Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uiss20

Operational cyber incident coordination revisited: providing cyber situational awareness across organizations and countries

Maria Leitner, Florian Skopik & Timea Pahi

To cite this article: Maria Leitner, Florian Skopik & Timea Pahi (18 Apr 2024): Operational cyber incident coordination revisited: providing cyber situational awareness across organizations and countries, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2024.2334787

To link to this article: https://doi.org/10.1080/19393555.2024.2334787

Published online: 18 Apr 2024.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2024.2334787

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS

Operational cyber incident coordination revisited: providing cyber situational awareness across organizations and countries

Maria Leitner[a,b], Florian Skopik[b], and Timea Pahi[b]

[a]University of Vienna, Faculty of Computer Science, Vienna, Austria; [b]AIT Austrian Institute of Technology, Center for Digital Safety & Security, Vienna, Austria

ABSTRACT

Cyber situational awareness (CSA) is a prerequisite for justified decision-making and to maintain cyber security. This becomes particularly complex when establishing inter-organizational awareness across sectors. For example, computer security incident response teams (CSIRTs) and national cyber security centers need to establish CSA among countries when coordinating regional cyber incident response. Today's state of the art of information sharing across larger numbers of organizations is often still the least common denominator in the shape of web-based forms and email reports. These are easily applicable by almost everyone who wants to report findings even in stressful situations. However, these do not prove to be efficient for the coordinator that aggregates and merges the data. Therefore, a cyber coordination platform using online surveys is proposed. This approach uses surveys to collect, aggregate and visualize data in a dashboard to support cyber coordination and knowledge management. Furthermore, the online surveys are easy to use and respond to and therefore simplify the participation of stakeholders. We propose an architecture and implement a prototype using popular web application frameworks. The evaluation in a user study revealed promising results with respect to increased efficiency and decreased resource requirements for establishing situational awareness.

KEYWORDS

Coordination and cooperation platform; cyber situational awareness; incident coordination; cyber security

1. Introduction

Establishing and maintaining an appropriate level of cyber security is an enormous task for today's organizations. This task can only be approached in a collaborative manner (Atif et al., 2012; Ruefle et al., 2014). Numerous types of bodies and authorities, including national computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), information sharing and analysis centers (ISACs), third-party managed security service providers (MSSPs), national cyber security centers (NCSCs) and the like, have emerged to act as incident information coordinators across companies, industry sectors and whole nation states. Vivid information exchange and the timely creation of cyber situational awareness (CSA) is a crucial prerequisite to establishing cyber security (Franke & Brynielsson, 2014). While the sharing of technical incident information or threat intelligence is already thriving (e.g., MISP, STIX and TAXII), gradually, initiatives to sharing cyber incident information (e.g., number of affected organizations, number of affected systems, the impact of systems) have also appeared that are related to information security or cyber incidents – such as promoted in the Network and Information Security (NIS2) directive (European Parliament, Council of the European Union, 2022) in the European Union (EU) such as outlined in Franke et al. (2021).

A cyber incident is defined by the European Union Agency for Cybersecurity (ENISA) (2017) as "*any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, independent if it's natural or human made; malicious or non-malicious intent; deliberate, accidental or due to incompetence; due to development or due to operational interactions.*" In this article, we focus not on intra-organizational incidents but on the cooperation and coordination of cyber incidents that affect more than one organization. Furthermore, the technology, digitization

CONTACT Maria Leitner ✉ maria.leitner@univie.ac.at University of Vienna, Faculty of Computer Science, Waehringerstrasse 29, Vienna 1090, Austria

and interconnectedness allows and requires that incident coordination is conducted between organizations and across borders.

Today's state of the art to operational cyber incident information sharing across larger numbers of organizations is often still to use the least common denominator in the shape of web-based forms, unstructured text and PDF reports attached to emails. For example, whether an organization experiences some certain type of problem, employs certain systems, is affected by a vulnerability or malware or has seen some specific indicator of compromise – just to name a few. Emails, forms and reports are low-barrier, easily applicable and well-proven technologies which can be utilized by almost everyone who wants to report findings even in stressful situations (Skopik et al., 2016). While filing web-based reports or even simply sending off emails in natural language to information coordinators poses no hurdle for the sender, it turns out to be a nightmare for the receiver of this information. Keeping track of the up-to-dateness of information, merging incoming new information with older reports, managing follow-up inquiries, and eventually maintaining an overview of the current situation by just using these standard tools is a labor-intensive task.

To improve the efficiency and effectiveness of incident coordinators during regular business, large-scale incident and crises, it is important to design and develop tools or systems that support their intensive line of work (Hodgson et al., 2022; Skopik, 2017). Particularly during situations where time and short response cycles are essential, cell phone or online messengers are still the main communication devices. Motivated by the need for a more efficient way for organizations to provide information, and at the same time quick and easy ways for information coordinators to digest this information, we developed a survey-based system that allows incident coordinators to quickly assess the current cyber security situation within an organization, a sector or the whole nation state.

In this article, we revisit the traditional approach to operational cyber incident coordination and propose a cyber situational awareness design to develop an incident coordination platform, called *KoordTool*. We refer to the military domain for the terminology such as by NATO (2022) where the operational level is "*defined by its role, which is to link the resource tactical-level activities to strategic objectives*." The scale of operational level is not predefined. With KoordTool, we can aggregate the information about activities of organizations at an operational level that can be leveraged by NCSCs, for example.

Our system uses a survey tool to create and distribute incident-specific queries to organizations. These queries, created and distributed by an incident coordinator, include questions on specifics of the incident and its impact (e.g., affected systems, indicators of compromise). While the cyber incident progress, the queries can be extended and revised. Queries can be redistributed in re-occurring time intervals to allow information coordinators to collect the most recent information. Centrally, the collected feedback is analyzed, merged and presented in the KoordTool. It allows to quickly assess a current situation, to drill into the answers or rate whether enough information to accurately assess the situation is available at all.

The main contributions of this article are:

- **Empirical state-of-the-art analysis on incident and crises coordination**: We assess the state of the art of inter-organizational, cross-border, cross-sectoral incident and crisis coordination and cooperation via the Internet. We analyze the challenges of incident coordination in terms of time, distribution of the stakeholders, information aggregation and security. We outline four use cases where incident and crises coordination is highly relevant.
- **Incident Coordination Proof-of-Concept Platform**: We further propose an approach with the KoordTool to manage, gather and aggregate operational incident information (e.g., with participant reports from multiple stakeholders) to establish situational awareness as a prerequisite for informed decision-making not only during regular incidents but particularly during large-scale incidents and crises. We demonstrate our approach with a proof-of-concept implementation of the KoordTool.
- **Qualitative Evaluation**: We evaluate the applicability of KoordTool in an experimental user study. In this study, 19 participants, incident coordinators of national authorities and CSIRTs, review and discuss the applicability of the

KoordTool for incident coordination and cooperation. In addition, we conduct a security analysis to conduct a review on (technical) security measures that need to be foreseen for enhancements of the KoordTool.

• **Actionable Recommendations for improving Incident Coordination**: We identify four key areas for improvement for establishing CSA, tool support, visualizations and technology. Based on the participants' feedback, we provide actionable advice that can be picked up by industry or research.

Our findings suggest that the KoordTool approach can significantly decrease the required resources to create CSA, is partly even applicable to non-domain experts, enables a more accurate view on current data, allows easy distribution of information across organizations, and significantly improves the creation of reports for decision makers.

The remainder of the article is organized as follows: Section 2 summarizes the background, motivation as well as challenges to establish CSA. Section 3 describes the design of the proposed approach and how it can tackle these challenges. Furthermore, the technical implementation of the KoordTool is described in Section 4. Section 5 highlights the evaluation of the approach and Proof-of-Concept (PoC). Section 6 investigates lessons learned and recommendations. Section 7 concludes the article.

2. Background and motivation

This section summarizes related work on cyber situational awareness, motivates challenges for the coordination of large-scale incidents and crises as well as use cases for coordination and investigates current tools to support inter-organizational cyber situational awareness.

2.1. Cyber situational awareness

First defined in the mid-1980s, most literature has adopted the definition for situation awareness (SA) proposed by Endsley (1995) as: "*Situation awareness is the perception of the element in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.*" Newer models have adapted this term to the cyber domain to cyber situational awareness (CSA) models. Franke and Brynielsson (2014) were the first to conduct a systematic review of cyber situational awareness. Furthermore, Pahi et al. (2017a) conduct a survey of cyber situational awareness models and reviewed several works on CSA (e.g., (Giacobe, 2010)). CSA can be established by public or private organizations (Lehto & Limnéll, 2021). However, especially CSIRTs, Security Operation Centers (SOCs) or NCSCs aim to establish a certain level of CSA as defined by Leitner, Pahi, and Skopik (2017). Furthermore, the cooperative work of incident response teams, such as SOCs, is investigated by Ahmad et al. (2021); Kokulu et al. (2019).

2.1.1. Cyber common operating pictures

One way to establish CSA for CSIRTs, SOCs or NCSCs is to create a national CCOP that provides the current state on major national incidents and responses at national level. Typically, Cyber Common Operating Pictures (CCOPs) aim to support the decision-making in operational environments by providing a comprehensive representation about the present situation (Conti et al., 2013; Pahi et al., 2017b). In general, CCOPs can come with different scopes depending on the requirements and needs of the stakeholders (e.g., a CCOP for small enterprise or a CCOP for a large global organization). CCOPs established at NCSCs or SOCs, for example, can serve as a basis for establishing effective CSA (Pahi et al., 2017a). CSA is a required capability of national stakeholders and governments to effectively perform their operations, thereby also relying on the knowledge about the technical status of critical infrastructures and occurring incident information. In recent years, research has investigated, e.g., the technical data gathering and processing within organizations or strategies for CSA as outlined by ENISA (2012).

2.1.2. CSIRT communication

Communication, such as sharing incident information between stakeholders, is highly relevant to enable CSA (Kokkonen et al., 2016). The setup of CSIRTs and their main operations and responsibilities are described by Bronk et al. (2006). CSIRT communication and its requirements for effective operations are analyzed by Kruidhof (2014). Besides trust as a major requirement, new challenges of CSIRT communication are identified by Hellwig et al. (2016) as commercialization of cyber space, new threat domains, growth of the CSIRT community and the emergence of cyber regime complex (Happa et al., 2021) assess decision support for SOC analysts by conducting a user study with 10 analysts, utilizing a mixed-method approach with questionnaires, eye tracking and semi-structured interviews.

2.2. Challenges for the coordination of large-scale incidents and crises

In situations of distress, e.g., cyber crises, national or international large-scale incidents or others where the coordination and management of CSIRTs, NCSCs or SOCs is necessary to establish CSA, several challenges exist. This situation often applies to, for example:

- CSIRT networks who aim to establish CSA within their networks,
- NCSCs who aim to establish CSA with operators of essential services (according to the NIS and the subsequent NIS2 directive (European Commission, 2016; European Parliament, Council of the European Union, 2022)), or
- SOCs who aim to establish CSA within their organization's subsidiaries.

So in such situations, the following questions typically arise:

(1) How can information be collected from distributed stakeholder organizations in an easy way?
(2) How can the responded information be processed efficiently?
(3) How can this information be aggregated and visualized to be interpreted quickly?

Hence, besides the timing, also the processing and aggregation of situation information may be of importance. This leads to the following challenges in these situations:

- **Time (T)**: Timing is essential in the coordination and management of large-scale incidents. It is important that information is sent, received and processed in a timely manner and allows the users to quickly establish CSA.
- **Distribution of Stakeholders (D)**: The coordination of the incidents is usually provided within a group of entities. Often, there is one main coordinator (e.g., a crisis handler, a NCSC, a CSIRT, etc.) that collects information from the other stakeholders (e.g., operators of essential services, other CSIRTs, other public authorities) to assess the current situation and establish CSA. The stakeholders consist of a set of organizations that are, e.g., scattered within a nation (e.g., operators of essential services) or are distributed across multiple countries (e.g., EU CSIRT network). Different time zones may also apply due to the distribution.
- **Aggregation of CSA Information (A)**: Information aggregation is another challenge. As mentioned above, when the main coordinator establishes CSA, he or she usually deals with various information from multiple stakeholders. Processing this information and aggregating it is essential to establish a CCOP (Pahi et al., 2017b). Hence, specific measures have to be foreseen to support the aggregation and further the visualization of information. However, it is not typically easy to use just "any" visualization. To establish CSA, specific visualizations need to be created to support the understanding and interpretation of the coordinator (Pahi et al., 2017b).
- **Security (S)**: Security concerns immediately arise when discussing sharing sensitive information about large-scale incidents at national or international level. For example, who is affected and the impact on organizations and citizens should be restricted and securely exchanged in stressful situations. Sensitive information must only be released after coordination and agreement. Also, sharing this information with third-party providers due to the usage of online documents or storage might be debatable.

This list of challenges does not claim to be exhaustive. On the contrary, we expect that more challenges arise with the number of participants, data complexity or usability. In the following, we will assess current tools based on these challenges in order to identify current gaps.

2.3. Use cases

In general, our approach can be used to coordinate and share information quickly between distributed stakeholders. In the following, we will briefly summarize potential use cases for information sharing in the information security community.

2.3.1. CSIRT/SOC/NCSC coordination

Our approach aims at supporting incident managers with a situation-dependent completion of the CCOPs. Incident or crisis coordinators (e.g., NCSCs) can direct inquiries (e.g., use of certain technology or protocols, distribution, impact) to certain communities (e.g., digital service providers) and gather relevant information for operational CCOPs. Furthermore, SOCs can establish CSA within their organization's subsidiaries. Current tools support the sharing of threat intelligence or loosely structured shared files that require a lot of manual effort to keep them updated and structured (see Section 2.4).

2.3.2. Cyber crisis liaison organisation network (CyCLONe) coordination

European Union Member States launch the Cyber Crisis Liaison Organisation Network[1] (CyCLONe) that contributes to the implementation of rapid emergency response in case of large-scale cross-border cyber incidents or crises. CyCLONe complements the existing cyber security structures at EU level by linking the cooperation at technical (e.g. CSIRTs) and political levels. The network needs tools to ensure the CCOPs at each level and how to transfer and transmit information to other levels. This also includes a coordinated impact assessment on the impacts of the incidents or crises.

2.3.3. Cyber exercise coordination

While incident managers may handle incidents on a daily basis, cyber security exercises or cyber drills may also be potential use cases of our approach. In general, cyber exercises are events where people can learn, train, test and experiment their information security skills and abilities (Kucek & Leitner, 2020; Seker & Huseyin Ozbenli, 2018). Cyber exercises can involve local, regional, national or international stakeholders. Particularly, in international or national cyber exercises which test and train also national and international processes (e.g., the NIS2 notification (European Parliament, Council of the European Union, 2022)), there is one participant role that focuses on the incident coordination – one coordination entity needs to establish CSA and therefore gathers information from multiple organizations or countries (e.g., scattered across Europe). So far, incident coordinators used shared online documents or emails as a means to communicate and gather data from other participants in the cyber exercise. However, this procedure is often time consuming and requires a lot of effort from the incident coordinators.

2.3.4. Coordination of public health information during pandemic

Even though this article focuses mainly on quickly sharing information related to cyber security, it may also be used in other domains. For example, during the COVID-19 pandemic it is vital to rapidly share public health and scientific information (Rourke et al., 2020). During the pandemic, the coordination of information related to the new infected cases, recovered cases, deceased cases could be transmitted between counties and states, states and federal government, federal government and interorganizational organizations (e.g., World Health Organization (WHO)). Furthermore, the coordination of hospitalizations between private/public hospitals and local/federal governments could be conducted (e.g., the number of active cases in a regular hospital ward, the number of active cases in intensive care, the number of additional hospital beds in regular wards or intensive care). This public health information is currently shared between stakeholders in various ways (e.g., using a tool of the European Medicines Agency, using tools developed by local governments, etc.).

These four use cases show that there are many opportunities to use a cyber incident coordination platform to rapidly share and distribute information between stakeholders.

2.4. Current tools to support inter-organizational cyber situational awareness

Current tools to exchange and share information have different purposes and meet some challenges (time, aggregation, distribution, security) described in Section 2.2. In the following, each tool is described and evaluated based on the aforementioned challenges. A short comparison of the tools is outlined in Table 1. Due to page limitations, we could not compare each individual tool in each category. For this purpose, we summarized the main points relevant to the challenges (each marked with T, A, D or S).

2.4.1. Web-based document sharing and file hosting services

These services provide online word processing capabilities or file hosting services to multiple stakeholders (e.g., Dropbox, GoogleDrive, OneDrive, and many others). While shared documents are often easily accessible (D) and available to various stakeholders (T), organizations often have to comply and agree to the terms of third-party providers (e.g., cloud services or file hosting services) or require to setup their own hosting service to enable sharing of documents. However, shared documents need a provided structure (A) in order to gather relevant and adequate information to establish CSA. This also requires a high amount of attention to the stakeholders where to input which information. In terms of security, it is arguable if security-critical information at national or international level shall be disclosed to third-party providers (S). In general, it depends on the level and where coordination is necessary.

2.4.2. Cyber threat intelligence (CTI) sharing tools

CTI sharing tools often focus on the exchange of technical information (e.g., incident information) within a range of stakeholders. Examples of technologies and tools are MISP[2] (Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing), STIX[3] (Structured Threat Information Expression), TAXII[4] (Trusted Automated eXchange of Indicator Information) and SABU (Husák et al., 2023). For CSA information on national or international level, the degree of detail might be too fine-grained (depending on the use case) and is heavily dependent on the user interfaces and aggregation that is provided by the tools (A). This is also applicable in terms of security measures (S). As most of the aforementioned tools are considered expert tools, expert knowledge might be required to use and support the tools (D). For some organizations, this might not be easy to achieve – especially in crisis situations.

2.4.3. Emails

Emails are a standard way to communicate and exchange information (T, D). However, they become challenging to process and follow with the amount of sent and received emails. As the content of emails is often unstructured text, it is cumbersome to identify and generate the most relevant information (A). In these cases, the information sent by mail is copied into additional tools (e.g., spreadsheets or other software) to oversee the information which requires time to process (T). Lastly, email security (S) is still challenging (Ng et al., 2009).

2.4.4. Online surveys

Online surveys provide a measure to ask for a response from various stakeholders. Online surveys can be hosted in cloud-based environments (e.g., SurveyMonkey, etc.) or “locally” within an organization (e.g., LimeSurvey). Web-based surveys are often easy to access and available to respondents (T, D). Surveys typically provide

Table 1. Comparison of current tools for information sharing.

	Time	Distribution	Aggregation	Security
Shared Docs & File Services	⊠	⊠	⊡	⊡
CTI Tools	⊠	⊡	⊡	⊡
Email	⊠	⊠	⊟	⊡
Online Surveys	⊠	⊠	⊡	⊡

⊠ . . . fully supported

⊡ . . . partially supported

⊟ . . . not supported

aggregation and visualizations for the responses (A) but not all of them might be useful to establish CSA. Often, developers do not focus in their implementation on security- or privacy-related features (S). For example, inviting participants to a survey might not require a signed email or the responses might not be entered via properly encrypted connections. Furthermore, security-related concerns arise in cloud-based environments as discussed before for shared document services.

Hence, there is a need for CSA support tools that enable the coordination and management of large-scale incidents across organizations and sectors. So far, existing tools manage certain aspects but cannot support all challenges: time, distribution, aggregation and security. In the following sections, we will propose an approach and a proof-of-concept tool that can support the aforementioned situations.

3. Cyber situational awareness incident coordination design

In this section, we discuss how we aim to address the aforementioned challenges and gaps by outlining the design and specification of the proposed solution.

3.1. *Approach*

To solve the challenges of large-scale incident coordination, we assume that there are several roles involved:

- **Main Coordinator** (i.e. a moderator) is coordinating the information exchange and sharing with various stakeholders. He or she is responsible for handling incoming information and to aggregate the information in order to establish CSA (e.g., in case of large-scale incidents).
- **Stakeholders** (i.e. participants) are respondents and interact with the coordinator. They respond to questions that the main coordinator provides. They may update their responses depending on the current status.

In these situations, we envision a supporting approach as outlined in Figure 1. The numbers of the following steps are also shown in the figure.

(1) In critical situations, the main coordinator (i.e. moderator) creates and sends out a survey to the stakeholders. For example, a NCSC sends out a survey to operators of essential services to find out if they are affected by a certain vulnerability or threat.

(2) The stakeholders respond to the questions and return the responses (i.e. participant reports). Some may answer faster than others.

(3) The answers are immediately processed and send to the Coop-app (coordination and cooperation application).

(4) The KoordTool (see Section 4) collects and aggregates the information based on the responses as coordination and cooperation report (coop-report). Visualizations always include the latest responses. Hence, if stakeholders answer later, their responses are immediately included.

(5) The coordinator can establish CSA, e.g., can interpret the criticality of the situation and propose

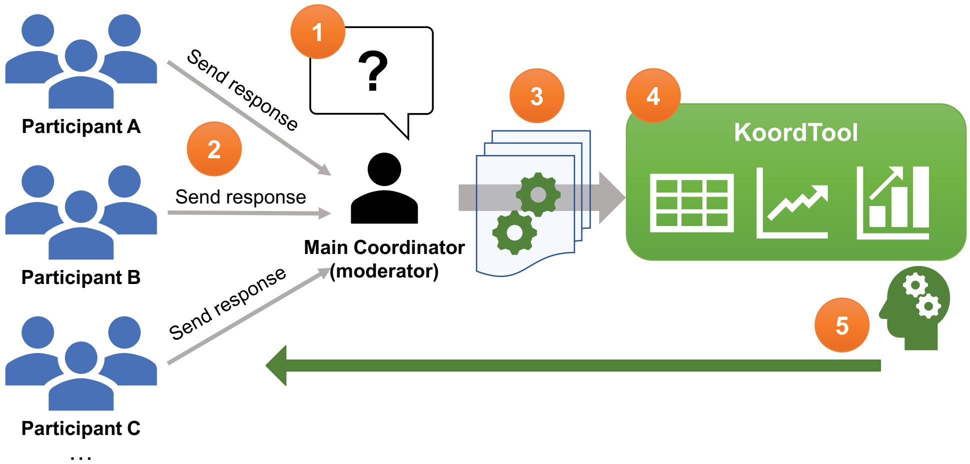


Figure 1. Outline of the approach that shows the survey responses being processed in the KoordTool.

measures. He or she can inform further stakeholders and make justified decisions on the next steps (Fielder et al., 2016). Furthermore, additional questions can be raised in subsequent iterations (starting with step (1)) to refine the gained CSA.

This approach effectively addresses the challenges (see Section 2.2):

- **Time**: Our approach supports timing by enabling coordinators to send out surveys and as soon as responses are received, the KoordTool dashboard (see Section 4.3) visualizes the responses. It also updates its view every 5 seconds. Furthermore, non-responding recipients are marked after a configurable time span.
- **Distribution**: The approach supports that respondents or participants are geographically distributed and supports the fast exchange between organizations, CSIRTs, teams or other stakeholders (Skopik et al., 2016).
- **Aggregation**: The KoordTool dashboard supports not only the aggregation of results of the participants but also provides visualizations in the form of feedback and trend graphs to efficiently enable the coordinator to establish CSA (Zhao et al., 2019).
- **Security**: Security is a relevant aspect when exchanging critical information between various stakeholders and organizations in these situations. Our tool allows for local hosting (e.g., of surveys) that may be shared with various stakeholders. For a further elaborate evaluation of security aspects, please see Section 5.

In this article, the focus is mainly on large-scale incident coordination. However, the KoordTool can support any incident coordination from small, medium-to-large incidents. The coordination could be also at lower levels (e.g., within a small enterprise or organization) and does not have to be always at national or international levels.

Compiling and maintaining a situation report during cyber security incidents is quite challenging. The effort needed to gather and maintain critical status information from multiple organizations in a stressful situation, especially when speed is vital, can be hard to manage. The Austrian CERT reported similar issues after a European cyber security exercise stating problems while communicating vital information from organizations, especially due to (i) the complexity of coordinating the collection of (unstructured) information from multiple organizations and (ii) the effort of compiling and updating a consistent situational overview.

3.2. Functional and quality requirements

Based on the background and motivation of the KoordTool, 18 functional and 9 qualitative requirements were identified through the course of several structured and semi-structured interviews with stakeholders from CSIRTs and NCSCs. The full list is outlined in Appendix A

4. Operational incident coordination and cooperation platform – KoordTool

4.1. Architecture

Based on the requirements defined in Section 3.2 and stakeholder interviews, we developed an architecture outline. We split the architecture into two main parts, as shown in Figure 2:

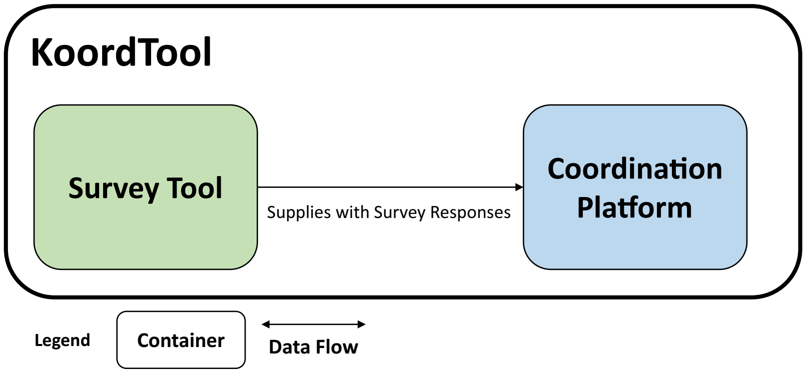


Figure 2. Architecture outline with the building blocks coop-app and survey tool.

- a **survey tool** that allows the collection of survey data and offers methods and tools to gather and process the data accordingly. The survey tool gathers the survey responses.
- a **coordination platform** that supports the aggregation and adequate representation of the survey responses (e.g., coop-reports).

We noticed that there are a number of existing open source and commercial solutions that could be used within the KoordTool. However, in order to be selected, the following three prerequisites have to be considered for implementation: First, the software has to be licensed as open source and provide APIs to extract survey responses. Second, the software's source code has to be well documented in order to provide and adapt APIs. Third, the software's structure and release must allow hosting on premise (i.e., no dependency on cloud providers).

After narrowing down software solutions based on the aforementioned prerequisites, only three suitable open-source software projects could be identified: LimeSurvey,[5] JDeSurvey[6] and Surveyproject.[7] The following analysis was conducted for the selection of a suitable survey tool:

- **Extensive Source Code Documentation**: LimeSurvey's manual describes each feature in detail including some insights into the underlying code. Their developer-oriented documentation is not as extensive and needs supplementary expertise in the *Yii framework*. Still, the effort needed to understand and be able to build on top of LimeSurvey was estimated as vastly smaller than when building on top of the less documented JDeSurvey or Surveyproject.
- **Regular Updates**: The availability of regular updates and bug fixes vastly increases the software's security and compatibility. LimeSurvey has an active development community with recent code updates compared to the last updates of JDeSurvey (when conducting the survey in October 2019 5 years ago) and Surveyproject (2 years ago).
- **Dynamic Surveys**: Surveyproject supports complete changeability of surveys, including questions, question groups and participant lists. LimeSurvey only allows changes in surveys while temporarily stopping the survey.
- **Central Participant Database and Survey Templates**: Both LimeSurvey and Surveyproject support saving questionnaires, question groups and participant lists. LimeSurvey additionally unites all of these into surveys that can be exported, imported, copied or used as templates. JDeSurvey only supports exporting and importing questionnaires.

These comparisons were further examined in terms of the fulfillment of the functional requirements outlined before, which resulted in the selection of LimeSurvey as survey tool.

4.2. Proof-of-concept implementation

Based on the preliminary architecture defined in Section 4.1, we designed a proof-of-concept implementation with the main building blocks in Figure 3:

- **Coop-app**: The coop-app (see Section 4.2.1) is responsible for generating a dynamic coop-report and visualizing it within the coop-app dashboard (see Section 4.3).
- **LimeSurvey**: An open-source survey application (see Section 4.2.2), which supports the creation of surveys and the processing of survey responses from multiple participants.
- **Email**: A standard SMTP service provided in order to allow LimeSurvey to send email invitations.

Coop-app and *LimeSurvey* are both full-stack web applications. Both containers are detached from each other allowing separation on multiple machines during deployment and for a more flexible secure environment (Cito et al., 2017).

Figure 3 outlines the proof-of-concept implementation[8] consisting of the following components:

- *KoordTool*: Proof-of-concept including the coop-app, the LimeSurvey and email containers.
- *Coop-app [Container]*: Software container responsible for aggregating coop-reports and providing access to coop-app dashboards for the main coordinator.
- *Coop-App Dashboard [Endpoint]*: Endpoint to the user. Displays the coop-report and is the primary interface for user interaction.

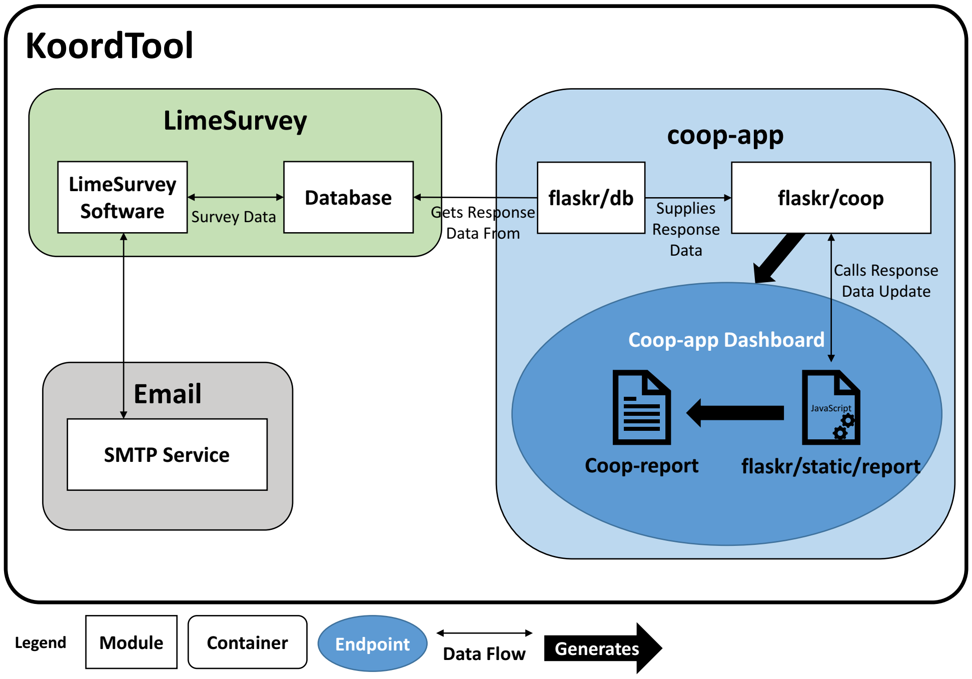


Figure 3. Proof-of-concept implementation and deployment outline with the containers coop-app, LimeSurvey and email.

- *Flaskr/db [Code]*: Flask class. Collects participant reports and survey data by accessing LimeSurvey/Database [Component].
- *Flaskr/coop [Module]*: Flask module. Responsible for generating accessible coop-app dashboard web pages.
- *Flaskr/static/report [Module]*: JavaScript file. Responsible for aggregating data, generating a coop-report to be visualized in a coop-app dashboard.
- *LimeSurvey [Container]*: Software container responsible for all survey functionality and storing survey data and participant reports.
- *LimeSurvey [Component]*:Instance of open-source software LimeSurvey Version 3.15.5 + 181115.
- *Email [Container]*: Email container responsible for SMTP service and used by LimeSurvey to manage email invitations to surveys.
- *Database [Component]*: MySQL database instance storing survey data and participant reports. Accesspoint for flaskr/db[Code].
- *SMTP Service [Module]*: Service on email server that is utilized by LimeSurvey to send and receive emails.

4.2.1. Coop-app implementation

The coop-app consists of a server and a client application (cf. Figure 3). The server application is developed with the web application framework Flask[9] (Grinberg, 2018). After start, the coop-app provides an index page accessible via the server's IP address or URL. In parallel, the *flaskr/db* module retrieves all existing surveys from the *LimeSurvey* database. For each survey, the *flaskr/coop* module generates a new web page (i.e. coop-app dashboard) on the Flask web server, which is accessible via a unique URL (for example, http://koordtool:5000/coop/1).

On the client side in Figure 3, as soon as a browser accesses the URL of a coop-app dashboard, an empty HTML skeleton page is delivered. The skeleton will be populated by the JavaScript module *flaskr/static/report* once the coop-app dashboard is accessed. Specifically, the JavaScript *flaskr/static/report* is sent with the coop-app dashboard when accessed. The coop-app dashboard then executes the JavaScript, which now queries survey response data from an AJAX interface in the *flaskr/coop* module. Afterwards, the *flaskr/static/report* processes this data into a coop-report consisting of the participant status table, feedback graphs and trend graphs (see Sections 4.3.1, 4.3.3 and 4.3.4). Finally, the coop-report is visualized in the coop-app dashboard.

In order to keep the coop-app dashboard up-to-date, the *flaskr/static/report* module frequently repeats this process by generating new coop-reports and replacing outdated ones in the coop-app dashboard. Hence, the user always retrieves an up-to-date coop-report in the coop-app dashboard.

For easier testing and deployment, the authors deployed the coop-app using Docker containers via a prepared Docker file.

4.2.2. LimeSurvey

LimeSurvey[10] is an open-source survey software that can be used, e.g., to create surveys, collect responses and export data to other applications. In the KoordTool, an unmodified instance of LimeSurvey Version 3.15.5 + 181115 is being used and deployed via *Docker*. The *Docker* container also includes a local MySQL database instance for the ease of deployment. In the cyber coordination and cooperation platform, LimeSurvey is primarily used to create surveys and collect responses. The responses are fetched by the coop-app (cf. Section 4.2.1).

The LimeSurvey question types yes/no, single choice (of a multiple-choice question), text question (all variations) and numerical input are supported in the KoordTool. Except for the text questions, all other questions can be visualized as feedback and trend graphs in the coop-app dashboard (see Section 4.3).

4.3. Coop-app dashboard

As described in Section 4.2, the coop-app generates a coop-report that can be accessed through the coop-app dashboard. An example view of the coop-app dashboard based on an example with the survey ID 1 can be seen in Figure 4. The idea behind the dashboard is that this dashboard supports the main coordinator in times of crisis or large-scale incidents quickly with the most relevant information from the respondents (cf. Section 3.1).

The coop-app dashboard in Figure 4 consists of the following elements. Each number, highlighted in red, in Figure 4 corresponds the listed elements:

- **(1) Toggle View**, switches between the participant status table (see (2), Section 4.3.1) and the details table (see Section 4.3.5)
- **(2) Participant Status Table** (see Section 4.3.1), an aggregated overview of each participant response
- **(3) Time Slider** (see Section 4.3.2), a time filter
- **(4) Export**, a drop-down button, supports quick and full coop-report export as html or pdf functionality
- **(5) Option**, a drop-down button, supports the configuration of highlight settings, e.g. for overdue responses
- **(6) Search Bar**, allows searching for keywords in the participant status table (see **(2)**)
- **(7) Feedback Graphs** (see Section 4.3.3), visualizations of the aggregated (up-to-date) responses
- **(8) Trend Graphs** (see Section 4.3.4), visualizations of responses over time

In the following sections, each of the elements are further described.

4.3.1. Participant status table

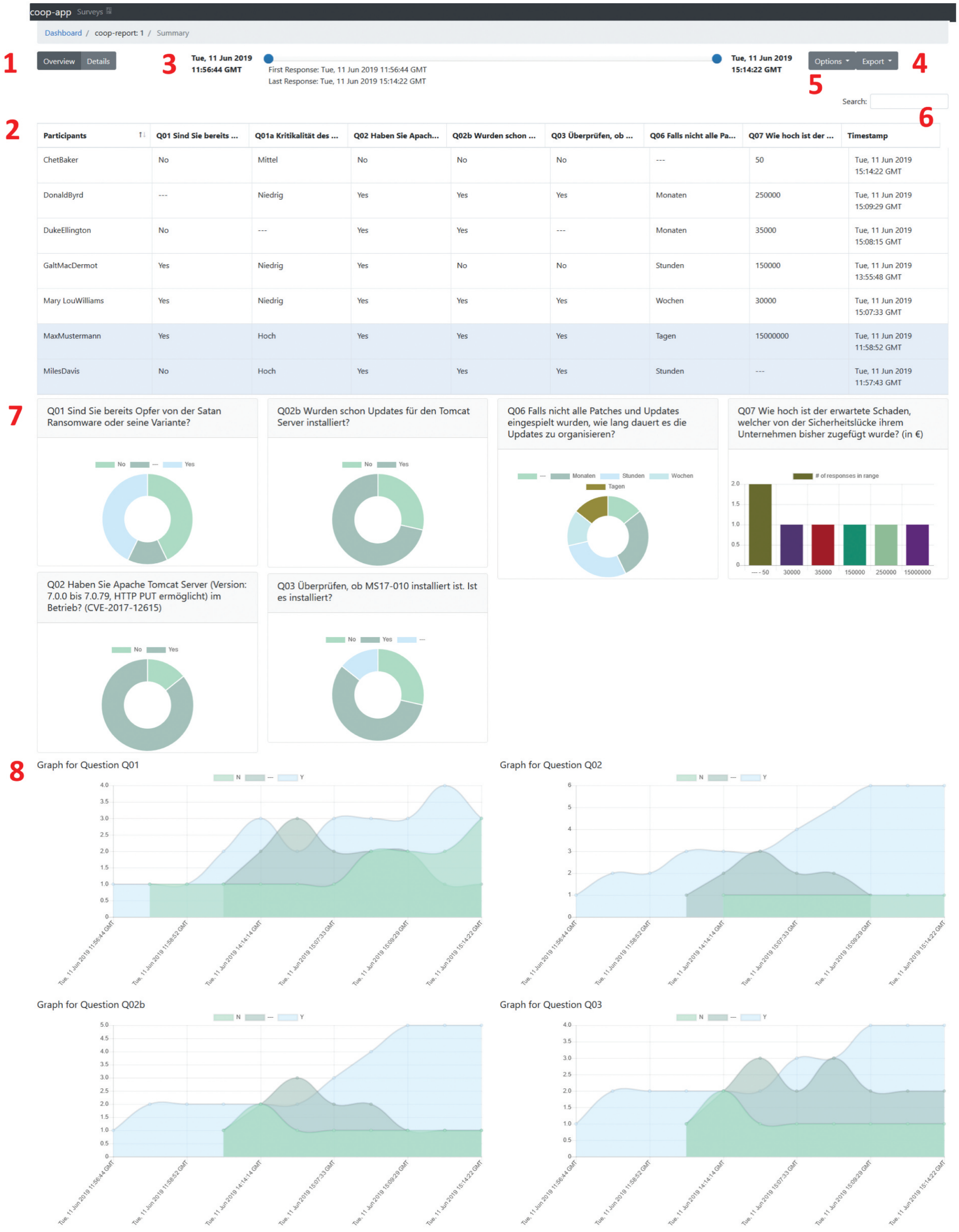
The participant status table (see **(2)** in Figure 4) provides an aggregated overview of the current status of each participant. A table row represents an individual participant and its most recent aggregated responses. By default, the participant status table is displayed in the coop-app.

4.3.1.1. Processes updated responses.

Within our app, it is possible that participants can update their status and submit revised surveys to the KoordTool. Therefore, we had to manage this in the participant status table. If a participant did not answer a question in the participant's most recent participant response, the last given answer (if there has been one before) is shown. Not answering a question therefore signifies that there are no further updates and "no change" from a data perspective. The only exceptions are answers in long text format. These are always taken from the most recent participant-report, even if empty.

4.3.1.2. Highlighting responses.

Participants who have not sent an update within a certain time frame are automatically highlighted in the participant status table. By default, any participants who have not submitted a participant report in the last *2 hours* will be marked in *blue*. For example, in Figure 4, the participants "*MaxMustermann*" and "*MilesDavis*" are highlighted in blue, i.e. they have not submitted an updated report within the last 2


coop-app Surveys
Dashboard / coop-report: 1 / Summary
1
Overview
Details
3
Tue, 11 Jun 2019 11:56:44 GMT
Tue, 11 Jun 2019 15:14:22 GMT
Options
Export
4
5
Search:
6
2
7
8

First Response: Tue, 11 Jun 2019 11:56:44 GMT
Last Response: Tue, 11 Jun 2019 15:14:22 GMT

Participants	Q01 Sind Sie bereits ...	Q01a Kritikalität des ...	Q02 Haben Sie Apach...	Q02b Wurden schon ...	Q03 Überprüfen, ob ...	Q06 Falls nicht alle Pa...	Q07 Wie hoch ist der ...	Timestamp
ChetBaker	No	Mittel	No	No	No	---	50	Tue, 11 Jun 2019 15:14:22 GMT
DonaldByrd	---	Niedrig	Yes	Yes	Yes	Monaten	250000	Tue, 11 Jun 2019 15:09:29 GMT
DukeEllington	No	---	Yes	Yes	---	Monaten	35000	Tue, 11 Jun 2019 15:08:15 GMT
GaltMacDermot	Yes	Niedrig	Yes	No	No	Stunden	150000	Tue, 11 Jun 2019 13:55:48 GMT
Mary LouWilliams	Yes	Niedrig	Yes	Yes	Yes	Wochen	30000	Tue, 11 Jun 2019 15:07:33 GMT
MaxMustermann	Yes	Hoch	Yes	Yes	Yes	Tagen	15000000	Tue, 11 Jun 2019 11:58:52 GMT
MilesDavis	No	Hoch	Yes	Yes	Yes	Stunden	---	Tue, 11 Jun 2019 11:57:43 GMT

Q01 Sind Sie bereits Opfer von der Satan Ransomware oder seine Variante?

Q02b Wurden schon Updates für den Tomcat Server installiert?

Q06 Falls nicht alle Patches und Updates eingespielt wurden, wie lang dauert es die Updates zu organisieren?

Q07 Wie hoch ist der erwartete Schaden, welcher von der Sicherheitslücke ihrem Unternehmen bisher zugefügt wurde? (in €)

Q02 Haben Sie Apache Tomcat Server (Version: 7.0.0 bis 7.0.79, HTTP PUT ermöglicht) im Betrieb? (CVE-2017-12615)

Q03 Überprüfen, ob MS17-010 installiert ist. Ist es installiert?

Graph for Question Q01

Graph for Question Q02

Graph for Question Q02b

Graph for Question Q03

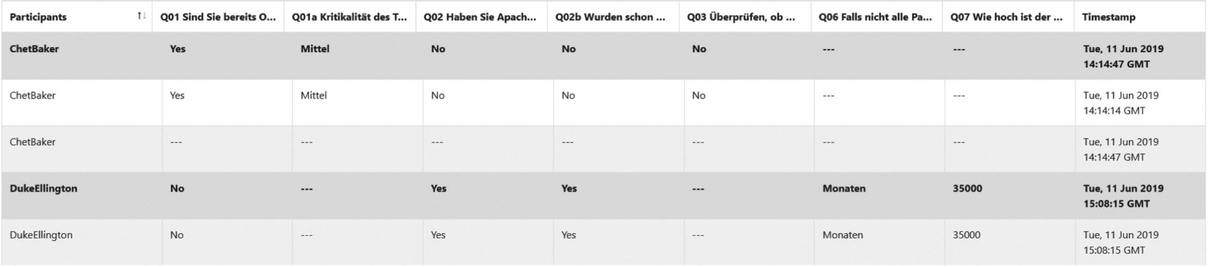
N
—
Y
Tue, 11 Jun 2019 11:56:44 GMT
Tue, 11 Jun 2019 11:58:52 GMT
Tue, 11 Jun 2019 14:14:14 GMT
Tue, 11 Jun 2019 15:07:33 GMT
Tue, 11 Jun 2019 15:09:29 GMT
Tue, 11 Jun 2019 15:14:22 GMT

Figure 4. Coop-app dashboard (screenshot).

hours. How much time must elapse before a participant row is highlighted as out-of-date can be specified in the option dropdown menu (see **(5)** in Figure 4) under "*Mark as outdated after*."

4.3.2. Time slider

The time slider (see **(3)** in Figure 4) filters the responses in the participant status table and details table in the form of a "from-to" filter. Each value of



Participants ↑↓	Q01 Sind Sie bereits O...	Q01a Kritikalität des T...	Q02 Haben Sie Apach...	Q02b Wurden schon ...	Q03 Überprüfen, ob ...	Q06 Falls nicht alle Pa...	Q07 Wie hoch ist der ...	Timestamp
ChetBaker	**Yes**	**Mittel**	**No**	**No**	**No**	**---**	**---**	**Tue, 11 Jun 2019 14:14:47 GMT**
ChetBaker	Yes	Mittel	No	No	No	---	---	Tue, 11 Jun 2019 14:14:14 GMT
ChetBaker	---	---	---	---	---	---	---	Tue, 11 Jun 2019 14:14:47 GMT
DukeEllington	**No**	**---**	**Yes**	**Yes**	**---**	**Monaten**	**35000**	**Tue, 11 Jun 2019 15:08:15 GMT**
DukeEllington	No	---	Yes	Yes	---	Monaten	35000	Tue, 11 Jun 2019 15:08:15 GMT

Figure 5. Coop-app: full response table (cropout).

the time slider specifies a time at which a participant report has arrived. For example, the time slider in Figure 4 shows that no messages are being filtered. All participant reports received at or between the two timestamps are displayed in the participant status table and details table. Any changes to the time slider will be considered at the next update (every 5 seconds).

4.3.3. Feedback graphs

Feedback graphs (see **(7)** in Figure 4) visualize the aggregated responses of the participants. The feedback graphs are sorted in the dashboard by question ID and are organized in foldable containers.

For the question types ”*multiple choice*” and ”*yes/no*”, a donut chart and, for numeric answers, a bar chart are generated to display the current status of the answers based on the participant status table (see **(2)** in Figure 4). Text question answers (e.g., open text questions) are not visualized in the feedback graphs. They can be read in the participant status table or the details table.

For the visualization of numerical questions, bar charts are generated. Using the k-means algorithm, the answers are subdivided in up to six different classes defined by numerical proximity. The Y-axis represents the amount of current responses in a specific class, while the X-axis represents the specified classes and their value ranges.

In general, 10 color sets are prepared for the visualization of records. If a question has more than 10 different answer choices, additional sets of colors will be generated randomly.

4.3.4. Trend graphs

Trend graphs (see **(8)** in Figure 4) are being generated for multiple choice and yes/no question types. Each question generates its own linear graph portraying changes in the aggregated feedback (i.e. the responses of the participants) over time.

In each chart, each answer option (including no answer) is a separate data set and is presented in the form of its own function (and thus also color). The Y-axis indicates the number of responses in all cases. The X-axis indicates the time since the first participant report arrived. Each step on the X-axis is a time when a participant report has arrived, but not necessarily every step is labeled.

4.3.5. Details table

The details table lists all received participant reports of the survey, grouped by participant and sorted by timestamp. This data table serves as the basis for generating the participant status table (see Section 4.3.1). An example screenshot can be seen in Figure 5. Each participant is summarized in an aggregated table row (highlighted bold). The aggregated table rows are highlighted by a dark gray background and bold font. These tables rows for the participants are identical to the participant's rows in the participant status table. Below, each aggregated table row, are all participant reports, which have been submitted, sorted by timestamp. These rows alternate between white and light gray background.

Furthermore, the table can be filtered using the options drop-down (see (5) in Figure 4), the time slider (see (3) in Figure 4) and the search bar (see (6) in Figure 4).

5. Evaluation and discussion

One of the main questions is of course if and to what extent the introduced approach and in particular the implemented KoordTool can improve incident coordination and information sharing processes compared to the state of the art (see Section 2). To evaluate the KoordTool, we conducted a user study and a security analysis to identify strengths and shortcomings.

5.1. User study

This user study was conducted as part of a stakeholder workshop that focused on performing key tasks of NCSCs using the KoordTool. In particular, it focused on the collection and aggregation of information to create common cyber operational pictures (CCOPs) and the interpretation of the same to establish CSA. Typically, NCSCs (as well as CSIRTs) act as information brokers and distributors and continuously request, collect, aggregate, summarize and distribute vital information in times of incidents and crises (Skopik et al., 2016). Thus, the target audience of this workshop were members of national authorities, CSIRTs and MSSPs.

In the workshop, participants were challenged with a large-scale cyber incident and had to coordinate their actions based on established CSA through the KoordTool. In the following, we outline the participants, the procedure of the workshop and the results with respect to the applicability of our approach.

5.1.1. Participants

A stakeholder workshop took place in November 2019 at T-System Austria with 19 participants. All participants were experts in CSA and had technical knowledge on cyber security incidents and attacks. In their regular jobs, participants are coordinators or engineers in NCSCs, CSIRTs or MSSPs.

5.1.2. Procedure

The workshop was structured into: (1) introduction, (2) cyber security exercise in two iterations and (3) evaluation. The workshop lasted altogether 5 hours.

5.1.2.1. Workshop introduction. The workshop started with an introduction to the workshop and an explanation of the agenda and goals of the workshop.

5.1.2.2. Cyber security exercise. The cyber security exercise was designed in two iterations. The iterations served as a common storyline in the investigation of required tool support for managing a cyber crisis with large inter-organizational incidents (see Appendix B). In particular, timed injects pushed forward a designed storyline and the participants had to solve tasks from the perspective of a NCSC. As main coordinator (see Section 3.1), they processed the incoming reports regarding various large-scale incidents using the KoordTool. They needed to keep track of the latest attack vectors, security status in certain industry sectors, and had the ability to send off reports on specific incidents or warnings.

In detail, during the scenarios, the participants had to fulfill the following tasks with the support of the KoordTool:

- Decide whom to survey for new information
- Gather and aggregate responses
- Prepare a management report accounting for the current situation
- Recommend possible short-term reactions
- Recommend possible long-term measures

5.1.2.3. Evaluation. After the exercise, the evaluation was conducted with a focus group and surveys. The main goal of the evaluation was to address the following research questions:

- (R1) How would you overall assess the KoordTool for NCSCs?
- (R2) Can the KoordTool be utilized to establish CSA?
- (R3) Which features of the KoordTool are an advantage or disadvantage compared to other existing tools?
- (R4) Which features were missing or which changes would you suggest?

The group feedback session was designed as focus group where each participant could state their feedback on the KoordTool. Individual surveys consisted of eight questions (see Appendix C) and were handed out on paper. Both aspects generated quantitative as well as qualitative evaluation results. On the one side, we let them rate the usefulness and applicability of certain features of the KoordTool (quantitative feedback); on the other side, we gave them the opportunity to express their needs that are not covered sufficiently (qualitative feedback).

Stakeholders were not obliged to participate in both evaluation steps. Their participation was on a voluntary basis.

5.1.3. Findings

The focus group was attended by all 19 participants. As the surveys were voluntarily completed, we collected 12 surveys in total. In the following, the findings of the experimental evaluation are discussed based on the aforementioned research questions.

5.1.3.1. (R1) How would you overall assess the KoordTool for NCSCs?. In the focus group, participants did not doubt that the KoordTool can be used in a NCSC. However, they discussed extensions that could make the tool even more useful (see Section 5.1.3.4). In the survey, most participants suggested that the KoordTool can be used in NCSCs (see Question C.1). In particular in Question C.1, participants rated the overall assessment of the KoordTool very well (3 participants), well (4), satisfactory (4), enough (1) and not satisfactory (0).

In Question C.3, users were asked to rate whether they agree or disagree with certain statements referring to the KoordTool. The statements (abbreviated as hypotheses) are centered on the applicability of the tool by different groups of users (novices, experts), feasibility of the aggregation and representation of results for gaining CSA, and suitability for the various tasks in a NCSC. The answers of the surveys are visualized in Figure 6.

The results in Figure 6 show that most participants (at least 60%) found that the KoordTool offered a structured format to gain CSA (H1), is equally applicable to experts (H3), has high up-to-dateness of data (H6), supports stakeholders that can be geographically distributed (H8), and supports the report creation (H11).

5.1.3.2. (R2) Can the KoordTool be utilized to establish CSA?. In the focus group, most participants found the application of the KoordTool useful for gaining CSA at a national level. The tool makes it much easier to create situation reports for decision makers, enables quick status queries for an incident, and displays the latest relevant information in a form that experts can understand. This aligns with the findings of the survey. Most participants suggested that the KoordTool can be useful for establishing CSA (see question C.2). In particular, participants rated the KoordTool very well (2 participants), well (3), satisfactory (6), enough (1) and

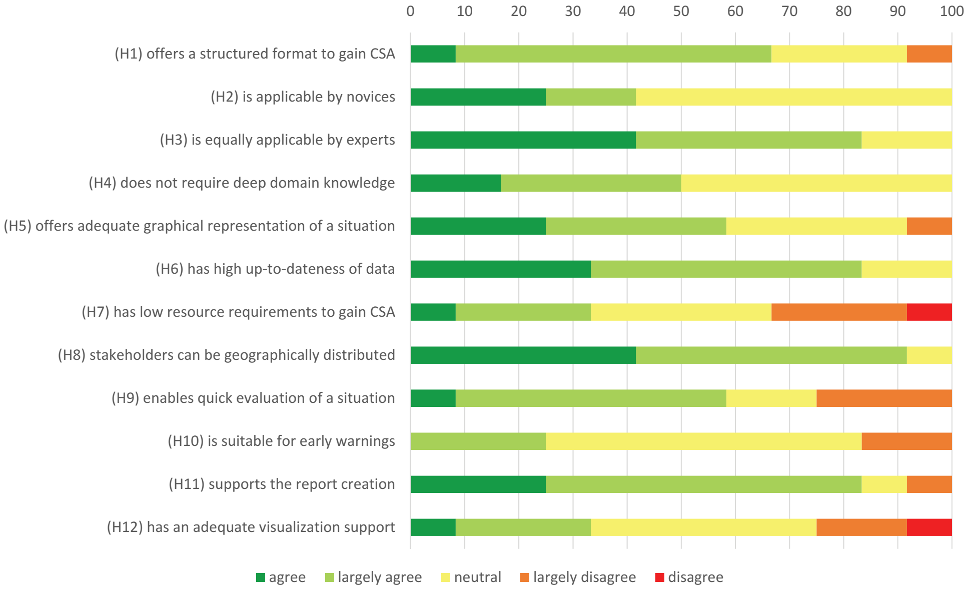


Figure 6. Survey question C.3: Visualization of statement ratings of participants.

not satisfactory (0). Additionally, survey question C.3 incidates that participants largely agree that the KoordTool supports CSA by offering a structured format (H1).

5.1.3.3. (R3) Which features of the KoordTool are an advantage or disadvantage compared to other existing tools?. The following features were most important and posed a clear benefit of the KoordTool compared to other solutions: donut graphs for the quick assessment of aggregated feedback, auto-generated management summary (overview of current situation), and time-slider to weight in only recent responses.

The main critique concerned the available visualization options (which are also reflected by answers to H7 and H12, see question C.3)). Most participants of the workshop mentioned that an overview of the degree of completion of a case would be useful. This means that the situation center would have a better overview of the pending answers and the significance of the current answers. It is also desirable to make changes within an organization more visible, for example, when an organization suddenly reports that it became affected by an issue, this needs to be better visualized.

5.1.3.4. (R4) Which features were missing or which changes would you suggest?. In the focus group and survey (e.g. Question C.7), the participants mentioned the following additional functions as desirable: *comment function* to enrich incoming reports with own interpretation wrt. importance and credibility, *stacked diagrams* to aggregate multiple cases, *extended sort function* to enable sorting by time and per column, *extended filtering* that allows filtering by specific column content, *context-specific filtering*, e.g. filter affected organizations in certain sectors only, *summary reports* aggregated from individual reports, *hiding rows or columns* e.g., concerning unrelated or irrelevant information, and *tagging* to quickly associate a report to a specific case.

In summary, the user study showed that the KoordTool can be used to establish CSA and may be used in the setting of NCSCs. It can reduce the effort to establish a CCOP and support CSIRTs in their operations to oversee reports such as defined in the EU NIS2 directive.

5.2. Security analysis and practical applicability

We finalize this evaluation with a critical review of (technical) security measures and design considerations of our application. In particular, we ensure the basic security properties (C-I-A as well as A-A-A (Forouzan, 2007)) as follows:

- **Confidentiality**: SSL/TLS for communication with the Web server; full disk encryption for the database; S/MIME for email notifications and survey invitations from LimeSurvey
- **Integrity**: measures similar to confidentiality which also effectively prevent tampering
- **Availability**: achieved through redundant deployments with separate network connections
- **Authentication**: dedicated user registration processes and on-boarding procedure (for personal and institutional accounts); established single points of contact per organization; central user management for LimeSurvey and KoordTool
- **Authorization**: extended rights management and individual “trustworthiness” weights to avoid hoaxes and account for potential low-quality reports from new participants
- **Accountability**: seamless logging of application events (answered surveys, delivered reports, etc) to achieve non-repudiation, as well as logging of underlying infrastructure (login attempts, connections, sessions, etc.)

6. Lessons learned and recommendations

6.1. Establish CSA in large-scale incidents requires a lot of information

Establishing cyber situational awareness is key to making justified decisions in challenging incident response scenarios. Information types and complexity can be manifold, ranging from simply knowing if an organization is being affected by a specific malware, to rather complex results of system dependency analysis. None of these types of information must be neglected – depending on the current situation, they all may highly influence decisions on next steps in an inter-organizational, cross-border incident response process.

6.2. Operational coordination in large-scale incidents and crises needs tool support

Coordinating the exchange of vital security information among potentially hundreds of entities is challenging, especially if the information being exchanged highly depends on a particular incident and situation. No pre-modeled information schema is feasible; however, some sort of structure is required to enable the quick automatic aggregation of information elements. Survey tools address the need for flexibility to adapt questions and answer candidates quickly on the one side and allow the structured interrogation of a large number of stakeholders on the other side.

6.3. Adequate visualizations support the main coordination

Different roles and types of people demand different visualizations which further depend on the particular situation and actions to take. Eventually, a supporting system is expected to show data relevant for decision-making and suppress everything else which might distract. The tricky part here is to visualize complex (and dynamically changing!) data in a way that a wide range of users can comprehend a situation quickly, and on the other side not to predetermine any decisions. Eventually, it is still the human expert who makes the decision, not the system that collects and visualizes the underlying data.

6.4. Technology needs to be flexible

Every incident is different, every crisis has its own characteristic. Although incident response playbooks are important for guided response, the actual response activities emerge dynamically during handling an incident. Thus, while timely response requires tool support to be efficient, these tools need to be adaptive in terms of handled information and executed workflows at the same time.

7. Conclusion and future work

This article presented an approach on how to support cyber situational incident coordination connecting inter-organizational stakeholders in a distributed environment. Therefore, we assessed the current state of the art and techniques to coordinate large-scale incidents across organizations and sectors (e.g., by NCSCs, CSIRTs, etc.). Current technologies that are utilized, such as email, shared online documents or CTI tools, provide some functionality to exchange information but often do not fully support the needs of the main coordinator. The reason for this is that the requirements of NCSCSs and CERTs, as analyzed in this article, are quite special and an excellent knowledge management is key. Therefore, we proposed a new approach and PoC implementation – the KoordTool – that enables the main coordinator to request information from participants via surveys and automatically aggregate and visualize the same in an appropriate fashion to answer incident-response-specific issues efficiently. A novelty here is that surveys can be updated and resent again to gather updates of participants and to adequately account for the quick changes of a cyber security situation. In this case, the answers and answer frequency can be tracked by the coordinator to estimate how up-to-date the aggregated information actually is. Both, the “updateability” and quick automatic aggregation of information, are vital to gain accurate CSA.

We evaluated our approach with a user study where we challenged a mix of domain experts and staff from CSIRTs, MSSPs and NCSCs with realistic situations and asked them to apply the KoordTool. Most participants found the application of the KoordTool useful for gaining CSA at national level. The tool makes it much easier to create situation reports for decision makers, enables quick status queries for an incident, and displays the latest relevant information in a form that experts can understand. However, the visualization still has room for improvement and the participants made several suggestions for the next release, as also documented in this article. Based on this evaluation, we derived several actionable recommendations for incident coordination.

Notes

1. https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone

2. https://www.misp-project.org/
3. https://stixproject.github.io/
4. https://taxiiproject.github.io/
5. https://www.limesurvey.org/
6. https://github.com/JD-Software/JDeSurvey
7. http://www.surveyproject.org/
8. The source is available at https://github.com/ait-cs-IaaS/koord2ool
9. https://palletsprojects.com/p/flask/
10. https://www.limesurvey.org/
11. Notice, we invented a fictional vulnerability to simplify our scenario. The original flaws, Spectre and Meltdown, have very specific properties, affect processors quite differently, and we wanted to avoid any technical discussions during the exercise, which are not relevant in this context.

Acknowledgments

Otmar Lendl from the Austrian Computer Emergency Response Team (CERT.at) provided valuable insights into the daily operations of national CERTs and supported the requirement phase. We would like to thank Benjamin Akhras, Manuel Warum, and Martin Galusinski for their valuable support with numerous implementation aspects of the KoordTool. We further like to thank Theodoros Nikolakopoulos and Rossella Mattioli both from ENISA, for their valuable feedback on the concept and PoC implementation.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work has been partly funded by the Connecting Europe Facility (CEF) program in course of the project AWAKE [2020- AT-IA-0254].

ORCID

Maria Leitner http://orcid.org/0000-0003-1371-5446
Florian Skopik http://orcid.org/0000-0002-1922-7892

References

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Atif, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643–652. https://doi.org/10.1016/j.cose.2012.04.001

Bronk, H., Thorbruegge, M., & Hakkaja, M. (2006). CSIRT setting up guide in english. *Technical Report*. ENISA. https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport

Cito, J., Schermann, G., Erik Wittern, J., Leitner, P., Zumberi, S., & Gall, H. C. (2017). An empirical analysis of the docker container ecosystem on github. *2017 IEEE/ACM 14th International conference on mining software repositories (MSR)* (pp. 323–333). IEEE, Buenos Aires, Argentina.

Conti, G., Nelson, J., & Raymond, D. (2013, June). Towards a cyber common operating picture. *2013 5th International Conference on Cyber Conflict (CyCon)* (pp. 1–17). IEEE, Thessaloniki, Greece.

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

ENISA. (2012). National cyber security strategies: Practical guide on development and execution. *Technical Report*. https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport

ENISA. (2017). ENISA overview of cybersecurity and related terminology. *Technical Report Version 1*. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology#:text=To.

European Commission. (2016). *The directive on security of network and information systems (NIS directive)*. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Parliament, Council of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, 12. http://data.europa.eu/eli/dir/2022/2555/oj.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Forouzan, B. A. (2007). *Cryptography & network security*. McGraw-Hill, Inc.

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

Franke, U., Johan, T., Ivar, J., & Cham, T. M. (2021). The cost of incidents in essential services—data from Swedish NIS reporting. In D. P. David & A. Mermoud (Eds.), *Critical* *information infrastructures security* (pp. 116–129). Springer International Publishing.

Giacobe, N. A. (2010, April). Application of the JDL data fusion process model for cyber security. In Jerome J. B. (Ed.), *Proceedings SPIE 7710, multisensor, multisource information fusion: Architectures, algorithms, and applications* (Vol. 7710, pp. 77100R–77100R–10). Society of Photo-Optical Instrumentation Engineers (SPIE).

Grinberg, M. (2018). *Flask web development: Developing web applications with python*. O'Reilly Media, Inc.

Happa, J., Agrafiotis, I., Helmhout, M., Bashford-Rogers, T., & Goldsmith, M. (2021). Assessing a decision support tool for SOC analysts. *Digital Threats: Research and Practice*, *2*(4), 1–26. https://doi.org/10.1145/3450973.

Hellwig, O., Quirchmayr, G., Huber, E., Goluch, G., Vock, F., & Pospisil, B. (2016, August). Major challenges in structuring and institutionalizing CERT-communication. *2016 11th International Conference on Availability, Reliability and Security (ARES)* (pp. 661–667). IEEE, Salzburg, Austria.

Hodgson, Q. E., Clark-Ginsberg, A., Haldeman, Z., Lauland, A., & Mitch, I. (2022). *Managing response to significant cyber incidents: Comparing event life cycles and incident response across cyber and non-cyber events*. RAND Corporation.

Husák, M., Sokol, P., Žádník, M., Bartoš, V., & Horák, M. (2023). Lessons Learned from Automated Sharing of Intrusion Detection Alerts: The Case of the SABU Platform. *Digital Threats: Research and Practice*, *4*(4), 1–48. https://doi.org/10.1145/3611391 Accessed2024-03-14.https://dl.acm.org/doi/10.1145/3611391.

Kocher, P., Horn, J., Fogh, A., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T. & Schwarz, M. (2019). Spectre attacks: Exploiting speculative execution. *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 1–19). IEEE, San Francisco, CA, USA.

Kokkonen, T., Hautamäki, J., Siltanen, J., & Hämäläinen, T. (2016, May). Model for sharing the information of cyber security situation awareness between organizations. *2016 23rd International Conference on Telecommunications (ICT)* (pp. 1–5). IEEE, Thessaloniki, Greece.

Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., & Ahn, G.-J. (2019, November 11–15). Matched and mismatched SOCs: A qualitative study on security operations center issues. In L. Cavallaro, J. Kinder, X. Wang, & J. Katz. (Eds.), *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019* (pp. 1955–1970). ACM, London, UK.

Kruidhof, O. (2014). Evolution of national and corporate CERTs-trust, the key factor. In M. Hathaway (Ed.), *Best practices in computer network defense: Incident detection and response* (pp. 81–96). IOS Press.

Kucek, S., & Leitner, M. (2020). An empirical survey of functions and configurations of open-source capture the flag (CTF) environments. *Journal of Network and Computer Applications*, *151*, 102470. https://doi.org/10.1016/j.jnca.2019.102470

Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 139–148. https://doi.org/10.1080/19393555.2020.1813851

Leitner, M., Timea, P., & Florian, S. (2017). Situational awareness for strategic decision making on a national level. In F. Skopik (Ed.), *Collaborative cyber threat intelligence* (pp. 225–276). CRC Press.

Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Fogh, A., Mangard, S., Kocher, P., Genkin, D., Yarom, Y. and Hamburg, M., & Horn, J. (2018). Meltdown: Reading kernel memory from user space. In Andrew A. C. (Ed.), *27th USENIX security symposium (USENIX security 18)* (pp. 973–990). USENIX Association.

NATO. (2022). Allied Joint Doctrine. In Allied joint publication *AJP-01 edition F version 1*. NATO Standardization Office (NSO).

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Pahi, T., Leitner, M., & Skopik, F. (2017a). Analysis and assessment of situational awareness models for national cyber security centers. *Proceedings of the 3rd International Conference on Information Systems Security and Privacy - ICISSP* (pp. 334–345). Porto, Portugal: INSTICC, SciTePress.

Pahi, T., Leitner, M., & Skopik, F. (2017b). Preparation, modelling, and visualisation of cyber common operating pictures for national cyber security centres. *Journal of Information Warfare*, *4*(16), 15.

Rourke, M., Eccleston-Turner, M., Phelan, A., & Gostin, L. (2020). Policy opportunities to enhance sharing for pandemic research. *Science*, *368*(6492), 716–718. https://doi.org/10.1126/science.abb9342

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

Seker, E., & Huseyin Ozbenli, H. (2018, June). The concept of cyber defence exercises (CDX): Planning, execution, evaluation. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1–9). Glasgow, UK.

Skopik, F. (2017). *Collaborative cyber threat intelligence: Detecting and responding to advanced cyber attacks at the national level*. CRC Press.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Zhao, H., Tang, W., Zou, X., Wang, Y., & Zu, Y. (2019). Analysis of visualization systems for cyber security. In Patnaik, S., & Jain, V. (Eds.), *Recent developments in intelligent computing, communication and devices* (pp. 1051–1061). Springer. https://doi.org/10.1007/978-981-10-8944-2_122

Appendix A. Functional and Quality Requirements

Eighteen functional and nine qualitative requirements were identified in the course of several structured and semi-structured interviews with stakeholders from CSIRTs and NCSCs. The following lists contain collections of the most important functional (abbreviated: F) and qualitative (abbreviated: Q) requirements.

The functional requirements are:

F-1 The system must provide moderators with the ability to create, delete and change questions within a survey.

F-2 The system must provide participants of a survey with the ability to examine questions within a survey.

F-3 The system must provide participants of a survey with the possibility to submit one or more participant-reports.

F-4 The system must provide moderators of a survey with the ability to grant access to an active survey (e.g., via email).

F-5 The system must provide moderators of a survey with the ability to add, change and remove questions in an active survey.

F-6 The system must provide moderators of a survey with the ability to add and remove participants from an active survey.

F-7 The system must provide participants with the ability to authenticate themselves before accessing an active survey.

F-8 The system should be able to visualize live participant reports that are being created.

F-9 The system should provide a table summarizing all participant reports of a survey.

F-10 The system must provide surveys for coordinating a coop-report (situation report).

F-11 The system must allow moderators to include participants in a survey.

F-12 The system must allow moderators to enable and disable surveys.

F-13 The system must allow moderators to modify a survey based on the progress of the related situation.

F-14 The system must allow moderators to access coop-reports for surveys within their authorization.

F-15 The system must be able to display the coop-report of a survey from any point in time since its creation.

F-16 The system must allow moderators to stop a survey.

F-17 The system should allow the survey participant to generate a Participant Report.

F-18 The system must allow administrators to create, delete and manage users.

F-19 The system must allow moderators and administrators to authenticate themselves to the system (for example, using a login page).

The qualitative requirements (with labels in brackets) are:

Q-1 The system must be accessible via a web-based user interface (GUI). *(usability)*

Q-2 The web interface should be responsive. *(usability)*

Q-3 The system should clearly separate the front-end from the back-end. *(transferability)*

Q-4 The system is able to save data of a deleted session inaccessible to the front-end. *(security)*

Q-5 The system is able to replicate all data regularly. *(security)*

Q-6 The system must store participants' reports in a traceable manner together with a timestamp. *(traceability)*

Q-7 The system must save changes to surveys in a traceable manner (including a timestamp). *(traceability)*

Q-8 The system must save any creation, modification and deletion of users in a traceable manner (e.g. with a timestamp). *(traceability)*

Appendix B. Cyber Security Exercise Scenario

Scenario, Participant Roles and Tasks

The participants assume the analysts' role in a fictitious NCSC, where they are challenged with handling a series of simulated large-scale incidents of which they get informed by a number of critical infrastructure providers. Their task is to aggregate incoming reports, rate the current situation, gain CSA and create summaries for decision makers. In order to keep the simulation realistic, the participants have to face a shift change (i.e., they take over in the middle of a simulated scenario where a number of events have already been reported) and all incidents and situations are based on real cases.

When the shift is handed over, some incidents are already recorded, identified or even properly evaluated. In the storyline, it means that the NCSC has already identified two more serious incidents (FreezeUp and BadRabbit – see below) and that they have already created and sent out surveys to single infrastructure providers to gather more insights. In a real NCSC, usually several incidents are handled in parallel, and the participants have to decide which events are connected and belong together. If there are findings that are relevant for multiple infrastructure providers, they can issue warnings. If the incidents have the potential to cause damage or affect a wide range of providers, then surveys can be used to request information directly from the providers.

Incidents

In the course of the workshop scenario, there are three simulated but unrelated incidents, which need to be identified by creating and sending surveys to the appropriate infrastructure providers, and evaluating the aggregated responses.

FreezeUp - CPU Flaw

FreezeUp is a fictional[11] hardware vulnerability in processors. The weakness in the scenario is based on the vulnerabilities found in 2018 called Meltdown (Lipp et al., 2018) and Spectre (Kocher et al., 2019). The public sector (ministries) and the health sector are mainly affected because they have exactly the vulnerable processors in use. The affected Intel processors are used by ministries and public services. The affected AMD processors are used in the healthcare sector. The exchange or change to other hardware components is rather problematic in the health sector, since the processors can also be found in numerous medical devices. The private sector is less affected. A research institute managed to develop and apply an unofficial patch within hours, which changed the status of organizations that applied the patch from "affected" to "likely not affected."

Before participants take over the shift, the NCSC received 12 messages about the FreezeUp incident. In the second shift, the NCSC receives another nine notifications by e-mail. An EU NCSC warns the CERT partners (also NCSC in Austria) that fake e-mails are being distributed in the name of the EU NCSC and ask the recipients to install (fake) security updates. Participants need to find out which organizations are affected, vulnerable and/or did fall prey to fake patches.

BadRabbit - Ransomware

The BadRabbit incident is ransomware active in 2019. At the point where the participants are confronted with this issue, the incident is already quite well developed. Participants take the information from the previous week and aggregate it with arriving reports. In the first shift, the NCL receives 11 reports. Several organizations have solved the incident, which switches their status from "affected" to "not affected." In the second shift, four messages arrive. There are also two voluntary reports. One organization applied the available patch too late (status changes from "not affected" to "affected"). Since an official patch is available, the incident is not as critical as FreezeUp, where no official solution exists. Here, participants need to track which organizations are vulnerable due to late patching.

Data Loss

The CERT from an EU Member State warns the NCSC that they have found leaked data on the Darknet, presumably from Austrian hospitals. The relation to the BadRabbit malware is unclear at that moment. Participants need to find out whether hospitals whose data has been leaked and hospitals affected by the malware are the same.

Appendix C. Survey

The survey contained eight questions. In the following, each question and answers are described.

C.1. Please rate the overall suitability of the KoordTool for a NCSC from your perspective?

(Scale from 5 (not suitable) to 1 (highly suitable))

C.2. Please rate the usefulness of the KoordTool for establishing CSA

(Scale from 5 (not useful) to 1 (highly useful))

C.3. Please rate the following statements for the KoordTool

(Scale: agree, largely agree, neutral, largely disagree, disagree)

- (H1) offers a structured format to gain CSA
- (H2) is applicable by novices
- (H3) is equally applicable by experts
- (H4) does not require deep domain knowledge
- (H5) offers adequate graphical representation of a situation
- (H6) has high up-to-dateness of data
- (H7) has low resource requirements to gain CSA

- (H8) stakeholders can be geographically distributed
- (H9) enables quick evaluation of a situation
- (H10) is suitable for early warnings
- (H11) supports the report creation
- (H12) has an adequate visualization support

C.4. Which features did you find useful?

(open text)

C.5. Would you like to see other visualizations (apart from tables, pie charts and trends)? If yes, which ones?

(open text)

C.6. Would you prefer other answer types (such as open text)? If yes, which ones?

(open text)

C.7. Which other features would you wish for?

(open text)

C.8. Finally, this is an open section for feedback and comments on the KoordTool

(open text)