CYBER THREAT OBSERVATORY: DESIGN AND EVALUATION OF AN INTERACTIVE DASHBOARD FOR COMPUTER EMERGENCY RESPONSE TEAMS

Research Paper

Marc-André Kaufhold, Technical University of Darmstadt, Darmstadt, Germany, kaufhold@peasec.tu-darmstadt.de

Ali Sercan Basyurt, University of Duisburg-Essen, Duisburg, Germany, ali-sercan.basyurt@uni-due.de

Kaan Eyilmez, Virtimo AG, Berlin, Germany, kaan.eyilmez@virtimo.de

Marc Stöttinger, Hessian Ministry of the Interior and Sports, Wiesbaden, Germany, marc.stoettinger@hmdis.hessen.de

Christian Reuter, Technical University of Darmstadt, Darmstadt, Germany, reuter@peasec.tu-darmstadt.de

Abstract

Computer emergency response teams (CERTs) of the public sector provide preventive and reactive cybersecurity services for authorities, citizens, and enterprises. However, their tasks of monitoring, analyzing, and communicating threats to establish cyber situational awareness are getting more complex due to the increasing information volume disseminated through public channels. Besides the time-consuming data collection for incident handling and daily reporting, CERTs are often confronted with irrelevant, redundant, or incredible information, exacerbating the time-critical prevention of and response to cyber threats. Thus, this design science research paper presents the user-centered design and evaluation of the Cyber Threat Observatory, which is an automatic, cross-platform and real-time cybersecurity dashboard. Based on expert scenario-based walkthroughs and semi-structured interviews (N=12), it discusses six design implications, including customizability and filtering, data source modularity, cross-platform interrelations, content assessment algorithms, integration with existing software, as well as export and communication capabilities.

Keywords: Cyber Situational Awareness, Cybersecurity, Computer Emergency Response Teams, Public Security Sector, Design Science Research.

1 Introduction

Looking at the 2015 Ukraine power grid cyberattack, the 2017 WannaCry ransomware attack, or the 2020 University Hospital of Düsseldorf hack, the vulnerability of critical infrastructures and thus also of society to cyberattacks becomes apparent (Al-rimy et al., 2018; Davis et al., 2017; Ehrenfeld, 2017). The transition of traditional infrastructures, business models, and services to cloud-based solutions, the rising level of interconnectivity, and the exploitation of technological innovations by malicious actors contributes to an increase of the number, variety, and professionalism of cyber threats (ENISA, 2021), challenging cyber security professionals (Conti et al., 2018; Krstić et al., 2019) and posing a growing threat not only to the virtual but also to the physical realm. As a consequence, securing information technology and cyber incident response for citizens, public services, and critical infrastructures has become part of national and organizational security agendas (Azmi et al., 2016; Dorantes et al., 2006; Kolini & Janczewski, 2017; Skopik et al., 2018). The necessity of incident

response and management led to the establishment of CERTs in the public and private sector across the world (Krstić et al., 2019; Slayton & Clarke, 2020). With the objective of providing reactive (e.g., publishing alerts and warnings; incident, vulnerability and artifact handling), proactive (e.g., monitoring intrusion detection systems, developing security tools), and security quality management services (e.g., risk analysis, security consulting, education, and certification) for public authorities, citizens, and enterprises (West-Brown et al., 2003), CERTs monitor, analyze and communicate threats and incidents to establish cyber situational awareness (Franke & Brynielsson, 2014).

However, establishing cyber situational awareness while processing the increasing amount of available data across different channels, such as blogs, feeds, social media, vulnerability databases, third-party services, and websites, has become a complex challenge (Franke & Brynielsson, 2014). While being capable of maintaining internal network awareness within their host authorities, empirical research on German state-level CERTs suggests that they lack automatic and efficient tools to extract and integrate relevant information in real-time (e.g., indicators of compromise, security advisories, social media notifications, and vulnerability reports), which are required to establish external threat awareness (Riebe, Kaufhold, et al., 2021). Besides the time-consuming manual collection of data for cyber incident handling and daily reports, they are often confronted with irrelevant, redundant and sometimes incredible information (Basyurt, Fromm, Kuehn, et al., 2022). While the consideration of goals, roles, and information needs of operators during design processes as well as their involvement in evaluations are central to ensuring that technologies actually support cyber situational awareness (Gutzwiller et al., 2020), to our best knowledge, there is a lack of design and evaluation studies focusing on tools for the cross-platform collection and analysis of cyber threats. Thus, this paper seeks to answer the following research question: **What are design requirements and implications for a cross-platform cybersecurity tool to facilitate the cyber situational awareness of CERTs?**

Following the design science research (DSR) methodology of Peffers et al. (2007), this paper seeks to contribute with the elaboration of user requirements as well as the design, development and evaluation of a novel artifact with German state-level CERTs to mitigate the time-consuming data collection for incident handling and daily reporting of CERTs, which is often exacerbated by irrelevant, redundant and incredible information. Thus, the designed Cyber Threat Observatory facilitates the automatic, cross-platform and real-time collection and analysis of cybersecurity information to enhance the cyber situational awareness of CERTs. Based on this, the paper outlines six design implications, including the customizability of cyber threat data sources and filtering of displayed entities, modular integration of closed and public information sources, the interrelation across different cyber threat information feeds, intelligent algorithms for credibility assessment and threat prioritization, integration with organizational security software and systems, as well as export, sharing, and communication of relevant cyber threat data. Thus, the paper is structured as follows: we conduct a literature review (Section 2) and then outline the overall DSR research method (Section 3). Then, we present the (I) problem identification and motivation, (I) design objectives, as well as the (III) design and development of the Cyber Threat Observatory (Section 4). Based on this, we present the (IV) demonstration and (V) evaluation of our dashboard based on scenario-based walkthroughs and semi-structured interviews (Section 5). The paper finishes with the (VI) communication of key findings, implications, limitations, and future work that can be derived from the evaluation results (Section 5).

2 Related Work

2.1 Cyber Situational Awareness and Challenges for CERTs

In order to prevent and respond to attacks effectively, CERT staff needs to establish situational awareness and undertake informed decisions (Ruefle et al., 2014). Endsley (1995, p. 36) coined a distinction of three phases to attain situational awareness, including “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future”. Cyber situational awareness refers to a state of knowledge of actors that enables them to perceive the relevant elements in the cyber environment within a certain

volume of time and space, to comprehend their meaning, and to project their status in the near future (Husák et al., 2020). Although it was established as a subset of situational awareness, it cannot be considered in isolation, because events in cyberspace usually also impact the physical world, for example financially, socially, or politically (Bada et al., 2014; Cashell et al., 2008; Maness & Valeriano, 2016). Its growing importance within public administration has been reflected in numerous national cybersecurity strategies (Franke & Brynielsson, 2014), especially among professionals in formalized security organizations such as CERTs, whose work is particularly challenging due to the necessity of coordination and information exchange within and beyond the team, benefit from a continuous improvement of their situational awareness (Gutzwiller et al., 2020).

The term cyber situational awareness is often related to knowledge about occurrences in one's own network, but CERTs have to look way further "to gain a common operational picture of the threat environment in which the constituency is operating" (Ruefle et al., 2014, p. 17). This includes not only internal information like network activity but also information about what is happening in the world, for example, information about current events, new vulnerabilities, possible mitigations, and new technologies. However, due to the steadily increasing number of attacks and security breaches the volume and variety of potentially relevant data and data sources is steadily increasing and thus obtaining and ensuring adequate cyber situational awareness is increasingly dependent on the properties and capacities of the tools used (Drodt et al., 2018). Thus, Husák et al., (2020) identify both the joint aggregation, analysis, and visualization of data from as diverse sources as possible in real-time as well as the support of operators in assessing the veracity and credibility of the provided information as novel challenges that have so far been addressed only very fragmentary in technology development. Even recently developed dashboards to support cyber situational awareness focus on data from within the organization, such as the allocation of tasks within the team and the status of resources and incidents (Mullins et al., 2020), or on internal network security data and vulnerability management (Matta & Husák, 2021), while external data sources are rarely included and credibility assessment of social media data is not supported (Basyurt, Fromm, Stieglitz, et al., 2022).

2.2 Data Sources and Tools for Cyber Threat Collection and Analysis

To obtain relevant information and enhance cyber situational awareness, several data sources are available today. Skopik et al. (2018), e.g., have identified *vulnerability databases*, specialized search engines, and alerting systems as key data sources for cyber incident response. One of the most well-known vulnerability databases is the National Vulnerability Database (NVD), but other well-known alternatives are the commercial tool Vulners or the open-source database Open CTI (Booth et al., 2013). In these databases, the Common Vulnerabilities and Exposures (CVEs) have become established as the standard (Papp et al., 2015). All newly discovered security vulnerabilities in software or hardware components can be found there, supplemented by an assessment of their criticality in the form of the CVSS score, which takes into account various factors such as the degree of difficulty for the attacker to exploit the vulnerability, the potential damage, or whether prior authentication in the system is required for the attack. However, vulnerability databases should not be used as the only source for attaining cyber situational awareness, since it does not contain all vulnerabilities (Sabottke et al., 2015), entries are sometimes inconsistent (Rodriguez et al., 2018), or vulnerabilities are not published there timely (Kuehn et al., 2021). Furthermore, many manufacturers publish information on vulnerabilities and fixes on their own channels first (Lekkas & Spinellis, 2005). Often manufacturers publish *security advisories* in which they provide information about new security-related updates to their products and also new or resolved security vulnerabilities.

Besides vulnerability databases and security advisories, *threat intelligence platforms* have been established to allow both the collection and analysis of cyber threat data. Threat intelligence is defined as "the task of gathering evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard" (Mavroeidis & Bromander, 2017, p. 91). To support this task, several tools exist. For example, the Malpedia database allows malware researchers to add information about malware to the database (Plohmann et al., 2017).

Indicators of Compromise (IoCs) are also often used to better prevent attacks, and tools such as MISP (Wagner et al., 2016), ThreatFox (Abuse.ch, 2021), and Pulsedive (Pulsedive, 2021) were designed to allow the collection and processing of IoCs. In recent years, social media has become another important data source for cyber incident response since on those platforms cybersecurity experts are able to exchange threat information more quickly than by using more formal channels (Mittal et al., 2016). In the recent decade, a lot of *social media intelligence tools* have been developed to facilitate the collection and analysis of data from social media but most focus on natural and anthropological damage situations like floods or earthquakes (Kaufhold, 2021). Regarding cyber incident response, Mittal et al. (2016) created a Twitter-based warning framework for IT security incidents, and Rodriguez and Okamura (2019) developed a cyber situational awareness system aimed at retrieving and classifying security relevant information from the same platform. Still, the available tools are not intended to support CERT employees through the whole process of multi-platform data acquisition, analysis and communication of cyber threats (Basyurt, Fromm, Kuehn, et al., 2022).

3 Research Method

The problem-focused research paradigm of DSR seeks to "extend the boundaries of human and organizational capabilities by creating new and innovative artifacts" (Hevner et al., 2004). The related artifact contributions arise from generative design- and invention-driven activities, resulting in "new systems, architectures, tools [and] toolkits" which are then "evaluated in a holistic fashion according to what they make possible and how they do so" (Wobbrock & Kientz, 2016). In our work, we followed the established DSR methodology of Peffers et al. (2007), which comprises six steps that allow for multiple process iterations (Figure 1). First, we conducted and analyzed qualitative semi-structured interviews with German state-level CERT employees (N=17) to strengthen our understanding of the application domain, identify and motivate the research problem (Section 4.1), elicit user requirements, and define eight design objectives of a potential solution (Section 4.2). Based on this, we designed and developed the Cyber Threat Observatory, which is a cross-platform and real-time cybersecurity dashboard for CERTs (Section 4.3). In order to demonstrate and evaluate the artifact, we presented the tool to the target audience of German state-level CERT employees (N=12) and conducted scenario-based walkthroughs with semi-structured expert interviews (Section 5). Finally, the communication of our findings is accompanied by a discussion of implications for design, contributions to the knowledge bases, as well as limitations and future work (Section 6).

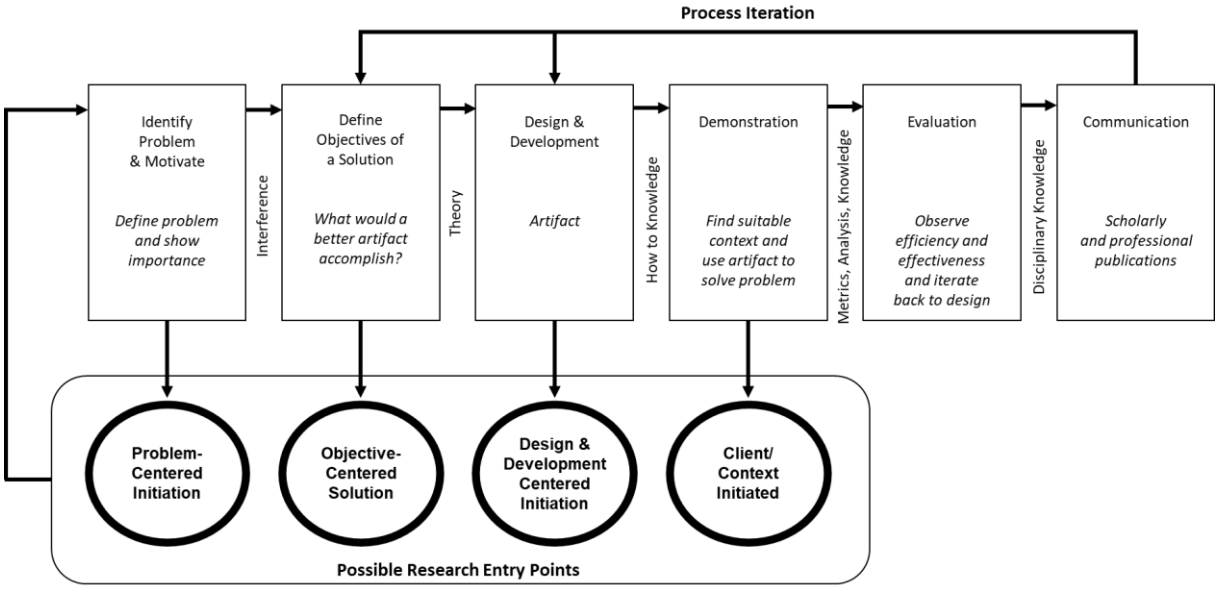

Figure 1. The six-step design science research methodology by Peffers et al. (2007).

4 Results I: Motivation, Objectives, and Technology Design

To define objectives for a solution as part of the DSR methodology, requirements were identified through interviews with people working at or with CERTs in two rounds in 2019 and 2021. To acquire the necessary data, requests for semi-structured expert interviews were sent out in two rounds. After receiving the participants' acceptance and informed consent, each interview session lasted around 50 minutes using a web conferencing tool. In the first round (I01 to I08) of interviews (n=8), a stronger emphasis was put on organizational factors and collaborative practices. The interview guideline comprised nine open-ended questions organized in three parts: (1) an introduction of the interviewee and his/her organizational role, (2) the deployment, organization, and work processes of the CERT, and (3) the communication and cooperation between CERTs. To get further insights into technology use by CERTs, a second round of interviews (n=7) has been conducted. In the second round (I09 to I15), the perspective of some non-CERT organizations that share information with CERTs has also been included (see I09, I10, I15). The second interview guideline comprised technology-focused questions on the (1) interviewees' role and organization, (2) reporting of cyber incidents, (3) monitoring of cyber incident data (e.g., IoCs), (4) analysis, prioritization, and verification of gathered evidence, as well as (5) communication of recommendations and warnings. We interviewed seven cyber incident managers, five team leaders, two information security officers, and one public safety answering point for cybersecurity issues. With the consent of the participants, all interview sessions were recorded and later transcribed. In order to account for the rich, qualitative interview data, we decided to conduct an inductive qualitative content analysis where categories emerge from the data analyzed (Mayring, 2000). Thus, the first and second authors independently employed open coding (Strauss & Corbin, 1998) to gather data into approximate categories reflecting the issues raised by respondents based on repeated readings of the data and its organization into similar statements. The authors then compared their categories and compiled a list of the most important user requirements identified during the coding process. Based on this, all authors participated in a workshop to identify the design objectives guiding the implementation of the Cyber Threat Observatory.

4.1 Problem Identification and Motivation

The German federal administration comprises independent cybersecurity organizations for the 16 states and the federal government. The states are represented by 13 CERTs within the public administrations or in state companies, whereas the federal CERT-Bund is integrated into the German Federal Office for Information Security (BSI). The individual CERTs are part of the administrative CERT network which provides an information exchange platform for public administration, thus offering an institutionalization of CERT partnerships. The structure, size, and skill set of these CERTs vary depending on available financial resources and the requirements of the respective target groups. They usually have a strategic head, the chief information security officer (CISO), and an operational team leader who leads a small number of incident managers and cybersecurity specialists. An attempt to generalize ICT use of German state CERTs is depicted in Figure 2. The process can be roughly divided into the steps of acquisition, analysis, and response. First, incidents are either reported by customers (via mail or telephone) or detected by software (such as intrusion detection). After initial information about the incident is gathered, CERTs use a ticketing and reporting system to collect their evidence for incident response. Second, this evidence is collected and analyzed using awareness-focused (e.g., manufacturer websites, security advisory feeds, and social media channels) and collaboration-oriented (e.g., malware information sharing platforms, the VCV collaborative chat) channels. Third, the collected evidence is then used to inform a certain stakeholder with specific recommendations, to provide (daily) reports for selected stakeholders (e.g., a daily vulnerability report for ministries), or to issue a general warning for multiple stakeholders (in case larger-scaled ICT infrastructures are threatened). In accordance with related research (Basyurt, Fromm, Kuehn, et al., 2022; Riebe, Kaufhold, et al., 2021), our interviews highlight a lack of automatic and efficient tools to extract and integrate relevant information in real-time, such as indicators of compromise, security advisories, social media notifications, and vulnerability reports, across multiple public data sources.

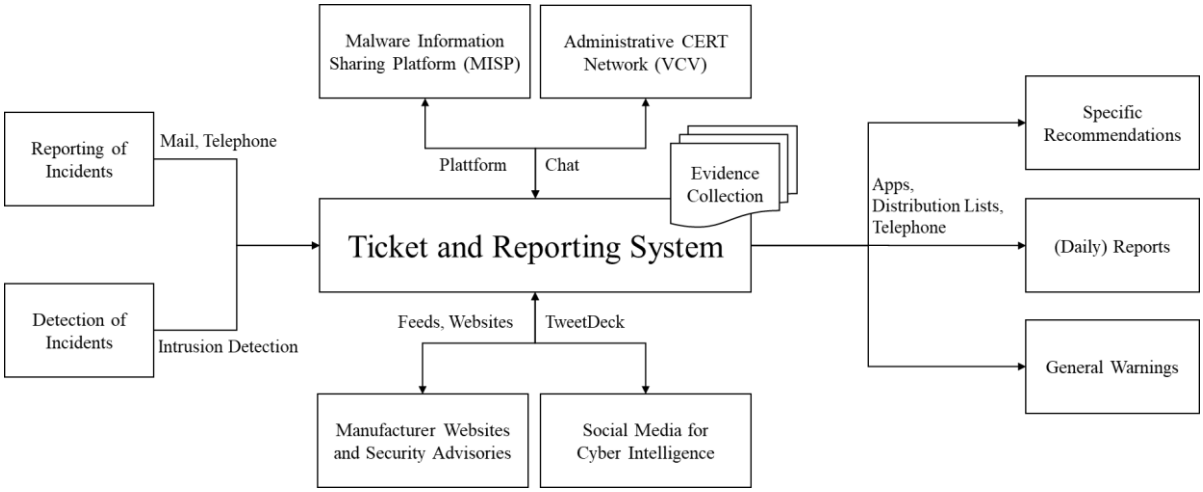

Figure 2. Exemplary ICT infrastructure and processes of a German state-level CERT.

4.2 Design Objectives

Existing design research suggests that dashboards are a suitable tool for enhancing network and task awareness (Matta & Husák, 2021; Mullins et al., 2020), but also for handling cross-platform social media data and the information overload triggered by the sheer amount of data available through such platforms (Avvenuti et al., 2018; Kaufhold, Rupp, et al., 2020). Based on our initial research and empirical findings, we assumed that this will also be true for publicly available threat awareness data (e.g., indicators of compromise, security advisories, and vulnerability reports). Thus, we decided to use an existing tool for open and social data collection as the base infrastructure (Section 4.3) and align our design objectives accordingly. The identified user requirements and design objectives that serve as the foundation of our design and development process are displayed in Table 1.

#	User Requirements	Design Objectives
1	Manual efforts of data collection should be replaced by (semi-)**automation**.	Security advisories, CVEs, IoCs, and social media information shall be collected automatically via APIs.
2	Enable **modularity** to add new data sources and features in the later course of development.	Interface-based programming allows to add further data sources and a modular design is used at the frontend.
3	Allow gathering of data from different sources and unify collected data for **interoperability**.	Data from different sources will be stored consistently using the ActivityStreams 2.0 Core Syntax.
4	Offer ways to support **data protection** (e.g., anonymization and data sparsity).	Users shall be able to select the metadata to collect and decide after how many days data should be deleted.
5	Automatically detect and filter out **redundant** information across different sources.	Unique database identifiers prevent redundant entities and redundant information (e.g., retweets) is filtered out.
6	Allow the **visualization** of important data to get an overview and accelerate decision making.	A feed is displayed per data source and important criteria are visualized via filterable charts.
7	Facilitate information **management** for different users or organizational roles.	Users shall be able to select the required data sources, adjust filter criteria, and pin important information.
8	Allow **customization** of data sources, filters, features, and settings to fit individual needs.	The displayed data of each feed shall be filterable based on the characteristic information of the specific source.
9	Display only **priority** (relevant) information to prevent the overload of human capacities.	Filtering of data sources with full text search or specific fields (e.g., software used by the organization).
10	Evaluate information based on trustworthiness and provide data to the user for **verification**.	Links to the original source, displayed metadata, and a team chat will facilitate the verification of content.

Table 1. Overview of the derived user requirements and design objectives.

4.3 Design and Development

Our designed artifact, the Cyber Threat Observatory, is based on an existing architecture whose technological foundation is documented in published research papers (Kaufhold, Bayer, et al., 2020; Reuter et al., 2016). The ODS is a web application based on Vue.js as the overall framework, Bootstrap for responsive design, and Chart.js for data visualization. Besides some local filtering options, all other actions of the ODS, such as searching for posts in open and social media or managing users, are forwarded to a backend called Open Data API (ODA). The ODA is realized as a service following the paradigm of a web-based and service-oriented architecture (SOA). It is a Java Tomcat application using the Jersey Framework for RESTful web services and the MongoDB database for document-oriented data management. Several libraries facilitate the automated and continuous real-time collection of data from open sources, such as NVD vulnerabilities, IoCs, and RSS feeds, or social media source APIs, including Flickr, Reddit, Tumblr, Twitter, and YouTube (#1). Interface-based programming was applied to achieve a modular application that enables the enhancement of these implemented sources in future iterations (#2). To overcome the diversity in data accessibility and structures, all entities are processed and stored according to the ActivityStreams 2.0 Core Syntax in JavaScript Object Notation (JSON) (#3). For the persistently stored data, the system operator has the possibility to specify an expiration date on which the data will be deleted (#4). Furthermore, unique database identifiers were utilized to prevent the storage of collected data that already exist in the database and would therefore represent redundant information (#5).

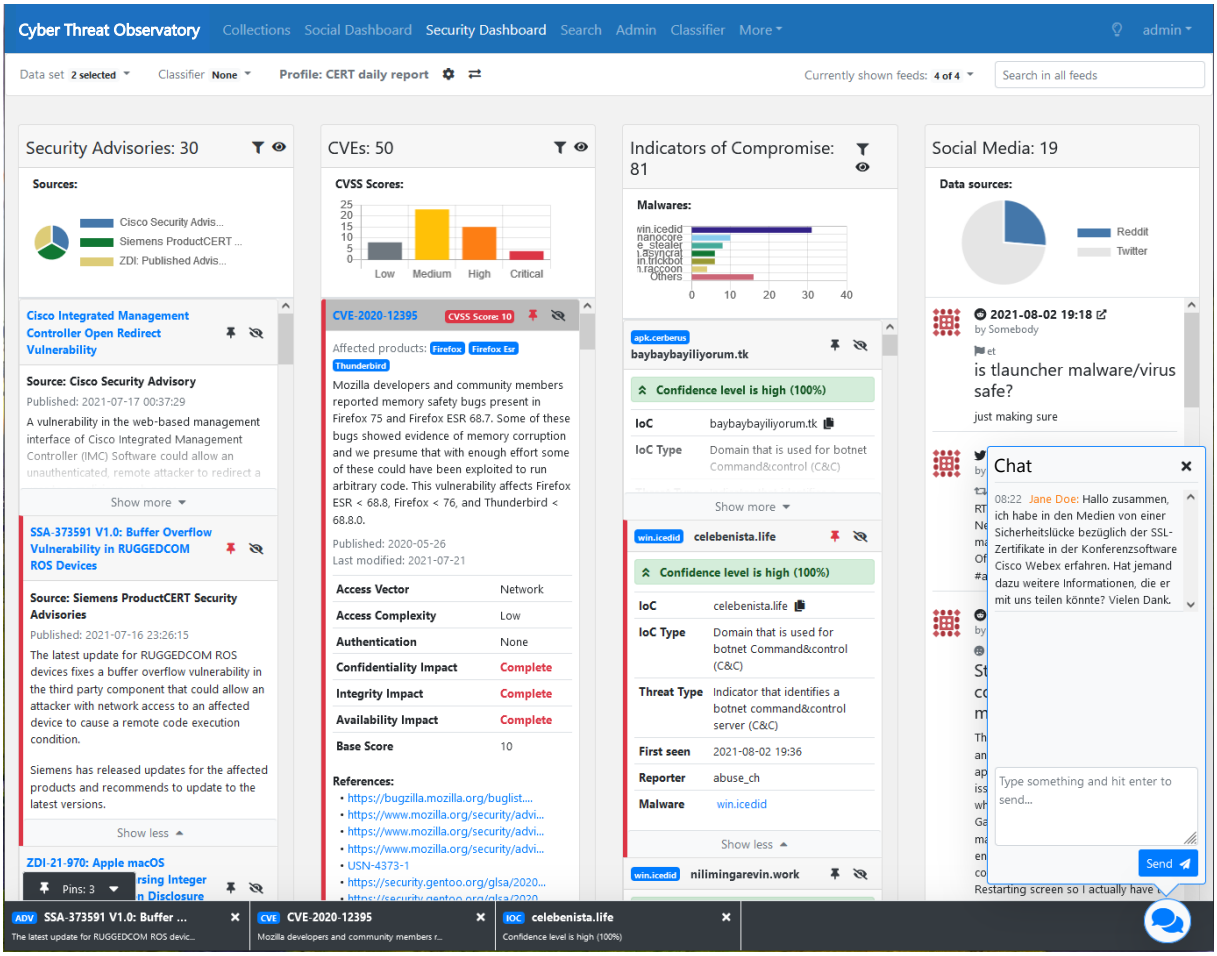

Figure 3. Interface of the Cyber Threat Observatory, a cross-platform cybersecurity dashboard featuring security advisories, vulnerability reports, indicators of compromise, and social media feeds.

The interface as depicted in Figure 3 comprises up to four feeds with security advisories, CVEs, IoCs, and social media data. The security advisories are embedded via RSS feeds provided by software and hardware vendors, and the API of the NVD database is used to populate the CVE feed with documented vulnerabilities. Furthermore, we decided to test using the ThreatFox platform to receive IoCs and individual platform APIs to gather information from social media (e.g., Reddit or Twitter). For each feed, specific charts and a different set of available and characteristic information is displayed per entry (e.g., a textual description and the CVSS score for CVEs, amongst others; the author, body of text, and retweets of a Twitter post) (#6). The displayed data set can be selected in the upper left corner and is based on predefined individual parameter settings used to query the various sources. On demand, users can display or hide individual or all feed entries and pin important entries that are then highlighted and displayed in the black bottom pin menu for quick access (#7). In order to filter the displayed information, users can either click on the interactive charts (e.g., on the critical bar to only show critical vulnerabilities within the CVE feed) or open an advanced filtering menu with additional options (e.g., also filtering by the CVE id or the affected product of a vulnerability) (#8). In the top-right corner, a full text search field allows searching for keywords across the different feeds simultaneously (#9). To make the collection and processing of data in the application transparent, each displayed information contains a link to the external source (e.g., the NVD for the vulnerabilities) (10). Additionally, we added a mockup chat interface in the bottom-right corner to evaluate the idea of CERT members exchanging knowledge on current cyber incidents or important vulnerabilities.

5 Results II: Demonstration and Evaluation

The evaluation design is based on the notion of situated evaluation in which qualitative methods are used to draw conclusions about the real-world use of technology involving domain experts (Twidale et al., 1994). The aim is not only to measure the relationship between evaluation goals and outcomes but also to derive subjective views from experts about how useful and relevant the technology might be in use. We evaluated the Cyber Threat Observatory with 12 users (E1-12) in sessions of 60 minutes on average using a web conferencing tool. The evaluation was conducted with a focus on operational staff, including five cyber incident managers and two information security offers, but only one team leader. We also invited three domain experts from (I) human-computer interaction to discuss the design and usability of the dashboard, (II) information security to investigate the integration and interrelation of different cybersecurity data streams, and (III) artificial intelligence to evaluate the potential of AI models automatically to assess the credibility of information or filter out irrelevant and redundant information. All interviews were recorded and subsequently transcribed with consent. All interviews were conducted in German and the following statements were translated into English.

The evaluation itself was based on a scenario-based walkthrough coupled with subsequent semi-structured interviews. The walkthrough comprised three tasks; to search for specific information on suspicious activity from three IP addresses, to check for critical vulnerabilities of a specific browser version, and to answer a chat request regarding SSL certificate issues on a conferencing software. In all four feeds, data was prepared so that the users could interact with all types of data during the course of the evaluation. Following the think-aloud protocol (McDonald et al., 2012), participants were asked to express their thoughts while completing the tasks. The semi-structured interviews which followed were intended to encourage reflection on the evaluation process. The twelve questions were specifically oriented towards the overall perceived usability, provided types of information, visual presentation of the dashboard, search and filter functionality, prioritization of relevant information, credibility assessment of data and sources, integration with communication tools, generation of reports, cross-platform information integration, the usefulness of the tool for daily work, further features or potentials, as well as challenges of the adoption of such tool. In accordance with the prior interview analysis, we conducted an inductive qualitative content analysis (Mayring, 2000). The first and second author independently employed open coding (Strauss & Corbin, 1998) to gather data into approximate categories reflecting the issues raised by respondents based on repeated readings of the data and its organization into similar statements. In multiple sessions, the authors compared their categories and discussed them until consensus was achieved.

5.1 General Feedback, Data Presentation, and Usability of the Dashboard

The first impression of the dashboard was generally positive among all participants. Many participants commented that they currently have to obtain much or all of their data manually from different sources or use several tools for this purpose. Therefore, all participants welcomed the integration of the most relevant data sources in one dashboard: "Above all, I like the fact that this information is already prepared, and you don't have to remember everything yourself in your head, I might see all the cross-references directly here. Even if, e.g., I enter something in this "search all feeds" I just see that there's something about "[software]" in all areas. So, I think it makes a lot of sense to have a unified tool that holds all the information" (E03, 45:33). However, E02, E03, and E06 also expressed concern that the initial amount of data displayed may be too large and that the tool may overwhelm the user. E02 also notes that there is often limited staff available to oversee a large amount of data: "The only problem is, in our case, it is just a half position dealing with this around the clock and that was simply far too much information. Because when it really gets busy, the art is to find out the information that is really important for someone sitting at the dashboard. If it's too much, it's no longer so goal-oriented" (E02, 07:06). Still, other participants liked the amount of information displayed and the way it is divided up.

Most participants think the dashboard provides a quick overview of the collected data. The diagrams in the header of each feed are considered very helpful by E02. E08, E09, and E10 would instead prefer a different chart in the social media feed, as they do not find it as important to know how many entries come from which social media page. Several participants reinforce this by stating they almost exclusively use Twitter as a social media source. E04 could imagine a display of further charts, such as the frequency of posts over a certain period. E10 suggests a diagram that shows how many times a keyword was found in all datasets. Although E01 feels that the dashboard is sufficiently clear, he imagines that in practice the clarity of the dashboard could be lost when significantly more data is loaded. For example, E03, E07, and E08 suggest that all entries should be initially collapsed and be expanded as needed: "[...] so at the beginning it's quite overwhelming, I would prefer to have it folded or even just the overview things and I can then look for the things myself [...]" (E03, 22:47). However, E08 counters that this could make it necessary to unfold many entries to check their relevance. The feed layout is considered reasonable by E01, E02, E04, E07, and E10. If additional data sources would be included, E02 and E10 would swap out more irrelevant feeds rather than adding a fifth or sixth column, as they feel four columns are ideal for usual display sizes. These participants also liked the option of hiding the feeds not in use. In addition, E07 would like to minimize individual feeds for a short time to focus on another feed.

5.2 Assessment of the Data Sources and Types of Information

In general, the participants expressed positive attitudes regarding the data feeds, but it is apparent that they have very different requirements for the type of data and its presentation. For example, E02 likes the integration of a *CVE feed* from NVD as the most common data source, but E07 and E10 would instead like to integrate vulnerability reports from the BSI. However, E05 and E10 not consider it useful to display all CVEs and would like to have some pre-filtering based on the products used in the own organization. The CVEs should then be filtered automatically according to a specified product list. Furthermore, E07 would like information on whether a CVE is new or was only updated. For E05 and E06, the *IoC feed* is not relevant because they already use another more advanced tool for IoCs. E08 and E09 also already employ tool support for IoCs, but generally like the integration of IoCs into the dashboard. However, E02 does not use a comparable tool yet. He sees great advantages with the IoC feed since he could enter the data from this feed directly into the firewall configuration. Still, E01, E03, and E10 miss more information about the reporter or more references to the IoCs in general.

Regarding the *security advisory feed*, E07, E08, E09, and E10 remark that they already have a list of websites they regularly check for new advisories. Besides RSS entries, they want to be able to add these websites as sources for the feed. In contrast, E11 considers the maintenance of advisory sources too time-consuming and would rather like to have an extensive predefined list of advisories. He would then prefer to filter this list himself in the dashboard. Since not all vendors provide RSS feeds for their

advisories, E05 has concerns about whether all the necessary sources can be integrated into the tool, thus requiring manual checking: "Especially many smaller manufacturers, and this is very annoying, have neither an RSS feeds nor a mailing list. They publish a new version and don't even say that there was a security gap in their software" (E05, 28:10). E04 and E06 suggest that CVEs linked in security advisories should be highlighted and connected to the respective CVE feed entries while duplicates are filtered out. Moreover, E01 and E07 like the display of CVSS scores in the CVE feed but miss a similar criticality measure for security advisories. While E01 would rather define the criticality manually, E07 would prefer to extract it automatically from the advisories. The *social media feed* is seen as particularly useful by some participants (e.g., E05, E06, and E08), while others state that they would not need it for their work, as the topic of social media plays a marginal or no role in their daily work (e.g., E10). E01, E05, and E06 wish to define a list of trusted cybersecurity experts, whose posts are highlighted in the feed or even displayed in a separate feed as E06 suggests.

Many participants stated that they already have some tools that provide them some of the dashboard's information, but they are not aware of any tool that collects and visualizes information from multiple sources. However, five participants would like to see some connection between the feeds, which might help them with establishing relationships between pieces of information and getting a better overview of the overall situation: "What is much more relevant to me is if we could get these, let's say, security advisories, CVSS, social media, to talk to each other in a logic, as I described. If a relevant security researcher writes something about [software], if I see a CVSS score of ten, and then that also shows up in the security advisories, then that has to flash deep red" (E06, 44:34). Moreover, participants suggested the integration of additional data sources. Four participants would like to integrate a ticket system they use in their organization to view the processing state of an incident, E03 would like to integrate other vulnerability databases besides the NVD, and E05 regularly checks press publications like Heise Security, which is why he would welcome such data sources in the dashboard: "Because when Heise Security picks up something, then I definitely know it's already 6 hours old at least, usually. But it seems to be very important in any case. [...] So maybe you don't just take one source, but say, I'm also including the RSS feeds of some serious press organs here to emphasize the score, the importance of a report" (E05, 25:45). Furthermore, E09 could also imagine incorporating the Metasploit database into the tool, but fears that the data might be too complex for the dashboard.

5.3 On the Usefulness of Search and Filter Functionality

In the next step, participants were also about the dashboard's search and filter functions. The global search field was rated positively by several participants, as it offers the possibility to search for specific terms across all feeds quickly. However, it was sometimes difficult for participants to figure out how to clear the search filter after a query in order to display all results again. The filter options for the individual feeds were often considered helpful, but numerous ideas were also expressed about which additional filters would be useful. For example, in the CVE feed, E01 would like to see a way to filter by manufacturers of products. For some places, E04 suggests rather offering a selection list instead of a free text field to avoid typos. Furthermore, E01 and E07 would also like to see the option to apply multiple filters of the same type to, e.g., filter for two products simultaneously in the CVE feed. E01, E09, and E10 would also find it useful to be able to predefine keywords or products in a kind of profile beforehand, which should then be selectable in the dashboard: "I would be useful to store and highlight products that are used in our organization. Information related to such products are certainly more relevant" (E10, 32:45).

In general, filter functions for the social media feed were missed, as they have not been implemented yet. The possibility to filter data sets by clicking on the charts was quickly discovered by some participants themselves, who found it helpful and intuitive. While generally filters are considered useful by most participants, E01 and E03 would tend to use the global search first, as they feel this is faster and easier than setting up filters in the individual feeds: "Exactly, I am so somehow a friend of it, when I search for things, I do that on the desktop PC... there I have an everywhere search. Then I enter a search term, and sometimes I have the feeling that I can find information faster than going

through any structures or hierarchies" (E01, 29:29). E03 and E12 would like to use Regex in the search field to filter the results without using the mouse. Moreover, E12 suggests that the search box should be designed to include as many standard features from Unix command lines as possible, such as a history like the one in Bash since CERT staff tend to be more technically inclined and work with terminals daily. Nevertheless, all functions should also be accessible with the mouse.

5.4 Further Wishes, Remarks, and Concerns

The question if such a tool could help with prioritization and relevance assessment was consistently answered positively. E03 and E07 see the search and filter functionalities in particular as a good support for these purposes. Besides, E05 would also like to see some data analysis, e.g., automatic filtering of duplicates and pattern recognition to help with the prioritization of content. While E03 and E04 indicated that the dashboard could also be used for credibility assessment, E02 and E07 rather do not see this as a task of such a tool. E09 would not unconditionally trust a tool for credibility assessment, especially for social media data, but would welcome additional information that supports the assessment of credibility. E03 imagines that a credibility analysis could also be used to identify trustworthy social media accounts. E02, however, thinks that with the pre-selection of trustworthy sources, a credibility analysis functionality is not needed in the tool anymore: "So the evaluation of the information, I do that by allowing or disallowing the sources. If I have a source that I don't like, then it doesn't come in. [...] This step, I do it at the beginning" (E02, 01:14:10).

With regard to the integrated chat mockup, most participants generally see a benefit in communicating with colleagues inside and outside their organization through chats. Most CERTs in Germany are able to communicate with each other via a chat platform. While E10 thinks integrating a chat feature is a good idea, E02 and E07 suggest that their chat tool is too extensive for integration since it offers different chat rooms and the possibility for private chats, which would take up much space in the dashboard and thus be rather distracting. E02 and E09 also express privacy concerns because chat histories should not be publicly known, unlike the rest of the data in the dashboard. E08 and E09 are not interested in a chat feature because they mostly communicate via e-mail or personally.

Participants were also asked whether they could imagine export and reporting functions in such a tool. All twelve participants generally consider export functions to be helpful. However, opinions on the design of exporting and reporting functions differ among participants. For example, E07, E08, and E09 would be satisfied with a simple export of records in list form as a PDF or Excel file. E03 would like to see the export of data in an open format and the ability to annotate records with further information, e.g., via a notes function. For E05, on the other hand, a pure PDF or Excel export would not be sufficient. Instead, an API that allows the retrieval of data from the security dashboard using self-developed software is seen as favorable. E10 notes that an export function may be needed only for certain feeds. The dashboard should allow the user to select the data to be exported, e.g., by specific keywords. E01, E02, and E04 can imagine exporting all pinned posts together. In urgent situations, however, E02 would also like to be able to export individual entries immediately or to send a collection of entries to a specific department: "If the thing is really highly critical, then of course I have to send it away immediately. With the federal government it was like that, I think they had eight categories, with eight different colors. That was simply the way it was with them. And what I know was red, was the firewalls. And then I pinned everything that I then felt was important for firewalls in red and that was sent together" (E02, 12:22).

6 Discussion and Conclusion

In this paper, we presented the design and evaluation of the Cyber Threat Observatory, an interactive dashboard for CERTs that allows to search and filter cyber threat information from security advisory feeds, CVEs, IoCs, and social media streams. By answering our research question on **design requirements and implications for a cross-platform cybersecurity tool to facilitate the cyber situational awareness of CERTs**, we present the main findings, design implications, limitations, and venues for future work based on our study.

6.1 Implications for Design

Overall, despite a multitude of constructive suggestions for extension and improvement, the Cyber Threat Observatory left a positive impression on most participants of our evaluation, and they could imagine continuing to use it in their everyday practice. By taking the perspective of cyber situational awareness, we identified six design implications regarding the cross-platform collection (D1, D2), algorithmic analysis (D3, D4), and exchange (D5, D6) of cyber threat information, which according to our DSR study with German state-level CERT employees contribute to an enhanced external threat awareness if realized in a properly designed artifact.

The **customizability of cyber threat data sources and filtering of displayed entities (D1)** was seen as the most crucial feature of the dashboard. With regard to data sources, it became apparent that some CERTs use other tools for processing IoCs and some had no interest in monitoring social media, highlighting the need to allow the selection of which data types should be displayed in the interface. Other participants collect their security advisories not only from RSS feeds but also from blogs or websites. Despite the varying structures of the latter, a further revision of the tool should explore the use of web scraping technologies (Stieglitz et al., 2018) to enhance the **modular integration of closed and public information sources (D2)**. Furthermore, some participants with technical expertise asked for the realization of a plug-in system to integrate relevant information sources (e.g., closed sources) on their own. While the participants valued the filtering by interactive charts and textual filter criteria (e.g., the affected hardware or software), some of them would prefer to use a cross-feed single search field with operators, regular expressions, and an autocomplete feature to repeat recent queries.

Although the dashboard currently contains data from four distinct source types, the only cross-platform interaction is facilitated by the global search field. Thus, our participants requested a stronger **interrelation between different cyber threat information feeds (D3)**. The evaluation showed a great need to find related information in other feeds quickly and easily. For example, CVE numbers are often referenced in security advisories. For instance, the dashboard could automatically detect these and display them in the CVE feed. By linking the information, CERT staff enhance relationship awareness and can better verify the relevance of a piece of information by comparing it to similar information from other data sources. Although the tool allows filtering for relevant information and displays information to facilitate the credibility assessment of content and sources, it lacks **intelligent algorithms for credibility assessment and threat prioritization (D4)**. Considering the large volumes of social big data generated in large-scale incidents (Olshannikova et al., 2017), the recent past saw a large body of research on using AI for clustering or topic modeling (Kolini & Janczewski, 2017), to detect events (Riebe, Wirth, et al., 2021), identify relevant information (Alam et al., 2019) or assess credibility (Viviani & Pasi, 2017; Zhou & Zafarani, 2020), which could be integrated and tailored to the domain of cybersecurity. However, even when following the principles of explainable AI (Samek et al., 2019), our participants stated that such algorithms may only be a useful addition but cannot replace the manual assessment of data.

Furthermore, the participants suggested a deeper **integration with organizational security software and systems (D5)** that are in use at their organization. For instance, some CERTs use a ticket system to track the status of their tasks and the evidence on cybersecurity threats and vulnerabilities collected via the dashboard would be useful to maintain and update their tickets. Moreover, some CERTs use infrastructure resource management (IRM) software, which could provide the IT resources (Weishäupl et al., 2015) used at the organization in order to automatically adapt the dashboard filters to relevant products. Regarding cyber situational awareness, such integration would strengthen the link between network and threat awareness (Franke & Brynielsson, 2014). Furthermore, the **export, sharing, and communication of relevant cyber threat data (D6)** were mentioned as important features. The pin feature was considered useful by most participants, but it was also requested to enable the sharing of pins with other users, as CERTs often want to share their insights on a specific topic with colleagues or even with other CERTs. The current version of the dashboard does not offer the option to export data. In addition to a structured and textual export of data records as a list, participants valued the idea of generating threat and vulnerability reports for clients or the management of an organization.

6.2 Contributions to the Knowledge Base

This paper provides an artifact contribution by the design and evaluation of the Cyber Threat Observatory. Existing research has highlighted the CERTs' need for better tool support (Van der Kleij et al., 2017) and even though our literature review revealed a variety of different tools for cyber incident response (Catakoglu et al., 2016; Mittal et al., 2016; Papp et al., 2015; West-Brown et al., 2003), they almost always focus on one specific data source and only rarely link them to other, thus not providing a cross-platform overview of cyber threat information. By discussing user requirements and outlining design implications for a tool designed to facilitate the collection and analysis of public cyber threat and vulnerability information for CERTs, we also provide empirical contributions to the knowledge base. Existing research on cyber situational awareness emphasizes the need to conduct more empirical research (Franke & Brynielsson, 2014), which is why we complement published empirical research on the collaborative, individual, and organizational needs of CERTs (Riebe, Kaufhold, et al., 2021; Van der Kleij et al., 2017) with insights on technology design. While existing studies focus more on cyber situational awareness at the network level (Franke & Brynielsson, 2014; Matta & Husák, 2021), our study contributes human-centered insights on the threat awareness level based on the real-time collection and analysis of publicly available threat information (Husák et al., 2020; Ruefle et al., 2014). In order to enhance the Cyber Threat Observatory with a credibility assessment module, it seems promising to integrate and evaluate the indicators for automated credibility assessment (Basyurt, Fromm, Stieglitz, et al., 2022). Furthermore, we complement existing findings on the collection and analysis of cyber threat information (Basyurt, Fromm, Kuehn, et al., 2022). In following design iterations, these empirical insights can serve as a foundation to achieve a higher DSR contribution level, including abstract models and design principles on how to gather, process and visualize cyber threat information from multiple open and public data sources, beyond the situated implementation of this artifact (Gregor & Hevner, 2013).

6.3 Limitations and Future Work

As this paper is subject to several limitations, potentials for future research can be derived. First, our research was conducted with German CERT employees at state and federal level. It is likely that enterprise CERTs, product CERTs, or incident response providers have different sets of user needs and design requirements (Ruefle et al., 2014). Differences in national capabilities and legislations likely influence the activity, competences, and tool utilization of CERTs (Boeke, 2018; Collier, 2017). Further in-depth research is required to compare different analytical technologies (e.g., with regard to the degrees of automation and modularity) and collaborative practices (e.g., cooperations or service level agreements) across nations on a fine-grained level. Second, cyber emergency response is a global problem requiring extensive collaboration and comparable practices across CERTs on a national and international level (Pethia & Wyk, 1990; Slayton & Clarke, 2020). On average, more than ten CERTs exist per European country (ENISA, 2020), highlighting the necessity for standardized threat intelligence exchange, transparency, and trust among teams. Third, despite the positive reception of the dashboard, it should benefit from another design iteration to integrate the enhanced feature wishes of the evaluation's participants and to enable a stronger integration with existing CERT systems, combining the issues of network and threat awareness (Franke & Brynielsson, 2014). From a design perspective, this will allow the integration of components for automated credibility assessment (Basyurt, Fromm, Stieglitz, et al., 2022) and cyber threat communication (Basyurt, Fromm, Kuehn, et al., 2022), amongst others. The evaluation should then be planned to integrate the viewpoints of further (international) CERT staff and the rigor definition of evaluation criteria, such as the pragmatic and hedonic value of the tool (Hassenzahl et al., 2003), to enhance the generalizability of results.

Acknowledgements. This work has been co-funded by the German Federal Ministry of Education and Research (BMBF) in the research project CYWARN (13N15407) (Kaufhold et al., 2021) as well as by the BMBF and the Hessian Ministry of Higher Education, Research, Science and the Arts (HMWK) within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

Abuse.ch. (2021). *ThreatFox: Share Indicators of Compromise*. https://threatfox.abuse.ch/

Alam, F., Ofli, F., & Imran, M. (2019). Descriptive and visual summaries of disaster events using artificial intelligence techniques: Case studies of Hurricanes Harvey, Irma, and Maria. *Behaviour & Information Technology (BIT)*, 1–31. https://doi.org/10.1080/0144929X.2019.1610908

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers and Security*, *74*, 144–166. https://doi.org/10.1016/j.cose.2018.01.001

Avvenuti, M., Cresci, S., Del Vigna, F., Fagni, T., & Tesconi, M. (2018). CrisMap: A Big Data Crisis Mapping System Based on Damage Detection and Geoparsing. *Information Systems Frontiers*, *20*(5), 993–1011. https://doi.org/10.1007/s10796-018-9833-z

Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. *Australasian Conference on Information Systems (ACIS)*, 1–12.

Bada, M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2014). Computer Security Incident Response Teams (CSIRTs): An Overview. *The Global Cyber Security Capacity Centre*.

Basyurt, A., Fromm, J., Kuehn, P., Kaufhold, M.-A., & Mirabaie, M. (2022). Help Wanted—Challenges in Data Collection, Analysis and Communication of Cyber Threats in Security Operation Centers. *Proceedings of the International Conference on Wirtschaftsinformatik (WI)*.

Basyurt, A., Fromm, J., Stieglitz, S., & Mirbabaie, M. (2022, January 17). Credibility of Cyber Threat Communication on Twitter – Expert Evaluation of Indicators for Automated Credibility Assessment. *Wirtschaftsinformatik 2022 Proceedings*. https://aisel.aisnet.org/wi2022/human_rights/human_rights/2

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449–464. https://doi.org/10.1111/gove.12309

Booth, H., Rike, D., & Witte, G. (2013). *The National Vulnerability Database (NVD): Overview*. *December*.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2008). Economic Impact Cyber-Attacks. In *Congressional research service documents, CRS RL32331 (Washington DC)*.

Catakoglu, O., Balduzzi, M., & Balzarotti, D. (2016). Automatic extraction of indicators of compromise for web applications. *25th International World Wide Web Conference, WWW 2016*, 333–343. https://doi.org/10.1145/2872427.2883056

Collier, J. (2017). Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom. In M. Taddeo & L. Glorioso (Eds.), *Ethics and Policies for Cyber Operations* (pp. 187–212). Springer International Publishing. https://doi.org/10.1007/978-3-319-45300-2_9

Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber Threat Intelligence: Challenges and Opportunities. In A. Dehghantanha, M. Conti, & T. Dargahi (Eds.), *Cyber Threat Intelligence* (pp. 1–6). Springer International Publishing. https://doi.org/10.1007/978-3-319-73951-9_1

Davis, J. S. I., Boudreaux, B., Welburn, J. W., Ogletree, C., McGovern, G., & Chase, M. S. (2017). *Stateless Attribution: Toward International Accountability in Cyberspace*.

Dorantes, C., Mcleod, A., Dietrich, G., Dorantes, C. A., & Dietrich, G. B. (2006). Cyber-Emergencies: What Managers Can Learn From Complex Systems and Chaos Theory. *Americas Conference on Information Systems (AMCIS)*, 1–12.

Drodt, M., Pagel, L., & Biedorf, T. (2018). Einbindung Datenschutz und Betriebsrat beim Aufbau eines SIEM. In M. Bartsch & S. Frey (Eds.), *Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden* (pp. 271–284). Springer Fachmedien. https://doi.org/10.1007/978-3-658-21655-9_22

Ehrenfeld, J. M. (2017). WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *Journal of Medical Systems*, *41*(7), 10916. https://doi.org/10.1007/s10916-017-0752-1

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

ENISA. (2020). *CSIRTs by Country—Interactive Map*. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

ENISA. (2021). *ENISA Threat Landscape 2021. April 2020 to mid-July 2021*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness—A systematic review of the literature. *Computers and Security*, *46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*(2), 337–355.

Gutzwiller, R., Dykstra, J., & Payne, B. (2020). Gaps and Opportunities in Situational Awareness for Cybersecurity. *Digital Threats*, *1*(3). https://doi.org/10.1145/3384471

Hassenzahl, M., Burmester, M., & Koller, F. (2003). AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität. In G. Szwillus & J. Ziegler (Eds.), *Mensch & Computer 2003: Interaktion in Bewegung* (pp. 187–196). Vieweg+Teubner Verlag. https://doi.org/10.1007/978-3-322-80058-9_19

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Husák, M., Jirsík, T., & Yang, S. J. (2020). SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In *ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland* (pp. 1–12). Association for Computing Machinery. https://doi.org/10.1145/3407023.3407062

Kaufhold, M.-A. (2021). *Information Refinement Technologies for Crisis Informatics: User Expectations and Design Principles for Social Media and Mobile Apps*. Springer Vieweg. https://doi.org/10.1007/978-3-658-33341-6

Kaufhold, M.-A., Bayer, M., & Reuter, C. (2020). Rapid relevance classification of social media posts in disasters and emergencies: A system and evaluation featuring active, incremental and online learning. *Information Processing & Management*, *57*(1), 1–32.

Kaufhold, M.-A., Fromm, J., Riebe, T., Mirbabaie, M., Kuehn, P., Basyurt, A. S., Bayer, M., Stöttinger, M., Eyilmez, K., Möller, R., Fuchß, C., Stieglitz, S., & Reuter, C. (2021). CYWARN: Strategy and Technology Development for Cross-Platform Cyber Situational Awareness and Actor-Specific Cyber Threat Communication. *Workshop-Proceedings Mensch Und Computer*. Mensch und Computer, Bonn. https://doi.org/10.18420/muc2021-mci-ws08-263

Kaufhold, M.-A., Rupp, N., Reuter, C., & Habdank, M. (2020). Mitigating Information Overload in Social Media during Conflicts and Crises: Design and Evaluation of a Cross-Platform Alerting System. *Behaviour & Information Technology (BIT)*, *39*(3), 319–342. https://peasec.de/paper/2020/2020_KaufholdRuppReuterHabdank_MitigatingInformationOverload_BIT.pdf. https://doi.org/10.1080/0144929X.2019.1620334

Kolini, F., & Janczewski, L. (2017). Clustering and Topic Modelling: A New Approach for Analysis of National Cyber security Strategies. *Pacific Asia Conference on Information Systems (PACIS)*, 1–12.

Krstić, M., Čabarkapa, M., & Jevremović, A. (2019). Machine Learning Applications in Computer Emergency Response Team Operations. *2019 27th Telecommunications Forum (TELFOR)*, 1–4. https://doi.org/10.1109/TELFOR48224.2019.8971040

Kuehn, P., Bayer, M., Wendelborn, M., & Reuter, C. (2021). OVANA: An Approach to Analyze and Improve the Information Quality of Vulnerability Databases. *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES)*, 11. https://doi.org/10.1145/3465481.3465744

Lekkas, D., & Spinellis, D. (2005). Handling and reporting security advisories: A scorecard approach. *IEEE Security Privacy*, *3*(4), 32–41. https://doi.org/10.1109/MSP.2005.98

Maness, R. C., & Valeriano, B. (2016). The Impact of Cyber Conflict on International Interactions. *Armed Forces and Society*, *42*(2), 301–323. https://doi.org/10.1177/0095327X15572997

Matta, L., & Husák, M. (2021). A Dashboard for Cyber Situational Awareness and Decision Support in Network Security Management. *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 716–717.

Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *2017 European Intelligence and Security Informatics Conference (EISIC)*, 91–98. https://doi.org/10.1109/EISIC.2017.20

Mayring, P. (2000). Qualitative Content Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *1*(2), Article 2. https://doi.org/10.17169/fqs-1.2.1089

McDonald, S., Edwards, H. M., & Zhao, T. (2012). Exploring think-alouds in usability testing: An international survey. *IEEE Transactions on Professional Communication*, *55*(1), 2–19. https://doi.org/10.1109/TPC.2011.2182569

Mittal, S., Das, P. K., Mulwad, V., Joshi, A., & Finin, T. (2016). CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities. *Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2016*, 860–867. https://doi.org/10.1109/ASONAM.2016.7752338

Mullins, R., Nargi, B., & Fouse, A. (2020). Understanding and Enabling Tactical Situational Awareness in a Security Operations Center. In I. Corradini, E. Nardelli, & T. Ahram (Eds.), *Advances in Human Factors in Cybersecurity* (pp. 75–82). Springer International Publishing.

Olshannikova, E., Olsson, T., Huhtamäki, J., & Kärkkäinen, H. (2017). Conceptualizing Big Social Data. *Journal of Big Data*, *4*(1), 1–19. https://doi.org/10.1186/s40537-017-0063-x

Papp, D., Ma, Z., & Buttyan, L. (2015). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. *13th Annual Conference on Privacy, Security and Trust (PST)*, 145–152.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pethia, R. D., & Wyk, K. R. van. (1990). *Computer Emergency Response—An International Problem*. Pittsburgh, Pa.: CERT Coordination Center., Software Engineering Institute, Carnegie Mellon University.

Plohmann, D., Clauss, M., Enders, S., & Padilla, E. (2017). Malpedia: A Collaborative Effort to Inventorize the Malware Landscape. *Proceedings of the Botconf*.

Pulsedive. (2021). *Pulsedive: Threat Intelligence Made Easy*. https://pulsedive.com/

Reuter, C., Ludwig, T., Kotthaus, C., Kaufhold, M.-A., von Radziewski, E., & Pipek, V. (2016). Big Data in a Crisis? Creating Social Media Datasets for Emergency Management Research. *I-Com: Journal of Interactive Media*, *15*(3), 249–264. https://doi.org/10.1515/icom-2016-0036

Riebe, T., Kaufhold, M.-A., & Reuter, C. (2021). The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study. *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing, CSCW*, 1–26. https://doi.org/10.1145/3479865

Riebe, T., Wirth, T., Bayer, M., Kuehn, P., Kaufhold, M.-A., Knauthe, V., Guthe, S., & Reuter, C. (2021). CySecAlert: An Alert Generation System for Cyber Security Events Using Open Source Intelligence Data. *Information and Communications Security*, 429–446. https://link.springer.com/chapter/10.1007/978-3-030-86890-1_24. https://doi.org/10.1007/978-3-030-86890-1_24

Rodriguez, A., & Okamura, K. (2019). Generating Real Time Cyber Situational Awareness Information Through Social Media Data Mining. *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, 502–507. https://doi.org/10.1109/COMPSAC.2019.10256

Rodriguez, L. G. A., Trazzi, J. S., Fossaluza, V., Campiolo, R., & Batista, D. M. (2018). Analysis of Vulnerability Disclosure Delays from the National Vulnerability Database. *Anais Do Workshop de Segurança Cibernética Em Dispositivos Conectados (WSCDC)*, *1*, 1–14.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer security incident response team development and evolution. *IEEE Security and Privacy*, *12*(5), 16–26. https://doi.org/10.1109/MSP.2014.89

Sabottke, C., Suciu, O., & Dumitras, T. (2015). Vulnerability disclosure in the age of social media: Exploiting twitter for predicting real-world exploits. *Proceedings of the 24th USENIX Security Symposium*, 1041–1056.

Samek, W., Montavon, G., Vedaldi, A., Hansen, L. K., & Müller, K.-R. (2019). *Explainable AI: interpreting, explaining and visualizing deep learning*. Springer Nature.

Skopik, F., Páhi, T., & Leitner, M. (Eds.). (2018). *Cyber Situational Awareness in Public-Private-Partnerships*. Springer Vieweg. https://doi.org/10.1007/978-3-662-56084-6

Slayton, R., & Clarke, B. (2020). Trusting infrastructure: The emergence of computer security incident response, 1989-2005. *Technology and Culture*, *61*(1), 173–206. https://doi.org/10.1353/tech.2020.0036

Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Social media analytics – Challenges in topic discovery, data collection, and data preparation. *International Journal of Information Management*, *39*, 156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

Strauss, A. L., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage Publications.

Twidale, M., Randall, D., & Bentley, R. (1994). Situated evaluation for cooperative systems. *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*, 441–452. https://doi.org/10.1145/192844.193066

Van der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer security incident response team effectiveness: A needs assessment. *Frontiers in Psychology*, *8*(DEC), 1–8. https://doi.org/10.3389/fpsyg.2017.02179

Viviani, M., & Pasi, G. (2017). Credibility in social media: Opinions, news, and health information—A survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1209--n/a. https://doi.org/10.1002/widm.1209

Wagner, C., Dulaunoy, A., & Iklody, A. (2016). MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. *ACM Workshop on Information Sharing and Collaborative Security (WISCS)*, 49–56. https://doi.org/10.1145/2994539.2994542

Weishäupl, E., Yasasin, E., & Schryen, G. (2015). IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review. *European Conference on Information Systems (ECIS)*, 1–19.

West-Brown, M. J., Stikvoort, D., Killcrece, G., Reufle, R., & Zajicek, M. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs)*.

Wobbrock, J. O., & Kientz, J. A. (2016). Research contribution in human-computer interaction. *Interactions*, *23*(3), 38–44. https://doi.org/10.1145/2907069

Zhou, X., & Zafarani, R. (2020). A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities. *ACM Computing Surveys*, *53*(5). https://doi.org/10.1145/3395046