UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Andres Oras

Online Cyber Security Exercise to Evaluate and Improve Individual Technical Specialists' Cyber Incident Reporting Skills

Master's Thesis (30 ECTS)

Supervisor: Sten Mäses
Supervisor: Margus Ernits
Supervisor: Raimundas Matulevičius

Tartu 2018

Võrgus olev õppus tehnilise spetsialisti küberintsidendi raporteerimisoskuse individuaalseks hindamiseks ja parendamiseks

Lühikokkuvõte:

Küberintsidentide dokumenteerimise ja raporteerimise õppimiseks väljaspool tootmiskeskkonda sobivad olemasolevad meeskondade vahelised mastaapsed küberõppused. Paraku on paljudes väikefirmades vähe ressursse ning üksikud IT lahenduste eest vastutavad ning neil puudub võimalus sellistel suurõppustel osaleda.

Käesolev töö on loodud tehniliste spetsialistide küberintsidentide raporteerimisoskuse individuaalseks hindamiseks ja parendamiseks. Töö sisaldab nõudeid mis kaasnevad võrgus oleva küberintsidendi raporteerimise õppuse loomisega, samuti lühiülevaadet alates 2018 a. 25. Maist Euroopa Liidus kehtivast isikuandmete kaitse määrusest käesoleva õppuse raames. Töös keskendutakse üksikisiku jaoks küberintsidendi raporteerimise õppuse loomise protsessile ning sellega kaasnevatele väljakutsetele. Töös analüüsitakse küberõppuse hindamismetoodikaid ning pakutakse, testitakse ja analüüsitakse uut küberintsidendi raporti hindamissüsteemi. Samuti pakutakse üks potentsiaalne küberintsidendi raporti standardi mall.

Loodud õppus koos genereeritud hindamissüsteemiga võimaldab üksikisikul Interneti vahendusel, väheste ressurssidega, hinnata ning parendada küberintsidendi raporteerimise oskust. Käesoleva töö raames loodi õppus mille eesmärk on andmelekke tuvastamine võrgulogidest. Produtseeritud hindamismetoodika on universaalne ning mõõduka vaevaga rakendatav ka teist tüüpi küberintsidentide raporteerimise õppuste loomisel.

Võtmesõnad:

Küberkaitse, küberkaitseõppused, küberintsidendi raporteerimine, küberintsidendi raporti hindamine.

CERCS: P170, Arvutiteadus, arvutusmeetodid, süsteemid,

juhtimine (automaatjuhtimisteooria)

Online Cyber Security Exercise to Evaluate and Improve Individual Technical Specialists' Cyber Incident Reporting Skills

Abstract:

Existing large-scale team based cyber exercises are well suitable for learning cyber incident documenting and reporting outside the production environments. However, taking part in these big exercises is not an option for many small companies with very limited resources, with only few persons responsible for IT solutions. This thesis is produced to evaluate and improve individual technical specialists' cyber incident reporting skills. Thesis introduces the requirements that are involved with creating online cyber incident reporting exercises. Also, in the context of this exercise, a short review is provided regarding the EU general data protection regulation, active from 25th of May 2018. Thesis also focuses on the process and challenges included with creating a cyber-incident reporting exercise for individuals. Thesis analyzes cyber security exercise evaluation methods and a new cyber incident report scoring method is produced, tested, and analyzed. Possible standard for cyber incident report template is presented. The created exercise with generated evaluation system enables individuals to evaluate and improve their cyber incident reporting skills individually online with low resources. An exercise, with the goal of discovering a data leak from network traffic, was created for this thesis. The produced cyber incident report scoring method is versatile, so that other types of cyber incident reporting exercises can be created upon it, with medium effort.

Keywords:

Cyber security, cyber defense exercise, cyber incident reporting, evaluating cyber incident reports

CERCS: P170, Computer science, numerical analysis, systems, control

Table of Contents

List of abbreviations and definitions

ADDIE model – Analyze, Design, Develop, Implement, and Evaluate (framework for designing and developing educational and training programs)
AI – Artificial Intelligence
CDX – Cyber Defense Exercise
CERT – Computer Emergency Response Team
CISO – Chief Information Security Officer
DPO – Data Protection Officer (enterprise security leadership role required by the General Data Protection Regulation (GDPR))
eIDAS – electronic IDentification, Authentication and trust Services (electronic identification and trust services for electronic transactions in the internal market)
ENISA – European Union Agency for Network and Information Security
GDPR – General Data Protection Regulation (regulation intended to strengthen and unify data protection for all individuals within the European Union (EU))
IEEE-SA – Institute of Electrical and Electronics Engineers Standards Association (organization within IEEE that develops global standards in a broad range of industries)
InfoSec – Information Security
IoT – Internet of Things
ISACA – Information Systems Audit and Control Association (nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management and governance)
ISF – Information Security Forum (delivers practical guidance to overcome wide-ranging security challenges)
I-tee – IT College distance laboratory system
NDA –non-disclosure agreement
NIST – National Institute of Standards and Technology (measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce)
OWASP – Open Web Application Security Project (worldwide not-for-profit charitable organization focused on improving the security of software)
RDP connection – Remote Desktop Connection (protocol that provides a user with a graphical interface to connect to another computer over a network connection
RSA Conference – Rivest, Shamir, and Adelman conference
SANS Institute– Sysadmin, Audit, Network and Security (largest source for information security training in the world)
VOIP – Voice Over Internet Protocol (delivery of voice communications and multimedia sessions over Internet Protocol)
vTA – Virtual Teaching Assistant

List of figures

List of tables

1 Introduction

Digital operations are successively becoming a part of every organizations daily routine regardless of its size or trade. Initially, information technology (IT) related tasks in small organizations were solved by the few that expressed knowledge or interest about computers, and later became responsible for the companies' IT. Over time these specialists gained more experience and knowledge and started working on the company items related to IT security as well. More work in turn meant less time for documenting their work. This course of action has raised many skilled technical specialists with great knowledge about their area of responsibility that tend to lack the necessary skills to document or report their work.

1.1 Problem Statement

Due to the nature of having to "do everything by themselves", technical specialists have exceptional knowledge in their field of expertise [1]. These individuals are very keen on their technical doings and work less on secondary skills like managing- or documenting technical information, regarding cyber incidents for example. Also, quite often they are exclusively responsible for everything related with their company' IT. Therefore, they do not have the required time to report incidents, are either not requested any reporting or do not see the value in it as they are responding to incidents alone. From personal experience the author can say that generally too little emphasis is put on documenting technical data regardless of the reason. Documenting- and reporting cyber incidents is no exception. This way of thinking cannot be the case anymore, regarding the major data protection changes in May 2018, for example [2].

For organizations to comply with the data protection changes, technically skilled personnel working with information or providing information security, need to exercise their technical cyber incident documenting skills. Currently, incident reporting exercising options for such individuals are limited by lack of resources and personnel. This is why the problem solved by this research is relevant in real life. While writing this thesis, there was no publicly available cyber incident documenting exercise that allows single persons to evaluate and improve their technical cyber incident reporting skills individually. There are numerous mostly on-site group exercises with cyber incident reporting implemented in them [3]. This thesis proposes a concept solution. A cyber-incident reporting exercise with low resource requirements, for technical persons individually. The goal of the created exercise is to evaluate and improve the cyber incident reporting skills of individual persons responsible for company IT technical side of security.

In short, the main problems addressed in this thesis are the following:

- Lack of cyber incident reporting training to exercise technical persons individually;
    - Available exercises are for large groups and on-site;
- Lack of methods to assess the value of cyber incident reports;

1.2 Related work and limitations

Incident handling and reporting is a major aspect of cyber security. Every year with the growth of organizations and the increase of cyber-attack complexity, collaboration becomes more important. As explained by NIST (National Institute of Standards and Technology),

collaboration within teams or between organizations could be done by many ways [4]. From thesis authors' cyber incident reporting experience, one of the customary cyber incident cooperation is done via incident reporting. In case of an incident, teams collect bits and pieces of information to understand the nature of the incident. It is a common knowledge in cyber security field that information is only useful if it is relevant and received in a timely manner [5]. Sadly, quite often created incident reports must be fully reconstructed based on the addressee' report form – this is both time-consuming and prone to error.

Thesis research started regarding the methods of how to improve documenting and incident reporting skills for technically advanced people individually. Research introduced many requirements. For example, the training should be very practical and must have a very real-life like story to keep people fully engaged [6]. Research also discovered that most of the already created incident reporting training exercises, in a form of Cyber Defense Exercises (CDX's) are on-site and meant for a larger group of people [3]. It was also ascertained that these CDX's have been proven very successful at educating as well as keeping participants entertained. Research discovered no evidence of any online cyber incident reporting exercises meant for individuals.

Among others, research included several papers that analyze the thesis subject. Some of the material from recent years include for example, analysis of evaluation methods for human aspects[7], developing evaluation method for e-learning that considers different psychological aspects [8] and methods for generating network traffic for exercises [9]. Research also included methods of hiding something in legitimate network traffic [9] as well as material about the challenges of incident reporting and different security reporting schemes [10]. Research includes scoring systems for cyber vulnerabilities [11][12], and numerical comprehensiveness scoring systems for scoring reports [13] and evaluating risk severity and incident priority [14]. Research identified no scoring systems for scoring the complete value of cyber incident reports.

Subject missing from literature is an online single person cyber incident reporting exercise. Many world-leading InfoSec companies' offer many guidelines and methods to improve organization' computer security incident handling, but there is evidently no online incident reporting training for individuals. The following are some of the world-leading companies that have produced excellent ground-materials for incident reporting: NIST [4], SANS institute (U.S. information security and cybersecurity training, private company) [15], IEEE-SA (Institute of Electrical and Electronics Engineers Standards Association) [16], ENISA (European Union Agency for Network and Information Security) [17] and CERT's (Computer Emergency Response Teams) [18]. The latest well appreciated incident reporting material (up to the writing of this thesis) was produced by ENISA on the first of March 2017. It is called "Incident reporting framework for eIDAS Article 19" and it focuses on implementing incident reporting [19].

One limitation introduced is the absence of a universally agreed standard cyber incident report form. One reason for this could be the distinct role that the reports are supposed to fulfill for different parties, meaning that what is suitable for one person, institution or part of business might not be so for another. For example, reports that contains very specific technical data necessary during the incident resolving is not suitable for management, based on what to make managerial decisions. Incident reporting also produces challenges like reporting timelines and levels of collection management – different levels introduce different challenges [20].

This study is also limited by the method of how to determine if the training exercise for this thesis has improved user's incident management skills and whether it was improved by the incident reporting training or some other unconsidered factor. For example, doing the same online exercise with the same storyline and same correct answers for the second time will surely yield a better result but not because of completing this kind of an exercise.

Another limitation for such an exercise is time. How to create an exercise to keep the students' attention and interest to provide meaningful input with a reasonable amount of time. Limitation in the context of this thesis is mainly human attention span and the ability to stay focused [21]. Also, if some form of extra time-consuming activities is involved in the exercise then what affect does it have on the outcome of the exercise?

1.3 Thesis main goal and contribution of the author

The main goal of this thesis is to propose and create a low-cost method to evaluate and improve technical specialist's cyber incident documenting skills individually. The goal is achieved by creating an online cyber security exercise with the students' objective of completing a cyber-incident report form during the exercise.

For empirically validating the achieving of main goal, thesis proposes a novel method to evaluate cyber incident reports. Thus, creating a solution to distinguish good cyber incident reports from appalling ones based on experts' opinion.

Also, one possible standard cyber incident report template is proposed. The student solving the incident will be completing this form during the lab. Evaluating whether the students' cyber incident reporting skills have improved after the exercise is done by using pre- and post-questionnaires explained in detail further in thesis. The student completing the lab exercise is provided automatic feedback for the cyber incident report that he is completing during the exercise. This evaluation method makes the exercise more scalable than human-evaluated exercises.

Thesis scope and objectives are the following:

1. Conducting literature research - identifying what already exists and what is missing in research area;
2. Identifying the requirements;
3. Designing the exercise storyline;
4. Proposing an incident report form;
5. Designing the evaluation reports;
6. Creating the online incident reporting exercise lab unit;
7. Producing incident data for the student to analyze;
8. Conducting expert interviews and creating the exercise value validation system;
9. Producing the students' cyber incident reports' scoring system;
10. Exercise implementation – initial testing, final evaluation;
11. Analyzing produced data;
12. Concluding the thesis;
13. Proposing future research;

1.4 Outline of the Thesis

The goal of this thesis is to produce a low-cost, method to evaluate and improve the cyber incident reporting skills for technical persons individually. The research outline is the following:

1. Chapter 1 introduces the topic and research problem, also describes related works and limitations. As well as provides the thesis outline, main objectives and the contribution of the author.
2. Chapter 2 presents the methodology used for thesis' exercise.
3. Chapter 3 is about design and development. This chapter describes the requirements for the solution. Chapter explains the exercise motives and analyses the proposed storylines as well as proposes one cyber-incident report template. Chapter also consists the process description of creating the incident reporting exercise lab environment, individual students' lab unit; and the exercise evaluation methods.
4. Chapter 4 is about implementation. The chapter consists of the description and steps of the implementation processes. This chapter describes the process and steps of the initial evaluation, as well as provides the students' self-evaluation results and a brief analysis of students' feedback, as well as exercise statistics.
5. Chapter 5 presents the analysis of students' self-evaluation and the result analysis for the thesis validation system.
6. Chapter 6 describes the contribution of the author and proposes future works.
7. Chapter 7 concludes the thesis.

This chapter introduced the research topic, problem statement and limitations. Thesis main goal was described, authors' contribution and the research outline was produced. Next chapter provides detailed description of the used methodology.

2 Methodology

The previous chapter introduced the research problem, the hypothesis and described the limitations. Chapter defined the thesis' main goal and contribution of the author. This chapter provides an analysis of frameworks and detailed description of used framework.

A learning design process must be used for learning material to meet the expected objectives. There are many well-known methods for designing e-learning material [22]. Some of the more known is the traditional ADDIE model and Bloom's Taxonomy; a more elastic methodology is Agile – used mainly in the software development industry but also has many merits. Also, TPACK, NSW Quality Teaching model and inquiry-based learning etc.

ADDIE Instructional Design method was used for this thesis. This model is suitable because the framework is for designing and developing educational- and training programs. Also, worth noting that it has been around for a long time and has proved to be easily implementable. By design, Agile method has many benefits compared to ADDIE, such as the incremental approach and frequent testing, and it is great for collaboration. Regardless, for the final product created in this thesis, ADDIE can be implemented by conducting sufficient tests as well, and collaboration is not a priority for this thesis. It is also significant that the author has previous experience with similar process modelling practices that ADDIE introduces – therefore simplifying the thesis exercise system development. ADDIE method was analyzed and implemented throughout the thesis creation with emphasis on details of every step. [23]

ADDIE stands for Analyze, Design, Develop, Implement and Evaluate. [23] This sequence, however, does not impose a strict linear progression through the steps as shown in *Figure 1*. Educators, instructional designers and training developers find this approach very useful because having stages clearly defined facilitates implementation of effective training tools. ADDIE was originally developed for the U.S. Army and later implemented across all branches of U.S. Armed Forces. As an ID model, Addie Model has found wide acceptance and use. [23]

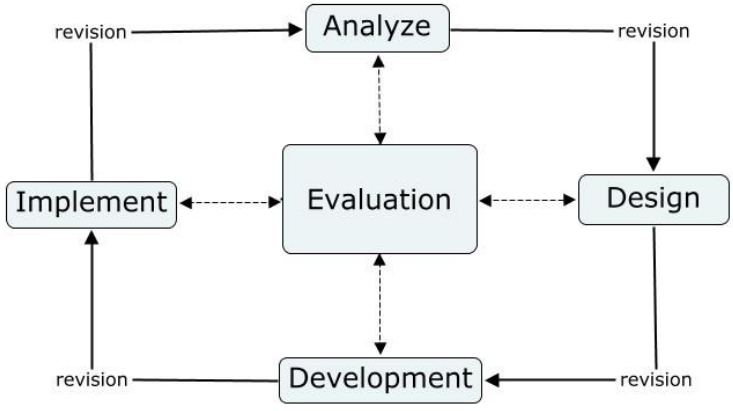


Figure 1. ADDIE learning process model [14].

For achieving the goal of this thesis, the steps that are analyzed within the ADDIE model include:

1. **Analysis**, which focuses the designer on the target audience to make the program match their skill and intelligence. Also, to distinguish what the students already know and what they should know after completing the program. [23]

2. **Design**, which determines all goals, tools to be used to gauge performance, various tests, subject matter analysis, planning and resources. The focus is on learning objectives, content, subject matter analysis, exercise, lesson planning, media selection and assessment instruments used. Being detail oriented is crucial to the success of the design stage. [23]

3. **Development** stage starts the production and testing of the methodology being used in the project. In this stage, designers make use of the data collected from the two previous stages, and use this information to create a program that will relay what needs to be taught to participants. If the two previous stages required planning and brainstorming, the Development stage is all about putting it into action. This phase includes three tasks, namely drafting, production and evaluation. Development involves creating and testing of learning outcomes. [23]

4. The **implementation** stage reflects the continuous modification of the program to make sure maximum efficiency and positive results are obtained. This is the phase to redesign, update, and edit the course to ensure that it can be delivered effectively. Students and content creators work hand in hand to train on new tools, so that the design can be continuously evaluated for further improvement. Since this stage gains much feedback both from content creators and participants alike, much can be learned and addressed. Developers should consistently analyze, redesign and enhance the product to ensure effective product delivery. Meticulous monitoring is a must. Proper evaluation of the product, course or program, with necessary and timely revisions, is done in this phase. When instructors and learners actively contribute during the implementation process, instantaneous modifications can be made to the project, thus making the program more effective and successful. [23]

5. **Evaluation**, which is the last stage of the ADDIE method. This is the stage in which the project is being subjected to meticulous final testing regarding the what, how, why, when of the things that were accomplished (or not accomplished) of the entire project. This phase can be broken down into two parts: Formative and Summative. The initial evaluation happens during the development stage. The Formative phase happens while students and IDs are conducting the study, while the Summative portion occurs at the end of the program. The main goal of the evaluation stage is to determine if the goals have been met, and to establish what will be required moving forward to further the efficiency and success rate of the project. Every stage of the ADDIE process involves formative evaluation. This is a multidimensional—and essential—component of the ADDIE process. [23]

This chapter introduced the framework that was used for thesis creation process. Chapter provided important details for the framework that was ground material for the thesis creation. Next chapter describes the process of design and development, introduces thesis requirements, as well as the lab exercise storyline analysis and design. Next section also proposes one possible cyber incident report template, and describes developing the solution. Next chapter also describes the processes of creating exercise lab environment; students'

lab unit; how the thesis evaluation reports were generated; and describes the exercise lab evaluation method as well as the exercise questions and answers.

3 Design and development

Previous chapter introduced the used ADDIE modelling framework. This chapter describes the process of thesis design and development, the research requirements, and the lab exercise storyline analysis and design. Paragraph also proposes one possible cyber incident report form and describes developing the solution, including the exercise lab environment; students' lab unit; process of generating the thesis evaluation reports; as well as describes the used exercise lab evaluation methods and concludes with questions and answers section.

3.1 Requirements

The incident reporting exercise has many requirements. Many of which are based on suggestions provided by the organizations/institutions discussed earlier in the thesis, regarding incident reporting procedures for enterprises (see chapter 1.2 for more info). These procedures are excellent guidelines for creating the exercise environment.

3.1.1 Requirements for the location of the exercise environment

The exercise lab system must be accessible from anywhere to remove or reduce the cost of all travel and accommodation bookings. Also, the exercise system must be accessible online to highly reduce the cost of hardware from the student's perspective.

These requirements are achievable because of the individual nature of the exercise. The requirement would be met with a system that provides the ability to create, recreate and restart the exact same individual lab environment. The online nature of the exercise lab introduces an important requirement which is network performance. The lab system should be accessible with a network speed of at least 5 Mb/s. The requirements are more thoroughly explained in chapter 3.6, regarding the exercise environment.

3.1.2 Requirements for the evaluation of the exercise lab

The lab system must be scalable to service many people simultaneously solving the exercise. This could be achieved with automatic evaluation. Some of the automation using the Rangeforce exercise lab environment system could be done with the use of multiple choice- or value retrieval methods. The first one means that the student is given a list of choices to choose all the correct answers from. Value retrieval method means that the student's input is evaluated correct upon filling the form with one of the predefined values from a previously defined list. This list of correct values is unseen by the student.

The biggest section of the incident report is usually the summary of the incident (see *chapter* 3.4 for more info on the incident report form). One of the major part of summary is the description and chronology of incident events. Automating the evaluation of these sections that are highly dependent on the student is the most difficult task. This is due to the different nature of how people perceive information. The students input could be influenced by many things such as culture, ethnicity, sex, background and skills etc. Every human being thinks and acts differently and therefore fills the incident form unlike the others.

There are many automatic evaluation methods usable for these sections but they are usually either extremely time consuming or require a massive set of data. One of those is to simplify the evaluating by giving the student a precise illustration of how this part of the form must be filled. There is currently no standard information input style for cyber incident report forms. There is also no correct (or incorrect) structure how incident report summary section

should be filled (see chapter 1.2 and 3.4 for more info). Proposing a standard structure for information in each section of the incident form would simplify the automation but would still require massive set of data and good analytics for every section of the report. Creating or proposing the default structure for these cyber incident report sections is not in this thesis' scope.

3.1.3 Requirements for the evaluation of the value of the exercise

There are many challenges and opportunities in evaluating learning in serious games and online exercises. One of the problems of evaluating this kind of exercises is to ascertain that the students' skills have improved using the technology alone. This major aspect is analyzed by S. A. Petersen et al. in the research paper: *Challenges and Opportunities in Evaluating Learning in Serious Games: A Look at Behavioral Aspects.*[24]

Another major issue is that most technologies to support learning are detached from the real world working environment and therefore the chances that, what has been learned, is transferred to the working environment may vary. In general, the validation of automated competence assessments might allow a wide range of different external criteria, such as standardized questionnaires, self-assessments by the learner, future grades at university courses etc. [24]

Some of the challenges and opportunities are also more thoroughly discussed by Sobah A. Petersen et al. in their research paper: *Challenges and Opportunities in Evaluating Learning in Serious Games: A Look at Behavioral Aspects*. These are more thoroughly discussed on research page 220 and in thesis *chapter 3.6.5*.

3.2 Motives for exercise lab storylines

Choosing the storyline for the exercise lab was probably one of the more important aspects because amongst other things it dictates the audience that the exercise is directed to [25]. Numerous exercise lab scenarios were produced for the thesis based on professional scenario building. Some of the proposed stories have a historical background while others a more futuristic one. There were three main motives kept in mind in each of the proposed settings.

First and foremost, the artefacts in the lab machines must be unquestionable. Meaning that the student should not be misled at any point of the lab. Second, to maximize the value gained from these exercises it is important for the exercises or serious games (along with their storylines) to be as realistic as possible. This is discussed further by Minhua Ma et al. in their paper "Serious Games Development and Applications" on page 60 chapter 2 (Personalization in Serious Games) [26]. Finally, the story should be appealing to as many students as possible.

In all the proposed scenarios, (*chapter 3.3*) the main task for the students to complete a cyber-incident report form with incident data. The stories were created by thesis author based on information from OWASP (The Open Web Application Security Project) [27] top 10 lists of risks regarding different computer related security aspects. After every 3 to 5 years OWASP has been providing top 10 lists of computer related risks. Many list items are related to data protection. Since 2013, data protection in OWASP top 10 is a separate category and its priority is further increased. The list of OWASP top 10 for 2010 in comparison to OWASP top 10 2013 can be seen on *Table 1.*

Table 1. OWASP Top 10 2010/2013 [17].

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

OWASP top 10 – 2017 compared to 2013, Sensitive Data Exposure has been moved from rank A6 to A3 (see *Table 2*).

Table 2. OWASP Top 10 2013/2017 [17].

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

One of the more significant project from OWASP regarding privacy and data security is "Top 10 Privacy Risks". This project was started in February 2014 and the first "Top 10 Privacy Risks v1.0" was published in September the same year [27]. Almost year and a half later, April 2016, OWASP also published "Countermeasures v1.0" [27]. OWASP has been constantly directing peoples' attention towards privacy and data protection for a long time. OWASP' recent work culminated in May 2016 with the entry of force for GDPR (General

Data Protection Regulation) [2]. The latter being one of the main reasoning for the exercise lab storylines.

GDPR could be considered one of the biggest changes for personal information in cyber domain for European Union and arguably in the World for 21'st century. From 1995 until now personal data protection in the EU (European Union) has been regulated by the Data Protection Directive (95/46/EC) but the massive changes for technology and personal data availability have rendered the directive hopelessly out of date. InfoSec has been in need for a large-scale reform for quite some time. This directive has finally been superseded by the GDPR, approved by the EU Parliament in April 2016 and enforced 2 years later – 25th May 2018 [2].

The aim of GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established [2]. After four years of preparation and debate the GDPR was approved by the EU Parliament on 14 April 2016 [2]. The regulation entered force in May 2016 and is followed by a 2 year post-adoption grace period [2]. Unlike a Directive it does not require any enabling legislation to be passed by government; meaning it will be in force May 2018 [2].

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals" [2]. This must be done within 72 hours of first having become aware of the breach [2]. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach [2].

Personal data means any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person [2]. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address [2].

GDPR introduces many new roles, one of them being the Data Protection Officer (DPO). The role of DPO is to ensure that the European Commission correctly applies the law protecting individuals' personal data and to keep a register of processing operations on personal data by Commission departments [20]. Also, to investigate data-protection matters and to cooperate with the European Data Protection Supervisor [20].

Failure to comply with the GDPR means that organizations can be fined up to 4% of annual global turnover or €20 Million. This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement. [2]

Had this (information security) InfoSec regulation been in force already it could have been catastrophic for many companies still operating today. For example, the Yahoo data leak incident in 2013, regarding possibly up to 3 billion hacked accounts. This is one of many arguments that emphasize the great need for advanced cyber incident handling procedures and -skills.

To sum the discussed motives: the artefacts in the lab machines should be unquestionable. The storyline must be realistic, recognizable by the student, and should be appealing to as many students as possible. The story is built upon an OWASP top 10 list item and more importantly, based around the GDPR.

3.3 Designing the storyline

Exercise storylines were composed to be as appealing to as many students as possible while also directing people's attention towards the GDPR. The initial idea was to create the lab virtual machines with Windows operating systems because Windows OS has over 88% of market share. Creating the lab virtual machines on Windows OS was initially ruled out due to licensing issues [28]. Instead the network traffic used during exercise lab was created in a standalone Windows workstation imitating the actions of a Windows OS user. The produced traffic was copied to the lab Linux virtual machines for the student to analyze.

The online exercise lab is built so that there is an individual lab environment for every student simultaneously solving the exercise. Every lab instance is created with separate virtual machines and therefore with separate operating systems (OS) (lab setup in *chapter 3.6*). To avoid licensing issues, the exercise lab environment itself was built upon UNIX systems but the traffic created on a Windows workstation. The following are three of the thesis authors' proposed storylines out of which one final choice was made.

- In the first storyline the attacker has gained access to the company back-end server database that was supposed to be well protected and behind a firewall. The back-end database was accessed through the front-end web application by an SQL injection. The hacker has stolen many company employee personal information including names, e-mail addresses and identification numbers. During the couple of months after the attack the employees have been getting an enormous number of fake e-mails from Indian e-mail domains. The e-mails claim to be from Gmail and PayPal and request that the account owner should immediately access the provided link to change their password. The Student is provided access to the front-end and back-end server and should access the logs to identify how the attacker gained access to the data.

- The attacker in the second scenario is the company's system administrator that was let go months ago to cut personnel costs. The resentful administrator had had access to all the company data and had exfiltrated and made public many of the employee's secret personal data. The administrator had previously signed a NDA (non-disclosure agreement) with the company and has therefore broken it. Now the company wants the administrator to take full responsibility for his actions. The company hopes to ease the GDPR related fine by putting much of the blame on the administrator. Now they need students' expertise to get viable evidence to support it. Student is provided access to only some of the administrator computer network logs. The student is provided a workstation that contains the logs and a log analysis tool called Wireshark.

- In the third scenario attacker has gained access to the company workstation and had escalated his privileges. The hacker gained access either due to an unpatched operating system, or an unpatched software residing on the computer. The attacker had moved from the workstation to the company servers and had been able successfully

extract highly personal employee information and had encrypted most of the company data. The attacker left behind files where he demands the company to pay a huge sum of crypto currency to have their data recovered. Unfortunately, the company does not have any form of backup. The CIO of the company is unwilling to pay the ransom and hopes that the student identifies who is behind this incident. In this case the student is provided a computer with certain traces of information. In this scenario, the Student is thought to put more emphasis on the incident report sections: possible cause, possible solution, recommendations for avoiding the incident in future (see *chapter 3.6.3* for more info on incident report form sections).

Selecting the final storyline from the proposed three was based upon the requirements described in *chapter 3.2*. The second proposed scenario was chosen after discussions with field experts. Some of the thought process from expert reviews include the following. Although the first storyline is appealing and modern, setting up the scenario without tampering or leaving misleading evidence regarding the logs for back-end and front-end server database and firewall, is considered a task slightly too difficult;

The third scenario is also considered modern and real-life like but appealing for a narrower group of students than the second scenario due to data encryption. In addition, setting up this lab scenario would require more research. Also, access to some variant of crypto locker software for successful implementation. Encrypting the files in some other way is considered to leave misleading evidence. Setting up this scenario without tampering the evidence is considered more difficult and costlier on the hardware than the first and second scenario;

The second storyline regarding the resentful administrator is chosen over the others after expert discussions because it is considered modern and appealing for a considerable number of people compared to other proposed scenarios. Also, setting up this lab scheme leaves less room for errors and evidence tampering for example, due to having the smallest lab environment.

3.4 Cyber incident report form

Although research done for this thesis discovered some talks regarding a generally approved cyber incident report template being worked on, nothing of such exists today. Among numerous other incident management guides and guidelines (also described earlier), thesis research discovered an incident handlers' checklist from SANS and list of items that an issue "tracking system" should contain from NIST [15][4]. As well as countless templates and forms from Internet websites of many organizations like US-CERT, Internet Crime Complaint Center (IC3), Australian Cyber Security etc. [29]–[31].

All these guides, guidelines, and checklists are excellent material to analyze for future works when proposing or possibly conducting analysis for producing a, default incident report template. Although one of the thesis' initial goal was possibly producing a default template, it soon became clear that it requires a lot more work than initially anticipated. Therefore, conducting such research is left out of the scope of this thesis. This thesis will propose the cyber incident report form used by the Estonian Defense Forces' Cyber Incident Capability team. EDF-CIRC is one of two Estonian teams accredited (since 2016) by Trusted Introducer [32].

This proposed report form was initially produced by Estonian CERT and was adapted from being emergency based to being incident based. This report template is used for this thesis

because the report template has been used for years and has proved to be sufficient in detail while easy to understand and read. For this reason, this template and therefore, this cyber incident reporting exercise might also be applicable for other organizations. Report templates with similar fields are, among others, used by organizations described in the research. Template selection was also influenced by the context of this thesis – template should include sections and fields necessary for technical people to document their cyber incident related information. Many challenges not described in this thesis, regarding cyber incident report template selection, are discussed in more detail by C. Johnson at al. in the: "Failure in Safety-Critical Systems: A Handbook of Incident and Accident Reporting" [33]. The described report template is shown in thesis appendix II.

3.5 Designing the evaluation technique

The validation and therefore the incident reports that are used for validation, are a major part of this thesis. The process, regarding the evaluation reports and their actual value, involved the following activities explained further in thesis:

1. Research regarding existing validation systems
2. Research regarding cyber incident report forms
3. Analysis of publicly well-known real-life cyber incidents
4. Numerous on-site interviews with cyber incident reporting experts
5. Analysis of the data gathered during expert interviews
6. Numerous online back-and-forth information exchanges with field experts

The complete thesis validation is roughly divided into three sections:

- Creating the validation reports that the student will be evaluating before and after the exercise;
- Creating the expert method to evaluate the previously created reports;
- Testing the created evaluation method;

3.5.1 Additional research and designing the validation reports

Creating the validation process started with researching into world leading companies and organizations operating in this area, for example ENISA, NIST, US-CERT etc. Research included searches for default cyber incident report form – with the conclusion that currently there is no default cyber incident report template. The document most relevant to this topic is produced by ENISA on the first of March 2017 and is called "Incident reporting framework for eIDAS Article 19" [19]. It focuses on implementing incident reporting for national Telecom organization.

This computer incident framework is used in thesis for creating the research validation system, because it appears relevant and applicable for cyber incidents in general as well. Part of the research includes searches for major cyber incidents until the end of 2016. Two of the more significant incidents were chosen. These will be used based on what to create the validation reports.

- One of the incidents is the Yahoo data leak that happened back in 2013.
- The second incident is regarding the Mirai DDoS cyberattack, also known as Dyn DDoS attack that happened in October 2016.

The first incident was chosen because it already has more than 2 major updates regarding the scope of the information leak. It was also chosen as it involves sensitive customer data – which is one of the lab motives. The second real-life incident was chosen because of the

massive scale and impact that it had on many well-known companies like Amazon, CNN, and PayPal.

The validation incident reports were generated by the lab author. Reports were created by lab author because of years of cyber incident reporting experience. Total of 5 reports were generated, 3 to be evaluated before the exercise, and 2 to be evaluated after. The goal was to aim the reports' actual values between 3 to 9 points out of 10. These validation reports are based on the same report template and contain the exact same fields as does the students' lab exercise. The report template is further explained in *chapter 3.4*.

Each of these evaluation reports were created to reflect a different level of complexity and detail, hence have different actual values. The evaluation process, to score the value of each of the reports, includes cyber incident reporting experts. The chosen experts have different level of incident reporting experience and background as well as- nationality. Also, they work in different companies. Some experts currently work as cyber incident managers, some have been promoted to cyber incident report team (CIRT) managers and some have advanced to even higher positions. Some of these experts have more than 10 years of cyber incident reporting experience.

To simplify the design process, the generated reports are numbered from 1 to 5. The lab student has no knowledge of the reports actual values. During the lab, the student is asked to evaluate the reports before and after his own lab experience. These reports are available to the student during the lab from two places. The students' computers' desktop contains two folders named pre-lab and post-lab. Pre-lab folder contains 3 reports designed to be evaluated before the exercise and post-lab folder contains 2 pdf validation reports designed to be evaluated after the exercise.

3.5.2 Expert interviews and creating the validation system

On-site interviews with field experts were conducted to produce objectively evaluated validation cyber incident reports. Every expert interview result was very much different from the rest. The goal for on-site discussions was to produce a list of all the values/features that a good incident report should have in their opinion. During the discussions, previous experts' results were not displayed. The interview consisted of three parts:

- Producing a list of necessary incident report features;
- Ordering the list items from most important to least important;
- Scoring the list of features with the total bank of 10 points;

The reason for ordering by importance was to simplify the scoring process. The result of every interview was a unique list of cyber incident report features with values of importance. The duration of these initial interviews was approximately 1 hour.

Analysis of the results was conducted after 3 experts had produced their feature/score lists. It became clear that continuing with this method produces many complications later. The main problem was assembling all the experts' features to produce a usable expert evaluation method. The main issue was that every expert interview resulted in duplicate-, linked- or mixed features. For example, one experts' individual feature called "risk" meant for them, making conclusions about the effect that the incident has on current situation, with the goal of preventing these types of incidents in the future.

Table 3. First experts' incident report features.

Feature/quality	What to look for	Score	Notes
Affect	User(s)	0,5	
	Technology - devices, services	0,5	
	Internal incident/external - outside partners informed or included in resolution process	0,5	Need to inform?
Report clearance level	Internal, classified or higher rapport clearance	0,3	Traffic light protocol
Priority	How many users X how many devices	0,5	How many users x how many devices = priority. Currently happening has instant High priority.
Risk		1,0	Making conclusions about the effect that the incident has on current situation - How to prevent
Date and time		0,3	Due to internationality - Server in Latvia etc.
Evidence reliability	Was data: produced verbally; electronically; Signed by hand or digitally signed; data hashed	0,2	Data reliable?
Data (technical details in supplement)	Who was involved	0,8	Mart
	What happened?	0,8	Virus was found
	Where did it take place?	0,8	Mart' Laptop
	When did it take place?	0,8	Date/time
	Why did that happen?	0,8	User browsed the Web
User explanation		0,2	In short - what happened?
Recommendations for mitigation and prevention	Clearly understandable proposal	1,0	
	Proposal realistic	1,0	

For the second expert the feature "risk" was considered as identifying the asset included in the incident and was a sub-section of the Identifying process; and for the third expert, risk was not a separate feature but rather a collection of 3 to 4 different features. To clarify the complications the process introduced, a full list of 1-st and 2-nd experts' cyber incident report features are shown on *Table 3* and *Table 4* with the example of "risk".

Table 4. Second experts' incident report features.

	Feature	Score		Notes	Description
Equally important	Identify	2,0	How did it happen? (Kill chain)	Description, what happened, what tool produced info	**(Produces criticality - Order of solving aka 2am, next steps are decided)** This is the step where you determine if an incident has occurred. Based on events observation, indicators, you look for deviations from normal operations.
		0,4	When did it happen? (Begin, duration, end)		
		0,8	With whom/who? (Victim)		
		0,8	Related risk (related asset) scope	Related business asset	
		1,0	Related business risk	Analysis - how affects the enterprise	
	Contain	1,8			The third stage of responding to incidents. It consists of limiting the damage. Steps to respond in case of incidents - password changes, remote wipes etc.
	Eradicate	1,8			After successfully contained the incident. The next step entails removing the cause of the incident.
	Recovery	0,3			It's where you return to normal operational status.
	Lessons learned	0,3			Follow up activity is crucial. It's where you can reflect and document what happened.
	Responsible (Dealing with incident resolution)	0,5			
	Who or what reported (user, system)	0,3			

To solve this matter, the next step involved analyzing the eIDAS Article 19 incident reporting framework. The possible solution is to produce a list of predefined categories and subcategories for cyber incidents using this framework. All the telecom related features were removed or modified, and previously produced cyber incident features were implemented into the eIDAS Article 19 framework categories and subcategories. The final list of categories and sub-categories can be seen on *Table 5*. Migrating all the experts' produced data into the eIDAS Article 19 categories and sub-categories, was the result of numerous online and on-site expert discussions, using online content sharing platforms. The following columns are excluded from thesis in *Table 5*:

- Comments;
- Example;
- Example 2;
- Evaluating criteria in the incident report;

For all involved experts, the migration process meant re-evaluating between 2 to 5 of their previously introduced features that did not fit to any single category. The average scores for the features produced during migration and re-evaluation process are shown in *Table 5*. It is worth noting that the average score of other experts that already evaluated the reports, was displayed to the experts during the final re-evaluation.

The result of this complete feature scoring process is a list of 14 cyber incident report validation features with respective importance scores (shown in *Table 5*). Also, worth noting

that the average scores for features' importance will even out further when more experts are added to the sample.

Table 5. Migrated list of categories, sub-categories, descriptions and score.

ENISA			
Category	Subcategory	Description	Avg Score
Impact	Affected service(s) + assets + data	Which **services/assets/data** where affected	0,98
	Affected users	Total number of **affected users**	0,53
	Duration	**Date and time of incident.** **Length of time** (in hours) when there was **significant impact** on the operation of the services	0,25
	Importance	Incident priority	0,40
Cause	Root cause	**Who is the responsible user (victim). The event or factor that triggered the incident: (***Human errors, System failiures, Malicious actions, Third party failiures vs internal*)	0,60
	Subsequent cause	**What happened - kill chain.** Connections between indicators	1,08
		When. Timeline of actions	0,78
	Initial assets affected	**Asset(s) first affected** in the incident	0,85
Desc+ follow-up	Description	Evidence reliability. Facts and assumptions not mixed up	0,70
	Response actions (Actions taken by the CIRT to mitigate the impact of the incident)	What was the reason for the incident to happen - **why?**	0,68
		Other parties included in resolution process **If internal resources insufficient**. + Who is responsible for the incident resolution	1,08
	Post-actions (Actions taken by CIRT to reduce the likelihood or impact of similar incidents)	**Proposed methods to mitigate and prevent**: clearly understandable + adequate and sufficient + realistic	1,38
		Possible to make decisions based on Technical info. Information useful to plan resources for effective mitigation. Technical info usable for "sysadmins" etc.	0,90
	Lessons learned (measures which will be implemented in the long-term)	**By who or what was CIRT informed?**	0,30

Next step is to produce values for the created validation reports using the average scores produced earlier. This step also involved field experts with extensive cyber incident reporting background (some even more than 11 years). The process of producing scores for validation reports can be divided into the following activities:

- 2 different real-life cyber incidents were chosen based on what to create the reports;
- 5 validation cyber incident reports (with different flaws and level of detail) were generated based on chosen real-life incidents;
- Generating expert evaluations for produced validation features, for all 5 validation reports by involved experts;

The scoring of validation reports' features was done using values from 0 to 1 (0% to 100%) regarding how evident the corresponding feature was in the specific validation report.

An example of the first 5 validation features are shown in *Table 6* (gray column) with the average importance scores (in green). The scores displayed are calculated averages from all

experts' evaluations. The 5 right-hand columns (1-st column in red) represent the 5 validation reports' scores from one expert. The average report value for individual expert (1-st report column displayed in blue) is calculated with the following formula:

```
Reports' value = Sum of all (green x red lines)
```

Previous formula as it is displayed in MS Excel (see rows/columns in *Table 6*):

```
=ROUNDUP (SUMPRODUCT (R3:R16*($K$3: $K$16)); 1)
```

Example of first report value for 1'st expert (shown in Table 6):

Report value = **2.5 points** [blue] and is calculated as follows:

```
0,93 [green] x 0,3 [red] + 0,53 [green] x 0,1 [red] + 0,25 [green] x 0,2 [red]
+ … = 2,5 [blue]
```

Table 6. Validation system example (first 5 features).

Row letter->					K	R	S	T	U	V
Line nr:	ENISA					1-st	2-nd	3-rd	4-th	5-th
3	Category	Sub-category	Description	Evaluating completed incident report based on this being present	Avg Score	2,5	2,8	3,5	1,7	4,8
4	Impact	Affected service(s) + assets + data	Which **services/assets/data** were affected	Name/nr of affected services	0,93	0,3	0,3	0,5	0	0,7
5		Affected users	Total number of **affected users**	Number of affected users	0,53	0,1	0,1	0,2	0,5	0,7
6		Duration	**Date and time of incident. Length of time** (in hours) when there was **significant impact** on the operation of the services	Date and time of incident (duration)	0,25	0,2	0,5	0,5	0,1	0,2
7		Importance	Incident priority	Is there a written priority	0,40	0,5	0,5	0,5	0,5	0,5
8	Cause	Root cause	**Who is the responsible user (victim). The event or factor that triggered the incident: (*Human errors, System failiures, Malicious actions, Third party failiures vs internal*)**	Responsible user (victim) (Person that received e-mail with malware, What triggered the incident etc)	0,60	0,2	0,2	0,2	0,2	0,2

It is worth noting that the values, for validation reports, for first expert are between 1.7 and 4.8 which are lower than estimated during the validation report design process. The final

score for all validation reports is the average of all experts' average values. The final reports' scores are shown in *Table 7* (blue background).

Table 7. Incomplete list of experts' scores for validation reports.

Average validation report values (blue)					First expert					Second					Third					Fourth				
avg1	avg2	avg3	avg4	avg5	1A	2A	3A	4A	5A	1B	2B	3B	4B	5B	1C	2C	3C	4C	5C	1D	2D	3D	4D	5D
2.9	**4.8**	**5.5**	**2.1**	**5.2**	**2.5**	**2.8**	**3.5**	**1.7**	**4.8**	**4.0**	**6.4**	**8.6**	**3.7**	**7.6**	**2.7**	**4.7**	**6.0**	**0.8**	**3.3**	**2.4**	**5.4**	**3.9**	**2.0**	**5.1**
0.25	0.25	0.63	0.12	0.78	0.3	0.3	0.5	0	0.7	0.3	0.4	1	0.2	1	0	0	0.5	0	0.9	0.4	0.3	0.6	0	0.5
0.20	0.13	0.63	0.67	0.78	0.1	0.1	0.2	0.5	0.7	0	0.4	1	1	1	0.5	0	1	0.5	0.9	0.1	0.1	0.1	0.6	0.6
0.08	0.82	0.77	0.07	0.67	0.2	0.5	0.5	0.1	0.2	0	1	1	0	1	0	1	1	0	1	0.1	0.8	0.6	0.1	0.3
0.92	0.92	0.92	0.92	0.92	0.5	0.5	0.5	0.5	0.5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0.50	0.62	0.58	0.03	0.43	0.2	0.2	0.2	0.2	0.2	0.5	1	1	0	0.8	1	1	1	0	0.5	0.3	0.5	0.3	0	0
0.13	0.68	0.72	0.10	0.30	0.1	0.1	0.3	0.1	0.4	0.4	1	1	0.2	0.6	0	1	1	0	0	0.1	0.4	0.4	0.1	0.3
0.47	0.90	0.87	0.13	0.48	0.4	0.6	0.6	0.1	0.3	0.8	1	1	0.1	1	0.5	1	1	0.1	0.1	0.1	1	0.8	0.2	0.4
0.05	0.57	0.62	0.10	0.43	0.2	0.2	0.4	0.3	0.5	0	1	1	0	0	0	0.5	0.8	0	0.8	0.1	0.6	0.1	0.3	0.5
0.18	0.38	0.47	0.10	0.58	0.3	0.3	0.3	0.2	0.5	0	0.3	0.6	0	1	0	0.3	0.3	0	0.3	0.5	0.7	0.5	0.2	0.6
0.55	0.58	0.58	0.52	0.72	0.2	0.2	0.3	0.2	0.6	1	1	1	1	1	0.5	0.5	0.5	0	0	0.4	0.7	0.4	0.6	1
0.03	0.03	0.05	0.02	0.03	0.2	0.2	0.2	0.1	0.2	0	0	0	0	0	0	0	0	0	0	0	0	0.1	0	0
0.45	0.53	0.55	0.10	0.53	0.4	0.4	0.4	0.1	0.7	0.6	0.4	0.8	0.5	1	0.5	0.5	0.5	0	0	0.3	0.8	0.5	0	0.8
0.15	0.28	0.20	0.32	0.58	0.1	0.2	0.2	0.1	0.5	0.5	0.5	1	1	1	0	0	0	0	0	0	0.4	0	0.2	0.7
0	0	0.10	0	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0	0	0	0	0	0	0

As shown in *Table 7*, experts scored the validation reports lower, than the author initially anticipated. Author aimed report scores between 3 to 9 points. Experts' average scores for validation reports were between 2.9 to 5.5 (out of 10 total). The second expert was the most optimistic (visible on *Table 7*), scoring closest to the authors anticipated values. One reason for these results could be that the reports were generated before designing the evaluation features system. Thus, creating the validation reports before creating the validation system (including the features) effected the reports' actual values, as scored by experts.

It is worth noting that research final results depend much on the experts used to create the evaluation system, as well as the number of students used to test the validation system. The results from lab final execution are displayed in *chapter 4.2*. The full list of 6 experts' scores is visible in thesis appendix.

3.6 Developing the exercise lab

The exercise, its storyline and objective created for this thesis was mostly done by keeping in mind the GDPR. One aim of the exercise and its storyline is to direct people's attention to the GDPR and to demonstrate what the lack of compliance to the GDPR could mean for a business.

The exercise was created to an online exercise test environment already set up by a company called Rangeforce. Rangeforce helps IT administrators and developers learn cyber defense by training with threats in a cloud based Cyber Simulator. The platform is meant for everyone who is interested in developing their professional skills in cyber security and IT field in general. Rangeforce differs from other learning platforms because it is a cloud based gamified learning space that is focused on real life hands-on practical learning experience. The

platform is a cloud based virtual environment and therefore accessible anywhere. The environment has real-life based scenarios with up-to-date practical hands-on materials crafted by various field professionals. Students' progress in exercises is monitored by user progress monitor that allows the student to compare his advancement with friends, co-workers and other learners in the system. Rangeforce system contains many exercises from different information technology areas with a variety of complexity, this allows the learner to customize their learning path and plan their career more freely. [34]

The system can be accessed by any computer that has a web browser and a Remote Desktop client installed and has a network connection a minimal of 5Mb/s to get the most out of the experience. Rangeforce offers a hands-on approach that provides real attacks, real defense and real learning for a serious training with serious attacks. The platform has engaging missions with scenario-based challenges that add a real-world dimension to labs. The system has its own safe, isolated network that simulates a real-life network. The attacks can be automated to imitate actual cyber-attacks and the system provides automated feedback through automated system checks. [34]

Each Rangeforce lab environment is different respective to the mission. Smaller labs may contain of a router that provides internet access and an isolated network for one workstation. Bigger labs for example may consist of many routers, servers, workstations and numerous isolated networks. Evaluation in Rangeforce platform is done by an automated bot that scans the information that the user provides. The evaluation is also possible by using remote automated scripts that scan for student actions in the lab machines. For the mission that was created for this thesis the evaluation bot evaluates the user inputs for an incident report form filled by the student during the lab. Some of the incident report fields will be manually graded, some automatically- hence the semiautomatic evaluation method. One example task for the exercise is to identify the name of a document, from within produced network logs that contains sensitive company employee data. This task is automatically evaluated by the evaluation bot and is marked completed when the user fills the incident form with the correct document's name.

3.6.1 Developing the online exercise lab environment and network traffic logs

This paragraph describes the necessary steps to create the exercise lab environment. Every individual lab setup is created when the student starts the lab. After the lab is started a personal set of lab machines with unique identifiers is created. The lab computers are created from template machines' latest snapshots that contain necessary configuration and artefacts. The average duration from the point of starting the lab until the user is presented the vTA (lab description) is roughly 1.5 minutes. The steps for creating the lab template is as follows:

1. Plan the lab environment - which computers, operating systems, vTA etc. is needed;
2. Start the new lab creation in vTA to acquire unique ID etc.
3. Create network template(s) for the virtual lab environment;
4. Create/import all necessary lab computers into the lab environment;
5. Create necessary network logs - pcap files;
6. Configure all previously created computers with necessary software, including Wireshark; artefacts, including pcap network logs, ssh key-pairs etc.
7. Configure the computer templates in virtual lab environment;
    a. Names;
    b. Select templates (from the list of previously created);
    c. Allow/deny remote connections;

    d. Set primary flag (remote connection started automatically);
    e. Set the network connections;
8. Create snapshots of created computers templates;
9. Configure the vTA with lab description, objectives, steps, question forms, correct inputs, evaluation methods, hints etc.
10. Create the users for students to access the lab environment;
11. Test the lab;

The lab environment in general contains of numerous labs. The student can choose from the list of labs that have been assigned to his user. The environment displays a brief description for every exercise. This brief lab description for the exercise in this thesis contains 96 words and is as follows:

Cyber incident reporting exercise

You are a Cyber Security specialist asked for help by a private company called Nano Labs.

Nano Labs has found themselves in a situation where many of their employee highly personal information has leaked to public media. Their CISO, John Smith, is certain that the personal documents were leaked by one of their former IT admin - Ned. Unfortunately, Nano Labs don't have any other evidence but some of Ned's work computer network traffic (PCAP files).

Your job is to complete a cyber incident report regarding this data leak incident.

Happy hunting!

Creating the network traffic logs.

As a part of cyber incident reporting lab, the student has 5 previously created network logs – pcap files, to analyze. These files were created in March and May of 2017 in a specifically created closed Windows environment to reduce the possibility of tampering evidence. From these network traffic files, the student must identify how the data was extracted from a factionary organization. The network analysis tool, Wireshark, is preinstalled on students' computer.

The network traffic files are situated on the computer's desktop for easy access. The data that the student should identify from the traffic is one single uploaded file containing a great number of employee personal data. This upload is masked by other everyday activities like watching YouTube videos, reading BBC news, browsing the Internet for pictures, downloading and uploading different files. The network traffic is divided into 5 pcap files of different size to make the exercise slightly more complicated and realistic.

3.6.2 Students' personal exercise lab unit

The exercise lab for each unique student is created from a pre-created snapshot of the exercise template. The template for this lab consists of an Ubuntu desktop computer that provides the student the necessary tools (Wireshark) and network logs (PCAP files) to analyze. The desktop computer is also used to fill an incident report on a web page using Chromium web browser. The lab also consists of a router computer that provides Internet connection to the desktop computer whilst also acting as the evaluation/feedback vTA (virtual Teaching Assistant) for that unique lab unit. Virtual Teaching Assistants (vTA) is used to describe lab tasks and assignments whilst also managing evaluating the user inputs against predefined

values. This is the initial place for the user to get confirmation if they have completed the required tasks as required. The exercise lab unit can be seen on *Figure 2*.

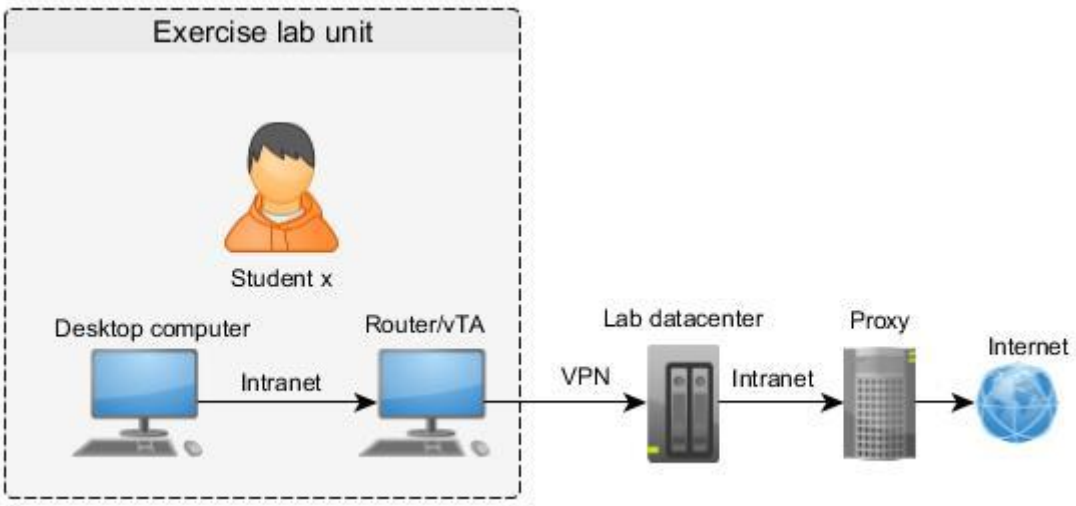


Figure 2. Students' exercise lab unit.

All lab computers are configured to start automatically with the lab. The student can restart either computer when necessary. This could be necessary upon technical issues with any of the lab computers. Current lab progress is saved in real time and is therefore purposely not reset with lab machines. The student has access to his lab computers via browser or via RDP connection from Windows, Mac or Linux computer. The RDP access for student is created with a unique password. Examples of Windows and Mac RDP command line connection strings:

```
Windows:
cmdkey /generic:labdev.itcollege.ee /user:localhost\aoras /pass:Iu-
fiHhPBS4054CNqNAI&&mstsc.exe /v:labdev.itcollege.ee:9002 /f

Mac:
open rdp://aoras:IufiHhPBS4054CNqNAI@labdev.itcollege.ee:9002
```

The student is provided more detailed lab description after starting the cyber incident reporting lab. The lab description includes all necessary information to complete the cyber incident report form. The description of the lab as it is displayed to the student at the start of the lab is as follows:

Cyber incident reporting exercise

You, Student, are a Cyber Security specialist asked for help by a private company called Nano Labs.

Nano Labs was unaware of the requirements of the General Data Protection Regulation (GDPR) that is in effect from May 2018. They had also taken no additional actions to ensure their employee personal information safety. Now Nano Labs has found themselves in a situation where many of their employee highly personal information has leaked to public media. Internally Nano Labs had found out about this incident months ago but had hoped that this wouldn't be publicly revealed.

Unfortunately, most of the employees whose personal data was made public have suffered financial losses, identity thefts or have been publicly discriminated. This has made their employees turn to legal authorities to have this matter sorted. Because of this cyber security incident, Nano Labs has been imposed an administrative fine for millions of euros.

Nano Labs CISO (John Smith, Phone NR: 555 012345) is certain that the sensitive info was leaked by Ned, one of their former IT admins that he was forced to cut loose to reduce IT personnel costs. John has made NDA's (non-disclosure agreements) with all his employees and is now hoping to reveal whoever is responsible for this incident to reduce at least some of GDPR induced fines. Nano Labs previous cyber incident nr was IR-0024.

You have been provided access to some of Ned's work computer network traffic to find out if Ned is the one that leaked the secret personal documents. You have also been provided an e-mail address "Student@nano.labs".

Nano Labs CISO has asked you to fill the incident report form with relevant information. The report template is produced by ENISA and is modified from being emergency incident based to being cyber incident based.

You can get a maximum of 100 points. Happy hunting!

Hint: Use the left-hand pane to move back-and-forth between questions.

3.6.3 Creating the students' cyber incident report form scoring

Maximizing learning impact and motivating students is done by real-time feedback for successfully completing lab items. Student is provided with an indication of correct, incorrect and partial answers, and score points towards lab completion. The complete hands-on exercise (completing the cyber incident report form) will award the student a total of 100 points. There are many ways to distribute these progress points, two of which are further analyzed.

First method to distribute the progress points is to provide the student with current lab progress. In this case the points are a rough estimate lab progress on a scale of 0 to 100. The downside is that this has no direct indication of the students' report value. The real value of the students' own report will be evident after his completed report has been manually graded by a group of experts after the lab.

The second method could be using the experts' average scores as maximum values for each exercise section. For example, let's assume that the experts proposed that indicating the

reports' critical level is worth 2 points. In this case if the student correctly indicates the reports' critical level then he is rewarded 2 points towards lab completion.

The major downside of this method is that the most points, based on conducted expert reviews, is given to "Incident Summary" section. More precisely "Description and chronology" sub-sections. These are mostly manually graded until there is enough data to support using machine learning. Therefore, using expert reviews for displaying students' feedback would diminish the goal of displaying any exercise progress to the student during the lab.

This is the main reason why the first described exercise scoring method will be used until there is enough data to support automating scoring majority of the students completed cyber incident report. During the lab the student will get the following progress feedback points. Rewarded progress points are in **bold** font after each incident report question. Section informational total is after each section in brackets. Total progress points for the whole lab exercise is 100.

- Pre-questionnaire **(Total for Pre-questionnaire: 6)**
    - Briefly describe your previous experience with incident reporting **2**
    - Please rate your confidence with incident reporting from 1 to 10 (10 being extremely confident) **2**
    - Please rate your confidence with pcap log analysis from 1 to 10 (10 being extremely confident) **2**
- Pre-Forms-(3 pieces) **(Total for Pre-Forms: 21)**
    - Pre- cyber Incident report forms
        - Pre - First cyber incident report form Score (1/3) **5**
        - Comments regarding 1'st report (voluntary) **2**
        - Pre - Second cyber incident report form Score (2/3) **5**
        - Comments regarding 2'nd report (voluntary) **2**
        - Pre - Third cyber incident report form Score (3/3) **5**
        - Comments regarding 3'rd report (voluntary) **2**
- Incident report basic info: **(Total for Incident report basic info: 10)**
    - Organization name **2**
    - Recipient name **2**
    - Recipient phone nr. **2**
    - Submitter name **2**
    - Submitter E-mail **2**
- Incident basic info: **(Total for Incident basic data: 10)**
    - Incident name & nr.
        - Incident name **2**
        - Incident nr. **2**
    - Incident effect, cause & critical level
        - Incident effect **2**
        - Incident cause **2**
        - Incident critical level **2**
- Incident summary: **(Total for Incident summary: 39)**
    - Incident occurred time **5**
    - Impact and influence **5**
    - Incident description - When, who, how, what **14**
    - Possible cause **5**
    - Possible solution **5**

    - Recommendations for avoiding the incident in future **5**
- Post-Forms (2 pieces) **(Total for Post-Forms: 14)**
    - Post- cyber incident report forms
        - Post - First cyber incident report form Score (1/2) **5**
        - Comments regarding 4th' report (voluntary) **2**
        - Post - Second cyber incident report form Score (2/2) **5**
        - Comments regarding 5th' report (voluntary) **2**

The points gained for every question is different based on the nature of the question. Some answers are initially manually graded until there is enough data to support the use of artificial intelligence and machine learning algorithms. Next paragraph contains the current evaluation methods used for every question currently in the lab exercise.

3.6.4 Exercise evaluation methods, questions, answers and lab objectives

This paragraph describes all the exercise lab questions, used evaluation methods and correct answers. As well as the objectives for the lab. The thought process for creating the questions and answers is explained in previous chapters. The use technical lab environment and vTA is produced by Rangeforce. The data produced and information created for this exercise is modifiable with medium effort. The first part consists of three self-evaluation questions:

- Pre-questionnaire
    - Briefly describe your previous experience with incident reporting
    - Please rate your confidence with incident reporting from 1 to 10 (10 being extremely confident)
    - Please rate your confidence with pcap log analysis from 1 to 10 (10 being extremely confident)

This paragraph is not a part of the proposed incident report form itself but is used to gain insight into the students' previous cyber incident reporting experience. This insight is useful for example to compare the complexity of the lab exercise and the time it took to complete the lab. The three questions in this paragraph give 2 points towards completing the lab exercise. Previous experience answer is marked complete when the student has filled the form with 5 to 500 characters. Confidence with incident reporting question is a multiple-choice question with 10 options from 1 to 10 and is evaluated complete when exactly 1 choice has been made. The next section is about estimating the actual value for previously created cyber incident report forms. There are also 3 voluntary comment sections, one for each report.

- Pre-Forms-(3 pieces)
    - Pre- cyber Incident report forms
        - Pre - First cyber incident report form' Score (1/3)
        - Comments regarding 1'st report (voluntary)
        - Pre - Second cyber incident report form' Score (2/3)
        - Comments regarding 2'nd report (voluntary)
        - Pre - Third cyber incident report form' Score (3/3)
        - Comments regarding 3'rd report (voluntary)

This paragraph is also not a part of the students' report form. This is one of the two questions of the thesis evaluation method. It contains 3 sub-questions that each represent one of the 3 previously created incident report forms. All three questions award 5 points toward lab progress. These reports are visible on the lab computers' desktop. The reports are also added to the vTA as a web link to Google Drive (as a backup location). These reports are more thoroughly explain in *chapter 3.1.3*. These questions are evaluated correct when the user input

is a number from 0 to 10 with a step of 0.1. For example: 5.4, 7.2, 9.2 etc. There is one comment field after every evaluation report question that awards 2 points toward lab completion. The next section is the beginning of the students' personal report form. It starts with the following 5 questions:

- Incident report basic info:
    - Organization name;
    - Recipient name;
    - Recipient phone nr.
    - Submitter name;
    - Submitter E-mail;

Every question provides 2 points towards completing the lab. These questions also contain real-time feedback. The checks for these types of questions are mostly done by simple string comparison. The correct answers for the questions can be seen in *Table 8*. All the data needed to complete these is given in lab description.

Table 8. Incident report basic info.

0 (2 points) **Organization name** the user needs to insert one of the following answers - Limited to 100 attempts Nano Labs
1 (2 points) **Recipient name** the user needs to insert one of the following answers - Limited to 100 attempts Nano Labs Nano Labs CISO John Smith
2 (2 points) **Recipient phone nr.** the user needs to insert one of the following answers - Limited to 100 attempts 555012345 555 012345
3 (2 points) **Submitter name** the user needs to insert one of the following answers - Limited to 100 attempts student
4 (2 points) **Submitter E-mail** the user needs to insert one of the following answers - Limited to 100 attempts student@nano.labs

- Incident basic info:
    - Incident name & nr.

        - Incident name;
        - Incident nr.
    - Incident effect, cause & critical level;
        - Incident effect;
        - Incident cause;
        - Incident critical level;

This paragraph is the second paragraph of the proposed incident report form. It contains two sub-paragraphs with 2 and 3 questions accordingly. The points and correct answers can be seen in *Table 9* and *Table 10* marked with green for multiple-choice questions. These questions award a total of 10 points. The necessary information to complete these is provided in the exercise description.

Table 9. Incident basic info - name and number.

0 (2 points) **Incident name** the user needs to check correct options in a multiple-choice question - Limited to 100 attempts Nano Labs data leak Nano labs data exfiltration Ned leaked data Secret documents leaked from Nano Labs Secret documents Secret data exfiltrated by Ned
1 (2 points) **Incident nr.** the user needs to insert one of the following answers - Limited to 100 attempts IR-0025

Table 10. Incident basic info - Incident effect, cause & critical level.

0 - (2 points) **Incident Effect** the user needs to check correct options in a multiple-choice question - Limited to 100 attempts Availability Integrity Confidentiality
1 - (2 points) **Incident cause** the user needs to check correct options in a multiple-choice question - Limited to 100 attempts Software Hardware Administration Attack User privileges Third party Lack of testing
2 - (2 points) **Incident critical level** the user needs to check correct options in a multiple-choice question - Limited to 100 attempts Low Medium High

- Incident summary:
    - Incident occurred time;
    - Impact and influence;
    - Description & chronology;
    - Possible cause;
    - Possible solution;
    - Recommendations for avoiding the incident in future;

Incident summary is the biggest section of the incident report form. Automating this paragraph needs a massive set of data and is therefore implemented in the future when there is enough data to support it. From this paragraph only the first question is automatically evaluated based on user input. The user must insert the correct date and time of the incident using a described time format. The incident occurred time for this lab exercise is identified from the network logs that are on the computers' desktop. The correct answer is the time for the sensitive file upload with the accuracy of 1 minute. The correct time rewards 5 points toward lab progress. The next questions are manually graded.

First manually scored question is *impact and influence* that rewards 5 points. *Description and chronology* is considered as one of the more important and thorough incident report

section and therefore rewards 14 points. *Possible cause*, *Possible solution* and *Recommendations for avoiding the incident (in future)* all reward 5 points. The whole paragraph awards 39 points (out of 100) towards lab completion. These questions are the end of the proposed cyber incident report form that the student completes.

Next paragraph is not part of the proposed report form but is the second part of the thesis evaluation method. The goal is to estimate the actual value for the 2 cyber incident report forms created for post-lab evaluation. Both questions award 5 points toward lab progress. These reports are available on the lab computers' desktop and are also added to the vTA as a web link to Google Drive (as a backup location). These reports are more thoroughly explained in chapters 3.5.2 and 3.6.5. These questions are evaluated correct when the users' input is a number from 0 to 10 with a step of 0.1, for example: 5.4 or 7.2. There is also one comment field after every evaluation report question that awards 2 points toward lab completion.

- Post-Forms (2 pieces)
    - Post- cyber incident report forms
        - Post - First cyber incident report form Score (1/2)
        - Comments regarding 4th' report (voluntary)
        - Post - Second cyber incident report form Score (2/2)
        - Comments regarding 5th' report (voluntary)

The described sections are part of the exercise lab objectives. The first questions' main purpose is to gain insight to students, the second and last paragraphs are for the exercise value evaluation. Other questions are part of the students' lab exercise.

To summarize, the exercise lab objectives for the student are as follows:

- Describe:
    - previous experience with incident reporting;
- Rate:
    - Confidence with incident reporting;
    - Confidence with pcap log analysis;
- Estimate:
    - The actual value of previously created cyber incident report forms;
- Select:
    - The name for the incident;
- Identify:
    - the name of the organization that the incident report is for;
    - the name and phone number of the persons that the report is composed for;
    - the name and phone number of the report submitter;
    - the e-mail address of the report submitter;
    - the unique identification number of the incident;
    - The impact and business influence of the incident;
- Categorize:
    - The effect of the incident;
    - The cause of the incident;
    - The critical level of the incident;
- Analyze and discover:
    - The time of the incident occurrence from network logs;
    - The cause for the incident;

- Explain:
    - The possible solutions for the incident;
    - The recommendations for avoiding these incidents in future;
- Identify and explain:
    - The description of the incident (when, who, how, what);

3.6.5 Exercise lab value evaluation

The evaluation method used in the thesis is based on research, as well as expert reviews and discussions. The implemented evaluation method is proposed by Petersen et al. [24]. Similar methods, challenges and potential limitations are also analyzed in *"Improving and measuring learning effectiveness at cyber defense exercises"* [35]. Also, challenges, introduced for measuring incident handling by different standards, practices and operating procedures. Research regarding the qualitative and quantitative measurement for pre- and post-game questionnaires is produced by Mayer et al. *"A brief methodology for researching and evaluating serious games and game-based learning"* [36]. For evaluating serious games and game-based learning the following general approaches are proposed:

- using validated pre-game and in-game questionnaires on relevant psychological constructs, including commitment to change;
- using pre-game and post-game questionnaires on learning satisfaction, game play and motivation in combination with maps and strategic decisions;
- using in-game logging and tracking of events and results in combination with questionnaires; [18]

The research papers also propose a couple methods to determine if learning is indeed facilitated by the technology and not by some other factor. A general approach that they recommend for evaluating learning is to conduct evaluations before and after the interventions with technology, as shown in *Figure 3.* The learners are tested for what they know before they start using the technology. Then the learners have a period of intervention where they use the technology or the learning environment and the subjects are finally tested after the intervention. This is a common approach in evaluations conducted in computer-assisted learning or other forms of technology-assisted learning such as Mobile and Ubiquitous learning. [24]

Figure 3. Evaluating Technology Enhanced Learning [24].

The pre-intervention evaluation may include learner profiling such as the technology literacy of the learner and their interests, tests based on the subject that the learner is intended to learn as well as interviews, questionnaires and supplementary behavioral observations to investigate the attitude and behavioral aspects of the learner. Similarly, the post-intervention component of the evaluations can include post-tests on the subject that the learner is intended to learn and interviews and questionnaires to establish if there has been a change in the learners' knowledge and skills, their attitudes and behavioral aspects. [24]

The pre- and post-intervention questionnaires for this exercise are previously filled cyber incident report forms. This evaluation method is considered more suitable for this exercise based on many merits. The main reasoning in favor of this method is that the exercise lab is considered to have direct impact on students' perception of the value of an incident report form. Therefore, using the pre- and post-questionnaire incident report method could be considered a more precise validation method while also arguably easier to implement and contextually interpret than such as learner self-assessments, tests on the subject or learner profiling [37][35].

The second reasoning in favor for this method is related to the duration of the exercise. This approach requires a rather small amount of time. This is important because of human attention span. Humans can be particularly engaged in a subject for 18 to 20 minutes, and after 45 minutes our attention or productivity drops greatly [21]. Also, humans tend to be hastier and less detail oriented when they are tired. In average this exercise lab is thought to be completed between 25 to 60 minutes depending on the student and his previous experience. Some people may be finished after 20 minutes while for others it could easily take 45 minutes or more, depending on numerous factors like previous experience. Duration is also affected by the approaches and the order of which the student is going to put them into practice. The major prolonging cause for this exercise is when the student has little- or no previous experience with network data analysis with tools like Wireshark or experience operating with UNIX based systems. In this case it will take the student more time to navigate the system and hence analyzing the artefacts. Artefacts for this exercise are previously created network logs (see *chapter 3.3* for more info on generating the network logs).
This exercise is divided into 3 logical separate tasks:

1. Firstly, the student will evaluate formerly filled incident report forms;
2. Secondly, the student will complete the exercise lab (analyzing the available information and network logs);
3. Thirdly, the student will evaluate a second subset of previously filled incident reports;

First task is presumed to take around 5-10 minutes, the exercise lab presumably 20 to 45 minutes and post-intervention around 5-10 minutes.

To sum up the evaluation method that will be used for this thesis is solved as follows. First the student will be presented with previously completed incident reports based on already happened real-life incidents. All the cyber incident reports are created unique – they reflect a different level of detail and -content. The student is asked to evaluate each of these reports. This evaluation is considered subjective but very dependent on the students' knowledge and perception of a cyber-incident reports' value. Then the student is graded based on how close he got to the actual value that these reports reflect based on expert reviews. After this the student will complete his own online cyber incident reporting exercise lab. Finally, after the exercise lab, the student will be grading the final set of previously created incident reports.

The hypothesis is that completing the online cyber incident reporting exercise will increase the students' skills to more precisely distinguish an exceptional incident report form from an appalling one. The students' cyber incident reporting skills are considered to have improved due of this exercise if after completing the exercise the student scores incident reports' values significantly closer to their actual value than he did before the exercise.

For example, let's assume that a student grades the value of a 7.5 report with a value of 4.5. In this case he is off by 3.0. Then the student completes the reporting exercise, after which he is again asked to grade previously created completed incident reports. The hypothesis is that the student has gained new incident reporting knowledge during the hands-on exercise. So, let's assume that because of completing this cyber incident reporting exercise, the student then grades the post-intervention report with an actual score of 5.0 with a value of 6.0. In this case he is off only by 1.0 points which is significantly closer to the reports actual value then student was before the exercise.

The reason why the students' documenting skills have improved after the exercise should be as indisputable as possible. Therefore, to make appropriate evaluations, the exercise should be in a controlled environment and repeatable under the same conditions. It is worth noting that with the current approach of 1 lab data set, including pcap files and evaluation incident reports, this lab is meant for a student to be solved once. The lab data set is further explained in *chapters 3.6.1, 3.6.2* and *3.6.4*. The exercise value requirements are explained in detail in *chapter 3.1.3*.

Chapter 3 describes the process of creating the proposed solution. First sub-chapter described the process of creating the online exercise lab environment; all the major steps that are needed to set up the lab environment with necessary artefacts, configuration-, vTA settings etc. Chapter also displays the brief lab description as it is displayed to the student in the labs environment. Chapter also describes the process of creating the evaluation incident reports and network traffic logs. Second sub-chapter described the student's personal lab unit, how to access it, and displays the lab full description as it is displayed during the cyber incident reporting lab. Next sub-chapter describes the scoring of students' cyber incident report forms and the process of rewarding student with points toward lab completion. Next section explains the evaluation methods for each of the lab task and question, and displays the correct answers for automatically evaluated tasks.

4 Implementation and evaluation

Previous chapter was about developing the solution. Regarding the requirements for the exercise medium; for the exercise evaluation method; and for the lab value evaluation system. Previous chapter also described the motives for the lab storyline and how the storyline design process. Chapter also proposes one possible default cyber incident report form. Chapter 3 ends with describing the process of solution development. That is developing the online exercise lab environment; student's personal lab unit; scoring the student's cyber incident report form; exercise evaluation methods; and exercise lab value evaluation.

This chapter is regarding the implementation and evaluating the created solution. This chapter starts with describing the processes and steps that were taken during the implementation phase. Also, the changes that were made during the initial evaluation. This chapter also describes the final evaluation run of the produced product. This chapter ends with feedback analysis and concludes with the evaluation of the validation system results.

4.1 Implementation and initial evaluation

For this exercise lab the implementation and evaluation loop was run many times due to the number of changes made to the lab throughout the creation process. Implementation was in fact one of the more time-consuming processes for this thesis. Initial tests were done by the lab author and after a minimum viable product [38] was produced, the lab was tested by chosen subjects (not the same selection as final evaluation). For the initial tests with subjects the think aloud method was used. During the lab, test subject was physically present and commented his every thought. The comments were afterwards analyzed and implemented. The identified flaws were corrected. The initial tests are not specifically documented in this thesis as they are mostly part of lab fine-tuning and many of the comments and errors were cosmetic. The lab implementation and initial evaluation process included:

- Reformulating part of lab name (from "Data Leak" to "Cyber incident");
- Reformulating the lab descriptions;
- Reconfiguring Lab settings;
    - Adding/removing the option to end the lab;
    - Adding/removing the option to managing machines one-by-one;
- Changing the lab setup;
    - Replacing the desktop computer;
    - Removing the server computer and implementing vTA functions to router computer;
    - Removing students' option to create RDP connection to router/vTA computer;
- Reformulating information provided by the vTA after starting the lab;
- Adding, removing, renaming the lab objectives, steps, instructions and web URL's in vTA;
- Reconfiguring the evaluation methods-, lists of vTA objectives, steps and correct answers;
- Revising the points that steps and objectives provide towards lab completion;

It is worth noting that the changes made to the vTA during the lab have no effect on the labs that are already in progress. New vTA configuration is loaded upon starting or restarting a lab. Next paragraph describes the final evaluation and students' feedback.

4.2 Final evaluation notes and students' exercise statistics

All students that were chosen for final lab exercise evaluation possess different information technology related backgrounds, cyber incident related experience, and network log analysis experience. The final evaluation run includes 9 persons that are employed in the following roles, for different organizations:

1. Programming and application security
2. Windows system administrator
3. Cyber incident response team member - antivirus systems (~1 year of experience)
4. Windows administrator and security specialist
5. Cyber incident response team member – log management (~2 years of experience)
6. VOIP (Voice Over Internet Protocol) systems administrator
7. Organizations IT support as well as administrator
8. IT support/administrator (5 years of experience)
9. Organization security specialist (6 years of experience as a former CIRT security events- and network data analyst)

The final evaluation run produced between 10 to 12 small comments and minor flaws that were analyzed and corrected as needed. Some of the minor changes made after the final run include the following:

- Minor reformulations to provide more clarity to the lab description and vTA objectives and steps;
- Added steps for voluntary comments regarding the evaluation of previously created incident reports to the vTA;
- Modified the minimum and maximum length for freestyle user text inputs (from 10-100 characters up to 1-500 characters);
- Changing the correct incident occurred time from UTC+3 to UTC and changing the step description to facilitate the change;
- Decreased the desktop computers' memory from 4GB to 3GB of RAM;

Analyzing and implementing students' comments and feedback was done for every participant. The feedback analysis process included questionnaires conducted before the lab exercise with the following three questions:

- Briefly describe your previous experience with incident reporting?
- Please rate your confidence with incident reporting from 1 to 10 (10 being extremely confident)
- Please rate your confidence with pcap log analysis from 1 to 10 (10 being extremely confident)

Students' comments were considered more thoroughly if the student already had previous incident reporting and/or network traffic analysis experience. When the student didn't have

any previous experience, but felt confident with incident reporting, then the suggestions were analyzed more critically. Regardless of the experience and confidence, most of the comments were implemented. Feedback or comments were provided by approximately half of the students. The following is an incomplete list of more significant feedback and overall exercise figures from final evaluation:

Exercise figures for first student:

- Reporting experience: 3
- Confidence: 6
- Log analysis experience: 0
- Lab duration 63 minutes
- Feedback score and notes: 4 (out of 5)
    - Before this lab exercise there should be some sort of a crash course on Wireshark or network traffic analysis;
    - The lab should provide a list of more common Wireshark features and filters;
    - GDPR should be implemented further into the exercise, it's currently too superficial;
    - There should be an extra field for comments regarding the validation reports (extra comment fields were promptly added);
    - Moving back-and-forth in the vTA is unclear (such instructions were promptly added to lab description);
    - PCAP filenames should be in timely order (change implemented);
    - The exercise was interesting; however, it was a bit unclear what needed to be done;
    - Reading network logs was difficult with no previous similar experience;

Exercise figures for second student:

- Reporting experience: 0
- Confidence: 4
- Log analysis experience: 2
- Lab duration (minutes): 45
- Feedback score and notes: none (out of 5)

Exercise figures for third student:

- Reporting experience: 4
- Confidence: 5
- Log analysis experience: 5
- Lab duration (minutes): 35
- Feedback score and notes: none (out of 5)

Exercise figures for fourth student:

- Reporting experience: 2
- Confidence: 3
- Log analysis experience: 3
- Lab duration (minutes): 50

- Feedback score and notes: none (out of 5)
    - No previous experience with Wireshark. Should have prepared for this.

Exercise figures for fifth student:

- Reporting experience: 7
- Confidence: 6
- Log analysis experience: 7
- Lab duration (minutes): 155 (notes: only person correctly answering the date/time question)
- Feedback score and notes: 3 (out of 5)
    - Time zone issues with lab

Exercise figures for sixth student:

- Reporting experience: 0
- Confidence: 5
- Log analysis experience: 2
- Lab duration (minutes): ~45 minutes
- Feedback score and notes: none (out of 5) (feedback was provided after the exercise)
    - Lab was very interesting, analyzing pcap files was catchy and created more interest to solve the incident;
    - Have previous experience with SIP network traffic analysis but not with this kind of things;
    - Lab setup was logical, tasks were interesting and required effort to find the correct answers
    - The lab completion process was not an obligation but personal interest;

Exercise figures for seventh student:

- Reporting experience: 0
- Confidence: 5
- Log analysis experience: 2
- Lab duration (minutes): 25-30
- Feedback score and notes: 4 (out of 5)

Exercise figures for eight' student:

- Reporting experience: 0
- Confidence: 4
- Log analysis experience: 4
- Lab duration (minutes): *unknown*
- Feedback score and notes: 4 (out of 5)

Exercise figures for ninth student:

- Reporting experience: 10
- Confidence:7
- Log analysis experience: 7

- Lab duration (minutes): *unknown*
- Feedback score and notes: none (out of 5)

During the few days following the lab experience, many students that participated in final evaluation, provided positive verbal feedback and extra remarks about the lab. Most of these remarks had, by that time, already been implemented – notes about the extra comment fields and minor misleading grammar, for example.

This paragraph provided insight to the background of students who participated in final evaluation and their questionnaire results; including their self-evaluations and feedback. The following paragraph provides analysis of produced data.

5 Analysis and results

Previous paragraph described the implementation and evaluation process as well as the background of sample students. The complete list of feedback, including scoring for self-evaluation, is also displayed in the previous section. This section includes analysis of the results for students' self-evaluations, and the exercise final run.

5.1 Students' self-evaluation analysis

The list of average lab duration and self-evaluation scores for students is displayed in *Table 11*.

Table 11. Students' feedback results.

Average lab duration in minutes		Average cyber incident reporting experience		Average level of confidence	Average network data analysis experience
With student nr 5	Without student nr 5	With unexperienced students	Without unexperienced students	5.0	3.6
60	44	2.9	5.2		

The average duration of 60 minutes, for the complete exercise lab, is within the expected duration as described in *chapter 3.6.5*. The average duration without student nr 5, is 44 minutes, which is well within the expected. The average duration was also provided without student nr 5 because his lab duration was 155 minutes. He is the only person who also correctly answered the question regarding the incident occurred date and time. The unusual lab duration was due to incorrect assumptions regarding the network traffic.

Average cyber incident reporting experience score based on students' self-evaluation is 2.9 (out of 10). The score is relatively low considering the background of sample subjects (see paragraph 4.2 for students' experience). Average students' experience score, without 4 sample students that scored their cyber incident reporting experience with 0, is 5.2.

The average self-evaluated confidence level for the sample students is 5.0. The lowest confidence level is introduced by the *Windows administrator and security specialist*. The most confident student is a security specialist with over 6 years of previous incident reporting expertise. The same student also displayed maximum incident management experience, and introduced the highest network log analysis experience score of 7 (out of 10). The average network data analysis experience score was 3.6 – which is also surprisingly low, considering the background of sample students.

To sum up, the self-evaluation feedback analysis provides interesting results. The sample students all work in areas that require log analysis and cyber incident handling, but surprisingly, their average self-evaluation scores are 3.6 and 2.9 respectively. The summary of described feedback analysis results is shown in *Table 11*.

Also, worth noting that 44% of test subjects described their cyber incident reporting experience as non-existent (score 0). It would have been good insight to know how the students would have evaluated their incident reporting experience after the exercise lab. Unfortunately, this was not part of the post questionnaire nor was provided in lab feedback. Detailed analysis of the students' self-evaluation results is not within the scope of this thesis.

5.2 Validation system result analysis

This paragraph provides analysis for validation system results. The complete process of producing the values for the validation reports used in this research, is described in detail in *chapter 3.5*. *Chapter 3.5* also provides detailed description of designing the reports'. Developing the exercise lab and research validation system is explained in detail in *chapter 3.6.5*. Briefly, the research evaluation method is using pre- and post-intervention questionnaires. Due to the context of this exercise, the questionnaires for this thesis are previously created and scored cyber incident report forms.

The hypothesis about the validation system, as described in *chapter 3.6.5*, is that completing the online cyber incident reporting exercise will increase the students' skills to more precisely distinguish an exceptional incident report form from an appalling one.

The research done for this thesis proposes that the students' cyber incident documenting skills will improve because of this exercise, if after completing the exercise, the student scores validation incident reports' values significantly closer to their actual value (explained in more detail in *chapter 3.6.5*.

Results for the students' deviation from the actual validation reports values is as follows:

- Students' absolute deviation from actual reports' values (expert' scores) before the lab, on average, is 2.04 score points;
- The deviation after the lab is 3.22 (58% higher than before the lab exercise);
- The students' average validation reports' score increase was almost identical with the experts' score increases for the same reports (44% vs 49%);

Meaning that, the average absolute deviation before the exercise was 1.18 score points smaller and hence, closer to the reports' actual values than after the exercise. The average score of experts was 3.48 for pre-lab reports and 5.01 for post-lab reports. The increase is 44%. The average score of students for pre-lab reports was 5.39 and 8.03 for post-lab reports. The increase is 49%. **This indicates that the students realized the different value of reports', but scored all the reports significantly higher than what is their actual values (scored by experts').** Students' score was 1.9 points higher for pre-lab reports and 3.0 for post-lab reports, compared to experts. The validation results are displayed in *Table 12*. Full list of students' validation reports' scores as well as experts' scores is displayed in *Appendix IV*.

Table 12. Validation system results.

Students' average score deviation from experts'		Experts' average scores for validation reports		Students' average scores for validation reports		Students' average score difference compared to report designer	
Before exercise	After exercise	Before exercise	After exercise	Before exercise	After exercise	Total average (all students)	Score difference less than 0,1
2,04	3,22	3,48	5,01	5,39	8,03	0,66	33%
		144%		149%			

The hypothesis was that the students' average evaluation score deviation from reports' actual value is lower after the exercise. Based on results from final evaluation, this is not the

case. **Although the student's average score increase, compared to experts' scores, remained roughly the same (~47%), the students' score deviation, from actual report values, did not lower after the exercise.** The produced data was further analyzed and the following conclusions were made.

After completing the exercise, the students' score deviation from experts' scores increased possibly due to a combination of the following possible reasons:

- Soft skill like incident reporting cannot be sufficiently taught with a short 60-minute exercise.
- Incident reporting cannot be taught with an online exercise.
- The order of validation reports. The possible effect that the order has on the evaluation outcome was not sufficiently considered.
- The validation reports' values did not fit in the value range they were initially designed. The range of reports' values could have been too small to make appropriate assumptions, for example.
- The level of complexity and content of validation reports' needs revising.
- The selected sample group of experts and students needs revising.
- Possible errors in the process of designing and implementing lab exercise tasks and designing the storylines, for example.
- The hypothesis in the context of this research is incorrect.

The following additional interesting notions about the validation results can be made (visible in *Table 12*):

- In 33% of the cases the students' scores and the report authors' scores were almost identical (summary for all 5 reports).
- The total score difference of students and report designer is 0.66, which is significantly lower (56%) than the students' deviation from experts'.

These results imply that the students were much more critical with evaluating the reports before the exercise. One possible reason for this is analyzed further in *chapter 3.6.5* regarding the connection between the duration of the exercise, and the average human attention span. Briefly, humans tend to lose focus and act hastier when tired or anxious. For example, anxious about being incapable of analyzing the network traffic.

The second possible reason is that, during the lab, valuable experience and knowledge was gained regarding the complexity of the cyber incident reporting task. Thus, students evaluated the reports less critical after the exercise. As reporting is generally considered a soft skill, the long-term learning impact from this type of learning method will be evidenced in time. Another cyber incident reporting exercise could be conducted on the same students, after a year for example, to make new conclusions about the results of this thesis.

6 Contribution of the author and future works

The developed exercise and the developed cyber incident report scoring system is a very cost-effective method to exercise cyber incident reporting for technical individuals. Especially when compared to currently available methods like on-site cyber defense exercises. The concept exercise has been created and tested, and is modifiable with medium effort. Also, a list of valuable cyber incident report features has been produced to score cyber incident reports. The produced list and scoring method can be used in wider context outside of this research area.

To sum up, the contribution of this thesis is the following:

- Concept online cyber incident reporting exercise, that is modifiable with medium effort, for technical individuals;
- Analysis, implementation and evaluation of the pre- and post-questionnaire validation method for an online cyber incident reporting exercise;
- List of cyber incident report features' categories and sub-categories with detailed descriptions;
- Possible default cyber incident report form is proposed;

The research done and work presented in this thesis revealed many new challenges and opportunities to be analyzed and implemented. Some of the unanswered questions and possible future work includes:

- Revising the incident type from network traffic analysis to something else to possibly broaden the target audience and improve exercise efficiency;
- Testing the proposed validation method with another set of lab data;
- Producing a universally agreed default cyber incident report template or form;
- Producing a universally agreed default structure for cyber incident report sections;
- Replacing the cyber incident report template used for this thesis with a universally agreed standard report form, when such a template is developed and agreed upon;
- Involving more experts in the validation system evaluation process;
- Increasing the level of automatic data evaluation with the use of machine learning once there is enough data to support it;
- Revising the pre- and post- questionnaires, including the questions regarding self-evaluation;
- Generating the lab exercise environment based on Windows operating system;
- Creating a timed process that would provide hints (link to a guide for example) for students when they seem to be stuck on some part of the lab;
- Automatic cyber incident report form completion based on specific cyber incidents;
- Connecting the evaluation system with students' managers, who would have to make managerial decisions based on subordinates' submitted incident report forms;

Work has already been started on some of the items in this list. For example, further analysis into the default structure of data for cyber incident report forms.

7 Conclusion

The goal of this thesis was to create a concept system to evaluate and improve the cyber incident documenting skills for technical specialists individually. Results from final evaluation propose that the generated concept online exercise, and the cyber incident report scoring system, might be applicable in the research area but need revising. Based on earlier research and the work done for this thesis, this validation method is considered plausible to evaluate cyber incident reports. Because of using the produced cyber incident report scoring system, the experts' scores for created cyber incident reports, were roughly similar.

The exercise validation method of using previously created cyber incident reports as pre- and post-questionnaires, is suitable for validating this exercise based on earlier research, but requires more analysis in the context of this research. The work done, and results produced in this thesis, propose that this exercise improved technical individuals' reporting skills. Mostly through knowledge and experience gained during the lab exercise. Knowledge about the complexity, and actual value of a cyber-incident report, for example. One proving factor is that the students evaluated the previously created incident reports significantly less critically after the exercise. As reporting is generally considered a soft skill, the long-term learning impact from the exercise created for this thesis will be evidenced in time.

Fully automating this type of cyber incident reporting exercises with this level of complexity should involve some form of already existing default templates, guidelines and examples. Furthermore, fully automating an exercise with this level of user input dependability is deemed possible, but would require analysis of large data sets. Data analysis could presumably be done with the use of machine learning but would still require human specialists' involvement. Analyzing and interpreting the data from humans' perspective for example.

Other notions from this research include:

- The amount, background- and nationality of experts, chosen for this thesis validation system should be increased to provide more accurate validation results.
- Increased number of students should complete the final exercise to gain more accurate results about the increase of students' cyber incident reporting skills.
- The conducted research and produced method is usable in wider context.
- The introduced validation system, including the list of produced valuable cyber incident report features and scores, is novel in the context of cyber incident reporting.
- The created exercise is modifiable with medium effort.

To sum up the thesis, the goals were generally achieved. A proposed, online individual cyber incident reporting exercise concept was created for technical cyber security specialists. One possible cyber incident report default template was proposed. A novel cyber incident report scoring system was produced and tested. Conducted tests resulted with many new challenges and opportunities for future works.

Acknowledgements. The author would like to thank Sten Mäses for providing great insight regarding evaluation methods for human aspects and Margus Ernits et al. (Rangeforce) for providing the platform, and exercise lab technical support. Also, special thanks to Kaie Maennel for providing material on evaluating serious games and game based learning.

References

[1] H. F. Lipson, “Tracking and Tracing Cyber-Attacks: Technical challenges and global policy issues,” 2002.

[2] E. P. European Commission, “EU GDPR,” 2017. [Online]. Available: http://www.eugdpr.org/. [Accessed: 14-May-2018].

[3] ENISA, *The 2015 Report on National and International Cyber Security Exercises*, no. December. European Union Agency for Network and Information Security, 2015.

[4] P. Cichonski, *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*, vol. 800. NIST, 2012.

[5] S. Lu and M. M. Kokar, “A Situation Assessment Framework for Cyber Security Information Relevance Reasoning,” p. 8, 2015.

[6] D. Clark, “Psychological myths in e-learning,” *Med. Teach.*, vol. 24, no. 6, pp. 598–604, 2002.

[7] S. Mäeses, “Evaluation method for human aspects of information security,” Tallinn University of Technology, 2015.

[8] A. Sumin, “Evaluation Method for Cyber Awareness Course,” Tallinn University of Technology, 2016.

[9] E. Naumanis, “CENTRALLY MANAGED NETWORK TRAFFIC GENERATION FOR CYBER SECURITY,” Tallinn University of Technology, 2014.

[10] C. W. Johnson, “Contrasting Approaches to Incident Reporting in the Development of Safety and Security- -Critical Software,” *Safecomp*, p. 19, 2015.

[11] I. Stine, M. Rice, S. Dunlap, and J. Pecarina, “A cyber risk scoring system for medical devices,” *Int. J. Crit. Infrastruct. Prot.*, vol. 19, pp. 32–46, 2017.

[12] Forum of Incident Response and Security Teams, “Common Vulnerability Scoring System V3,” *Development Update*, 2018. [Online]. Available: http://www.first.org/cvss. [Accessed: 14-May-2018].

[13] J. E. Morhardt, “Scoring corporate environmental reports for comprehensiveness: A comparison of three systems,” *Environ. Manage.*, vol. 27, no. 6, pp. 881–892, 2001.

[14] C. Security and I. Handling, “Nccic Cyber Incident Scoring System,” *Natl. Cybersecurity Commun. Integr. Cent.*, pp. 1–8.

[15] P. Kral, *The Incident Handlers Handbook*. The SANS Institute, 2011.

[16] S. (Raytheon C. Hennin, “Control System Cyber Incident Reporting Protocol,” *Technologies for Homeland Security, 2008 IEEE Conference on*, 2008. [Online]. Available: https://www.ieee.org/. [Accessed: 14-May-2018].

[17] ENISA, “European Union Agency for Network and Information Security,” *ENISA*. [Online]. Available: https://www.enisa.europa.eu/. [Accessed: 14-May-2018].

[18] Software Engineering Institute, “Incident Management Resources,” *CERT Division, Carnegie Mellon University*. [Online]. Available: https://www.cert.org/incident-management/. [Accessed: 14-May-2018].

[19] E. Union and A. For, *Incident reporting framework for eIDAS Article 19*, no. December. ENISA, 2016.

[20] S. L. Allen, “Cyber Intelligence : Challenges and Best Practices,” *Carnegie Mellon Univ.*, no. January, p. 26, 2015.

[21] A. Rehn, “The Art of Keynoting,” 2016. [Online]. Available: https://medium.com/the-art-of-keynoting/the-20-minute-rule-for-great-public-speaking-on-attention-spans-and-keeping-focus-7370cf06b636. [Accessed: 14-May-2018].

[22] Instructional Design Central, “Instructional Design Models,” 2018. [Online]. Available: https://www.instructionaldesigncentral.com/instructionaldesignmodels. [Accessed: 15-May-2018].

[23] K. Shelton and G. Saltsman, *Using the Addie Model for Teaching Online*. IGI Global, 2006.

[24] Sobah A. Petersen and Michael A. Bedek, *Challenges and Opportunities in Evaluating Learning in Serious Games: A Look at Behavioural Aspects*. 2009.

[25] M. Amer, D. U. Tugrul, and A. Jetter, “A review of scenario planning,” *Elsevier*, pp. 23–40, 2012.

[26] R. Abide, “Exercising Your Enterprise Cyber Response Crisis Management Capabilities,” 2015.

[27] S. Burgmair *et al.*, “OWASP Top 10 Privacy Risks Project,” 2017. [Online]. Available: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project. [Accessed: 14-May-2018].

[28] N. Marketshare, “Market Share Statistics for Internet Technologies.” [Online]. Available: https://www.netmarketshare.com/operating-system-market-share.aspx? [Accessed: 14-May-2018].

[29] US-CERT, “UC-CERT incident report form.” [Online]. Available: https://www.us-cert.gov/forms/report. [Accessed: 14-May-2018].

[30] I. C. C. Center, “Complaint Referral Form.” [Online]. Available: https://complaint.ic3.gov/default.aspx? [Accessed: 14-May-2018].

[31] Australian Cyber Security Centre, “Cyber Security Incident Report Form,” *Australian Cyber Security Centre*. [Online]. Available: https://www.acsc.gov.au/incident.html. [Accessed: 14-May-2018].

[32] T. Introducer, “Trusted Introducer.” [Online]. Available: https://www.trusted-introducer.org/. [Accessed: 14-May-2018].

[33] C. Johnson, “Failure in Safety-Critical Systems: A Handbook of Incident and Accident Reporting,” *Glas. Univ. Press*, p. 986, 2003.

[34] Rangeforce, “RANGEFORCE.” [Online]. Available: https://rangeforce.com/. [Accessed: 14-May-2018].

[35] K. Maennel, “Improving and measuring learning effectiveness at cyber defense exercises,” Tallinn University of Technology, 2017.

[36] I. Mayer, G. Bekebrede, H. Warmelink, and Q. Zhou, *A Brief Methodology for Researching and Evaluating Serious Games and Game-Based Learning*. IGI Global, 2014.

[37] C. Girard, J. Ecalle, and A. Magnan, “Serious games as new educational tools: How

effective are they? A meta-analysis of recent studies," *J. Comput. Assist. Learn.*, vol. 29, no. 3, pp. 207–219, 2013.

[38] A. Alliance, "Lean Startup - MVP," 2018. [Online]. Available: https://www.agilealliance.org/glossary/mvp/. [Accessed: 14-May-2018].

Appendix

I. GDPR – General Data Protection Regulation

The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects [2]. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location [2]. The GDPR will also apply to the processing of personal data of data subjects in the EU, by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU [2]. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU [2].

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent [2]. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language [2]. It must be as easy to withdraw consent as it is to give it [2].

Another major shift is towards data transparency and empowerment of data subjects [2]. Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose [2]. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format [2].

Data subjects have the right to be forgotten which entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data [2]. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent [2]. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests [2]. GDPR also introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' [2]. In addition Privacy by Design is now more than just a concept, with the GDPR it is a legal requirement – data protection has to be part of systems design rather than an addition [2]. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing [2].

Appointment of the DPO will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences [2].

II. Cyber incident report template

Security incident report

Organization:		**Phone:**	
Recipient:		**Phone:**	
Submitter name:		**Submitter E-mail:**	
Incident name:		**Incident number:**	

Incident Effect:	
Availability	
Integrity	
Confidentiality	
Other	

Incident Cause:			
Software		User privileges	
Hardware		Third party	
Administration		Lack of testing	
Attack		Other	

Critical level	Low		Medium		High	

Incident summary	
Incident occurred at (time):	
Impact and business influence of the incident:	
Description of the incident and chronology:	
Possible cause:	
Possible solution:	

Recommendations for avoiding the incident in the future:	

III. Full list of experts' validation report scores (every feature)

Average validation report values (blue)				First expert				Second				Third				Fourth				Fifth				Sixth			
avg1	avg2	avg3	avg4	avg5	1A	2A	3A	4A	5A	1B	2B	3B	4B	5B	1C	2C	3C	4C	5C	1D	2D	3D	4D	5D	1E	2E	3E	4E	5E	1F	2F	3F	4F	5F
2.9	**4.8**	**5.5**	**2.1**	**5.2**	**2.5**	**2.8**	**3.5**	**1.7**	**4.8**	**4.0**	**6.4**	**8.6**	**3.7**	**7.6**	**2.7**	**4.7**	**6.0**	**0.8**	**3.3**	**2.4**	**5.4**	**3.9**	**2.0**	**5.1**	**2.4**	**4.5**	**5.7**	**1.9**	**4.8**	**3.3**	**5.2**	**5.5**	**2.2**	**5.4**
0.25	0.25	0.63	0.12	0.78	0.3	0.3	0.5	0	0.7	0.3	0.4	1	0.2	1	0	0	0.5	0	0.9	0.4	0.3	0.6	0	0.5	0	0	0.6	0	0.8	0.4	0.3	0.6	0	0.8
0.20	0.13	0.63	0.67	0.78	0.1	0.1	0.2	0.5	0.7	0	0.4	1	1	1	0.5	0	1	0.5	0.9	0.1	0.1	0.1	0.6	0.6	0.2	0	1	0.7	0.8	0.3	0.2	0.5	0.7	0.7
0.08	0.82	0.77	0.07	0.67	0.2	0.5	0.5	0.1	0.2	0	1	1	0	1	0	1	1	0	1	0.1	0.8	0.6	0.1	0.3	0	0.8	0.8	0	0.8	0.2	0.8	0.7	0.2	0.7
0.92	0.92	0.92	0.92	0.92	0.5	0.5	0.5	0.5	0.5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0.50	0.62	0.58	0.03	0.43	0.2	0.2	0.2	0.2	0.2	0.5	1	1	0	0.8	1	1	1	0	0.5	0.3	0.5	0.3	0	0	0.5	0.5	0.5	0	0.5	0.5	0.5	0.5	0	1
0.13	0.68	0.72	0.10	0.30	0.1	0.1	0.3	0.1	0.4	0.4	1	1	0.2	0.6	0	1	1	0	0	0.1	0.4	0.4	0.1	0.3	0	0.8	0.8	0	0	0.2	0.8	0.8	0.2	0.5
0.47	0.90	0.87	0.13	0.48	0.4	0.6	0.6	0.1	0.3	0.8	1	1	0.1	1	0.5	1	1	0.1	0.1	0.1	1	0.8	0.2	0.4	0.5	0.8	0.8	0.1	0.6	0.5	1	1	0.2	0.5
0.05	0.57	0.62	0.10	0.43	0.2	0.2	0.4	0.3	0.5	0	1	1	0	0	0	0.5	0.8	0	0.8	0.1	0.6	0.1	0.3	0.5	0	0.5	0.8	0	0.8	0	0.6	0.6	0	0
0.18	0.38	0.47	0.10	0.58	0.3	0.3	0.3	0.2	0.5	0	0.3	0.6	0	1	0	0.3	0.3	0	0.3	0.5	0.7	0.5	0.2	0.6	0	0.3	0.4	0	0.5	0.3	0.4	0.7	0.2	0.6
0.55	0.58	0.58	0.52	0.72	0.2	0.2	0.3	0.2	0.6	1	1	1	1	1	0.5	0.5	0.5	0	0	0.4	0.7	0.4	0.6	1	0.6	0.6	0.6	1	1	0.6	0.5	0.7	0.6	1
0.03	0.03	0.05	0.02	0.03	0.2	0.2	0.2	0.1	0.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0.45	0.53	0.55	0.10	0.53	0.4	0.4	0.4	0.1	0.7	0.6	0.4	0.8	0.5	1	0.5	0.5	0.5	0	0	0.3	0.8	0.5	0	0.8	0.5	0.5	0.6	0	0	0.4	0.6	0.5	0	0.7
0.15	0.28	0.20	0.32	0.58	0.1	0.2	0.2	0.1	0.5	0.5	0.5	1	1	1	0	0	0	0	0	0	0.4	0	0.2	0.7	0	0	0	0	1	0	0.4	0	0.3	0.5
0	0	0.10	0	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

IV. Full list of students' and experts' validation reports' scores

List of all students' scores for all 5 validation reports.

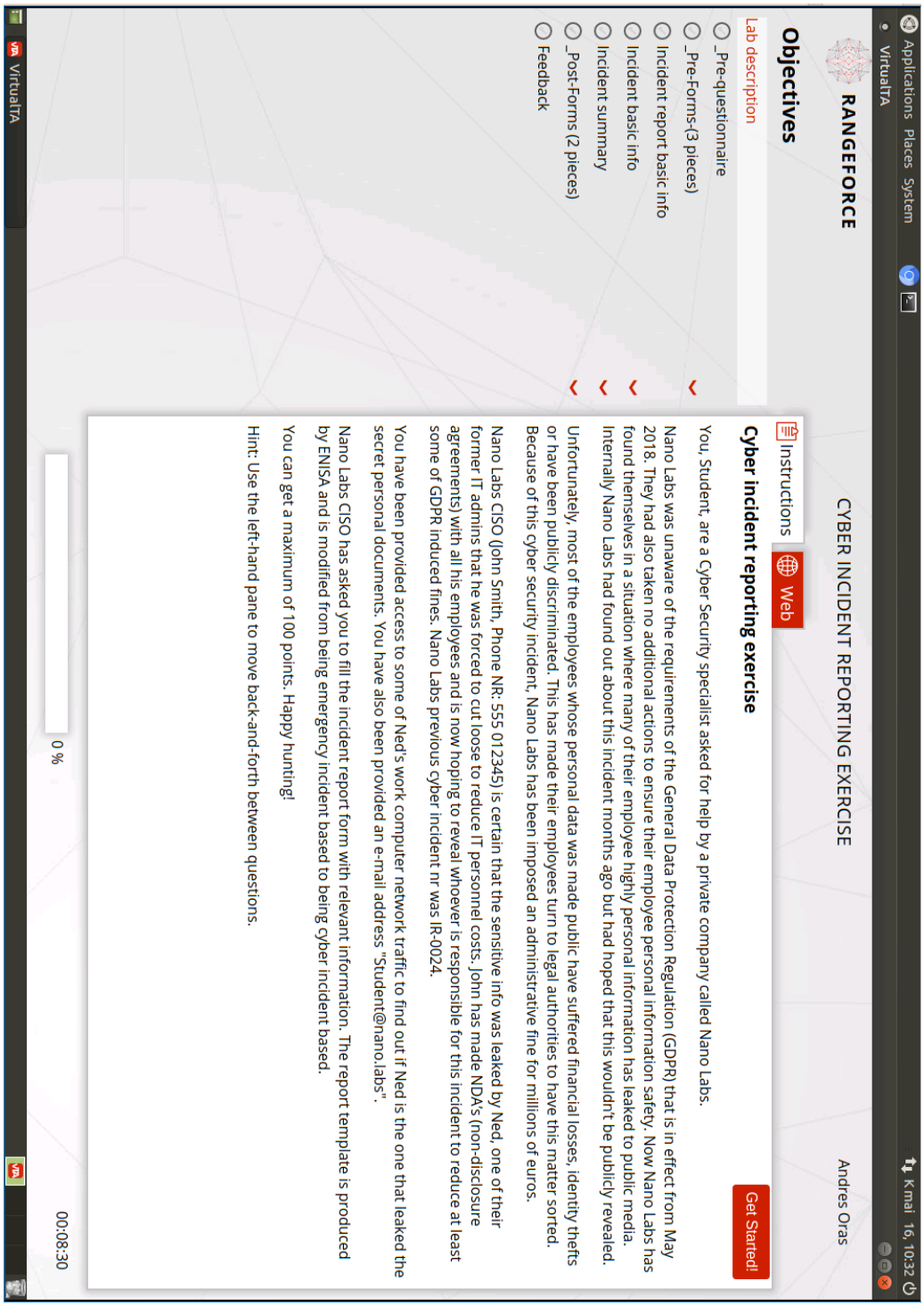
Students' number		1	2	3	4	5	6	7	8	9	Average reports' value		Experts' report value lower
											Students	Experts	
Reports' number	**1-st**	**3,5**	**6,5**	**2,0**	**3,0**	**4,0**	**5,0**	**3,0**	**6,0**	**5,0**	4,2	2,9	69%
	2-nd	**7,0**	**9,0**	**6,0**	**6,0**	**10,0**	**3,0**	**7,0**	**9,0**	**7,5**	7,2	4,8	67%
	3-rd	**7,9**	**9,0**	**8,0**	**9,0**	**9,0**	**8,0**	**8,0**	**10,0**	**8,5**	8,6	5,5	64%
	4-th	**4,0**	**4,0**	**5,0**	**3,0**	**1,2**	**3,0**	**2,0**	**5,0**	**3,0**	3,4	2,1	61%
	5-th	**7,5**	**10,0**	**7,5**	**9,0**	**10,0**	**8,0**	**10,0**	**9,0**	**9,0**	8,9	5,2	59%

List of all experts' scores for all 5 validation reports.

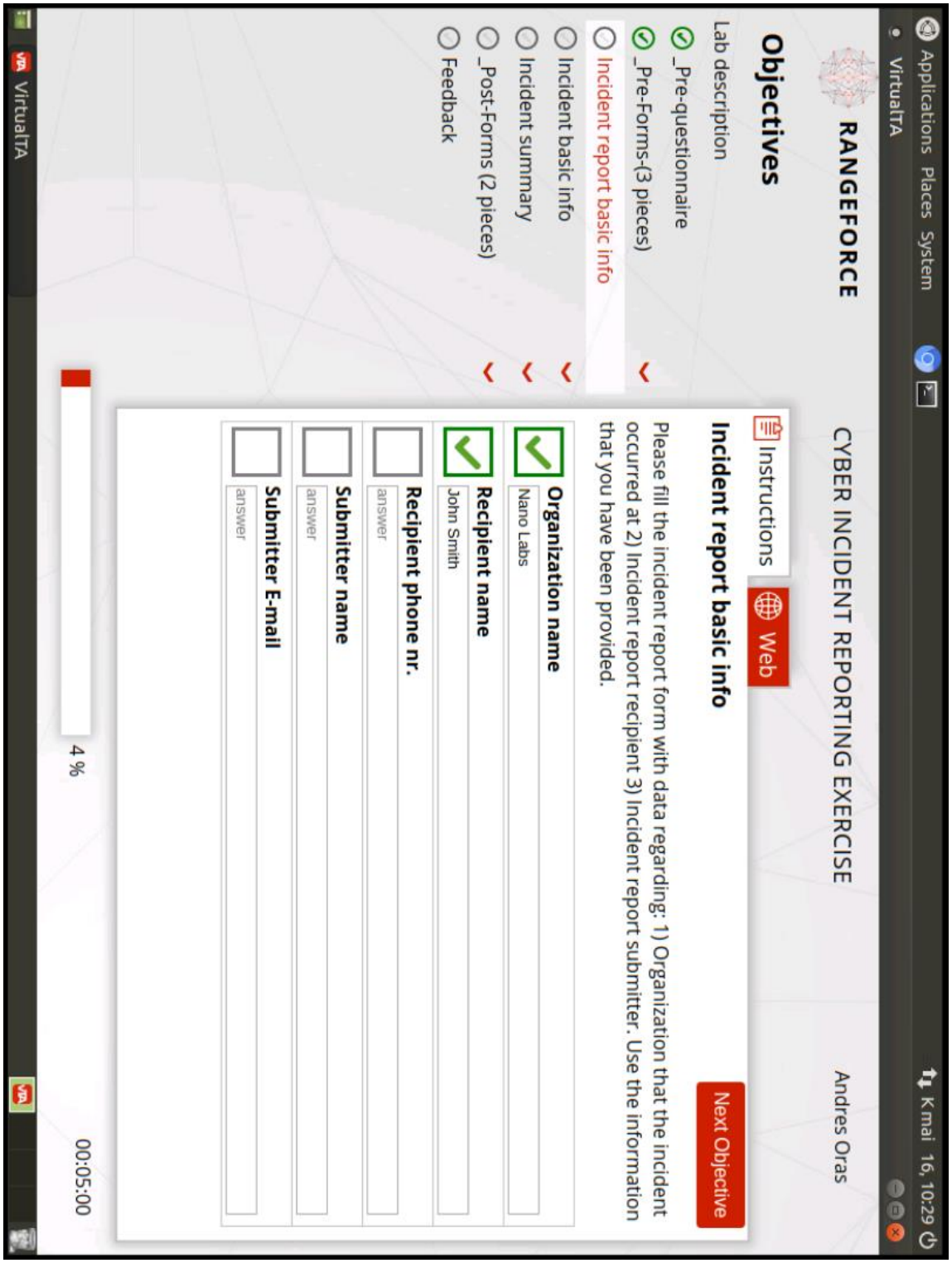
Experts' number		1	2	3	4	5	6	Average
Reports' number	**1-st**	**2,5**	**4,0**	**2,7**	**2,4**	**2,4**	**3,3**	**2,9**
	2-nd	**2,8**	**6,4**	**4,7**	**5,4**	**4,5**	**5,2**	**4,8**
	3-rd	**3,5**	**8,6**	**6,0**	**3,9**	**5,7**	**5,5**	**5,5**
	4-th	**1,7**	**3,7**	**0,8**	**2,0**	**1,9**	**2,2**	**2,1**
	5-th	**4,8**	**7,6**	**3,3**	**5,1**	**4,8**	**5,4**	**5,2**

V. Screenshots from lab

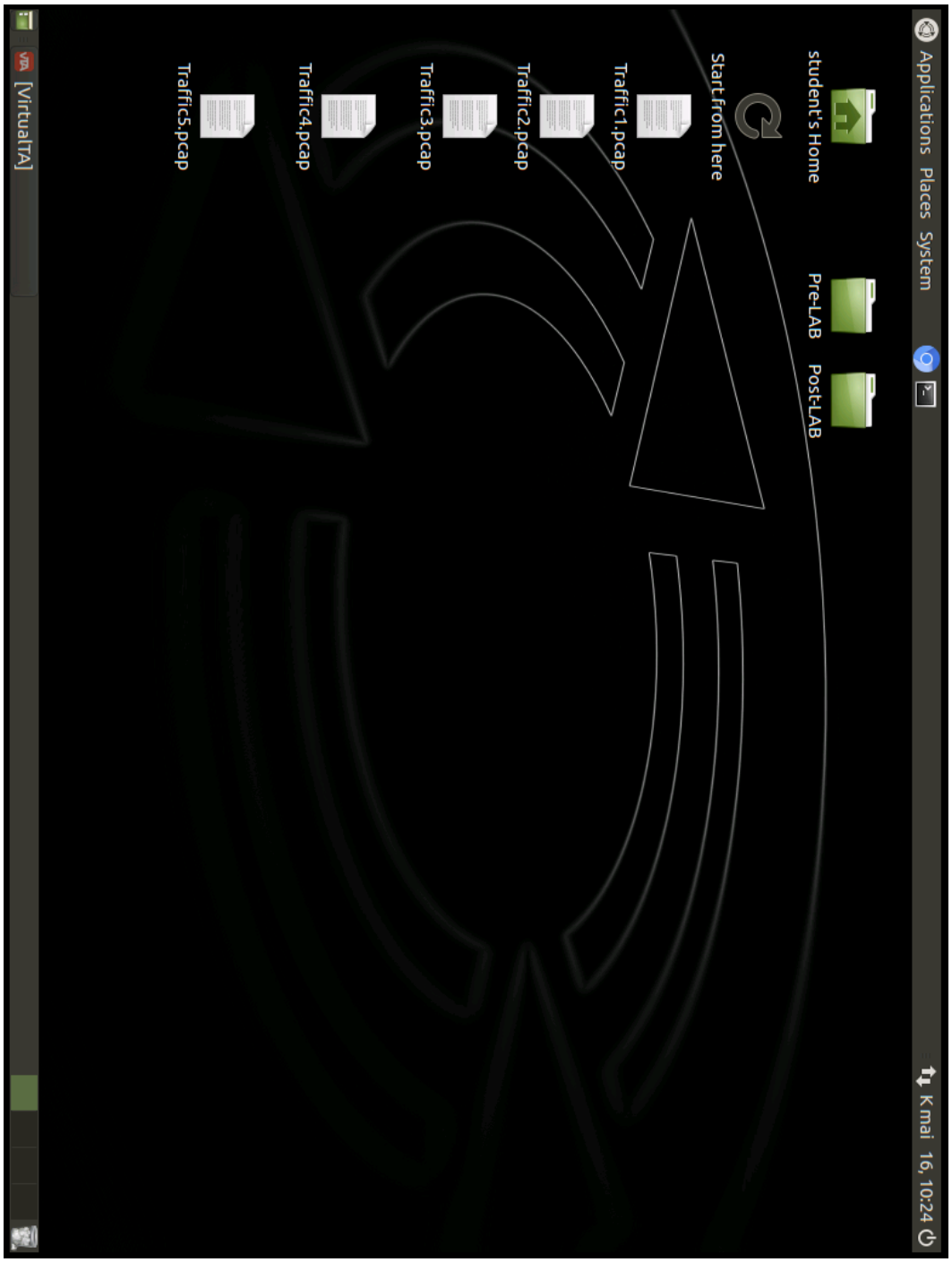
VirtualTA at the beginning of the lab.



Partially filled VirtualTA.



Screenshot of lab computers' desktop with 5 network traffic files waiting to be analysed. Desktop also contains two folders containing validation reports for evaluation before and after the exercise. Desktop includes a browser link to VirtualTA – "Start from here" that is also automatically started with the computer.



VI. License

Non-exclusive license to reproduce thesis and make thesis public

I, **Andres Oras**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:
    1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and
    1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright, of my thesis

Online Cyber Security Exercise to Evaluate and Improve Individual Technical Specialists' Cyber Incident Reporting Skills,

supervised by Sten Mäses, Margus Ernits, Raimundas Matulevičius,

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **21.05.2018**