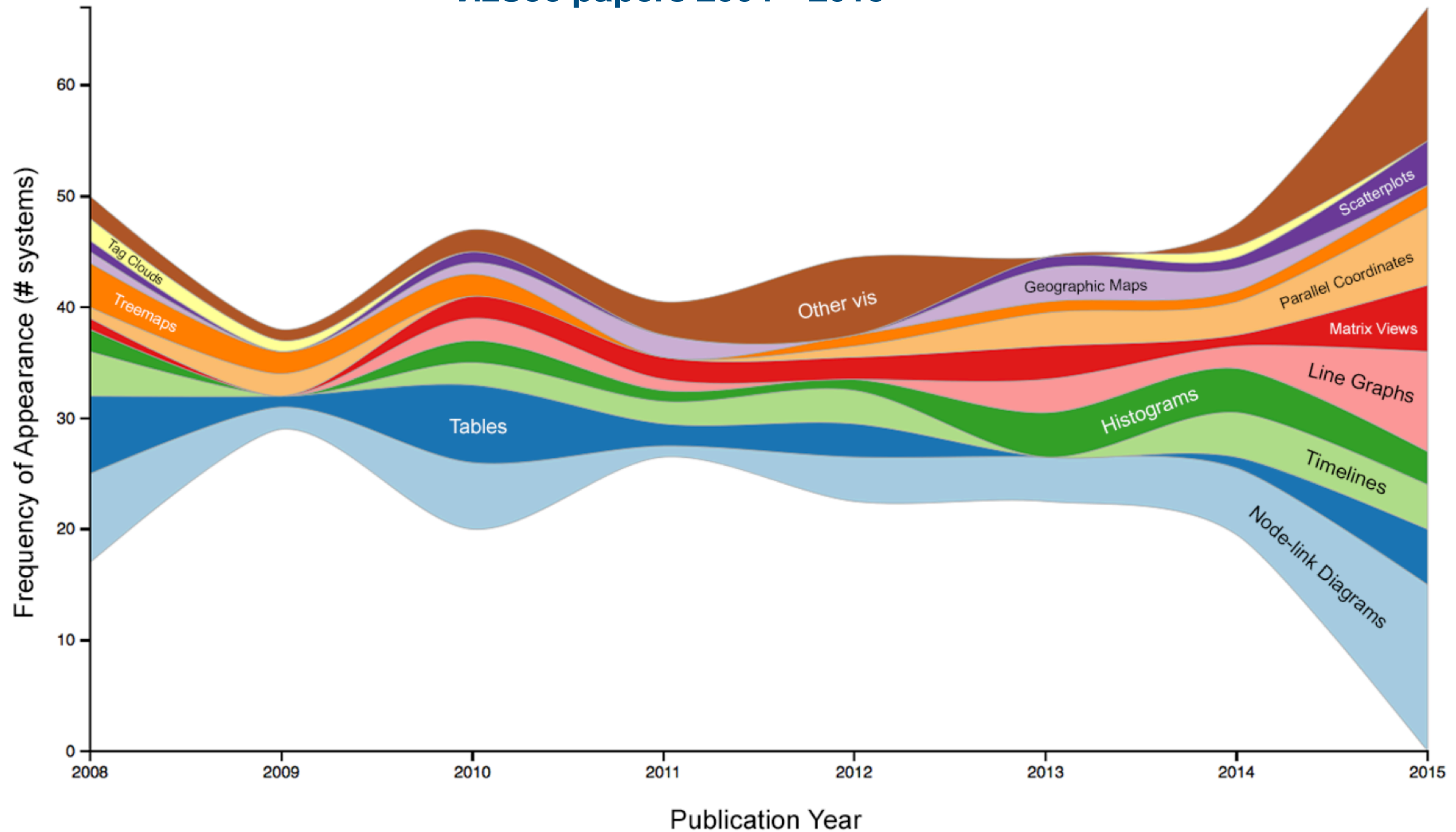
# Interface Complexity

**VizSec papers 2004—2015**



Source: [3]
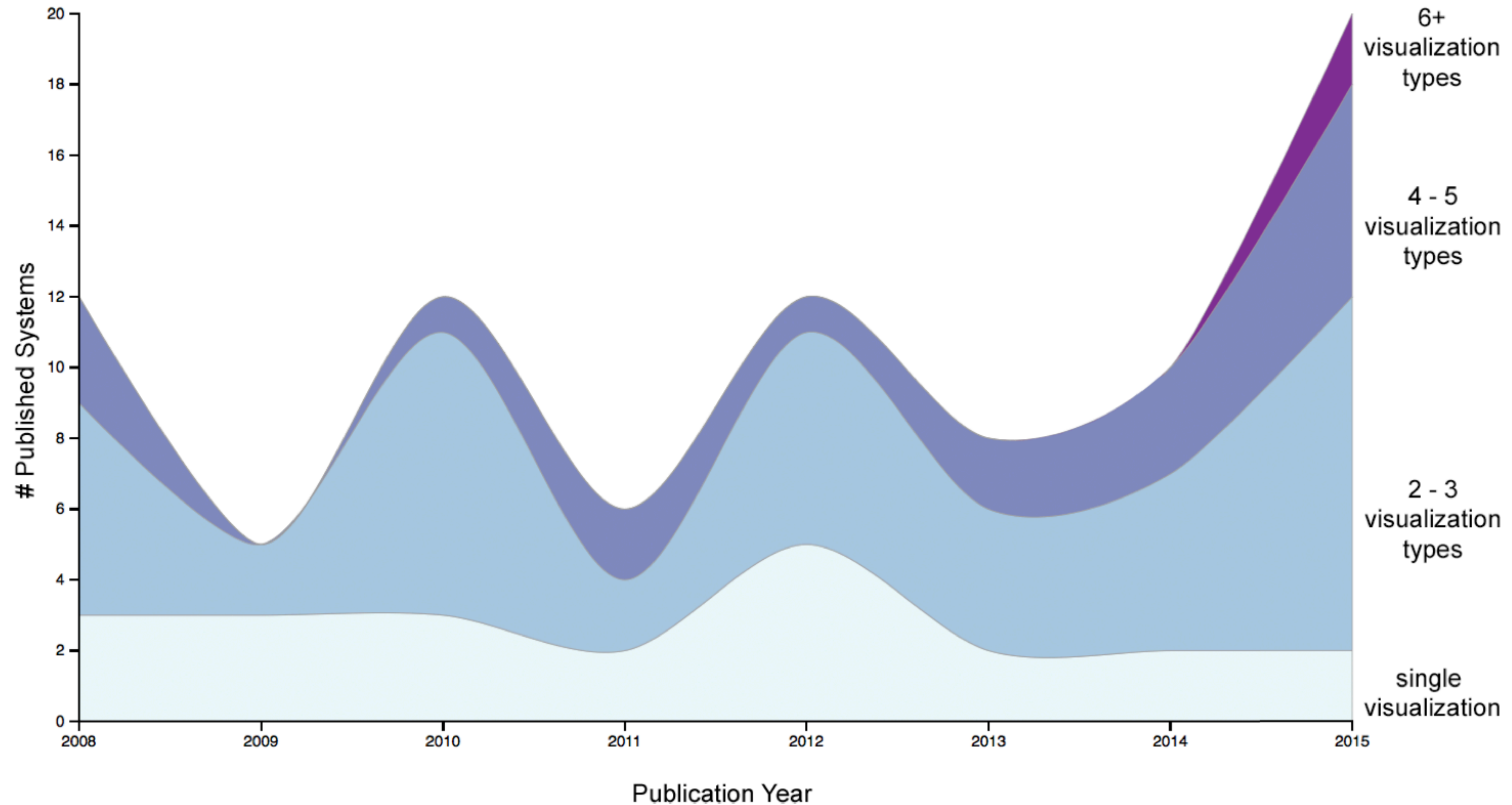
# Take-aways

- Cybersecurity visualizations (as many others) span multiple subcategories

- Common 2D charts are predominant, complex visualizations are mostly research prototypes only

- The commercial tools use only common charts and visualizations …

  … → lot of space for improvements

- Growing area of interest due to the lack of skilled personnel.

# Resources

- [1] Raffael Marty. 2008. Applied Security Visualization (1st. ed.). Addison-Wesley Professional.

- [2] Jay Jacobs, Bob Rudis. 2014. Data-Driven Security: Analysis, Visualization and Dashboards.

- [3] R. J. Crouser, E. Fukuda and S. Sridhar, "Retrospective on a decade of research in visualization for cybersecurity," *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, USA, 2017, pp. 1-5, doi: 10.1109/THS.2017.7943494.

- [4] S. Mckenna, D. Staheli and M. Meyer, "Unlocking user-centered design methods for building cyber security visualizations," *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Chicago, IL, USA, 2015, pp. 1-8, doi: 10.1109/VIZSEC.2015.7312771.

- [5] M. Angelini *et al*., "SymNav: Visually Assisting Symbolic Execution," *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Vancouver, BC, Canada, 2019, pp. 1-11, doi: 10.1109/VizSec48167.2019.9161524.

- [6] M. Beran, F. Hrdina, D. Kouřil, R. Ošlejšek and K. Zákopčanová, "Exploratory Analysis of File System Metadata for Rapid Investigation of Security Incidents," *2020 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Salt Lake City, UT, USA, 2020, pp. 11-20, doi: 10.1109/VizSec51108.2020.00008.

- [7] B. C. M. Cappers, P. N. Meessen, S. Etalle and J. J. van Wijk, "Eventpad: Rapid Malware Analysis and Reverse Engineering using Visual Analytics," *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Berlin, Germany, 2018, pp. 1-8, doi: 10.1109/VIZSEC.2018.8709230.

- [8] A. Ulmer, D. Sessler and J. Kohlhammer, "NetCapVis: Web-based Progressive Visual Analytics for Network Packet Captures," *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Vancouver, BC, Canada, 2019, pp. 1-10, doi: 10.1109/VizSec48167.2019.9161633.

- [9] A. Sopan, M. Berninger, M. Mulakaluri and R. Katakam, "Building a Machine Learning Model for the SOC, by the Input from the SOC, and Analyzing it for the SOC," *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Berlin, Germany, 2018, pp. 1-8, doi: 10.1109/VIZSEC.2018.8709231.

- [10] B. C. M. Cappers and J. J. van Wijk, "SNAPS: Semantic network traffic analysis through projection and selection," *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Chicago, IL, USA, 2015, pp. 1-8, doi: 10.1109/VIZSEC.2015.7312768.

- [11] Moskal S, Yang SJ, Kuhl ME. Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach. *The Journal of Defense Modeling and Simulation*. 2018;15(1):13-29. doi:10.1177/1548512917725408

**Other**

- IEEE Symposium on Visualization for Cyber Security https://vizsec.org and its database of published papers: https://vizsec.dbvis.de

- Shixia Liu, Xiting Wang, Mengchen Liu, Jun Zhu, Towards better analysis of machine learning models: A visual analytics perspective, Visual Informatics, Volume 1, Issue 1, 2017, Pages 48-56, ISSN 2468-502X