# *Development and evaluation of information elements for simplified cyber-incident reports*

Patrik Lif, Teodor Sommestad, Dennis Granåsen
Division for C4IS
Swedish Defence Research Agency
Linköping, Sweden
{patrik.lif, teodor.somemstad, dennis.granasen}@foi.se

*Abstract* — **In cyber security incident handling one of the most important tasks is to report what has occurred. Several frameworks have been developed to support this reporting, all with their own pros and cons. As a first step in the development of a practically useful incident description standard, we set to determine the appropriateness of sixteen plausible information elements relating to traceability and analysis.**

**The information elements were evaluated during an exercise with 30 participants in which the participants were instructed to report cyber threats and incidents in their assigned networks. The evaluation assessed the extent to which the proposed information elements were used in the reports, if the sixteen information elements correlate with the quality of the incident reports, and the participants' subjective experiences of using the elements. The results show that the usage ratio of information elements varies a lot both between different reporters and between incidents. Further, the number of information elements used in a report correlated with the exercise management's quality assessments. Finally, the results reveal that although the overall assessment of content relevance of the simplified cyber-incident reporting template was positive, there is need for further validation of the template.**

***Keywords— Cyber security; incident report; information elements; cyber situation awareness; log analysis; log analyst.***

## I. Introduction

Cyber security lacks a clear and unified definition, but there are several overall ideas about what the concept includes and what work it requires. For example, the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework developed by the US National Institute for Standards and Technology (NIST) describes 1007 tasks, 374 skills, 176 abilities, and 630 knowledge aspects related to the cyber security professions [1]. This paper focuses on professional role known as log analyst and the specialty area Cyber Defence Analysis, which is a part of the workforce category Protect and Defend in NICE. This is an active research field in which over a thousand new articles are presented annually in scientific forums. The vast majority of these publications focus on technical solutions and only a small portion involve the people that are supposed to use the technical solutions.

NICE is a comprehensive framework that serves as a reference to support a workforce to meet organization's cybersecurity needs. This workforce could be log analyst's that is in focus here. Log analyst's main tasks are to monitor, analyze and decide on appropriate measures for the detection of threats and attacks. Log analysis consists of information collection, automatic analysis and manual analysis [2]. During the manual analysis log analysts need to assess events, the state of the system and alarms from automated analysis tools. Based on this, log analysts try to get a good understanding of their own system, identify threats to the system and find appropriate countermeasures to address these threats. Appropriate countermeasures include system reconfiguration, software updating, and disconnecting computers. Often, e.g. when something proved to be a false alarm, the analysis may end with feedback to those who configure the system. The log analyst's incident reports are sometimes produced for recordkeeping and traceability, but often also as input to other log analysts' work and for external stakeholders.

The amount of data and level of detail needed in a cyber-incident report naturally depends on the purpose of the report, but it is good practice to create a record of detected incidents shortly after they are detected to reduce the risk of forgetting important information. There are, to the authors' knowledge, no established standards for incident reports for the purpose of understanding incidents and their potential role in a larger scheme, e.g. a targeted cyber-attack. This study sets to determine what information elements are appropriate to support such incident management in a time-critical and high mental workload situation.

The next section gives a brief overview on relevant research, e.g. log analysts' work situation, information elements for cyber situation awareness and frameworks for incident handling. The following sections presents three common cyber security frameworks (STIX, VERIS and NIST) and a task analysis of log analyst work, all reviewed in light of the related work. A simplified incident report with 16 information elements is then presented, followed by an evaluation of the developed incident report in a realistic setting with cyber security experts. Finally, a discussion of findings and implications is presented together with a description of proposed future work.

## II. Related work

To provide a better understanding of the information elements that are relevant for incident reports, this section describes the role of log analysts; information elements and their coupling to log analysts' situation awareness; and established frameworks for incident reports.

### *A. Experience from earlier work with log analysts*

To monitor an information system for cyber security incidents is normally a rather monotonous task, which involves identifying discrepancies, irregular patterns and other signs of real threats among many alerts. The work typically involves visually checking event logs in multiple systems and correlating them with each other. Tasks are often divided so that some people prioritize alerts from security sensors and others perform deeper analysis tasks involving manual correlation of data from multiple systems [3]. A goal directed task analysis [4] and a hierarchical task analysis [5], both in security operations centers, have confirmed that log analysts' essentially work in three different roles: scouts, analyst, and team leaders. The team leaders' tasks are to prioritize between possible events, monitor if some events escalate, retrieve external information (e.g. from open sources on internet) and keep a journal of incidents. The scout should identify incidents and potential threats, choose software for analysis and notify team leader and the analysts. The analysts receive cases from team leader or scout, select analysis software, conduct a thorough analysis and report back to the team leader. Traceability is essential for all roles, hence systematic record-keeping and incident reporting is major part of the analysts work, regardless of their role. However, the purpose and recipients of these reports, and therefore their contents, can differ between roles. Regardless of role the incident handler need good situation awareness. Research about incident handling has been extensive, often with a technical focus [6]–[8].

Lif et al. [4] have developed and validated a freeze-probe technique to measure log analysts' situation awareness. Two questionnaires were designed separately for the scout and analyst roles and evaluated in a realistic setting during an exercise involving five professionals. The questionnaires were well received by the log analysts. The results suggest that the technique can be used to evaluate cyber situation awareness for log analysts, as well as function as a tool in log analysts' daily work to keep track of incidents. The latter is probably the most important result coupled to this paper.

### *B. Log analysis, situation awareness and information elements*

A literature review was conducted in order to obtain and understand the field of log analysis with focus on situation awareness and information elements. This review found a number of relevant papers.

Gutzwiller, Fugate, Sawyer and Hancock [9] state that technology has a critical role in the fight against cyber-attacks, but also emphasize that technology does not exist in isolation from human factors. Their article outlines links between cyber defense challenges and major human factors and ergonomics research, e.g. situation awareness.

Barford et al. [10] state that situation awareness for cyber defense is an aggregate of at least seven aspects that the incident handler needs to be aware of: current situation; impact of the attack; how the situation evolves; actor (adversary) behavior; why and how the current situation was caused; quality (trustworthiness) of collected information; and plausible future evolvement of the situation.

Mahoney et al. [11] present preliminary findings from a cognitive task analysis conducted on a subject matter expert. The effort was to develop a software tool to support cyber situation awareness. Their analysis highlights some preliminary categories of requirements and questions that could affect the design and development of a situation awareness tool.

Dressler, Bowen, Moody and Koepke [12] argue that six classes of information should be utilized to establish operationally relevant situation awareness: threat environment, anomalous activity, vulnerabilities, key terrain, operational readiness, and ongoing operations.

Shiravi, Shiravi and Ghorbani [13] conducted a review of network security visualization that provide six potential data sources: network traces, network events, application logs, security events, as well as context related to network activity, users and assets. These data sources encompass only a limited portion of situation awareness since focus is on anomalous activities, and not the other five aspects in Dressler's classification.

Brynielsson, Franke and Varga [14] report that cyber situation awareness is loosely defined and the literature describing which information elements that give situation awareness is limited. However, their review gives some insight into what information is considered important, and thereby should be included in incident reports.

Detection and management of threats presumes good understanding of the systems that are monitored, including awareness of vulnerabilities, the capability of available tools (sensors) for detecting anomalies and the significance of detected anomalies [15], [16].

### *C. Frameworks for incident handling*

There are several suggestions on how to describe cyber incidents. Here follows description of three established frameworks that is considered to be the most relevant frameworks to evaluate which information elements that should be included in a simplified incident report: Structured Threat Information Expression (STIX) [17], Vocabulary for Event Recording and Incident Sharing (VERIS) [18], and NIST's Computer Security Incident Handling Guide [19]. The STIX framework (Fig. 1) is especially interesting because it offers a standardized vocabulary and data exchange format for cyber information threats, and therefore implements many features that could be useful in a cyber incident reporting template.

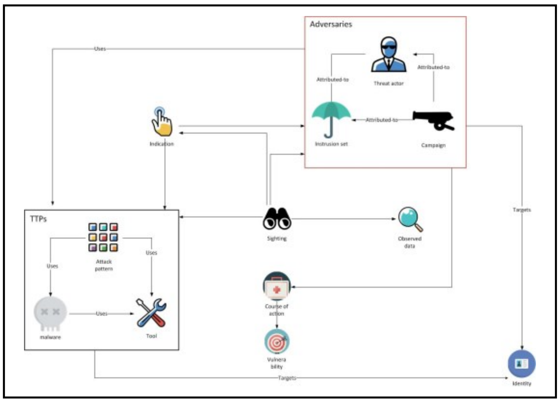

Fig. 1. *STIX architecture. Icons from* [20]–[22].

STIX contains twelve domain objects, some of which (here presented in parenthesis) give a hint to what log analysts need to observe when analyzing an incident. The log analyst monitors the computer network and searches (sighting) for suspected malicious code. The adversaries is described by specifying who is behind the current attack (threat actor), whether the attack is part of larger attack scheme (campaign) and opponent's resources and behaviors (intrusion set). Based on knowledge of the attack, the person, group or organization behind the attack is searched for (identity), and also what needs to be done to prevent attacks or stop an ongoing attack (course of action). This often means ensuring that vulnerabilities do not exist in the own network. To detect and identify who is behind the attack, it is also necessary to gather information about the opponent's tactics, methods and procedures, e.g. attack patterns, tools and malware. This information specifies how to detect the attack (indicator) and what information collection is required (observed data).

The twelve domain objects are described by content and relationships to other objects (lines and arrows shown in Fig. 1). Domain objects hold ten common properties (type, id, created_by_ref, created, modified, revoked, labels, external_references, object_marking_refs, granular_markings). In addition, each domain object has specific characteristics. For example, attack pattern requires the user to enter name, text description and where in the kill-chain the attack is located [23]. With 58 specific properties (3-10 per object) and 120 common (12 objects with 10 each as specified above) the total number of properties is 178. Add to that the many relationships between objects and STIX must be described as a rich model with high granularity. The model can be complicated and time consuming to use due to the amount of information needed to fully populate the model, although the framework itself does not enforce strict usage of all attributes.

VERIS is a framework consisting of a set of metrics to create a standardized way of describing incidents. The basic idea is to start lightly with seven metrics: year, month, day, who discovered the incident, what happened and how it happened. Two levels of information are added on top of this, in VERIS is denoted as enumerations. At the first level, it is judged whether it was an attack or not (could be a false alarm), and how the attack was detected. On the second level, actors, actions, attributes, and asset (4A) should be described. Each VERIS enumeration allows for additional details for a total of 74 information fields, but there is also a documentation schema divided into incident tracking (32 fields), victim demographics (45 fields), discovery & response (46 fields) and impact assessment (30 fields). Similar to STIX, VERIS may be perceived as complicated and time consuming to use.

NIST's Computer Security Incident Handling Guide [19] aims to support organizations in their work on incident management in an effective and efficient manner. According to this framework organizations should identify incident-related data elements that facilitate an effective and consistent incident handling. The framework serves as a guide to help organizations meet applicable incident reporting requirements. The guide contains basic elements and incident-handler data elements. The basic elements are divided into information about the reporter (6 elements), details about the incident (11 elements) and general comments. Incident handler data elements has seven fields (e.g. current status of incident response, summery of incident and incident handling actions). Each organization should create its own list of elements. This guide is more general and contains fewer formalized details than STIX and VERIS. The details of the incident are instead given in the form of textual descriptions, e.g. which resources were affected, how the incident was detected and what countermeasures were used.

## III. SELECTION OF INFORMATION ELEMENTS AND DEVELOPMENT OF TEMPLATE FOR SIMLIFIED INCIDENT REPORTS

There is limited consensus on what information elements are needed in an incident report. Some suggestions include, for example, abstract information elements such as health [11] while others suggest more factual data elements such as IP addresses [24]. As described above, templates available in guides and standards include many details (often over 100 attributes) or detailed textual descriptions of the incidents. This is not surprising because there is a lot of information that could be collected and included in different incident description. Frameworks such as STIX and VERIS are meant to capture the information available after an incident and are not necessary suitable to use during an ongoing incident. Due to workload and potential urgency to respond to critical events, incident handlers may require simplified reporting tools to keep track during their immediate response actions, and to preserve notes for post-handling incident reports.

Based on findings from our own previous work [4] and the reviewed work, a proposal was developed regarding what information elements should be included in rapid cyber-incident reports. Most important for the selection of information elements is previous developed technique to measure cyber situation awareness [4]. Several of the questions used to measure cyber situation awareness can also be used as information elements in an incident report. Examples of questions used to measure situational awareness and which are also considered to be important in incident reports included description of the incident, which system that was under attack, assessment of severity, and assessment of urgency for countermeasures. The proposal presented here contains five categories: background, victim, attacker, description and damage (Table 1). These categories contain between two and four information elements each, which sums up to a total of 16 elements.

Table 1. *Incident examples and scoring template.*

| **Background** | **Victim** | **Attacker** | **Incident description** | **Damage assessment** |
|---|---|---|---|---|
| Rapporteur<br>Observations/ indications | Node<br>User<br>Comment | Node<br>User<br>Comment | Suspected attack objective<br>Attack or vulnerability details<br>Attack mechanisms<br>Attack domains (e.g. social engineering, software & hardware) | Probability that the attacker suceeded with the attack.<br>Asset criticality<br>Attack impact<br>Response urgency |

The selected information elements are essentially consistent with the content of the reviewed frameworks. The VERIS and NIST frameworks both contain all five categories, while STIX contain background, attacker and description. As STIX was designed for information exchange, it focuses on generic elements of an attack and therefore does not include information tied to specific assets and their value, information that may potentially be confidential.

While the proposal presented here focuses on similar elements as established standards, it is significantly simplified with only sixteen information elements. This simplification is believed to make it useful for information sharing activities where there is limited time to write full incident reports, e.g. in communication between scouts and analysts. The purpose of the present research was to determine what information elements are appropriate to support incident management in a time-critical and high mental workload situation. The result can be used to customize different templates for incident reports.

## IV. Evaluation of information elements

The information elements were evaluated during the incident handling exercise iPilot [25]. The participants' primary task was to ensure the operation of an IT-system in a simulated coal power plant and maintain adequate production levels while detecting intrusions and misconfigurations in the computer networks. The exercise was conducted over four days with introduction and training the first day, exercise the second and third day, and evaluation on day four. The template with sixteen information elements was evaluated with respect to the following research questions:

1. To what extent are each of the sixteen information elements used by the log analysts during the exercise?
2. To what extent does the use of each of the sixteen elements correlate with the quality of the incident reports?
3. How did the log analysts experience answering the sixteen information elements and using the tool for answering the incident report?
4. Was there any training effects and how did the participants' experience the usability of the exercise tool?

The exercise organization during iPilot consisted of a white, a red, a yellow, and a green team in accordance with international practice and terminology [26]. Five blue teams of six IT professionals each participated in the exercise. The white team consisted of an exercise leader (overall responsibilities), game leader (responsible for game implementation), group of people for evaluation, and a supportive exercise staff. The red team was responsible for planning and implementation of incidents prior to and during the exercise. The yellow team had one representative in each team observing teamwork and making sure data collection routines were followed. The green team provided technical support to make sure that computers and the networks were operational throughout the exercise.

### *A. Environment*

The exercise was performed in the Swedish Defence Research Agency's Cyber range and testing environment (CRATE) [27]. Each team were given a virtual environments to monitor and protect, with typical office networks containing a number of web servers, mail servers, file servers, network equipment and about 50 office computers. The office networks were separated from the industrial control systems via firewalls. The cyber environments represent small coal production plants, with industrial control systems connected to their production process. OpenSimulator [28] which is an open source multi-platform and multi-user 3D application server was used to visualize the coal production plant. The coal plant simulation contained coal transportation, fuel production, burning flame, turbines, and a sub-station with transformers and transmission lines.

The system was intentionally pre-configured with dated, unpatched software and some poorly configured services to generate enough vulnerabilities that the red team can attack the blue teams with widely known exploits.

The attacks were carried out using an in-house developed tool called Scanning, Vulnerabilities, Exploits and Detection (SVED) [29]. Using SVED attacks could be scripted and launched in parallel against all blue teams which made it possible to compare the teams' response efforts. Example attacks include simple network scans (on both sides of the firewalls), brute force attack on network services, malware-infected thumb drives, denial of service attacks, and emails with malicious code attachments.

Participants had been provided with a description of the cyber environment before the exercise started. Each of the six participants was equipped with 1-2 laptops with 15-inch screens. The teams monitored the network traffic with sensors at twelve distinct probe locations in their respective network. For analysis they had access to the log analysis tools Wireshark [30], ELK [31] and Snort [32]. System events such as Windows Event Log [33] were collected in a central system.

### B. Participants and task

All exercised participants were professional IT administrators or cyber security specialists with experience from cyber incident handling. Most of the 30 participants worked at organizations within the Swedish nuclear sector, and the rest worked for the Swedish police. They were divided into five groups, where members from different organizations were mixed. Thus, they did not know the other within the group before the exercise started. Even though the participants were accustomed to work with incident management, their experience was limited in terms of writing incident reports. The participants' task was to detect incidents, gather information and use the provided template to report their findings.

### C. Data collection

The white team reviewed all incident reports and assessed their quality according to a predefined scoring system. This information scoring system was developed independently of the information elements and there was no direct match between the 16 information elements in the template and the predefined scoring template. Thus, the scoring represented an independent expert opinion of the incident reports' quality. Table 2 shows two examples of incidents and how white team scored the incident reports.

Table 2. *Information elements used during exercise.*

| Name | Description | Scoring |
|---|---|---|
| Bittorrent in the network | The µTorrent client is run by users to download and share material. Malware is downloaded. | Discovered with Snort (60 points). Description of affected computers (60 points), users (40 points) and tracker (40 points). Must be described to obtain 200 points. |
| DDos against company webserver | A DDoS attack is started against the web server. | Detection within 15 minutes gives 120 points, after 15 minutes 60 points. Detection of attacking IP addresses gives an additional 40 points. Suggestions to block IP numbers in the firewall or other similar solution provide an additional 40 points. |

### D. Results

The results are reported on the basis of the aforementioned research questions. The five groups with six participants each submitted 172 incident reports in total. Group one submitted 22 reports, group two 33 reports, group three 23 reports, group four 73 reports and group five 21 reports. These reports were analyzed quantitatively and qualitatively with respect to information elements usage and applicability, as well as the perceived value of each of the sixteen information elements. Also, *training effects and participants' experience of the exercise tool* is reported here.

#### 1) Quantitative use of the information elements

The proportion of used information elements varies greatly between different elements, see Table 3.

Table 3. Proportion used information elements day one and two.

| **Category** | **Information element** | **Usage ratio day 1** | **Usage ratio day 2** |
|---|---|---:|---:|
| **1.Background** | Rapporteur | 48% | 94% |
| | Observation or indicators | 92% | 98% |
| **2.Victim** | Node | 77% | 91% |
| | User | 18% | 30% |
| | Comment | 17% | 37% |
| **3.Attacker** | Node | 25% | 56% |
| | User | 5% | 19% |
| | Comment | 6% | 24% |
| **4.Incident description** | Suspected attack objective | 60% | 86% |
| | Attack details | 50% | 60% |
| | Attack mechanism(s) | 49% | 52% |
| | Attack domain(s) | 46% | 54% |
| **5.Damage assessment** | Success probability | 61% | 73% |
| | Asset criticality | 64% | 83% |
| | Attack impact | 62% | 81% |
| | Response urgency | 62% | 84% |
| **Mean** | --- | **46%** | **64%** |

Background (category 1) was frequently used, except the reporter's name day one. In the description of victims (category 2), the attacked node was often reported, but rarely the user and the detailed description requested. One possible reason for the low numbers is that it was not always possible to use these elements since the teams were unable to retrieve the information. This is because such understanding requires a more comprehensive analysis that the participants' were to stressed to carry out, or did not prioritize during the exercise. The information elements in attackers (category 3) were rarely used. This may also be due to a lack of time and that the teams did not analyze the background of the attack. The more detailed description of the attack's execution (category 4) and damage assessment (category 5) were used relatively often considering the stressful situation.

#### 2) Qualitative use of the information elements

There is small, but statistically significant, correlation (r = 0.22 and p = 0.003 between the number of elements used and the exercise management's quality assessment, i.e. the score given for each incident report. Fig. 2 illustrates the correlation with regression line and the variation. The lightest gray dots represent one single data point, while darker gray dots correspond to two or three samples. The black samples (all on the zero score line) correspond to four or more samples, note that these samples mostly correspond to false positives and duplicate reports. The figure shows that there is a clear roof and floor effect. That is, some reports received either zero or 200 points. With only samples reports with 1-199 points are included in the analysis, the correlation coefficient increases to r=0.34. Thus, the roof and floor effects appears to limit the relationship, and a scoring system that gave negative scores for erroneous reports and more than 200 points for excellent reports is likely to yield a stronger relationship. Furthermore, there are many samples where fields have been used improperly or when they have been assigned incorrect information (e.g. because a false positive is reported). Thus, the relationship can be expected to be stronger if only fields used correctly and true positives are considered.

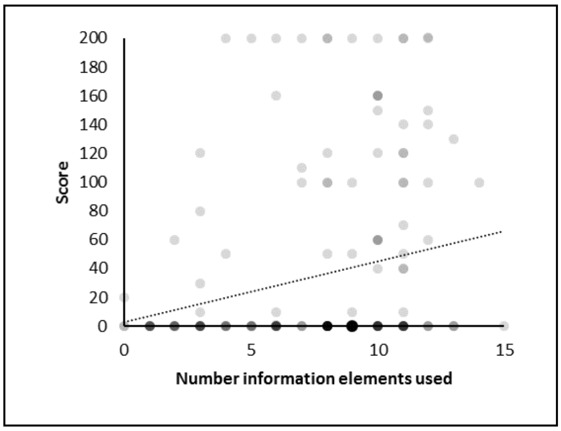

Fig. 2. STIX architecture. Icons from Frost and Lapin [20]; [22]; and Langella [21].

*3) Subjective experience to use information elements and template*

In order to answer whether the information elements were meaningful to use in the incident reports, the participants answered questionnaires on a seven-point grading scale. A low value was always negative and a high value positive, such as 1=very low and 7=very high. The questionnaire was concluded with one open question where the participants could write overall subjective comments.

The participants' average rating of the content relevance of the information elements included in the cyber-incident report was 4.3. This value indicates that continued work is required to determine an appropriate set of information elements for cyber incident reports targeted at professionals with the same or similar background as in this exercise. A common comment from the participants was that they found that they needed to report too much information despite the efforts to create a simple template with only sixteen information elements. However, discussion with one of the teams also showed that several of them used more detailed incident reports in their daily operations. A possible source of frustration was the high pace of the exercise, which meant that they needed to write many incident reports in a short period of time.

*4) Training effect and usability of exercise tool*

As Table 2 shows, there is a noticeable difference between how the elements were used during day one and two. A t-test show that there is a statistically significant training effect (t = 4.7; df = 62, p <0.001). Fig. 3 illustrates the effect graphically.

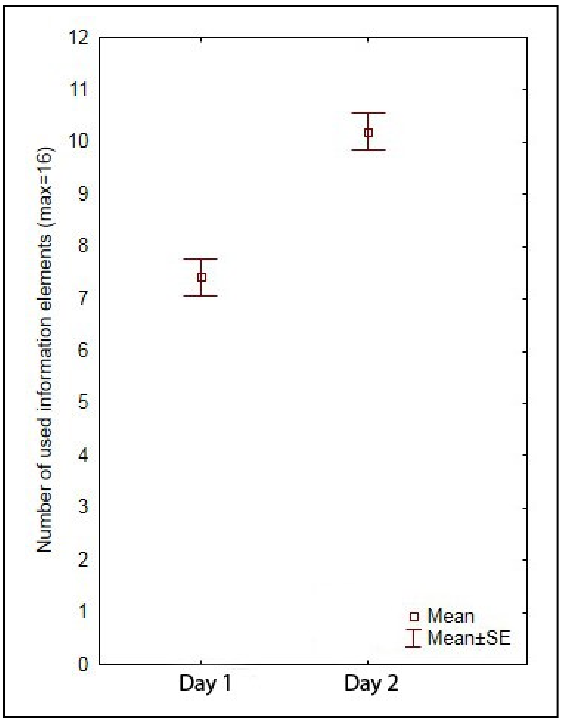

Fig. 3. Mean number of used information elements with ± standard error.

109 reports were submitted during day one and the teams received on average 29.8 points per submitted report. The second day, 63 reports were submitted and the groups received on average 44.4 points per submitted description. The participants' subjective estimates of the CEC Exercise Management Tools' usability were relatively low (overall average 3.7, specifically for incident reports 3.4). Since CEC's primary purpose is not to describe incidents but gather all information needed for the exercise, this relatively low rating was expected and may have affected the results. There is a risk that the participants experienced the content relevance of the sixteen information elements negatively due to inadequate usability of the tool (CEC) used to collect information.

## V. Discussion

The academic value of the results presented in this paper is evaluated in the following section against the seven guidelines of design science [34]. Thereafter the authors' conclusions are presented with focus on the significance of the presented results and future work.

### A. Research contribution

The purpose of this study was to investigate what information elements are suitable in a simplified cyber incident reports produced in stressful situations with high mental workload. This by evaluating to what extent the proposed information elements were used respectively, and whether the choice to report a particular element had any influence of the assessed quality of the reports. The participants' subjective experiences of reporting the elements were also evaluated.

The work presented in this paper is based on a literature review on information elements for cyber situation awareness, three frameworks for incident handling, and task analysis conducted with log analysts. Based on this aggregated background information, a proposed incident report template was developed with sixteen information elements. This template was evaluated in an exercise with 30 participants.

One way to evaluate scientific design research in information systems is the use of the seven guidelines in design science [34]. According to these guidelines, an artifact must first be created (guideline 1), and the artefact should solve an important and relevant problem (guideline 2). The artefact needs to be evaluated to ensure its usefulness for the specified problem (guideline 3). To ensure that the artefact is a meaningful contribution to the research community, the artefact should either solve an existing problem or provide a more effective solution than previously announced (guideline 4). Both the design and evaluation should be rigorously performed (guideline 5). The process through which the artefact is developed should resemble an iterative process that search for new effective ways to solve problems (guideline 6). Finally, the results of the research ought to be presented effectively both to people with technology-oriented focus and to people in management positions (guideline 7).

The study presented in this paper meets the guidelines for design science:

1. The incident report with the sixteen information elements was developed as a simplified incident report tool for log analysts to use in a practical situation. Thus, an artefact was produced (guideline 1).

2. What information elements that should be included in incident reports is a relevant and current issue, which researchers and organizations try to find a good solution to (guideline 2).

3. The artefact has been evaluated (guideline 3), although it is recognized that the evaluation should be repeated in more realistic contexts with professional log analysts to increase its validity.

4. A shortcoming in this study is that the proposed incident report has not been compared with other alternatives. However, unlike existing frameworks, such as STIX and VERIS, the proposed incident report template has been customized to fit situations with limited time to write reports, and therefore it fills a need that is not covered by the more extensive frameworks. This artefact is therefore an improvement from existing frameworks (guideline 4).

5. In order to ensure that an adequate set of information elements are used, literature reviews and task analysis with log analysts have been conducted in accordance with accepted scientific methods. Thus, the development of the artefact (guideline 5) has been careful and thorough.

6. An earlier version of the incident report has been tested during an exercise. The development has thus been conducted iteratively and provided new knowledge about which information elements should be used (guideline 6). At the same time this proposal cannot be considered fully developed. More research is required to adapt the incident report template to different situations.

7. This paper describes the information elements and their utility in incident reporting and is part of choosing an adequate set of information elements, and thus a step towards acceptance. Also, the research has been communicated to some stakeholders (guideline 7).

### B. Conclusions and future work

The presented evaluation shows that the extent to which the information elements were used varies. The information elements rapporteur, observation or indicators, victim node, description of suspected attack objective, asset criticality, attack impact, and response urgency were used in over 80% of the incident reports in day two. Information on the source of the attacks and the description of this entity were reported far less frequently, which is not surprising as it is a much more difficult task than to describe the indicators that the reporter reacted to. Although the participants could identify which node was attacked, they rarely reported what users were affected and did not give any further descriptions of the victim. This was not surprising, because in several incidents targeted entire systems and services rather than particular users.

The incident report template was created to be used for different incidents, which resulted in that the information elements did not always fit the incident. This was also evident in discussion with one of the groups that stated that it was not always possible to use the entire incident report, which probably explains the participants' modest subjective rating of the content relevance of the information elements in the incident reports.

The result showed a correlation between the number of fields used and the points given, but more work is needed to better understand for example which fields are of the greatest importance and how incorrectly filled descriptions affected the results.

It is also worth noting that there was a clear difference between how the information elements were used day one and day two, which also had an effect on the score. On the first day, 109 incidents were reported and the groups received 29.8 points on average per submitted report. On the second day, 63 incidents were reported and the groups received 44.4 points on average per submitted report. One reason that the number of submitted reports dropped from day one to day two could be that more effort was put into each report. This is also shown by the improved quality of reports from day one to day two. Another reason could be that the participants had developed an increased knowledge of their own networks and thus were able to better distinguish between false alarms and true incidents, and thereby were able to reduce the amount of false reports.

The participants' reactions to the selected information elements in the developed simplified cyber incident report template were positive and as such the template can be useful during exercises, but training is recommended to use the template more effectively, as the difference between day one and day two shows. Whether the incident report template can be used by log analysts in operational incident handling has not been investigated and therefore cannot be answered in this paper. However, the evaluation with participants working with cybersecurity indicates that these information elements can be used as a starting point for incident reports in different situations. The evaluated incident report template is a promising candidate for rapid reporting in stressful situations of critical information relating to cyber incidents, e.g. when a scout first detects a suspected incident and passes over the incident report to an analyst for deeper analysis.

## VI. References

[1] B. Newhouse, S. Keith, B. Scribner, and G. Witte, "National Initiative for Cybersecurity Eduction (NICE) Cybersecurity Workforce Framework," Gaithersburg, MD, USA, 2017.

[2] T. Sommestad and A. Hunstad, "Intrusion detection and the role of the system administrator," *Inf. Manag. Comput. Secur.*, vol. 21, no. 1, pp. 30–40, Mar. 2013.

[3] C. Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center*. Bedford, MA: The Mitre Coropration, 2000.

[4] P. Lif, M. Granåsen, and T. Sommestad, "Development and validation of technique to measure cyber situation awareness," in *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 2017, pp. 1–8.

[5] P. M. Salmon *et al.*, "Measuring Situation Awareness in complex systems: Comparison of measures study," *Int. J. Ind. Ergon.*, vol. 39, no. 3, pp. 490–500, 2009.

[6] S. Miserendino, C. Maynard, and J. Davis, "ThreatVectors: Contextual workflows and visualizations for rapid cyber event triage," in *Proceedings of the 2017 International Conference On Cyber Incident Response, Coordination, Containment & Control (Cyber Incident)*, 2017.

[7] T. Sommestad, M. Ekstedt, and P. Johnson, "Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models," in *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences*, 2009, pp. 1–10.

[8] S. J. Yang, H. Du, J. Holsopple, and M. Sudit, "Attack Projection," in *Advances in Information Security 62: Cyber Defense and Situational Awareness*, A. Kott, C. Wang, and R. F. Erbacher, Eds. Cham, Switzerland: Springer, 2014, pp. 239–261.

[9] R. S. Gutzwiller, S. Fugate, B. D. Sawyer, and P. A. Hancock, "The Human Factors of Cyber Network Defense," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 59, no. 1, pp. 322–326, Sep. 2016.

[10] P. Barford *et al.*, "Cyber SA: Situational Awareness for Cyber Defense," in *Cyber Situation awareness*, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. London: Springer, 2010, pp. 3–14.

[11] S. Mahoney, E. Roth, K. Steinke, J. Pfautz, C. Wu, and M. Farry, "A Cognitive Task Analysis for Cyber Situational Awareness," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 54, no. 4, pp. 279–283, Sep. 2010.

[12] J. Dressler, C. L. Bowen, W. Moody, and J. Koepke, "Operational data classes for establishing situational awareness in cyberspace," in *International Conference on Cyber Conflict, CYCON*, 2014.

[13] H. Shiravi, A. Shiravi, and A. A. Ghorbani, "A Survey of Visualization Systems for Network Security," *IEEE Trans. Vis. Comput. Graph.*, vol. 18, no. 8, pp. 1313–1329, Aug. 2012.

[14] J. Brynielsson, U. Franke, and S. Varga, "Cyber Situational Awareness Testing," in *Combatting Cybercrime and Cyberterrorism. Advanced Sciences and Technologies for Security Applications.*, B. Akhgar and B. Brewster, Eds. Springer International Publishing, 2016, pp. 209–233.

[15] J. R. Goodall, W. G. Lutters, and A. Komlodi, "Developing expertise for network intrusion detection," *Inf. Technol. People*, vol. 22, no. 2, pp. 92–108, Jun. 2009.

[16] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: the diagnostic work of IT security incident response," *Inf. Manag. Comput. Secur.*, vol. 18, no. 1, pp. 26–42, Mar. 2010.

[17] STIX, "STIX Whitepaper | STIX Project Documentation," 2017. [Online]. Available: http://stixproject.github.io/getting-started/whitepaper/. [Accessed: 24-Mar-2017].

[18] VERIS, "The VERIS Framework," 2017. [Online]. Available: http://veriscommunity.net/. [Accessed: 13-Nov-2017].

[19] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology," Gaithersburg, MD. USA, 2012.

[20] N. Frost and G. Lapin, "Icons," *Smallicons*, 2017. [Online]. Available: http://smallicons.net.

[21] M. Langella, "Icon arrow," *Manuela Langella*, 2017. [Online]. Available: http://www.manuelalangella.com.

[22] Iconshock, "Icon man," *Smashingmagazine*, 2017. [Online]. Available: SmashingMagazine.com.

[23] LockheedMartin, "Cyber Kill Chain® · Lockheed Martin," *Lockheed Martin*, 2017. [Online]. Available: http://www.lockheedmartin.com/us/news/features/2014/isgs-cyber-kill-chain.html. [Accessed: 15-Feb-2017].

[24] A. D'Amico, K. Whitley, D. Tesone, B. O'Brien, and E. Roth, "Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 49, no. 3, pp. 229–233, Sep. 2005.

[25] Strålsäkerhetsmyndigheten, "IT-attack mot kärntekniska anläggningar övas - Strålsäkerhetsmyndigheten," *Strålsäkerhetsmyndigheten*, 2017. [Online]. Available: https://www.stralsakerhetsmyndigheten.se/press/nyheter/2017/it-attack-mot-karntekniska-anlaggningar-ovas/. [Accessed: 20-Dec-2017].

[26] N. Wilhelmson and T. Svensson, "Handbook for planning, running and evaluating information technology and cyber security exercises," Swedish National Defence College, Stockholm, 2013.

[27] T. Sommestad, "STO-MP-IST-133 Experimentation on operational cyber security in CRATE," 2015.

[28] OpenSimulatar.org, "OpenSimulator," 2018. [Online]. Available: http://opensimulator.org/wiki/Main_Page. [Accessed: 17-Jan-2018].

[29] H. Holm and T. Sommestad, "SVED: Scanning, Vulnerabilities, Exploits and Detection," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 2016, pp. 976–981.

[30] Wireshark, "Wireshark · Go Deep.," 2017. [Online]. Available: https://www.wireshark.org/. [Accessed: 08-Nov-2017].

[31] "ELK Product Overview," 2017. [Online]. Available: https://www.elastic.co/products. [Accessed: 15-Feb-2017].

[32] Snort, "Snort - Network Intrusion Detection & Prevention System," 2017. [Online]. Available: https://www.snort.org/. [Accessed: 14-Feb-2017].

[33] "Windows Event Logs," 2017. [Online]. Available: https://technet.microsoft.com/en-us/library/cc722404(v=ws.11).aspx. [Accessed: 14-Feb-2017].

[34] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004.