Technische Universität Berlin

Master Thesis Survey - Winter 2020

## Standard Frageblock

This survey is part of the Master Thesis "Interactive Network Visualization for Intrusion Detection" by David Krüger at the DAI Labor at the TU Berlin. The survey is about visualization techniques for Intrusion Detection and focuses on opinions and ratings of computer science students who are familiar with the basics of cyber security and Intrusion Detection.

**Note:**
Please proceed only if your are familiar with the term of Intrusion Detection in Cyber Security. The field of Intrusion Detection deals with the challenge of detecting, logging and analyzing attacks in networks (e.g. Trojan or Worm) or on local machines (e.g. Virus or Spyware). The thesis and this survey focuses on network-based Intrusion Detection but requires no special knowledge.

The survey will take about 10 minutes.

**Thanks for participating in this survey!**

## Visualization Genral

**Visualizations in general**
The following questions deal with visualizations in general. Please keep this in mind.

Please consider visualizations **in general**.
Prioritize (drag&drop) the following characteristics of visualizations according to your opinion. Which characteristics or features are less important than others.

Interactive features to filter or search the data

Expert functions like correlations for deep analysis

Build upon state-of-the-art technology

Simple design and easy to use

Detailed data inspection

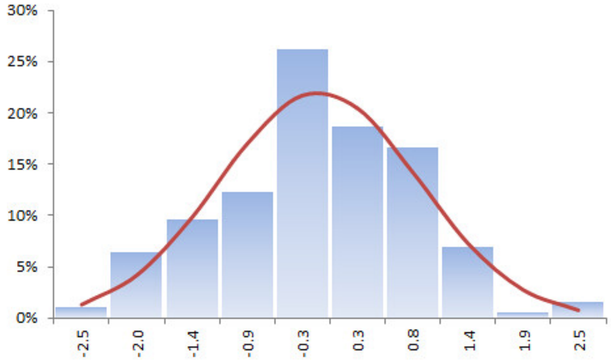
Using of coloring and proportions to highlight only the most important properties of the data

Global overview over the data with one look

# Which types of visualizations are you familiar with? (Already seen or worked with)

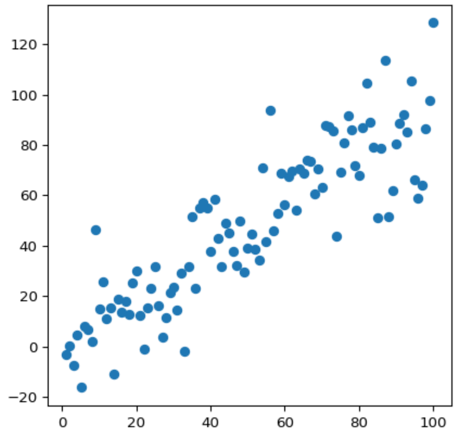
## Histogram

□



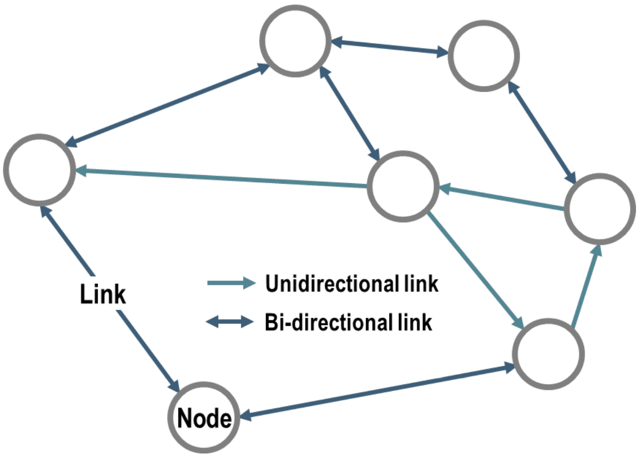
## Scatter plots

□



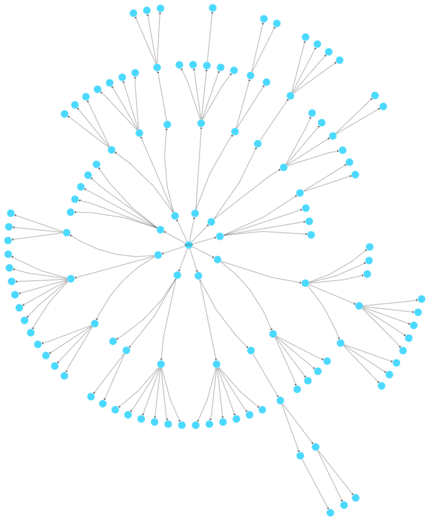
## Node-link/Network diagrams

□



## Radial graphs/diagrams

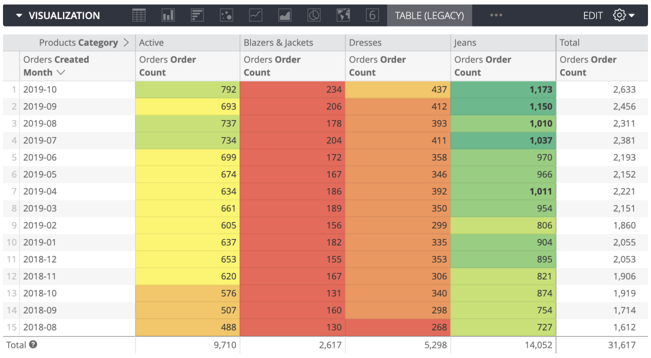
□



□

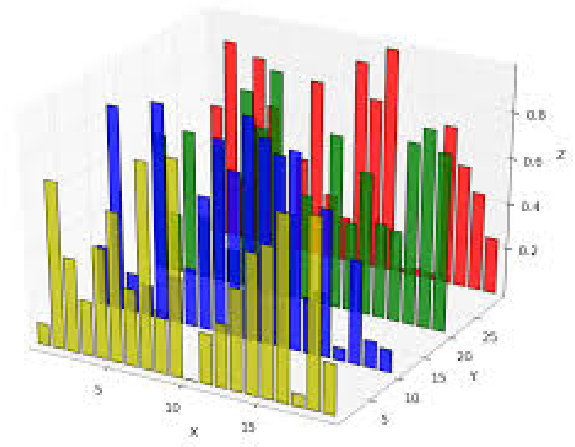
## Advanced tabular form

□



| | Products **Category** > | Active | Blazers & Jackets | Dresses | Jeans | Total |
|---|---|---|---|---|---|---|
| | Orders **Created Month** | Orders **Order Count** | Orders **Order Count** | Orders **Order Count** | Orders **Order Count** | Orders **Order Count** |
| 1 | 2019-10 | 792 | 234 | 437 | **1,173** | 2,633 |
| 2 | 2019-09 | 693 | 206 | 412 | **1,150** | 2,456 |
| 3 | 2019-08 | 737 | 178 | 393 | **1,010** | 2,311 |
| 4 | 2019-07 | 734 | 204 | 411 | **1,037** | 2,381 |
| 5 | 2019-06 | 699 | 172 | 358 | 970 | 2,193 |
| 6 | 2019-05 | 674 | 167 | 346 | 966 | 2,152 |
| 7 | 2019-04 | 634 | 186 | 392 | **1,011** | 2,221 |
| 8 | 2019-03 | 661 | 189 | 350 | 954 | 2,151 |
| 9 | 2019-02 | 605 | 156 | 299 | 806 | 1,860 |
| 10 | 2019-01 | 637 | 182 | 335 | 904 | 2,055 |
| 11 | 2018-12 | 653 | 155 | 353 | 895 | 2,053 |
| 12 | 2018-11 | 620 | 167 | 306 | 821 | 1,906 |
| 13 | 2018-10 | 576 | 131 | 340 | 874 | 1,919 |
| 14 | 2018-09 | 507 | 160 | 298 | 754 | 1,714 |
| 15 | 2018-08 | 488 | 130 | 268 | 727 | 1,612 |
| Total | | 9,710 | 2,617 | 5,298 | 14,052 | 31,617 |

### 3-D diagrams



## Visualization Intrusion Detection

**Visualizations for Intrusion Detection**
The following questions deal with visualizations specifically for Intrusion Detection. Please keep this in mind.
Visualization for Intrusion Detection basically deals with the visualization of (large) datasets of network events or intrusion alerts generated by Intrusion Detection Systems.

Please consider visualizations **for Intrusion Detection**. Please rate the listed characteristics on the following scale according to their importance.

| | 1<br>(not important) | 2 | 3 | 4 | 5<br>(very important) |
|---|---|---|---|---|---|

| | 1<br>(not important) | 2 | 3 | 4 | 5<br>(very important) |
|---|---|---|---|---|---|
| Design & Usability | | | | | |
| Global overview with one look | ○ | ○ | ○ | ○ | ○ |
| Easy to use / self-explanatory control | ○ | ○ | ○ | ○ | ○ |
| Using of coloring and proportions to highlight only the most important aspects of the data | ○ | ○ | ○ | ○ | ○ |
| Features | | | | | |
| Detailed data inspection | ○ | ○ | ○ | ○ | ○ |
| Expert functions like correlations for deep analysis | ○ | ○ | ○ | ○ | ○ |
| Flexibility in terms of integration and multiple data sources | ○ | ○ | ○ | ○ | ○ |
| Real-time connection (life data analysis) | ○ | ○ | ○ | ○ | ○ |
| Advanced | | | | | |
| Scalability to process large datasets in short time | ○ | ○ | ○ | ○ | ○ |
| Build upon state-of-the-art technology | ○ | ○ | ○ | ○ | ○ |

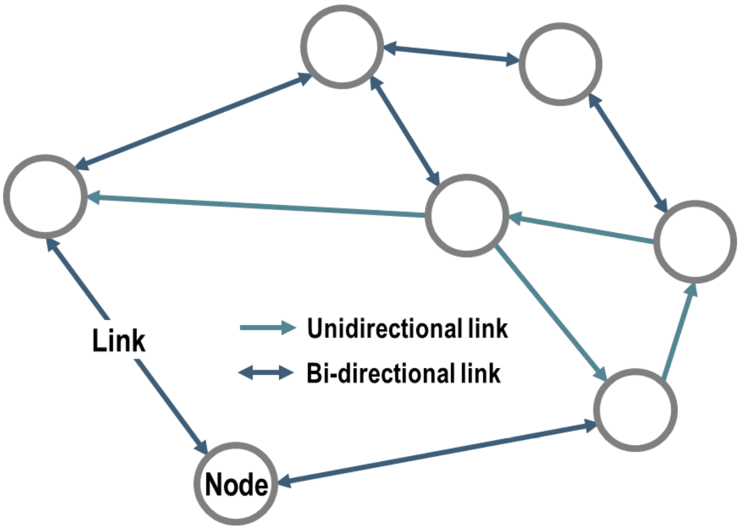
## Visualizations for Intrusion Detection

The following questions deal with visualizations specifically for Intrusion Detection. Please keep this in mind.

In your opinion, which of the following visualization types are suitable **for Intrusion Detection** analysis. If you think of different diagrams for different data, try to order them according to the importance.
Please prioritize them via drag&drop.

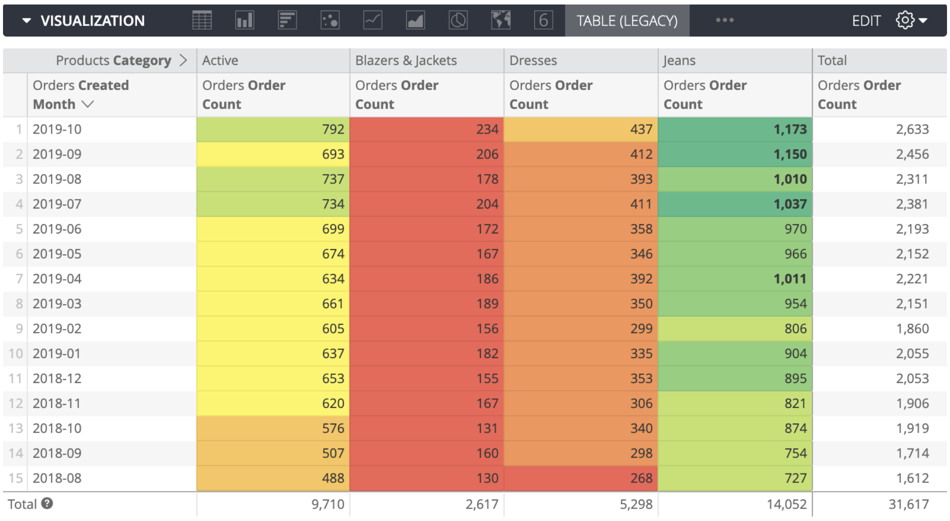
»

**Node-link/Network diagrams**



»

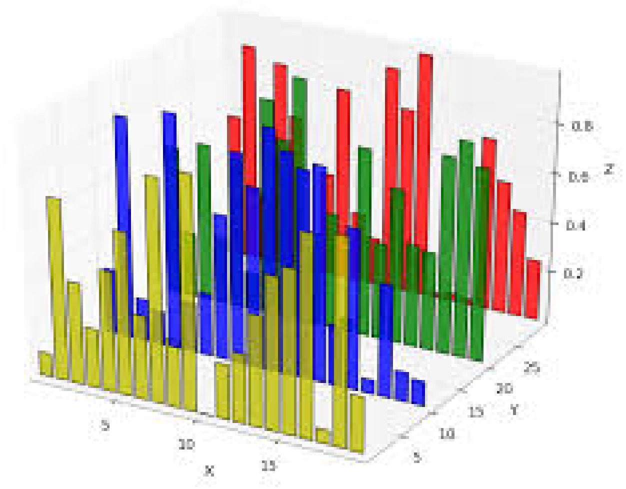
## Advanced tabular form



| | Products Category > | Active | Blazers & Jackets | Dresses | Jeans | Total |
|---|---|---|---|---|---|---|
| | Orders Created Month ∨ | Orders Order Count | Orders Order Count | Orders Order Count | Orders Order Count | Orders Order Count |
| 1 | 2019-10 | 792 | 234 | 437 | **1,173** | 2,633 |
| 2 | 2019-09 | 693 | 206 | 412 | **1,150** | 2,456 |
| 3 | 2019-08 | 737 | 178 | 393 | **1,010** | 2,311 |
| 4 | 2019-07 | 734 | 204 | 411 | **1,037** | 2,381 |
| 5 | 2019-06 | 699 | 172 | 358 | 970 | 2,193 |
| 6 | 2019-05 | 674 | 167 | 346 | 966 | 2,152 |
| 7 | 2019-04 | 634 | 186 | 392 | **1,011** | 2,221 |
| 8 | 2019-03 | 661 | 189 | 350 | 954 | 2,151 |
| 9 | 2019-02 | 605 | 156 | 299 | 806 | 1,860 |
| 10 | 2019-01 | 637 | 182 | 335 | 904 | 2,055 |
| 11 | 2018-12 | 653 | 155 | 353 | 895 | 2,053 |
| 12 | 2018-11 | 620 | 167 | 306 | 821 | 1,906 |
| 13 | 2018-10 | 576 | 131 | 340 | 874 | 1,919 |
| 14 | 2018-09 | 507 | 160 | 298 | 754 | 1,714 |
| 15 | 2018-08 | 488 | 130 | 268 | 727 | 1,612 |
| Total ? | | 9,710 | 2,617 | 5,298 | 14,052 | 31,617 |

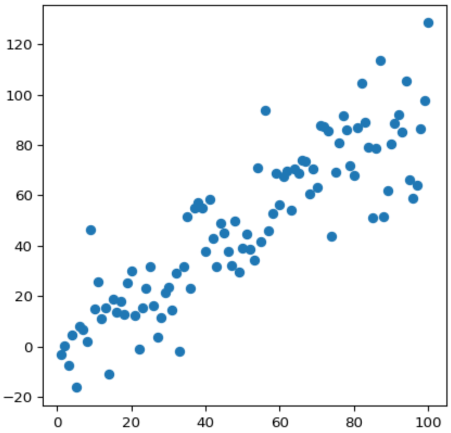
»

## 3-D diagrams



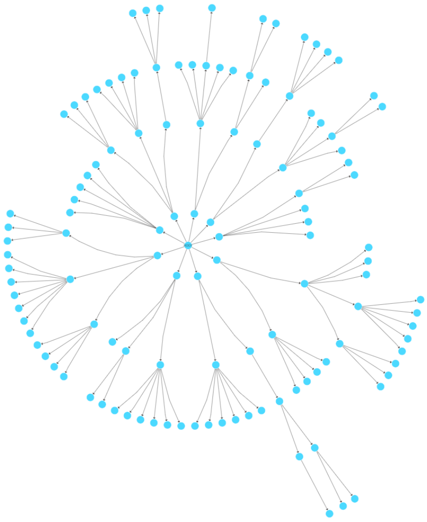
»

## Scatter plots

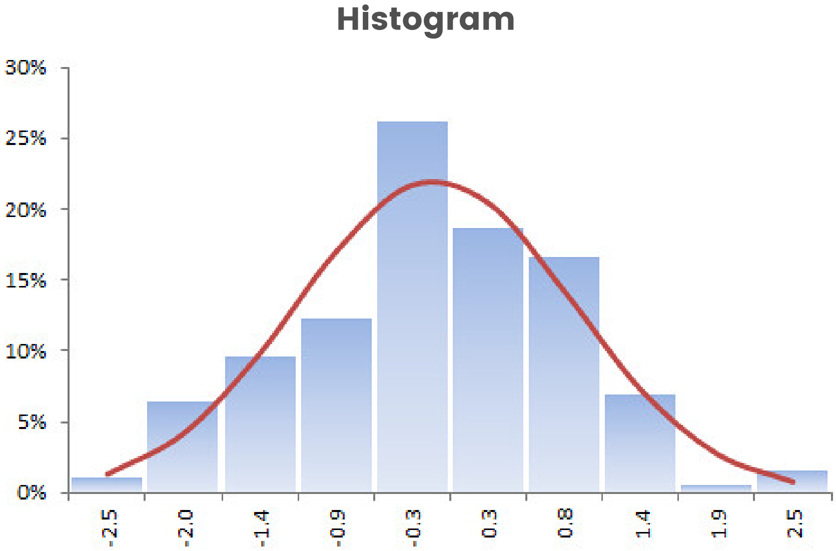


»

### Radial graphs/diagrams



»



## Which of the following statements do you agree with?

□ Visualizations and Dashboards replace completely the manual viewing of classical log files.

□ In the daily life, we increasingly work with highly user-friendly interfaces and visualizations. Therefore also visualization frameworks for intrusion detection must be simple and easy to use as much as possible.

□ Visualizations can often simplify only specific aspects of the data. A comprehensive view (e.g. in tabular form) must still be provided to enable the user to discover all details.

□ Visualizations help to find insights (e.g. new attack patterns) which are hard to identify in classical representation like log files or tables.

□ Visualization frameworks for intrusion detection should be used only by security administrators or analysts

Which challenges do you see for visualization techniques for Intrusion Detection?

□ The user can misinterpret or miss important insights of the data if the visualization highlights the "wrong" aspects of the data or "hide" important details

□ Some insights can not be found if the filter capabilities are missing

□ The definition of a "good looking" and "valuable" visualization is differently by everyone

□ The visualization of large datasets/log files cause long processing times and huge resource consumption

## Evaluation Framework

### SnortNetViewer

The following questions are about the visualization framework "SnortNetViewer". Please keep this in mind.

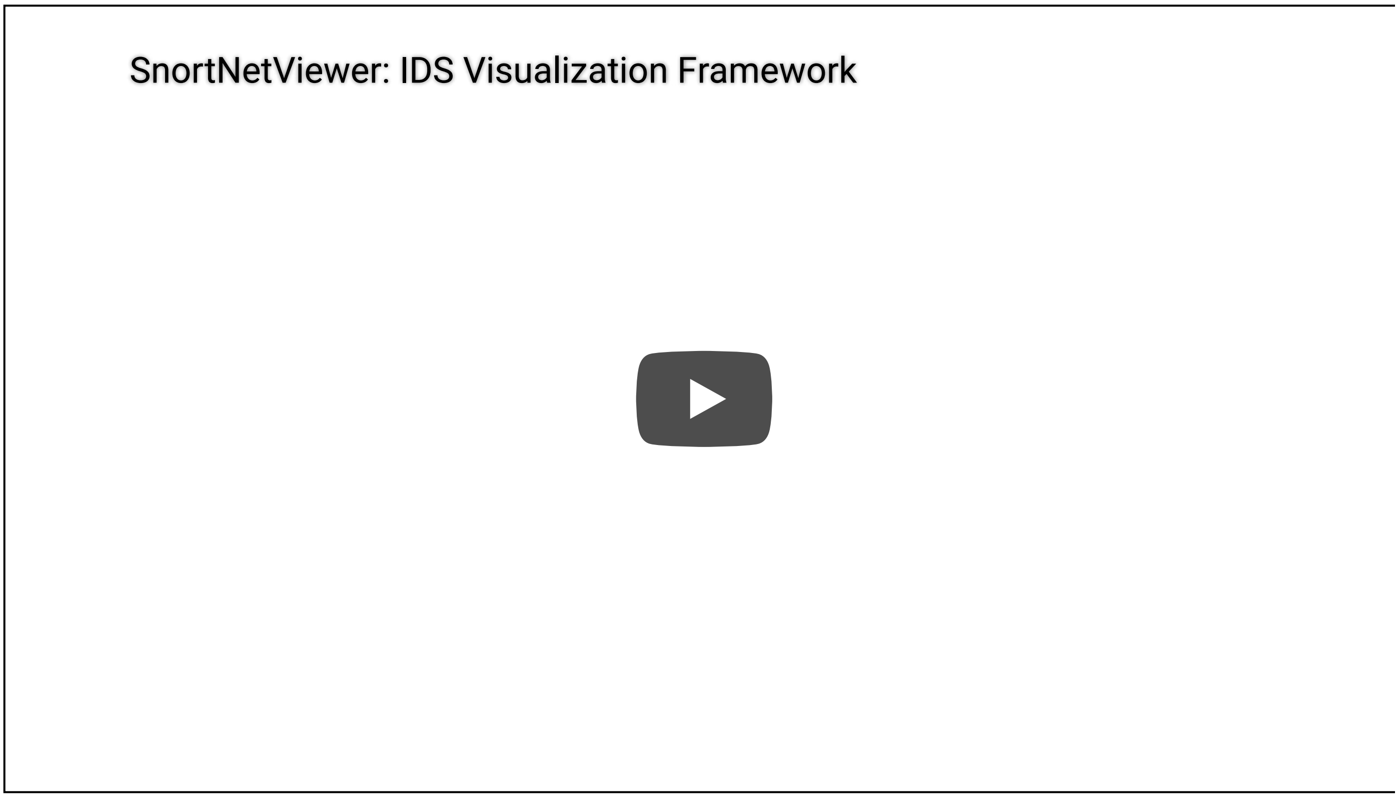
SnortNetViewer is visualization framework build with

Python and Dash to visualize Snort alerts in a node-link diagram (network). It also implements interactive features and csv import and export functionality.

**Main features:**

- visualization of Snort alerts from imported log file
- Interactive features like temporal course of the alerts, tooltips, zoom features and more
- detailed view of attacks in a table
- export and import of csv files (contain the defintions of the nodes and edges)

Please watch the short video below to get an impression of the framework.



SnortNetViewer: IDS Visualization Framework

Please rate the features of the framework according to your impression from the video.

| | 1<br>(missing) | 2 | 3 | 4 | 5<br>(well implemented) |
|---|---|---|---|---|---|
| Design & Usability | | | | | |
| Global overview with one look | ○ | ○ | ○ | ○ | ○ |
| Easy to use / self-explanatory control | ○ | ○ | ○ | ○ | ○ |
| Using of coloring and proportions to highlight only the most important aspects of the data | ○ | ○ | ○ | ○ | ○ |
| Features | | | | | |
| Detailed data inspection | ○ | ○ | ○ | ○ | ○ |
| Expert functions like correlations for deep analysis | ○ | ○ | ○ | ○ | ○ |
| Flexibility in terms of integration and multiple data sources | ○ | ○ | ○ | ○ | ○ |
| Real-time connection (life data analysis) | ○ | ○ | ○ | ○ | ○ |
| Advanced | | | | | |

| | 1<br>(missing) | 2 | 3 | 4 | 5<br>(well implemented) |
|---|---|---|---|---|---|
| Scalability to process large datasets in short time | ○ | ○ | ○ | ○ | ○ |
| Build upon state-of-the-art technology | ○ | ○ | ○ | ○ | ○ |

Powered by Qualtrics