International Journal of Information Security
https://doi.org/10.1007/s10207-022-00613-7

REGULAR CONTRIBUTION

From scattered data to actionable knowledge: flexible cyber security reporting in the military domain

Florian Skopik[1] · Arndt Bonitz[1] · Volker Grantz[2] · Günter Göhler[3]

Abstract
Numerous cyber situational awareness models have been proposed in recent years. Yet, one of the main challenges still remains mostly unsolved, which is what information sources contribute to the process for establishing cyber situational awareness and how is relevant information collected. While previous scientific works focused on situational awareness models and decision support based on common operating pictures, ingesting and maintaining a consistent data basis for the cyber domain has rarely been studied in detail. However, this is crucial when data distributed across different systems need to be collected, vetted, correlated, de-duplicated, enriched and finally stored as a basis for flexible cyber security reporting. In this paper, we design an approach and a data model that enable to ingest and store the essential information from disparate organizational units and act as a basis for the flexible creation of cyber security reports. We describe the application of this approach and model in a case study together with the Austrian Ministry of Defense (MoD), in which we surveyed existing data sources and transfer paths and rated the applicability of the CCOP data model and accompanying processes in course of a proof-of-concept implementation.

Keywords Cyber security · Cyber situational awareness · Cyber common operating picture · Decision making · Cyber security data sources · Cyber security reporting

1 Introduction

Situational awareness is a cornerstone of justified decision making. It deals with 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* [1]. Cyber situational awareness [2] specifically deals with building awareness in a cyber environment, where in contrast to physical environments, time and space have different meanings. Common operating pictures (COP) include common elements, i.e., relevant to a wide range of actors that help to establish situational awareness and to act upon accordingly. This means that *information must be collected, disseminated, and represented in a way that is useful to several stakeholders* in order to get a common understanding of an ongoing situation [3]. A definition of a COP could be any *actively selected information that is useful to multiple stakeholders with a common overarching mission* [3]. A cyber common operating picture (CCOP) aims to achieve to create this common view for the cyber domain and is an important pillar of establishing cyber situational awareness. Therefore, a CCOP *provides situational awareness despite cyberspace's largely opaque nature, enhances a leader's ability to make quicker critical decisions* [4]. From this definition, it can be inferred that the audience of CCOPs in the military domain is the command level, with the CCOP focusing on the current state of the military organization's cyber assets. The dissemination of a CCOP can be achieved in different ways, tool-based or in paper form. This paper focuses on a tool-based approach using reports.

Dozens of situational awareness models have been discussed in recent decades. For the cyber domain, several of

✉ Florian Skopik
florian.skopik@ait.ac.at

Arndt Bonitz
arndt.bonitz@ait.ac.at

Volker Grantz
volker.grantz@frequentis.com

Günter Göhler
guenter.goehler@bmlv.gv.at

[1] AIT Austrian Institute of Technology, Vienna, Austria

[2] Frequentis AG, Vienna, Austria

[3] Ministry of Defence Austria, Vienna, Austria

Published online: 14 September 2022

these have been adopted. Yet, one of the main challenges still remains mostly unsolved, which is what information sources contribute to the process for establishing cyber situational awareness and how is relevant information collected. While hundreds of scientific works focus on situational awareness models and decision support based on common operating pictures [5], ingesting and maintaining a consistent data basis for the cyber domain has rarely been studied in detail. However, this is crucial when data distributed across different systems need to be collected, vetted, correlated, de-duplicated, enriched and finally stored as a basis for flexible cyber security reporting.

A cyber situation center (CSC) is an organizational unit that centrally perceives and interprets the security status of ICT-based technical infrastructures of one or more organizations, and creates CCOPs as the basis for flexible cyber security reporting. In addition to commercial use in large enterprises, cyber situation reports (CSR) are created in national cyber situation centers for a wide variety of stakeholders.

Unfortunately, there is hardly any publicly available, international literature on the creation of cyber situation reports from highly dispersed data at the state level, specifically for the military domain. We therefore investigate this aspect in this paper. For that purpose, we carefully distinguish the notions of *information source*, *information class* and *transmission path*, which are often confused. For instance, e-mail is not a source, it is rather a technical transmission path, since the actual information comes however from a technical audit or a commercial threat intelligence feed. Different types, i.e., classes, of information exist, including information about incidents, events, assets, new risks, audit findings, threat intent or threat actors. We aim to survey the different data sources and investigate how they are utilized to enable cyber security reporting in context of a military case study. Notice, the detailed implementation and choice of technologies is not in scope of this paper, which merely focuses on the methodological aspects only.

The contributions of this paper are:

- **Methodology to cyber common operating pictures (CCOP):** We introduce the key properties of CCOPs and outline a methodology together with a process to establish them.
- **CCOP data model:** We specifically focus on a concept to ingest and store the essential information from disparate organizational units into a common model, which acts as a basis for the flexible creation of cyber security reports.
- **Survey and case study with the Austrian MoD:** We describe the results of a case study together with the Austrian Ministry of Defense (MoD), in which we surveyed existing data sources and transfer paths and rated the applicability of the CCOP data model and accompanying processes in course of a proof-of-concept implementation.

The remainder of the paper is organized as follows. Section 2 contains background and related work. Section 3 outlines a methodology for the creation of CCOPs, while Sect. 4 shows the underlying data model, containing the various entities and their relations to capture all the relevant information for the creation of CCOPs. Section 5 reports the findings of a detailed case study carried out 2021 with the Austrian MoD that investigated the application of the introduced CCOP model. Finally, Sect. 6 concludes the paper.

2 Background and related work

In order to understand the rationale behind this paper, it is important to identify what the research objectives are. The main driver was the streamlining and optimization of processes to generate cyber situational awareness for MoDs, with a special focus on the Austrian MoD. Therefore, it is necessary to create the foundations of automation capabilities, which encompasses the definition of a homogenized data model tailored to the needs of the MoD. This is the basis for developing a tool that will assist the experts within the Austrian MoD in creating situational awareness by the means of a CCOP for the command level.

2.1 Terms and definitions

Many definitions of situational awareness already exist and the use of the term can be traced back to the First World War. The early definitions—for example the definition of Hamilton [6], Harwood [7] or Billings [8]—focus on human aspects in different crisis situations. They describe situation awareness as cognitive perception and knowledge transfer. One of the most frequently used definitions of situational awareness is from Endsley [9]. In the literature, decision makers try to understand and evaluate the situation (i.e., to build up situational awareness) in order to then decide which measures should be taken. Munir et al. [10] have defined and explained situational awareness, which is an integral part of command and control, from a military and air force perspective. The authors break down situational awareness into three distinct parts, namely perception (*perception of the status, attributes and dynamics of the entities)*, comprehension (*understanding of entities*) and projection (*estimation of the status of entities in the future*).

Furthermore, in the military domain, the information environment is considered a part of the operational environment, thus influencing decisions of the command level and the employment of capabilities [11]. Gaining a complete picture of the cyber situation is therefore crucial. The term cyber sit-

uational awareness (CSA) transports these basic ideas into the cyber domain. Models for (cyber) situational awareness already exist, including the Situational Awareness Model by Endsley [9], Situational Awareness Model by Okolica et al. [12], and Situational Awareness Reference Model by Tadda and Salerno [13]. The authors of [14] propose a methodology to set up CSA measurement experiments. However, this is done within the context of simulated cyber defense exercises. Focusing on CSA in the networking domain, the authors of [15] propose CRUSOE, an extensible layered data model, which consists of layers describing a system. For example, a layer may describe mission statements, detection and response capabilities or a network topology. In [16], the authors aim to develop a taxonomy of CSA tools and components for network security, while following a three-level model (perception of data and elements of an environment, comprehension of a situation and projection of future states and events). In summary, the literature shows that the models attempt to depict the human cognitive processes in the creation of situational awareness [2]. However, these processes do not yet have a high degree of maturity and the models mentioned in the literature only depict partial aspects.

A cyber common operating picture (CCOP) [4], derived from the concept of general COPs [5], captures the actual cyber security status of an organization's systems for a wide variety of stakeholders, including security staff and decision makers. A CCOP is expected to support security staff and managers to assess a situation and properly respond to risks and security threats. In order to do that many different types and classes of data and information must be collected, aggregated and interpreted. The cyber attack information system (CAIS) framework by Skopik et al. [17] suggests that the national cyber situation center develops nation-wide situational awareness from the information collected, and recommendations for action for effective response to security incidents, as well as long-term recommendations for increasing resilience. Other works focus more on the attribution process and the question to what extent cyber attacks can be associated with known actor groups [18].

2.2 Operational, tactical and strategic levels

CCOPs can have different focus and have diverse functions for the addressees. In order to understand the requirements formulated in Sect. 3.1, it is of great importance to understand the three target levels of a CCOP, namely operational, tactical and strategic. One major concept of modern military theory is the division of war into strategic, operational, and tactical levels. Here, the strategic level focuses on defining and supporting national policy, the operational level focuses on the use of military forces in a theater of operations and the tactical level is concerned with the details of how battles are conducted and is sensitive to the changing parameters of an ongoing engagement [19]. Similar concepts can also be found in other domains for instance in decision making [20]. A good definition, tailored to the military domain is given by Ardil [21]: Strategic military decisions affect all or most of the organization and directly contribute to the achievement of the common goals of the organization. Tactical military decisions serve the implementation of strategic decisions. Operational military decisions are focused on day-to-day operations and have a have a short-term horizon. Also relevant for this paper, the three terms are used in information security management. White [22] postulates three questions that must be addressed by the different levels of security management: Strategic management answers the question "why do security enterprise problems exist?" and is concerned with developing security policies. Tactical management answers the question "how are security problems mitigated?" and deals with the development of security systems which enforce the security policies. Operational management answers the question "what security procedures and practices are to be utilized?" and focuses on the use concrete security tools and technologies.

2.3 Standards and building blocks for a military-oriented CCOP

On a technical level, standards, taxonomies and ontologies already exist to represent relevant information for generating a CCOP in a structured way. The structured threat information expression (STIX) [23] specification from OASIS defines some of these information classes, including incident, event, asset, campaign, malware, threat actor and so on. Others, such as the NISTIR 8138 vulnerability description ontology [24] is more vulnerability-focused, than threat-centric. Also focusing on vulnerabilities, the Common Vulnerability Scoring System (CVSS) is a commonly used framework communicating the characteristics and impacts of vulnerabilities [25]. This rating approach has also been endorsed by the US Department of Defense [26]. The NIST Special Publication 1800-5: IT Asset Management [27] on the other side, contains valuable hints on IT asset management, and the ENISA Reference Incident Classification Taxonomy [28], elaborates, among others, on methods to capture and categorize incident information. Guidelines for assessing information in terms of relevance and reliability of sources are provided by the US Army Field Manual 2-22.3 [29]. Although none of these standards can be used as the exclusive basis for a CCOP in the military environment due to their limited scope on partial aspects, elements can be used or integrated as building blocks into a harmonized data model.

2.4 Tools for supporting the creation of a CCOP

Tools for supporting the creation of a CCOP can be roughly grouped into four categories:

1. Information sources;
2. Information collection tools;
3. Evaluation tools; and
4. Visualization or representation tools.

The (technical) information sources can be anything from simple RSS web feeds, websites or (internal) reporting and ticketing systems to highly specialized information systems such as configuration management databases (CMDBs) or dedicated threat sharing platforms. For instance, MISP[1] is a threat intelligence platform, which allows for sharing indicators of compromise (IOC) within and between organizations. MISP also defines taxonomies, for tagging, classifying and organizing information. Collaborative cyber threat intelligence [30] deals with solutions to enable sharing of security-relevant information, including incident and vulnerability information, across organizational boundaries. While this work is relevant to some extent, we rather focus on sharing of such information within the same organization to make it centrally available for flexible cyber security reporting to decision makers. Help desk software, such as Zendesk, Spiceworks or Jira Service Desk, can also serve as an important information source for the status of different services within the own organization.

Once all the relevant information for CCOPs have been identified, preferably automated mechanisms help to collect this information from diverse sources through technical sources. Ontology-based threat intelligence collection frameworks have been proposed, e.g., [31]; the solution intelMQ[2] is one example of such an automated crawler and collection framework that helps to collect, categorize, de-duplicate, transform and process incoming information in a structures manner. Another project focusing on receiving, enriching and redistributing information is AbuseHelper[3]. Although there have been no updates in the last three years (as of May 2022), AbuseHelper is very well-known for the automated collection of abuse information, especially among national CERTs.

Several approaches for interpretation of collected information and creation of situational awareness exist [32]. In principle, a manual, semi-automated or completely automated approach is feasible. In the latter case, very precise data are essential, should such data not be available, it is valuable to have human experts carry out assessments. Rule-based evaluation engines can aid with the evaluation of a situation. For instance, Cimino et al. [33] describe an adaptive rule-based approach for managing situation-awareness. They detail a generic software architecture for generating situation awareness and propose the use of fuzzy context ontology in order to generate a knowledge base. In addition to approaches that have been described in the scientific literature, there are a number of tools that can be helpful in the automated interpretation of a situation. Focusing on IT security incidents, the semi-automated framework YAFRA[4] aims to extract IOCs from reports and augment them with additional information from external sources. Cortex[5] an observable analysis and active response engine, which offers the possibility to analyze certain chunks of information (called *observables*, i.e., IP addresses, files, domain names, etc.). For example, Cortex allows to automatically check files or their hashes against online antivirus detection engines. It is also part of the Hive Project[6], an open-source platform with the focus on incident response. Taranis NG[7] is another open-source platform, but has a broader focus on OSINT gathering and analysis. It aims to create structured report from unstructured news items. A highly specialized tool is Maltego[8], which is used for open-source intelligence and forensics. Maltego aims to support an analyst with generating a visual representation of a wide variety of OSINT information blocks.

CCOPs can be represented in various ways, depending on the requirements. CCOP systems *should provide tailored and timely information* [4]. The representation can range from fully interactive web-based frameworks, over highly specialized 3D toolkits [34] to text-based reports. Existing visual analytics tools can be used in order to represent a CCOP. Here, several open-source tools exist. Grafana[9] is a popular analytics and interactive visualization tool that may be used to visualize metrics, generate reports, or even generate alarms. Another example is Apache Superset[10], which is concerned with the visualization massive amounts of data. The previously mentioned Taranis NG can generate reports via various presenter modules, such as PDF, HTML or simple text output.

[1] See https://www.misp-project.org/

[2] See https://github.com/certtools/intelmq

[3] See https://github.com/abusesa/abusehelper

[4] See https://github.com/hm-seclab/YAFRA

[5] See https://github.com/TheHive-Project/Cortex/

[6] See https://thehive-project.org/

[7] See https://github.com/SK-CERT/Taranis-NG

[8] See https://www.maltego.com/

[9] See https://grafana.com/

[10] See https://superset.apache.org/

3 Methodology for a cyber common operating picture

In this section, we define the requirements schema to guide the development of cyber common operating pictures (CCOPs), as well as an abstract model to develop a CCOP. We further define metrics that constitute the basis of CCOPs, i.e., the data that are visualized and interpreted in a CCOP, and roughly explain how data are ingested into the underlying data model in the first place.

3.1 CCOP requirements schema

CCOPs can be quite diverse, and depending on their application context, specific requirements arise along five dimensions, specifically if they are used to flexibly create cyber security reports:

Scope and level: The scope and the target level of the situation reports shape the structure of the CCOP development process, as these strongly influence the selection of the information sources. At the operational level, for example, significantly more technical data sources and more detailed information are required than at the strategic level. Cyber situation centers aim to create strategic situation reports, which is why significantly more external context data may have to be included. Contextual data includes political, economic, and demographic information. For instance, it might be helpful to understand the background of an APT [30] or a wave of cyber industrial espionage and thus to create an early warning for potential victims. The aim is to be able to prepare long-term and medium-term decisions, therefore the essential relationships and possible forecasts must be prepared without detailed technical explanations.

Frequency and interval: CCOPs must be created periodically (daily, weekly, monthly). They must be available on an ad hoc basis in case of incidents, which implies a high degree of flexibility of the CCOP process. It must be noted, however, that the ad-hoc creation of CCOPs can lead to loss of information. Ad hoc reports (snapshots) can only incorporate the information available at one point in time into the construction process. Therefore, the completeness and thus ultimately also the correctness (at the time of completion) is deliberately neglected here. In case of ongoing attacks, cyber campaigns and possibly APTs, there may be greater deviations between the snapshots and the actual status, as the information basis and thus also the assessment of the situation can change quickly.

Output: Output consist of the results of the CCOP process, including warnings, incident reports or stakeholder-specific reports. The recipient of the output strongly influences the content as well as the level of detail of the description of the situation assessment. However, a comprehensive description of the variety of display options is beyond the scope of this paper.

Sources of information: Particular consideration must be given to the diversity of the information sources in the process of creating a CCOP, as the quality of the sources has a strong impact on the assessment of the situation. A distinction can primarily be made between internal and external sources of information. Internal information sources include all information about an organization's own systems and services (e.g., relevant tickets and the extent to which the internal processes and capabilities are affected) and own information channels about new threats (e.g., intelligence information). The external information includes purchased cyber threat information channels, information from partner organizations and OSINT sources [30]. Information sources with appropriate degree of abstraction directly contribute to a situation report, while technical information sources are usually first prepared to meet a suitable form (e.g., the purchased threat intelligence sources often offer technical indicators such as IP addresses, FQDN, hashes, mutexes and the like. These data are compared with own log data and analyzed. The results can then be incorporated into situation reports in a suitable form).

Visualization: A CCOP must be able to visualize the current situation, historical situations, chronological events, the course of communication and the national cyber situation. The relevant information can be visualized in many different ways, e.g., as diagrams (bars, pies), trend lines, traffic light systems, tables with percentages or with the help of geographic maps.

3.2 CCOP process

After the definition of the requirements for a CCOP development process, we present a generalized model in Fig. 1. This model foresees different types of data and information "flowing" into the CCOP development process from a multitude of sources and via various transfer paths. Besides data collection, in the middle part, data aggregation and interpretation takes place and effectively "transforms" data into actionable knowledge. Eventually, the output process depicts this knowledge in an effective way to support decision making.

In CSCs, situation reports are created with different methods depending on their purpose, e.g., a report that supports the assessment of a current incident differs from a report that forecasts the impact of a recently discovered vulnerability.

Input: The input block includes all types of sources and feasible transmission paths to integrate them into the cyber situation center's CCOP development. Based on recent research projects [30], common sources that contribute to CCOPs are for instance incident tickets, asset information,

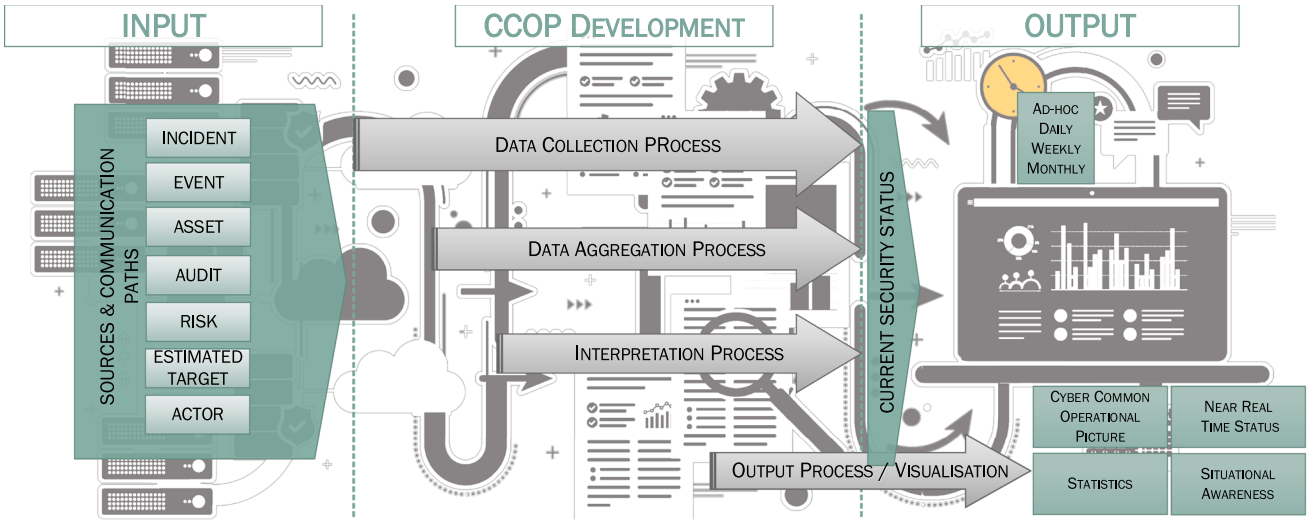

Fig. 1 Elements of the cyber common operating picture (CCOP) development process, structured as (1) Input, (2) CCOP development, and (3) Output

audit reports, identified risks, and threat actors and their estimated objectives.

CCOP development process: The general CCOP development process consists of four main steps: the data collection process (this also includes the storage of all relevant information, messages and historical reports), the aggregation process, the interpretation process and the output process. The individual steps are highly dependent on the application context and investigated in more detail in the case study in Sect. 5. The process of creating a situation report begins with the collection of data from a wide variety of information sources. This process runs permanently, as relevant information about cyber threats and attacks can arise at any time. With regard to the data collection process, a distinction can be made between automated and manual information retrieval. In the aggregation process, the data and information are assigned to predefined information classes. The interpretation process identifies, analyzes and evaluates the information relevant to the development process.

Output: The last step is the output process, where reports are generated for different stakeholders and needs, as well as periods of time and in different forms. The current security status can, for example, be displayed in the form of reports, statistics or dashboards at daily, weekly or monthly intervals.

3.3 CCOP metrics

In order to assess the overall cyber security situation, the state of each individual service is taken into account. A number of metrics are available for this purpose, which are explained in Table 1 for characterizing the overall cyber security situation within an organization, and in Table 2 to reflect the security status of a specific service. Notice, the last column shows for which type of reports these figures were considered in the case study in Sect. 5.

The metrics for the overall cyber security situation (Table 1) are structured into *Cyber situation general*, including various types of internal and external reports that reflect the current situation with respect to incidents; *risk management*, including the knowledge of risks, prevented risks and the effectiveness of risk management; and *information security management* figures that report on the implemented controls to mitigate risks.

On the other hand, the metrics for specific services (Table 2) report information on the *service status in general*, including metrics such as uptime, data volume, costs etc.; *vulnerability management*, including number of found or fixed vulnerabilities and average times to discover or patch them; and *incident handling*, reporting on the number of incidents detected or handled, and average times and costs to resolve them.[11]

These information, the general view on the infrastructure and the service-centric view, provide valuable insights to make justified decisions on the usage and maintenance of services. For instance, cost-intensive services with re-occurring vulnerabilities or frequently targeted by adversaries need to be protected differently or are used under more stringent constraints, compared to services not having these issues.

Both, Tables 1 and 2, include suggestions for evaluation intervals of the single metrics. While we suggest to calculate the value of most metrics on a regular basis, e.g., daily

[11] Notice that defining KPIs based on the number of incidents detected or handled can be problematic. An incident handling process may be triggered by a false positive. Furthermore, one incident might be part of other incidents. An organization must be aware of this and maintain a clean set of records.

Table 1 Metrics of the overall security situation

Cyber situation general	*"Global cyber-security climate."*	
Reports(External)	Reports from the media that currently have a major impact on the global cyber situation (ransomware waves, very large DDoS attacks, critical exploits such as Eternal Blue, etc.)	In the reporting period
	Reports from external partner organizations about existing attacks (number)	In the reporting period, difference from previous period, total, annual
	Reports from external partner organizations that have triggered the incident handling process	
	Reports from external partner organizations that triggered vulnerability handling	
Reports (internal)	Reports from internal organizational units that have triggered the incident handling process	
	Messages from internal organizational units that have triggered vulnerability handling	
Risk management	*Risks are analyzed with regard to their impact on processes within an organization and countered by appropriate countermeasures*	
Knowledge of risks	Percentage of services with analyzed risks in the risk inventory	Current status,difference from previous period
Risk prevention	Percentage of services with defined activities to prevent risk occurrence in the risk inventory	
Effectiveness of risk management	Number of known risks that have arisen	In the reporting period, difference from previous period, total, annual
	Number of previously unknown risks that have arisen	
	Number of incidents due to known risks	
	Number of incidents due to previously unknown risks in absolute figures	
	Service downtimes due to known risks that have occurred (hours)	
	Service downtime due to previously unknown risks (hours)	
	Follow-up costs of known risks that have occurred	
	Follow-up costs of previously unknown risks that have occurred	
	Operations of the organization that have been severely affected by known risks that have arisen	
	Operations of the organization that have been severely affected by unknown risks that have occurred	
Information security management	*Continuous knowledge of the risk situation and effective activities to prevent them are in place.*	
Coverage	Number of implemented security controls	In the reporting period, total, annual
	Number of preventive activities implemented for identified security threats	
	Number of security tests performed	
Effectiveness	Number of incidents due to security-relevant events	In the reporting period, diff. from previous period, total, annual
	Number of security incidents due to security-relevant events	
	Number of identified deficiencies during security tests	
	Service outages due to security-relevant events (hours)	

Table 2 Metrics of services

Service status general	*Operating indicators for a service*	
	Uptime	In the reporting period, difference from previous period, total, annual
	Data volume	
	Costs	
	Downtime due to incidents	
	Downtime due to maintenance	
Vulnerability management	*Reports on Vulnerability Management Activities*	
	Number of vulnerabilities found for Service X	In the reporting period, difference from previous period, total, annual
	Number of vulnerabilities handled	
	Number of addressed vulnerabilities that need to be re-addressed ("Reopen Rate")	
	Escalation rate, i.e., vulnerabilities that require a decision from a higher level (e.g., in case of HW failures, financial decisions about new purchases have to be made)	
	Average time to discover a vulnerability	
	Average time to fix a vulnerability	
	Average cost to fix a vulnerability	
	Distribution of criticality of vulnerabilities found	In the reporting period
	Number of vulnerabilities still open	By fixed point situation assessment
Incident handling	*Reports on the activities of the incident handling team*	
	Number of incidents at service X	In the reporting period, difference from previous period, total, annual
	Number of incidents handled	
	Number of handled incidents that need to be re-handled ("Reopen Rate")	
	Escalation rate, i.e., incidents that require a decision from a higher level (e.g., involvement of external resources, e.g., DDoS protection)	
	Average time between two incidents	
	Number of incidents resulting from detected vulnerabilities	
	Number of special situation images triggered by an incident	
	Average time to detect an incident	
	Average time to resolve an incident	
	Average cost to resolve an incident	
	Distribution of criticality of incidents handled	In the reporting period
	Number of incidents still open	By fixed point situation assessment

or weekly—depending on the reporting period—for others it makes more sense to evaluate their difference to the previous period. This way, the change, e.g., a growth rate, can be calculated, which might be more expressive. For instance, the presence of remediation costs of 50,000 Euros might be less alarming than the increase in remediation costs by 50% since the last reporting period.

3.4 CCOP data ingestion

An essential part of creating CCOPs is getting the relevant data to aggregate and interpret into a common data model in the first place. We identified the classes given in Table 3 as viable data sources for CCOPs, which are commonly available as reports at different abstraction levels.

4 A common data model for CCOPs

This section focuses on the design and implementation aspects of a common data model that holds all the relevant information for the flexible creation of cyber security reports. We also look at the processes in which this data model can be embedded to support the work of a CSC in a meaningful way.

4.1 Design patterns and requirements

In order to define the requirements for a common data model for CCOP, it is essential to understand the processes and working methods of a CSC. As noted in subsection 3.2, the process of generating a CCOP, and therefore the task of a CSC, is to interpret the information, some of which can be technical, from a wide variety of sources and to break it down to the essentials in order to inform the command level and facilitate decision making. In most cases, the CSC relies in this regard on the technical analysis and reports from other specialized organizational units, like incident handling teams or vulnerability handling teams. However, information from other sources such as websites, newsletters, OSINT reports or notifications can also be incorporated into the CCOP. Therefore, the tasks performed by a CSC differ from those of other units such as information security operations centers (SOC), whose tasks are located at a lower, more technical level. This places *event reports* in a central position in the CCOP process and requires them to be mapped into a generalized data model, which includes a mapping of typical *internal and external messages* and *security-relevant incidents*. The model must therefore also support an *efficient analysis* of the information available in the event reports. The model must further be able to represent the *quality* of an information source and allow the *relevancy* of information to be specified. Efficient analysis also relies on finding appropriate information, hence it must be possible to make search queries efficient by *keywording*.

Since some of the original information must be used for analysis, the model must also have a way of making *raw data* available. These can be, for example, e-mail attachments or scrapped web pages. This also allows for better *traceability*, as it cannot be assumed that all sources of information that have led to a certain situation assessment will exist permanently. To further improve traceability, the model must support versioning and linking of references to all information sources (both reports and data sources).

As different data sources need to be integrated, the model should be *extensible* and *not locked into any particular technologies*. To aid interoperability and adoption, the data model should reference *existing standards and conventions*, for example certain vocabularies and terms.

4.2 The CCOP data model

The data model consists of various data-types, categorization inventories or vocabularies (modelled as enumerations) and relationships. Figure 2 provides a full overview of the data model in the form of an UML Class Diagram. In the following, these different elements of the data model will be discussed in detail.

The `Report` is the abstract base class for all events or messages that can be relevant for a CCOP. It contains information about the author, source, information rating and references. It can also feature a list of attachments. The CCOP data model defines a set of specialized reports which are relevant for the processes within a CSC:

The `EventReport` is used to describe any type of security event. In addition to data fields for time classification, this report offers the possibility to define the incident type and the affected status. `IncidentReport` is derived from the `EventReport` and describes an security incident. It enables the mapping of the affected status of concrete assets within the own organization and the specification of a threat actor. According to NIST [35], an incident is an "occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." The `CampaignReport` describes an attack campaign. A campaign comprises a series of malicious activities or attacks (sometimes referred to as waves) carried out over a period of time against a specific group of targets. The description contains the target (desired effects), first and last sighting and, if known, the threat actor. The `AuditReport` represents a penetration test report. It contains one or more targets that were considered in the audit, the textual report itself, classification of the "depth" of the audits, as well informa-

Table 3 Preselection of internal and external sources

Internal	Asset Management	Information on all hardware and software systems.
	CMDB	Configuration items for devices, applications, communications/networks, sites, databases, services, documentation, and people (employees and contractors).
	Service Catalog	Cross-cutting services and their associated subordinate systems and assets.
	Workflow Management System	Assists in receiving, acknowledging, classifying, and processing issues and requests.
	Internal Reports	Messages or reporting to the CSC or from the CSC to the command level.
	Incident Handling	Notifications of internal security-related incidents.
	Internal Audits	Automated tests or internal penetration testing for own systems. Audits or pentests check the effectiveness of measures at semi-regular intervals ("random samples" or on an ad-hoc basis with more in-depth tests).
	Vulnerability Management	Checks IT systems for known technical vulnerabilities (monitoring of vulnerability situation, continuous in-depth review)
External	External Reports	Reports on security-relevant incidents from domestic and foreign partner organizations.
	OSINT	Intelligence gathering, cyber-threat information from freely available, open sources (e.g., MISP Open Source Threat Intelligence and Sharing Platform, Maltego).
	(Cyber) Threat Intelligence Feeds	Subscribed third-party feeds with information on potential or existing threats, vulnerabilities and risks, including indicators or artifacts (IOCs). Examples include Emerging Threats, Blocklist.com or AlienVault OTX.
	External Audits	Audits by external organizations, for example ISO 27001 audits or as part of NATO or EU requirements.

tion what was audited. It also describes the vulnerabilities (or findings) that have been identified within the own organization. The term vulnerabilities covers all inadequacies or defects in the requirements, design or implementation of the computational logic (e.g., code) in software and possibly also hardware components (e.g., firmware).

A `Summary` can combine one or more reports of different types. It features a textual summary for the reports contained. It also contains a risk level determined by experts, related to the own organization. Several versions of summaries can be stored via the `History`. The `History` can be used to implement versioning. This is done via a `HistoryEntry`, consisting of a mandatory time stamp (representing the modification date of the entry) and the corresponding `Summary`.

An `Attachment` is a representation of an arbitrary information object that is attached to a report. A specialization of the `Attachment` is the `Indicator`, which is an representation of an Indicator of Compromise (IoC). An IoC in IT forensics is an artifact that has a high probability of indicating unauthorized access to a computer [36]. It contains further information of the validity time span and the type of the IoC.

A `DataSource` contains all the meta-information of an data source. This includes the source name and type, keywords, a rating and if possible a `DSCheckPoint`. A `DSCheckPoint` allows to determine when a concrete information source was last interacted with, for example, when information was last imported from an RSS feed or when data was last processed from a log management system. As an example, the data model defines two typical checkpoints (`RSS` and `Website`) for data sources. However, it is expected that adopters will extend this list with their own data sources.

The data model defines several support data types, which are mainly used for the mapping of information. The `StringTuple` is the most basic data type and serves as an helper construct for various other data types. The `AuditStatusMapping` allows an assignment of a service, system or asset to one or more findings, as well as the audit status. If there are findings, they are listed individually as a finding and assigned a status. If a vulnerability has already been closed during the audit, the status "Closed" is set. A `Finding` describes a vulnerability found by an audit (or penetration test). It can also include additional infor-

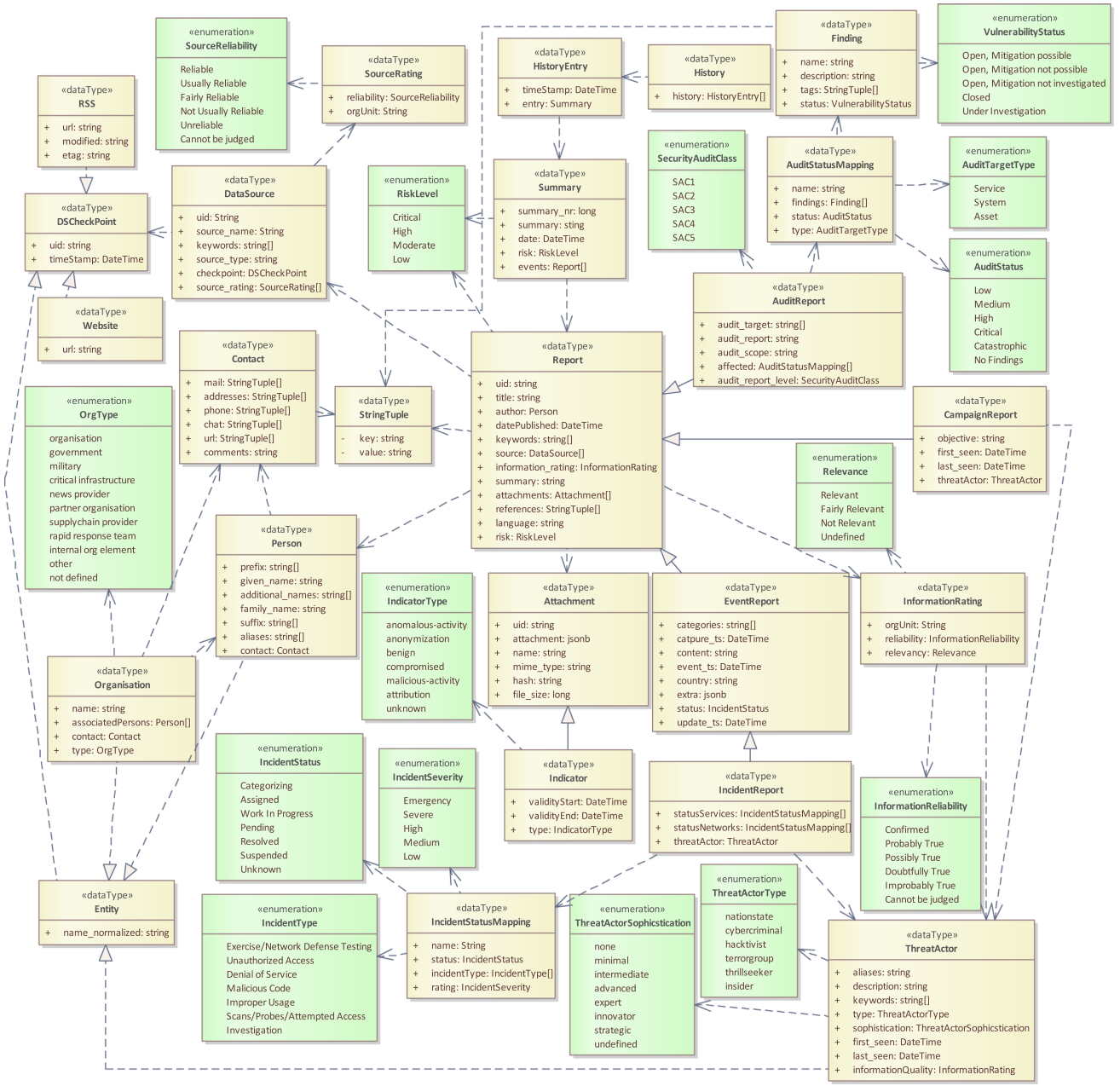

Fig. 2 Complete CCOP data model as UML class diagram

mation, such as a CVE number[12] or a CVSS rating[13]. The `InformationRating` allows to store reliability and relevance of an information and the `SourceRating` allows the storage of reliability of an information source, both in reference to an internal organizational unit.

The data model furthermore defines several types of entities (i.e., natural persons, organizations and attackers). An `Entity` can be a natural person, an organization or a threat actor. Entities themselves thus have the task of creating a basis for various forms of entities in the data model. Since they can also be a source of information, they are also a realization of a `DataSource`. Natural persons are mapped to `Person` and organizations to `Organization`. Both can have a `Contact` attribute, which encapsulates all contact information known. The `ThreatActor` is the realization of an entity for threat actors. Threat actors are individuals, groups or organizations that are believed to act with malicious

[12] Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org/

[13] Common Vulnerability Scoring System (CVSS), https://www.first.org/cvss/

Table 4 Security audit classes

Criterion	SAC1	SAC2	SAC3	SAC4	SAC5
Automated security tests	✓	✓	✓	✓	✓
Manual verification of test results		✓	✓	✓	✓
Threat image and mitigation measures		✓	✓	✓	✓
Manual security tests			✓	✓	✓
Organizational audit				✓	✓
Risk analysis					✓

intent. The can be described by various properties, such as aliases, type, capabilities or level of sophistication.

The categorization inventories or vocabularies in the CCOP data model allow a precise classification of events, entities and processes. For instance, the `AuditStatus` allows the assessment of vulnerabilities or issues found during an audit the `IncidentStatus` allows to define the status of a security incident and the `IncidentType` allows specifying the type of a security incident and is based on `IncidentCategoryVocab-1.0`[14]. `IncidentSeverity` allows for specifying the severity of an incident, based on the Cyber Incident Severity Schema [37]. `Relevance` allows the assessment of the relevance, in relation to the own organization, of a certain piece of information. `SecAuditClass` allows an assessment of the "depth" of the security audit. The selection of the appropriate value is made in accordance with Table 4. `AuditTargetType` describes the type of infrastructure (service, system or asset) to which a certain finding relates to. `RiskLevel` refers to the risk assessment of experts regarding the information from one or more reports for their own organization. The four levels shown here are intended as a proposal and are based on the AS/NZS 4360 standard; however, other methods are available [38].

Some categorization inventories are directly taken from existing specifications, for example `IndicatorType` is based on the `indicator-type-ov` and `ThreatActorSophistication` on `threat-actor-sophistication-ov` of STIX 2.0[15]. `InformationReliability` and `SourceReliability` both use the categorization scheme from FIRST.org [39], which is again based on which is based on the US Army Field Manual 2-22.3 [29].

[14] See https://stixproject.github.io/data-model/1.2/stixVocabs/IncidentCategoryVocab-1.0/

[15] See https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html

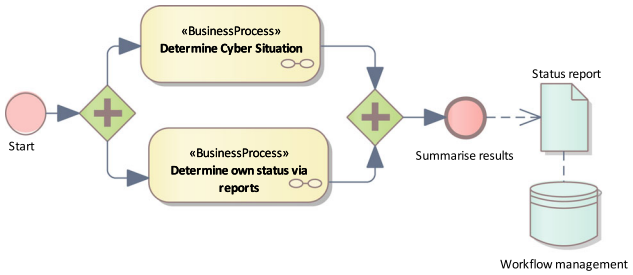

Fig. 3 BPMN workflow: determine the overall security status (CCOP)

`ThreatActorType`, which allows the type of a threat actor to be specified, is based on the perpetrator groups defined by the Canadian Centre for Cyber Security [40]. Options for extending this list are provided for example by Sailio et al. [41]. `OrgType` is to be seen as a first draft for a list of relevant organization types in the military context. `VulnerabilityStatus` allows the handling status of a vulnerability to be set.

4.3 Application of the data model

In order to use the data model presented here effectively, it is necessary to embed it in suitable processes. In this section, a generic process for determining the overall security status (i.e., the CCOP), which is nevertheless typical for a CSC, will be presented. Figure 3 depicts this overall process for generating the CCOP. Based on the established and well-proven approach found in the Austrian MoD, this generalized process for generating a CCOP has been derived. Here, two major views are relevant for the command level: an "external" view, which encompasses the general cyber situation worldwide, with a certain focus on the national level. In addition to this overarching cyber situation, an "internal" overview of all security-relevant processes, potential issues and risks and in the own organization must be created. Therefore, creating a CCOP consists of two main activities that can be carried out in parallel: (1) Determining the general cyber situation; and (2) determining the security status of the own organization via internal reports from specialized departments and other organizational elements. For this purpose, it is necessary for the CSC to be able to make use of different information sources. A list of the most common sources is provided by Table 3.

As shown in Figure 4, the general cyber situation is mostly deducted from different information sources. This includes public sources, such as news and media articles or OSINT feeds, and more private or restricted sources, such as reports from partner organizations and reports from internal departments or organization units. The process begins with information gathering from these different sources (see `Report`). If a source is new, it needs to be evaluated first (see also `SourceRating` in the CCOP DM). Internal doc-

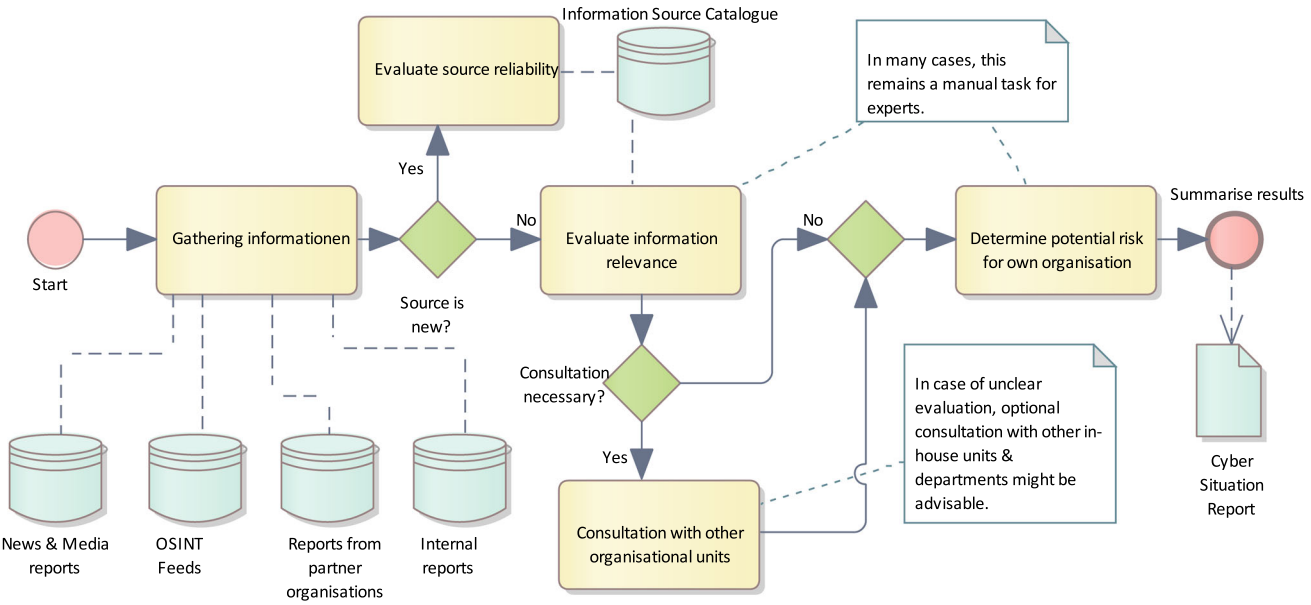

Fig. 4 BPMN workflow: determine the overall cyber situation based on reports

umentation of risk management and information security management (see Table 1 for an exemplary selection of metrics for these two fields) are an important part of the general overview of the security situation. Reports and statistics from incident handling and vulnerability management, as well as general service status information should also be included the CCOP. Table 2 provides a selection of metrics that give an indication of the security status of one' s own services. Information from external sources can, for example, be included in your own information system as an `EventReport` or `CampaignReport`. Information will also need to be evaluated (see `InformationRating`). This step is crucial for the final risk assessment of the information at hand. For instance, if new vulnerabilities become known, it must be checked whether they can also affect the own infrastructure; if new threat actors appear, it must be clarified whether one's own organization fits into their target scheme; if new TTPs become known, it must be clarified whether they have already been taken into account in the security controls; and also in the case of general events in the cyber security landscape, it must be investigated whether these are relevant for a situation picture for informing the command level. The information gathered will then be evaluated for potential risk to the own organization. This can be a manual task, but also machine learning techniques can be used. In some cases, consultation with other organizational units may be needed. This risk analysis depends on the needs and characteristics of the own organization. However, it is advisable to rely on established procedures, such as ISO 27005 [42] or NIST SP 800-30 [43]. Depending on the information situation or the required scope of the CCOP, it might be sufficient to only consider consequences and likelihood of a security risks, however considering asset value, threat, and vulnerability can significantly increase the informative value of this assessment. A statistical evaluation of certain security-relevant metrics (see Tables 1 and 2) can also be included in the risk assessment. At the end of this process, a report will summarize the results of the evaluation).

A more specialized workflow is shown in Fig. 5. In this case, we assume that our own organization provides different services (e.g., email or telephone) that use one or more systems (e.g., mail server, DNS server, VoIP server, etc.), which in turn consist of different assets (such as the physical hardware or VoIP phones). The infrastructure should be mapped in service, Asset and CMDB databases to support targeted evaluation. In order to gain an overview of the security situation of one's own infrastructure, all available relevant internal reports (see also `IncidentReport` and `AuditReport`) must be evaluated. The relevant reports can be selected via the keywords and the stored meta information (e.g., timeliness/date, scope, creator, etc.). If certain systems or assets are not linked to a service, reports on these must be evaluated separately as shown in Fig. 5. Since internal reports prepared by qualified experts are used here, their evaluations can be used. In the case of incidents, an assessment of the severity of the incident should already have been carried out. If the incident is still ongoing and has not yet been fully dealt with, it is necessary to consult with the incident handling team. The same applies to security audits; an assessment should be available for each infrastructure element examined. If a CVE number or a CVSS score was specified in the finding, these can also be used for the assessment [44], [45]. At the end of

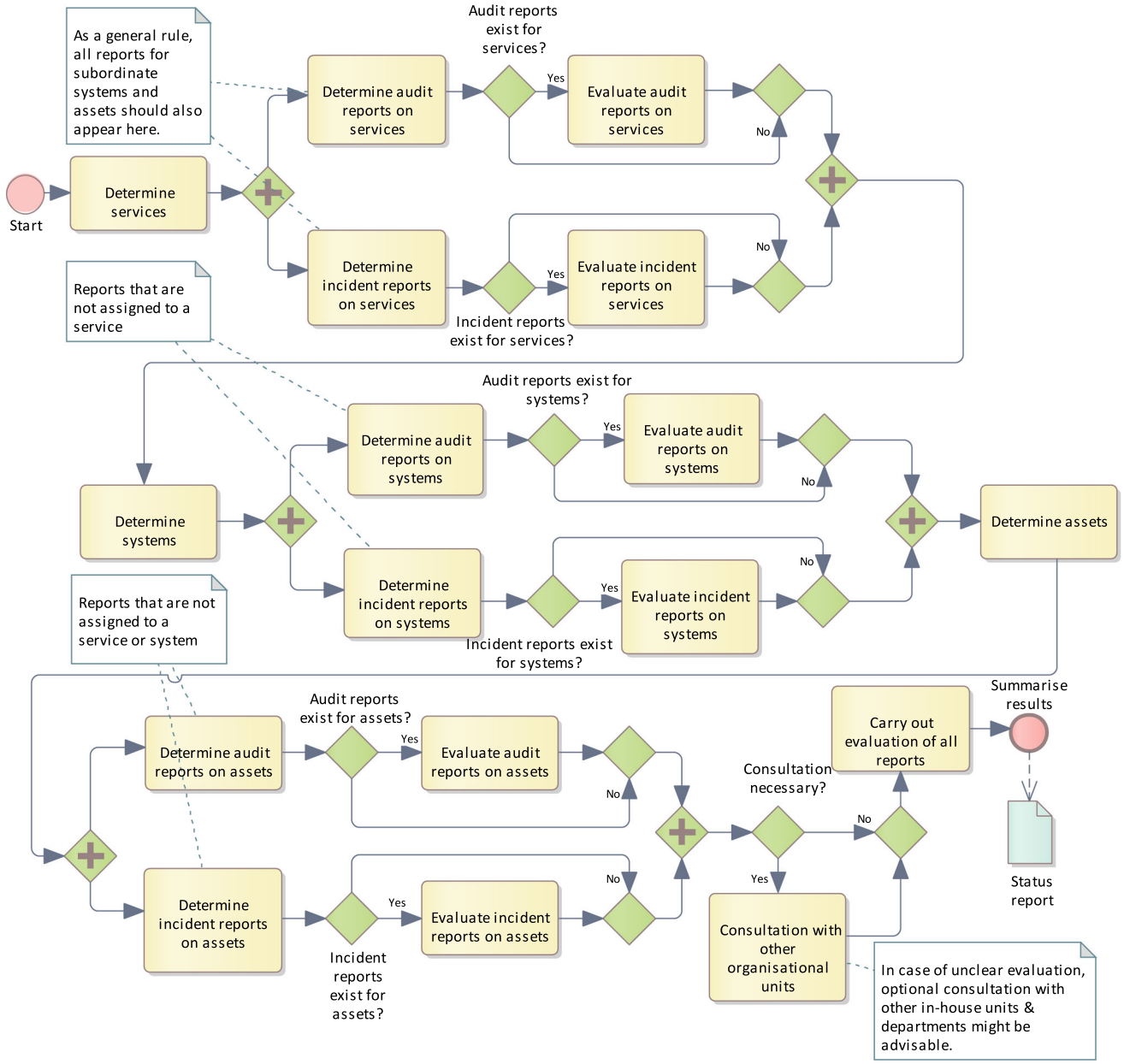

Fig. 5 BPMN workflow: determine the own cyber situation based on reports

the process, there is again a (possibly joint) evaluation of the information collected and the preparation of a report with the presentation of one's own security situation.

5 Case study with the Austrian MoD

In the end of 2021, a case study together with the Austrian MoD was carried out, which carefully followed the design methodology described in this paper.

5.1 Use case context

In this case study, CCOPs are used to capture the current cyber security situation and serve as the basis to flexibly create cyber security reports for specific stakeholder. With respect to the CCOP requirements defined in Sect. 3, we defined the requirements summarized in Table 5. As shown in Sect. 4, the CSC relies heavily on reports and information generated by other departments, experts and sub-organizations. For this case study, the following entities within the Austrian MoD had to be taken into account:

Table 5 Requirements and properties for the creation of a CCOP (as realized in the case study in Sect. 5)

CCOP property	Requirement	Description
Scope	Organizational elements and security environment	The scope of the situation reports mainly covers the infrastructure (ICT systems) of the Federal Ministry of Defence and the Austrian Federal Armed Forces. Since the cyber situation cannot be analyzed locally and in isolation, the overall threat situation must be taken into account, such as the latest attack vectors, software or hardware vulnerabilities, etc.
Target level	Strategic/operational	The CCOPs aim at supporting decision making and the preparation of forecasts for long- and medium-term decisions. Therefore, the information sources with the appropriate abstraction levels must be used in the creation process.
Duration	Periodic, ad hoc	In the military cyber situation center, both periodic (daily, weekly, monthly) and event-driven (immediate) CCOP building is desired. This requires a flexible process.
Output	Alerts, incident reports, reports tailored to the needs of the user. Warnings for awareness building for users.	The findings of the situation assessment are summarized in the form of cyber alerts, incident reports, and situation assessment reports. The CCOP building processes must be able to provide the information in formats appropriate for the user.
Sources	Internal and classified external sources, and OSINT	The diversity of information sources must be particularly well managed in the CCOP building process, as the quality of the sources strongly shapes the situation assessment.
Visualization	Current and historic situation, chronological events, communication history, overall cyber situation	The CCOP should be capable of recording and reproducing the current situation (including the situation of the whole country) as well as the past situation, events and communication.

- The cyber situation center (CSC) is responsible for generating situational reports for the purpose of providing information to the command level. These reports can be generated from different occasions. Basically, a distinction is made here between two types of reports. Regular, periodic reports (e.g., daily reports, weekly reports or quarterly reports) cover a defined period of time and contain all relevant information necessary for decision makers. In contrast, there are ad hoc reports that focus on a specific topic, such as an incident. The information sources that are potentially relevant for a situation report are shown in Table 3.
- The *Point of Contact* (PoC) is a defined point of contact for external partner organizations. Different partner organizations may have different PoCs, which may also differ according to the concern.
- The *Command Level* is above the other actors involved in the command hierarchy and has the authority to make decisions. These decisions are made, among other factors, based on the reports of the CSC.
- The *Incident Handling* (IH) is tasked with dealing with security incidents. The focus of the IH is of a technical nature, the IH thus performs the tasks of an SOC.
- The *Vulnerability Management* (VM) is responsible for dealing with technical vulnerabilities in MoD services, systems, and assets. The VM's duties also include performing technical audits, such as penetration testing.
- A *Service Owner* is the operator of a specific IT service within the MoD. These services can be specifically assigned to a department or unit. The service owner here is also responsible for asset management and infrastructure monitoring.

5.2 CCOP process implementation at the Austrian MoD

In order to validate the CCOP generation processes and the corresponding data model, a number of exemplary use cases were defined. One objective of these use cases is to embed the processes described in Sect. 4.3 into an overarching process. One of these use cases is modeled as a business process in Fig. 6 and will be discussed in this section. This use case includes a wide array of information sources and means of technical communication. The situational picture to be drawn here has to be included in an ad hoc situation report of the CSC for the short-term information of the command level.

In the fictitious scenario presented here, an APT[16] has been detected in a partner organization (PO). Based on traces left behind by the attackers, the PO's security experts conclude that the attack must have been carried out by state-sponsored hackers from the country of Ostarrichi. The initial infection took place most likely in January 2020. The PO then sends an encrypted mail to a defined point of contact (PoC) at Thursday, November 11, 2021, which contains the following information:

- **Tactics, Techniques, and Procedures** (TTPs) [47]: The APT was most likely introduced via spear-phishing mails with malicious attachments or with links to malicious files on cloud storage drives. Attackers leveraged exploits in Microsoft Office and .NET products. The APT relied on web shells for an initial foothold. The APT targeted then VPN and remote desktop credentials to establish the foothold. To evade detection, the APT used well-known web resources as Google Drive, Microsoft OneDrive or Apple iCloud for file exchange.
- **Vulnerabilities**[17]: A list of vulnerabilities that are probably related to the attack.
  - `CVE-1337`: Affects Microsoft .NET and exists since June 2015, made public 2021-08-08.
  - `CVE-0815`: Affects Microsoft Office and exists since August 2018, made public 2021-09-01.
  - `CVE-4711`: Affects Microsoft Office and exists since August 2018, made public 2021-09-01.
- **IoCs**: A list of indicators for a possible compromise.
  - IP addresses used for the APT Command and Control (C2) infrastructure.
  - File hashes of the malicious attachments and files on cloud stores.
  - Set of registry key values associated with APT.

This report triggers a series of internal activities. In the first step, the PoC identifies Incident Handling (IH) as the internal organizational unit that must be informed first. If an incident should also occur in the own organization, the IH can react quickly and, if necessary, initiate mitigation measures. The mail with the report is therefore forwarded to IH by the PoC.

The IH begins with a relevance check of the report. The IH clarifies here, for example, on the basis of the aforementioned security vulnerabilities, whether its own systems can be affected at all. In addition, the assessment includes whether the own organization has structural and functional similarities to the PO, and can thus be a potential target of the hacker group. The IH may also use the Information Source Catalogue to access information on the reliability of the partner organization (see `DataSource` with `SourceRating`); if no assessment is available, this can be carried out for the first time by the IH. If the information contained in the report

[16] The description of the APT is adapted from the real-life APT40, which became known in 2019. [46]

[17] The CVE numbers and vulnerabilities are fictitious.

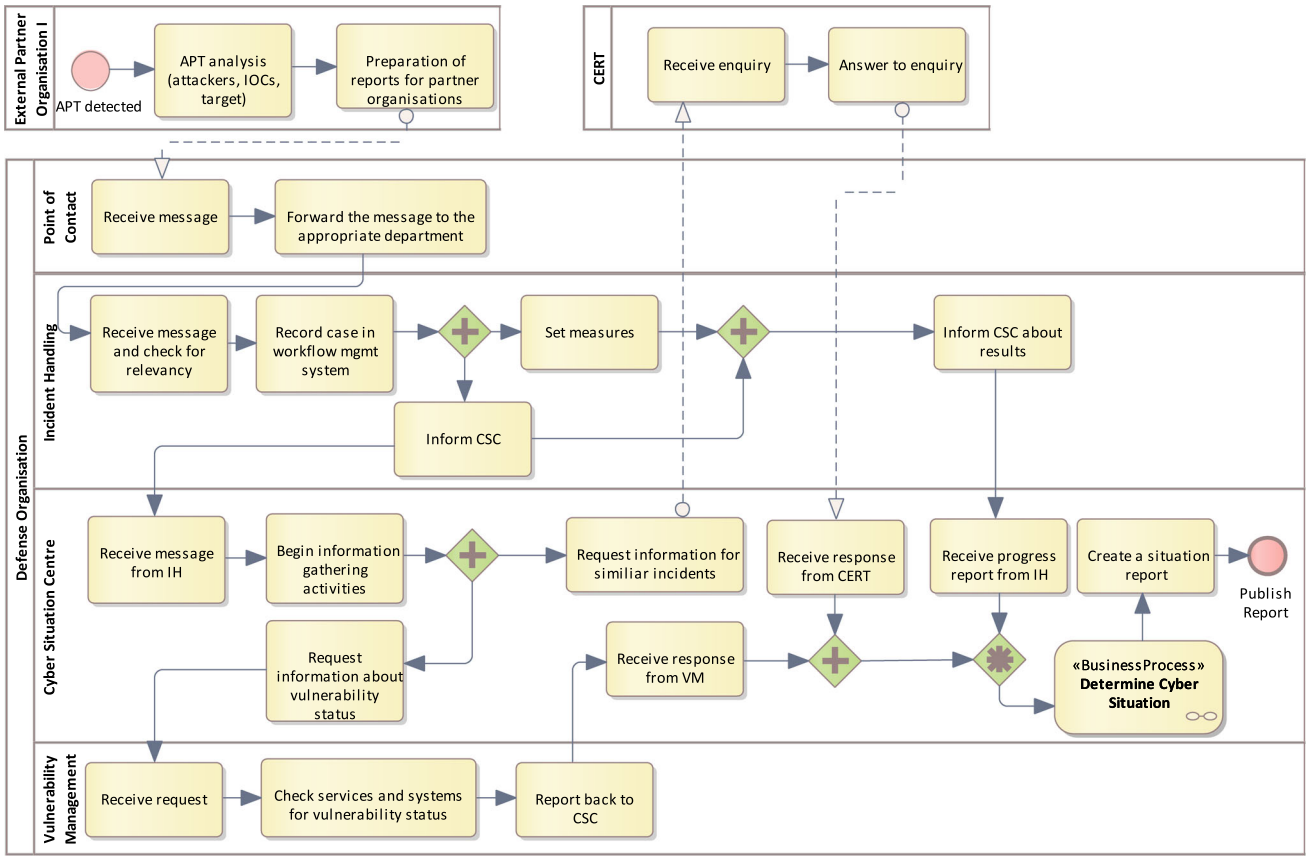

Fig. 6 Example use case: security incident at an external partner organization

is deemed relevant, i.e., if the own organization is possibly also affected, the report is included together with a `Summary` (including a first risk assessment, see `RiskLevel` in Fig. 2) in the work-flow management system (WMS) and thus the CSC is informed automatically. In this case, the IH concludes that the own organization falls within the profile of the attackers and that its own systems potentially could have been affected by the vulnerabilities.

The CSC now starts to collect all available information in order to inform the command level by means of a CCOP. In this specific scenario, two different entities are being contacted, on the one hand the internal Vulnerability Management (VM), and on the other hand the national CERT, which is an external organization. The VM is contacted via internal chat to find out the current status of the company's own services and systems. A reference to the summary with the original report, including the list of vulnerabilities in WMS, is provided to the VM as well. The VM begins to compile a report (see `AuditReport`), which concludes that currently, there are no known open vulnerabilities in the infrastructure. However, the report notes that the vulnerabilities listed in the original warning from the PO were once present, with `CVE-1337` mitigated on 2021-08-09 and patched on 2021-09-01, as well as `CVE-0815` and `CVE-4711` both mitigated on 2021-09-05 and patched on 2021-10-01.

The CERT is contacted via encrypted mail to find out whether similar incidents are known or whether there is a major wave of attacks (i.e., campaigns). The CSC can obtain this contact information from the CERT profile backed by the data model (`Organization` with a `ContactPoint`). The CERT reports back that there have been several suspicious activities which are connected with Ostarrichi in the last months. For instance, critical infrastructure operators have reported that there have been probing attacks from the Ostarrichi IP address range. The CSC receives this information and records it as a `CampaignReport`. The information of the adversary from this report is integrated into the `ThreatActor` entity which is assigned to the original APT report from the PO.

In parallel to these processes, which have been kicked off by the CSC, IH is focusing on the incident handling process. Here, the IH begins to set up initial mitigation measures, which include entering IoCs into detection systems, creating new SIEM rules, analyzing logs, and so on. The IH also starts an investigation to find traces of the TTPs, respectively, IoCs, on its own infrastructure. The IH detects that there are suspicious attachments on the mail server of the Public Rela-

tions Department. As a result, mail service and operation of this department's workstations will be temporarily suspended pending a comprehensive analysis. This is carried out in coordination with the service owners, here the operators of the mail server and the user client network. An ongoing APT can neither be confirmed nor ruled out at this point. The results are recorded in an `IncidentReport`. This report is then attached to a new instance of the original `Summary`, together with the original report and an updated risk rating.

Once the various information and reports have reached the CSC, it can begin to create a CCOP that reflects the current status. As quick reaction is required in this ad hoc cyber situational picture, this is done in the process detailed in Fig. 3, with a focus on the sub-process displayed in Fig. 4. The evaluation of the historical vulnerability reports has been carried out by the VM. The initial report of the PO (already assessed by IH), the incident report of IH, the vulnerability report of VM and the campaign report of CERT are selected by the CSC as the basis for the situation report to be prepared. Since there are already risk assessments by the IH and VM, they can be incorporated into the final situation assessment in an automated process. This also applies to the existing relevance assessments for information and reliability evaluation for information sources. Clear guidelines for assessment are absolutely essential, but are not the focus of this work. Ultimately, however, a final sanity check must be made by security experts before the report is published. In the present scenario, IH and VM experts should also be consulted for a final assessment. No information matching the APT was identified in the relevant OSINT feeds and specialized media. Based on the risk ratings from IH and VM, the CSC concludes that the own organization is possibly at risk.

Finally, the results are summarized in a situational report for the command level (see Fig. 7 for a truncated version). The ad hoc report contains a brief summary of the current situation, including an assessment of the situation by the CSC, partly based on the assessments given in the IH and VM reports. In addition to the current incident, the situational picture shown here contains other exemplary elements. The upper part briefly summarizes the assessments on various topics (in addition to ICT services abroad and domestic, the cyber security situation, which is the actual subject of the report). The metrics for services (see Table 2) are aggregate into combined indicators for (in this scenario) three distinct service classes (mission critical, essential, and other) for the different departments of the own organization. For instance, a high number of incidents or a high number of unmitigated incidents can lead to a warning ("yellow traffic light"), in severe cases to an alert ("red traffic light"). The threshold values that lead to this combined indicator going to another warning level must be defined in cooperation with service operators, command level, CSC, IH, VM and possibly other involved stakeholders (e.g., user representatives). The statistical data for effectiveness of risk management and information security management activities (see Table 1) are consolidated into a graph, which represents their respective trend for the various regular reporting periods. As with the services, the idea here is to calculate a combined indicator value from various metrics, which will provide the command level with an overview of the trend in the effectiveness of these activities. Internal and external reports from this table are also integrated into the situation picture. These information blocks can be automatically generated and integrated into any situational awareness report—be it ad hoc or periodic. The visualization shown here is to be seen as a draft of how these types of information can be prepared into a (static) situational report. Using dashboards, such as the open source tools Grafana[18], Chronograf[19] or Kibana[20], this data can also be visualized interactively and in virtually any desired form.

5.3 Proof of concept application

The proof of concept application is a browser-based application. The implementation covers the defined use cases and uses the designed CCOP data model to gather, modify, and store data. Hereby, actually two databases are used. The first database contains persistent data, whereby persistent data refers to the original data sources and stored common operational pictures. The second database is used to work on a near real-time operational picture that represents the current status. All modification made to data and all additional information added by a user will first be cached in this second database and only be persisted once the user decided to save a snapshot in the form of a report whereby the report could be a daily, weekly or monthly report, as well as an ad hoc report.

The goal with the proof-of concept application is to demonstrate that our solution makes the creation of cyber security reports more efficient. In order to achieve this goal, the application is split into several views, whereby the three major ones are:

- Notifications ("Meldungen"): an overview of currently relevant events or messages with the ability to create new events and enhance these with new information
- CCOP ("Lagebild"): showing the common operational picture of a selected time
- Search ("Suche in Lagebildern"): enabling the search for a specific common operational picture

With these three views, the proof of concept application follows the CCOP development process of data collection,

[18] https://grafana.com/

[19] https://www.influxdata.com/time-series-platform/chronograf/

[20] https://www.elastic.co/kibana/

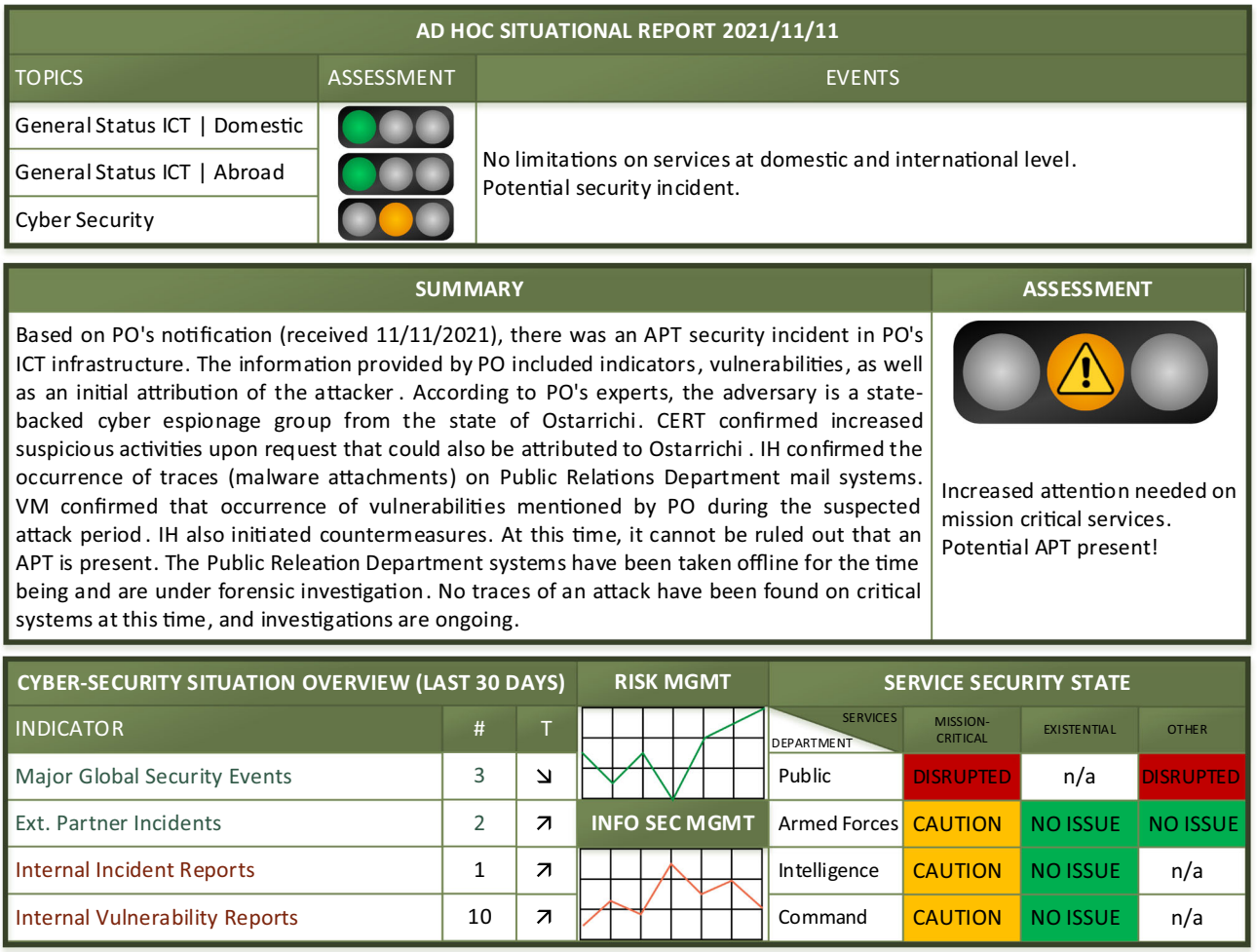

Fig. 7 Conceptual draft of a situational picture

aggregation, interpretation and the output process outlined in Fig. 1. The data collection however is partly performed outside the proof of concept application by saving data into our database or creating events in other applications. The proof of concept application uses this data to display relevant events and messages/notifications for the CCOP development process (cf. Fig. 8).

Having the discussed use cases in mind the proof-of concept application follows a logical sequence of steps supporting the various tasks of the CCOP development process. As such, the user can view events and messages by selecting an entry from the list, mark events that are of relevance for a report, combine them or enhance them with new information as part of the data collection and aggregation step. Hereby, it is possible to select for which kind of report the event is relevant, for a daily, weekly, monthly, or ad-hoc report. The attachment of other relevant information to a created or edited event, be it other messages or documents, is also possible. With the ability to further add and describe countermeasures also the interpretation step is supported.

Switching to the "Lagebild" view the user gets information about the current situation. As the proof of concept application focuses mainly on the creator role of a CCOP the last entry in the time line of the top of the page represents the currently worked on status. The other entries represent CCOPs that have already been persisted and saved to the database. The overall layout although is the same, whether the user is a creator or recipient of a report. On the left side, always the summary is shown, while on the right side details to a selected entry in the CCOP will be shown. The recipients can in general not make any further modifications.

A role management mechanism defines access rights so that only roles defined with appropriate rights can perform modifications to some information already in this view. This page is the main page related to the interpretation step of the CCOP development process since here the information relevant for a report is marked, enhanced, and measures are added to an event. Once a user with appropriate rights decided to build a specific report by selecting the kind of report required

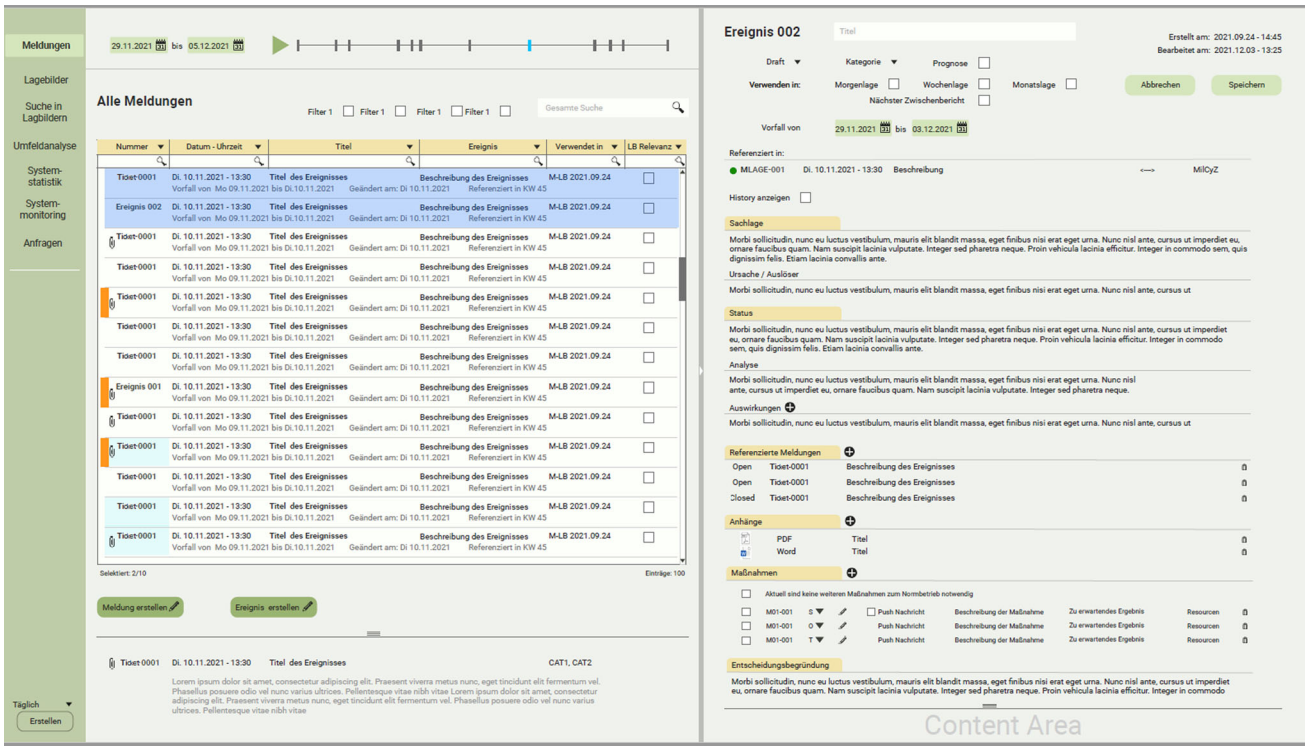

Fig. 8 Notification page displaying relevant events and messages

and pressing the Create-button on the lower left side of the page a snapshot of the currently shown (filtered) situation is taken, and information marked as relevant for the chosen report type are copied and a new report is prepared as shown in Fig. 9.

Roles with appropriate rights can still make modification to this report. It also still uses the temporary database to store information and changes. Only after pressing the Create-button this report is persisted and saved into the other database for later viewing. By pressing this button, the report also becomes available to other recipients, finalizing the output process. Additionally, the proof of concept application offers the possibility to view and search for persisted reports in the database. The "Suche in Lagebildern" allows to define a time frame. Reports within this time frame are displayed in a list and can be further narrowed down by additional search terms (see Fig. 10).

Details of the reports will then be displayed on the right side of the page once an entry is selected. The overall layout of the HMI was defined together with the stakeholders at the Austrian MoD to cover the relevant information and to be flexible to support the needs of various stakeholders in the information chain, the creator as well as various kinds of recipients which all have slightly other information rights and needs. Dependent on the rights and needs of the recipient of the report some of the text fields and information may be filtered out and thus is not visible to them. The screen shots used in this section however are taken from the report creator role, thus all information and all fields are visible.

5.4 Discussion and evaluation

The proof of concept application was validated by means of a virtual presentation, in which not only the prototype was presented, but also the main use (creating an overview, creating a situation picture) was demonstrated. Meanwhile, questions and suggestions were welcome. After the presentation, questions were asked in a focus group, which led to further discussions. Finally, the well-established System Usability Scale (SUS) questionnaire [48] was distributed to evaluate the usability of the implemented application. The main scenario was also tested with future creators of CCOPs in order to receive feedback on the information hierarchy, the presentation and the process, and to be able to draw qualitative conclusions about usability.

5.4.1 Test process

Basically, the test process was composed of three phases:

– **Phase I: Pre-test**—In a pre-test, it was the task of a test participant to carry out the planned scenarios with the help of the PoC. Important usability problems were

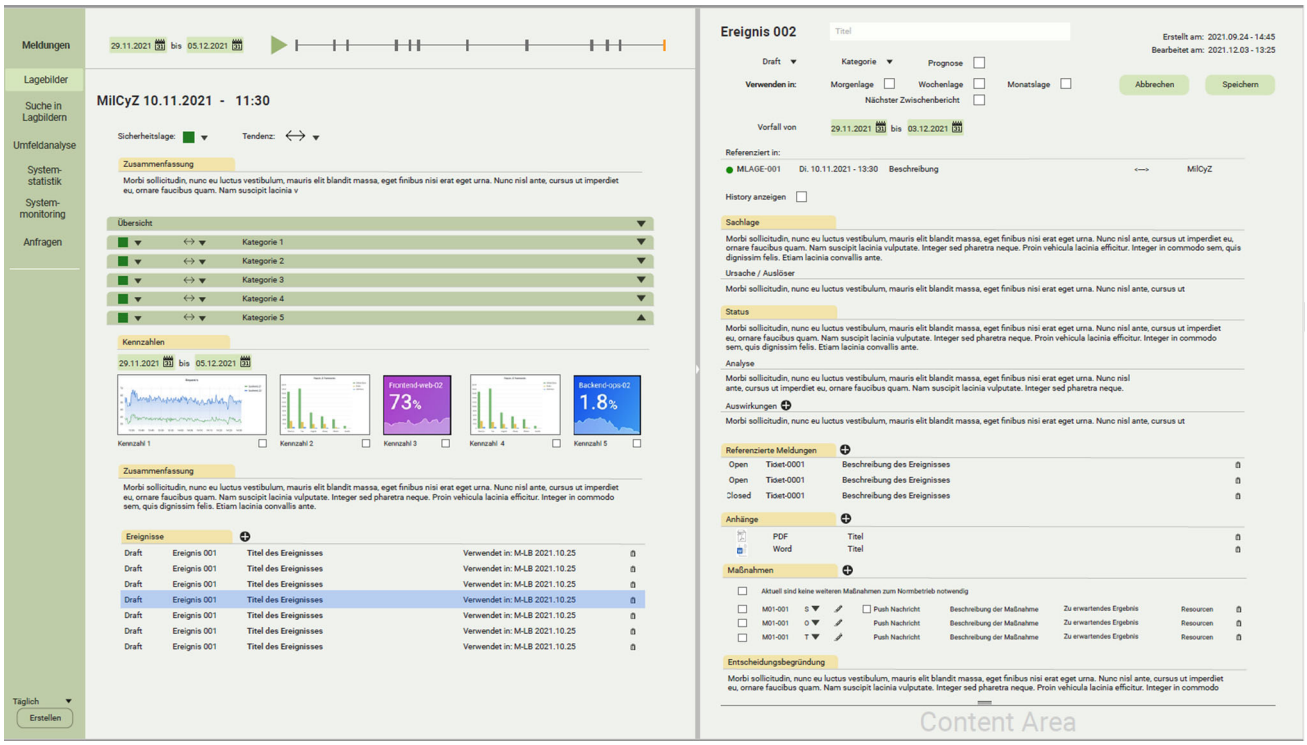

Fig. 9 Creation of a CCOP ("Lagebild") using events and messages

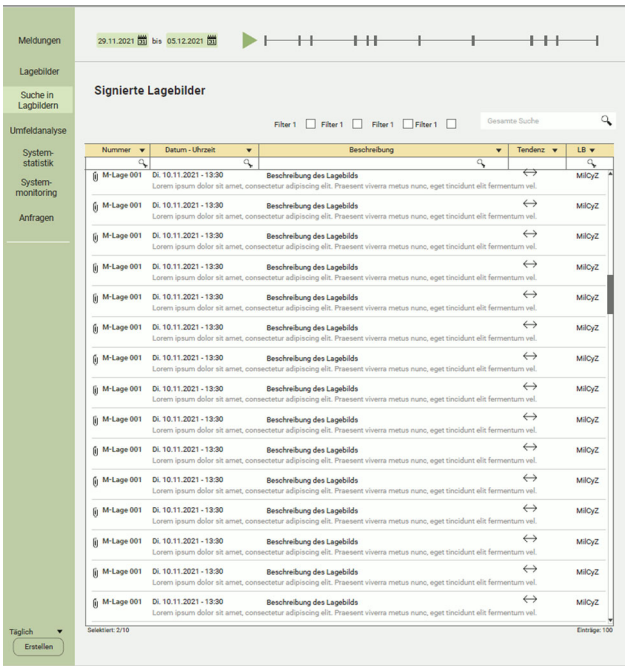

Fig. 10 Overview of all created CCOPs over time, searchable by key terms

discovered, which were immediately forwarded to the development team and fixed.

– **Phase II: Video conferences**—A total of 10 people were able to participate in two video conferences that were held on different days. These people are typical consumers of CCOPs, i.e., located at the command level.

– **Phase III: Validation with CCOP creators**—During the validation with creators of CCOPs, the use case "creating a situational picture" was played through and improved through observations and collected feedback. The creators of CCOPs are typically analysts within the CSC.

5.4.2 Test procedures

All phases were carried out according to well-defined procedures that were designed as follows:

1. **Introduction to the system:** We provided a brief introduction to the topic of the project and the PoC, as well as an overview of the main activity of the concerned CCOP end user.
2. **Execution of the main scenario:** The individual steps required to create a CCOP were shown on the prototype.
3. **Focus group:** Based on prepared questions, the practicability, comprehensibility and possibilities for improvement of the prototype were discussed in a focus group.
4. **Distribution of the SUS:** The SUS questionnaire was electronically distributed to all participants and feedback collected.

5.4.3 Validation

Execution of the main scenario. The participants carried out the following steps, in order to evaluate the degree of support that the proof of concept application provides for the creation and assessment of CCOPs:

- Create an overview of new messages (cf. Fig. 8)
  - Verifying the new reports
  - Marking of all reports relevant to the situation picture
  - Editing reports
- Creating a new event
  - Opening a new event
  - Description of the current situation
  - Selection of the period
  - Identification of potential impacts
  - Marking of relevant categories (multiple choices possible)
  - Creation of organizational and tactical measures
  - Possible marking of a measure as a "push" message
  - Change of event status to "Active"
- Verification of the current events in the "live" situation picture (cf. Fig. 9)
  - Open the current situation picture
  - Addition of general information
  - Verification of current events
  - Set current status and trend
  - Review of the "live" situation picture
- Creation of a daily situation picture (snapshot of the "live" situation picture) (cf. Fig. 10)
  - Selection of the template (daily situation picture)
  - Verification and supplementation of the content
  - Enter the planned release
  - Approval of the situation picture

Focus group. After the demonstration, a set of questions were asked and discussed in the group. These questions were the basis to discuss any open issues, collect individual feedback, but also to prepare the participants for the final questionnaire, designed according to the SUS methodology. The following questions have been asked:

- Does the proof of concept support you in completing your tasks without burdening you unnecessarily?
  - Are all functions available?
  - Is all information available?
  - How could work-flows be optimized?
- Is the proof of concept sufficiently understandable?
  - Operation prompts
  - Information display
  - Intelligibility
- Does the design of the proof of concept meet your expectations and habits?
  - Does it support orientation?
  - Is information structured in an understandable way?
- Is the concept flexible enough to meet future needs?
  - Integration of further situation reports...
- Do you see an improvement in this concept compared to the current work processes?
  - What could still be improved?

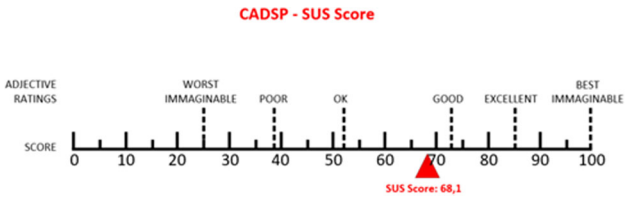

Fig. 11 Final SUS score for the proof of concept application

Calculation of the SUS. The SUS is a way of simply evaluating the usability of a product or system. It consists of ten usability statements that are rated on a scale from **1** (totally agree) to **5** (totally disagree). The SUS contains five positive and five negative statements on the usability of the system to be evaluated. Based on this evaluation of these statements, a usability value is calculated, which can then also be used to compare with other products. The final score, calculate among all participants, was *68.1* as also illustrated and interpreted in Fig. 11.

Qualitative key statements. During the interviews hundreds of qualitative statements were collected that form the basis for further improvements. Besides quite detailed feedback regarding the user interface design and general usability issues, most feedback revolved around a few topics:

- **Usability improvement:** The positioning of user interface elements, the font and the positioning of information elements should be investigated in more detail in course of a user experience evaluation.
- **Tool architecture:** Possibilities for off-line usage (e.g., abroad missions) and isolated operations should further be investigated.
- **Transparency and auditability:** It is important to understand how a CCOP was created, how the different informational elements were evaluated and a current situation assessed. If a human analyst performed some of the steps, it should be transparent who did the work.

- **Automatism and interfacing:** More interfaces for enrichment with further information, e.g., photos, geographic information and non-IT systems are essential to complete the picture. Automatically fetching this information, annotating and linking it to is further vital for swift CCOP creation.
- **Information labelling:** Manual annotation, tagging and justifications, e.g., of derived and interpreted situations shall be stored, however a high degree of automation shall be achieved with as little human involvement as possible. With regard to that processing of classified information, e.g., according to the traffic light protocol, must be enabled.
- **Going beyond state-of-the-art:** Today's processes involve lots of manual effort, such as copying and pasting in standard tools (such as MS Office). Centrally collecting information, having them processed and interpreted by dedicated actors, and having them distributed along predefined lines, has tremendous potential to streamline and optimize existing processes.

6 Conclusion and future work

This paper presented an approach to create cyber situational awareness through collecting and interpreting messages, events and notifications from various organizational data sources. Current technologies that are utilized such as e-mail, ticketing systems, shared documents or CTI tools provide some functionality to exchange information; however, these are usually spread across different systems and services and therefore do not efficiently support the fast creation of cyber situational reports. Therefore, we proposed a new approach and introduced a common data model that frequently captures all the relevant information in a coherent manner that are used in the CCOP creation process. Two major views are relevant for the command level: an external view, which encompasses the general cyber situation world-wide, with a certain focus on the national level; and a second view which provides insights on the threat level of the own organization only. The investigation of typical metrics complemented these efforts. We analyzed the applicability of this approach by implementing a proof-of-concept application together with the Austrian ministry of defense that quickly enables the re-occurring or on-demand creation of reports (e.g., in case of incidents).

A novelty of our solution is, that complex and diverse data elements, relevant for cyber security, can be collected over a multitude of interfaces and reviewed, interpreted and reported upon in an aggregated form at a central point. From there, adequate mitigation actions can be taken, relevant stakeholders informed, and the cyber situation tracked over time.

Future work includes the in-depth evaluation in the operational military environment, were future users will be challenged with realistic situations. This evaluation will focus on the applicability of the tool in the target environment on the one side (e.g., fulfillment of domain-specific requirements, etc.) and overall usability aspects on the other side. Regarding the further development of the tool, more automation for the evaluation of a situation based on data inputs using, for instance, rule-engines for reasoning, seems to be a promising field.

Funding Open access funding provided by AIT Austrian Institute of Technology GmbH This work has been funded by the Austrian defense research programme FORTE of the Federal Ministry of Agriculture, Regions and Tourism (BMLRT) in course of the project CADSP (873425).

Data availability The datasets created during the usability evaluation are not publicly available due to their military background.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Endsley, M.R.: Design and evaluation for situation awareness enhancement. In: Proceedings of the Human Factors Society annual meeting, vol. 32, pp. 97–101. Sage Publications Sage CA: Los Angeles, CA (1988)
2. Pahi, T., Leitner, M., Skopik, F.: Analysis and assessment of situational awareness models for national cyber security centers. In: International Conference on Information Systems Security and Privacy, vol. 2, pp. 334–345. SCITEPRESS (2017)
3. Varga, S., Brynielsson, J., Franke, U.: Information requirements for national level cyber situational awareness. In: 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 774–781. IEEE (2018)
4. Conti, G., Nelson, J., Raymond, D.: Towards a cyber common operating picture. In: 2013 5th International Conference on Cyber Conflict (CYCON 2013), pp. 1–17. IEEE (2013)

5. Danielsson, E., Alvinius, A., Larsson, G.: From common operating picture to situational awareness. Int. J. Emerg. Manag. **10**(1), 28–47 (2014)
6. Hamilton, W.L.: Situation awareness metrics program. Tech. Rep., SAE Technical Paper (1987)
7. Harwood, K., Barnett, B., Wickens, C.D.: Situational awareness: A conceptual and methodological framework. In: Proceedings of the 11th Biennial Psychology in the Department of Defense Symposium, pp. 23–7. US Air Force Academy (1988)
8. Billings, C.E.: Situation awareness measurement and analysis: a commentary. In: Proceedings of the International Conference on Experimental Analysis and Measurement of Situation Awareness, vol. 1. Daytona Beach, FL: Embry-Riddle Aeronautical University Press (1995)
9. Endsley, M.R.: Measurement of situation awareness in dynamic systems. Human Factors **37**(1), 65–84 (1995)
10. Munir, A., Aved, A., Blasch, E.: Situational awareness: techniques, challenges, and prospects. AI **3**(1), 55–77 (2022). https://doi.org/10.3390/ai3010005
11. Chiefs of Staff, J.: JP 2-01.3 Joint intelligence preparation of the operational environment (2009)
12. Okolica, J., McDonald, J.T., Peterson, G.L., Mills, R.F., Haas, M.W.: Developing systems for cyber situational awareness. In: 2nd Cyberspace Research Workshop, vol. 46 (2009)
13. Tadda, G.P., Salerno, J.S.: Overview of cyber situation awareness. In: Cyber situational awareness, pp. 15–35. Springer (2010)
14. Brynielsson, J., Franke, U., Varga, S.: Cyber Situational awareness testing. In: Combatting cybercrime and cyberterrorism: challenges, trends and priorities, pp. 209–233. Springer (2016)
15. Komárková, J., Husák, M., Laštovička, M., Tovarňák, D.: CRUSOE data model for cyber situational awareness. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018. Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3230833.3232798
16. Husák, M., Jirsík, T., Yang, S.J.: 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, pp. 1–10 (2020)
17. Skopik, F., Ma, Z., Smith, P., Bleier, T.: Designing a cyber attack information system for national situational awareness. In: Future Security Research Conference, pp. 277–288. Springer (2012)
18. Skopik, F., Pahi, T.: Under false flag: using technical artifacts for cyber attack attribution. Cybersecurity **3**(1), 1–20 (2020)
19. Maxwell Air Force Base, A.: Three Levels of War; USAF College of Aerospace Doctrine, Research and Education (CADRE). In: Air and Space Power Mentoring Guide. Air University Press (1997)
20. Harrington, R.J., Ottenbacher, M.C.: Decision-making tactics and contextual features: strategic, tactical and operational implications. Int. J. Hosp. Tour. Adm. **10**(1), 25–43 (2009). https://doi.org/10.1080/15256480802557259
21. Ardil, C.: A comparative analysis of multiple criteria decision making analysis methods for strategic, tactical, and operational decisions in military fighter aircraft selection. Int. J. Aeros. Mech. Eng. **14**(7), 275–288 (2021)
22. White, G.: Strategic, tactical, & operational management security model. J. Comput. Inf. Syst. **49**(3), 71–75 (2009). https://doi.org/10.1080/08874417.2009.11645326
23. OASIS: Open and cyber threat intelligence technical committee and others: Introduction to stix (2019)
24. Booth, H., Turner, C.: Vulnerability description ontology (vdo): a framework for characterizing vulnerabilities (2016)
25. Mell, P., Scarfone, K., Romanosky, S.: A complete guide to the common vulnerability scoring system version 2.0 (2007). https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51198
26. Office of the DoD Chief Information Officer: DoD instruction 8531.01: DoD vulnerability management (2020)
27. Stone, M., Irrechukwu, C., Perper, H., Wynne, D., Kauffman, L.: NIST special publication 1800-5: IT asset management
28. Schmitt, S., Kopriva, J., Lepik, T., et al.: Reference incident classification taxonomy. (2018)
29. United States Department of the Army Headquarters: FM 2-22.3 Human Intelligence Collector Operations. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/fm2_22x3.pdf
30. Skopik, F.: Collaborative cyber threat intelligence: detecting and responding to advanced cyber attacks at the national level. CRC Press (2017)
31. Zhao, Y., Lang, B., Liu, M.: Ontology-based unified model for heterogeneous threat intelligence integration and sharing. In: 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), pp. 11–15. IEEE (2017)
32. Franke, U., Brynielsson, J.: Cyber situational awareness-a systematic review of the literature. Comput. Secur. **46**, 18–31 (2014)
33. Cimino, M.G.C., Lazzerini, B., Marcelloni, F., Ciaramella, A.: An adaptive rule-based approach for managing situation-awareness. Expert Syst. Appl. **39**, 10796–10811 (2012). https://doi.org/10.1016/j.eswa.2012.03.014
34. Langton, J.T., Newey, B.: Evaluation of current visualization tools for cyber security. In: Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II, vol. 7709, p. 770910. International Society for Optics and Photonics (2010)
35. Paulsen, C., Byers, R.: NISTIR 7298 revision 3: Glossary of key information security terms. https://doi.org/10.6028/NIST.IR.7298r3
36. Gragido, W.: Understanding indicators of compromise (IOC) Part I
37. United States Federal Cybersecurity Centers: Cyber Incident Severity Schema. https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf
38. Kovačević, N., , Stojiljković, A., Kovač, M: Application of the matrix approach in risk assessment **2**(3), 55–64. https://doi.org/10.31181/oresta1903055k
39. Forum of incident response and security teams: source evaluation and information reliability. https://www.first.org/global/sigs/cti/curriculum/source-evaluation
40. Canadian Centre for Cyber Security: Cyber threat and cyber threat actors. https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors
41. Sailio, M., Latvala, O.M., Szanto, A.: Cyber threat actors for the factory of the future **10**(12), 4334 (2020). Multidisciplinary Digital Publishing Institute
42. ISO/IEC 27005:2018 Information technology—security techniques — information security risk management
43. Blank, R.M., Gallagher, P.D.: NIST Special Publication 800-30 Revision 1: guide for conducting risk assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
44. Houmb, S.H., Franqueira, V.N., Engum, E.A.: Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Softw. **83**(9), 1622–1634. https://doi.org/10.1016/j.jss.2009.08.023
45. Lee, J.: An enhanced risk formula for software security vulnerabilities https://www.isaca.org/resources/isaca-journal/past-issues/2014/an-enhanced-risk-formula-for-software-security-vulnerabilities
46. Plan, F., Fraser, N., O'Leary, J., Cannon, V., Read, B.: APT40: Examining a China-nexus espionage actor. https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html
47. Johnson, C., Badger, L., Waltermire, D.: NIST Special Publication 800-150 Revision 1: Guide for Cyber Threat Information Shar-

ing. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
48. Bangor, A., Kortum, P., Miller, J.: Determining what individual SUS scores mean: adding an adjective rating scale. J. Usability Stud. **4**(3), 114–123 (2009)