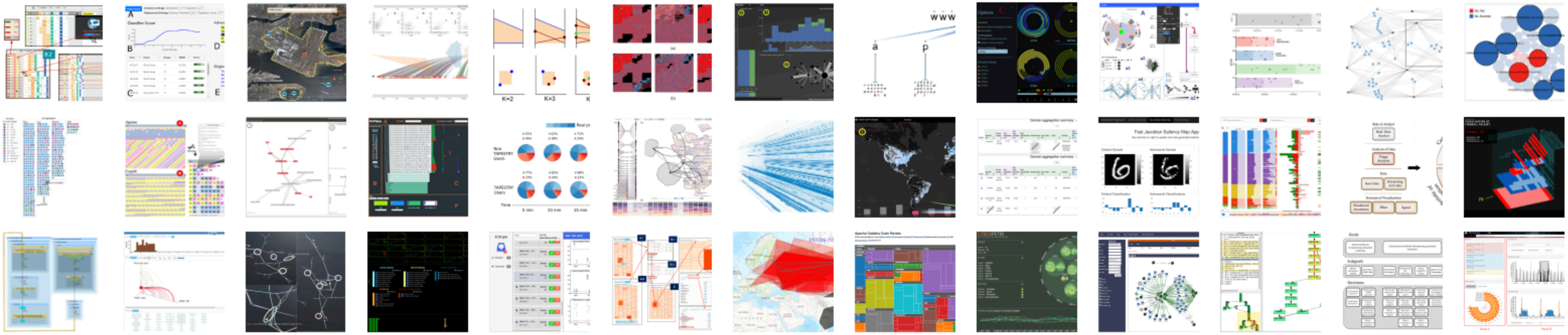
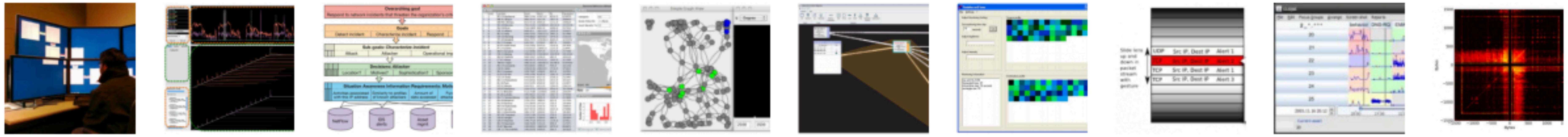


Visualizations for Cybersecurity

PA214 — Visualization II



Vít Rusňák

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

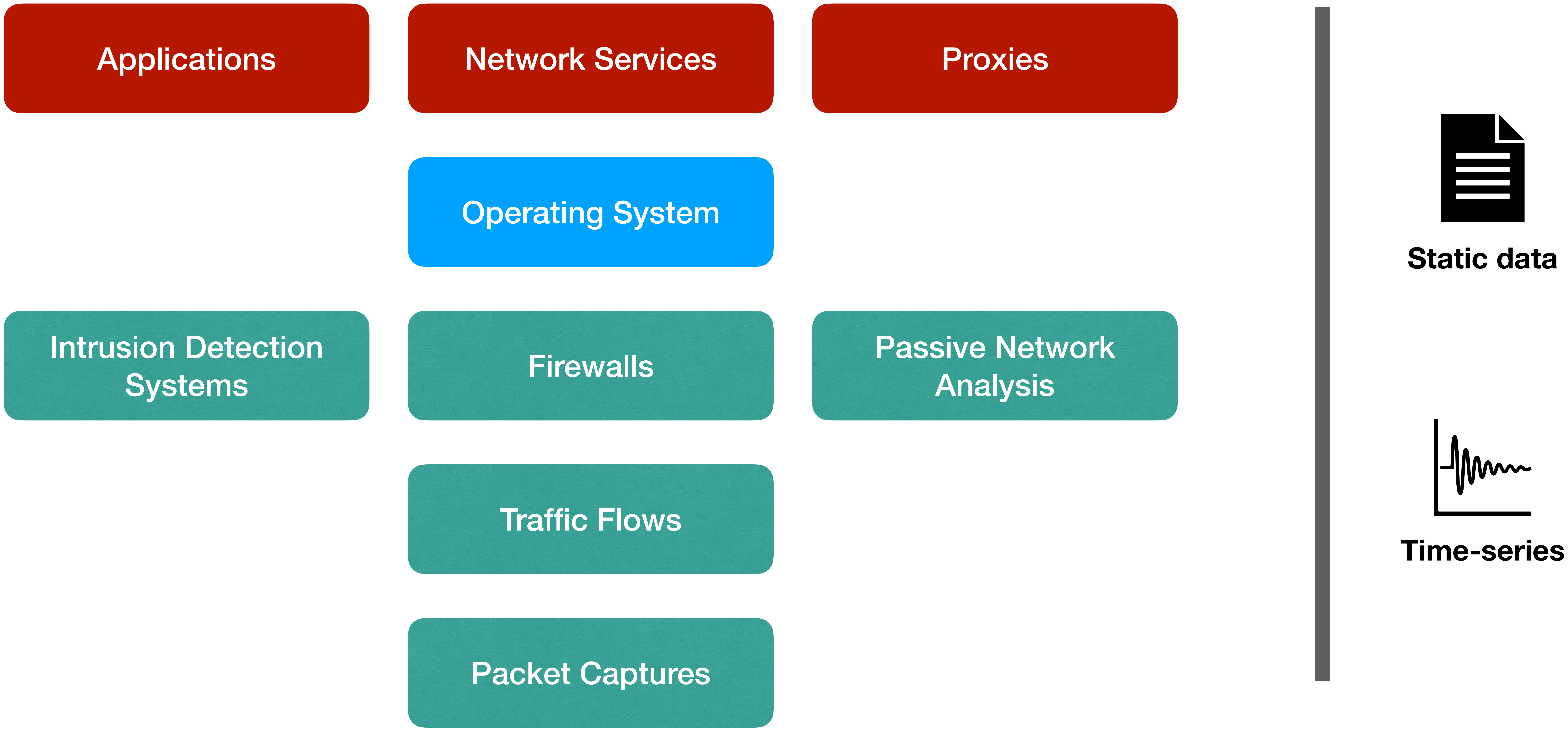
Management (both IT and non-IT background)

- 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

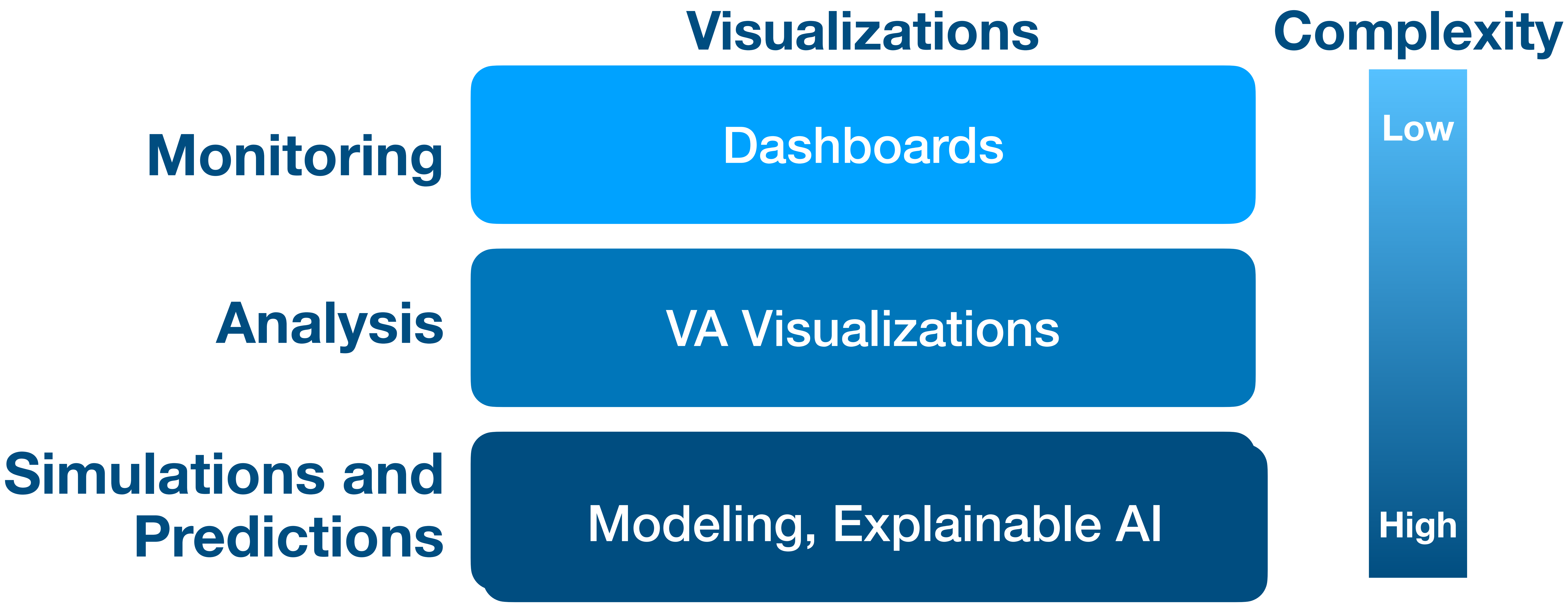
Packet Captures

Static data

Time-series

Adapted from [1]

Complexity of Visualizations



Visualizations

Complexity

Monitoring

Dashboards

Low

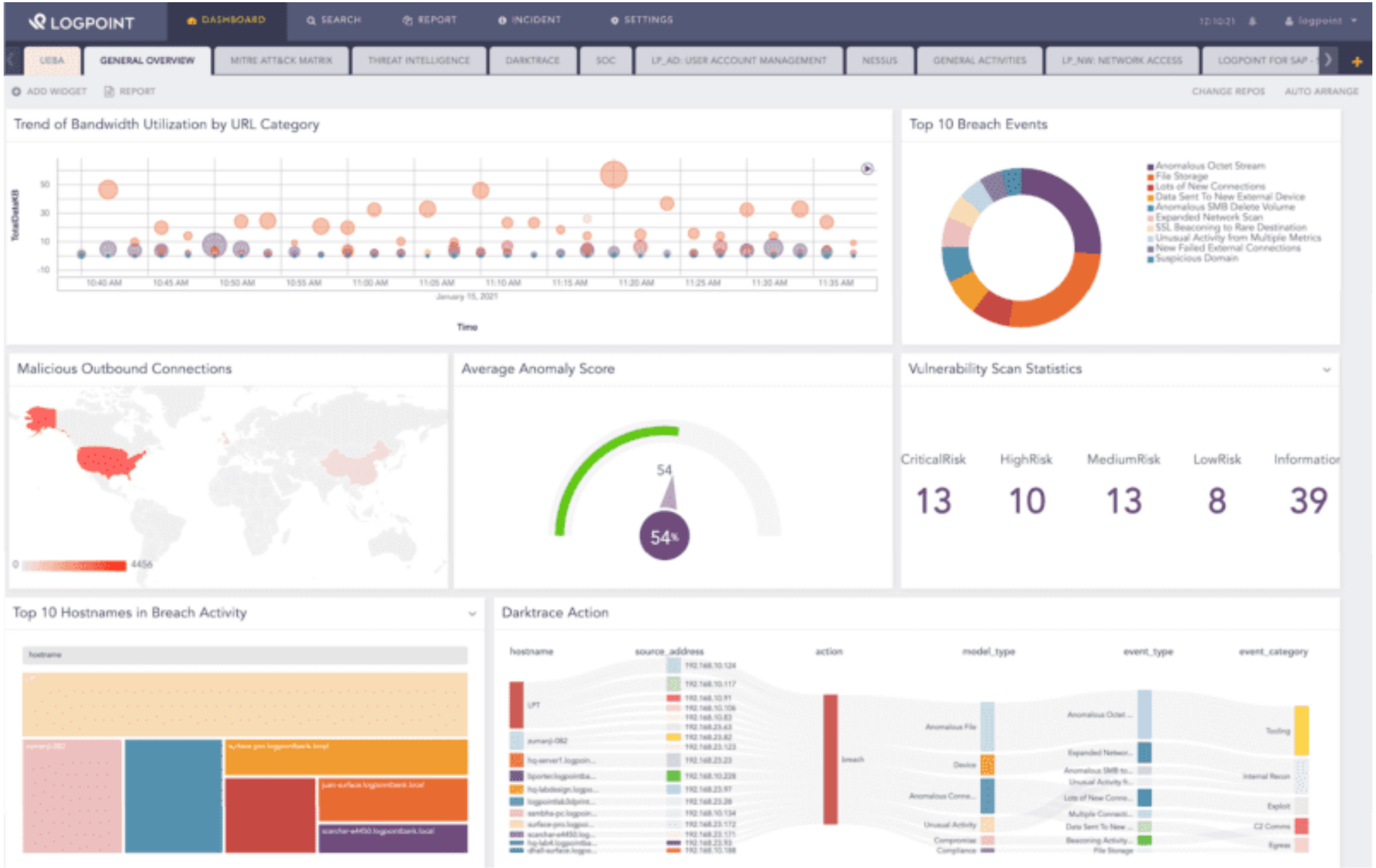
Analysis

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

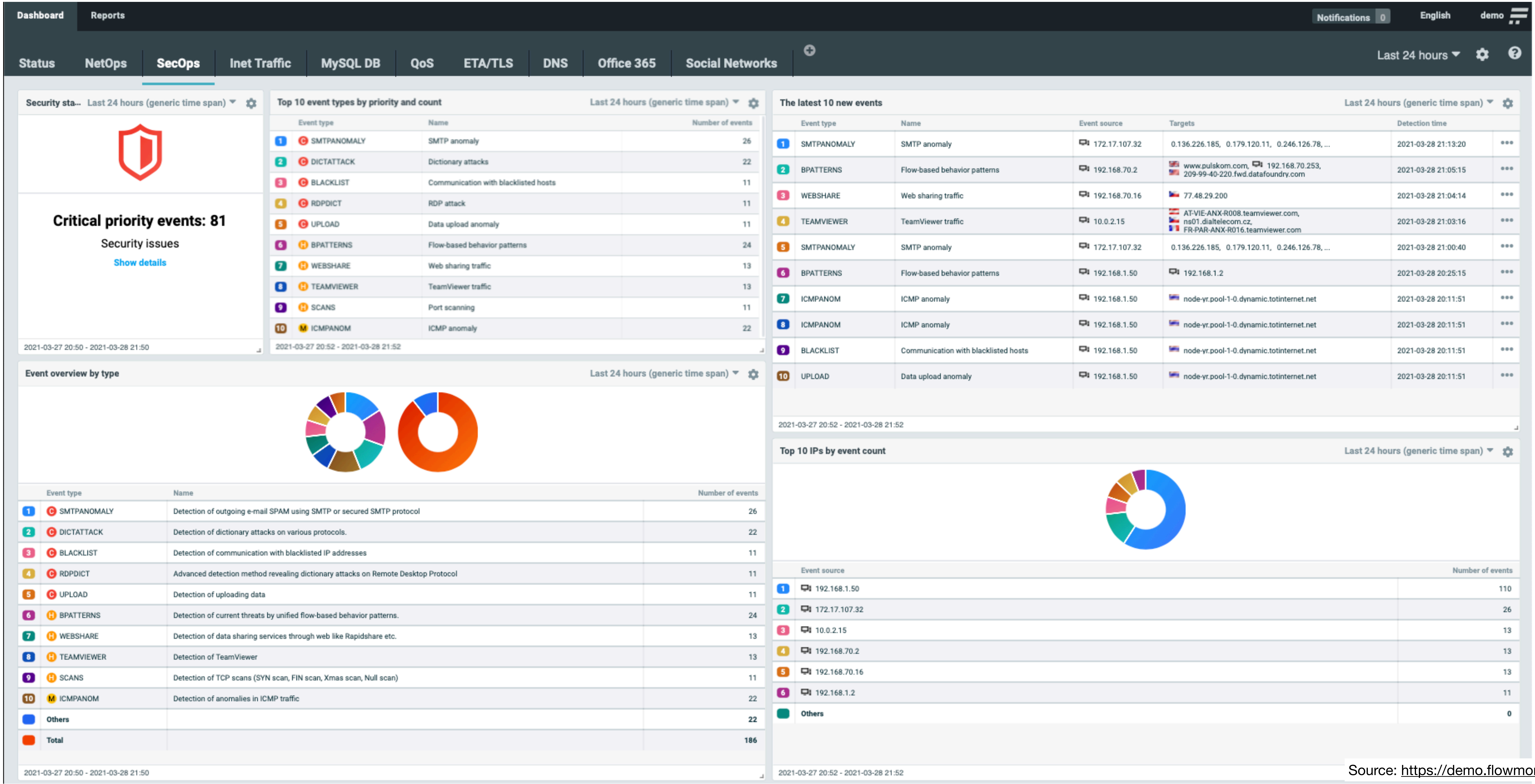
Provide

- 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



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

Critical priority events: 81

Security issues

Show details

2021-03-27 20:50 - 2021-03-28 21:50

Top 10 event types by priority and count Last 24 hours (generic time span)

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

2021-03-27 20:52 - 2021-03-28 21:52

The latest 10 new events Last 24 hours (generic time span)

	Event type	Name	Event source	Targets	Detection time
1	SMTPANOMALY	SMTP anomaly	172.17.107.32	0.136.226.185, 0.179.120.11, 0.246.126.78, ...	2021-03-28 21:13:20
2	BPATTERNS	Flow-based behavior patterns	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	Web sharing traffic	192.168.70.16	77.48.29.200	2021-03-28 21:04:14
4	TEAMVIEWER	TeamViewer traffic	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	SMTP anomaly	172.17.107.32	0.136.226.185, 0.179.120.11, 0.246.126.78, ...	2021-03-28 21:00:40
6	BPATTERNS	Flow-based behavior patterns	192.168.1.50	192.168.1.2	2021-03-28 20:25:15
7	ICMPANOM	ICMP anomaly	192.168.1.50	node-yr.pool-1-0.dynamic.totinternet.net	2021-03-28 20:11:51
8	ICMPANOM	ICMP anomaly	192.168.1.50	node-yr.pool-1-0.dynamic.totinternet.net	2021-03-28 20:11:51
9	BLACKLIST	Communication with blacklisted hosts	192.168.1.50	node-yr.pool-1-0.dynamic.totinternet.net	2021-03-28 20:11:51
10	UPLOAD	Data upload anomaly	192.168.1.50	node-yr.pool-1-0.dynamic.totinternet.net	2021-03-28 20:11:51

2021-03-27 20:52 - 2021-03-28 21:52

Event overview by type Last 24 hours (generic time span)

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

2021-03-27 20:50 - 2021-03-28 21:50

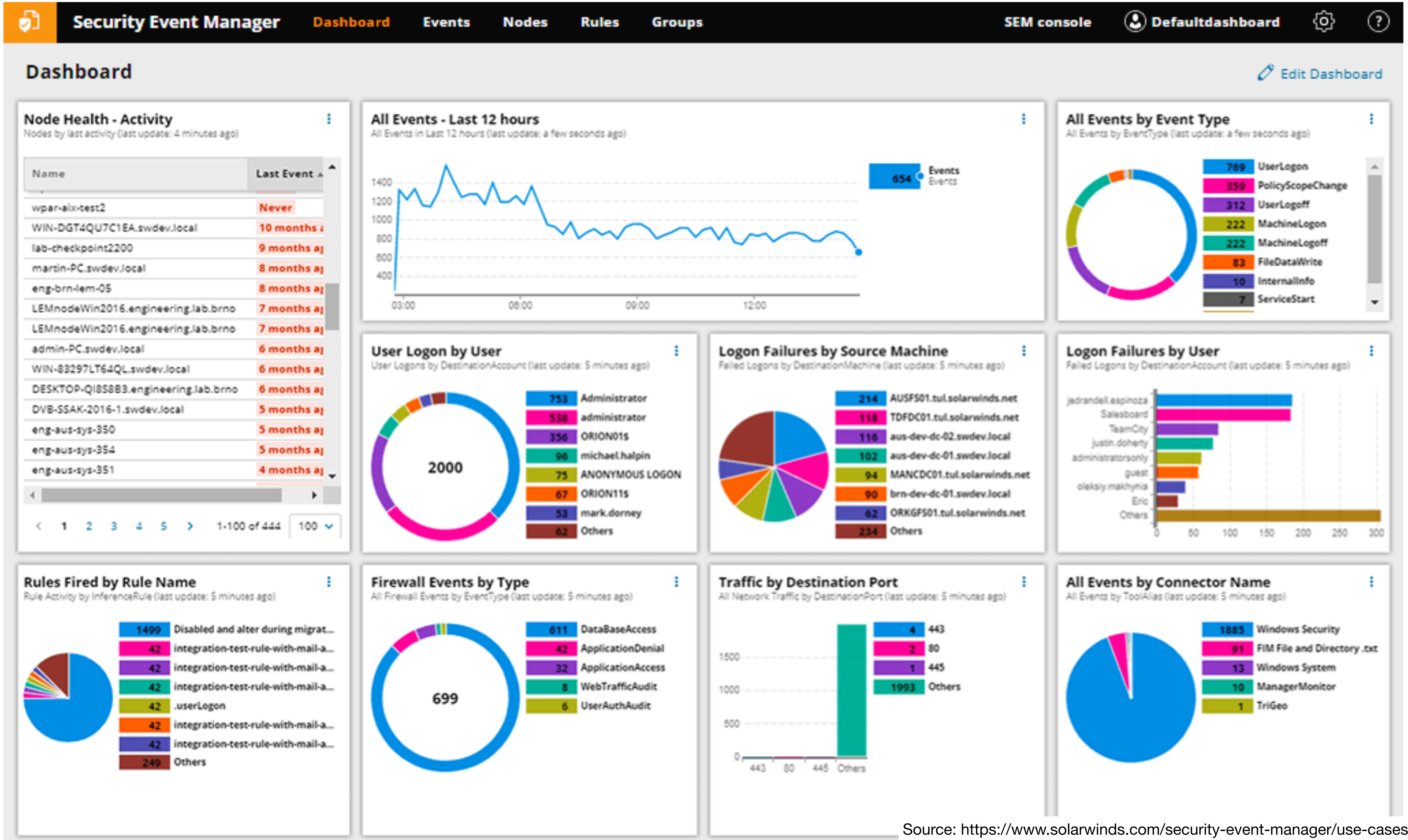
Top 10 IPs by event count Last 24 hours (generic time span)

	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

2021-03-27 20:52 - 2021-03-28 21:52

Source: https://demo.flowmon.com

Examples: Commercial Tools



Node Health - Activity

Nodes by last activity (last update: 4 minutes ago)

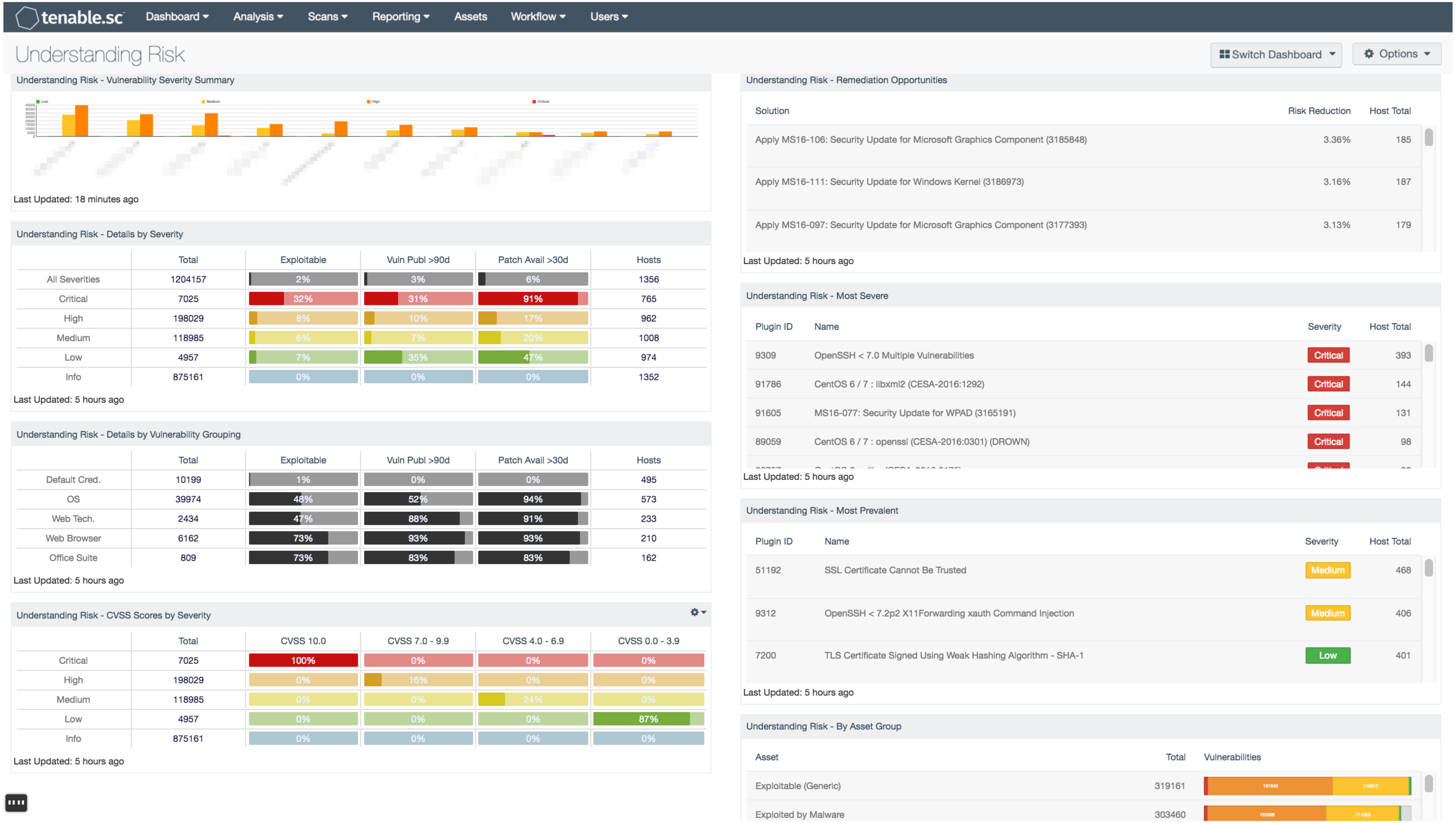
Name	Last Event
wpar-aix-test2	Never
WIN-DGT4QU7C1EA.swdev.local	10 months a
lab-checkpoint2200	9 months a
martin-PC.swdev.local	8 months a
eng-brn-lem-05	8 months a
LEMnodeWin2016.engineering.lab.brno	7 months a
LEMnodeWin2016.engineering.lab.brno	7 months a
admin-PC.swdev.local	6 months a
WIN-83297LT64QL.swdev.local	6 months a
DESKTOP-QI8S8B3.engineering.lab.brno	6 months a
DVB-SSAK-2016-1.swdev.local	5 months a
eng-aus-sys-350	5 months a
eng-aus-sys-354	5 months a
eng-aus-sys-351	4 months a

< 1 2 3 4 5 > 1-100 of 444 100

All Events - Last 12 hours
All Events in Last 12 hours (last update: a few seconds ago)
1400
1200
1000
800
600
400
03:00
06:00
09:00
12:00
654 Events
Events
All Events by Event Type
All Events by EventType (last update: a few seconds ago)
769 UserLogon
359 PolicyScopeChange
312 UserLogoff
222 MachineLogon
222 MachineLogoff
83 FileDataWrite
10 InternalInfo
7 ServiceStart
User Logon by User
User Logons by DestinationAccount (last update: 5 minutes ago)
2000
753 Administrator
538 administrator
356 ORION01$
96 michael.halpin
75 ANONYMOUS LOGON
67 ORION11$
53 mark.dorney
62 Others
Logon Failures by Source Machine
Failed Logons by DestinationMachine (last update: 5 minutes ago)
214 AUSFS01.tul.solarwinds.net
118 TDFDC01.tul.solarwinds.net
116 aus-dev-dc-02.swdev.local
102 aus-dev-dc-01.swdev.local
94 MANCDC01.tul.solarwinds.net
90 brn-dev-dc-01.swdev.local
62 ORKGFS01.tul.solarwinds.net
234 Others
Logon Failures by User
Failed Logons by DestinationAccount (last update: 5 minutes ago)
jedrandell.espinoza
Salesboard
TeamCity
justin.doherty
administratorsonly
guest
oleksiy.makhynia
Eric
Others
0
50
100
150
200
250
300
Rules Fired by Rule Name
Rule Activity by InferenceRule (last update: 5 minutes ago)
1499 Disabled and alter during migrat...
42 integration-test-rule-with-mail-a...
42 integration-test-rule-with-mail-a...
42 integration-test-rule-with-mail-a...
42 .userLogon
42 integration-test-rule-with-mail-a...
42 integration-test-rule-with-mail-a...
249 Others
Firewall Events by Type
All Firewall Events by EventType (last update: 5 minutes ago)
699
611 DataBaseAccess
42 ApplicationDenial
32 ApplicationAccess
8 WebTrafficAudit
6 UserAuthAudit
Traffic by Destination Port
All Network Traffic by DestinationPort (last update: 5 minutes ago)
1500
1000
500
0
443
80
445
Others
4 443
2 80
1 445
1993 Others
All Events by Connector Name
All Events by ToolAlias (last update: 5 minutes ago)
1885 Windows Security
91 FIM File and Directory .txt
13 Windows System
10 ManagerMonitor
1 TriGeo

Source: https://www.solarwinds.com/security-event-manager/use-cases/event-log-analyzer-tool

Examples: Commercial Tools



Understanding Risk

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

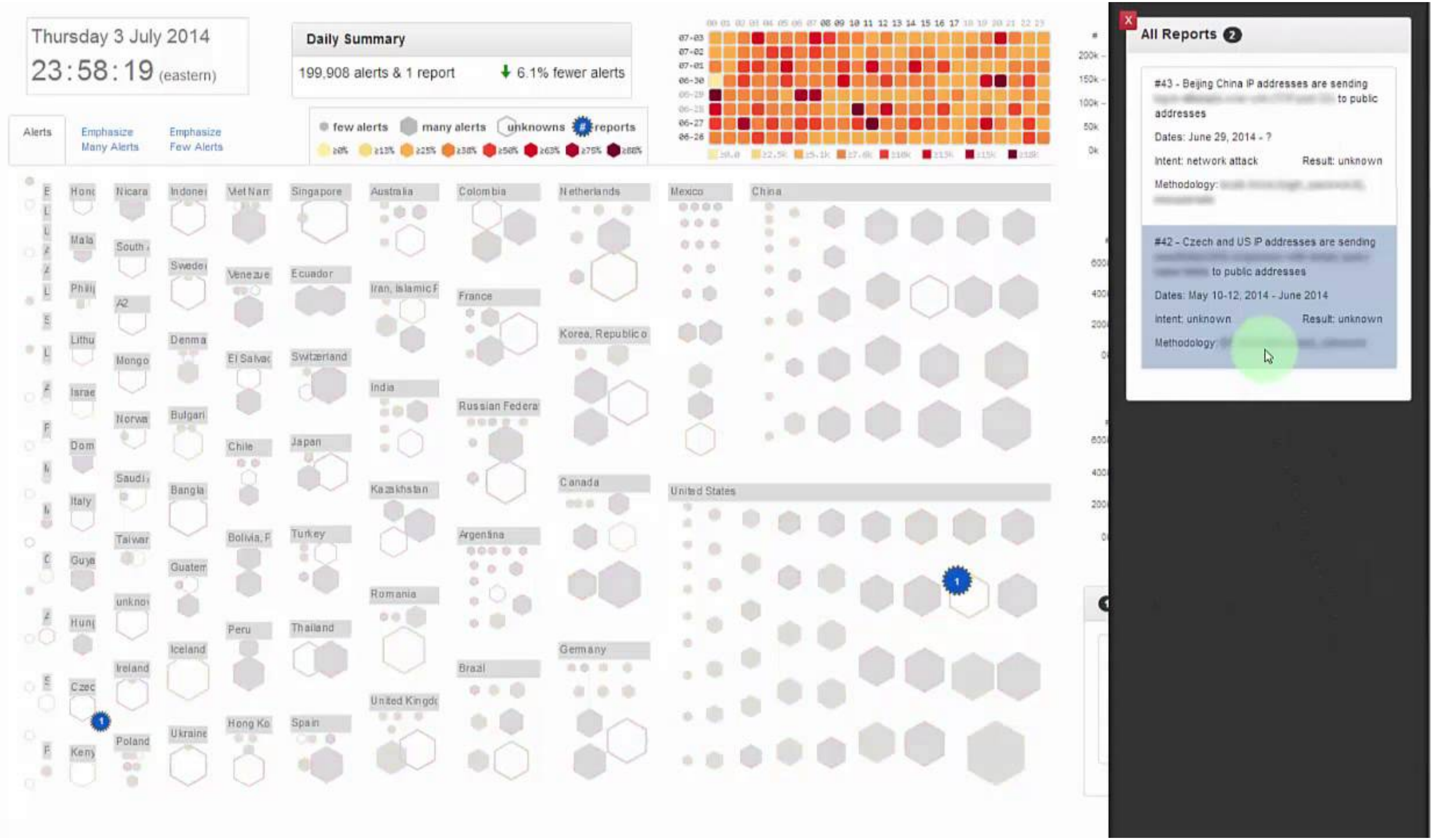
Last Updated: 5 hours ago

Understanding Risk - By Asset Group

Asset	Total	Vulnerabilities
Exploitable (Generic)	319161	191640 116612
Exploited by Malware	303460	182596 111359

Source: https://www.tenable.com/sc-dashboards/cyber-essentials-scheme-dashboard

Examples: Research



Thursday 3 July 2014

23:58:19 (eastern)

Daily Summary

199,908 alerts & 1 report ↓ 6.1% fewer alerts

All Reports 2

#43 - Beijing China IP addresses are sending [redacted] to public addresses

Dates: June 29, 2014 - ?

Intent: network attack Result: unknown

Methodology: [redacted]

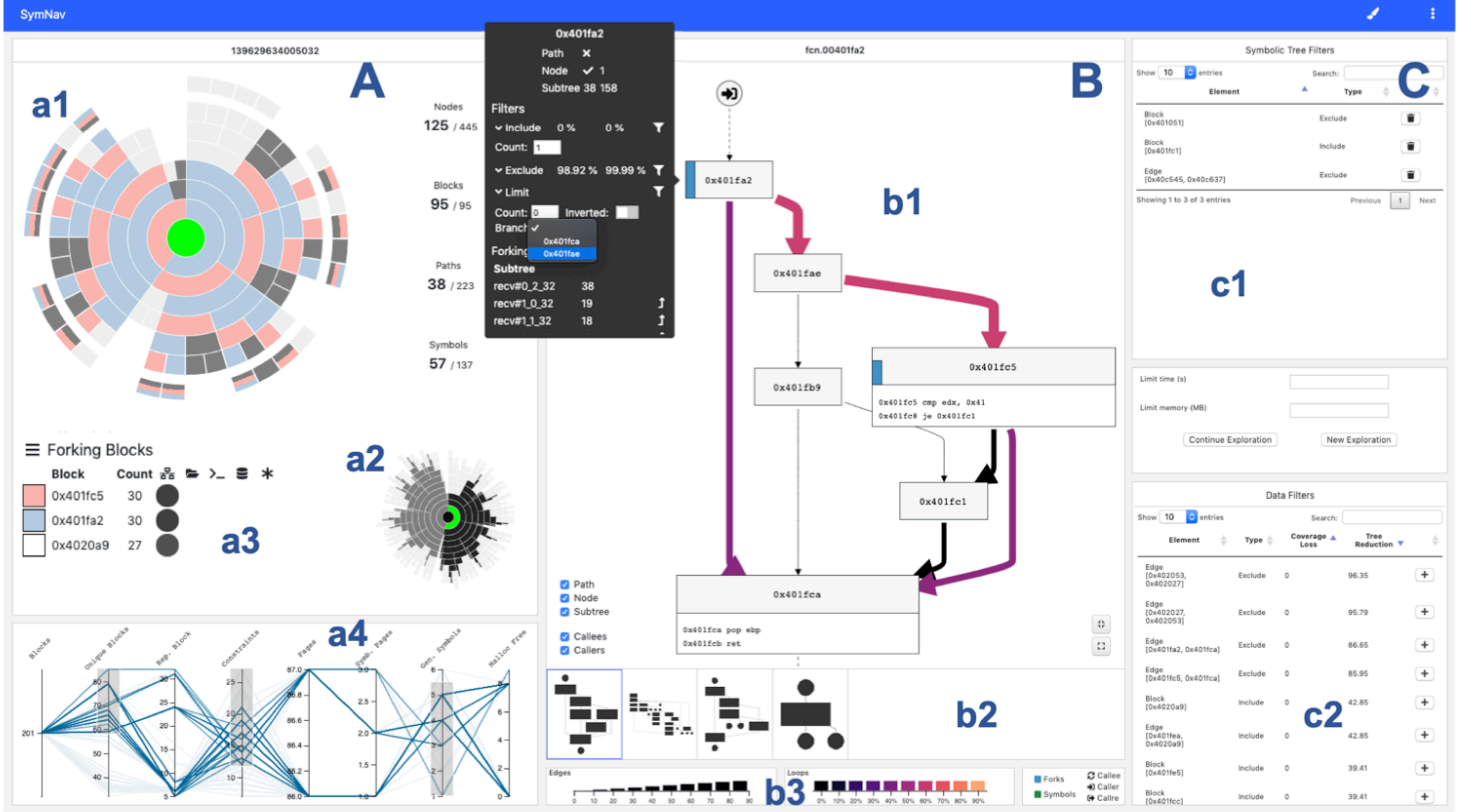
#42 - Czech and US IP addresses are sending [redacted] to public addresses

Dates: May 10-12, 2014 - June 2014

Intent: unknown Result: unknown

Methodology: [redacted]

Source [4], video from https://www.youtube.com/watch?v=7-RkJOdqHvI



0x401fa2

Path ✕
Node ✓ 1
Subtree 38 158

Filters
Include 0 % 0 %
Count: 1
Exclude 98.92 % 99.99 %
Limit
Count: 0 Inverted:
Branch ✓ 0x401fca 0x401fae
Forking
Subtree

recv#0_2_32	38
recv#1_0_32	19
recv#1_1_32	18

☰ Forking Blocks

	Block	Count
🟥	0x401fc5	30
🟦	0x401fa2	30
□	0x4020a9	27

```
0x401fc5 cmp edx, 0x41
0x401fc8 je 0x401fc1
```

```
0x401fca pop ebp
0x401fcb ret
```

☑ Path
☑ Node
☑ Subtree

☑ Callees
☑ Callers

Symbolic Tree Filters

Show 10 entries Search:

Element	Type	
Block [0x401051]	Exclude	🗑
Block [0x401fc1]	Include	🗑
Edge [0x40c545, 0x40c637]	Exclude	🗑

Showing 1 to 3 of 3 entries Previous 1 Next

Limit time (s)

Limit memory (MB)

Continue Exploration New Exploration

Data Filters

Show 10 entries Search:

Element	Type	Coverage Loss	Tree Reduction	
Edge [0x402053, 0x402027]	Exclude	0	96.35	+
Edge [0x402027, 0x402053]	Exclude	0	95.79	+
Edge [0x401fa2, 0x401fca]	Exclude	0	86.65	+
Edge [0x401fc5, 0x401fca]	Exclude	0	85.95	+
Block [0x4020a9]	Include	0	42.85	+
Edge [0x401fea, 0x4020a9]	Include	0	42.85	+
Block [0x401fe5]	Include	0	39.41	+
Block [0x401fcc]	Include	0	39.41	+

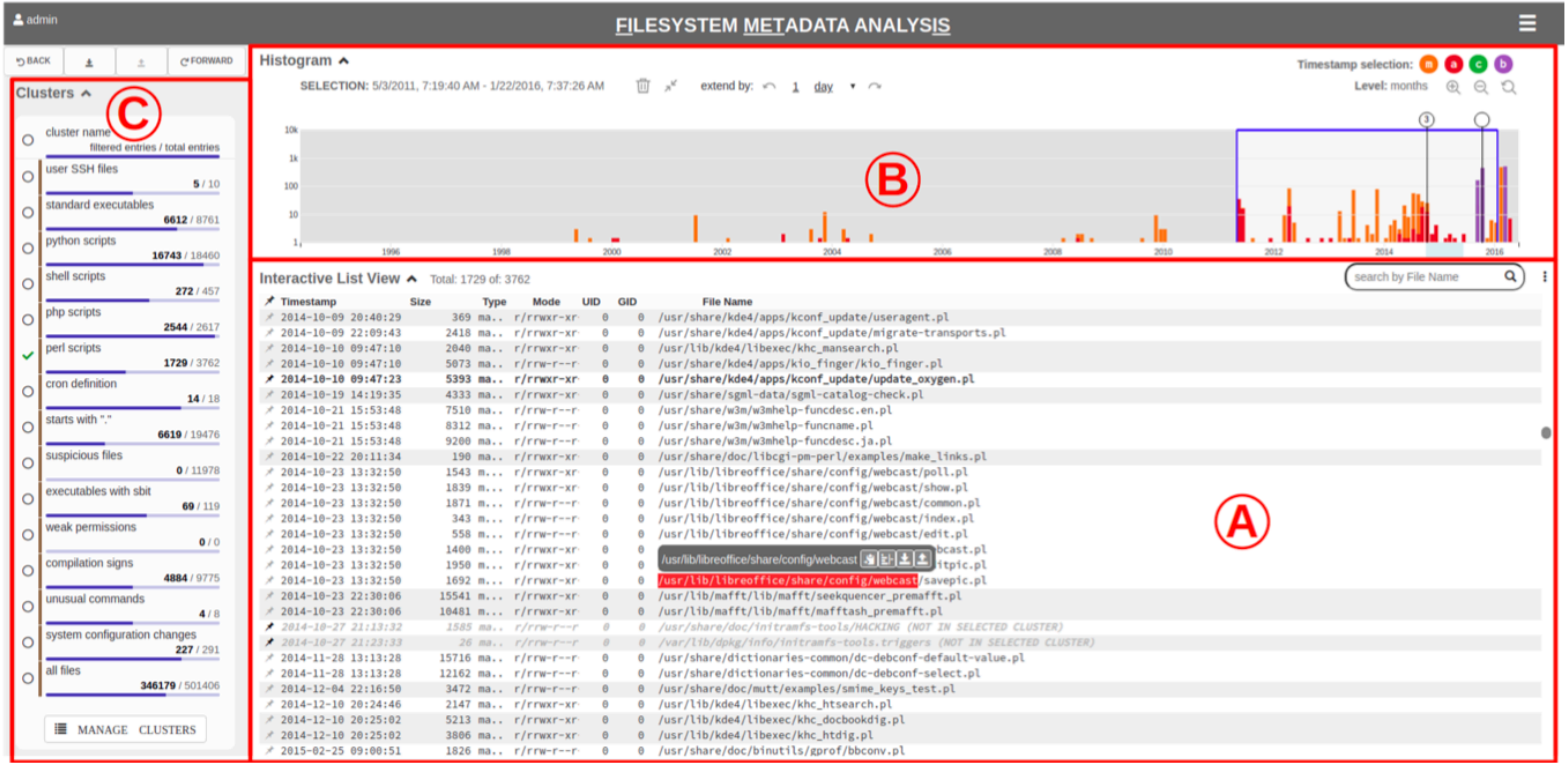
Analysis

Source: [5]

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 visualizations, but also novel visualizations
- Extend command line tools, 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



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

Clusters

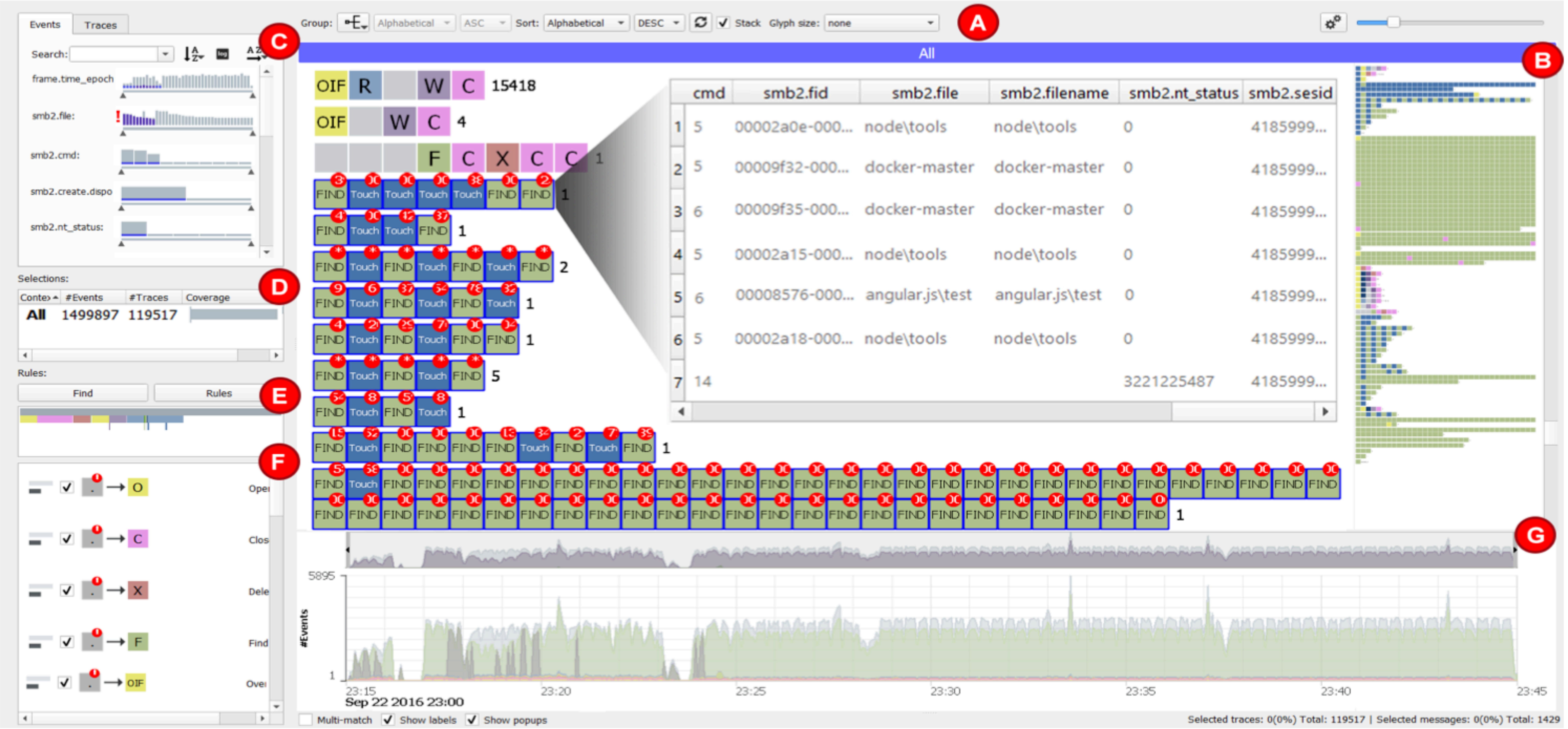
cluster name	filtered entries / total entries
○ user SSH files	**5** / 10
○ standard executables	**6612** / 8761
○ python scripts	**16743** / 18460
○ shell scripts	**272** / 457
○ php scripts	**2544** / 2617
✓ perl scripts	**1729** / 3762
○ cron definition	**14** / 18
○ starts with "."	**6619** / 19476
○ 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

Interactive List View Total: 1729 of: 3762

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-transports.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 bcast.pl
2014-10-23 13:32:50	1950	m...	r/rrwxr-xr	0	0	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

Source: [6]

Example: Malware Analysis



Group: Alphabetical ASC Sort: Alphabetical DESC ☑ Stack Glyph size: none

Selections:

Context	#Events	#Traces	Coverage
All	1499897	119517	

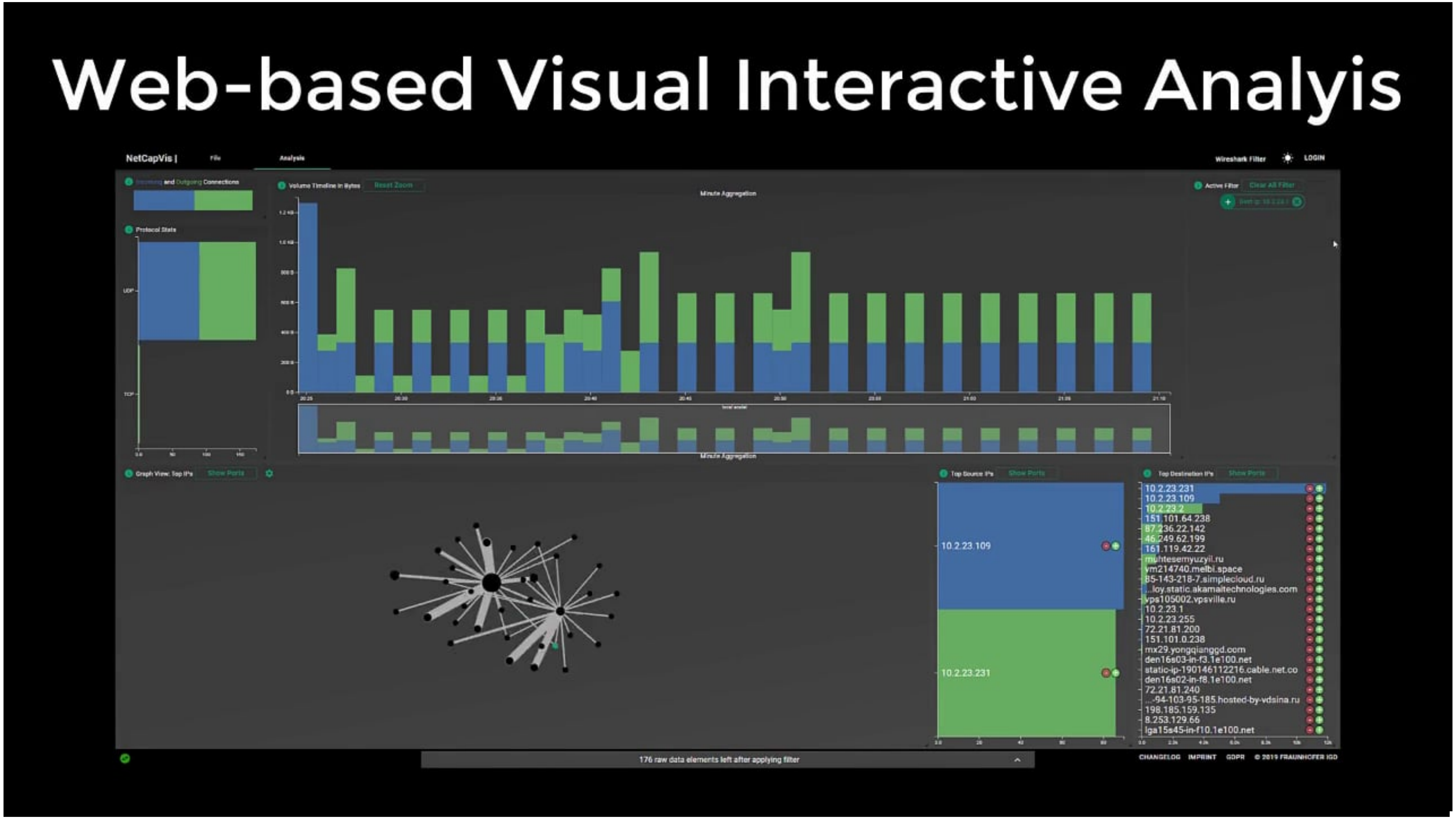
	cmd	smb2.fid	smb2.file	smb2.filename	smb2.nt_status	smb2.sesid
1	5	00002a0e-000...	node\tools	node\tools	0	4185999...
2	5	00009f32-000...	docker-master	docker-master	0	4185999...
3	6	00009f35-000...	docker-master	docker-master	0	4185999...
4	5	00002a15-000...	node\tools	node\tools	0	4185999...
5	6	00008576-000...	angular.js\test	angular.js\test	0	4185999...
6	5	00002a18-000...	node\tools	node\tools	0	4185999...
7	14				3221225487	4185999...

□ Multi-match ☑ Show labels ☑ Show popups

Selected traces: 0(0%) Total: 119517 | Selected messages: 0(0%) Total: 1429

Source: [7]

Example: Network Analysis

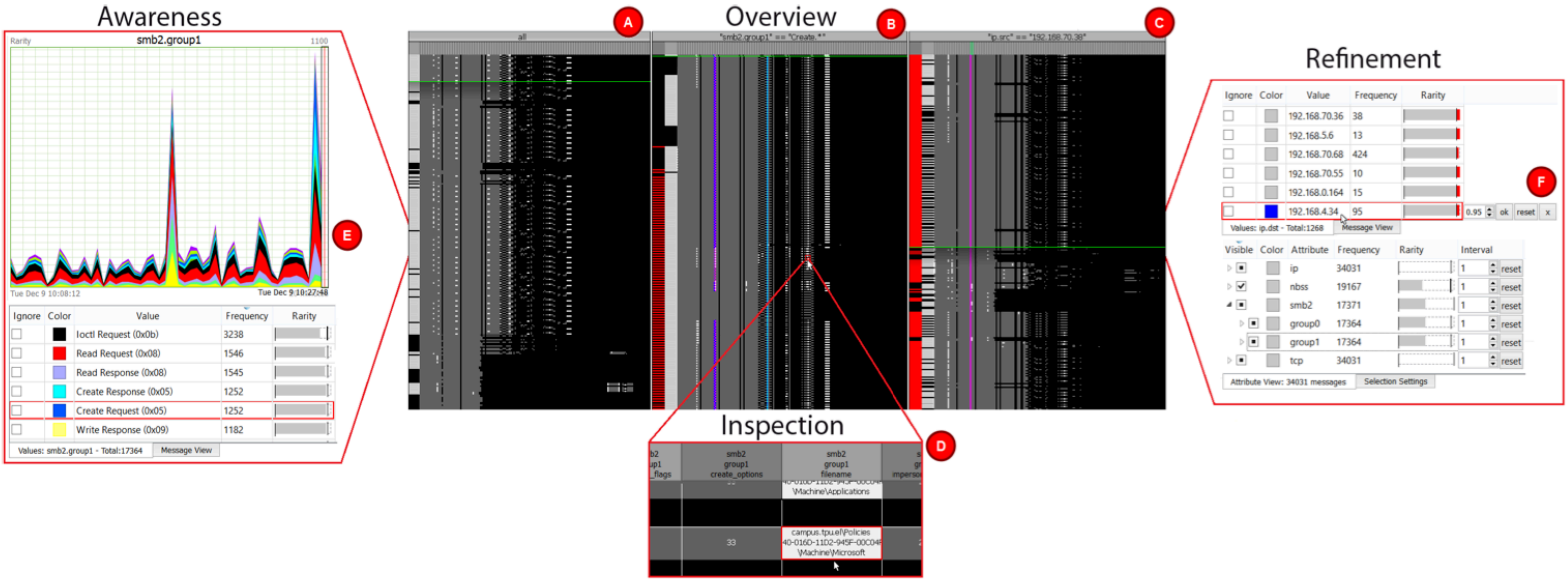


Web-based Visual Interactive Analyis

176 raw data elements left after applying filter

Source: [8]

Example: Traffic Analysis



Ignore	Color	Value	Frequency	Rarity
□	■	Ioctl Request (0x0b)	3238	
□	🟥	Read Request (0x08)	1546	
□	■	Read Response (0x08)	1545	
□	■	Create Response (0x05)	1252	
□	🟦	Create Request (0x05)	1252	
□	🟨	Write Response (0x09)	1182	

Values: smb2.group1 - Total:17364 | Message View

b2 up1 _flags	smb2 group1 create_options	smb2 group1 filename	s gr imperso
		40-016D-11D2-945F-00C04F \Machine\Applications	
	33	campus.tpu.el\Policies 40-016D-11D2-945F-00C04F \Machine\Microsoft	

Ignore	Color	Value	Frequency	Rarity
□	■	192.168.70.36	38	
□	■	192.168.5.6	13	
□	■	192.168.70.68	424	
□	■	192.168.70.55	10	
□	■	192.168.0.164	15	
□	🟦	192.168.4.34	95	

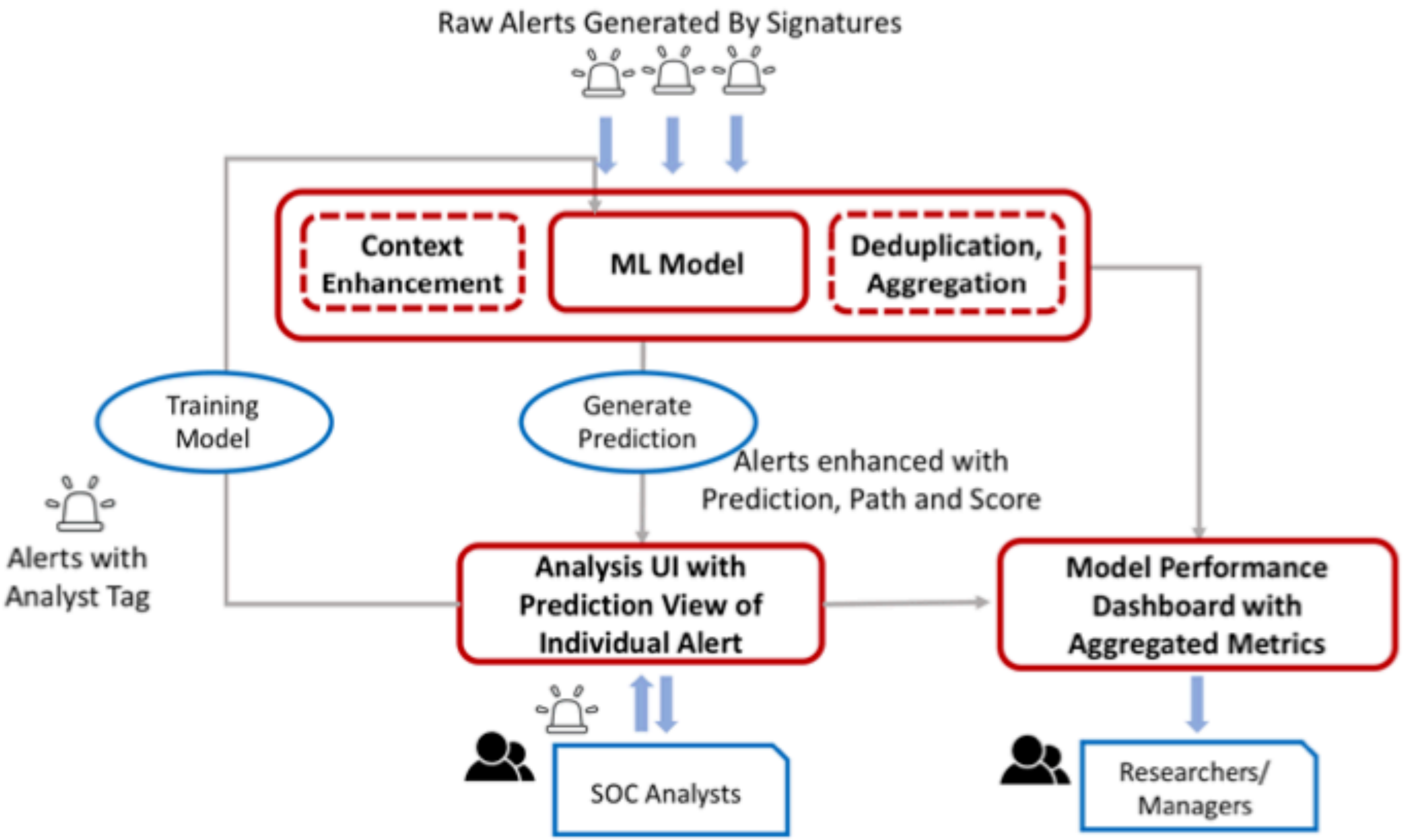
0.95 | ok | reset | x

Values: ip.dst - Total:1268 | Message View

Visible	Color	Attribute	Frequency	Rarity	Interval
▷ ■	■	ip	34031		1 reset
▷ ☑	■	nbss	19167		1 reset
◢ ■	■	smb2	17371		1 reset
▷ ■	■	group0	17364		1 reset
▷ ■	■	group1	17364		1 reset
▷ ■	■	tcp	34031		1 reset

Attribute View: 34031 messages | Selection Settings

Source: [10]


Raw Alerts Generated By Signatures
Context Enhancement
ML Model
Deduplication, Aggregation
Training Model
Generate Prediction
Alerts enhanced with Prediction, Path and Score
Alerts with Analyst Tag
Analysis UI with Prediction View of Individual Alert
Model Performance Dashboard with Aggregated Metrics
SOC Analysts
Researchers/ Managers

Predictions and Simulations

Source: [9]

Characteristics

- Visual support for understanding **ML/AI** techniques, visualizations for **eXplainable AI**

- **Goal(s):** early warning, understanding ML/AI techniques, explain their behavior, gain trust in them

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

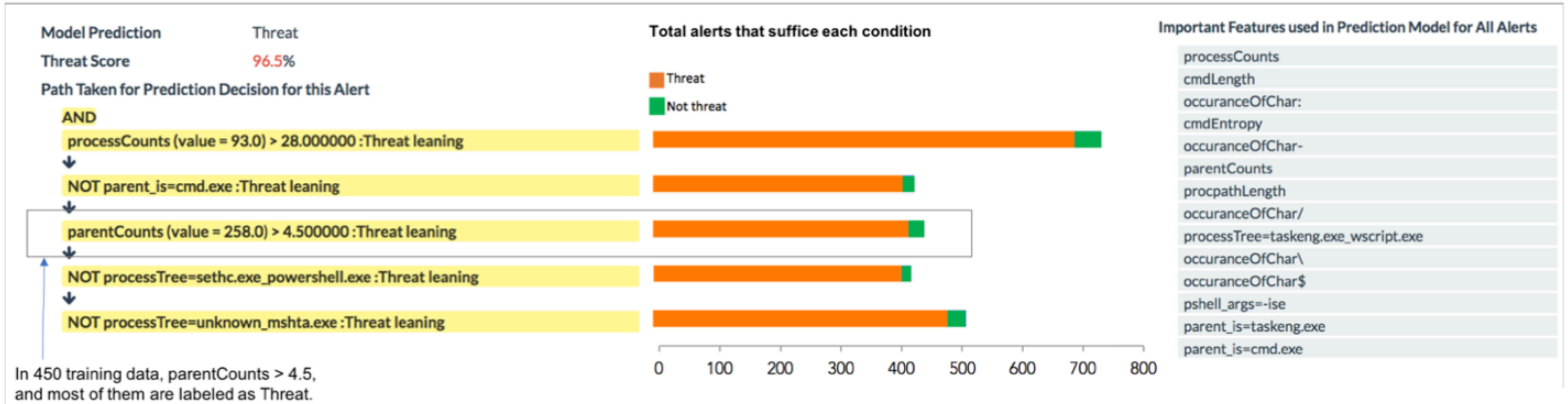
- Rise on popularity correlates with growing application of ML/AI in cybersecurity

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 humans authorization.

Example: Alert Predictions



Model Prediction Threat

Threat Score 96.5%

Path Taken for Prediction Decision for this Alert

AND

processCounts (value = 93.0) > 28.000000 :Threat leaning

NOT parent_is=cmd.exe :Threat leaning

parentCounts (value = 258.0) > 4.500000 :Threat leaning

NOT processTree=sethc.exe_powershell.exe :Threat leaning

NOT processTree=unknown_mshta.exe :Threat leaning

Total alerts that suffice each condition

Threat

Not threat

Important Features used in Prediction Model for All Alerts

processCounts
cmdLength
occuranceOfChar:
cmdEntropy
occuranceOfChar-
parentCounts
procpathLength
occuranceOfChar/
processTree=taskeng.exe_wscript.exe
occuranceOfChar\
occuranceOfChar$
pshell_args=-ise
parent_is=taskeng.exe
parent_is=cmd.exe

In 450 training data, parentCounts > 4.5,
and most of them are labeled as Threat.
In our current data the feature parentCount = 258,
which makes it more likely to be a Threat.

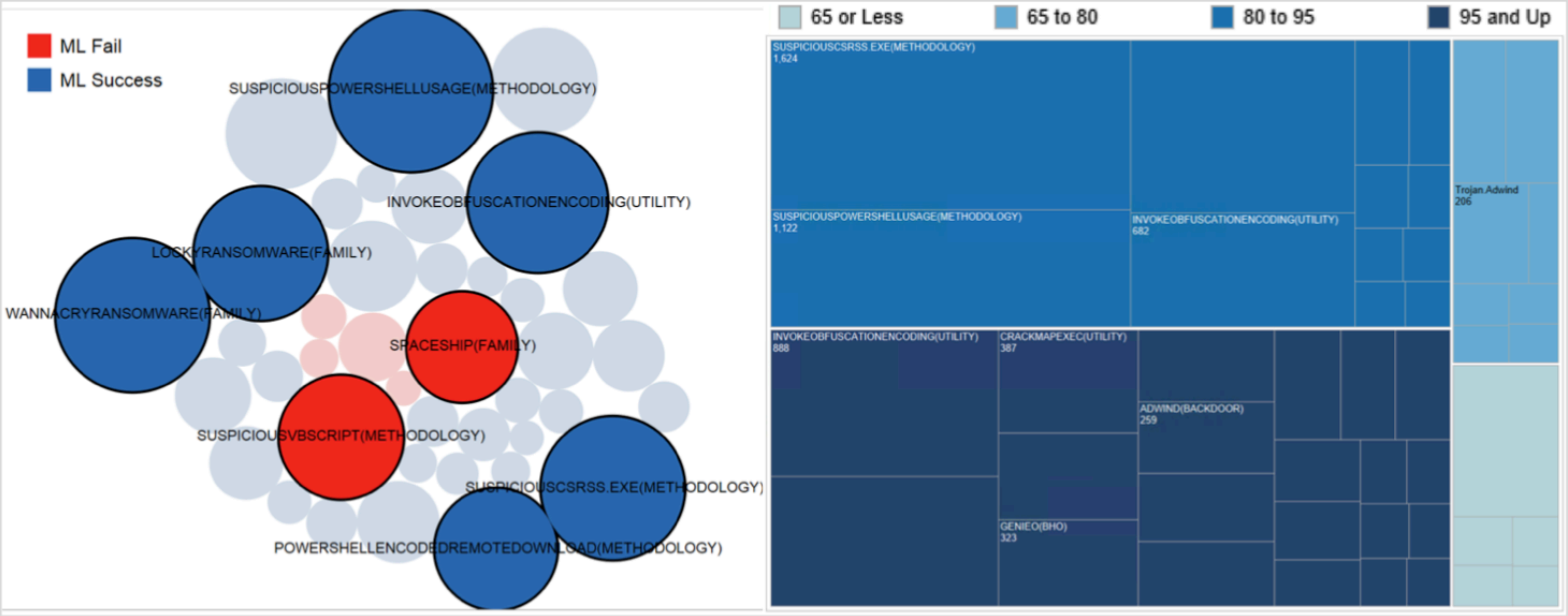
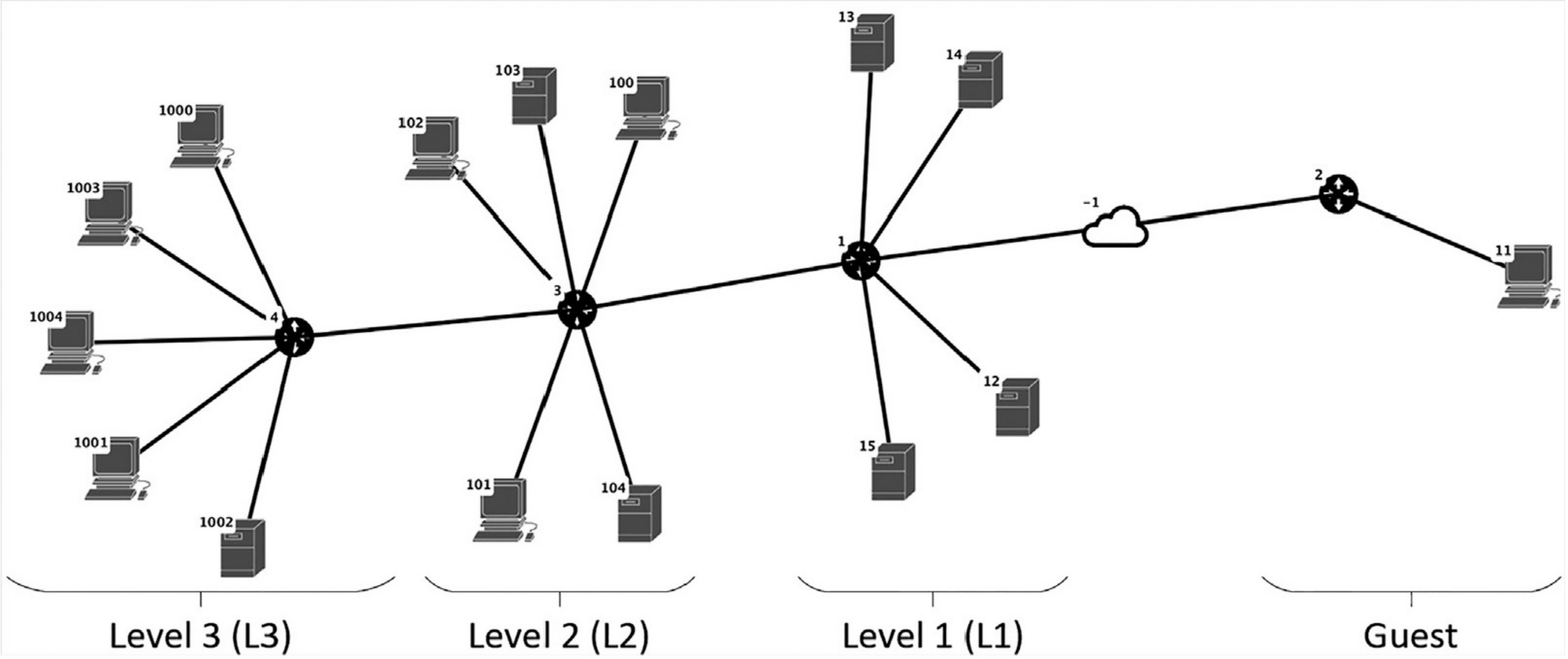


Figure 7: Left: Circle pack visualization showing alerts by signatures. Each circle represents alerts from a particular signature. Circles are sized by the total alerts of that signature and color coded by the ML Model success of ML failure. Right: A Treemap visualization showing only alerts that are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

Source: [9]

Simulations

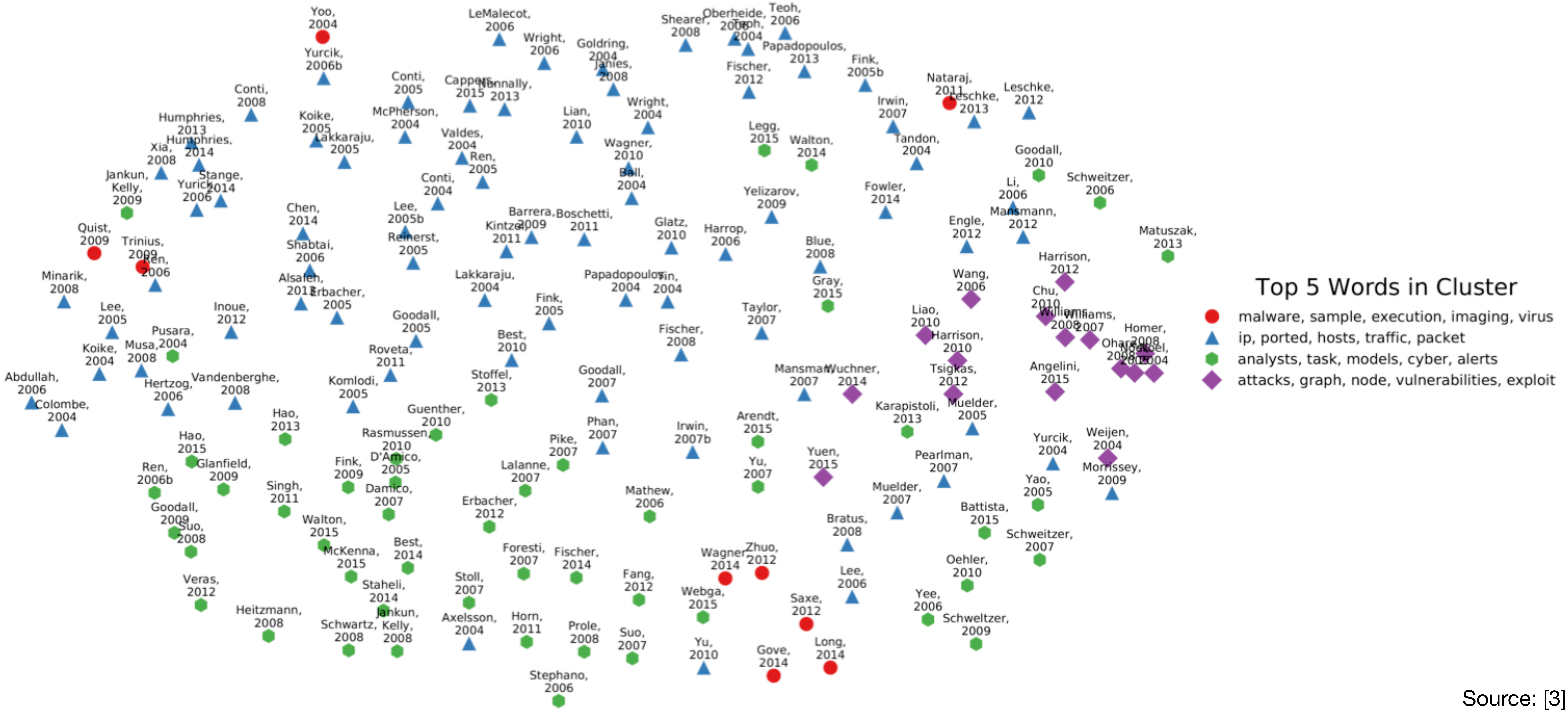
- Largely unexplored
- Areas:
  - Attack surface and attack vectors
  - Scenario modelling tool
  - Autonomous agents (attackres) behavior
  - Comparison and explanation of their decisions



Source: [11]

CyberSecVis Research

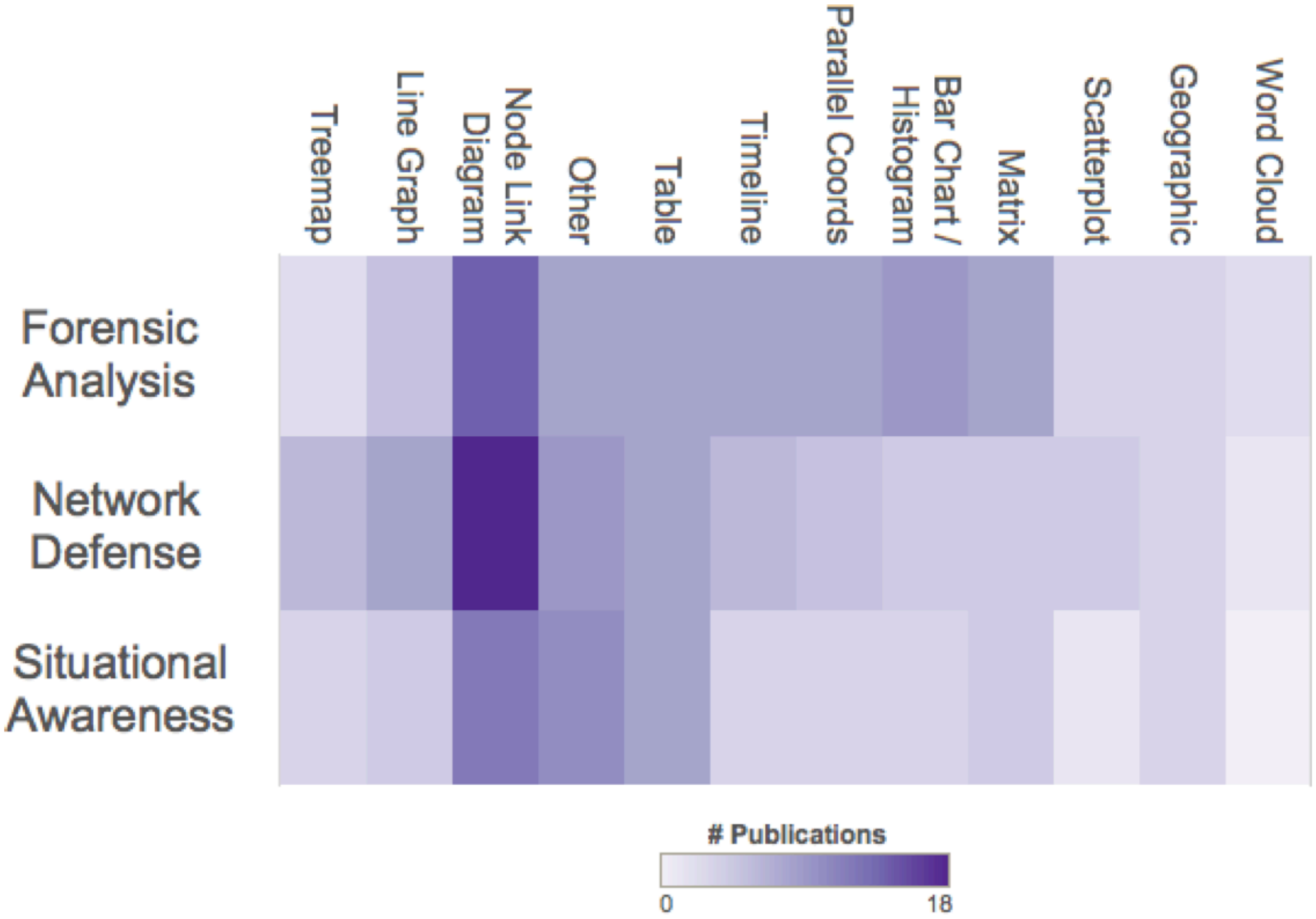
VizSec papers 2004—2015



Source: [3]

Utilization of Visualizations

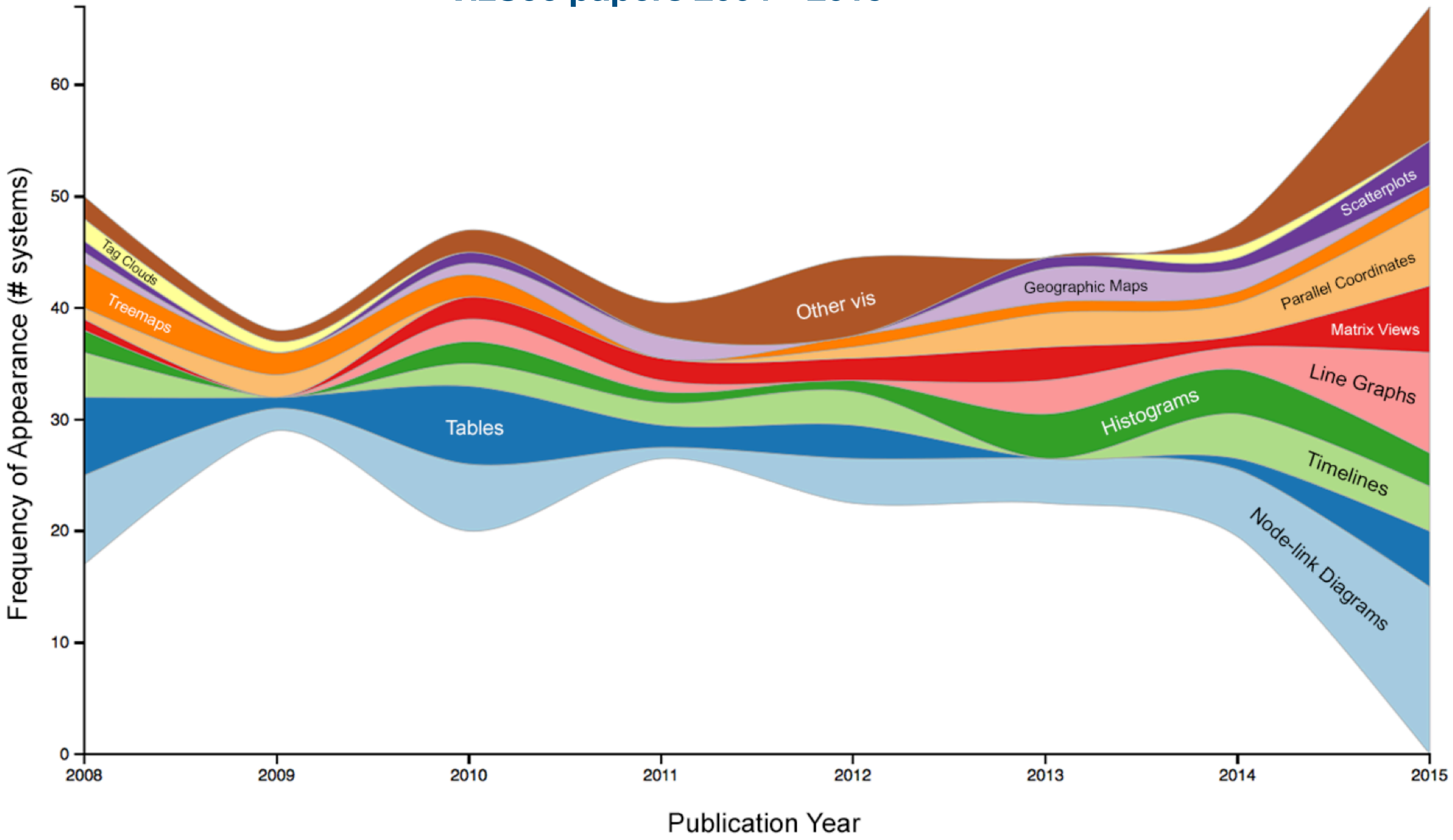
VizSec papers 2004—2015



Source: [3]

Utilization of Visual Metaphors

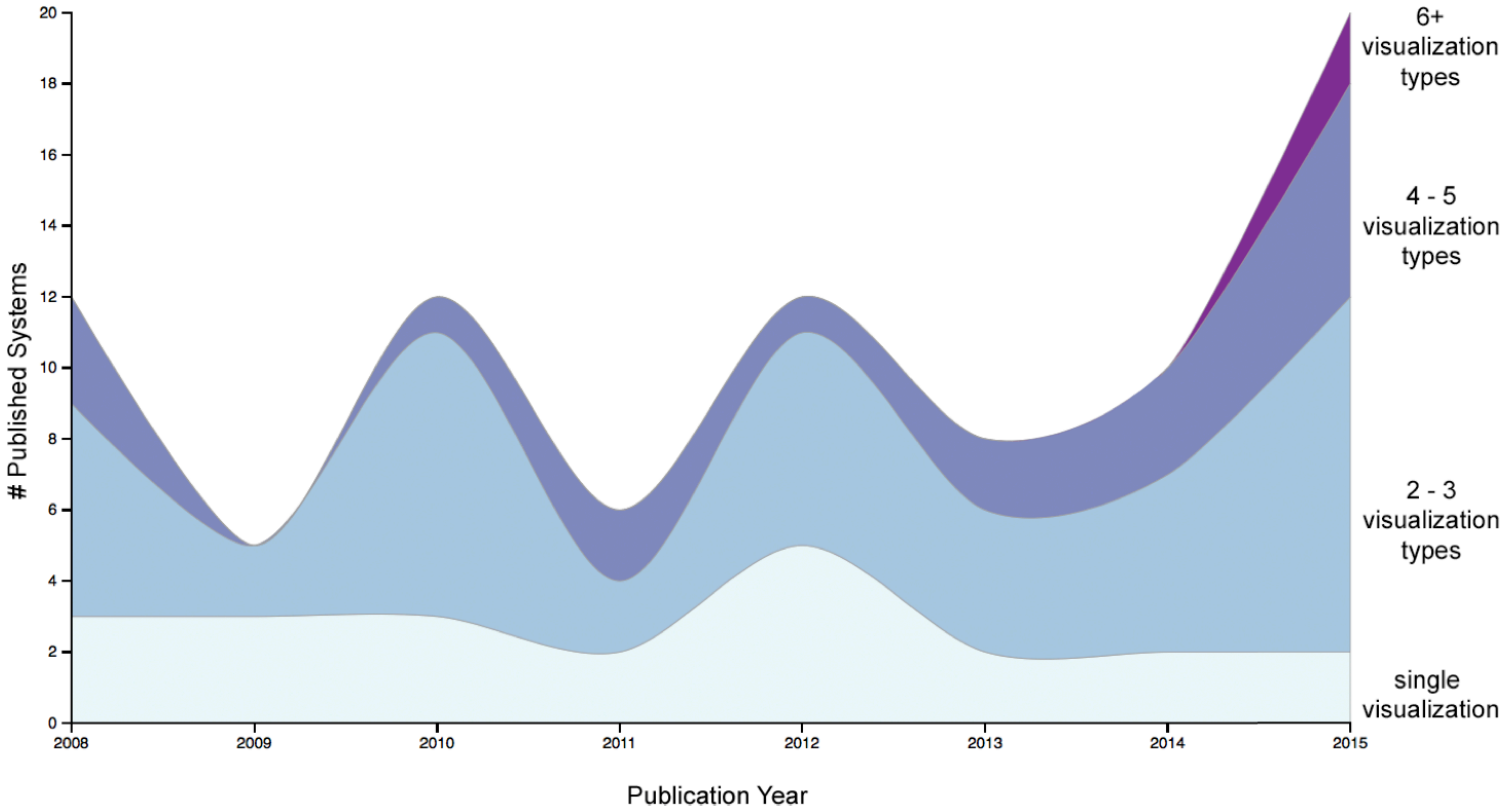
VizSec papers 2004—2015



Source: [3]

Interface Complexity

VizSec papers 2004—2015



Source: [3]

Take-aways

- Cybersecurity visualizations (as any 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

- Research prototypes

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