# Visual Firewall Log Analysis - At the Border Between Analytical and Appealing



Figure 1: With the goal to provide insights into the firewall logs of an organization, we identified two types of interests: high-level overview and low-level analysis. A persona with the main targeted psychological needs was defined for each role (information security officer and network analyst). We developed two concepts to fit to the requirements for each usage context and two interfaces that can be used together as a combined visual firewall log analysis system. (Need cards ©Hassenzahl et al. [31])

## ABSTRACT

In this paper, we present our design study on developing an interactive visual firewall log analysis system in collaboration with an IT service provider. We describe the human-centered design process, in which we additionally considered hedonic qualities by including the usage of personas, psychological need cards and interaction vocabulary. For the problem characterization we especially focus on the demands of the two main clusters of requirements: high-level overview and low-level analysis, represented by the two defined personas, namely information security officer and network analyst. This resulted in the prototype of a visual analysis system consisting of two interlinked parts. One part addresses the needs for rather strategical tasks while also fulfilling the need for an appealing appearance and interaction. The other part rather addresses the requirements for operational tasks and aims to provide a high level of flexibility. We describe our design journey, the derived domain tasks and task abstractions as well as our visual design decisions, and present our final prototypes based on a usage scenario. We also report on our capstone event, where we conducted an observed experiment and collected feedback from the information security officer. Finally, as a reflection, we propose the extension of a widely used design study process with a track for an additional focus on hedonic qualities.

**Index Terms:** Human-centered computing—Visualization— Information visualization; Security and privacy—Human and societal aspects of security and privacy;

#### **1** INTRODUCTION

A strong network security is an indispensable requirement for all organizations with an IT infrastructure. This is especially true for IT service providers. In this context, effective methods to support the routine tasks of the responsible persons can have a valuable impact on the organizations network security [9]. Applying visualization methods to increase the visibility of different logs gathered from the IT network can increase the level of insight and lead to better decisions [72]. A firewall provides an important perimeter for the network that also allows the observation of incoming and outgoing traffic. This traffic (accepted and denied connections) is recorded in firewall logs that may contain valuable information concerning the activities on and around the network [7, 52]. The visual analysis of firewall logs was the main goal of a joint project with an IT service provider. During our multi-year design study [70], we have encountered a number of challenges, which we present in this paper together with our proposed solutions.

The first challenge was the often-encountered problem to balance conflicting requirements of several stakeholders. We show how we have identified two clusters of users, represented each of them by a persona [56] and designed the joint solution with respect to these requirements. Our proposed system approach interlinks two interfaces in one solution, while addressing the individual needs of the user groups with each interface. Our second challenge was to find appropriate visual solutions to enable flexible and interactive insights from firewall log analysis. Our solution combines an analytical interface with interactive overview visualizations. The third challenge was to adequately integrate non-pragmatic (or hedonic) aspects into our design process. The need for this emerged as our collaborators, beside the functional requirements, expressed the desire for a notably positive and aesthetic appeal of the final solution. Researchers in HCI emphasize the role of considering subjectively perceived qualities for the design of products and software since

©2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

<sup>\*</sup>The first two authors contributed equally to this work.

<sup>&</sup>lt;sup>†</sup>e-mail: marija.schufrin@igd.fraunhofer.de

<sup>&</sup>lt;sup>‡</sup>e-mail: hendrik.luecke-tieke@igd.fraunhofer.de

<sup>§</sup>e-mail: joern.kohlhammer@igd.fraunhofer.de

many years [36]. Hassenzahl et al. [36] coined the term *hedonic* as opposed to pragmatic qualities. While pragmatic qualities comprise quality dimensions that are related to traditional usability and focus on task-related functions or design issues (targeting the so called *do-goals*), "hedonic qualities comprise quality dimensions with no obvious relation to the task the user wants to accomplish with the system, such as originality, innovativeness, beauty" [36], addressing the so-called *be-goals*. Hassenzahl et al. propose to consider basic psychological needs to achieve hedonic qualities [34]. In this paper we describe how we used this approach in our design study and finally propose a process model to include this approach into the infovis design study pipeline. In particular, we considered psychological needs [34] and interaction vocabulary [47]. Along the lines of Sedlmair et al. [70], the three contributions of this paper are:

- Problem characterization and abstraction: Domain characterization for visual firewall log analysis in IT organizations for multiple decision makers with strongly different requirements
- 2. Validated visualization solution: Proposed concept of a visualization system consisting of two interlinked parts, considering pragmatic as well as hedonic aspects, which is implemented and validated as a web-based prototype
- Reflection: Proposition of an extended design process model taking into account hedonic qualities by including personas and the psychological needs theory

#### 2 RELATED WORK

Three topics are relevant for the related work: existing visualization approaches for IT network logs, visual environments based on data flows, and work addressing pragmatic and hedonic design choices.

Visualizations for network log analysis There are already many visual analytics approaches for the analysis of network logs (see surveys from Shiravi et al. [72] and Zhang et al. [79, 80]). There are approaches that only focus on the interactive visualization of these logs [1, 22, 46, 49], but also approaches that incorporate automatic data processing and detection in some way [28, 29, 54]. Several publications focus on one visualization technique [4, 18, 77], while others combine various visualizations and different views [2, 13, 26,27]. Further, some approaches focus only on one log type (e.g. firewall log data) [26,54], while others aim to combine logs from different data sources [23, 25, 28] or existing information about known malware or attacks. The most frequently used visualization techniques we observed were node-link diagrams [3,8], matrices [25, 26], and parallel coordinates [18,77]. Also symbol or glyph based visualizations [22, 44] are present. There are also many approaches with hierarchical layouts. These range from binary arrangement (internal vs external) [4, 23] to rectangular [23] and circular [2, 3, 22] tree maps. Apart from hierarchical layouts, overlays are frequently applied to visualize the actual communication behaviour. For example, edges are drawn between sources and targets to show the detailed connections on top of the hierarchical context [2, 4, 23, 43], as we do in ClusterVis. Several cyber-security visualizations use static or animated bubbles to convey information ranging from global scale down to the individual packet [2, 3, 44, 55]. There are also several approaches that we perceived as appealing or pleasing to the eye, such as [22], [55] or [17]. In summary, while there are approaches for network log analysis that are well suited for their goals of which some provide an appealing appearance, most of them have limited flexibility. Therefore, we added the concept of visual flow-based data analysis to our design solution. We have not found an approach for network log analysis that uses a visual flow-based data analysis in combination with an interactive visualization for the analysis of network log data.

Flow-based data processing and analysis Visual environments based on data flows are well suited to allow users to flexibly and interactively choose analytical methods to process the firewall log data. Several approaches for general data analysis exist, such as KNIME [6] or YALE [57]. Lately, more interactive elements are embedded directly into the workflow [19, 78]. Although visual programming environments have strongly advanced in recent years and enable users to solve problems computationally without the need of learning programming languages, they are mostly suited for data analysts. Thus, one valuable extension is to enrich such environments with attractive and interactive visualizations. For example, VisFlow [78] integrates interactive visualizations directly on the canvas. We have used this approach in the analytical *Whiteboard*, which especially allows to integrate the more appealing *ClusterVis* and other visualizations. Additionally, we feature a full data-flow processing model instead of data subset flows.

Pragmatic and hedonic visualization design Along the lines of the human-centered design process (HCD) [41] and the research of Hassenzahl et al. [32], in our design process we tried to consider both pragmatic and hedonic qualities. Looking at established process models for infovis and visual analytics design, we observed a lack of guidance with regard to hedonic qualities. For example, while in the visualization pipeline of Card and Mackinlay [14] the user is an integral part of the process of the interactive transformation of data into visual forms, the focus is on the pragmatic, visualization-related aspects. The same is true for the design triangle of Miksch and Aigner [59]: while they characterize user needs along various axes, the main focus is on pragmatic qualities. Munzner's Nested Model [62] as well as the methodology proposed by Sedlmair et al. [70] provide frameworks for design studies in information visualization. While they leave room to integrate hedonic qualities into each step, these potential choices are not explicitly mentioned. Several authors promote a stronger interplay of art and information visualization [45, 60,68,74], while others stress the importance of engagement [38,50] and user experience [69]. However, we have not found related work that actually reports on such methods in their visualization design process. Thus, to the best of our knowledge, there is currently no model that gives guidance on integrating both pragmatic and hedonic design choices in visualization design study.

## **3 OUR DEVELOPMENT JOURNEY**

This section gives an overview of the development process, highlights the key events, and outlines the challenges we had to overcome (see Figure 2). Our journey took around three and a half years and involved several iterations. The first HCD iteration started with the goal to interactively investigate data from the cyber-security domain. A first meeting (a) with an IT service provider revealed the demand for a visual security solution (1). More precisely there was a requirement for analytics of available internal logs (2). Based on that we foraged for related visualization approaches for network security (3) and presented them in a meeting (b) to our partners at the IT provider (4). Summarizing the findings within the second HCD iteration, we observed that there are various stakeholders with different interests in the context of network data analysis (5). Further, the main interest was to provide visual insights into internal network logs of the organization with a focus on perimeter firewall logs (6). We started with baseline work on a research prototype (7) based on our initial understanding with several updates during our journey. Thereby, we worked both on the analytical part - which analysis could be applied to firewall logs (Whiteboard) and on the visual part, how the content of firewall logs can be visualized (which later resulted in ClusterVis). Initially, we used the VAST challenge 2012 dataset [75]. The third HCD iteration started with a meeting with the information security officer (c), where we specified the context of current technical possibilities, infrastructure, data and possible targeted users and goals (8). Based on that we derived a first description of the requirements and the relevant data, users and tasks (9). Our collaborators also emphasized non-functional requirements in the direction of "aesthetically pleasing" elements, literally asking for "eye candy" to complement the more analytics-



Figure 2: The journal of events of our design study with six iterations. The timeline shows the events with other participants (yellow and green) and milestones according to the four steps of the HCD cycle [41]. Selected screenshots at particular events show the parallel development of the two prototypes *Whiteboard* and *ClusterVis*.

oriented approaches. Therefore, we integrated user experience (UX) techniques into our design process. At this stage, we employed personas [16] and considered the psychological need cards [31]. We identified two main groups of stakeholders: technical experts and non-technical staff. Thus, we decided to proceed with the parallel development of two prototypes - one with a stronger analytical and one with a stronger visual focus. These two prototypes were planned to be interlinked with each other by integrating the *ClusterVis* visualization into the analytical Whiteboard. We concluded the third iteration by presenting the prototypes to the information security officer in a follow-up meeting (d) and received an anonymized sample of the real record of the firewall logs of this organization. We used the findings for the fourth HCD iteration to fine-tune our understanding of the targeted users, involved data and tasks (12) as well as the requirements (13). We also improved the prototypes on this basis and adapted them to the new data (14). The highlight of this iteration was a workshop (e) with the information security officer, a network analyst and a firewall expert. Focusing on the interests and feedback of the network analyst, we could collect more detailed information about actual daily tasks, fine-tune our requirements, and receive feedback on the current version (15). This feedback and an improved understanding of the needs and use cases of the potential stakeholders directly influenced the fifth HCD iteration, which consisted of improvements of our descriptions of the context of use (16), the requirements (17) and the prototypes (18). At this stage we also applied the interaction vocabulary [31,47] to sharpen the interaction design of the prototypes. Further we conducted a usability evaluation of Whiteboard (f) (19) with n=13 students and of ClusterVis (g)(21) with n=31 students, and presented the results to related stakeholders (h)(22). We concluded with a feedback meeting with the information security officer (i)(23). Meanwhile, we continuously worked on the prototypes (20). The results of the evaluation helped fix many usability issues of both prototypes. At the end of the sixth HCD iteration, after further prototype improvements (24), we conducted a capstone event with feedback session and final evaluation (25) with the information security officer.

#### 4 PROBLEM CHARACTERIZATION AND ABSTRACTION

We identified the demand to *get visual insights into internal network logs of the organization* as the main point of interest for our collaboration. However, during the first interviews we observed that different potential stakeholders and interests are involved. After multiple interviews, we identified two prominent clusters of requirements from different stakeholders with intersecting interests (see Table 1). Two main global usage scenarios emerged: On the one hand, there was the need for *high-level overview* tasks and a focus on *prevention* and *reporting*, including an appealing appearance. On the other hand, there was a demand for *low-level analysis* during daily routine with a focus on *inspection* and *detection*. In this paper, Cluster A is represented by the persona *information security officer* and Cluster B by the persona *network analyst* (see Figure 3).

Table 1: Selected characteristics of the two identified cluster	rs.
---	-----

	Characteristics	Cluster A	Cluster B	
1	Main goal	high-level overview	low-level inspection	
2	Main character	"big picture"	effective and flexible analysis	
3	Type of tasks	strategic	operational	
4	Focus of tasks	prevention	inspection	
5	Persona	information security officer	network analyst	
6	Usage experience	intuitive and appealing	profound inspection	
7	Cognitive load level	easy to understand	technically-demanding	
8	Time claim	instant	time-consuming	
9	Stakeholders	management, pr, security offier, etc.	div. technical staff, network analyst, etc.	
10	Communication target	communication with non-technical staff	communication with technical staff	
11	Communication purpose	reporting	collaborating	

**Users** The research process revealed a wide range of potential stakeholders for the visualization solution we are targeting. With regard to the two identified usage scenarios we decided to represent each cluster by one persona [16]. In Figure 3 we abstractly present the two personas *information security officer* as a representative for the staff with a potentially more strategic point of view, and the *network analyst* as a representative for the operational staff. The selection of these personas was also nicely related to our main contacts at our collaboration partner, but is also representative for the broader group of stakeholders. It is clear, that the interests of the two personas partly overlap. As an additional method, we decided

to consider the dimension of psychological needs to support our design decisions during our design process. In the course of this, we used the design cards of Hassenzahl et al. [31]. Based on the interviews, we selected the most appropriate psychological needs and assigned them to the personas. For the information security officer we chose security and stimulation as the primary needs, and additionally popularity. Security is described as "feeling safe and in control of your life" and stimulation as "feeling that you get plenty of enjoyment and pleasure" [31]. For the network analyst, we focused on the need for competence and autonomy. Competence supports a "feeling that you are very capable and effective in your actions" and autonomy a "feeling that you are the cause of your own actions" [31]. Figure 3 shows the assigned cards. We provide more details on how this inspired our approach and gave us orientation for our design decisions in section 5. Another aspect to highlight is the requirement to communicate findings in the network log between different stakeholders. In Figure 4, we have summarized some of the identified communication needs of both information security officer and network analyst. Note that there are communication relationships both within and between the two clusters.



Figure 3: Two personas: the information security officer requires an appealing and fast high-level overview of the network situation. The network analyst is interested in a faster detection of suspicious activities. To support the design process we have assigned psychological needs to each persona. (Need cards ©Hassenzahl et al. [31])

Requirements and Tasks In Figure 5 we summarize the requirements R1-R6 and tasks T1.1-T6.2 that we identified based on the exchange with our stakeholders. We have defined the six requirements from the perspective of our two personas and assigned each requirement to exactly one persona. While the information security officer (high-level activities) focuses on getting an intuitive overall impression of the current situation in the presented log, the tasks of the network analysis expert (low-level activities) focus on a deep and efficient inspection of the log data. However in reality, representatives of both user groups can be interested in each of the task and can benefit from both interfaces. This is also what our final evaluation reveals (see section 7). For each requirement, the list contains a selection of domain tasks, which are defined based on the identified requirements. From an infovis perspective, we have translated the six domain requirements to six abstract tasks (AT1-AT6) according to the taxonomy of Munzner et al. [10,64] (see Figure 5 and the supplemental materials for further details). Additionally, we assigned the requirements to the psychological needs which is represented by color in Figure 5. While there is more than one affiliation (e.g., the communication aspect R3 also addresses the need of competence), we have focused on the most prominent property for more clarity.

**Data** The data of interest are firewall logs that our project partner stores in large amounts and wants to analyze in a faster and better way. We received an anonymized example record by the organiza-



Figure 4: Communication relationships: Information security officer - many communications to persons with a low technical level. Network analyst - mostly regards technical-savvy communication partners. The communication between information security officer and network analysis expert is of particular relevance.

tion, which was recorded at the perimeter firewall and converted into csv format. The log contained more than 100 attributes, of which many were only present under certain conditions. Our solution is generally applicable to firewall logs, which mostly have a similar basic structure as described in *data abstraction*. In this collaboration, csv was used, but pcap is supported, too. Also other parsers can be added with low effort. For initial experiments, e.g., we also used the data set of the VAST challenge 2012 [75].

Data Abstraction: Firewall logs usually contains a lot of relevant information, because all incoming and outgoing traffic has to pass the firewall. Recording both accepted and rejected connections thus leads to a valuable data set. Each log entry contains information about one connection between two IP addresses (inside and outside). Dataset type: The data set type is primarily *tabular* [64]. However, as each activity describes the communication of two IP addresses, it can be also viewed as a network. Attribute types: Each log entry includes at least the timestamp (ordinal), the source and destination addresses (categorical), and the performed actions of the captured activity (*categorical*). Depending on the firewall, the log can contain further attributes with different data types, for example, port (categorical/ordinal) or protocol (categorical). Amount of items: The amount of items in the data set strongly depends on the activity on the network and on the amount of devices connected to the firewall. The exemplary data record of 10 minutes included around 1.5 million lines. However, in our solution we primarily focused on subsets of around 1.000 to 50.000 entries.

### **5** VISUALIZATION DESIGN

In this section, we present our two resulting inter-playing interfaces and explain our design decisions based on the findings presented in section 4. To support our two personas, we designed two interlinked prototypes: A flexible analytical tool (*Whiteboard*) and an interactive visualization with a particular focus on visual appeal (*ClusterVis*). The two prototypes can be used stand-alone, but can also be combined by either embedding *ClusterVis* in *Whiteboard* or by exchanging data-exports **T3.1**. This approach balances the need for independence and collaboration.

## 5.1 Decisions for ClusterVis (High Level)

*ClusterVis* (see Figure 7) is designed for the requirements of the *information security officer* (see Figure 5). The recorded firewall log, in csv format, can be dragged and dropped directly into the interface. The visualization shows each IP address from the log as a separate filled circle collected in a cluster, represented by the dotted lines. The main functionality of *ClusterVis* is to interactively arrange the IP addresses (the circles). This is possible through dividing the

High-level overview					Networ	Low-level analysis		
	R1	Get an insight into the firewall logs in an intuitive way	• Stimulation •		R 4	Expose suspicious activities on the network		
AT1: ENJOY the EXPLORATION of insights in the dataset	T 1.1	See the contained data in an appealing way	14 Harden		T 4.1	Inspect the data visually regarding suspicious spots through visual patterns and anomalies	AT4: DISCOVER suspicious spots	
	T 1.2 Interact with the presented data and organizing the into a comprehensive form.		Competence	T 4.2	Draw in an automated support for the identification of anomalies and patterns in the log data			
AT2: DISCOVER	R 2	Get a feeling regarding the picture of the current security situation within the scope of the recorded log	Stimulation	Stimulation		R 5	Examine the reasons for suspicious behavior or network problems more closely	
the situation on the network	T 2.1 At o the	At one glance get an overview over the situation on the network.			T 5.1	Zoom into the suspicious spots and inspect the reasons for that.	AT5: DISCOVER	
(elements, activity, critical areas)	T 2.2	See, which objects are active on the network and how they communicate with each other.		Competence			suspicious behavior	
urcusy	T 2.3	Perceive the extent of the critical situation as well as locating the critical areas (at one glance)			Autoroccury	т 5.2	Move flexible through the data	
	R 3	Being able to communicate selected issues in a	Security	in a second seco	R 6	Being able to communicate selected issues in a		
AT3: PRESENT		comprehensive and appealing way to others	Popularity			comprehensive and detailed/accurate way to others		
selected issues	T 3.1	Exchange information about particular issues with the	Transmission	1922.15 C	T 6.1	Communicate the results of my analysis in a	AT6: PRESENT	
and summaries	cyber analyst in a fast way	The second secon	Autonomy		comprehensive way to my technical supervisor	selected issues to		
non-technical audience	Т 3.2	Communicate selected issues in an appealing and understandable way to the management level.	意	Autonomy	Т 6.2	Facilitate the introduction to the topic for new employees	technical and less- technical	
	Т 3.3	Provide selected issues to the publicity in an appealing way (PR).	Popularity				addiente	

Figure 5: Requirements (R), domain tasks (T) and abstract tasks (AT) resulting from the two main usage areas: high-level overview and low-level analysis representend by the personas information security officer and network analyst. Requirements and tasks are linked to the psychological needs and are translated into abstract tasks according to the taxonomy of Munzner [64]. (Need cards ©Hassenzahl et al. [31])

clusters based on different attributes of the log file or by creating own clusters. Communication behavior can be inspected interactively.

Visual Encoding As the main visual paradigm we decided to use unit visualization [20, 39, 65]. These often combine the intuitiveness of unit visualizations with the appeal of physics-based animation and interactions, and are easy to learn for end users. This paradigm supports all three requirements of the information security officer R1-R3. The familiar character of the unit visualization provides insights into the firewall logs in an easily accessible way (R1). Representing the data as countable units also supports T1.1, namely to see the contained data. We decided for a cluster layout (Figure 7 (a-e)) as the main view to facilitate an interactive organization of the presented data in a comprehensive form T1.2. We chose the IP addresses to be represented by the units also with regard to R2, namely to get a picture of the current security situation within the scope of the recorded log. This includes T2.1 to get an overview of the situation on the network and T2.2 to see, which objects are active on the network and how they communicate with each other. Therefore, the amount of recorded connections for each IP address is encoded by the size of the circle. Connections between the IP addresses can be displayed on demand through links with arrows, resulting in a local node-link diagram. We used the colors blue, yellow and white to encode whether an IP address is acting only as source, only as destination address, or as both. Further anomalies can be displayed in red. This especially supports T2.3, allowing users to perceive the extent of the critical situation as well as locating the critical areas. The metaphorical unit visualization also supports **R3**, i.e. the communication of selected issues in a comprehensive way. With the situation mode (Figure 7 (f)) we added an additional layout to best support R2. Thereby the IP addresses are arranged in inside and outside with respect to the perimeter depending on their communication activity. Additionally, to support inspection over time, a stacked bar chart is used showing the amount of active IP addresses over time.

**Interactions** To allow users to explore and organize the data with regard to personal needs **T1.2**, the main interaction provides means to cluster the circles according to different attributes. Selecting a cluster leads to a selection menu with attributes (Figure 7 (b,c)). Users can also create their own clusters and drag&drop the circles from one cluster to another through direct manipulation [40]. Further details and connections can be explored by selecting a particular

circle (hovering/clicking) to support **T2.2**. Additional characteristics, such as "anomaly" can be added to the circle with regard to **T2.3**. The bar chart acts as a filter to select a time frame. In the *situation mode*, no clustering is supported, but users can explore the connections of the IP addresses through hovering and clicking on the circles.

**Data Abstraction & Transformation** For *ClusterVis* we mainly pursued the following approaches to derive relevant information from the data: *Derive set of unique IP addresses:* Selecting all unique IP addresses from the source IP and destination IP attributes. *Attributes for each IP address:* Summarizing the attributes of connections to "most common" for each IP address. *Count amount of connections:* Counting the amount of entries for each IP address or for two communicating IP addresses. *Amount of IP addresses over time:* Collecting the amount of IP addresses per time-frame based on the timestamp.

Considering the psychological needs To satisfy the psychological need for stimulation, the visualization is organized as an interactive playground. A force-based layout is used to arrange the units in circles. In this way, the layout is not predefined, supporting serendipity [48, 51, 74] and an exploratory character (R1). To address the psychological need for security, we have designed an additional mode where the IP addresses are arranged in a more structured way, allowing the user to get a "picture of the situation" on the network (R2). Following the approach in [47], we selected interaction vocabulary based on the psychological needs and used them as inspiration for our design decisions. For ClusterVis we decided for the interaction vocabulary fast, powerful and spatial proximity as we perceived that to be appropriate for the psychological need of stimulation. Additionally, to also support the psychological need of security we decided for direct, instant and uniform. Our decisions also goes along with the findings in [47]. Thus, the user can directly interact with the units through direct manipulation [40], namely by moving the clusters and units across the field. Direct manipulation also reflects spatial proximity. The movement instantly follows the user's mouse movements and clicks. The cluster can be iteratively split into more clusters by clicking on the cluster and selecting an attribute in the pop-up menue. This interaction stays the same (uniform) for each level of clustering. Splitting a cluster results in a fast and powerful force-based division of the units. To evoke the positive experience of *popularity* as well as *stimulation*, we designed

© 2023 IEEE. This is the author's version of the article that has been published in the proceedings of IEEE Visualization conference. The final version of this record is available at: 10.1109/VizSec56996.2022.9941462



Figure 6: Usage scenario - *Whiteboard*: (a) Overview of the complete workflow built up with analysis blocks of *Whiteboard*, consisting of 4 sections (color-coded): load data (yellow), inspect data (green), anomaly detection with LOF [11], *ClusterVis* preview (violet), downstream analysis (dark green). (b) Automated part of the anomaly detection. A LOF algorithm is used and its results are displayed in various forms. (c) Manual and visual part of the anomaly detection including a scatterplot based on a PCA. (d) A simplified version of *ClusterVis* is integrated in *Whiteboard* and can be used as a preview. Detected anomalies in the cluster are directly highlighted in red.

for an appealing appearance. This requirement was also explicitly stated by the stakeholders (especially **T1.1, T3.2, T3.3**) which led us to particularly focus on the visual aesthetics. We used circles for the units, as round objects are known to be especially aesthetically appealing [5, 12, 37]. Further, we chose an aesthetically pleasing color scheme, fluid animations (force-based layout) and a lot of direct interaction (the user can perform many interactions by directly interacting with the visualized items). The main view is kept clean and simple, containing only the visualized and interactive data units. We used a dark mode [21, 30], which makes the content of the visualization stand out more prominently. However, as noticeable in Figure 6, we do not enforce the dark mode and color selection.

#### 5.2 Decisions for Whiteboard (Low-Level)

The analytical part, called *Whiteboard*, is a flow-based interface for interactive and flexible data analysis and is intended for the *network analyst* (see Figure 5). Analogous to a real-world whiteboard, users can place and connect analytical nodes on a white canvas and arrange them according to their needs. With the available data wrangling, machine learning and visualization nodes, the network analyst has a high degree of freedom to explore and inspect the firewall logs. While the development of *Whiteboard* started before the provider's requirements for flexible data analysis became apparent, the requirements guided the further development of the tool.

Visual Encoding To support R4, R5 and R6, *Whiteboard* is designed to be an interface to create and execute data flows in a customized and flexible way. To support the flexibility (T5.2), the interface follows the interactive whiteboard metaphor. The analysis steps are represented as rectangular interactive nodes and the data flows as lines connecting the nodes. Domain experts can graphically create workflows by connecting executable nodes with each other to define the order of execution, visually resulting in a node-link diagram (see Figure 6). To support the inspection of the data analytically and visually (T4.1) and to zoom into suspicious spots (T5.1), *Whiteboard* contains multiple different predefined nodes for data processing (e.g. filter - see e.g.Figure 6 (c)) and visualizations (e.g., table, bar chart, pie chart, or node-link diagram - see e.g. Figure 6

(b,c)), and also for machine learning to support **T4.2**. Especially the visualization nodes are also well suited for the communication of issues to the supervisor (**T6.1**) as well as to new employees (**T6.2**) in an easily understandable way (**R6**). In particular, we integrated a version of *ClusterVis* into *Whiteboard* (Figure 6 (a,d)).

Interaction design To provide a high level of flexibility for the user (**T5.2**) the interface is based on the following basic interactions: Users can select an area on the white space, create a new analysis node (block) and adjust the characteristics of the node directly at the node. Second, users can draw connections between the nodes and adjust the layout by moving the nodes around, enabling T4.2 and **T5.1**. They can also navigate over the whiteboard by zoom and pan. To fulfill R4, users can create a processing or machine learning pipeline, by creating and connecting appropriate blocks, such as visualizations or trainable anomaly detectors. From intermediate results, subsets of data can be derived for more focused analysis (R5). Finally, to address R6 beyond other visualizations, user can add a node with the appealing *ClusterVis* inside of *Whiteboard* to communicate the findings to the supervisor or colleagues. Interactions with the visualizations, such as brushing, can be carried out in the nodes themselves and can be linked to other nodes by connecting them. Through this, **T5.1** and **T5.2** are well supported.

**Data Abstraction & Transformation** As *Whiteboard* intrinsically provides functionalities to transform data, only transformation into a supported input format is required. Further transformation depends on the goals of the analyst and is part of the interactive analysis process. For the anomaly detection through machine learning, we used the original data table and used the log lines with selected attributes as input. To use the internal *ClusterVis*, the data table has to be transformed to match the expected input format.

**Considering the psychological needs** The need for *competence* is mainly addressed through the large collection of (more than 100) different node types, covering data processing, machine learning, and visualization, which the users can use as a toolkit to accomplish their goals. The need for *autonomy* is addressed through the flexible concept of the interface. For the *Whiteboard* the interaction vocabulary *spatial proximity, fluent*, and *powerful* interactions over their

© 2023 IEEE. This is the author's version of the article that has been published in the proceedings of IEEE Visualization conference. The final version of this record is available at: 10.1109/VizSec56996.2022.9941462



Figure 7: Usage scenario - *ClusterVis*: (a) The data export from *Whiteboard* is displayed; contained IP addresses are shown as bubbles; anomalous addresses are marked in red. (b) Clicking on a cluster reveals a menu, where the attribute "anomalous" is chosen for a further split. (c) The anomalous IP addresses are now in a separate cluster. (d) The anomalous cluster is further split based on the attribute "most common action", revealing three clusters. (e) The accepted anomalies are of particular interest and were brushed green by the user. (f) In situation mode, all IP addresses are arranged near the perimeter. IP addresses with more connections to the other side are closer to the perimeter.

opposites *spatial separation, stepwise*, and *gentle* guided our decisions for the interaction design. Following them, there are two ways how users can create new nodes: Either by clicking on the canvas and selecting the node of interest (*spatial proximity, powerful*) or by dragging the mouse from a node output to an empty space on the canvas (*spatial proximity, fluent*). *Spatial proximity* also inspired the decision to visualize data in place, within the node (opposed to *spatial separation*, as e.g. in RapidMiner [57]). Also the direct manipulation in the nodes (especially in the visualization nodes) reflects the principle of *spatial proximity* well.

## 6 USAGE SCENARIO

With the usage scenario as presented in Figure 6 and Figure 7 we want to demonstrate the potential for anomaly detection and exploration. The task is to detect suspicious activities of anomalous IP addresses within a selected snippet of a firewall log. Whiteboard: The detection starts in *Whiteboard* (see Figure 6 a). The analyst has constructed a pipeline based on the basic analytical elements on the canvas. The main workflow consists of loading the data set and processing the content through two analysis pipelines. The upper green pipeline (b) covers an automatic anomaly detection of abnormal log entries using the Local Outlier Factor (LOF) algorithm [11] and extracts the identified outliers into a new list. As the workflow is dynamic, it could be adjusted, extended or replaced anytime. The lower blue pipeline (c) covers the interactive analysis of the data. The raw data is presented to the analyst in a 2D scatterplot after a PCA dimensionality reduction has been applied. Within the scatterplot node, the analyst can interactively decide which entries to select as outliers. The resulting selection is extracted into a new list, postprocessed to fit the data format requirements of ClusterVis, which then displays the data and highlights anomalous IP addresses (see Figure 6 d). As soon as the input data changes (e.g. the selection in the scatterplot), the downstream nodes will be updated with the new data automatically. ClusterVis: The analyzed data log can then be exported as a log including a new column with the attribute Anomaly. This export can be loaded into ClusterVis for further exploration. Figure 7 (a) shows the IP addresses that occur in the log during the selected time span. The anomalies are marked in red. Then, the anomalies can be separated from the rest by dividing the cluster

accordingly (b,c). The anomalous values can, for example, be further divided according to the *action* attribute (d). The anomalies in cluster *accepted* might be of special interest and can be marked (green). Finally, the situation mode can be used to see the selected and anomalous IP addresses in a larger context (f). In this view, the IP addresses are arranged around the perimeter (firewall) as outside and inside the perimeter. IP addresses with a higher connectivity to the other side are positioned nearer to the perimeter.

#### 7 WRAP-UP WITH INFORMATION SECURITY OFFICER

To validate our solution we conducted an observed experiment with the information security officer of our collaborating IT service provider. Reserving time with the security experts was difficult due to a high workload in this time frame. However, we were glad to secure 4 hours with the information security officer, who has an excellent overview of the roles and tasks of various stakeholders in his organization. Therefore, he could give us valuable insights from the perspectives of management as well as network analysis. The core of the evaluation was a series of three prepared usage scenario with the real prototypes following a step-by-step description. For the usage scenario, real data of the organization was used. We observed the information security officer virtually through the shared screen. Thereby, he was free to express his thoughts and give comments. The wrap-up was conducted per video conference. The three usage scenarios were: (1) detecting and highlighting an outlier in Cluster-Vis and conducting a deeper analysis on the identified IP addresses in Whiteboard; (2) identifying anomalies in Whiteboard with visual and with automated support and displaying them in ClusterVis as critical areas; (3) detecting noticeable activities in ClusterVis and analyzing them further within ClusterVis. We have designed the usage scenarios in such a way, that all of the tasks as defined in Figure 5 are covered. Usage scenario (2) has been presented insection 6 and shown in Figure 6 and Figure 7. The second important component of the evaluation was a structured interview, in which we asked whether the evaluated interfaces covered the requirements and tasks as listed in Figure 5 as well as specific questions regarding Witheboard, ClusterVis and the combination of the two interfaces in the overall system.

Overall system: The information security officer agreed that

© 2023 IEEE. This is the author's version of the article that has been published in the proceedings of IEEE Visualization conference. The final version of this record is available at: 10.1109/VizSec56996.2022.9941462



Figure 8: Design process model: Extension of design study process [14, 70] by including a track taking into account hedonic qualities [36] through the incorporation of psychological needs [34], personas and interaction vocabulary [47].

the combination of the two interfaces is enriching and helpful. He rather agreed that it provides a good balance between an appealing possibility to communicate and a profound analysis. Here again, he rated possibility for T 3.2 as neutral. But he rather agreed on T 6.2. He also stated that he could imagine to use the system for the analysis of data other than firewall logs. Finally, while he personally preferred the analytical Whiteboard, he claimed that he would rather use the combination of both systems. Whiteboard: After the assessment of the three usage scenarios, the information security officer rather agreed that all but two tasks in Figure 5 can be supported by our prototypes. One exception was the *neutral* assessments for tasks T 5.2 and T 6.1, where he was not able to assess that based on the guided usage scenarios. He expressed the wish for a more high-level representation of the analysis results. However, he rather agreed that it was helpful for the identification of anomalies and patterns in the log data. The implications regarding usability mainly addressed the reduction of complexity and the provision of ready-to-go pipelines and building blocks for specific common use cases. He also asked for an adaption of the interface's labels to the jargon of a network analyst. ClusterVis: Here again, the information security officer rather agreed on the fulfillment of most requirements tasks listed in Figure 5 for the strategical perspective. One exception was R2 with a neutral assessment. The information security officer also explicitly commented on all three sub-items of R2. He stressed that he can only rather agree with the fulfillment of tasks that concern the analyst experts and those with a focus on the analysis of the specific firewall log. Related to this, he has also rated T3.2 as rather *disagree*. For **T 3.3** the answer was between *neutral* and *rather agree* and dependent on the purpose and form in which the application would be reasonable. However, the application of ClusterVis to communicate some information to the information center (and then to citizens) has been rated as rather likely. The security officer rather agreed, that he found the interaction with *ClusterVis* as particularly pleasant and aesthetically appealing and that the interaction provided him with a good feeling. Overall the interface was assessed as intuitive and usable. The main implication regarding the usability was to develop concepts to process and display larger data sets with a higher number of IP addresses covering larger time spans and, if possible, in real-time.

#### 8 REFLECTION: PROPOSED DESIGN PROCESS

In this section, we summarize how we integrated psychological needs and interaction characteristics [34] into the design process for information visualization to strengthen the focus on user experience design. Figure 8 shows our proposed pipeline of an extended process model for design studies that takes these needs and characteristics into account. It is divided into three parts, denoted by vertical blocks. This division is based on the first three steps of a design study as defined by Sedlmair et al. [70], namely: *analyze real-world problem*, *design visualization system*, *validate design*. Our process contains a pragmatic track (depicted in gray), largely following the information visualization pipeline on top and integrates UX design methods at the bottom (the *hedonic track*). When comparing to the actual framework proposed by Sedlmair et al. [70], our proposed design process refers to the *core* design stage that consists of the steps *discover*, *design*, *implement* and *deploy*.

Analyze real-world problem This first block relates to the discover stage [70], where we extend the pragmatic steps of identifying the context of use [41] and specifying the requirements according to data, user and task [58] by additional hedonic methods. The first step of the pragmatic track is to identify the domain expert's problem or challenge. This includes the actual topic, the stakeholders, the requirements of the different stakeholders, and an overview of the available data. In our case, this has been done mainly through conversations with the stakeholders and related research (see section 4). For the hedonic track, we want to motivate the inclusion of the following steps. Collect statements To better deduce the hedonic requirements, a collection of relevant phrases from the stakeholders can be gathered. These should be phrases expressing wishes for positive experience expressed by the stakeholders. Appropriate phrases can for example be captured during the interviews or by foraging the protocols afterwards. These phrases can further be used for decisions about psychological needs and for the definition of personas. Choosing appropriate psychological needs To further support the empathy for the targeted UX, psychological needs can be taken into account. Considering psychological needs in the design process has two main advantages. On the one hand, they are helpful to better understand the users by taking into account their subjective preferences. On the other hand, they are helpful to make appropriate design decisions by "designing the experience" according to the so called be-goals [32]. Collecting relevant statements, choosing appropriate needs and defining personas all take

place iteratively. Later, the selected needs are used to choose an appropriate interaction vocabulary. Different collections of the main psychological needs of a human exists, which can be used for this step (for example [24, 53, 67, 71]). Further design frameworks from HCI, which incorperate these needs can be used as well [35, 66]. We made use of the collection proposed by Hassenzahl et al. [35] containing 8 basic needs and the related tool need cards [31]. The illustrations and exemplary statements help to get a feeling for the needs. Define Personas To further support the empathy for the users during the design process, personas [56] can be designed based on the information gathered about the targeted user group. Thereby, a group of multiple stakeholders can be summarized in one or multiple persona(s). For the definition and design of the personas both the collected statements and the psychological needs should be taken into account. In Figure 3 we present an abstract version of the personas, including the collected statements and selected needs. However, during the design process we have developed more detailed persona descriptions following [61]. Assigning needs to tasks A valuable step is to assign the selected psychological needs to the identified tasks either. Each task should be linked to the most appropriate need. This can help to define the tasks more precisely and identify tasks that are rather inappropriate for the targeted user. Further this can contribute to more accurate design decisions. We recommend to apply the needs to the domain tasks, as the abstract visualization tasks contain less information about the user. In hindsight and reflecting on our project, this step helped us refine the definition and grouping of the tasks and recalibrated our design goal.

Design visualization system This step relates to the stages design and implement in Sedlmair et al. [70], including the generation and validation of data abstractions, visual encoding and interaction mechanisms. The pragmatic track includes the classical steps of the information visualization process, as for example represented by the pipeline of Card et al. [14] or the three inner layers of Munzner's nested model [63]. We also considered user interface design [73] as an important building block in this step. Additionally, going along with other authors promoting a stronger integration of artistic design to increase the attractiveness or aesthetics in visualizations [45,60], we argue to consider the following two aspects for the hedonic track. Interaction Vocabulary In addition to the pragmatic rationale about appropriate interactions, a vocabulary with selected interaction characteristics [47] can be used with regard to the design for user experience [32]. Therefore, a set of interaction characteristics should be chosen for the targeted user experience. Here again, Hassenzahl et al. provides a tool, the interaction cards [31]. According to Hassenzahl [32] there is no predefined way to select the interaction characteristics or to implement the characteristics. These choices are left to the designers and their creative ideas. However, in Lenz et al. [47] some explanations for each attribute are provided, which can be used to map the interactions to the psychological needs. The characteristics can then be used as inspiration and reflection for each decision during the interaction design. The design process should be highly iterative and interlinked with the pragmatic interaction design. In section 5 we have shown how the selected characteristics influenced our design decisions. Aesthetic Design As visual aesthetics are known to be important factors for users, on judgement about the appeal of a product [36], aesthetic design is the second crucial component of our hedonic track. While design choices in InfoVis have been largely motivated by knowledge about human perception [76], there are few guidelines for the use of visual aesthetics [45]. At this step decisions on aesthetics (e.g. color harmony) have to be iteratively balanced with decisions from the pragmatic track (e.g. visual encoding). Related work that tries to incorporate aesthetics and artistic design to the domain of information visualization, as e.g. [45, 60, 68], can be used for deeper understanding.

Validate design This step can be related to the *deploy* stage by SedImair et al. [70], covering the validation and evaluation of the design. Beyond the question, how the validation has to be conducted in detail (for which there are other sources [70], [15], [42]), to validate the design in accordance with our proposed design process, we suggest to enhance evaluation of the known pragmatic qualities of utility and usability with evaluation of the hedonic qualities. **Evaluate user experience** For the hedonic track it should be evaluated, whether the result meets the targeted psychological needs [71], how the character of the interactions is perceived [47] and also the overall perceived attractiveness (e.g., [33]) of the visualization.

### 9 DISCUSSION

Appropriateness of the solution: Our approach to design and implement separate but interlinked interfaces for each user group was perceived as adequate. The feedback revealed that our system would be particularly beneficial to support the operational activities around the analysis and planning of network-related issues. For Whiteboard a promising direction would be to allow user-specific nodes in the form of "custom scripts" or "external service integration". Cluster-Vis showed up as a conducive approach to facilitate the interactive exploration but lacks the capacity for large data sets. Generalizability of the approach: While we presented a solution based on the data and requirements of one particular organization, the solution is also applicable for other providers. Thereby, the particular role of the users might vary, as our personas represent a group of users with similar interests. For example, a level-2 SOC analyst might also benefit from the interactive *ClusterVis* to analyse the alerts prepared in Whiteboard. The information security officer also stated that he can well imagine to use the system even for other application areas and with other data. In fact, due to the high flexibility of Whiteboard, the data input is not even constrained to network data. ClusterVis is also appropriate for other network data but can also be used for any data set with a unique identifier and an arbitrary number of data attributes. Moreover, a core functionality of Whiteboard is the possibility to flexibly incorporate other visualizations than Cluster-Vis to best suit a particular use case. Inclusion of hedonic user experience methods: We have found the inclusion of personas, psychological needs and interaction vocabulary as beneficial. Being able to also include the affective notion of user statements helped us to keep more relevant context that informed our design process. Therefore, the extended model explicitly includes a hedonic track as part of the design process. However, evaluating the hedonic quality was challenging as the questions on emotions were quite unusual for the participant in the security context. The helpful information on psychological needs and emotional states that we received from the interviews nevertheless encourages us to further explore the application of UX methods to information visualization design study.

#### **10 CONCLUSION**

In this paper, we have presented the process and the results of our design study on visualization solutions for firewall log analysis. Thereby, we have encountered two main clusters of interests and therefore have designed a solution consisting of two interlinked prototypes. While one targets the needs of the rather strategic group and exhibits a strong focus on appealing appearance, the other targets the operative group by focusing on flexible in-depth analysis. We showed how the prototypes evolved and were evaluated over time and also presented the feedback from a final assessment by our partner's information security officer. We also presented a usage scenario to validate the appropriateness of the solution. We reflected on this design study with its diverse requirements for hedonic qualities by extending a visualization design process, widely used in the community, by a hedonic track. In future work we aim to refine the derived process model by applying it to our further projects and by

examining possible extensions, e.g. incorporating other methods from user experience design.

#### ACKNOWLEDGMENTS

This work was partly funded by the Hessian Ministry of the Interior and Sports (HMdIS) within the "Round Table Cybersecurity@Hessen" and by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE. We want to thank the Hessian Central Office for Data Processing (HZD) for the fruitful collaboration and feedback.

### REFERENCES

- [1] K. Abdullah, C. P. Lee, G. J. Conti, J. A. Copeland, and J. T. Stasko. Ids rainstorm: Visualizing ids alarms. In *VizSEC*, p. 1, 2005.
- [2] D. Arendt, D. Best, R. Burtner, and C. L. Paul. CyberPetri at CDX 2016: Real-time network situation awareness. In 2016 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–4, 2016. doi: 10.1109/ VIZSEC.2016.7739584
- [3] D. L. Arendt, R. Burtner, D. M. Best, N. D. Bos, J. R. Gersh, C. D. Piatko, and C. L. Paul. Ocelot: User-centered design of a decision support visualization for network quarantine. In 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–8, 2015. doi: 10. 1109/VIZSEC.2015.7312763
- [4] R. Ball, G. A. Fink, and C. North. Home-centric visualization of network traffic for security administration. In *Proceedings of the* 2004 ACM Workshop on Visualization and Data Mining for Computer Security, VizSEC/DMSEC '04, pp. 55–64. Association for Computing Machinery, 2004. doi: 10.1145/1029208.1029217
- [5] M. Bar and M. Neta. Humans prefer curved visual objects. *Psychological science*, 17(8):645–648, 2006.
- [6] M. R. Berthold, N. Cebron, F. Dill, T. R. Gabriel, T. Kötter, T. Meinl, P. Ohl, C. Sieb, K. Thiel, and B. Wiswedel. KNIME: The Konstanz Information Miner. In *Data Analysis, Machine Learning and Applications*, Studies in Classification, Data Analysis, and Knowledge Organization, pp. 319–326. Springer, Berlin, Heidelberg, 2008. doi: 10 .1007/978-3-540-78246-9\_38
- [7] T. Bond. Visualizing Firewall Log Data to Detect Security Incidents, 2009.
- [8] T. Bond. Visualizing firewall log data to detect security incidents. *Global Information Assurance Certification Paper Copyright*, pp. 722– 729, 2009.
- [9] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher. Towards understanding IT security professionals and their tools. In *Proceedings of the 3rd Symposium on Usable Privacy* and Security, SOUPS '07, pp. 100–111. Association for Computing Machinery, 2007. doi: 10.1145/1280680.1280693
- [10] M. Brehmer and T. Munzner. A multi-level typology of abstract visualization tasks. *IEEE transactions on visualization and computer* graphics, 19(12):2376–2385, 2013.
- [11] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander. LOF: Identifying density-based local outliers. 29(2):93–104, 2000. doi: 10.1145/335191 .335388
- [12] M. Burch. The aesthetics of diagrams. In IVAPP, 2015.
- [13] B. C. Cappers and J. J. van Wijk. Snaps: Semantic network traffic analysis through projection and selection. In 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–8. IEEE, 2015.
- [14] M. Card. Readings in information visualization: using vision to think. Morgan Kaufmann, 1999.
- [15] S. Carpendale. Evaluating information visualizations. In *Information visualization*, pp. 19–45. Springer, 2008.
- [16] Y.-n. Chang, Y.-k. Lim, and E. Stolterman. Personas: From theory to practices. In *Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges*, NordiCHI '08, pp. 439–442. Association for Computing Machinery, 2008. doi: 10.1145/1463160. 1463214
- [17] V. Y. Chen, A. M. Razip, S. Ko, C. Z. Qian, and D. S. Ebert. Semanticprism: A multi-aspect view of large high-dimensional data. In 2012

IEEE Conference on Visual Analytics Science and Technology (VAST), pp. 259–260, 2012. doi: 10.1109/VAST.2012.6400527

- [18] H. Choi, H. Lee, and H. Kim. Fast detection and visualization of network attacks on parallel coordinates. 28(5):276–288, 2009. doi: 10. 1016/j.cose.2008.12.003
- [19] Demšar, Janez, Curk, Tomaž, Erjavec, Aleš, Gorup, Črt, Hočevar, Tomaž, Milutinovič, Mitar, Možina, Martin, Polajnar, Matija, Toplak, Marko, Starič, Anže, Štajdohar, Miha, Umek, Lan, Žagar, Lan, Žbontar, Jure, Žitnik, Marinka, and Zupan, Blaž. Orange: Data Mining Toolbox in Python. 14:2349–2353, 2013.
- [20] S. Drucker and R. Fernandez. A unifying framework for animated and interactive unit visualizations. https: //www.microsoft.com/en-us/research/wp-content/ uploads/2016/02/sanddance.pdf, 2015. (accessed 2022-09-05).
- [21] H. Eisfeld and F. Kristallovich. The rise of dark mode: A qualitative study of an emerging user interface design trend, 2020.
- [22] F. Fischer, J. Fuchs, and F. Mansmann. ClockMap: Enhancing Circular Treemaps with Temporal Glyphs for Time-Series Data. The Eurographics Association, 2012. (accessed 2021-06-21). doi: 10.2312/ PE/EuroVisShort/EuroVisShort2012/097-101
- [23] F. Fischer, F. Mansmann, D. A. Keim, S. Pietzko, and M. Waldvogel. Large-Scale Network Monitoring for Visual Analysis of Attacks. In J. R. Goodall, G. Conti, and K.-L. Ma, eds., *Visualization for Computer Security*, Lecture Notes in Computer Science, pp. 111–118. Springer, 2008. doi: 10.1007/978-3-540-85933-8\_11
- [24] J. H. Flavell. The development of children's knowledge about the appearance–reality distinction. *American Psychologist*, 41(4):418, 1986.
- [25] A. Frei and M. Rennhard. Histogram Matrix: Log File Visualization for Anomaly Detection. In 2008 Third International Conference on Availability, Reliability and Security, pp. 610–617, 2008. doi: 10.1109/ ARES.2008.148
- [26] M. Ghoniem, G. Shurkhovetskyy, A. Bahey, and B. Otjacques. VAFLE: Visual analytics of firewall log events. In *Visualization and Data Analysis 2014*, vol. 9017, p. 901704. International Society for Optics and Photonics, 2014. doi: 10.1117/12.2037790
- [27] J. Goodall, W. Lutters, P. Rheingans, and A. Komlodi. Preserving the big picture: Visual network traffic analysis with TNV. In *IEEE Workshop on Visualization for Computer Security*, 2005. (VizSEC 05)., pp. 47–54, 2005. doi: 10.1109/VIZSEC.2005.1532065
- [28] R. Gove. Automatic narrative summarization for visualizing cyber security logs and incident reports. In 2021 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–9, 2021. doi: 10.1109/ VizSec53666.2021.00005
- [29] J. L. Guerra, E. Veas, and C. A. Catania. A study on labeling network hostile behavior with intelligent interactive tools. In 2019 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–10, 2019. doi: 10.1109/VizSec48167.2019.9161489
- [30] L. Hakobyan and R. Saha. The impact of dark mode on the visual attractiveness of social media postings: A users' perception study based on facebook, 2021.
- [31] M. Hassenzahl. Experience design tools, University Siegen. http: //www.experienceandinteraction.com/tools. Accessed: 2021-06-28.
- [32] M. Hassenzahl. Experience design: Technology for all the right reasons. Synthesis lectures on human-centered informatics, 3(1):1–95, 2010.
- [33] M. Hassenzahl, M. Burmester, and F. Koller. Attrakdiff: Ein fragebogen zur messung wahrgenommener hedonischer und pragmatischer qualität. In *Mensch & computer 2003*, pp. 187–196. Springer, 2003.
- [34] M. Hassenzahl, S. Diefenbach, and A. Göritz. Needs, affect, and interactive products – Facets of user experience. 22(5):353–362, 2010. doi: 10.1016/j.intcom.2010.04.002
- [35] M. Hassenzahl, K. Eckoldt, S. Diefenbach, M. Laschke, E. Lenz, and J. Kim. Designing Moments of Meaning and Pleasure . Experience Design and Happiness. 7:21–31, 2013.
- [36] M. Hassenzahl, A. Platz, M. Burmester, and K. Lehner. Hedonic and ergonomic quality aspects determine a software's appeal. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 201–208, 2000.
- [37] C.-H. Ho, Y.-N. Lu, and C.-H. Chen. Influence of curvature and exper-

tise on aesthetic preferences for mobile device designs. *International Journal of Design*, 10(3), 2016.

- [38] Y.-H. Hung and P. Parsons. Assessing user engagement in information visualization. In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 1708–1717, 2017.
- [39] S. Huron, R. Vuillemot, and J. D. Fekete. Visual Sedimentation. 19(12):2446–2455, 2013. doi: 10.1109/TVCG.2013.227
- [40] E. L. Hutchins, J. D. Hollan, and D. A. Norman. Direct manipulation interfaces. *Human–computer interaction*, 1(4):311–338, 1985.
- [41] International Organization for Standardization. ISO 9241-210:2019 -Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems, 2019.
- [42] P. Isenberg, T. Zuk, C. Collins, and S. Carpendale. Grounded evaluation of information visualizations. In *Proceedings of the 2008 Workshop on BEyond time and errors: novel evaLuation methods for Information Visualization*, pp. 1–8, 2008.
- [43] C. Kintzel, J. Fuchs, and F. Mansmann. Monitoring Large IP Spaces with ClockView. In *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, VizSec '11, pp. 2:1–2:10. ACM, 2011. doi: 10.1145/2016904.2016906
- [44] A. Komlodi, P. Rheingans, U. Ayachit, J. Goodall, and A. Joshi. A usercentered look at glyph-based security visualization. In *IEEE Workshop* on Visualization for Computer Security, 2005. (VizSEC 05)., pp. 21–28, 2005. doi: 10.1109/VIZSEC.2005.1532062
- [45] A. Lau and A. V. Moere. Towards a model of information aesthetics in information visualization. In 2007 11th International Conference Information Visualization (IV'07), pp. 87–92. IEEE, 2007.
- [46] C. Lee, J. Trost, N. Gibbs, R. Beyah, and J. Copeland. Visual firewall: Real-time network security monitor. In *IEEE Workshop on Visualization for Computer Security*, 2005. (VizSEC 05)., pp. 129–136, 2005. doi: 10.1109/VIZSEC.2005.1532075
- [47] E. Lenz, S. Diefenbach, and M. Hassenzahl. Exploring relationships between interaction attributes and experience. In *Proceedings of the* 6th international conference on designing pleasurable products and interfaces, pp. 126–135, 2013.
- [48] T. Leong, S. Howard, and F. Vetere. Choice: abidcating or exercising? In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 715–724, 2008.
- [49] K.-L. Ma. Visualization for security. ACM SIGGRAPH Computer Graphics, 38(4):4–6, 2004.
- [50] N. Mahyar, S.-H. Kim, and B. C. Kwon. Towards a taxonomy for evaluating user engagement in information visualization. In *Workshop* on Personal Visualization: Exploring Everyday Life, vol. 3, p. 2, 2015.
- [51] G. Marchionini. Exploratory search: from finding to understanding. *Communications of the ACM*, 49(4):41–46, 2006.
- [52] R. Marty. Applied Security Visualization. Addison-Wesley, 2009.
- [53] A. H. Maslow. Motivation. Personality N ew York: Harper & Row Publishers Inc, 1954.
- [54] S. Matsumoto, A. Sato, Y. Shinjo, H. Nakai, K. Itano, Y. Shomura, and K. Yoshida. A method for analyzing network traffic using cardinality information in firewall logs. In 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, pp. 241–244. IEEE, 2010.
- [55] S. McKenna, D. Staheli, C. Fulcher, and M. D. Meyer. BubbleNet: A Cyber Security Dashboard for Visualizing Patterns. 35(3):281–290, 2016. doi: 10.1111/cgf.12904
- [56] T. Miaskiewicz and K. A. Kozar. Personas and user-centered design: How can personas benefit product design processes? *Design studies*, 32(5):417–430, 2011.
- [57] I. Mierswa, M. Wurst, R. Klinkenberg, M. Scholz, and T. Euler. YALE: Rapid Prototyping for Complex Data Mining Tasks. In *Proceedings* of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '06, pp. 935–940. ACM, 2006. doi: 10.1145/1150402.1150531
- [58] S. Miksch and W. Aigner. A matter of time: Applying a data–users– tasks design triangle to visual analytics of time-oriented data. *Comput*ers & Graphics, 38:286–290, 2014.
- [59] S. Miksch and W. Aigner. A matter of time: Applying a data–users–tasks design triangle to visual analytics of time-oriented data. 38:286–290, 2014. doi: 10.1016/j.cag.2013.11.002

- [60] A. V. Moere and H. Purchase. On the role of design in information visualization. *Information Visualization*, 10(4):356–371, 2011.
- [61] C. Moser. User experience design. In User experience design, pp. 1–22. Springer, 2013.
- [62] T. Munzner. A Nested Model for Visualization Design and Validation. 15(6):921–928, 2009. doi: 10.1109/TVCG.2009.111
- [63] T. Munzner. A nested model for visualization design and validation. *IEEE transactions on visualization and computer graphics*, 15(6):921– 928, 2009.
- [64] T. Munzner. Visualization analysis and design. CRC press, 2014.
- [65] D. Park, S. M. Drucker, R. Fernandez, and N. Elmqvist. Atom: A Grammar for Unit Visualizations. 24(12):3032–3043, 2018. doi: 10. 1109/TVCG.2017.2785807
- [66] D. Peters, R. A. Calvo, and R. M. Ryan. Designing for motivation, engagement and wellbeing in digital experience. *Frontiers in psychology*, 9:797, 2018.
- [67] S. Reiss and S. M. Havercamp. Toward a comprehensive assessment of fundamental motivation: Factor structure of the reiss profiles. *Psychological assessment*, 10(2):97, 1998.
- [68] F. Samsel, L. Bartram, and A. Bares. Art, affect and color: Creating engaging expressive scientific visualization. In 2018 IEEE VIS Arts Program (VISAP), pp. 1–9. IEEE, 2018.
- [69] M. Schufrin, A. Ulmer, D. Sessler, and J. Kohlhammer. Towards bridging the gap between visual cybersecurity analytics and non-experts by means of user experience design. In 2019 IEEE Symposium on Visualization for Cyber Security (VizSec), 2018.
- [70] M. Sedlmair, M. Meyer, and T. Munzner. Design study methodology: Reflections from the trenches and the stacks. *IEEE transactions on visualization and computer graphics*, 18(12):2431–2440, 2012.
- [71] K. M. Sheldon, A. J. Elliot, Y. Kim, and T. Kasser. What is satisfying about satisfying events? testing 10 candidate psychological needs. 80(2):325–339, 2001. doi: 10.1037/0022-3514.80.2.325
- [72] H. Shiravi, A. Shiravi, and A. A. Ghorbani. A Survey of Visualization Systems for Network Security. 18(8):1313–1329, 2012. doi: 10.1109/ TVCG.2011.144
- [73] B. Shneiderman and C. Plaisant. Designing the user interface: Strategies for effective human-computer interaction. Pearson Education India, 2010.
- [74] A. Thudt, U. Hinrichs, and S. Carpendale. The bohemian bookshelf: supporting serendipitous book discoveries through information visualization. In *Proceedings of the SIGCHI Conference on human factors in computing systems*, pp. 1461–1470, 2012.
- [75] VAST. Vast challenge 2012 bank world. http://www. vacommunity.org/VAST+Challenge+2012, 2012. Accessed: 2021-06-28.
- [76] C. Ware. *Information Visualization: Perception for Design*. Morgan Kaufmann Series in Interactive Technologies. Morgan Kaufmann, 3 ed., 2012.
- [77] X. Yin, W. Yurcik, M. Treaster, Y. Li, and K. Lakkaraju. VisFlowConnect: Netflow Visualizations of Link Relationships for Security Situational Awareness. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, VizSEC/DMSEC '04, pp. 26–34. Association for Computing Machinery, 2004. doi: 10. 1145/1029208.1029214
- [78] B. Yu and C. T. Silva. VisFlow Web-based Visualization Framework for Tabular Data with a Subset Flow Model. 23(1):251–260, 2017. doi: 10.1109/TVCG.2016.2598497
- [79] T. Zhang, X. Wang, Z. Li, F. Guo, Y. Ma, and W. Chen. A survey of network anomaly visualization. 60(12):121101, 2017. doi: 10.1007/ s11432-016-0428-2
- [80] Y. Zhang, Y. Xiao, M. Chen, J. Zhang, and H. Deng. A survey of security visualization for computer network logs. *Security and Communication Networks*, 5(4):404–421, 2012.