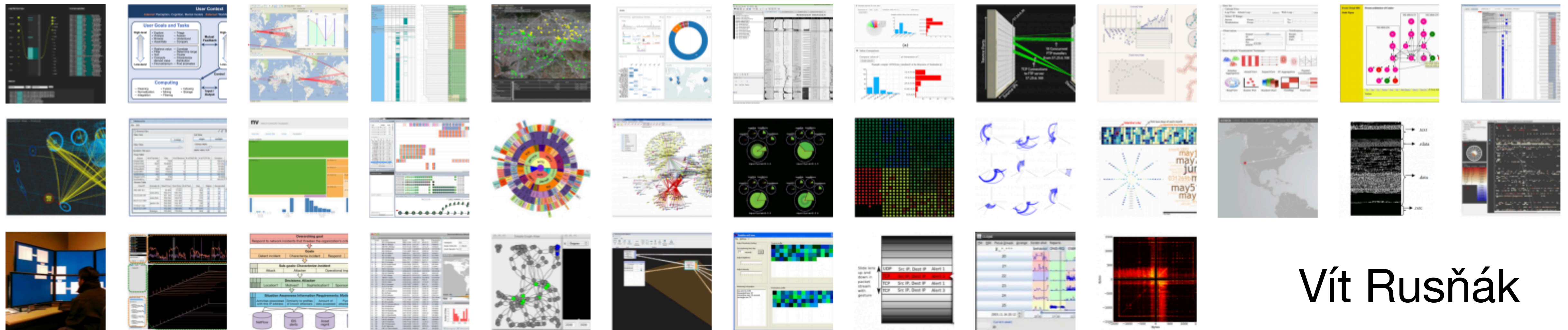
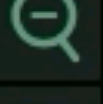
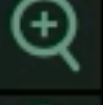
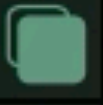


Visualizations for Cybersecurity

PA214 — Visualization II



Vít Rusňák



DEMO
ON

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)



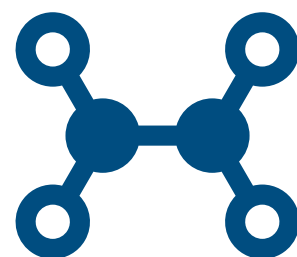
- network traffic anomalies, malware analysts, penetration testing

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

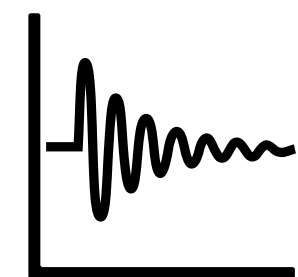
Passive Network
Analysis

Traffic Flows

Packet Captures

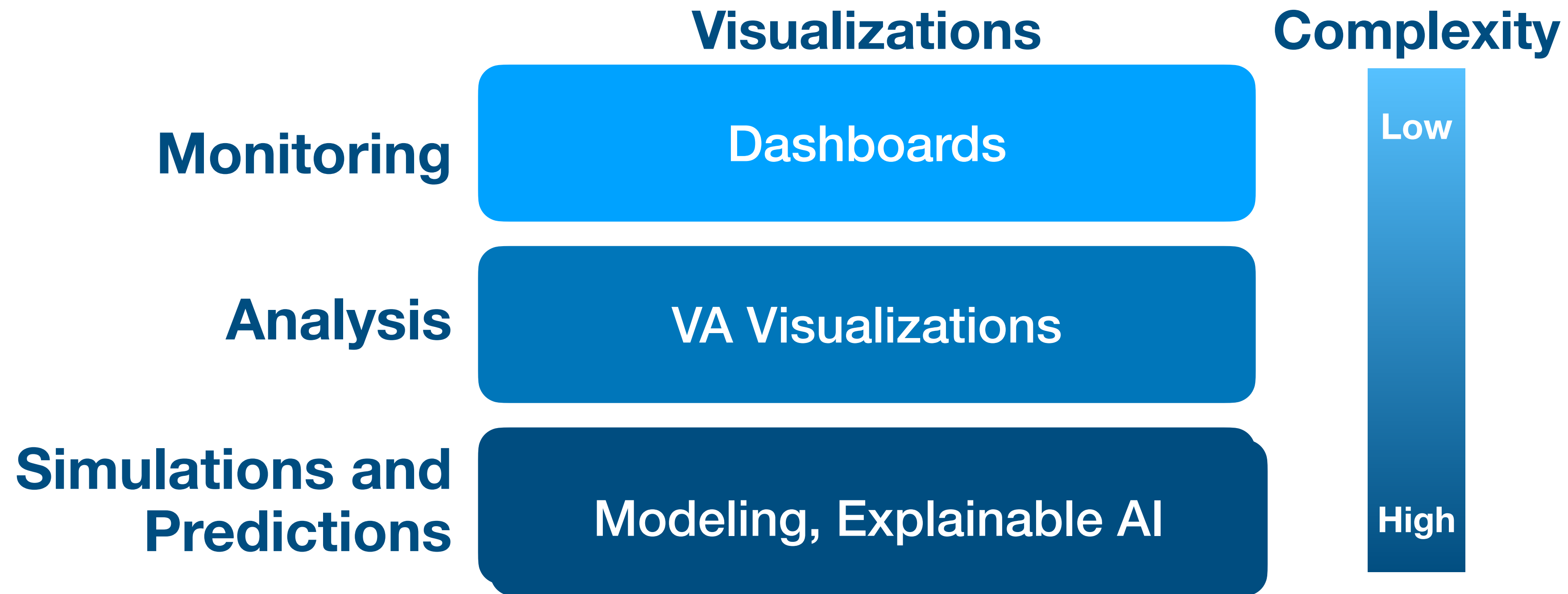


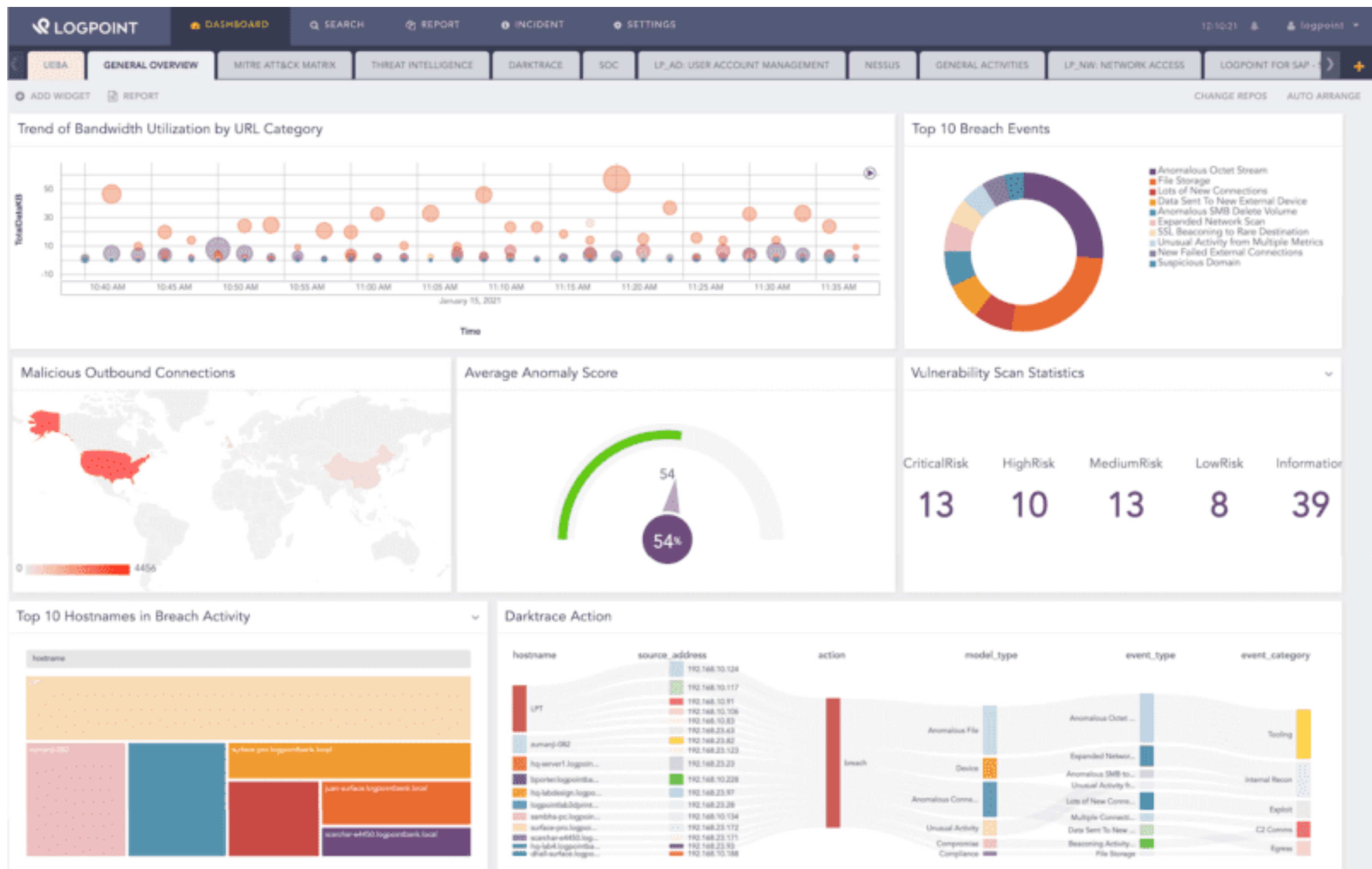
Logs



Time-series

Complexity of Visualizations





Monitoring

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

Dashboard Reports Notifications 0 English demo

Status NetOps SecOps Inet Traffic MySQL DB QoS ETA/TLS DNS Office 365 Social Networks Last 24 hours

Security sta... Last 24 hours (generic time span)




Critical priority events: 81

Security issues

[Show details](#)

Event overview by type



Event type	Name	Number of events	
1	SMTPANOMALY	Detection of outgoing e-mail SPAM using SMTP or secured SMTP protocol	26
2	DICTATTACK	Detection of dictionary attacks on various protocols.	22
3	BLACKLIST	Detection of communication with blacklisted IP addresses	11
4	RDPDICT	Advanced detection method revealing dictionary attacks on Remote Desktop Protocol	11
5	UPLOAD	Detection of uploading data	11
6	BPATTERNS	Detection of current threats by unified flow-based behavior patterns.	24
7	WEBSHARE	Detection of data sharing services through web like Rapidshare etc.	13
8	TEAMVIEWER	Detection of TeamViewer	13
9	SCANS	Detection of TCP scans (SYN scan, FIN scan, Xmas scan, Null scan)	11
10	ICMPANOM	Detection of anomalies in ICMP traffic	22
	Others		22
	Total		186


Top 10 event types by priority and count

Event type	Name	Number of events	
1	SMTPANOMALY	SMTP anomaly	26
2	DICTATTACK	Dictionary attacks	22
3	BLACKLIST	Communication with blacklisted hosts	11
4	RDPDICT	RDP attack	11
5	UPLOAD	Data upload anomaly	11
6	BPATTERNS	Flow-based behavior patterns	24
7	WEBSHARE	Web sharing traffic	13
8	TEAMVIEWER	TeamViewer traffic	13
9	SCANS	Port scanning	11
10	ICMPANOM	ICMP anomaly	22

The latest 10 new events

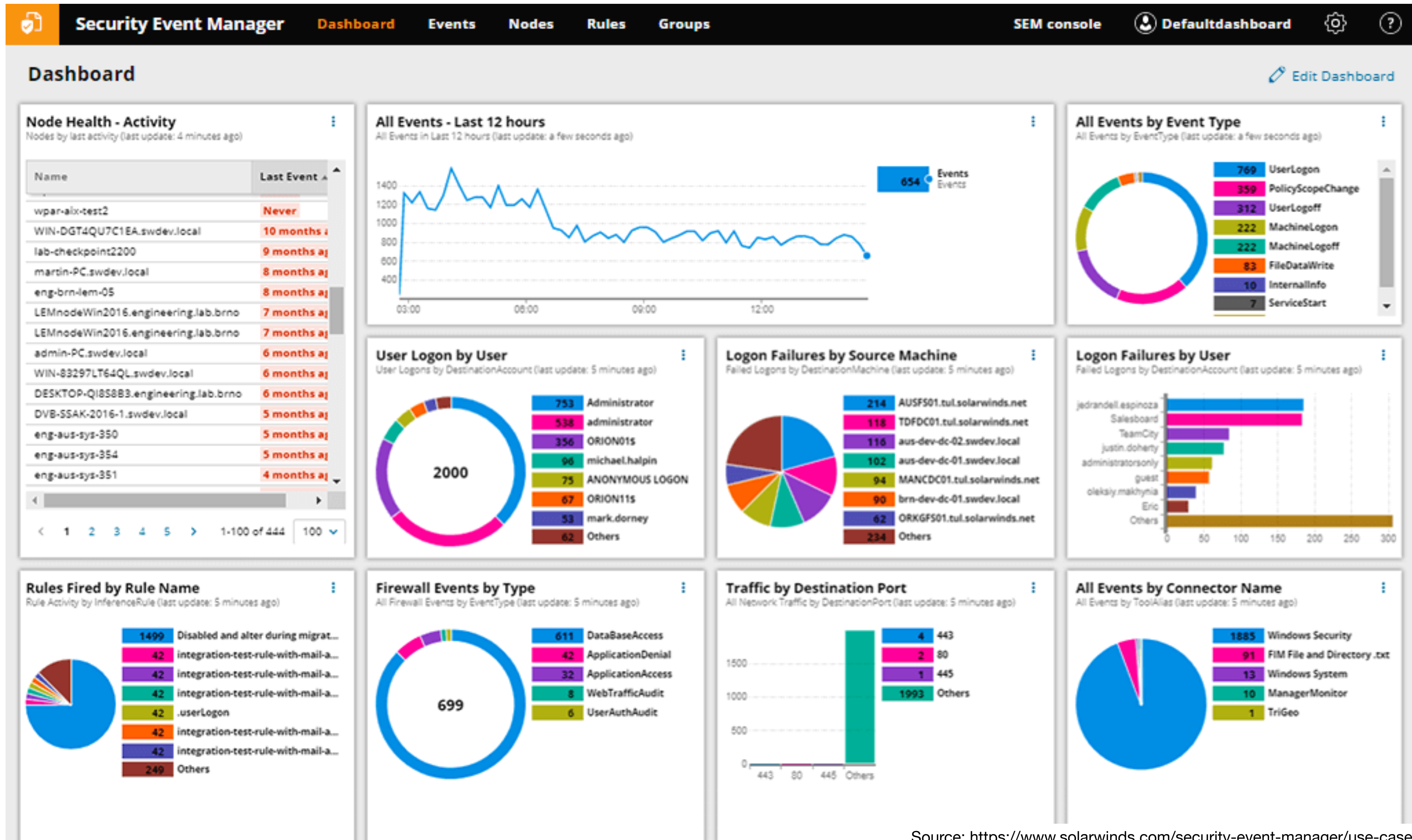
Event type	Name	Event source	Targets	Detection time
1	SMTPANOMALY	172.17.107.32	0.136.226.185, 0.179.120.11, 0.246.126.78, ...	2021-03-28 21:13:20
2	BPATTERNS	192.168.70.2	www.pulskom.com, 192.168.70.253, 209-99-40-220.fwd.datafoundry.com	2021-03-28 21:05:15
3	WEBSHARE	192.168.70.16	77.48.29.200	2021-03-28 21:04:14
4	TEAMVIEWER	10.0.2.15	AT-VIE-ANX-R008.teamviewer.com, ns01.dialtelecom.cz, FR-PAR-ANX-R016.teamviewer.com	2021-03-28 21:03:16
5	SMTPANOMALY	172.17.107.32	0.136.226.185, 0.179.120.11, 0.246.126.78, ...	2021-03-28 21:00:40
6	BPATTERNS	192.168.1.50	192.168.1.2	2021-03-28 20:25:15
7	ICMPANOM	192.168.1.50	node-yr.pool-1-0.dynamic.totinternet.net	2021-03-28 20:11:51
8	ICMPANOM	192.168.1.50	node-yr.pool-1-0.dynamic.totinternet.net	2021-03-28 20:11:51
9	BLACKLIST	192.168.1.50	node-yr.pool-1-0.dynamic.totinternet.net	2021-03-28 20:11:51
10	UPLOAD	192.168.1.50	node-yr.pool-1-0.dynamic.totinternet.net	2021-03-28 20:11:51

Top 10 IPs by event count



Event source	Number of events	
1	192.168.1.50	110
2	172.17.107.32	26
3	10.0.2.15	13
4	192.168.70.2	13
5	192.168.70.16	13
6	192.168.1.2	11
	Others	0

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

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

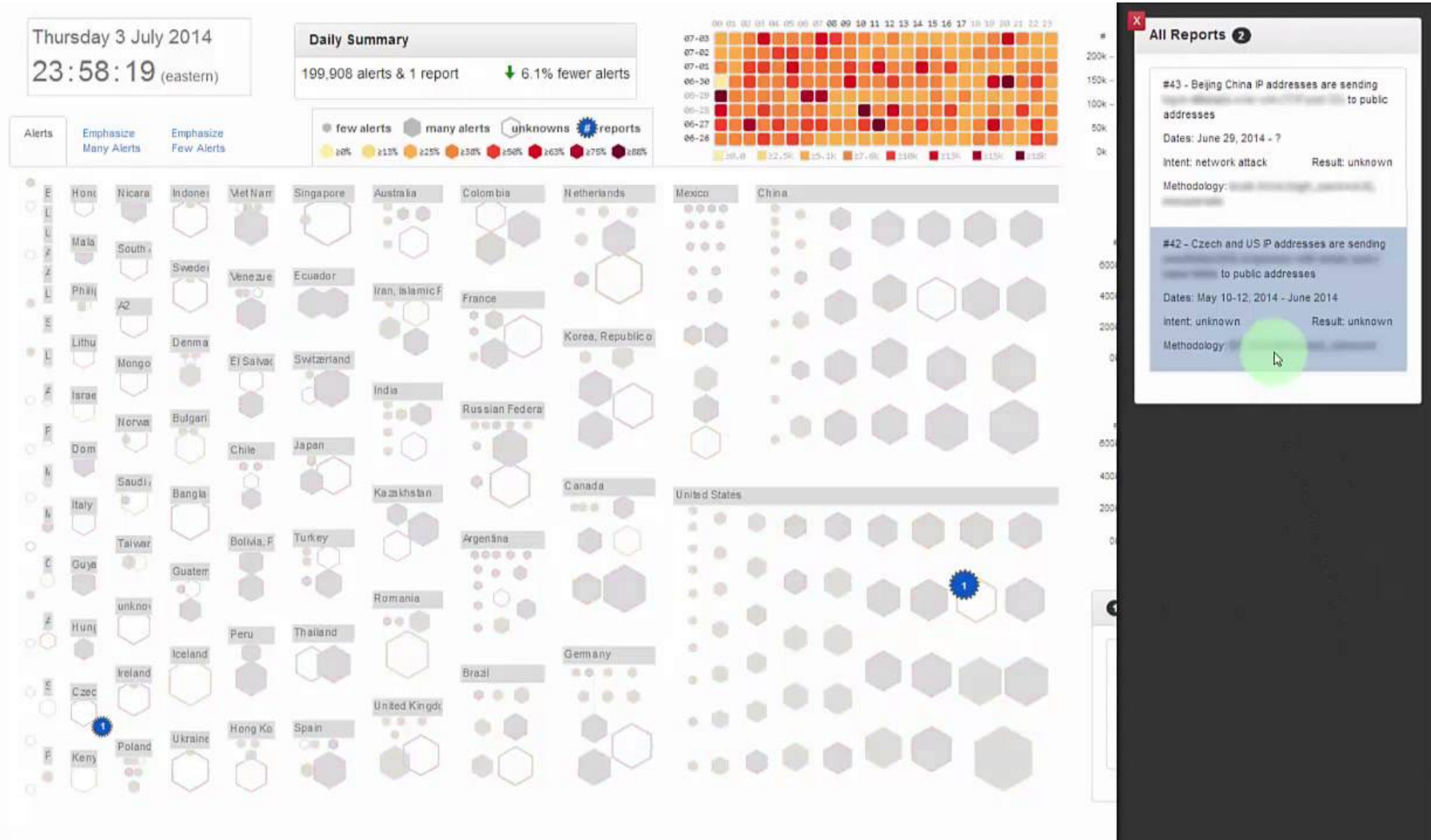
Plugin ID	Name	Severity	Host Total
51192	SSL Certificate Cannot Be Trusted	Medium	468
9312	OpenSSH < 7.2p2 X11Forwarding xauth Command Injection	Medium	406
7200	TLS Certificate Signed Using Weak Hashing Algorithm - SHA-1	Low	401

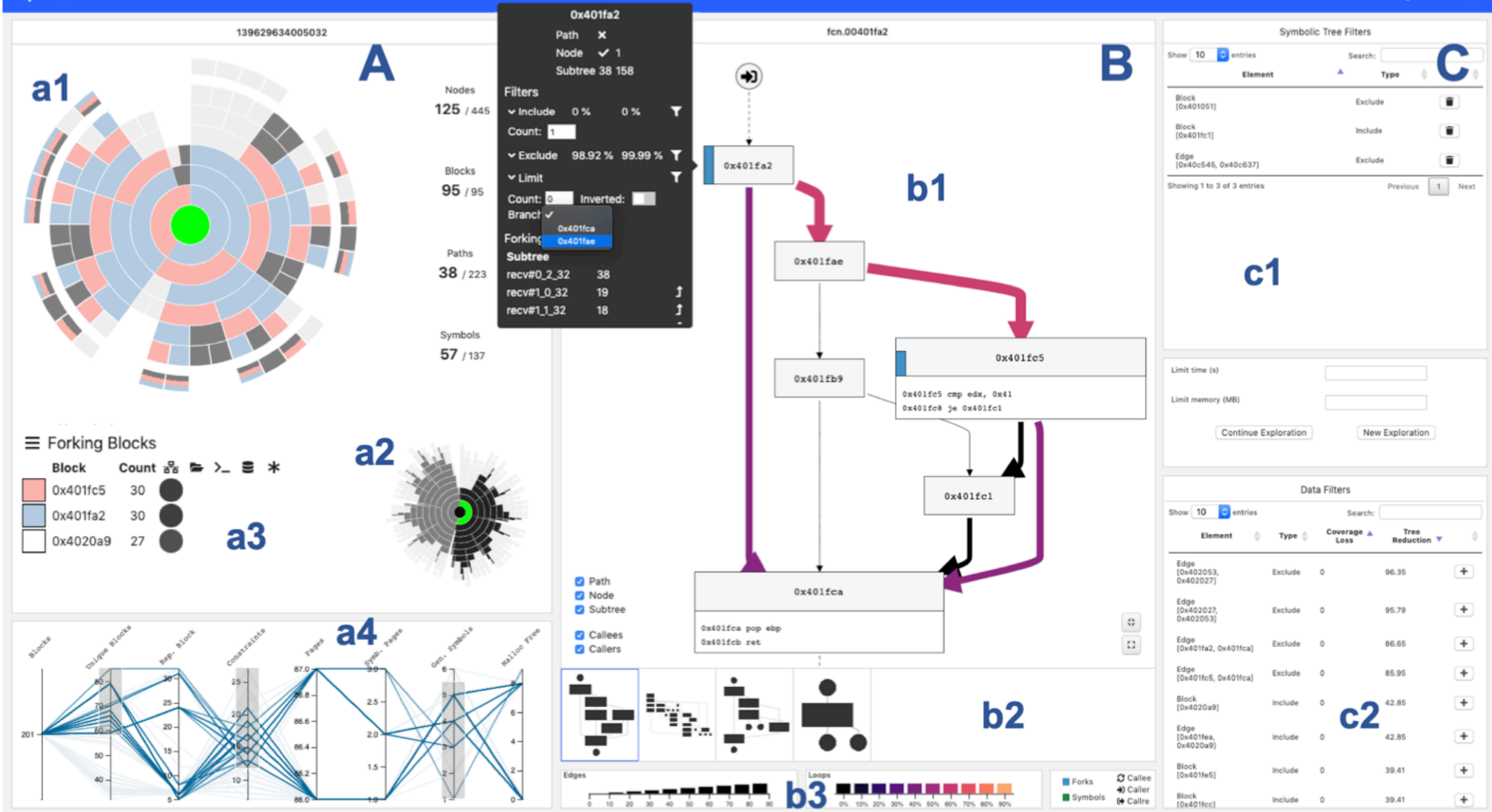
Last Updated: 5 hours ago

Understanding Risk - By Asset Group

Asset	Total	Vulnerabilities
Exploitable (Generic)	319161	191640 / 110612
Exploited by Malware	303460	182596 / 111368

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

admin FILESYSTEM METADATA ANALYSIS

BACK [] FORWARD

Clusters

- cluster name **C**
- filtered entries / total entries
- user SSH files 5 / 10
- standard executables 6612 / 8761
- python scripts 16743 / 18460
- shell scripts 272 / 457
- php scripts 2544 / 2617
- perl scripts **1729 / 3762**
- cron definition 14 / 18
- starts with "." 6619 / 19476
- suspicious files 0 / 11978
- executables with sbit 69 / 119
- weak permissions 0 / 0
- compilation signs 4884 / 9775
- unusual commands 4 / 8
- system configuration changes 227 / 291
- all files 346179 / 501406

MANAGE CLUSTERS

Histogram

SELECTION: 5/3/2011, 7:19:40 AM - 1/22/2016, 7:37:26 AM extend by: 1 day

Timestamp selection: [m] [a] [c] [b] Level: months

Interactive List View

Total: 1729 of: 3762 search by File Name

Timestamp	Size	Type	Mode	UID	GID	File Name
2014-10-09 20:40:29	369	ma..	r/rrwxr-xr	0	0	/usr/share/kde4/apps/kconf_update/useragent.pl
2014-10-09 22:09:43	2418	ma..	r/rrwxr-xr	0	0	/usr/share/kde4/apps/kconf_update/migrate-transport.pl
2014-10-10 09:47:10	2040	ma..	r/rrwxr-xr	0	0	/usr/lib/kde4/libexec/khc_mansearch.pl
2014-10-10 09:47:10	5073	ma..	r/rrw-r--r	0	0	/usr/share/kde4/apps/kio_finger/kio_finger.pl
2014-10-10 09:47:23	5393	ma..	r/rrwxr-xr	0	0	/usr/share/kde4/apps/kconf_update/update_oxygen.pl
2014-10-19 14:19:35	4333	ma..	r/rrwxr-xr	0	0	/usr/share/sgml-data/sgml-catalog-check.pl
2014-10-21 15:53:48	7510	ma..	r/rrw-r--r	0	0	/usr/share/w3m/w3mhelp-funcdesc.en.pl
2014-10-21 15:53:48	8312	ma..	r/rrw-r--r	0	0	/usr/share/w3m/w3mhelp-funcname.pl
2014-10-21 15:53:48	9200	ma..	r/rrw-r--r	0	0	/usr/share/w3m/w3mhelp-funcdesc.ja.pl
2014-10-22 20:11:34	190	ma..	r/rrwxr-xr	0	0	/usr/share/doc/libcgi-pm-perl/examples/make_links.pl
2014-10-23 13:32:50	1543	m...	r/rrwxr-xr	0	0	/usr/lib/libreoffice/share/config/webcast/poll.pl
2014-10-23 13:32:50	1839	m...	r/rrwxr-xr	0	0	/usr/lib/libreoffice/share/config/webcast/show.pl
2014-10-23 13:32:50	1871	m...	r/rrw-r--r	0	0	/usr/lib/libreoffice/share/config/webcast/common.pl
2014-10-23 13:32:50	343	m...	r/rrw-r--r	0	0	/usr/lib/libreoffice/share/config/webcast/index.pl
2014-10-23 13:32:50	558	m...	r/rrw-r--r	0	0	/usr/lib/libreoffice/share/config/webcast/edit.pl
2014-10-23 13:32:50	1400	m...	r/rrwxr-xr	0	0	/usr/lib/libreoffice/share/config/webcast/broadcast.pl
2014-10-23 13:32:50	1950	m...	r/rrwxr-xr	0	0	/usr/lib/libreoffice/share/config/webcast/itpic.pl
2014-10-23 13:32:50	1692	m...	r/rrwxr-xr	0	0	/usr/lib/libreoffice/share/config/webcast/savepic.pl
2014-10-23 22:30:06	15541	m...	r/rrwxr-xr	0	0	/usr/lib/mafft/lib/mafft/seekquencer_premafft.pl
2014-10-23 22:30:06	10481	m...	r/rrwxr-xr	0	0	/usr/lib/mafft/lib/mafft/mafftash_premafft.pl
2014-10-27 21:13:32	1585	ma..	r/rrw-r--r	0	0	/usr/share/doc/initramfs-tools/HACKING (NOT IN SELECTED CLUSTER)
2014-10-27 21:23:33	26	ma..	r/rrw-r--r	0	0	/var/lib/dpkg/info/initramfs-tools.triggers (NOT IN SELECTED CLUSTER)
2014-11-28 13:13:28	15716	ma..	r/rrw-r--r	0	0	/usr/share/dictionaries-common/dc-debconf-default-value.pl
2014-11-28 13:13:28	12162	ma..	r/rrw-r--r	0	0	/usr/share/dictionaries-common/dc-debconf-select.pl
2014-12-04 22:16:50	3472	ma..	r/rrw-r--r	0	0	/usr/share/doc/mutt/examples/smime_keys_test.pl
2014-12-10 20:24:46	2147	ma..	r/rrwxr-xr	0	0	/usr/lib/kde4/libexec/khc_htsearch.pl
2014-12-10 20:25:02	5213	ma..	r/rrwxr-xr	0	0	/usr/lib/kde4/libexec/khc_docbookdig.pl
2014-12-10 20:25:02	3806	ma..	r/rrwxr-xr	0	0	/usr/lib/kde4/libexec/khc_htdig.pl
2015-02-25 09:00:51	1826	ma..	r/rrw-r--r	0	0	/usr/share/doc/binutils/gprof/bbconv.pl

A

B

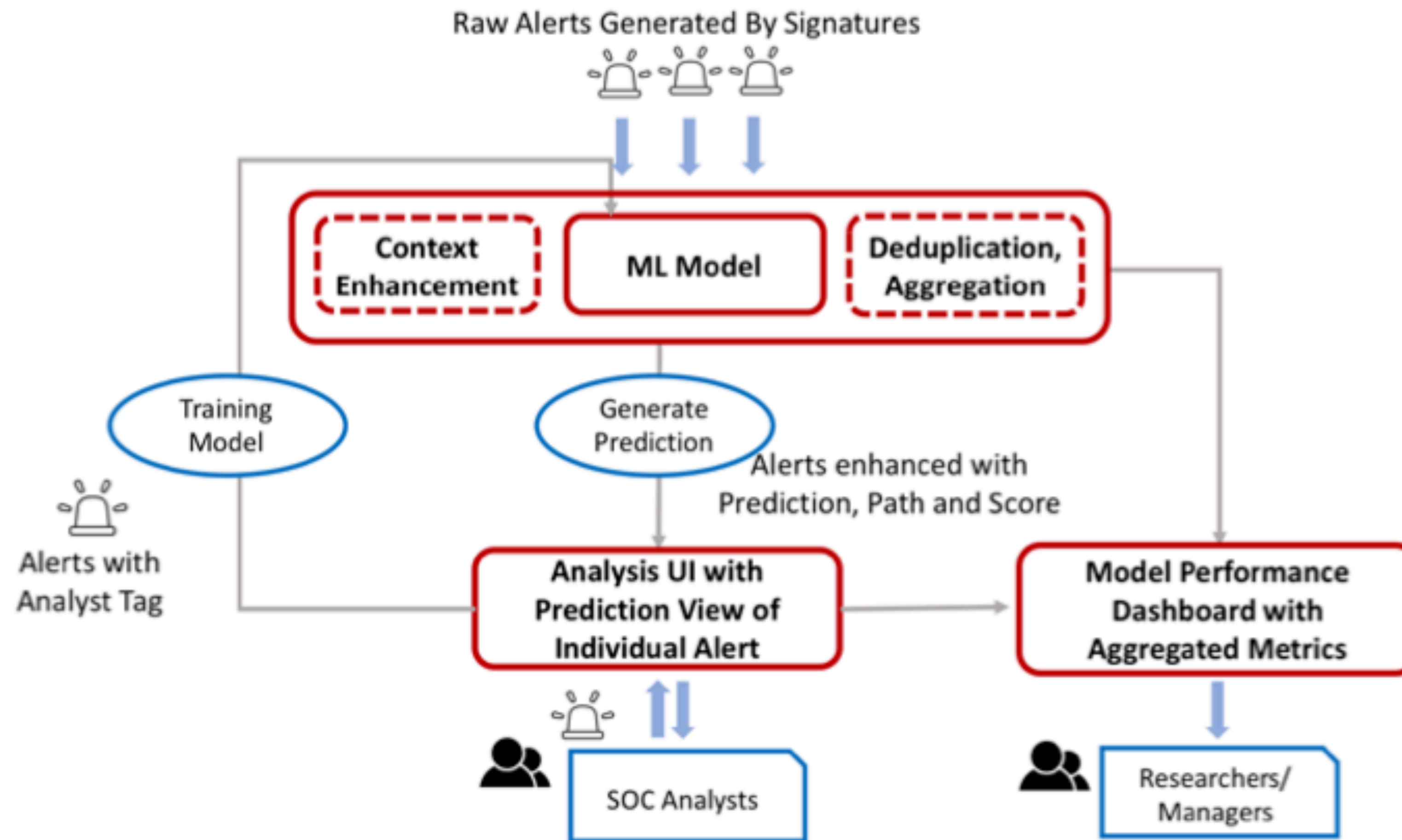
C

Source: [6]

Example: Traffic Analysis

Web-based Visual Interactive 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

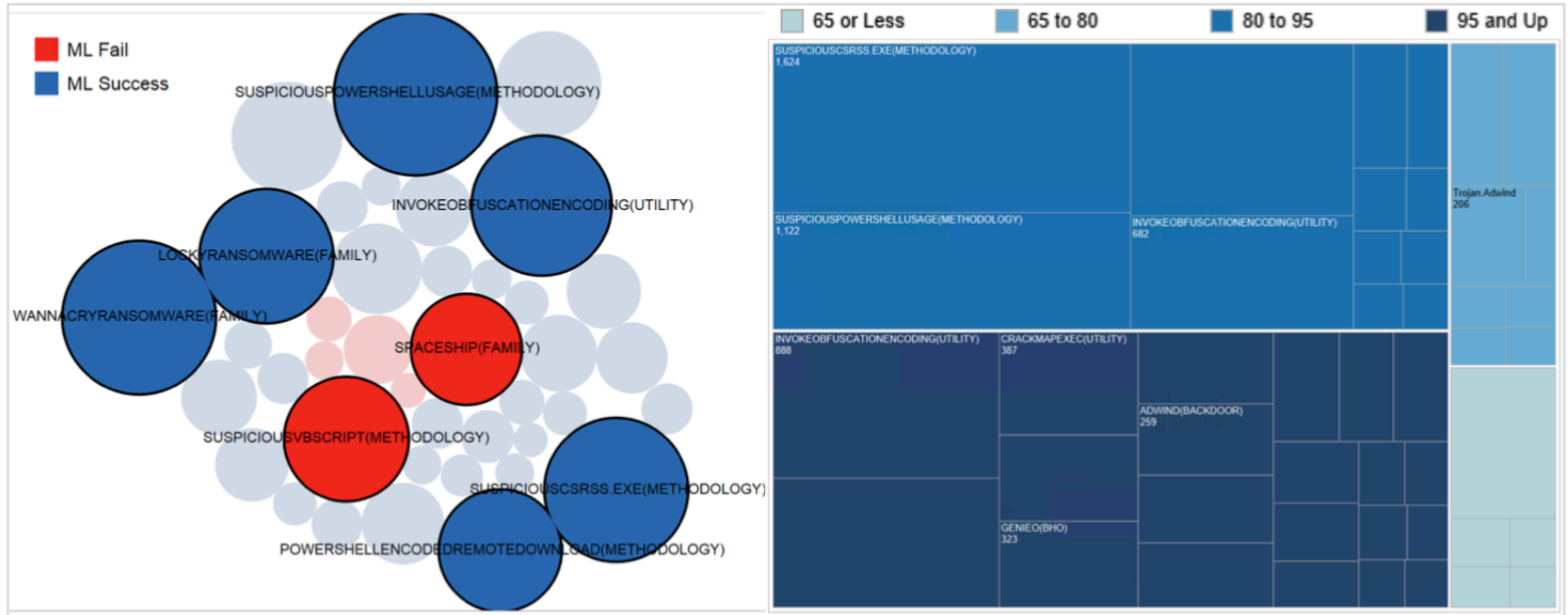
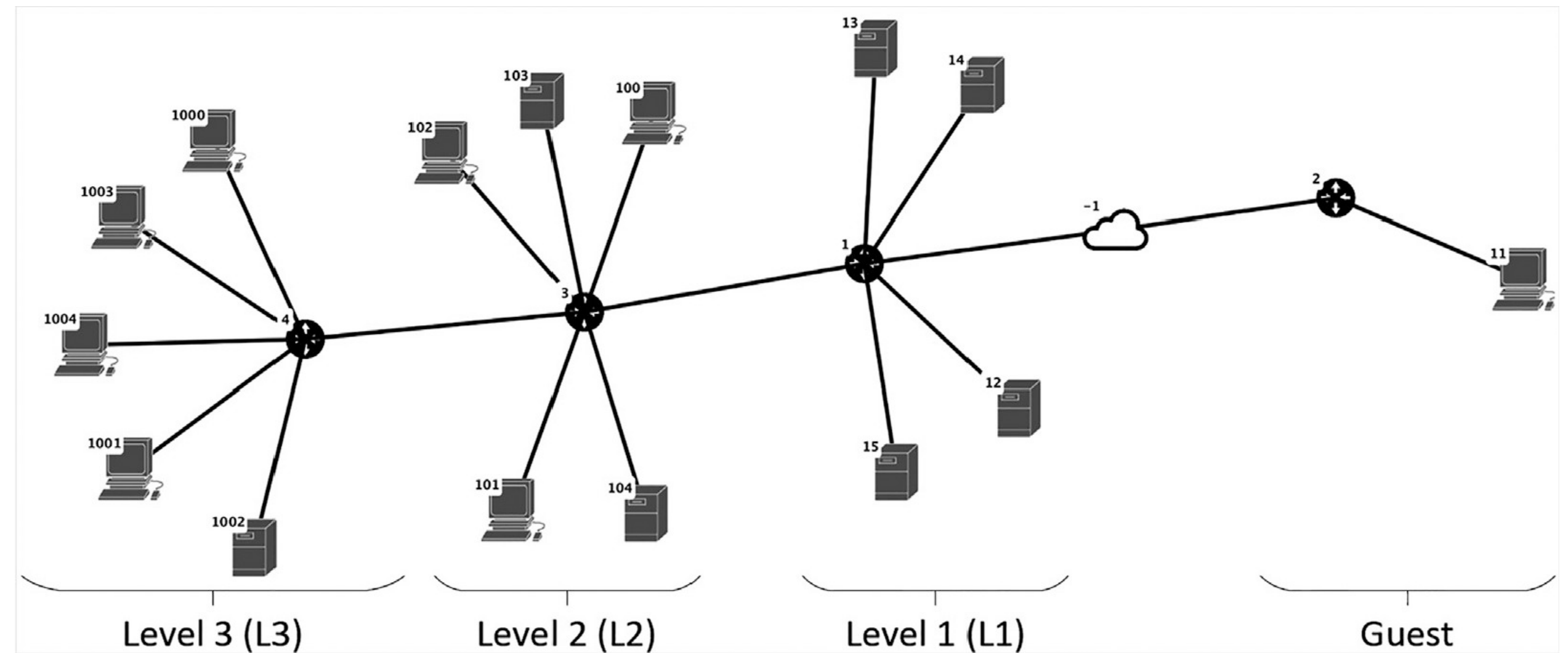


Figure 7: Left: Circle pack visualization showing alerts by signatures. Each circle represents alerts from a particular signature. Circles are sized by the total alerts of that signature and color coded by the ML Model success of ML failure. Right: A Treemap visualization showing only alerts that are 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.

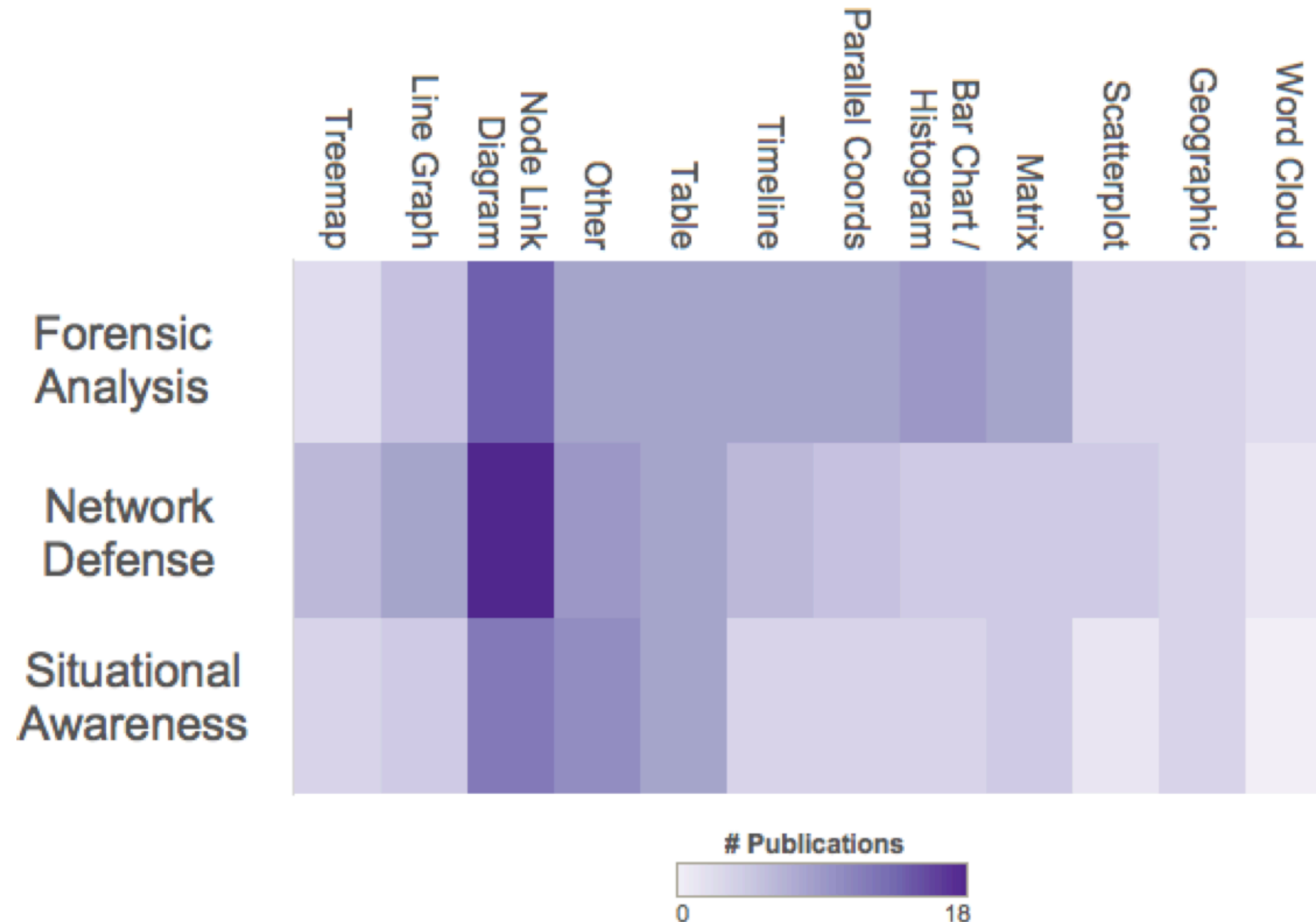
Simulations

- Largely unexplored
- Areas:
 - Attack surface and attack vectors
 - Scenario modelling tool
 - Autonomous agents (attackers) behavior
 - Comparison and explanation of their decisions



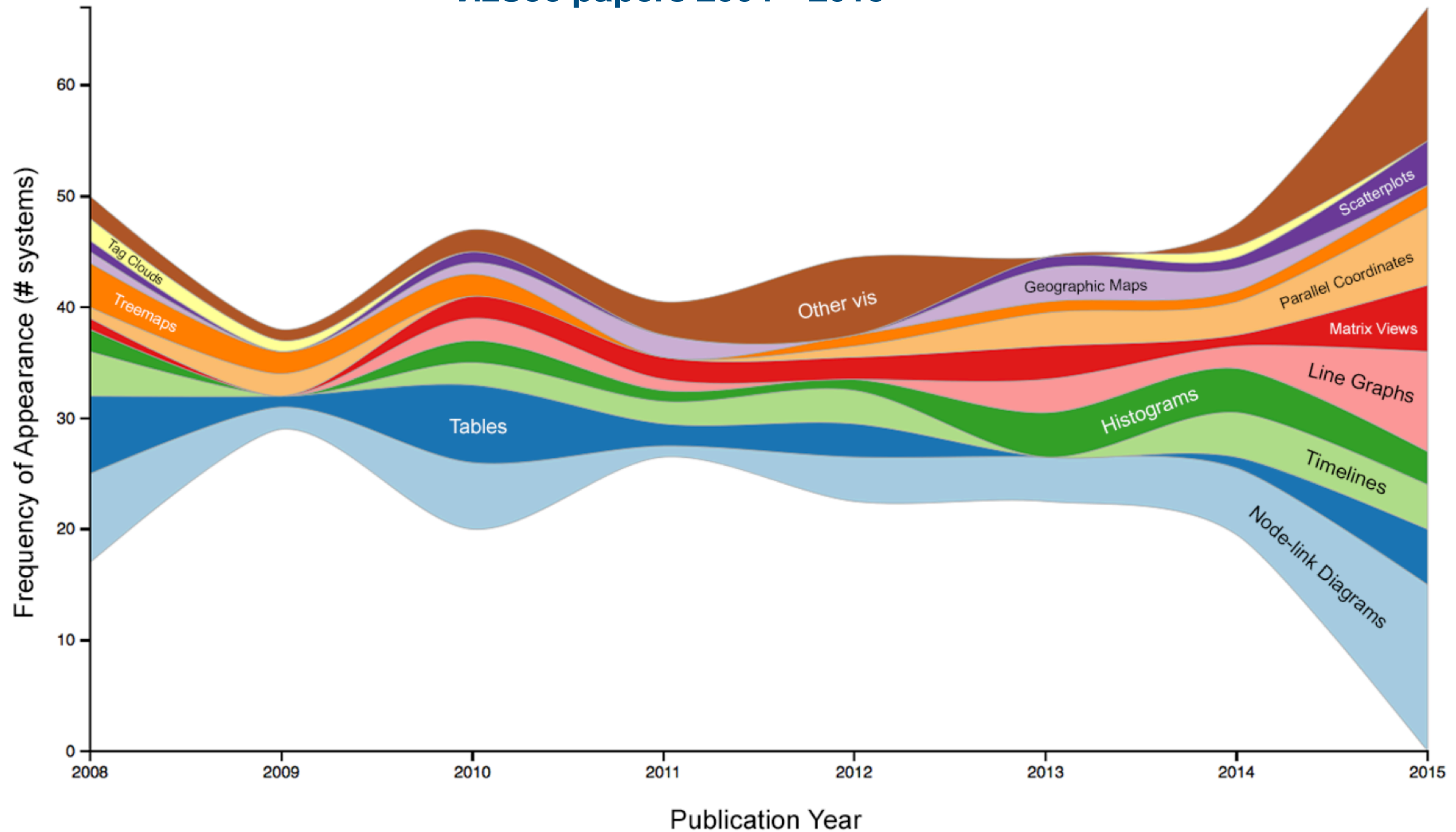
Utilization of Visualizations

VizSec papers 2004–2015



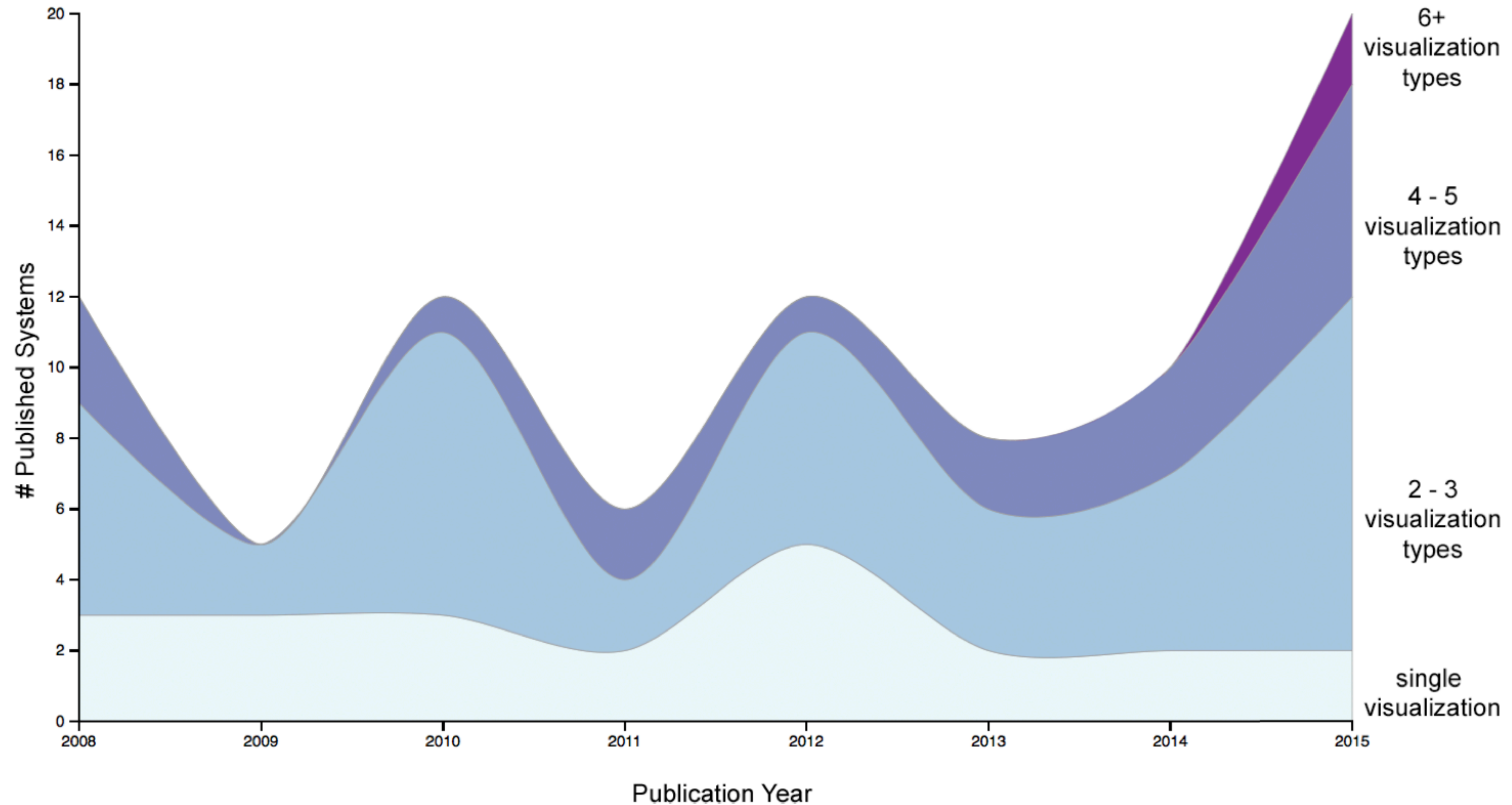
Utilization of Visual Metaphors

VizSec papers 2004–2015



Interface Complexity

VizSec papers 2004–2015



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