‘We Do Not Have the Capacity to Monitor All Media’: A Design Case Study on Cyber Situational Awareness in Computer Emergency Response Teams

Marc-André Kaufhold
Thea Riebe
Markus Bayer
Christian Reuter
Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC)
Darmstadt, Germany
{kaufhold,riebe,bayer,reuter}@peasec.tu-darmstadt.de

ABSTRACT

Computer Emergency Response Teams (CERTs) provide advisory, preventive and reactive cybersecurity services for authorities, citizens, and businesses. However, their responsibility of monitoring, analyzing, and communicating cyber threats have become challenging due to the growing volume and varying quality of information disseminated through public channels. Based on a design case study conducted from 2021 to 2023, this paper combines three iterations of expert interviews, design workshops and cognitive walkthroughs to design an automated, cross-platform and real-time cybersecurity dashboard. By adopting the notion of cyber situational awareness, the study extracts user requirements and design heuristics for enhanced threat awareness and mission awareness in CERTs, discussing the aspects of source integration, data management, customizable visualization, relationship awareness, information assessment, software integration, (inter-)organizational collaboration, and communication of stakeholder warnings.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; • **Security and privacy** → *Usability in security and privacy*.

KEYWORDS

Cyber Situational Awareness, Security and Privacy, Computer Emergency Response Teams, Design Case Studies

ACM Reference Format:
Marc-André Kaufhold, Thea Riebe, Markus Bayer, and Christian Reuter. 2024. ‘We Do Not Have the Capacity to Monitor All Media’: A Design Case Study on Cyber Situational Awareness in Computer Emergency Response Teams. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI ’24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3613904.3642368

CHI ’24, May 11–16, 2024, Honolulu, HI, USA
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642368

1 INTRODUCTION

The importance of cybersecurity is not only motivated by the ever advancing digitization and networking of infrastructures and society, but also by the increasing frequency and sophistication of cyberattacks [29]. Recognizing the need for incident management, Computer Emergency Response Teams (CERTs) have been established in public and private sectors [40, 67] to provide a range of services for authorities, citizens, and enterprises, including *reactive measures* such as issuing alerts, managing incidents, vulnerabilities, and artifacts, *proactive actions* like monitoring intrusion detection systems and developing security tools, and *security quality management*by risk analysis, security consultation, education, and certification [58]. To provide these services, CERTs must first establish cyber situational awareness by monitoring, analyzing, and communicating cyber threats and security vulnerabilities [16].

Coined by the theory of situational awareness [15], cyber situational awareness comprises the three elements of network, threat, and mission awareness [46]. Yet, the often collaborative establishment and maintenance of cyber situational awareness is becoming more difficult due to the increasing volume and varying quality information accessible through public channels, including feeds, social media, vulnerability databases, third-party services, and websites [2, 7, 14, 29]. Empirical studies with German state CERTs indicate a lack of efficient mechanisms for extracting and seamlessly incorporating real-time threat intelligence, such as indicators of compromise, security advisories, social media alerts, and vulnerability reports [58]. Moreover, CERTs often encounter irrelevant, duplicated and occasionally implausible information [4], limiting the time available to align network awareness and threat intelligence insights with the organization’s mission or business.

While considering the goals, roles, and information needs of operators during design processes, their involvement in evaluation and appropriation studies is central to ensure that technologies actually enhance cyber situational awareness [22]. However, we identified a lack of design and evaluation studies focusing on tools for the cross-platform collection, analysis and communication of cyber threats and security vulnerabilities [29, 53]. Thus, taking the lens of Human-Computer Interaction (HCI), this paper examines the following research question: **What are user requirements and design heuristics for a cross-platform cybersecurity tool to facilitate the cyber situational awareness of CERTs?**

Based on a literature review (Section 2) and the framework of design case studies (Section 3), which follows the approach of Grounded Design [61] and has been previously employed in various HCI studies [76, 77], this paper conducts three iterations of (I) empirical pre-studies to understand existing practice in German state CERTs (Section 4), (II) design interventions to apply novel technology to identified needs and problems (Section 5), and (3) cognitive walkthroughs to reflect the technology with practitioners and identify potential for future improvement (Section 6). Our objective is to improve the time-consuming process of incident handling and daily reporting in CERTs, a process frequently compounded by the influx of irrelevant, repetitive, and implausible information. Thus, the designed artifact serves to facilitate the automated, real-time, and cross-platform management of cybersecurity data, thereby enhancing the cyber situational awareness of CERTs. Finally, we discuss design heuristics (Section 7) and provide a conclusion (Section 8), outlining empirical and artifact contributions:

- First, we provide empirical insights into the practices of German state CERTs, outlining user requirements for the design of technology conducive to cyber situational awareness.
- Second, we provide an artifact contribution by the design of our real-time monitoring dashboard for gathering, analyzing, and communicating cyber threat information.
- Third, we provide empirical insights by evaluating artifacts and subsequently discussing design heuristics to enhance threat awareness and mission awareness by technology.

2 RELATED WORK

Cyber situational awareness describes a level of understanding possessed by individuals that allows them to perceive pertinent elements in the cyber environment within a defined timeframe and spatial context, interpret their significance, and anticipate their future status [26]. The term commonly refers to understanding events in one's own network, yet CERTs must extend their scope "to gain a common operational picture of the threat environment in which the constituency is operating" [62, p. 17]. This entails not solely internal details such as network awareness, but also external threat intelligence such as ongoing events, emerging vulnerabilities, potential remedies, and novel technologies. The role of incident response is therefore to protect the organization's field from attacks, requiring mission awareness [46], and to restore the integrity of that shield after an attack [2].

2.1 Organizational Network Awareness

In most cases, the primary task of CERTs lies in the protection of their respective authority, enterprise or organization against cyberattacks, requiring awareness of their used infrastructure and networks [62]. The establishment of network awareness thus requires understanding the structure of organizational networks, management of all assets and configurations, robust patch and upgrade management, as well as routine vulnerability auditing to prevent exploitation [46]. In accordance, several categories of tools have been established in organizational practice [41], such as security information and event management (SIEM) for the detection, aggregation and real-time analysis of security related information, as well as intrusion detection and prevention systems (IDPS) to prevent organizational or societal damage from cyberattacks.

Furthermore, research approaches such as Bubblenet [51], CRUSOE [27], InSight2 [37], MAD [3] or Situ [19], combine algorithms and visualizations for visualizing network traffic, detecting anomalies or attacks, identifying conspicuous patterns, comparing network activities with known vulnerabilities, or providing recommendations for resilient configurations of the IT infrastructure. In most cases, their central component constitutes a dashboard to provide an overview, facilitate filtering and zooming, and display details on demand [29]. Sometimes, they integrate explainable approaches which seek to allow "a better comprehension of the attack status and its probable evolution" [3] or provide "context to help operators understand why [events] are anomalous" [19].

2.2 External Threat Awareness

Still, CERTs need to overview the general threat landscape to align organizational security measures and provide services to external clients, requiring the identification of suspicious behaviors, current information on external threats, and the participation in information sharing communities to stay updated on new and emerging threats [46]. In terms of vulnerabilities, the National Vulnerability Database (NVD), Vulners and OpenCTI are examples of databases where Common Vulnerabilities and Exposures (CVEs) are applied for vulnerability classification [57] and the Common Vulnerability Scoring System (CVSS) is used to evaluate the severity of CVEs using base, temporal, and environmental metrics. In addition, numerous manufacturers release information regarding vulnerabilities and solutions through their own communication channels [44]. These security advisories provide information about new security vulnerabilities and recent security updates to their products.

Furthermore, threat intelligence platforms have been established to facilitate the collection and analysis of data regarding cyber threats [47]. For instance, Indicators of Compromise (IoCs) are also frequently employed by CERTs to enhance preemptive measures against attacks, and tools like AlliaCERT TI, ThreatFox, and Pulsedive were designed to streamline the aggregation and processing of IoCs [72]. MISP [75], in particular, is widely used by European CERTs for sharing, storing and correlating IoC of targeted attacks. In recent times, social media has emerged as a pivotal data source as cybersecurity experts can swiftly exchange threat-related information on these platforms, surpassing the pace of more formal communication channels [52]. For instance, CyberTwitter was introduced as a warning framework for IT security incidents [52], SONAR facilitates the automatic detection of cyber security events over Twitter [43], and another social media analytics system was designed for real-time gathering and categorizing security-related information from Twitter [60].

2.3 Collaborative Mission Awareness

Finally, mission awareness comprises an appropriate response to security events, to triage or prioritize security incidents with regard to their impact on the organization's mission or business, and anticipating threats and risks by conducting risk and readiness assessments [46]. The work of CERTs is demanding, notably, because it requires effective training [17, 70], coordination and information sharing both within the team and with external entities [24, 74]. In Germany, the collaboration between federal, state and private CERTs is emphasized as crucial for obtaining a clear understanding of the extent and seriousness of an incident and for making informed decisions regarding the appropriate response [66]. In the establishment of CERTs in Germany, it was observed that, in addition to a lack of time resources, insufficient mutual trust resulted in low levels of cooperation [58].

As a result, the efforts of cybersecurity experts involve a collection of diverse practices aimed at fostering a collective dedication to cybersecurity [36]. By now, German state CERTs are part of the Administrative CERT Network (VCV) which provides an information exchange platform for public administration, including a chat platform and regular meetings, thus offering an institutionalization of CERTs' partnerships [58]. Furthermore, besides the collaborative features of the operationally deployed MISP platform [75], the prototype Palantir [35] was designed to empower effective multi-site cyber incident response, encompassing a collaborative workspace for discussions and data exchange. Another prototype for shared cyber situational awareness facilitates the allocation of tasks within the team and presents the status of resources and incidents [54]. However, to the best of our knowledge, there are no approaches that support the communication of warning messages across various platforms and stakeholders [4].

2.4 Research Objective

Existing design research suggests that dashboards are a suitable tool for enhancing network and task awareness [54], but also for handling cross-platform social media data and the information overload triggered by the sheer amount of data available through such platforms [34]. It has also highlighted the CERTs' need for better and usable tool support [58, 74] and even though our literature review revealed a variety of different tools for cyber incident response [13, 52, 57], they mostly focus on one network awareness or a specific data source, thus not providing a cross-platform overview required for threat awareness and mission awareness [16, 46].

Furthermore, a systematic review of 54 cyber situational awareness visualization approaches highlighted that "only 15 studies that provide evidence for some form of user evaluations of the proposed visualization after the design is complete" [29]. By investigating these studies, we found that most evaluation studies are not tailored towards the CERT context, employ a low sample of participants, nor provide rich descriptions of user feedback. By conducting focus group discussions with participants from 15 national CERTs, a further study confirmed the need for a systematic evaluation of used tools [53]. We seek to address this research gap since evaluations, ideally embedded into a iterative and participatory design approach, are useful measures to refine identified user requirements, reflect assumptions of designers and researchers, tailor artifacts for practical utility, and derive practice-informed design knowledge [61, 64].

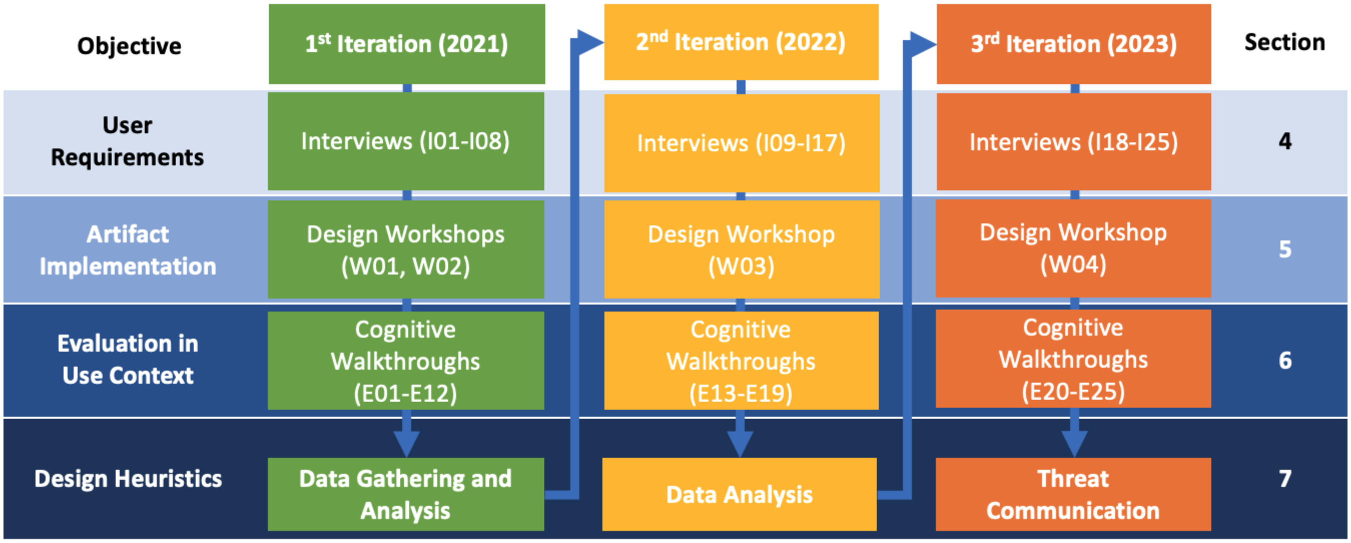
By discussing user requirements and outlining design heuristics, alongside an artifact designed to facilitate the collection, analysis and communication of public cyber threat and vulnerability information for CERTs, we also aim for empirical contributions to the knowledge base, complementing existing research on the collaborative, individual, and organizational needs of CERTs [58, 74] with insights on technology design. Thus, our study seeks to contribute human-centered insights on the threat awareness and mission awareness levels based on the real-time collection, analysis, and communication of publicly available threat information [26, 62].

3 METHODOLOGICAL FRAMEWORK

We followed the design research approach of Grounded Design, which seeks to design tentative artifacts to satisfy user requirements grounded in practice and generate new design ideas by means of formative evaluation of artifacts in use [61]. In HCI research, the elicitation of user requirements has been characterized as *fieldwork-informed design knowledge*, which are “highly prescriptive and implementable but are difficult to generalize beyond the settings where they have been explored” [64]. Conducting formative evaluations, then, is suitable to identify design heuristics, which represent a type of *practice-informed design knowledge* and seek to “incrementally improve the design of specific systems, [which are] usually depicted in terms of technology properties [and] maintain their generalizability for a class of technologies” [64]. Allowing us to generate both specialized user requirements and more generalizable design heuristics, Grounded Design advocates the use of design case studies [77] as a research framework, ideally comprising three key steps: (1) pre-study, (2) IT design, and (3) evaluation.

The empirical pre-study should offer insights into the social practices before any intervention occurs and aims to “describe already existing tools, media, and their usage” [76, p. 119]. This phase seeks to comprehend the current practices from technological, organizational, and social standpoints, employing empirical research methods to pinpoint issues, requirements, or opportunities for IT design [69]. Based on these, the IT design process should include the description of “the innovative IT artifact from a product as well as from a process perspective” [76, p. 119]. Through a participatory approach, design iterations may continue even after the technology is introduced to potential future users. Lastly, evaluation studies should "allow the transformative impact of certain functions and design options realized within the IT artifact to be analyzed” [76, p. 119]. To capture enduring changes in social practices stemming from the introduction of IT artifacts, ongoing dialogues and reflections with practitioners are necessary. Although there is a natural order of starting points of the phases, Wulf et al. [76] do not understand the phases as being strictly successive, but interrelated: “once an analysis of existing practices has started, it does not make sense to stop reflecting upon the momentum of the existing practice; rather, it continues throughout the design and the study of appropriation” [76, p. 120]. In this paper, we conducted three iterations of pre-study, evaluation, and design (Figure 1).

Although each iteration comprised the steps of pre-study, design and evaluation (i.e., vertically), we decided to report the cumulative findings of our pre-study, implementation and evaluation findings as separate sections (i.e., horizontally). In this way, we could combine methods and results of each step, but also give a short overview of what changed between iterations. While the empirical pre-study (Section 4) focuses on deriving user requirements, the implementation (Section 5) describes the features implemented across three iterations. Finally, the evaluation (Section 6) reports findings on the usability and functionality of the developed tool.



Objective	1st Iteration (2021)	2nd Iteration (2022)	3rd Iteration (2023)	Section
User Requirements	Interviews (I01-I08)	Interviews (I09-I17)	Interviews (I18-I25)	4
Artifact Implementation	Design Workshops (W01, W02)	Design Workshop (W03)	Design Workshop (W04)	5
Evaluation in Use Context	Cognitive Walkthroughs (E01-E12)	Cognitive Walkthroughs (E13-E19)	Cognitive Walkthroughs (E20-E25)	6
Design Heuristics	Data Gathering and Analysis	Data Analysis	Threat Communication	7

Figure 1: Three iterations of our design case study, comprising pre-studies to obtain user requirements, design interventions for the artifact implementation, and evaluation sessions in use contexts.

4 EMPIRICAL PRE-STUDY

The initial semi-structured interviews were designed to gain insights into the strategies and technologies used by German CERTs [18, 31]. The interview guidelines encompassed inquiries related to several key areas, including (1) the roles and affiliations of the interviewees, (2) their procedures for reporting cyber incidents, (3) methods for monitoring cyber incident data such as indicators of compromise, (4) processes for analyzing, prioritizing, and validating collected evidence, (5) collaborations among CERTs, and (6) how recommendations and warnings are communicated. After an initial round of eight interviews (n=8, I01-I08), the second round comprised nine (n=9, I09-I17) and the third round additional eight interviews (n=7, I18-25). Each interview session, conducted with the acceptance and informed consent of the participants, lasted approximately 60 minutes. We used a purposive sampling strategy [12] in order to primarily involve personnel on operational (e.g., incident managers as technology operators), but also tactical level (e.g., internal team leaders) among German state CERTs. In most instances after our initial e-mail request, we had a short e-mail or telephone exchange with the respective CERT's team leaders who then suggested personnel on operational level suitable to conduct interviews according to our research goals. In summary, our interviews comprised fifteen internal incident managers (I01, I04-I07, I14, I17-I24), six internal team leaders (I02, I08-I10, I12, I16), three external information security officers (I11, I12, I15), and one external public safety answering point (I13). Overall, participants (23 male, two female) from twelve organizations, including nine CERTs and three other organizations, were included in our pre-study interviews. Due to the sensitive nature of our organizational research, we did not elicit further demographic data from our participants and refrain from mapping them to explicit organizations.

The analysis was conducted by three researchers (two white male, one white female) from the domains of HCI, CSCW, and information security. We conducted a qualitative content analysis using the inductive category application step model, which involves a bottom-up process that includes open coding, as described by Mayring [48]. For the analysis and interpretation of the conducted interviews, we followed the approach of Kaiser [30], which includes several key steps: transcription of the interviews, coding of the transcribed text, identification of core statements, expansion of the data corpus, and finally, theoretical analysis and interpretation. Initially, we generated complete transcripts of the interview data and then analyzed the gathered documents and interview transcripts, applying emerging codes derived from the data. As our goal was to identify requirements as a means of fieldwork-informed design knowledge [64] for the design of novel and supportive technology, our main codes reflect the high-level requirements (N=16) outlined in Table 1, while our sub codes constitute more fine-grained requirements (N=83). These requirements categorized into the areas of gathering (4 main and 28 sub codes), analysis (8 main and 40 sub codes) and communication (4 main and 15 sub codes). During biweekly team meetings, we iteratively discussed and revised these codes until we reached consensus [49]. Qualitative reliability and validity was achieved by the iterative approach of the research design, which created a feedback loop between the derived requirements, their implementation and the evaluation by the experts during the cognitive walkthroughs throughout three iterations. Thus, subsequent iterations allowed us not only to reflect upon existing user requirements, but also to add and contextualize newly elicited requirements.

4.1 ICT Use in German State CERTs

An attempt to generalize ICT use of German state CERTs is depicted in Figure 2. The technology use can be roughly categorized by the three components of cyber situational awareness. First, in order to establish network awareness, incidents are either reported by

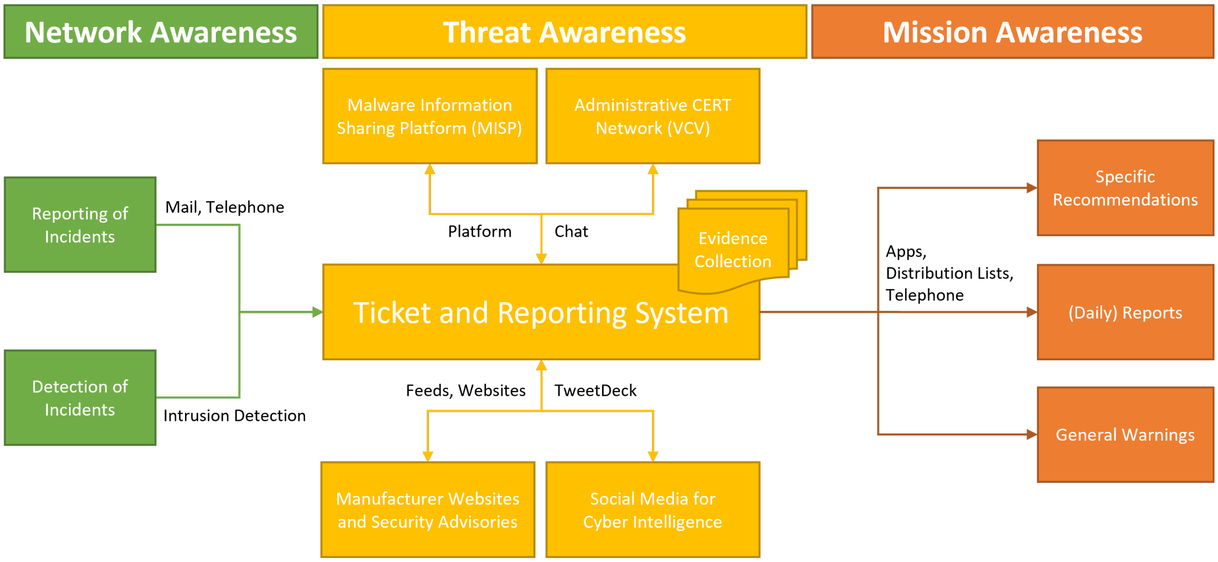


Figure 2: Example of a state CERT information and communication technology infrastructure.

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, threat awareness 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. Finally, in order to achieve mission awareness, 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 (if large ICT infrastructures are threatened).

4.2 Threat Awareness and Processing

In terms of awareness-focused evidence, the backbone of CERT activities lies in analyzing manufacturer websites and security advisories to identify IoCs. However, they are provided in different, regularly changing formats, thus **lacking interoperability**, which makes it hard to maintain software for structured acquisition and sometimes requires the development of individual scripts.

> "I work with Python and I deal with data streams among systems, e.g., parsing data from one system, transforming and cleaning the data received and finally pushing them to another system" (I23).

As a consequence, CERTs have to manually check manufacturer websites and security advisories on a daily basis for their reporting, which can consume up to two hours daily (I10, I12). Thus, the sheer volume of publicly available data may lead to information overload, requiring measures to **prioritize relevant information**.

> "Handling security alerts manually can be overwhelming. The volume can lead to information overload, and there’s a risk of missing critical details. Automation would greatly enhance our capabilities" (I19).

Since multiple security advisories are used for gathering information, CERTs are confronted with the issue of **redundant information** as "an unsolved problem in the CERT community" (I10), requiring a manual deduplication of entries or information.

> "Manual data correlation is challenging and prone to errors. Each tool generates data in a different format, and making sense of it requires a lot of effort. Lack of integration among tools hampers efficiency" (I20).

While, in principle, a **cross-platform visualization** of gathered information was seen as useful, it should support users in correlating information from different data steams, requiring **modularity**:

> "Current practices can be cumbersome and time-consuming. While a dashboard would help centralize information, manually correlating data from various sources can slow down the process" (I18).

Some CERTs actively monitor social media to identify IoCs (I1, I3, I5, I6). Their main approach is to follow and monitor Twitter accounts of security experts and organizations, occasionally combined with topic-specific searches. Although **automated monitoring** of social media is generally desired, a major part is still conducted manually:

> "Currently, we do not have the capacities to monitor all media. We would benefit from a higher degree of automation, however, we need the legal foundations before" (I1).

Thus, when using automation for gathering public data, **data minimization, protection, and privacy regulations** of individual organizations and states must be considered (I09, I15).

> "Ensuring data privacy and security is an ongoing challenge. As we centralize more data, we need to guarantee its confidentiality and protect against unauthorized access" (I25).

Furthermore, keeping up with evolving threats is a significant challenge, since "threat actors constantly adapt their tactics and tools need to evolve just as quickly" (I24), requiring **flexible adaptations** of the used technology.

4.3 Mission Awareness and Collaboration

Due to the different capabilities and resources of CERTs, two CERTs do not monitor social media but receive the information from a different state division or other organizations, such as the BSI or another CERT. Thus, the VCV constitutes a crucial "web of trust" (I03) for **information verification**, which is, however, limited by manual processes:

> "But there is potential for improvement, i.e., the timely exchange of technical safety-relevant information is still done manually between teams today" (I3).

Besides the **need for collaboration** in the VCV, IoCs are collected using a shared instance of MISP, which allows the provision of structured malware information that can be imported into IDS software to enhance their detection capabilities. Although it "works better than solutions using pattern detection" (I10), if IoCs are detected by multiple CERTs, there is a risk for redundant entries:

> "In the VCV, we talk about IoCs and check [manually] if they [have] already [been] entered twice or threefold [into MISP]. The redundancy check has not been automated yet" (I6).

However, the need to switch between different tools affects productivity as "analysts spend more time navigating tools than analyzing threat" (I23), suggesting that a centralized or **integrated solution** would be more efficient.

> "The absence of a unified platform leads to disjointed workflows. Analysts have to switch between different tools to gather insights, which can be time-consuming and counterproductive" (I21).

For the communication of cyber threats, six participants described **reaching specific target groups** as challenging because currently, not all CERTs use multiple channels for dissemination. An expert further described that depending on their IT knowledge and skills, users often have additional questions when receiving a general warning message:

> “There are often inquiries from individuals because the people out there are not all technically savvy, and then we have to give advice and provide support over the phone” (I10).

Although cyber incidents are often documented in a ticket system, three participants described the challenging manual effort to convert and publish them as a security warning:

> “HTML code can be generated from the ticket, which then has to be imported relatively easily, but manually, into the TYPO3 system” (I10).

Thus, further three participants wished for **customizable warning messages for target groups** in the form of selecting keywords to generate a message for a group instead of writing individual messages. One expert described a potential form of automation:

> “The message is automatically created, through the case, category and target being automatically identified [...]" (I12).

Moreover, three participants described the lengthy approval process of warning messages as challenging due to having to wait for approval from multiple individuals.

> “What is always very time-consuming from my point of view is the internal approval of warning messages, because there are also other things that the approving parties need to take care of” (I13).

Finally, two CERT members wished for an **approval platform for warning messages** that speeds up the approval process of a message, for example, by creating “[. . .] a platform on which to revise this document without constantly sending it back and forth. Maybe that would make it a little easier” (I13).

5 IMPLEMENTATION

To design our demonstrator, we organized four design workshops involving a total of nine participants from our project consortium. Our team consisted of three researchers specializing in cross-media cyber situation picture creation, two researchers focused on actor-specific cyber alert communication, two CERT incident managers representing the application domain, and two developers responsible for the frontend and backend implementation of our artifact. Each workshop had a duration of approximately two hours, but it is important to note that we also discussed further design progress during our monthly jour fixe meetings, each lasting 45 minutes. However, these meetings covered various topics within the project's scope. These workshop were designed to discuss user requirements and derive design objectives for the implementation (Table 1). While the empirical pre-study served as the primary source of user requirements, additional requirements were gathered in follow-up evaluation sessions, which allowed participants to reflect requirements during the use of our demonstrator. For instance, the evaluations allowed for a better understanding of the requirements A1, A5 and A6, while A4 and A7 were completely new requirements elicited in evaluation sessions.

Following the analysis of initial pre-study interviews, the authors conducted the first design workshops (W01, W02). While W01 aimed to outline the backend architecture and discuss an initial set of requirements, we created a low-fidelity mockup of the intended artifact in W02. The input from these workshops allowed us to refine the requirements, while our developers began working on the initial tool version for subsequent evaluation. Based on these evaluations and the second round of interviews, we compiled a nearly complete list of requirements. The subsequent workshop, W03, was dedicated to fine-tuning, prioritizing (using the MoSCoW technique [11]), and discussing the progress regarding the initial requirements. Following the redesign of the artifact, a second round of evaluations and a third round of interviews were conducted. Finally, W04 was used to review the progress on requirements and reassess priorities for the remaining rounds of redesign and evaluation. While few practitioners were included in the workshops, multiple rounds of evaluation with CERT employees allowed for a participatory integration into the design process [68].

#	User Requirements	Design Objectives	It.
G	*Gathering*		
G1	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.	1
G2	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.	1
G3	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.	1
G4	Offer ways to support **data privacy** and **security** (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.	2
A	*Analysis*		
A1	Allow for 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.	1
A2	Allow for **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.	1
A3	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.	1
A4	Facilitate the **relationship awareness** between different data feeds.	Implement a global search function to filter information across different feeds.	2
A5	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).	2
A6	Evaluate information based on trustworthiness and provide data to the user for **verification**.	Links to the original source, displayed metadata, and traffic light indications for the verification of content.	2
A7	Enable the bidirectional integration into existing **organizational software**.	The backend includes a RESTful web service for data gathering by external software and users.	2
A8	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.	2
C	*Communication*		
C1	Support the (inter-)organizational **collaboration** of teams across organizational hierarchies.	Integrate the VCV chat for organizational collaboration and provide reporting functionality for decision-makers.	3
C2	Simplify the intra-organizational **approval** of cybersecurity warnings.	Warnings should be uploadable to a platform where supervisors can approve them.	3
C3	Facilitate the **communication** of cybersecurity warnings for diverse cybersecurity stakeholders.	Provide customizable warning templates for the communication with authorities, citizens, and enterprises.	3
C4	Allow for the **dissemination** of reports and warnings across multiple platforms.	Provide measures to export reports (DOC/PDF) and dissemination warnings messages (E-mail, Twitter).	3

Table 1: Overview of the derived user requirements, design objectives and the iteration (1, 2, 3) of their implementation.

5.1 Conceptualization

The functional and technical concept comprises three modules which are further differentiated by multiple components (Figure 3). First, the gathering module operates entirely in the backend and comprises the task, scraping and interface components. The task component initially accepts the search requests of the users. In addition to keywords and other metadata, these search requests define in particular the data sources from which information is obtained. For data sources that are not connected via an API (e.g., advisories and websites), the scraping component returns the found results to the task component together with web scraping technologies; however, if the data sources are accessible via an API (e.g., social media, vulnerability databases), the interface component returns the requested information to the task component. However, before the Task Component stores the results in the database (remote storage), the analysis module is addressed to enrich the data.

The analysis module includes the credibility, priority (backend) and dashboard (frontend) components. The task component sends the collected data to the credibility component to calculate the credibility of the data and then to the priority component to prioritize the data. After the analytically enriched data is saved in the database, the task component sends the data to the dashboard component for visualization. Furthermore, the data is now stored in a local database (web storage) so that users can perform certain analytical operations (e.g. interactive filtering of data) directly in the frontend. Finally, the communication module is connected to the dashboard, which links the message and export components. The message component allows to send information and warning messages via different channels (e.g., e-mail) to target group actors and the formulation of messages is supported by templates. In addition, the export component allows relevant information to be exported to other applications (e.g., Excel, MISP, OTRS, VCV).

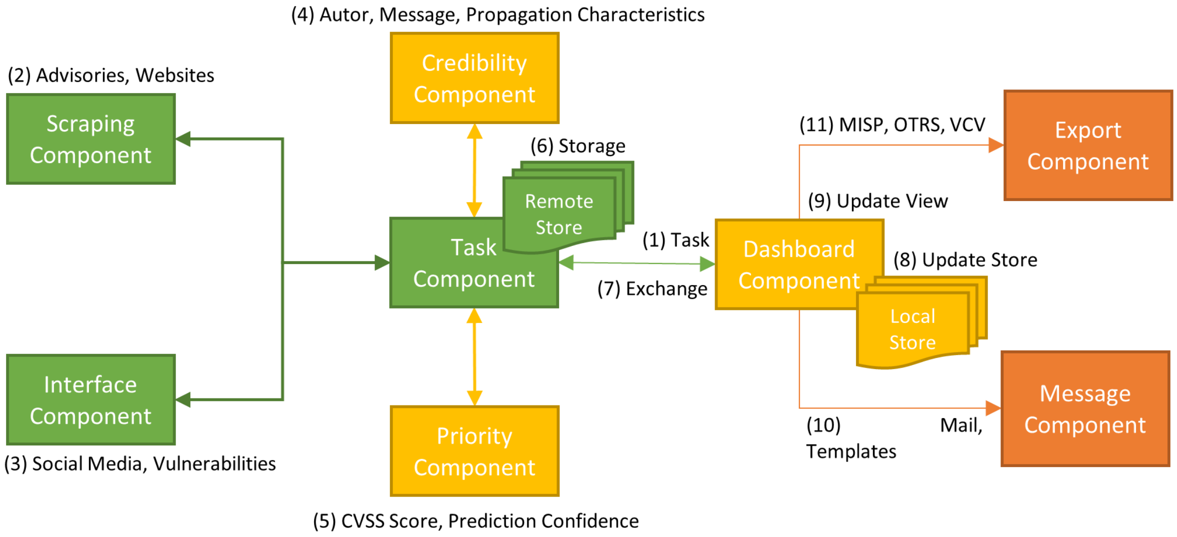


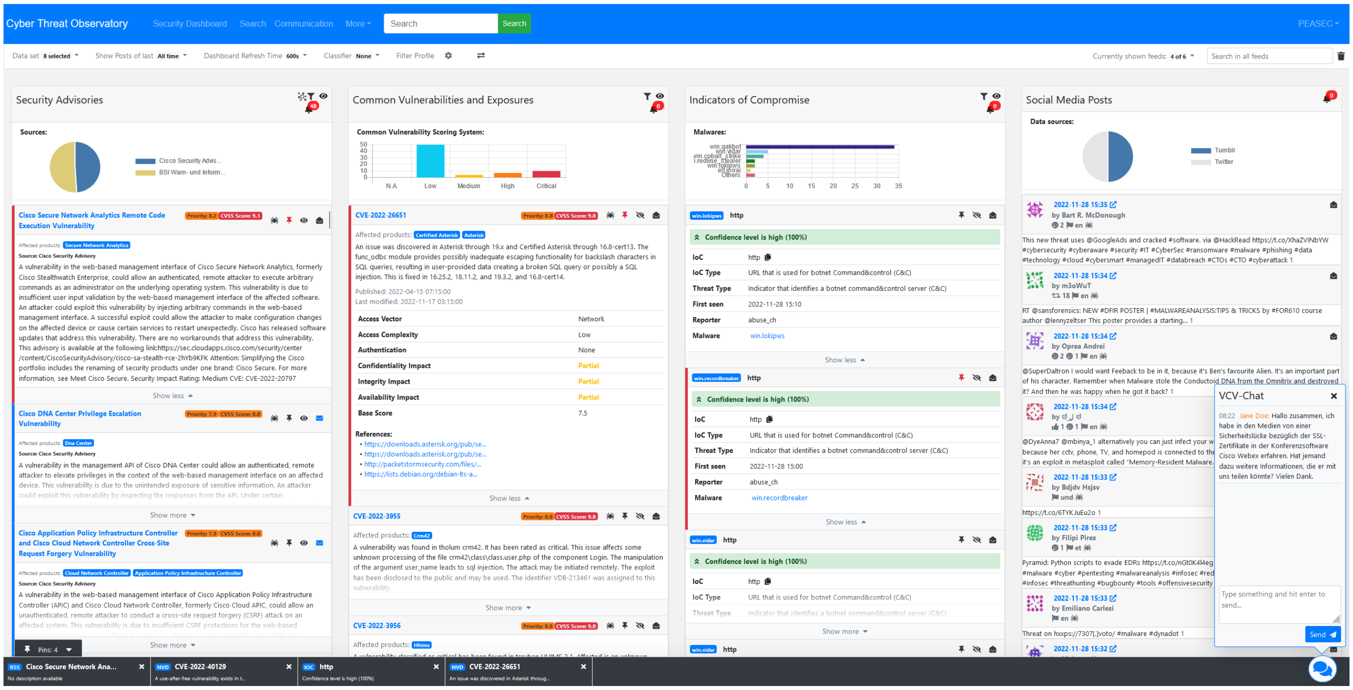
Figure 3: Current architecture of the artifact with basic (green), analysis (yellow) and communication components (orange).

5.2 Implementation

The frontend of our artifact is a web application based on Vue.js, including Bootstrap for responsive design and Chart.js for data visualization. Besides some local filtering options, all other actions of the frontend, such as searching for posts in open and social media or managing users, are forwarded to an API backend. The backend is realized as a service following the paradigm of a web-based and service-oriented architecture, which allows data provision for external organizational software (A7). It is a Python application using the Flask 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 (G1). Interface-based programming was applied to achieve a modular application that enables the enhancement of these implemented sources in future iterations (G2). 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) (G3). For the persistently stored data, the system operator has the possibility to specify an expiration date on which the data will be deleted (G4). 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 (A3).

The interface as depicted in Figure 4 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 use 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) (A1). 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 (A8). 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) (A2). In the top-right corner, a full text search field allows searching for keywords across the different feeds simultaneously (A4), while an algorithm is used to compute the priority of CVE entries using contextual data (A5). When CVE entries are posted to vulnerability databases, their initial CVSS score is mostly calculated with base score metrics. Our algorithm includes environmental and temporal score metrics to better prioritize information. As a rigor evaluation of the algorithm is not within the scope of this paper, we did not include further detailed information. 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) to enhance verification capabilities (A6). Although the use of a credibility assessment algorithm was discussed, it was not finished within the scope of the research project.

Furthermore, we implemented a Mastodon chat interface in the bottom-right corner to evaluate the idea of CERT members exchanging knowledge on current cyber incidents or important vulnerabilities (C1). In order to share detected threats with third parties, the communication module was implemented (Figure 5). The module supports the generation of warning messages using a template to adapt the information and language for the corresponding target group (C3). By the use of drop-down menus, the user can select



Cisco Secure Network Analytics Remote Code Execution Vulnerability Priority: 8.2 CVSS Score: 9.1

Affected products: Secure Network Analytics

Source: Cisco Security Advisory

A vulnerability in the web-based management interface of Cisco Secure Network Analytics, formerly Cisco Stealthwatch Enterprise, could allow an authenticated, remote attacker to execute arbitrary commands as an administrator on the underlying operating system. This vulnerability is due to insufficient user input validation by the web-based management interface of the affected software. An attacker could exploit this vulnerability by injecting arbitrary commands in the web-based management interface. A successful exploit could allow the attacker to make configuration changes on the affected device or cause certain services to restart unexpectedly. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link:https://sec.cloudapps.cisco.com/security/center /content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-2hYb9KFK Attention: Simplifying the Cisco portfolio includes the renaming of security products under one brand: Cisco Secure. For more information, see Meet Cisco Secure. Security Impact Rating: Medium CVE: CVE-2022-20797

Cisco DNA Center Privilege Escalation Vulnerability Priority: 7.9 CVSS Score: 8.8

Affected products: Dna Center

Source: Cisco Security Advisory

A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the responses from the API. Under certain

Cisco Application Policy Infrastructure Controller and Cisco Cloud Network Controller Cross-Site Request Forgery Vulnerability Priority: 7.9 CVSS Score: 8.8

Affected products: Cloud Network Controller Application Policy Infrastructure Controller

Source: Cisco Security Advisory

A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based

CVE-2022-26651 Priority: 8.8 CVSS Score: 9.8

Affected products: Certified Asterisk Asterisk

An issue was discovered in Asterisk through 19.x and Certified Asterisk through 16.8-cert13. The func_odbc module provides possibly inadequate escaping functionality for backslash characters in SQL queries, resulting in user-provided data creating a broken SQL query or possibly a SQL injection. This is fixed in 16.25.2, 18.11.2, and 19.3.2, and 16.8-cert14.

Published: 2022-04-15 07:15:00
Last modified: 2022-11-17 03:15:00

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial
Base Score	7.5

References:
- https://downloads.asterisk.org/pub/se...
- https://downloads.asterisk.org/pub/se...
- http://packetstormsecurity.com/files/...
- https://lists.debian.org/debian-lts-a...

CVE-2022-3955 Priority: 8.8 CVSS Score: 9.8

Affected products: Crm42

A vulnerability was found in tholum crm42. It has been rated as critical. This issue affects some unknown processing of the file crm42\class\class.user.php of the component Login. The manipulation of the argument user_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213461 was assigned to this vulnerability.

CVE-2022-3956 Priority: 8.8 CVSS Score: 9.8

Affected products: Hhims

win.lokipws http

Confidence level is high (100%)

IoC	http
IoC Type	URL that is used for botnet Command&control (C&C)
Threat Type	Indicator that identifies a botnet command&control server (C&C)
First seen	2022-11-28 15:10
Reporter	abuse_ch
Malware	win.lokipws

win.recordbreaker http

Confidence level is high (100%)

IoC	http
IoC Type	URL that is used for botnet Command&control (C&C)
Threat Type	Indicator that identifies a botnet command&control server (C&C)
First seen	2022-11-28 15:00
Reporter	abuse_ch
Malware	win.recordbreaker

win.vidar http

Confidence level is high (100%)

IoC	http
IoC Type	URL that is used for botnet Command&control (C&C)
Threat Type	Indicator that identifies a botnet command&control server (C&C)

win.vidar http

2022-11-28 15:35
by Bart R. McDonough
2 en

This new threat uses @GoogleAds and cracked #software. via @HackRead https://t.co/XhaZVINbYW #cybersecurity #cyberaware #security #IT #CyberSec #ransomware #malware #phishing #data #technology #cloud #cybersmart #managedIT #databreach #CTOs #CTO #cyberattack 1

2022-11-28 15:34
by m3oWuT
18 en

RT @sansforensics: NEW #DFIR POSTER | #MALWAREANALYSIS:TIPS & TRICKS by #FOR610 course author @lennyzeltser This poster provides a starting... 1

2022-11-28 15:34
by Oprea Andrei
2 1 en

@SuperDaltron I would want Feeback to be in it, because it's Ben's favourite Alien. It's an important part of his character. Remember when Malware stole the Conductoid DNA from the Omnitrix and destroyed it? And then he was happy when he got it back? 1

2022-11-28 15:34
by ᓀ‸ᓂ
1 1 en

@DyeAnna7 @mbinya_1 alternatively you can just infect your w
because her cctv, phone, TV, and homepod is connected to the
it's an exploit in metasploit called “Memory-Resident Malware.

2022-11-28 15:33
by Bdjdv Hsjsv
und

https://t.co/6TYKJuEu2o 1

2022-11-28 15:33
by Filipi Pires
1 et

Pyramid: Python scripts to evade EDRs https://t.co/nGt0K4l4eg
#malware #cyber #pentesting #malwareanalysis #infosec #red
#infosec #threathunting #bugbounty #tools #offensivesecurity

2022-11-28 15:33
by Emiliano Carlesi
en

Threat on hxxps://7307[.]voto/ #malware #dynadot 1

2022-11-28 15:32

VCV-Chat

08:22 Jane Doe: Hallo zusammen, ich habe in den Medien von einer Sicherheitslücke bezüglich der SSL-Zertifikate in der Konferenzsoftware Cisco Webex erfahren. Hat jemand dazu weitere Informationen, die er mit uns teilen könnte? Vielen Dank.

Type something and hit enter to send...

Send

RSS Cisco Secure Network Ana... No description available
NVD CVE-2022-40129 A use-after-free vulnerability exists in t...
IOC http Confidence level is high (100%)
NVD CVE-2022-26651 An issue was discovered in Asterisk throug...

Figure 4: Interface of the cross-platform cybersecurity dashboard featuring security advisories, vulnerability reports, indicators of compromise, and social media feeds.

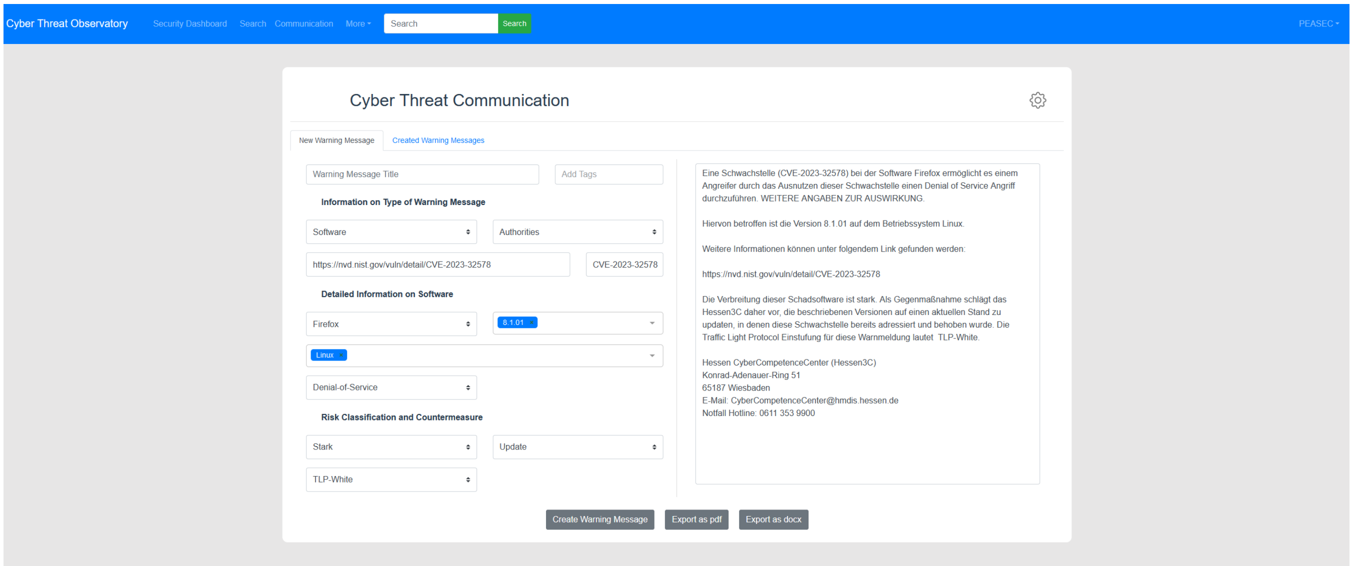
information regarding the message (e.g, type of incident, affected target group, hyperlinks, and related CVEs), the affected software (e.g. name, version, operating system, and type of attack), and provide a risk classification and countermeasures. Depending on the selected properties, the generated text comprises placeholders to further specify the characteristics of the threat and countermeasure instructions. While it also allows to classify the sensitivity of information based on the Traffic Light Protocol (TLP), due to the limited time of the research project, we were not able to implement an approval system at sufficient maturity for evaluation with CERT employees (C2). However, different channels (currently e-mail, Reddit and Twitter) are provided to disseminate the previously generated alerts and reach the affected stakeholders (C4).

6 EVALUATION

Following the notion of situated evaluation, the primary objective of our evaluation was not only to assess the alignment between evaluation objectives and outcomes but also to elicit subjective perspectives from experts regarding the practicality and relevance of the technology in real-world scenarios [73]. Thus, our evaluation approach involved cognitive walkthroughs with users [45] followed by short semi-structured interviews. For the cognitive walkthroughs, we initially defined three tasks: searching for specific information related to suspicious activities from three IP addresses, assessing critical vulnerabilities of a particular browser version, and responding to a chat request concerning SSL certificate issues within conferencing software. To ensure comprehensive interaction with various types of data, data sets were prepared for all tasks throughout the evaluation process. Participants were instructed to vocalize their thoughts as they navigated through the tasks, following the think-aloud protocol [50]. We applied a coaching-oriented approach by asking direct questions about different areas of the tool (e.g., if the participant stopped verbalizing their thoughts) or providing help when the participant was struggling [56].

During our first evaluation sessions, we saw that participants preferred to freely explore the tool or chose their own tasks known from daily practice. We thus offered subsequent participants the opportunity to carry out the predefined tasks (N=3) or a free exploration of the tool (N=22), potentially with own tasks in mind. Although this limited the comparability of the task performance, it was more important to us to not restrict the free expression of ideas through an overly rigid design, which also allowed us to get more realistic insights from their actual work practice. Subsequent semi-structured interviews were designed to prompt participants to reflect on the evaluation process and thus allowed the comparison of participant statements with regard to the key topics of the evaluation. The interview questions focused on perceived (1) usability and visual presentation, (2) data sources and types of information, (3) search and filter functionality, (4) information prioritization and credibility assessment, as well as (5) collaboration and communication functionality.

The evaluation with German CERT employees was conducted in three iterations, with twelve participants in the first round (N=12, E01-E12) [33], seven in the second round (N=7, E13-I19), and seven in the third round (N=7, E20-25). Each evaluation session, conducted via web conferencing tools after obtaining informed consent, lasted approximately 60 minutes. Following the purposive sampling strategy [12], we used our contacts established during pre-study sessions



Cyber Threat Communication

Warning Message Title

Add Tags

Information on Type of Warning Message

Software

Authorities

https://nvd.nist.gov/vuln/detail/CVE-2023-32578

CVE-2023-32578

Detailed Information on Software

Firefox

8.1.01

Linux

Denial-of-Service

Risk Classification and Countermeasure

Stark

Update

TLP-White

Eine Schwachstelle (CVE-2023-32578) bei der Software Firefox ermöglicht es einem Angreifer durch das Ausnutzen dieser Schwachstelle einen Denial of Service Angriff durchzuführen. WEITERE ANGABEN ZUR AUSWIRKUNG.

Hiervon betroffen ist die Version 8.1.01 auf dem Betriebssystem Linux.

Weitere Informationen können unter folgendem Link gefunden werden:

https://nvd.nist.gov/vuln/detail/CVE-2023-32578

Die Verbreitung dieser Schadsoftware ist stark. Als Gegenmaßnahme schlägt das Hessen3C daher vor, die beschriebenen Versionen auf einen aktuellen Stand zu updaten, in denen diese Schwachstelle bereits adressiert und behoben wurde. Die Traffic Light Protocol Einstufung für diese Warnmeldung lautet TLP-White.

Hessen CyberCompetenceCenter (Hessen3C)
Konrad-Adenauer-Ring 51
65187 Wiesbaden
E-Mail: CyberCompetenceCenter@hmdis.hessen.de
Notfall Hotline: 0611 353 9900

Figure 5: Interface of messaging component, which allows the interactive and template-based creation and dissemination of warning messages across multiple channels.

and put a stronger emphasis on incident managers as technology operators in practice. Thus, the participant pool (23 male, two female) consisted of nineteen internal incident managers (E05-E10, E13-19, E20-E25), three internal team leaders (E02, E11, E12), and three researchers specializing in HCI, information security, and artificial intelligence (E01, E03, E04). All interviews were recorded and transcribed with participant's consent. As not all organizations from our empirical pre-study were able to engage in a more in-depth cooperation (e.g., due to a lack of resources), participants from seven organizations, including five CERTs and two other organizations, were included in our evaluation sessions.

In accordance with the pre-study (Section 4), the three researchers conducted an inductive qualitative content analysis using the described consensus coding approach [30, 48]. Overall, our analysis yielded 58 codes, reflecting the categories of usability and visual presentation (13 codes), data sources and types of information (10 codes), search and filter functionality (14 codes), information prioritization and credibility assessment (11 codes), as well as communication and collaboration (10 codes). Since the dashboard was developed in three iterations, not all features were available from the beginning of our evaluations (Table 1). While the first evaluation was limited to the features of data collection and the customizable visualization, the second iteration allowed for more insights on the credibility and priority components. The third iteration included the export and message components. However, since we asked for further wishes and remarks in every iteration, we were also able to distill information on the yet to be implemented components.

6.1 Presentation and Usability of the Tool

During our walkthroughs, the first impression of the dashboard was generally positive among most participants, highlighting the capability to **provide a quick overview of collected data** and acknowledging that the "interface is incredibly user-friendly, making navigation and task execution a seamless experience" (E22). Many participants commented that they 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, allowing them to conduct cross-feed searches and perform tasks more efficiently:

> "As a digital forensics and incident response specialist, quick access to relevant data is crucial for effective response, and this system delivers exactly that. The interface is not only well-organized but also responsive, allowing me to perform tasks efficiently" (E23).

However, some participants also expressed concern that the **initial amount of data displayed may be too large** and that the tool may overwhelm the user by not managing information overload properly (E02, E03, E06) combined with limited staff available to oversee large amount of data:

> "The only problem is [that] a half position is 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 using the dashboard" (E02).

Still, the **interactive diagrams and visualizations** in the header of each feed are considered very helpful. Some participants would prefer a different chart in the social media feed (E08, E09, E10), which displays the frequency of posts over a certain period (E04) or shows how many times a keyword was found in all datasets (E10). Some participants suggest that all feed entries should be initially collapsed and be expanded as needed (E03, E07, E08):

> "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).

During system use, the feed layout was considered reasonable by many participants (E01, E02, E04, E07, E10). If additional data sources would be included, some would **hide less relevant feeds** as they consider four columns to be ideal (E02, E10), or minimize individual feeds for a short time to focus on another feed (E07).

6.2 Data Sources and Types of Information

In general, our 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**. When analyzing the CVE feed, some participants did 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 (E05, E10) or would like to receive information on whether a CVE is new or was only updated (E07). The CVEs should then be filtered automatically according to a specified product list:

> "I would like to have a pre-filtering in certain areas, namely that one could configure in some form which advisories are relevant for the state administration or which software is used by critical infrastructure operators, for example" (E10).

For some participants, the indicators of compromise feed is not relevant because they already use more advanced tools for IoCs, such as MISP (E05, E06), while others liked the integration of IoCs into the dashboard (E08, E09), for instance, to enter data directly into the firewall configuration (E02). Regarding the security advisory feed, some participants remark that they maintain a list of websites they regularly check for new advisories (E07, E10), but since not all vendors provide RSS feeds for their advisories, they have concerns if all necessary sources can be integrated into the tool:

> “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).

The social media feed is seen as particularly useful by some participants (E01, E05, E06, E08), while others state that social media plays a marginal or no role in their daily work (E10). However, five participants would like to see some **connection between different feeds** to establish 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 security advisories, CVSS, social media, to talk to each other in a logic. 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, it has to flash deep red” (E06).

Moreover, participants suggested the integration of **additional data sources**, such as other vulnerability databases (E03), vulnerability reports from the BSI (E07, E10), websites with security news (E05), and external threat intelligence feeds:

> "Having real-time access to relevant threat data from multiple sources would elevate our proactive defense capabilities. Additionally, the ability to customize alerts and notifications based on specific criteria would further streamline our incident response process" (E20).

6.3 Cross-Feed Search and Filter Functionality

Considering the dashboard’s search and filter functions, especially the global search field was rated positively by several participants, as it allows to search for specific terms across all feeds quickly:

> "It helps us narrow down our focus and identify relevant details swiftly. The user-friendly interface makes searching and filtering a straightforward process, which contributes to a more effective analysis" (E22).

However, during the walkthroughs, 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 (E02, E12). Thus, some participants would like to use **Regex to filter the results** (E03, E12) and suggest 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.

> "I would prefer to use regex filters for including and excluding terms to get the relevant output across all feeds and data. I would also suggest to add a history in a drop-down box so that the last 50 or so entries can still be displayed and clicked on again" (E12).

The filter options for the individual feeds were often considered helpful, but numerous ideas for additional filters were expressed. For example, the CVE feed should include a way to **filter by manufacturers or products** (E01, E11), which should rather offer a selection list instead of a free text field to avoid typing mistakes (E04). While some participants would find it useful to be able to predefine keywords or products in a kind of profile beforehand (E01, E09, E10), others suggested to connect infrastructure research modeling software (e.g., Netbox) to automatically filter for the products used in the respective organization (E11):

> “It would be useful to store and highlight products that are used in our organization. Information related to such products are certainly more relevant” (E10).

The possibility to filter data sets by clicking on the charts was quickly discovered during exploration by some participants, who found it helpful and intuitive. While in general, filters are considered useful by most participants, some would tend to use the global search first (E01, E03), as they feel this is faster and easier than setting up filters in the individual feeds:

> “On the desktop PC, 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).

6.4 Credibility and Priority Assessment

While some participants saw the search and filter function as a good starting point for identifying and prioritizing relevant information (E03, E07), others stated that the **CVSS score provided by vulnerability databases is highly relevant**, but sometimes rather seen as an upper bound (E14, E15, E16). One participant mentioned that the CVSS 3.1 algorithm is not justified empirically nor formally, sometimes requiring employees to act against their intuition:

> "When the CVSS score is high, then it's a high notification. I could never argue in front of a secretary of state that I personally didn't find it that severe" (E16).

Thus, the use of **environmental score metrics** was seen as highly relevant for improving the usefulness of CVSS scores, especially the affected product and its version are among the most important attributes (E13, E14, E15, E16). Beyond, widely used software was considered more relevant, such as office products and web browsers.

> "For the administration, this means office products, browsers and video conferencing. In a medium-sized enterprise, then the attacked party will perhaps say: yes, for us it is important that the accounting system works, because we have to make money with it" (E13).

In terms of **temporal score metrics**, participants expressed that they deem an attack more likely, the more resources exist for an exploit and the more attention a vulnerability receives (E13, E16). A measure for the attention a vulnerability receives is the number of notifications that mention a particular CVE.

> "I have written a parser, which uses RSS feeds from website like Golem, Heise Security, Register, BleepingComputer, and so on. And there you can already see, when everyone starts to report about something then you should urgently follow up on it" (E16).

Further participants state that the dashboard would benefit from **clustering and deduplication algorithms** (E05, E13, E16). To reduce information overload, notifications that report about the same vulnerability should be grouped and there should be an indicator about the number of notifications in that group.

> "If there are really many reports about [the incident], you should have a cluster and to see, for example: okay, there are 20 messages in there about one topic, and then you get a few specific pieces of information extracted, so that you have an overview of it and it's not loaded full by any duplicates" (E13).

The priority of information further depends on the credibility of authors and content. Those involved in social media would like to define a **list of trusted experts**, whose posts are highlighted in the feed (E01, E05) or even displayed in a separate feed (E06).

> "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).

Participants discussed diverse **indicators for credibility assessment**, which are especially relevant for social media content (E17, E18, E19). Especially links to known trusted websites, the confirmation of information by experts, further mentions of the incident in other source media or the style of writing (i.e., grammar) were seen as important precursors to estimate the credibility of information. However, also the credibility of the author must be considered, which might be traceable by a known username, a URL to a professional profile, or previous posts on cybersecurity incidents.

6.5 Collaboration and Communication

With regard to the **integrated collaborative chat**, some participants suggested that their chat environment is too extensive for integration since it offers different chat rooms and the possibility for private chats, which takes up too much space in the dashboard and thus is rather distracting (E02, E07). However, most participants generally see a benefit in communicating with colleagues inside and outside their organization through chats.

> "I value systems that streamline collaboration and communication. Sharing data with colleagues is seamless, and the balance between automation and manual analysis is well-thought-out" (E24).

While the **integration into existing organizational software** was already suggested to automatically filter for relevant products (E11), another opportunity lies in the integration of **case management features**, such as provided by ticket systems, to further enhance collaboration:

> "The ability to create and manage incident cases directly within the platform would streamline collaboration among team members and external stakeholders [and] create a holistic environment for handling incidents from identification to resolution" (E24).

When exploring the system, several participants valued the **semi-automation provided by interactive message templates** across multiple platforms, because messages were often created and sent manually by the use of Word templates (E23, E24). While one participant requested the option to select multiple target groups to create multiple warning messages simultaneously (E25), the section of different message parameters and use of placeholders were well received and described as intuitive (E23).

> "In practice, the module would save a lot of work. Here you could really achieve optimal results in a short time" (E22).

When participants were asked about the **export and reporting capabilities** of the tool, multiple participants were satisfied with a simple export of records in list form as a PDF or Excel file (E07, E08, E09), while one requested the ability to annotate records with further information (E03). Thus, the dashboard should allow the user to select the data to be exported, such as by specific keywords or using the pinned posts from the dashboard (E01, E02, E04).

> "If it is critical, then I have to send it away immediately. I think the federal government had eight categories with different colors. When the firewall were marked as red, I pinned everything that I then felt was important for firewalls and that was sent together" (E02).

7 DESIGN HEURISTICS

By reflecting the results gathered from three iterations of empirical pre-study, design and evaluation using the analytical frame of cyber situational awareness, we identified eight design heuristics regarding the cross-platform collection (D1, D2), analysis (D3, D4, D5), integration (D6), and communication (D7, D8) of cyber threat information, which according to our design case study with German state CERTs contribute to an enhanced threat awareness and mission awareness if realized in a properly designed artifact. To contextualize and discuss the identified design heuristics with previous findings, we will refer to participant IDs (I01, E02) and identified user requirements (G3, A1, C4).

7.1 Design Heuristics for Threat Awareness

In terms of threat awareness, the **support the automatic and modular integration of closed and public information sources (D1)** was seen as an important foundation of the dashboard. While we could achieve the automatic gathering of security advisories, vulnerabilities, indicators of compromise, and social media data, as not all sources are provided by APIs suitable for automation of data access (G1). Especially the different, regularly changing structure of security advisories was seen a challenge for software development (E05, E07, E10), which might be alleviated by the recent introduction and promotion of the Common Security Advisory Framework (CSAF) [42] or the use of web scraping technologies [71]. While our architecture allows for a modular implementation of new data sources on code level, some participants (E05, E06) with technical expertise asked for the realization of a plug-in system to integrate relevant (closed) information sources on their own (G2).

Furthermore, the need to **provide an interoperable and privacy-preserving data management (D2)** became apparent. First, we used the ActivityStreams 2.0 Core Syntax to be able to provide heterogeneous data in a unified format as a web service (G3). However, due to the scope of our study, we were not able to evaluate the usefulness of this design decision. Furthermore, multiple participants (I09, I15, I25) highlighted that data minimization, protection, and privacy regulations are an ongoing challenge (G4). While we implemented options to select collected metadata and decide after how many days data should be deleted, the legal foundation of monitoring of social media varies by federal state and necessitates at least the option to deactivate non-compliant data sources.

The **customizable visualization of relevant cyber threat information (D3)** was seen as the core feature of the dashboard. When considering different interaction types, such as proposed by the visual information-seeking mantra [65], participants valued the provided *overview* (E03, E22, E23) and *filtering* (E01, E02, E22) by interactive charts and textual filter criteria (A1), such as the affected hardware or software, some more technical staff would prefer to use a cross-feed single search field with operators, regular expressions, and an auto-complete feature to repeat recent queries (E03, E12). With regard to data sources, it became apparent that some CERTs use other tools for processing IoCs (E05, E06) and some had no interest in monitoring social media (E10). These statements highlighted the need to allow the *customization* of which data types should be displayed in the interface, which was subsequently implemented in the interface (A2). While the dashboard also provides *details on demand* by extend views and hyperlinks and allows to *share* exported data, future revisions should explore further interaction types [29], such as *zooming* into aggregated data, providing a *history*, supporting the *linking* of different visualizations, and enabling to view *relationships* between items.

Especially the latter became apparent as our participants requested to **facilitate relationship awareness between different cyber threat information and feeds (D4)**. The evaluation showed a great need to find related information in other feeds quickly and easily (E06). While the filtering of irrelevant information (I10, I20) was seen as an important precursor of relationship awareness (A3), participants also envisioned the use of clustering (E05, E13, E16) to combine similar content in a meaningful manner. Relevant studies have already investigated clustering and topic modelling techniques for various application domains in the cybersecurity field [28]. To alleviate information overload, a suitable approach is to embed the data in a meaningful numerical space and apply clustering techniques to it [39]. Following the completion of this process, an automatic method for labelling clusters can provide an overview and description of the resulting clusters [5, 20] Although the dashboard currently contains data from four distinct source types, the only cross-platform interaction is facilitated by the global search field (A4). For example, CVE numbers are often referenced in security advisories and in a future revision 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 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 further requires **intelligent algorithms for credibility assessment and threat prioritization (D5)**. While the use of enhanced CVSS metrics was seen as a useful approach (E13-E16) to improve the prioritization of vulnerabilities (A5) and the display of relevant metadata (E17-E19) was valued to facilitate the verification of information (A6), a big potential lies in the application of machine learning. Considering the large volumes of social big data generated in large-scale incidents, the recent past saw a large body of research on using AI for clustering or topic modeling [38], to detect events [59], identify relevant information [32], or assess credibility [78], which could be integrated and tailored to the domain of cybersecurity. However, even when following the principles of explainable AI [63], our participants stated that such algorithms may be a useful addition but cannot replace the manual assessment of data. Due to recent enhancements in large language models, few-shot learning [9], data augmentation [6], and explainable AI [21], we suggest the design of human-centered machine learning pipelines allowing the rapid training and adaption of cybersecurity models (Figure 6).

7.2 Design Heuristics for Mission Awareness

Taking the perspective of mission awareness, the participants suggested a deeper **integration with organizational structure and security systems (D6)** 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 (I10, E24). Moreover, some CERTs use infrastructure resource management (IRM) software, which could provide the IT resources used at the organization in order to automatically adapt the dashboard filters to relevant products (E11) but is missing in the current implementation of the dashboard (A7). Furthermore, the integration of products used in the respective organizational network (e.g., as a separate feed) would enable the inclusion of network awareness features into the dashboard [41]. Given the different roles and tasks processed by CERTs [58], a role management is vital to facilitate the customization of relevant data sources and visualized information feeds according to the preferences of individual operators (A8).

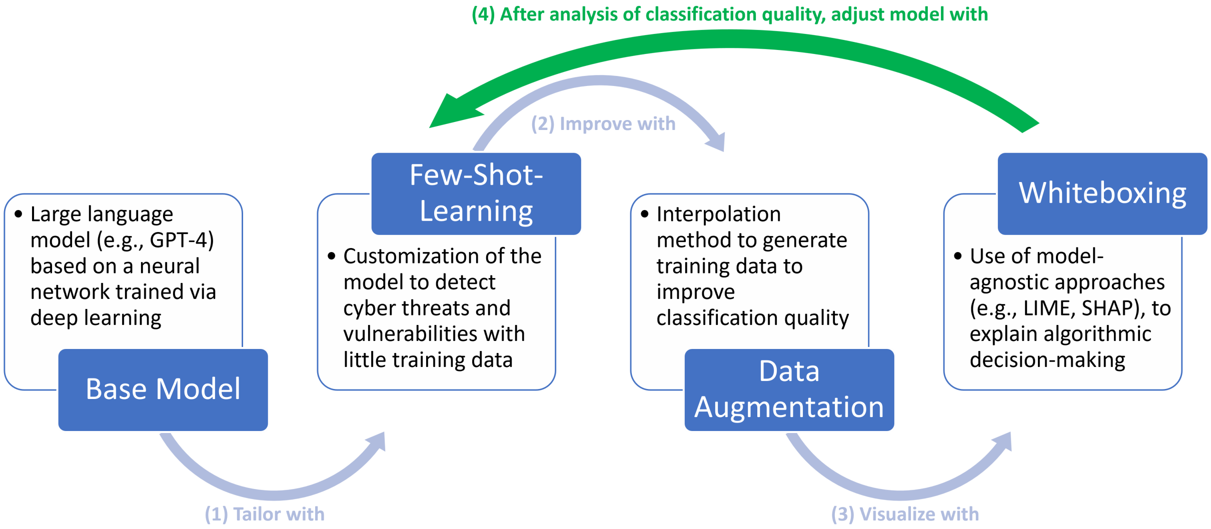

(4) After analysis of classification quality, adjust model with
(2) Improve with
Few-Shot-Learning
Whiteboxing
• Large language model (e.g., GPT-4) based on a neural network trained via deep learning
• Customization of the model to detect cyber threats and vulnerabilities with little training data
• Interpolation method to generate training data to improve classification quality
• Use of model-agnostic approaches (e.g., LIME, SHAP), to explain algorithmic decision-making
Base Model
Data Augmentation
(1) Tailor with
(3) Visualize with

Figure 6: Method for a customizable and transparent classification of cyber threats. The explanations and probabilities of cyber threat classification can then be visualized in the dashboard, allowing a quick adaptation of the base model with few-shot learning and data augmentation when new detection requirements are formulated or classification results are insufficient.

Furthermore, the **facilitation of (inter-)organizational collaboration for threat management (D7)** was mentioned as an important feature. The pin feature was considered useful by many participants (E01, E02, E04), 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 [58]. In addition to a structured and textual export of data records, participants valued the idea of using the pin function to generate (daily) threat and vulnerability reports for clients or the management of an organization (C1). Since it was desired to facilitate the approval processes for recommendation and warning messages (C2), the platform should facilitate parties to make corrections, sign, and finally approve alerts, rather than sending alerts back and forth until mutual agreement is achieved (I13.

One major problem for the communication of cyber threats mentioned was **enabling the cross-platform dissemination of tailored warning messages (D8)**, which requires different formulations and information depending on their IT knowledge, skills and type of organization. The customization of pre-written templates with placeholders for more detailed information (C3) was well received among participants (I10, I12). In this way, the suggested solution reduced the high effort necessary to create warnings manually. When providing services and warnings to citizens and organizations [23], HCI research suggests the consideration of demographic variables, such as age and region, as well as security misconceptions for a stakeholder-oriented communication strategy [1, 25, 55]. Furthermore, warning messages should communicate the severity and convey actionable coping responses, consider message framing and provide countermeasures on habituation effects [4]. As requested by participants (E22-E24), the tool facilitates the semi-automatic dissemination of warning messages across platforms (C4), including e-mail, Reddit, or Twitter.

8 CONCLUSION

In this paper, we presented a design case study to conceptualize, implement, and evaluate an interactive dashboard for CERTs that allows to search, filter, and communicate cyber threat information from security advisories, CVEs, IoCs, and social media. Furthermore, we identified user requirements (N=16) on the gathering, analysis and communication of cyber threat information, as well as design heuristics (N=8) for threat awareness and mission awareness. However, this paper is subject to limitations. First, our research was conducted with German state CERTs. It is likely that enterprise or product CERTs have different sets of user needs and design requirements [62]. Differences in financial resources, national capabilities and legislation likely influence the activity, competences, and tool utilization of CERTs [8]. Thus, further research is required to compare different analytical technologies and collaborative practices across nations and organizations on a fine-grained level. Second, due to its nature as a research demonstrator and its evaluation in scenario-based settings, the technology readiness level of the dashboard can be at best described as *technology validated in lab* (TRL4) [10]. While readers are invited to request a demo access from the first author, the authors are currently applying for funding to evaluate the tool under operational, more stressful conditions [29], to reach the state of *technology demonstrated in relevant environment* (TRL6) before considering an open-source publication.

ACKNOWLEDGMENTS

This work has been funded by the German Federal Ministry for Education and Research, in the projects CYWARN (13N15407) and CYLENCE (13N16636), 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. Furthermore, we would like to thank Ali Sercan Basyurt und Kaan Eyilmez for their work on the communication module.

REFERENCES

[1] Ruba Abu-Salma, Reem Talhouk, Jose Such, Claudia Aradau, Francesca Meloni, Shijing He, Syed Ishtiaque Ahmed, Cansu Ekmekcioglu, Dina Sabie, Rikke Bjerg Jensen, Jessica McClearn, Anne Weibert, Max Krüger, Faheem Hussain, and Rehema Baguma. 2023. Diverse Migration Journeys and Security Practices: Engaging with Longitudinal Perspectives of Migration and (Digital) Security. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–7. https://doi.org/10.1145/3544549.3573800

[2] Atif Ahmad, Sean B Maynard, Kevin C Desouza, James Kotsias, Monica T Whitty, and Richard L Baskerville. 2021. How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security* 101 (2021), 102122. https://doi.org/10.1016/j.cose.2020.102122

[3] M. Angelini, S. Bonomi, S. Lenti, G. Santucci, and S. Taggi. 2019. MAD: A visual analytics solution for Multi-step cyber Attacks Detection. *Journal of Computer Languages* 52 (June 2019), 10–24. https://doi.org/10.1016/j.cola.2018.12.007

[4] Ali Sercan Basyurt, Jennifer Fromm, Philipp Kuehn, Marc-André Kaufhold, and Milad Mirabaie. 2022. Help Wanted - Challenges in Data Collection, Analysis and Communication of Cyber Threats in Security Operation Centers. In *Proceedings of the International Conference on Wirtschaftsinformatik (WI)*. AIS, Nürnberg.

[5] Markus Bayer, Marc-André Kaufhold, and Christian Reuter. 2021. Information Overload in Crisis Management: Bilingual Evaluation of Embedding Models for Clustering Social Media Posts in Emergencies. In *Proceedings of the European Conference on Information Systems (ECIS)*. AIS, 1–18.

[6] Markus Bayer, Marc-André Kaufhold, and Christian Reuter. 2023. Survey on Data Augmentation for Text Classification. *ACM Computing Surveys (CSUR)* 55, 7 (2023), 1–39. https://doi.org/10.1145/3544558

[7] Yasmine Belghith, Sukrit Venkatagiri, and Kurt Luther. 2022. Compete, Collaborate, Investigate: Exploring the Social Structures of Open Source Intelligence Investigations. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–18. https://doi.org/10.1145/3491102.3517526

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

[9] Tom Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared D Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, et al. 2020. Language models are few-shot learners. *Advances in neural information processing systems* 33 (2020), 1877–1901.

[10] Ilenia Bruno, Georges Lobo, Beatrice Valente Covino, Alessandro Donarelli, Valeria Marchetti, Anna Schiavone Panni, and Francesco Molinari. 2020. Technology readiness revisited: a proposal for extending the scope of impact assessment of European public services. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*. ACM, Athens Greece, 369–380. https://doi.org/10.1145/3428502.3428552

[11] Faiza Allah Bukhsh, Zaharah Allah Bukhsh, and Maya Daneva. 2020. A systematic literature review on requirement prioritization techniques and their empirical evaluation. *Computer Standards & Interfaces* 69 (2020), 103389. https://doi.org/10.1016/j.csi.2019.103389

[12] Steve Campbell, Melanie Greenwood, Sarah Prior, Toniele Shearer, Kerrie Walkem, Sarah Young, Danielle Bywaters, and Kim Walker. 2020. Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing* 25, 8 (Dec. 2020), 652–661. https://doi.org/10.1177/1744987120927206

[13] Onur Catakoglu, Marco Balduzzi, and Davide Balzarotti. 2016. Automatic Extraction of Indicators of Compromise for Web Applications. In *Proceedings of the 25th International Conference on World Wide Web* (Montréal, Québec, Canada) *(WWW '16)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 333–343. https://doi.org/10.1145/2872427.2883056

[14] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Claude P. R. Heath. 2020. Too Much Information: Questioning Security in a Post-Digital Society. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–14. https://doi.org/10.1145/3313831.3376214

[15] Mica R. Endsley. 1995. Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37, 1 (1995), 32–64. https://doi.org/10.1518/001872095779049543

[16] Ulrik Franke and Joel Brynielsson. 2014. Cyber situational awareness - A systematic review of the literature. *Computers & Security* 46 (2014), 18–31. https://doi.org/10.1016/j.cose.2014.06.008

[17] Magdalena Glas, Manfred Vielberth, and Guenther Pernul. 2023. Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–19. https://doi.org/10.1145/3544548.3581046

[18] Jochen Gläser and Grit Laudel. 2010. *Experteninterviews und qualitative Inhaltsanalyse: als Instrumente rekonstruierender Untersuchungen* (4th ed.). VS Verlag für Sozialwissenschaften, Wiesbaden.

[19] John R. Goodall, Eric D. Ragan, Chad A. Steed, Joel W. Reed, G. David Richardson, Kelly M.T. Huffer, Robert A. Bridges, and Jason A. Laska. 2019. Situ: Identifying and Explaining Suspicious Behavior in Networks. *IEEE Transactions on Visualization and Computer Graphics* 25, 1 (Jan. 2019), 204–214. https://doi.org/10.1109/TVCG.2018.2865029

[20] Maarten Grootendorst. 2022. BERTopic: Neural topic modeling with a class-based TF-IDF procedure. http://arxiv.org/abs/2203.05794 arXiv:2203.05794 [cs].

[21] David Gunning, Mark Stefik, Jaesik Choi, Timothy Miller, Simone Stumpf, and Guang-Zhong Yang. 2019. XAI—Explainable artificial intelligence. *Science Robotics* 4, 37 (2019), eaay7120. https://doi.org/10.1126/scirobotics.aay7120

[22] Robert Gutzwiller, Josiah Dykstra, and Bryan Payne. 2020. Gaps and opportunities in situational awareness for cybersecurity. *Digital Threats: Research and Practice* 1, 3 (2020), 1–6. https://doi.org/10.1145/3384471

[23] Julie M. Haney and Wayne G. Lutters. 2017. The Work of Cybersecurity Advocates. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, Denver Colorado USA, 1663–1670. https://doi.org/10.1145/3027063.3053134

[24] Kirstie Hawkey, David Botta, Rodrigo Werlinger, Kasia Muldner, Andre Gagne, and Konstantin Beznosov. 2008. Human, organizational, and technological factors of IT security. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems*. ACM, Florence Italy, 3639–3644. https://doi.org/10.1145/1358628.1358905

[25] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. 2023. A World Full of Privacy and Security (Mis)conceptions? Findings of a Representative Survey in 12 Countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–23. https://doi.org/10.1145/3544548.3581410

[26] Martin Husák, Tomáš Jirsík, and Shanchieh Jay Yang. 2020. SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (Virtual Event, Ireland) *(ARES '20)*. Association for Computing Machinery, New York, NY, USA, Article 2, 10 pages. https://doi.org/10.1145/3407023.3407062

[27] Martin Husák, Lukáš Sadlek, Stanislav Špaček, Martin Laštovička, Michal Javorník, and Jana Komárková. 2022. CRUSOE: A toolset for cyber situational awareness and decision support in incident handling. *Computers & Security* 115 (2022), 102609. https://doi.org/10.1016/j.cose.2022.102609

[28] Luciano Ignaczak, Guilherme Goldschmidt, Cristiano André Da Costa, and Rodrigo Da Rosa Righi. 2022. Text Mining in Cybersecurity: A Systematic Literature Review. *Comput. Surveys* 54, 7 (Sept. 2022), 1–36. https://doi.org/10.1145/3462477

[29] Liuyue Jiang, Asangi Jayatilaka, Mehwish Nasim, Marthie Grobler, Mansooreh Zahedi, and M Ali Babar. 2022. Systematic literature review on cyber situational awareness visualizations. *IEEE Access* 10 (2022), 57525–57554. https://doi.org/10.1109/ACCESS.2022.3178195

[30] Robert Kaiser. 2014. *Qualitative Experteninterviews. Konzeptionelle Grundlagen und praktische Durchführung*. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-02479-6

[31] Hanna Kallio, Anna-Maija Pietilä, Martin Johnson, and Mari Kangasniemi. 2016. Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing* 72, 12 (Dec. 2016), 2954–2965. https://doi.org/10.1111/jan.13031

[32] Marc-André Kaufhold. 2021. *Information Refinement Technologies for Crisis Informatics: User Expectations and Design Principles for Social Media and Mobile Apps*. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-33341-6

[33] Marc-André Kaufhold, Ali Sercan Basyurt, Kaan Eyilmez, Marc Stöttinger, and Christian Reuter. 2022. Cyber Threat Observatory: Design and Evaluation of an Interactive Dashboard for Computer Emergency Response Teams. In *Proceedings of the European Conference on Information Systems (ECIS)*. AIS, Timisoara, Romaina, 1–17.

[34] Marc-André Kaufhold, Nicola Rupp, Christian Reuter, and Matthias Habdank. 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 (2020), 319–342. https://doi.org/10.1080/0144929X.2019.1620334

[35] Himanshu Khurana, Jim Basney, Mehedi Bakht, Mike Freemon, Von Welch, and Randy Butler. 2009. Palantir: a framework for collaborative incident response and investigation. In *Proceedings of the 8th Symposium on Identity and Trust on the Internet - IDtrust '09*. ACM Press, New York, New York, USA, 38. https://doi.org/10.1145/1527017.1527023

[36] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT security: Accountabilities, moralities, and oscillations in IT security practices. *Proceedings of the ACM on Human-Computer Interaction (CSCW)* 2 (2018). https://doi.org/10.1145/3274361

[37] Hansaka Angel Dias Edirisinghe Kodituwakku, Alex Keller, and Jens Gregor. 2020. InSight2: A Modular Visual Analysis Platform for Network Situational Awareness in Large-Scale Networks. *Electronics* 9, 10 (Oct. 2020), 1747. https://doi.org/10.3390/electronics9101747

[38] Farzan Kolini and Lech Janczewski. 2017. Clustering and Topic Modelling: A New Approach for Analysis of National Cyber security Strategies. In *PACIS 2017 Proceedings*, Vol. 126. AIS. https://aisel.aisnet.org/pacis2017/126

[39] Linn-Mari Kristiansen, Vinti Agarwal, Katrin Franke, and Raj Sanjay Shah. 2020. CTI-Twitter: Gathering Cyber Threat Intelligence from Twitter using Integrated

Supervised and Unsupervised Learning. In *2020 IEEE International Conference on Big Data*. IEEE, 2299–2308. https://doi.org/10.1109/BigData50022.2020.9378393

[40] Marko Krstic, Milan Cabarkapa, and Aleksandar Jevremovic. 2019. Machine Learning Applications in Computer Emergency Response Team Operations. In *2019 27th Telecommunications Forum (TELFOR)*. IEEE, 1–4. https://doi.org/10.1109/TELFOR48224.2019.8971040

[41] Philipp Kuehn, Julian Bäumler, Marc-André Kaufhold, Marc Wendelborn, and Christian Reuter. 2022. The Notion of Relevance in Cybersecurity: A Categorization of Security Tools and Deduction of Relevance Notions. In *Workshop-Proceedings Mensch und Computer*. Gesellschaft für Informatik, Darmstadt. https://doi.org/10.18420/muc2022-mci-ws01-220

[42] Philipp Kuehn, David N. Relke, and Christian Reuter. 2023. Common vulnerability scoring system prediction based on open source intelligence information sources. *Computers & Security* (2023), 103286. https://doi.org/10.1016/j.cose.2023.103286

[43] Quentin Le Sceller, ElMouatez Billah Karbab, Mourad Debbabi, and Farkhund Iqbal. 2017. SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*. ACM, Reggio Calabria Italy, 1–11. https://doi.org/10.1145/3098954.3098992

[44] Dimitrios Lekkas and Diomidis Spinellis. 2005. Handling and reporting security advisories: A scorecard approach. *IEEE security & privacy* 3, 4 (2005), 32–41. https://doi.org/10.1109/MSP.2005.98

[45] Thomas Mahatody, Mouldi Sagar, and Christophe Kolski. 2010. State of the Art on the Cognitive Walkthrough Method, Its Variants and Evolutions. *International Journal of Human-Computer Interaction* 26, 8 (July 2010), 741–785. https://doi.org/10.1080/10447311003781409

[46] Vincent Mancuso, Sarah McGuire, and Diane Staheli. 2020. Human Centered Cyber Situation Awareness. In *Advances in Human Factors in Cybersecurity*, Tareq Ahram and Waldemar Karwowski (Eds.). Springer International Publishing, Cham, 69–78. https://doi.org/10.1007/978-3-030-20488-4_7

[47] Vasileios Mavroeidis and Siri Bromander. 2017. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 91–98. https://doi.org/10.1109/EISIC.2017.20

[48] Philipp Mayring. 2000. Qualitative Content Analysis. *Forum: Qualitative Social Research* 1, 2 (2000). https://doi.org/10.17169/fqs-1.2.1089

[49] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–23. https://doi.org/10.1145/3359174

[50] Sharon McDonald, Helen M. Edwards, and Tingting Zhao. 2012. Exploring think-alouds in usability testing: An international survey. *IEEE Transactions on Professional Communication* 55, 1 (2012), 2–19. https://doi.org/10.1109/TPC.2011.2182569

[51] Sean McKenna, Diane Staheli, Cody Fulcher, and Miriah Meyer. 2016. Bubblenet: A cyber security dashboard for visualizing patterns. In *Computer Graphics Forum*, Vol. 35. Wiley Online Library, 281–290. Issue 3. https://doi.org/10.1111/cgf.12904

[52] Sudip Mittal, Prajit Kumar Das, Varish Mulwad, Anupam Joshi, and Tim Finin. 2016. CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities. In *Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2016*. IEEE, 860–867. https://doi.org/10.1109/ASONAM.2016.7752338

[53] Sharifah Roziah Binti Mohd Kassim, Shujun Li, and Budi Arief. 2023. Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions. *Digital Threats: Research and Practice* 4, 3 (Sept. 2023), 1–24. https://doi.org/10.1145/3609230

[54] Ryan Mullins, Ben Nargi, and Adam Fouse. 2020. Understanding and enabling tactical situational awareness in a security operations center. In *Advances in Human Factors in Cybersecurity: AHFE 2020 Virtual Conference on Human Factors in Cybersecurity, July 16–20, 2020, USA*. Springer, 75–82. https://doi.org/10.1007/978-3-030-52581-1_10

[55] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–11. https://doi.org/10.1145/3290605.3300579

[56] Erica L. Olmsted-Hawala, Elizabeth D. Murphy, Sam Hawala, and Kathleen T. Ashenfelter. 2010. Think-aloud protocols: a comparison of three think-aloud protocols for use in testing data-dissemination web sites for usability. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Atlanta Georgia USA, 2381–2390. https://doi.org/10.1145/1753326.1753685

[57] Dorottya Papp, Zhendong Ma, and Levente Buttyan. 2015. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In *2015 13th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 145–152. https://doi.org/10.1109/PST.2015.7232966

[58] Thea Riebe, Marc-André Kaufhold, and Christian Reuter. 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* 5 (2021). https://doi.org/10.1145/3479865

[59] Thea Riebe, Tristan Wirth, Markus Bayer, Philipp Kuehn, Marc-André Kaufhold, Volker Knauthe, Stefan Guthe, and Christian Reuter. 2021. CySecAlert: An Alert Generation System for Cyber Security Events Using Open Source Intelligence Data. In *Information and Communications Security (ICICS)*. Springer, 429–446. https://doi.org/10.1007/978-3-030-86890-1_24

[60] Ariel Rodriguez and Koji Okamura. 2019. Generating Real Time Cyber Situational Awareness Information Through Social Media Data Mining. In *2019 IEEE 43rd Annual Computer Software and Applications Conference* (Milwaukee, WI, USA). IEEE, New York, 502–507. https://doi.org/10.1109/COMPSAC.2019.10256

[61] Markus Rohde, Peter Brödner, Gunnar Stevens, Matthias Betz, and Volker Wulf. 2017. Grounded Design - a praxeological IS research perspective. *Journal of Information Technology* 32, 2 (2017), 163–179. https://doi.org/10.1057/jit.2016.5

[62] Robin Ruefle, Audrey Dorofee, David Mundie, Allen D. Householder, Michael Murray, and Samuel J. Perl. 2014. Computer security incident response team development and evolution. *IEEE Security & Privacy* 12, 5 (2014), 16–26. https://doi.org/10.1109/MSP.2014.89

[63] Wojciech Samek, Grégoire Montavon, Andrea Vedaldi, Lars Kai Hansen, and Klaus-Robert Müller. 2019. *Explainable AI: interpreting, explaining and visualizing deep learning*. Vol. 11700. Springer Nature. https://doi.org/10.1007/978-3-030-28954-6

[64] Corina Sas, Steve Whittaker, Steven Dow, Jodi Forlizzi, and John Zimmerman. 2014. Generating implications for design through design research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Toronto Ontario Canada, 1971–1980. https://doi.org/10.1145/2556288.2557357

[65] B. Shneiderman. 1996. The eyes have it: a task by data type taxonomy for information visualizations. In *Proceedings 1996 IEEE Symposium on Visual Languages*. IEEE, Boulder, CO, USA, 336–343. https://doi.org/10.1109/VL.1996.545307

[66] Florian Skopik, Timea Pahi, and Maria Leitner. 2018. Cyber Situational Awareness in Public-Private-Partnerships. In *Cyber Situational Awareness in Public-Private-Partnerships*. Springer Vieweg, Berlin. https://doi.org/10.1007/978-3-662-56084-6

[67] Rebecca Slayton and Brian Clarke. 2020. Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005. *Technology and Culture* 61, 1 (2020), 173–206. https://doi.org/10.1353/tech.2020.0036

[68] Clay Spinuzzi. 2005. The methodology of participatory design. *Technical communication* 52, 2 (2005), 163–174. https://www.ingentaconnect.com/content/stc/tc/2005/00000052/00000002/art00005

[69] Gunnar Stevens, Markus Rohde, Matthias Korn, and Volker Wulf. 2018. Grounded Design: A Research Paradigm in Practice-based Computing. In *Socio-Informatics: A Practice-Based Perspective on the Design and Use of IT Artifacts*. Oxford University Press, 23–46. https://doi.org/10.1093/oso/9780198733249.003.0002

[70] Rock Stevens, Daniel Votipka, Josiah Dykstra, Fernando Tomlinson, Erin Quartararo, Colin Ahern, and Michelle L. Mazurek. 2022. How Ready is Your Ready? Assessing the Usability of Incident Response Playbook Frameworks. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–18. https://doi.org/10.1145/3491102.3517559

[71] Stefan Stieglitz, Milad Mirbabaie, Björn Ross, and Christoph Neuberger. 2018. Social media analytics – Challenges in topic discovery, data collection, and data preparation. *International Journal of Information Management* 39, October 2017 (2018), 156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

[72] Wiem Tounsi and Helmi Rais. 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security* 72 (Jan. 2018), 212–233. https://doi.org/10.1016/j.cose.2017.09.001

[73] Michael Twidale, David Randall, and Richard Bentley. 1994. Situated Evaluation for Cooperative Systems. In *Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work* (Chapel Hill, North Carolina, USA) *(CSCW '94)*. Association for Computing Machinery, New York, NY, USA, 441–452. https://doi.org/10.1145/192844.193066

[74] Rick Van der Kleij, Geert Kleinhuis, and Heather Young. 2017. Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Frontiers in Psychology* 8 (2017). https://doi.org/10.3389/fpsyg.2017.02179

[75] Cynthia Wagner, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. 2016. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (WISCS '16)*. Association for Computing Machinery, New York, NY, USA, 49–56. https://doi.org/10.1145/2994539.2994542

[76] Volker Wulf, Claudia Müller, Volkmar Pipek, David Randall, Markus Rohde, and Gunnar Stevens. 2015. *Practice-Based Computing: Empirically Grounded Conceptualizations Derived from Design Case Studies*. Springer London, London, 111–150. https://doi.org/10.1007/978-1-4471-6720-4_7

[77] Volker Wulf, Markus Rohde, Volkmar Pipek, and Gunnar Stevens. 2011. Engaging with Practices: Design Case Studies as a Research Framework in CSCW. In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work* (Hangzhou, China) *(CSCW '11)*. Association for Computing Machinery, New York, NY, USA, 505–512. https://doi.org/10.1145/1958824.1958902

[78] Xinyi Zhou and Reza Zafarani. 2020. A survey of fake news: Fundamental theories, detection methods, and opportunities. *ACM Computing Surveys (CSUR)* 53, 5 (2020), 1–40. https://doi.org/10.1145/3395046