SecureRole

Bachelor thesis

Department of Computer Science

Eastern Switzerland University of Applied Science

Campus Rapperswil-Jona

Spring Term 2022

Authors Anina Bytyçi
Isaac Würth
Marco Zanetti

Advisor Nathalie Weiler
Project Partner Giorgio Tresoldi
Co-Examiner Mitra Purandare

Abstract

Over the last couple of years, cyber security attacks have become a dominant issue in the global landscape. Phishing campaigns are on the rise and the world is in a current “gold rush for ransomware”. Companies are being targeted with an increased frequency all around the world. This calls for IT experts, which often receive their first in-depth training in security during their time at college or in secondary education. The goal of this thesis is to better prepare students with the development of an incident response role-playing game. This can be achieved by collaborative training and using simulations to mimic a situation as close as possible to the real-world scenario. Teaching with versatile and adaptable scenarios builds up skills to prepare a company against different kinds of attacks and how to mitigate them, should one of its systems be compromised. Additionally, they learn to appropriately react, how to communicate, and on which basis to make meaningful decisions, as a key to success for eradication of the attacker and recovery to normal operation.

The result of the bachelor thesis is a framework, that gives guidance for the creation of packages and scenarios in a versatile and adaptable way, packages, that can be chained to create scenarios, and predefined scenarios to directly start a cybersecurity role-playing game. The framework allows for interchangeable content, which makes it possible to change certain parts of the role-play giving it an agile nature. The packages also include additional materials, such as text scripts, presentations, and curated internet content to deepen the knowledge about cyber security attack techniques and mitigations. The predefined scenarios are created with the packages and were tested during the thesis.

It started with an analysis of existing products, we evaluated if any of them could be an exact fit for our purposes. Sadly, none of them fully met the requirements. So we then used them to draw inspiration for our product. After we defined how the game is going to be played and how the framework for content creation is structured, we started the process of content creation itself. For verification and improvements of the content, we established a process of peer-reviews, asked external educators for their opinions, and tested it with our target audience. The created content was finally verified with an acceptance test, the results of which allowed for final improvements to be made to the product.

The landscape of cybersecurity threats is ever-changing, and incident responders need to be trained with an adequately agile approach. Our product offers a solid framework that allows us to create, edit and change our scenarios to keep the simulation dynamic and tailor it to the user’s needs. This allows us to provide an interactive learning experience that helps inexperienced students take their first steps in a simulated environment, or advanced students hone their skills.

Keywords: *Instructional design, Cyber security simulation, Tabletop game, Game-based learning*

Management Summary

Purpose

The purpose of our project is to provide role-playing games and learning material about different topics in cybersecurity, so the theoretically learned cybersecurity concepts can be put into practice. This would be very helpful since enterprises and individuals are increasingly facing various cyber attacks. Our product will better prepare students of OST for the threats they will face in their professional career. Each of these attacks is different from the others, and therefore each of them requires a different way of responding to the attack, what to do when it occurs, how to mitigate it, and how to return the system to normal. The goal was to combine different scenarios from different types of attacks and integrate them into the role-playing game.

Procedure

First, we created concepts of what our game should look like and how we could make it more engaging for our players. We discussed in detail what kind of role-playing game we would create and what medium it could be played in. It was also important for the game how the players could interact with it, how they could stay motivated and what goals they should have achieved at the end of the game.
We then started developing a tabletop role-playing game with good quality content regarding the various incidents we wanted to show to our participants. The first developed table-top game consisted of phishing combined with a ransomware.
Since our product would feature a variety of different incidents, we had the idea to modularize it for a better user experience and increased scalability. This would allow us to reduce time needed for developing and creating more games in the future. It also offers the user a more varied palette of topics from which they can choose when assembling their ideal incident response scenario. This resulted in topics, which are part of the role-playing game, being divided into the corresponding categories according to the Lockheed Martin cybersecurity kill chain. Each topic is then considered as a package that can be worked on independently and then combined with other topics. A complete role-play would consist of multiple packages from different categories of the kill chain.

Results

As a result, for each game, we provided a game master document which is helpful to moderate the game, as well as six different character sheets for participants which take part in the exercise by impersonating different employees in a mock company. Additional material is created for each topic covered in the game. This includes scripts and slides, as well as a list of helpful third-party content gathered from the team. In total, five packages were created, including Phishing, Ransomware, Man-in-the-Middle and Valid Accounts, as well as a package called Reconnaissance, which consists of OSINT, Active Scanning and Phishing for Information. When combined, these packages create a variety of incident response role-playing games.

Outlook

With the help of the framework created, new topics can be more easily incorporated into the game. We also identified further quality of life improvements which we want to bring to this project in the future. One improvement would be to automate the combination of different packages and the creation of a game, as currently this all has to be done manually. This way, the user does not need to directly modify the master document structure to get the desired content with the desired packages in the game. This will be the next goal of the project to be achieved after the completion of the bachelor thesis. Overall, role-playing games were created with high-quality content along with free educational material.

Aknowledgements

We want to thank everybody who supported us during the writing of this essay. While countless supporters have helped in their way, we wanted to single out a few for a special mention.

Nathalie Weiler, Professor for cybersecurity at OST Rapperswil, for her guidance, support, and encouragement. Her inputs and feedback were always highly valued giving us the possibility to improve our product and the thesis. Thank you.

Thanks to our external co-examiner, Giorgio Tresoldi, and our internal co-examiner, Mitra Purandare, for taking the time to listen to our presentations, allowing us to get great input and new approaches that we could pursue.

We would like to thank Thomas Würth. He read through our work several times and pointed out little imperfections. With his help, we were able to add some finishing touches to our work. Thank you very much.

We would further like to kindly thank Anja von Rotz. She offered us advice from a teachers point of view and helped us to understand how good education has to be undertaken. We can now confidently say that we followed best known practices regarding educational methods thanks to her. Thank you very much.

An important group which we would like to thank as well are our testers. They dedicated their free time, to help us gather feedback about our project, which led to substantial improvements for future participants. We would like to thank everyone of them very much.

- Myriam Assunção
- Petra Heeb
- Simon Kindhauser
- Claudio Knaus
- Lukas Leuenberger
- Liliana Stratan

- Anton Rasi
- Liburn Gjonbalaj

And last, but certainly not least we want to thank you. Thank you, for reading this thesis, and hopefully considering using our material to improve how cybersecurity is discussed and taught in your environment.

Contents

1. Introduction

1.1. Purpose and Scope

As we live in a digital world today, online cyberattacks place every day. We read it in blog posts, on social media, and sometimes even in the news, if the event is noteworthy enough, or has hit a large infrastructure provider once again. Usually, the attackers' main goal is to steal users' credentials and use them to gain access to accounts and cause damage not only to individual users but also to large companies.

The goal of this project is to provide free and easily accessible interactive training for various scenarios in the world of cybersecurity attacks. In addition to the interactive role-playing games, additional scripts and slides are provided for each topic covered.

1.2. Audience

The project is primarily addressed to students willing to learn more in the field of cybersecurity. The main goal is to teach them different attack scenarios to find the right defensive measure and reduce personal exposure and know-how to act in case of an attack.

The scripts and slides provide theoretical information about different cybersecurity attacks while the role-playing games allow them to put the freshly learned theory into practice.

The project also targets professors teaching cybersecurity modules, as they are provided with slides and scripts for the topic, as well as guides on how to facilitate the role-playing game for their students. The slides and scripts provided as part of the project can be used and modified depending on the professor's needs.

1.3. Structure

This thesis is structured into three parts. The first part contains the technical report, the second part is the project documentation itself, and the third part consists of the glossary, the bibliography, and further appendices.

1.3.1. Technical report

The technical report is spread out over eleven chapters. It does not represent a chronological order of events, since topics were created, improved, and revisited, which does not allow for a coherent document. We instead grouped it into topics that allow easy reading.

The documentation begins with the first steps in the project which consist in researching how educational materials are generally created. We also consulted literature aimed at teachers to increase knowledge and produce meaningful educational material. It then continues in regarding other ways of conveying cybersecurity education in a playful manner, such as other games, role-playing games, and possible frameworks which we could use to gather inspiration, or in the case of the frameworks, to base our game upon.

After closing the chapter on our research, the documentation gives an overview of the decision process and what our game should look like. This includes all discussions on good and bad ideas. Finally, it led to the current idea SecureRole.

After the prototype was completed, the project went into alpha testing with our first testing group and its following feedback. This assessment combined with the one gathered at our interim presentation from our examiners was worked into the product. We also asked a teacher for feedback regarding our educational approach to the product and included it also. All this led to major improvements, such as the introduction of our new framework “SecureRole Flavors” which allowed for a more structured approach to our content creation.

These upgrades were then used for the acceptance testing and are documented in the next step. We handed out questionnaires that tested certain metrics. Even with a smaller group of testers than foreseen, the quality of the feedback exceeded our expectations and led to some important improvements before the project came to a close. The last chapter in the technical report consisting personal and technical conclusions where we reflect upon the project and find out if we managed to achieve our goals.

Last but not least you will find a short chapter overviewing the whole documentation. It showcases if we reach our personal and technical goals and finish the technical documentation.

1.3.2. Project documentation

The second part is the project documentation. This contains all important files which were created during the project and gathered in the project plan. It contains things like processes, quality assurance, and use cases. It offers a more detailed picture of the

project proceedings with a deep view into certain aspects of the daily work.

Our thesis was not a “classical” software engineering task, but rather the creation of materials for the education of students. So we tailored the administrative tools which we used for the project documentation to our needs, cutting out some files which simply were unnecessary for our course of work.

1.3.3. Appendixes

Last but not least are the appendixes. Here you can find all important files which were considered essential enough to be included in the documentation, but not important enough to warrant their chapter, or they are simply necessary to paint a clearer picture.

Part I.

Technical Report

2. Educational research

We wanted our game to be as educationally valuable as possible. We first needed to assess how good educational content is created, and what factors can be improved for the students to contribute to a more positive learning experience. Our main goal is to create a lasting learning effect for the participants in this role-playing game.

While researching these topics, we knew we needed support from an external source. We are all skilled in Cyber Security, but not in didactics. No literature research was comparable to the skills of an educational professional. So we reached out to Anja von Rotz, a teacher in Rapperswil. She helped us during our literature research regarding books and other sources Furthermore, she agreed to review our work from an educator's point of view and give us feedback on how to improve the role-playing game, once we had created some content. You can find her detailed feedback in chapter 7.

2.1. General research

Most of the findings in the section are based on the book "Was ist guter Unterricht" written by Hilbert Meyer. [1]

His book describes 10 main aspects which are crucial to a good learning experience:

1. * Clearly structured teaching
2. * High proportion of actual learning time
3. Climate which sustains learning
4. * Clarity of content
5. Meaningful communication
6. * Variety of methods
7. Individual support
8. * Purposeful practice
9. * Transparent performance expectations
10. * Prepared environment

Since these points all contribute to an enhanced learning experience, we had to find out which aspects could actively influence design in SecureRole. We have marked these aspects with an asterisk. As you can see, we believe that a well-structured SecureRole exercise can improve the learning experience in many important aspects.

Let's take a closer look at the individual learning aspects we can influence, and how we were planning to do exactly that.

2.1.1. Clearly structured teaching

SecureRole offers clear instructions on how the role-playing game can be carried out. It furthermore offers teaching material such as a script, slides and additional materials for the students. While it does not set a firm limit on how students should interact with the content, it does provide a guideline on how this can be done. This allows for clearly structured teaching and learning and supports the teacher in doing so.

2.1.2. High proportion of actual learning time

With the introduction of the structured approach of SecureRole, the students spend less time searching for content. It also reduces the chances for misunderstandings and confusion for the students, since the content was created by students themselves, knowing of the main pitfalls which have also occurred to them. This allows for a higher proportion of actual learning time.

2.1.3. Clarity of content

The content of SecureRole was written in a well-structured and comprehensible manner. This reduces the possibility of confusion and increases clarity about what the content hopes to accomplish and is thus beneficial to students.

2.1.4. Variety of methods

It is strongly encouraged, if not even neccessary, to use different teaching methods. We achieve this in SecureRole with the inclusion of different ways a student could approach our content. He can choose to read something about the topic (scripts and additional material) or watch videos or listen to audio (additional material).

Sadly, we couldn't bring multiple methods into the role-playing game itself. This is an aspect where SecureRole has potential for improvements in the future.

2.1.5. Purposeful practice

This is the point where SecureRole excels. The simulation of a realistic case is a good way to prepare and beef up the skills for practical situations.

2.1.6. Transparent performance expectations

We provide learning goals for the students in the role-playing game. While they are not exactly performance expectations, we still believe that they have a similar effect. We don't want to force the student to live up to certain expectations. Everyone can participate in their way and find out what is important to them.

We know that teachers might not share this view, or simply want to use SecureRole in an examified way. This is possible, but we do not provide any support for that. The teacher needs to create his grading scales, criteria, etc. . . .

2.1.7. Prepared environment

The lightweight way in which SecureRole is delivered suits this aspect perfectly. No lengthy preparation or setup is required for starting the game. All they need to do is to receive the role description from the teacher and they are ready to engage in the exercise. Everything else falls into place during the game or is taken care of by the teacher. This allows for SecureRole to be a fully prepared learning environment, without distractions.

2.2. Further learning techniques

There are many different educational tactics we could employ to our advantage to make the role-playing game an optimal learning experience for the students. The most promising ones, which we found during our research, are:

- Generally all student-centered approaches
- Game-based learning
- Inquiry-based learning
- Flipped classroom
- Universal design learning

The most important ones will be explained below, with a description of how they could benefit our cause and increase the educational purpose of our role-playing games.

2.2.1. Student centered learning

This should be a general approach to our role-playing games. While a teacher/professor sure is important to the educational success of our role-playing game, we need to put the student in the main focus. In our approach, it's not the teacher to simply provide students with information, but it is more an explorative approach, in which the students need to gather information themselves.

2.2.2. Inquiry-based learning

Inquiry-based learning is the approach that lets the teacher (or the student) ask questions, and then simply supports the student in finding the answers to these questions.

Our role-playing game can't do this directly during the game, but it can provide questions during the role-playing game, which the student then can answer during the additional reading of the supportive material.

More about inquiry-based learning

2.2.3. Flipped classroom

The flipped classroom approach is watching a prerecorded lecture or reading a script and then doing exercises together with the teacher.

Flipped classroom learning

2.2.4. Universal design learning

An article about the different learning strategies
A video with a quick explanation about UDL

3. Related Work

This chapter is an overview of all the research we conducted regarding already existing materials going in a similar direction such as our aspirations. This means interactive exercises which teach the user something in regards to cyber security. Some are simple browser games, others are interactive media, and some are frameworks on which we could base our work.

Our goal was to look at a variety of different kinds of games to gather inspiration for possible interactive elements which we could include in our game. In the case of the frameworks in section 3.2, we were scouting the internet for a possible underlying framework to convey our content to the students in a playful manner.

3.1. Security Games

This section contains the research for security games. These are interactive ways of learning about cyber security. We outlined the creator, how it is usually played and what its main interactive elements are. This was assessed for each game and then introduced in the section “What could we use as inspiration” in regards to our product.

3.1.1. Backdoors and Braches

Figure 3.1.: The SecureRole Team playing *Backdoors and Breaches*

Overview

Backdoors and Breaches is an incident response card playing game, which was designed to playfully train teams for incident response. We analyzes it and looked at how the developers used it to playfully convey information.

How is it played?

It's a card-playing game portraying a security incident, which is structured around the steps of the *Mitre Attack Framework*. A game master, who is called the Incident Master, takes the lead and guides players through the experience. The players can ask questions to solve the issue and get handed procedure cards to solve the issue. They can use these procedure cards and dice to determine if they are successful at containing the breach. To win, the defenders have 10 turns to find out all the details of the breach.

What are the main interactive elements?

Cards force the players to make choices. The dice determine if the players are suc-

cessful and add a good element of surprise.

What could we use as inspiration?

The way the game is structured around an incident master and the defenders. The game uses a combination of luck and critical thinking to contain the breach and it adds a little bit of time pressure to keep the players engaged.

3.1.2. Texas A&M

Overview

Texas A&M Division of Information Technology creates a campus-wide IT security game for *National Cyber Security Awareness Month*. Each game is designed to be fun and engaging while educating students, faculty, and staff about how to be safe online. We took a deeper look into them and saw how they conveyed information and how we could similarly do something.

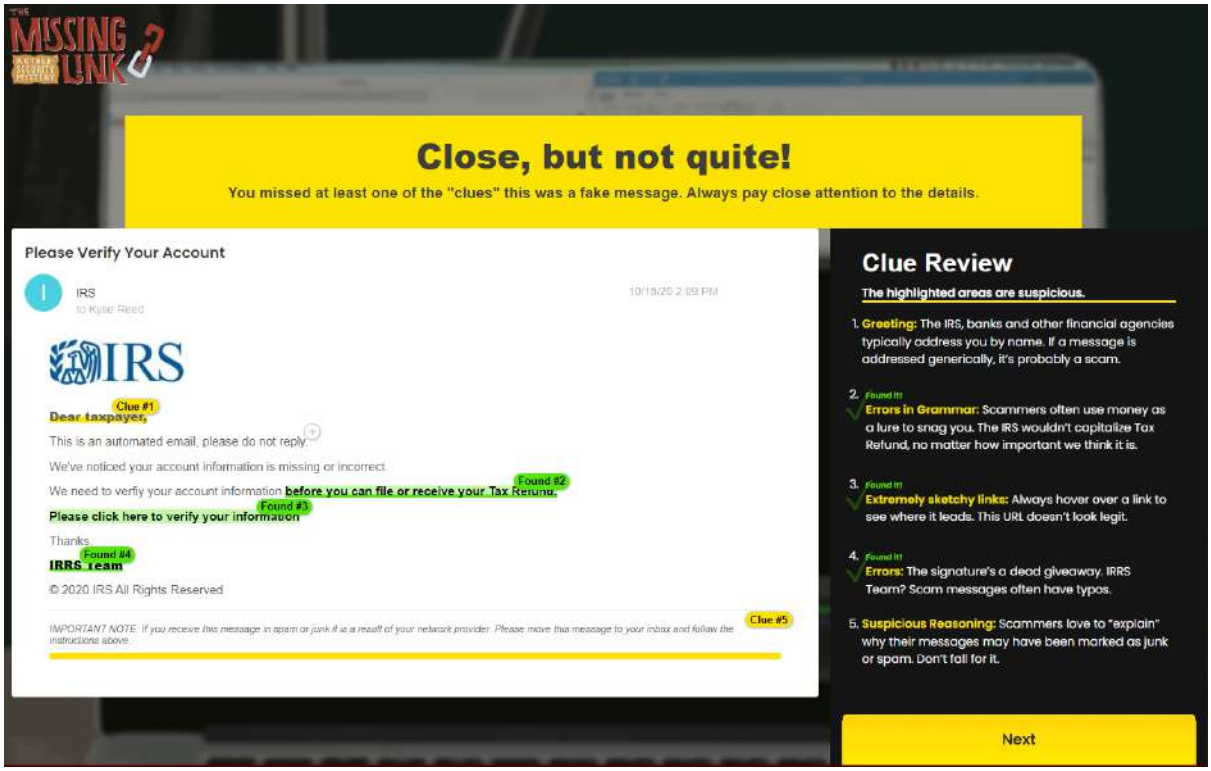


Figure 3.2.: A screenshot of the *Texas A&M* game “The missing Link”

How is it played?

We only tested “The missing Link”, which is their latest installment. The game is held

in a classical point-and-click adventure style to be played alone.

The player then needs to solve a mystery which he can achieve by reading the dialogue presented to him. He is then confronted with things such as phishing e-mails, in which he then highlights the parts of the message he finds suspicious. This continues as the player progresses.

What are the main interactive elements?

The player can read messages and highlight what he thinks is suspicious. The webpage then tells him if he was correct, and why certain aspects are important.

What could we use as inspiration?

This product can be used as an example of how to build something for a single player. It gives the player a companion who guides him along.

3.1.3. Hack Me 2

Overview

Hack_me and Hack_me2, are two games developed by *EasyWays Team*. While they focus their gameplay on being a gray/black hat hacker, they convey the sense of sitting in front of a computer and doing security-related tasks pretty well in the manner of an engaging computer game. If we followed their approach and built something similar for the individual learning experience.

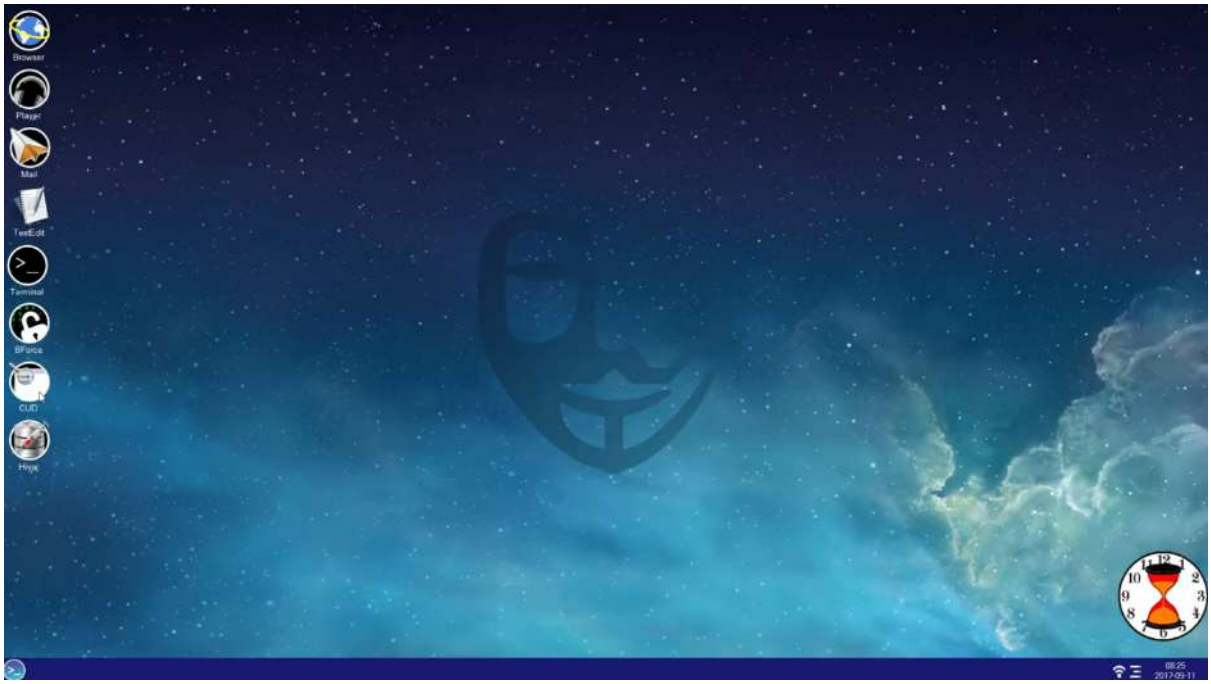


Figure 3.3.: A screenshot of Hack Me 2

How is it played?

It is also a single-player game. The player is presented with a normal desktop environment, in which the user pretends to be using a computer. He then receives tasks that he can fulfill with the tools he has at his disposal. The participant learns some basic Linux handling and terminal skills. He also learns about some possible vulnerabilities and general computer knowledge.

What are the main interactive elements?

The player can interact with a fake virtual machine. He also gets tasks and notifications via an e-mail client to keep him engaged.

What could we use as inspiration?

The game is not directly what we are trying to achieve, so we did not draw any inspiration from it.

3.1.4. The Fugle company

Overview

The *Fugle* company is an educational game about cybersecurity threats that was created by the company *Trendmicro*.

Figure 3.4.: A screenshot of *Fugle*

How is it played?

The player is presented with an interactive movie in which he can choose what he wants to do. He makes choices that influence the gameplay and the outcome of the story. He is continually put into new situations.

What are the main interactive elements?

The player is kept invested by showing him video sequences that display the vital information he needs. The player can actively choose what will happen next and his actions have consequences.

What could we use as inspiration?

I doubt we can do something similar since this was done with a team of actors to create the live-action sequences.

3.1.5. Nova Labs

Overview

Nova Labs has an array of small games focused on cyber security. Mainly conveyed through videos and quizzes, they seem a good source of inspiration to show us how we could tackle this challenge.

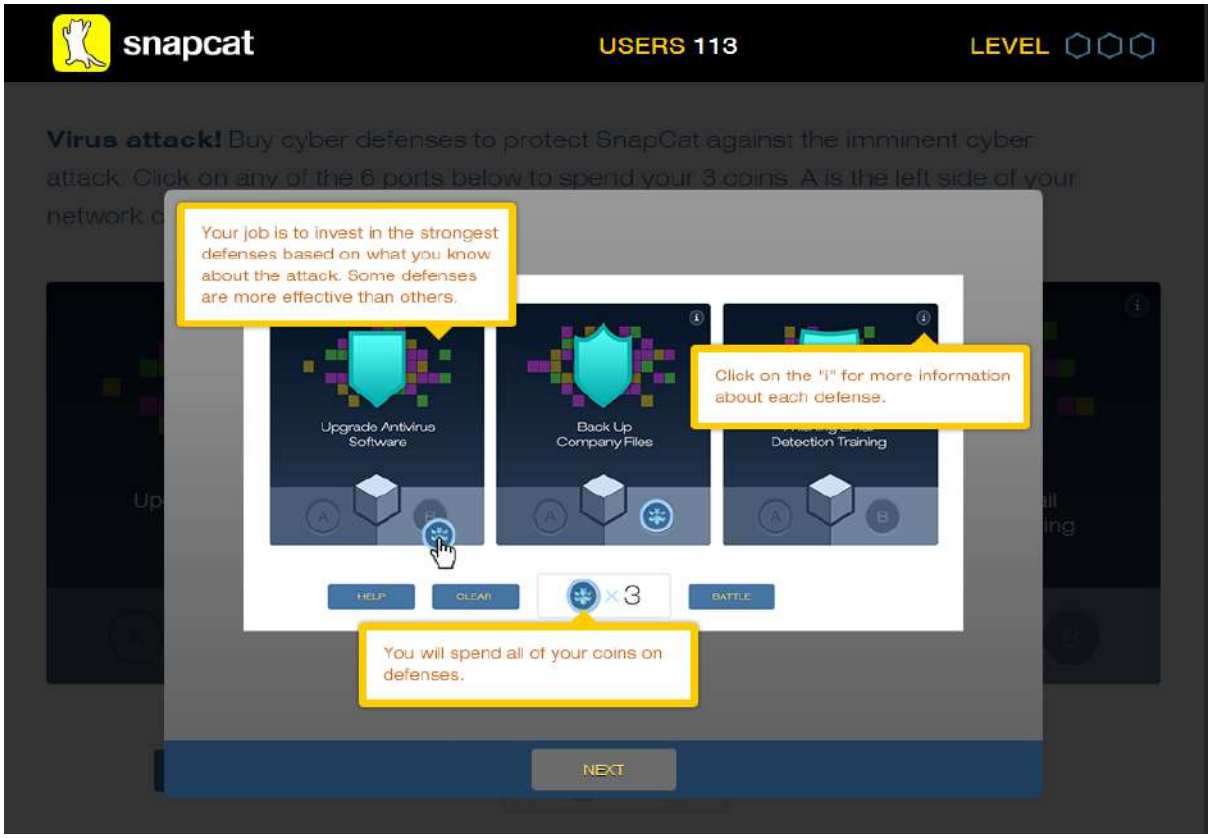


Figure 3.5.: A screenshot of the *Nova Labs*, showing the basic game mechanics

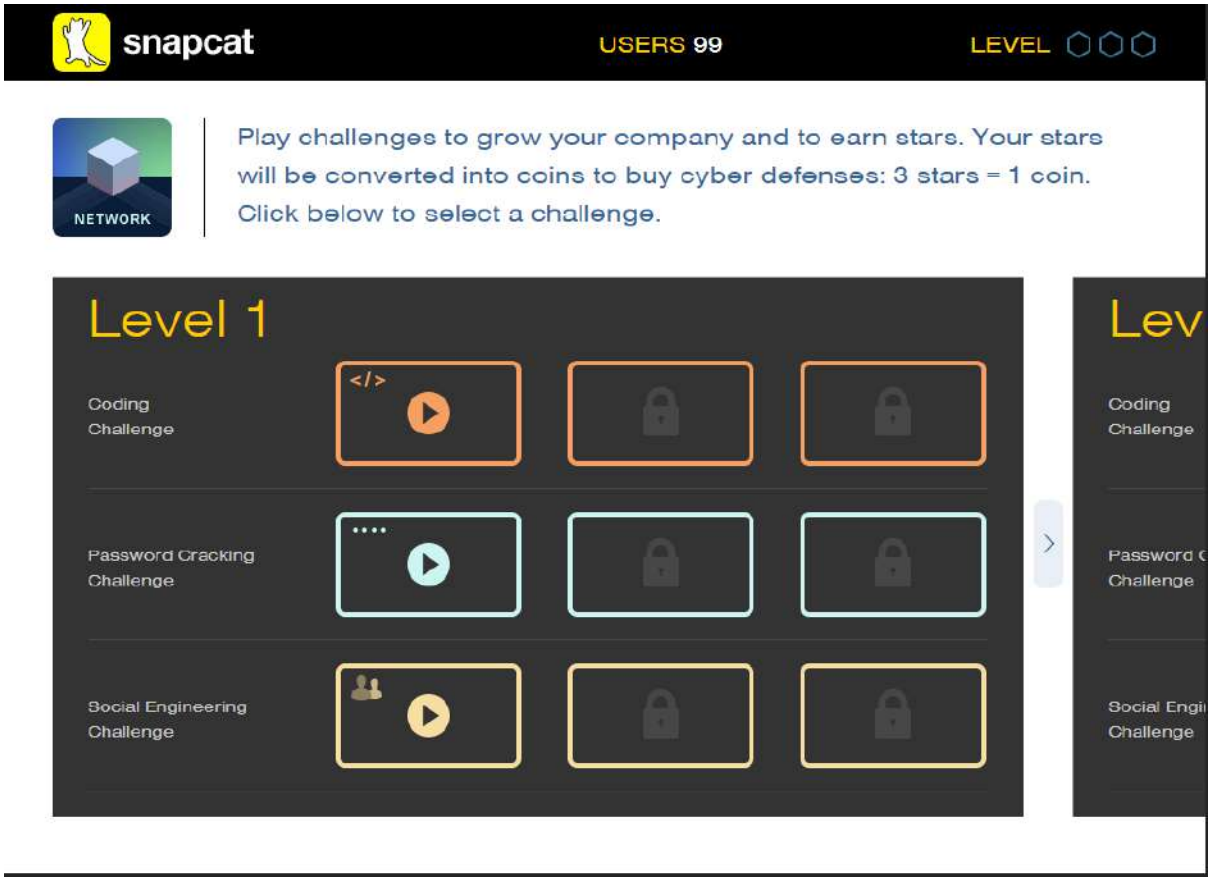


Figure 3.6.: A screenshot of the *Nova Labs*, showing additional courses

How is it played?

The user is in charge of a company. He is then faced with threats, displayed to him via dialogue text boxes. He can choose from three different ways to protect his system but has insufficient resources and needs to choose the best way to defend it from the incoming cyberattack.

The user can then complete small “classes” which teach him about different coding and cyber security skills. He gets tokens to protect his company.

What are the main interactive elements?

The user has to actively choose which mitigations he wants to pick for every attack. He has to do this based on his knowledge, the game does not help him in any way.

What could we use as inspiration?

The game forces the player to find out about threats and choose good mitigations. If he chooses incorrectly, he loses points. We could try to do something similar, where something (a score or something similar) is at stake for the player if he chooses incor-

rectly

Maybe we could let the students who consume additional content have some bonus. Like additional information for the role-playing game.

3.1.6. Cyberescape online

Overview

Cyberescape online promises to be an online escape room, created by living security. We could design our game in a way similar to this approach.

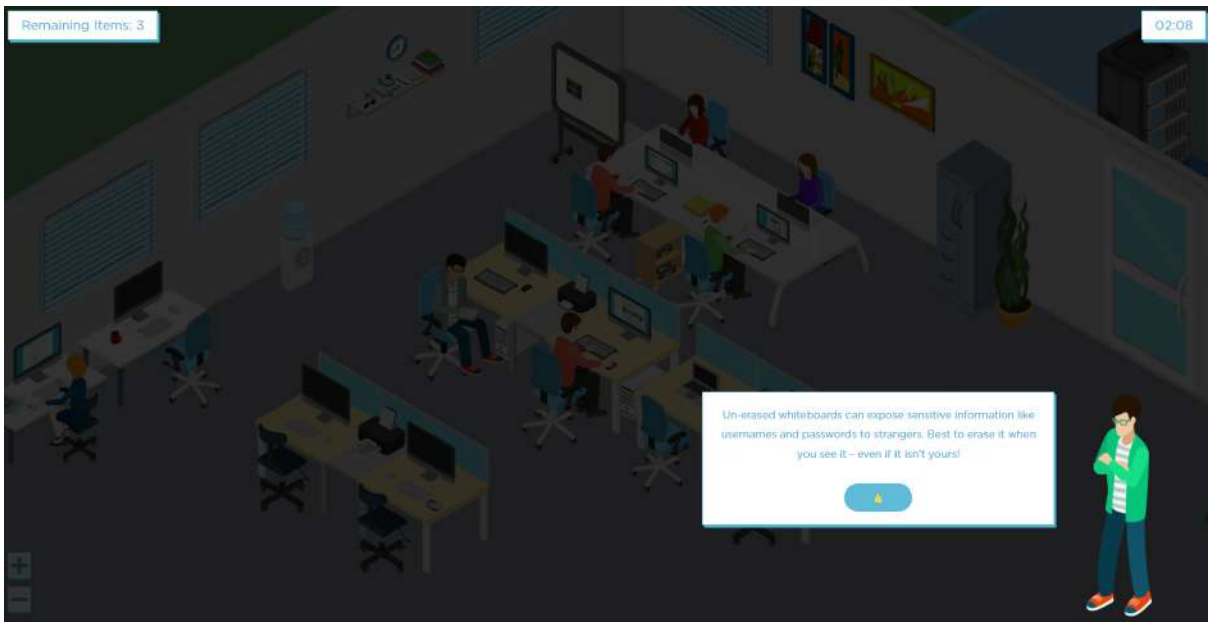


Figure 3.7.: A screenshot of *Cyberescape online*

How is it played?

It is a short interactive point-and-click scenario in which you have to identify security threats. It's similar to a "where is waldo", but more like "where is the security issue".

What are its main interactive elements?

The player is just clicking on a screen.

What could we use as inspiration?

We could create images (like phishing e-mails or log files), in which the participant needs to point out the suspicious behavior.

3.2. Game engines

The game engines were assessed to see if any of them could be used as an underlying framework to carry a possible game of ours. We checked what they offer in regards to functionality and how this could be put to good use.

3.2.1. Conducttr

Overview

Conducttr was proposed to us by Giorgio Tresoldi during the interim presentation, so we evaluated it at a later stage of the project.

Conducttr is a British-based company that has developed a platform for crisis simulations. They offer this platform to their customers on a subscription-based model. Their customers can then use their platform to create scenarios in which they can then put their employees to train and test their knowledge regarding real-life incidents.

You can find their webpage here. We signed up for one of their free demos, in which Marco Zanetti was able to take part in a short presentation of their product. After this, he participated in a demo, in which he could play a malware infection scenario on their training platform.

How is it played?

Conducttr offers an interactive platform that is displayed in your browser. It mimics a “classical OS” which has apps on it, such as an e-mail client, different social media platforms and browsers, some instant messaging services, and some further tools such as a network view of your company. This allows for a real-life feeling and a high grade of immersion when using the platform, as it feels like a normal day at the office. You can see an overview of the screen in Figure 3.8

While the game is going on, the exercise facilitator has an overview screen in which he has an overview of the whole event. He can:

- See a timeline
- Trigger events
- Respond to messages sent from participants
- Oversee every action the participants are taking
- etc.

This allows for a good picture of everything that is going on and gives the facilitator a smooth experience when guiding the game. There can be more than just one

facilitator. This can be necessary, for example, to answer the many messages the participants are sending (these can also be automated by bots).

They also offer a powerful editor to their customers to ease the creation of new events that can then be played out with participants. The supervisor of the exercise has a special overview board to direct and control the whole exercise. It offers an array of different tools and controls to help him to manage and supervise the ongoing exercise.

What are its main interactive elements?

The app offers a variety of different ways to interact. It has different screens with apps mimicking real-world programs. During the demo, we had tools at our disposal such as:

- E-mail client
- Social Media (Twitter, Facebook)
- A browser
- A shared drive
- Instant messaging (Slack, Microsoft Teams)
- A network overview
- etc.

These all helped to feel more emerged in the exercise and made it feel like a genuine real-life workstation. They had two ways of conveying information. The first was a passive way of spreading information, such as posting it on social media or displaying it as articles on media pages in the browser. The second one was a direct way. They showed news videos on the screen or a fake phone call was displayed on-screen with information relaying to the player.

What could we use as inspiration?

Conducttr is not something we aspire to be and is more a tool that is used to convey our content. It is a platform that helps to put user-created stories in a realistic environment on a simulated platform. *Conducttr* itself does not offer this content! The user needs to create the scenarios himself. We can use our generated content and implement it in *Conducttr* to create an amazing simulation for our participants.

Conducttr and SecureRole seem to match in many aspects. We reached out to the *Conducttr* team. They were very kind and offered us a free trial license, to use the full functionality of *Conducttr*. This means we can see if SecureRole content is suitable to be ported onto the *Conducttr* framework.

Because of the time constraints of this thesis we were unable to put it into action during our bachelor thesis. The evaluation is to be evaluated as a post-project exercise.

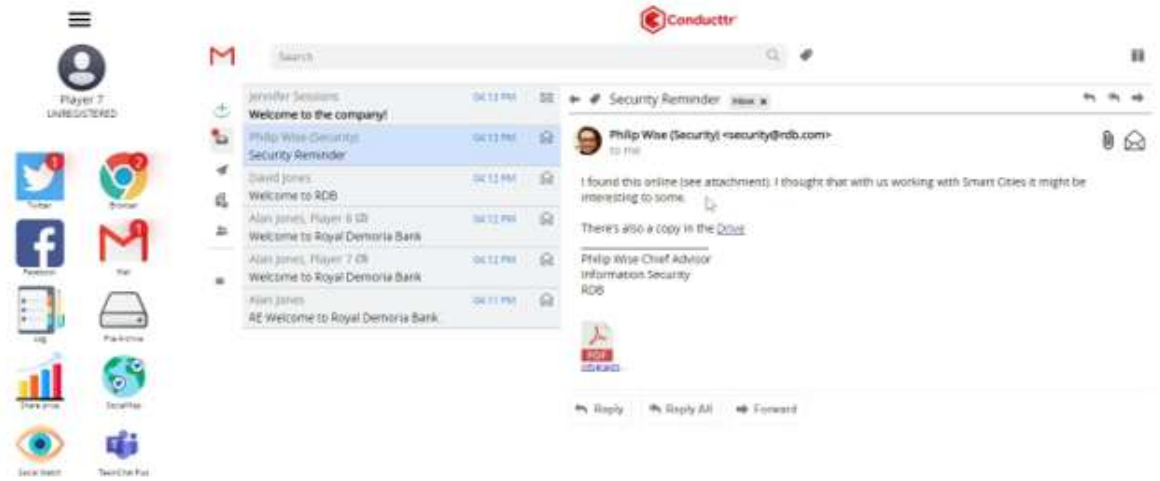


Figure 3.8.: The *Conducttr* user screen, with the e-mail client on display

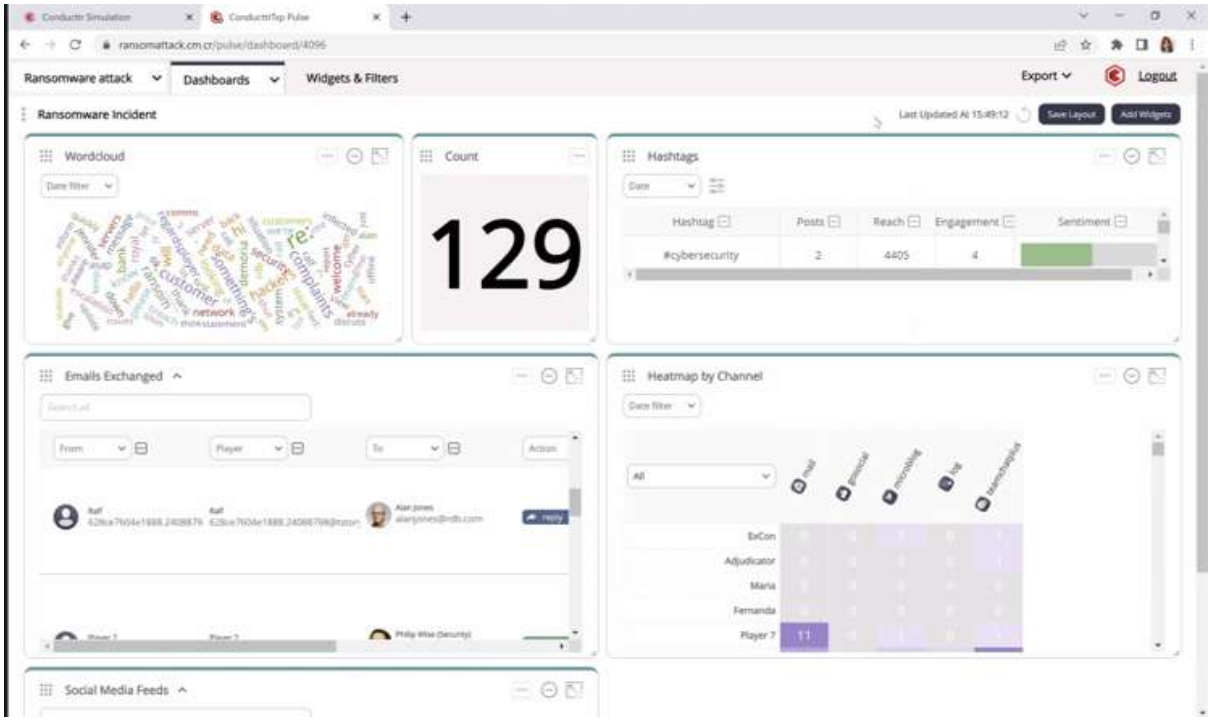


Figure 3.9.: The *Conducttr* admin screen with the key metrics overview displayed.

So which features could we also as an inspiration? Well, *Conducttr* uses a few tools to their advantage we could use in our low-tech setting. One of the most striking uses of a good improvement was the network overview.

The phone calls, e-mails, social media posts, news videos, etc. raining down on the participants create a great sense of urgency and immersion. The player feels like he is in the scenario, rather than pretending to be. If we can add some of these elements to our game, we could increase the immersion and improve the game for our participants.

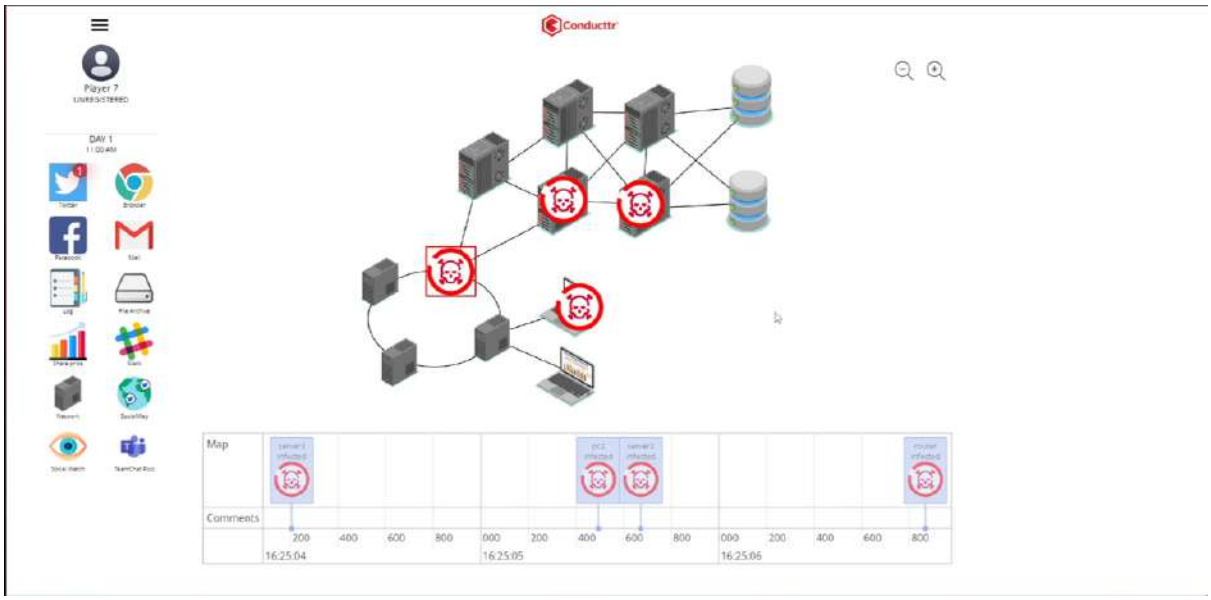


Figure 3.10.: The *Conducttr* network screen

3.2.2. Gameace

Overview

Gameace has this interesting article about the many things we would need to consider before we even try to create an educational game. It also has a list of the most common game engines which are used to create educational games.

What do they offer?

Gameace is a company that specialized to create games for you. They are a team of developers who create games on a contractual basis.

How could we use it?

The article can serve as a good source of information in case we would try to develop our own game. It also offers great insight into the most rewarding aspects of keeping

player interaction high. This could prove to be crucial in creating an engaging RPG.

3.2.3. RPG Maker

Overview

The *RPG maker* is a powerful lightweight game engine that can be used easily to develop small role-playing games. It promises easy to use for creators and minimal coding required.

What do they offer?

They offer a game engine, with a built-in editor. It was created to make older style RPG's with maps to move around, stats to level up, and a combat system.

How could we use it?

It could be possible to adapt our role-playing game into an *RPG maker* game. But the engine surely seems quite focused on older style RPG's, which might not suit.

3.2.4. RPG Playground

Overview

RPG playground is akin to the *RPG maker* but more limited in its functionality since it was specifically made to be a game engine for educational games.

What do they offer?

It also offers a small, lightweight game engine for RPG's.

How could we use it?

RPG Playground offers less adaptability than RPG maker.

3.2.5. YOYO Games gamemaker

Overview

YOYO Games gamemaker is probably the strongest entry in this list regarding the evaluated game engines since it was made to create full-fledged games. But it can also be utilized to make small interactive educational games, such as ours.

What do they offer?

Gamemaker Studio 2 is a powerful engine to create any 2D or even 3D game. It is quite extensive, but still easy to create games quickly.

How could we use it?

It is a quite powerful game engine which can offer us a lot. The question was if we actually could and wanted to sink that much time into creating a game for our users. We decided not to do this since none of us possessed enough knowledge to create something in a game engine like this.

3.3. Role-Playing Game (RPG)

3.3.1. DSA

Overview

Das schwarze Auge (The black eye), is a german tabletop role-playing game akin to games such as “dungeons and dragons”. We took it as inspiration to build something similar but geared towards cyber security with players engaging in security incidents and having to play a character with certain skills and predetermined knowledge. This would force the players to act as a team and solve the problem together. *Das schwarze Auge (The black eye)* furthermore employs a Game Master (GM) who guides the session. This can either be a student as well or a teacher.

What do they offer?

DSA is a comprehensive rule set that was designed for interactive tabletop games. It offers a lot of rules on social interaction and combat.

How could we use it?

We could use its rules for social interaction to create a game-like approach to our content. This could make the whole experience a little more playful and would provide more elements to keep players engaged. We can also extend the rules and use them to create our rule set for a game-like approach to incident response.

3.4. Papers

3.4.1. Paper What.Hack

In this chapter, we summarized what we learned by reading the publication of the paper “What.Hack”(pronounce what dot hack)[2]. It’s a role-playing phishing simulation

game that simulates a real situation by mimicking a company.

This paper was suggested to us by Mitra Purandare during the interim presentation and was thus evaluated at a later point in the project.

Summary of *Introduction*

This section states the cause for this paper, mainly with the US Election of 2016, and shows different reasons for creating a new platform. It proposes *What.Hack* as a solution to mimic a company and to teach the user about phishing e-mails by creating puzzles.

Summary of *Related work*

The authors want to clarify that training programs that typically emphasize the reading of theoretical materials aren't as efficient as game-based learning. In the following table, they show which designs exist for different game-based cybersecurity training designs:

Game Type & Examples	Description	System Attack	URL Phishing	Spear Phishing
Board Games [28, 32, 49, 57, 62]	Teach high-level security concepts.	✓	✓	✓
Capture-The-Flag [3, 16, 18, 47, 52, 64]	Let coders compete for scores by defending their systems and hacking others'.	✓		
Sys-Attack Sim RPG [2, 6, 20, 58]	Teach players to defend against computer system attacks in a realistic system attacks simulation game.	✓		
Non-Phishing RPG [14, 44, 56, 67]	Teach players to identify phishing URLs in a cartoon-like game without phishing attempts.		✓	
Phishing Sim RPG *What.Hack*	Teach players to defend against URL and spear phishing attempts in a realistic phishing simulation game.		✓	✓

Figure 3.11.: Game-based Cybersecurity Training Design Comparisons [2]

For a further explanation of the designs, please read chapter 2 in the paper [2].

In the last section of this chapter, the author writes that the product *Anti-Phishing Phil*[1] has the needed elements for pishing training. *What.Hack* has all the elements of the anti-phishing design, but also has the aspects of the real word phishing design.

Summary of *Gameplay design*

What.Hack has the following primary learning goals:

1. Teach e-mail phishing defense in context by replicating as many real-life conditions as possible.

[1] A video game which was also aimed at detecting phishing e-mails.

2. Engages the player by setting clear goals and tasks that become more difficult over time.
3. Provide immediate feedback about the consequences of decisions the player makes.

Situational learning consists of rules that give the user/player the constraints on how to act on phishing e-mails. Besides the rules, a user also sees directly what he was missing or which important aspects he misjudged in the simulation. Instant feedback helps to learn more efficiently.

It simulates the e-mail processing context, including the user following a workflow, it adds pressure to finish within a given time frame, interacts with the IT support and shows the harmful effects of phishing.

It mainly focuses on three types of phishing attacks:

1. Similar domain attack: The domain is very similar to the one of a legit e-mail domain.
2. URL Manipulation: The URL is manipulated to make it look like a legit e-mail.
3. Malicious attachments.

The User has to perform different shifts and in each shift new rules are introduced, which allows for a progression during the learning process.

Shift 1	Allow emails from Trusted domains Block emails from Unsafe domains Block emails masquerading as Trusted domains
Shift 2	Block any email with inappropriate content Block non-business related emails from unknown domains Allow business-related emails from unknown domains
Shift 3	Block emails that contain hyperlinks to unknown or suspicious URLs
Shift 4	Block all emails with attachment with the following file types: EXE, COM and HTML Block all emails with ZIP attachment that is not from a trusted domain
Shift 5	Block all emails with DOC attachment that is not from a trusted domain but DOCX attachment is acceptable Ask IS advisor about emails from unknown domains that has a business-related attachment

Figure 3.12.: Game-based Cybersecurity Training Desing Comparisons [2]

Summary of *Performance Evaluation*

The study was undertaken with students from the campus of Cornell, with the preconditions being that they have to be older than 18 years and have never done any cyber security lessons or training.

What.Hack was compared against, *Anti-Phishing Phil* and *PhishLine*[2]. The participants had to do a pre- and posttest with an e-mail that they had to analyze.

The participants then had to choose if an e-mail is legit or phishing and how confident they are about the choice (rating their confidence on a scale of one to five). This was done for eleven phishing e-mails and nine legit e-mails. After the test, they had to answer the following questions:

- What is the strategy you used to process these e-mails? Please write in bullet points.
- Did you learn any new concepts or skills from this training that will help you prevent yourself from being hacked by unsafe or phishing e-mails? Please write in bullet points.
- On a scale from one (very boring) to five (very engaging), how would you rate

[2]Which are both gamified approaches to learning about phishing e-mails

the engagement of each training?

- On a scale from one (strongly disagree) to five (strongly agree), how likely are you to recommend this training if your friends want to learn to defend against attacks from phishing emails?

The Results were as following:

Figure 3.13.: You can see how the participants faired in correctly identifying the phishing e-mails before and after they were trained with one of the three products(which is here displayed in a percentage of correctly identified e-mails). *What.Hack* was the only one to offer a substantial increase in the correct identifications of phishing e-mails.

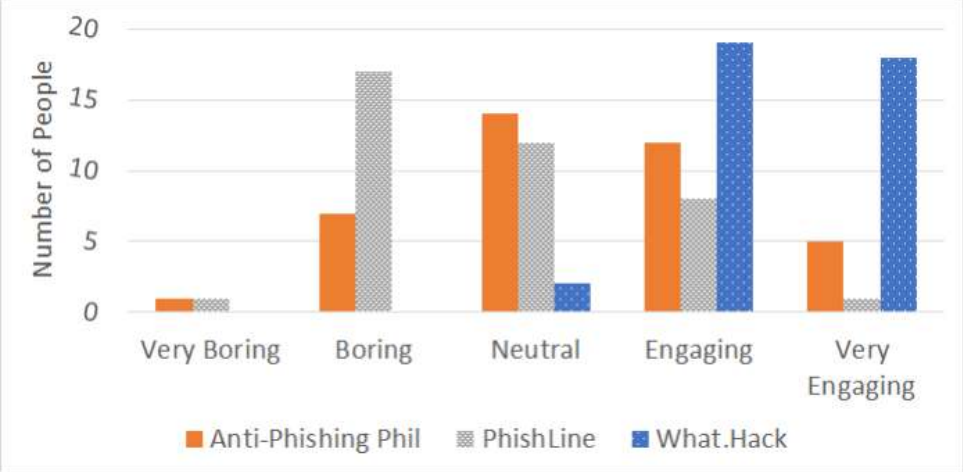


Figure 3.14.: In the engagement ratings, 95% of the participants find *What.Hack* being engaging or very engaging. While only 44% rated Anti-Phishing Phil in the same brackets, and only rated 23% PhishLine accordingly. [2]

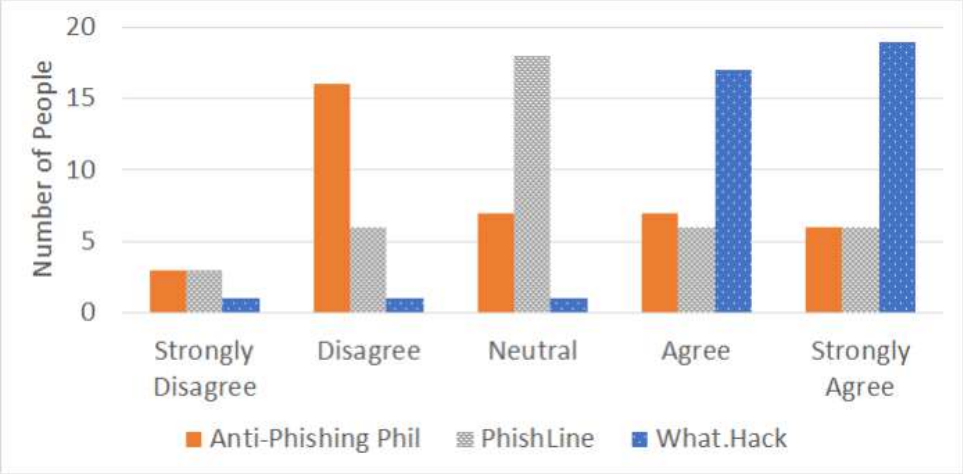


Figure 3.15.: The rates to which the participants would recommend using the different application to others.

Summary of *Discussion*

They offer interesting discussion points in their paper, in which they highlight the main pros and cons of their product.

- In comparison with the other compared games, the game includes a better real-world scenario and is more focused on the threats.
- The game has a limitation of social engineering attacks.
- The game is a good starting point for other cyber security games.

Summary of *Conclusion*

> We presented results from a lab study demonstrating that *What.Hack* improved players' correctness in identifying incoming threats by 36.7%, whereas a control group that played a different game did not achieve a statistically significant improvement.[2]

4. Game Type

This chapter looks at the process of choosing the correct game type for our product. But first of all, what do we mean when saying “game type”?

The “game type” describes what kind of game we strive to provide for our participants. We divided this question up into four categories:

- Medium of the game (Which way will it be played?)
- Game type itself (solo, multiplayer, group)
- What is the player’s goal?
- How do we keep the players engaged?

4.1. Process

To produce an array of choices for our game, we decided to gather ideas by brainstorming. We drew up an array of ideas for all of these categories, which we then combined into one big mind map, decorated with many post-it notes. You can see this in the following mind map.

After this, we decided, which of these ideas we wanted to include, by coloring them with the following key:

- Yes: green
- Maybe: yellow
- No: red
- Only in additional documents: blue

4.2. Previous research

Some of the ideas used in this mind map were inspired by the content of the two previous chapters. This allowed us to propose being were educationally valuable, fun and engaging mechanics have seen in other games.

4.3. Result

With the conducted research as a cornerstone, we managed to create a satisfactory mind map. It contained many ideas for all branches which we deemed interesting for a possible game. The mind map clearly shows that we had many ideas, some unconventional, but also aware of not being able to include all of them in the game. That was the purpose of the coloring phase. To make sure we only picked aspects, we were confident served a purpose and were able to be implemented in time. It might look slightly conservative right now, but we kept the option open to adopting this mind map at any time.

Our current game would be a “classical” role-playing game. It would provide character sheets to all players with their role inscription on them. The game master role, which is strongly advised to be played by an educator or teacher, will guide the students during the session. He receives additional information

The game will be played in a group of players, who all work together to solve an issue presented to them. The attacker may be also part of the group itself.

The main player’s goals are:

- Detection (Detect the issue)
- Containment (Uncover the extent of the incident)
- Recovery (Restore the system to normal operations)

To keep the players engaged, the game will include the possibility to make decisions to influence the gameplay. The decisions will have consequences. While the scenario will result in the same end goal (eradicating the threat) the participants can take many different ways to get there.

4.3.1. Documentation

While this document is perfectly fine for documenting our findings and the process we took to achieve them, we need to persist in the concrete goals we wish to achieve with this. For that reason, we worked all of these decisions into our use cases[1] (UC). The proposed ideas discussed here mainly influenced UC 1 and UC 1.1. This allowed us to extract measurable goals which we could try to achieve with our product.

On the following pages, you will find a figure with a small overview of the mind map we created, and each branch separately in a close-up, for improved readability.

[1] You can find the use cases in the project documentation in chapter 19

Secure Role

Player goal

Prevention

Detection

Human Firewall

Containment

Uncover the incident as fast as possible

Contain spread as good as possible

Prevent lateral movement

Time based

Action based

Revocery

Recover to normal operation

Achievement

Gain maximum points

Achieve good grade

Win something

Getting extra hints

Get achievements

Punishment

If breach is not contained

Fun fact about student is shown to class

Attackers wipe tracks

Student must advertise college on social media

Contain breach too fast (sloppy)

Player interaction

Make decisions

Decisions have consequences

Branching stories

Multiple ends

Show consequences of a choice

Progressive Story

Story over several weeks

Additional escalations for Game Master

Tips offered based on the difficulty of the game

Procedural

Random Events

Random generated threat sequence/spread

Real world scenario

Mimic an actual past attack

Speak with real Incident Reponders

Win something

Unlock extra content

Get achievements

NIDS but the player has to detect things

Recover to normal operation

Prevent sensitive data from being oncovered

Prevent attacker access from getting maintained

Prevent privilege escalation

RE with real maleware

Progressing threat

Speak with real Incident Reponders

Show consequences of a choice

Real word scenario

Mimic an actual past attack

Random mishaps occur

Attacks outreach is procedurally generated (eg python script)

The story master can add additional tips or escalations so the story continues

Story overall serveal weeks

Story adapts to players knowledge

Tips are offered based on the difficulty of the game

Game type

Difficulty

Depending on experience

Players

Single

vs Bot

Prefabriacted

Multi

Group vs Group

Group exercise

Red vs Blue

Adhere to cyber kill chain

No random choices

Start with a tabletop material, with three different scenarios grouped by difficulty

Group vs group competition

Single vs Bot

Medium

Paper

"Normal" RPG

Tabletop pen and paper RPG

Boardgame

Classic Exercise sheets

Computer

Game

Sandboxing

Malware sandboxing

Tool usage

Real time chat

Attacker can read everything

Card game

Sound

Voice Lines explaining game

Movie

Video introduction to scenario

Link additional material

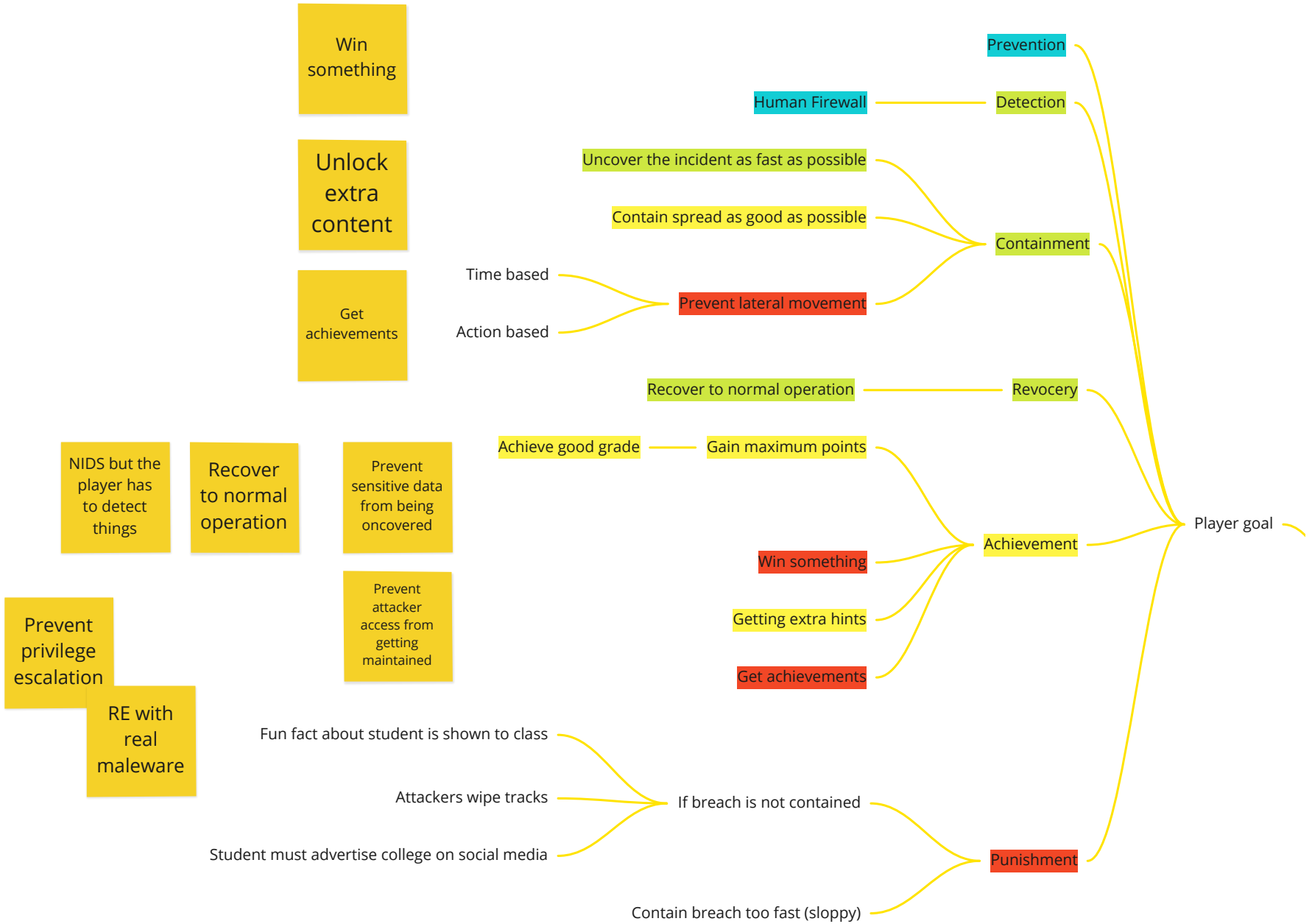
Groupchat on discord / Teams

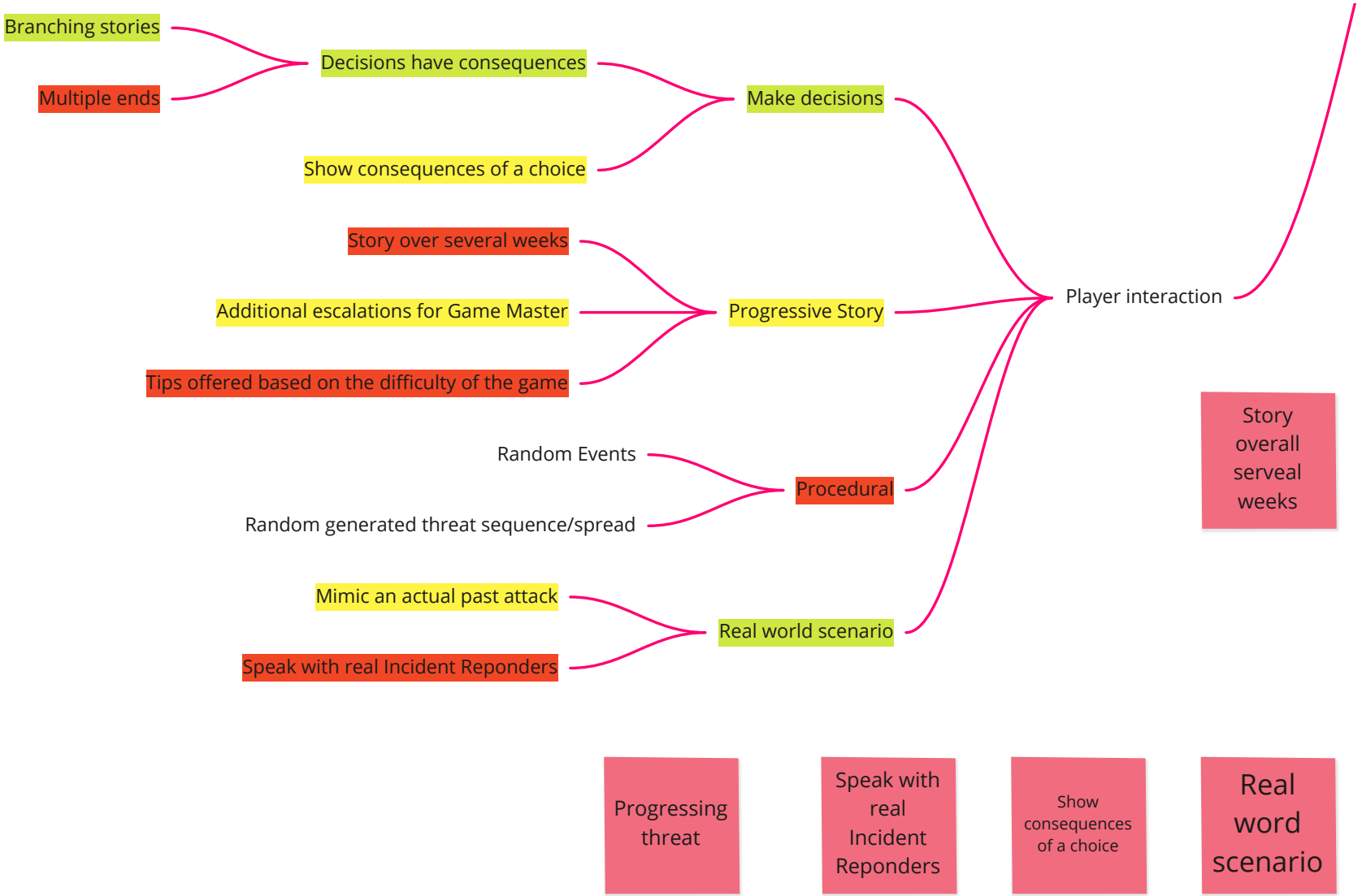
Interactive voice recording

Classic exercises

Acting with real word tools

Movie snippets


Win something
Unlock extra content
Get achievements
NIDS but the player has to detect things
Recover to normal operation
Prevent sensitive data from being oncovered
Prevent attacker access from getting maintained
Prevent privilege escalation
RE with real maleware
Prevention
Human Firewall
Detection
Uncover the incident as fast as possible
Contain spread as good as possible
Containment
Time based
Action based
Prevent lateral movement
Recover to normal operation
Revocery
Achieve good grade
Gain maximum points
Win something
Getting extra hints
Get achievements
Achievement
Player goal
Fun fact about student is shown to class
Attackers wipe tracks
Student must advertise college on social media
If breach is not contained
Contain breach too fast (sloppy)
Punishment


Branching stories
Multiple ends
Decisions have consequences
Show consequences of a choice
Make decisions
Story over several weeks
Additional escalations for Game Master
Tips offered based on the difficulty of the game
Progressive Story
Random Events
Random generated threat sequence/spread
Procedural
Mimic an actual past attack
Speak with real Incident Reponders
Real world scenario
Player interaction
Random mishaps occur
Story overall serveal weeks
Attacks outreach is procedurally generated (eg python script)
The story master can add additional tips or escalations so the story continues
Progressing threat
Speak with real Incident Reponders
Show consequences of a choice
Real word scenario
Story adapts to players knowledge
Mimic an actual past attack
Tips are offered based on the difficulty of the game

Game type

Difficulty — Depending on experience

Players
- Single
  - vs Bot
  - Prefabriacted
- Multi
  - Group vs Group
  - Group exercise
  - Red vs Blue

Adhere to cyber kill chain

No random choices

Start with a tabletop material, with three different scenarios grouped by difficulty

Group vs group competition

Single vs Bot

Link additional material

Groupchat on discord / Teams

Interactive voice recording

Classic exercises

Acting with real word tools

Movie snippets

5. Creation

5.1. The process

After we had completed all research we had considered it necessary to create a Minimum Viable Product. We had researched educational methods, had looked at other ideas that had already been used to teach about cybersecurity playfully and had agreed on how our game would look. At least in theory.

We were almost ready to start building our first role-playing game prototype. But we lacked a topic. So we drew up a Kanban board and listed all possible topics which we wanted to tackle as a team. We chose the ones we deemed the most interesting and got to work. Our choice fell on “OSINT, Phishing and Ransomware”.

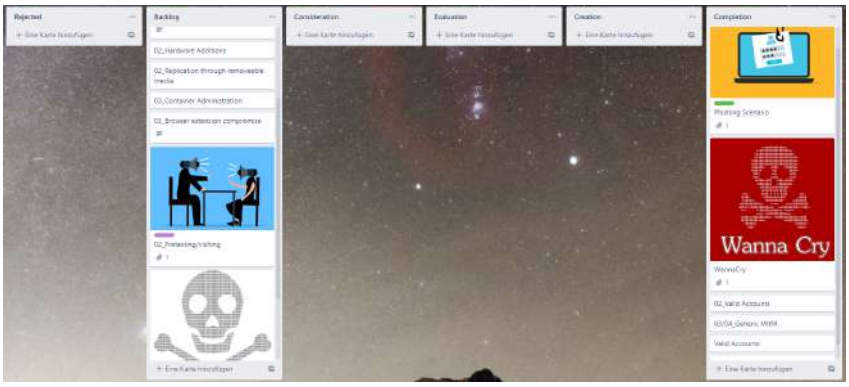


Figure 5.1.: A screenshot of the topics board at the end of our project

5.2. The product

5.2.1. The game

So what did we achieve?
We created a game allowing participants to react as a team to a security incident. This meant creating the character sheets for each participant, strongly inspired by tabletop games[1]. Also a comprehensive guide for the so-called Game Master (GM), the

[1] The character sheet in a tabletop game usually contains multiple pages and serves as an overview over the character a player will impersonate during a tabletop game. This includes this character’s name, abilities, knowledge, etc. . .

role being taken by the teacher. His main responsibility is to facilitate the game and help the participants by guiding them along and making sure they interact with each other. He is also responsible to track their progress and making decisions regarding the scenario if questions should arise. We also needed to come up with an imaginary company, that includes all characters, to have the role-play be set in a realistic simulated environment where the attack could take place.

5.3. How do you play it?

The main part of our product is the game itself. The GM reads the description of the incident being layed out in front of him on a continuous storyboard consisting of different events. He familiarizes himself with the help of the Game Master document and prepares the game for the students.

The participants then receive their character sheets being an introduction to the role they will enact during the tabletop role-playing game. They have time to familiarize themselves with who they are, how they should behave and what their duties are. But they do not receive any information about the threat itself.

Then everybody gathers around (either online or in-person) and the game begins, just like your normal tabletop role-playing game. The Game Master introduces the players to the game, and the players start engaging with each other. But instead of slaying dragons and haggling with townsfolk, our players will combat an emerging cybersecurity threat. They try to contain and eradicate any ongoing infection and restore their system to normal.

5.3.1. Further content

While the basic game was our main goal we also wanted to provide more to students and teachers, so the educational benefits would be more than simply an incident response game. We made sure to include more to a well-balanced learning experience. Including the following topic:

- Slides, a teacher can use to give a lecture
- Scripts, the students can read to gain a deeper knowledge about the topics
- Additional materials such as podcasts, articles, reports, videos and more, allowing the students to widen their knowledge of interested topics

So all in all, our product offers a comprehensive learning experience for everyone interested in cyber security!

6. Alpha testing

It was always a big priority to gather continuous feedback throughout the project. We aimed to test regularly, but due to time constraints, we only managed to test twice throughout the project. This was mainly due to the time it takes to prepare a test and to integrate the feedback into the product.

This chapter gives an overview of the first test conducted. It was conducted shortly after the first prototype was finished.

6.1. Test Procedures

To test and verify the quality of the role-playing game we developed and also the quality of the material we created, we conducted usability tests. During the elaboration phase and also still during the construction phase, we assembled a group of testers who agreed to participate in the testing of our product. The idea when gathering the testers was to get IT students from different schools so that we would have students with differing levels of knowledge about the topics we were covering in our material.
We also asked Weiler Nathalie to participate in the testing. She assured us to be constantly reviewing the material. The first part of the tests began when the first role play was created.

6.2. Review Procedure

The documentation and material collected by the group members are read by at least two group members using the merge requests[1]. For each merge, there is a reviewer and an assigner who creates the merge request. Comments and suggestions will be added to the documentation from the reviewer as seen as necessary.
After the review is completed and the comments/suggestions are added to the document, the branch is merged with the development branch and then deleted[2].

[1] A merge request is a GitLab feature that allows the creation of different versions of a document. They can then be merged through a review process.
[2] If you want to know more about our processes, please read about our quality assurance in chapter 17

6.3. Introduction

The purpose of this subsection is to provide a summary and overview of the results of the usability test conducted with selected users. This means that the results shown below are a summary of all four test documents completed by the test candidates.
The users were asked to play the first version of the role-playing game, about phishing, while the observers watched the game and took notes about the whole process.
The main goal of the tests is to find out if the users had any difficulties or problems while playing the role-playing game and if they were satisfied with the final result of the product. The feedback and recommendations from the test participants were incorporated into the product.

6.4. Background Summary

We tested the role-playing game we created for phishing. In general, four candidates agreed to take part.
Before the test began, each candidate received an email with a character sheet description and the test document they needed to fill out. The test was held online on 7.4.2022. The moderator of the game, Anina Bytyçi, who was also the supervisor of the test, used the Game Master document the whole time to make the game easier to manage and moderate.

6.5. Methodology

The players were left alone to play their roles and find a solution to the problem they were facing. When the game was not moving forward or the players were repeating themselves, new hints or instructions were given by the moderator.

6.6. Test Results

As mentioned above, each candidate was given a test document to complete after the role-playing game.
The test session lasted 65 minutes and the role-play game 55 minutes. In the end, the team managed to find a solution to the problem and there were helpful discussions during the role-playing game.

6.6.1. Pre-Testing

Following you will find the average of all questionnaires filled out by the participants combined into an overview.

1. Phishing knowledge:

- ☒ ++
- ☐ +
- ☐ 0
- ☐ -
- ☐ –

2. Ever played a role-playing game before:
   - ☐ +
   - ☒ 0
   - ☐ -

6.6.2. During Testing

1. Read character description:
   - ☒ The text was understandable, the user knew what should be done.
   - ☐ The text was comprehensible, the user had questions about what was to be done
   - ☐ The text was not understandable, the user had no idea how to proceed
2. Game situation
   - ☒ Understandable and interesting
   - ☐ Understandable but not interesting
   - ☐ Not understandable and not interesting
3. Hints and instruction from the Game Master
   - ☒ Clear and helpful
   - ☐ Clear but not helpful
   - ☐ Unclear and not helpful

6.6.3. After Testing

1. Are the character sheets understandable?
   - ☐ ++
   - ☒ +

- ☐ 0
- ☐ -
- ☐ –

2. Is the game situation understandable?
   - ☐ ++
   - ☒ +
   - ☐ 0
   - ☐ -
   - ☐ –
3. Helpful hints and instructions were given from Game Master
   - ☐ ++
   - ☒ +
   - ☐ 0
   - ☐ -
   - ☐ –
4. Better understanding of phishing as a topic after playing the game
   - ☐ ++
   - ☐ +
   - ☒ 0
   - ☐ -
   - ☐ –

   Comments: The users were already familiar with phishing

5. Any problems during testing? Comments from users:
   - Was not clear how big the company is (amount of employees)
   - There was nowhere mentioned how big the max. budget is to be able to pay
6. A new feature could be added:
   - a CSIRT role

- Time based/triggered events (e.g. after deciding to ask a CSIRT the team gets the information that ...)
- Additional information about some topics that were mentioned in the game: I did not really remember what WannaCry malware was.
- More information about OSINT since it sounded really interesting.
- Add more information about the attack in the documents
- Add more information about the malware, not only phishing

7. Features that were interesting for the users:
   - The challenge is to find the best solution possible and to find the right words
   - How we approached the solution was quite interesting
   - The whole role-play was really interesting, the way how we discussed about finding a solution

8. Improvement recommendations from users:
   - To explain from the beginning that there are just two department (IT and Accounting)
   - Indicate if the company has an internal, hybrid or external CSIRT (or none at all)
   - More information from the moderator to give more directions to the play
   - In the character sheets tell what it is really important to remember from the role. Because we kept forgetting how many employees are in the company, and how many departments there are
   - Explain how employees there were
   - Explain more about the malware, so the user knows what it is.
   - Explain on a technical level, how can the whole department be infected by that malware

9. Additional comments
   - The role-play was interesting and clearly pointed out the damages of mail phishing

10. Discussions after testing:
    - The possibility of replacing the names of the players with the expressions

player 1, player 2. After the acceptance test it is decided which variant is better.

- Highlight the most important information from the character sheet with a cheat sheet so users can identify what was important. For IT staff, the infrastructure of the company will be portrayed.
- Game Master document will be edited. Define the budget of the company.
- Add OSINT material and malware material to the additional material document.

11. Documents to be edited after testing results:
    - Game Master document
    - Character sheets
    - Additional material document

7. Teacher Feedback

As previously mentioned in chapter 2 we received help during our bachelor thesis from Anja von Rotz. She agreed to review our work from a teacher's point of view and tell us how we could improve it to enhance the educational experience.

7.1. Scope of the review

Anja's review consisted of how we conducted the game itself. She had access to the game master document and the character sheets. So she could see it from the teacher and the student's position to give us feedback regarding those two roles.

7.2. Suggested Improvements

The suggestions in this section are directly aimed at the role descriptions of the player and the game master file.

Performance expectations:
One of the first things she noticed, was the lack of "Transparent performance expectations". While you can see in subsection 2.1.6 that we have added this issue in the meantime, she pointed out that it is crucial to include them in every course to make sure that the students know exactly what we expect from them at the beginning of the exercise. This helps them to set a clear goal for themselves and maximizes educational value.

Company Overview:
The next thing she mentioned was the character sheet wasn't exactly clear on how the company was structured and how the different participants would fit into it. It should be more clearly addressed how the company hierarchy looks like and what role each participant plays in it. We have already addressed this issue with the creation of an improved overview that shows all participants what they need to know about the company on one page.

Add the company overview for the GM
One of the most important aspects of a good lead in the game is that the teacher is

supplied with all the crucial information he needs. So we should include the overview for the company in his file as well.

Increase interaction for students
While the role-play in itself is already a good interactive experience in a changing environment, we could increase the interactivity of the game further. This could be done, for example, by adding an actual infected VM with a sample of the malware to show students exactly what it looks like. More interactive media is good for an increased learning experience and enhances the learning environment. We will check if this is feasible for our use case.

7.3. General Questions / Suggestions

The suggestions in this section are more general and affect the whole game.

How is the game prepared and how is the game reviewed?
The preparation and review of the game play a big part in the learning process for the students. It's important to ensure that these two phases are well described for the participants and the teacher. Instructions are included for the roles during the game. We could include instructions on how the participants should prepare for their roles. While the game master document already describes how the teacher should prepare, there should be a retrospective for the students to reflect and learn after the game. Our current description is not sufficient.

Bloom's taxonomy
Another important aspect that Anja von Rotz brought into our work was *Bloom's taxonomy*. For anyone unfamiliar with this term (such as ourselves) let us elaborate. Bloom's taxonomy is the distinction of the learning progress into different levels. It is usually represented in the form of a pyramid with the stages stacked on top of each other. You can see this pyramid in Figure 7.1

The idea behind the pyramid is that the better a student understands a topic and the further he progresses on his learning journey, the higher he climbs on the pyramid. We need to help move the participant as many levels upward as we can. Anja von Rotz's comments regarding these are as follows:

- Create & Evaluate: Reflection on how the game went and what the students learned during it. Reflect with them and help them if different approaches or further learning would improve their understanding of the topics.
- Analyze & Apply: This is done during the game by the students and should be mentioned during the retrospective.
- Remember & Understand: This has already to be present before the game starts. Students can't be thrown into this without any preparation regarding the mentioned topics.

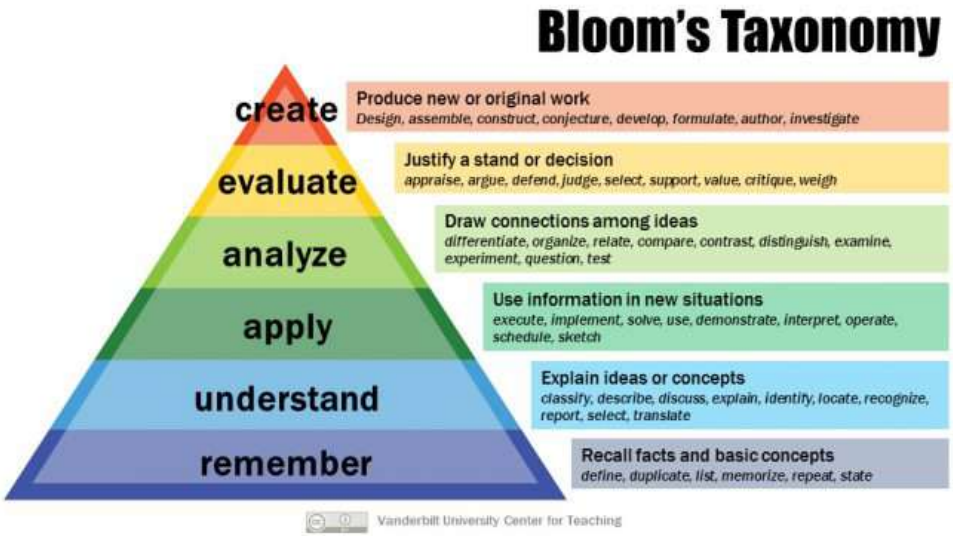


Figure 7.1.: Blooms taxonomy [3]

Let's quickly discuss what that means for us regarding how we can implement these suggestions into our game. Please note that we split "Remember & Understand" into two separate sections since we see different aspects of our game apply to these topics.

Create & Evaluate:
We will need to provide clearer instructions on how a retrospective of the game should take place to maximize the learning support.

Analyze & Apply:
This is already addressed during the game, no need for further improvements here.

Understand:
While Anja von Rotz correctly stated that this should fall into the category of "Requirements before the game" we think that our game can still add to this. The students understand the topic and its different aspects. We can offer a direct display of certain aspects, that is increasing the understanding of the students. One example is the consequences that a phishing e-mail can trigger. Our game shows that such a small incident can provoke wide damage to a company if it is not handled correctly.

Remember:
Since this already needs to be present before the game, we needed to ensure that the responsible teacher knows after this. He either needs to give a lecture about the topics used in the role-playing game, or he needs to instruct the students to read the scripts beforehand. If this is not the case, it could hamper the learning efforts during the game, since the participants will be overwhelmed by all the new information. This can reduce learning success and jeopardizes the goals of our game!

We introduced materials, such as the scripts, the slides and the additional materials, to help with the topic. We structure these in such a way that they are most beneficial to the learning of the students.

8. Interim Presentation Feedback

After we had concluded our alpha test, we went to the next step of the interim presentation for all our examiners (Weiler Nathalie, Mitra Purandare and Giorgio Tresoldi[1]). It serves as information for them to evaluate the work progress. The goals were to have feedback and allow us to prepare for the final presentation.

The presentation lasted thirty minutes and was followed by a discussion and feddback section. Below is a list of received feedback sorted by person.

8.1. Mitra Purandare

- *We should talk more about our product and less about the process involved to create it during the presentation.* The documentation can be used to talk about the process. (Which we are doing right here)
- *While the first round of testing was well executed and yielded good feedback we need to ensure for the second round that we define metrics on how our game helps students and teachers.* We did this using questionnaire, but more about that in section 10.3.
- *And how can we assure that all participants have the same learning effects during the game? Or asked differently, how do we avoid roles not part of the decision making have a smaller learning experience?* We tried to tackle this issue by analyzing this factor in the second test.

8.2. Giorgio Tresoldi

- *Make it clearer what your product is (we called it a phishing malware game during the presentation) and call it something along the lines of an "Incident response tabletop role-playing game".*
- *It is also important to clarify to our customers that our product does not encompass any software written by us.* We solely provide the content for a possible software adaptation.

[1] Mitra Purandare and Giorgio Tresoldi participated remotely in the presentation.

- *We need to show how we plan on making our product scalable*[2].
- *We should check out Conducttr, a framework for simulating incident response type scenarios with an immersive virtual environment.* This is worked out in subsection 3.2.1.

8.3. Weiler Nathalie

Weiler Nathalie had little feedback to add at the end of the presentation itself. But upon discussing our findings regarding the feedback from Anja von Rotz from chapter 7, she offered us additional advice regarding educational strategies:

We should check our materials for even distribution between the three "main stages" on Bloom's taxonomy. This means that our materials should not contain more than 30% "Remember" (Definitions, Abbreviations, things to learn by heart, etc.), not more than 30% "Understand" (Comprehensions, advanced explanations, examples), and roughly 40% or more from all four other levels "Analyze, Apply, Create & Evaluate" (Which contains everything that the student actively does to deepen his knowledge by practical and interactive means). We should strive to ensure that all our documents in combination as a whole roughly strive towards that aspect. We know that not all documents will have the same distribution (A storyboard will have almost no remember, while a script has more than 30%) but we should try to meet this metric as a whole. It will not be possible to exactly measure this, so we will rely on the feedback from our acceptance testing to see if we achieved a well-rounded learning experience.

8.4. Conlusion

The interim presentation showed us and our examiners we were going in the right direction. The feedback provided by them gave us the most important objectives to pursue. We identified them as:

- Make sure the product has increased scalability.
- Ensure a good experience for all participants.
- And get the most out of testing.

[2] At this time we already had an idea on how to do this at this point but were not confident enough to show. You can find it in chapter 9. with the new framework "SecureRole Flavors"

9. SecureRole Flavors

This chapter will provide an overview of the newest addition to our thesis and subsequently to “SecureRole”.

Figure 9.1.: The SecureRole Flavors Logo

SecureRole Flavors

A new concept on how the content will be structured and combined to create the best combinations for our users!

9.1. Why Flavors?

Flavors is a new addition to SecureRole that aims to improve in many different aspects. Nothing will change regarding the basic idea of SecureRole. We will continue to provide free educational materials by creating tabletop incident response exercises for students and teachers. The core of the game will remain the same.

Everything about the way we develop, share, combine, and deliver stories to participants will change. Until now, when playing a game from SecureRole the users had

to pick one of the fully-fledged scenarios that are offered on Github. This was before Flavors was introduced in the “MalwarePhish” story.

What if our users wanted to play a phishing game without the malware part? The storyline for a game would be incomplete and only the phishing part would be played. Or if they wanted to play the game, but preferred to learn about NotPetya instead of WannaCry? It would result in a lot of changes in a different part of the material.

9.2. What is “Flavors”

First of all the name. As you might have guessed from the logo, we devised it with the idea of combining different ice cream flavors to create whatever suits the user. And that should also be possible with our game.

So what we wanted, to make it is possible to take different aspects from our games and play mix and match. To give this a clear framework, we provided a guideline to group the topics into categories. As shown in Figure 9.2, the categories we chose came from two main inspirations. At the top, we put the *Lockheed Martin Cybersecurity Killchain*, which is probably the most well-known categorization for attacks. And at the bottom, we placed the categorization from the card game *Backdoors and Breaches*[1]. The advantage of those categories is, that they focus on the aspect that a defender can control. While the *Lockheed Martin* categories include things, that are entirely in the hands of the attacker, such as “Recon” and “Weaponization”. The decision was to use the *Lockheed Martin Cybersecurity Killchain* for the game to have all possible categories in our content properly.

There are topics (WannaCry for example) that fall into multiple categories. The Killchain gives the most complete set of categories we can use to distinguish our flavors.

9.3. The way from SecureRole to flavors

Flavors is a completely new concept of delivering content to users. This will demand changes to our current material to work with the new framework. We have determined the necessary tasks and included them in a chart for a better overview. They are listed in Figure 9.3.

Once these changes had been made in the project structure to “SecureRole Flavors” was being able to be delivered to users and enhance their experience.

[1] A game which we evaluated during our assessment of existing materials. More about it in subsection 3.1.1

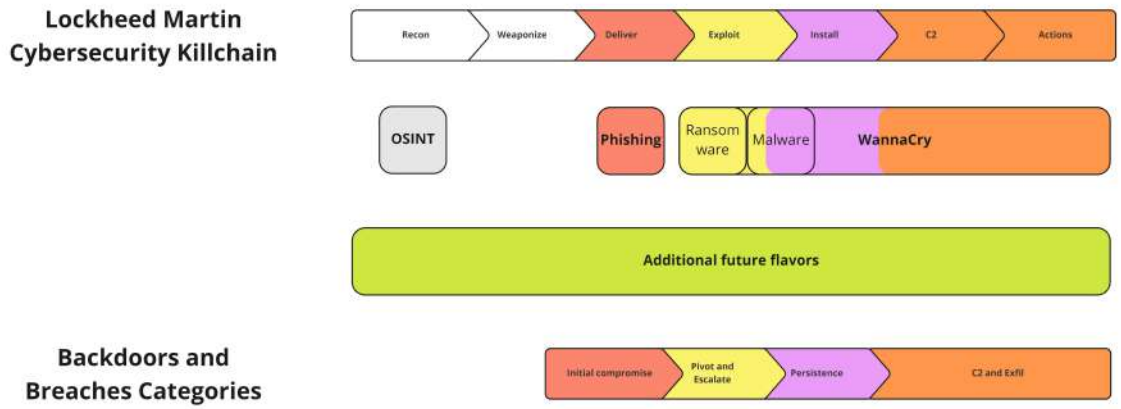


Figure 9.2.: The categorization for our different flavors. At the top are the current flavors.

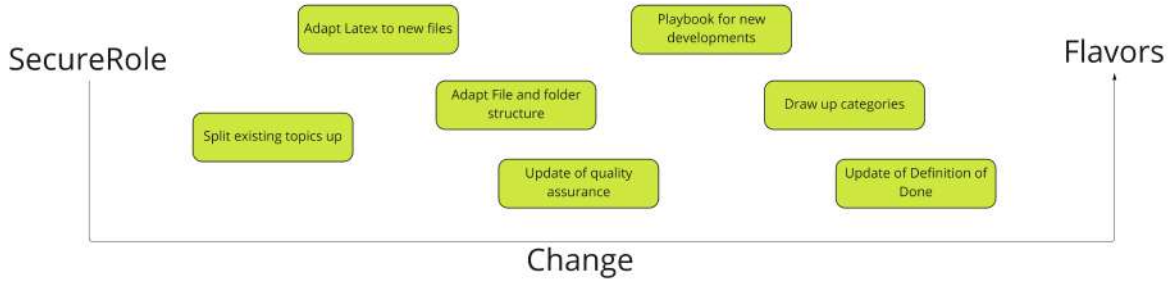


Figure 9.3.: The neccessary changes to move from the previous game mode towards "SecureRole Flavors"

9.4. Content delivery

One thing that is a slight drawback of SecureRole Flavors is the user-friendliness when choosing the right content. Previously, it was enough to select one of the pre-made stories, download the files from the content folder and the user was ready to go. But now it is up to the user to mix and match all flavors and create the game he wants.

This poses two major challenges.

- There is not yet the technical framework to mix and match
- The user is overwhelmed

9.4.1. There is not yet the technical framework to mix and match

This is probably most notable and important to our users. In its current state “SecureRole” is not technically built to mix and match and then receive nicely combined PDFs in the way a user would like. While it is seen as a challenge, it can’t be fixed fully during this bachelor thesis due to time constraints.

There are ideas on how to fully fix this, with an application that supports the user in mixing the documents and creating the optimal PDFs for him. We call it the “Flavor mixer”. While a nice idea, there will not be enough time to develop it and this has to be put as a future possibility for SecureRole.

Currently there is only the following option:
We will simply mix and match them by ourselves. There is a very small number of variables at hand, meaning that the possible combinations are slim. (There are currently only one or two flavors per category.) As a result of this, a few predefined games are created and the user nevertheless has the chance to mix and match himself. The precondition here is that he has to pick the correct PDFs and combine them himself if he wants to deviate from the main topics. We know this isn’t optimal for the user experience and therefore “Flavors mixer” has to be created in the future development of the game.

9.4.2. The user is overwhelmed

What if the user is simply not proficient enough in attack and incident response scenarios to pick the correct flavors for himself? Well, this is a bit easier to fix than the previous issue.

- The Flavors will be graded with a difficulty setting.
- The Flavors will be graded with a target audience.
- The Flavors will be graded regarding the necessary experience from the game master.
- Examples stories will be shown that work well together (as mentioned previously).
- There will be a list of flavors that match and won’t match.

This will be shown for each of the flavors, making matching and mixing easier. Once the “Flavor mixer” is implemented, it will make the whole experience even better for the game masters.

10. Acceptance Testing

This chapter offers a complete overview of the second testing run. It includes everything on the procedures, the issues encountered along the way and the gathered results and feedbacks at the end. It concludes by stating the created tasks from the learnings in the testing run.

10.1. Procedures

This section has been reworked by the learnings from the first testing. This helped to perform better and have better-targeted testing on the second and final acceptance testing run.

10.1.1. Introduction

The test procedures had the main goal of clearly describing what should be done during testing and what metrics had to be achieved. Our most important goals were:

- Verify the usability of the created role-playing games
- Verify the quality of the created role-playing games
- Verify the quality of the created materials we created in general
- Verify that the game is educational to the students

The findings from these tests were taken into consideration to improve the product further.

10.1.2. Testing basics

This testing was conducted in a real-life scenario. It was planned to perform the test with a similarly composed test group as during our alpha trials. This allowed seeing the enhancing effect the script had on the participants and how they perceived the refined and improved role-playing game. But we took the opportunity to test it with a bigger group of testers, which Weiler Nathalie offered to us. We had the chance to test our product during one of her exercise sessions.

This also allowed to test the product under realistic circumstances, since the content was used in exactly that setting. The test was performed on one of the “Ransomphish” topics being curated for the teachers.

10.1.3. Initial plans

The initial plan was to test the product with students from the “SecureSoftware” course, currently held at the Ostschweizer Fachhochschule (Eastern University of Applied Sciences) (OST) under the supervision of Weiler Nathalie. The course had roughly 80 students enlisted. The hop was for a 10-20% application rate, hence resulting in 8-16 students participating in the tests.

Because of the increase in the testing scale (the last test had only four participants), it was needed to increase the preparations for the tests. This included the following measures to ensure a smooth testing experience for the tester and the supervisors:

- Participants needed to register before testing
- Participants were assigned into groups and to teachers
- Three teachers were asked to be present (depending on participant count)
- Three supervisors of SecureRole were present (depending on participant count)
- One questionnaire before the exercise
- One questionnaire after the exercise

After the measurements were prepared and uploaded a call to all students of the course, asking them to participate. After the passed deadline, there was one person registered, this was short of the expected number. The next option was finding other people that we gathered autonomously from the course “SecureSoftware”. This resulted in only four testers once more.

While this did not allow for testing to test all planned metrics and variables, there was nevertheless the will to conduct this test instead of canceling it. The hope was still for valuable feedback regarding the current state of work.

10.1.4. Future Testing

Due to the reduced numbers of test groups and metrics the final acceptance test could not find a good significants. As a result of this, there was a list of questions put together to be addressed in a future test lifecycle maintenance of this project.

- Test the new content that was created in parallel to our acceptance tests.
- Test if students consume the additional materials offered to them or if they didn’t

needed them.

- Test with two groups if reading the script has a positive influence on the game outcome. One group receives the script and one doesn't (to have a control group), then compare the outcome of the games to each other.
- Test the GM document with a multitude of teachers of different skill levels and ask them for their feedback.

10.2. Preparations

10.2.1. Testers

Our testers were students from Ostschweizer Fachhochschule (Eastern University of Applied Sciences) (OST). The testers already had a basic understanding of the most pressing issues in cybersecurity and had some experience in incident response. While this wasn't exactly the audience these games are created for, it helped during testing since it allowed for a more in-depth analysis of the game and thus more detailed feedback. There was confidence that this group of testers would deliver valuable feedback that would lead to the preparation of the game for its main target audience.

10.2.2. Teachers

The presentation of the idea to the teachers and they were told they were expected to do with the GM file. This would show what the intended achievements were with the testing round and what exactly the expectations for them were. They also had to fill out a questionnaire regarding the GM file and a questionnaire after they had concluded the game to give feedback. So the feedback was split into a teacher and a participant section.

10.2.3. Testing

At the beginning of the testing, the idea of SecureRole was presented to participants and they were told what the expectations were. Afterward, they had time to fill in the first questionnaire. The questionnaires were Microsoft Forms[1] this time. This allowed for easier data collection and a better overview of the results. The first questionnaire contained existing knowledge of the topic and their expectations of the game.

The testing was conducted like a normal game. This means the participants had received their character sheets before for preparation. Since the testing was conducted online, they had to join a virtual room with their fake name assigned to them in the

[1] A Microsoft software to conduct online surveys and hand out questionnaires.

role-play.

Notes were taken during the game and any issues were written into the protocol. The game ran one interference, an intervention was necessary because of a game-breaking issue. This intervention ensured a clear flow for the participants and optimal test results.

After the game was concluded, the teacher had a review with the students. The students then received a second questionnaire. This allowed analyzing different metrics before and after the game to get a more complete picture.

10.2.4. Adaptation of learnings

Once testing was concluded all the gathered learnings of our tests were taken and discussed. Once this discussion happened, new issues were opened and the most pressuring issues were addressed for the next improvements, whereas less time-sensitive issues were added to the backlog.

10.3. Results

This section provides a summary of the results of the acceptance test conducted with the testers. The findings below are a summary of all questionnaires filled out by the participants and the supervisors, as well as the notes taken by the SecureRole members. The whole questionnaires were not included but the most important points were correlated in an overview.

The users were asked to play the beta version of the role-playing game part of SecureRole. A predefined story was choosen with the following elements:

- Recon: OSINT
- Delivery: Phishing
- Exploitation: Malware (WannaCry)

For a more in-depth description of the testing procedure, please refer to the previous sectionsection 10.1

10.3.1. General observations

One of the first observations made by Anina Bytyçi was that the acceptance test went already quite a lot smoother than the alpha test. This gave the first impression that SecureRole had already matured since the first test and was approaching a release

version.

A large amount of feedback was received from the participants and the GM. One part came from the questionnaires filled out, and another part from interacting with them and listening to their concerns during and after the game. After implementing the proposed changes, the game seems to be in a presentable state and is ready to be enjoyed by our target audience.

Due to the constrained time frame, not all concerns raised by the test participants can be implemented. The most important points will be implemented directly and some improvements will be done at a later maintaining stage.

10.3.2. Actual test

Challenges

Directly before the game, the participants were asked if they had any issues preparing for the test. They remarked the following important concerns:

- The character sheets to contain the org-chart with the company cheatsheet
- The supplied org chart contained errors and was confusing
- They had received very little background information regarding the company

Sequence of events

The test got underway and the GM (Simon Kindhauser) gave a quick introduction to everybody about what the expectations were. He informed the participants about the threats that OSINT posed and showed them the phishing e-mail. After a quick introduction of why it was indeed a phishing attempt, he started the game.

The participants then quickly started engaging in the game and handling the issue. George called the IT department and started to ask around who could help him. Sergio got in contact with him and informed him what steps he had to follow. The group was already quite proficient in the area of malware, as the Figure 10.1 shows. It thus prompted a fast reaction. They disconnected the laptop and collected it from George. Once the initial assessment was done, the IT department collectively decided to inform the CEO about the occurrence. Stefania then decided to include an external IT company to help them solve the issue. The GM tried to persuade them into doing the incident handling themselves, but the group argued realistically that it would be the best course of action to involve an external company. This concluded the game, with an overview by the GM what the external company had found and how they had solved the issue.

While this was not the planned course of action, the SecureRole observers decided that the data gathered in the test was sufficient and they moved on to the retrospective, in which the participants gave feedback regarding how they felt during the game. This gave more time to ask the participants for detailed feedback on how they perceived the game and what they would like to change.

10.3.3. Feedback

From the participants after the game

Participants gave a big amount of direct feedback after the game[2]:

Sergio:

- "The context around the game is not fully clear, I would appreciate some more background information such as what am I allowed to do, who am I allowed to contact, etc."
- "Maybe provides a little more in-depth background story for our characters and tells us what our capacities and responsibilities are."
- "Idea: Each character gets a special 'joker' which he can use when the game gets stuck to free himself. This could be accompanied by a vote from the other team members or would need the Game Master approval."

Christian:

- "Which IT infrastructure do we have at hand? It would be handy to have a rough idea of which tools we have at our disposal."
- "But you should still give the participants a little leeway on what exactly they want to use tooling-wise."
- "Keep the overview short and simple or do it fully visually."

George:

- "Make it clearer what my character knows and how he would act. It would be beneficial to the game to play a role with predefined knowledge and priorities instead of simply playing myself."
- "I would not give an introduction at the beginning regarding OSINT and phishing, but rather throw the participants directly in, head first, and see how they manage. This would probably yield a more authentic result."

Stefania:

[2]This feedback portion was discussed orally and is thus only an approximate transcript and not a reference to the actual submitted written feedback in the questionnaires. The suggestions from the questionnaires are mentioned in later portions of this document.

- "Maybe add a second salesperson, so George can discuss his e-mail with someone before going to the IT department. This could increase the authenticity of the game and improve the setting."
- "Give the CEO a better picture of the company. She should have the most important numbers regarding headcount and financial assets."

From the GM after the game

- "Maybe first play a mundane setting, such as a normal business day or a Christmas party in which all of the participants get to know each other. This could also add to the realism of the game."
- "The game is fun to play, but being GM for the first time is not easy. I am sure the experience will increase during succeeding runs of the same game and improve the experience for the students and myself."
- "Maybe adds a few additional storylines for events such as the participants reaching out to law enforcement or external IT companies to ease the job of the GM. The section 'additional tasks' already helps, but this could increase the GM experience even more."
- "The company 'Field castle financial' might not be optimally suited for this task (referring to the predefined MalwarePhish scenario). Since they handle highly sensitive customer data, it quickly drives the participants towards more drastic measures which often drive the game to an earlier conclusion than intended. This could be avoided if instead, the company was from a less critical field."

10.3.4. Test Outcome

The four questionnaires were conducted in total. They were (in chronological order) the following ones:

1. GM questionnaire before the game
2. Participant questionnaire before the game
3. Participant questionnaire after the game
4. GM questionnaire after the game

Each candidate was given the link to the Microsoft forms documents at the appropriate time. This allowed to correlate their feedback and get an insight into why and even if they liked the game, gather metrics we defined before and ask if they would suggest any improvements that could enhance the experience for them. There was also the question of what specific parts of the experience were most enjoyable for them, to gauge the parts needed to be a staple for all future games created.

Knowledge

Some standard questions were to find out their knowledge of the topics in the test scenario. This with the intent to see if the game increased their knowledge. The Figure 10.1 looks at a direct comparison of the topics pre- and post-game. Apparently little has changed.

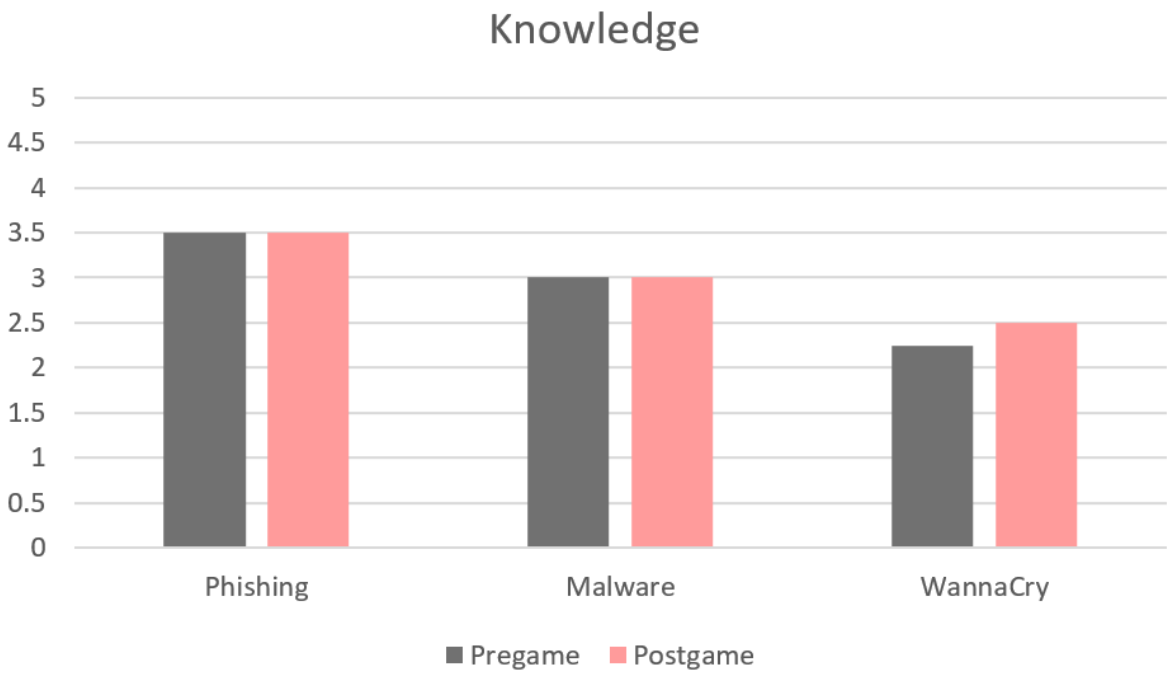


Figure 10.1.: The self rated knowledge of the participants pre- and postgame on a scale from one to five on average.

As seen the knowledge about the topics did not increase (at least not by any significant amount). This is more or less in line with how the participants felt. They were asked to rate if they think they learned something new on a scale from one to five, with one being nothing new and five being a lot of new things. Their average was 3.25, so they thought they learned some new things, but nothing outstanding. This shows that the game does not succeed in teaching our participants something new. While this might be given to the fact that they were already quite proficient with some topics, as seen in the figure, we believe this has another root cause.

The game itself is simply not good for teaching new concepts.

This does not mean the goal of the game failed, or that the game is useless. The game simply has another main advantage.

It strengthens already learned knowledge and helps the students to apply it in a simulated situation.

If more knowledge is required about how the game is structured to achieve its maximal educational potential, please read chapter 2

This thesis could be confirmed by the following statement of the participants[3]:

- “It was really interesting to learn how to react correctly because I never learned it.”
- “I enjoyed this new mode of learning since it was refreshing and educational. It trained my knowledge and experience.”

This shows that the students did indeed learn something (this coincides with their rating). Just not a lot of new concepts, rather they cemented their knowledge about already learned theoretical topics with a call to action!

This could induce a problem if a teacher has a class being new to this field and without experience. The students would probably struggle to adapt to the game, it wouldn’t go as fluid as it did with the testers and most importantly, it wouldn’t create a lasting effect since these participants would have little knowledge that could be reinforced by the exercise. An array of ideas was identified on how to counter this issue:

- Advise inexperienced students to read the provided scripts for each topic, to give them a basic understanding of what they are dealing with.
- Advise the teacher to hold a lecture with the students before playing the game, to ensure all students have a basic understanding of the issues.
- Build a game that has a lower entry bar that allows participants with very little knowledge to participate in it.

All of these measures are currently purely theoretical. We would need another round of testing to measure their effectiveness and give a clear statement on which of the previous measures should be the preferred way. This duty will be passed down to the maintainers of this project since we will not be able to hold another round of testing. But we will try to implement measures that will counter these issues, see subsection 10.3.6.

The role-playing game

It is a strange experience to be in a role-playing game for the first time. Persons are suddenly supposed to pretend to be someone they are not. And as the survey showed, only 50% of the participants had ever played something similar before (such as *DnD* or *Pathfinder*). But high interactivity between the participants led to a lively game. This was also increased by a good GM who helped the players when they got stuck or had out-of-character questions.

[3]Some of the statements made by the test participants were in german. So while not all of these statements are direct quotes we tried to translate them as closely as possible

There were smaller issues due to the participants being inexperienced with role-playing games, such as breaking characters sometimes, or using information that their character could not have possessed at the time (due to not being present in certain interactions in the game itself). Another small issue was the occurrence of “hearsay”. Meaning one participant simply made an assumption about the setting and shared it with the rest of the group. This led to the rest of the group accepting this information as a fact, even though it was not correct.

But all of these issues were minor and did not substantially hamper the flow of the game. Some of them were addressed by a quick reminder of the Game Master, while others were left unchecked (for example the hearsay issue) since they would also occur in a real-life scenario. This gives the confidence that the game can also be played by audiences having little to no experience with these type of games.

Equal interaction

One of the questions asked during our interim presentation was “How do you ensure equal player interaction”. This question has stuck since there was no clear answer for it and the question carried a lot of weight:

- How can it be ensured all players interact equally with each other?
- How can it be prevented players from getting bored?
- How can it be ensured that all players have an equal learning experience?

Luckily exactly this case pops up during the testing run: Sergio made the quick decision to take George offline to prevent any potential spread of malware from being introduced into the company. This left George with nothing left to do. He was locked out of the game (at least his character was).

While this was an issue, it never came across as one. The participant playing George stayed engaged and offered his opinion on certain steps being taken. While this wasn’t in character for George, it helped the participant stay engaged in the game and keep participating in the learning experience. Understandably, this level of engagement will vary from player to player. Another player might have completely disengaged from the exercise and let his thoughts wander. The following conclusions can be drawn from testing:

- It does not prevent an engaged player from participating in the game if a player’s character is inactive during a certain period.
- Should a player disengage from the game, it is also up to the GM to make sure everybody stays engaged. (We should provide information in the GM file regarding this.)
- Players are still part of the learning experience, even when their characters are inactive. They might still participate in discussions and debate the other player’s

proposed solutions.

One important aspect to keep in mind: It's like a role-playing game in that all players can't be engaged equally. This is an issue in all role-playing games played so far by the team and is just something that cannot be changed. The inclusion of all characters equally is difficult, because there will always be some downtime for certain participants.

Replayability

Another important aspect was the replayability value. The implementation of flavors is provide a strong framework of interchangeability and flexibility in the role play. It would allow a teacher to use SecureRole to teach and strengthen students' knowledge about a variety of different topics. But what good would this be, if the students saw no replayability in the game? The current efforts to build this game would be in vain.

The participants were asked during the test if they would be willing to play the game once more if the setting would be changed. The answers were unanimously positive. They loved the idea of playing the game again and tackling a different challenge. Their reasoning for this was:

- "I think that if you can go through different thinking steps to get through unknown situations in an environment that is more playful and relaxed helps to learn and practice better for real-life incidents."
- "Absolutely! Diversity is great. The role-playing game could be made easier or harder and you could combine already known topics with new ones."

As it is seen the introduction of SecureRole Flavors was not only a good decision regarding scalability and interchangeability but also helped to increase the replay value for future usages to provide the students with new formats.

Fun

The engagement and fun the players had while playing the role-playing game are also to be considered. The goal was to offer an exciting and interactive learning experience that is different from classical approaches. The participant engagement was high throughout the game and every member of our test group participated in a meaningful way. They were asked to rate the "overall experience" they had interacting with SecureRole and they rated it 4.25 out of a maximum of 5.

10.3.5. Comments from SecureRole supervisors

The whole testing was supervised by the two SecureRole members Anina Bytyçi and Marco Zanetti. It is important to voice the observations of the SecureRole members.

One of the first things that were observed is that the GM chose to show the students the e-mail and discuss with them the telling signs that it was a phishing e-mail. Is the decision of the GM, but it gave the students a head start in the game, which allowed them to quickly react and shut the threat down. This should be moved towards the end of the exercise and put in the retrospective.

Further, it is to notice that there are issues with our phone book if not all roles are populated by participants. George first tried to reach Max, but since we only had four testers, Max was not reachable. This is to be fixed to make it clearer who is available and who isn't. (This could be done by telling the participants that the missing roles are currently on vacation and their phones have been redirected).

The participants were not certain how their timeline looked. But the GM stepped in and informed them what time it was when the time jumps occurred and how much time had passed since the incident had occurred. This is to provide in the GM file or in the storyboard to give the GM and the players a better outline of the whole scenario. We cannot always count on the GM being this proactive and ready to improvise.

Another issue that came up from time to time was the question regarding the budget of the company. While the participants remarked that the information provided by Sergio was helpful, they would have wished for a more in-depth view of the company's finances. If it is unknown how the company is situated, it is hard to make decisions. Also, the costs for the help of an external IT company were not clear. This led to some confusion (which was luckily resolved by the GM in our case). There is the need to address this in a more detailed account of the company.

And the last issue that plagued the role play was the org chart. It contained a few errors and was not intuitive enough for the participants. They were struggling to find the correct person to talk to and were confused by its appearance. There was no clear structure to it and they defined the lower section as too confusing and containing irrelevant information.

10.3.6. Improvements

The two most important issues taken away from this acceptance test are:

- SecureRole is a strong product, which heads in the right direction.
- But the product still has a lot of rough attention which needs attention. Details and improvements on the small quality of life change for our participants and the GM need to be improved.

While the first point gathered in the conclusion is reassuring, the second one serves as a drive to improve SecureRole even further. Listed below are the most post improvements which will be converted into issues to improve our product.

Each point identified needs to be improved upon next. After the acceptance test achievements for SecureRole are ongoing.

After revision of this part of the documentation, it is state what is done and what needs to be postponed to the backlog, to be completed once the project has passed into the lifecycle management stage.

Equal participation

Future improvements:
A hint towards the GM will be included to ensure equal participation as well as possible. This point can only be achieved with the cooperation of the participants.

Achieved improvements:
A hint box in the GM will be included to file let him know that equal participation is an important aspect of our game. It informs him that, while he shouldn't interfere in the game, he can make sure that students are equally participating by giving hints or questions directed at them.

Replay value (SecureRole Flavors)

Future improvements:
It's important to pursue SecureRole Flavors to create new content. This helps to keep the replay value high for the participants.

Achieved improvements:
The package count is creased and offers thus more flexibility while maintaining the SecureRole Flavors framework.

Preparations

Future improvements:
A suggestion for the GM is included that makes sure to adequately prepare the students before engaging in the game. It must be clear that the strength of the role-play lies in the consolidation of acquired knowledge, not in the acquisition of new knowledge. The acquisition of new knowledge can be achieved by reading the scripts or listening to a lecture held with the provided slides. This needs to be made clear to the students as well, preferably on the GitHub page.

It could make sense to write a short teacher manual to give an overview of how to prepare a game and how to structure the course around it.

Achieved improvements:
The finalized README on GitHub now contains a section that guides the GM and the player through the interaction with the content. It gives a short introduction to how our content is structured, and how it should be consumed to achieve a satisfying experience.

Create an easier game

Future improvements:
Due to the time constraints, it will not be possible to create enough new modules to provide an easier game for participants with little to no knowledge.

Achieved improvements:
There could be an evaluation in the future to find out if this feature could be a welcome addition to SecureRole.

Rework organizational chart

Future improvements:
The organizational chart was described as confusing, unintuitive and lacking a clear structure. Our participants need a clearer overview of what the key indicators of the company are.

Achieved improvements:
The organizational chart from scratch is a leaner and more user-friendly version that is included in current character sheets.

Rework character sheet

Future improvements:
The character sheets lack important information for the participants. While they got a somewhat satisfactory rating from the testers (the participants rated their use of them with a 3.75 out of five), there have to be changes to be done. They requested to receive a concise list of people they would usually speak to, what exactly their tasks were and their usual routines. It is also to be considered to include a set of rules, for allowed and disallowed actions. This could be either done directly on the character sheets or a separate rule sheet/booklet.

A further comment by a tester was that the character sheets are already quite convoluted with text. He suggested increasing the use of visual aids in favor of the “wall of text”.

Achieved improvements:

The cheat sheet is reworked from scratch and additional information is included, such as general rules that apply to the game as a whole. This should make it clearer for the participants what they are allowed to do. The phonebook will be scrapped in favor of the new organization chart.

Improve the Game Master document

Future improvements:
The Game Master document, while regarded as helpful and comprehensive, still needs a little smoothening of the edges. It contains minor issues and continuity errors that need fixing.

Achieved improvements:
The Game Master document has been refactored, and the wishes from the test have been implemented. It has been checked for small imperfections and continuity errors which were fixed.

Add additional information

Future improvements:
One main request by the participants was the addition of further information to play the game. The wishlist includes[4]:

- Financial information
- Overview over IT capabilities
- Network overview
- Timeline of events

An important request from the participants was not to simply add the information in the form of text but to better understand it through visual overviews.

Achieved improvements:
The requested information was added during the rework of the cheatsheets. A board with fake financial information was added for the participants, so they can gauge the current financial situation of their company, and see if they can afford certain services. The metrics added include figures such as the daily loss if the company can't operate, the IT budget and many more. There was also a network topology added to reflect a coarse overview of the on-premise network that the company operates. This helps the participants to see what they can work with and how they can respond to certain devices being offline.

As a last measure, there was a timeline included in the storyboard and also in the

[4]Excluding points discussed before such as an improved character sheet.

Game Master file. This allows the GM to follow an estimated timeline, which adds to the immersion and can create some pressure due to the time passing in the game.

GitHub

Future improvements:
One last thing to improve is how to advertise our GitHub page to the students. For the test, a link was included in the e-mail and this way asked the students to visit the page if they had any desire to do so. This resulted in 75% of the participants not visiting the SecureRole page at all[5].

There is a need to inform the students more precisely about what they can find on the GitHub page and why it is beneficial for them to visit it. By showing the advantage to visit the GitHub page for enhancing their learning experience and it is beneficial for them to play the game.

Achieved improvements:
There were not taken any extra measures to improve the visibility of the GitHub page instead improved the README document was improved, to give a better overview to the students of what the product has to offer. It allows the students to see how they should interact with the content, and which documents are important to them and which are not.

10.3.7. Conclusion

The test was successful, even though the planned amount of data was not gathered, due to the small test group. But this meant also a better output of information because a bunch of students were very motivated.

Overall, the test went smoothly, the participants were engaged and enjoyed their time. This led to a relaxed atmosphere in which they were comfortable voicing concerns and giving detailed feedback. The received feedback is immensely valuable. “Quality over quantity” is probably the best way to describe the acceptance test. The acceptance test resulted in fewer data points, but the ones gathered were of higher quality and offered more insight.

[5]While we are not sure, a contributing factor of this could be that the time frame was rather short. They received the information regarding the test one day before the actual date, leaving them little time to prepare themselves.

11. Conclusion

This chapter features retrospectives and reviews from the team members regarding the goals, the process and the final product. It also contains an overview of all use cases, their status and if they were completed during this project.

11.1. Review of personal goals

At the beginning of this project, each team member has given a personal statement that contained the most important goals they wanted to achieve. These goals were revisited towards the end of the project and each team member evaluated if they achieved the goals they had set for themselves.

These are the goals set at the beginning. They are a direct quote from section 13.2:

- **Isaac Würth:** “The project should give me a better understanding of the agile world and implement what I have learned in Scrum. In addition, I would like to improve my understanding of the open-source, expand the handling with external partners/stakeholders and get to know better different scenarios on how to behave in such situations.”
- **Anina Bytyçi:** “I am interested in working with a team on a project that does not primarily involve software development. After the engineering project where we used the agile development process, I am interested in getting better at it. Also, the main goal is to collect material and knowledge about different kinds of cyber-attacks and put it together in one place where people interested in cyber security can access it.”
- **Marco Zanetti:** “First I want to improve my experiences of working in an agile team, with a clean project structure, following an agile workflow. Secondly, I feel that everyone should have access to free education. I want to provide that with the help of SecureRole, to bring cybersecurity education closer to students in a playful, but thorough way”

And following, the evaluations by the team members to see if we achieved our goals:

- **Isaac Würth:** “My first goal is related to the Agile world that we implemented with Scrum. The implementation with Scrum has shown me that more time is spent on planning and more focus is placed on the quality of the product. Changes can also be implemented faster without compromising the planning. We were

not able to work with external partners, however, with our GitHub repository, we made the documentation public and accessible to all. With the development of the framework, I also had the realization that security training for students cannot be developed in a static scenario as the threats keep changing. For me, the goals are met, except for communication."

- **Anina Bytyçi:** "Throughout the project we used the Scrum framework, and its implementation helped us to move forward and organize the whole project. In doing so, I learned that several meetings and roles need to be defined for us to get the work done. Also very helpful were the Sprint Retrospective and Sprint Review meetings, which allowed us to reflect on our work at the end of each sprint, analyze what slowed us down, what improvements can be made, and what we did well so we could move forward with it. I can say that I have improved in implementing Scrum in a project. Second, we completed a role-playing game, which was also tested and improved according to the feedback we received. We have also developed and defined a new framework, SecureRole flavors, which will allow us to create role-playing games more easily by defining topics as packages and dividing them into categories. This framework will help make the project easier to develop after the thesis is complete. We have also created scripts and slides for each topic covered in the game, in addition to linking third-party content that can be helpful for the user. Therefore, I can say that the goal of developing content about different types of cybersecurity attacks has been completed. And more importantly, the content can be found in one place and accessed for free."
- **Marco Zanetti:** "Well I gathered more experience working in an agile team. Working independently with little guidance in a three-person team requires a lot of communication and good documentation. We managed to tackle this quite successfully. This meant that a significant portion of our allocated time went towards managing the project and not working on the product. But a well-managed project rewards you with lower maintenance costs along the way, so I believe the time was well spent, and even saved us time in the long run. The second goal was far more important to me and I believe we made a good step towards it. Our material is freely accessible to anyone who wants to read it. It offers an interactive and playful way to learn and practice cybersecurity, which was exactly what we were aiming for. Overall I'd say my goals are met, but more ideas for further content have sprung up, which will be put to got use once the project goes into the post-bachelor thesis phase."

11.2. Project Goals

While the review of the personal goals is important, it is of higher importance to revisit the project goals set in the beginning. The best way to reflect if we managed to achieve the project goals, is by revisiting our use cases. You can find the full overview in chapter 19 in the project documentation. We included the overview graphic here for your convenience.

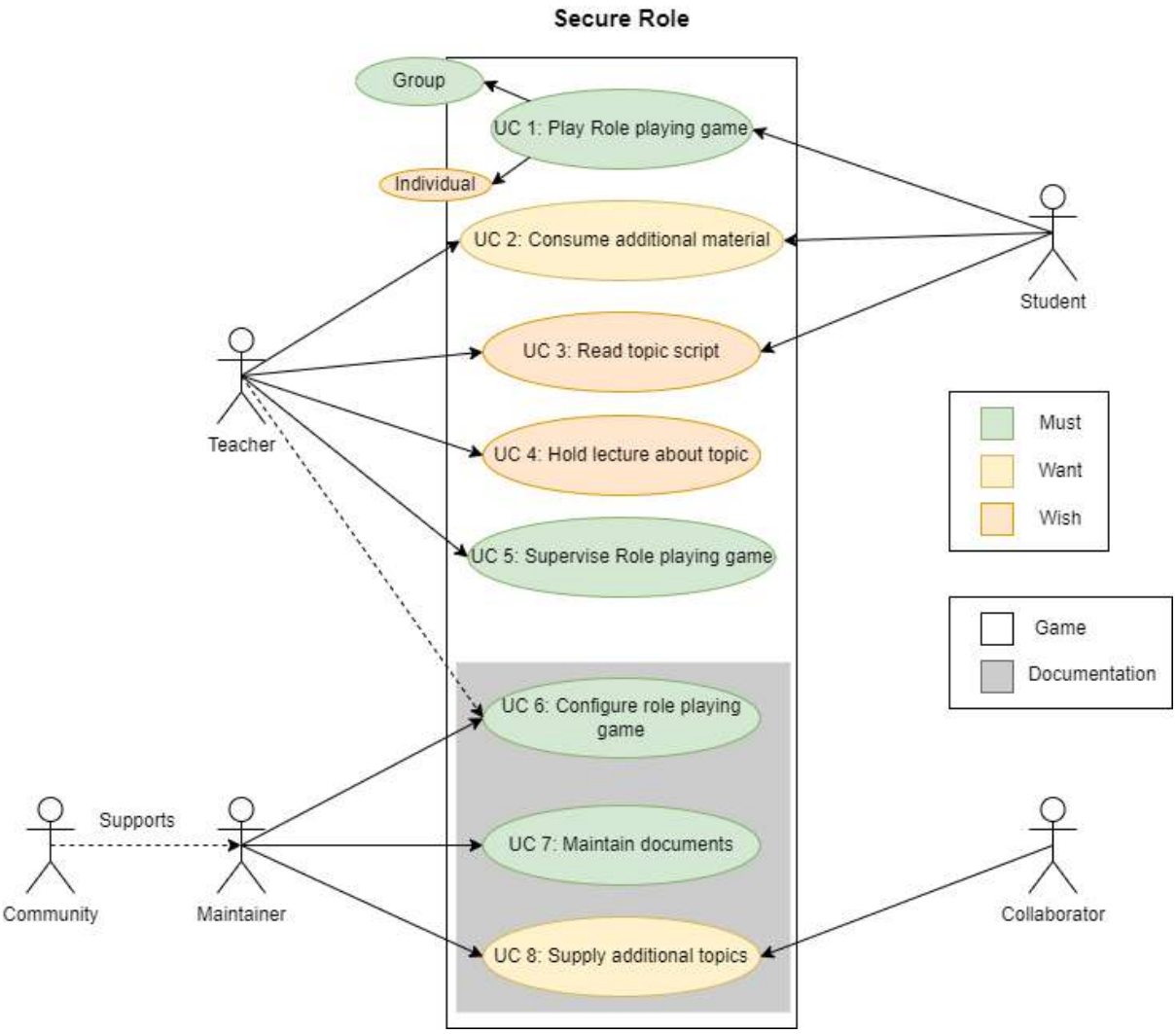


Figure 11.1.: The use case diagram as seen in Figure 19.1

Use Case 1: (Must) Play Role-playing game

Use case one was the main focus of our effort and was thus clearly met by our product. We have a strong product that contains the framework for a fun and interactive role-playing game which can be used to educate students.

Use Case 1.1: (Must) Playing the role-playing game in a group

Use case 1.1 is a sub-use case of the first one. It specifies that the game can be played by a group. Our product also meets this requirement, since we placed our focus on providing a game for a group of students when we worked on the underlying framework. This makes our product well aligned with this use case, which we marked as an absolute must by our goals. The final product is tailored to groups playing it, fulfilling this use case.

Use Case 1.2: (Wish) Playing role-playing game individually

We were unable to fulfill this use case by now. Our game framework caters specifically to groups and not to single individuals. While the whole product of SecureRole with all of its aspects has things to offer for individuals, the role-playing game has not yet been adapted to suit this use case. This would necessitate a rework of the underlying framework with a whole new approach. It could be a possible goal for the future of our product.

Use Case 2: (Want) Consume additional material

We created collections of additional materials such as videos, podcasts, articles, reports, etc to allow students using our product to dive deeper into the material, or simply have an explanation from a different angle. Our educational research paired with our personal experience led us to the conclusion that we could greatly enhance our product by providing additional forms of media to help students which learn through multiple cognitive ways. The collections of the additional content make this possible.

Use Case 3: (Wish) Read topic script

We wrote scripts for all of the topics we created so far, allowing students a deeper look at the covered topics. But it can also be used by teachers to prepare for their lecture or the game itself. The creation of extensive scripts allows beginners to find an easy entry into the topics and allows for better participation in the role-playing games.

Use Case 4: (Wish) Hold lecture about the topic

We created slides for each topic, to be can directly used by a teacher to hold a lecture. They contain the most important aspects of each topic and allow for a well-composed overview of the topics. This takes work away from the teachers, who can use that time to provide a well-composed learning experience for their students with fewer preparations from their side.

Use Case 5: (Must) Supervise role-playing game

The GM document prepares the supervisor for the role-playing game. It contains all important information to prepare someone for the role of the Game Master and give important hints, tips and tricks on how to increase the interaction with the participants and how to guide them through a satisfying learning experience.

Use Case 6: (Must) Configure role-playing game

While this is a “Must” use case, we did not manage to fulfill it to our satisfaction. We had ideas early on about how to achieve this, but our framework was simply not cut out to handle a fully configurable game. The introduction of “SecureRole Flavors”[1] shortly after the halftime mark of our project brought us closer to our goal of a fully configurable game. But while it is configurable for us now, it still isn’t for the educator using our product. We identified possible solutions to this, that will have to be pursued after this thesis is completed. But at the moment, we need to admit that this use case can’t be marked as fully met.

Use Case 7: (Must) Maintain documents

All of our content documents are published publicly on our Github page. Everyone who is fluent in LaTeX can simply download our code, change files and open a merge request with us. Our product is fully maintainable by anyone who wants to help us.

Use Case 8: (Want) Supply additional topics

While we currently did not have any of our stakeholders express any interest in supplying topics, we have an e-mail address to which new topic ideas can be supplied. They then are put into a public kanban board in which the stakeholders can see the progress being made on their topic. This allows for full transparency regarding their supplied topics. The framework is in place, now all we need is good topic suggestions by our stakeholders to showcase its functionality.

11.3. Outlook

While the thesis now comes to an end, SecureRole is just getting started. We have a lot more ideas in stock, that came up during the thesis.

The main documentation will remain hosted on our internal GitLab instance at OST. The content was published to GitHub (as we had done so during the project as well), but while we worked on our internal GitLab instance before and then published it, the move to GitHub will be final this time. We moved all relevant files, media and most important issues to the GitHub instance. This marks the end of our thesis and the release of *SecureRole v1.0*. From now on, all work will be done on the GitHub instance.

While we currently do not know how much time we will be able to spend on maintaining the project, we already have the most important issues defined, which we want to tackle in the future:

[1] Find more about SecureRole Flavors by visiting chapter 18

- Create one interactive game with the help of the Conducttr game engine.[2]
- Create the “SecureRole FlavorMixer”, which will allow teachers to mix and match our packages automatically into one role-playing game.
- Create more packages, to increase the variety offered by SecureRole Flavors

11.4. Final words

We hope that we could give you an overview of how our product “SecureRole” came to life and how it can be used in educational environments all around the world. The following chapters will include the project plan to give a more detailed view of all the necessary files needed for the creation of a project of this scale.

We would kindly like to thank you very much for reading our bachelor thesis documentation.
- Your SecureRole Team

[2]For more information about Conducttr please visit subsection 3.2.1

Part II.

Project Documentation

12. Introduction

12.1. Purpose

This document will provide an overview over all project planning duties which have been undertaken during the bachelor thesis "Cyber Security RPG". You can see an overview over all relevant topics in the table of contents.

13. Project Overview

Nowadays, many cyber attacks are carried out by different and creative types of attackers. The organizations concerned are usually not prepared for such situations and need procedures and proper training to deal with security incidents.

For the implementation of such trainings, different methods can be used. A very effective method is the simulation of such incidents, which creates real conditions and allows the participants to get to know a procedure in an interactive way.

The aim of this work is to develop scenarios that allow the implementation of such a role play. These scenarios and the material created for role plays are primarily intended for the Ostschweizer Fachhochschule (Eastern University of Applied Sciences) (OST) as the main stakeholder, but collaborators are also welcome to participate in the project. Within the project, the implementation will consist of three parts. The first part consists of collecting information and analysing the existing materials. The next step is to decide which method is suitable for the training, more precisely how the teacher/coach can transfer the analyzed materials to the students/employees in a suitable form. And the last phase is content creation and testing of the created material. It is very important for us to test the content that is created so that we can get feedback from users and make changes to the content based on that feedback so that we can have a user-friendly material.

As we find it essential that companies and individuals can prepare for such situations, we will make the training materials freely available under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) license.

13.1. Submisson

Table 13.1.: Overview of all important submissions

Document	Type	Submission	Scope	Links
Projectplan	PDF	17.06.2022		Submisson to `https://avt.i.ost.ch/`
Report	PDF	17.06.2022	Scientific abstract, management summary or lay summary, declaration of independence, references	Submisson to `https://avt.i.ost.ch/`
Poster	PDF	17.06.2022		Submisson to `https://avt.i.ost.ch/`
Finalpresentation	PDF	Erst zur Bachelorprüfung		Submisson to `https://avt.i.ost.ch/`
Booklet Abstract	PDF	13.06.2022	Pictures, Headings, Abstract: Deeper than Lay Summary (for lay audience)	Submisson to `https://avt.i.ost.ch/`

13.2. Personal goals

Each of us in the team has decided to work on this project, as each of us has a different background. We want to set our personal goals at the beginning of the project and at the end of the project reflect on whether they have been achieved and what lessons we have learned.

- **Isaac Würth** The project should give me a better understanding of the agile world and implement what I have learned in Scrum. In addition, I would like to improve my understanding of open source, expand the handling with external partners/stakeholders and get to know better different scenarios on how to behave in such situations.
- **Anina Bytyçi** Personally, I am interested in working with a team on a project that does not primary involve software development. After the engineering project where we used the agile development process, I am interested in getting better at it. Also, the main goal is to collect material and knowledge about different kinds of cyber attacks and put it together in one place where people interested in cyber security can access it.
- **Marco Zanetti** First I want to improve my experiences of working in an agile team, with a clean project structure, following an agile workflow. Secondly, I feel that everyone should have access to free education. I want to provide that with the help of SecureRole, to bring cybersecurity education closer to students in a playful, but thorough way

13.3. Goals

Simulating cybersecurity attacks helps to better understand attacks and improves response in real-world attacks. In reality, however, they are very time-consuming to perform and are therefore rarely used as a training measure. In this thesis, a cybersecurity attack role-playing game is developed to be used as an online game. This will be done creating theoretical scenarios for possible cyberattacks (corporate environment, home office, industrial plant, smart building), for which a playful implementation is created. These will then be tested with a group representing our target audience. The expected number of stories depends on the form of the SA and BA.

13.4. Project Organisation

In this section, all project participants are listed. The partners will be listed in the documentation if they agree.

Table 13.2.: Project Organisation

Name	**Role**	**Contact**
Isaac Würth	Scrum Master	isaac.wuerth@ost.ch
Anina Bytyçi	Developer	anina.bytyci@ost.ch
Marco Zanetti	Developer	marco.zanetti@ost.ch
Nathalie Weiler	Advisor (Indirect)	nathalie.weiler@ost.ch
Girogio Tresoldi	Examiner (Indirect)	giorgio.tresoldi@armasuisse.ch
Mitra Purandare	Proofreader (Indirect)	mitra.purandare@ost.ch

14. Project process

14.1. Time estimate

The requirement for a bachelor thesis is 360 hours meanwhile it is 240 hours for a semester thesis. The team consists of two people doing a Bachelor's thesis and one person doing a semester thesis, which means a total of 960 hours.

14.1.1. Milestones

Table 14.1.: Milestones

ID	Name	Date	Description
M1	End of Inception	27.02.2022	The project plan together with risk assessment and quality assurance are created. Tools are also selected for the project.
M2	End of Elaboration	13.03.2022	Contact external collaborators, gather non-functional requirements and use cases. Create vision of the project and personas. Research for existing material on this field
M3	Preliminary presentation	26.04.2022	Create the material for the first role-playing game. The material consists of the game master document and the character sheets. Create scripts, slides and additional material for the topic. Conduct the first usability testing. Prepare for interim presentation.
M4	End of product 2	30.05.2022	The second product is created.
M5	End of acceptance test	06.06.2022	The acceptance test is conducted. Testing results are analysed and implemented into the project.
M6	Submission	17.06.2022	The submission are finished. The whole project is submitted and the project is completed.

14.1.2. Phases

Table 14.2.: Projectphases

Name	Start	End	Description
Inception	21.02.2022	27.02.2022	Definition of project plan, risk assessment and quality assurance document. The scope and time estimates of the project are roughly defined.
Elaboration	28.02.2022	13.03.2022	Definition of requirements, use cases, vision.
Construction	14.03.2022	05.06.2022	Role-playing material along with additional and supporting material are created.
Transition	06.05.2022	18.06.2022	Documents necessary for submission are prepared.

14.2. Planning

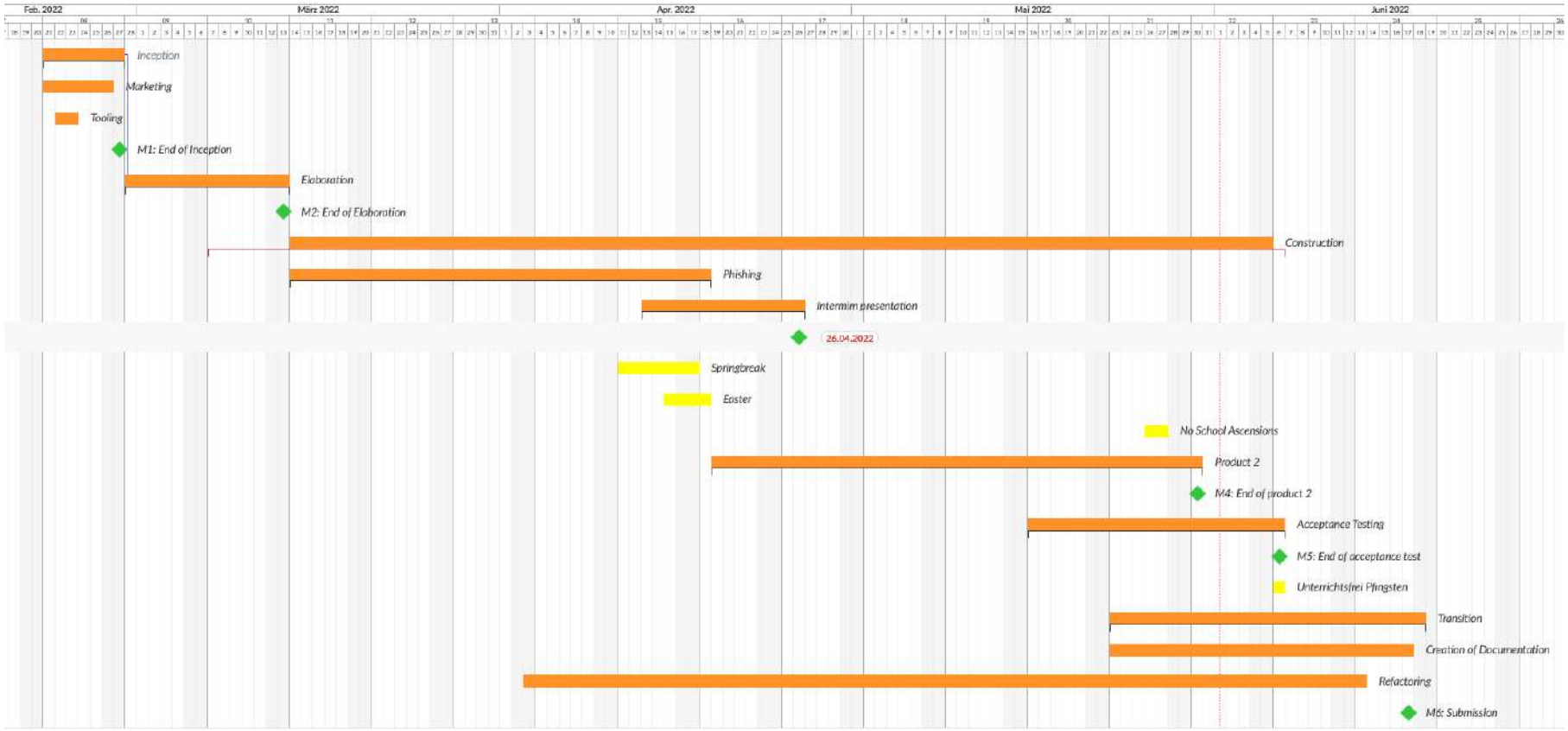


Figure 14.1.: Gantt chart with phases, milestones and vacations

15. Tooling

15.1. Project planning and management

15.1.1. OpenProject

OpenProject is a collaborative project management software. The application is offered as a free "Community Edition" (GNU General Public License Version 3) and as a paid Enterprise Edition (on-premises or cloud).

We used OpenProject to create and maintain a time plan for our project. One of the main features which make OpenProject enticing, is the graphical overview in a chart, that displays the whole project.

OpenProject webpage

15.1.2. Clockify

Clockify is a simple time tracking and timesheet app that allows you and your team to track working hours on projects. We use it to track time spent working on the thesis, and to categorize how much time we spent on which issues. This will allow us to constantly have a good overview over our current time budget.

Clockify webpage

15.1.3. Gitlab hosted by OST

GitLab is a Version Control System (VCS). It is based entirely on Git, a distributed versioning system provided as open source software. The main task of the web-based version control system is to store and document all changes to files and their source code so that they can be traced at any time.

We mainly used it to version our LaTeX files (or just about any files), and to implement processes around GitLab features, which allowed us to implement quality control features. For more information about that, consult chapter 17.

Gitlab also supports the use of a CI/CD, which helped us automate the compilation of LaTeX code into PDF documents. This made the whole compilation process much

smoother and easier.

While we mainly used it for code versioning it also has powerful project management features.
The main features which we used were:

- Creation and status tracking of “Issues”
- Branching and merging of code for the purpose of quality control
- Tagging to mark certain timestamps in the development process

OST Gitlab webpage

15.2. Documentation

15.2.1. LaTeX

LaTeX, is a document preparation system for high-quality typesetting. It is most often used for medium-to-large technical or scientific documents but it can be used for almost any form of publishing. We will use it to create our documents for the product SecureRole, but also to create the documentation for our thesis. We feel that it is easier to modify, version and compile compared to other text editors.

LaTeX webpage

15.2.2. Visual Studio Code

Visual Studio Code (VS Code for short) is a free source code editor from Microsoft. It is available cross-platform for the operating systems Windows, macOS and Linux, which was important to us, due to our team working with different operating systems. The main features of Visual Studio Code which were relevant for us are syntax highlighting, auto-completion, and the native integration of additional packages which introduce additional features. This helped us work with LaTeX, since many such packages increase the usability of VSCode with LaTeX.

We mainly used the packages LaTeX Workshop and LaTeX language support. This in a combination with local scripts, such as latexpdf, allow for smooth compilation of the LaTeX documents into PDFs.

Visual Studio Codes webage

15.2.3. GitHub

GitHub provides Git for free on an online platform. It offers the distributed version control and Source Code Management (SCM) functionality of Git, plus its own features. The reason we used GitHub, besides having access to the locally hosted GitLab instance of OST was, that we could not share our product with external users via the OST GitLab instance. So we use GitHub to publish our product for everybody to download. We also used it to create a sort of “webpage” for our product, to show potential users what our product is trying to accomplish.

- GitHub webpage
- The SecureRole GitHub webpage

16. Vision

16.1. Positioning

16.1.1. Business Opportunity

Role-playing games are helpful for the students to better understand how to put the concepts that are learned theoretically in class into practice. Let us take the example of a phishing email. With a role play, players understand what happens behind the scenes in this attack and what they can do in such a situation if the attack occurs, and they have an important role in an organization.

All the material will be publicly available and accessible free of charge. We will always try to make sure that the provided material is up-to-date and does not contain any errors or mistakes.

16.1.2. Similar products

An identical project does not exist, but we have created a file where we have listed similar projects that already exist and that we will analyze to get more information and help for our project. A better overview of similar projects can be found in the file chapter 3

16.2. Stakeholders

16.2.1. Stakeholders Description

The main stakeholder in this project is Ostschweizer Fachhochschule (Eastern University of Applied Sciences) (OST), as the initial idea was to provide course materials for our school. Weiler Nathalie will thus act as a representative of OST and give us active feedback on the materials. We also invited other educational institutions to be part of our project, but none of them expressed interest in participating.

16.2.2. User Summary

The main users who will use the final product are students and professors of OST.

With the help of role-playing materials, slides and scripts provided for different topics, users will be able to increase their knowledge on specific topics about different cybersecurity attacks and learn how to act in case of a cyber attack.

16.2.3. High-level Goals of Stakeholders

- Good quality role-playing material with correct information
- Easy to understand learning material
- Well structured material, with an easy to understand overview

16.2.4. User-level Goals

- Students: Get well-structured learning material that is easy to understand. Also, the material for role-playing is well-structured and provides enough details about which cyber attack is happening and which is the role of the student in this game.
- Professors: Get a guide for moderating the role play. And to get high quality scripts and slides on the topics covered in the role plays.
- Maintainers: Ensure that the material is kept up to date and that new topics are added from time to time. If an error is found on the project, it will be corrected from the maintainers.

16.3. Product Overview

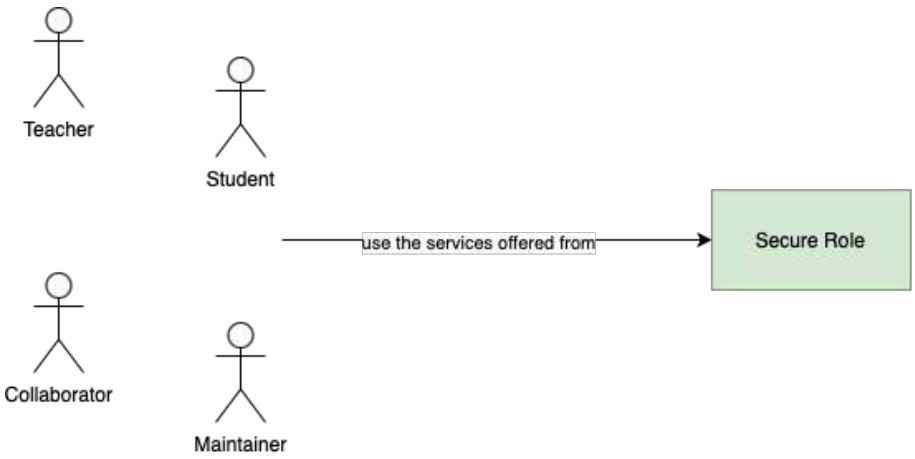


Figure 16.1.: Context Diagram

16.3.1. Summary of Benefits

- Role-play material on various topics about cyber security attacks.

- Text scripts explaining attacks in detail.
- Slides that can be used to teach the material covered.
- Third party articles that can be used to help better understand the material.
- All of the material provided is free and available at any time.

16.3.2. Licensing

Since our project is open source and consists mainly of educational material, all of our work will be licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0).

Under this license, users are free to distribute this project in any medium or format, and also to change and/or add new features to the material, provided however, that the original creators of this material are credited. It should also be indicated when changes have been made to the material.

In addition, if the material is modified or new features are added, the new material should be distributed under the same license as the original project. It was decided within the group that if the source code is included in the project, a new additional license would be added to license the code portion.

16.4. Summary of main features

For better workflow and results, we have prioritized the features and labeled them as **must**. Below we have listed the features that will complete the Minimum Viable Product.

- The project includes and is divided into: Material for role-playing games, additional accompanying material, scripts and slides on different topics.
- Since different topics will be covered during this project, there will be a table that addresses the attributes and characteristics of each role-playing game and material.
- Since our main focus is providing role-playing material, it should include a description of the role for each participant and, in addition, some material for the teacher to guide the role-play.

16.4.1. Other requirements and constraints

Further information about usability, reliability, performance, supportability, documentation and other important constraints, please refer to Non-functional requirements and Use Cases. It should be noted that as a group we decided not to collect functional requirements because it is difficult to define them at this point in the project and they

could change significantly over time. Instead, we decided to create more detailed use case documentation.

17. Quality Assurance

Quality assurance was an important staple in our project. We used it to our advantage to help increase the quality of our project and thus our final product. We achieved this through differing means.

Since we were a team of three our project management had to live up to high quality standards, to ensure that no mistakes were made which would have slowed down the collaborative work. This meant a high level of autonomy for each project member through the means of predefined processes, which paved the way.

Another factor was that we were creating content for educational purposes. It was of high importance to us that our content was peer reviewed, to reduce the possibility of content errors. We defined processes and a “Definition of done” which helped us to make sure each piece of content lived up to our quality expectations.

All the measures taken during the project, have been collected in this and the following chapter.

17.1. Agile workflow

17.1.1. Agile methodology

This project was created using SCRUM as it’s agile methodology. SCRUM was chosen due to its outstanding capabilities for individual tailoring and flexibility for projects.

17.1.2. Agile team management

Due to the use of an agile workflow, the team forwent any specific role assignments apart from a scrum master, which also serves as team manager.

Isaac Würth was chosen as scrum master, due to his extensive knowledge regarding the SCRUM process and his recent participation in the course “Project and quality management” at OST.

17.1.3. SCRUM Meetings

The following SCRUM meetings will be performed by the team:

Table 17.1.: SCRUM Meetings Overview

SCRUM		
Name	***Occurence***	***Time***
Spring Planning	Every second Monday	14:00-15:00
Sprint Review	Every second Monday	10:00-11:00
Sprint Retrospective	After Sprint Review	11:00-11:30
Daily Scrum	Every Monday till Wednesday	08:15-08:30
Sprint Duration	2 Weeks	
Other Meetings		
Weekly Meeting with Weiler Nathalie	Each Monday	14:00-15:00
Interval Presentation	26.04.2022	

For a more in depth look at how the sprints are being planned, please refer to our time management table in the appendices.

17.2. General quality assurance

Since this project involves the creation of educational material, we strive to achieve the highest possible quality. We want to assure anybody using this material that it has been validated, tested and been confirmed as educational. Feel free to send us feedback regarding any possible mistakes in the source material to secure_role@outlook.com.

17.2.1. Definition of done

The current definition of done for the documentation includes, but is not limited to:

- All tables have a caption and a label
- All figures have a caption and a label
- All acronyms are defined in the main.tex
- LaTeX compiles with no errors
- Spellcheck the whole file with a tool of your choice:
  - https://languagetool.org/
  - https://instatext.io/
  - https://app.grammarly.com/
- Avoid negative connotations

- LaTeX Main filenames are ending with _main.tex

17.2.2. Gitlab workflow

The Gitlab workflow is the parent process through which all issues need to pass. The flow varies slightly if the work is being done on the content or the documentation repository.

For the content workflow please see Figure 17.3.

And for the documentation workflow please see Figure 17.4.

These workflows only outline the overall process. Issue need to pass the detailed subprocesses as well, which are detailed below.

Each task which we will tackle will be defined as an issue in our GitLab project. To ensure that we only select worthwhile tasks for our project, we implemented the selection process which you can see in Figure 17.2a.

Once the task passed the selection process, it will then undergo our task completion process, which is outline in Figure 17.2b.

It is important to note that multiple smaller tasks can be grouped together in one big main-task. These main-tasks shall then be completed according to the same process, without the need to undergo the full process for each subtask.

17.2.3. Time tracking

Time tracking will be done with clockify. A free to use time tracking tool that offers great flexibility and collaboration capabilities. The whole time sheet shall not be included in the public release of the project. If you want to access it nevertheless, you can contact our SCRUM master and he will send you the requested data.

17.2.4. Review process for releases

The review Process will be performed according to the schema outlined in Figure 17.2c.

All work being done which is relevant to the product is conducted on the SecureRole/-Content repository, whereas all work on the documentation of the thesis is done on the SecureRole/Documentation repository. The procedures are then identical for both repositories (with small exceptions regarding the publishing of content, you can see the differences by comparing Figure 17.3 with Figure 17.4).

The Dev branch is our main branch of work, we merge all of our feature branches into it. At the end of each sprint, when we merged all branches into the Dev branch, we will proceed to merge the Dev into the Main branch. That means each “sprint release” will be mirrored to the Main branch. The SCRUM master will then create a tag to clearly mark the time in which all branches relevant to the tagged sprint had been merged.

There is a publish branch in the SecureRole/Content repository. All important documents which shall be uploaded to the GitHub page are merged into the publish branch at the end of the sprint.

Only when everything has been correctly released to the Publish branch, it can be considered for the public release to the GitHub page.

17.2.5. Branch structure

To have a good overview over what is currently being worked on, we require a strict branch structure. We have two main modes of editing files. You can find an overview in the Table 17.2 and in the Figure 17.1.

Branch	Description	Examples
Directly in the Dev branch	Minor changes to files	Meeting Minutes
`feature/feature_name`	For all features not belonging directly to a topic for which content is being generated. The feature name shall be written in snake case.	Use Cases, Risk analysis
`refactoring/feature_name`	For all refactorings (Aka improvements of the files without big content changes)	all files

Table 17.2.: The branch structure we strive to achieve

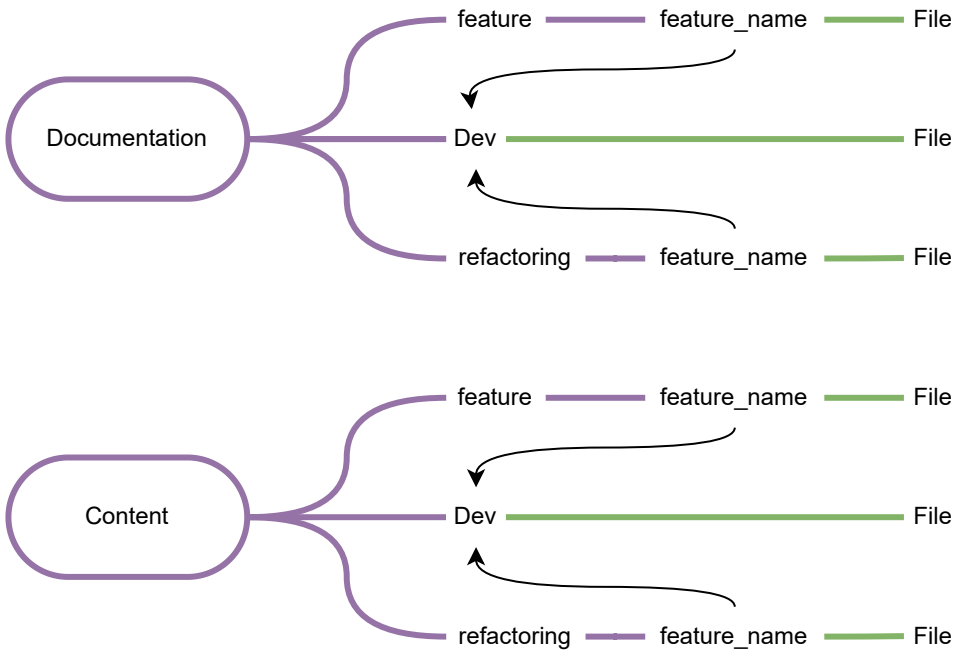


Figure 17.1.: The branch structure we strive to achieve

17.3. Testing

Due to our main goal being the creation of educational material for clients, our main priority will be to create user friendly content.

But what exactly is user friendly content? User friendly content, lives up to our functional and non functional requirements. This will change during the course of the project, due to us getting customer feedback and refining those requirements.

Our customers and thus our test groups will play a key role in defining the word “user friendly” for our project. This can only be achieved with continuous testing, which we aim to implement, starting as soon as possible. Included testing from an early stage, will help us to maintain our quality and achieve improved results. Our testing efforts are recorded in Table 17.3

Run	Date	Description
Alpha Testing	7.4.2022	Alpha testing for user feedback
Acceptance testing	25.05.2022	Acceptance testing for final feedback

Table 17.3.: Testing schedule

Testing can be achieved with different techniques. While we cannot use all of them, we want to show the ones we considered below:

17.3.1. Usability testing

Usability testing will be performed with volunteers suiting our target audience. They will include, but are not limited to:

- Design and clarity of educational material
- Clarity of exercises
- Quality of solutions

17.3.2. Continuous Testing

Due to the fact that testing and continuous feedback is an important aspect of our thesis, we would like to include continuous testing into our testing strategy. This will be achieved by creating a large enough group of testers which will then be requested to examine and provide feedback for our documents.

This allows us to draw up some sort of soft testing metric, which we can use to see if we are heading in the right direction.

17.3.3. Correctness of content Testing

The correctness of the content of our exercises will be assessed by our bachelor thesis advisor and our technical reviewer. If they should find any issues within our work, they will let us know and we will initiate an issue.

17.3.4. Relevance Testing

We will ask our internal and external collaborators to review our main releases, and give us feedback if the provided material is relevant to their classes and courses.

We will furthermore ask them to provide specific feedback if their expectations, which were determined during the requirements engineering phase, were met.

If one of these two reviews results in negative feedback, we will include it in an issue, trying to initiate the needed changes.

17.3.5. Hallway testing

We will show our test group some early drafts of our work and ask them to rate it in different aspects. Regarding readability, visible appeal, technical depth, etc. This will give us early feedback if we are heading in the correct direction.

We were unable to perform hallway testing during our thesis, due to time constraints and the nature of our product not being easily adaptable for hallway testing.

17.3.6. Legal disclaimer

Due to this project striving to be an open source repository for course material for schools, companies and individuals we need to protect it with a license. This will ensure that all contents will remain available free of charge to anyone who wants to use it.

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. This material may be used freely by public schools for educational purposes. This is the only agreeable exemption from the non commercial restrictions.

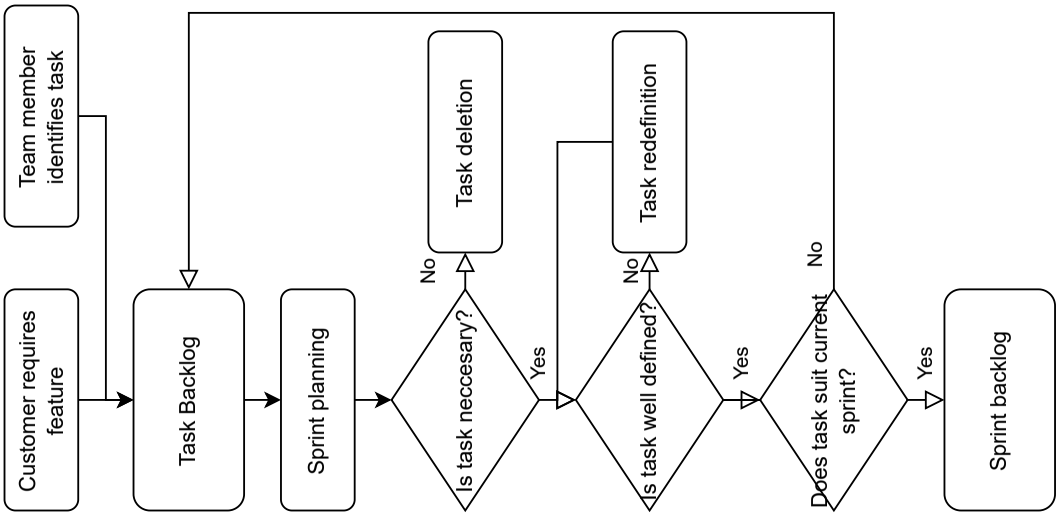
17.3.7. Errors in the course material

Even though we strive for a high level of quality through the measures outlined in this documents, errors can occur. We do not claim this work is error free and take no responsibility for errors included in our work.

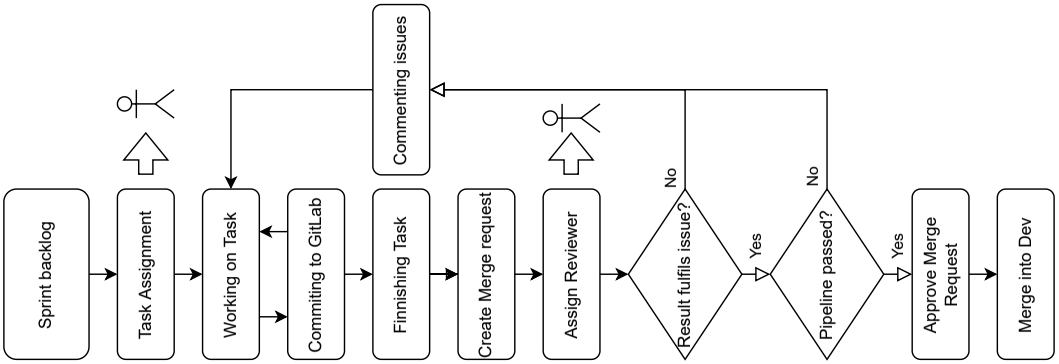
If you spot a mistake, we would be incredibly grateful if you reach out to us. You can either do this by e-mail to secure_role@outlook.com, or you can open a feature

request on our public github page which is located right here.

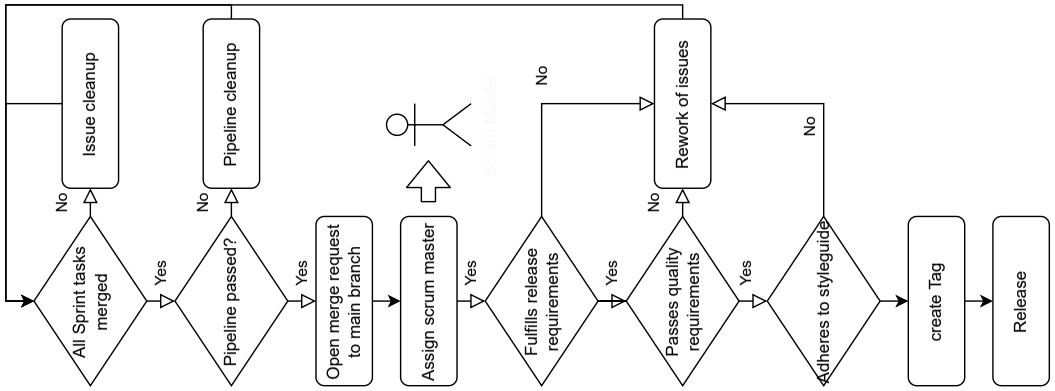
Thank you for your participation.



(a) Selection process



(b) Completion process



(c) Release process

Figure 17.2.: Process charts

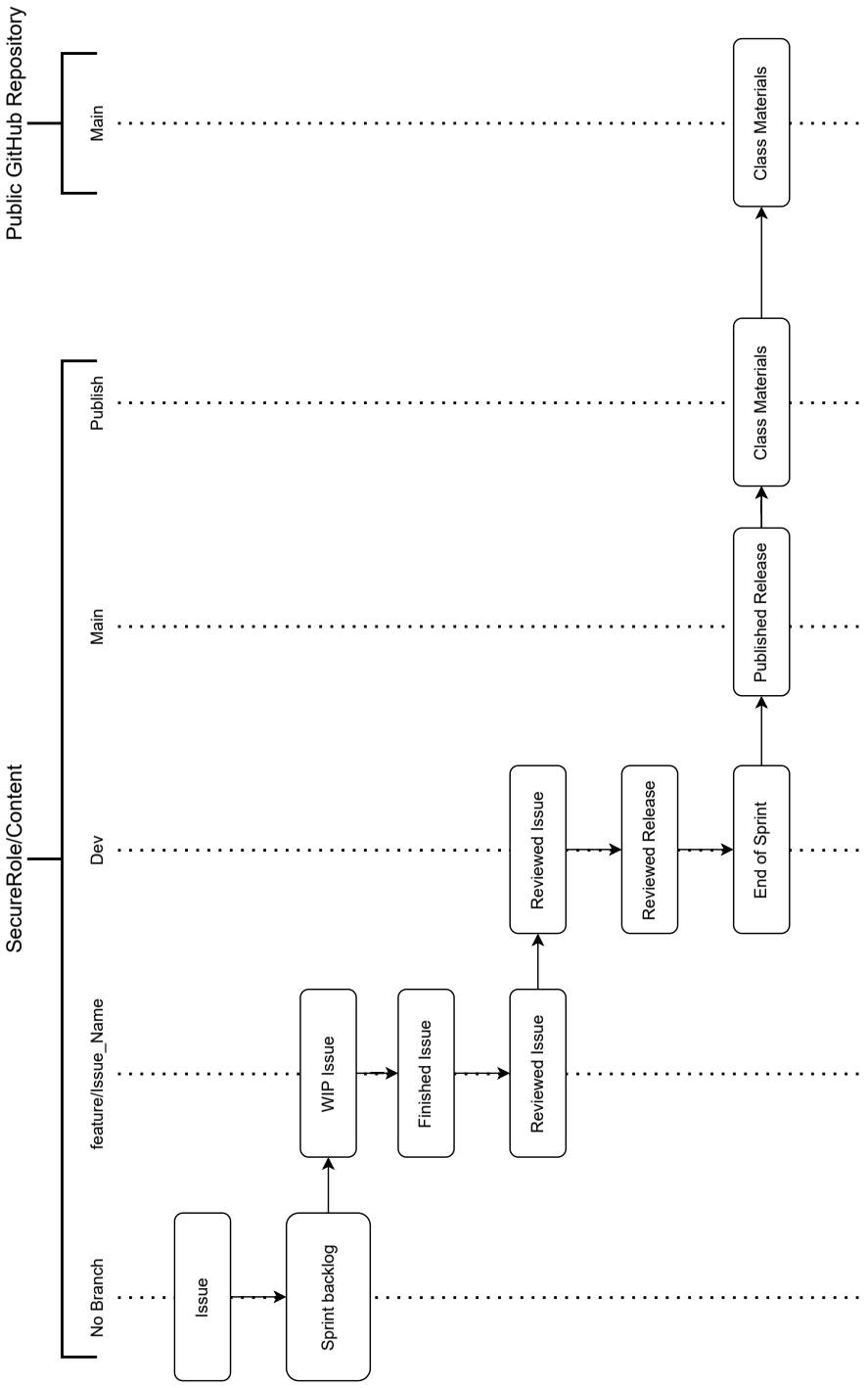


Figure 17.3.: The GitLab Workflow for the content

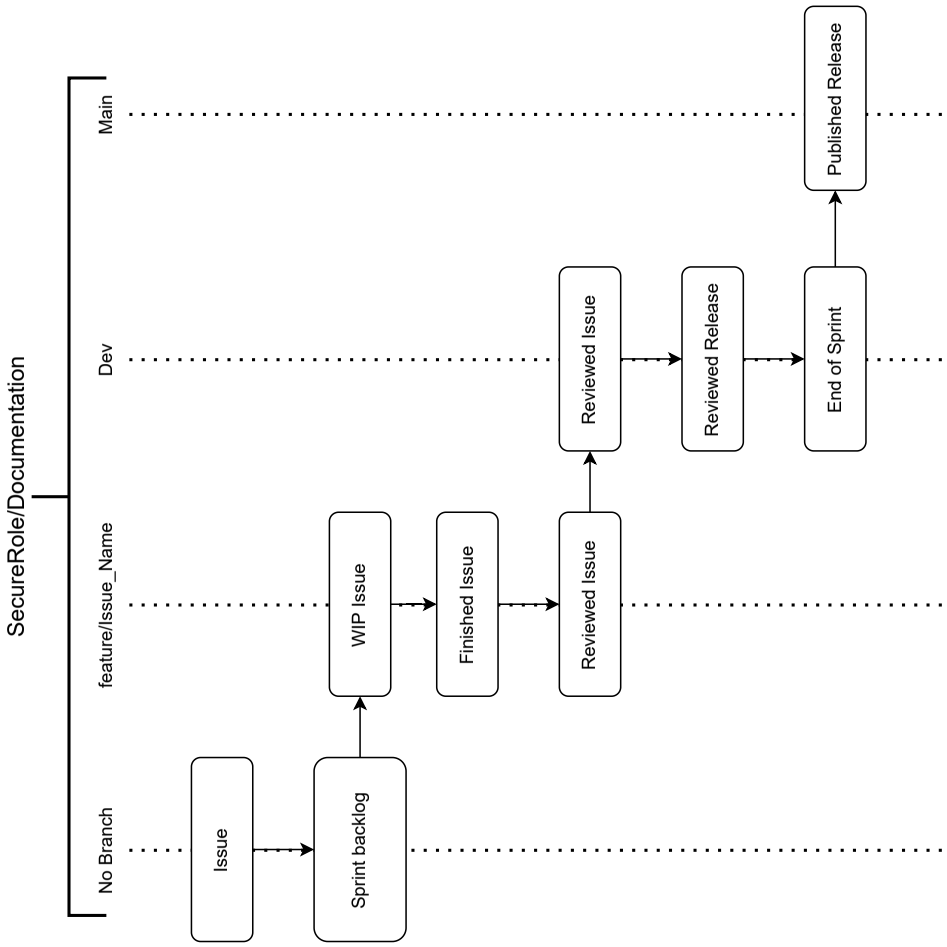


Figure 17.4.: The GitLab Workflow for the documentation

18. Quality Assurance Flavors

18.1. Introduction

Up until now our quality assurance, while being agile and always staying up to date, had little to do with the way we created content. It mainly showed the different ways we went about processes and guidelines. This will change now.

We feel, that with the introduction of SecureRole Flavors, it is at the time to introduce regulations on how content is created into our quality assurance files. We want to establish clear guidelines on how content must be structured and maintained to meet our aspiration of providing a package-like framework, as known from systems like npm.

Everything needs to be interchangeable!

This should be one of the main things to keep in mind when creating new flavors. All flavors **in the same category** need to be interchangeable. They need to be created in such a way that they can be easily swapped with another flavor without necessitating changes to the files. Only a change to the main file should suffice.

18.2. Content is king!

We will keep our main mantra intact. Solid content is the most important thing for SecureRole, this will not change with the introduction of Flavors. All quality measures regarding reviews, merges and publications remain the same as they have before. So please refer to the previous chapter.

18.3. Clean division of topics

When introducing flavors, it is important that all topics are self-contained to avoid issues during mixing them. So there will be no more mixed topics such as “MalwarePhish” but clean separations into “Phishing” and “Malware”.

18.4. Division of files

As a consequence they need to be divided into separate subfiles. This applies to all files for a topic.

A flavor needs the following files to be considered complete:

- Description of scenario (for GM document)
- Learning goals (for the role descriptions)
- Learning goals (for the GM document)
- Scenario description (for GM document)
- Storyboard (in miro)

A flavor can contain the following files additionaly:

- File with additional content
- Script
- Slides

18.5. Everything is a package!

All newly created flavors need to come as a package. There are no “combined topics”, no “quick additions”, nothing of the sort. Flavors has already reduced the time it takes to introduced a new topic. So to ensure the quality and integrity of Flavors, anything new introduced into SecureRole must be considered as a package, a flavor.

19. Use Cases

19.1. Introduction

This chapter contains all identified use cases, in their different forms (brief, casual, fully dressed). They directly reference functional requirements, which will be marked with an R and a number, indicating which functional requirement they reference.

19.2. Overview

This file contains all identified use cases, in their different forms (brief, casual, fully dressed). They directly reference functional requirements, which will be marked with an R and a number, indicating which functional requirement they refer to.

The Figure 19.1 gives an overview of th use cases.

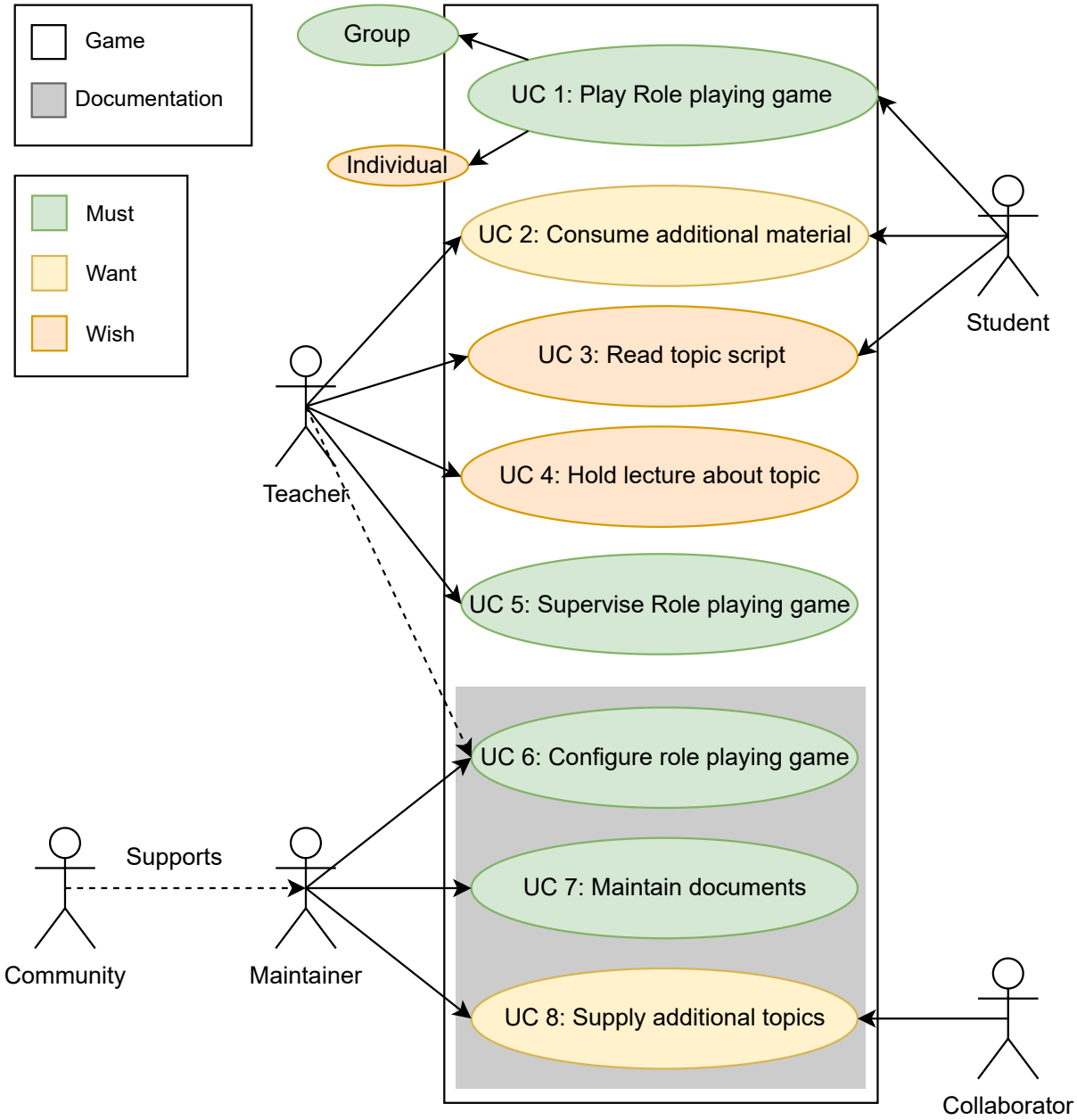


Figure 19.1.: The use case diagram

19.3. Brief

19.3.1. UC 1.2: Playing role playing game individually

Main Actor: Student

Main Success Scenario: The user receives instructions from our github page, on how he can play the role playing game individually.

Success Guarantee: We will put a tag on certain role playing games, which allow to be played by a single individual. They will then include specific instructions in case a student wants to play it by themselves.

Alternative Scenario: The role playing game does not contain such a tag, und thus can only be played in a group. The student can nevertheless consume the script and additional material, should it be available.

19.3.2. UC 4: Hold lecture about topic

Main Actor: Teacher

Main Success Scenario: The teacher can look up a topic they want to teach and find all the information and materials they need to create a lecture.

Success Guarantee: We will host an array of information and finished slides, which assists the teacher on our GitHub. The slides should be in a presentable state, to be used in class. We will provide them in a PDF format.

Alternative Scenario: If there are no finished slides, the teacher will need to construct them himself from the script and additional material. We will structure our content so that it can be used to create slides.

19.3.3. UC 8: Supply additional topics

Main Actor: Collaborator, (Maintainer)

Main Success Scenario: Our Collaborators can supply their own topics, which they want us to cover, via feature requests or e-mail.

Success Guarantee: We will ensure to openly communicate with our collaborators. This includes replies to feature requests and a evaluation if their wishes are possible.

All topics, regardless of current priority, are collected in a Kanban board where we have an overview of which phase they are currently in. You can find this Kanban board right here.

New topics can be requested via a new feature request or via e-mail.

Alternative Scenario: They will need to supply their wishes once our bachelor thesis has concluded, and we will tackle their possible wishes at a later point in time.

Alternative Scenario:

19.4. Casual

19.4.1. UC 1.1: Playing role-playing game in a group

Main Actor: Student, Teacher

Stakeholders and Interests:

Student: Wants to learn more about cybersecurity and incident response. The student is interested in a deviation from the norm during the exercises. An interactive game increases his interest in completing the exercise.

Teacher: Teach students about cybersecurity and incident response in an interactive way. The teacher can also gauge how well the students know the topic depending on their interaction with it and their confidence level.

Main Success Scenario:

Student: The students receive their character sheets from their professor for the session. They are provided with the following information:

- Name of their character.
- Position in the company.
- Short role description.
- Knowledge of events during the session.

Success Guarantee:

We provide the necessary course materials on our github page for anyone to download. This includes the character sheets for the students and the game master playbook for the professor.

Alternative Scenario:

The users can download the character sheets themselves, without the need for a professor handing them out to them. Students can then either decide to play the game without instructions and take a look at the guide if they get stuck, or appoint a student to be the game master.

19.4.2. UC 2 Consume additional material

Main Actor: Student

Stakeholders and Interests:

Student: Wants to learn more about the topic. Either through classical means such as texts, or if the student prefers other media, through video and audio.

Teacher: Wants their students to learn more about the topic in self study.

Main Success Scenario:

All topics are grouped into separate packages. Those packages contain a folder with an “Additional content” file, which servers as a reference sheet on where to find additional content for the regarding topic.

The file provides information on what media is relevant to which part of the topic and how it can increase the learning effect of the participants. While we do provide some additional materials ourselves (see subsection 19.4.3 as an example), most of the additional material comes from external sources. That means we will simply provide a hyperlink to the content. There is no need for a bibliography, as all content is already provided as hyperlinks.

Success Guarantee:

We will host additional material alongside the course materials on our GitHub page. This can contain but is not limited to:

- News Articles
- CVE’s
- Educational videos
- Book references or recommendations
- Podcasts
- Conference Talks

Quality Assurance:

The content must be reviewed by the SecureRole team before it is saved to the file, as any dissatisfaction the customer may have with the linked content will reflect directly on SecureRole, as we recommended it. It should be clear that it is not the SecureRole team’s job to spend hours consuming content just to make sure it is flawless for our customers. However, the SecureRole team must select well-known platforms with strict community guidelines or review content from unknown platforms to ensure quality.

The file contains metadata for the additional content, such as the type of media, publisher, and estimated time required for interaction.

Alternative Scenario:

Should there not be any additional content for a topic, it will not contain a folder with the same name. Also, the project will not receive the “additional content” tag in the overview table. These should suffice as indicators that this topic has no additional

content.

19.4.3. UC 3: Read topic script

Main Actor: Student

Stakeholders and Interests:

Student: Wants to have a comprehensive overlook regarding the topic.

Teacher: Wants their students to learn more about the topic in self study.

Main Success Scenario:

Topics which are added to our github page can contain a script. The script is a text that helps the student understand more about a topic.

Success Guarantee:

We will host the script alongside the course materials on our GitHub page. The script will contain a text, describing the topic in detail and guiding the students through the most important aspects of it.

The most important aspects are defined as all technical knowledge needed to fully understand the attack to have a deeper insight into it. While this can vary from topic to topic, we will leave the exact grade of detail up to the author.

Alternative Scenario:

There will be a comment, which states that no script has been added to this role playing game.AI Also, the project will not receive the “script” tag in the overview table.

19.4.4. UC 5: Supervising role playing game

Main Actor:

Teacher

Main Success Scenario:

The teacher can download a clear instruction for the role playing game from our GitHub page.

Stakeholders and Interests:

Teacher: Wants a clear and comprehensive instruction on how to supervise the role playing game.

Preconditions:

The teacher knows which game he would like to play and has found the right link to

the game master document.

Success Guarantee:

We will provide such a playbook on our GitHub page, accessible for everyone. It supports the teacher in directing the play and give him an concise overview over all available information and the possible steps to drive the narrative along. It also contains clues about important turning points in the narrative, and provides aid, in case the students get stuck at the intended decision points of the story.

Main Success Scenario (or Basic Flow):

1. The teacher knows which game he wants to play
2. He opens up the github page of SecureRole
3. He selects the correct entry in the table
4. He downloads the document
5. He can then read it and prepare for the game
6. He supervises the game and gets supported by the game master document

Alternative Scenario:

None.

Frequency of Occurrence:

Whenever the teacher wants to play a game. So once per semester.

Open Issues:

No issues identified yet.

19.4.5. UC 6: Configure role playing game

Main Actor: Teacher

Stakeholders and Interests:

Teacher: Can mix and match the desired topics to create his own personal role-playing game.

Maintainer: Can create reconfigured games for the convenience of the teacher.

Preconditions:

1. The documents have been create in such a way that they allow to be mixed.
2. The teacher or maintainer has access to an easy way to mix and match the documents

Main Success Scenario: The role playing game is written in such a way that it can be adapted to the needs of teacher. This includes but is not limited to aspects such as:

- Player count
- Role distribution
- Play duration
- Topics
- etc. . .

Success Guarantee: The role-playing games are written in such a way that certain elements remain flexible and the distribution of roles can be changed without making the game unplayable.

Main Success Scenario (or Basic Flow):

1. User wants to configure game
2. They go to our webpage and check which topics we have in stock
3. They choose the desired topics
4. They now need to create their own latex document which contains the desired topic parts

Alternative Scenario:

This is difficult to accomplish if the user is not familiar with the project structure. Therefore, maintainers provide pre-made documents until a tool is available to mix and match the files for the user.

Frequency of Occurrence:

Maintainer: Rarely, only to create new prefabricated games.

Teacher: Regularly, probably not every time he wants to play a game, but every time he wants to change the game or adapt it. Could be once in a year, could be more.

Open Issues:

We currently do not have the technical framework to support mixing and matching of our topics. Maintainers can do it fairly easily, when they are fluent in LaTeX and know the document structure. For teachers, it is far more complicated, since they don't know the document structure. It would be necessary to create a tool which aids them to create their desired game.

19.4.6. UC 7: Maintain documents

Main Actor: Maintainer, (Community)

Stakeholders and Interests:

Maintainer: Wants to maintain the documents, for the to stay relevant and up-to-date.

Community: Wants to help keep content relevant and accurate for them.

Preconditions:

The documents are publicly accessible so they can be changed. And a change process has to be implemented to assure quality control for all future topics.

Main Success Scenario: Contributors and a possible community can keep maintaining the project after the conclusion of our bachelor thesis.

Success Guarantee: We will set up the project so that once the bachelor's thesis is complete, it will allow us to work independently on future features without the need for the GitLab project. All finished topics will be uploaded to our public git repository. This is to ensure that they are openly accessible and maintainable.

Main Success Scenario (or Basic Flow):

1. A contributor picks a new topic to create or an existing one to change
2. He opens a change request
3. He then starts working on the topic
4. He opens a merge request for his newly created content
5. His content will be accepted or denied dependent if it meets the quality guidelines
6. We will also provide a release history, in which we show the changes between releases and present our newest additions for each release.

Alternative Scenario:

This is hard to do when the user is not familiar with the project structure. Therefore, maintainers provide pre-made documents until a tool is available to mix and match the files for the user.

Frequency of Occurrence:

Maintainer: Rarely, only to create new prefabricated games.

Teacher: Regularly, probably not every time he wants to play a game, but every time he wants to change the game or adapt it. Could be once in a year, could be more.

Open Issues:

- We need a release history
- We need a change process
- We need a merge request

19.5. Fully dressed

19.5.1. UC 1: Playing role-playing game

Main Actor:

Teacher

Stakeholders and Interests:

Teacher: The teacher wants to play the game with his students to create an engaging exercise for them.

Students: Want to play a game with their teacher, to have an educational exercise session.

Preconditions:

The teacher knows which game he wants to play.

Main Success Scenario:

The students or professor are able to pick the correct role-playing game for the current lecture content. They can then enact the role playing game, with as much guidance as needed from the professor.

Success Guarantee:

The role playing game will be published on the github page. It can be downloaded by anyone.

A summary table that is available on the public github README page, shows which topics are available. That table also contains information such as: name, length, number of players, required time, topic, target audience.

General:

We will divide the documentation into categories. These categories indicate what material is contained within the file. Role playing material, supporting material, script, slides.

It is furthermore divided into specific topics such as Malware, Phishing, Social Engineering, etc. . . .

Game medium:

The game will be provided in PDF form on our github page. It is akin to a “classical” role-playing game being enacted in a classroom. Meaning every participant gets a character sheet with his role to play before they enact the role-playing game together.

The teacher can download all necessary character sheets from our github repository. This allows him to plan the role playing game. He receives a special document which contains:

- All character sheets for the students.
- Additional roles, designated for the teacher (such as law enforcement, external company, etc. . .)
- A storyboard which shows him the rough planned storyline for the whole role playing game.
- An “additional information” section, which informs him about anything he needs to know to guide the session.

Player goal:

The role playing game will contain these aspects as the main player goals:

- Detection
- Containment
- Recovery

Detection entails that the participants realize that they are dealing with a threat.

Containment entails that the participants need to uncover the nature of the full incident. The teacher who has the playbook knows the full extent of the threat and therefore can guide the students in this process. The storyboard contains critical steps in the containment process, such as events, hints and also time based consequences, should the students fail to address important containment strategies.

Recovery is also a phase in the role playing game. Students must restore the system as best they can. The moment the system is back to its original configuration is the end of the role-playing game and marks the goal.

Player engagement:

The player will be kept engaged in the game by providing him with choices, which will have consequences. Meaning some choices the player takes lead to better and some to worse outcomes of the current situations. But the game always ends with the same goal, which is to eradicate the threat and restore the system to its previous state.

The game will try to be as close as possible to a real world scenario, to make it realistic. That means we will create a fake organization, with a fake org-chart that mimics a company. This will be provided to the teacher in the game master document.

Our first role-playing game will be a group game. Thus, we have updated UC 1.1 in subsection 19.4.1 in accordance to this to reflect the chosen direction of development.

Main Success Scenario (or Basic Flow):

1. The teacher checks the github page which topics are interesting for him
2. He either chooses a prefabricated one or creates on for himself (see subsection 19.4.5)

3. He downloads all the content which he needs to play the game (the game master manual and the character sheets)
4. He distributes the files among the students and explains the situation
5. The players engage in the game
6. After the game is concluded, the teacher and the students discuss their learnings

Extensions (or Alternative Flows):

No alternative flows yet.

Special Requirements:

- Github needs to be setup properly.

Technology and Data Variations List:

- Files are in pdf format

Frequency of Occurrence:

Regularly, this is our main use case. It happens the most frequent, but is still dependent on how many times the teacher chooses to use our game. Probably once per semester.

Open Issues:

- Currently no known issues

20. Non-Functional Requirements

The non-functional requirements were made with the help of ISO 25010 as a reference.

Figure 20.1.: ISO 25010

20.1. NFR 1 Functional Suitability

NFR 1.1 Functional completeness

NFR1.1.1 The story packages can be chained together to create a new story.

NFR1.1.2 The story packages are created according to the Quality Assurance.

NFR1.1.1 The story packages slide can be used for exercises or lessons.

NFR 1.2 Functional correctness

NFR 1.2.1 The story packages are grammatically correct.

NFR 1.2.3 The story packages slides contains elements from the scripts.

NFR 1.3 Functional appropriateness

NFR 1.3.1 The story packages are preapred to conduct a role-playing game by the participants.

NFR 1.3.2 The story packages are created with the use-cases in mind.

20.2. NFR 2 Performance efficiency

NFR 2.1 Time behavior

NFR 2.1.1 The predefined stories can be played in less than 90 min.

NFR 2.2 Resource utilization

NFR 2.2.1 The predefined story can be played with one game master.

NFR 2.3 Capacity

NFR 2.3.1 The predefined stories can be played with more than two players.

20.3. NFR 3 Compatibility

NFR 3.1 Co-existence

NFR 3.1.1 Story packages of different categories can be chained together.

NFR 3.1.2 Story packages of the same category need to be interchangeable to be used in the role-playing games.

20.4. NFR 4 Usability

NFR 4.2 Learnability

NFR 4.2.1 The character sheets give the players the ability to be prepared for the role play.

NFR 4.2.1 The game master can conduct the role-playing game by reading the game master document.

NFR 4.3 Operability

NFR 4.3.1 The game master can conduct the role-playing game without external material.

NFR 4.4 User error protection

NFR 4.4.1 The game master document contains helpful information to reduce errors during the game.

NFR 4.4.2 Goals are given to the players before the game starts, to ensure the game is played in the right direction and the goals are achieved in the best way possible.

20.5. NFR 5 Reliability

NFR 5.1 Maturity

NFR 5.1.1 The game gives the user a path to follow during the game.

NFR 5.1.2 The game master has a path to follow during the game.

20.6. NFR 6 Maintainability

NFR 6.1 Modularity

NFR 6.1.1 A story package isn't dependent other story packages.

NFR 6.2 Reusability

NFR 6.2.1 The game creator can combine different story packages to create a new story.

NFR 6.3 Modifiability

NFR 6.3.1 The creation of new stories is possible with the use of the predefined packages.

20.7. NFR 7 Portability

NFR 7.1 Adaptability

NFR 7.1.1 The simulation can be conducted on-site or online.

21. Risk Management

This chapter provides an overview of the high-level and low-level risks that may be encountered in this project. It will be updated in the coming weeks as low-level risks and new, unidentified risks may emerge over time.

The project has a weighed risk of 49.4 h

21.1. Risk analysis at inception phase

At the beginning of the inception phase, i.e., at the start of the project, a risk analysis is performed. Since the scope of the project and the cost estimates are only roughly defined, the probability of occurrence of the risks and the maximum possible damage may not be very reliable. Therefore, risk management is reassessed during the construction phase, and kept up to date throughout the project.

21.2. Risks

Table 21.1.: Risks as created during the inception phase

ID	Description	maximal Damage [h]	Probability of occurrence [%]	Weighted Damage	Prevention	Behaviour on occurrence
R1	Requirements or tasks that need to be implemented may not be defined properly or at all. This may lead to more work at a later time.	35	30	10.5	Formulate requirements at the appropriate level of generality; Discuss with the group about the requirements that are already fulfilled and those that are planned for the next sprint	Define additional alternative requirements and try to complete them in time.
R2	The complexity of a work package might be unknown, so low time estimate is given for a task when more time is needed to complete it.	20	30	6	Try to research the topic in advance to get a better idea of the complexity of the task.	If a task requires more time than estimated, group members can use this experience to improve their estimates.
R3	Unfamiliar technologies	20	20	4	Try to select technologies that team members are already familiar with. If you choose an unfamiliar technology, try to acquire the knowledge as quickly as possible.	Ask for help outside the group or choose alternative technologies that are familiar to the group.

Continued on next page

Table 21.1 – continued from previous page

ID	Description	maximal Damage [h]	Probability of occurrence [%]	Weighted Damage	Prevention	Behaviour on occurrence
R4	Features that are marked as MVP and have higher priority cannot be implemented due to lack of time or complexity of the feature	30	30	9	Mark necessary features as part of the MVP and work on them with priority. If they are too complicated, break them into smaller tasks.	Define additional alternative requirements
R5	Implementing the CI/CD pipeline takes more time than necessary or may not be implemented at all.	17	30	5.1	Work is often integrated from the beginning of the project.	Ask for external help
R6	Communication has stalled due to unforeseen problems.	18	10	1.8	Schedule regular meetings with the team and also with the supervisor.	Change the meeting schedule, make more frequent meetings so that the team can communicate better.
R7	Lack of external collaborators.	25	10	2.5	Collaborators are contacted in the early stages of the project to avoid any problems	Team members are focused on creating a project that is primarily useful to OST and then to other collaborators/schools.

Continued on next page

Table 21.1 – continued from previous page

ID	Description	maximal Damage [h]	Probability of occurrence [%]	Weighted Damage	Prevention	Behaviour on occurrence
R8	Either one of the team members or the supervisor becomes ill and is unable to attend meetings and complete certain tasks.	25	40	10	-	Discuss alternative solutions: if a task cannot be completed on time: extend the deadline; if meetings cannot be attended: reschedule meetings
R9	Unavailability of the main repository.	5	10	0.5	Each team member has a local copy of the project from GitLab. Part of the project is also additionally stored on GitHub	If the project or documentation is lost, team members upload their local versions.

End of Table

21.3. Risk Analysis Matrix

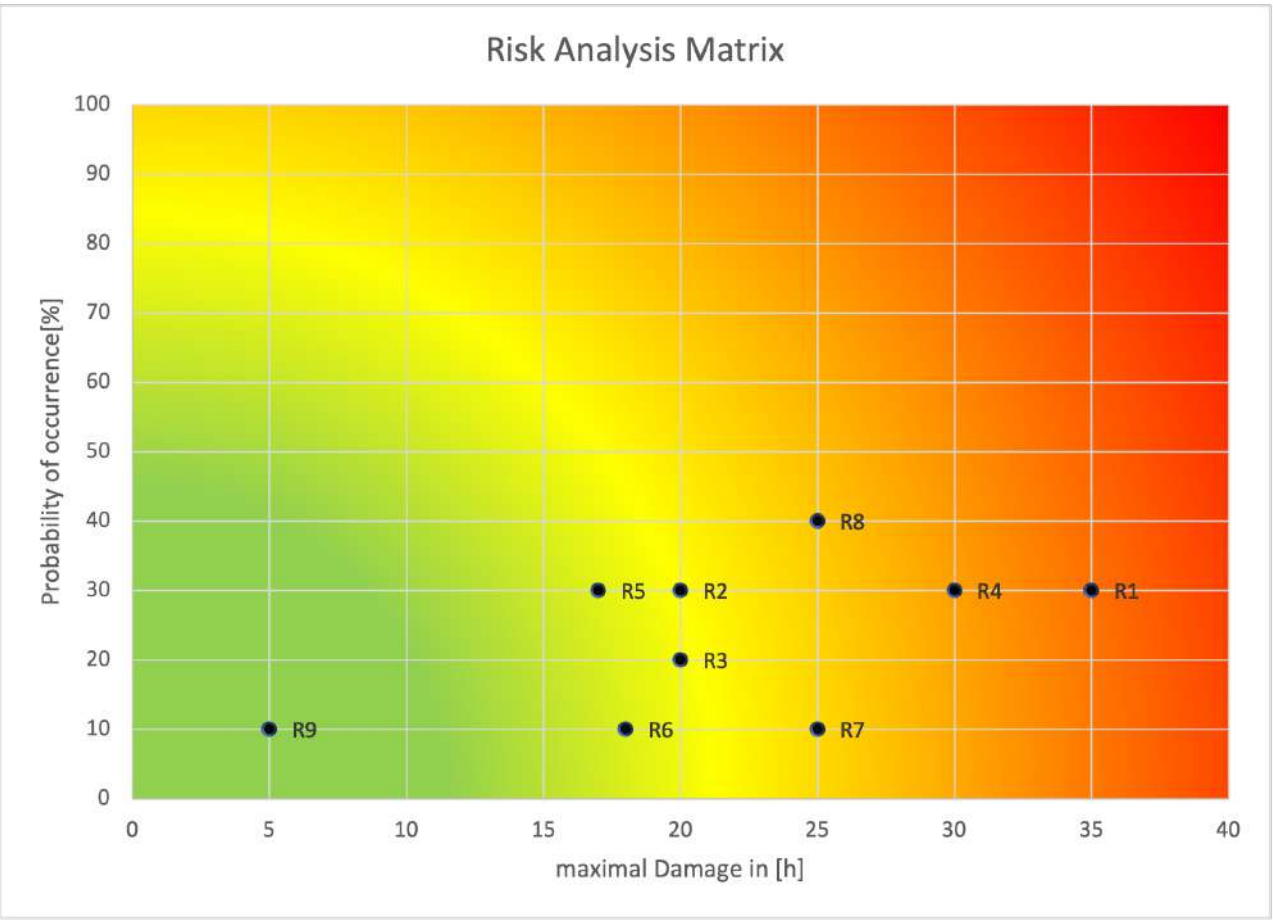


Figure 21.1.: Risk Analysis Matrix

21.4. Risk analysis at construction phase

Project risks are reassessed in the construction phase, when the scope and estimates of the project are better known.

21.5. Risks

Table 21.2.: Risks revisited during the construction phase

ID	Description	maximal Damage [h]	Probability of occurrence [%]	Weighted Damage	Prevention	Behaviour on occurrence
R1	Requirements or tasks that need to be implemented may not be defined properly or at all. This may lead to more work in a later time.	15	15	2.25	Formulate requirements at the appropriate level of generality; Discuss with the group about the requirements that are already fulfilled and those that are planned for the next sprint	Define additional alternative requirements and try to complete them in time.
R2	The complexity of a work package might be unknown, so low time estimate is given for a task when more time is needed to complete it.	10	20	2	Try to research the topic in advance to get a better idea of the complexity of the task.	If a task requires more time than estimated, group members can use this experience to improve their estimates.
R3	Unfamiliar technologies	10	10	1	Try to select technologies that team members are already familiar with. If an unfamiliar technology is choosen, try to acquire the knowledge as quickly as possible.	Ask for help outside the group or choose alternative technologies that are familiar to the group.

Continued on next page

Table 21.2 – continued from previous page

ID	Description	maximal Damage [h]	Probability of occurrence [%]	Weighted Damage	Prevention	Behaviour on occurrence
R4	Features that are marked as MVP and have higher priority cannot implemented due to lack of time or complexity of the feature	20	20	4	Mark necessary features as part of the MVP and work on them with priority. If they are too complicated, break them into smaller tasks.	Define additional alternative requirements
R5	Implementing the CI/CD pipeline takes more time than necessary or may not be implemented at all.	5	20	1	Work is often integrated from the beginning of the project.	Ask for external help
R6	Communication has stalled due to unforeseen problems.	5	10	0.5	Schedule regular meetings with the team and also with the supervisor.	Change the meeting schedule, make more frequent meetings so that the team can communicate better.
R7	Lack of external collaborators.	-	-	-	Collaborators are contacted in the early stages of the project to avoid any problems	Team members are focused on creating a project that is primarily useful to OST and then to other collaborators/schools.

Continued on next page

Table 21.2 – continued from previous page

ID	Description	maximal Damage [h]	Probability of occurrence [%]	Weighted Damage	Prevention	Behaviour on occurrence
R8	Either one of the team members or the supervisor becomes ill and is unable to attend meetings and complete certain tasks.	20	30	6	-	Discuss alternative solutions: if a task cannot be completed on time: extend the deadline; if meetings cannot be attended: reschedule meetings
R9	Unavailability of the main repository.	5	20	1	Each team member has a local copy of the project from GitLab. Part of the project is also additionally stored on GitHub	If the project or documentation is lost, team members upload their local versions.

End of Table

21.6. Risk Analysis Matrix

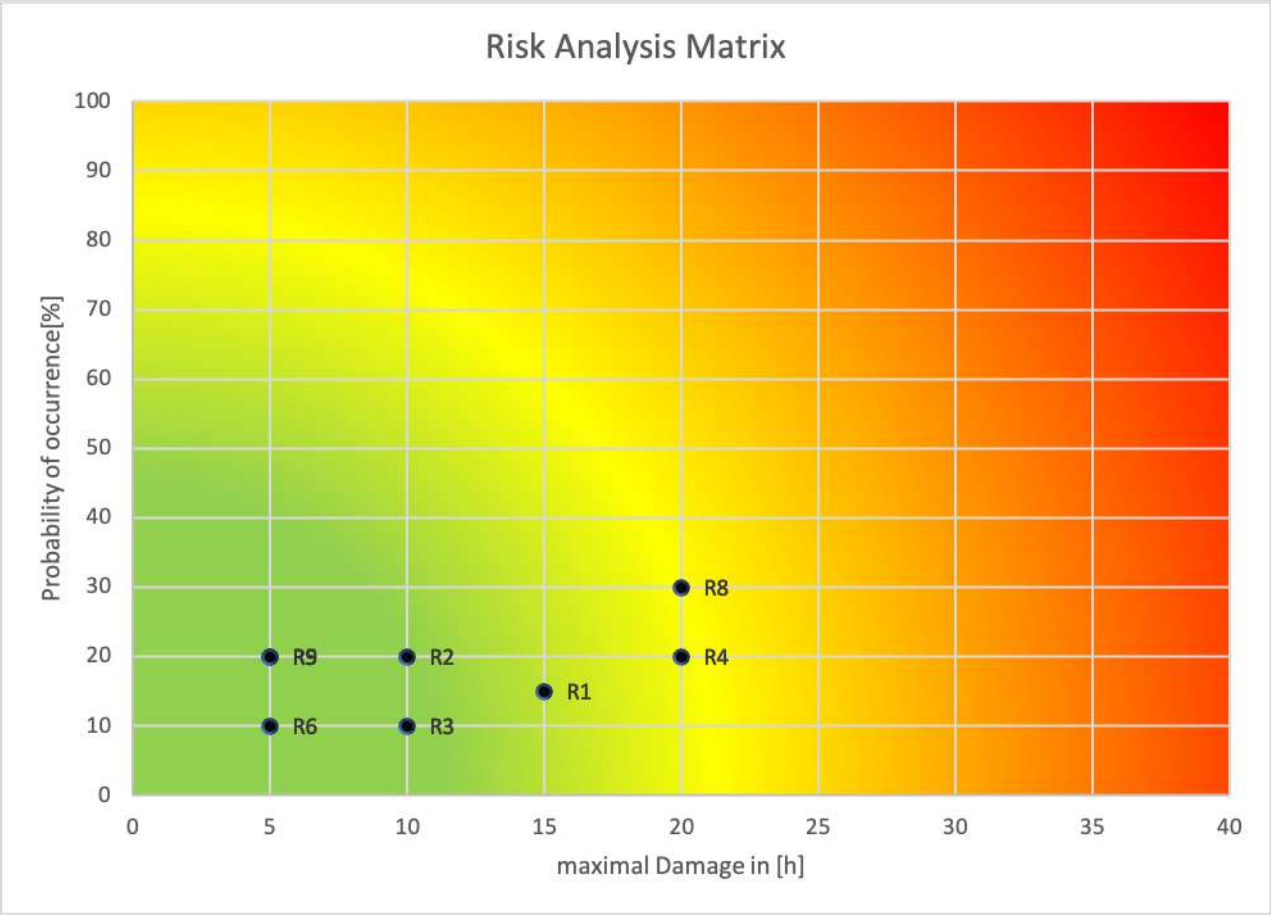


Figure 21.2.: Risk Analysis Matrix - Updated

21.7. Reasons for updates

The weighted risk is now reduced from 49.4 to 17.75.
R1 - Up to this stage of the project, it has not occurred that a task has been defined incorrectly or not at all. Therefore, the risk of this happening in the future during the project is not as great as previously estimated.
R2 - So far, it has not happened that very low estimates have been given for a complex task, so that the probability of occurrence and the damage are not so high.
R3 - No new technologies have been introduced or used so far.
R4 - MVP is defined in the use cases and has a higher priority compared to the other features. Therefore, the team works continuously on higher priories and the probability that they cannot be implemented due to lack of time is not so high.
R5 - CI/CD is implemented early in the project, reducing this risk. No major problems have been encountered during implementation.
R6 - The risk of team communication faltering is also reduced by holding frequent meetings to discuss the important issues.
R7 - At this stage of the project, there are no estimates for this risk because collaborators have already been invited to be part of the project, and no collaborators have

agreed to participate in the project. The team's focus is on providing the content for OST.
R8 - This has already occurred, but the damage and the probability of occurrence are not as high as estimated at the beginning.
R9 - It has happened in some cases that the main repository in GitLab was unavailable due to maintenance, but the damage and the probability of occurrence is not as high as estimated at the beginning.

22. Personas

22.1. Introduction

In general, the users that will interact with our project are either IT students, professors, or employees working in the IT field. The material provided will be for educational purposes in the field of cybersecurity, presenting various attack scenarios as role-playing games with the goal of finding a mitigation to the attack, reducing the personal attack surface, and learning how to behave when being attacked.

22.2. Marie Meier

Age: 23
Occupation: Student
University: OST
Location: Rapperswil

> "It is critical to understand the importance of every step we take that can help improve the security of a system."

Personality

- Introvert
- Perceiving
- Organized

Figure 22.1.: Personas 1

Personal Goals:

- Gain knowledge about different types of attacks and their mitigations.
- Know how to behave when under attack and how to reduce personal attack surface area.
- Access to free educational materials.

Motivations

- Increase in knowledge
- Prepare for future job in cyber security

Frustrations

- Paying to access learning material.
- Spend a lot of time searching for good educational material.

22.3. Thomas Fischer

Age: 45
Occupation: Professor
University: OST
Location: Zürich

> "It takes so many years to build a reputation and only one negative incident to ruin it"

Personality

- Innovative
- Thoughtful
- Observant

Figure 22.2.: Personas 2

Personal Goals:

- Get learning materials for different types of attacks to help his students better understand the topics with the help of role plays, course slides, scripts, videos and much more

Motivations

- Receive good teaching materials for his classes
- Minimal effort to prepare for lectures and exercises

Frustrations

- Badly stuctured learning material
- Poor websites with unsufficient overview over topics and contents

22.4. Jakob Blenk

Age: 35
Occupation: IT security engineer
Location: Zug
Role: Collaborator

> “Two tips to remember: Never share your password with anyone and change it very often”

Personality

- Punctual
- Logical
- Self-Reliant

Personal Goals:

- Get good material for topics in cyber security for company training

Motivations

- Get good material on topics he requests
- Use material for IT staff training

Frustrations

- Poor websites that do not provide coherent information about security attacks

Figure 22.3.: Personas 3

22.5. Martin Müller

Age: 25
Occupation: IT security engineer
Location: St. Gallen
Role: Maintainer

> “IoT - security = Internet of Threats”

Personality

- Ambitious
- Patient
- Self-Disciplined

Personal Goals:

- Help developing good material on different topics of cyber security attacks
- Add his suggestions for different materials and topics

Motivations

- Get good material on material he requests
- Maintain and improve documents

Frustrations

- Bad websites that provide little good information about security attacks
- Poor learning materials that are not go maintained

Figure 22.4.: Personas 4

Part III.

Appendix

List of Figures

List of Tables

Bibliography

[1] H. Meyer, *Was ist guter Unterricht? Sonderausgabe mit 65 Min.-Vortrag (DVD)*, 1st ed. Berlin: Cornelsen Verl. Scriptor, 2004. [Online]. Available: https://swbplus.bsz-bw.de/bsz112601251rez.htm

[2] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, Erik Andersen, "What.hack: Engaging anti-phishing training through a role-playing phishing simulation game." [Online]. Available: https://www.cs.cornell.edu/~eland/papers/chi2019_whathack.pdf

[3] Patricia Armstrong, "Bloom's taxonomy," 2010. [Online]. Available: https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

Glossary

Pathfinder Pathfinder is (if put simply) a tabletop role-playing game akin to Dungeons and Dragons 61

Acronyms

BA Bachelorarbeit (Bachelor thesis) 79

CEO Chief Executive Officer 57, 59

CI/CD Continuos Integratio / Continuos Delivery 84

CSIRT Computer Security Incident Response Team 41, 42

DnD Dungeons and Dragons 61

DSA Das schwarze Auge (The black eye) . . . . . VIII, 23

GM Game Master . . 23, 36, 37, 39, 40, 41, 43, 44, 55, 57, 58, 59, 61, 62, 64, 65, 66, 67, 68, 72, 103

MVP Minimum Viable Product 36, 121, 125, 127

OS Operating System 18

OSINT Open Source Intelligence 42, 43, 56, 57, 58

OST Ostschweizer Fachhochschule (Eastern University of Applied Sciences) . III, 54, 55, 73, 77, 86, 87, 91, 121, 125, 128, 129, 130

RPG Role-Playing Game . . . . . VIII, 22, 23, 76

SA Studienarbeit (Semester thesis) 79

SCM Source Code Management 86

UC Use Case 30

UDL Universal design learning 8

URL Infirom Resource Locator 25

US United States of America 24

VCS Version Control System 84

VM Virtual Machine 45